

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Д. С. Кулябов, А. В. Королькова

Основы администрирования операционных систем

Лабораторные работы

Учебное пособие

Москва

Российский университета дружбы народов

2018

УДК 004.051(075.8)
ББК 018.2*32.972.11
К 90

Утверждено
РИС Учёного совета
Российского университета
дружбы народов

Рецензенты:

доктор технических наук, профессор, начальник отдела УИТО и СТС РУДН
К. Е. Самуйлов
доцент, кандидат физико-математических наук, с.н.с. ЛИТ ОИЯИ О. И. Стрельцова

Кулябов, Д. С.
К90 Основы администрирования операционных систем: лабораторные работы :
учебное пособие / Д. С. Кулябов, А. В. Королькова. — Москва : РУДН,
2018. — 121 с. : ил.

Пособие рекомендуется для проведения лабораторных работ по курсу «Основы администрирования операционных систем» для направления 09.03.03 «Прикладная информатика».

УДК 004.451(075.8)
ББК 018.2*32.972.11

Оглавление

Лабораторная работа № 1. Установка и конфигурация операционной системы на виртуальную машину	6
1.1. Цель работы	6
1.2. Указания к работе	6
1.3. Последовательность выполнения работы	6
1.4. Домашнее задание	18
1.5. Содержание отчёта	18
1.6. Контрольные вопросы	19
Лабораторная работа № 2. Управление пользователями и группами	20
2.1. Цель работы	20
2.2. Предварительные сведения	20
2.3. Задание	24
2.4. Последовательность выполнения работы	24
2.5. Содержание отчёта	26
2.6. Контрольные вопросы	27
Лабораторная работа № 3. Настройка прав доступа	28
3.1. Цель работы	28
3.2. Задание	28
3.3. Последовательность выполнения работы	28
3.4. Содержание отчёта	31
3.5. Контрольные вопросы	31
Лабораторная работа № 4. Работа с программными пакетами	33
4.1. Цель работы	33
4.2. Предварительные сведения	33
4.3. Задание	37
4.4. Последовательность выполнения работы	37
4.5. Содержание отчёта	40
4.6. Контрольные вопросы	40
Лабораторная работа № 5. Управление системными службами.	42
5.1. Цель работы	42
5.2. Предварительные сведения	42
5.3. Задание	44
5.4. Последовательность выполнения работы	44
5.5. Содержание отчёта	47
5.6. Контрольные вопросы	47
Лабораторная работа № 6. Управление процессами	48
6.1. Цель работы	48
6.2. Предварительные сведения	48
6.3. Задание	50
6.4. Последовательность выполнения работы	50
6.5. Самостоятельная работа	51
6.6. Содержание отчёта	52
6.7. Контрольные вопросы	53

Лабораторная работа № 7. Управление журналами событий в системе .	54
7.1. Цель работы	54
7.2. Предварительные сведения	54
7.3. Задание	55
7.4. Последовательность выполнения работы	55
7.5. Содержание отчёта	58
7.6. Контрольные вопросы	58
Лабораторная работа № 8. Планировщики событий	60
8.1. Цель работы	60
8.2. Предварительные сведения	60
8.3. Задание	61
8.4. Последовательность выполнения работы	61
8.5. Содержание отчёта	62
8.6. Контрольные вопросы	62
Лабораторная работа № 9. Управление SELinux.	64
9.1. Цель работы	64
9.2. Предварительные сведения	64
9.3. Задание	65
9.4. Последовательность выполнения работы	66
9.5. Содержание отчёта	68
9.6. Контрольные вопросы	69
Лабораторная работа № 10. Основы работы с модулями ядра операционной системы	70
10.1. Цель работы	70
10.2. Предварительные сведения	70
10.3. Задание.	70
10.4. Последовательность выполнения работы	70
10.5. Содержание отчёта	71
10.6. Контрольные вопросы	72
Лабораторная работа № 11. Управление загрузкой системы.	73
11.1. Цель работы	73
11.2. Предварительные сведения	73
11.3. Задание.	73
11.4. Последовательность выполнения работы	73
11.5. Содержание отчёта	75
11.6. Контрольные вопросы	75
Лабораторная работа № 12. Настройки сети в Linux	77
12.1. Цель работы	77
12.2. Предварительные сведения	77
12.3. Задание.	79
12.4. Последовательность выполнения работы	79
12.5. Содержание отчёта	81
12.6. Контрольные вопросы	81
Лабораторная работа № 13. Фильтр пакетов	82
13.1. Цель работы	82
13.2. Предварительные сведения	82
13.3. Задание.	83
13.4. Последовательность выполнения работы	83
13.5. Самостоятельная работа	84
13.6. Содержание отчёта	84

13.7. Контрольные вопросы	85
-------------------------------------	----

Лабораторная работа № 14. Партиции, файловые системы, монтирование 86

14.1. Цель работы	86
14.2. Предварительные сведения	86
14.3. Задание.	86
14.4. Последовательность выполнения работы	87
14.5. Самостоятельная работа	91
14.6. Содержание отчёта	91
14.7. Контрольные вопросы	91

Лабораторная работа № 15. Управление логическими томами 93

15.1. Цель работы	93
15.2. Предварительные сведения	93
15.3. Задание.	94
15.4. Последовательность выполнения работы	95
15.5. Самостоятельная работа	96
15.6. Содержание отчёта	97
15.7. Контрольные вопросы	97

Лабораторная работа № 16. Программный RAID 98

16.1. Цель работы	98
16.2. Предварительные сведения	98
16.3. Задание.	98
16.4. Последовательность выполнения работы	99
16.5. Содержание отчёта	101
16.6. Контрольные вопросы	102

Учебно-методический комплекс 103

Программа дисциплины 105

1. Цели и задачи дисциплины	105
2. Место дисциплины в структуре ОП ВО	105
3. Требования к результатам освоения дисциплины	105
4. Объем дисциплины и виды учебной работы.	107
5. Содержание дисциплины	107
6. Лабораторный практикум	108
7. Практические занятия (семинары)	108
8. Материально-техническое обеспечение дисциплины	109
9. Информационное обеспечение дисциплины.	109
10. Учебно-методическое обеспечение дисциплины	109
11. Методические указания для обучающихся по освоению дисциплины	109

Паспорт фонда оценочных средств 111

Фонд оценочных средств 113

Балльно-рейтинговая система оценки уровня знаний	113
Критерии оценки по дисциплине	115
Примерный перечень оценочных средств	116
Комплект заданий для итогового контроля знаний	117
Комплект разноуровневых задач (заданий)	120

Сведения об авторах 121

Лабораторная работа № 1. Установка и конфигурация операционной системы на виртуальную машину

1.1. Цель работы

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

1.2. Указания к работе

1.2.1. Техническое обеспечение

Лабораторная работа подразумевает установку на виртуальную машину VirtualBox (<https://www.virtualbox.org/>) операционной системы Linux (дистрибутив CentOS).

Выполнение работы возможно как в дисплейном классе факультета физико-математических и естественных наук РУДН, так и дома. Описание выполнения работы приведено для дисплейного класса со следующими характеристиками техники:

- Intel Core i3-550 3.2 GHz, 4 GB оперативной памяти, 8 GB свободного места на жёстком диске;
- ОС Linux Gentoo (<http://www.gentoo.ru/>);
- VirtualBox верс. 4.3.18 или старше.

1.2.2. Соглашения об именовании

При выполнении работ следует придерживаться следующих правил именования:

- пользователь внутри виртуальной машины должен иметь имя, совпадающее с логином студента, выполняющего лабораторную работу. Вы можете посмотреть ваш логин, набрав в терминале команду:
`id -un`
- имя хоста вашей виртуальной машины должно совпадать с логином студента, выполняющего лабораторную работу.
- имя виртуальной машины должно совпадать с логином студента, выполняющего лабораторную работу.

1.3. Последовательность выполнения работы

Загрузите в дисплейном классе операционную систему Linux. Осуществите вход в систему.

Запустите терминал. Перейдите в каталог `/var/tmp`:

```
cd /var/tmp
```

Создайте каталог с именем пользователя (совпадающий с логином студента в дисплейном классе). Для этого можно использовать команду:

```
mkdir /var/tmp/`id -un`
```

Запустите виртуальную машину, введя в командной строке:

```
VirtualBox &
```

Проверьте в свойствах VirtualBox месторасположение каталога для виртуальных машин. Для этого в VirtualBox выберите **Файл** > **Свойства**, вкладка **Общие**. В поле **Папка для машин** (рис. 1.1) должно стоять

`/var/tmp/имя_пользователя`

Здесь `имя_пользователя` — логин (учётная запись) студента в дисплейном классе. Если указан другой каталог, то требуется **изменить его**, как указано выше.

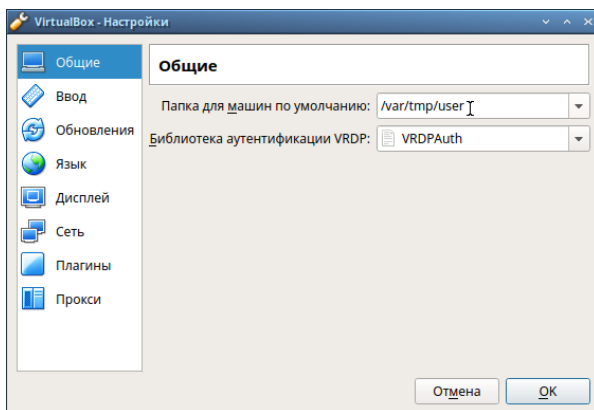


Рис. 1.1. Окно «Свойства» VirtualBox

Создайте новую виртуальную машину. Для этого в VirtualBox выберите **Машина** > **Создать**.

Укажите имя виртуальной машины (ваш логин в дисплейном классе), тип операционной системы — Linux, RedHat (рис. 1.2).

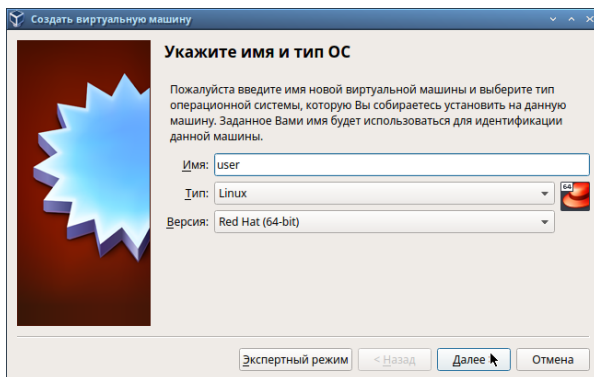


Рис. 1.2. Окно «Имя машины и тип ОС»

Укажите размер основной памяти виртуальной машины — 1024 МБ (рис. 1.3).

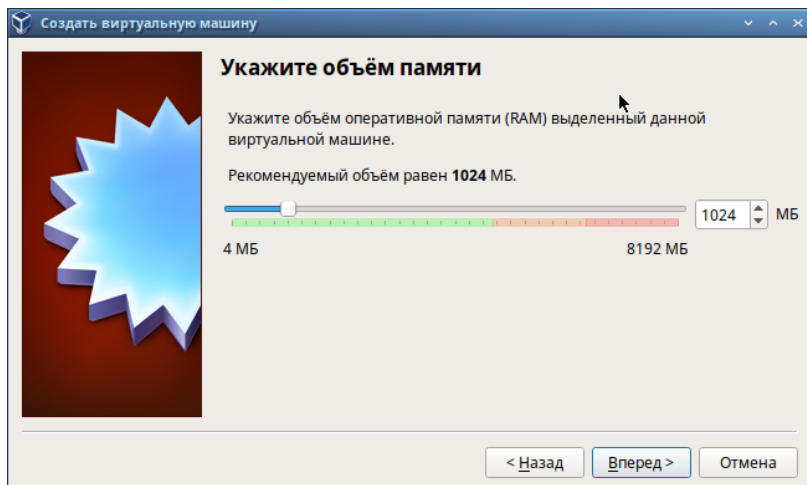


Рис. 1.3. Окно «Размер основной памяти»

Задайте конфигурацию жёсткого диска — загрузочный, VDI (VirtualBox Disk Image), динамический виртуальный диск (рис. 1.4–1.6).

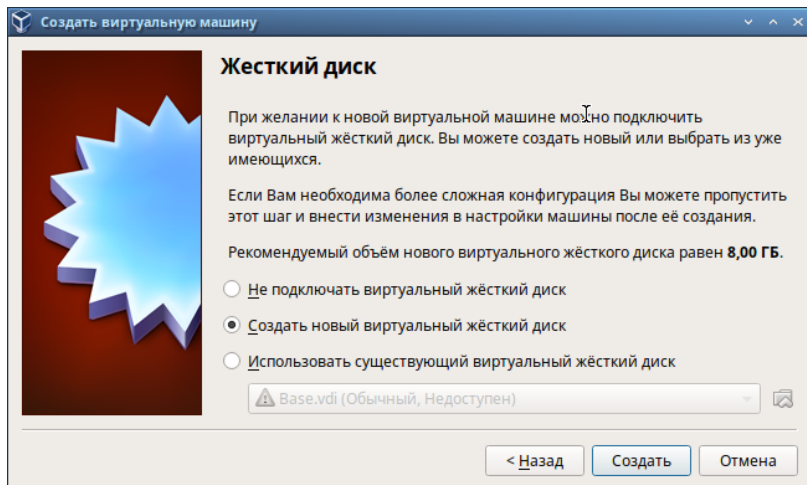


Рис. 1.4. Окно подключения или создания жёсткого диска на виртуальной машине

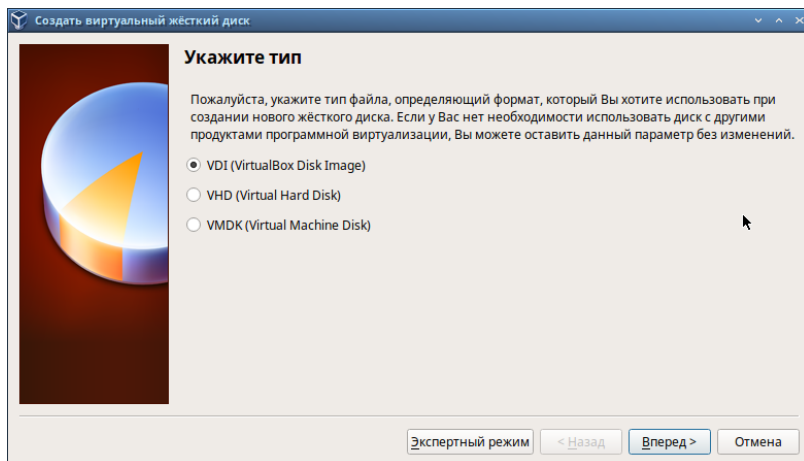


Рис. 1.5. Окно определения типа подключения виртуального жёсткого диска

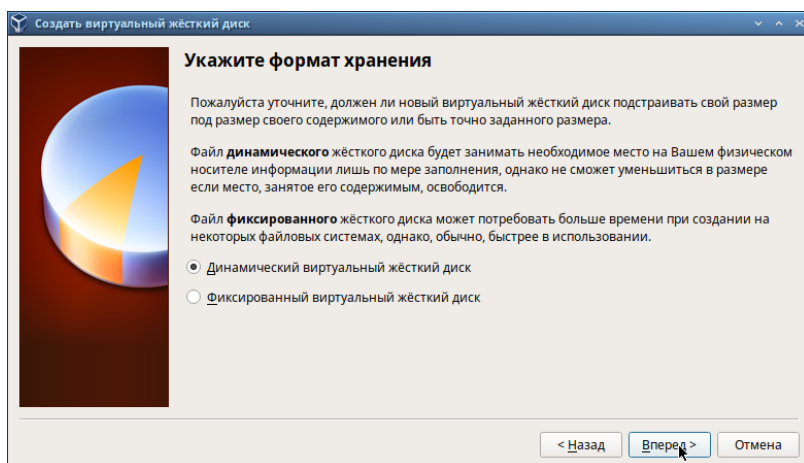


Рис. 1.6. Окно определения формата виртуального жёсткого диска

Задайте размер диска — 40 ГБ (или больше), его расположение — в данном случае `/var/tmp/имя_пользователя/centos.vdi` (рис. 1.7).

Выберите в VirtualBox **Свойства** > **Носители** Вашей виртуальной машины. Добавьте новый привод оптических дисков и выберите образ `/afs/dk.sci.pfu.edu.ru/common/files/iso/CentOS-7-x86_64-DVD.iso` (рис. 1.8).

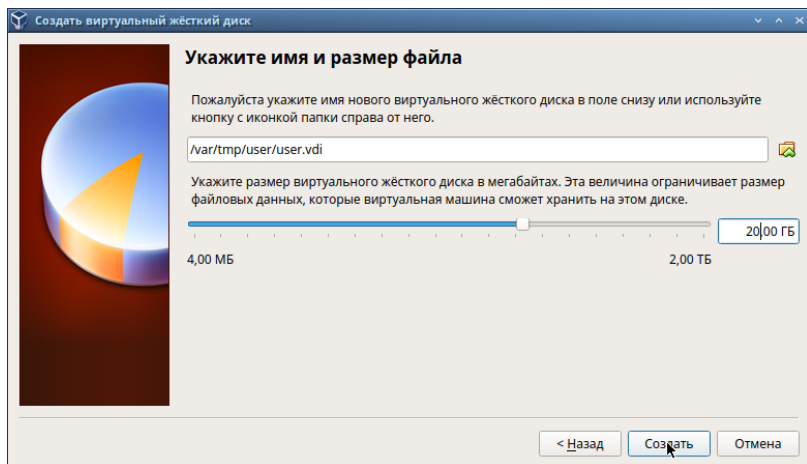


Рис. 1.7. Окно определения размера виртуального динамического жёсткого диска и его расположения

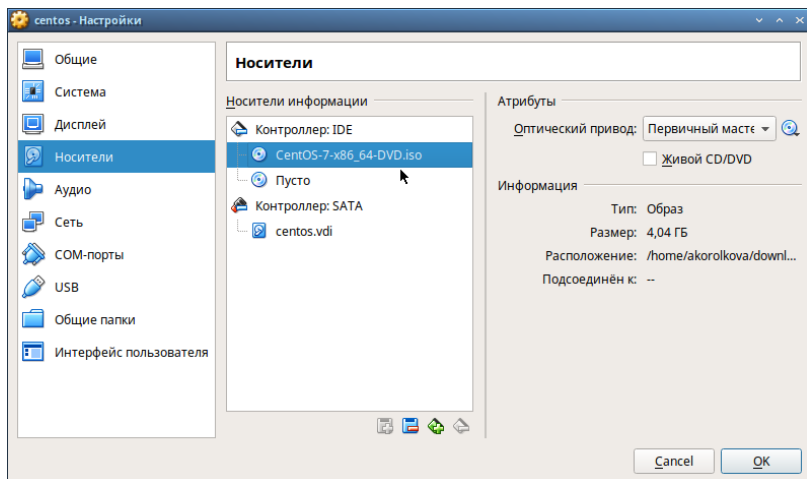


Рис. 1.8. Окно «Носители» виртуальной машины: выбор образа оптического диска

Запустите виртуальную машину, выберите язык интерфейса и перейдите к настройкам установки операционной системы (рис. 1.9).

При необходимости скорректируйте часовой пояс, раскладку клавиатуры (рекомендуется в качестве языка по умолчанию указать английский язык).

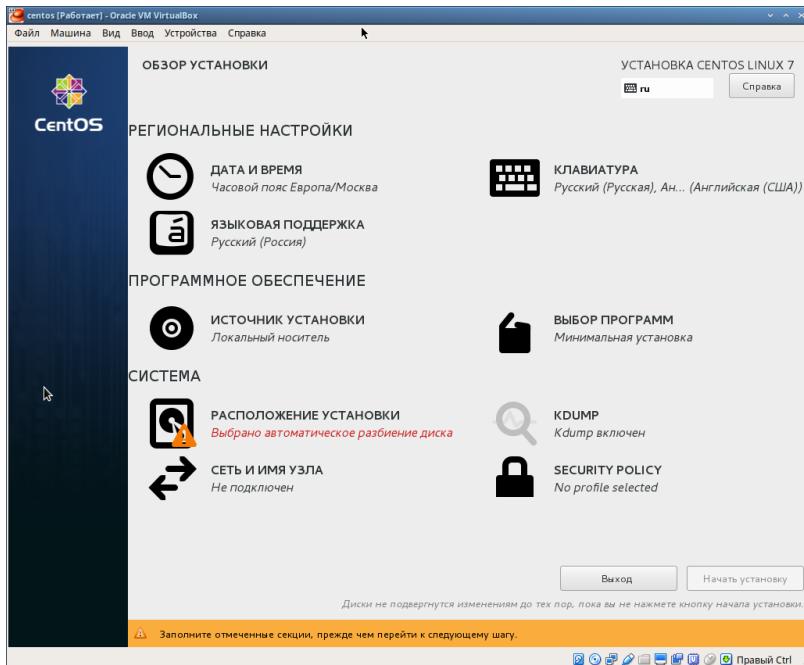


Рис. 1.9. Окно настройки установки образа ОС

В разделе выбора программ укажите в качестве базового окружения **Сервер с GUI**, а в качестве дополнения — **Средства разработки** (рис. 1.10).

Отключите KDUMP (рис. 1.11).

Место установки ОС оставьте без изменения (рис. 1.12).

Включите сетевое соединение и в качестве имени узла укажите имя_пользователя.localdomain (рис. 1.13).

Установите пароль для root и пользователя с правами администратора (рис. 1.14–1.16).

После завершения установки операционной системы корректно перезапустите виртуальную машину и примите условия лицензии (рис. 1.17–1.18).

В VirtualBox оптический диск должен отключиться автоматически, но если это не произошло, то необходимо отключить носитель информации с образом, выбрав

Свойства » **Носители** » **CentOS-7-x86_64-DVD.iso** » **Удалить устройство**.

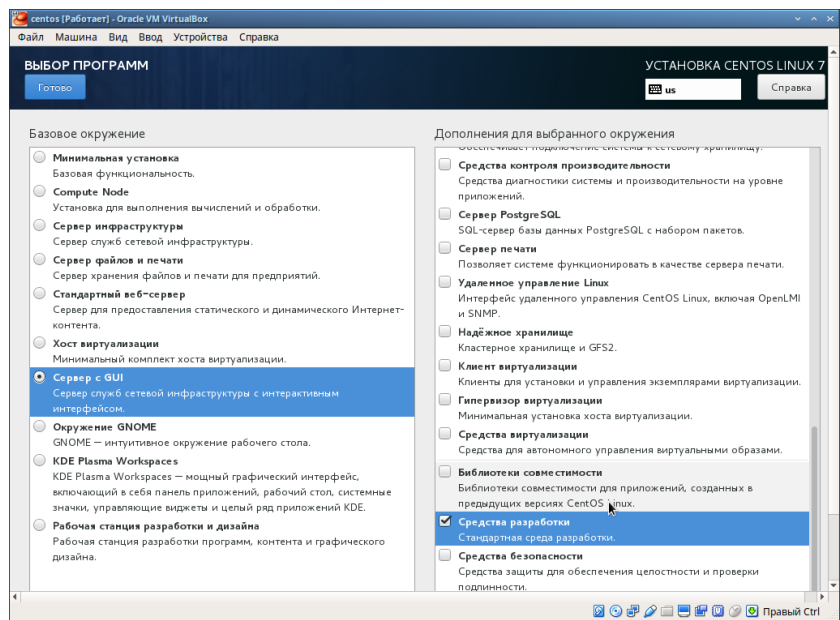


Рис. 1.10. Окно настройки установки: выбор программ

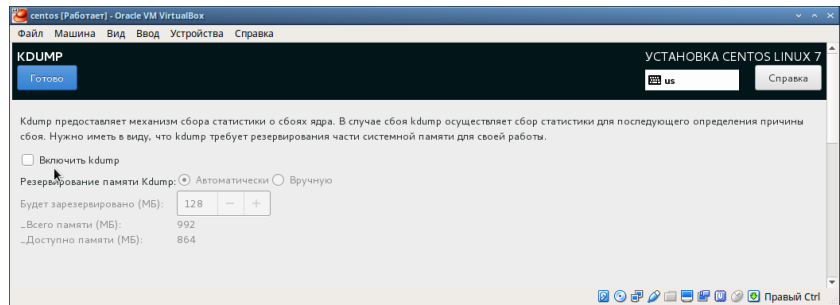


Рис. 1.11. Окно настройки установки: отключение KDUMP

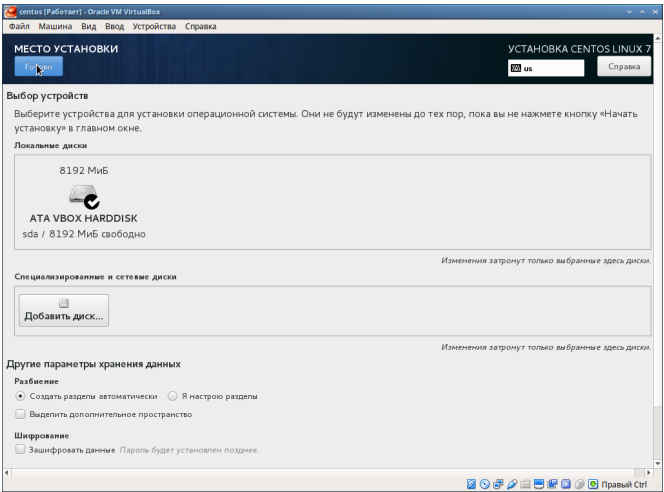


Рис. 1.12. Окно настройки установки: место установки

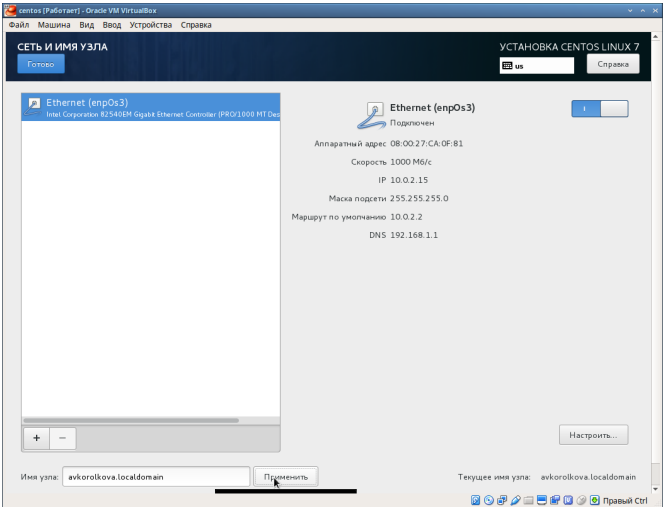


Рис. 1.13. Окно настройки установки: сеть и имя узла

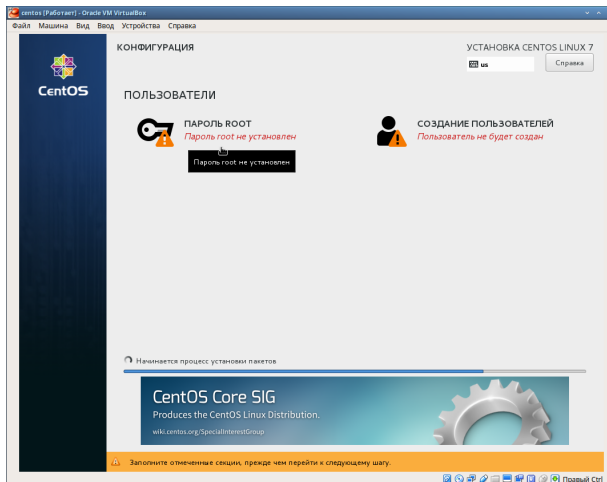


Рис. 1.14. Окно конфигурации пользователей

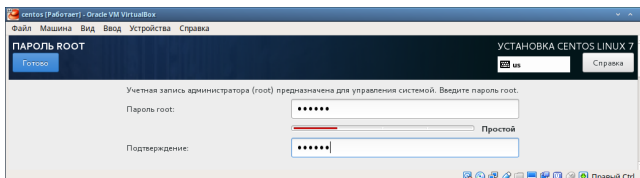


Рис. 1.15. Установка пароля для root

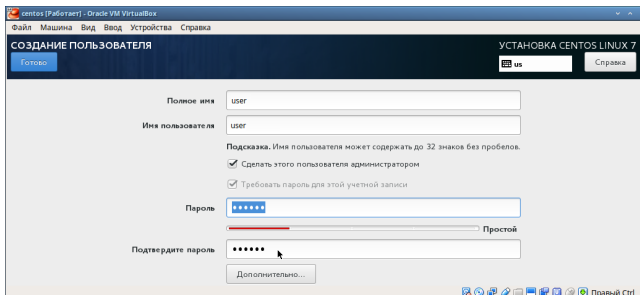


Рис. 1.16. Установка пароля для пользователя с правами администратора

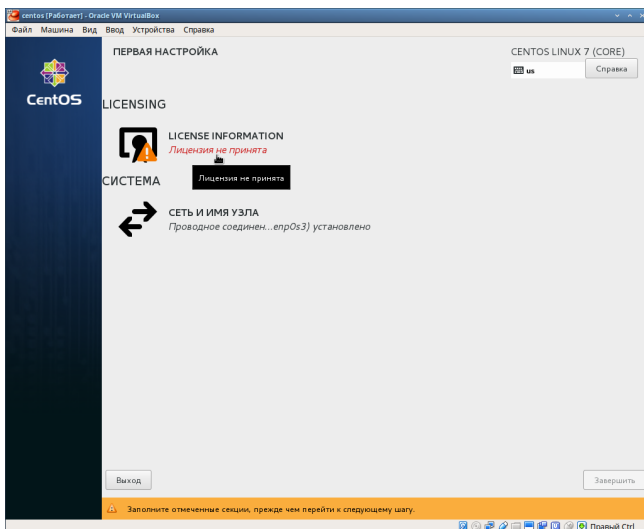


Рис. 1.17. Первоначальная настройка ОС

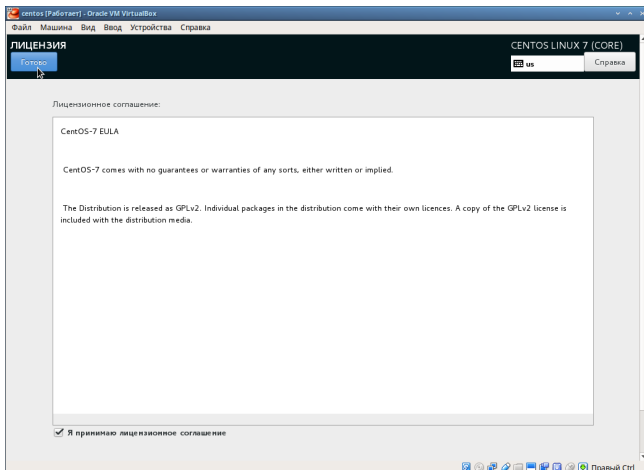


Рис. 1.18. Первоначальная настройка ОС: лицензия

Войдите в ОС под заданной вами при установке учётной записью. В меню **Устройства** виртуальной машины подключите образ диска дополнений гостевой ОС (рис. 1.19), при необходимости введите пароль пользователя `root` вашей виртуальной ОС.

