

Презентация по шестой лабораторной. Предмет - Информационная безопасность.

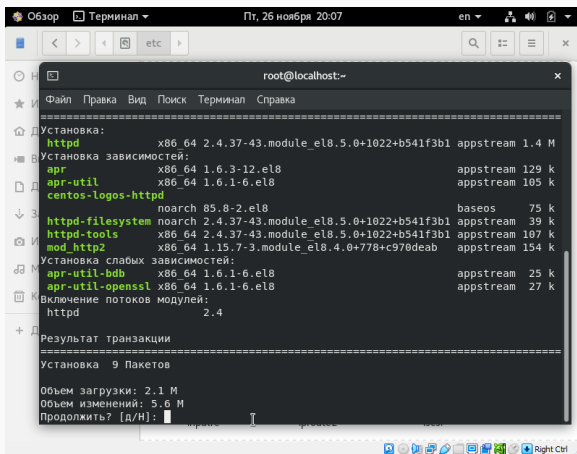
Попов Олег Павлович¹

2021, 18 Сентября – 18 Сентября

¹RUDN University, Moscow, Russian Federation

Выполнение лабораторной

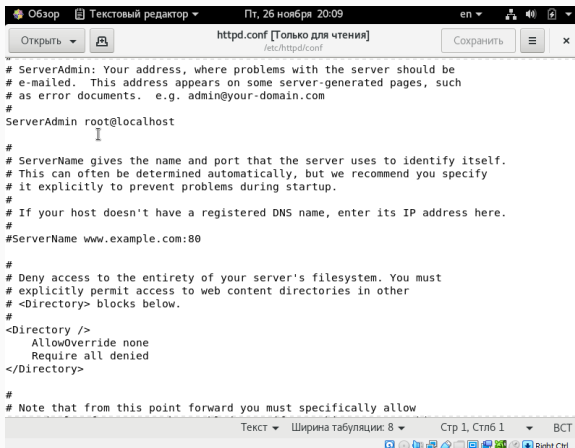
Подготовка к работе



The screenshot shows a terminal window titled "root@localhost:~" with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal output displays the installation of the httpd package and its dependencies. The packages are listed in a table-like format with columns for architecture, version, release, and size. The total download size is 2.1 M and the total update size is 5.6 M. The prompt "Продолжить? [д/н]:" is shown at the bottom, indicating the installation is about to proceed.

```
Установка:
  httpd                x86_64 2.4.37-43.module_el8.5.0+1022+b541f3b1 appstream 1.4 M
Установка зависимостей:
  apr                  x86_64 1.6.3-12.el8                      appstream 129 k
  apr-util             x86_64 1.6.1-6.el8                      appstream 105 k
  centos-logos-httpd   noarch 85.8-2.el8                      baseos     75 k
  httpd-filesystem     noarch 2.4.37-43.module_el8.5.0+1022+b541f3b1 appstream  39 k
  httpd-tools          x86_64 2.4.37-43.module_el8.5.0+1022+b541f3b1 appstream 107 k
  mod_http2            x86_64 1.15.7-3.module_el8.4.0+778+c970deab appstream 154 k
Установка слабых зависимостей:
  apr-util-bdb         x86_64 1.6.1-6.el8                      appstream  25 k
  apr-util-openssl     x86_64 1.6.1-6.el8                      appstream  27 k
Включение потоков модулей:
  httpd                2.4
=====
Результат транзакции
Установка 9 Пакетов
Объем загрузки: 2.1 М
Объем изменений: 5.6 М
Продолжить? [д/н]:
```

