Шаблон отчёта по лабораторной работе

Простейший вариант

Дмитрий Сергеевич Кулябов

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Задание

1. Продемонстрируйте навыки работы с журналом мониторинга событий в реальном времени .
2. Продемонстрируйте навыки создания и настройки отдельного файла конфигурации мониторинга отслеживания событий веб-службы.
3. Продемонстрируйте навыки работы с journalctl.
4. Продемонстрируйте навыки работы с journald.

# 3 Выполнение лабораторной работы

Сначала я открыл 3 терминала под пользователя root (рис. 1).

su -

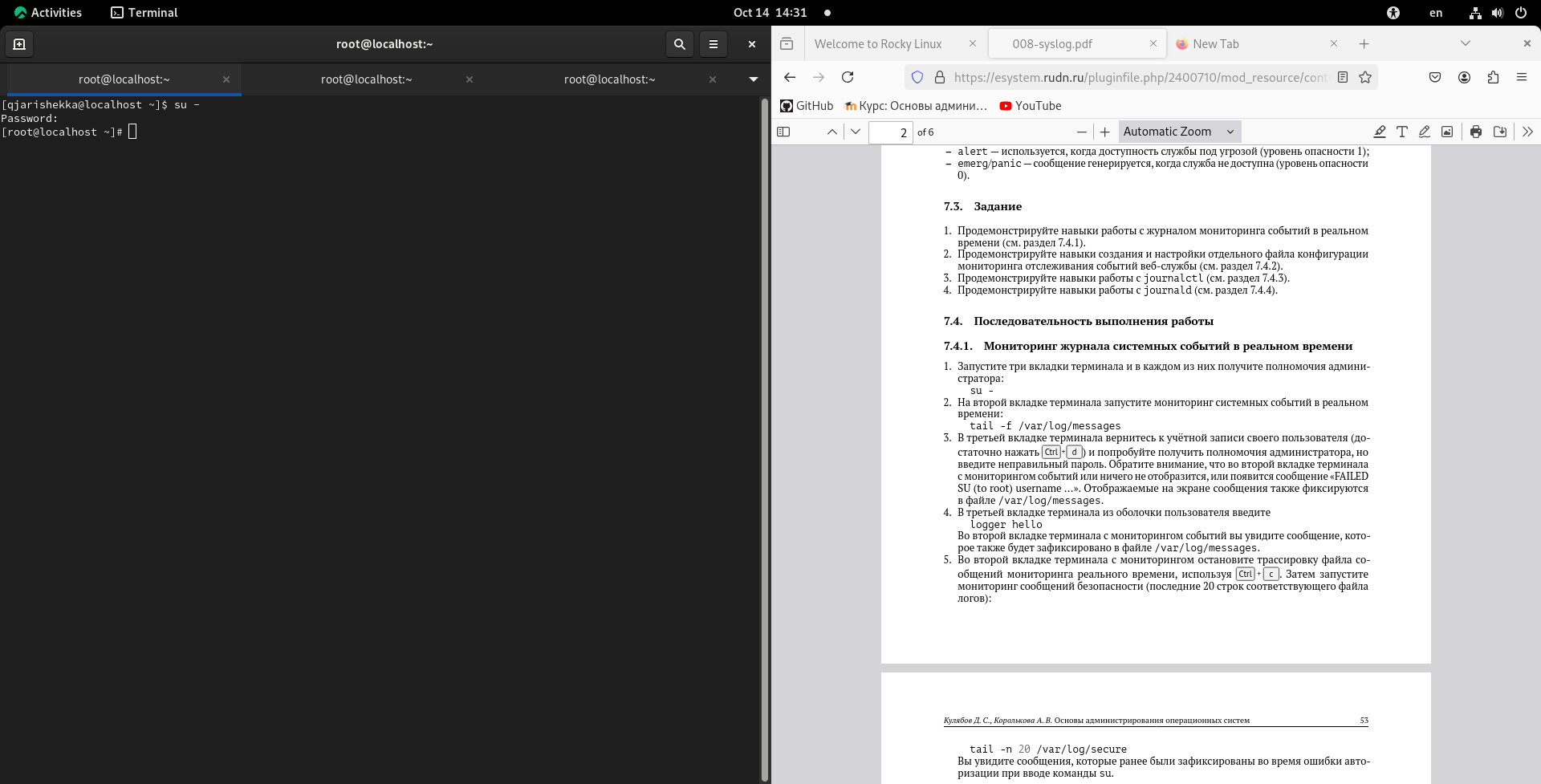


Рис. 1: терминалы

Потом во втором терминале я выполнил команду tail чтобы смотреть журнал в каталоге /var/log/messages (рис. 2).

tail -f var/log/messages

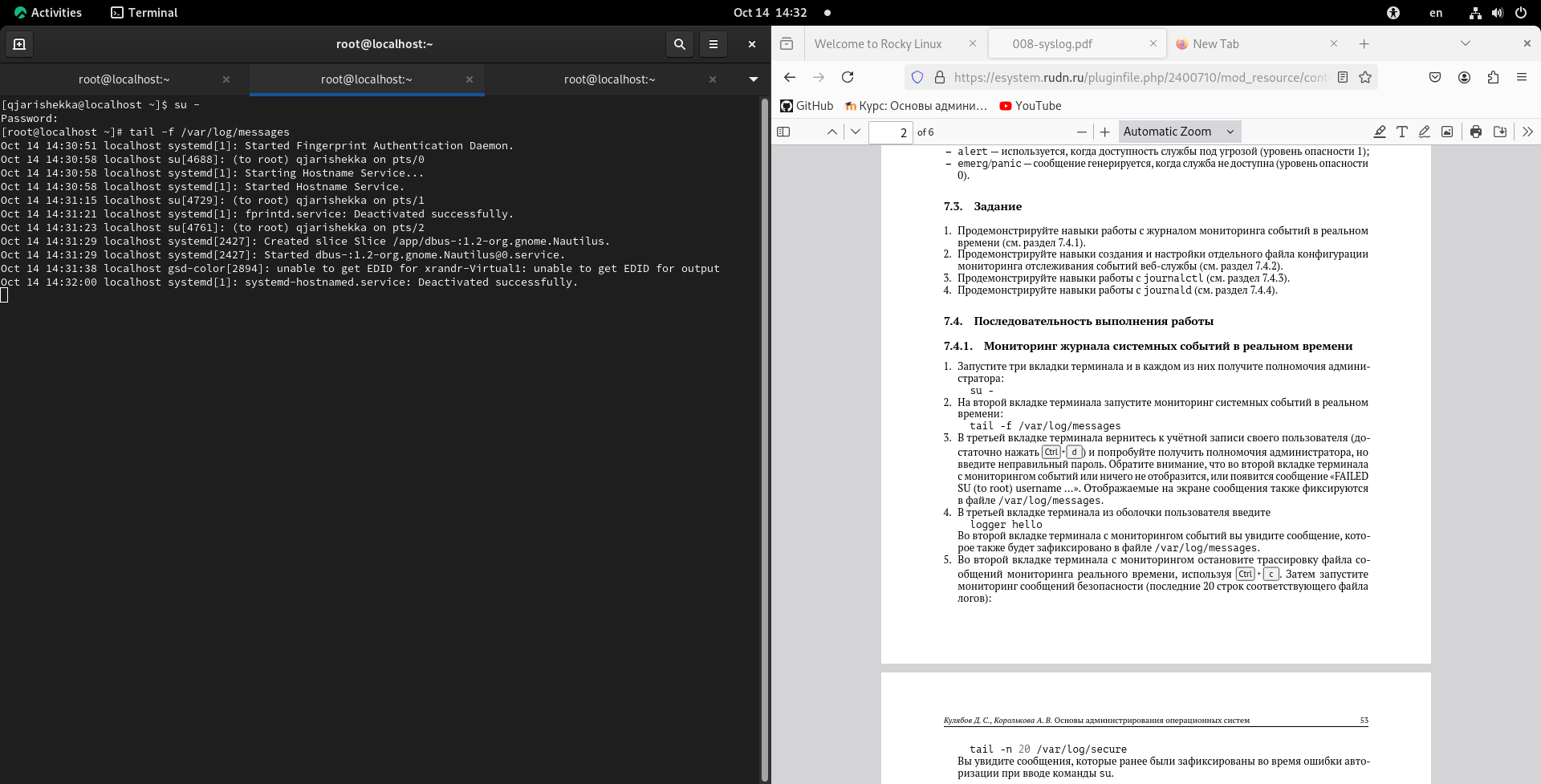


Рис. 2: журнал каталога /var/log/messages

Дальше в третем терминале я вышел из режима администратора нажая клавиши Ctrl+d (рис. 3).

Ctrl + d

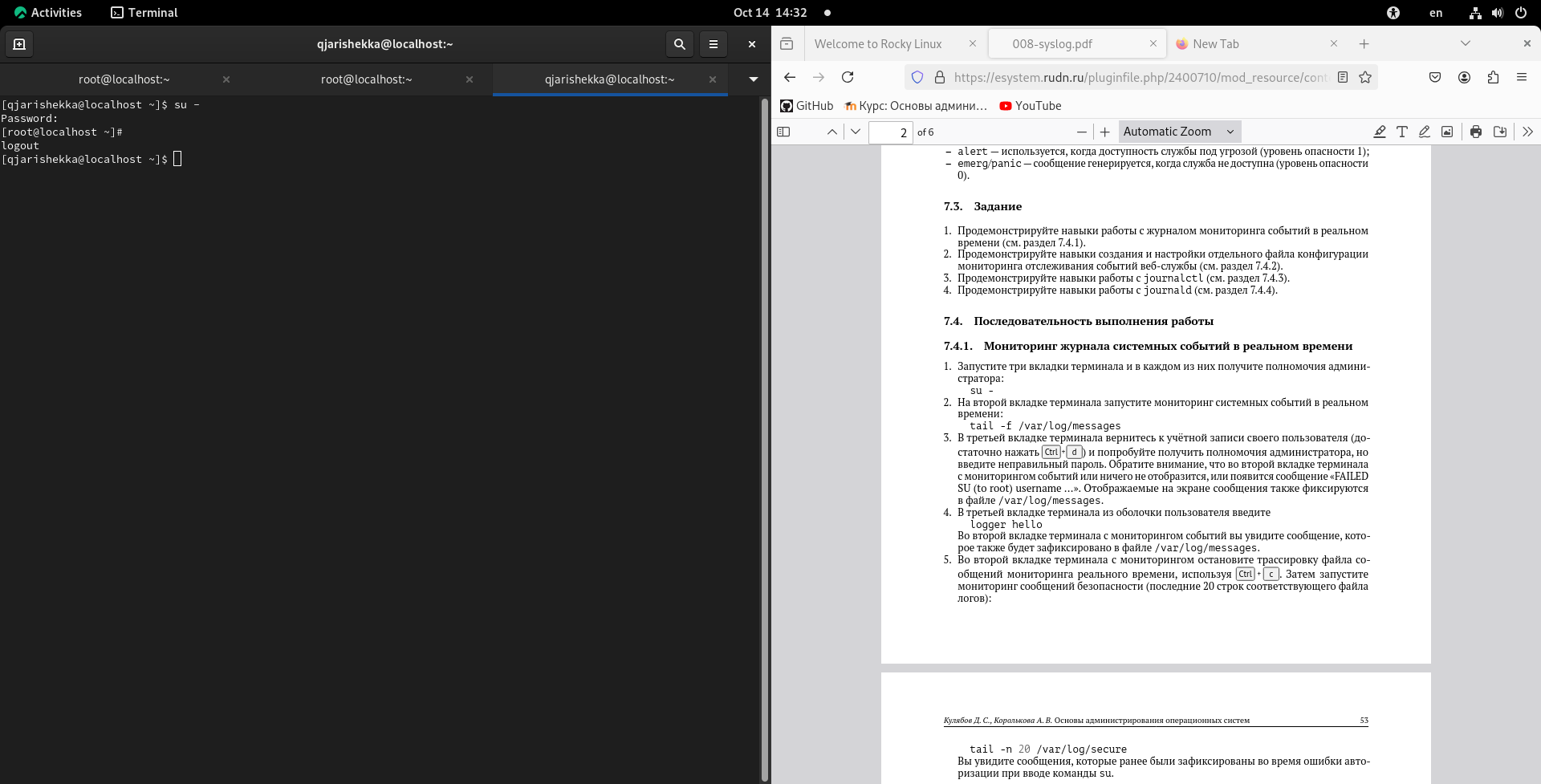


Рис. 3: выход из режима администратора

Затем я попытался входить в режим суперпользователя но с неправильным паролем не удаваясь (рис. 4).