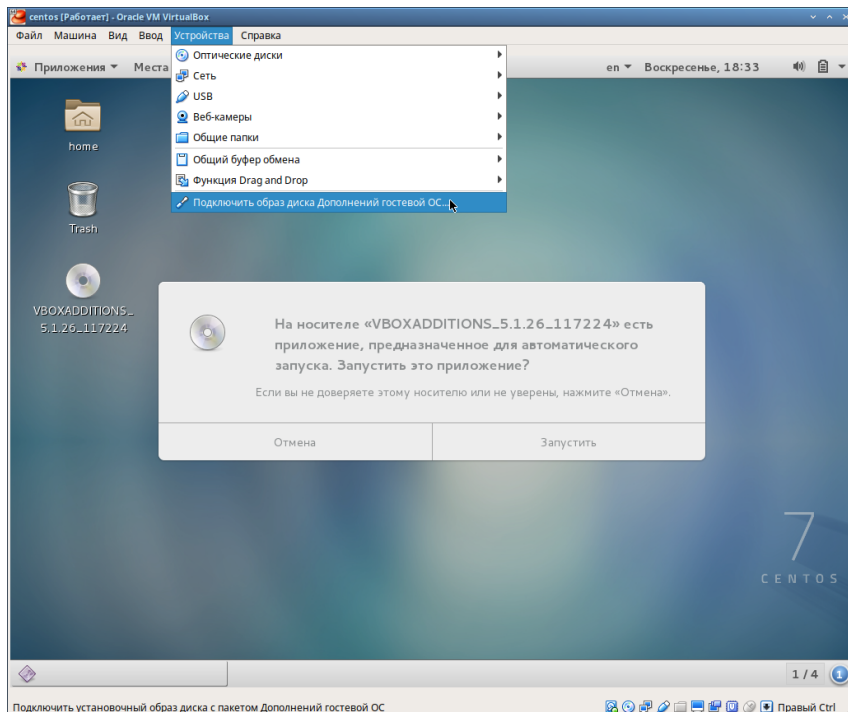


Рис. 1.19. Подключение образа диска дополнений гостевой ОС

После загрузки дополнений нажмите **Return** или **Enter** (рис. 1.20) и корректно перезагрузите виртуальную машину.

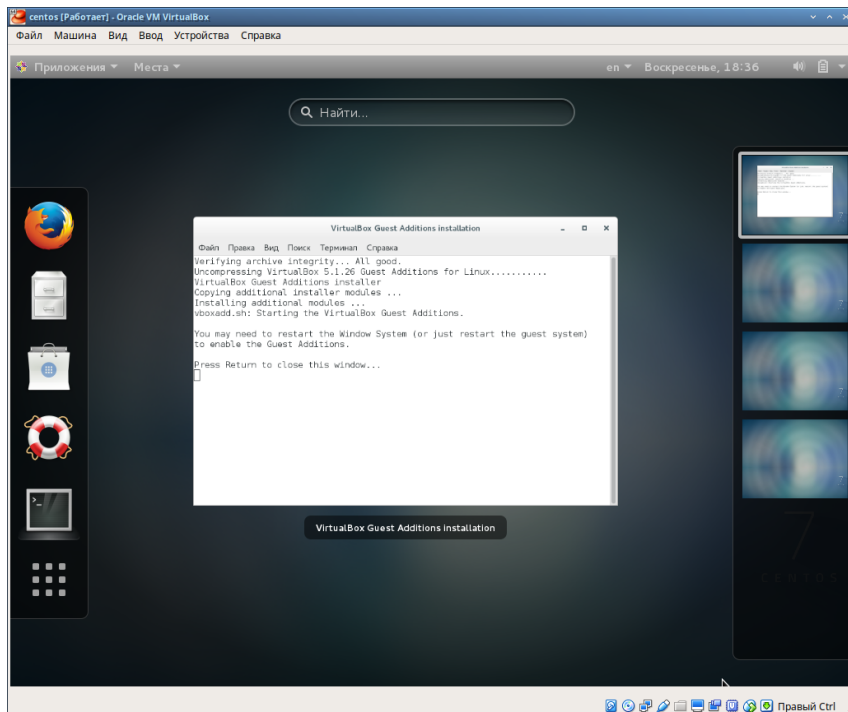


Рис. 1.20. Завершение подключения образа диска дополнений гостевой ОС

1.3.1. Установка имени пользователя и названия хоста

Если при установке виртуальной машины вы задали имя пользователя или имя хоста, не удовлетворяющее соглашению об именовании (см. раздел 1.2.2), то вам необходимо исправить это.

1. Запустите виртуальную машину и залогиньтесь.
2. Запустите терминал и получите полномочия администратора:
`su -`
3. Создайте пользователя (вместо `username` укажите ваш логин в дисплейном классе):
`adduser -G wheel username`
4. Задайте пароль для пользователя (вместо `username` укажите ваш логин в дисплейном классе):
`passwd username`
5. Установите имя хоста (вместо `username` укажите ваш логин в дисплейном классе):
`hostnamectl set-hostname username`
6. Проверьте, что имя хоста установлено верно:
`hostnamectl`

1.4. Домашнее задание

Дождитесь загрузки графического окружения и откройте терминал. В окне терминала проанализируйте последовательность загрузки системы, выполнив команду `dmesg`. Можно просто просмотреть вывод этой команды:

```
dmesg | less
```

Можно использовать поиск с помощью `grep`:

```
dmesg | grep -i "то, что ищем"
```

Получите следующую информацию.

1. Версия ядра Linux (Linux version).
2. Частота процессора (Detected Mhz processor).
3. Модель процессора (CPU0).
4. Объем доступной оперативной памяти (Memory available).
5. Тип обнаруженного гипервизора (Hypervisor detected).
6. Тип файловой системы корневого раздела.
7. Последовательность монтирования файловых систем.

1.5. Содержание отчёта

Отчёт должен включать:

- 1) титульный лист;
- 2) формулировку задания работы;
- 3) описание результатов выполнения задания:
 - краткое описание действия;
 - вводимую команду или команды;
 - результаты выполнения команд (снимок экрана);
- 4) выводы, согласованные с заданием работы;
- 5) ответы на контрольные вопросы;
- 6) отчёт о выполнении дополнительного задания.

1.6. Контрольные вопросы

1. Какую информацию содержит учётная запись пользователя?
2. Укажите команды терминала и приведите примеры:
 - для получения справки по команде;
 - для перемещения по файловой системе;
 - для просмотра содержимого каталога;
 - для определения объёма каталога;
 - для создания / удаления каталогов / файлов;
 - для задания определённых прав на файл / каталог;
 - для просмотра истории команд.
3. Что такое файловая система? Приведите примеры с краткой характеристикой.
4. Как посмотреть, какие файловые системы подмонтированы в ОС?
5. Как удалить зависший процесс?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–12].

Список литературы

1. *Купер М.* Искусство программирования на языке сценариев командной оболочки. — 2004. — URL: https://www.opennet.ru/docs/RUS/bash_scripting_guide/.
2. *Newham C.* Learning the bash Shell: Unix Shell Programming. — O'Reilly Media, 2005. — 354 p. — (In a Nutshell). — ISBN 0596009658.
3. *Робачевский А., Немнюгин С., Стесик О.* Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010. — 656 с. — ISBN 978-5-94157-538-1.
4. *Колисниченко Д. Н.* Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
5. *Dash P.* Getting Started with Oracle VM VirtualBox. — Packt Publishing Ltd, 2013. — 86 p. — ISBN 1782177825.
6. *Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли.* — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
7. *Colvin H.* VirtualBox: An Ultimate Guide Book on Virtualization with VirtualBox. — CreateSpace Independent Publishing Platform, 2015. — 70 p. — ISBN 978-1522769880.
8. *Таненбаум Э., Бос Х.* Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — 1120 с. — (Классика Computer Science).
9. *GNU Bash Manual.* — 2016. — URL: <https://www.gnu.org/software/bash/manual/>.
10. *Robbins A.* Bash Pocket Reference. — O'Reilly Media, 2016. — 156 p. — ISBN 978-1491941591.
11. *Vugt S. van.* Red Hat RHCSA/RHCE 7 cert guide : Red Hat Enterprise Linux 7 (EX200 and EX300). — Pearson IT Certification, 2016. — 1008 p. — (Certification Guide). — ISBN 978-0-7897-5405-9.
12. *Zarrelli G.* Mastering Bash. — Packt Publishing, 2017. — 502 p. — ISBN 9781784396879.

Лабораторная работа № 2. Управление пользователями и группами

2.1. Цель работы

Получить представление о работе с учётными записями пользователей и группами пользователей в операционной системе типа Linux.

2.2. Предварительные сведения

В операционных системах типа Linux чаще всего применяется дискреционное управление доступом субъектов к объектам системы. В качестве субъектов системы чаще всего выступают пользователи или группы, а в качестве субъектов — файлы (в том числе системные), каталоги, устройства и т.п. В качестве особого субъекта выделяется суперпользователь (пользователь `root`), имеющий право устанавливать права владения для всех остальных субъектов системы.

Под доступом к ресурсу системы понимают чтение (`read`), запись (`write`) и выполнение (`execute`). Тот или иной тип доступа может быть применён к пользователю и/или группе, владеющими тем или иным ресурсом операционной системы, а также ко всем остальным субъектам, не являющимся владельцами ресурса.

Права доступа к ресурсу представляются в системе следующим образом:

Флаг	Пользователь-владелец	Группа-владелец	Все остальные
#	gwx	gwx	gwx

В качестве флага может быть указано:

Флаг	Описание
-	указывает на отсутствие флага
l	указывает, что ресурс является символической ссылкой
d	указывает, что ресурс является каталогом
b	указывает, что ресурс является блочным устройством
c	указывает, что ресурс является символьным устройством
p	указывает, что ресурс является каналом, устройством fifo
s	указывает, что ресурс является Unix сокетом

Пример отображения информации о правах доступа, владельце, группе и т.п. файла `/etc/passwd`:

```
ls -l /etc/passwd
-rw-r--r-- 1 root root 5302 ноя 13 2017 /etc/passwd
```

Первая колонка отображает права доступа к файлу (в данном случае `-rw-r--r--`), в третьей и четвёртой колонке указано, что владельцем файла является пользователь `root` и одноимённая группа `root`.

Для установки атрибутов прав доступа используется утилита `chmod`. При этом можно использовать как восьмеричное представление, так и символьное:

Восьмеричная запись	Бинарная запись	Маска
0	000	---
1	001	--x
2	010	-w-
3	011	-wx
4	100	r--
5	101	r-x
6	110	rw-
7	111	rwX

Пример установки прав доступа `rwXr--r--` для файла `file1`:

```
chmod 744 file1
```

или

```
chmod u=rwx,go+r,go-wx file1
```

2.2.1. Системные базы учётных записей

2.2.1.1. Файл `/etc/passwd`

В операционных системах типа Linux информация о пользователях располагается в файле `/etc/passwd`. Запись о пользователе в этом файле имеет определённую структуру в виде набора полей, разделённых двоеточием:

имя_пользователя:пароль:UID:GID:комментарий:каталог:оболочка

Фрагмент файла `/etc/passwd`:

```
ntp:x:38:38::/etc/ntp:/sbin/nologin
chrony:x:994:993::/var/lib/chrony:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
pulse:x:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
gnome-initial-setup:x:993:991::/run/gnome-initial-setup:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
```

Ниже приведён краткий обзор полей файла `/etc/passwd`, за которым следует краткое описание их цели.

- *Имя пользователя* — это уникальное имя для пользователя. Имена пользователей важны для соответствия пользователю пароля, который хранится отдельно в файле `/etc/shadow`. В Linux не может быть пробелов в имени пользователя.
- *Пароль* — раннее второе поле в файле `/etc/passwd` использовалось для хранения хэшированного пароля пользователя. Доступ на чтение файла `/etc/passwd` имеют все пользователи системы, поэтому хранение пароля в этом файле создаёт угрозу безопасности. По этой причине в современных системах Linux хэшированные пароли хранятся в файле `/etc/shadow`, а в файле `/etc/passwd` есть только указание на это в виде символа `x`.
- *UID, User ID* — каждый пользователь имеет уникальный числовой идентификатор пользователя (UID). Именно UID определяет возможные разрешения для пользователя. UID хранится в метаданных файла, а не в имени пользователя. UID 0 зарезервирован для пользователя `root` с неограниченными правами. Более низкие UID (обычно до 999) используются для системных учётных записей, а более высокие UID (от 1000) зарезервированы для остальных пользователей. Диапазон UID, который используется для создания обычных учётных записей пользователей, устанавливается в файле `/etc/login.defs`.

- *GID, group ID* — в Linux каждый пользователь является членом хотя бы одной группы, называемой первичной (или основной). Первичная группа играет центральную роль в управлении разрешениями.
- Поле комментариев — используется для описания назначения учётной записи пользователя. Это поле является необязательным. Некоторые утилиты, например *finger*, могут получать информацию из этого поля. Это поле также называется *GEOS* (от названия операционной системы фирмы General Electric).
- *Каталог* — это начальный (домашний) каталог, в котором пользователь находится после входа в систему. Если учётная запись пользователя используется человеком, то здесь человек будет хранить свои личные файлы и программы. Для системной учётной записи этот каталог используется для хранения служебных файлов, используемых в работе.
- *Оболочка (shell)* — это программа, которая запускается после успешного подключения пользователя к системе. Для большинства пользователей это будет */bin/bash* — стандартная оболочка Linux. Для системных учётных записей в качестве оболочки обычно выступает */sbin/nologin* — это специальная команда, которая запрещает доступ злоумышленника к системе (для гарантии недоступности оболочки, а, соответственно, и невозможности внесения изменений куда бы то ни было). Можно создать файл с именем */etc/nologin.txt*, содержащий сообщение, которое будет отображаться, когда пользователь с оболочкой */sbin/nologin* попытается войти в систему.

2.2.1.2. Файл /etc/shadow

Файл */etc/shadow* предназначен для хранения зашифрованных паролей пользователей системы. Поля записей в этом файле разделены двоеточием.

Фрагмент файла */etc/shadow*:

```
ntp:!:16420::::
chrony:!:16420:~::~:
abrt:!:16420:~::~:
pulse:!:16420:~::~:
gdm:!:16420:~::~:
gnome-initial-setup:!:16420:~::~:
postfix:!:16420:~::~:
sshd:!:16420:~::~:
tcpdump:!:16420:~::~:
user:$6$3VZbGx1djo6FfyZo9/Trg7Q.3foIsIFYxBm6UnHuxxBrxQxHDnDuZxgS.We/
↔ MAuHn8HboBZpaMD8gfm.fmlB/ML9LnuaT7CbWVxx31:16420:0:99999:7:::
```

В файле */etc/shadow* определены следующие поля:

1. *Имя пользователя*. В файле */etc/shadow* содержатся только имена пользователей, а не UID, что позволяет работать нескольким пользователям с одинаковым UID, но разными паролями.
2. *Зашифрованный пароль* — это поле содержит пароль пользователя.
3. *Количество дней с 1 января 1970 года, когда пароль был изменён в последний раз*.
4. *Количество дней до того, как пароль может быть изменён*. Это поле позволяет системным администраторам использовать более строгую политику паролей, когда невозможно сразу вернуться к исходному паролю при его изменении. Обычно это поле устанавливается в значение 0.
5. *Количество дней, после которых необходимо изменить пароль*. Это поле содержит максимальный срок действия пароля. По умолчанию установлено 99999 (около 273 лет).
6. *За сколько дней до истечения срока действия пароля пользователь получает предупреждение*. Это поле используется для предупреждения пользователя о сроке,

когда происходит принудительное изменение пароля. По умолчанию установлено значение 7.

7. *Через сколько дней после истечения срока действия пароля учётная запись будет отключена.* После истечения срока действия пароля пользователи больше не смогут входить в систему.
8. *Количество дней с 1 января 1970 года, когда эта учётная запись была отключена.* Администратор может установить это поле для отключения учётной записи. Обычно это лучший подход, чем удаление учётной записи, так как все связанные с ней свойства и файлы учётной записи будут сохранены.
9. *Зарезервированное поле*, которое добавлено для будущего использования.

2.2.1.3. Файл /etc/group

Файл /etc/group содержит имена групп и списки членов каждой группы. Поля записей в этом файле разделены двоеточием.

Фрагмент файла /etc/group:

```
kvm:x:36:qemu
qemu:x:107:
libstoragemgmt:x:994:
rpc:x:32:
rpcuser:x:29:
```

В файле /etc/group используются следующие поля:

- *Название группы* — это поле содержит имя группы.
- *Групповой пароль*. Групповой пароль может использоваться пользователями, которые хотят временно присоединиться к группе, чтобы разрешить доступ к файлам, доступ к которым имеет группа. В настоящее время эта функциональность больше не используется.
- *Идентификатор группы (GID)* — уникальный цифровой идентификационный номер группы.
- *Члены группы* — здесь перечислены имена пользователей, которые являются членами этой группы (для пользователей подобная группа является вторичной). Тут не отображаются пользователи, для которых данная группа является основной.

2.2.2. Параметры учётных записей

Для создания учётных записей пользователей удобно использовать утилиту типа useradd:

```
useradd -m -g [основная группа] -G [дополнительные группы]
-s [командная оболочка] [имя пользователя]
```

Ключ -m указывает на создание домашнего каталога пользователя вида /home/[имя пользователя].

Ключ -g задаёт имя или номер основной группы пользователя; если параметр не указан, пользователю будет присвоена группа в соответствии с переменной USERGROUPS_ENAB, расположенной в каталоге /etc/login.defs.

Ключ -G задаёт список дополнительных групп, в которые входит пользователь; каждая группа отделяется от другой запятой без пробелов.

Ключ -s задаёт командную оболочку пользователя.

При этом файл /etc/default/useradd содержит устанавливаемые для новой учётной записи значения по умолчанию.

Описание действий других возможных ключей можно посмотреть, используя команду `man useradd`.

Фрагмент файла `/etc/default/useradd`:

```
# useradd defaults file
GROUP=100
HOME=/home
INACTIVE=-1
EXPIRE=
SHELL=/bin/bash
SKEL=/etc/skel
CREATE_MAIL_SPOOL=yes
```

В файле `/etc/login.defs` устанавливаются разные переменные для команды `login`. Этот файл связан с настройкой соответствующей среды для новых пользователей. Ниже приведён список некоторых наиболее значимых переменных, которые могут быть установлены из `/etc/login.defs`:

- `MOTD_FILE` — определяет файл, который используется как файл «сообщение дня». В этом файле можно включать сообщения, которые будут отображаться после того, как пользователь успешно войдёт в систему.
- `ENV_PATH` — определяет переменную `$PATH`, список каталогов, в которых необходимо искать исполняемые файлы после входа в систему.
- `PASS_MAX_DAYS`, `PASS_MIN_DAYS` и `PASS_WARN_AGE` — определяют свойства по умолчанию истечения срока действия пароля при создании новых пользователей.
- `UID_MIN` — первый `UID` для использования при создании новых пользователей.
- `CREATE_HOME` — указывает, следует ли создавать домашний каталог для новых пользователей.
- `USERGROUPS_ENAB` — создавать ли частную группы для новых пользователей. Это означает, что у нового пользователя есть группа с тем же именем, что и имя пользователя в качестве своей группы по умолчанию. Если установлено `no`, все пользователи становятся членами группы пользователей (`users`).

2.3. Задание

1. Прочитайте справочное описание `man` по командам `ls`, `whoami`, `id`, `su`, `passwd`, `vi`, `visudo`, `useradd`, `usermod`, `userdel`, `groupadd`, `groupdel`.
2. Выполните действия по переключению между учётными записями пользователей, по управлению учётными записями пользователей (раздел 2.4.1).
3. Выполните действия по созданию пользователей и управлению их учётными записями (раздел 2.4.2).
4. Выполните действия по работе с группами пользователей (раздел 2.4.3).

2.4. Последовательность выполнения работы

2.4.1. Переключение учётных записей пользователей

1. Войдите в систему как обычный пользователь и откройте терминал.
2. Определите, какую учётную запись пользователя вы используете, введя команду `whoami`
`whoami`
Выведите на экран более подробную информацию, используя команду `id`
`id`
В отчёте дайте пояснение по отображённой информации.

3. Используйте команду `su` для переключения к учётной записи `root`. При запросе пароля введите пароль пользователя `root`. Наберите
`id`
В отчёте дайте пояснение по отображённой информации.
4. Просмотрите в безопасном режиме файл `/etc/sudoers`, используя, например,
`visudo`
и убедитесь, что в нём присутствует строка
`% wheel ALL = (ALL) ALL`
В отчёте поясните, что это означает и для чего нужна группа `wheel`.
5. Создайте пользователя `alice`, входящего в группу `wheel`:
`useradd -G wheel alice`
6. Убедитесь, что пользователь `alice` добавлен в группу `wheel`, введя
`id alice`
7. Задайте пароль для пользователя `alice`, набрав
`passwd alice`
Пароль требуется ввести дважды.
8. Выйдите из системы (из своей учётной записи) и войдите в систему как пользователь `alice`.
9. Создайте пользователя `bob`:
`sudo useradd bob`
Введите пароль при запросе. Проверьте, что пользователь `bob` создан.

2.4.2. Создание учётных записей пользователей

Применим общие решения для создания учётных записей пользователей.

1. Откройте файл конфигурации `/etc/login.defs` для редактирования, используя, например, `vim` (не забудьте, что требуются полномочия пользователя `root`):
`vim /etc/login.defs`
Измените несколько параметров. Например, найдите параметр
`CREATE_HOME`
и убедитесь, что он установлен в значение `yes`. Также установите параметр
`USERGROUPS_ENAB no`
Это позволит не добавлять нового пользователя в группу с тем же именем, что и пользователь, а использовать группу `users`.
2. Перейдите в каталог `/etc/skel`:
`cd /etc/skel`
Создайте каталоги `Pictures` и `Documents`:
`mkdir Pictures`
и
`mkdir Documents`
Это позволит добавить эти каталоги по умолчанию во все домашние каталоги пользователей.
3. Измените содержимое файла `.bashrc`, добавив строку
`export EDITOR=/usr/bin/vim`
Эта запись означает, что текстовый редактор `vim` будет установлен по умолчанию для инструментов, которые нуждаются в изменении текстовых файлов.
4. Используя утилиту `useradd`, создайте пользователя `carol`:
`useradd carol`
Посмотрите и прокомментируйте информацию об этом пользователе:
`id carol`

Проверьте, в какую первоначальную группу входит пользователь `carol`. Также убедитесь, что каталоги `Pictures` и `Documents` были созданы в домашнем каталоге пользователя `carol`.

5. Установите пароль для пользователя `carol`:

```
passwd carol
```

6. Измените свойства пароля пользователя `carol` следующим образом:

```
passwd -n 30 -w 3 -x 90 carol
```

В этой записи срок действия пароля истекает через 90 дней (`-x 90`). За три дня до истечения срока действия пользователь получит предупреждение (`-w 3`). Пароль должен использоваться как минимум за 30 дней (`-n 30`) до того, как его можно будет изменить.

7. Создайте ещё несколько пользователей: `dan`, `dave`, `david`, используя скрипт:

```
for i in dan dave david; do useradd $i; done
```

8. Убедитесь, что идентификатор `alice` существует во всех трёх файлах:

```
grep alice /etc/passwd /etc/shadow /etc/group
```

9. Убедитесь, что идентификатор `carol` существует не во всех трёх файлах:

```
grep carol /etc/passwd /etc/shadow /etc/group
```

2.4.3. Работа с группами

В этом упражнении требуется создать две группы и добавить некоторых пользователей в эти группы.

1. Создайте группы `main` и `third`:

```
groupadd main
```

```
groupadd third
```

2. Используйте `usermod` для добавления пользователей `alice` и `bob` в группу `main`, а `carol`, `carlos` и `charlie` — в группу `third`:

```
usermod -aG main alice
```

```
usermod -aG main bob
```

```
usermod -aG third carol
```

```
usermod -aG third dan
```

```
usermod -aG third dave
```

```
usermod -aG third david
```

3. Убедитесь, что пользователь `carol` правильно добавлен в группу `third`:

```
id carol
```

Пользователю `carol` должна быть назначена основная группа с идентификатором `gid = 100` (`users`). Определите, в какие вторичные группы входит `carol`.

4. Определите, участниками каких групп являются другие созданные вами пользователи.

2.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
 - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
 - результаты проверки корректности настроек в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

2.6. Контрольные вопросы

1. Какой UID имеет пользователь `root`?
2. В каком конфигурационном файле определяются параметры `sudo`?
3. Какую команду следует использовать для изменения конфигурации `sudo`?
4. Какие два файла можно использовать для определения параметров, которые будут использоваться при создании пользователей?
5. Сколько групп вы можете создать в файле `/etc/passwd`?
6. Если вы хотите предоставить пользователю доступ ко всем командам администратора через `sudo`, членом какой группы он должен быть?
7. Какую команду следует использовать для изменения файла `/etc/group` вручную?
8. Какие две команды вы можете использовать для изменения информации о пароле пользователя?
9. В каких файлах хранятся пароли пользователей и учётные записи групп?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–7].

Список литературы

1. UNIX Power Tools / M. Loukides, T. O'Reilly, J. Peek, S. Powers. — O'Reilly Media, 2009. — 1160 p.
2. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010. — 656 с. — ISBN 978-5-94157-538-1.
3. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
4. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли. — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
5. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — 1120 с. — (Классика Computer Science).
6. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
7. Goyal S. K. Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.

Лабораторная работа № 3. Настройка прав доступа

3.1. Цель работы

Получение навыков настройки базовых и специальных прав доступа для групп пользователей в операционной системе типа Linux.

3.2. Задание

1. Прочитайте справочное описание `man` по командам `ls`, `su`, `chgrp`, `chmod`, `getfacl`, `setfacl`.
2. Выполните действия по управлению базовыми разрешениями для групп пользователей (раздел 3.3.1).
3. Выполните действия по управлению специальными разрешениями для групп пользователей (раздел 3.3.2).
4. Выполните действия по управлению расширенными разрешениями с использованием списков ACL для групп пользователей (раздел 3.3.3).

3.3. Последовательность выполнения работы

Предпосылки: в лабораторной работе № 2 были созданы пользователи `alice` и `bob`, входящие в группу `main`, и пользователь `carol`, входящий в группу `third`.

3.3.1. Управление базовыми разрешениями

Требуется создать структуру каталогов с разными разрешениями доступа для разных групп пользователей.

1. Откройте терминал с учётной записью `root`:
`su -`
2. В корневом каталоге создайте каталоги `/data/main` и `/data/third`:
`mkdir -p /data/main /data/third`
Посмотрите, кто является владельцем этих каталогов. Для этого используйте:
`ls -Al /data`
3. Прежде чем устанавливать разрешения, измените владельцев этих каталогов с `root` на `main` и `third` соответственно:
`chgrp main /data/main`
`chgrp third /data/third`
Посмотрите, кто теперь является владельцем этих каталогов.
4. Установите разрешения, позволяющие владельцам каталогов записывать файлы в эти каталоги и запрещающие доступ к содержимому каталогов всем другим пользователям и группам:
`chmod 770 /data/main`
`chmod 770 /data/third`
Проверьте установленные права доступа.
5. В другом терминале перейдите под учётную запись пользователя `bob`:
`su - bob`
6. Под пользователем `bob` перейдите в каталог `/data/main`:
`cd /data/main`
Попробуйте создать файл `emptyfile` в этом каталоге:

```
touch emptyfile
```

Опишите и поясните результат этого действия.