Подготовка к работе



The screenshot shows a text editor window titled "httpd.conf [Только для чтения]" (httpd.conf [Read-only]) with the path "/etc/httpd/conf". The editor contains the following configuration text:

```
# ServerAdmin: Your address, where problems with the server should be
# e-mailed. This address appears on some server-generated pages, such
# as error documents. e.g. admin@your-domain.com
#
ServerAdmin root@localhost

#
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
#ServerName www.example.com:80

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

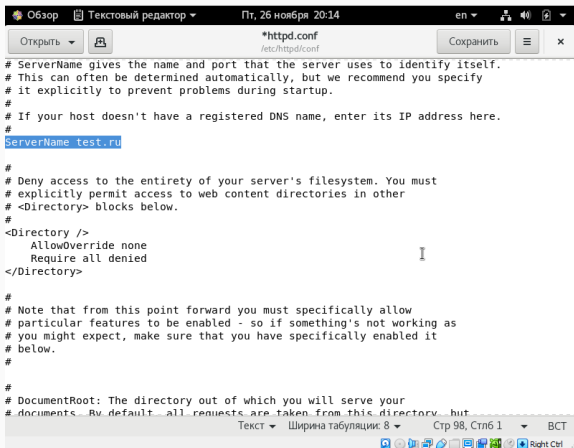
#
# Note that from this point forward you must specifically allow
```

The status bar at the bottom indicates "Текст" (Text), "Ширина табуляции: 8" (Tab width: 8), "Стр 1, Стлб 1" (Line 1, Column 1), and "ВСТ" (UTF-8).

Подготовка к работе

```
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--r--. 1 root root 11899 ноя 12 07:54 /etc/httpd/conf/httpd.conf
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--rw-. 1 root root 11899 ноя 12 07:54 /etc/httpd/conf/httpd.conf
[root@localhost ~]#
```

Подготовка к работе



```
# ServerName gives the name and port that the server uses to identify itself.
# This can often be determined automatically, but we recommend you specify
# it explicitly to prevent problems during startup.
#
# If your host doesn't have a registered DNS name, enter its IP address here.
#
ServerName test.ru

#
# Deny access to the entirety of your server's filesystem. You must
# explicitly permit access to web content directories in other
# <Directory> blocks below.
#
<Directory />
    AllowOverride none
    Require all denied
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
```

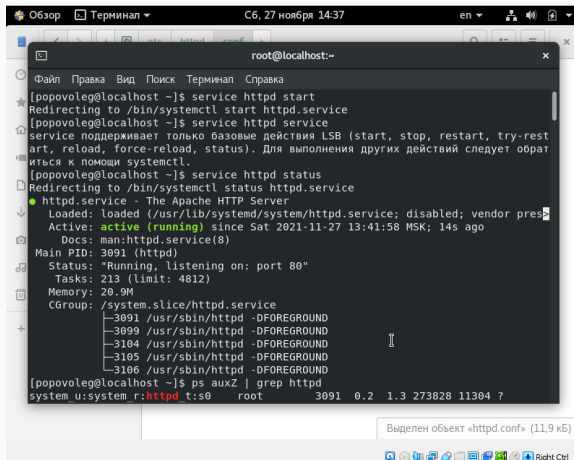
Подготовка к работе

```
[root@localhost ~]# lsmod /etc/httpd/conf/httpd.conf
Usage: lsmod
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--r--. 1 root root 11899 ноя 12 07:54 /etc/httpd/conf/httpd.conf
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--rw-. 1 root root 11899 ноя 12 07:54 /etc/httpd/conf/httpd.conf
[root@localhost ~]# chmod o-w /etc/httpd/conf/httpd.conf
[root@localhost ~]# ls -l /etc/httpd/conf/httpd.conf
-rw-r--r--. 1 root root 11887 ноя 26 20:15 /etc/httpd/conf/httpd.conf
[root@localhost ~]#
```

Подготовка к работе

```
[root@localhost ~]# iptables -F  
[root@localhost ~]# iptables -P INPUT ACCEPT  
[root@localhost ~]# iptables -P OUTPUT ACCEPT  
[root@localhost ~]#
```


