

# **Отчёт о лабораторной работе**

**Лабораторная работа №7**

Приходько Иван Иванович

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Задание</b>	<b>6</b>
<b>3 Выполнение лабораторной работы</b>	<b>7</b>
<b>4 Выводы</b>	<b>11</b>
<b>5 Ответы на контрольные вопросы</b>	<b>12</b>

# **Список иллюстраций**

3.1 Вывод сообщений в журнале действий . . . . .	7
3.2 Изменение файла httpd.conf . . . . .	8
3.3 Вывод сообщений через файл . . . . .	8
3.4 Вывод сообщений черезиной способ . . . . .	9
3.5 Открытие сордержимого терминала . . . . .	9
3.6 Открытие сордержимого терминала . . . . .	9
3.7 Открытие сордержимого терминала . . . . .	10
3.8 Сорздание инастройка каталога для записи журнала . . . . .	10

# **Список таблиц**

# **1 Цель работы**

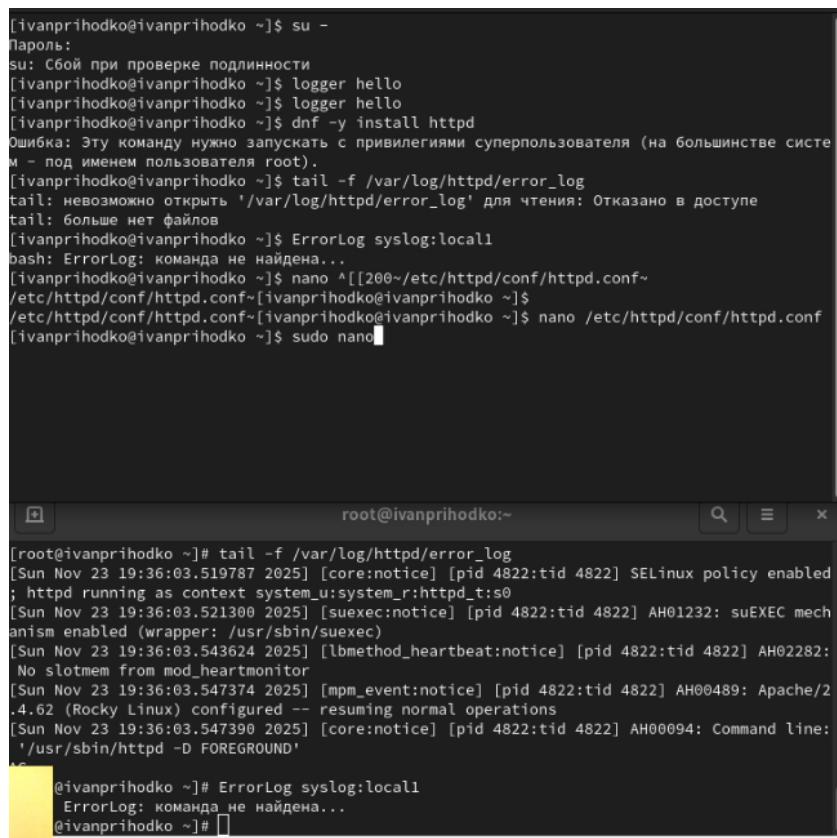
Получить навыки работы с журналами мониторинга различных событий в системе.

## **2 Задание**

Поработать с журналом мониторинга событий в системе

### 3 Выполнение лабораторной работы

Для начала запустим журнал событий в другом терминале и попробуем вывести пару сообщений (рис. [3.1]).