su -  
 asdfasdlkfj

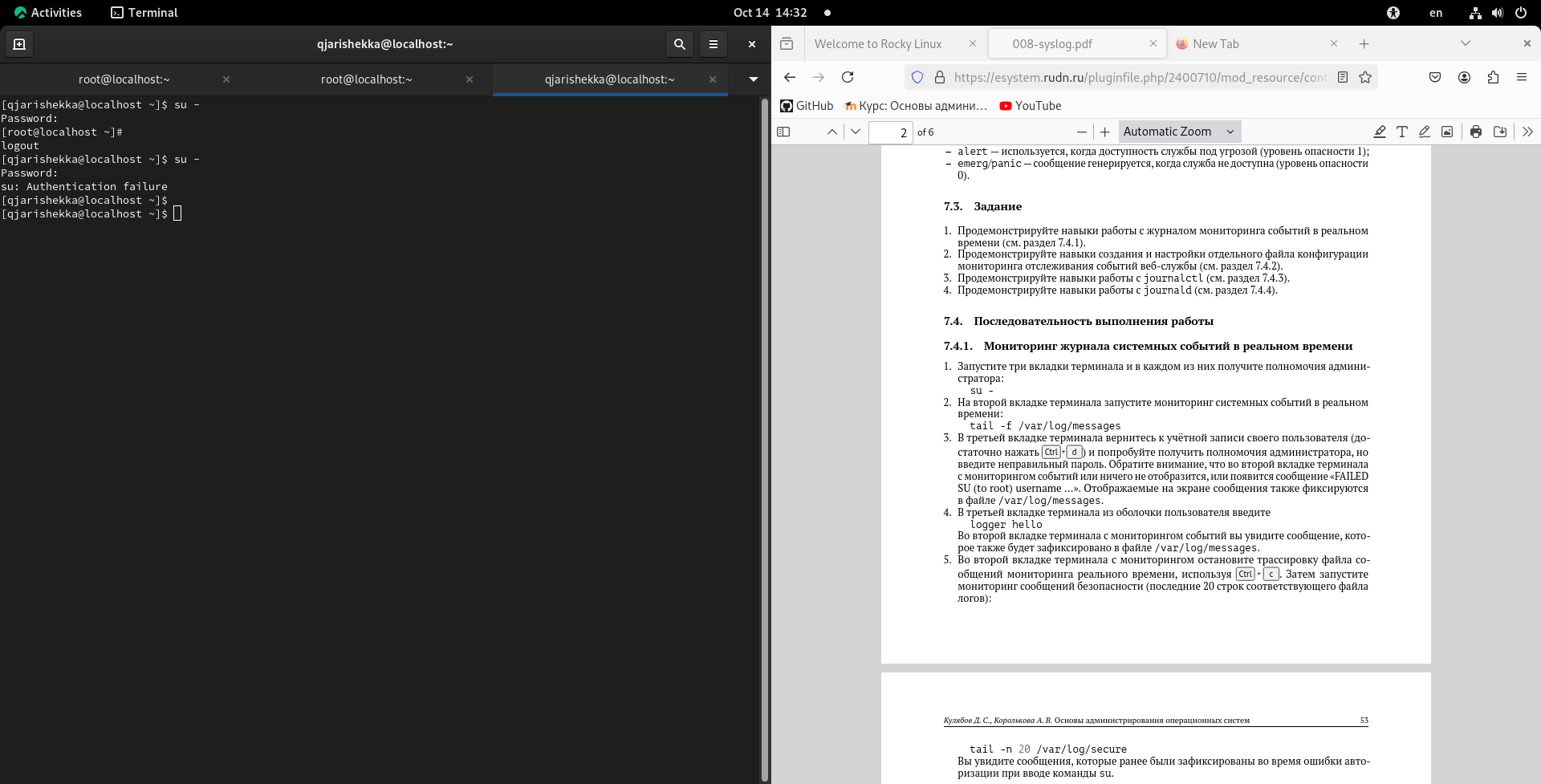


Рис. 4: неправильный пароль

Потом я вернулся в первую вкладку и там я смог смотерть сообщение “Failed su (to root) username….”(рис. 5).

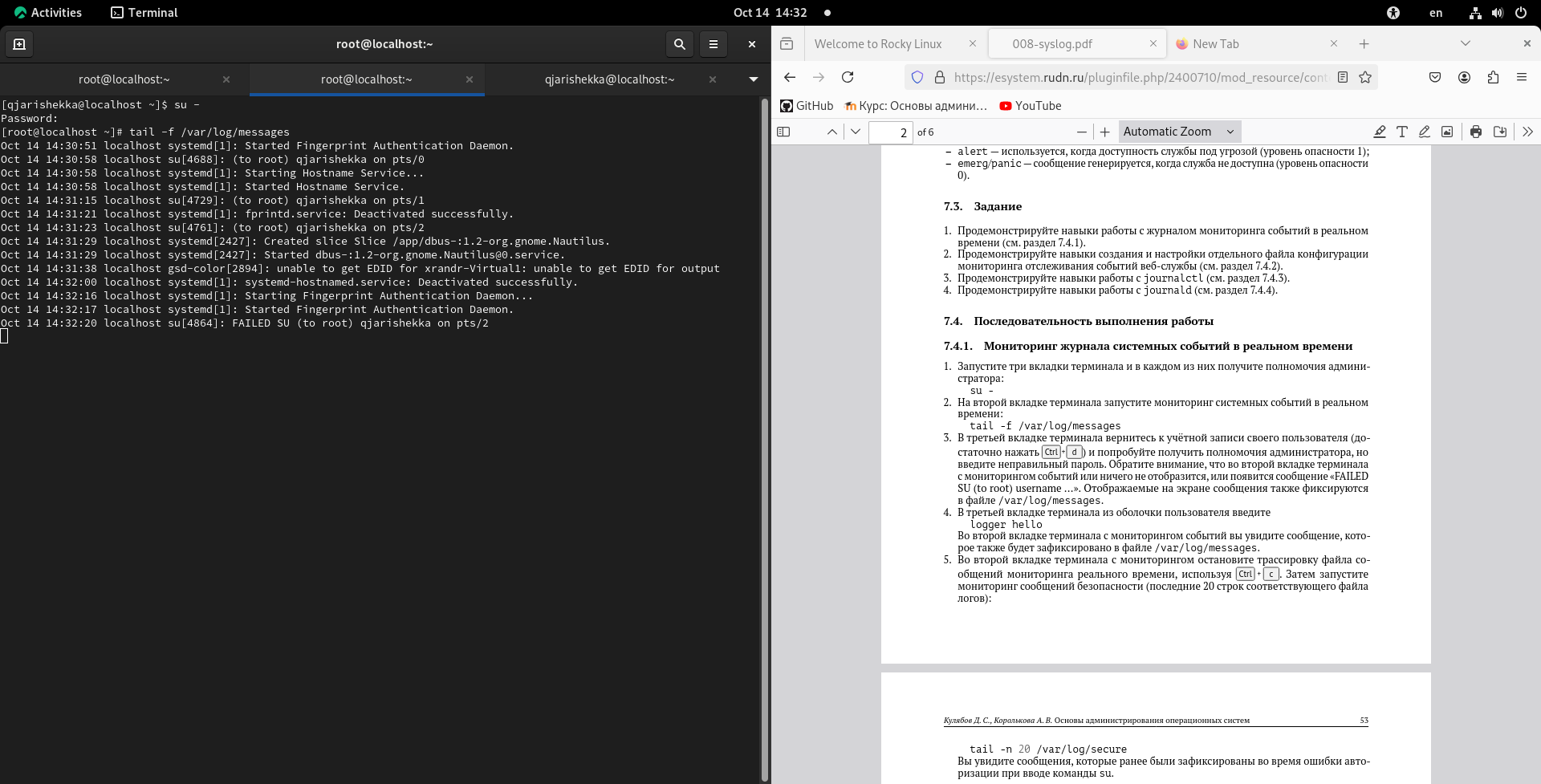


Рис. 5: сообщение о ошибке

Дальше я выполнил следующую комнаду (рис. 6):

