

# **Лабораторная работа**

Номер 7

---

Приходько Иван Иванович

27 ноября 2025

Российский университет дружбы народов, Москва, Россия

## Информация

---

## Докладчик

---

- Приходько Иван Иванович
- Студент
- Российский университет дружбы народов

## Цель работы

---

Получить навыки работы с журналами мониторинга различных событий в системе.

## Задание

---

Поработать с журналом мониторинга событий в системе

# Работа с журналом действий

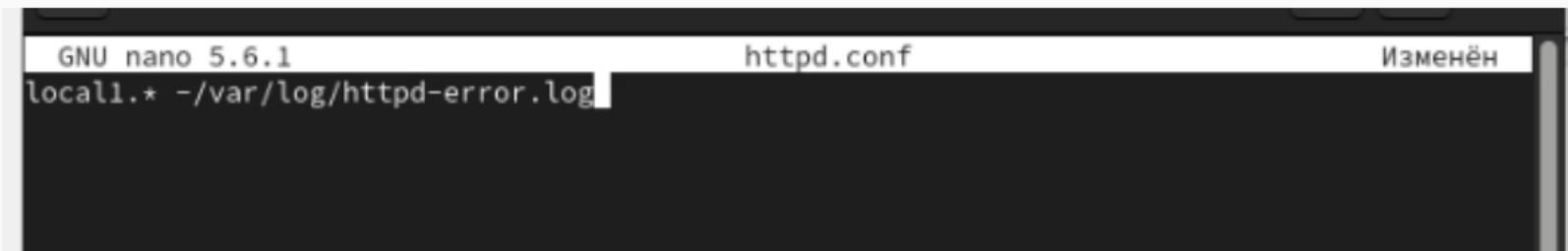
Для начала запустим журнал событий в другом терминале и попробуем вывести пару сообщений

```
[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 ~]$
/etc/httpd/conf/httpd.conf-[ivanprihodko@ivanprihodko ~]$ nano /etc/httpd/conf/httpd.conf
[ivanprihodko@ivanprihodko ~]$ sudo nano
```

```
[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_heartmonitor
```

# Работа с журналом действий

Изменим файл httpd.conf



The screenshot shows a terminal window with the following content:

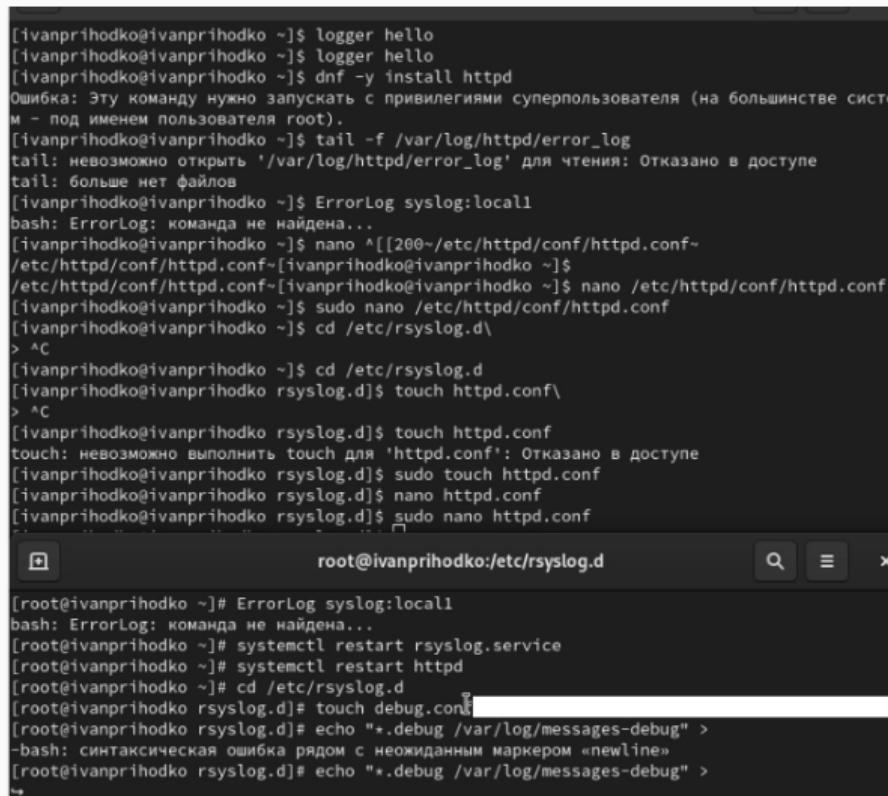
```
GNU nano 5.6.1          httpd.conf          Изменён
local.* -/var/log/httpd-error.log
```

The terminal title is "httpd.conf" and the status bar indicates it has been modified ("Изменён"). The command entered is "local.\* -/var/log/httpd-error.log".

**Рис. 2:** Изменение файла httpd.conf

# Работа с журналом действий

Выведем еще пару сообщений в терминале



The screenshot shows a terminal window with the following content:

```
[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 ~]$
/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" >
```

The terminal window has a title bar "root@ivanprihodko:/etc/rsyslog.d".

