Отчёт по лабораторной работе №7

Управление журналами событий в системе

Амина Аджигалиева

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Ход выполнения работы

## 2.1 Анализ системных журналов

Сначала я просмотрела логи сбоев процессов, связанных с **VBoxClient**, и сообщения о неудачных попытках получения привилегий root.  
На скриншоте видно, что при выполнении команды su вход был отклонён, а также зафиксированы ошибки в работе клиента VirtualBox.

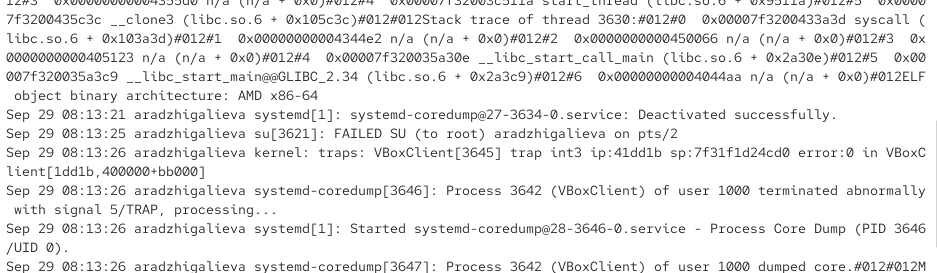


Рис. 1: Сообщения о сбоях VBoxClient и неудачной попытке входа под root

Далее я проанализировала системный журнал, где видно серию сообщений «hello» от пользователя **aradzhlgalieva**, а также повторяющиеся ошибки VBoxClient, сопровождающиеся завершением процессов с генерацией дампа памяти.

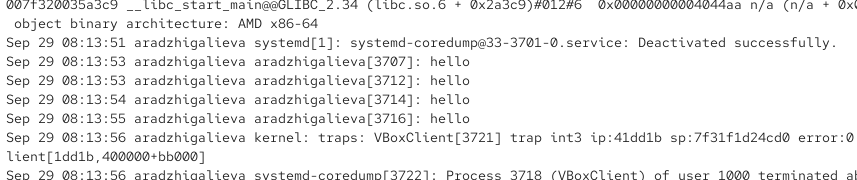


Рис. 2: Системные сообщения и повторные ошибки VBoxClient

Затем я обратилась к журналу **/var/log/secure**, чтобы отследить авторизации пользователей.  
В выводе отчётливо видно открытие сессий для пользователей gdm, aradzhlgalieva и root. Также зафиксированы ошибки проверки паролей и события, связанные с PAM (Pluggable Authentication Modules).

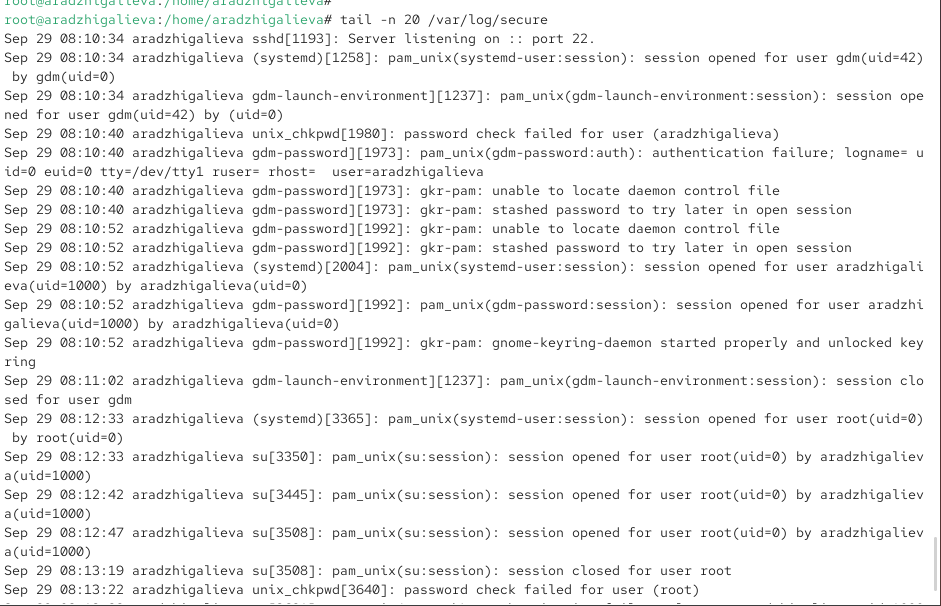


Рис. 3: Просмотр журнала /var/log/secure

## 2.2 Настройка регистрации сообщений через rsyslog

Сначала я установила веб-сервер Apache и запустила его службу. Также я настроила автоматический запуск httpd при старте системы.