logger hello

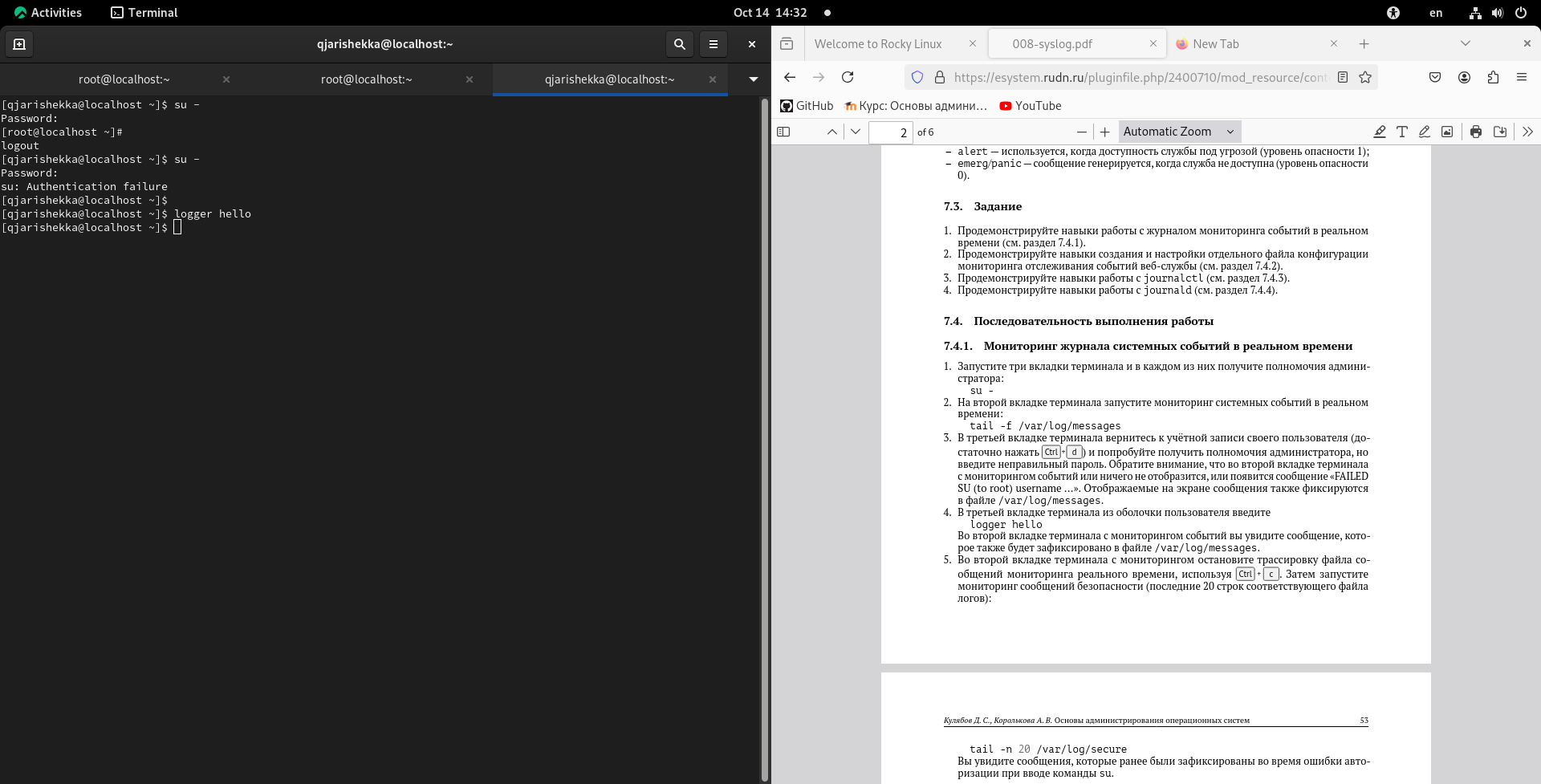


Рис. 6: logger hello

Тогда когда я вернулся во вторую вкладку там появились сообщение “hello” (рис. 7).

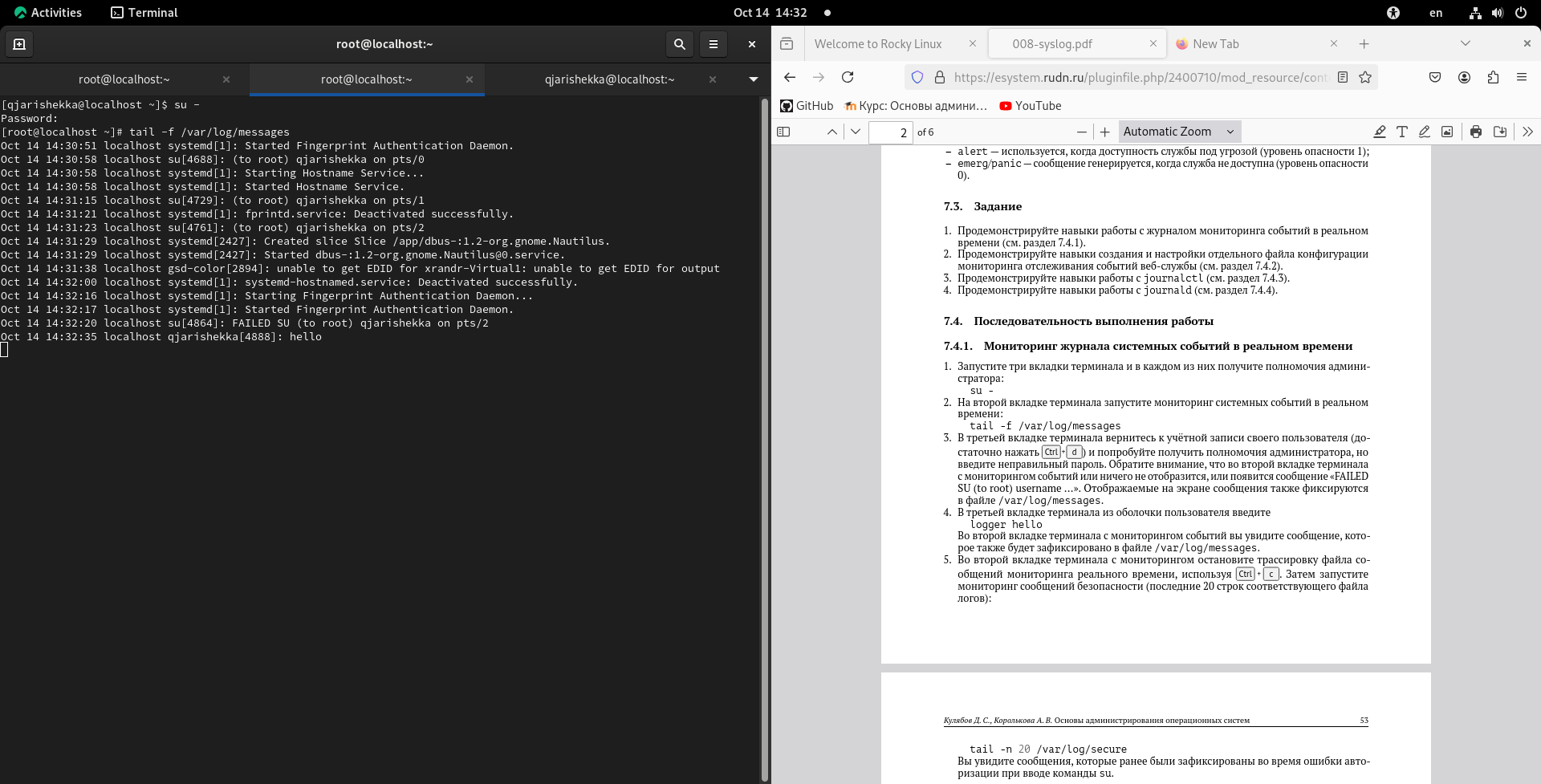


Рис. 7: сообщение hello

Потом я завершил просмотр журнала (рис. 8).

Ctrl + c

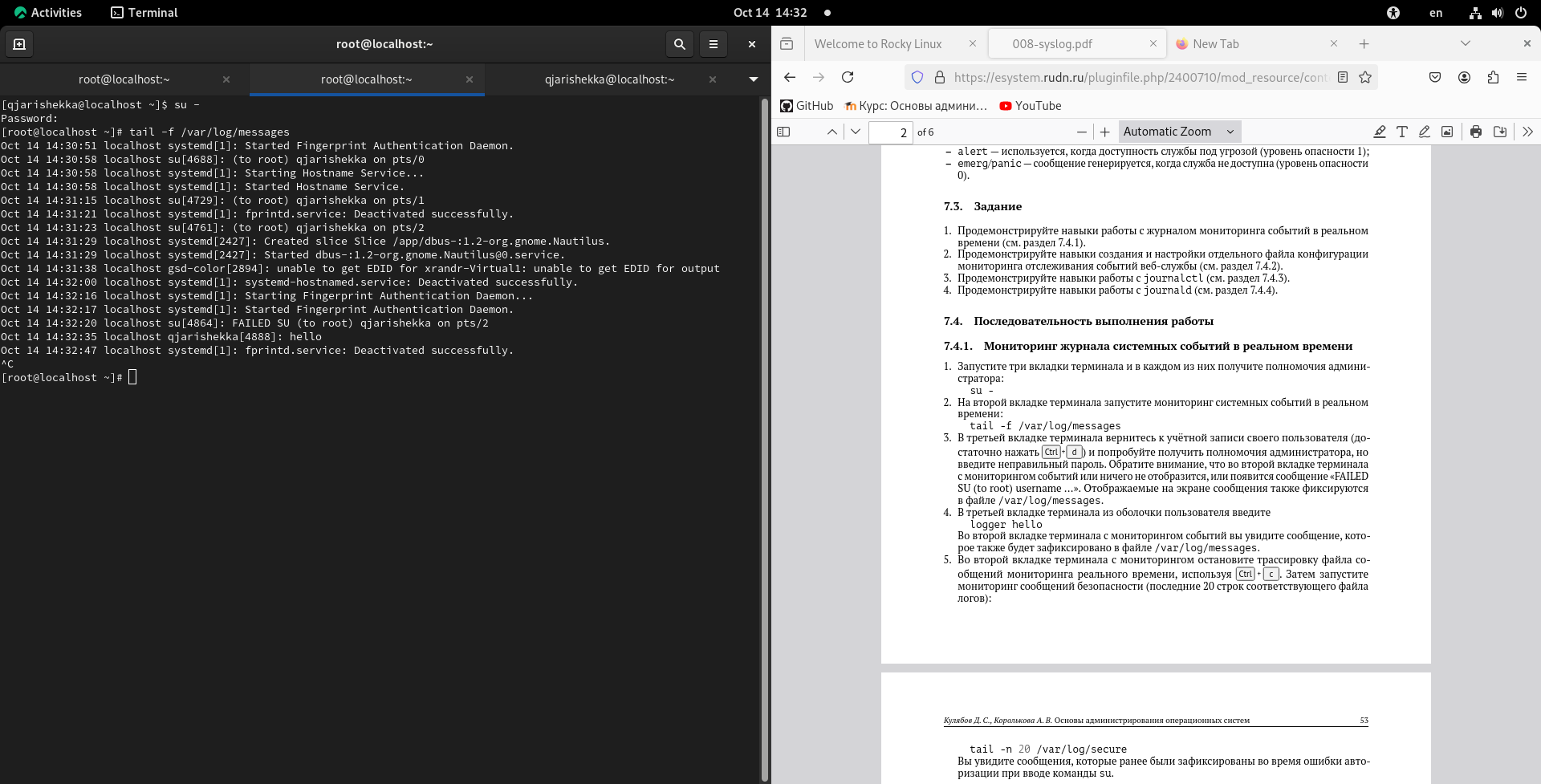


Рис. 8: завершение журнала

Дальше я запустил мониторинг сообщений безопасности (рис. 9).