The screenshot shows two terminal windows. The top window is run by a regular user ('ivanprihodko') and shows commands like 'logger hello' and 'dnf -y install httpd'. The bottom window is run by root ('root@ivanprihodko') and shows the configuration of the 'ErrorLog' directive in the httpd.conf file. Both windows display log messages from the system's error log.

```
[ivanprihodko@ivanprihodko ~]$ su -
Пароль:
su: Сбой при проверке подлинности
[ivanprihodko@ivanprihodko ~]$ logger hello
[ivanprihodko@ivanprihodko ~]$ logger hello
[ivanprihodko@ivanprihodko ~]$ dnf -y install httpd
Ошибка: Эту команду нужно запускать с привилегиями суперпользователя (на большинстве систем - под именем пользователя root).
[ivanprihodko@ivanprihodko ~]$ tail -f /var/log/httpd/error_log
tail: невозможно открыть '/var/log/httpd/error_log' для чтения: Отказано в доступе
tail: больше нет файлов
[ivanprihodko@ivanprihodko ~]$ ErrorLog syslog:local1
bash: ErrorLog: команда не найдена...
[ivanprihodko@ivanprihodko ~]$ nano ^[[200~ /etc/httpd/conf/httpd.conf~ /etc/httpd/conf/httpd.conf~[ivanprihodko@ivanprihodko ~]$ nano /etc/httpd/conf/httpd.conf~[ivanprihodko@ivanprihodko ~]$ sudo nano^[[200~[root@ivanprihodko ~]# tail -f /var/log/httpd/error_log
[Sun Nov 23 19:36:03.519787 2025] [core:notice] [pid 4822:tid 4822] SELinux policy enabled
; httpd running as context system_u:system_r:httpd_t:s0
[Sun Nov 23 19:36:03.521300 2025] [suexec:notice] [pid 4822:tid 4822] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Sun Nov 23 19:36:03.543624 2025] [lbmethod_heartbeat:notice] [pid 4822:tid 4822] AH02282: No slotmem from mod_heartbeat
[Sun Nov 23 19:36:03.547374 2025] [mpm_event:notice] [pid 4822:tid 4822] AH00489: Apache/2.4.62 (Rocky Linux) configured -- resuming normal operations
[Sun Nov 23 19:36:03.547390 2025] [core:notice] [pid 4822:tid 4822] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
@ivanprihodko ~]# ErrorLog syslog:local1
ErrorLog: команда не найдена...
@ivanprihodko ~]#
```

Рис. 3.1: Вывод сообщений в журнале действий

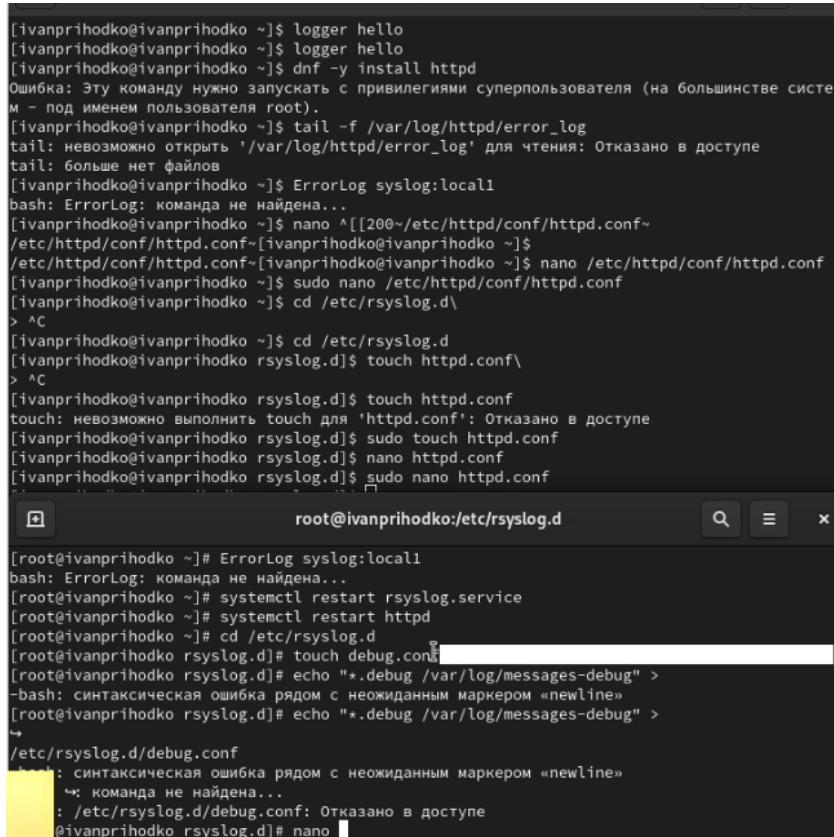
Изменим файл httpd.conf (рис. [3.2]).



```
GNU nano 5.6.1 httpd.conf Изменён
local1.* -/var/log/httpd-error.log
```

