

Прохождение внешнего курса. Часть 2.

Работа с файлами и управление доступами

Отчёт

Сергеев Даниил Олегович

Содержание

1 Цель работы	9
2 Задание	10
3 Ход выполнения лабораторной работы	11
3.1 Модуль 4. Получение справки. Использование справочных систем, работа с текстовыми файлами и логами	11
3.1.1 Задания по теме «Поиск справочной информации в Linux»	11
3.1.2 Тест по теме «Поиск справочной информации в Linux»	15
3.1.3 Задания по теме «Работа с текстовыми файлами в Linux»	17
3.1.4 Тест по теме «Работа с текстовыми файлами в Linux»	20
3.1.5 Задания по теме «Анализ системных логов»	23
3.1.6 Тест по теме «Анализ системных логов»	24
3.1.7 Задания по теме «Автоматизация анализа логов и работы с текстом»	26
3.1.8 Тест по теме «Автоматизация анализа логов и работы с текстом»	28
3.2 Модуль 5. Управление пользователями и группами	31
3.2.1 Задания по теме «Основы управления пользователями и группами»	31
3.2.2 Тест по теме «Основы управления пользователями и группами»	34
3.2.3 Задания по теме «Основы управления доступом и разрешениями»	37
3.2.4 Тест по теме «Основы управления доступом и разрешениями»	40
3.2.5 Задания по теме «Повышение безопасности работы с учетными записями»	42
3.2.6 Тест по теме «Повышение безопасности работы с учетными записями»	44
3.2.7 Задания по теме «Политика паролей и учетных записей»	47
3.2.8 Тест по теме «Политика паролей и учетных записей»	50
3.3 Модуль 6. Управление доступом	53
3.3.1 Задания по теме «Что такое права доступа в Linux»	53
3.3.2 Тест по теме «Что такое права доступа в Linux»	55
3.3.3 Задания по теме «Изменение прав доступа: chmod, chown, chgrp»	57
3.3.4 Тест по теме «Изменение прав доступа: chmod, chown, chgrp»	58
3.3.5 Задания по теме «Расширенные списки доступа (ACL) для управления доступом»	60

3.3.6	Задания по теме «Специальные разрешения: SUID, SGID, Sticky Bit»	63
3.3.7	Тест по теме «Специальные разрешения: SUID, SGID, Sticky Bit»	65
3.4	Модуль 7. Управление процессами	67
3.4.1	Задания по теме «Основы управления процессами в Linux»	67
3.4.2	Тест по теме «Основы управления процессами в Linux»	70
3.4.3	Задания по теме «Управление приоритетами процессов: nice и renice»	72
3.4.4	Тест по теме «Управление приоритетами процессов: nice и renice»	74
3.4.5	Задания по теме «Контроль системных сервисов: systemd и systemctl»	76
3.4.6	Тест по теме «Контроль системных сервисов: systemd и systemctl»	79
3.4.7	Задания по теме «Управление фоновыми процессами (демонами) в Linux»	81
3.4.8	Тест по теме «Управление фоновыми процессами (демонами) в Linux»	85
3.5	Вывод	87

Список иллюстраций

3.1 «Поиск справочной информации в Linux». Условия заданий	11
3.2 Справочная информация о grep	12
3.3 Справочная информация о systemctl	13
3.4 Поиск файла документации info	14
3.5 Подтверждение прохождения теста «Поиск справочной информации в Linux»	15
3.6 «Поиск справочной информации в Linux». Вопрос №1	15
3.7 «Поиск справочной информации в Linux». Вопрос №2	16
3.8 «Поиск справочной информации в Linux». Вопрос №3	16
3.9 «Работа с текстовыми файлами в Linux». Условия заданий	17
3.10 Вывод команды less	17
3.11 Вывод команды grep для /var/log/messages	18
3.12 Изменение параметра PermitRootLogin	18
3.13 Вывод фильтра awk	19
3.14 Подтверждение прохождения теста «Работа с текстовыми файлами в Linux»	20
3.15 «Работа с текстовыми файлами в Linux». Вопрос №1	20
3.16 «Работа с текстовыми файлами в Linux». Вопрос №2	21
3.17 «Работа с текстовыми файлами в Linux». Вопрос №3	21
3.18 «Работа с текстовыми файлами в Linux». Вопрос №4	22
3.19 «Работа с текстовыми файлами в Linux». Вопрос №5	22
3.20 «Анализ системных логов». Условия заданий	23
3.21 Просмотр ошибок в системном журнале за последний день	23
3.22 Просмотр ошибок авторизации SSH	24
3.23 Подтверждение прохождения теста «Анализ системных логов»	24
3.24 «Анализ системных логов». Вопрос №1	25
3.25 «Анализ системных логов». Вопрос №2	25
3.26 «Анализ системных логов». Вопрос №3	26
3.27 «Автоматизация анализа логов и работы с текстом». Условия заданий	26
3.28 Написание скрипта	27
3.29 Редактирование crontab	27
3.30 Проверка применения фильтра awk для ошибок входа	28
3.31 Подтверждение прохождения теста «Автоматизация анализа логов и работы с текстом»	28
3.32 «Автоматизация анализа логов и работы с текстом». Вопрос №1	29
3.33 «Автоматизация анализа логов и работы с текстом». Вопрос №2	29
3.34 «Автоматизация анализа логов и работы с текстом». Вопрос №3	29

3.35 «Автоматизация анализа логов и работы с текстом». Вопрос №4	30
3.36 «Основы управления пользователями и группами». Условия заданий	31
3.37 Создание пользователя ivan	32
3.38 Создание группы developers	32
3.39 Добавление пользователя ivan в группу	32
3.40 Изменение групп пользователя ivan	33
3.41 Удаление пользователя ivan	33
3.42 Подтверждение прохождения теста «Основы управления пользователями и группами»	34
3.43 «Основы управления пользователями и группами». Вопрос №1	34
3.44 «Основы управления пользователями и группами». Вопрос №2	35
3.45 «Основы управления пользователями и группами». Вопрос №3	35
3.46 «Основы управления пользователями и группами». Вопрос №4	36
3.47 «Основы управления доступом и разрешениями». Условия заданий	37
3.48 Проверка прав файла и маски	38
3.49 Изменение прав доступа к файлу	38
3.50 Возврат к изначальным правам доступа	38
3.51 Смена владельца файла на root	39
3.52 Смена владельца файла на dosergeev	39
3.53 Подтверждение прохождения теста «Основы управления доступом и разрешениями»	40
3.54 «Основы управления доступом и разрешениями». Вопрос №1	40
3.55 «Основы управления доступом и разрешениями». Вопрос №2	41
3.56 «Основы управления доступом и разрешениями». Вопрос №3	41
3.57 «Повышение безопасности работы с учетными записями». Условия заданий	42
3.58 Вывод всех команд с sudo	42
3.59 Ошибка при использовании sudo	43
3.60 Добавление ivan в группу wheel	44
3.61 Подтверждение прохождения теста «Повышение безопасности работы с учетными записями»	44
3.62 «Повышение безопасности работы с учетными записями». Вопрос №1	45
3.63 «Повышение безопасности работы с учетными записями». Вопрос №2	45
3.64 «Повышение безопасности работы с учетными записями». Вопрос №3	46
3.65 «Повышение безопасности работы с учетными записями». Вопрос №4	46
3.66 «Политика паролей и учетных записей». Условия заданий	47
3.67 Фильтр пользователей по алгоритму хэширования SHA-512	47
3.68 Смена времени действия пароля для ivan	48
3.69 Блокировка пользователя ivan	49
3.70 Разблокировка пользователя ivan	49
3.71 Подтверждение прохождения теста «Политика паролей и учетных записей»	50
3.72 «Политика паролей и учетных записей». Вопрос №1	50
3.73 «Политика паролей и учетных записей». Вопрос №2	51

3.74 «Политика паролей и учетных записей». Вопрос №3	51
3.75 «Политика паролей и учетных записей». Вопрос №4	52
3.76 «Политика паролей и учетных записей». Вопрос №5	52
3.77 «Что такое права доступа в Linux». Условия заданий	53
3.78 Проверка прав доступа для файлов и каталогов корневого раздела	53
3.79 Редактирование маски для новых файлов	54
3.80 Подтверждение прохождения теста «Что такое права доступа в Linux»	55
3.81 «Что такое права доступа в Linux». Вопрос №1	55
3.82 «Что такое права доступа в Linux». Вопрос №2	56
3.83 «Что такое права доступа в Linux». Вопрос №3	56
3.84 «Изменение прав доступа: chmod, chown, chgrp». Условия заданий	57
3.85 Создание файла и настройка прав доступа	57
3.86 Создание группы и модификация группы файла	58
3.87 Подтверждение прохождения теста «Изменение прав доступа: chmod, chown, chgrp»	58
3.88 «Изменение прав доступа: chmod, chown, chgrp». Вопрос №1	59
3.89 «Изменение прав доступа: chmod, chown, chgrp». Вопрос №2	59
3.90 «Изменение прав доступа: chmod, chown, chgrp». Вопрос №3	60
3.91 «Расширенные списки доступа (ACL) для управления доступом». Условия заданий	60
3.92 Установка прав доступа конкретному пользователю	61
3.93 Установка права на выполнение для конкретной группы	61
3.94 Сброс расширенных списков доступа ACL для файла	62
3.95 «Специальные разрешения: SUID, SGID, Sticky Bit». Условия заданий	63
3.96 Установка SUID для файла	63
3.97 Установка SGID для каталога	64
3.98 Установка Sticky-bit для общего каталога	64
3.99 Подтверждение прохождения теста «Специальные разрешения: SUID, SGID, Sticky Bit»	65
3.100 «Специальные разрешения: SUID, SGID, Sticky Bit». Вопрос №1	65
3.101 «Специальные разрешения: SUID, SGID, Sticky Bit». Вопрос №2	66
3.102 «Специальные разрешения: SUID, SGID, Sticky Bit». Вопрос №3	66
3.103 «Основы управления процессами в Linux». Условия заданий	67
3.104 «Процесс потребляющий наибольшее количество памяти - PID 2384	67
3.105 «Работа с передним и задним фоном задач	68
3.106 «Настройка колонок вывода htop	69
3.107 «Фильтрация процесса по названию	69
3.108 Подтверждение прохождения теста «Основы управления процессами в Linux»	70
3.109 «Основы управления процессами в Linux». Вопрос №1	70
3.110 «Основы управления процессами в Linux». Вопрос №2	71
3.111 «Основы управления процессами в Linux». Вопрос №3	71
3.112 «Управление приоритетами процессов: nice и renice». Условия заданий	72
3.113 «Запуск процесса с низким приоритетом	72

3.114Повышение приоритета для процесса	73
3.115Изменение nice у процесса с самым маленьким приоритетом	73
3.116Подтверждение прохождения теста «Управление приоритетами процессов: nice и renice»	74
3.117Управление приоритетами процессов: nice и renice». Вопрос №1	74
3.118Управление приоритетами процессов: nice и renice». Вопрос №2	75
3.119Управление приоритетами процессов: nice и renice». Вопрос №3	75
3.120Контроль системных сервисов: systemd и systemctl». Условия заданий	76
3.121Список всех активных сервисов Network	76
3.122Проверка статуса и перезапуск httpd	77
3.123Последние сообщения httpd	77
3.124Статус службы httpd после отключения автозапуска	78
3.125Статус службы после перезапуска	78
3.126Подтверждение прохождения теста «Контроль системных сервисов: systemd и systemctl»	79
3.127Контроль системных сервисов: systemd и systemctl». Вопрос №1	79
3.128Контроль системных сервисов: systemd и systemctl». Вопрос №2	80
3.129Контроль системных сервисов: systemd и systemctl». Вопрос №3	80
3.130Управление фоновыми процессами (демонами) в Linux». Условия заданий	81
3.131Запуск сервиса mydaemon	83
3.132Завершение юнита mydaemon	83
3.133Юнит mydaemon после перезапуска	84
3.134Подтверждение прохождения теста «Управление фоновыми процессами (демонами) в Linux»	85
3.135Управление фоновыми процессами (демонами) в Linux». Вопрос №1	85
3.136Управление фоновыми процессами (демонами) в Linux». Вопрос №2	86
3.137Управление фоновыми процессами (демонами) в Linux». Вопрос №3	86

Список таблиц

1 Цель работы

Глубже погрузиться в работу с Linux. Научиться находить справочную информацию, редактировать текстовые файлы, работать с выводом команд. Узнать, как управлять пользователями и доступом к файлам или каталогам. А еще – изучить мониторинг и управление процессами, сервисами и демонами.

2 Задание

- Модуль 4. Получение справки. Использование справочных систем, работа с текстовыми файлами и логами
- Модуль 5. Управление пользователями и группами
- Модуль 6. Управление доступом
- Модуль 7. Управление процессами

3 Ход выполнения лабораторной работы

3.1 Модуль 4. Получение справки. Использование справочных систем, работа с текстовыми файлами и логами

3.1.1 Задания по теме «Поиск справочной информации в Linux»

Задание №1

Используйте man чтобы узнать, как работает команда grep.

Задание №2

Найдите документацию о systemctl с помощью info.

Задание №3

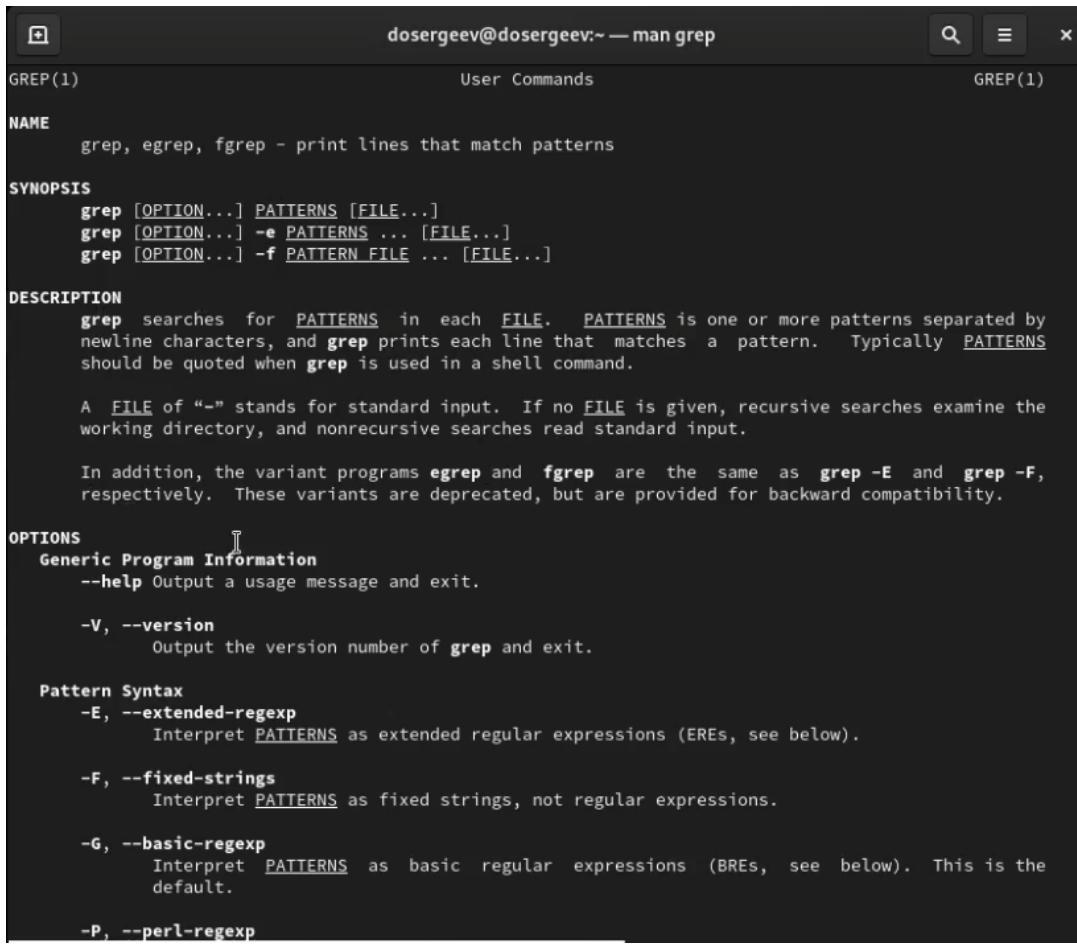
Откройте локальную документацию о info.

Рис. 3.1: «Поиск справочной информации в Linux». Условия заданий

3.1.1.1 Задание №1

Выведем справочную информацию

`man grep`



The screenshot shows a terminal window with the title bar "dosergeev@dosergeev:~ — man grep". The window content is the man page for the grep command, titled "GREP(1)". The page is divided into sections: NAME, SYNOPSIS, DESCRIPTION, OPTIONS, and Pattern Syntax. The SYNOPSIS section shows three ways to use grep: with patterns and files, with -e, or with -f. The DESCRIPTION section explains what grep does and how it handles standard input. The OPTIONS section covers generic program information, version output, and pattern syntax options (-E, -F, -G, -P). The Pattern Syntax section details the four interpretation modes: extended regular expressions (-E), fixed strings (-F), basic regular expressions (-G), and perl regular expressions (-P).