7. Под пользователем bob перейдите в каталог /data/third:

```
cd /data/third
```

Попробуйте создать файл emptyfile в этом каталоге:

```
touch emptyfile
```

Опишите и поясните результат этого действия.

3.3.2. Управление специальными разрешениями

Требуется, используя специальные разрешения для групп пользователей, обеспечить обмен файлами в общем для групп каталоге. При этом каталогу назначается бит идентификатора группы, а также *sticky bit*.

Sticky bit — дополнительный атрибут файлов или каталогов в ОС типа Linux, применяющийся в основном для каталогов с целью защиты содержимого каталогов от повреждения или удаления пользователями, не являющимися их владельцами. Для установки этого атрибута используется утилита `chmod`. Восьмеричное значение `stiky`-бита: 1000, а символическое: `+t`.

1. Откройте новый терминал под пользователем alice.
2. Перейдите в каталог /data/main:

```
cd /data/main
```

Создайте два файла, владельцем которых является alice:

```
touch alice1
```

```
touch alice2
```

3. В другом терминале перейдите под учетную запись пользователя bob (пользователь bob является членом группы main, как и alice):

```
su - bob
```

4. Перейдите в каталог /data/main:

```
cd /data/main
```

и в этом каталоге введите:

```
ls -l
```

Вы увидите два файла, созданные пользователем alice. Попробуйте удалить файлы, принадлежащие пользователю alice:

```
rm -f alice*
```

Убедитесь, что файлы будут удалены пользователем bob.

5. Создайте два файла, которые принадлежат пользователю bob:

```
touch bob1
```

```
touch bob2
```

6. В терминале под пользователем root установите для каталога /data/main бит идентификатора группы, а также `stiky`-бит для разделяемого (общего) каталога группы:

```
chmod g+s,o+t /data/main
```

7. В терминале под пользователем alice создайте в каталоге /data/main файлы `alice3` и `alice4`:

```
touch alice3
```

```
touch alice4
```

Теперь вы должны увидеть, что два созданных вами файла принадлежат группе main, которая является группой-владельцем каталога /data/main.

8. В терминале под пользователем alice попробуйте удалить файлы, принадлежащие пользователю bob:

```
rm -rf bob*
```

Убедитесь, что sticky-bit предотвратит удаление этих файлов пользователем `alice`, поскольку этот пользователь не является владельцем этих файлов. Обратите внимание: поскольку пользователь `alice` является владельцем каталога `/data/main`, то он может удалить все свои файлы в любом случае.

3.3.3. Управление расширенными разрешениями с использованием списков ACL

В этом упражнении продолжим работать в созданных ранее каталогах `/data/main` и `/data/third`. В предыдущих упражнениях для группы `main` были установлены разрешения на каталог `/data/main`, а у группы `third` — на каталог `/data/third`.

Требуется установить для группы `third` разрешения на чтение в каталоге `/data/main`, а для группы `main` — разрешения на чтение в каталоге `/data/third`. Затем требуется установить права доступа по умолчанию, чтобы убедиться в правильности установки разрешений для новых элементов этих каталогов. Для этого будет использоваться пакет `acl` и команды `setfacl` (для установки прав) и `getfacl` (для просмотра установленных прав).

Кратко опишем синтаксис команды `setfacl`.

Установить разрешения для пользователя:

```
setfacl -m "u:user:permissions" <file/dir>
```

Установить разрешения для группы:

```
setfacl -m "g:group:permissions" <file/dir>
```

Наследование записи ACL родительского каталога:

```
setfacl -dm "entry" <dir>
```

Удаление записи ACL:

```
setfacl -x "entry" <file/dir>
```

Синтаксис команды `getfacl`:

```
getfacl <file/dir>
```

Применим команды `setfacl` и `getfacl` для выполнения поставленной задачи.

1. Откройте терминал с учётной записью `root`
`su -`
2. Установите права на чтение и выполнение в каталоге `/data/main` для группы `third` и права на чтение и выполнение для группы `main` в каталоге `/data/third`:

```
setfacl -m g:third:rx /data/main  
setfacl -m g:main:rx /data/third
```
3. Используйте команду `getfacl`, чтобы убедиться в правильности установки разрешений:

```
getfacl /data/main  
getfacl /data/third
```
4. Создайте новый файл с именем `newfile1` в каталоге `/data/main`:

```
touch /data/main/newfile1
```

Используйте `getfacl /data/main/newfile1` для проверки текущих назначений полномочий. Какие права доступа у этого файла? Объясните, почему?

Выполните аналогичные действия для каталога `/data/third`. Дайте пояснения.
5. Установите ACL по умолчанию для каталога `/data/main`:

```
setfacl -m d:g:third:rxw /data/main
```
6. Добавьте ACL по умолчанию для каталога `/data/third`:

```
setfacl -m d:g:main:rxw /data/third
```
7. Убедитесь, что настройки ACL работают, добавив новый файл в каталог `/data/main`:

- ```
touch /data/main/newfile2
```
- Используйте
- ```
getfacl /data/main/newfile2
```
- для проверки текущих назначений полномочий.
- Выполните аналогичные действия для каталога /data/third.
8. Для проверки полномочий группы third в каталоге /data/third войдите в другом терминале под учётной записью члена группы third:
- ```
su - carol
```
- Проверьте операции с файлами:
- ```
rm /data/main/newfile1
rm /data/main/newfile1
```
- Проверьте, возможно ли осуществить запись в файл:
- ```
echo "Hello, world" >> /data/main/newfile1
echo "Hello, world" >> /data/main/newfile2
```
- Объясните результат произведённых действий.

### 3.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание произведённых в соответствии с заданием настроек;
  - результаты проверки корректности настроек в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

### 3.5. Контрольные вопросы

1. Как следует использовать команду `chown`, чтобы установить владельца группы для файла? Приведите пример.
2. С помощью какой команды можно найти все файлы, принадлежащие конкретному пользователю? Приведите пример.
3. Как применить разрешения на чтение, запись и выполнение для всех файлов в каталоге /data для пользователей и владельцев групп, не устанавливая никаких прав для других? Приведите пример.
4. Какая команда позволяет добавить разрешение на выполнение для файла, который необходимо сделать исполняемым?
5. Какая команда позволяет убедиться, что групповые разрешения для всех новых файлов, создаваемых в каталоге, будут присвоены владельцу группы этого каталога? Приведите пример.
6. Необходимо, чтобы пользователи могли удалять только те файлы, владельцами которых они являются, или которые находятся в каталоге, владельцами которого они являются. С помощью какой команды можно это сделать? Приведите пример.
7. Какая команда добавляет ACL, который предоставляет членам группы права доступа на чтение для всех существующих файлов в текущем каталоге?
8. Что нужно сделать для гарантии того, что члены группы получают разрешения на чтение для всех файлов в текущем каталоге и во всех его подкаталогах, а также

для всех файлов, которые будут созданы в этом каталоге в будущем? Приведите пример.

9. Какое значение `umask` нужно установить, чтобы «другие» пользователи не получали какие-либо разрешения на новые файлы? Приведите пример.
10. Какая команда гарантирует, что никто не сможет удалить файл `myfile` случайно?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–7].

## Список литературы

1. UNIX Power Tools / M. Loukides, T. O'Reilly, J. Peek, S. Powers. — O'Reilly Media, 2009. — 1160 p.
2. *Робачевский А., Немнюгин С., Стесик О.* Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010. — 656 с. — ISBN 978-5-94157-538-1.
3. *Колисниченко Д. Н.* Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
4. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли. — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
5. *Таненбаум Э., Бос Х.* Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — 1120 с. — (Классика Computer Science).
6. *Neil N. J.* Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
7. *Goyal S. K.* Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.



## Лабораторная работа № 4. Работа с программными пакетами

### 4.1. Цель работы

Получить навыки работы с репозиториями и менеджерами пакетов.

### 4.2. Предварительные сведения

Пакетный менеджер `yum` (Yellowdog Updater, Modified) используется в популярных Linux-дистрибутивах для установки/удаления и других действий с пакетами.

#### 4.2.1. Основные команды yum

Далее приведены основные команды `yum`:

- отображение команд и опций:  
`yum help`
- список названий пакетов из репозитория:  
`yum list`
- список всех доступных пакетов:  
`yum list available`
- список всех (или конкретных) установленных пакетов:  
`yum list installed`  
`yum list installed httpd`
- список всех установленных и доступных пакетов:  
`yum list all`
- список пакетов, относящихся к ядру:  
`yum list kernel`
- отображение информации о пакете `httpd`:  
`yum info httpd`
- перечень зависимостей и необходимых для установки `httpd` пакетов:  
`yum deplist httpd`
- поиск пакета, содержащего файл:  
`yum provides "*bin/top"`
- поиск пакета по имени и описанию:  
`yum search httpd`
- отображение информации о доступных обновлениях безопасности:  
`yum updateinfo list security`
- отображение списка групп пакетов:  
`yum grouplist`
- отображение описания и содержимого группы `Basic Web Server`:  
`yum groupinfo "Basic Web Server"`
- установка группы пакетов `Basic Web Server`:  
`yum groupinstall "Basic Web Server"`
- удаление группы `Basic Web Server`:  
`yum groupremove "Basic Web Server"`
- проверка на доступные в системе обновления:  
`yum check-update`
- отображение списка подключённых репозиторийев:  
`yum repolist`
- отображение информации об определённом репозитории:

- `yum repoinfo epel`
- вывод информации о пакетах в указанном репозитории:  
`yum repo-pkgs epel list`
- установка всех пакетов из репозитория:  
`yum repo-pkgs reponame install`
- удаление пакетов, установленных из репозитория:  
`yum repo-pkgs reponame remove`
- создание кэша:  
`yum makecache`
- проверка локальной базы rpm (поддерживаются параметры `dependencies`, `duplicates`, `obsoletes`, `provides`):  
`yum check`  
`yum check dependencies`
- просмотр yum истории (вывод списка транзакций):  
`yum history list`
- просмотр информации определённой транзакции:  
`yum history info 9`
- отмена транзакции:  
`yum history undo 9`
- повторить транзакции:  
`yum history redo 9`
- просмотр лог-файла выполнения транзакций:  
`cat /var/log/yum.log`
- удаление пакетов, сохранённых в кэше:  
`yum clean packages`
- удаление всех пакетов и метаданных:  
`yum clean all`
- установка пакета `httpd`:  
`yum install httpd`
- удаление пакета `httpd`:  
`yum remove httpd`
- обновление пакета `httpd`:  
`yum update httpd`
- обновление всех пакетов:  
`yum update`
- обновление до определённой версии:  
`yum update-to`
- установка из сети или локальной директории:  
`yum install http://server/repo/httpd.rpm`  
`yum install httpd.rpm`
- откат к предыдущей версии пакета:  
`yum downgrade`
- переустановка пакета (восстановление удалённых файлов):  
`yum reinstall httpd`
- удаление неиспользуемых более пакетов:  
`yum autoremove`
- создание локальных репозитория:  
`createrepo`
- установка обновлений по заданному расписанию:  
`yum-cron`

### 4.2.2. Опции yum

При работе с yum могут использоваться следующие опции:

- ответить «yes» при запросе:  
    -y  
    yum update -y
- ответить «no» при запросе:  
    --assumeno
- использовать yum без плагинов:  
    --noplugins
- отключить определённый плагин:  
    --disableplugin=fastestmirror
- включить плагины, которые установлены, но отключены:  
    yum --enableplugin=ps
- включить отключённый репозиторий:  
    yum update -y --enablerepo=epel
- отключить репозиторий:  
    yum update -y --disablerepo=epel
- скачать пакеты, но не устанавливать их:  
    yum install httpd --downloadonly

### 4.2.3. Расширение возможностей yum

Следующие команды доступны после установки пакета yum-utils.

- найти, из какого репозитория установлен пакет:  
    find-repos-of-install httpd
- найти процессы, пакеты которых обновлены и требуют рестарта:  
    needs-restarting
- запрос к репозиторию о зависимостях пакета без его установки:  
    repoquery --requires --resolve httpd
- синхронизация yum репозитория updates в локальную директорию repol:  
    reposync -p repol --repoid=updates
- проверка локального репозитория на целостность:  
    verifytree URL
- завершение транзакции:  
    yum-complete-transaction
- установка необходимых зависимостей для сборки rpm-пакета:  
    yum-builddep
- управление конфигурационными опциями и репозиториями yum:  
    yum-config-manager
- запрос к локальной базе yum, отображение информации о пакете (использованная команда, контрольная сумма, URL, с которого был установлен пакет, и др.):  
    yumdb info httpd
- скачать rpm-пакеты из репозитория:  
    yumdownloader
- скачать src.rpm пакет из репозитория (должен быть подключён соответствующий репозиторий, например в '/etc/yum.repos.d/CentOS-Sources.repo' в CentOS)  
    yumdownloader --source php

#### 4.2.4. Конфигурационные файлы yum и их расположение

Основной конфигурационный файл: `/etc/yum.conf`.

Директория с конфигурациями (например, yum плагины): `/etc/yum/`.

Директория с информацией о репозиториях: `/etc/yum.repos.d/`.

#### 4.2.5. Некоторые опции yum.conf

Директория, где yum хранит кэш и файлы базы (по умолчанию `/var/cache/yum`):

```
cachedir=/var/cache/yum/$basearch/$releasever
```

Опция, определяющая, должен или нет yum хранить кэш заголовков и пакетов после успешной установки. Значения опции: 0 или 1 (по умолчанию 1):

```
keepcache=1
```

Уровень вывода отладочных сообщений. Значения: 1–10 (по умолчанию 2):

```
debuglevel=2
```

Лог-файл (по умолчанию `/var/log/yum.log`):

```
logfile=/var/log/yum.log
```

Обновлять устаревшие пакеты:

```
obsoletes=1
```

Проверка подписи пакетов. Значения: 0 или 1 (по умолчанию 1):

```
gpgcheck=1
```

Включение плагинов. Значения: 0 или 1 (по умолчанию 1):

```
plugins=1
```

#### 4.2.6. Некоторые полезные плагины

Полезные плагины:

- добавление опции командной строки для просмотра изменения лог-файла до или после обновления: `yum-plugin-changelog`;
- выбор более быстрого репозитория из списка зеркал: `yum-plugin-fastestmirror`;
- добавление команд `keys`, `keys-info`, `keys-data`, `keys-remove` для работы с ключами: `yum-plugin-keys`;
- блокировка указанных пакетов от обновления (команда `yum versionlock`): `yum-plugin-versionlock`;
- добавление команд `yum verify-all`, `verify-multilib`, `verify-rpm` для проверки контрольных сумм пакетов: `yum-plugin-verify`.

#### 4.2.7. Работа Yum через прокси-сервер

Если требуется работать через прокси-сервер, то нужно добавить в секцию `[main]` в файле `/etc/yum.conf` запись:

```
proxy="http://server:3128"
```

При необходимости можно указать пароль:

```
proxy_proxy_username=user
```

```
proxy_password=pass
```

Для отдельного пользователя прокси указывается следующим образом:

```
export http_proxy="http://server:3128"
```

### 4.3. Задание

1. Изучите, как и в каких файлах подключаются репозитории для установки программного обеспечения; изучите основные возможности (поиск, установка, обновление, удаление пакета, работа с историей действий) команды `yum` (см. раздел 4.4.1).
2. Изучите и повторите процесс установки/удаления определённого пакета с использованием возможностей `yum` (см. раздел 4.4.2).
3. Изучите и повторите процесс установки/удаления определённого пакета с использованием возможностей `rpm` (см. раздел 4.4.3).

### 4.4. Последовательность выполнения работы

#### 4.4.1. Работа с репозиториями

1. В консоли перейдите в режим работы суперпользователя (используйте команду `su -`).
2. Перейдите в каталог `/etc/yum.repos.d` и изучите содержание каталога и файлов репозитория:

```
cd /etc/yum.repos.d
ls
cat CentOS-Base.repo
```

Пример файла репозитория:

```
CentOS-Base.repo
#
The mirror system uses the connecting IP address of the client and
↪ the
update status of each mirror to pick mirrors that are updated to and
↪ geographically close to the client. You should use this for CentOS
↪ updates
unless you are manually picking other mirrors.
#
If the mirrorlist= does not work for you, as a fall back you can try
↪ the
remarked out baseurl= line instead.
#
#
[base]
name=CentOS-$releasever - Base
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&
↪ arch=$basearch&repo=os&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
#released updates

[updates]
name=CentOS-$releasever - Updates
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&
↪ arch=$basearch&repo=updates&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/updates/
↪ $basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that may be useful
[extras]
name=CentOS-$releasever - Extras
```

```
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&
↪ arch=$basearch&repo=extras&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/extras/ $basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7

#additional packages that extend functionality of existing packages
[centosplus]
name=CentOS-$releasever - Plus
mirrorlist=http://mirrorlist.centos.org/?release=$releasever&
↪ arch=$basearch&repo=centosplus&infra=$infra
#baseurl=http://mirror.centos.org/centos/$releasever/centosplus/
↪ $basearch/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
```

3. Выведите на экран список репозиториев:  
yum repolist  
и поясните полученную информацию.
4. Выведите на экран список пакетов, в названии или описании которых есть слово user:  
yum search user  
и поясните полученную информацию.
5. Установите nmap, предварительно изучив информацию по имеющимся пакетам:  
yum search nmap  
yum info nmap  
yum install nmap  
yum install nmap\\*  
Поясните разницу между yum install nmap и yum install nmap\\*.  
Удалите nmap:  
yum remove nmap  
yum remove nmap\\*
6. Выведите на экран список всех пакетов, затем только пакетов, относящихся к ядру операционной системы:  
yum list  
yum list kernel
7. Обновите ядро операционной системы, а затем саму операционную систему:  
yum update kernel  
yum update
8. Получите список имеющихся групп пакетов, затем установите группу пакетов Basic Web Server:  
yum groups list  
LANG=C yum groups list  
yum groups info "Basic Web Server"  
yum groupinstall "Basic Web Server"  
Для удаления группы пакетов Basic Web Server можно воспользоваться командой:  
yum groupremove "Basic Web Server"
9. Посмотрите историю использования команды yum:  
yum history  
и отмените последнее, например шестое по счёту, действие:  
yum history undo 6

#### 4.4.2. Установка определённой программы

Предположим, что требуется установить программу `xeyes`.

1. Введите

```
yum search xeyes
```

Убедитесь, что система не выдаст полезной информации о пакете с данной программой.

2. Для вывода информации о пакете, содержащем программу `xeyes`, используйте команду:

```
yum provides */xeyes
```

Убедитесь, что пакет `xorg-x11-apps-<версия>` содержит файл с `xeyes`.

3. Установите пакет `xorg-x11-apps`, используя команду:

```
yum install -y xorg-x11-apps
```

```
yum list xorg-x11-apps
```

4. Удалите последний установленный пакет, используя возможности команды `yum history`:

```
yum history
```

```
yum history
```

```
yum history undo <nn>
```

(где `<nn>` заменяется номером действия, которое требуется отменить).

Убедитесь, что пакет `xorg-x11-apps` указан как доступный, но не установленный:

```
yum list xorg-x11-apps
```

#### 4.4.3. Использование `rpm`

1. Скачайте `rpm`-пакет `nmap`:

```
yum install nmap --downloadonly
```

и перейдите в каталог, в котором сохраняются файлы после загрузки:

```
cd /var/cache/yum/x86_64/7/base/packages/
```

```
ls
```

Установите `rpm`-пакет `nmap`:

```
rpm -Uhv nmap-<версия>.rpm
```

Удалите пакет:

```
rpm -e nmap
```

```
ls
```

2. Установите пакет `dnsmasq` (DNS-, DHCP- и TFTP-сервер):

```
yum list dnsmasq
```

```
yum install dnsmasq
```

и определите расположение исполняемого файла:

```
which dnsmasq
```

3. Используя `rpm`, определите по имени файла, к какому пакету принадлежит `dnsmasq`:

```
rpm -qf $(which dnsmasq)
```

и получите дополнительную информацию о содержимом пакета, введя:

```
rpm -qi dnsmasq
```

4. Получите список всех файлов в пакете, используя:

```
rpm -ql dnsmasq
```

а также выведите перечень файлов с документацией пакета, введя:

```
rpm -qd dnsmasq
```

Посмотрите файлы документации, применив команду `man dnsmasq`.

5. Выведите на экран перечень и месторасположение конфигурационных файлов пакета:

```
rpm -qc dnsmasq
```

6. Выведите на экран расположение и содержание скриптов, выполняемых при установке пакета:

```
rpm -q --scripts dnsmasq
```

и поясните, для чего предназначены скрипты.

#### 4.4.4. Исправление установки драйверов для VirtualBox

Установка необходимого программного обеспечения.

```
yum groupinstall "Development Tools"
```

```
yum install kernel-devel
```

Установка репозитория EPEL <https://fedoraproject.org/wiki/EPEL>.

```
yum install epel-release
```

Установка DKMS [https://ru.wikipedia.org/wiki/Dynamic\\_Kernel\\_Module\\_Support](https://ru.wikipedia.org/wiki/Dynamic_Kernel_Module_Support).

```
yum install dkms
```

#### 4.5. Содержание отчёта

Отчёт должен включать:

- 1) титульный лист с указанием номера лабораторной работы и ФИО студента;
- 2) формулировку задания работы;
- 3) описание результатов выполнения задания:
  - краткое описание действия;
  - вводимую команду или команды;
  - результаты выполнения команд (снимок экрана);
- 4) выводы, согласованные с заданием работы;
- 5) ответы на контрольные вопросы.

#### 4.6. Контрольные вопросы

1. Какая команда позволяет вам искать пакет `rpm`, содержащий файл `useradd`?
2. Какие команды вам нужно использовать, чтобы показать имя группы `yum`, которая содержит инструменты безопасности и показывает, что находится в этой группе?
3. Какая команда позволяет вам установить `rpm`, который вы загрузили из Интернета и который не находится в репозиториях?
4. Вы хотите убедиться, что пакет `rpm`, который вы загрузили, не содержит никакого опасного кода сценария. Какая команда позволяет это сделать?
5. Какая команда показывает всю документацию в `rpm`?
6. Какая команда показывает, какому пакету `rpm` принадлежит файл?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–4].



## Список литературы

1. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли. — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
2. *Neil N. J.* Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
3. *Vugt S. van.* Red Hat RHCSA/RHCE 7 cert guide : Red Hat Enterprise Linux 7 (EX200 and EX300). — Pearson IT Certification, 2016. — 1008 p. — (Certification Guide). — ISBN 978-0-7897-5405-9.
4. *Goyal S. K.* Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.

## Лабораторная работа № 5. Управление системными службами

### 5.1. Цель работы

Получить навыки управления системными службами операционной системы посредством `systemd`.

### 5.2. Предварительные сведения

*Systemd (system daemon)* — система инициализации служб операционной системы. Под системой инициализации в данном случае понимается набор скриптов, выполняемых на этапе загрузки операционной системы.

Для выполнения операций над системными службами в `systemd` используются юниты (units) — файлы конфигурации с определённым синтаксисом.

Посмотреть, какие типы юнитов используются в системе, можно при помощи следующей команды:

```
systemctl -t help
```

На данный момент выделяют следующие типы юнитов:

- `.service` — для запуска, остановки или перезагрузки системных служб;
- `.socket` — для работы с сокетами, связанными с определёнными службами;
- `.device` — для определения правил `udev` работы с устройствами;
- `.mount` — для монтирования файловой системы;
- `.automount` — для задания автоматического монтирования файловой системы;
- `.target` — логическая группировка юнитов, ссылающаяся на другие юниты (аналог концепции уровней запуска (runlevel));
- `.snapshot` — позволяет создавать ссылки на другие юниты, а также восстанавливать список ранее запущенных служб;
- `.timer` — позволяет задавать правила работы со службами по определённому расписанию (аналог `cron`);
- `.swap` — используется для управления файлами подкачки;
- `.path` — позволяет управлять службами, работающими с подсистемой `inotify` ядра Linux, управляющей уведомлениями о событиях, связанных с файлами и каталогами файловой системы

Каталоги расположения юнитов:

- `/usr/lib/systemd/system/` — автоматически созданные при установке пакетов юниты;
- `/run/systemd/system/` — юниты, созданные во время выполнения какой-либо службы;
- `/etc/systemd/system/` — юниты, созданные системным администратором.

Файлы юнитов содержат разделы с набором параметров и их значений, разделённых знаком «`=`»:

**[Название секции]**

имя переменной = значение

Обработка зависимостей запуска служб может быть описана с помощью конструкций `Requires=B` (или `Wants=B`) и `After=B` в секции `[Unit]`.

Тип запуска службы определяется параметром `Type=` в секции `[Service]`. Например, `Type=simple` предполагает, что служба будет запущена незамедлительно, но процесс при этом не должен разветвляться. Запись `Type=forking` предполагает, что служба будет запущена однократно и процесс разветвится с завершением родительского процесса.

Более детальное пояснение содержания файлов юнитов см. в справочном руководстве `systemd.service(5)`.

Далее приведены несколько примеров файлов юнитов.

Пример файла юнита сервиса `vsftpd.service`:

```
[Unit]
Description=Vsftpd ftp daemon
After=network.target

[Service]
Type=forking
ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

[Install]
WantedBy=multi-user.target
```

Пример файла юнита монтирования `tmp.mount`:

```
[Unit]
Description=Temporary Directory
Documentation=man:hier(7)
Documentation=http://www.freedesktop.org/wiki/Software
↳ /systemd/APIFileSystems
DefaultDependencies=no
Conflicts=umount.target
Before=local-fs.target umount.target

[Mount]
What=tmpfs
Where=/tmp
Type=tmpfs
Options=mode=1777,strictatime

Make 'systemctl enable tmp.mount' work:
[Install]
WantedBy=local-fs.target
```

Файл цели на примере `multi-user.target`:

```
[Unit]
Description=Multi-User System
Documentation=man:systemd.special(7)
Requires=basic.target
Conflicts=rescue.service rescue.target
After=basic.target rescue.service rescue.target
AllowIsolate=yes

[Install]
Alias=default.target
```

Основные команды работы с юнитами `systemd`:

- запустить юнит:  
    `systemctl start название_юнита`
- остановить юнит:  
    `systemctl stop название_юнита`
- перезапустить юнит:  
    `systemctl restart название_юнита`
- перезагрузить настройки юнита:

- `systemctl reload название_юнита`
- посмотреть статус юнита:  
`systemctl status название_юнита`
- проверить, включён ли юнит в автозапуск при загрузке системы:  
`systemctl is-enabled название_юнита`
- добавить юнит в автозапуск при загрузке системы:  
`systemctl enable название_юнита`
- удалить юнит из автозапуска при загрузке системы:  
`systemctl disable название_юнита`
- маскировать юнит, чтобы сделать невозможным его запуск:  
`systemctl mask название_юнита`
- снять маску юнита:  
`systemctl unmask название_юнита`
- вызвать справку по юниту:  
`systemctl help юнит`
- перезагрузить `systemd` для поиска новых или изменённых юнитов:  
`systemctl daemon-reload`

Для просмотра значений опций юнита используется следующая команда (на примере `sshd`):

```
systemctl show sshd
```

### 5.3. Задание

1. Выполните основные операции по запуску (останову), определению статуса, добавлению (удалению) в автозапуск и пр. службы Very Secure FTP (раздел 5.4.1).
2. Продемонстрируйте навыки по разрешению конфликтов юнитов для служб `firewalld` и `iptables` (раздел 5.4.2).
3. Продемонстрируйте навыки работы с изолированными целями (разделы 5.4.3, 5.4.4).

## 5.4. Последовательность выполнения работы

### 5.4.1. Управление сервисами

1. Получите полномочия администратора  
`su -`
2. Проверьте статус службы Very Secure FTP:  
`systemctl status vsftpd`  
Вывод команды должен показать, что сервис в настоящее время отключён, так как служба Very Secure FTP не установлена.
3. Установите службу Very Secure FTP:  
`yum -y install vsftpd`
4. Запустите службу Very Secure FTP:  
`systemctl start vsftpd`
5. Проверьте статус службы Very Secure FTP:  
`systemctl status vsftpd`  
Вывод команды должен показать, что служба в настоящее время работает, но не будет активирована при перезапуске операционной системы.