Рис. 3.2: Изменение файла httpd.conf

Выведем еще пару сообщений в терминале (рис. [3.3]).



```
[ivanprihodko@ivanprihodko ~]$ logger hello
[ivanprihodko@ivanprihodko ~]$ logger hello
[ivanprihodko@ivanprihodko ~]$ dnf -y install httpd
Ошибка: Этую команду нужно запускать с привилегиями суперпользователя (на большинстве систем под именем пользователя root).
[ivanprihodko@ivanprihodko ~]$ tail -f /var/log/httpd/error_log
tail: невозможно открыть '/var/log/httpd/error_log' для чтения: Отказано в доступе
tail: больше нет файлов
[ivanprihodko@ivanprihodko ~]$ ErrorLog syslog:local1
bash: ErrorLog: команда не найдена...
[ivanprihodko@ivanprihodko ~]$ nano ^[[200~/etc/httpd/conf/httpd.conf~
/etc/httpd/conf/httpd.conf-[ivanprihodko@ivanprihodko ~]$
/etc/httpd/conf/httpd.conf-[ivanprihodko@ivanprihodko ~]$ nano /etc/httpd/conf/httpd.conf
[ivanprihodko@ivanprihodko ~]$ sudo nano /etc/httpd/conf/httpd.conf
[ivanprihodko@ivanprihodko ~]$ cd /etc/rsyslog.d\
> ^C
[ivanprihodko@ivanprihodko ~]$ cd /etc/rsyslog.d
[ivanprihodko@ivanprihodko rsyslog.d]$ touch httpd.conf\
> ^C
[ivanprihodko@ivanprihodko rsyslog.d]$ touch httpd.conf
touch: невозможно выполнить touch для 'httpd.conf': Отказано в доступе
[ivanprihodko@ivanprihodko rsyslog.d]$ sudo touch httpd.conf
[ivanprihodko@ivanprihodko rsyslog.d]$ nano httpd.conf
[ivanprihodko@ivanprihodko rsyslog.d]$ sudo nano httpd.conf
[ivanprihodko@ivanprihodko ~]# ErrorLog syslog:local1
bash: ErrorLog: команда не найдена...
[root@ivanprihodko ~]# systemctl restart rsyslog.service
[root@ivanprihodko ~]# systemctl restart httpd
[root@ivanprihodko ~]# cd /etc/rsyslog.d
[root@ivanprihodko rsyslog.d]# touch debug.conf
[root@ivanprihodko rsyslog.d]# echo "*.*.debug /var/log/messages-debug" >
-bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
[root@ivanprihodko rsyslog.d]# echo "*.*.debug /var/log/messages-debug" >
-
/etc/rsyslog.d/debug.conf
bash: синтаксическая ошибка рядом с неожиданным маркером «newline»
: команда не найдена...
: /etc/rsyslog.d/debug.conf: Отказано в доступе
@ivanprihodko rsyslog.d]# nano
```

Рис. 3.3: Вывод сообщений через файл

Теперь выведем сообщение через другой способ (рис. [3.4]).

```
[ivanprihodko@ivanprihodko ~]$ cd /etc/rsyslog.d
[ivanprihodko@ivanprihodko rsyslog.d]$ touch httpd.conf
> ^C
[ivanprihodko@ivanprihodko rsyslog.d]$ touch httpd.conf
touch: невозможно выполнить touch для 'httpd.conf': Отказано в доступе
[ivanprihodko@ivanprihodko rsyslog.d]$ sudo touch httpd.conf
[ivanprihodko@ivanprihodko rsyslog.d]$ nano httpd.conf
[ivanprihodko@ivanprihodko rsyslog.d]$ sudo nano httpd.conf
[ivanprihodko@ivanprihodko rsyslog.d]$ systemctl restart rsyslog.service
[ivanprihodko@ivanprihodko rsyslog.d]$ logger -p daemon.debug "Daemon Debug Message"
root@ivanprihodko:/etc/rsyslog.d# .0-1.e19" x-pid="5233" x-info="https://www.rsyslog.com"] exiting on signal 15.
Nov 23 19:39:47 ivanprihodko systemd[1]: rsyslog.service: Deactivated successfully.
Nov 23 19:39:47 ivanprihodko systemd[1]: Stopped System Logging Service.
Nov 23 19:39:47 ivanprihodko systemd[1]: Starting System Logging Service...
Nov 23 19:39:47 ivanprihodko rsyslogd[5549]: [origin software="rsyslogd" swVersion="8.2412
.0-1.e19" x-pid="5549" x-info="https://www.rsyslog.com"] start
Nov 23 19:39:47 ivanprihodko systemd[1]: Started System Logging Service.
Nov 23 19:39:47 ivanprihodko rsyslogd[5549]: imjournal: journal files changed, reloading..
. [v8.2412.0-1.e19 try https://www.rsyslog.com/e/0 ]
Nov 23 19:39:47 ivanprihodko polkitd[824]: Unregistered Authentication Agent for unix-proc
ess:5505:184531 (system bus name :1.149, object path /org/freedesktop/PolicyKit1/Authentic
ationAgent, locale ru_RU.UTF-8) (disconnected from bus)
Nov 23 19:40:03 ivanprihodko ivanprihodko[5593]: Daemon Debug Message
3 19:40:17 ivanprihodko ivanprihodko[5593]: Daemon Debug Message
root@ivanprihodko rsyslog.d#
```