Выполнение лабораторной



```
root@localhost:~  
[popovoleg@localhost ~]$ service httpd start  
Redirecting to /bin/systemctl start httpd.service  
[popovoleg@localhost ~]$ service httpd status  
service поддерживает только базовые действия LSB (start, stop, restart, try-restart, reload, force-reload, status). Для выполнения других действий следует обратиться к помощи systemctl.  
[popovoleg@localhost ~]$ service httpd status  
Redirecting to /bin/systemctl status httpd.service  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: enabled)  
   Active: active (running) since Sat 2021-11-27 13:41:58 MSK; 14s ago  
     Docs: man:httpd.service(8)  
   Main PID: 3091 (httpd)  
    Status: "Running, listening on: port 80"  
   Tasks: 213 (limit: 4812)  
  Memory: 20.9M  
    CGroup: /system.slice/httpd.service  
            └─3091 /usr/sbin/httpd -DFOREGROUND  
              └─3099 /usr/sbin/httpd -DFOREGROUND  
                └─3104 /usr/sbin/httpd -DFOREGROUND  
                  └─3105 /usr/sbin/httpd -DFOREGROUND  
                    └─3106 /usr/sbin/httpd -DFOREGROUND  
[popovoleg@localhost ~]$ ps auxZ | grep httpd  
system_u:system_r:httpd_t:s0 root      3091  0.2  1.3 273828 11304 ?
```

Выделен объект «httpd.conf» (11,9 кБ)

Выполнение лабораторной

The screenshot shows a terminal window titled "root@localhost:~" with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка). The terminal displays the following content:

```
Ss 13:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3099 0.0 1.0 289832 8508 ?
S 13:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3104 0.0 1.2 1347640 10176 ?
Sl 13:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3105 0.0 1.2 1478768 10176 ?
Sl 13:41 0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0 apache 3106 0.0 1.2 1347640 10176 ?
Sl 13:41 0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 popovolg+ 3378 0.0 0.1 121
36 1100 pts/0 R+ 13:42 0:00 grep --color=auto httpd

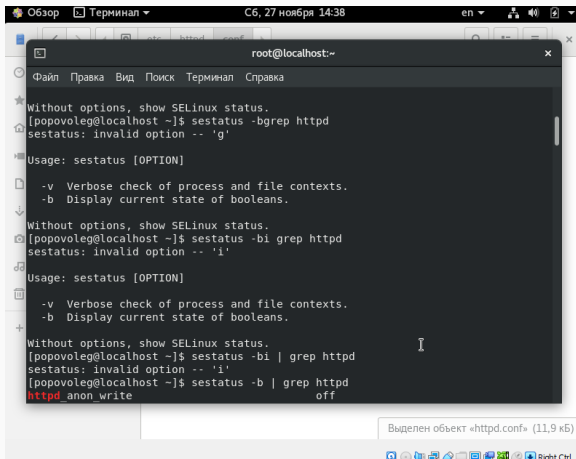
[popovoleg@localhost ~]$ ps -eZ | grep httpd
system_u:system_r:httpd_t:s0 3091 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3099 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3104 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3105 ? 00:00:00 httpd
system_u:system_r:httpd_t:s0 3106 ? 00:00:00 httpd

[popovoleg@localhost ~]$ sestatus -bigrep httpd
+ sestatus: invalid option -- 'i'

Usage: sestatus [OPTION]
  -v Verbose check of process and file contexts.
  -b Display current state of booleans.
```

Below the terminal window, a status bar indicates: "Выделен объект «httpd.conf» (11,9 кБ)". At the bottom of the desktop environment, a taskbar shows various application icons and the text "Right Ctrl".

Выполнение лабораторной



The screenshot shows a Linux desktop environment. In the foreground, a terminal window titled 'root@localhost:~' is open. It displays the output of several 'sestatus' commands. The first command 'sestatus -bgrep httpd' results in an error: 'sestatus: invalid option -- 'g''. The second command 'sestatus -bi grep httpd' also results in an error: 'sestatus: invalid option -- 'i''. The third command 'sestatus -bi | grep httpd' results in an error: 'sestatus: invalid option -- 'i''. The fourth command 'sestatus -b | grep httpd' shows the output: 'httpd_anon_write' and 'off'. In the background, a file manager window is open, showing the contents of the '/etc/httpd/conf/' directory. The file 'httpd.conf' is selected, and a status bar at the bottom indicates 'Выделен объект «httpd.conf» (11,9 КБ)'. The system clock in the top right corner shows 'Сб, 27 ноября 14:38'.

```
root@localhost:~  
Without options, show SELinux status.  
[popovoleg@localhost ~]$ sestatus -bgrep httpd  
sestatus: invalid option -- 'g'  
Usage: sestatus [OPTION]  
-v Verbose check of process and file contexts.  
-b Display current state of booleans.  
Without options, show SELinux status.  
[popovoleg@localhost ~]$ sestatus -bi grep httpd  
sestatus: invalid option -- 'i'  
Usage: sestatus [OPTION]  
-v Verbose check of process and file contexts.  
-b Display current state of booleans.  
Without options, show SELinux status.  
[popovoleg@localhost ~]$ sestatus -bi | grep httpd  
sestatus: invalid option -- 'i'  
[popovoleg@localhost ~]$ sestatus -b | grep httpd  
httpd_anon_write  
off
```