tail -n 20 /var/log/secure

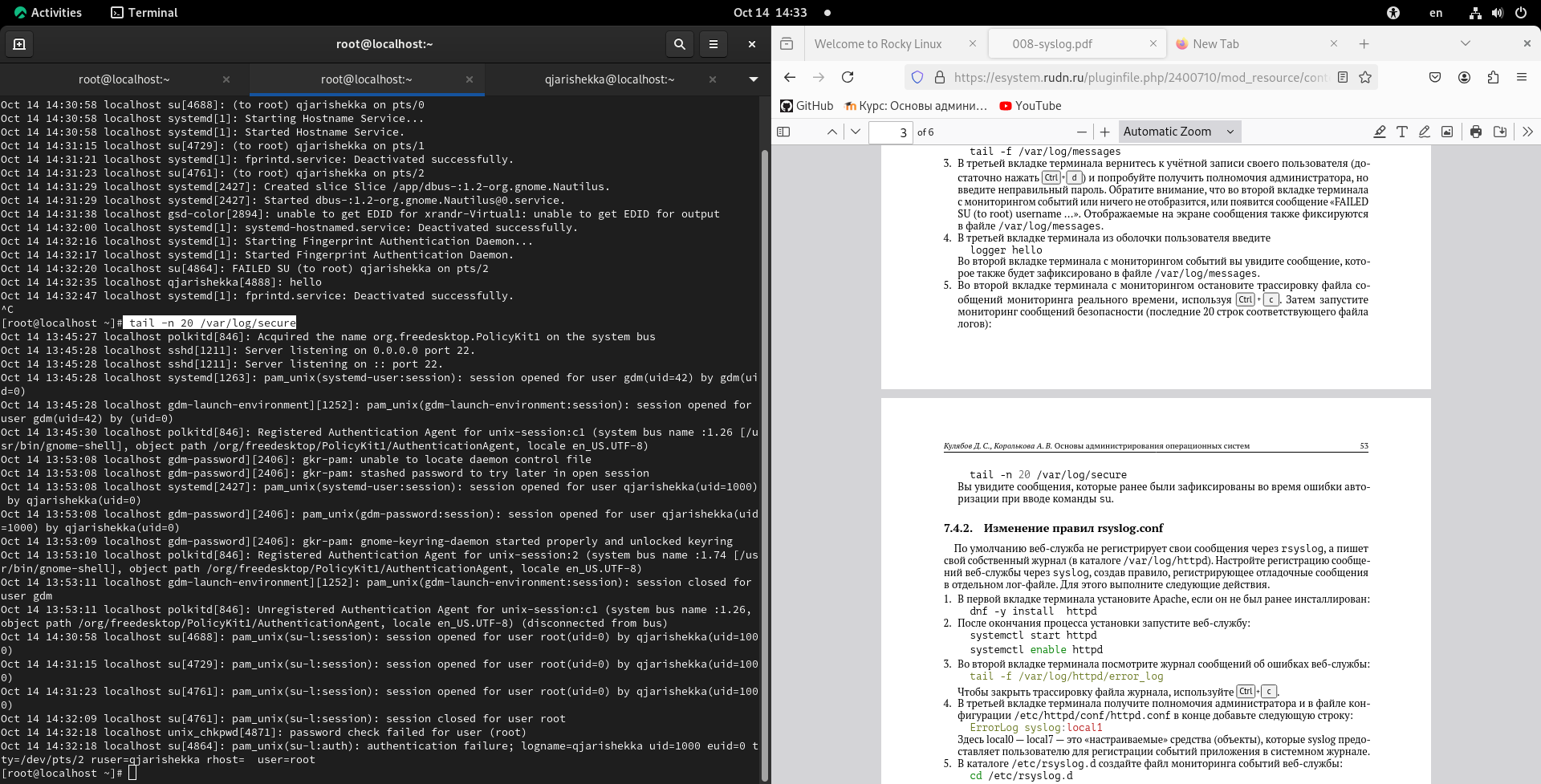


Рис. 9: мониторинг сообщений безопасности

Дальше я начал другую часть лабораторной работы.

Сначала я установил утилит httpd (рис. 10).

dnf -y install httpd

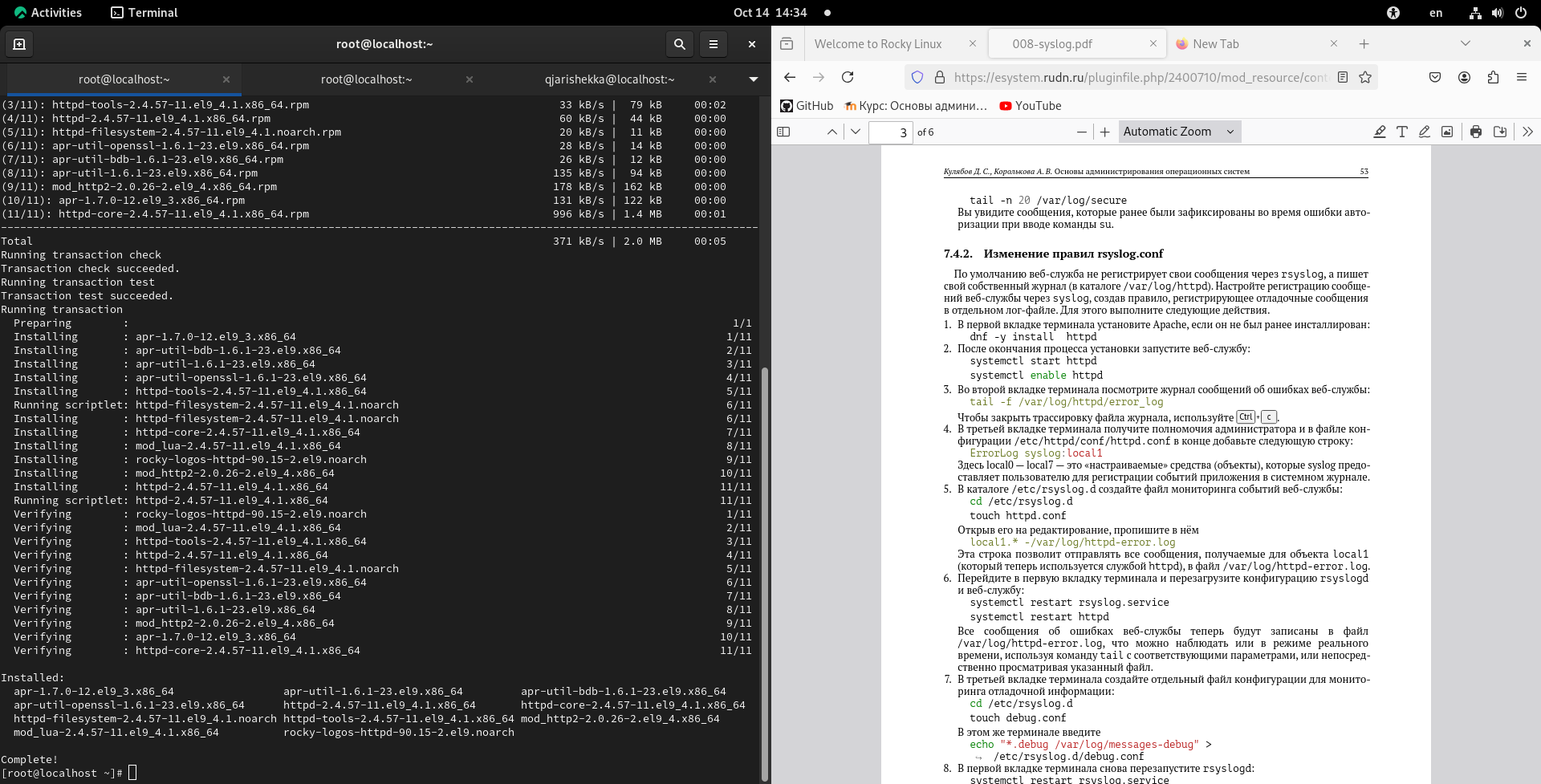


Рис. 10: установка httpd

Потом я инициализировал его (рис. 11).

systemctl start httpd  
 systemctl enable httpd

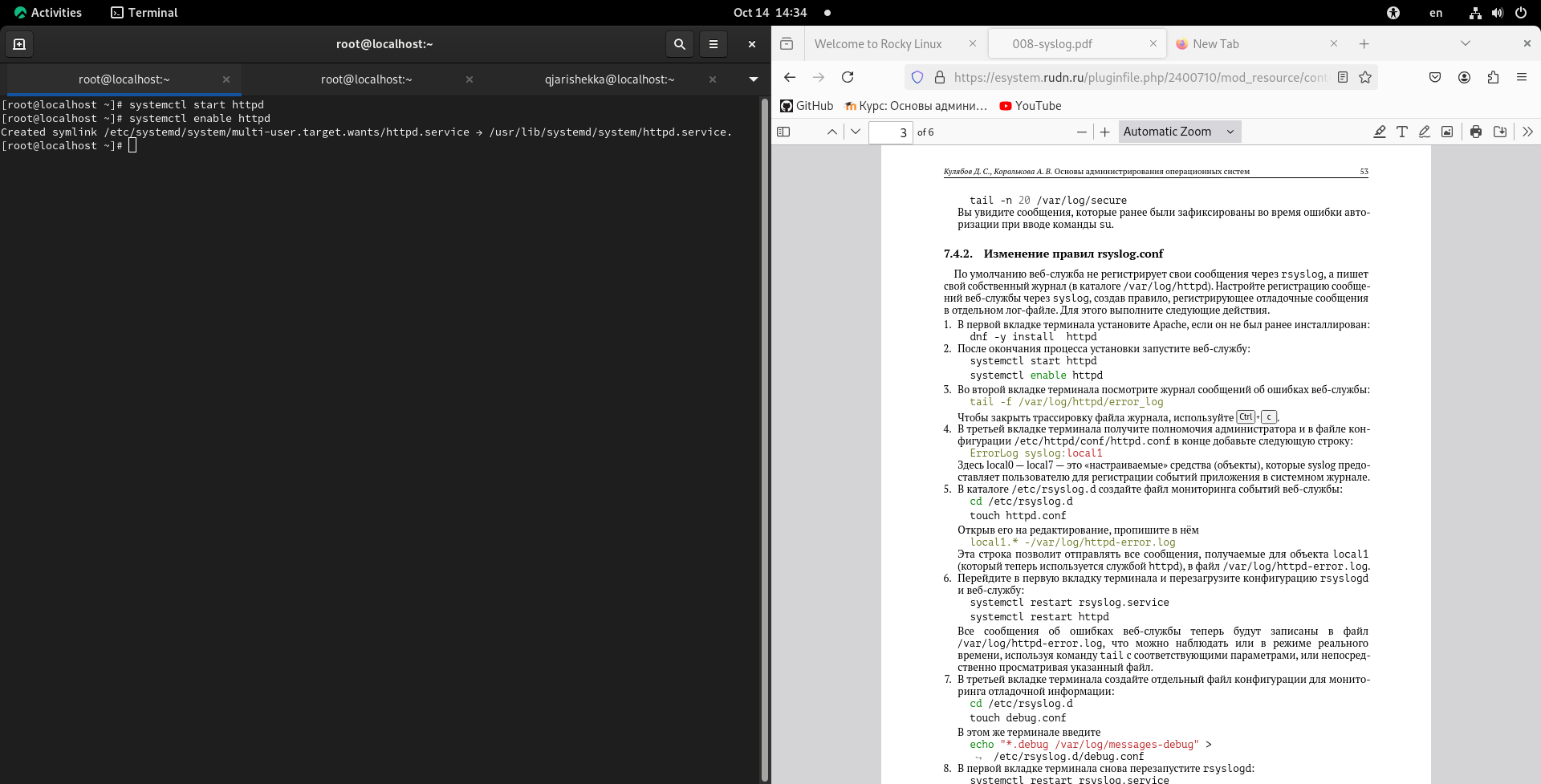


Рис. 11: запуск утилита

Потом во второй вкладке терминала я смотрел журнал сообщений об ошибах веб-службы (рис. 12).