Рис. 3.2: Справочная информация о grep

3.1.1.2 Задание №2

Теперь узнаем информацию о systemctl, но уже другой командой

```
info systemctl
```

```
dosergeev@dosergeev:~ — info systemctl
SYSTEMCTL(1)           systemctl                   SYSTEMCTL(1)

NAME
    systemctl - Control the systemd system and service manager

SYNOPSIS
    systemctl [OPTIONS...] COMMAND [UNIT...]

DESCRIPTION
    systemctl may be used to introspect and control the state of the "systemd" system and service
    manager. Please refer to systemd\(1\) for an introduction into the basic concepts and
    functionality this tool manages.

COMMANDS
    The following commands are understood:

    Unit Commands (Introspection and Modification)
        list-units [PATTERN...]
            List units that systemd currently has in memory. This includes units that are either
            referenced directly or through a dependency, units that are pinned by applications
            programmatically, or units that were active in the past and have failed. By default only
            units which are active, have pending jobs, or have failed are shown; this can be changed
            with option --all. If one or more PATTERNs are specified, only units matching one of them
            are shown. The units that are shown are additionally filtered by --type= and --state=
            if those options are specified.

            Note that this command does not show unit templates, but only instances of unit templates.
            Units templates that aren't instantiated are not runnable, and will thus never show up in
            the output of this command. Specifically this means that foo@.service will never be shown
            in this list – unless instantiated, e.g. as foo@bar.service. Use list-unit-files (see
            below) for listing installed unit template files.

            Produces output similar to

            UNIT          LOAD  ACTIVE SUB      DESCRIPTION
            sys-module-fuse.device   loaded active plugged /sys/module/fuse
            -.mount         loaded active mounted Root Mount
            boot-efi.mount    loaded active mounted /boot/efi
            systemd-journald.service loaded active running Journal Service
```

Рис. 3.3: Справочная информация о systemctl

3.1.1.3 Задание №3

Справочная информация команды `info` находится в каталоге `/usr/share/info`

```
ls /usr/share/info
```

Перейдем в каталог и откроем файл документации через vim

```
cd /usr/share/info
# -R открыть только для чтения
vim -R info-stnd.info.gz
```

```
[dosergeev@dosergeev ~]$ ls /usr/share/info
accounting.info.gz      find.info-1.gz      kpathsea.info.gz      R-exts.info-2.gz
annobin.info.gz         find.info-2.gz      latex2man.info.gz    R-exts.info-3.gz
as.info.gz              find.info.gz       ld.info.gz          R-exts.info.gz
autoconf.info.gz        find-maint.info.gz libcdio.info.gz      R-FAQ.info.gz
automake-history.info.gz flex.info-1.gz     libgomp.info.gz      R-intro.info.gz
automake.info-1.gz      flex.info-2.gz     liblouis.info.gz    R-ints.info.gz
automake.info-2.gz      flex.info.gz       libquadmath.info.gz R-lang.info.gz
automake.info.gz        gawkinet.info.gz   libtool.info-1.gz    rluserman.info.gz
autosprintf.info.gz     gawk.info.gz       libtool.info-2.gz    sed.info.gz
bash.info.gz            gawkworkflow.info.gz libxmi.info.gz      source-highlight.info.gz
bc.info.gz              gcc.info.gz       m4.info-1.gz        tar.info-1.gz
bfd.info.gz             gccinstall.info.gz m4.info-2.gz        tar.info-2.gz
binutils.info.gz        gccint.info.gz    make.info-1.gz      tar.info.gz
bison.info.gz           gettext.info.gz   m4.info.gz         tds.info.gz
coreutils.info.gz       gfortran.info.gz  nano.info.gz       texinfo.info-1.gz
cpio.info.gz            gnupg.info-1.gz   nettle.info.gz     texinfo.info-2.gz
cpp.info.gz             gnupg.info-2.gz   parted.info.gz    texinfo.info-3.gz
cppinternals.info.gz   gnupg.info-3.gz   pinentry.info.gz   tlbbuild.info.gz
dc.info.gz              gprof.info.gz    pinfo.info.gz      web2c.info.gz
diffutils.info.gz       grep.info.gz     plotutils.info.gz wget.info.gz
dir                   grub2-dev.info.gz  R-admin.info.gz    which.info.gz
dir.old                grub2.info.gz    R-data.info.gz
dvipng.info.gz          gzip.info.gz     R-exts.info-1.gz
```

Рис. 3.4: Поиск файла документации info

3.1.2 Тест по теме «Поиск справочной информации в Linux»

The screenshot shows a user interface for a test. On the left, there's a vertical sidebar with the text 'Системный администратор Linux с нуля'. The main area has a title 'Тест по теме «Поиск справочной информации в Linux»'. Below it, a box displays 'Результат тестирования' with the message 'Тест пройден' and '3 из 3'. In the top right corner, there's a user profile for 'Даниил Сергеев' with options to 'Редактировать профиль' and 'Личный кабинет'. At the bottom, there are navigation links: '← Задания по теме «Поиск справочной информации в Linux»' and 'Ответы на тест «Поиск справочной информации в Linux» →'.

Рис. 3.5: Подтверждение прохождения теста «Поиск справочной информации в Linux»

Какая команда поможет узнать, как работает утилита grep?

- a) grep --info
- б) man grep
- в) grep /?
- г) info man

Верный ответ: man grep

Рис. 3.6: «Поиск справочной информации в Linux». Вопрос №1

Выбранный ответ: **man grep**.

- grep --info - такой опции не существует у команды grep;
- grep /? - аналогично с первым вариантом ответа;
- info man - откроет справку о команде man, а не grep;

Что делает команда info?

- а) Показывает список всех установленных программ
- б) Открывает справку в формате info для заданной команды
- в) Проверяет системные обновления
- г) Запускает файловый менеджер

Верный ответ: Открывает справку в формате info для заданной команды

Рис. 3.7: «Поиск справочной информации в Linux». Вопрос №2

Выбранный ответ: Открывает справку в формате info для заданной команды.

info - справочная система, которая предоставляет детальную и структурированную информацию по утилитам. Она не показывает список установленных программ, не проверяет обновления и не запускает файловый менеджер.

Где чаще всего находятся текстовые справочные файлы (документация) к установленным программам в Linux?

- а) /etc/configs
- б) /var/log/info
- в) /usr/share/doc
- г) /bin/documents

Верный ответ: /usr/share/doc

Рис. 3.8: «Поиск справочной информации в Linux». Вопрос №3

Выбранный ответ: /usr/share/doc.

- /etc/configs - такой директории не существует, конфигурационные файлы обычно находятся в /etc;
- /var/log/info - в /var/log хранятся логи программ, а не документация;
- /bin/documents - в /bin находятся бинарные исполняемые файлы, документация там отсутствует;

3.1.3 Задания по теме «Работа с текстовыми файлами в Linux»

Задание №1

Откройте файл /etc/os-release с помощью less и найдите название дистрибутива.

Задание №2

Используйте grep, чтобы найти строки, содержащие «error» в файле /var/log/syslog.

Задание №3

Отредактируйте конфигурацию SSH с помощью nano или vim и измените параметр PermitRootLogin no.

Задание №4

Создайте небольшой файл с матрицей чисел произвольного размера, и поэкспериментируйте с числами при помощи утилиты awk – например, посчитайте сумму чисел в каждой четной строке.

Рис. 3.9: «Работа с текстовыми файлами в Linux». Условия заданий

3.1.3.1 Задание №1

Используем команду

```
less /etc/os-release
```

```
NAME="Rocky Linux"
VERSION="9.6 (Blue Onyx)"
ID="rocky"
ID_LIKE="rhel centos fedora"
VERSION_ID="9.6"
PLATFORM_ID="platform:el9"
PRETTY_NAME="Rocky Linux 9.6 (Blue Onyx)"
ANSI_COLOR="0;32"
LOGO="fedora-logo-icon"
CPE_NAME="cpe:/o:rocky:rocky:9::baseos"
HOME_URL="https://rockylinux.org/"
VENDOR_NAME="RESF"
VENDOR_URL="https://resf.org/"
BUG_REPORT_URL="https://bugs.rockylinux.org/"
SUPPORT_END="2032-05-31"
ROCKY_SUPPORT_PRODUCT="Rocky Linux-9"
ROCKY_SUPPORT_PRODUCT_VERSION="9.6"
REDHAT_SUPPORT_PRODUCT="Rocky Linux"
REDHAT_SUPPORT_PRODUCT_VERSION="9.6"
/etc/os-release (END)
```

Рис. 3.10: Вывод команды less

Название дистрибутива - Rocky Linux.

3.1.3.2 Задание №2

Так как файл логов syslog отсутствует на Rocky Linux, выведем сообщения из messages

```
# --color=auto выделение вхождений красным цветом  
sudo grep --color=auto "error" /var/log/messages
```

```
[dosergeev@dosergeev ~]$ sudo grep --color=auto "error" /var/log/messages  
[sudo] password for dosergeev:  
Nov  8 15:54:51 dosergeev alsactl[828]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to im  
port hw:0 use case configuration -2  
Nov  8 18:31:47 dosergeev alsactl[826]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to im  
port hw:0 use case configuration -2  
Nov  8 18:34:05 dosergeev gnome-shell[5700]: g_error_free: assertion 'error != NULL' failed  
Nov  8 18:34:30 dosergeev alsactl[826]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to im  
port hw:0 use case configuration -2  
Nov  8 18:39:17 dosergeev alsactl[829]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to im  
port hw:0 use case configuration -2  
Nov 10 20:56:51 dosergeev alsactl[832]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to im  
port hw:0 use case configuration -2  
Nov 11 00:03:12 dosergeev gnome-shell[2389]: libinput error: event5 - VirtualBox mouse integration: cli  
ent bug: event processing lagging behind by 16ms, your system is too slow  
Nov 11 17:31:15 dosergeev alsactl[825]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to im  
port hw:0 use case configuration -2  
[dosergeev@dosergeev ~]$ █
```

Рис. 3.11: Вывод команды grep для /var/log/messages

3.1.3.3 Задание №3

Откроем файл конфигурации sshd_config и изменим параметр

```
cd /etc/ssh  
sudo vi sshd_config
```



Рис. 3.12: Изменение параметра PermitRootLogin

3.1.3.4 Задание №4

Создадим файл a.txt в домашней директории и заполним его матрицей чисел.
Откроем его с использованием фильтра

```
cd ~  
vi a.txt  
# редактируем новый файл, затем :wq  
awk 'NR % 2 == 0 {for (i=1; i<=NF; i++) count += $i; print NR ":", count; count = 0}'
```

```
[dosergeev@dosergeev ~]$ cat a.txt  
1 2 3 4  
3 4 5 -3  
0 8 -2 3  
8 3 7 2  
4 3 -1 0  
-1 2 -10 5  
0 0 0 1  
[dosergeev@dosergeev ~]$ awk 'NR % 2 == 0 {for (i=1; i<=NF; i++) count += $i; print NR ":", count; count = 0 }' a.txt  
2: 9  
4: 20  
6: -4
```

Рис. 3.13: Вывод фильтра awk

3.1.4 Тест по теме «Работа с текстовыми файлами в Linux»

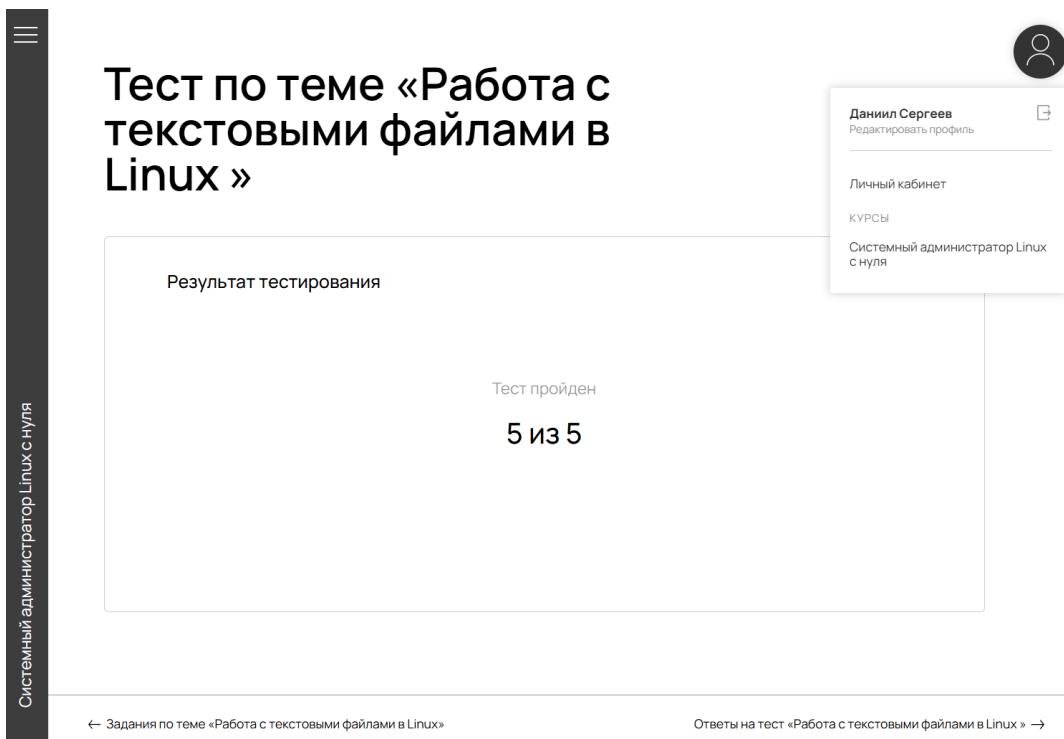


Рис. 3.14: Подтверждение прохождения теста «Работа с текстовыми файлами в Linux»

Что делает команда `cat > файл.txt?`

- а) Показывает содержимое файла
- б) Объединяет файлы
- в) Создает новый файл и записывает в него
- г) Добавляет строку в конец файла

Верный ответ: Создает новый файл и записывает в него

Рис. 3.15: «Работа с текстовыми файлами в Linux». Вопрос №1

Выбранный ответ: **Создает новый файл и записывает в него.**

Оператор `>>` дописывает в конец файла, а `>` перезаписывает файл. Использование команды `cat` без указания файла позволит записать ввод с клавиатуры, после чего выведет его повторно (закончить ввод можно сочетанием `Ctrl+D`).

Чем отличается `cat >> файл.txt` от `cat > файл.txt`?

- a) >> удаляет файл полностью, > – помещает в корзину
- б) >> дописывает в конец, > – перезаписывает
- в) >> копирует файл, , > – вырезает
- г) Нет отличий

Верный ответ: >> дописывает в конец, > – перезаписывает

Рис. 3.16: «Работа с текстовыми файлами в Linux». Вопрос №2

Выбранный ответ: » дописывает в конец, > – перезаписывает.

Принцип работы операторов описан в самом ответе и был указан в предыдущем ответе на вопрос.

Чем `less` отличается от `cat` при просмотре больших файлов?

- а) Нет принципиальных отличий
- б) less не поддерживает поиск по содержимому
- в) less показывает содержимое файла постранично с навигацией и поиском
- г) less работает только с бинарными файлами

Верный ответ: less показывает содержимое файла постранично с навигацией и поиском

Рис. 3.17: «Работа с текстовыми файлами в Linux». Вопрос №3

Выбранный ответ: less показывает содержимое файла постранично с навигацией и поиском.

Утилита less позволяет постранично просматривать файл, выполнять поиск по содержимому, а также предоставляет удобную навигацию. cat выводит всю информацию разом, что неудобно для больших объемов текста.

Какой клавишей можно выйти из утилиты less?

- a) Esc
- б) q
- в) Ctrl+X
- г) Ctrl+Q

Верный ответ: q

Рис. 3.18: «Работа с текстовыми файлами в Linux». Вопрос №4

Выбранный ответ: q.

Выход из утилиты less можно, нажав q

С помощью какой клавиши в Vim можно переключиться из Normal mode в Command mode?

- a) Tab
- б) :
- в) Esc
- г) Shift

Верный ответ: :

Рис. 3.19: «Работа с текстовыми файлами в Linux». Вопрос №5

Выбранный ответ: ::.

- Tab используется для автодополнения;
- Esc переходит из других режимов в нормальный режим;
- Shift используется для других целей;

3.1.5 Задания по теме «Анализ системных логов»

Задание №1

Найдите все ошибки в системном журнале за последний день.

Задание №2

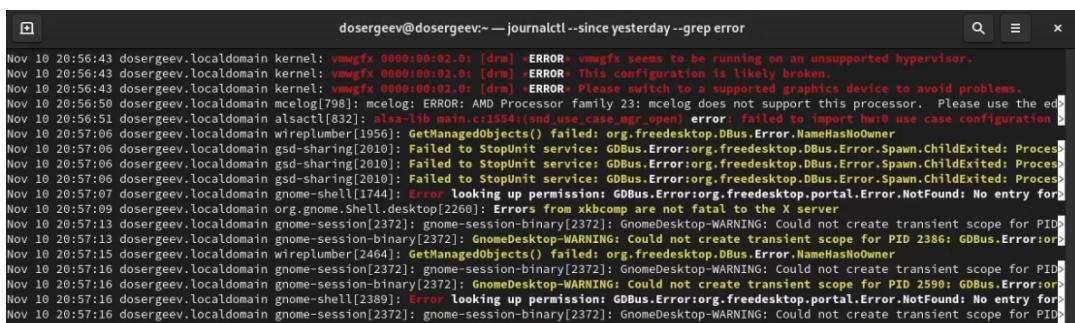
Проверьте логи SSH и найдите неудачные попытки входа.