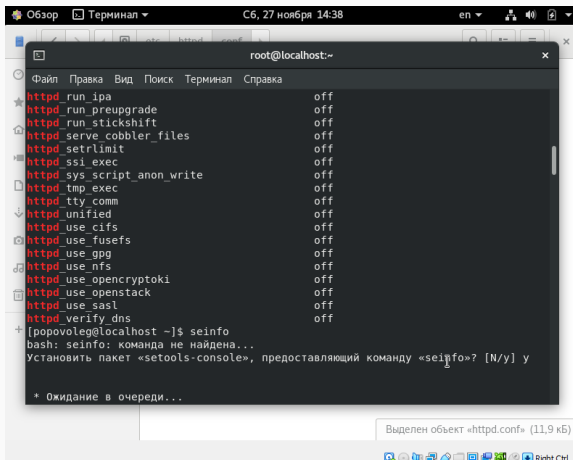
Выделен объект «httpd.conf» (11,9 КБ)

Выполнение лабораторной

```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
★ httpd_builtin_scripting on  
★ httpd_can_check_spam off  
★ httpd_can_connect_ftp off  
★ httpd_can_connect_ldap off  
★ httpd_can_connect_mythtv off  
★ httpd_can_connect_zabbix off  
★ httpd_can_network_connect off  
★ httpd_can_network_connect_cobbler off  
★ httpd_can_network_connect_db off  
★ httpd_can_network_memcache off  
★ httpd_can_network_relay off  
★ httpd_can_sendmail off  
★ httpd_dbus_avahi off  
★ httpd_dbus_sssd off  
★ httpd_dontaudit_search_dirs off  
★ httpd_enable_cgi on  
★ httpd_enable_ftp_server off  
★ httpd_enable_homedirs off  
★ httpd_execmem off  
★ httpd_graceful_shutdown off  
★ httpd_manage_ipa off  
★ httpd_mod_auth_ntlm_winbind off  
★ httpd_mod_auth_pam off  
★ httpd_read_user_content off
```

Выделен объект «httpd.conf» (11,9 кБ)

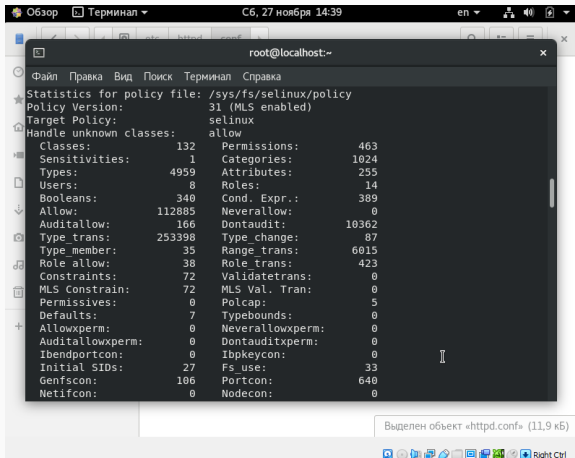
Выполнение лабораторной



```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
httpd_run_ipa off  
httpd_run_preupgrade off  
httpd_run_stickshift off  
httpd_serve_cobbler_files off  
httpd_setrlimit off  
httpd_ssi_exec off  
httpd_sys_script_anon_write off  
httpd_tmp_exec off  
httpd_tty_comm off  
httpd_unified off  
httpd_use_cifs off  
httpd_use_fusefs off  
httpd_use_gpg off  
httpd_use_nfs off  
httpd_use_opencryptoki off  
httpd_use_openstack off  
httpd_use_sasl off  
httpd_verify_dns off  
[porovoleg@localhost ~]$ seinfo  
bash: seinfo: команда не найдена...  
Установить пакет «setools-console», предоставляющий команду «seinfo»? [N/y] y  
* Ожидание в очереди...
```