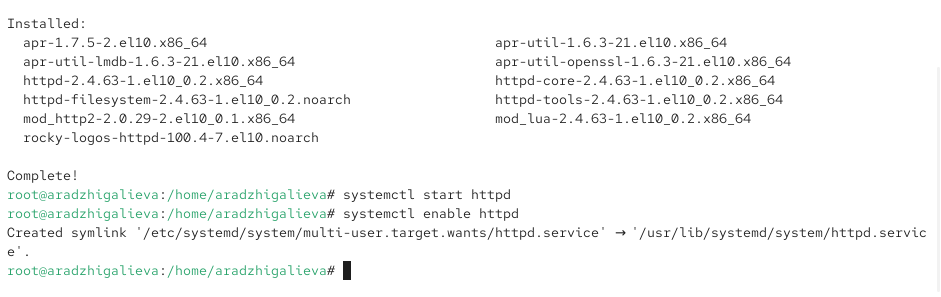


Рис. 4: Установка и запуск Apache

Затем я просмотрела журнал ошибок веб-службы, чтобы убедиться в корректности её работы.  
На скриншоте видно сообщения о запуске Apache и успешной конфигурации.

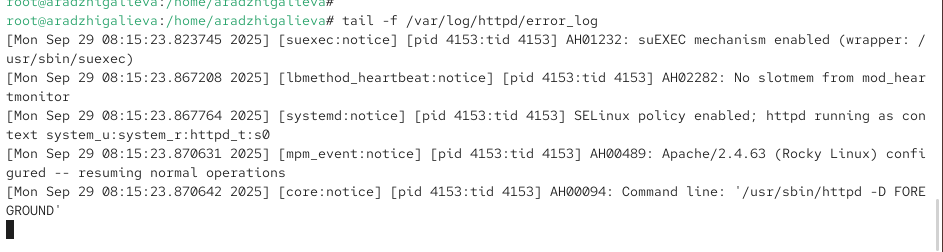


Рис. 5: Просмотр error\_log веб-сервера

После этого я изменила конфигурацию веб-сервера, добавив в файл /etc/httpd/conf/httpd.conf строку:  
ErrorLog syslog:local1.  
Эта настройка позволяет перенаправлять сообщения об ошибках Apache в системный журнал.



Рис. 6: Редактирование httpd.conf

В каталоге /etc/rsyslog.d я создала новый файл конфигурации и добавила правило, которое направляет все сообщения объекта local1 в файл /var/log/httpd-error.log.

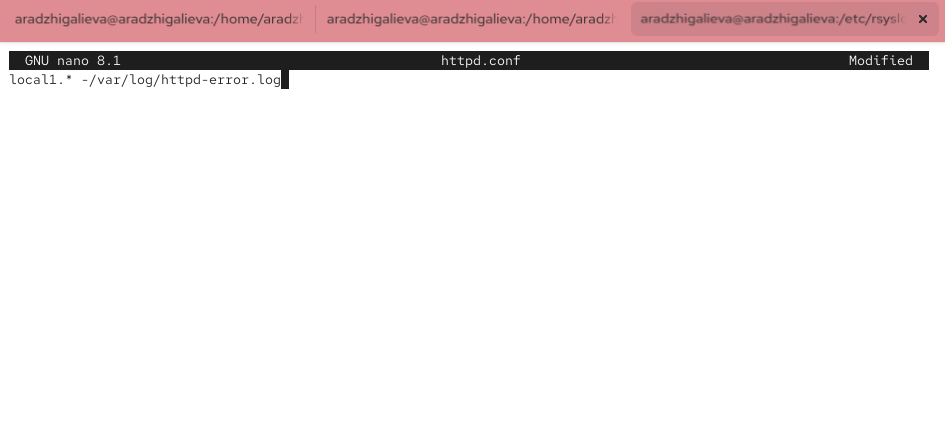


Рис. 7: Создание правила для регистрации ошибок Apache

Затем я создала отдельный файл debug.conf для регистрации отладочных сообщений и указала в нём правило:  
\*.debug /var/log/messages-debug.