Рис. 3.4: Вывод сообщений черезиной способ

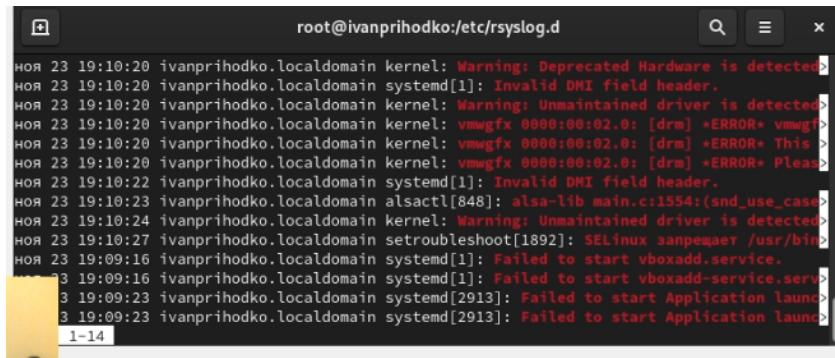
Теперь откроем содержимое терминала (рис. [3.5]-[3.7]).

```
Nov 23 19:39:47 ivanprihodko.localdomain systemd[1]: Stopped System Logging Service.
Nov 23 19:39:47 ivanprihodko.localdomain systemd[1]: Starting System Logging Service...
Nov 23 19:39:47 ivanprihodko.localdomain rsyslogd[5549]: [origin software="rsyslogd" swVersion="8.2412.0-1.e19" x-pid="5549" x-info="https://www.rsyslog.com"] start
Nov 23 19:39:47 ivanprihodko.localdomain systemd[1]: Started System Logging Service.
Nov 23 19:39:47 ivanprihodko.localdomain rsyslogd[5549]: imjournal: journal files changed,
reloading... [v8.2412.0-1.e19 try https://www.rsyslog.com/e/0 ]
Nov 23 19:39:47 ivanprihodko.localdomain polkitd[824]: Unregistered Authentication Agent f
or unix-process:5505:184531 (system bus name :1.149, object path /org/freedesktop/PolicyKi
t1/AuthenticationAgent, locale ru_RU.UTF-8) (disconnected from bus)
Nov 23 19:40:03 ivanprihodko.localdomain ivanprihodko[5593]: Daemon Debug Message
Nov 23 19:40:17 ivanprihodko.localdomain systemd[1]: fprintd.service: Deactivated successf
ul
root@ivanprihodko rsyslog.d# journalctl
```

Рис. 3.5: Открытие сордержимого терминала

```
Nov 23 19:10:20 ivanprihodko.localdomain kernel: [Firmware Bug]: TSC doesn't count with P
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-provided physical RAM map:
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000>
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x0000>
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000000f0000-0x0000>
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000>
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000dffff0000-0x0000>
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000fec00000-0x0000>
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000fee00000-0x0000>
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000ffffc0000-0x0000>
Nov 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000>
1-14
```