Выделен объект «httpd.conf» (11,9 кБ)

Выполнение лабораторной



```
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow

Classes:                 132      Permissions:             463
Sensitivities:           1        Categories:             1024
Types:                   4959     Attributes:              255
Users:                   8         Roles:                  14
Booleans:                340      Cond. Expr.:            389
Allow:                   112885    Neverallow:              0
Auditallow:              166      Dontaudit:              10362
Type_trans:              253398    Type_change:             87
Type_member:              35       Range_trans:            6015
Role_allow:              38       Role_trans:              423
Constraints:              72      Validatetrans:           0
MLS Constrain:           72      MLS Val. Tran:           0
Permissives:             0       Polcap:                  5
Defaults:                7        Typebounds:              0
Allowxperm:              0       Neverallowxperm:         0
Auditallowxperm:         0       Dontauditxperm:         0
Ibendportcon:            0       Ibpkeycon:               0
Initial SIDs:            27       Fs_use:                  33
Genfscon:                106      Portcon:                 640
Netifcon:                0        Nodecon:                 0
```

Выделен объект «httpd.conf» (11,9 кБ)

Выполнение лабораторной

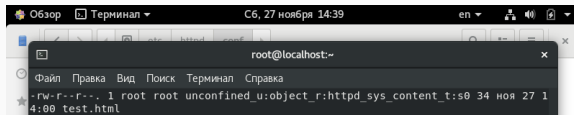
```
Обзор Терминал C6, 27 ноября 14:39 en
```

```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
[popovoleg@localhost ~]$ ls -lZ /var/www  
итого 0  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 ноя 12 07  
:58 cgi-bin  
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 ноя 12 07  
:58 html  
[popovoleg@localhost ~]$ ls -lZ /var/www/html  
итого 0  
[popovoleg@localhost ~]$ ls -la /var/www  
итого 4  
drwxr-xr-x. 4 root root 33 ноя 26 20:08 .  
drwxr-xr-x. 22 root root 4096 ноя 26 20:08 ..  
drwxr-xr-x. 2 root root 6 ноя 12 07:58 cgi-bin  
drwxr-xr-x. 2 root root 6 ноя 12 07:58 html  
[popovoleg@localhost ~]$ su -  
Пароль:  
[root@localhost ~]# touch /var/www/html/test.html  
[root@localhost ~]# ls -la /var/www/html  
итого 0  
-rw-r--r--. 1 root root 0 ноя 27 13:59 test.html  
[root@localhost ~]# chmod o+w /var/www/html/test.html  
[root@localhost ~]# chmod o-w /var/www/html/test.html  
[root@localhost ~]# ls -lZ /var/www/html  
итого 4
```

Выделен объект «httpd.conf» (11,9 кБ)

Right Ctrl

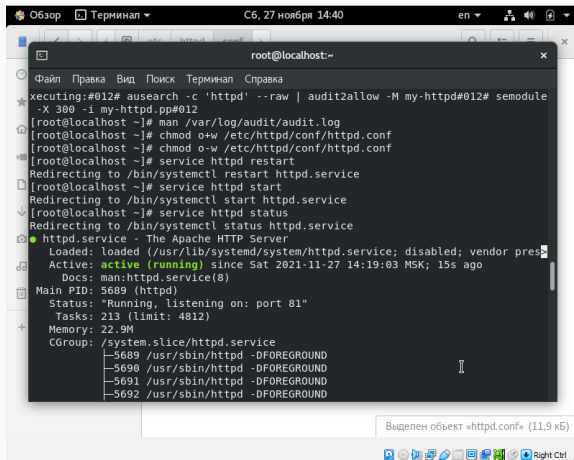
Выполнение лабораторной



The image shows a terminal window titled "root@localhost:~" with a menu bar containing "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal output displays the command "ls -l" and its result for a file named "test.html".

```
root@localhost:~  
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 34 ноя 27 14:00 test.html
```