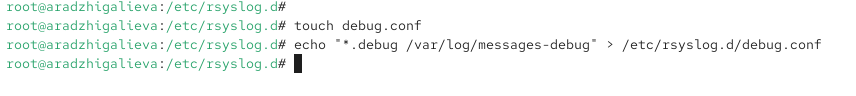


Рис. 8: Создание файла debug.conf

После перезапуска служб rsyslog и httpd я проверила работу конфигурации. Для этого выполнила команду logger -p daemon.debug "Daemon Debug Message".  
На скриншоте видно, что отладочные сообщения корректно записываются в файл /var/log/messages-debug, а ошибки VBoxClient продолжают фиксироваться.

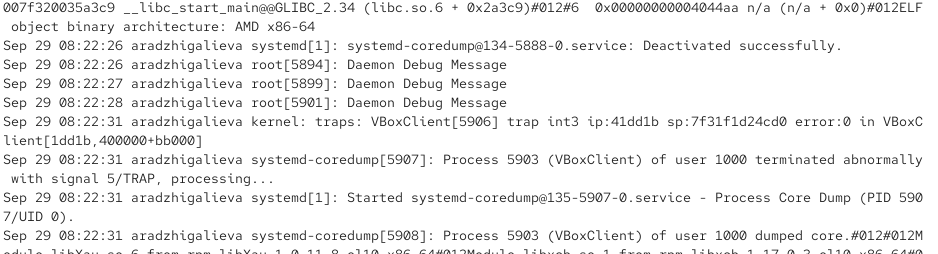


Рис. 9: Проверка работы отладочного логирования

## 2.3 Использование journalctl

Сначала я просмотрела журнал системы, чтобы получить список событий, начиная с последней загрузки.  
Команда journalctl показала записи ядра и системных служб, включая параметры запуска и информацию о виртуальной машине.

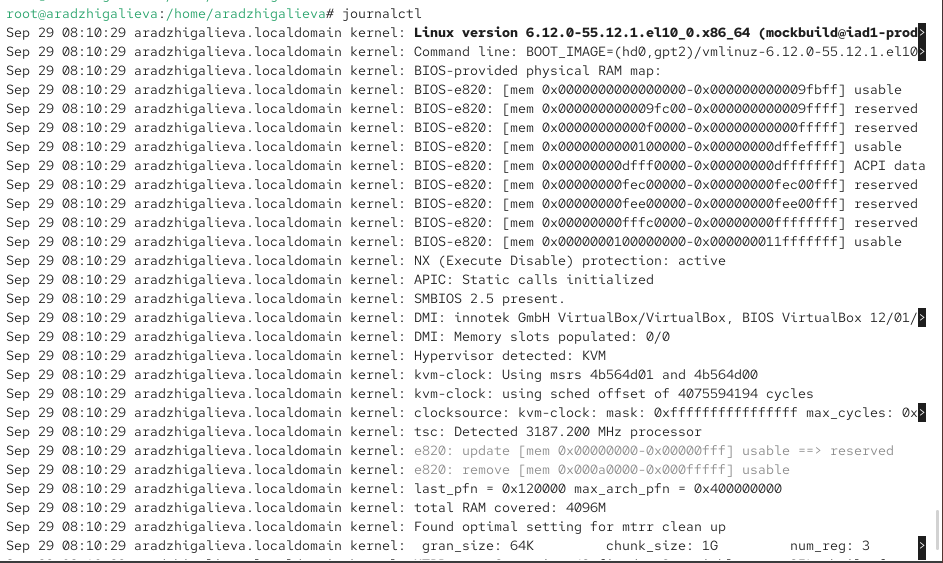


Рис. 10: Просмотр системного журнала

Затем я проанализировала ошибки, связанные с библиотеками и аварийным завершением процессов.  
Скриншоты фиксируют трассировки стека (stack trace), полученные при падении процессов.


Для фильтрации событий я использовала встроенные параметры. При вводе команды journalctl и двойном нажатии Tab был отображён список доступных фильтров.



Рис. 11: Отображение доступных фильтров journalctl

Затем я просмотрела только те события, которые связаны с пользователем root (UID=0).  
В журнале отображаются действия системных служб и процессы, запускаемые от имени суперпользователя.