Рис. 3.20: «Анализ системных логов». Условия заданий

3.1.5.1 Задание №1

Используем команду

```
journalctl --since "yesterday" --grep error
```



```
Nov 10 20:56:43 dosergeev.localdomain kernel: vmmfx 0000:00:02.0: [drm] -ERROR vmmfx seems to be running on an unsupported hypervisor.
Nov 10 20:56:43 dosergeev.localdomain kernel: vmmfx 0000:00:02.0: [drm] -ERROR This configuration is likely broken.
Nov 10 20:56:43 dosergeev.localdomain kernel: vmmfx 0000:00:02.0: [drm] -ERROR Please switch to a supported graphics device to avoid problems.
Nov 10 20:56:50 dosergeev.localdomain mclog[798]: mclog: ERROR: AMD Processor family 23: mclog does not support this processor. Please use the ed...
Nov 10 20:56:51 dosergeev.localdomain alsactl[832]: alsa-lib main.c:1554:(snd_use_case_mgr_open) error: failed to import hw0 use case configuration >
Nov 10 20:57:06 dosergeev.localdomain wireplumber[1956]: GetManagedObject() failed: org.freedesktop.DBus.Error.NameHasNoOwner
Nov 10 20:57:06 dosergeev.localdomain gsd-sharing[2010]: Failed to StopUnit service: GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process
Nov 10 20:57:06 dosergeev.localdomain gsd-sharing[2010]: Failed to StopUnit service: GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process
Nov 10 20:57:06 dosergeev.localdomain gsd-sharing[2010]: Failed to StopUnit service: GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process
Nov 10 20:57:06 dosergeev.localdomain gsd-sharing[2010]: Failed to StopUnit service: GDBus.Error:org.freedesktop.DBus.Error.Spawn.ChildExited: Process
Nov 10 20:57:06 dosergeev.localdomain gnome-shell[1744]: Error looking up permission: GDBus.Error:org.freedesktop.portal.Error.NotFound: No entry for
Nov 10 20:57:09 dosergeev.localdomain org.gnome.Shell.desktop[2260]: Errors from xkbcomp are not fatal to the X server
Nov 10 20:57:13 dosergeev.localdomain gnome-session[2372]: gnome-session-binary[2372]: GnomeDesktop-WARNING: Could not create transient scope for PID...
Nov 10 20:57:13 dosergeev.localdomain gnome-session-binary[2372]: GnomeDesktop-WARNING: Could not create transient scope for PID 2386: GDBus.Error:or...
Nov 10 20:57:15 dosergeev.localdomain wireplumber[2464]: GetManagedObject() failed: org.freedesktop.DBus.Error.NameHasNoOwner
Nov 10 20:57:16 dosergeev.localdomain gnome-session[2372]: gnome-session-binary[2372]: GnomeDesktop-WARNING: Could not create transient scope for PID...
Nov 10 20:57:16 dosergeev.localdomain gnome-session[2372]: gnome-session-binary[2372]: GnomeDesktop-WARNING: Could not create transient scope for PID...
Nov 10 20:57:16 dosergeev.localdomain gnome-shell[2389]: Error looking up permission: GDBus.Error:org.freedesktop.portal.Error.NotFound: No entry for
Nov 10 20:57:16 dosergeev.localdomain gnome-session[2372]: GnomeDesktop-WARNING: Could not create transient scope for PID...
```

Рис. 3.21: Просмотр ошибок в системном журнале за последний день

3.1.5.2 Задание №2

Для службы SSH

```
journalctl -u sshd --grep "Failed"
```

```
[dosergeev@dosergeev ~]$ journalctl -u sshd --grep "Failed"
-- Boot 54f590bce30b4d7db7490e2c59da5b4c --
-- Boot 5c2c69d963a74894b7a1701f350acc74 --
-- Boot feaa256b05f74ddeae6e6d99cd93ffec0 --
-- Boot eeba94996c834c3aad34279a93643b93 --
-- Boot fbbcc9567fe34ee1b5019ffa6a341337 --
-- Boot 18c4489463fe4c6d8d850ad852153823 --
-- Boot d0310b39a5cb47f299b2defcaccaa22 --
-- Boot b6ebe2bbbf640a885266f7b9479723e --
-- Boot 9e0a1fa6659944589602610dc16f457a --
-- Boot 05d297df1eb4715ab7a7e1eb1b2ac3c --
-- Boot 14816f2212b54a96822f6afda06802df --
Nov 10 23:30:30 dosergeev.localdomain sshd[6101]: Failed password for invalid user user from ::1 port 54690 ssh2
Nov 10 23:30:35 dosergeev.localdomain sshd[6101]: Failed password for invalid user user from ::1 port 54690 ssh2
Nov 10 23:30:43 dosergeev.localdomain sshd[6101]: Failed password for invalid user user from ::1 port 54690 ssh2
Nov 10 23:32:09 dosergeev.localdomain sshd[6192]: Failed password for invalid user user from ::1 port 44976 ssh2
Nov 10 23:39:56 dosergeev.localdomain sshd[6399]: Failed password for invalid user user from ::1 port 52234 ssh2
-- Boot 2bee596fef4a422a94be5fab907b98b6 --
[dosergeev@dosergeev ~]$
```

Рис. 3.22: Просмотр ошибок авторизации SSH

3.1.6 Тест по теме «Анализ системных логов»

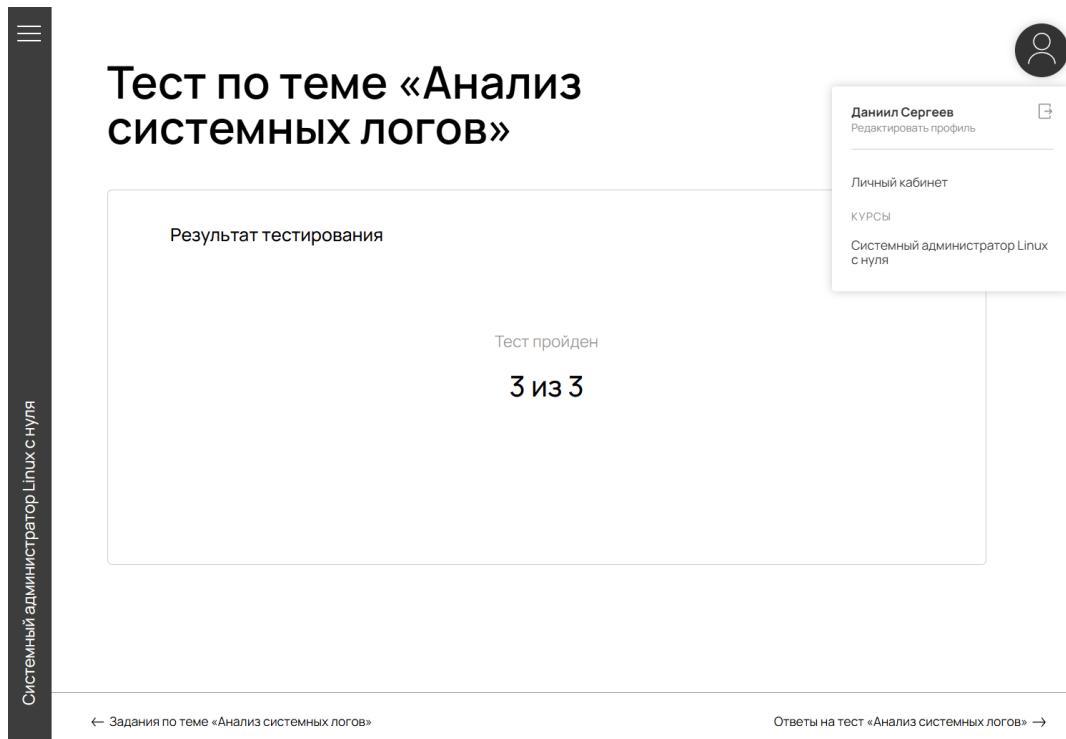


Рис. 3.23: Подтверждение прохождения теста «Анализ системных логов»

Где хранятся основные лог-файлы в Linux?

- a) /etc/logs/
- б) /var/log/
- в) /usr/logs/
- г) /tmp/logs/

Верный ответ: /var/log/

Рис. 3.24: «Анализ системных логов». Вопрос №1

Выбранный ответ: **/var/log/**.

- /etc/logs/ - в /etc хранятся файлы конфигурации;
- /usr/logs/ - в /usr хранятся пользовательские файлы;
- /tmp/logs/ - в /tmp хранятся временные файлы;

Что делает команда journalctl -u sshd --since today?

- а) Показывает ошибки входа за сегодня
- б) Показывает все логи sshd до сегодняшнего дня
- в) Показывает логи sshd за сегодня
- г) Показывает логи sshd за вчера

Верный ответ: Показывает логи sshd за сегодня

Рис. 3.25: «Анализ системных логов». Вопрос №2

Выбранный ответ: **Показывает логи sshd за сегодня.**

Опция `-u` позволяет указать конкретный юнит, а `--since` время, с которого стоит искать сообщения.

Какой параметр journalctl показывает последние 20 записей?

- а) -e
- б) -u
- в) --tail 20
- г) -n 20

Верный ответ: -n 20

Рис. 3.26: «Анализ системных логов». Вопрос №3

Выбранный ответ: **-n 20.**

- -e - переходит сразу к концу журнала;
- -u - фильтрует записи по конкретному юниту;
- --tail 20 - такой опции нет в journalctl;

3.1.7 Задания по теме «Автоматизация анализа логов и работы с текстом»

Задание №1

Напишите скрипт, который ежедневно сохраняет в файл все ошибки из /var/log/syslog.

Задание №2

Настройте cron, чтобы скрипт выполнялся раз в день.

Задание №3

Используйте awk, чтобы посчитать количество неудачных попыток входа за последние 24 часа.

Рис. 3.27: «Автоматизация анализа логов и работы с текстом». Условия заданий

3.1.7.1 Задание №1

Напишем скрипт в файле /usr/bin/daily_save.sh и сделаем его исполняемым

```
#!/bin/bash
```

```
grep -i "error" /var/log/messages > /var/log/daily_save.log
```

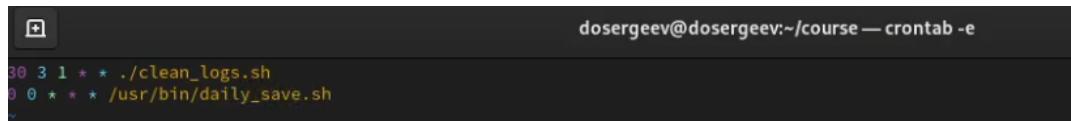
```
[dosergeev@dosergeev ~]$ cd course/
[dosergeev@dosergeev course]$ ls
archive_test.tar.gz bin extracted extracted.tar.gz file1.txt file2.txt file3.txt
[dosergeev@dosergeev course]$ rm -r *
[dosergeev@dosergeev course]$ ls
[dosergeev@dosergeev course]$ vi daily_save.sh
[dosergeev@dosergeev course]$ chmod +x daily_save.sh
[dosergeev@dosergeev course]$ ls
daily_save.sh
[dosergeev@dosergeev course]$ ./daily_save.sh
./daily_save.sh: line 2: /var/log/daily_save.log: Permission denied
[dosergeev@dosergeev course]$ sudo ./daily_save.sh
[sudo] password for dosergeev:
```

Рис. 3.28: Написание скрипта

3.1.7.2 Задание №2

Теперь проведем настройку crontab

```
crontab -e
# в редакторе crontab
0 0 * * * /usr/bin/daily_save.log
```



```
dosergeev@dosergeev:~/course — crontab -e
30 3 1 * * ./clean_logs.sh
0 0 * * * /usr/bin/daily_save.log
```

Рис. 3.29: Редактирование crontab

3.1.7.3 Задание №3

Используем несколько фильтров

```
journalctl -u sshd --since "yesterday" | grep "Failed password" | awk '{count += 1} END {print count}'
```

Сделаем несколько ошибок входа и проверим вывод команды

```
[dosergeev@dosergeev course]$ journalctl -u sshd --since "yesterday" | grep "Failed password" | awk '{count += 1} END {print count}'
5
[dosergeev@dosergeev course]$ systemctl start httpd
[dosergeev@dosergeev course]$ cd ..
[dosergeev@dosergeev ~]$ ls
a.txt course Desktop Documents Downloads Music opt Pictures Public R Templates texmf Videos work
[dosergeev@dosergeev ~]$ scp a.txt dosergeev@localhost:/
dosergeev@localhost's password:
dest open("/a.txt"): Permission denied
failed to upload file a.txt to /a.txt
[dosergeev@dosergeev ~]$ scp a.txt dosergeev@localhost:/
dosergeev@localhost's password:
dest open("/a.txt"): Permission denied
failed to upload file a.txt to /a.txt
[dosergeev@dosergeev ~]$ scp a.txt dosergeev@localhost:/
dosergeev@localhost's password:
Permission denied, please try again.
dosergeev@localhost's password:
Permission denied, please try again.
dosergeev@localhost's password:
dosergeev@localhost: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
Connection closed
[dosergeev@dosergeev ~]$ journalctl -u sshd --since "yesterday" | grep "Failed password" | awk '{count += 1} END {print count}'
8
```

Рис. 3.30: Проверка применения фильтра awk для ошибок входа

3.1.8 Тест по теме «Автоматизация анализа логов и работы с текстом»

Системный администратор Linux с нуля

Тест по теме
«Автоматизация анализа
логов и работы с
текстом»

Результат тестирования

Тест пройден

4 из 4

Даниил Сергеев
Редактировать профиль

Личный кабинет

КУРСЫ

Системный администратор Linux с нуля

← Задания по теме «Автоматизация анализа логов и работы с текстом»

Ответы на тест «Автоматизация анализа логов и работы с текстом» →

Рис. 3.31: Подтверждение прохождения теста «Автоматизация анализа логов и работы с текстом»

Какая команда позволяет в реальном времени отслеживать новые строки в лог-файле?

- a) cat /var/log/nginx.log
- б) less /var/log/nginx.log
- в) tail -f /var/log/nginx.log
- г) watch -n 5 /var/log/nginx.log

Верный ответ: tail -f /var/log/nginx.log

Рис. 3.32: «Автоматизация анализа логов и работы с текстом». Вопрос №1

Выбранный ответ: tail -f /var/log/nginx.log.

Опция -f позволяет отслеживать добавление новых строк в файл в реальном времени.

Где по умолчанию хранятся пользовательские задания cron?

- a) /var/spool/cron/
- б) /home/user/.cronjobs
- в) /etc/cron.d/
- г) /opt/cron/tasks

Верный ответ: /var/spool/cron/

Рис. 3.33: «Автоматизация анализа логов и работы с текстом». Вопрос №2

Выбранный ответ: /var/spool/cron/.

- /home/user/.cronjobs - такой стандартной директории не существует;
- /etc/cron.d/ - здесь хранятся системные cron-задания;
- /opt/cron/tasks - нестандартный путь для хранения cron-заданий;

Какой символ в crontab означает «любое значение»?

- а) *
- б) -
- в) /
- г) %

Верный ответ: *

Рис. 3.34: «Автоматизация анализа логов и работы с текстом». Вопрос №3

Выбранный ответ: *.

- - - используется для указания диапазонов значений;
- / - используется для указания шага значений;
- % - не является специальным символом в crontab;

Как удалить все задания cron для текущего пользователя?

- a) cron --clear
- б) rm -rf /var/spool/cron
- в) crond -reset
- г) crontab -r

Верный ответ: crontab -r

Рис. 3.35: «Автоматизация анализа логов и работы с текстом». Вопрос №4

Выбранный ответ: **crontab -r**.

- cron --clear - такой команды не существует;
- rm -rf /var/spool/cron - удалит задания всех пользователей;
- crond -reset - такой команды не существует.

3.2 Модуль 5. Управление пользователями и группами

3.2.1 Задания по теме «Основы управления пользователями и группами»

Задание №1

Создайте нового пользователя ivan и задайте ему пароль.

Задание №2

Создайте новую группу developers.

Задание №3

Добавьте пользователя ivan в группу developers.

Задание №4

Создайте группу testers и поменяйте принадлежность пользователя ivan группам с developers на testers.

Задание №5

Удалите учетную запись пользователя ivan вместе с его домашним каталогом.

Рис. 3.36: «Основы управления пользователями и группами». Условия заданий

3.2.1.1 Задание №1

Создадим пользователя и зададим пароль

```
sudo adduser ivan
# проверим, что пользователь создался
sudo cat /etc/passwd | grep ivan
sudo passwd ivan
```

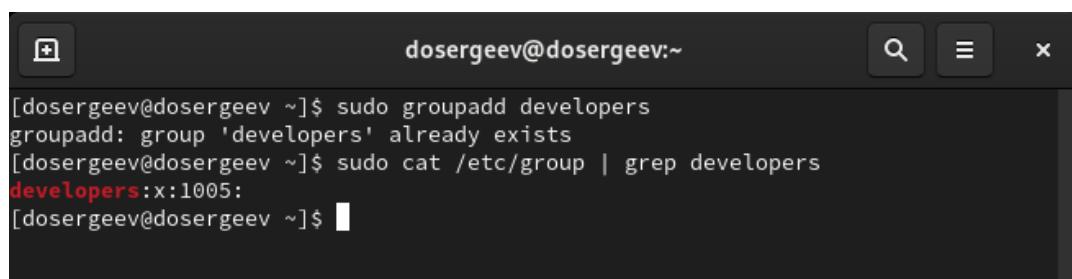
```
[dosergeev@dosergeev ~]$ sudo adduser ivan
[sudo] password for dosergeev:
[dosergeev@dosergeev ~]$ sudo cat /etc/passwd | grep ivan
ivan:x:1004:100::/home/ivan:/bin/bash
[dosergeev@dosergeev ~]$ man passwd
[dosergeev@dosergeev ~]$ sudo passwd ivan
Changing password for user ivan.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[dosergeev@dosergeev ~]$
```

Рис. 3.37: Создание пользователя ivan

3.2.1.2 Задание №2

Создадим группу developers

```
sudo groupadd developers
sudo cat /etc/group | grep developers
```



The screenshot shows a terminal window with the title 'dosergeev@dosergeev:~'. The command 'sudo groupadd developers' is run, followed by 'groupadd: group 'developers' already exists'. Then, 'sudo cat /etc/group | grep developers' is run, showing the entry 'developers:x:1005:'. The terminal has a dark background with light-colored text.

```
[dosergeev@dosergeev ~]$ sudo groupadd developers
groupadd: group 'developers' already exists
[dosergeev@dosergeev ~]$ sudo cat /etc/group | grep developers
developers:x:1005:
[dosergeev@dosergeev ~]$
```

Рис. 3.38: Создание группы developers

3.2.1.3 Задание №3

Добавим ivan в developers

```
sudo usermod -aG developers ivan
```

```
[dosergeev@dosergeev ~]$ sudo usermod -aG developers ivan
[dosergeev@dosergeev ~]$ groups ivan
ivan : users developers
```

Рис. 3.39: Добавление пользователя ivan в группу

3.2.1.4 Задание №4

Создадим группу testers и поменяем принадлежность ivan с developers на testers.

```
sudo usermod -G "" ivan  
sudo usermod -aG testers ivan
```

```
[dosergeev@dosergeev ~]$ sudo usermod -G "" ivan  
[sudo] password for dosergeev:  
[dosergeev@dosergeev ~]$ groups ivan  
ivan : users  
[dosergeev@dosergeev ~]$ sudo usermod -aG testers ivan  
[dosergeev@dosergeev ~]$ groups ivan  
ivan : users testers  
[dosergeev@dosergeev ~]$
```

Рис. 3.40: Изменение групп пользователя ivan

3.2.1.5 Задание №5

Завершаем все процессы пользователя ivan и удаляем его

```
sudo pkill -u ivan  
sudo userdel -r ivan
```

```
[dosergeev@dosergeev ~]$ sudo pkill -u ivan  
[sudo] password for dosergeev:  
[dosergeev@dosergeev ~]$ sudo userdel -r ivan  
[dosergeev@dosergeev ~]$ sudo cat /etc/passwd | ivan  
bash: ivan: command not found...  
[dosergeev@dosergeev ~]$ sudo cat /etc/passwd | grep ivan  
[dosergeev@dosergeev ~]$ █
```