Выполнение лабораторной



The screenshot shows a terminal window titled "root@localhost:~" with a menu bar (Файл, Правка, Вид, Поиск, Терминал, Справка) and a toolbar. The terminal output shows the following commands and their results:

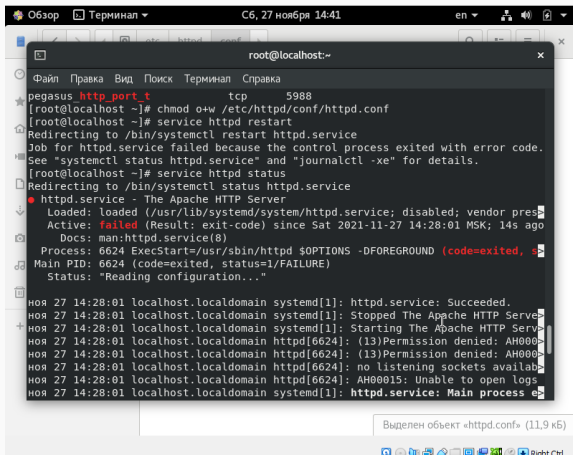
```
xeccuting:012# ausearch -c 'httpd' --raw | audit2allow -M my-httpd#012# semodule
-X 300 -i my-httpd.pp#012
[root@localhost ~]# man /var/log/audit/audit.log
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf
[root@localhost ~]# chmod o-w /etc/httpd/conf/httpd.conf
[root@localhost ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
[root@localhost ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@localhost ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pres
   Active: active (running) since Sat 2021-11-27 14:19:03 MSK; 15s ago
     Docs: man:httpd.service(8)
   Main PID: 5689 (httpd)
    Status: "Running, listening on: port 81"
     Tasks: 213 (limit: 4812)
    Memory: 22.9M
   CGroup: /system.slice/httpd.service
           └─5689 /usr/sbin/httpd -DFOREGROUND
             └─5690 /usr/sbin/httpd -DFOREGROUND
               └─5691 /usr/sbin/httpd -DFOREGROUND
                 └─5692 /usr/sbin/httpd -DFOREGROUND
```

Below the terminal window, a notification bar states: "Выделен объект «httpd.conf» (11,9 кБ)". At the bottom of the screen, a taskbar shows various application icons and the text "Right Ctrl".

Выполнение лабораторной

```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
★ ноя 27 14:20:04 localhost.localdomain systemd[1]: Starting The Apache HTTP Server  
ноя 27 14:20:04 localhost.localdomain systemd[1]: Started The Apache HTTP Server  
ноя 27 14:20:04 localhost.localdomain httpd[6231]: Server configured, listening  
[root@localhost ~]# tail -nl /var/log/messages  
tail: неверное число строк: «l»  
[root@localhost ~]# tail -nl /var/log/messages  
Nov 27 14:20:16 localhost dbus-daemon[2000]: [session uid=1000 pid=2000] Success  
fully activated service 'org.gnome.gedit'  
[root@localhost ~]# man /var/log/http/error_log  
man: /var/log/http/error_log: Нет такого файла или каталога  
Нет справочной страницы для /var/log/http/error_log  
[root@localhost ~]# man /var/log/http/access_log  
man: /var/log/http/access_log: Нет такого файла или каталога  
Нет справочной страницы для /var/log/http/access_log  
[root@localhost ~]# man /var/log/httpd/error_log  
[root@localhost ~]# man /var/log/httpd/access_log  
[root@localhost ~]# semanage port -a -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 уже определен  
[root@localhost ~]# semanage port -l | grep http port t  
semanage port: error: one of the arguments -a/--add -d/--delete -m/--modify -l/-  
-list -E/--extract -D/--deleteall is required  
[root@localhost ~]# semanage port -l | grep http port t  
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000  
Выделен объект «httpd.conf» (11,9 кБ)
```