# Работа с журналом действий

Теперь выведем сообщение через другой способ

```
[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.el9" 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.el9" 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.el9 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)
```

# Работа с журналом действий

Теперь откроем содержимое терминала

```
ноя 23 19:39:47 ivanprihodko.localdomain systemd[1]: Stopped System Logging Service.  
ноя 23 19:39:47 ivanprihodko.localdomain systemd[1]: Starting System Logging Service...  
ноя 23 19:39:47 ivanprihodko.localdomain rsyslogd[5549]: [origin software="rsyslogd" swVersion="8.2412.0-1.el9" x-pid="5549" x-info="https://www.rsyslog.com"] start  
ноя 23 19:39:47 ivanprihodko.localdomain systemd[1]: Started System Logging Service.  
ноя 23 19:39:47 ivanprihodko.localdomain rsyslogd[5549]: imjournal: journal files changed,  
    reloading... [v8.2412.0-1.el9 try https://www.rsyslog.com/e/0 ]  
ноя 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)  
ноя 23 19:40:03 ivanprihodko.localdomain ivanprihodko[5593]: Daemon Debug Message  
ноя 23 19:40:17 ivanprihodko.localdomain systemd[1]: fprintd.service: Deactivated successfully  
@ivanprihodko rsyslog.d]# journalctl
```

Рис. 5: Открытие сордормимого терминала

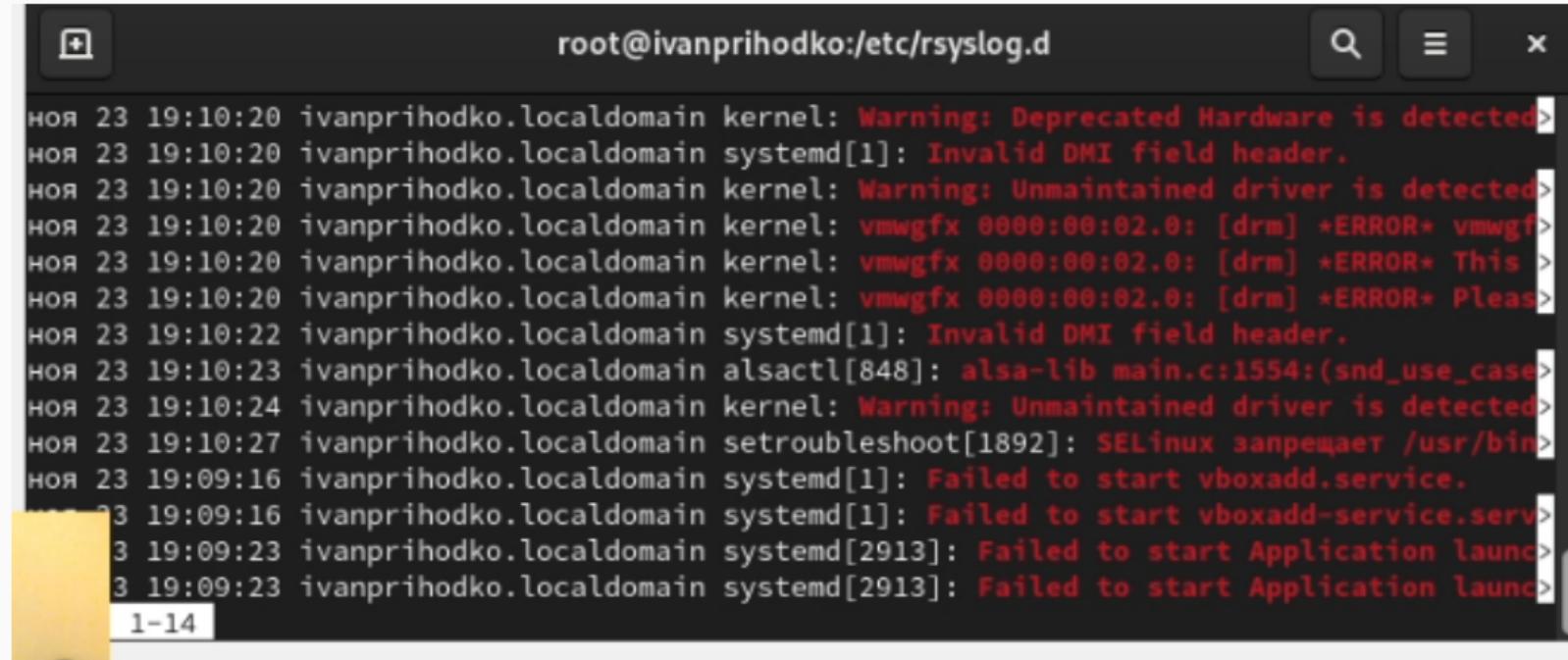
# Работа с журналом действий

```
ноя 23 19:10:20 ivanprihodko.localdomain kernel: [Firmware Bug]: TSC doesn't count with P>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-provided physical RAM map:
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x0000000000000000-0x0000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000009fc00-0x0000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000000f0000-0x0000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x0000000000100000-0x0000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x000000000dfffc0000-0x0000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000fec00000-0x0000>
ноя 23 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000fee00000-0x0000>
3 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000fffc0000-0x0000>
3 19:10:20 ivanprihodko.localdomain kernel: BIOS-e820: [mem 0x00000000100000000-0x0000>
```

1-14

Рис. 6: Открытие сордержимого терминала

## Работа с журналом действий



The screenshot shows a terminal window with the following details:

- Terminal title: root@ivanprihodko:/etc/rsyslog.d
- Icon: A small icon with a plus sign.
- Buttons: Search (magnifying glass), Minimize (three horizontal lines), and Close (X).
- Log content:

```
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* vmwgf>
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>
3 19:09:23 ivanprihodko.localdomain systemd[2913]: Failed to start Application launc>
3 19:09:23 ivanprihodko.localdomain systemd[2913]: Failed to start Application launc>
```
- Bottom status bar: "1-14"

Рис. 7: Открытие содержимого терминала

## Работа с журналом действий

Теперь создадим и настроим каталог для записи журнала

```
root@ivanprihodko:~# 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
@ivanprihodko rsyslog.d]# chmod 2755 /var/log/journal
@ivanprihodko rsyslog.d]# chmod 2755 /var/log/journal
@ivanprihodko rsyslog.d]# killall -USR1 systemd-journald
```

Рис. 8: Создание инастройка каталога для записи журнала

## Выводы

---

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