Рис. 3.41: Удаление пользователя ivan

3.2.2 Тест по теме «Основы управления пользователями и группами»

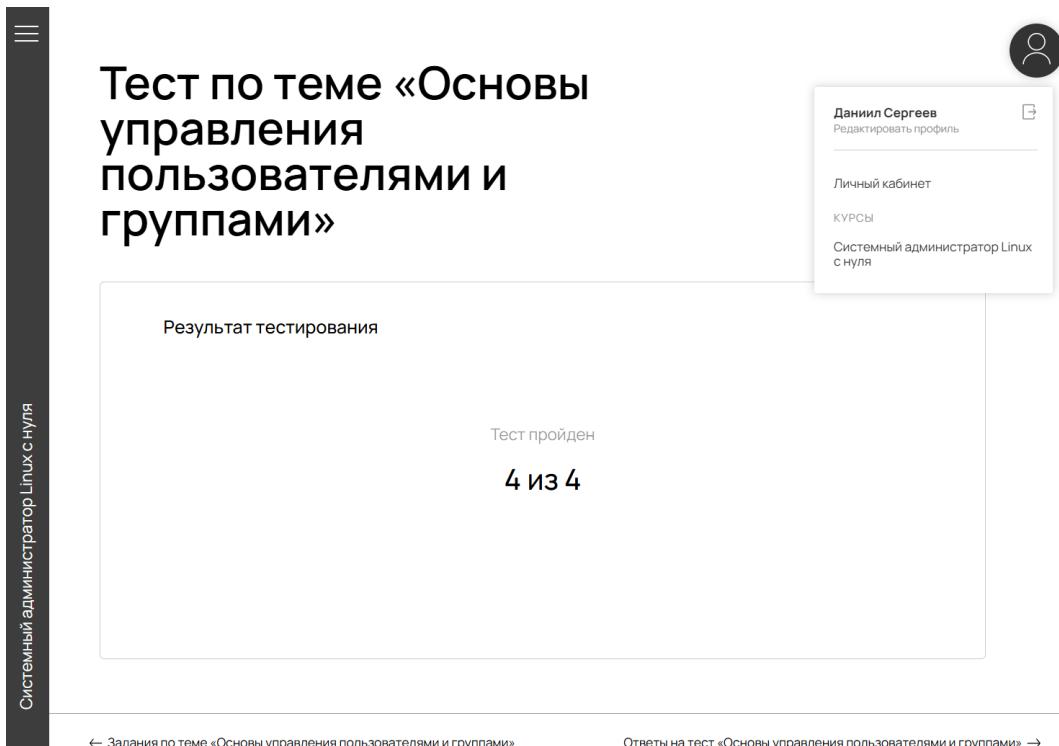


Рис. 3.42: Подтверждение прохождения теста «Основы управления пользователями и группами»

Какой флаг команды useradd используется для создания домашней директории пользователя?

- a)-s
- б)-G
- в)-m
- г) -d

Верный ответ: -m

Рис. 3.43: «Основы управления пользователями и группами». Вопрос №1

Выбранный ответ: **-m.**

- -s - указывает командную оболочку пользователя;

- -G - задает дополнительные группы пользователя;
- -d - указывает путь к домашней директории;

Какая команда удалит пользователя вместе с его домашней директорией?

- a) sudo userdel admin
- б) sudo deluser admin
- в) sudo userdel -r admin
- г) sudo deluser --remove-all-files admin

Верный ответ: sudo userdel -r admin

Рис. 3.44: «Основы управления пользователями и группами». Вопрос №2

Выбранный ответ: **sudo userdel -r admin.**

- sudo userdel admin - удаляет только пользователя, домашняя директория остается;
- sudo deluser admin - в некоторых дистрибутивах может не удалить домашнюю директорию;
- sudo deluser --remove-all-files admin - не является стандартным синтаксисом;

Что делает команда sudo usermod -aG sudo admin?

- а) Заменяет основную группу пользователя admin на sudo
- б) Добавляет пользователя admin в группу sudo, сохранив остальные группы
- в) Удаляет пользователя admin из группы sudo
- г) Создает новую группу sudo

Верный ответ: Добавляет пользователя admin в группу sudo, сохранив остальные группы

Рис. 3.45: «Основы управления пользователями и группами». Вопрос №3

Выбранный ответ: **Добавляет пользователя admin в группу sudo, сохранив остальные группы.**

Команда usermod используется для изменения данных учетной записи пользователя, в том числе для добавления его в уже существующую группу. Это можно сделать с помощью опций -a и -G, что означают добавить к существующим группам и указать конкретную группу соответственно.

Какая команда используется для безопасного редактирования файла /etc/passwd?

а) nano /etc/passwd

б) vipw

в) vim /etc/passwd

г) usermod

Верный ответ: **vipw**

Рис. 3.46: «Основы управления пользователями и группами». Вопрос №4

Выбранный ответ: **vipw**.

- nano /etc/passwd - прямое редактирование может быть небезопасным, поэтому ответ неверный;
- vim /etc/passwd - аналогично;
- usermod - команда для модификации пользователей, а не редактирования файла;

3.2.3 Задания по теме «Основы управления доступом и разрешениями»

Задание №1

Создайте где-нибудь новый файл. Изучите разрешения, которые он получил автоматически. Объясните, почему они имеют именно такие значения.

Задание №2

Для созданного файла уберите права на запись для группы и на чтение для всех остальных.

Задание №3

Верните первоначальные доступы файлу, используя числовую форму.

Задание №4

Сделайте владельцем файла пользователя root.

Задание №5

Верните себе владение файлом.

Рис. 3.47: «Основы управления доступом и разрешениями». Условия заданий

3.2.3.1 Задание №1

Создадим файл test.txt и проверим права пользователя

```
touch test.txt  
ls -l | grep test.txt
```

Он создался с правами -rw-r--r--. Изначально файлы создаются с правами -rw-rw-rw-, после чего из них вычитается маска (по умолчанию 022), которая убирает право на запись для группы и остальных - файл получает права 644, которые равны тем, что мы получили при создании файла.

```
[dosergeev@dosergeev ~]$ touch test.txt
[dosergeev@dosergeev ~]$ ls -l | grep test.txt
-rw-r--r--. 1 dosergeev dosergeev 0 Nov 11 20:38 test.txt
[dosergeev@dosergeev ~]$ umask
0022
```

Рис. 3.48: Проверка права файла и маски

3.2.3.2 Задание №2

Теперь для созданного файла уберем права на запись для группы и на чтение для всех остальных

```
chmod g-w,o-r test.txt
ls -l | grep test.txt
```

```
0022
[dosergeev@dosergeev ~]$ chmod g-w,o-r test.txt
[dosergeev@dosergeev ~]$ ls -l | grep test.txt
-rw-r-----. 1 dosergeev dosergeev 0 Nov 11 20:38 test.txt
```

Рис. 3.49: Изменение прав доступа к файлу

3.2.3.3 Задание №3

Вернем первоначальные доступы к файлу, через числовую форму ($644 = 666 - 022$)

```
chmod 644 test.txt
ls -l | grep test.txt
```

```
[dosergeev@dosergeev ~]$ chmod 644 test.txt
[dosergeev@dosergeev ~]$ ls -l | grep test
-rw-r--r--. 1 dosergeev dosergeev 0 Nov 11 20:38 test.txt
```

Рис. 3.50: Возврат к изначальным правам доступа

3.2.3.4 Задание №4

Сделаем root владельцем файла

```
chown root test.txt  
ls -l | grep test.txt
```

```
[dosergeev@dosergeev ~]$ sudo chown root test.txt  
[sudo] password for dosergeev:  
[dosergeev@dosergeev ~]$ ls  
a.txt Desktop Downloads opt Public Templates texmf work  
course Documents Music Pictures R test.txt Videos  
[dosergeev@dosergeev ~]$ ls -l | grep test  
-rw-r--r--, 1 root dosergeev 0 Nov 11 20:38 test.txt
```

Рис. 3.51: Смена владельца файла на root

3.2.3.5 Задание №5

Вернем своему пользователю владение файлом

```
chown dosergeev test.txt  
ls -l | grep test.txt
```

```
[dosergeev@dosergeev ~]$ sudo chown dosergeev test.txt  
[dosergeev@dosergeev ~]$ ls -l | grep test  
-rw-r--r--, 1 dosergeev dosergeev 0 Nov 11 20:38 test.txt  
[dosergeev@dosergeev ~]$ █
```

Рис. 3.52: Смена владельца файла на dosergeev

3.2.4 Тест по теме «Основы управления доступом и разрешениями»

The screenshot shows a user interface for a test. On the left, there's a vertical sidebar with three horizontal lines at the top and the text 'Системный администратор Linux с нуля' at the bottom. The main content area has a dark header bar with the title 'Тест по теме «Основы управления доступом и разрешениями»'. Below the title is a light gray box containing the text 'Результат тестирования'. Inside this box, it says 'Тест пройден' and '3 из 3'. To the right of the main content is a white sidebar with a user profile icon at the top. The profile information includes 'Даниил Сергеев', a link to 'Редактировать профиль', 'Личный кабинет', 'КУРСЫ', and 'Системный администратор Linux с нуля'. At the bottom of the sidebar are navigation links: '← Задания по теме «Основы управления доступом и разрешениями»' and 'Ответы на тест «Основы управления доступом и разрешениями» →'.

Рис. 3.53: Подтверждение прохождения теста «Основы управления доступом и разрешениями»

Что означает первый символ d в строке прав доступа при выполнении команды ls -l?

- а) Обычный файл
- б) Символическая ссылка
- в) Директория (каталог)
- г) Специальный системный файл

Верный ответ: Директория (каталог)

Рис. 3.54: «Основы управления доступом и разрешениями». Вопрос №1

Выбранный ответ: **Директория (каталог).**

- Символ d не является отображением специальных системных файлов;
- Обычный файл отображается как -;
- Символическая ссылка отображается как l;

Какая команда сменит владельца и группу файла /home/ivan/file.txt на ivan и friends соответственно?

- a) chown ivan /home/ivan/file.txt
- б) chgrp friends /home/ivan/file.txt
- в) chown ivan:friends /home/ivan/file.txt
- г) chmod ivan:friends /home/ivan/file.txt

Верный ответ: chown ivan:friends /home/ivan/file.txt

Рис. 3.55: «Основы управления доступом и разрешениями». Вопрос №2

Выбранный ответ: **chown ivan:friends /home/ivan/file.txt.**

- chown ivan /home/ivan/file.txt - меняет только владельца, но не группу;
- chgrp friends /home/ivan/file.txt - меняет только группу, но не владельца;
- chmod ivan:friends /home/ivan/file.txt - команда chmod используется только для изменения прав доступа;

Какие права доступа соответствуют числовому значению 754?

- а) rwxr--r-
- б) rwxr-xr-
- в) rwxr-xr-x
- г) rwxrw-r--

Верный ответ: rwxr-xr-

Рис. 3.56: «Основы управления доступом и разрешениями». Вопрос №3

Выбранный ответ: **rwxr-xr-.**

- rwxr--r--- соответствует 744;
- rwxr-xr-x - соответствует 755;
- rwxrw-r--- соответствует 764;

3.2.5 Задания по теме «Повышение безопасности работы с учетными записями»

Задание №1

Выполните несколько действий, используя sudo, и найдите их в системном журнале.

Задание №2

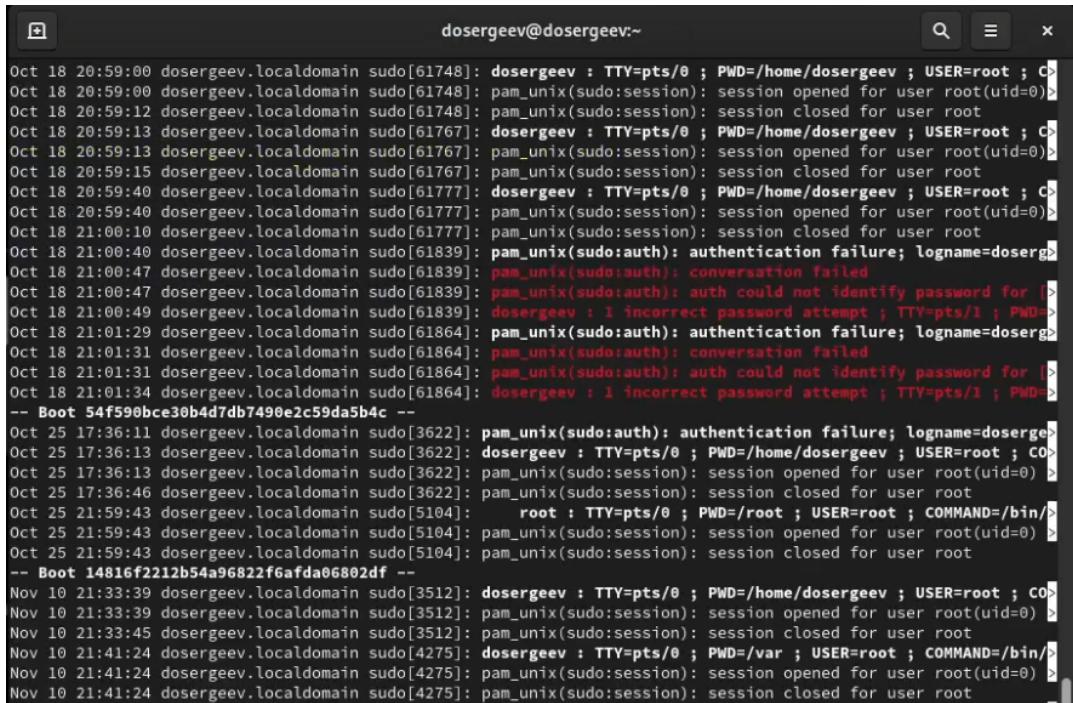
Воспользуемся учетной записью ivan из предыдущих уроков. Если такого пользователя нет, создайте его. Проверьте, может ли он выполнять команды суперпользователя. Если нет, предоставьте ему такую возможность.

Рис. 3.57: «Повышение безопасности работы с учетными записями». Условия заданий

3.2.5.1 Задание №1

Используем специальный фильтр, встроенный в команду journalctl

```
sudo journalctl _COMM=sudo
```



```
dosergeev@dosergeev:~ Oct 18 20:59:00 dosergeev.localdomain sudo[61748]: dosergeev : TTY=pts/0 ; PWD=/home/dosergeev ; USER=root ; C Oct 18 20:59:00 dosergeev.localdomain sudo[61748]: pam_unix(sudo:session): session opened for user root(uid=0) > Oct 18 20:59:12 dosergeev.localdomain sudo[61748]: pam_unix(sudo:session): session closed for user root Oct 18 20:59:13 dosergeev.localdomain sudo[61767]: dosergeev : TTY=pts/0 ; PWD=/home/dosergeev ; USER=root ; C Oct 18 20:59:13 dosergeev.localdomain sudo[61767]: pam_unix(sudo:session): session opened for user root(uid=0) > Oct 18 20:59:15 dosergeev.localdomain sudo[61767]: pam_unix(sudo:session): session closed for user root Oct 18 20:59:40 dosergeev.localdomain sudo[61777]: dosergeev : TTY=pts/0 ; PWD=/home/dosergeev ; USER=root ; C Oct 18 20:59:40 dosergeev.localdomain sudo[61777]: pam_unix(sudo:session): session opened for user root(uid=0) > Oct 18 21:00:10 dosergeev.localdomain sudo[61777]: pam_unix(sudo:session): session closed for user root Oct 18 21:00:40 dosergeev.localdomain sudo[61839]: pam_unix(sudo:auth): authentication failure; logname=doserg > Oct 18 21:00:47 dosergeev.localdomain sudo[61839]: pam_unix(sudo:auth): conversation failed Oct 18 21:00:47 dosergeev.localdomain sudo[61839]: pam_unix(sudo:auth): auth could not identify password for [> Oct 18 21:00:49 dosergeev.localdomain sudo[61839]: dosergeev : 1 incorrect password attempt ; TTY=pts/1 ; PWD=> Oct 18 21:01:29 dosergeev.localdomain sudo[61864]: pam_unix(sudo:auth): authentication failure; logname=doserg > Oct 18 21:01:31 dosergeev.localdomain sudo[61864]: pam_unix(sudo:auth): conversation failed Oct 18 21:01:31 dosergeev.localdomain sudo[61864]: pam_unix(sudo:auth): auth could not identify password for [> Oct 18 21:01:34 dosergeev.localdomain sudo[61864]: dosergeev : 1 incorrect password attempt ; TTY=pts/1 ; PWD=> -- Boot 54f59bce30b4d7db7490e2c59da5b4c -- Oct 25 17:36:11 dosergeev.localdomain sudo[3622]: pam_unix(sudo:auth): authentication failure; logname=doserg > Oct 25 17:36:13 dosergeev.localdomain sudo[3622]: dosergeev : TTY=pts/0 ; PWD=/home/dosergeev ; USER=root ; CO > Oct 25 17:36:13 dosergeev.localdomain sudo[3622]: pam_unix(sudo:session): session opened for user root(uid=0) > Oct 25 17:36:46 dosergeev.localdomain sudo[3622]: pam_unix(sudo:session): session closed for user root Oct 25 21:59:43 dosergeev.localdomain sudo[5104]: root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/bin/ > Oct 25 21:59:43 dosergeev.localdomain sudo[5104]: pam_unix(sudo:session): session opened for user root(uid=0) > Oct 25 21:59:43 dosergeev.localdomain sudo[5104]: pam_unix(sudo:session): session closed for user root -- Boot 14816f2212b54a96822f6afda06802df -- Nov 10 21:33:39 dosergeev.localdomain sudo[3512]: dosergeev : TTY=pts/0 ; PWD=/home/dosergeev ; USER=root ; CO > Nov 10 21:33:39 dosergeev.localdomain sudo[3512]: pam_unix(sudo:session): session opened for user root(uid=0) > Nov 10 21:33:45 dosergeev.localdomain sudo[3512]: pam_unix(sudo:session): session closed for user root Nov 10 21:41:24 dosergeev.localdomain sudo[4275]: dosergeev : TTY=pts/0 ; PWD=/var ; USER=root ; COMMAND=/bin/ > Nov 10 21:41:24 dosergeev.localdomain sudo[4275]: pam_unix(sudo:session): session opened for user root(uid=0) > Nov 10 21:41:24 dosergeev.localdomain sudo[4275]: pam_unix(sudo:session): session closed for user root
```

Рис. 3.58: Вывод всех команд с sudo

3.2.5.2 Задание №2

Создадим пользователя ivan, как в прошлых заданиях, и попробуем выполнить команду ls с помощью sudo

```
# перейдем на пользователя ivan
su ivan
sudo ls
```

```
[dosergeev@dosergeev ~]$ su ivan
Password:
[ivan@dosergeev dosergeev]$ sudo
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt]
          [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-D directory] [-g group] [-h host] [-p prompt]
...
[ivan@dosergeev dosergeev]$ sudo ls
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for ivan:
ivan is not in the sudoers file. This incident will be reported.
[ivan@dosergeev dosergeev]$ █
```

Рис. 3.59: Ошибка при использовании sudo

Выводит ошибку, так как пользователь ivan не имеет доступа к команде sudo. Добавим его в группу wheel, которая позволяет пользователям использовать sudo.

```
sudo usermod -aG wheel ivan
su ivan
sudo ls
```

```
[dosergeev@dosergeev ~]$ sudo usermod -aG wheel ivan
[dosergeev@dosergeev ~]$ su ivan
Password:
[ivan@dosergeev dosergeev]$ sudo ls
[sudo] password for ivan:
Sorry, try again.
[sudo] password for ivan:
a.txt course Desktop Documents Downloads Music opt Pictures Public R
[ivan@dosergeev dosergeev]$ su dosergeev
Password:
[dosergeev@dosergeev ~]$
```

Рис. 3.60: Добавление ivan в группу wheel

3.2.6 Тест по теме «Повышение безопасности работы с учетными записями»

The screenshot shows a test results page. At the top, the title is 'Тест по теме «Повышение безопасности работы с учетными записями»'. Below the title, there's a large box containing the text 'Результат тестирования'. Inside this box, it says 'Тест пройден' and '4 из 4'. To the right of the main content is a sidebar with a user profile for 'Даниил Сергеев'. The sidebar includes links for 'Редактировать профиль', 'Личный кабинет', 'КУРСЫ', and 'Системный администратор Linux с нуля'. At the bottom of the page, there are navigation links: '← Задания по теме «Повышение безопасности работы с учетными записями»' and 'Ответы на тест «Повышение безопасности работы с учетными записями» →'.

