

Политика безопасности в ОС Ubuntu 24.04.3 LTS

Настройка политики безопасности в операционной системе Ubuntu 24.04.3 LTS будет состоять из 3 основных пунктов:

1. Настройка брандмауэра
2. Шифрование данных
3. Аудит системы

Они позволят оптимизировать и обезопасить систему от несанкционированных действий вредоносного ПО или пользователей.

1. Настройка брандмауэра.

1.1. Откройте терминал через список приложений

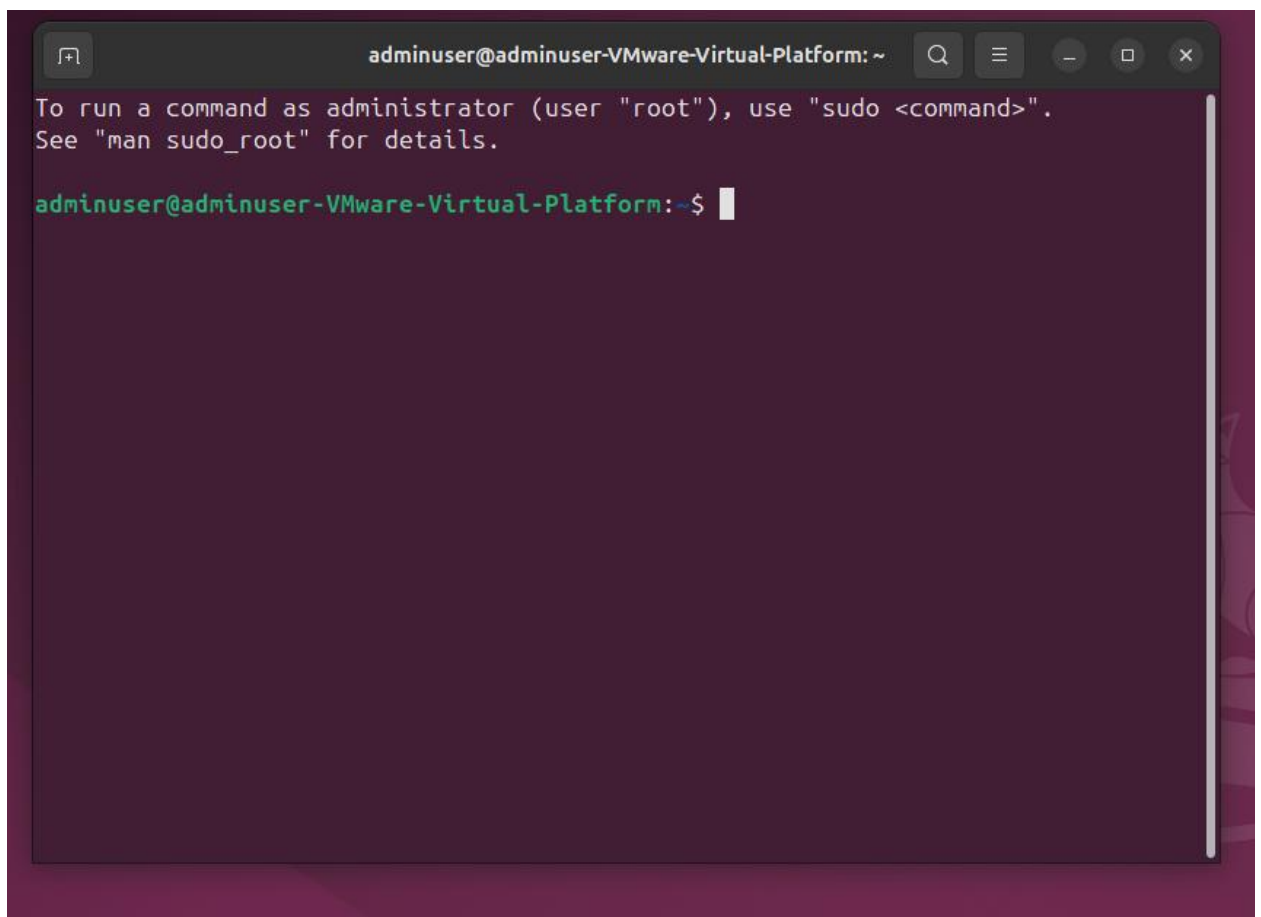
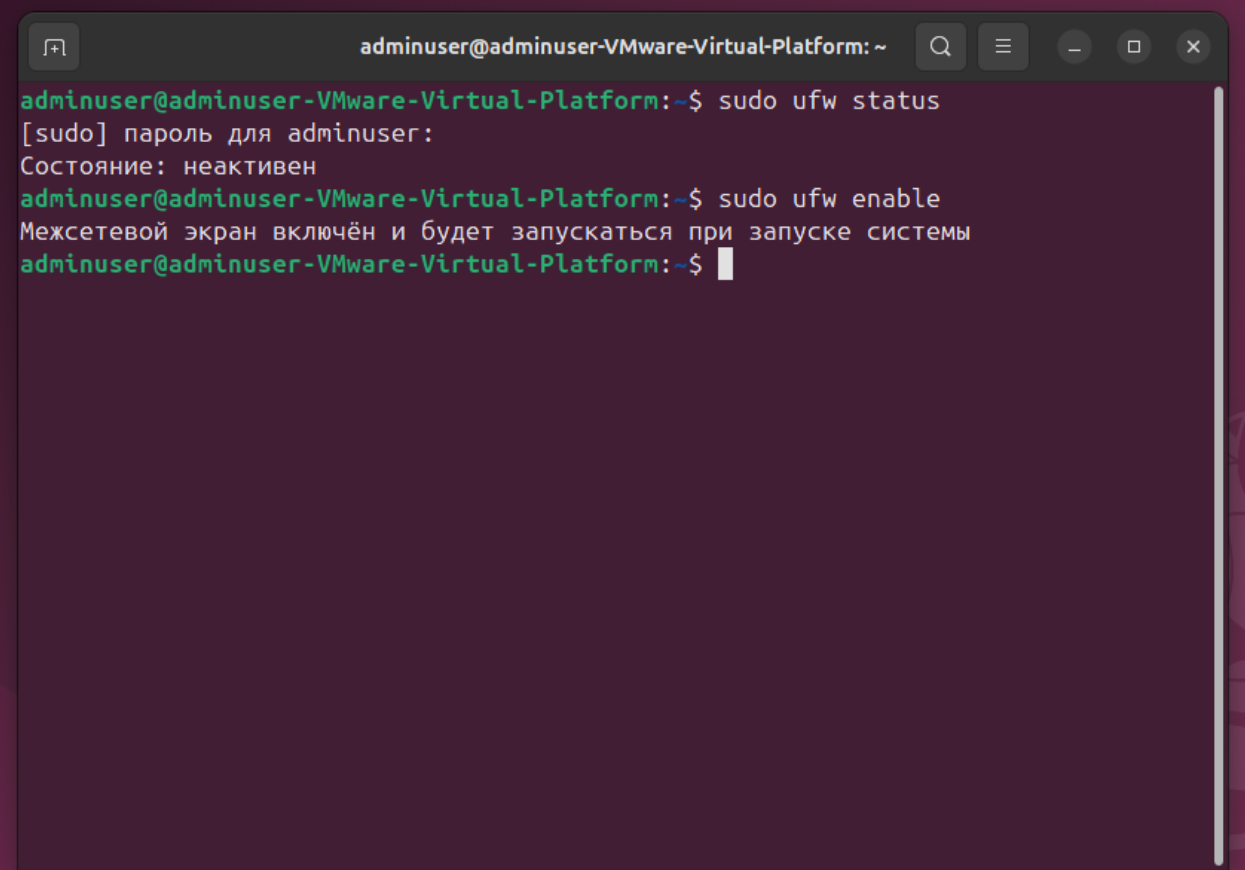