tail -f /var/log/httpd/error\_log

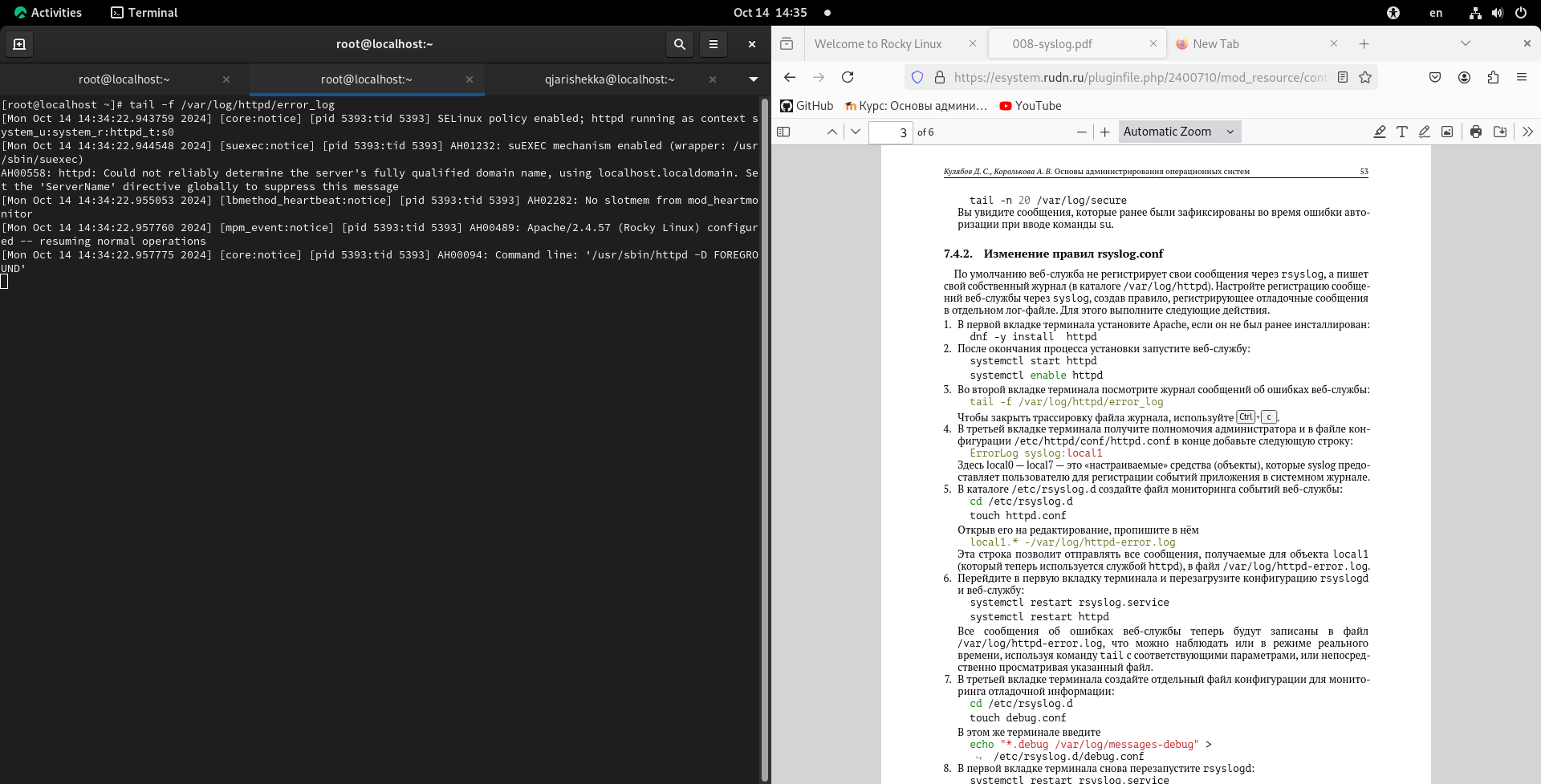


Рис. 12: журнал сообщений об ошибах

Потом я перешел в третьюю вкладку и получил полномочия администратора (рис. 13). и в файле /etc/httpd/conf/httpd.conf я добавил одну строку (рис. 14).

su -  
 vim /etc/httpd/conf/httpd.conf  
 Errorlog syslog:local1  
 :wq

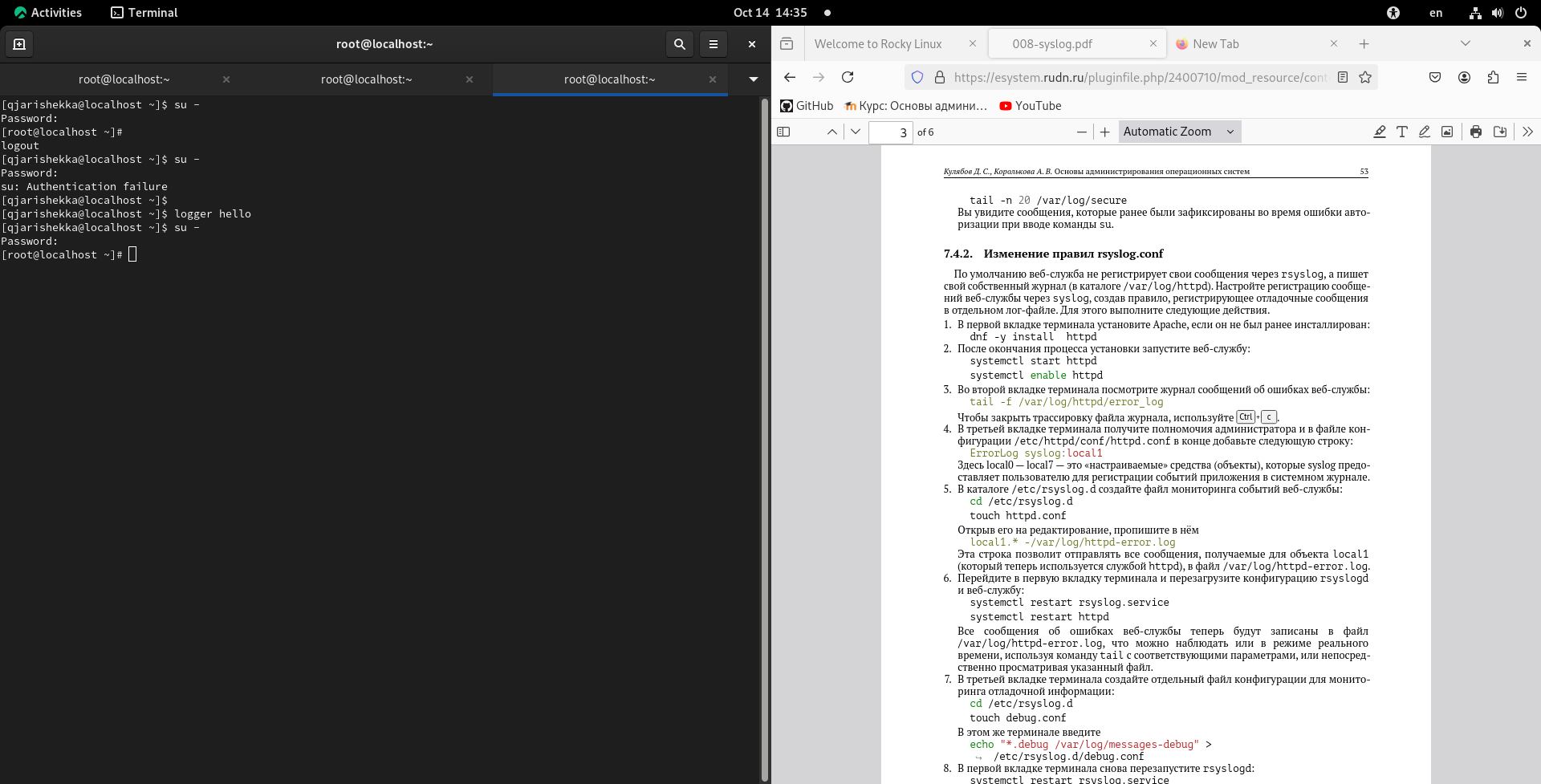


Рис. 13: пользователь root

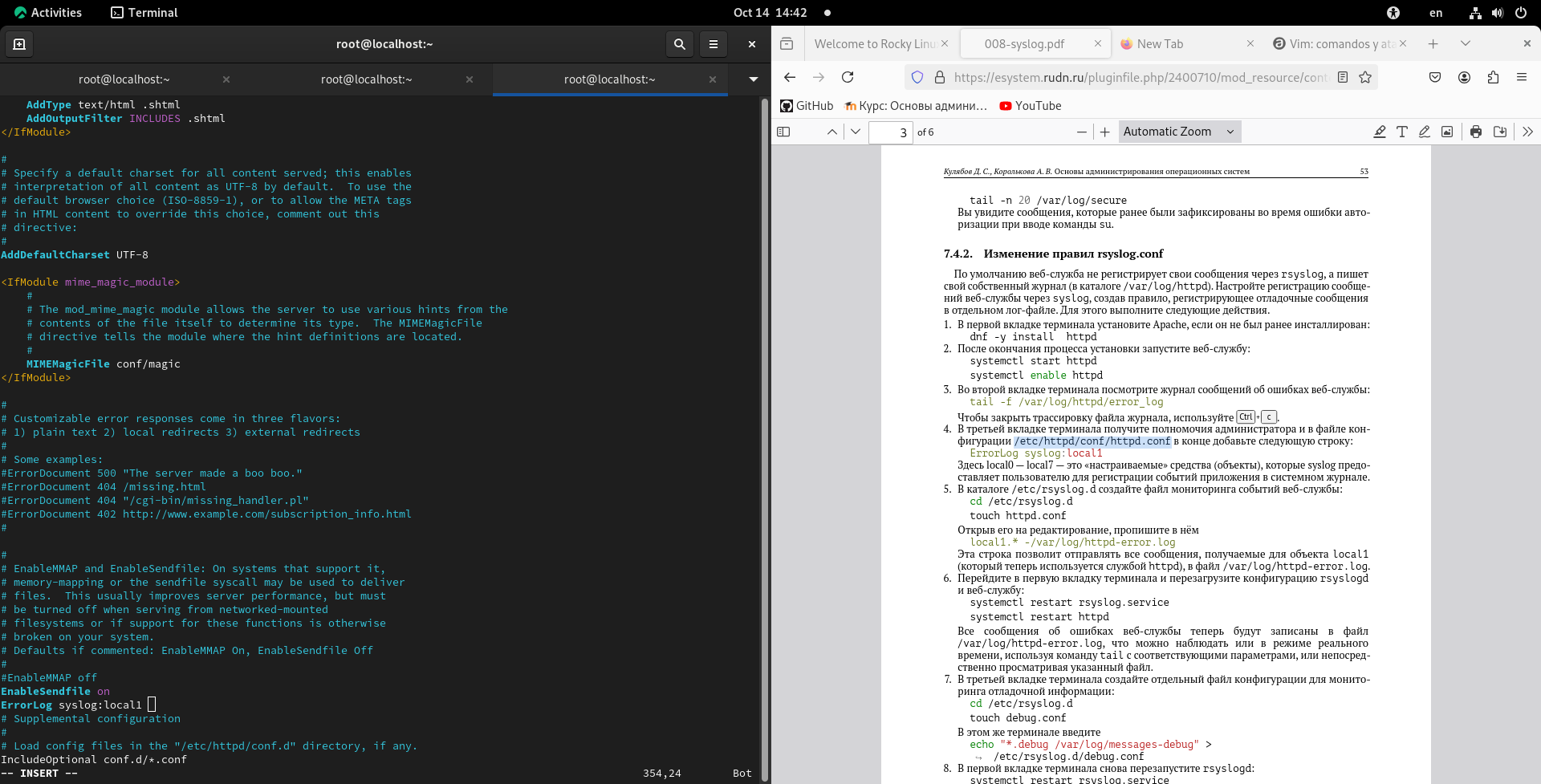


Рис. 14: изменение файла /etc/httpd/conf/httpd.conf

Потом я перешел в друкой каталог /etc/rsyslog.d и создал один файл “httpd.conf” (рис. 15).