6. Добавьте службу Very Secure FTP в автозапуск при загрузке операционной системы, используя команду `systemctl enable`. Затем проверьте статус службы. Удалите службу из автозапуска, используя команду `systemctl disable`, и снова проверьте её статус.
7. Выведите на экран символические ссылки, ответственные за запуск различных сервисов:  

```
ls /etc/systemd/system/multi-user.target.wants
```

Должно отобразиться, что ссылка на `vsftpd.service` не существует.
8. Снова добавьте службу Very Secure FTP в автозапуск:  

```
systemctl enable vsftpd
```

и выведите на экран символические ссылки, ответственные за запуск различных сервисов.  
Вывод команды покажет, что создана символическая ссылка для файла `/usr/lib/systemd/system/vsftpd.service` в каталоге `/etc/systemd/system/multi-user.target.wants`.
9. Снова проверьте статус службы Very Secure FTP:  

```
systemctl status vsftpd
```

Теперь вы увидите, что для файла юнита состояние изменено с `disabled` на `enabled`.
10. Выведите на экран список зависимостей юнита:  

```
systemctl list-dependencies vsftpd
```
11. Выведите на экран список юнитов, которые зависят от данного юнита:  

```
systemctl list-dependencies vsftpd --reverse
```

### 5.4.2. Конфликты юнитов

Некоторые юниты могут конфликтовать друг с другом и, соответственно, не могут работать одновременно, например, `mount` и `umount`, `network` и `NetworkManager`, `iptables` и `firewalld`, `cronyd` и `ntpd`.

На примере `iptables` и `firewalld` продемонстрируем навыки разрешения конфликтов запуска сервисов.

1. Получите полномочия администратора. Установите `iptables`:  

```
yum -y install iptables*
```
2. Проверьте статус `firewalld` и `iptables`:  

```
systemctl status firewalld
systemctl status iptables
```
3. Попробуйте запустить `firewalld` и `iptables`:  

```
systemctl start firewalld
systemctl start iptables
```

Вы увидите, что `iptables` отказывается запускаться, так как служба `firewalld` уже активирована.
4. Введите  

```
cat /usr/lib/systemd/system/firewalld.service
```

и опишите настройки конфликтов для этого юнита.
5. Введите  

```
cat /usr/lib/systemd/system/iptables.service
```

и опишите настройки конфликтов для этого юнита.
6. Выгрузите службу `iptables` (на всякий случай, чтобы убедиться, что данная служба не загружена в систему):  

```
systemctl stop iptables
```
7. Заблокируйте запуск `iptables`, введя:  

```
systemctl mask iptables
```

Будет создана символическая ссылка на `/dev/null` для `/etc/systemd/system/iptables.service` (проверьте это). Поскольку юнит-файлы в `/etc/systemd` имеют приоритет над файлами в `/usr/lib/systemd`, то это сделает невозможным случайный запуск сервиса `iptables`.

8. Попробуйте запустить `iptables`:

```
systemctl start iptables
```

Должно появиться сообщение об ошибке, указывающее, что служба замаскирована и по этой причине не может быть запущена.

9. Попробуйте добавить `iptables` в автозапуск:

```
systemctl enable iptables
```

Сервис будет неактивен, а статус загрузки отобразится как замаскированный.

### 5.4.3. Изолируемые цели

В системе `systemd` существует несколько специальных наборов юнитов — целей. Некоторые цели играют особую роль, поскольку могут быть изолированы.

Изолируемые цели — это объекты, которые могут быть установлены в качестве цели по умолчанию. Они примерно соответствуют уровням запуска *SystemV init*:

- `poweroff.target` — `runlevel 0`;
- `rescue.target` — `runlevel 1`;
- `multi-user.target` — `runlevel 3`;
- `graphical.target` — `runlevel 5`;
- `reboot.target` — `runlevel 6`.

Изолируя цель, вы запускаете эту цель со всеми её зависимостями. Не все цели могут быть изолированы.

Если вы посмотрите на содержимое изолируемых целей, вы увидите, что они содержат строку `AllowIsolate = yes`. Чтобы получить список всех активных загруженных целей, введите:

```
systemctl --type=target
```

Чтобы получить список всех целей, введите:

```
systemctl --type=target --all
```

1. Получите полномочия администратора. Перейдите в каталог `systemd` и найдите список всех целей, которые можно изолировать:

```
cd /usr/lib/systemd/system
grep Isolate *.target
```

2. Переключите операционную систему в режим восстановления:

```
systemctl isolate rescue.target
```

При этом необходимо ввести пароль `root` на консоли сервера для входа в систему.

3. Перезапустите операционную систему следующим образом:

```
systemctl isolate reboot.target
```

### 5.4.4. Цель по умолчанию

1. Получите полномочия администратора. Выведите на экран цель, установленную по умолчанию:

```
systemctl get-default
```

2. Для установки цели по умолчанию используется команда

```
systemctl set-default
```

Например, для запуска по умолчанию графического режима введите:

```
systemctl set-default graphical.target
```

Для запуска по умолчанию текстового режима введите:

```
systemctl set-default multi-user.target
```

## 5.5. Содержание отчёта

Отчёт должен включать:

- 1) титульный лист с указанием номера лабораторной работы и ФИО студента;
- 2) формулировку задания работы;
- 3) описание результатов выполнения задания:
  - краткое описание действия;
  - вводимую команду или команды;
  - результаты выполнения команд (снимок экрана);
- 4) выводы, согласованные с заданием работы;
- 5) ответы на контрольные вопросы.

## 5.6. Контрольные вопросы

1. Что такое юнит (`unit`)?
2. Какая команда позволяет вам убедиться, что цель больше не входит в список автоматического запуска при загрузке системы?
3. Какую команду вы должны использовать для отображения всех сервисных юнитов, которые в настоящее время загружены?
4. Как вы создаёте потребность (`wants`) в сервисе?
5. Как вы переключаете текущее состояние на цель восстановления (`rescue target`)?
6. Поясните причину получения сообщения о том, что цель не может быть изолирована?
7. Вы хотите отключить службу `systemd`, но, прежде чем сделать это, вы хотите узнать, какие другие юниты зависят от этой службы. Какую команду вы бы использовали?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–4]

## Список литературы

1. *Поттеринг Л.* Systemd для администраторов: цикл статей. — 2010. — URL: <http://wiki.opennet.ru/Systemd>.
2. *systemd*. — 2015. — URL: <https://wiki.archlinux.org/index.php/Systemd>.
3. *Neil N. J.* Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
4. *Goyal S. K.* Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.

## Лабораторная работа № 6. Управление процессами

### 6.1. Цель работы

Получить навыки управления процессами операционной системы.

### 6.2. Предварительные сведения

Под процессом в операционной системе понимается абстракция, описывающая выполняющуюся программу.

Информацию о выполняющихся в операционной системе типа Unix процессах можно получить, например, с помощью команд `ps`, `top`, `htop`.

#### 6.2.1. Команда `ps`

В выводе программы `ps` могут присутствовать следующие поля:

- `USER` — имя владельца процесса;
- `PID` — идентификатор процесса в системе;
- `PPID` — идентификатор родительского процесса;
- `%CPU` — доля времени центрального процессора (в процентах), выделенного для данного процесса;
- `%MEM` — доля реальной памяти (в процентах), используемая данным процессом;
- `VSZ` — виртуальный размер процесса (в килобайтах);
- `RSS` — размер резидентного набора (количество 1К-страниц в памяти);
- `STIME` — время старта процесса;
- `TTY` — указание на терминал, с которого запущен процесс;
- `S` или `STAT` — статус процесса;
- `PRI` — приоритет планирования;
- `NI` — значение `nice`;
- `TIME` — сколько времени центрального процессора занял данный процесс;
- `CMD` или `COMMAND` — командная строка запуска программы, выполняемой данным процессом.

В поле *Статус процесса* могут быть указаны следующие значения:

- `R` (Running) — в настоящее время процесс активен и использует процессорное время или находится в очереди запущенных процессов, ожидающих выделения ему очередного кванта времени;
- `S` (Sleeping) — процесс ожидает завершения события;
- `D` (Uninterruptable sleep) — процесс находится в состоянии ожидания, которое невозможно остановить; обычно это происходит, когда процесс ожидает ввода-вывода;
- `T` (Terminated) — процесс остановлен;
- `Z` (Zombie) — процесс был остановлен, но не может быть остановлен его родителем, который поставил его в неуправляемое состояние.

GNU-версия команды `ps` поддерживает для совместимости опции BSD (без дефиса) и опции System V (с дефисом перед однобуквенными опциями). При этом опции разных типов нельзя употреблять в одной команде.

Вывести список всех процессов в системе (System V вариант):

```
ps -e
```

Можно к той же команде добавить опцию `-o`, после которой указать через запятую, какие именно поля вы хотите видеть в выводе команды:



```
ps -eo pid,user,cmd
```

Вывести список всех процессов в системе (BSD вариант):

```
ps ax
```

Вывести список всех процессов в системе, отобразив отношения предок–потомок:

```
ps fax
```

Также можно воспользоваться командой `pstree`.

## 6.2.2. Задания

Процессы, запущенные из текущего экземпляра оболочки *shell*, называют *заданиями (jobs)*.

Команда `jobs` выводит порядковый номер задания в виде числа в квадратных скобках. После номера указывается состояние процесса: *stopped (остановлен)*, *running (выполняется)* или *suspended (приостановлен)*. В конце строки указывается команда, которая выполняется данным процессом.

В выводе результата выполнения команды `jobs` один из порядковых номеров заданий отмечен знаком «-» и обозначает таким образом задание по умолчанию. Задание, отмеченное знаком «-», станет заданием по умолчанию после завершения текущего задания по умолчанию.

Если вы запускаете какой-то процесс путём запуска программы из командной строки, то обычно процесс запускается *на переднем плане*, то есть он захватывает терминал, с которого запущен, воспринимая ввод с этого терминала и осуществляя на него вывод. Можно запустить процесс *в фоновом режиме*, чтобы он не был связан с терминалом. Для этого в конце строки вызова команды добавляют символ `&`.

В оболочке `bash` две встроенные команды служат для перевода процессов на передний план (команда `fg`) или возврата их в фоновый режим (команда `bg`). В качестве аргумента этим командам передаются номера заданий. Если аргументы отсутствуют, то подразумевается задание, помеченное знаком `+`. Можно указать задание и по номеру, предваряя его знаком процента:

```
fg %1
```

## 6.2.3. Приоритеты

Приоритет для каждого процесса устанавливается в тот момент, когда процесс порождается и задаётся величиной *nice*. Значение этой величины лежит в пределах от `+20` (наименьший приоритет — процесс выполняется только тогда, когда ничто другое не занимает процессор) до `-20` (наивысший приоритет).

Значение *nice* устанавливается для каждого процесса в момент его порождения и при обычном запуске команд или программ принимается равным приоритету родительского процесса. Существует специальная команда *nice*, которая позволяет изменять значение приоритета процесса при запуске программы:

```
nice [-<add-nice>] command [args]
```

Здесь *add-nice* — значение (от `-20` до `+19`), добавляемое к значению *nice* процесса-родителя. Полученная сумма и будет значением *nice* для запускаемого процесса. Отрицательные значения может устанавливать только суперпользователь. Если опция *add-nice* не задана, то по умолчанию для процесса-потомка устанавливается значение *nice*, увеличенное на 10 по сравнению со значением *nice* родительского процесса.

Команда `renice` служит для изменения значения *nice* для уже выполняющихся процессов:

```
renice [-n] priority [[-p] PID] [[-g] grp] [[-u] user]
```

или

```
renice [-n] priority [[-p] PID] [[-g] grp] [[-u] user]
```

Например, команда

```
renice -1 987 -u daemon -p 32
```

увеличивает на 1 приоритет процессов с PID 987 и 32, а также всех процессов пользователя `daemon`.

Суперпользователь может изменить приоритет любого процесса в системе. Другие пользователи могут изменять значение приоритета только для тех процессов, для которых данный пользователь является владельцем. При этом обычный пользователь может только уменьшить значение приоритета (увеличить значение *nice*).

#### 6.2.4. Команда `nohup`

Предположим, вы запустили из оболочки `bash` несколько процессов, часть из них в фоновом режиме, а затем завершили её. При завершении сессии оболочка завершает порождённые ею процессы. Если вы хотите запустить в фоновом режиме программу, которая должна выполняться и после вашего выхода из оболочки, то её нужно запускать с помощью утилиты `nohup`:

`nohup команда &`

Стандартный выходной поток и стандартный поток ошибок при таком запуске команд перенаправляются в файл `nohup.out` в текущем каталоге или `$HOME/nohup.out`. Команда `nohup` имеет побочный эффект, заключающийся в том, что значение *nice* для запускаемого процесса увеличивается на 5, т.е. процесс выполняется с более низким приоритетом.

### 6.3. Задание

1. Продемонстрируйте навыки управления заданиями операционной системы (см. раздел 6.4.1).
2. Продемонстрируйте навыки управления процессами операционной системы (см. раздел 6.4.2).
3. Выполните задания для самостоятельной работы (см. раздел 6.5)

### 6.4. Последовательность выполнения работы

#### 6.4.1. Управление заданиями

1. Получите полномочия администратора  
`su -`
2. Введите следующие команды:  

```
sleep 3600 &
dd if=/dev/zero of=/dev/null &
sleep 7200
```
3. Поскольку вы запустили последнюю команду без `&` после неё, у вас есть время 2 часа, прежде чем вы снова получите контроль над оболочкой. Введите `Ctrl + z`, чтобы остановить процесс.
4. Введите  
`jobs`  
Вы увидите три задания, которые вы только что запустили. Первые два имеют состояние `Running`, а последнее задание в настоящее время находится в состоянии `Stopped`.
5. Для продолжения выполнения задания 3 в фоновом режиме введите:  
`bg 3`

6. Для перемещения задания 1 на передний план введите:  
`fg 1`
7. Введите `Ctrl`+`c`, чтобы отменить задание 1.
8. Просмотрите текущее состояние процесса:  
`jobs`
9. Прodelайте то же самое для отмены заданий 2 и 3.
10. Откройте второй терминал и введите в нём:  
`dd if=/dev/zero of=/dev/null &`
11. Введите `exit`, чтобы закрыть второй терминал.
12. На другом терминале запустите  
`top`  
Вы увидите, что задание `dd` всё ещё запущено.
13. Внутри `top` используйте `k`, чтобы убить задание `dd`.

### 6.4.2. Управление процессами

1. Получите полномочия администратора  
`su -`
2. Введите следующие команды:  
`dd if=/dev/zero of=/dev/null &`  
`dd if=/dev/zero of=/dev/null &`  
`dd if=/dev/zero of=/dev/null &`
3. Введите  
`ps aux | grep dd`  
Это показывает все строки, в которых есть буквы `dd`. Запущенные процессы `dd` идут последними.
4. Используйте PID одного из процессов `dd`, чтобы изменить приоритет. Используйте  
`renice -n 5 <PID>`
5. Введите  
`ps fax | grep -B5 dd`  
Параметр `-B5` показывает соответствующие запросу строки, включая пять строк до этого. Поскольку  
`ps fax`  
показывает иерархию отношений между процессами, вы также увидите оболочку, из которой были запущены все процессы `dd`, и её PID
6. Найдите PID оболочки, из которой были запущены процессы `dd`, и введите  
`kill -9 <PID>`  
(заменяв `<PID>` на значение PID оболочки). Вы увидите, что ваша корневая оболочка закрылась, а вместе с ней и все процессы `dd`. Остановка родительского процесса — простой и удобный способ остановить все его дочерние процессы.

## 6.5. Самостоятельная работа

### 6.5.1. Задание 1

1. Запустите команду  
`dd if=/dev/zero of=/dev/null`  
трижды как фоновое задание.
2. Увеличьте приоритет одной из этих команд, используя значение приоритета `-5`.
3. Измените приоритет того же процесса ещё раз, но используйте на этот раз значение `-15`. В чём разница?
4. Завершите все процессы `dd`, которые вы запустили.

### 6.5.2. Задание 2

1. Запустите программу `yes` в фоновом режиме с подавлением потока вывода.
2. Запустите программу `yes` на переднем плане с подавлением потока вывода. Приостановите выполнение программы. Заново запустите программу `yes` с теми же параметрами, затем завершите её выполнение.
3. Запустите программу `yes` на переднем плане без подавления потока вывода. Приостановите выполнение программы. Заново запустите программу `yes` с теми же параметрами, затем завершите её выполнение.
4. Проверьте состояния заданий, воспользовавшись командой `jobs`.
5. Переведите процесс, который у вас выполняется в фоновом режиме, на передний план, затем остановите его.
6. Переведите любой ваш процесс с подавлением потока вывода в фоновый режим.
7. Проверьте состояния заданий, воспользовавшись командой `jobs`. Обратите внимание, что процесс стал выполняющимся (Running) в фоновом режиме.
8. Запустите процесс в фоновом режиме таким образом, чтобы он продолжил свою работу даже после отключения от терминала.
9. Закройте окно и заново запустите консоль. Убедитесь, что процесс продолжил свою работу.
10. Получите информацию о запущенных в операционной системе процессах с помощью утилиты `top`.
11. Запустите ещё три программы `yes` в фоновом режиме с подавлением потока вывода.
12. Убейте два процесса: для одного используйте его PID, а для другого его идентификатор конкретного задания.
13. Попробуйте послать сигнал 1 (SIGHUP) процессу, запущенному с помощью `nohup`, и обычному процессу.
14. Запустите ещё несколько программ `yes` в фоновом режиме с подавлением потока вывода.
15. Завершите их работу одновременно, используя команду `killall`.
16. Запустите программу `yes` в фоновом режиме с подавлением потока вывода. Используя утилиту `nice`, запустите программу `yes` с теми же параметрами и с приоритетом, большим на 5. Сравните абсолютные и относительные приоритеты у этих двух процессов.
17. Используя утилиту `renice`, измените приоритет у одного из потоков `yes` таким образом, чтобы у обоих потоков приоритеты были равны.

### 6.6. Содержание отчёта

Отчёт должен включать:

- 1) титульный лист с указанием номера лабораторной работы и ФИО студента;
- 2) формулировку задания работы;
- 3) описание результатов выполнения задания:
  - краткое описание действия;
  - вводимую команду или команды;
  - результаты выполнения команд (снимок экрана);
- 4) выводы, согласованные с заданием работы;
- 5) ответы на контрольные вопросы.

## 6.7. Контрольные вопросы

1. Какая команда даёт обзор всех текущих заданий оболочки?
2. Как остановить текущее задание оболочки, чтобы продолжить его выполнение в фоновом режиме?
3. Какую комбинацию клавиш можно использовать для отмены текущего задания оболочки?
4. Необходимо отменить одно из начатых заданий. Доступ к оболочке, в которой в данный момент работает пользователь, невозможен. Что можно сделать, чтобы отменить задание?
5. Какая команда используется для отображения отношений между родительскими и дочерними процессами?
6. Какая команда позволит изменить приоритет процесса с идентификатором 1234 на более высокий?
7. В системе в настоящее время запущено 20 процессов `dd`. Как проще всего остановить их все сразу?
8. Какая команда позволяет остановить команду с именем `mycommand`?
9. Какая команда используется в `top`, чтобы убить процесс?
10. Как запустить команду с достаточно высоким приоритетом, не рискуя, что не хватит ресурсов для других процессов?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–7].

## Список литературы

1. UNIX Power Tools / M. Loukides, T. O'Reilly, J. Peek, S. Powers. — O'Reilly Media, 2009. — 1160 p.
2. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010. — 656 с. — ISBN 978-5-94157-538-1.
3. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
4. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли. — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
5. Таненбаум Э., Бос Х. Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — 1120 с. — (Классика Computer Science).
6. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
7. Goyal S. K. Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.

## Лабораторная работа № 7. Управление журналами событий в системе

### 7.1. Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

### 7.2. Предварительные сведения

#### 7.2.1. Основные файлы журналов

В системах на базе Unix/Linux важное место при администрировании занимает отслеживание системных событий (и в частности, возникновение возможных ошибок в процессе настройки каких-то служб) через ведение log-файлов процессов системы. Журналирование системных событий заключается в фиксировании с помощью сокета `syslog` в лог-файлах сообщений об ошибках и сообщений о состоянии работы практически всех процессов системы. Обычно лог-файлы располагаются в каталоге `/var/log`:

- `/var/log/messages` — общий файл журнала, в который записывается большинство сообщений системы (наиболее часто используемый файл журнала);
- `/var/log/dmesg` — журнал сообщений ядра системы;
- `/var/log/secure` — журнал сообщений, связанных с аутентификацией в системе;
- `/var/log/boot.log` — журнал сообщений, связанных с запуском системы;
- `/var/log/audit/audit.log` — журнал сообщений аудита (например, в него записываются сообщения *SELinux*);
- `/var/log/maillog` — журналы сообщений, связанных с почтовой службой;
- `/var/log/samba` — журналы сообщений службы *samba* (*samba* по умолчанию не управляется через *rsyslogd*);
- `/var/log/sssd` — журналы сообщений службы *sssd*;
- `/var/log/cups` — журналы службы печати *cups*;
- `/var/log/httpd/` — каталог с журналами веб-службы *Apache* (*Apache* записывает сообщения в эти файлы напрямую, а не через *rsyslog*).

#### 7.2.2. Категории rsyslogd

Сообщения в `rsyslogd` относятся к той или иной категории. Категории сообщений и их приоритетность обеспечивают иерархичность системы хранения журналов сообщений системы и скорость реагирования на возникновение критичных для её работы событий.

Выделяют следующие категории:

- `auth/authpriv` — сообщения, связанные с аутентификацией;
- `cron` — сообщения, генерируемые службой *cron*;
- `daemon` — сообщения от неспецифицированных демонов;
- `kern` — сообщения ядра;
- `lpr` — сообщения, созданные через устаревшую систему печати *lpr*;
- `mail` — сообщения, связанные с электронной почтой;
- `mark` — специальный объект, который можно использовать для записи маркера;
- `news` — сообщения, созданные системой новостей *NNTP*;
- `security` — то же, что и `auth/authpriv` (не нужно использовать);

- `syslog` — сообщения, созданные системой `syslog`;
- `user` — сообщения, сгенерированные в пространстве пользователя;
- `uucp` — сообщения, созданные устаревшей системой `UUCP`;
- `local0-7` — сообщения, генерируемые службами, которые настроены любым из локальных объектов.

### 7.2.3. Приоритеты `rsyslogd`

По важности (уровню опасности) сообщения разделяются по приоритетам:

- `debug` — отладочные сообщения (уровень опасности 7);
- `info` — информационные сообщения о нормальной работе (уровень опасности 6);
- `notice` — используется для информационных сообщений об элементах, которые могут стать проблемой позже (уровень опасности 5);
- `warning/warn` — что-то происходит, но пока нет реальной ошибки (уровень опасности 4);
- `err/error` — некритическая ошибка (уровень опасности 3);
- `crit` — критическая ошибка (уровень опасности 2);
- `alert` — используется, когда доступность службы под угрозой (уровень опасности 1);
- `emerg/panic` — сообщение генерируется, когда служба не доступна (уровень опасности 0).

## 7.3. Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени (см. раздел 7.4.1).
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы (см. раздел 7.4.2).
3. Продемонстрируйте навыки работы с `journalctl` (см. раздел 7.4.3).
4. Продемонстрируйте навыки работы с `journald` (см. раздел 7.4.4).

## 7.4. Последовательность выполнения работы

### 7.4.1. Мониторинг журнала системных событий в реальном времени

1. Запустите терминал и получите полномочия администратора:  
`su -`
2. Запустите мониторинг системных событий в реальном времени:  
`tail -f /var/log/messages`
3. В дополнительном терминале попробуйте получить полномочия администратора, но введите неправильный пароль. Обратите внимание, что в первом терминале с мониторингом событий ничего не отображается, так же как и в файле `/var/log/messages`. Это связано с тем, что ошибки входа в систему сюда не записываются.
4. Во втором терминале из оболочки пользователя введите:  
`logger hello`  
В первом терминале с мониторингом событий вы увидите сообщение, которое также будет зафиксировано в файле `/var/log/messages`.
5. В первом терминале остановите трассировку файла сообщений мониторинга реального времени, используя `Ctrl` + `C`.

6. Запустите мониторинг сообщений безопасности (последние 20 строк соответствующего файла логов):

```
tail -n 20 /var/log/secure
```

Вы увидите сообщения, которые ранее были зафиксированы во время ошибки авторизации при вводе команды `su`.

### 7.4.2. Изменение правил `rsyslog.conf`

По умолчанию веб-служба не регистрирует свои сообщения через `rsyslog`, а пишет свой собственный журнал (в каталоге `/var/log/httpd`). Настройте регистрацию сообщений веб-службы через `syslog`, создав правило, регистрирующее отладочные сообщения в отдельном лог-файле. Для этого выполните следующие действия.

1. Запустите терминал и получите полномочия администратора. Установите Apache, если он не был ранее установлен:

```
yum -y install httpd
```
2. Запустите веб-службу:

```
systemctl start httpd
```

```
systemctl enable httpd
```
3. Посмотрите журнал сообщений об ошибках веб-службы:

```
tail -f /var/log/httpd/error_log
```
4. В файле конфигурации `/etc/httpd/conf/httpd.conf` в конце добавьте следующую строку:

```
ErrorLog syslog:local1
```

5. В каталоге `/etc/rsyslog.d` создайте файл мониторинга событий веб-службы:

```
cd /etc/rsyslog.d
```

```
touch httpd.conf
```

Открыв его на редактирование, пропишите в нём:

```
local1.* -/var/log/httpd-error.log
```

Эта строка позволит отправлять все сообщения, получаемые для объекта `local1` (который теперь используется службой `httpd`), в файл `/var/log/httpd-error.log`.

6. Перезагрузите конфигурацию `rsyslogd` и веб-службу:

```
systemctl restart rsyslog.service
```

```
systemctl restart httpd
```
7. Все сообщения об ошибках веб-службы теперь будут записаны в файл `/var/log/httpd-error.log`.
8. Создайте отдельный файл конфигурации для мониторинга отладочной информации:

```
cd /etc/rsyslog.d
```

```
touch debug.conf
```

В терминале введите:

```
echo "*.debug /var/log/messages-debug" >
```

```
↵ /etc/rsyslog.d/debug.conf
```

9. Снова перезапустите `rsyslogd`:

```
systemctl restart rsyslog.service
```
10. Запустите мониторинг отладочной информации:

```
tail -f /var/log/messages-debug
```
11. В дополнительном терминале введите:

```
logger -p daemon.debug "Daemon Debug Message"
```



12. В терминале с мониторингом посмотрите сообщение отладки. Используйте `Ctrl` + `c`, чтобы закрыть трассировку файла журнала.

### 7.4.3. Использование `journalctl`

1. В терминале получите полномочия администратора:  
`su -`
2. Посмотрите содержимое журнала с событиями с момента последнего запуска системы:  
`journalctl`  
Для пролистывания журнала используйте или `Enter` (построчный просмотр), или пробел (постраничный просмотр). Для выхода из просмотра используйте `q`.
3. Просмотр содержимого журнала без использования пейджера:  
`journalctl --no-pager`
4. Режим просмотра журнала в реальном времени:  
`journalctl -f`  
Используйте `Ctrl` + `c` для прерывания просмотра.
5. Для использования фильтрации просмотра конкретных параметров журнала введите `journalctl` и дважды нажмите клавишу `Tab`.
6. Посмотрите события для `UID0`:  
`journalctl _UID=0`
7. Для отображение последних 20 строк журнала введите:  
`journalctl -n 20`
8. Для просмотра только сообщений об ошибках введите:  
`journalctl -p err`
9. Если вы хотите просмотреть сообщения журнала, записанные за определённый период времени, вы можете использовать параметры `--since` и `--until`. Обе опции принимают параметр времени в формате `YYYY-MM-DD hh:mm:ss`  
Кроме того, вы можете использовать *yesterday*, *today* и *tomorrow* в качестве параметров. Например, для просмотра всех сообщений со вчерашнего дня введите:  
`journalctl --since yesterday`
10. Если вы хотите показать все сообщения с ошибкой приоритета, которые были зафиксированы со вчерашнего дня, то используйте:  
`journalctl --since yesterday -p err`
11. Если вам нужна детальная информация, то используйте:  
`journalctl -o verbose`
12. Для просмотра дополнительной информации о модуле `sshd` введите:  
`journalctl _SYSTEMD_UNIT=sshd.service`

### 7.4.4. Постоянный журнал `journald`

По умолчанию журнал *journald* хранит сообщения в оперативной памяти системы и записи доступны в каталоге `/run/log/journal` только до перезагрузки системы. Для того чтобы сделать журнал *journald* постоянным, выполните следующие действия.

1. Запустите терминал и получите полномочия администратора:  
`su -`
2. Создайте каталог для хранения записей журнала:  
`mkdir -p /var/log/journal`

3. Скорректируйте права доступа для каталога `/var/log/journal`, чтобы *journal*d смог записывать в него информацию:  

```
chown root:systemd-journal /var/log/journal
chmod 2755 /var/log/journal
```
4. Для принятия изменений необходимо или перезагрузить систему (перезапустить службу `systemd-journald` недостаточно), или использовать команду:  

```
killall -USR1 systemd-journald
```
5. Журнал *systemd* теперь постоянный. Если вы хотите видеть сообщения журнала с момента последней перезагрузки, используйте:  

```
journalctl -b
```

## 7.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание настроек системы в соответствии с заданием;
  - полные тексты конфигурационных файлов настраиваемых в работе служб;
  - результаты проверки корректности настроек системы в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы со скриншотами результатов запуска команд в случае, если вопрос подразумевает выполнение упражнения.