Рисунок 1 – Окно терминала

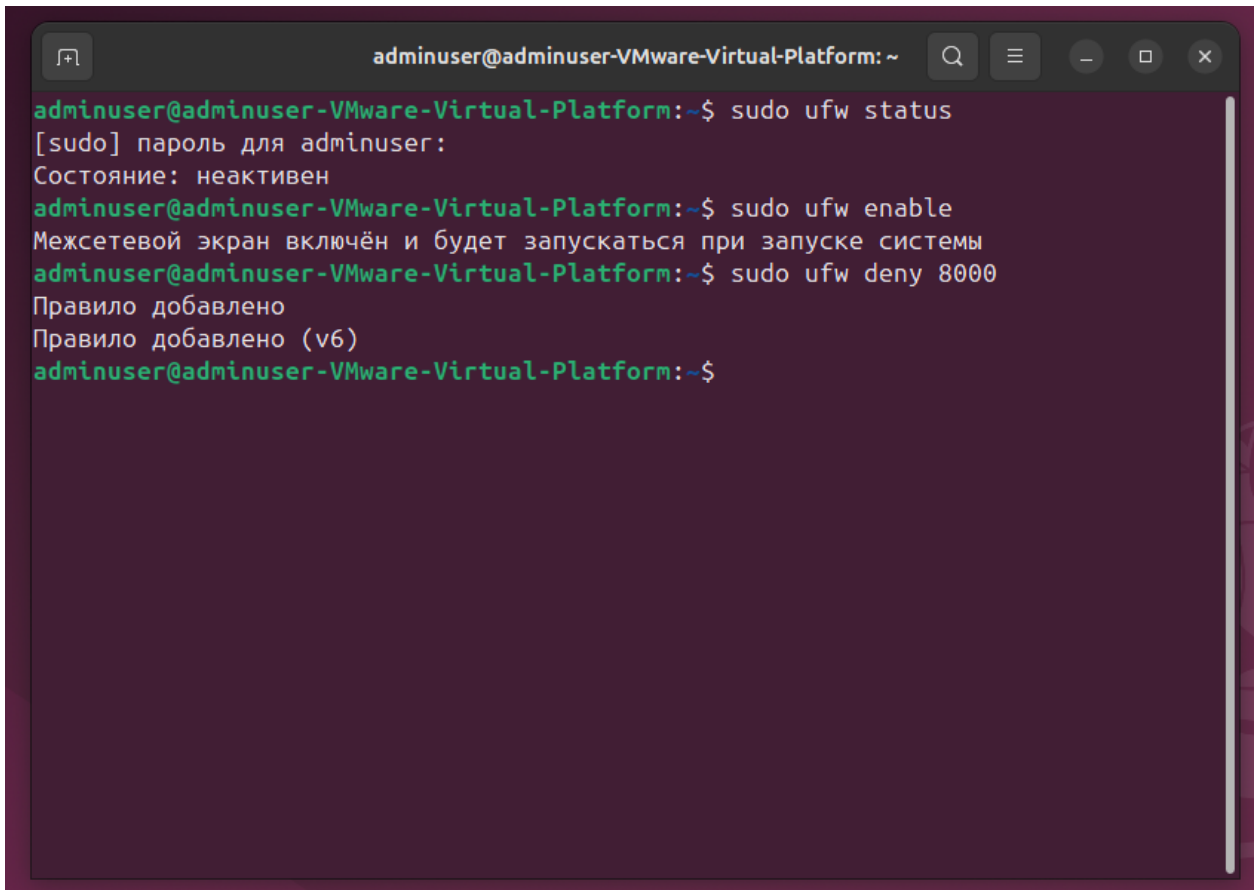
- ##### 1.2. Проверьте статус брандмауэра с помощью команды `sudo ufw status`. Если он выключен, то включите его через команду `sudo ufw enable`

A terminal window with a dark purple background and a title bar. The title bar contains the text 'adminuser@adminuser-VMware-Virtual-Platform: ~' and standard window control icons (search, menu, zoom, close). The terminal shows the following commands and output:

```
adminuser@adminuser-VMware-Virtual-Platform:~$ sudo ufw status
[sudo] пароль для adminuser:
Состояние: неактивен
adminuser@adminuser-VMware-Virtual-Platform:~$ sudo ufw enable
Межсетевой экран включён и будет запускаться при запуске системы
adminuser@adminuser-VMware-Virtual-Platform:~$
```

Рисунок 2 – Результат включения брандмауэра

1.3. Для закрытия порта `sudo ufw deny (порт)`

A terminal window with a dark purple background and a title bar. The title bar contains the text 'adminuser@adminuser-VMware-Virtual-Platform: ~' and standard window controls (search, menu, zoom, close). The terminal shows the following commands and output:

```
adminuser@adminuser-VMware-Virtual-Platform:~$ sudo ufw status
[sudo] пароль для adminuser:
Состояние: неактивен
adminuser@adminuser-VMware-Virtual-Platform:~$ sudo ufw enable
Межсетевой экран включён и будет запускаться при запуске системы
adminuser@adminuser-VMware-Virtual-Platform:~$ sudo ufw deny 8000
Правило добавлено
Правило добавлено (v6)
adminuser@adminuser-VMware-Virtual-Platform:~$
```

Рисунок 3 – Результат закрытия порта

2.1. Шифрование данных.