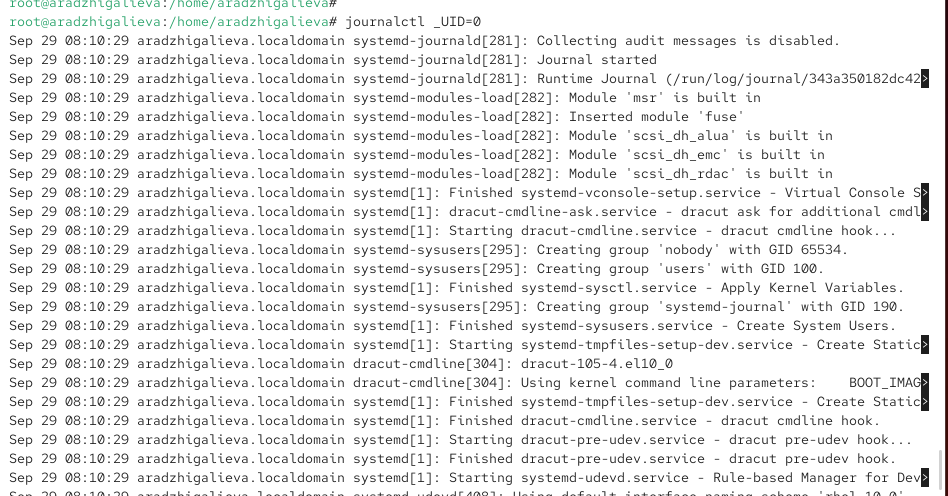


Рис. 12: Просмотр событий для UID=0

Для анализа последних записей я вывела последние 20 строк журнала с помощью команды journalctl -n 20.  
В сообщениях видны ошибки клиента VirtualBox и созданные дампы процессов.

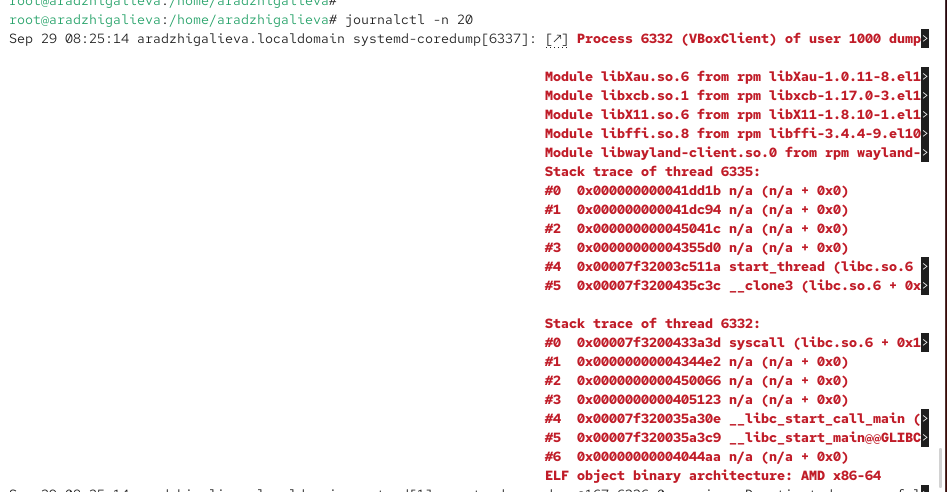


Рис. 13: Вывод последних строк журнала

Далее я просмотрела только сообщения уровня ошибок с помощью команды journalctl -p err.  
В выводе содержатся ошибки графического драйвера vmwgfx, предупреждения ядра и сбои процессов VBoxClient.