## 7.6. Контрольные вопросы

1. Какой файл используется для настройки *rsyslogd*?
2. В каком файле журнала *rsyslogd* содержатся сообщения, связанные с аутентификацией?
3. Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?
4. Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом `info` в файл `/var/log/messages.info`?
5. Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?
6. Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?
7. Какая команда позволяет вам видеть сообщения *journal*d после последней перезагрузки системы?
8. Какая процедура позволяет сделать журнал *journal*d постоянным?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–5].

## Список литературы

1. Поттеринг Л. Systemd для администраторов: цикл статей. — 2010. — URL: <http://wiki.opennet.ru/Systemd>.

2. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли. — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
3. Емельянов А. Управление логгированием в systemd. — 2015. — URL: <https://blog.selectel.ru/upravlenie-loggirovaniem-v-systemd/>.
4. Neil N. J. Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
5. Goyal S. K. Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.

## Лабораторная работа № 8. Планировщики событий

### 8.1. Цель работы

Получение навыков работы с планировщиками событий `cron` и `at`.

### 8.2. Предварительные сведения

При администрировании часто возникают задачи автоматизации выполнения каких-то одноразовых или регулярных рутинных действий по заданному расписанию (например, резервное копирование, ротация системных журналов и пр.). Для этих целей могут применяться, в частности, служба `at` (для одноразовых задач) и служба `cron` (для регулярных задач).

Общесистемные файлы конфигурации расписаний запуска службы `cron` располагаются в `/etc/crontab` и в файлах каталога `/etc/cron.d`. Файлы с настройками расписания запуска заданных пользователем задач обычно располагаются в каталоге `/var/spool/cron`.

Демон `crond` регулярно считывает расписания, загруженные в оперативную память системы, и запускает задачи от имени соответствующего пользователя согласно указанному в расписании времени.

Формат общесистемного расписания:

```
Установка переменных окружения
name = value
Строка расписания
mm hh DD MM DW user cmd [arg...]
```

Формат пользовательского расписания:

```
Установка переменных окружения
name = value
Строка расписания
mm hh DD MM DW cmd [arg...]
```

Здесь `mm hh DD MM DW` — время выполнения в формате минута, час, день месяца, месяц, день недели; `cmd [arg...]` — задаваемая для запуска команда с аргументами. При задании полей времени можно использовать регулярные выражения, а в командах — переменные окружения (`LOGNAME`, `HOME`, `SHELL` и т.п.).

Для просмотра имеющихся у пользователя задач используется:

```
crontab -u username -l
```


Для редактирования задач пользователя используется:

```
crontab -u username -e
```

Для однократного запуска задачи в заданное время используется демон `atd`.

Синтаксис:

```
at <время> [дата] команды
```

Время задаётся в АМ/PM-формате (например, для выполнения задачи в 14:00 необходимо задать `at 2pm` или `at 14:00`). Для завершения ввода необходимо нажать комбинацию клавиш `Ctrl+`.

Для просмотра задач `atd` используется команда `atq`, для отмены выполнения задачи — команда `atrm`.

### 8.3. Задание

1. Выполните задания по планированию задач с помощью `crond` (см. раздел 8.4.1).
2. Выполните задания по планированию задач с помощью `atd` (см. раздел 8.4.2).

### 8.4. Последовательность выполнения работы

#### 8.4.1. Планирование задач с помощью `cron`

1. Запустите терминал и получите полномочия администратора:

```
su -
```

2. Посмотрите статус демона `crond`:

```
systemctl status crond -l
```

3. Посмотрите содержимое файла конфигурации `/etc/crontab`:

```
cat /etc/crontab
```

4. Откройте файл расписания на редактирование:

```
crontab -e
```

Команда запустит интерфейс редактора (по умолчанию используется `vi`). Добавьте следующую строку в файл расписания (запись сообщения в системный журнал):

```
0 */2 * * 1-5 logger This message is written from root cron
```

В отчёте поясните синтаксис этой записи.

5. Закройте сеанс редактирования `vi` и сохраните изменения, используя команду `vi`:

```
[Esc] [:] [w] [q]
```

6. Посмотрите список заданий в расписании:

```
crontab -l
```

7. Перейдите в каталог `/etc/cron.hourly` и создайте в нём файл сценария с именем `eachhour`:

```
cd /etc/cron.hourly
```

```
touch eachhour
```

8. Откройте файл `eachhour` для редактирования и пропишите в нём следующий скрипт (запись сообщения в системный журнал):

```
#!/bin/sh
```

```
logger This message is written at $(date)
```

9. Сделайте файл сценария `eachhour` исполняемым:

```
chmod +x eachhour
```

10. Теперь перейдите в каталог `/etc/crond.d` и создайте в нём файл с расписанием `eachhour`:

```
cd /etc/crond.d
```

```
touch eachhour
```

Откройте этот файл для редактирования и поместите в него следующее содержимое:

```
11 * * * * root logger This message is written from
```

```
↵ /etc/crond.d
```

Сохраните изменения. В отчёте поясните синтаксис этой записи.

11. Не выключая систему, через некоторое время (2–3 часа) просмотрите журнал системных событий:

```
grep written /var/log/messages
```

По журналу определите, был ли осуществлён запуск сценария `eachhour` в соответствии с заданным расписанием.

### 8.4.2. Планирование заданий с помощью `at`

1. Запустите терминал и получите полномочия администратора:  
`su -`
2. Проверьте, что служба `atd` загружена и включена:  
`systemctl status atd`
3. Задайте выполнение команды `logger message from at` в 9:30 (или замените на любое другое время, когда вы работаете над этим упражнением). Для этого введите:  
`at 9:30`  
Затем введите:  
`logger message from at`  
Используйте `Ctrl` + `d`, чтобы закрыть оболочку.
4. Убедитесь, что задание действительно запланировано:  
`atq`

### 8.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание настроек системы в соответствии с заданием;
  - результаты проверки корректности настроек системы в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы со скриншотами результатов запуска команд в случае, если вопрос подразумевает выполнение упражнения.

### 8.6. Контрольные вопросы

1. Как настроить задание `cron`, чтобы оно выполнялось раз в 2 недели?
2. Как указать время выполнения задания `cron`, которое должно выполняться два раза в месяц, 1-го и 15-го числа в 2 часа ночи?
3. Как определить время выполнения `cron` для задания, которое должно выполняться каждые 2 минуты каждый день?
4. Как вы определить задание, которое должно быть выполнено 19 сентября и каждый четверг сентября?
5. Какая команда позволяет вам назначить задание `cron` для пользователя *alice*?
6. Как указать, что пользователю *bob* никогда не разрешено назначать задания через `cron`?
7. Вам нужно убедиться, что задание выполняется каждый день, даже если сервер во время выполнения временно недоступен. Как это сделать?
8. Какая команда позволяет узнать, запланированы ли какие-либо задания на выполнение планировщиком `atd`?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–7].

## Список литературы

1. UNIX Power Tools / M. Loukides, T. O'Reilly, J. Peek, S. Powers. — O'Reilly Media, 2009. — 1160 p.
2. *Робачевский А., Немнюгин С., Стесик О.* Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010. — 656 с. — ISBN 978-5-94157-538-1.
3. *Колисниченко Д. Н.* Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
4. Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли. — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
5. *Таненбаум Э., Бос Х.* Современные операционные системы. — 4-е изд. — СПб. : Питер, 2015. — 1120 с. — (Классика Computer Science).
6. *Neil N. J.* Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
7. *Goyal S. K.* Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.

## Лабораторная работа № 9. Управление SELinux

### 9.1. Цель работы

Получить навыки работы с контекстом безопасности и политиками SELinux.

### 9.2. Предварительные сведения

*SELinux (Security-Enhanced Linux)* — реализация мандатного управления доступом в ядре Linux.

*Мандатное управление доступом (Mandatory Access Control, MAC)* — разграничение прав доступа субъектов к объектам системы на базе меток конфиденциальности.

Под объектами понимаются файлы, каталоги, устройства операционной системы. В качестве субъектов выступают процессы операционной системы. Метка в SELinux — контекст SELinux, содержащий информацию о принадлежности объекта системы пользователю SELinux, о его роли, типе и уровне безопасности.

Основное назначение архитектуры MAC [5] — возможность принудительного назначения административно-установленной политики безопасности над всеми процессами и файлами системы.

Политики безопасности SELinux работают поверх стандартного *дискреционного управления контролем доступа (Discretionary Access Control, DAC)* в Unix/Linux операционных системах.

Основные понятия в SELinux:

- policy (политика) — набор правил, определяющих, какой источник имеет доступ к какой цели;
- source domain (исходный домен) — объект, который пытается получить доступ к цели (обычно пользователь или процесс);
- target domain (целевой домен) — то, к чему пытается получить доступ исходный домен (обычно файл или порт);
- context (контекст) — метка безопасности, которая используется для категоризации объектов в SELinux;
- rule (правило) — часть политики, определяющая, к какому исходному домену принадлежат разрешения доступа к целевому домену;
- labels (метки) — то же, что и метка контекста, служащая для определения того, какой исходный домен имеет доступ к целевому домену.

Синтаксис контекста SELinux:

```
SELinux user_u:role_r:type_t:level:
```

Здесь:

- user\_u (пользователь SELinux) — сущность с набором ролей и уровней многоуровневой модели безопасности (Multi-Level Security, MLS);
- role\_r (роль) — атрибут модели безопасности с ролевым управлением доступом (Role-Based Access Control, RBAC), который определяет, к каким доменам (множествам объектов) имеет доступ пользователь;
- type\_t (тип) — атрибут Type Enforcement, который определяет домен для процессов и тип для файлов;
- level (уровень) — атрибут многоуровневого управления доступом MLS и MCS (Multi-Category Security).

По умолчанию в SELinux определены:

- пользователи SELinux:
  - system\_u — системный пользователь;



- `unconfined_u` — прочие пользователи;
- роли в SELinux:
  - `system_r` — роль уровня системы, используемая для запуска системных процессов с указанием конкретного типа субъекта, определяемого типом объекта (файла), из которого они запускаются (например, субъект `httpd_t`, объект `httpd_exec_t`);
  - `unconfined_r` — роль уровня обычных пользователей;
  - `object_r` — роль, указываемая для объектов типа файл или каталог.

Пример просмотра контекста безопасности файла [5]:

```
ls -Z file1
```

```
-rwxrw-r-- user1 group1 unconfined_u:object_r:user_home_t:s0
↪ file1
```

В этом примере для объекта `file1`:

- определён DAC доступ типа `-rwxrw-r--` для пользователя `user1`, входящего в группу `group1`;
- задан пользователь SELinux `unconfined_u`;
- определена его роль `object_r`;
- задан тип `user_home_t`;
- задан уровень `s0`.

Для просмотра контекста безопасности процесса можно использовать команду `ps -eZ`

Для просмотра контекста безопасности процесса можно использовать команду `id -Z`

Для управления изменениями в контексте безопасности используется утилита `semanage`. Для восстановления меток контекста безопасности со значениями по умолчанию используется команда `restorecon`.

Для основных служб системы и распространённых приложений (например, `httpd`, `named`, `dhcpd`, `mysqld` и т.п.) сформированы целевые политики безопасности SELinux. Приложения с неопределённой политикой безопасности выполняются в домене `unconfined_t`, и на них правила работы SELinux не распространяются.

Конфигурационный файл SELinux располагается в файле `/etc/selinux/semanage.conf`. Файл `config` с настройками режимов работы SELinux располагается в том же каталоге.

Режимы работы SELinux:

- `Enforcing` (режим принудительного исполнения) — действия, нарушающие политику безопасности, блокируются, попытка нарушения фиксируется в журнале;
- `Permissive` (разрешающий режим) — действия, нарушающие политику безопасности, не блокируются, но попытка нарушения фиксируется в журнале;
- `Disabled` (режим отключения SELinux) — полное отключение системы принудительного контроля доступа.

Для проверки статуса и режима работы SELinux используются команды `sestatus` и `getenforce`. Команда `setenforce` позволяет переключать режимы работы SELinux.

### 9.3. Задание

1. Продемонстрируйте навыки по управлению режимами SELinux (см. раздел 9.4.1).
2. Продемонстрируйте навыки по восстановлению контекста безопасности SELinux (см. раздел 9.4.2).
3. Настройте контекст безопасности для нестандартного расположения файлов веб-службы (см. раздел 9.4.3).

4. Продемонстрируйте навыки работы с переключателями SELinux (см. раздел 9.4.4).

## 9.4. Последовательность выполнения работы

### 9.4.1. Управление режимами SELinux

1. Запустите терминал и получите полномочия администратора:  
`su -`
2. Посмотрите содержание файла `/etc/selinux/config`. В отчёте поясните, в каких режимах может работать SELinux.
3. Просмотрите текущую информацию о состоянии SELinux:  
`sestatus -v`  
В отчёте построчно поясните выведенную на экран информацию.
4. Посмотрите, в каком режиме работает SELinux:  
`getenforce`  
По умолчанию SELinux находится в режиме принудительного исполнения (Enforcing).
5. Измените режим работы SELinux на разрешающий (Permissive):  
`setenforce 0`  
и снова введите  
`getenforce`
6. В файле `/etc/sysconfig/selinux` с помощью редактора установите:  
`SELINUX=disabled`  
Перезагрузите систему.
7. После перезагрузки запустите терминал и получите полномочия администратора.
8. Посмотрите статус SELinux:  
`getenforce`  
Вы увидите, что SELinux теперь отключён.
9. Попробуйте переключить режим работы SELinux:  
`setenforce 1`  
Какая реакция системы? Вы не можете переключаться между отключённым и принудительным режимом без перезагрузки системы.
10. Откройте файл `/etc/sysconfig/selinux` с помощью редактора и установите:  
`SELINUX=enforcing`  
Перезагрузите систему.
11. После перезагрузки в терминале с полномочиями администратора просмотрите текущую информацию о состоянии SELinux:  
`sestatus -v`

### 9.4.2. Использование restorecon для восстановления контекста безопасности

1. Запустите терминал и получите полномочия администратора.
2. Посмотрите контекст безопасности файла `/etc/hosts`:  
`ls -Z /etc/hosts`  
Вы увидите, что у файла есть метка контекста `net_conf_t`.
3. Скопируйте файл `/etc/hosts` в домашний каталог:  
`cp /etc/hosts ~/`  
Поскольку копирование считается созданием нового файла, то параметр контекста в файле `~/hosts`, расположенном в домашнем каталоге, станет `admin_home_t`.  
Проверьте контекст файла `~/hosts`:  
`ls -Z ~/hosts`

4. Попробуйте перезаписать существующий файл `hosts` из домашнего каталога в каталог `/etc`:  

```
mv ~/hosts /etc
```

и подтвердите, что вы хотите сделать это.
5. Убедитесь, что тип контекста по-прежнему установлен на `admin_home_t`:  

```
ls -Z /etc/hosts
```
6. Исправьте контекст безопасности:  

```
restorecon -v /etc/hosts
```

Опция `-v` покажет процесс изменения.
7. Для массового исправления контекста безопасности на файловой системе введите:  

```
touch /.autorelabel
```

и перезагрузите сервер. Во время перезапуска не забудьте нажать клавишу `[Esc]` на клавиатуре, чтобы вы видели загрузочные сообщения. Вы увидите, что файловая система автоматически перемаркирована.

### 9.4.3. Настройка контекста безопасности для нестандартного расположения файлов веб-сервера

1. Запустите терминал и получите полномочия администратора.
2. Установите необходимое программное обеспечение:  

```
yum -y install httpd elinks
```
3. Создайте новое хранилище для файлов веб-сервера:  

```
mkdir /web
```
4. Создайте файл `index.html` в каталоге с контентом веб-сервера:  

```
cd /web
```

```
touch index.html
```

и поместите в файл следующий текст:  

```
Welcome to my web-server
```
5. В файле `/etc/httpd/conf/httpd.conf` измените параметр `DocumentRoot`:  

```
DocumentRoot "/web"
```

и добавьте следующий раздел, определяющий правила доступа:  

```
<Directory "/web">
 AllowOverride None
 Require all granted
</Directory>
```
6. Запустите веб-сервер и службу `httpd`:  

```
systemctl start httpd
```

```
systemctl enable httpd
```
7. При обращении к веб-серверу в текстовом браузере `elinks`:  

```
elinks http://localhost
```

Вы увидите веб-страницу `Red Hat` по умолчанию, а не содержимое только что созданного файла `index.html`.
8. Переключите SELinux в разрешающий режим:  

```
setenforce 0
```
9. Снова обратитесь к веб-серверу:  

```
elinks http://localhost
```

Теперь вы получите доступ к своей пользовательской веб-странице. Это показывает, что SELinux делает что-то для блокировки доступа.
10. Примените новую метку контекста к `/web`:  

```
semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
```
11. Восстановите контекст безопасности:  

```
restorecon -R -v /web
```

12. Установите SELinux в режим принудительного исполнения:  
`setenforce 1`
13. Снова обратитесь к веб-серверу:  
`elinks http://localhost`  
Теперь вы получите доступ к своей пользовательской веб-странице.

#### 9.4.4. Работа с переключателями SELinux

1. Запустите терминал и получите полномочия администратора.
2. Посмотрите список переключателей SELinux для службы ftp:  
`getsebool -a | grep ftp`  
Вы увидите переключатель `ftpd_anon_write` с текущим значением `off`.
3. Для службы `ftpd_anon` посмотрите список переключателей с пояснением, за что отвечает каждый переключатель, включён он или выключен:  
`semanage boolean -l | grep ftpd_anon`
4. Измените текущее значение переключателя для службы `ftpd_anon_write` с `off` на `on`:  
`setsebool ftpd_anon_write on`
5. Повторно посмотрите список переключателей SELinux для службы `ftpd_anon_write`:  
`getsebool ftpd_anon_write`
6. Посмотрите список переключателей с пояснением:  
`semanage boolean -l | grep ftpd_anon`  
Обратите внимание, что настройка времени выполнения включена, но постоянная настройка по-прежнему отключена.
7. Измените постоянное значение переключателя для службы `ftpd_anon_write` с `off` на `on`:  
`setsebool -P ftpd_anon_write on`
8. Посмотрите список переключателей с пояснением:  
`semanage boolean -l | grep ftpd_anon`  
Каково состояние переключателя?

#### 9.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание настроек системы в соответствии с заданием;
  - результаты проверки корректности настроек системы в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

## 9.6. Контрольные вопросы

1. Вы хотите временно поставить SELinux в разрешающем режиме. Какую команду вы используете?
2. Вам нужен список всех доступных переключателей SELinux. Какую команду вы используете?
3. Каково имя пакета, который требуется установить для получения легко читаемых сообщений журнала SELinux в журнале аудита?
4. Какие команды вам нужно выполнить, чтобы применить тип контекста `httpd_sys_content_t` к каталогу `/web`?
5. Какой файл вам нужно изменить, если вы хотите полностью отключить SELinux?
6. Где SELinux регистрирует все свои сообщения?
7. Вы не знаете, какие типы контекстов доступны для службы `ftp`. Какая команда позволяет получить более конкретную информацию?
8. Ваш сервис работает не так, как ожидалось, и вы хотите узнать, связано ли это с SELinux или чем-то ещё. Какой самый простой способ узнать?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1—5].

## Список литературы

1. Mayer F., MacMillan K., Caplan D. SELinux by example: using Security Enhanced Linux. — Prentice Hall, 2006. — 460 p. — ISBN 978-0131963696.
2. Vermeulen S. SELinux Cookbook. — Packt Publishing Ltd, 2014. — 240 p. — ISBN 9781783989669.
3. Vermeulen S. SELinux System Administration. — 2nd Edition. — Packt Publishing Ltd, 2016. — 285 p. — ISBN 978-1787126954.
4. Vugt S. van. Red Hat RHCSA/RHCE 7 cert guide : Red Hat Enterprise Linux 7 (EX200 and EX300). — Pearson IT Certification, 2016. — 1008 p. — (Certification Guide). — ISBN 978-0-7897-5405-9.
5. Security-Enhanced Linux. Linux с улучшенной безопасностью: руководство пользователя / M. McAllister, S. Radvan, D. Walsh, D. Grift, E. Paris, J. Morris. — URL: [https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced\\_Linux/index.html](https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/index.html).

## Лабораторная работа № 10. Основы работы с модулями ядра операционной системы

### 10.1. Цель работы

Получить навыки работы с утилитами управления модулями ядра операционной системы.

### 10.2. Предварительные сведения

По своей структуре операционная система состоит из ядра и системных программ, позволяющих управлять аппаратными ресурсами компьютера. Модули ядра представляют собой отдельный программный код, расширяющий функциональные возможности системы, который можно загрузить в ядро операционной системы. Для управления модулями ядра используются специальные утилиты:

- `modprobe` — загрузка/выгрузка модулей;
- `modinfo` — вывод информации о модуле;
- `lsmod` — вывод всех загруженных модулей в виде таблицы.

Подробнее о параметрах команд см. в соответствующих `man` руководствах.

### 10.3. Задание

1. Продемонстрируйте навыки работы по управлению модулями ядра (см. раздел 10.4.1).
2. Продемонстрируйте навыки работы по загрузке модулей ядра с параметрами (см. раздел 10.4.2).

### 10.4. Последовательность выполнения работы

#### 10.4.1. Управление модулями ядра из командной строки

1. Запустите терминал и получите полномочия администратора:  
`su -`
2. Посмотрите, какие устройства имеются в вашей системе и какие модули ядра с ними связаны:  
`lspci -k`
3. Посмотрите, какие модули ядра загружены:  
`lsmod | sort`
4. Загрузите модуль ядра `ext4`:  
`modprobe ext4`  
Убедитесь, что модуль загружен, посмотрев список загруженных модулей:  
`lsmod | sort`
5. Посмотрите информацию о модуле ядра `ext4`:  
`modinfo ext4`  
Обратите внимание, что у этого модуля нет параметров. В отчёте построчно поясните выведенную на экран информацию.
6. Выгрузите модуль ядра `ext4`:  
`modprobe -r ext4`
7. Попробуйте выгрузить модуль ядра `xfs`:

```
modprobe -r xfs
```

Обратите внимание, что вы получаете сообщение об ошибке, поскольку модуль ядра в данный момент используется.

### 10.4.2. Загрузка модулей ядра с параметрами

1. Запустите терминал и получите полномочия администратора.
2. Посмотрите список модулей ядра, отвечающих за работу с CD-приводом:  

```
lsmod | grep cdrom
```

Если вы используете оптический привод на своём компьютере, этот модуль должен быть загружен. Также должно быть указано, что он используется модулем `sr_mod`.
3. Попробуйте удалить модуль работы с CD-приводом из ядра системы:  

```
modprobe -r cdrom
```

Это не сработает, так как модуль используется модулем `sr_mod`.
4. Выгрузите последовательно модули `sr_mod` и `cdrom`:  

```
modprobe -r sr_mod
modprobe -r cdrom
```
5. Посмотрите информацию о модуле `cdrom`:  

```
modinfo cdrom
```

Одним из поддерживаемых параметров является параметр `debug` со значением типа *Boolean*.
6. Загрузите модуль `cdrom` с установленным параметром `debug`:  

```
modprobe cdrom debug=1
```
7. Посмотрите информацию буфера сообщений ядра:  

```
dmesg
```

Для некоторых модулей ядра информация о загрузке записывается в кольцевой буфер ядра, который может отображаться с помощью команды `dmesg`. К сожалению, это не относится к модулю ядра `cdrom`.
8. В каталоге `/etc/modprobe.d` создайте файл `cdrom.conf`:  

```
touch /etc/modprobe.d/cdrom.conf
```

Запишите в него следующий текст:  

```
options cdrom debug=1
```

Это позволит устанавливать параметр каждый раз, когда будет загружен модуль ядра `cdrom`.

### 10.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание настроек системы в соответствии с заданием;
  - результаты проверки корректности настроек системы в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

## 10.6. Контрольные вопросы

1. Какая команда показывает текущую версию ядра, которая используется на вашем компьютере?
2. Где можно посмотреть информацию о текущей версии ядра RHEL 7?
3. Какая команда показывает список загруженных модулей ядра?
4. Какая команда позволяет вам определять параметры модуля ядра?
5. Как выгрузить модуль ядра?
6. Что вы можете сделать, если получите сообщение об ошибке при попытке выгрузить модуль ядра?
7. Как вы определяете, какие параметры модуля ядра поддерживаются?
8. Где вы указываете параметры модуля ядра, которые должны использоваться постоянно?
9. Пусть модуль *cdrom* имеет параметр *debug*, который должен быть установлен в 1, чтобы включить режим отладки. Какую строку вы бы включили в файл, который будет автоматически загружать этот модуль?
10. Как вы устанавливаете новую версию ядра?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–4].

## Список литературы

1. *Колисниченко Д. Н.* Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
2. *Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли.* — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
3. *Neil N. J.* Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
4. *Goyal S. K.* Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.



## Лабораторная работа № 11. Управление загрузкой системы

### 11.1. Цель работы

Получить навыки работы с загрузчиком системы GRUB2.

### 11.2. Предварительные сведения

#### 11.2.1. Общие сведения о GRUB

Загрузка операционной системы непосредственно после включения и запуска начальной загрузочной последовательности действий компьютера осуществляется специальным программным обеспечением — загрузчиком операционной системы.

Наиболее распространённый загрузчик для Unix/Linux операционных систем — GRUB (GRand Unified Bootloader).

Определить версию загрузчика можно с помощью команды

```
grub-install --version
```

Основной файл конфигурации GRUB2 — `/boot/grub/grub.cfg`. Этот файл генерируется автоматически с помощью файла настроек `/etc/default/grub` и скриптов из директории `/etc/grub.d`.

#### 11.2.2. Запуск целей устранения неполадок

В случае возникновения неполадок в работе GRUB при загрузке системы можно использовать несколько параметров, вводя их в приглашении загрузки GRUB:

- `rd.break` — останавливает процедуру загрузки на этапе `initramfs` (этот параметр полезен, если у вас нет пароля `root`);
- `init=/bin/sh` или `init=/bin/bash` — указывает, что оболочку следует запускать сразу после загрузки ядра и `initrd`;
- `systemd.unit=emergency.target` — загружается минимальное количество системных единиц;
- `systemd.unit=rescue.target` — режим восстановления.

### 11.3. Задание

1. Продемонстрируйте навыки по изменению параметров GRUB и записи изменений в файл конфигурации (см. раздел 11.4.1).
2. Продемонстрируйте навыки устранения неполадок при работе с GRUB (см. раздел 11.4.2).
3. Продемонстрируйте навыки работы с GRUB без использования `root` (см. раздел 11.4.3).

### 11.4. Последовательность выполнения работы

#### 11.4.1. Модификация параметров GRUB2

1. Запустите терминал и получите полномочия администратора:

```
su -
```

2. В файле `/etc/default/grub` удалите параметры `rhgb` и `quiet` из строки указания параметров запуска ядра системы  

```
GRUB_CMDLINE_LINUX
```

Параметры `rhgb` и `quiet` отвечают за показ графической заставки при запуске системы (для дистрибутивов, основанных на Red Hat), скрывая процесс загрузки от пользователя.
3. В этом же файле установите параметр отображения меню загрузки в течение 10 секунд:  

```
GRUB_TIMEOUT=10
```

Сохраните изменения в файле и закройте редактор.
4. Запишите изменения в GRUB2, введя в командной строке  

```
grub2-mkconfig > /boot/grub2/grub.cfg
```

или  

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```
5. Перезагрузите систему и убедитесь, что при загрузке вы видите прокрутку загрузочных сообщений.

### 11.4.2. Устранения неполадок

1. Запустите (перегрузите) систему. Как только появится меню GRUB, выберите первую строку в меню и нажмите **e** для редактирования.
2. Прокрутите вниз до строки, начинающейся с `linux16 /vmlinuz`. В конце этой строки введите  

```
systemd.unit=rescue.target
```

и удалите опции `rhgb` и `quit` из этой строки, если они там есть.
3. Нажмите **Ctrl** + **x** для продолжения процесса загрузки.
4. Введите пароль пользователя `root` при появлении запроса.
5. Посмотрите список всех файлов модулей, которые загружены в настоящее время:  

```
systemctl list-units
```

Вы можете видеть, что загружена базовая системная среда.
6. Посмотрите действовавшие переменные среды оболочки:  

```
systemctl show-environment
```
7. Перегрузите систему, используя команду:  

```
systemctl reboot
```
8. Как только отобразится меню GRUB, ещё раз нажмите **e**, чтобы войти в режим редактора. В конце строки, загружающей ядро, введите  

```
systemd.unit=emergency.target
```
9. Нажмите **Ctrl** + **x** для продолжения процесса загрузки.
10. Введите пароль пользователя `root` при появлении запроса.
11. После успешного входа в систему посмотрите список всех загруженных файлов модулей:  

```
systemctl list-units
```

Обратите внимание, что количество загружаемых файлов модулей уменьшилось до минимума.

### 11.4.3. Сброс пароля root

Обычный сценарий для администратора Linux заключается в том, что пароль `root` отсутствует. Если это произойдёт, вам необходимо сбросить его. Единственный способ сделать это — загрузить систему в минимальном режиме, который позволяет войти в систему без ввода пароля. Для этого выполните следующие действия.