Откройте терминал и введите команду `sudo apt install cryptsetup` для установки пакета

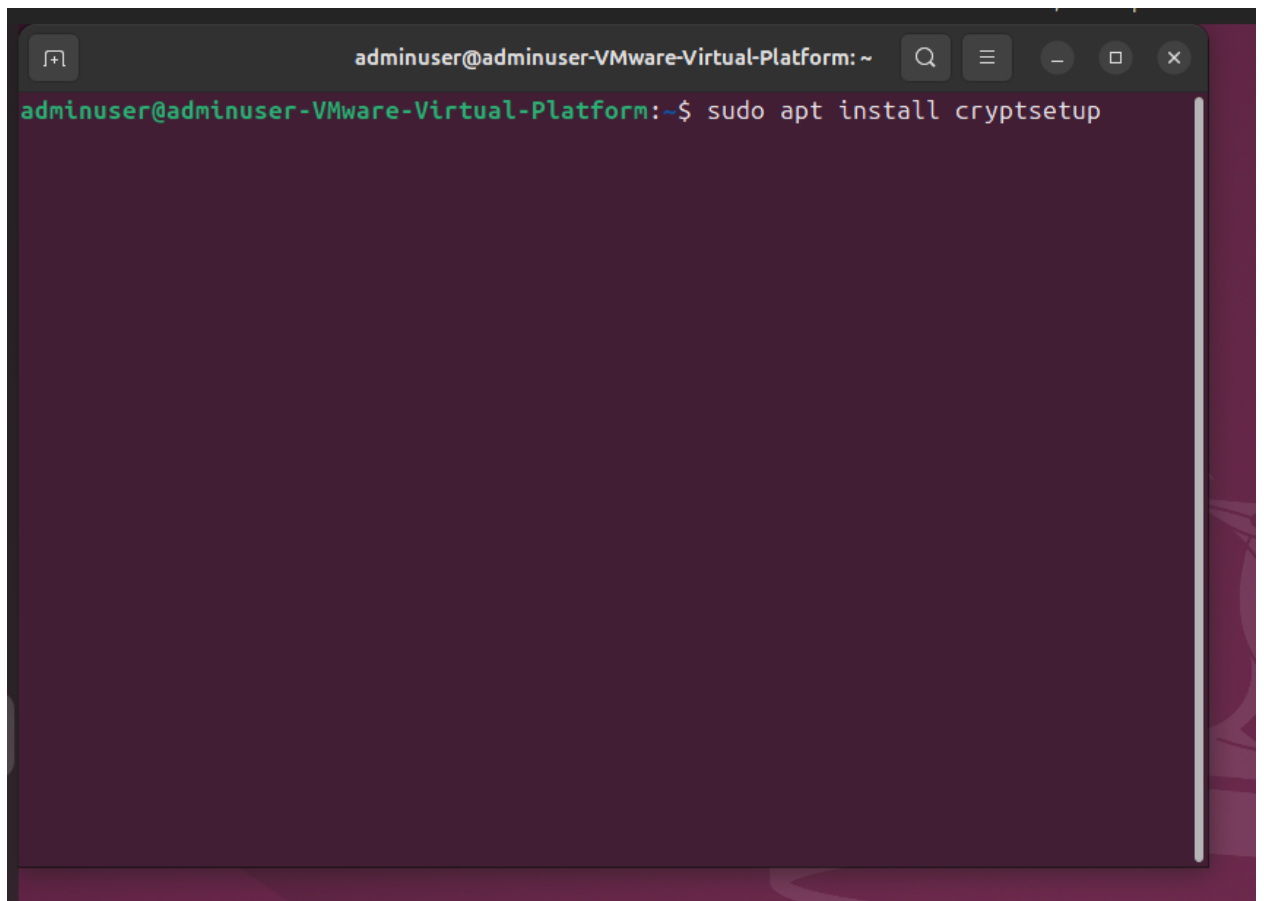


Рисунок 4 – Окно терминала

2.2. После установки сделайте зашифрованный раздел командой
`sudo cryptsetup luksFormat /dev/sdX`