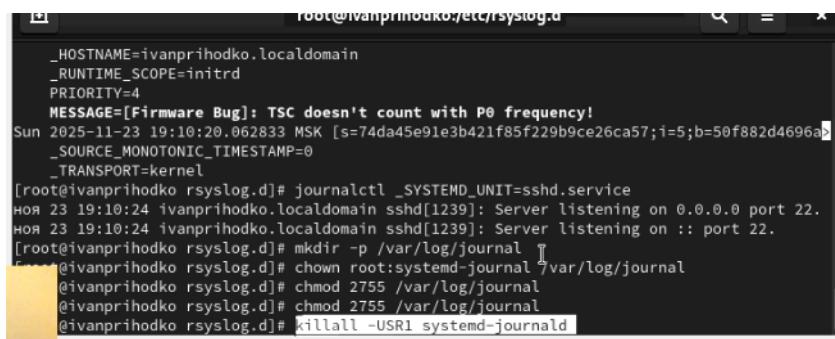
Рис. 3.6: Открытие сордержимого терминала



```
root@ivanprihodko:/etc/rsyslog.d
...
ноя 23 19:10:20 ivanprihodko.localdomain kernel: Warning: Deprecated Hardware is detected>
ноя 23 19:10:20 ivanprihodko.localdomain systemd[1]: Invalid DMI field header.
ноя 23 19:10:20 ivanprihodko.localdomain kernel: Warning: Unmaintained driver is detected>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ vmwg>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ This >
ноя 23 19:10:20 ivanprihodko.localdomain kernel: vmwgfx 0000:00:02.0: [drm] +ERROR+ Please >
ноя 23 19:10:22 ivanprihodko.localdomain systemd[1]: Invalid DMI field header.
ноя 23 19:10:23 ivanprihodko.localdomain alsactl[848]: alsa-lib main.c::1554:(snd_use_case>
ноя 23 19:10:24 ivanprihodko.localdomain kernel: Warning: Unmaintained driver is detected>
ноя 23 19:10:27 ivanprihodko.localdomain setroubleshoot[1892]: SELinux запрещает /usr/bin/>
ноя 23 19:09:16 ivanprihodko.localdomain systemd[1]: Failed to start vboxadd.service.
ноя 23 19:09:16 ivanprihodko.localdomain systemd[1]: Failed to start vboxadd-service.serv>
ноя 23 19:09:23 ivanprihodko.localdomain systemd[2913]: Failed to start Application launc>
ноя 23 19:09:23 ivanprihodko.localdomain systemd[2913]: Failed to start Application launc>
...
1-14
```

Рис. 3.7: Открытие сордержимого терминала

Теперь создадим и настроим каталог для записи журнала (рис. [3.8]).



```
root@ivanprihodko:/etc/rsyslog.d
...
_HOSTNAME=ivanprihodko.localdomain
_RUNTIME_SCOPE=initrd
_PRIORITY=4
MESSAGE=[Firmware Bug]: TSC doesn't count with P0 frequency!
Sun 2025-11-23 19:10:20.062833 MSK [s=74da45e91e3b421f85f229b9ce26ca57;i=5;b=50f882d4696a
_SOURCE_MONOTONIC_TIMESTAMP=0
_TRANSPORT=kernel
[root@ivanprihodko rsyslog.d]# journalctl _SYSTEMD_UNIT=sshd.service
ноя 23 19:10:24 ivanprihodko.localdomain sshd[1239]: Server listening on 0.0.0.0 port 22.
ноя 23 19:10:24 ivanprihodko.localdomain sshd[1239]: Server listening on :: port 22.
[root@ivanprihodko rsyslog.d]# mkdir -p /var/log/journal
[root@ivanprihodko rsyslog.d]# chown root:systemd-journal /var/log/journal
[root@ivanprihodko rsyslog.d]# chmod 2755 /var/log/journal
[root@ivanprihodko rsyslog.d]# chmod 2755 /var/log/journal
[root@ivanprihodko rsyslog.d]# killall -USR1 systemd-journald
```

Рис. 3.8: Сорздение инастройка каталога для записи журнала

## **4 Выводы**

В ходе данной лабораторной работы были получены навыки работы с журнальными мониторинга различных событий в системе.

## **5 Ответы на контрольные вопросы**

1. /etc/rsyslog.conf или /etc/rsyslog.d/
2. /etc/rsyslog.conf или файлы в /etc/rsyslog.d/, связанные с auth или authpriv
3. Зависит от настроек, обычно — несколько секунд или минут, сразу после триггера ротации.
4. \*.info /var/log/messages.info
5. tail -f /var/log/messages или journalctl -f
6. journalctl \_PID=1 –since “09:00” –until “15:00”
7. journalctl –boot или journalctl -b
8. Использовать systemctl restart systemd-journald после настройки /etc/systemd/journald.conf.