1. Запустите (перегрузите) компьютер. Когда отобразится меню GRUB, выберите первую строку в меню и нажмите **[e]** для редактирования.
2. Прокрутите вниз до строки, начинающейся с `linux16 /vmlinuz`. В конце этой строки введите  
`rd.break`  
и удалите опции `rhgb` и `quit` из этой строки, если они там есть.
3. Нажмите **[Ctrl]+[x]** для продолжения процесса загрузки.
4. Этап загрузки системы остановится в момент загрузки `initramfs`, непосредственно перед монтированием корневой файловой системы в каталоге `/`.
5. Чтобы получить доступ к системному образу для чтения и записи, наберите:  
`mount -o remount,rw /sysroot`
6. Сделайте содержимое каталога `/sysimage` новым корневым каталогом, набрав:  
`chroot /sysroot`
7. Теперь вы можете ввести команду задания пароля:  
`passwd`  
и установить новый пароль для пользователя `root`.
8. Поскольку на этом очень раннем этапе загрузки SELinux ещё не активирован, то тип контекста SELinux для файла `/etc/shadow` будет испорчен. Если вы перезагрузитесь в этот момент, то никто не сможет войти в систему. Поэтому вы должны убедиться, что тип контекста установлен правильно. Чтобы сделать это, на этом этапе вы должны загрузить политику SELinux с помощью команды:  
`load_policy -i`
9. Теперь вы можете вручную установить правильный тип контекста для `/etc/shadow`. Для этого введите:  
`chcon -t shadow_t /etc/shadow`
10. Перезагрузите систему и войдите в систему с изменённым паролем для пользователя `root`.

## 11.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание настроек системы в соответствии с заданием;
  - результаты проверки корректности настроек системы в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

## 11.6. Контрольные вопросы

1. Какой файл конфигурации следует изменить для применения общих изменений в GRUB2?
2. Как называется конфигурационный файл GRUB2, в котором вы применяете изменения для GRUB2?
3. После внесения изменений в конфигурацию GRUB2, какую команду вы должны выполнить?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–4].

## Список литературы

1. *Колисниченко Д. Н.* Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
2. *Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли.* — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
3. *Neil N. J.* Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
4. *Goyal S. K.* Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.

## Лабораторная работа № 12. Настройки сети в Linux

### 12.1. Цель работы

Получить навыки настройки сетевых параметров системы.

### 12.2. Предварительные сведения

#### 12.2.1. IP-адрес и MAC-адрес сетевого интерфейса

В компьютерных сетях типа TCP/IP для идентификации устройств при сетевом взаимодействии по протоколу IP используются IP-адреса (Internet Protocol Address). IP-адрес присваивается сетевому интерфейсу устройства — физическому или виртуальному устройству, предназначенному для передачи данных через компьютерную сеть. В качестве сетевого интерфейса часто выступает сетевая карта.

В настоящее время существует две версии IP-адресов:

- IPv4-адреса — 32-битные адреса в десятично-точечной нотации, например, 192.168.10.4;
- IPv6-адреса — 128-битные адреса, записанные в шестнадцатеричной нотации, например, fe80:badb:abe01:45bc:34ad:6723:8798.

Каждая сетевая карта также имеет MAC-адрес — адрес управления доступом к среде (Media Access Control Address или Hardware Address). Пример MAC-адреса Ethernet: 00:e0:4c:42:ac:06.

MAC-адреса присваиваются сетевым интерфейсам на этапе изготовления. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, ARP (Address Resolution Protocol) и RARP (Reverse Address Resolution Protocol) в сетях IPv4, и NDP (Neighbor Discovery Protocol) в сетях на основе IPv6). По сути, MAC-адреса помогают компьютерам найти конкретную сетевую карту, которой принадлежит IP-адрес.

#### 12.2.2. Наименования сетевых интерфейсов в ОС типа Linux

До недавнего времени в ОС типа Linux имена сетевых интерфейсов состояли из префикса, характеризующего тип интерфейса, и порядкового номера интерфейса данного типа в системе. Например, `eth0` — первая сетевая карта, обнаруженная BIOS при загрузке устройства, `eth1` — вторая и так далее.

С переходом на `systemd` некоторые разработчики дистрибутивов типа Linux (например, Fedora, CentOS, Red Hat Enterprise Linux (RHEL)) перешли на другую схему наименования интерфейсов: сначала указывается обозначение типа интерфейса (`en` — Ethernet, `wl` — WLAN (сетевой интерфейс Wi-Fi адаптеров), `ww` — WWAN (разновидность беспроводных сетевых адаптеров)), затем указывается тип адаптера (`o` — встроенное устройство, `s` — слот `hotplug`, `p` — PCI, `x` — имя устройства, которое основано на MAC-адресе сетевой карты), затем следует число, которое используется для представления индекса, идентификатора или порта. Если фиксированное имя не может быть определено, то используются традиционные имена, такие как `eth0`. Пример обозначения первого по порядку интерфейса Ethernet, подключённого через третий слот на PCI шине: `enp0s3`.

### 12.2.3. Мониторинг конфигурации сетевых интерфейсов, портов и служб

Традиционные средства мониторинга состояния сетевых интерфейсов в ОС типа Linux — команды `ifconfig` (выдаёт список интерфейсов) и `route` (отвечает за отображение или изменение таблиц сетевых маршрутов).

Более современным средством мониторинга и конфигурирования сетевых интерфейсов является утилита `ip` из пакета `iproute2`. С её помощью можно контролировать многие аспекты сетевого взаимодействия, такие как:

- `ip link` — настройка и мониторинг состояния физических соединений;
- `ip addr` — настройка и мониторинг сетевых адресов;
- `ip route` — настройка и мониторинг информации о маршрутизации.

Общий синтаксис команды `ip`:

```
ip [OPTIONS] OBJECT { COMMAND | help }
```

где

```
OBJECT := { link | addr | addrlabel | route | rule | neigh |
↳ ntable | tunnel | maddr | mroute | monitor | xfrm }
OPTIONS := { -V[ersion] | -s[tatistics] | -d[etails] |
↳ -r[esolve] | -f[amily] { inet | inet6 | ipx | dnet | link
↳ } | -o[neline] | -t[imestamp] }
```

Для мониторинга состояния TCP-соединений, таблиц маршрутизации, числа сетевых интерфейсов и отслеживания сетевой статистики по протоколам используют утилиту `netstat` или её более современный аналог `ss`.

Общий синтаксис команды `netstat`:

```
netstat [-Aan] [-f семейство_адресов] [-I интерфейс] [-p
↳ имя_протокола] [система] [core] netstat [-n] [-s] [-i |
↳ -r] [-f семейство_адресов] [-I интерфейс] [-p
↳ имя_протокола] [система] [core] netstat [-n] [-I
↳ интерфейс] интервал [система] [core]
```

Общий синтаксис команды `ss`:

```
ss опции [фильтр_состояния] [фильтр_адреса]
```

Дополнительным полезным инструментом при манипулировании настройками операционной системы является утилита `lsof`, которая выводит информацию о файлах и службах, используемых теми или иными процессами. Например, при отслеживании TCP-соединений можно использовать следующую команду:

```
lsof | grep TCP
```

### 12.2.4. Настройка конфигурации сети с помощью `nmtui` и `nmcli`

Управление сетью осуществляется службой `NetworkManager`. Можно использовать команду

```
systemctl status NetworkManager
```

для проверки текущего статуса этой службы. Когда запускается `NetworkManager`, он считывает сценарии конфигурации сетевой карты, которые находятся в каталоге `/etc/sysconfig/network-scripts` и имеют имя, начинающееся с `ifcfg`, после которого следует имя сетевой карты.

Для манипулирования настройками сетевых соединений требуется знать как имена устройств, так и имя DNS-сервера. Имена устройств можно посмотреть в файле `/etc/hosts`, имена и адреса DNS-серверов прописываются в файле `/etc/resolv.conf`. Если в системе работает `NetworkManager`, то последний файл генерируется автоматически при запуске (или переключении) сетевых соединений. Для изменения имени устройства можно использовать команду `hostnamectl`.

При работе с конфигурацией сети необходимо понимать разницу между устройством и соединением:

- устройство представляет собой сетевую карту (сетевой адаптер);
- соединение — это конфигурация, используемая на устройстве.

Можно создать несколько соединений для устройства. Это может быть полезно на мобильных устройствах для обеспечения переключения между настройками при перемещении. Переключение между соединениями на устройствах является обычным для компьютеров конечного пользователя и не столь распространено на серверах. Для управления сетевыми подключениями используют команды `nmtui` или `nmcli`.

## 12.3. Задание

1. Продемонстрируйте навыки использования утилиты `ip` (см. раздел 12.4.1).
2. Продемонстрируйте навыки использования утилиты `nmcli` (см. раздел 12.4.2 и 12.4.3).

## 12.4. Последовательность выполнения работы

### 12.4.1. Проверка конфигурации сети

1. Получите полномочия администратора:  
`su -`
2. Выведите на экран информацию о существующих сетевых подключениях, а также статистику о количестве отправленных пакетов и связанных с ними сообщениях об ошибках:  
`ip -s link`  
Поясните в отчёте полученную информацию об одном из интерфейсов.
3. Выведите на экран информацию о текущих назначениях адресов для сетевых интерфейсов на устройстве:  
`ip addr show`  
Поясните в отчёте полученную информацию для одного из интерфейсов.
4. Выведите на экран информацию о текущих маршрутах:  
`ip route show`  
Поясните в отчёте выведенную на экран информацию.
5. Определите IPv4-адрес устройства и обозначение сетевого адаптера:  
`ip addr show`
6. Используйте команду `ping` для проверки правильности подключения к Интернету. Например, для отправки четырёх пакетов на IP-адрес 8.8.8.8 введите:  
`ping -c 4 8.8.8.8`
7. Добавьте дополнительный адрес к вашему интерфейсу:  
`ip addr add 10.0.0.10/24 dev <yourdevicename>`  
Здесь `<yourdevicename>` — название интерфейса, которому добавляется IP-адрес.
8. Проверьте, что адрес добавился:  
`ip addr show`
9. Сравните вывод информации от утилиты `ip` и от команды `ifconfig`:  
`ifconfig`
10. Выведите на экран список всех прослушиваемых системой портов UDP и TCP:  
`ss -tul`

### 12.4.2. Управление сетевыми подключениями с помощью nmcli

1. Получите полномочия администратора. Выведите на экран информацию о текущих соединениях:  
`nmcli connection show`
2. Добавьте Ethernet-соединение с именем `dhcp` к интерфейсу:  
`nmcli connection add con-name "dhcp" type ethernet ifname`  
`↪ <ifname>`  
Здесь `<ifname>` — название интерфейса.
3. Добавьте к этому же интерфейсу Ethernet-соединение с именем `static`, статическим IPv4-адресом адаптера и статическим адресом шлюза:  
`nmcli connection add con-name "static" ifname <ifname>`  
`↪ autoconnect no type ethernet ip4 10.0.0.10/24 gw4`  
`↪ 10.0.0.1`
4. Выведите информацию о текущих соединениях:  
`nmcli connection show`
5. Переключитесь на статическое соединение:  
`nmcli connection up "static"`  
Проверьте успешность переключения при помощи `nmcli con show` и `ip addr`.
6. Вернитесь к соединению `dhcp`:  
`nmcli connection up "dhcp"`  
Проверьте успешность переключения при помощи `nmcli con show` и `ip addr`.

### 12.4.3. Изменение параметров соединения с помощью nmcli

1. Получите полномочия администратора. Отключите автоподключение статического соединения:  
`nmcli connection modify "static" connection.autoconnect no`
2. Добавьте DNS-сервер в статическое соединение:  
`nmcli connection modify "static" ipv4.dns 10.0.0.10`  
Обратите внимание, что при добавлении сетевого подключения используется `ip4`, а при изменении параметров для существующего соединения используется `ipv4`.
3. Для добавления второго и последующих элементов для тех же параметров, используется знак `+`. Если этот знак проигнорировать, то произойдёт замена, а не добавление элемента. Добавьте второй DNS-сервер:  
`nmcli connection modify "static" +ipv4.dns 8.8.8.8`
4. Измените IP-адрес статического соединения:  
`nmcli connection modify "static" ipv4.addresses 10.0.0.20/24`
5. Добавьте другой IP-адрес для статического соединения:  
`nmcli connection modify "static" +ipv4.addresses`  
`↪ 10.20.30.40/16`
6. После изменения свойств соединения активируйте его:  
`nmcli connection up "static"`  
Проверьте успешность переключения при помощи `nmcli con show` и `ip addr`.
7. Используя `nmtui`, посмотрите и опишите в отчёте настройки сети на устройстве.
8. Посмотрите настройки сетевых соединений в графическом интерфейсе операционной системы.



## 12.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание настроек системы в соответствии с заданием;
  - результаты проверки корректности настроек системы в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

## 12.6. Контрольные вопросы

1. Какая команда отображает только статус соединения, но не IP-адрес?
2. Какая служба управляет сетью в RHEL7?
3. Какой файл содержит имя узла (устройства) в RHEL7?
4. Какая команда позволяет вам задать имя узла (устройства)?
5. Какую команду нужно выполнить после изменения содержимого файла `/etc/sysconfig/ifcfg?`
6. Какой конфигурационный файл можно изменить для включения разрешения имён для конкретного IP-адреса?
7. Какая команда показывает текущую конфигурацию маршрутизации?
8. Как проверить текущий статус службы `NetworkManager`?
9. Какая команда позволяет вам изменить текущий IP-адрес и шлюз по умолчанию для вашего сетевого соединения?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–7].

## Список литературы

1. *Робачевский А., Немнюгин С., Стесик О.* Операционная система UNIX. — 2-е изд. — БХВ-Петербург, 2010. — 656 с. — ISBN 978-5-94157-538-1.
2. *Королькова А. В., Кулябов Д. С.* Прикладные протоколы Интернет и www: лабораторные работы. — М. : РУДН, 2012. — 135 с. — ISBN 9785209049357.
3. *Королькова А. В., Кулябов Д. С.* Сетевые технологии: лабораторные работы. — М. : РУДН, 2014. — 106 с. — ISBN 785209056065.
4. *Vugt S. van.* Red Hat RHCSA/RHCE 7 cert guide : Red Hat Enterprise Linux 7 (EX200 and EX300). — Pearson IT Certification, 2016. — 1008 p. — (Certification Guide). — ISBN 978-0-7897-5405-9.
5. Сети и системы передачи информации: телекоммуникационные сети / К. Е. Самуйлов, И. А. Шалимов, Д. С. Кулябов, В. В. Василевский, Н. Н. Васин, А. В. Королькова. — М. : Издательство Юрайт, 2016. — 363 с. — ISBN 978-5-9916-7198-9.
6. Сайт проекта `NetworkManager`. — URL: <https://wiki.gnome.org/Projects/NetworkManager>.
7. Сайт проекта `nmcli`. — URL: <https://developer.gnome.org/NetworkManager/stable/nmcli.html>.

## Лабораторная работа № 13. Фильтр пакетов

### 13.1. Цель работы

Получить навыки настройки пакетного фильтра в Linux.

### 13.2. Предварительные сведения

FirewallD представляет собой службу динамического управления межсетевым экраном (брандмауэром).

Управление межсетевым экраном `firewalld` осуществляет через настройки доверенных зон сетевых соединений или конкретных интерфейсов. В данном случае под зоной понимается набор правил, применяемых к входящим в систему пакетам, соответствующим конкретному адресу источника или сетевому интерфейсу. Firewalld работает только с входящими пакетами, фильтрация на исходящих пакетах не проводится. Использование зон особенно важно на серверах с несколькими интерфейсами. На таких серверах зоны позволяют администраторам достаточно легко назначать определённый набор правил обработки входящих пакетов.

Firewalld работает с некоторыми стандартными зонами:

- **block** — все входящие сетевые соединения отклоняются с сообщением «`isrp-host-forbidden`», при этом разрешены только сетевые подключения, которые были инициированы в этой системе;
- **dmz** — используется на компьютерах, находящихся в демилитаризованной зоне, при этом принимаются только выбранные входящие соединения, разрешён ограниченный доступ к внутренней сети;
- **drop** — все входящие пакеты отбрасываются, не информируя об этом источник, при этом разрешены исходящие соединения;
- **external** — используется во внешних сетях с включённым маскарadingом (Network Address Translation, NAT), например, на маршрутизаторах, при этом принимаются только выбранные входящие соединения;
- **home** — используется в домашних сетях, принимая во внимание, что большинство компьютеров в этой сети доверяют друг другу, при этом разрешено принимать только выбранные входящие соединения;
- **internal** — используется во внутренних сетях, в которых большинство компьютеров сети доверяют друг другу, при этом принимаются только выбранные входящие соединения;
- **public** — используется в общественных местах, принимая во внимание, что компьютеры в таких сетях не доверяют друг другу, при этом эта зона является зоной по умолчанию для всех вновь создаваемых сетевых интерфейсов;
- **trusted** — все сетевые подключения принимаются;
- **work** — используется во внутренних сетях организаций, где большинство компьютеров в сети доверяют друг другу, при этом принимаются только выбранные входящие соединения.

На серверах, имеющих только один сетевой интерфейс, вполне можно обойтись одной зоной, которая является зоной по умолчанию. Каждый пакет, который поступает в систему, анализируется для исходного адреса, и на основе этого исходного адреса анализируется `firewalld` на принадлежность к определённой зоне. Если какая-либо конкретная зона недоступна, пакет обрабатывается настройками в зоне по умолчанию.

### 13.3. Задание

1. Используя `firewall-cmd`:
  - определить текущую зону по умолчанию;
  - определить доступные для настройки зоны;
  - определить службы, включённые в текущую зону;
  - добавить сервер VNC в конфигурацию брандмауэра.
2. Используя `firewall-config`:
  - добавьте службы `http` и `ssh` в зону `public`;
  - добавьте порт 2022 протокола UDP в зону `public`;
  - добавьте службу `ftp`.
3. Выполните задание для самостоятельной работы (раздел 13.5).

### 13.4. Последовательность выполнения работы

#### 13.4.1. Управление брандмауэром с помощью `firewall-cmd`

1. Получите полномочия администратора:  
`su -`
2. Определите текущую зону по умолчанию, введя:  
`firewall-cmd --get-default-zone`
3. Определите доступные зоны, введя:  
`firewall-cmd --get-zones`
4. Посмотрите службы, доступные на вашем компьютере, используя  
`firewall-cmd --get-services`
5. Определите доступные службы в текущей зоне:  
`firewall-cmd --list-services`
6. Сравните результаты вывода информации при использовании команды  
`firewall-cmd --list-all`  
и команды  
`firewall-cmd --list-all --zone=public`
7. Добавьте сервер VNC в конфигурацию брандмауэра:  
`firewall-cmd --add-service=vnc-server`
8. Проверьте, добавился ли `vnc-server` в конфигурацию:  
`firewall-cmd --list-all`
9. Перезапустите службу `firewalld`:  
`systemctl restart firewalld`
10. Проверьте, есть ли `vnc-server` в конфигурации:  
`firewall-cmd --list-all`  
Обратите внимание, что служба `vnc-server` больше не указана. Поясните, почему это произошло.
11. Добавьте службу `vnc-server` ещё раз, но на этот раз сделайте её постоянной, используя команду  
`firewall-cmd --add-service=vnc-server --permanent`
12. Проверьте наличие `vnc-server` в конфигурации:  
`firewall-cmd --list-all`  
Вы увидите, что VNC-сервер не указан. Службы, которые были добавлены в конфигурацию на диске, автоматически не добавляются в конфигурацию времени выполнения.
13. Перезагрузите конфигурацию `firewalld`:  
`firewall-cmd --reload`
14. Добавьте в конфигурацию межсетевого экрана порт 2022 протокола TCP:

```
firewall-cmd --add-port=2022/tcp --permanent
```

Затем перезагрузите конфигурацию firewalld:

```
firewall-cmd --reload
```

15. Проверьте, что порт добавлен в конфигурацию:

```
firewall-cmd --reload
```

### 13.4.2. Управление брандмауэром с помощью firewall-config

1. Откройте терминал и запустите интерфейс GUI firewall-config:

```
firewall-config &
```

2. Нажмите выпадающее меню рядом с параметром **Configuration**. Откройте раскрывающийся список и выберите **Permanent**. Это позволит сделать постоянными все изменения, которые вы вносите при конфигурировании.
3. Выберите зону **public** и отметьте службы **http** и **ssh**, чтобы включить их.
4. Выберите вкладку **Ports** и на этой вкладке нажмите **Add**. Введите порт 2022 и протокол **udp**, нажмите **OK**, чтобы добавить их в список.
5. Активируйте вкладку **Services** и выберите службы **http** и **https**. Сделайте то же самое для службы **ftp**.
6. Закройте утилиту firewall-config.
7. В окне терминала введите

```
firewall-cmd --list-all
```

Обратите внимание, что изменения, которые вы только что внесли, ещё не вступили в силу. Это связано с тем, что вы настроили их как постоянные изменения, а не как изменения времени выполнения.

8. Перегрузите конфигурацию firewall-cmd:

```
firewall-cmd --reload
```

и список доступных сервисов:

```
firewall-cmd --list-all
```

Вы увидите, что изменения были применены.

### 13.5. Самостоятельная работа

1. Создайте конфигурацию межсетевого экрана, которая позволяет получить доступ к следующим службам:
- web;
  - ftp;
  - ssh.
2. Сделайте это как в командной строке, так и в графическом интерфейсе.
3. Убедитесь, что конфигурация является постоянной и будет активирована после перезагрузки компьютера.

### 13.6. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
- скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание настроек системы в соответствии с заданием;

- результаты проверки корректности настроек системы в соответствии с заданием (подтверждённые скриншотами).
- 4. Выводы, согласованные с заданием работы.
- 5. Ответы на контрольные вопросы.

### 13.7. Контрольные вопросы

1. Какую службу следует запустить, прежде чем пытаться создать конфигурацию брандмауэра с помощью `firewall-config`?
2. Какая команда добавляет UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?
3. Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах?
4. Какая команда позволяет удалить службу `vnc-server` из текущей конфигурации брандмауэра?
5. Какая команда `firewall-cmd` позволяет активировать новую конфигурацию, добавленную опцией `--permanent`?
6. Какой параметр `firewall-cmd` позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна?
7. Какая команда позволяет добавить интерфейс `enol` в зону `public`?
8. Если добавить новый интерфейс в конфигурацию брандмауэра, пока не указана зона, в какую зону он будет добавлен?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1—4].

### Список литературы

1. *Purdy G. N.* Linux iptables Pocket Reference. — O'Reilly Media, 2004. — 96 p. — (Pocket Reference).
2. *Колисниченко Д. Н.* Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
3. *Vugt S. van.* Red Hat RHCSA/RHCE 7 cert guide : Red Hat Enterprise Linux 7 (EX200 and EX300). — Pearson IT Certification, 2016. — 1008 p. — (Certification Guide). — ISBN 978-0-7897-5405-9.
4. Динамический брандмауэр с использованием FirewallD. — URL: <https://fedoraproject.org/wiki/FirewallD/ru>.

## Лабораторная работа № 14. Партиции, файловые системы, монтирование

### 14.1. Цель работы

Получить навыки создания разделов на диске и файловых систем. Получить навыки монтирования файловых систем.

### 14.2. Предварительные сведения

Единицы измерения объёмов данных представлены в табл. 14.1.

Единицы измерения объёмов данных

Таблица 14.1

| Символ | Наименование | Значение | Символ | Наименование | Значение |
|--------|--------------|----------|--------|--------------|----------|
| KB     | Kilobyte     | $1000^1$ | KiB    | Kibibyte     | $1024^1$ |
| MB     | Megabyte     | $1000^2$ | MiB    | Mebibyte     | $1024^2$ |
| GB     | Gigabyte     | $1000^3$ | GiB    | Gibibyte     | $1024^3$ |
| TB     | Terabyte     | $1000^4$ | TiB    | Tebibyte     | $1024^4$ |
| PB     | Petabyte     | $1000^5$ | PiB    | Pebibyte     | $1024^5$ |
| EB     | Exabyte      | $1000^6$ | EiB    | Exbibyte     | $1024^6$ |
| ZB     | Zettabyte    | $1000^7$ | ZiB    | Zebibyte     | $1024^7$ |
| YB     | Yottabyte    | $1000^8$ | YiB    | Yobibyte     | $1024^8$ |

### 14.3. Задание

1. Добавьте два диска на виртуальной машине (раздел 14.4.1).
2. Продемонстрируйте навыки создания разделов MBR с помощью fdisk (раздел 14.4.2).
3. Продемонстрируйте навыки создания логических разделов с помощью fdisk (раздел 14.4.3).
4. Продемонстрируйте навыки создания раздела подкачки с помощью fdisk (раздел 14.4.4).
5. Продемонстрируйте навыки создания разделов GPT с помощью gdisk (раздел 14.4.5).
6. Продемонстрируйте навыки форматирования файловой системы XFS (раздел 14.4.6).
7. Продемонстрируйте навыки форматирования файловой системы EXT4 (раздел 14.4.7).
8. Продемонстрируйте навыки ручного монтирования файловых систем (раздел 14.4.8).
9. Продемонстрируйте навыки монтирования файловых систем с помощью `/etc/fstab` (раздел 14.4.9).
10. Выполните задание для самостоятельной работа (раздел 14.5).

## 14.4. Последовательность выполнения работы

### 14.4.1. Создание виртуальных носителей

Добавьте к вашей виртуальной машине два диска размером 512 MiB.

### 14.4.2. Создание разделов MBR с помощью fdisk

1. Получите полномочия администратора:

```
su -
```

2. Откройте корневую оболочку и запустите команду `fdisk`. Эта команда требует в качестве аргумента имя дискового устройства, на котором необходимо создать раздел. Измените название раздела, если необходимо, в соответствии с вашим оборудованием:

```
fdisk /dev/sdb
```

Изменения останутся в памяти только до тех пор, пока вы не решите их записать. Будьте внимательны перед использованием команды записи. Утилита `fdisk` записывает изменения на диск только при вводе команды `w`. Если вы допустили ошибку и хотите выйти, то нажмите `q` для выхода из `fdisk` без записи изменений.

3. Введите `m`, чтобы получить справку по командам.
4. Прежде чем делать что-либо, рекомендуется проверить, сколько дискового пространства у вас есть. Нажмите `p`, чтобы просмотреть текущее распределение пространства диска. Обратите внимание на общее количество секторов и последний сектор, который в настоящее время используется. Если последний раздел не заканчивается в последнем секторе, то у вас есть свободное место для создания нового раздела.
5. Введите `n`, чтобы добавить новый раздел.
6. Выберите `p`, чтобы создать основной раздел. Примите номер раздела, который предлагается.
7. Укажите первый сектор на диске, с которого начнётся новый раздел. По умолчанию предлагается первый доступный сектор, нажмите `Enter` для подтверждения выбора.
8. Укажите последний сектор, которым будет завершён раздел. По умолчанию предлагается последний сектор, доступный на диске. Если вы согласитесь с предложенным по умолчанию вариантом, то после этого упражнения у вас не останется свободного места на диске для создания дополнительных разделов или логических томов. Поэтому вы должны использовать другой последний сектор, остановившись на одном из следующих вариантов:
  - ввести номер последнего сектора, который вы хотите использовать;
  - ввести +номер, чтобы создать раздел, размер которого составляет определённое количество секторов;
  - ввести +номер (K, M, G), чтобы указать размер, который вы хотите назначить разделу в KiB, MiB или GiB.

Например, введите `+100M`, чтобы создать раздел на 100 MiB.

После этого `fdisk` потребует подтверждение.

9. На этом этапе можно определить тип раздела. По умолчанию используется тип раздела Linux. Если вы хотите, чтобы раздел имел какой-либо другой тип, используйте для изменения `t`. Вам интересны следующие типы разделов:
  - 82: Linux swap;
  - 83: Linux;

– 8e: Linux LVM.

Нажмите **[Enter]**, чтобы принять тип раздела по умолчанию 83.

10. Нажмите **[w]**, чтобы записать изменения на диск и выйти из `fdisk`.

11. Таблица разделов находится только в памяти ядра. Сравните вывод команды

```
fdisk -l /dev/sdb
```

с выводом команды

```
cat /proc/partitions
```

Последняя команда отображает таблицу разделов в памяти ядра. Опишите разницу.

12. Запишите изменения в таблицу разделов ядра:

```
partprobe /dev/sdb
```

### 14.4.3. Создание логических разделов

1. Получите полномочия администратора

```
su -
```

2. Запустите

```
fdisk /dev/sdb
```

3. Введите **[n]**, чтобы добавить новый раздел.

4. Введите **[e]**, чтобы создать расширенный раздел.

5. Если расширенный раздел — четвёртый раздел, который вы записываете в MBR, он также будет последним разделом, который можно добавить в MBR. По этой причине он должен заполнить всю оставшуюся часть жёсткого диска вашего компьютера. Нажмите **[Enter]**, чтобы принять первый сектор по умолчанию и снова нажмите **[Enter]**, когда `fdisk` запросит последний сектор.