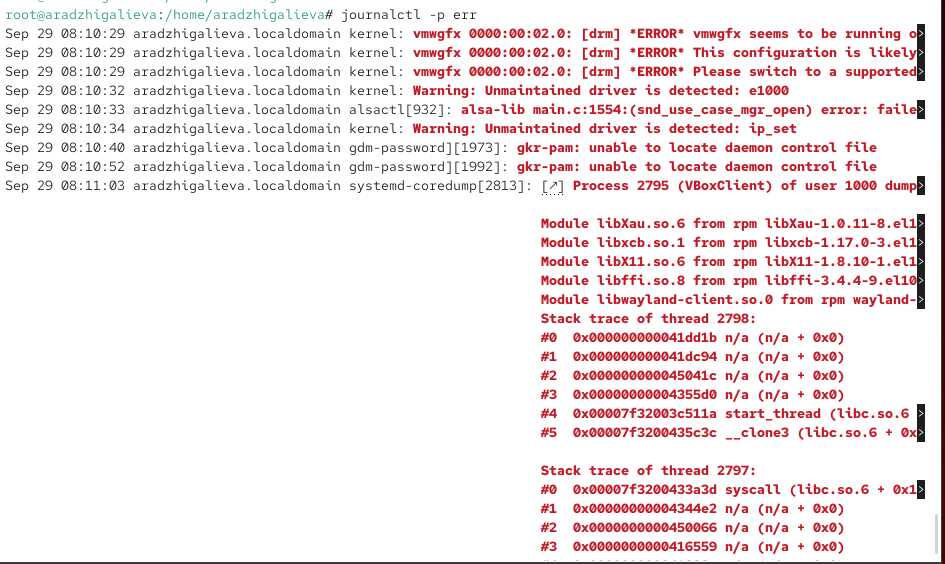


Рис. 14: Фильтрация сообщений по приоритету ошибок

Используя параметр --since yesterday, я просмотрела все события, начиная со вчерашнего дня.  
Журнал снова показал последовательность загрузки системы и параметры ядра.

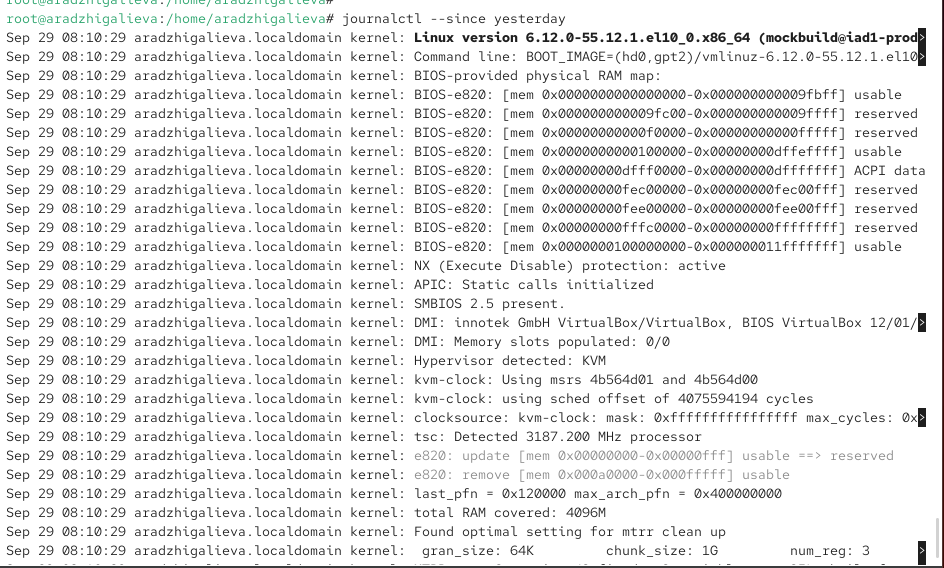


Рис. 15: События со вчерашнего дня

Затем я объединила фильтры и вывела только ошибки, зафиксированные со вчерашнего дня: journalctl --since yesterday -p err.  
Результат включает сообщения о проблемах с драйвером vmwgfx, PAM-авторизацией и сбоями VBoxClient.