cd /etc/rsyslog.d  
 touch httpd.conf

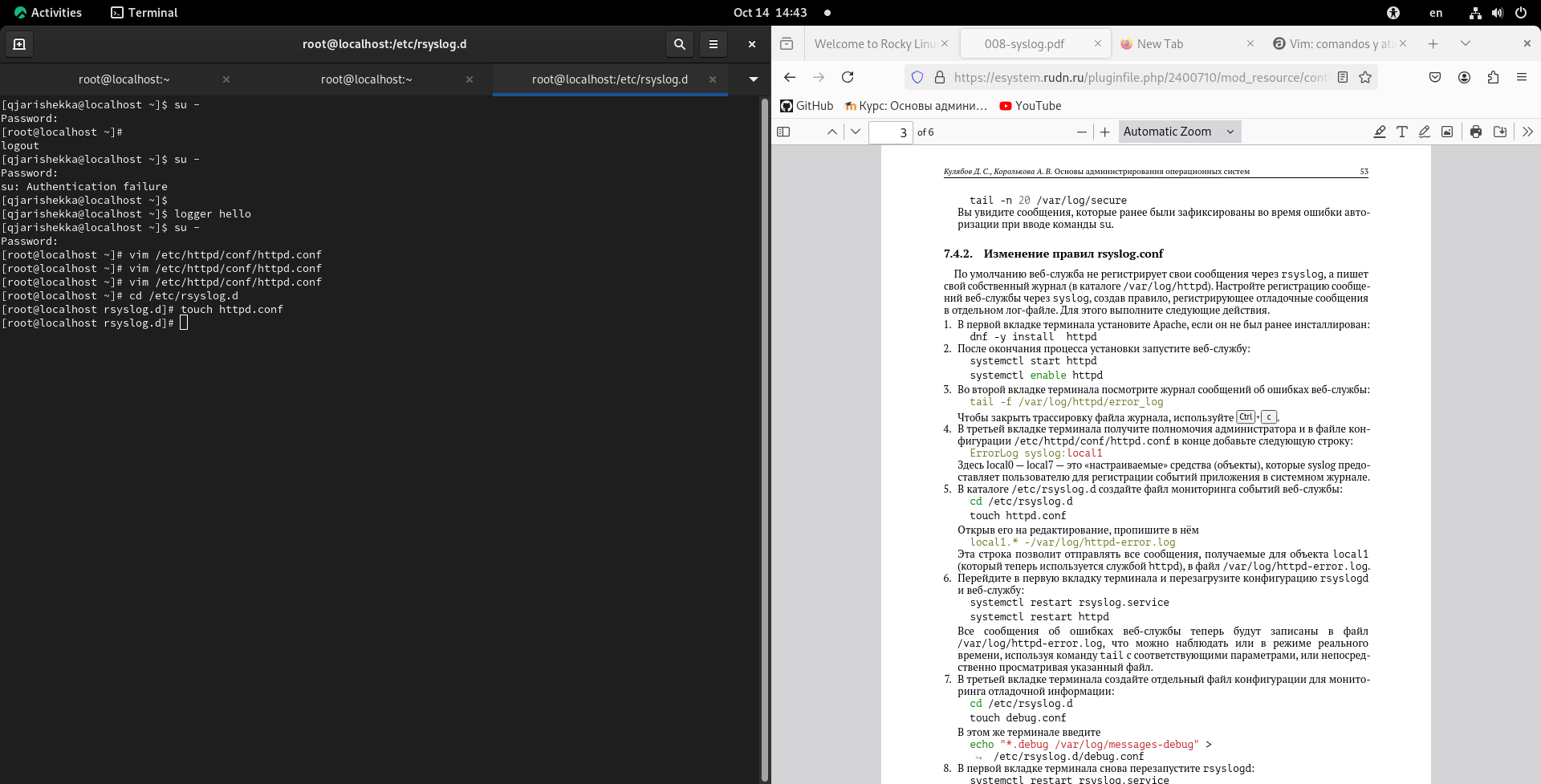


Рис. 15: httpd.conf

В этом файле я добавил одну строку и сохранил его (рис. 16).

mcedit httpd.conf  
 local1.\* -/var/log/httpd-error.log  
   
 f10

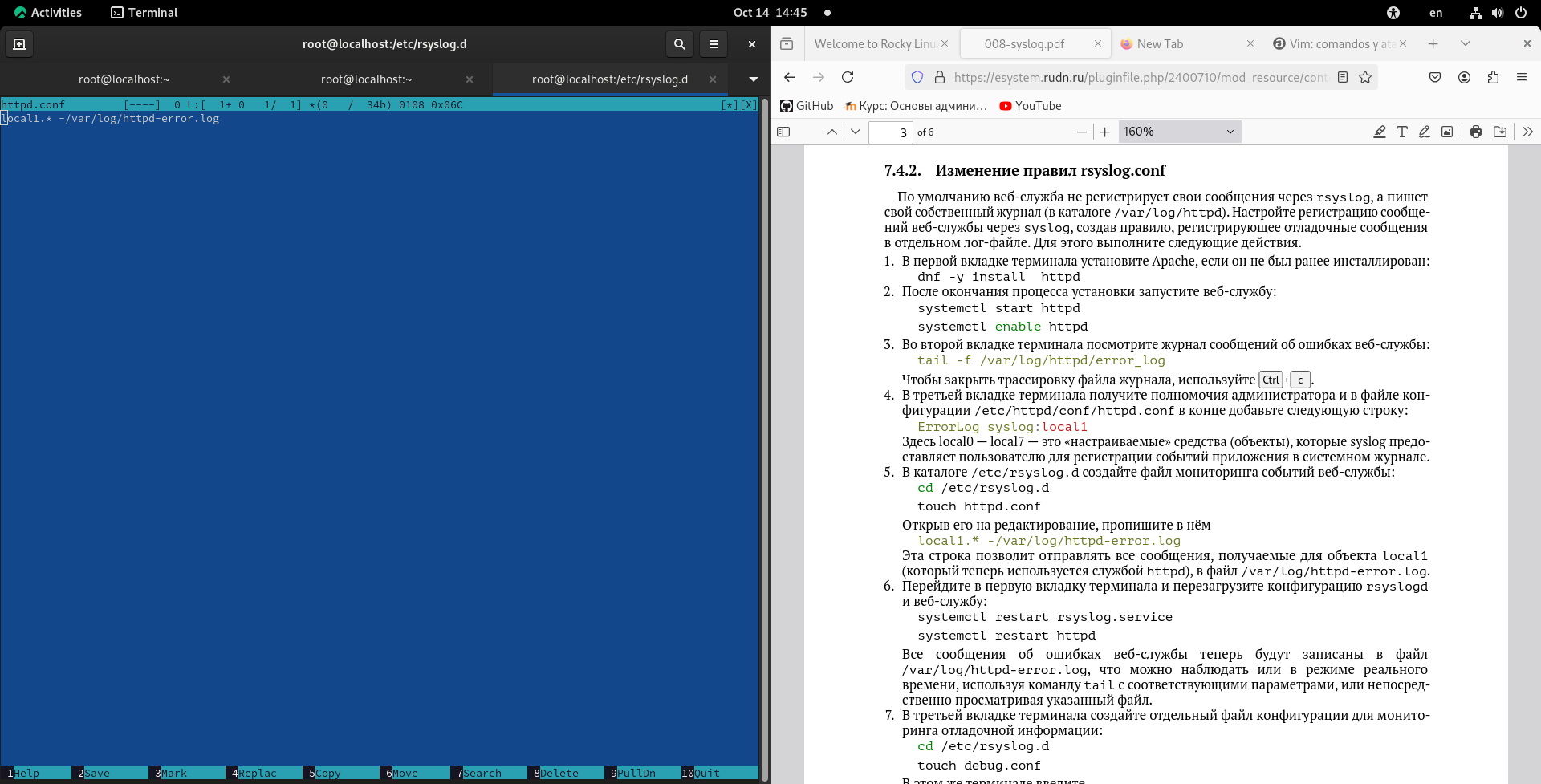


Рис. 16: новая строка

Дальше я перешел в первую вкладку терминала и перезагрузил конфигурацию rsyslogd и веб-службу (рис. 17).