6. Теперь, когда расширенный раздел создан, вы можете создать в нём логический раздел. Из интерфейса `fdisk` снова нажмите **[n]**. Утилита сообщит, что нет свободных первичных разделов и по умолчанию предложит добавить логический раздел с номером 5.

7. Нажмите **[Enter]**, чтобы принять выбор первого сектора в качестве сектора по умолчанию. На вопрос о последнем секторе введите +100M (или любой другой размер, который вы хотите использовать).

8. После создания логического раздела введите **[w]**, чтобы записать изменения на диск и выйти из `fdisk`. Чтобы завершить процедуру, введите

```
partprobe /dev/sdb
```

чтобы обновить таблицу разделов ядра. Новый раздел теперь готов к использованию.

### 14.4.4. Создание раздела подкачки

1. Получите полномочия администратора. Запустите `fdisk`:

```
fdisk /dev/sdb
```

2. Нажмите **[n]**, чтобы добавить новый раздел. Утилита сообщит, что нет свободных первичных разделов и по умолчанию предложит добавить логический раздел с номером раздела 6.

3. Нажмите **[Enter]**, чтобы принять первый сектор по умолчанию. На вопрос о последнем секторе введите +100M (или любой другой размер, который вы хотите использовать).

4. Введите **[t]**, чтобы изменить тип раздела. Используйте тип раздела 82.



## 5. Используйте

```
mkswap /dev/sdb6
```

для форматирования раздела в качестве раздела подкачки.

## 6. Для просмотра размера пространства подкачки, которое в настоящее время выделено, введите:

```
free -m
```

## 7. Для включения вновь выделенного пространства подкачки используйте

```
swapon /dev/sdb6
```

## 8. Введите

```
free -m
```

Вы видите, что новое место подкачки было добавлено.

### 14.4.5. Создание разделов GPT с помощью gdisk

## 1. Получите полномочия администратора. Создайте раздел с помощью gdisk:

```
gdisk /dev/sdc
```

Программа gdisk попытается определить текущее разбиение диска, и если ничего не обнаружено, то будет создана таблица разделов GPT и соответствующее разбиение диска.

2. Введите , чтобы добавить новый раздел. Вы можете выбрать любой номер раздела между 1 и 128, но разумно принять номер раздела по умолчанию, который предлагается.3. Теперь вас попросят задать первый сектор. По умолчанию будет использоваться первый сектор, доступный на диске, но также можно указать смещение. Нажмите , чтобы принять предлагаемый по умолчанию первый сектор.

## 4. При запросе последнего сектора, по умолчанию предлагается последний сектор, доступный на диске (создаётся раздел, который заполняет весь жёсткий диск). Можно указать другой последний сектор или указать размер диска, используя +, размер и размерность (KMGTp). Чтобы создать раздел диска размером 100 MiB, используйте +100M.

5. Теперь предлагается установить тип раздела. Если ничего не делать, то тип раздела устанавливается в 8300, что является типом раздела файловой системы Linux. Также доступны другие варианты. Можно нажать , чтобы отобразить список доступных типов разделов. Вам интересны следующие типы разделов:

- 8200: Linux swap;
- 8300: Linux;
- 8e00: Linux LVM.

Обратите внимание, что это те же типы разделов, которые используются в MBR, с двумя нулями, добавленными к их именам. Можно просто нажать , чтобы принять тип раздела 8300 по умолчанию.

6. Теперь раздел создан (но ещё не записан на диск). Нажмите , чтобы отобразить разбиение диска.7. Если текущее разбиение устраивает, нажмите , чтобы записать изменения на диск.

## 8. Если в этот момент вы получите сообщение об ошибке, указывающее, что таблица разделов используется, то для её обновления введите:

```
partprobe /dev/sdc
```

#### 14.4.6. Форматирование файловой системы XFS

1. Получите полномочия администратора. Создайте файловую систему XFS:  
`mkfs.xfs /dev/sdb1`
2. Для установки метки файловой системы в `xfsdisk` используйте команду:  
`xfs_admin -L xfsdisk /dev/sdb1`

#### 14.4.7. Форматирование файловой системы EXT4

1. Получите полномочия администратора.  
Создайте файловую систему EXT4:  
`mkfs.ext4 /dev/sdb5`
2. Для установки метки файловой системы в `ext4disk` используйте команду:  
`tune2fs -L ext4disk /dev/sdb5`
3. Для установки параметров монтирования по умолчанию для файловой системы используйте команду:  
`tune2fs -o acl,user_xattr /dev/sdb5`  
В данном случае включены списки контроля доступа и расширенные атрибуты пользователя.

#### 14.4.8. Ручное монтирование файловых систем

Для ручной установки файловой системы используется команда `mount`. Чтобы отключить смонтированную файловую систему, используется команда `umount`.

1. Получите полномочия администратора. Для создания точки монтирования для раздела введите:  
`mkdir -p /mnt/tmp`
2. Чтобы смонтировать файловую систему, используйте следующую команду:  
`mount /dev/sdb5 /mnt/tmp`
3. Для проверки корректности монтирования раздела введите:  
`mount`
4. Чтобы отмонтировать раздел, можно использовать `umount` либо с именем устройства, либо с именем точки монтирования. Таким образом, обе следующие команды будут работать:  
`umount /dev/sdb5`  
или  
`umount /mnt/tmp`
5. Проверьте, что раздел отмонтирован:  
`mount`

#### 14.4.9. Монтирование разделов с помощью `/etc/fstab`

В этом упражнении требуется подмонтировать отформатированный раздел XFS `/dev/sdb1`, который был создан в предыдущих упражнениях.

1. Получите полномочия администратора. Введите  
`blkid`  
Используйте мышь, чтобы скопировать часть `UUID = "nnnn"` для `/dev/sdb1`.
2. Создайте точку монтирования для этого раздела:  
`mkdir -p /mnt/data`
3. Откройте файл `/etc/fstab` на редактирование и добавьте следующую строку:  
`UUID="nnnn" /mnt/data xfs defaults 1 2`

4. Перед попыткой автоматического монтирования при перезагрузке рекомендуется проверить конфигурацию. Следующая команда монтирует всё, что указано в `/etc/fstab`:  

```
mount -a
```
5. Проверьте, что раздел примонтирован правильно  

```
df -h
```

### 14.5. Самостоятельная работа

1. Добавьте две партии на диск с разбиением GPT. Создайте оба раздела размером 100 MiB. Один из этих разделов должен быть настроен как пространство подкачки, другой раздел должен быть отформатирован файловой системой EXT4.
2. Настройте сервер для автоматического монтирования этих разделов. Установите раздел EXT4 на `/mnt/data-ext` и установите пространство подкачки в качестве области подкачки.
3. Перезагрузите сервер и убедитесь, что всё установлено правильно.

### 14.6. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания со скриншотами (снимками экрана), фиксирующими выполнение лабораторной работы.
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

### 14.7. Контрольные вопросы

1. Какой инструмент используется для создания разделов GUID?
2. Какой инструмент используется для создания разделов MBR?
3. Какая файловая система по умолчанию для RHEL 7?
4. Каково имя файла, который используется для автоматического монтирования разделов во время загрузки?
5. Какой вариант монтирования используется, если необходимо, чтобы файловая система не была автоматически примонтирована во время загрузки?
6. Какая команда позволяет форматировать раздел с типом 82 с соответствующей файловой системой?
7. Вы только что добавили несколько разделов для автоматического монтирования при загрузке. Как можно безопасно проверить, будет ли это работать без реальной перезагрузки?
8. Какая файловая система создаётся, если вы используете команду `mkfs` без какой-либо спецификации файловой системы?
9. Как форматировать раздел EXT4?
10. Как найти UUID для всех устройств на компьютере?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–4].

## Список литературы

1. *Колисниченко Д. Н.* Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
2. *Unix и Linux: руководство системного администратора / Э. Немец, Г. Снайдер, Т. Р. Хейн, Б. Уэйли.* — 4-е изд. — Вильямс, 2014. — 1312 с. — ISBN 978-0-13-148005-6.
3. *Neil N. J.* Learning CentOS: A Beginners Guide to Learning Linux. — CreateSpace Independent Publishing Platform, 2016. — 86 p.
4. *Goyal S. K.* Precise Guide to Centos 7: Beginners guide and quick reference. — Independently published, 2017. — 162 p. — ISBN 978-1521163566.

## Лабораторная работа № 15. Управление логическими томами

### 15.1. Цель работы

Получить навыки управления логическими томами.

### 15.2. Предварительные сведения

#### 15.2.1. Система управления логическими томами LVM

В архитектуре системы управления томами с данными (Logical Volume Manager, LVM) можно выделить несколько уровней. На нижнем уровне используются устройства хранения, например, диски, разделы, логические блоки (Logical Unit Number, LUN) в сети хранения данных (Storage Area Network, SAN).

Следующий уровень LVM образуют группы физических томов — разновидности меток LVM для устройств хранения. В группу томов можно добавить запоминающее устройство, представляющее собой отдельный физический том, которое является абстракцией всего доступного хранилища. Группа томов не является фиксированной. При необходимости она может быть изменена. Идея проста: если у вас заканчивается дисковое пространство на логическом томе, вы выбираете доступное дисковое пространство из группы томов. И если в группе томов нет свободного места, просто увеличиваете его, добавив физический том.

Поверх группы томов находятся логические тома. Логические тома не взаимодействуют непосредственно с дисками, а получают пространство из доступного дискового пространства в группе томов. Файловые системы создаются на логических томах. Поскольку логические тома являются гибкими в отношении размера, то это делает гибкими и файловые системы. Если в файловой системе заканчивается дисковое пространство, то относительно легко расширить файловую систему или уменьшить её, если это предусмотрено файловой системой.

LVM предлагает гибкое решение для управления хранилищем. Объёмы больше не связаны ограничениями физических жёстких дисков. Если требуется дополнительное пространство для хранения, группа томов может быть легко расширена, так что дисковое пространство может быть добавлено к логическим томам. Также возможно уменьшить размер логического тома, но только если файловая система, созданная на этом томе, поддерживает изменение размера. Это относится к файловой системе Ext4, но не для файловой системы XFS.

LVM поддерживает моментальные снимки. Снимок сохраняет текущее состояние логического тома и может использоваться для возврата к предыдущей ситуации или для создания резервной копии файловой системы на логическом томе. Снимки LVM создаются путём копирования административных данных логических томов (метаданных), которые описывают текущее состояние файлов. Когда блоки изменяются, то блоки, содержащие предыдущее состояние файла, копируются на том моментального снимка, который по этой причине будет расти. Использование этого метода гарантирует, что путём доступа к тому снимка LVM можно получить точное состояние файлов на момент создания моментального снимка.

Ещё одним важным преимуществом использования логических томов LVM является возможность замены неисправного оборудования. Если жёсткий диск выходит из строя, то данные могут быть перемещены внутри группы томов (через команду `pvmove`). Тогда повреждённый диск можно удалить из группы томов, а новый жёсткий диск можно добавить динамически, не тратя времени простоя для самого логического тома.

### 15.2.2. Создание логических томов

Прежде чем приступить к созданию логических томов, необходимо на каждом из дисков/разделов создать *физический том* (*physical volume*):

```
pvccreate /dev/sdb1
pvccreate /dev/sdc
```

На созданных физических томах нужно создать группу томов с названием `vg`:

```
vgcreate -s 4M vg /dev/sdb1 /dev/sdc
```

Информацию о группе томов можно получить при помощи команды `vgdisplay`:  
`vgdisplay vg`

За создание группы томов отвечает команда `lvcreate`. Например, в группе томов для создания логических томов `lv1` и `lv2` размером 20 ГБ и 30 ГБ необходимо ввести:

```
lvcreate -n lv1 -L 20G vg
lvcreate -n lv2 -L 30G vg
```

Таким образом получим блочные устройства `/dev/vg/lv1` и `/dev/vg/lv2`.

Файловая система на них создаётся стандартным образом:

```
mkfs.ext4 /dev/vg/lv1
mkfs.xfs /dev/vg/lv2
```

Для изменения размера логического тома нужно сначала изменить сам логический том:

```
lvresize -L 40G /dev/vg/lv1
```

Затем нужно изменить размер файловой системы:

```
resize2fs /dev/vg/lv1
```

### 15.2.3. Добавление физических томов

Для добавления нового диска, например `sdd`, в группу томов сначала необходимо создать физический том:

```
pvccreate /dev/sdd
```

Затем нужно добавить его в группу томов:

```
vgextend vg /dev/sdd
```

### 15.2.4. Удаление физических томов

Чтобы убрать из работающей группы томов, например, диск `sdc`, сначала требуется перенести с него все данные на другие диски:

```
pvmove /dev/sdc
```

Затем нужно удалить диск из группы томов:

```
vgreduce vg /dev/sdc
```

После можно удалить и сам физический том:

```
pvremove /dev/sdc
```

## 15.3. Задание

1. Продемонстрировать навыки создания физических томов на LVM (см. раздел 15.4.1).
2. Продемонстрировать навыки создания группы томов и логических томов на LVM (см. раздел 15.4.2).
3. Продемонстрировать навыки изменения размера логических томов на LVM (см. раздел 15.4.3).
4. Выполнить задание для самостоятельной работы (см. раздел 15.5).

## 15.4. Последовательность выполнения работы

Добавьте к вашей виртуальной машине один диск размером 512 MiB.

### 15.4.1. Создание физического тома

В этом упражнении вы создаёте физический том. Для этого вам нужен жёсткий диск с свободным (нераспределённым) дисковым пространством.

1. Получите полномочия администратора:  
`su -`
2. Введите  
`fdisk /dev/sdb`
3. Введите `[n]`, чтобы создать новый раздел. Выберите `[p]`, чтобы сделать его основным разделом, и используйте номер раздела, который предлагается по умолчанию. Если вы используете чистое устройство, это будет номер раздела 1.
4. Нажмите `[Enter]` при запросе для первого сектора и введите +100M, чтобы выбрать последний сектор.
5. Вернувшись в приглашение `fdisk`, введите `[t]`, чтобы изменить тип раздела. Поскольку существует только один раздел, `fdisk` не спрашивает, какой раздел использовать.
6. Программа запрашивает тип раздела, который вы хотите использовать. Выберите `8e`. Затем нажмите `[w]`, чтобы записать изменения на диск и выйти из `fdisk`.
7. Теперь, когда раздел был создан, вы должны указать его как физический том LVM. Для этого введите (с учётом наименования дисков в вашей системе):  
`pvccreate /dev/sdb1`
8. Теперь введите `pvs`, чтобы убедиться, что физический том создан успешно. Обратите внимание, что в этом списке уже существует другой физический том, так как RHEL по умолчанию использует LVM для организации хранилища.

### 15.4.2. Создание группы томов и логических томов

Вы продолжаете работу над созданным физическим томом и назначаете его группе томов. Затем требуется добавить логический том из этой группы томов.

1. Получите полномочия администратора. Откройте корневую оболочку. Проверьте доступность физических томов в вашей системе:  
`pvs`  
Вы должны увидеть созданный вами физический том `/dev/sdb1`.
2. Создайте группу томов с присвоенным ей физическим томом:  
`vgcreate vgdata /dev/sdb1`
3. Убедитесь, что группа томов была создана успешно:  
`vgs`  
Затем введите  
`pvs`  
Обратите внимание, что теперь эта команда показывает имя физических томов с именами групп томов, которым они назначены.
4. Введите  
`lvcreate -n lvdata -l 50%FREE vgdata`  
Это создаст логический том LVM с именем `lvdata`, который будет использовать 50% доступного дискового пространства в группе томов `vgdata`.
5. Для проверки успешного добавления тома введите

- lvs
- 6. На этом этапе вы готовы создать файловую систему поверх логического тома. Для этого введите
  - mkfs.ext4 /dev/vgdata/lvdata
- 7. Чтобы создать папку, на которую можно смонтировать том, введите
  - mkdir -p /mnt/data
- 8. Добавьте следующую строку в /etc/fstab:
  - /dev/vgdata/lvdata /mnt/data ext4 defaults 1 2
- 9. Проверьте, монтируется ли файловая система:
  - mount -a

### 15.4.3. Изменение размера логических томов

Вы создали физический том, группу томов и логический том. В этом упражнении требуется увеличить размер логического тома и файловой системы.

- 1. Получите полномочия администратора. Введите `pvs` и `vgs`, чтобы отобразить текущую конфигурацию физических томов и группы томов.
- 2. С помощью `fdisk` добавьте раздел /dev/sdb2 размером 100 М. Задайте тип раздела 8e.
- 3. Создайте физический том:
  - pvccreate /dev/sdb2
- 4. Расширьте `vgdata`:
  - vgextend vgdata /dev/sdb2
- 5. Проверьте, что размер доступной группы томов увеличен:
  - vgs
- 6. Проверьте текущий размер логического тома `lvdata`:
  - lvs
- 7. Проверьте текущий размер файловой системы на `lvdata`:
  - df -h
- 8. Увеличьте `lvdata` на 50% оставшегося доступного дискового пространства в группе томов:
  - lvextend -r -l +50%FREE /dev/vgdata/lvdata
- 9. Убедитесь, что добавленное дисковое пространство стало доступным:
  - lvs
  - df -h
- 10. Уменьшите размер `lvdata` на 50 МБ:
  - lvreduce -r -L -50M /dev/vgdata/lvdataОбратите внимание, что при этом том временно размонтируется.

### 15.5. Самостоятельная работа

- 1. Создайте логический том `lvgroup` размером 500 МБ. Отформатируйте его в файловой системе XFS и смонтируйте его постоянно на `/mnt/groups`. Перезагрузите виртуальную машину, чтобы убедиться, что устройство подключается.
- 2. После перезагрузки добавьте ещё 250 МБ к тому `lvgroup`. Убедитесь, что размер файловой системы также изменится при изменении размера тома.
- 3. Убедитесь, что расширение тома выполнено успешно.



## 15.6. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
  - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
  - подробное описание настроек сетевого оборудования в соответствии с заданием;
  - результаты проверки корректности настроек сетевого оборудования в соответствии с заданием (подтверждённые скриншотами).
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

## 15.7. Контрольные вопросы

1. Какой тип раздела используется в разделе GUID, который должен использоваться в LVM?
2. Какой командой можно создать группу томов с именем `vggroup`, которая содержит физическое устройство `/dev/sdb3` и использует физический экстенд 4 MiB?
3. Какая команда показывает краткую сводку физических томов в вашей системе, а также группу томов, к которой они принадлежат?
4. Что вам нужно сделать, чтобы добавить весь жёсткий диск `/dev/sdd` в группу томов группы?
5. Какая команда позволяет вам создать логический том `lvvol1` с размером 6 MiB?
6. Какая команда позволяет вам добавить 100 МБ в логический том `lvvol1`, если предположить, что дисковое пространство доступно в группе томов?
7. Каков первый шаг, чтобы добавить ещё 200 МБ дискового пространства в логический том, если требуемое дисковое пространство недоступно в группе томов?
8. Какую опцию нужно использовать с командой `lvextend`, чтобы также изменить размер файловой системы?
9. Как посмотреть, какие логические тома доступны?
10. Какую команду нужно использовать для проверки целостности файловой системы на `/dev/vgdata/lvdata`?

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1–3]

## Список литературы

1. UNIX Power Tools / M. Loukides, T. O'Reilly, J. Peek, S. Powers. — O'Reilly Media, 2009. — 1160 p.
2. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб.: БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.
3. Levine S. Logical Volume Manager Administration. — URL: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/logical\\_volume\\_manager\\_administration/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/logical_volume_manager_administration/index).

## Лабораторная работа № 16. Программный RAID

### 16.1. Цель работы

Освоить работу с RAID-массивами при помощи утилиты `mdadm`.

### 16.2. Предварительные сведения

#### 16.2.1. RAID-массивы

Аббревиатура RAID расшифровывается как Redundant Array of Inexpensive Disks (избыточный массив недорогих дисков) или Redundant Array of Independent Disks (избыточный массив независимых дисков).

Основные спецификации RAID-массивов:

- RAID 0 (striping). Чередувание. Высокая скорость, но не обеспечивается отказоустойчивость. Поэтому фактически не считается RAID.
- RAID 1. Зеркалирование. Каждый диск представляет собой полную копию другого. Минимальное количество дисков — 2.
- RAID 2. Использует коды Хемминга для контроля чётности. Минимальное количество дисков — 7.
- RAID 3. Один из дисков используется для хранения блоков чётности, остальные — для хранения данных. Данные разбиваются на байты.
- RAID 4. Аналогичен RAID 3, но данные при этом разбиваются на блоки (stripes).
- RAID 5. Блоки данных и контрольные суммы записываются на все диски циклично. Для хранения контрольных сумм используется объём одного диска. Минимальное количество дисков при использовании RAID 5 равно трём.
- RAID 6. Аналогичен RAID 5. Для хранения контрольных сумм используется объём двух дисков. Основан на кодах Рида–Соломона. Минимальное количество дисков — четыре.
- RAID 10. Массив RAID 1, составленный из массивов RAID 0.
- RAID 50, RAID 60. Аналог RAID 10, составленного из массивов RAID 5 и RAID 6 соответственно.

#### 16.2.2. Команды `mdadm`

- `create`. Создание RAID-массива из нескольких дисков.
- `assemble`. Сборка массива и его активация.
- `build`. Объединение дисков в массив (без суперблоков). Для таких массивов `mdadm` не различает создание и последующую сборку.
- `manage`. Управление массивом: добавление новых свободных дисков (spares) и удаление неработоспособных (faulty devices).
- `monitor`. Отслеживание состояния.
- `grow`. Расширение или уменьшение размера массива.
- `misc`. Прочие операции.

### 16.3. Задание

1. Прочитайте руководство по работе с утилитами `fdisk`, `sfdisk` и `mdadm`.

2. Добавить три диска на виртуальную машину (объёмом от 512 MiB каждый). При помощи `sfdisk` создать на каждом из дисков по одной партии, задав тип раздела для RAID (см. разделы 16.4.1, 16.4.2).
3. Создать массив RAID 1 из двух дисков, смонтировать его. Эмитировать сбой одного из дисков массива, удалить искусственно выведенный из строя диск, добавить в массив работающий диск (см. раздел 16.4.2).
4. Создать массив RAID 1 из двух дисков, смонтировать его. Добавить к массиву третий диск. Эмитировать сбой одного из дисков массива. Проанализировать состояние массива, указать различия по сравнению с предыдущим случаем (см. раздел 16.4.3).
5. Создать массив RAID 1 из двух дисков, смонтировать его. Добавить к массиву третий диск. Изменить тип массива с RAID1 на RAID5, изменить число дисков в массиве с 2 на 3. Проанализировать состояние массива, указать различия по сравнению с предыдущим случаем (см. раздел 16.4.4).

## 16.4. Последовательность выполнения работы

### 16.4.1. Создание виртуальных носителей

Добавьте к вашей виртуальной машине три диска размером 512 MiB: в VirtualBox выбрать «Настроить», «Носители», к контроллеру SATA последовательно добавить три носителя. Для этого в открывшемся окне укажите местоположение каждого носителя (обычно `/var/tmp/имя_пользователя`), имя диска (`hdb.vdi`, `hdc.vdi`, `hdd.vdi` соответственно), его размер (от 512 MiB). Затем запустите виртуальную машину.

### 16.4.2. Создание RAID-диска

1. Получите полномочия администратора:  

```
su -
```
2. Проверьте наличие созданных вами на предыдущем этапе дисков:  

```
fdisk -l | grep /dev/sd
```
3. Создайте на каждом из дисков раздел:  

```
sfdisk /dev/sdb <<EOF
;
EOF
sfdisk /dev/sdc <<EOF
;
EOF
sfdisk /dev/sdd <<EOF
;
EOF
```
4. Проверьте текущий тип созданных разделов:  

```
sfdisk --print-id /dev/sdb 1
sfdisk --print-id /dev/sdc 1
sfdisk --print-id /dev/sdd 1
```

В отчёте укажите, какой тип имеют созданные вами разделы на дисках.
5. Просмотрите, какие типы партий, относящиеся к RAID, можно задать:  

```
sfdisk -T | grep -i raid
```
6. Установите тип разделов в *Linux raid autodetect*:

- ```
sfdisk --change-id /dev/sdb 1 fd
sfdisk --change-id /dev/sdc 1 fd
sfdisk --change-id /dev/sdd 1 fd
```
7. Просмотрите состояние дисков:

```
sfdisk -l /dev/sdb
sfdisk -l /dev/sdc
sfdisk -l /dev/sdd
```

Опишите состояние дисков в отчёте.
 8. Если утилита mdadm не установлена в вашей системе, то установите её.
 9. При помощи утилиты mdadm создайте массив RAID 1 из двух дисков:

```
mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2
↪ /dev/sdb1 /dev/sdc1
```
 10. Проверьте состояние массива RAID, используя команды:

```
cat /proc/mdstat
mdadm --query /dev/md0
mdadm --detail /dev/md0
```

Опишите состояние массива в отчёте.
 11. Создайте файловую систему на RAID:

```
mkfs.ext4 /dev/md0
```
 12. Подмонтируйте RAID:

```
mkdir /data
mount /dev/md0 /data
```
 13. Добавьте запись в /etc/fstab:

```
/dev/md0 /data ext4 defaults 1 2
```
 14. Сымитируйте сбой одного из дисков:

```
mdadm /dev/md0 --fail /dev/sdc1
```
 15. Удалите сбойный диск:

```
mdadm /dev/md0 --remove /dev/sdc1
```
 16. Замените диск в массиве:

```
mdadm /dev/md0 --add /dev/sdd1
```
 17. Посмотрите состояние массива и опишите его в отчёте.
 18. Удалите массив и очистите метаданные:

```
umount /dev/md0
mdadm --stop /dev/md0
mdadm --zero-superblock /dev/sdb1
mdadm --zero-superblock /dev/sdc1
mdadm --zero-superblock /dev/sdd1
```

16.4.3. RAID-массив с горячим резервом (hotspare)

1. Получите полномочия администратора:

```
su -
```
2. Создайте массив RAID 1 из двух дисков:

```
mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2
↪ /dev/sdb1 /dev/sdc1
```
3. Добавьте третий диск:

```
mdadm --add /dev/md0 /dev/sdd1
```
4. Проверьте состояние массива:

```
cat /proc/mdstat
mdadm --query /dev/md0
mdadm --detail /dev/md0
```

Опишите состояние массива в отчёте.

5. Сымитируйте сбой одного из дисков:

```
mdadm /dev/md0 --fail /dev/sdc1
```

6. Проверьте состояние массива:

```
mdadm --detail /dev/md0
```

Убедитесь, что массив автоматически пересобирается. Отобразите и поясните состояние массива в отчёте.

7. Удалите массив и очистите метаданные:

```
umount /dev/md0
mdadm --stop /dev/md0
mdadm --zero-superblock /dev/sdb1
mdadm --zero-superblock /dev/sdc1
mdadm --zero-superblock /dev/sdd1
```

16.4.4. Преобразование массива RAID 1 в RAID 5

1. Получите полномочия администратора:

```
su -
```

2. Создайте массив RAID 1 из двух дисков:

```
mdadm --create --verbose /dev/md0 --level=1 --raid-devices=2
↪ /dev/sdb1 /dev/sdc1
```

3. Добавьте третий диск:

```
mdadm --add /dev/md0 /dev/sdd1
```

4. Проверьте состояние массива:

```
cat /proc/mdstat
mdadm --query /dev/md0
mdadm --detail /dev/md0
```

Опишите состояние массива в отчёте.

5. Измените тип массива RAID:

```
mdadm --grow /dev/md0 --level=5
```

6. Проверьте состояние массива:

```
mdadm --detail /dev/md0
```

Опишите состояние массива в отчёте.

7. Измените количество дисков в массиве RAID 5:

```
mdadm --grow /dev/md0 --raid-devices 3
```

8. Проверьте состояние массива:

```
mdadm --detail /dev/md0
```

Опишите состояние массива в отчёте.

9. Удалите массив и очистите метаданные:

```
umount /dev/md0
mdadm --stop /dev/md0
mdadm --zero-superblock /dev/sdb1
mdadm --zero-superblock /dev/sdc1
mdadm --zero-superblock /dev/sdd1
```

16.5. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания: скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы.
4. Выводы, согласованные с заданием работы.
5. Ответы на контрольные вопросы.

16.6. Контрольные вопросы

1. Приведите определение RAID.
2. Какие типы RAID-массивов существуют на сегодняшний день?
3. Охарактеризуйте RAID 0, RAID 1, RAID 5, RAID 6, опишите алгоритм работы, назначение, приведите примеры применения.

При ответах на контрольные вопросы рекомендуется ознакомиться с информацией из [1—3].

Список литературы

1. *Vadala D.* Managing RAID on Linux. — O'Reilly, 2004. — 264 с.
2. UNIX Power Tools / M. Loukides, T. O'Reilly, J. Peek, S. Powers. — O'Reilly Media, 2009. — 1160 p.
3. *Колисниченко Д. Н.* Самоучитель системного администратора Linux. — СПб. : БХВ-Петербург, 2011. — 544 с. — (Системный администратор). — ISBN 978-5-9775-0639-7.