Рис. 3.61: Подтверждение прохождения теста «Повышение безопасности работы с учетными записями»

Что произойдет, если вы используете команду sudo для выполнения действий?

- a) Команда выполнится с правами суперпользователя, и действия не будут записаны в журнал
- б) Будет зафиксировано, кто и когда выполнил команду с правами суперпользователя
- в) Все действия, выполненные с помощью sudo, не записываются
- г) Все команды под sudo выполняются с ограниченными правами, независимо от пользователя

Верный ответ: Будет зафиксировано, кто и когда выполнил команду с правами суперпользователя

Рис. 3.62: «Повышение безопасности работы с учетными записями». Вопрос №1

Выбранный ответ: Будет зафиксировано, кто и когда выполнил команду с правами суперпользователя.

Команда sudo записывает все действия в системный журнал, отмечая, кто именно, когда и какую команду выполнял с правами суперпользователя. Такой подход обеспечивает прозрачность операций и облегчает расследование в случае инцидента.

Что произойдет, если вы измените порт SSH с 22 на 47022, но не обновите файрвол?

- a) SSH будет работать на новом порту, но файрвол не разрешит подключения
- б) Подключение возможно только по стандартному порту 22
- в) Все подключения будут заблокированы

Верный ответ: SSH будет работать на новом порту, но файрвол не разрешит подключения

Рис. 3.63: «Повышение безопасности работы с учетными записями». Вопрос №2

Выбранный ответ: SSH будет работать на новом порту, но файрвол не разрешил подключения.

Если SSH настроен слушать нестандартный порт (47022 из вопроса), то SSH-сервер будет работать, но поскольку файрвол блокирует входящие соединения, подключиться не получится. Файрвол по умолчанию может разрешать подключения только к стандартному порту 22.

Какую команду следует выполнить для того, чтобы добавить в файрвол ufw разрешение на подключение к нестандартному порту 47022 по протоколу TCP?

- a) sudo ufw allow 22/tcp
- б) sudo ufw allow 47022
- в) sudo ufw allow 47022/tcp

Верный ответ: sudo ufw allow 47022/tcp

Рис. 3.64: «Повышение безопасности работы с учетными записями». Вопрос №3

Выбранный ответ: **sudo ufw allow 47022/tcp.**

- sudo ufw allow 22/tcp - команда разрешит порт 22, а не 47022;
- sudo ufw allow 47022 - команда разрешит оба протокола (TCP и UDP);

Почему рекомендуется использовать sudo, а не su?

- а) sudo позволяет работать с командой от имени root без предоставления пароля
- б) sudo не требует ввода пароля root, а выполняемые команды журналируются, обеспечивая прозрачность действий
- в) su позволяет больше команд, чем sudo
- г) su более безопасен, чем sudo

Верный ответ: sudo не требует ввода пароля root, а выполняемые команды журналируются, обеспечивая прозрачность действий

Рис. 3.65: «Повышение безопасности работы с учетными записями». Вопрос №4

Выбранный ответ: **sudo не требует ввода пароля root, а выполняемые команды журналируются, обеспечивая прозрачность действий.**

Команда su требует ввода пароля суперпользователя. Команда sudo, напротив, требует пароль текущего пользователя, проверяя его членство в группе или права, определенные в конфигурации /etc/sudoers. Такое ограничение позволяет сохранить root-пароль в секрете и сократить количество лиц, которые его знают. Также sudo, в отличие от su, осуществляет журналирование действий.

3.2.7 Задания по теме «Политика паролей и учетных записей»

Задание №1

Выведите имена всех пользователей, у которых в качестве алгоритма хеширования пароля указан устаревший SHA-512 (его префикс \$6\$).

Задание №2

Создайте пользователя ivan (см. урок 5.2). Установите для него следующие параметры политики паролей с помощью команды chage (воспользуйтесь man chage при необходимости):

- максимальный срок действия пароля: 60 дней;
- минимальный срок между сменами пароля: 5 дней;
- время начала предупреждений: за 10 дней до истечения срока действия пароля.

Проверьте, что изменения вступили в силу.

Задание №3

Заблокируйте вход пользователю ivan. Убедитесь, что он не может войти в систему.

Задание №4

Верните пользователю ivan возможность авторизоваться.

Рис. 3.66: «Политика паролей и учетных записей». Условия заданий

3.2.7.1 Задание №1

Алгоритм хэширования указан сразу же после имени пользователя в файле /etc/shadow, отфильтруем по виду алгоритма. Используем экранирование чтобы ввести символ доллара

```
sudo cat /etc/shadow | grep --color=auto '\$6\$'
```

```
[dosergeev@dosergeev ~]$ sudo cat /etc/shadow | grep --color=auto '\$6\$'
root:$6$yHli7pCgWQS6u/8W$1gTYJcHZlxT5oflF9Na5Uc.m73m8rqiwoizVBMpPsIkkHu7Vxt71LZdumjn9CPwUdv
dosergeev:$6$X2/eQt3svrb2B1pv$g8DqBNibDEqOs.Fu60VDqfEVuG9qF6qsnbvuK6clKewSqJlQD705nwyM14x1
alice:$6$rounds=100000$f11swwXvsdx1iNL.S$LXZxdBn.TNYU49joe9LRh97eSgvEEKVkQl3CBcQ1pt7Lz3MRQ98
::
bob:$6$rounds=100000$PYgGlPV5/q/oHnoY$wyJfgjE0iHWla7gibSySxdn4aK9MAuVncyrHvZcxhAfvetgFwdF3
carol:$6$rounds=100000$ljY0tKFkJP4v4eL/$wTua/FX5yIwl/0IBhrnSUv/R.2SpXZM3In92Y7sSjTpK0Q5KX/3
ivan:$6$rounds=100000$0nJmNsWiHUXMoZIs$R086QhWQM/nZ1vFVN..GBg8FkHfeNFhPhXiYPkIykkg3Lv1w/UYV
:
```

Рис. 3.67: Фильтр пользователей по алгоритму хеширования SHA-512

3.2.7.2 Задание №2

Узнать время срока действия пароля можно командой

```
chage -l <пользователь>
```

Узнаем время пароля для пользователя ivan и поменяем на то, что указано в условии

```
sudo chage -l ivan
# -M максимальный срок действия пароля
# -m минимальный срок между сменами пароля
# -W время начала предупреждений
sudo chage -M 60 -m 5 -W 10 ivan
```

```
[dosergeev@dosergeev ~]$ sudo chage -l ivan
Last password change : Nov 11, 2025
Password expires      : never
Password inactive     : never
Account expires        : never
Minimum number of days between password change : 0
Maximum number of days between password change : 99999
Number of days of warning before password expires : 7
[dosergeev@dosergeev ~]$ sudo chage -M 60 -m 5 -W 10 ivan
[dosergeev@dosergeev ~]$ sudo chage -l ivan
Last password change : Nov 11, 2025
Password expires      : Jan 10, 2026
Password inactive     : never
Account expires        : never
Minimum number of days between password change : 5
Maximum number of days between password change : 60
Number of days of warning before password expires : 10
[dosergeev@dosergeev ~]$
```

Рис. 3.68: Смена времени действия пароля для ivan

3.2.7.3 Задание №3

Заблокируем вход командой usermod и попробуем зайти в него через su

```
# -L блокировка пользователя
sudo usermod -L ivan
su ivan
```

```
[dosergeev@dosergeev ~]$ sudo usermod -L ivan
[dosergeev@dosergeev ~]$ su ivan
Password:
su: Authentication failure
[dosergeev@dosergeev ~]$
```

Рис. 3.69: Блокировка пользователя ivan

3.2.7.4 Задание №4

Теперь разблокируем ivan и попробуем зайти в него снова

```
# -U разблокировка пользователя
sudo usermod -U ivan
su ivan
```

```
[dosergeev@dosergeev ~]$ sudo usermod -U ivan
[dosergeev@dosergeev ~]$ su ivan
Password:
^C
[dosergeev@dosergeev ~]$ su ivan
Password:
[ivan@dosergeev dosergeev]$
```

Рис. 3.70: Разблокировка пользователя ivan

3.2.8 Тест по теме «Политика паролей и учетных записей»

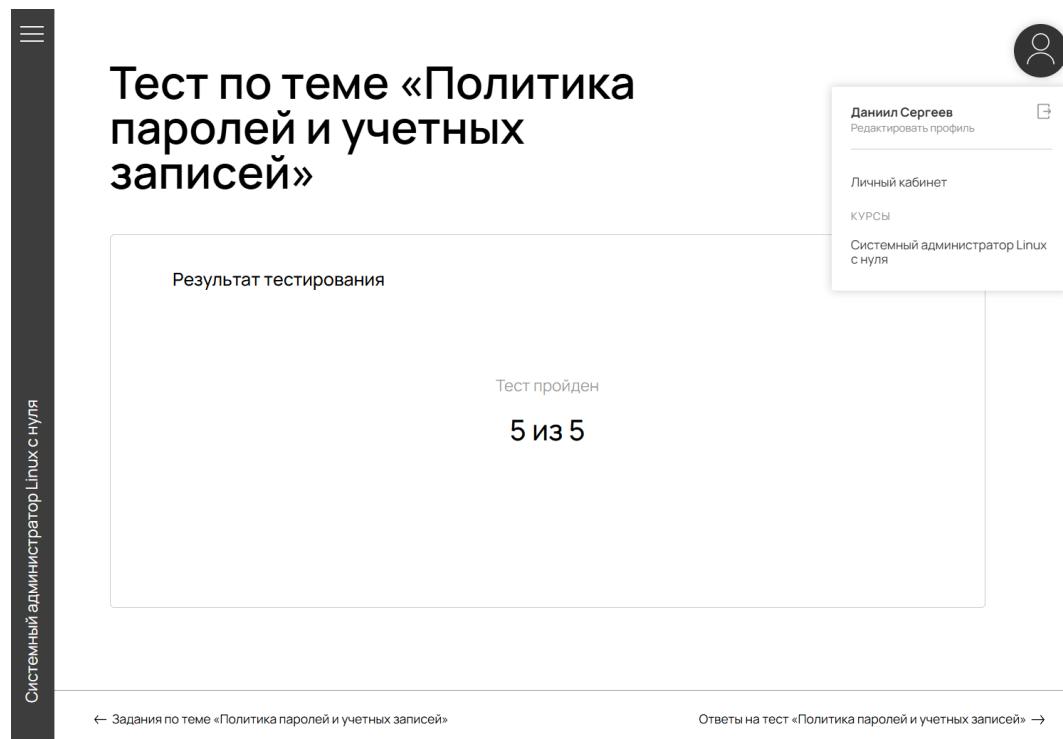


Рис. 3.71: Подтверждение прохождения теста «Политика паролей и учетных записей»

Какой из следующих вариантов наиболее точно описывает хеширование пароля?

- а) Пароль шифруется с возможностью обратного расшифрования
- б) Пароль сохраняется в виде обычного текста
- в) Пароль преобразуется в уникальный отпечаток, который нельзя восстановить обратно
- г) Пароль кодируется с помощью Base64

Верный ответ: Пароль преобразуется в уникальный отпечаток, который нельзя восстановить обратно

Рис. 3.72: «Политика паролей и учетных записей». Вопрос №1

Выбранный ответ: **Пароль преобразуется в уникальный отпечаток, который нельзя восстановить обратно.**

Хеширование - это одностороннее необратимое преобразование. Оно создает уникальный “отпечаток” входных данных, при этом обратное действие - восста-

новление исходного текста - невозможно, даже если известен алгоритм и его параметры.

Что обозначает первая часть строки пароля в /etc/shadow, которая начинается с символа \$ (например, \$y)?

- a) Уровень безопасности пользователя
- б) Алгоритм шифрования
- в) Используемый алгоритм хеширования
- г) Имя пользователя

Верный ответ: Используемый алгоритм хеширования

Рис. 3.73: «Политика паролей и учетных записей». Вопрос №2

Выбранный ответ: Используемый алгоритм хеширования.

\$y - это префикс, обозначающий используемый алгоритм хеширования (а не шифрования). В данном случае \$y указывает на Yescrypt. Имя пользователя находится в начале строки и не имеет префикса.

Какова функция «соли» (salt) при хешировании пароля?

- а) Обеспечить возможность расшифровать хеш
- б) Сделать пароль легче для пользователя
- в) Сделать каждый хеш уникальным и предотвратить атаки с использованием rainbow-таблиц
- г) Изменить пароль на другой

Верный ответ: Сделать каждый хеш уникальным и предотвратить атаки с использованием rainbow-таблиц

Рис. 3.74: «Политика паролей и учетных записей». Вопрос №3

Выбранный ответ: Сделать каждый хеш уникальным и предотвратить атаки с использованием rainbow-таблиц.

“Соль” - уникальное случайное слово, которое добавляется во время хеширования, чтобы сделать итоговый хэш невозможным для восстановления

Какая команда позволяет просмотреть текущие параметры политики пароля для пользователя ivan?

- а) passwd -s ivan
- б) cat /etc/shadow | grep ivan
- в) chage -l ivan
- г) usermod -p ivan

Верный ответ: chage -l ivan

Рис. 3.75: «Политика паролей и учетных записей». Вопрос №4

Выбранный ответ: chage -l ivan.

- passwd -s ivan - команда показывает статус пароля, а не подробные параметры политики;
- cat /etc/shadow | grep ivan - покажет захешированный пароль и некоторые параметры;
- usermod -p ivan - используется для установки пароля;

Что произойдет после выполнения команды sudo usermod -L username?

- а) Удалится пользователь из системы
- б) У пользователя сменится оболочка
- в) Учетная запись будет заблокирована, и вход станет невозможным
- г) Пользователю будет назначен временный пароль

Верный ответ: Учетная запись будет заблокирована, и вход станет невозможным

Рис. 3.76: «Политика паролей и учетных записей». Вопрос №5

Выбранный ответ: Учетная запись будет заблокирована, и вход станет невозможным.

Данная команда (с флагом -L) добавляет ! в начало хеша пароля в /etc/shadow, делая вход невозможным даже тогда, когда пароль известен.

3.3 Модуль 6. Управление доступом

3.3.1 Задания по теме «Что такое права доступа в Linux»

Задание №1

Проверьте права доступа к /etc/passwd, /home и /var/log.

Задание №2

Создайте файл в домашнем каталоге, проверьте его права и настройте umask, чтобы у новых файлов не было прав для категории остальных пользователей.