systemctl restart rssyslog.service  
 systemctl restart httpd

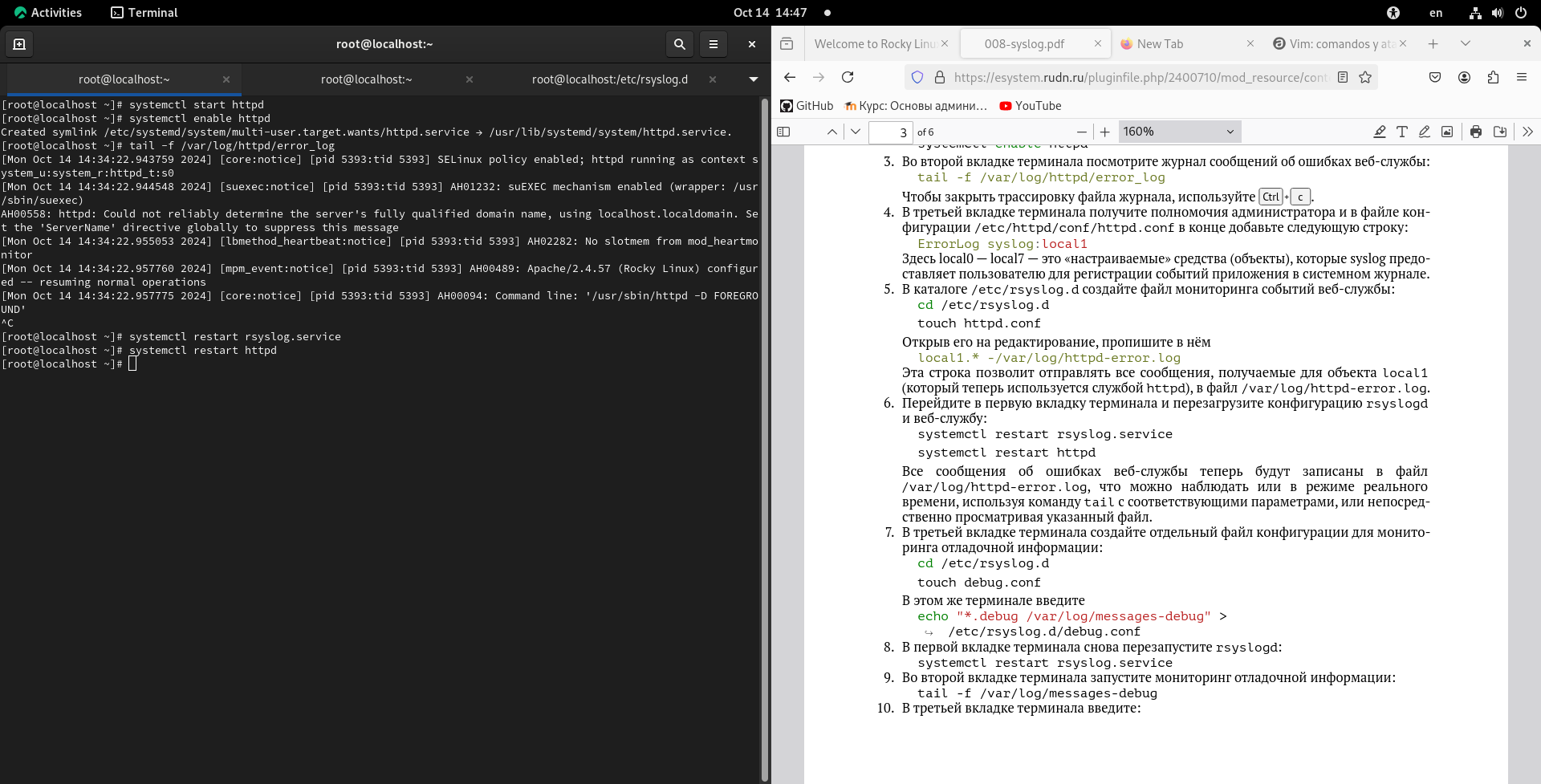


Рис. 17: перезагрузка конфигурацию rsyslogd и веб-службу

Затем я перешел в третьюю вкладку и создал отдельный файл конфигурации для мониторинга отладочной информации (рис. 18).

cd /etc/rsyslog.d  
 touch debug.conf  
 echo "\*.debug /var/log/messages-debug" > /etc/rsyslog.d/debug.conf

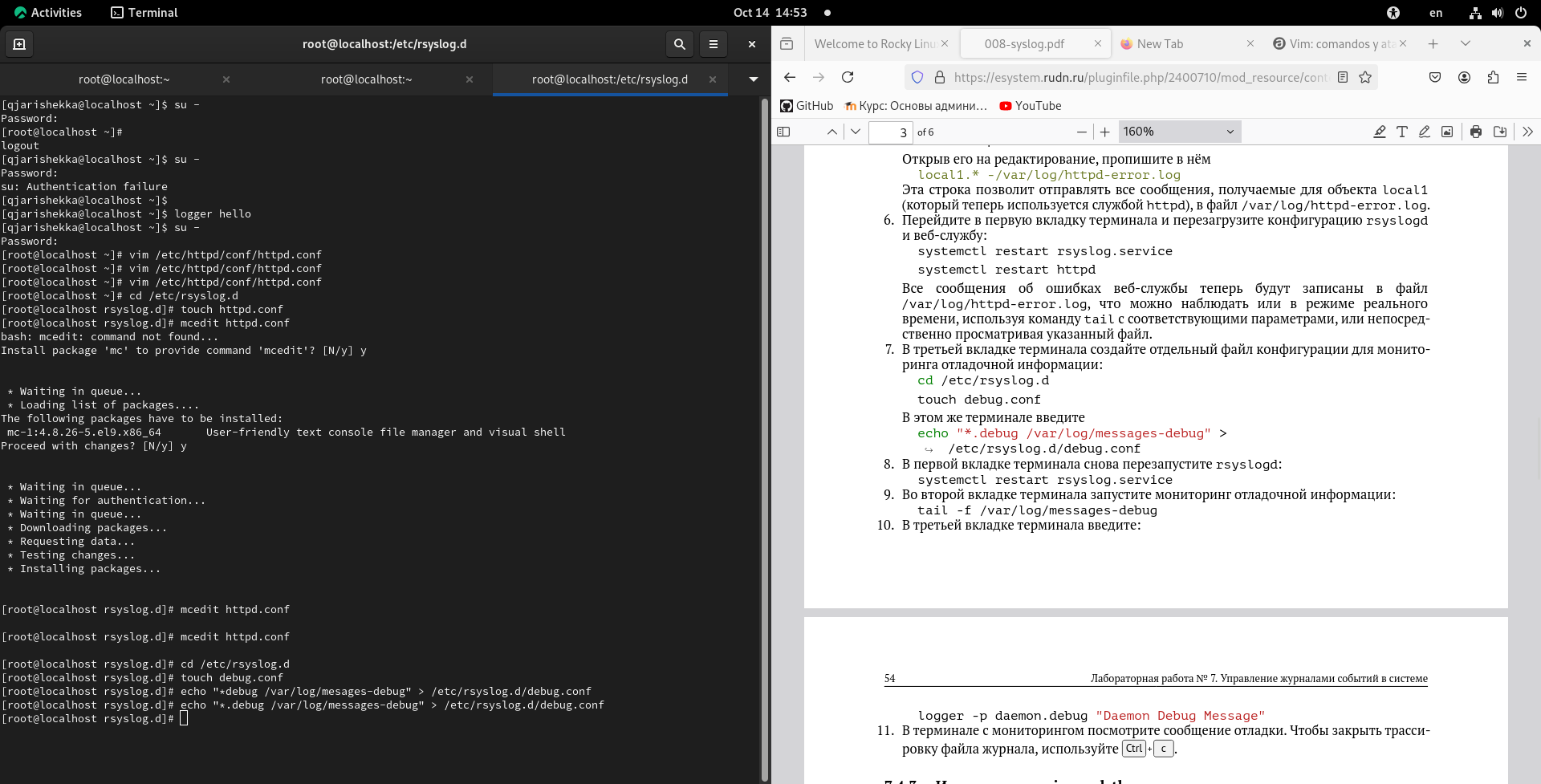


Рис. 18: конфигурация для мониторинга отладочной информации

Потом еще раз в первой вкладке терминала снова перезапустил rsyslogd (рис. 19).

systemctl restart rsyslog.service

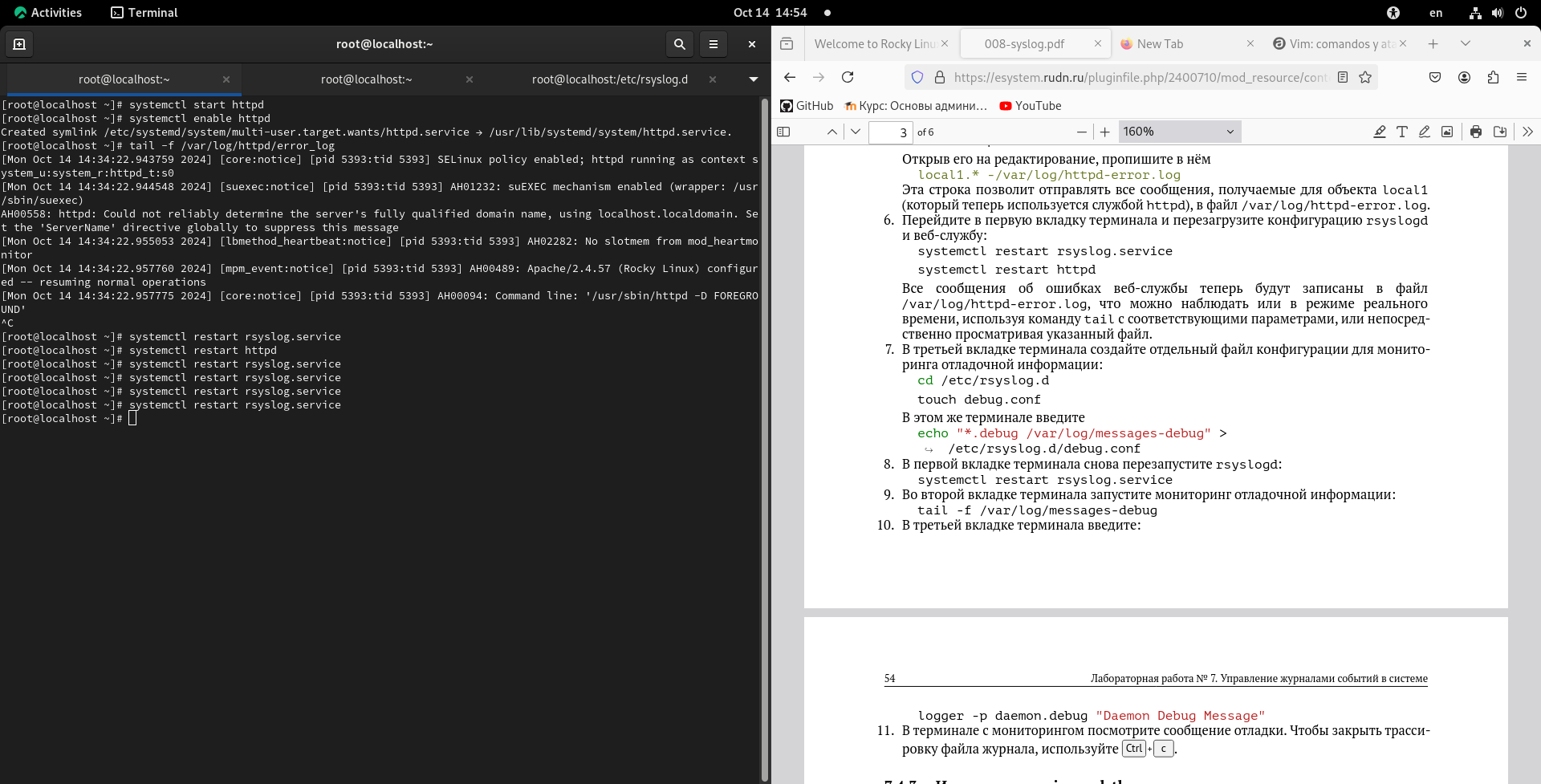


Рис. 19: перезапуск rsyslogd

Затем во второй вкадке терминала я запустил мониторинг отладочной информации (рис. 20).