Учебно-методический комплекс

Рекомендуется для направления подготовки

09.03.03 «Прикладная информатика»

Квалификация (степень) выпускника: бакалавр

Программа дисциплины

1. Цели и задачи дисциплины

Целью дисциплины является введение учащихся в предметную область администрирования современных операционных систем на базе Linux/Unix.

В процессе преподавания дисциплины решаются следующие задачи:

- анализ принципов построения и архитектур операционных систем Linux/Unix;
- обучение основам администрирования операционной системы типа Linux Unix.

2. Место дисциплины в структуре ОП ВО

Дисциплина относится к базовой части блока 1 «Дисциплины (модули)» учебного плана.

В табл. 16.1 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций обучающегося.

Описание компетенций для направления 09.03.03:

ОПК-3 — способность использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности;

ОПК-4 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности;

ПК-10 — способность принимать участие во внедрении, адаптации и настройке информационных систем;

ПК-11 — способность эксплуатировать и сопровождать информационные системы и сервисы;

ПК-13 — способность осуществлять установку и настройку параметров программного обеспечения информационных систем.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций: ОПК-3; ОПК-4; ПК-10; ПК-11; ПК-13.

В результате изучения дисциплины студент должен:

Знать:

- типы и виды современных операционных систем;
- концепции функционирования и администрирования современных ОС;
- архитектуру современных операционных систем.

Уметь:

- применять в профессиональной деятельности операционные системы;
- осуществлять настройку сервисов операционных систем для использования в профессиональной деятельности.

Владеть:

- навыками установки и настройки операционных систем и их сервисов для использования в профессиональной деятельности;
- способностью использовать современные инструментальные средства, установленные под операционной системой.

Таблица 16.1

Предшествующие и последующие дисциплины, направленные на формирование компетенций по направлению 09.03.03

№ п/п	Шифр компетенции	Предшествующие дисциплины	Последующие дисциплины (группы дисциплин)
Общекультурные компетенции			
1.	—	—	—
Общепрофессиональные компетенции			
1.	ОПК-3	—	Вычислительные системы, сети и телекоммуникации; Сетевые технологии; Администрирование сетевых подсистем; Администрирование локальных систем
2.	ОПК-4	Архитектура вычислительных систем; Операционные системы	Вычислительные системы, сети и телекоммуникации; Сетевые технологии; Администрирование сетевых подсистем; Администрирование локальных систем; Информационная безопасность
Профессиональные компетенции — производственно-технологическая деятельность			
1.	ПК-10	—	Сетевые технологии; Администрирование сетевых подсистем; Администрирование локальных систем; Управление ИТ-сервисами и контентом
2.	ПК-11	Операционные системы	Управление ИТ-сервисами и контентом, Информационная безопасность
3.	ПК-13	Операционные системы	Сетевые технологии; Администрирование сетевых подсистем; Администрирование локальных систем; Управление ИТ-сервисами и контентом; Информационная безопасность
Профессионально-специализированные компетенции специализации			
—	—	—	—

4. Объем дисциплины и виды учебной работы

Общая трудоёмкость дисциплины составляет 3 зачётные единицы.

Вид учебной работы	Всего часов	Семестры
		3
Аудиторные занятия (всего)	51	51
В том числе:		
<i>Лекции</i>	17	17
<i>Практические занятия (ПЗ)</i>	-	-
<i>Семинары (С)</i>	-	-
<i>Лабораторные работы (ЛР)</i>	34	34
Самостоятельная работа (всего)	57	57
Общая трудоёмкость:		
час.	108	108
зач. ед.	3	3

5. Содержание дисциплины

5.1 Содержание разделов дисциплины

Раздел 1. Общее администрирование.

Тема 1.1. Введение в операционную систему Linux. Установка Linux. Принципы организации ОС типа виртуальной машины. Архитектура ОС типа клиент-сервер.

Тема 1.2. Управление пользователями и группами.

Тема 1.3. Настройка прав доступа.

Тема 1.4. Работа с программными пакетами. Управление программным обеспечением, роли и задачи.

Тема 1.5. Управление системными службами.

Тема 1.6. Процессы. Управление процессами.

Тема 1.7. Управление журналами событий в системе.

Тема 1.8. Планировщики событий.

Тема 1.9. Управление SELinux.

Тема 1.10. Основы работы с модулями ядра ОС.

Тема 1.11. Управление загрузкой системы.

Раздел 2. Администрирование сети.

Тема 2.1. Настройка сети в Linux.

Тема 2.2. Пакетный фильтр. Виды пакетных фильтров. Настройка пакетных фильтров.

Раздел 3. Администрирование файловых систем.

Тема 3.1. Монтирование файловых систем. Точки монтирования. Виртуальные файловые системы.

Тема 3.2. Управление логическими томами.

Тема 3.3. Программный RAID.

5.2 Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Лекц.	Практ. зан.	Лаб. зан.	Се-мин.	СРС	Всего час.
1.	Общее администрирование	12		24		37	73
2.	Администрирование сети	2		4		8	14
3.	Администрирование файловых систем	3		6		12	21
Итого:		17		34		55	108

6. Лабораторный практикум**Раздел 1. Общее администрирование.**

Лабораторная работа 1. Установка и конфигурация операционной системы на виртуальную машину.

Лабораторная работа 2. Управление пользователями и группами.

Лабораторная работа 3. Настройка прав доступа.

Лабораторная работа 4. Работа с программными пакетами.

Лабораторная работа 5. Управление системными службами.

Лабораторная работа 6. Управление процессами.

Лабораторная работа 7. Управление журналами событий в системе.

Лабораторная работа 8. Планировщики событий.

Лабораторная работа 9. Управление SELinux.

Лабораторная работа 10. Основы работы с модулями ядра операционной системы.

Лабораторная работа 11. Управление загрузкой системы.

Раздел 2. Администрирование сети.

Лабораторная работа 12. Настройки сети в Linux.

Лабораторная работа 13. Фильтр пакетов.

Раздел 3. Администрирование файловых систем.

Лабораторная работа 14. Партиции, файловые системы, монтирование.

Лабораторная работа 15. Управление логическими томами.

Лабораторная работа 16. Программный RAID.

Контроль знаний.

7. Практические занятия (семинары)

Практические занятия (семинары) не предусмотрены.

8. Материально-техническое обеспечение дисциплины

Мультимедийная аудитория, оснащённая современным сетевым оборудованием и компьютерной техникой (комплект жидкокристаллический дисплей Sharp PNL702B, монитор 24" Acer V243HABD, системный блок (процессор Intel Core i7-2600 OEM <3.40GHz, 8Mb, 95W, LGA1155(Sandy Bridge)>, 16GB ОП, HDD 2 TB).

Дисплейные классы (ДК3, ДК4, ДК6, расположенные по адресу Москва, ул. Орджоникидзе, д. 3, корп. 5), с компьютерными рабочими местами пользователей с процессором не ниже Intel Core i3-550 3.2 GHz.

9. Информационное обеспечение дисциплины

- а) программное обеспечение: ОС Linux, VirtualBox, дистрибутив CentOS 7.
- б) базы данных, информационно-справочные и поисковые системы:
 - Request for Comments (RFC). — URL: <https://www.ietf.org/rfc.html>.
 - Security-Enhanced Linux. Linux с улучшенной безопасностью: руководство пользователя. Редакция 1.4 / М. McAllister, S. Radvan, D. Walsh, D. Grift, E. Paris, J. Morris; fedoraproject.org. — URL: <https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced-Linux/index.html>;
 - Проект ArchWiki. — URL: <https://wiki.archlinux.org/>;
 - Документация по продуктам RedHat. — URL: <https://access.redhat.com/documentation/en-us/>;
 - Портал The Linux Foundation. — URL: <https://www.linuxfoundation.org/>;
 - Портал IBM для разработчиков под Linux. — URL: <https://www.ibm.com/developerworks/learn/linux/index.html>.

10. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Кулябов Д. С., Королькова А. В. Основы администрирования операционных систем: лабораторные работы: учебное пособие. — Москва: РУДН, 2018;
2. Немец Э. и др. Unix и Linux. Руководство системного администратора. — Вильямс, 2014. — 4-е изд. — 1312 с.
3. Колисниченко Д. Н. Самоучитель системного администратора Linux. — СПб.: БХВ-Петербург, 2011. — 544 с.

Дополнительная литература:

1. Робачевский А., Немнюгин С., Стесик О. Операционная система UNIX. — 2-е изд. — Санкт-Петербург: BHV, 2010.
2. Vugt S. van. Red Hat RHCSA/RHCE 7 cert guide: Red Hat Enterprise Linux 7 (EX200 and EX300): Pearson IT Certification, 2016. — 1008 с.
3. Таненбаум Э., Бос Х. Современные операционные системы. — СПб.: Питер, 2015. — 4-е изд. — 1120 с.

11. Методические указания для обучающихся по освоению дисциплины

Учебным планом на изучение дисциплины отводится один семестр. В дисциплине предусмотрены лекции, лабораторный практикум, контрольные мероприятия. В конце семестра проводится итоговый контроль знаний.

11.1 Методические указания по самостоятельному освоению теоретического материала по дисциплине

Лекционный материал дисциплины охватывает темы, указанные в разделе 5.1 программы дисциплины. В ТУИС (<http://esystem.pfur.ru>) по темам лекций размещены презентации. Рекомендуется по указанным темам в дополнение к презентациям изучить литературу, указанную в п. 10 программы дисциплины.

11.2 Методические указания по выполнению лабораторных работ

Задания по лабораторным работам выполняются индивидуально каждым студентом в дисплейных классах в соответствии с календарным планом и методическими указаниями по выполнению лабораторных работ по дисциплине. Часть лабораторных работ предусматривает задания для индивидуальной самостоятельной работы студента, обязательные для выполнения. Выполнение заданий для самостоятельной работы позволяет студенту приобрести дополнительные навыки и закрепить знания по изучаемой теме.

По результатам выполнения каждой лабораторной работы студентом готовится отчёт. Отчёты в электронном виде сдаются студентом на проверку через соответствующие разделы ТУИС (<http://esystem.pfur.ru>).

11.3. Методические указания по подготовке к контрольным мероприятиям

Контрольные мероприятия по дисциплине проводятся в форме тестирования в ТУИС (<http://esystem.pfur.ru>). Итоговый контроль в форме теста проводится по темам всех разделов дисциплины. Вопросы для подготовки к промежуточному и итоговому тестированию размещены в соответствующем разделе ТУИС (<http://esystem.pfur.ru>).

Паспорт фонда оценочных средств

Код компетенции	Контролируемый раздел	Контролируемая тема	ФОСы		Баллы темы	Баллы раздела
			Ауд. раб.	Зачёт		
			Вып. ЛР	Итог. контроль		
ОПК-3, ОПК-4, ПК-10, ПК-11, ПК-13 (для направления 09.03.03)	Общее администрирование	Установка Linux	5	10	6	65
		Управление пользователями и группами	5		6	
		Настройка прав доступа	5		6	
		Работа с программными пакетами. Управление пакетами	5		6	
		Управление системными службами	5		6	
		Процессы. Управление процессами	5		6	
		Управление журналами событий в системе	5		6	
		Планировщики событий	5		6	
		Управление SELinux	5		6	
		Основы работы с модулями ядра операционной системы	5		6	
		Управление загрузкой системы	5		6	
	Администрирование сети	Настройки сети в Linux	5	5	7	15
		Пакетный фильтр	5		7	
	Администрирование файловых систем	Монтирование файловых систем	5	5	7	20
		Управление логическими томами	5		7	
		Программный RAID	5		7	
Итого:			80	20	100	100

Описание компетенций для направления 09.03.03:

ОПК-3 — способность использовать основные законы естественнонаучных дисциплин и современные информационно-коммуникационные технологии в профессиональной деятельности;

ОПК-4 — способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учётом основных требований информационной безопасности;

ПК-10 — способность принимать участие во внедрении, адаптации и настройке информационных систем;

ПК-11 — способность эксплуатировать и сопровождать информационные системы и сервисы;

ПК-13 — способность осуществлять установку и настройку параметров программного обеспечения информационных систем.

Фонд оценочных средств

Балльно-рейтинговая система оценки уровня знаний

Сводная оценочная таблица дисциплины

Раздел	Тема	Формы контроля		Баллы темы	Баллы раздела
		Ауд. раб.	Зачёт		
		Вып. ЛР	Итог. контр.		
Общее администрирование	Установка Linux	5	10	6	65
	Управление пользователями и группами	5		6	
	Настройка прав доступа	5		6	
	Работа с программными пакетами. Управление пакетами	5		6	
	Управление системными службами	5		6	
	Процессы. Управление процессами	5		6	
	Управление журналами событий в системе	5		6	
	Планировщики событий	5		6	
	Управление SELinux	5		6	
	Основы работы с модулями ядра операционной системы	5		6	
	Управление загрузкой системы	5		6	
Администрирование сети	Настройки сети в Linux	5	5	7	15
	Пакетный фильтр	5		7	
Администрирование файловых систем	Монтирование файловых систем	5	5	7	20
	Управление логическими томами	5		7	
	Программный RAID	5		7	
Итого:		80	20	100	100

Таблица соответствия баллов и оценок

Баллы БРС	Традиционные оценки РФ	Оценки ECTS
95–100	5	A
86–94		B
69–85	4	C
61–68	3	D
51–60		E
31–50	2	FX
0–30		F
51–100	Зачёт	Passed

Правила применения БРС

1. Раздел (тема) учебной дисциплины считается освоенным, если студент набрал более 50% от возможного числа баллов по этому разделу (теме).
2. Студент не может быть аттестован по дисциплине, если он не освоил все темы и разделы дисциплины, указанные в сводной оценочной таблице дисциплины.
3. По решению преподавателя и с согласия студентов, не освоивших отдельные разделы (темы) изучаемой дисциплины, в течение учебного семестра могут быть повторно проведены мероприятия текущего контроля успеваемости или выданы дополнительные учебные задания по этим темам или разделам. При этом студентам за данную работу засчитывается минимально возможный положительный балл (51% от максимального балла).
4. При выполнении студентом дополнительных учебных заданий или повторного прохождения мероприятий текущего контроля полученные им баллы засчитываются за конкретные темы. Итоговая сумма баллов не может превышать максимальное количество баллов, установленное по данным темам (в соответствии с приказом Ректора № 564 от 20.06.2013). По решению преподавателя предыдущие баллы, полученные студентом по учебным заданиям, могут быть аннулированы.
5. График проведения мероприятий текущего контроля успеваемости формируется в соответствии с календарным планом курса. Студенты обязаны сдавать все задания в сроки, установленные преподавателем.
6. Время, которое отводится студенту на выполнение мероприятий текущего контроля успеваемости, устанавливается преподавателем. По окончании отведённого времени студент должен сдать работу преподавателю, вне зависимости от того, завершена она или нет.
7. Использование источников (в том числе конспектов лекций и лабораторных работ) во время выполнения контрольных мероприятий возможно только с разрешения преподавателя.
8. Отсрочка в прохождении мероприятий текущего контроля успеваемости считается уважительной только в случае болезни студента, что подтверждается наличием у него медицинской справки, заверенной круглой печатью в поликлинике № 25, предоставляемой преподавателю не позднее двух недель после выздоровления.

В этом случае выполнение контрольных мероприятий осуществляется после выздоровления студента в срок, назначенный преподавателем. В противном случае отсутствие студента на контрольном мероприятии признается неуважительным.

9. Студент допускается к итоговому контролю знаний с любым количеством баллов, набранных в семестре.
10. Итоговый контроль знаний оценивается из 20 баллов, независимо от числа баллов за семестр.
11. Если в итоге за семестр студент получил менее 31 балла, то ему выставляется оценка F и студент должен повторить эту дисциплину в установленном порядке. Если же в итоге студент получил 31–50 баллов, т. е. FX, то студенту разрешается добор необходимого (до 51) количества баллов путём повторного одноразового выполнения предусмотренных контрольных мероприятий, при этом по усмотрению преподавателя аннулируются соответствующие предыдущие результаты. Ликвидация задолженностей проводится в период с 07.02 по 28.02 (с 07.09 по 28.09) по согласованию с деканатом.

Критерии оценки по дисциплине

95–100 баллов:

- полное и своевременное выполнение на высоком уровне лабораторных работ с оформлением отчётов, успешное прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное, глубокое и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответов на вопросы, умение делать обоснованные выводы;
- безупречное владение программным обеспечением, умение эффективно использовать его в постановке и решении научных и профессиональных задач;
- выраженная способность самостоятельно и творчески решать поставленные задачи;
- полная самостоятельность и творческий подход при изложении материала по программе дисциплины;
- полное и глубокое усвоение основной и дополнительной литературы, рекомендованной программой дисциплины и преподавателем.

86–94 балла:

- полное и своевременное выполнение на хорошем уровне лабораторных работ с оформлением отчётов, успешное прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное, глубокое и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- использование научной терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы;
- хорошее владение программным обеспечением, умение эффективно использовать его в постановке и решении научных и профессиональных задач;
- способность самостоятельно решать поставленные задачи в нестандартных производственных ситуациях;
- усвоение основной и дополнительной литературы, нормативных и законодательных актов, рекомендованных программой дисциплины и преподавателем.

69–85 баллов:

- своевременное выполнение на хорошем уровне лабораторных работ с оформлением отчётов, прохождение контрольных мероприятий, предусмотренных программой курса;

- хороший уровень культуры исполнения лабораторных работ;
- систематизированное и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- владение программным обеспечением, умение использовать его в постановке и решении научных и профессиональных задач;
- способность самостоятельно решать проблемы в рамках программы дисциплины;
- усвоение основной литературы.

51-68 баллов:

- выполнение на удовлетворительном уровне лабораторных работ с оформлением отчётов, прохождение контрольных мероприятий, предусмотренных программой курса;
- систематизированное и полное освоение навыков и компетенций по всем разделам программы дисциплины;
- удовлетворительное владение программным обеспечением, умение использовать его в постановке и решении научных и профессиональных задач;
- способность решать проблемы в рамках программы дисциплины;
- удовлетворительное усвоение основной литературы;

31-50 баллов, НЕ ЗАЧТЕНО:

- невыполнение, несвоевременное выполнение или выполнение на неудовлетворительном уровне лабораторных работ, непрохождение контрольных мероприятий, предусмотренных программой курса;
- недостаточно полный объем навыков и компетенций в рамках программы дисциплины;
- неумение использовать в практической деятельности научную терминологию, изложение ответа на вопросы с существенными стилистическими и логическими ошибками;
- слабое владение программным обеспечением по разделам программы дисциплины, некомпетентность в решении стандартных (типовых) производственных задач;
- способность решать проблемы в рамках программы дисциплины;
- удовлетворительное усвоение основной литературы.

0-30 баллов, НЕ ЗАЧТЕНО:

- отсутствие умений, навыков, знаний и компетенций в рамках программы дисциплины;
- невыполнение лабораторных заданий, непрохождение контрольных мероприятий, предусмотренных программой курса; отказ от ответов по программе дисциплины;
- игнорирование занятий по дисциплине по неуважительной причине.

Примерный перечень оценочных средств

Учебным планом на изучение дисциплины отводится один семестр. В дисциплине предусмотрены лекции, лабораторный практикум, контрольные мероприятия. В конце семестра проводится итоговый контроль знаний.

Оценивание результатов освоения дисциплины производится в соответствии с балльно-рейтинговой системой. По дисциплине предусмотрен зачёт.

Итоговый контроль знаний по дисциплине проводится в форме тестирования, но при необходимости зачёт может проводиться в форме письменного ответа на вопросы из билетов.

п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Аудиторная работа			
1.	Лабораторная работа	Система практических заданий, направленных на формирование практических навыков у обучающихся	Фонд практических заданий
2.	Тест	Система стандартизированных заданий (вопросов), позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося	База тестовых заданий
3.	Зачёт	Форма проверки качества выполнения студентами лабораторных работ, домашних заданий и других заданий, контрольных мероприятий в соответствии с утверждённой программой	Примеры заданий
Самостоятельная работа			
1.	Подготовка отчётов по результатам выполнения лабораторных работ	Форма проверки качества выполнения студентами лабораторных работ в соответствии с утверждённой программой	Фонд практических заданий в рамках лабораторного практикума по дисциплине

Комплект заданий для итогового контроля знаний

Итоговый контроль знаний по дисциплине проводится в форме компьютерного тестирования.

Примерный перечень вопросов итогового контроля знаний:

1. Необходимо определить, какие пары файлов являются жёсткими ссылками друг на друга, не изменяя содержимое файлов (выбор всех возможных вариантов).
2. Укажите аналог `ipconfig` из Windows для анализа сетевых карт в Linux.
3. Укажите аналог глобального сообщения об ошибке BSOD в Windows для Unix.
4. В каком виде представлена файловая система в Unix?
5. В каком файле содержатся настройки логинов пользователей, их домашних каталогов и переменных окружения?
6. В каком файле хранится список примонтированных устройств?
7. В текущей директории имеется файл `file`. Какие права на файл будут установлены после выполнения следующей команды: `chmod u+rx-w,g-wr+x,o-rwx file`?

8. В текущем каталоге есть файл `file`. Какие права доступа будут у этого файла после выполнения следующей команды: `chmod u+r-x+w,g-r+xw,a-r+w-x file`?
9. Вам необходимо пересобрать ядро ОС. Перед новой компиляцией какой командой можно полностью удалить файлы конфигураций и объектные файлы, оставшиеся после предыдущей компиляции?
10. Вам нужно добавить информацию в уже созданный `tar`-файл. Что для этого нужно сделать?
11. Вам нужно найти полный путь определённой команды. Как это можно сделать?
12. Вам нужно произвести поиск во всех каталогах, чтобы найти определённый файл. Как это можно сделать, используя команду `find`, чтобы во время поиска сохранить возможность ввода команд?
13. Вам поручили работу по администрированию нового сервера. На нем хранится база данных, используемая в коммерческом отделе компании. Данная информация часто меняется и нигде не дублируется. Какие меры нужно принять для защиты данных в случае непредвиденных обстоятельств?
14. Ввод какой строки повторит предыдущую команду?
15. Вы ввели следующую командную строку: `ls -al /home/ hadden`. Какое сочетание клавиш можно использовать, чтобы убрать пробел между `/` и `hadden` без необходимости вводить повторно всю строку?
16. Вы вводите команду: `cat MyFile | sort > DirList &`. В ответ операционная система выдаёт: `[4] 3499`. Что это значит?
17. Вы находитесь в директории с исходниками ядра Linux. В каком файле хранится конфигурация для компиляции (подразумевается что файл существует от предыдущей компиляции или он был создан одной из конфигурационных утилит)?
18. Вы находитесь в процессе пересборки ядра. Какая команда компилирует модули?
19. Вы пытаетесь выйти из системы, но получаете сообщение об ошибке, в котором говорится, что вам отказано в этом. После выдачи команды `jobs` вы замечаете, что один из процессов выполняется в фоновом режиме. Что нужно сделать для корректного завершения процесса?
20. Вы хотите повторить команду, начинающуюся с `'ab'`. Как вы это сделаете?
21. Выберите все правильные утверждения. Чем отличается `kill -KILL PID [kill -9 PID]` от `kill -TERM PID [или kill -15 PID]`?
22. Вывод справки в Unix системах производится по команде...
23. Для чего используется команда `wc`?
24. Если значение `umask` равно `0022`, каким будет значение прав доступа к новым файлам?
25. За основную единицу измерения количества информации принят...
26. Имя учётной записи встроенного администратора любой Unix системы...
27. Информация о том, какие файловые системы следует монтировать при загрузке, находится в файле...
28. Использование какого командного интерпретатора обеспечивает переносимость `shell`-скриптов на все POSIX-системы?
29. К стационарному компьютеру под управлением Linux подключён 1 диск на второй IDE канал в режиме `master`, как будет называться файл устройства по умолчанию?
30. Как записывается десятичное число 2 в двоичной системе счисления?
31. Как можно просмотреть состояние использования оперативной и виртуальной памяти?
32. Как очистить заблокированный файл?
33. Как примонтировать директорию `/somePath/1` на директорию `/somePath/2`?
34. Как удаляются документы в Unix системах?
35. Какая из перечисленных аббревиатур не является программной оболочкой?

36. Какая из следующих команд может быть использована для отображения большого списка файлов с удобочитаемым размером файла (к примеру 6.8 МБ вместо 6819467)?
37. Какая из следующих команд позволит выполнить поиск текста в файле без предварительного открытия файла другой командой?
38. Какая команда выводит на экран путь к текущему каталогу?
39. Какая команда изменяет права доступа к файлам и директориям?
40. Какая команда используется для отображения информации о модуле ядра?
41. Какая команда Linux используется для сборки программы из исходного кода?
42. Какая команда отображает в реальном времени запущенные процессы, сортируя их по заданному критерию?
43. Какая команда отобразит размер каталога `/usr/lib`?
44. Какая команда показывает информацию о запущенных в системе процессах?
45. Какая команда показывает статистику загрузки процессора и памяти в реальном времени?
46. Какая команда предназначена для просмотра и изменения конфигурации сетевых интерфейсов?
47. Какая команда служит для создания файлов устройств?
48. Какая опция команды `shutdown` используется для отмены ожидания завершения работы системы?
49. Какая переменная среды определяет рабочий каталог после успешной регистрации в системе?
50. Какая последовательность символов отдаёт команду текстовому редактору `vi` выйти из редактора с сохранением результатов ввода?
51. Каким образом в `vi/vim` отменить операцию (допустим вы случайно удалили длинную строку)?
52. Какое значение `run level` соответствует многопользовательскому режиму?
53. Какой `run level` соответствует перезагрузке системы?
54. Какой `run level` соответствует режиму администрирования?
55. Какой процесс в Linux не имеет родительского процесса?
56. Какой файл необходимо создать для запрета входа в систему непривилегированных пользователей?
57. Команда изменения атрибутов доступа объекта...
58. Команда изменения владельца объекта...
59. Команда просмотра каталога в Unix системах...
60. Командный интерпретатор пользователя — `bash`, производится логин в систему. Команды из каких файлов обязательно выполнит `bash` напрямую (при условии, что все перечисленные файлы существуют и доступны для чтения)?
61. Копирование файла производится командой...
62. Наиболее часто используемая команда в Unix системах для запуска графического интерфейса...
63. Основные задачи ядра системы...
64. Отметьте все варианты правильного использования команды `cd`.
65. Перевод режима работы в режим суперпользователя.
66. Права доступа `1777` на директорию означают, что в ней (укажите все подходящие варианты)...
67. При помощи какой утилиты можно просмотреть загруженные модули ядра ОС Linux?
68. При форматировании файловой системы `ext2` определённый фиксированный процент блоков на диске резервируется для пользователя `root`. С помощью какой утилиты этот процент можно изменить?
69. С помощью какой команды можно определить размер файла?

70. С помощью какой команды можно определить, встроена ли некоторая другая команда в оболочку?
71. С помощью какой команды можно получить список подсоединённых PCI устройств?
72. Укажите корректный вариант использования grep.
73. Укажите привилегии пользователя в восьмеричной системе для файла с атрибутами `rw-xrw-rw-`.
74. Фильтром в UNIX-системах называется...
75. Чему эквивалентна запись права доступа 644?
76. Что из перечисленного не является фильтром?
77. Что из указанного является прослойкой между оборудованием и программной оболочкой в операционной системе Linux?
78. Что находится в каталоге `/etc/init.d` в Linux-системе?
79. Что не является загрузчиком ОС?
80. Что такое LILO (в терминах Linux)?
81. Что такое виртуальная память?

Критерии оценки итогового тестирования

Итоговое тестирование оценивается в соответствии с БРС и паспортом ФОС. Проверяется правильность ответов на вопросы теста.

Комплект разноуровневых задач (заданий)

1. Задания репродуктивного уровня

В качестве заданий репродуктивного уровня предлагаются вопросы для самопроверки и обсуждения по темам курса (см. лабораторный практикум).

2. Задания реконструктивного уровня

В качестве заданий реконструктивного уровня предполагаются задания лабораторного практикума.

Критерии оценки выполнения заданий по лабораторным работам

Оцениваются полнота выполнения работы, оформление результатов, полнота ответов на контрольные вопросы, если это предусмотрено заданием.

Сведения об авторах

Кулябов Дмитрий Сергеевич — доцент, доктор физико-математических наук, доцент кафедры прикладной информатики и теории вероятностей РУДН.

Королькова Анна Владиславовна — доцент, кандидат физико-математических наук, доцент кафедры прикладной информатики и теории вероятностей РУДН.

Учебное издание

**Дмитрий Сергеевич Кулябов,
Анна Владиславовна Королькова**

Основы администрирования операционных систем

Редактор *И. Л. Панкратова*
Технический редактор *Н. А. Ясько*
Компьютерная вёрстка *А. В. Королькова, Д. С. Кулябов*

Подписано в печать 22.10.2018 г. Формат 60×84/16. Печать офсетная.
Усл. печ. л. _____. Тираж 500 экз. Заказ № 1228.

Российский университет дружбы народов
115419, ГСП-1, г. Москва, ул. Орджоникидзе, д. 3

Типография РУДН
115419, ГСП-1, г. Москва, ул. Орджоникидзе, д. 3, тел. 952-04-41