Рис. 3.77: «Что такое права доступа в Linux». Условия заданий

3.3.1.1 Задание №1

Проверим права доступа через ls

```
ls -l /etc | grep passwd
```

```
ls -l / | grep home
```

```
ls -l /var | grep log
```

- /etc/passwd - -rw-r--r--
- /home - drwxr-xr-x
- /var/log - drwxr-xr-x

```
[dosergeev@dosergeev ~]$ ls -l /etc | grep passwd & ls -l / | grep home & ls -l /var | grep log
[1] 8615
[2] 8617
drwxr-xr-x. 7 root root 72 Nov 11 20:56 home
drwxr-xr-x. 15 root root 4096 Nov 11 19:53 log
[2]+ Done                  ls --color=auto -l / | grep --color=auto home
[dosergeev@dosergeev ~]$ -rw-r--r--. 1 root root 2321 Nov 11 21:25 passwd
-rw-r--r--. 1 root root 2321 Nov 11 21:24 passwd-
[1]+ Done                  ls --color=auto -l /etc | grep --color=auto passwd
```

Рис. 3.78: Проверка прав доступа для файлов и каталогов корневого раздела

3.3.1.2 Задание №2

Перейдем в домашний каталог и создадим файл b.txt. Поменяем маску так, чтобы новые файлы не имели прав для категории остальных пользователей. Так как изначально маска имеет вид 666 (для файлов), ты мы должны поменять umask на 026 (666 - 026 = 640, у остальных нет прав)

```
cd  
ls -l | grep b.txt  
umask 0026  
touch c.txt  
ls -l | grep c.txt
```

```
[dosergeev@dosergeev ~]$ cd  
[dosergeev@dosergeev ~]$ ls  
a.txt course Desktop Documents Downloads Music opt Pictures Public R Templates test.txt  
[dosergeev@dosergeev ~]$ touch b.txt  
[dosergeev@dosergeev ~]$ ls -l | grep b  
-rw-r--r--. 1 dosergeev dosergeev 0 Nov 11 21:30 b.txt  
drwxr-xr-x. 2 dosergeev dosergeev 6 Sep 6 17:53 Public  
[dosergeev@dosergeev ~]$ ls -l | grep b.txt  
-rw-r--r--. 1 dosergeev dosergeev 0 Nov 11 21:30 b.txt  
[dosergeev@dosergeev ~]$ umask  
0022  
[dosergeev@dosergeev ~]$ umask 0026  
[dosergeev@dosergeev ~]$ umask  
0026  
[dosergeev@dosergeev ~]$ touch c.txt  
[dosergeev@dosergeev ~]$ ls -l | grep c.txt  
-rw-r-----. 1 dosergeev dosergeev 0 Nov 11 21:31 c.txt  
[dosergeev@dosergeev ~]$ █
```

Рис. 3.79: Редактирование маски для новых файлов

3.3.2 Тест по теме «Что такое права доступа в Linux»

The screenshot shows a user interface for a test. On the left, there's a vertical sidebar with the text 'Системный администратор Linux с нуля'. The main area has a title 'Тест по теме «Что такое права доступа в Linux»' and a sub-section 'Результат тестирования'. Below that, it says 'Тест пройден' and '3 из 3'. At the bottom, there are navigation links: '← Задания по теме «Что такое права доступа в Linux»' and 'Ответы на тест «Что такое права доступа в Linux» →'. A profile sidebar on the right shows the user 'Даниил Сергеев', a 'Личный кабинет' section, and a 'КУРСЫ' section with the course 'Системный администратор Linux с нуля'.

Рис. 3.80: Подтверждение прохождения теста «Что такое права доступа в Linux»

Какую команду надо ввести, чтобы посмотреть, какие права выданы файлам?

- a) ls -a
- б) lshb
- в) rwx -l
- г) ls -l

Верный ответ: ls -l

Рис. 3.81: «Что такое права доступа в Linux». Вопрос №1

Выбранный ответ: **ls -l**.

- ls -a - ключ -a показывает скрытые файлы;
- lshb - такой команды не существует;
- rwx -l - такой команды не существует;

Какую команду надо ввести, чтобы посмотреть, какие права выданы файлам, в том числе – скрытым?

- а) ls -a
- б) grep etc/files
- в) ls -la
- г) umask 006

Верный ответ: ls -la

Рис. 3.82: «Что такое права доступа в Linux». Вопрос №2

Выбранный ответ: **ls -la.**

- ls -a - показывает скрытые файлы, но без подробной информации о правах;
- grep etc/files - не имеет отношения к просмотру прав доступа;
- umask 006 - команда для установки маски прав;

Как будут записаны права r w - в восьмеричном формате?

- а) 3
- б) 110
- в) 6
- г) ---

Верный ответ: 6

Рис. 3.83: «Что такое права доступа в Linux». Вопрос №3

Выбранный ответ: **6.**

- 3 - равносильно -wx (021);
- 110 - двоичное представление, а не восьмеричное;
- ----- символическое представление отсутствия прав, а не восьмеричное;

3.3.3 Задания по теме «Изменение прав доступа: chmod, chown, chgrp»

Задание №1

Создайте файл и настройте ему права 644, чтобы владелец мог редактировать, а остальные – только читать.

Задание №2

Создайте группу admins, поменяйте группу у созданного файла в первом задании на эту и передайте группе право на изменение (запись).

Рис. 3.84: «Изменение прав доступа: chmod, chown, chgrp». Условия заданий

3.3.3.1 Задание №1

Создадим файл wrr.txt и настроим ему права 644

```
touch wrr.txt  
chmod 644 wrr.txt  
ls -l | grep wrr.txt
```

```
[dosergeev@dosergeev ~]$ touch wrr.txt  
[dosergeev@dosergeev ~]$ chmod 644 wrr.txt  
[dosergeev@dosergeev ~]$ ls -l | grep wrr.txt  
-rw-r--r--. 1 dosergeev dosergeev 0 Nov 11 21:35 wrr.txt
```

Рис. 3.85: Создание файла и настройка прав доступа

3.3.3.2 Задание №2

Создадим группу admins, поменяем группу файла wrr.txt с dosergeev на admins

```
sudo groupadd admins  
sudo chgrp admins wrr.txt  
ls -l | grep wrr.txt
```

```
[dosergeev@dosergeev ~]$ sudo groupadd admins
[sudo] password for dosergeev:
groupadd: group 'admins' already exists
[dosergeev@dosergeev ~]$ sudo chgrp admins wrr.txt
[dosergeev@dosergeev ~]$ ls -l | grep wrr.txt
-rw-r--r--. 1 dosergeev admins      0 Nov 11 21:35 wrr.txt
```

Рис. 3.86: Создание группы и модификация группы файла

3.3.4 Тест по теме «Изменение прав доступа: chmod, chown, chgrp»

The screenshot shows a user profile on the right with the name 'Даниил Сергеев', a 'Personal cabinet' section, and course links for 'КУРСЫ' and 'Системный администратор Linux с нуля'. The main area displays the results of a test titled 'Тест по теме «Изменение прав доступа: chmod, chown, chgrp»'. It shows a green box with the message 'Результат тестирования' and 'Тест пройден' followed by '3 из 3'.

Рис. 3.87: Подтверждение прохождения теста «Изменение прав доступа: chmod, chown, chgrp»

Какую команду нужно использовать для изменения прав файлов и каталогов?

- a) chown
- б) chmod
- в) chgrp
- г) nano file.txt

Верный ответ: chmod

Рис. 3.88: «Изменение прав доступа: chmod, chown, chgrp». Вопрос №1

Выбранный ответ: **chmod**.

- chown - меняет владельца файла;
- chgrp - меняет группу файла;
- nano file.txt - текстовый редактор для редактирования содержимого файла;

С помощью каких операторов можно указать тип изменения прав?

- а) + - =
- б) r w x
- в) u g o a

Верный ответ: + - =

Рис. 3.89: «Изменение прав доступа: chmod, chown, chgrp». Вопрос №2

Выбранный ответ: + - =.

- r w x - обозначения самих прав (read, write, execute);
- u g o a - обозначения категорий пользователей (user, group, others, all);

Какую опцию нужно применить, чтобы изменить прав ко всем каталогам, в которые вложен целевой файл?

- а) -R
- б) -man
- в) -la
- г) о-рх

Верный ответ: -R

Рис. 3.90: «Изменение прав доступа: chmod, chown, chgrp». Вопрос №3

Выбранный ответ: **-R.**

- -man - не опция команды chmod;
- -la - опции команды ls для просмотра файлов;
- о-рх - часть синтаксиса изменения прав, а не опция рекурсивного применения;

3.3.5 Задания по теме «Расширенные списки доступа (ACL) для управления доступом»

Задание №1

Разрешите конкретному пользователю изменять файл, не добавляя его в основную группу владельца.

Задание №2

Установите особые права для группы, чтобы она могла только выполнять файл.

Задание №3

Проверьте и сбросьте все ACL с файла.

Рис. 3.91: «Расширенные списки доступа (ACL) для управления доступом». Условия заданий

3.3.5.1 Задание №1

Воспользуемся списками доступа ACL. Для этого выполним команду

```
setfacl -m u:ivan:rw b.txt
```

```
[dosergeev@dosergeev ~]$ setfacl -m u:ivan:rw b.txt
[dosergeev@dosergeev ~]$ getfacl b.txt
# file: b.txt
# owner: dosergeev
# group: admins
user::rw-
user:ivan:rw-
group::rw-
mask::rw-
other::r--
```

Рис. 3.92: Установка прав доступа конкретному пользователю

3.3.5.2 Задание №2

Теперь, также используя ACL, установим особые права (только на выполнение файла) для одной из групп, например admins

```
setfacl -m g:admins:x b.txt
```

```
^[[A[dosergeev@dosergeev setfacl -m g:admins:x b.txt
[dosergeev@dosergeev ~]$ getfacl b.txt
# file: b.txt
# owner: dosergeev
# group: dosergeev
user::rw-
user:ivan:rw-
group::rw-
group:admins:--x
mask::rwx
other::r--
```

Рис. 3.93: Установка права на выполнение для конкретной группы

3.3.5.3 Задание №3

За сброс ACL отвечает ключ **-b** в команде setfacl, выполним

```
setfacl -b b.txt  
# проверка прав ACL  
getfacl b.txt
```

```
[dosergeev@dosergeev ~]$ getfacl b.txt  
# file: b.txt  
# owner: dosergeev  
# group: dosergeev  
user::rw-  
user:ivan:rw-  
group::rw-  
group:admins:--x  
mask::rwx  
other::r--  
  
[dosergeev@dosergeev ~]$ man setfacl  
[dosergeev@dosergeev ~]$ setfacl -b b.txt  
[dosergeev@dosergeev ~]$ getfacl b.txt  
# file: b.txt  
# owner: dosergeev  
# group: dosergeev  
user::rw-  
group::rw-  
other::r--
```



Рис. 3.94: Сброс расширенных списков доступа ACL для файла

3.3.6 Задания по теме «Специальные разрешения: SUID, SGID, Sticky Bit»

Задание №1

Установите SUID на исполняемый файл, чтобы он запускался от имени владельца.

Задание №2

Настройте SGID для каталога, чтобы новые файлы наследовали группу.

Задание №3

Сделайте так, чтобы категория других пользователей могли записывать в /public_folder, но не могли удалять чужие файлы.

Рис. 3.95: «Специальные разрешения: SUID, SGID, Sticky Bit». Условия заданий

3.3.6.1 Задание №1

Установим SUID на исполняемый файл test.txt.

```
# +s установка SUID
chmod u+s test.txt
ls -l | grep test.txt
```

```
[dosergeev@dosergeev ~]$ ls
a.txt b.txt course c.txt Desktop Documents Downloads Music opt Pictures Public R Templates test.txt
[dosergeev@dosergeev ~]$ chmod u+s test.txt
[dosergeev@dosergeev ~]$ ls -l | grep test.txt
-rwsr-xr--. 1 dosergeev dosergeev 0 Nov 11 20:38 test.txt
```

Рис. 3.96: Установка SUID для файла

Теперь вместо права на исполнение для владельца указан специальный символ s.

3.3.6.2 Задание №2

Создадим каталог ~/sgid_test и установим для него SGID

```
mkdir sgid_test  
ls -l | grep sgid_test  
# +s установка SGID  
chmod g+s sgid_test  
ls -l | grep sgid_test
```

```
[dosergeev@dosergeev ~]$ mkdir sgid_test  
[dosergeev@dosergeev ~]$ ls -l | grep sgid_test  
drwxr-x--x. 2 dosergeev dosergeev 6 Nov 11 21:57 sgid_test  
[dosergeev@dosergeev ~]$ chmod g+s sgid_test/  
[dosergeev@dosergeev ~]$ ls -l | grep sgid_test  
drwxr-s--x. 2 dosergeev dosergeev 6 Nov 11 21:57 sgid_test  
[dosergeev@dosergeev ~]$
```

Рис. 3.97: Установка SGID для каталога

3.3.6.3 Задание №3

Сделать так, чтобы категории других пользователей могли записывать в /public_folder, но не могли удалять чужие файлы, можно, установив Sticky-bit.

Создадим общий каталог public_folder. Установим Sticky-bit через chmod

```
sudo mkdir /public_folder  
ls -l / | grep public_folder  
sudo chmod +t /public_folder  
ls -l / | grep public_folder
```

```
[dosergeev@dosergeev ~]$ sudo mkdir /public_folder  
[sudo] password for dosergeev:  
[dosergeev@dosergeev ~]$ ls -l / | grep public_folder  
drwxr-x--x. 2 root root 6 Nov 11 21:58 public_folder  
[dosergeev@dosergeev ~]$ sudo chmod +t /public_folder/  
[dosergeev@dosergeev ~]$ ls -l / | grep public_folder  
drwxr-x--t. 2 root root 6 Nov 11 21:58 public_folder
```

Рис. 3.98: Установка Sticky-bit для общего каталога

3.3.7 Тест по теме «Специальные разрешения: SUID, SGID, Sticky Bit»

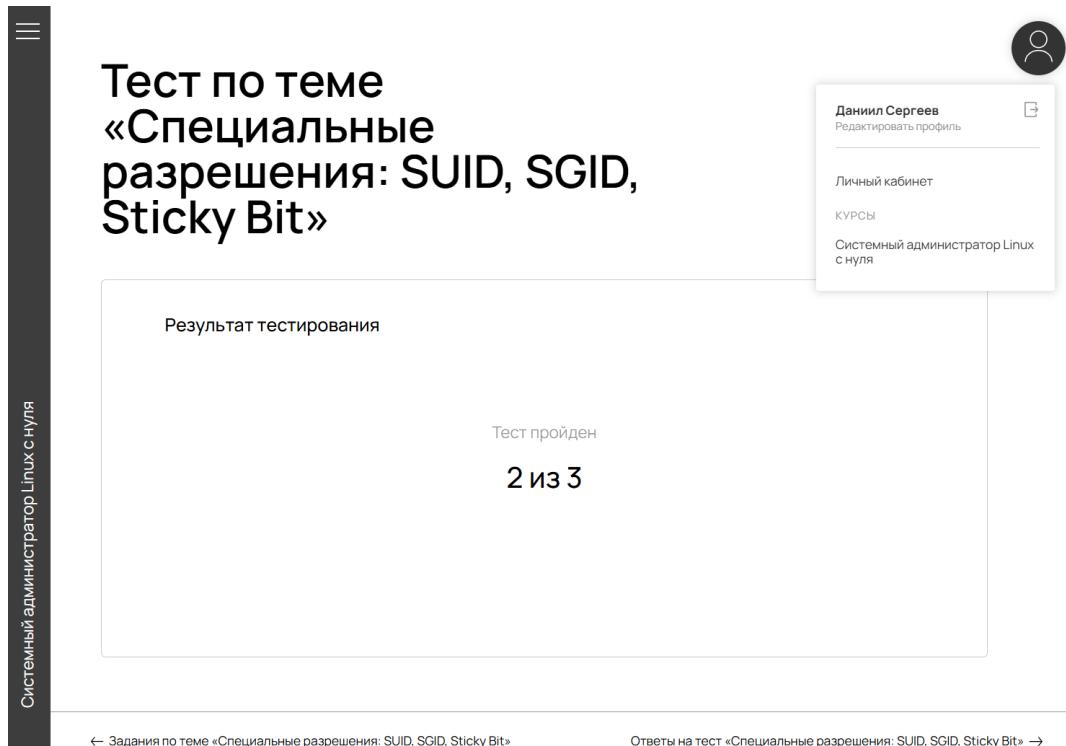


Рис. 3.99: Подтверждение прохождения теста «Специальные разрешения: SUID, SGID, Sticky Bit»

Как называется специальное разрешение, благодаря которому файлы в каталоге, которому выставлен этот бит разрешения, могут быть удалены только их владельцами или владельцами каталога, где лежит этот файл?

- a) Sticky Bit
- b) SGID
- c) SUID
- d) total

Верный ответ: Sticky Bit

Рис. 3.100: «Специальные разрешения: SUID, SGID, Sticky Bit». Вопрос №1

Выбранный ответ: **Sticky Bit.**

- SGID - заставляет файлы создаваться с группой владельца каталога;

- SUID - позволяет выполнять файл с правами владельца файла;
- total - слово из вывода команды ls -l, показывающее общий размер блока;

Как называется параметр безопасности, благодаря которому можно разрешить пользователям запускать программу от имени владельца? При условии, что права на выполнение выданы изначально.

- a) SGID
- б) SUID
- в) Sticky Bit
- г) нет правильного ответа

Верный ответ: SUID

Рис. 3.101: «Специальные разрешения: SUID, SGID, Sticky Bit». Вопрос №2

Выбранный ответ: **SUID**.

- SGID - заставляет файлы создаваться с группой владельца каталога;
- Sticky Bit - относится к правам удаления в каталогах;

Как называется параметр безопасности, благодаря которому можно разрешить пользователям запускать файл от имени владельца группы файла? При условии, что права на выполнение не выданы изначально.

- a) SCID
- б) Sticky Bit
- в) SUID
- г) нет правильного ответа

Верный ответ: нет правильного ответа

Рис. 3.102: «Специальные разрешения: SUID, SGID, Sticky Bit». Вопрос №3

Выбранный ответ: **SGID**.

Правильный ответ: **нет правильного ответа**.

Специальные биты SUID/SGID/Sticky не могут обойти базовое право на выполнение. Если право на выполнение не выдано, файл нельзя запустить, независимо от установленных битов.

3.4 Модуль 7. Управление процессами

3.4.1 Задания по теме «Основы управления процессами в Linux»

Задание №1

Найдите процесс, потребляющий больше всего памяти и завершите его.

Задание №2

Запустите процесс в фоновом режиме, верните его на передний план, приостановите процесс, затем верните в фон.

Задание №3

Установите и запустите htop, настройте нужные вам колонки, найдите по фильтру процесс и «убейте его».

Рис. 3.103: «Основы управления процессами в Linux». Условия заданий

3.4.1.1 Задание №1

Откроем htop и отсортируем процессы по памяти. Найдем процесс с наибольшим значением %MEM и завершим его, нажав F9.