Выполнение лабораторной

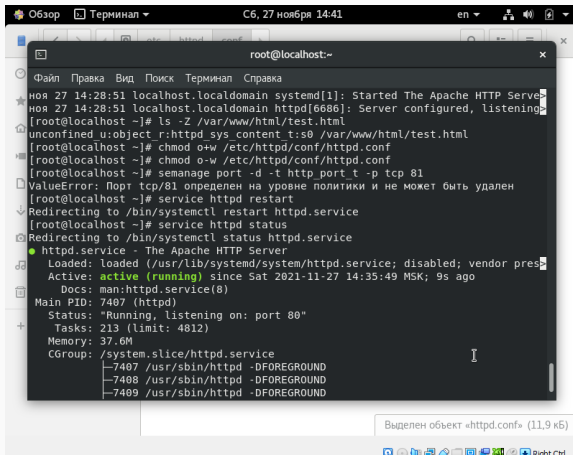


```
Обзор Терминал C6, 27 ноября 14:41 en
root@localhost:~
Файл Правка Вид Поиск Терминал Справка
pegasus http_port_t tcp 5988
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf
[root@localhost ~]# service httpd restart
Redirecting to /bin/systemctl restart httpd.service
Job for httpd.service failed because the control process exited with error code.
See "systemctl status httpd.service" and "journalctl -xe" for details.
[root@localhost ~]# service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Sat 2021-11-27 14:28:01 MSK; 14s ago
     Docs: man:httpd.service(8)
   Process: 6624 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND (code=exited, status=1/FAILURE)
   Main PID: 6624 (code=exited, status=1/FAILURE)
   Status: "Reading configuration..."

ноя 27 14:28:01 localhost.localdomain systemd[1]: httpd.service: Succeeded.
ноя 27 14:28:01 localhost.localdomain systemd[1]: Stopped The Apache HTTP Server.
ноя 27 14:28:01 localhost.localdomain systemd[1]: Starting The Apache HTTP Server: .
ноя 27 14:28:01 localhost.localdomain httpd[6624]: (13)Permission denied: AH00004: cannot open file /etc/httpd/conf/httpd.conf: (13)Permission denied
ноя 27 14:28:01 localhost.localdomain httpd[6624]: (13)Permission denied: AH00004: cannot open file /etc/httpd/conf/httpd.conf: (13)Permission denied
ноя 27 14:28:01 localhost.localdomain httpd[6624]: no listening sockets available, shutting down
ноя 27 14:28:01 localhost.localdomain httpd[6624]: AH00015: Unable to open logs
ноя 27 14:28:01 localhost.localdomain systemd[1]: httpd.service: Main process exited, code=exited, status=1/FAILURE
```

Выделен объект «httpd.conf» (11,9 кБ)

Выполнение лабораторной



```
root@localhost:~  
Файл Правка Вид Поиск Терминал Справка  
ноя 27 14:28:51 localhost.localdomain systemd[1]: Started The Apache HTTP Server  
ноя 27 14:28:51 localhost.localdomain httpd[6686]: Server configured, listening  
[root@localhost ~]# ls -Z /var/www/html/test.html  
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html  
[root@localhost ~]# chmod o+w /etc/httpd/conf/httpd.conf  
[root@localhost ~]# chmod o-w /etc/httpd/conf/httpd.conf  
[root@localhost ~]# semanage port -d -t http_port_t -p tcp 81  
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален  
[root@localhost ~]# service httpd restart  
Redirecting to /bin/systemctl restart httpd.service  
[root@localhost ~]# service httpd status  
Redirecting to /bin/systemctl status httpd.service  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pres  
   Active: active (running) since Sat 2021-11-27 14:35:49 MSK; 9s ago  
     Docs: man:httpd.service(8)  
   Main PID: 7407 (httpd)  
   Status: "Running, listening on: port 80"  
   Tasks: 213 (limit: 4812)  
  Memory: 37.6M  
   CGroup: /system.slice/httpd.service  
           └─7407 /usr/sbin/httpd -DFOREGROUND  
           └─7408 /usr/sbin/httpd -DFOREGROUND  
           └─7409 /usr/sbin/httpd -DFOREGROUND
```

Выделен объект «httpd.conf» (11,9 кБ)