tail -f /var/log/messages-debug

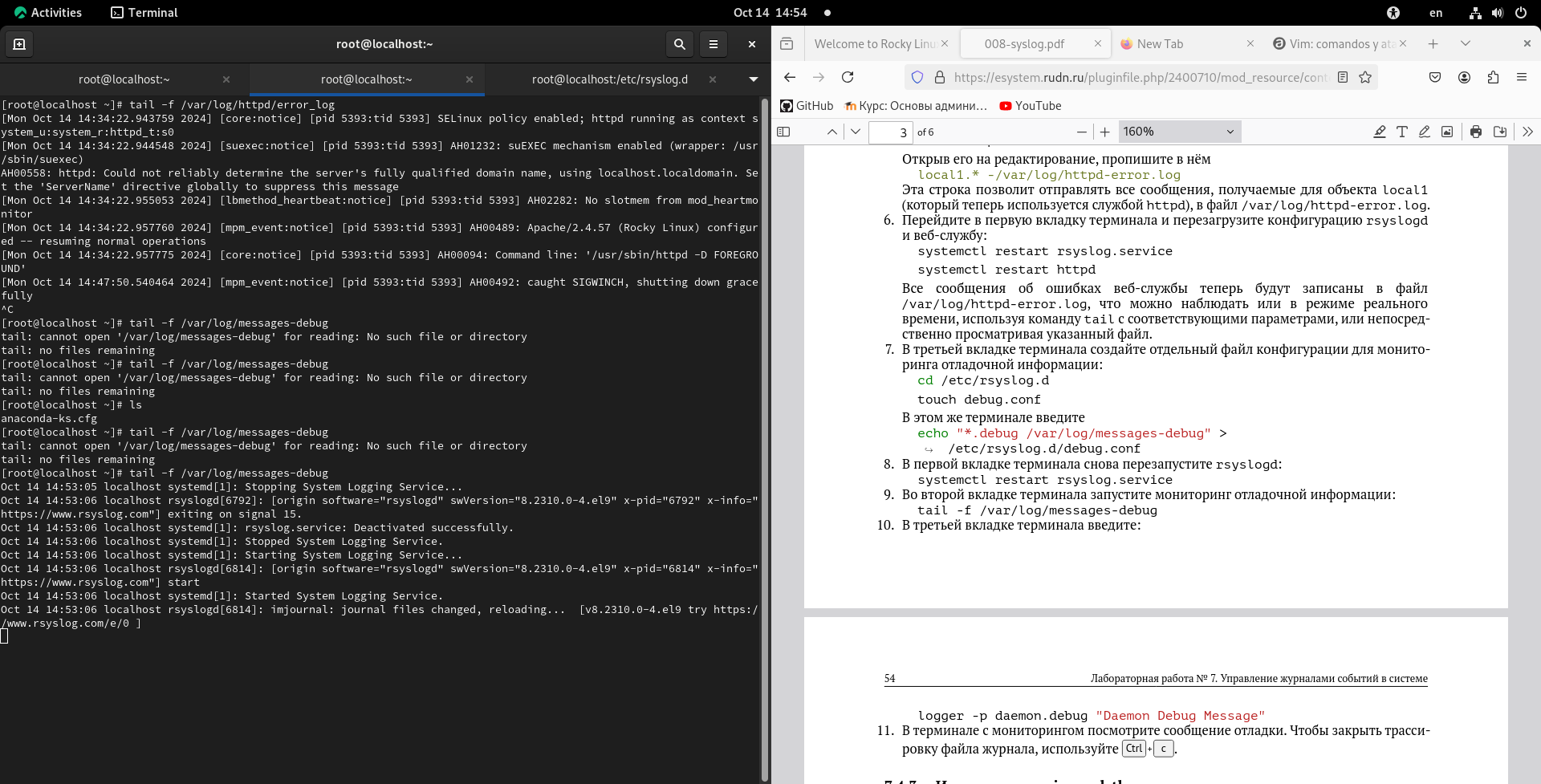


Рис. 20: мониторинг отладочной информации

Потом я в третьей вкладке терминала выполнил команду logger (рис. 21).

logger -p daemon.debug "Daemon Debug Message

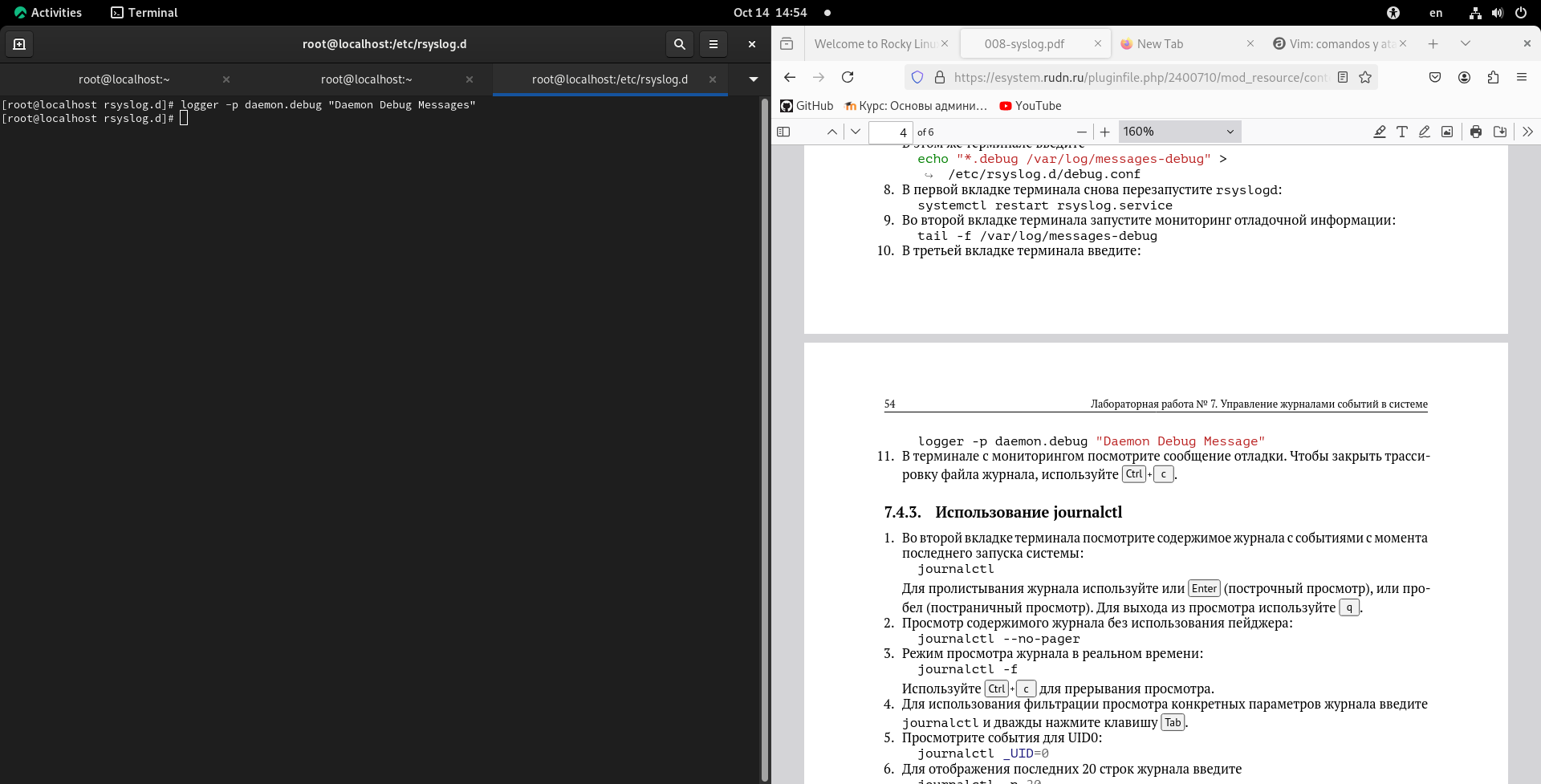


Рис. 21: logger

Затем я закрыл трассиворку файла журнала во второй вкладке (рис. 22).

Ctrl + c

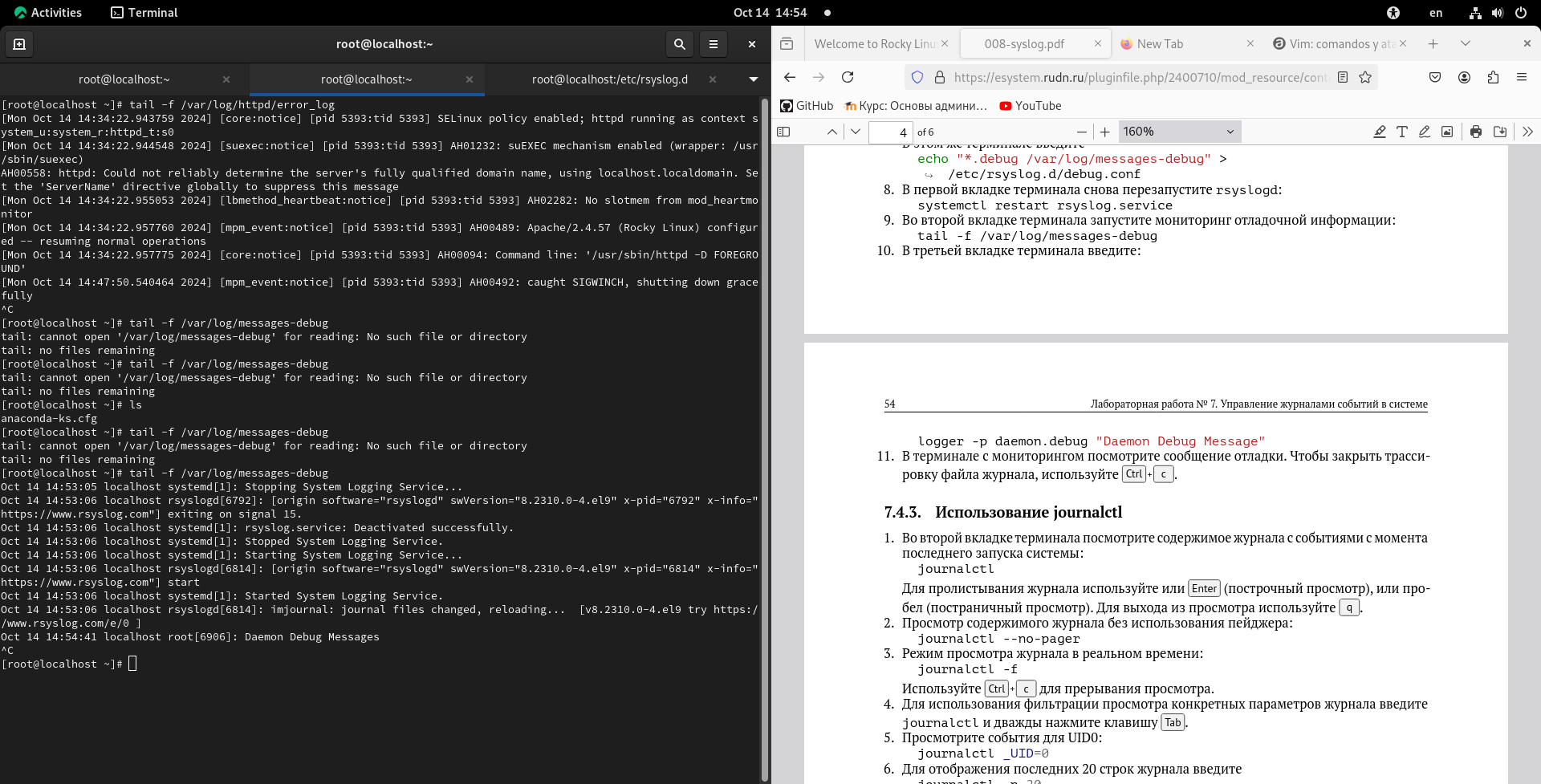


Рис. 22: закрытие трассироваки файла журнала

(рис. 23).

|  |
| --- |
| Рис. 23: Название |

Рис. 23: Название

# 4 Выводы

После выполнения лабораторной работы я смог смотреть работу команд tail и journalctl чтобы смотреть журналы, которые сохраняют все выполнённые процессы и как настройт его.

# Список литературы