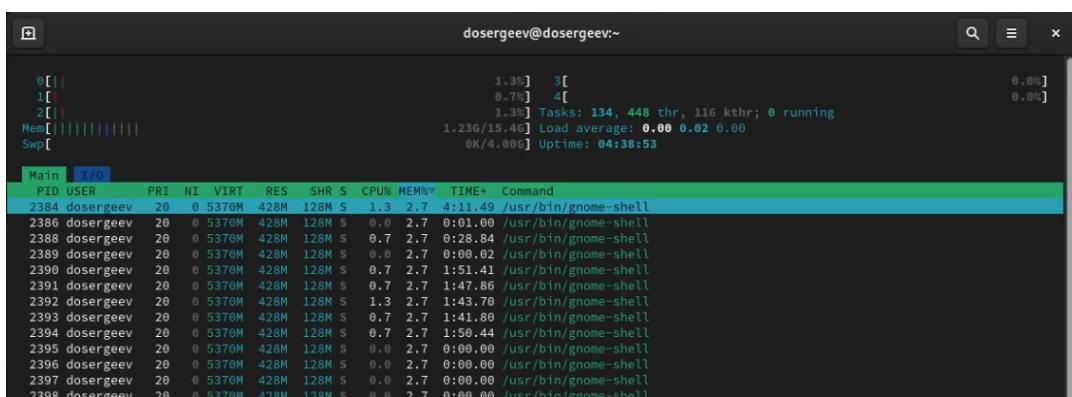


Рис. 3.104: Процесс потребляющий наибольшее количество памяти - PID 2384

3.4.1.2 Задание №2

Запустим службу httpd и запустим команду ping в фоновом режиме (&), отправив вывод в /dev/null.

```
systemctl start httpd  
ping localhost > /dev/null &
```

Переведем задачу в фоновой режим, для этого используем относительный номер задачи из списка jobs

```
jobs  
fg %1
```

Теперь приостановим задачу (CTRL+Z) и переведем её обратно на фон

```
# CTRL+Z  
bg %1
```

```
[dosergeev@dosergeev ~]$ systemctl start httpd  
[dosergeev@dosergeev ~]$ ping localhost > /dev/null &  
[1] 3462  
[dosergeev@dosergeev ~]$ jobs  
[1]+ Running ping localhost > /dev/null &  
[dosergeev@dosergeev ~]$ fg %1  
ping localhost > /dev/null  
^Z  
[1]+ Stopped ping localhost > /dev/null  
[dosergeev@dosergeev ~]$ bg %1  
[1]+ ping localhost > /dev/null &  
[dosergeev@dosergeev ~]$
```

Рис. 3.105: Работа с передним и задним фоном задач

3.4.1.3 Задание №3

Настроим колонки в htop (F2). Затем применим фильтр по имени процесса (ping) и убьём его (F9)

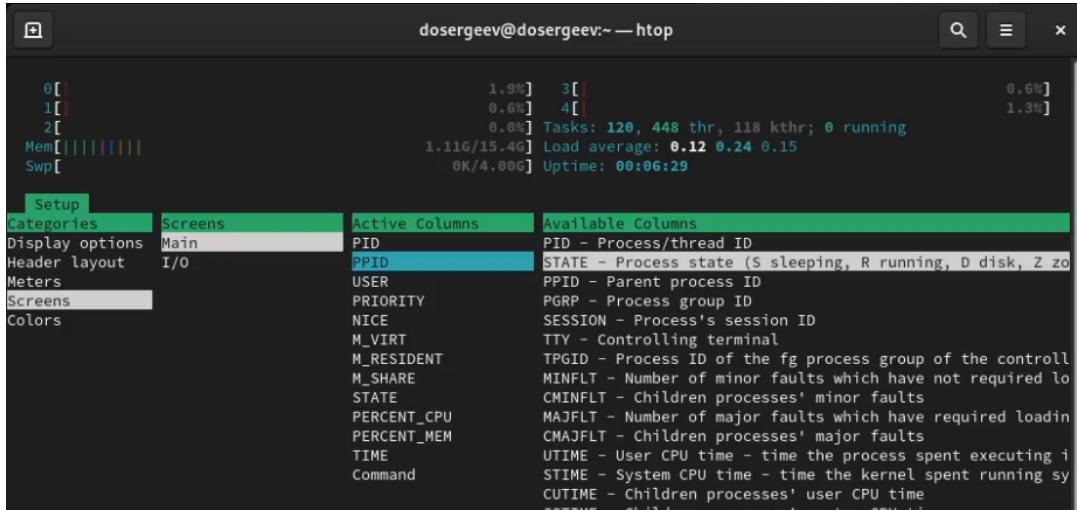


Рис. 3.106: Настройка колонок вывода htop

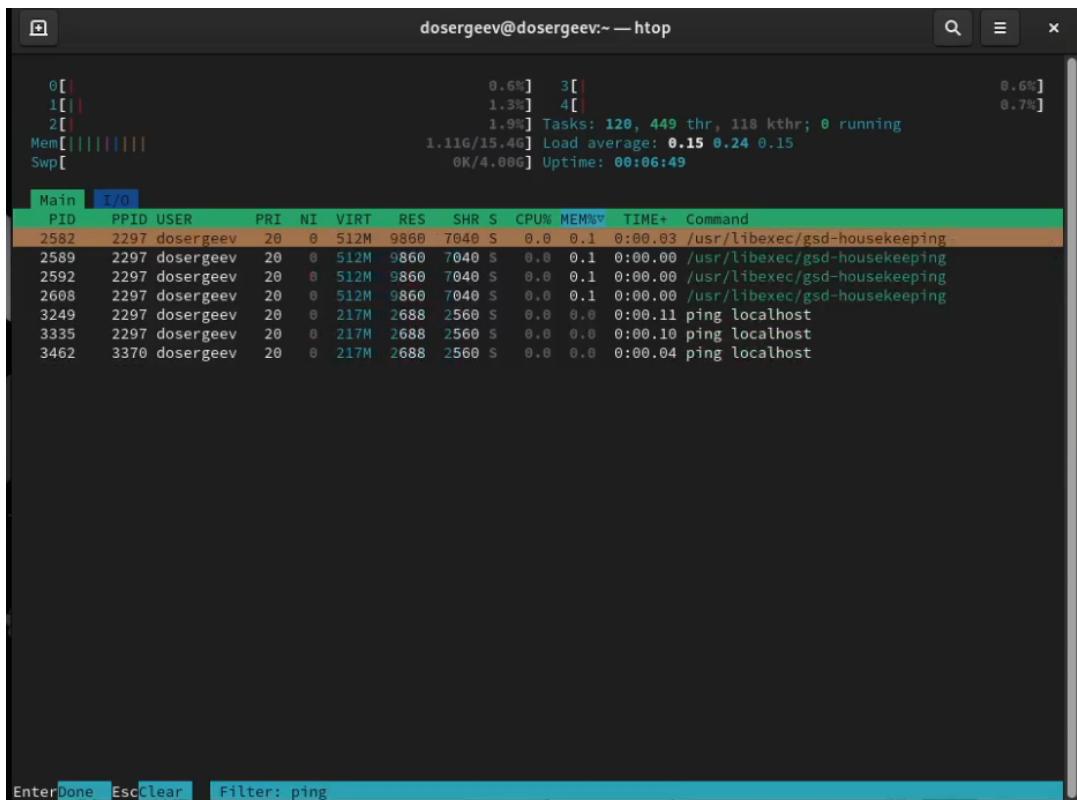


Рис. 3.107: Фильтрация процесса по названию

3.4.2 Тест по теме «Основы управления процессами в Linux»

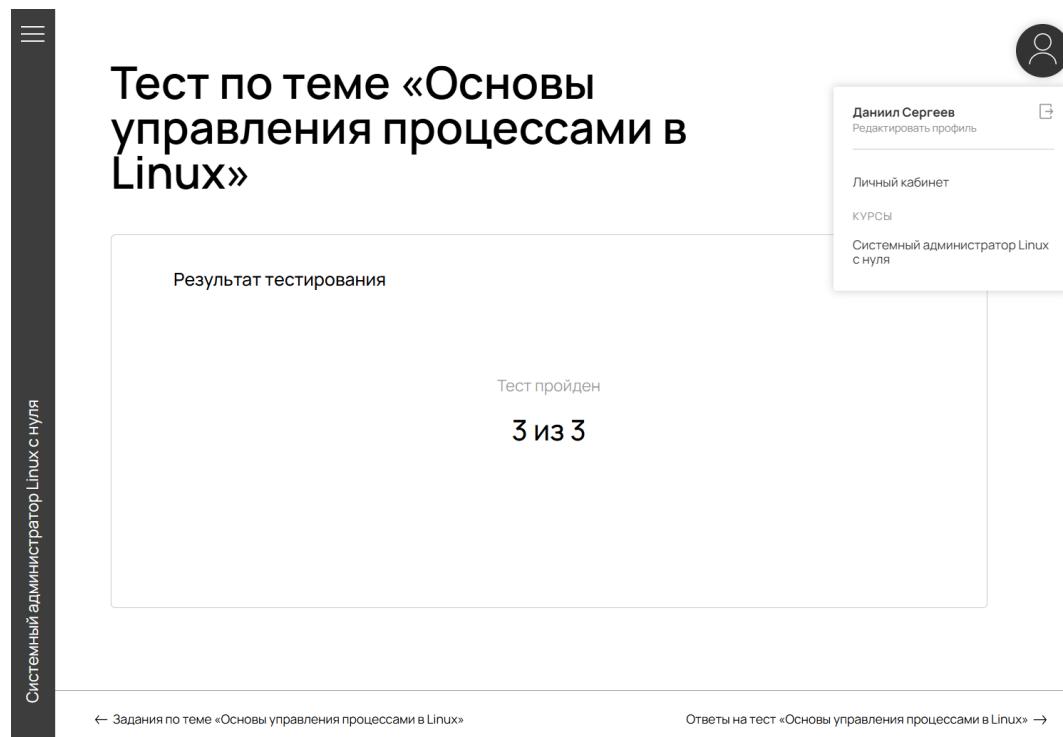


Рис. 3.108: Подтверждение прохождения теста «Основы управления процессами в Linux»

Какой командой можно вывести список всех процессов с детальной информацией об использовании CPU и памяти?

- a) ps -ef
- б) ps aux
- в) top -n 1

Верный ответ: ps aux

Рис. 3.109: «Основы управления процессами в Linux». Вопрос №1

Выбранный ответ: **ps aux**.

- ps -ef - показывает все процессы, но без детальной информации об использовании ресурсов;
- top -n 1 - покажет один снимок процессов;

Какой сигнал отправляется процессу командой kill -9?

а) SIGTERM (15)

б) SIGKILL (9)

в) SIGSTOP (19)

Верный ответ: SIGKILL (9)

Рис. 3.110: «Основы управления процессами в Linux». Вопрос №2

Выбранный ответ: **SIGKILL (9).**

- SIGTERM (15) - “вежливый” сигнал завершения (по умолчанию для kill);
- SIGSTOP (19) - сигнал приостанавливает выполнение процесса;

Какой командой можно приостановить выполнение процесса и перевести его в фон?

а) Ctrl+Z, затем bg %1

б) kill -STOP

в) fg %1

Верный ответ: Ctrl+Z, затем bg %1

Рис. 3.111: «Основы управления процессами в Linux». Вопрос №3

Выбранный ответ: **Ctrl+Z, затем bg %1.**

- kill -STOP - только приостанавливает процесс, но не переводит в фон;
- fg %1 - переводит процесс из фона на передний план;

3.4.3 Задания по теме «Управление приоритетами процессов: nice и renice»

Задание №1

Запустите задачу у низким приоритетом – например, с nice=15.

Задание №2

Найдите PID процесса, который запускали ранее, и повысьте приоритет до -5.

Задание №3

Найдите процесс с самым низким приоритетом и попробуйте повысить приоритет данного процесса.

Рис. 3.112: «Управление приоритетами процессов: nice и renice». Условия заданий

3.4.3.1 Задание №1

Запустим ping с низким приоритетом nice (15) в фоновом режиме.

```
sudo nice -n 15 ping localhost > /dev/null &
```

```
[dosergeev@dosergeev ~]$ nice -n 15 ping localhost > /dev/null &
[1] 3573
[dosergeev@dosergeev ~]$
```

Рис. 3.113: Запуск процесса с низким приоритетом

3.4.3.2 Задание №2

PID запущенного процесса нам известен из команды jobs (номер выводится во время запуска процесса на фоне, вместе с PID). По известному номеру повысим приоритет

```
sudo renice -n -5 3573
```

```
[dosergeev@dosergeev ~]$ sudo renice -n -5 3573
[sudo] password for dosergeev:
3573 (process ID) old priority 15, new priority -5
[dosergeev@dosergeev ~]$ █
```

Рис. 3.114: Повышение приоритета для процесса

3.4.3.3 Задание №3

Выведем через список процессов те, что равны минимальному приоритету (19) и установим новый (-5)

```
ps -eo pid,ni,cmd | awk '$2 == 19'
```

Самый низкий приоритет у процесса 60

```
sudo renice -n -5 60
```

```
[dosergeev@dosergeev ~]$ ps -eo pid,ni,cmd | awk '$2 == 19'
60 19 [khugepaged]
[dosergeev@dosergeev ~]$ ps -eo pid,ni,cmd | awk '$2 == 18'
[dosergeev@dosergeev ~]$ sudo renice -n -5 60
60 (process ID) old priority 19, new priority -5
[dosergeev@dosergeev ~]$ ps -eo pid,ni,cmd | awk '$2 == -5'
60 -5 [khugepaged]
3573 -5 ping localhost
[dosergeev@dosergeev ~]$ █
```

Рис. 3.115: Изменение nice у процесса с самым маленьким приоритетом

3.4.4 Тест по теме «Управление приоритетами процессов: nice и renice»

The screenshot shows a user interface for a test. On the left, there's a vertical sidebar with three horizontal lines at the top and the text "Системный администратор Linux с нуля" at the bottom. The main content area has a dark header bar with the title "Тест по теме «Управление приоритетами процессов: nice и renice»". Below the header, a large white box contains the text "Результат тестирования" and "Тест пройден". In the center, it says "3 из 3". At the bottom of this box, there are two links: "← Задания по теме «Управление приоритетами процессов: nice и renice»" and "Ответы на тест «Управление приоритетами процессов: nice и renice» →". In the top right corner, there's a user profile box with a person icon, the name "Даниил Сергеев", a "Редактировать профиль" link, and a "Личный кабинет" section. Below that, it says "КУРСЫ" and "Системный администратор Linux с нуля".

Рис. 3.116: Подтверждение прохождения теста «Управление приоритетами процессов: nice и renice»

Какое значение nice имеет наивысший приоритет?

- a) -20
- б) 0
- в) 19
- г) ps

Верный ответ: -20

Рис. 3.117: «Управление приоритетами процессов: nice и renice». Вопрос №1

Выбранный ответ: **-20**.

Приоритет nice меняет своё значение от -20 до 19

Какой командой изменить приоритет уже запущенного процесса с PID 1234 на nice=10?

- a) nice -n 10 -p 1234
- б) renice -n 10 -p 1234
- в) priority -n 10 1234
- г) nice == 10 -f 1234

Верный ответ: renice -n 10 -p 1234

Рис. 3.118: «Управление приоритетами процессов: nice и renice». Вопрос №2

Выбранный ответ: **renice -n 10 -p 1234.**

- nice -n 10 -p 1234 - команда nice используется для запуска процесса с заданным приоритетом, а не для изменения приоритета уже работающего;
- priority -n 10 1234 - такой команды не существует;
- nice == 10 -f 1234 - синтаксис неверный;

Какой параметр в unit-файле systemd устанавливает приоритет CPU для сервиса?

- a) CPUPriority=10
- б) Nice=10
- в) Priority=10
- г) Renice=10

Верный ответ: Nice=10

Рис. 3.119: «Управление приоритетами процессов: nice и renice». Вопрос №3

Выбранный ответ: **Nice=10.**

Всех параметров, кроме Nice не существует в systemd;

3.4.5 Задания по теме «Контроль системных сервисов: systemd и systemctl»

Задание №1

Выведите список всех активных сервисов и отфильтруйте их по фильтру «Network».

Задание №2

Определите, какой веб-сервер установлен, проверьте статус сервиса и перезапустите его. После перезапуска проверьте журнал на наличие ошибок.

| Примечание: если веб-сервер не установлен, сделайте это самостоятельно.

Задание №3

Найдите ненужный сервис. Сделайте так, чтобы при перезапуске системы данный процесс не запускался. Перезагрузите устройство, на котором работаете, и проверьте, что выбранный сервис выключен.

Рис. 3.120: «Контроль системных сервисов: systemd и systemctl». Условия заданий

3.4.5.1 Задание №1

Выведем список всех юнитов и отфильтруем его с помощью встроенной опции `--type`. Передадим вывод в grep

```
systemctl list-units --type=service --state=active | grep Network
```

```
[dosergeev@dosergeev ~]$ systemctl list-units --type=service --state=active | grep Network
NetworkManager-wait-online.service loaded active exited Network Manager Wait Online
NetworkManager.service           loaded active running Network Manager
```

Рис. 3.121: Список всех активных сервисов Network

3.4.5.2 Задание №2

Проверим статус веб-сервера httpd и перезапустим его.

```
systemctl status httpd
systemctl restart httpd
```

```
[dosergeev@dosergeev ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Tue 2025-11-11 22:12:13 MSK; 36min ago
     Docs: man:httpd.service(8)
      Main PID: 1167 (httpd)
        Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
         Tasks: 177 (limit: 100279)
        Memory: 50.5M
       CPU: 10.765s
      CGroup: /system.slice/httpd.service
              ├─1167 /usr/sbin/httpd -DFOREGROUND
              ├─1291 /usr/sbin/httpd -DFOREGROUND
              ├─1293 /usr/sbin/httpd -DFOREGROUND
              ├─1294 /usr/sbin/httpd -DFOREGROUND
              └─1296 /usr/sbin/httpd -DFOREGROUND

Nov 11 22:12:12 dosergeev.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 11 22:12:13 dosergeev.localdomain systemd[1]: Started The Apache HTTP Server.
Nov 11 22:12:13 dosergeev.localdomain httpd[1167]: Server configured, listening on: port 80
[dosergeev@dosergeev ~]$ systemctl restart httpd
```

Рис. 3.122: Проверка статуса и перезапуск httpd

Проверим журнал на наличие ошибок

```
# -u вывод конкретного юнита
# -n последние 10 сообщений
journalctl -u httpd -n 10
```

```
[dosergeev@dosergeev ~]$ journalctl -u httpd -n 10
Nov 11 22:12:12 dosergeev.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 11 22:12:13 dosergeev.localdomain systemd[1]: Started The Apache HTTP Server.
Nov 11 22:12:13 dosergeev.localdomain httpd[1167]: Server configured, listening on: port 80
Nov 11 22:48:33 dosergeev.localdomain systemd[1]: Stopping The Apache HTTP Server...
Nov 11 22:48:34 dosergeev.localdomain systemd[1]: httpd.service: Deactivated successfully.
Nov 11 22:48:34 dosergeev.localdomain systemd[1]: Stopped The Apache HTTP Server.
Nov 11 22:48:34 dosergeev.localdomain systemd[1]: httpd.service: Consumed 10.896s CPU time.
Nov 11 22:48:34 dosergeev.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 11 22:48:34 dosergeev.localdomain httpd[3842]: Server configured, listening on: port 80
Nov 11 22:48:34 dosergeev.localdomain systemd[1]: Started The Apache HTTP Server.
[dosergeev@dosergeev ~]$
```

Рис. 3.123: Последние сообщения httpd

В журнале ошибок не имеется.