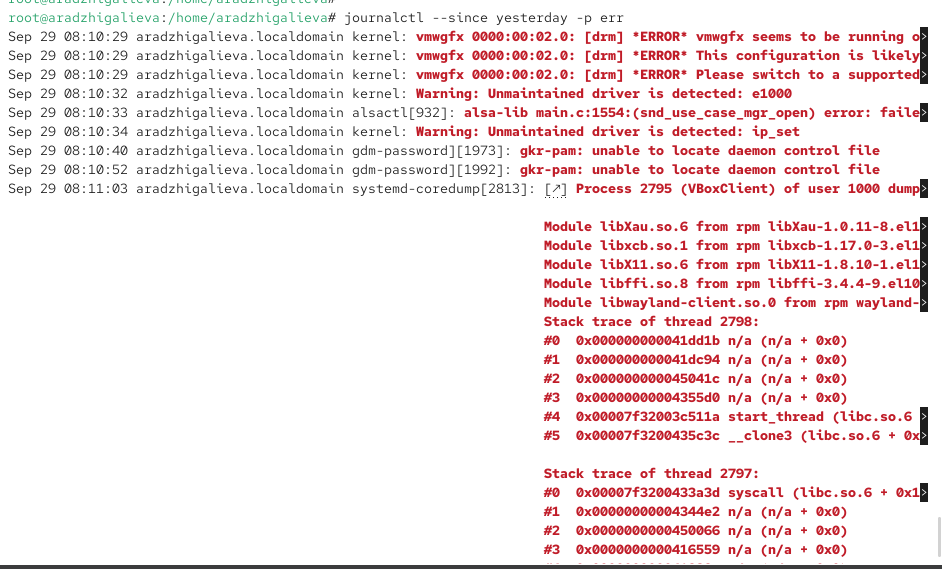


Рис. 16: Ошибки со вчерашнего дня

Для получения более подробных сведений я использовала режим journalctl -o verbose.  
На скриншоте видно, что каждая запись сопровождается расширенными атрибутами: временем, хостом, идентификатором процесса и приоритетом.



Рис. 17: Подробный вывод журнала

Я использовала команду journalctl \_SYSTEMD\_UNIT=sshd.service, чтобы просмотреть сообщения, относящиеся к службе sshd.  
В выводе отразились предупреждение об unset-переменной окружения, а также информация о том, что сервер слушает порт 22.

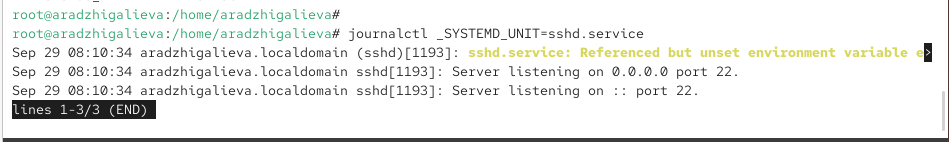


Рис. 18: Просмотр журнала sshd

## 2.4 Настройка постоянного журнала journald

По умолчанию система хранит журнал journald во временном каталоге /run/log/journal, и после перезагрузки записи теряются.  
Чтобы сделать журнал постоянным, я создала каталог /var/log/journal, назначила владельца и права доступа, а затем отправила сигнал USR1 процессу systemd-journald.



Рис. 19: Создание постоянного журнала journald

После этого я выполнила команду journalctl -b, чтобы убедиться, что журнал сохраняет записи с момента последней загрузки системы.  
В выводе отразились стандартные сообщения ядра и параметры запуска.

# 3 Контрольные вопросы

1. **Какой файл используется для настройки rsyslogd?**  
   Основной файл конфигурации — /etc/rsyslog.conf. Дополнительные правила могут храниться в каталоге /etc/rsyslog.d/.
2. **В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**  
   Сообщения об аутентификации обычно записываются в файл /var/log/secure.
3. **Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?**  
   По умолчанию ротация журналов выполняется еженедельно (настраивается через logrotate).
4. **Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?**  
   В конфигурацию нужно добавить строку:  
   \*.info /var/log/messages.info
5. **Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?**  
   Для этого используется команда:  
   journalctl -f
6. **Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?**  
   Используется команда:  
   journalctl \_PID=1 --since "09:00" --until "15:00"
7. **Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?**  
   Для этого используется команда:  
   journalctl -b
8. **Какая процедура позволяет сделать журнал journald постоянным?**  
   Нужно создать каталог /var/log/journal, назначить владельца и права:

* mkdir -p /var/log/journal   
  chown root:systemd-journal /var/log/journal   
  chmod 2755 /var/log/journal   
  killall -USR1 systemd-journald

# 4 Заключение

В ходе выполнения лабораторной работы я изучила принципы работы системных журналов Linux и научилась настраивать их хранение и просмотр.  
Я освоила использование команд journalctl и различных параметров фильтрации, научилась отслеживать ошибки и события в режиме реального времени, а также работать с приоритетами сообщений.  
Кроме того, я настроила службу rsyslogd для перенаправления логов веб-сервера Apache и добавила правила для записи отладочной информации в отдельный файл.  
Я также сделала журнал journald постоянным, чтобы записи сохранялись после перезагрузки системы.

Все выполненные действия позволили закрепить знания о механизмах логирования в Linux, а также получить практические навыки администрирования, которые необходимы для обеспечения контроля и диагностики работы системы.