3.4.5.3 Задание №3

Сделайте так, чтобы httpd при перезапуске системы не запускался, для этого выполним команду

```
sudo systemctl disable httpd
```

проверим статус службы

```
systemctl status httpd
```

```
[dosergeev@dosergeev ~]$ sudo systemctl disable httpd
[sudo] password for dosergeev:
Removed "/etc/systemd/system/multi-user.target.wants/httpd.service".
[dosergeev@dosergeev ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
      Active: active (running) since Tue 2025-11-11 22:48:34 MSK; 1min 19s ago
        Docs: man:httpd.service(8)
    Main PID: 3842 (httpd)
      Status: "Total requests: 0; Idle/Busy workers 100/0;Requests/sec: 0; Bytes served/sec: 0 B/sec"
         Tasks: 177 (limit: 100279)
        Memory: 27.6M
       CPU: 463ms
      CGroup: /system.slice/httpd.service
              ├─3842 /usr/sbin/httpd -DFOREGROUND
              ├─3844 /usr/sbin/httpd -DFOREGROUND
              ├─3845 /usr/sbin/httpd -DFOREGROUND
              ├─3846 /usr/sbin/httpd -DFOREGROUND
              └─3848 /usr/sbin/httpd -DFOREGROUND

Nov 11 22:48:34 dosergeev.localdomain systemd[1]: Starting The Apache HTTP Server...
Nov 11 22:48:34 dosergeev.localdomain httpd[3842]: Server configured, listening on: port 80
Nov 11 22:48:34 dosergeev.localdomain systemd[1]: Started The Apache HTTP Server.
[dosergeev@dosergeev ~]$
```

Рис. 3.124: Статус службы httpd после отключения автозапуска

Перезапустим систему и проверим статус службы httpd

```
reboot
```

после перезапуска

```
systemctl is-enabled httpd
```

```
systemctl status httpd
```

```
[dosergeev@dosergeev ~]$ systemctl is-enabled httpd
disabled
[dosergeev@dosergeev ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
    Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; preset: disabled)
      Active: inactive (dead)
        Docs: man:httpd.service(8)
[dosergeev@dosergeev ~]$
```

Рис. 3.125: Статус службы после перезапуска

3.4.6 Тест по теме «Контроль системных сервисов: systemd и systemctl»

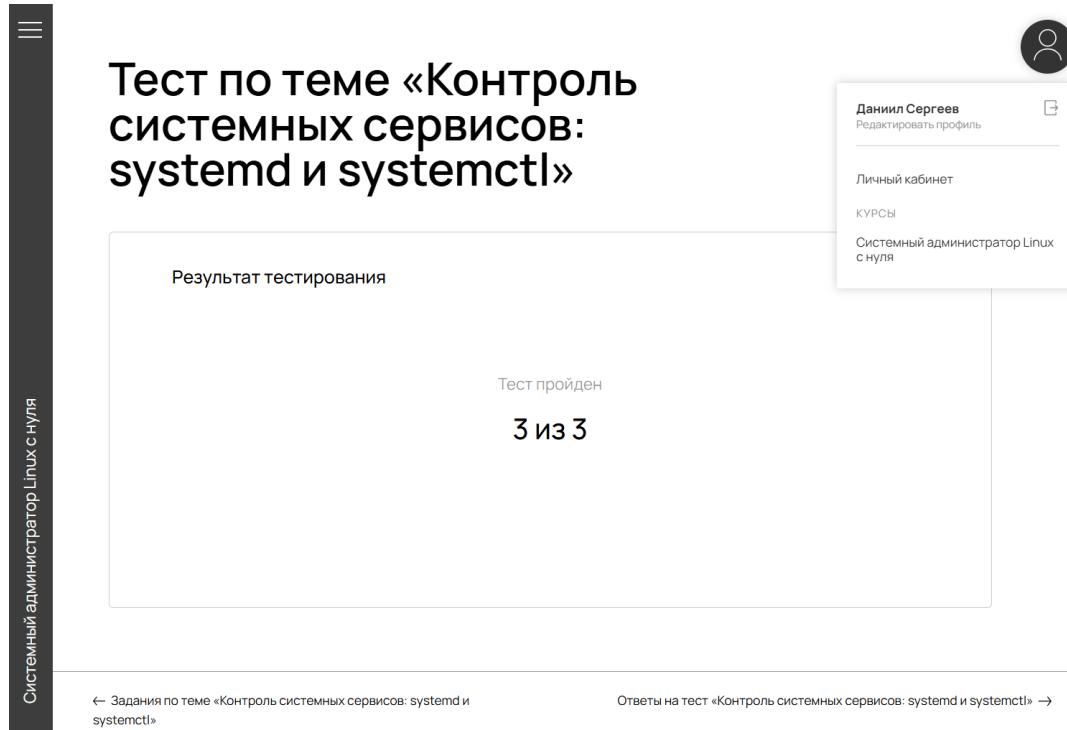


Рис. 3.126: Подтверждение прохождения теста «Контроль системных сервисов: systemd и systemctl»

Какой командой проверить статус сервиса nginx?

- a) systemctl status nginx
- б) service nginx check
- в) ps aux | grep nginx
- г) нет правильного ответа

Верный ответ: systemctl status nginx

Рис. 3.127: «Контроль системных сервисов: systemd и systemctl». Вопрос №1

Выбранный ответ: **systemctl status nginx.**

- service nginx check - неверный синтаксис команды (status вместо check);

- `ps aux | grep nginx` - покажет процессы nginx, но не информацию о статусе сервиса;

Какой параметр в таймере systemd указывает ежедневный запуск в полночь?

- a) `OnTime=daily`
- б) `OnCalendar=daily`
- в) `Schedule=24h`
- г) нет правильного ответа

Верный ответ: `OnCalendar=daily`

Рис. 3.128: «Контроль системных сервисов: systemd и systemctl». Вопрос №2

Выбранный ответ: **OnCalendar=daily**.

Параметров `OnTime` и `Schedule` не существует в таймере systemd.

Какой командой включить автозапуск сервиса при загрузке системы?

- a) `systemctl start servicename`
- б) `systemctl enable servicename`
- в) `systemctl reload servicename`
- г) нет правильного ответа

Верный ответ: `systemctl enable servicename`

Рис. 3.129: «Контроль системных сервисов: systemd и systemctl». Вопрос №3

Выбранный ответ: **systemctl enable servicename**.

- `systemctl start servicename` - команда запускает сервис;
- `systemctl reload servicename` - команда перезагружает конфигурацию сервиса;

3.4.7 Задания по теме «Управление фоновыми процессами (демонами) в Linux»

Задание №1

Создайте простой Python-скрипт и дайте данному файлу права на запуск. Создайте unit-файл – активируйте и проверьте статус вашего юнита.

Пример Python-скрипта:

```
import time
while True:
    with open("/tmp/mydaemon.log", "a") as f:
        f.write("Working...\n")
    time.sleep(10)
```

Задание №2

Принудительно завершите процесс, который был запущен в предыдущем задании, и проверьте статус сервиса.

Задание №3

Перезагрузите устройство, на котором вы работаете, и проверьте, сработал ли автозапуск вашего процесса.

Рис. 3.130: «Управление фоновыми процессами (демонами) в Linux». Условия заданий

3.4.7.1 Задание №1

Возьмем пример python скрипта из условия и дадим ему автозапуск.

Перейдем в каталог /usr/bin и создадим новый скрипт - myscripy.py. Сделаем его исполняемым.

```
cd /usr/bin
sudo vi myscripy.py
sudo chmod +x myscripy.py
```

Теперь перейдем в каталог /etc/systemd/system и создадим unit-файл.

```
cd /etc/systemd/system/
sudo vi mydaemon.service
```

Запишем параметры unit-файла

```
# /etc/systemd/system/mydaemon.service
[Unit]
Description=Мой тестовый сервис
After=network.target
Documentation=https://example.com/docs

[Service]
Type=simple
ExecStart=/usr/bin/python3 /usr/bin/myscripy.py
Restart=always
RestartSec=10
User=dosergeev
Group=dosergeev
Environment="PATH=/usr/bin:/bin"
WorkingDirectory=/home/dosergeev
StandardOutput=syslog
StandardError=syslog

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

Активируем сервис

```
sudo systemctl daemon-reload
sudo systemctl start mydaemon
sudo systemctl status mydaemon
sudo systemctl enable mydaemon
sudo systemctl status mydaemon
```

```
[dosergeev@dosergeev system]$ sudo systemctl daemon-reload
[dosergeev@dosergeev system]$ sudo systemctl start mydaemon
[bash: 1: command not found...
[dosergeev@dosergeev system]$ systemctl status mydaemon
● mydaemon.service - Мой тестовый сервис
    Loaded: loaded (/etc/systemd/system/mydaemon.service; disabled; preset: disabled)
      Active: active (running) since Tue 2025-11-11 23:15:41 MSK; 5s ago
        Docs: https://example.com/docs
     Main PID: 3726 (python3)
        Tasks: 1 (limit: 100279)
       Memory: 2.6M
          CPU: 23ms
        CGroup: /system.slice/mydaemon.service
            └─3726 /usr/bin/python3 /usr/bin/myscripy.py

Nov 11 23:15:41 dosergeev.localdomain systemd[1]: Started Мой тестовый сервис.
[dosergeev@dosergeev system]$ systemctl enable mydaemon
Created symlink /etc/systemd/system/multi-user.target.wants/mydaemon.service → /etc/systemd/system/mydaemon.service.

^[[A[dosergeev@dosergeev system]$ systemctl status mydaemon
● mydaemon.service - Мой тестовый сервис
    Loaded: loaded (/etc/systemd/system/mydaemon.service; enabled; preset: disabled)
      Active: active (running) since Tue 2025-11-11 23:15:41 MSK; 27s ago
        Docs: https://example.com/docs
     Main PID: 3726 (python3)
        Tasks: 1 (limit: 100279)
       Memory: 2.6M
          CPU: 23ms
        CGroup: /system.slice/mydaemon.service
            └─3726 /usr/bin/python3 /usr/bin/myscripy.py

Nov 11 23:15:41 dosergeev.localdomain systemd[1]: Started Мой тестовый сервис.
Nov 11 23:16:06 dosergeev.localdomain systemd[1]: /etc/systemd/system/mydaemon.service:16: Standard output type sy>
Nov 11 23:16:06 dosergeev.localdomain systemd[1]: /etc/systemd/system/mydaemon.service:17: Standard output type sy>
lines 1-14/14 (END)
```

Рис. 3.131: Запуск сервиса mydaemon

3.4.7.2 Задание №2

Узнаем PID процесса из systemctl status и принудительно завершим процесс, затем проверим его статус

```
systemctl status mydaemon
kill -9 3726
systemctl status mydaemon
```

```
[dosergeev@dosergeev system]$ kill -9 3726
[dosergeev@dosergeev system]$ systemctl status mydaemon
● mydaemon.service - Мой тестовый сервис
    Loaded: loaded (/etc/systemd/system/mydaemon.service; enabled; preset: disabled)
      Active: activating (auto-restart) (Result: signal) since Tue 2025-11-11 23:17:15 MSK; 2s ago
        Docs: https://example.com/docs
    Process: 3726 ExecStart=/usr/bin/python3 /usr/bin/myscripy.py (code=killed, signal=KILL)
   Main PID: 3726 (code=killed, signal=KILL)
     CPU: 26ms

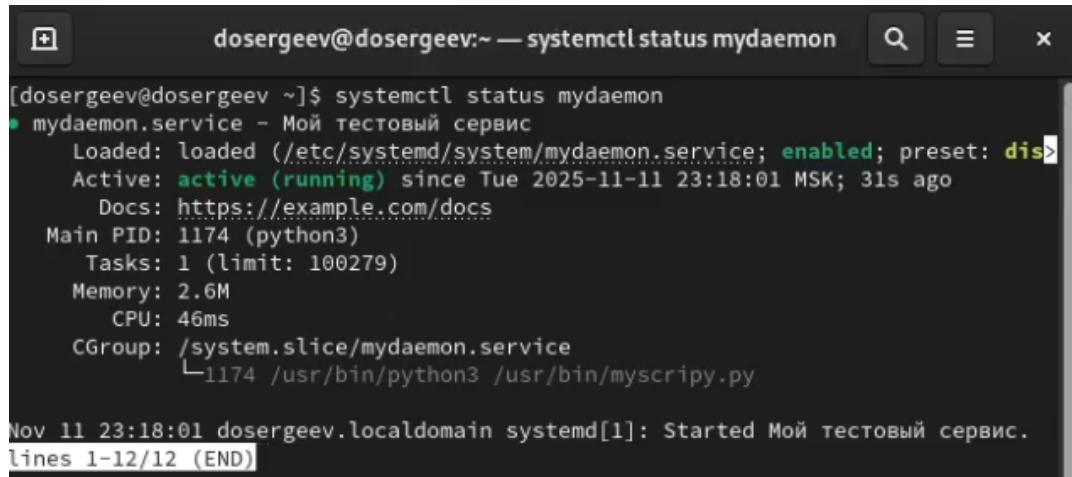
Nov 11 23:17:15 dosergeev.localdomain systemd[1]: mydaemon.service: Failed with result 'signal'.
[dosergeev@dosergeev system]$
```

Рис. 3.132: Завершение юнита mydaemon

3.4.7.3 Задание №3

Перезагрузим устройство и проверим, сработал ли автозапуск

```
reboot  
# после перезапуска  
systemctl status mydaemon
```



The screenshot shows a terminal window with the title bar "dosergeev@dosergeev:~ — systemctl status mydaemon". The main content of the terminal is the output of the command "systemctl status mydaemon". It shows the service "mydaemon.service" is active (running) since November 11, 2025, at 23:18:01 MSK. The service is loaded and enabled. It has a Main PID of 1174, which is running python3. The service is associated with a task ID of 1, memory usage of 2.6M, and CPU usage of 46ms. The CGroup path is /system.slice/mydaemon.service. A log message at the bottom indicates the service was started at 23:18:01 on Nov 11.

```
[dosergeev@dosergeev ~]$ systemctl status mydaemon
● mydaemon.service - Мой тестовый сервис
  Loaded: loaded (/etc/systemd/system/mydaemon.service; enabled; preset: disabled)
  Active: active (running) since Tue 2025-11-11 23:18:01 MSK; 31s ago
    Docs: https://example.com/docs
   Main PID: 1174 (python3)
     Tasks: 1 (limit: 100279)
    Memory: 2.6M
      CPU: 46ms
     CGroup: /system.slice/mydaemon.service
             └─1174 /usr/bin/python3 /usr/bin/myscripy.py

Nov 11 23:18:01 dosergeev.localdomain systemd[1]: Started Мой тестовый сервис.
lines 1-12/12 (END)
```

Рис. 3.133: Юнит mydaemon после перезапуска

3.4.8 Тест по теме «Управление фоновыми процессами (демонами) в Linux»

Системный администратор Linux с нуля

Тест по теме «Управление фоновыми процессами (демонами) в Linux»

Результат тестирования

Тест пройден

3 из 3

← Задания по теме «Управление фоновыми процессами (демонами) в ...

Ответы на тест «Управление фоновыми процессами (демонами) в ...

Даниил Сергеев
Редактировать профиль

Личный кабинет

КУРСЫ

Системный администратор Linux с нуля

Рис. 3.134: Подтверждение прохождения теста «Управление фоновыми процессами (демонами) в Linux»

Какой параметр в unit-файле обеспечивает перезапуск сервиса при любом завершении?

- a) Restart=on-failure
- б) Restart=always
- в) AutoRestart=true
- г) Type=simple

Верный ответ: Restart=always

Рис. 3.135: «Управление фоновыми процессами (демонами) в Linux». Вопрос №1

Выбранный ответ: **Restart=always.**

- Restart=on-failure - перезапускает сервис только при ошибке (ненулевом коде завершения);

- AutoRestart=true - такого параметра не существует в systemd;
- Type=simple - определяет тип запуска сервиса, а не политику перезапуска;

Какой командой просмотреть логи сервиса в реальном времени?

- a) tail -f /var/log/syslog
- б) journalctl -u servicename -f
- в) systemctl log servicename
- г) watch -n 1 "ps aux | grep 'python3 /home/user/myscript.py'"

Верный ответ: journalctl -u servicename -f

Рис. 3.136: «Управление фоновыми процессами (демонами) в Linux». Вопрос №2

Выбранный ответ: **journalctl -u servicename -f.**

- tail -f /var/log/syslog - показывает общий системный лог, а не логи конкретного сервиса;
- systemctl log servicename - такой команды не существует;
- watch -n 1 "ps aux | grep 'python3 /home/user/myscript.py'" - показывает статус процесса, а не логи;

Какой командой проверить синтаксис unit-файла перед запуском?

- a) systemctl check mydaemon.service
- б) systemd-analyze verify mydaemon.service
- в) validate-unit mydaemon.service
- г) sudo systemctl daemon-reload

Верный ответ: systemd-analyze verify mydaemon.service

Рис. 3.137: «Управление фоновыми процессами (демонами) в Linux». Вопрос №3

Выбранный ответ: **systemd-analyze verify mydaemon.service.**

- systemctl check mydaemon.service - такой команды не существует;
- validate-unit mydaemon.service - такой команды не существует;
- sudo systemctl daemon-reload - обновляет конфигурацию системного менеджера systemd;

3.5 Вывод

В результате прохождения второй части внешнего курса «Системный администратор Linux с нуля» я глубже погрузился в работу системного администратора Linux. Я научился находить справочную информацию, редактировать файлы и работать с выводом команд. Также я узнал как управлять правами доступа к файлам и каталогам, как добавлять и менять права пользователей и как управлять процессами и юнитами.