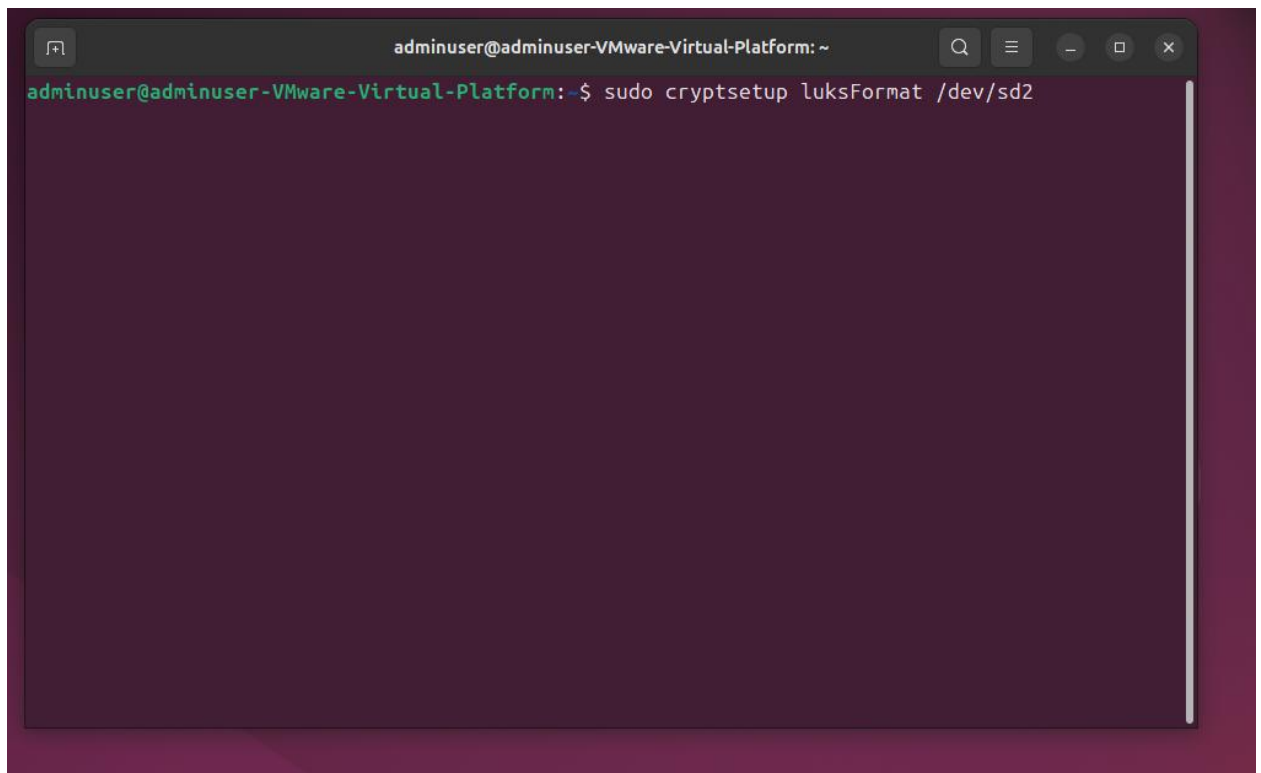


Рисунок 5 – Команда шифрования раздела диска

2.3. Подтвердите

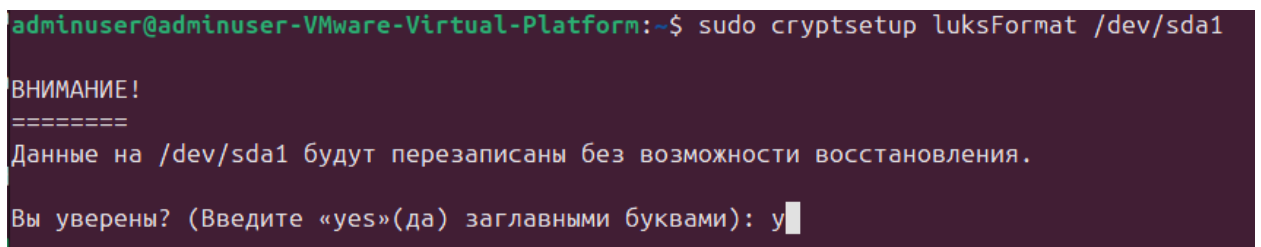


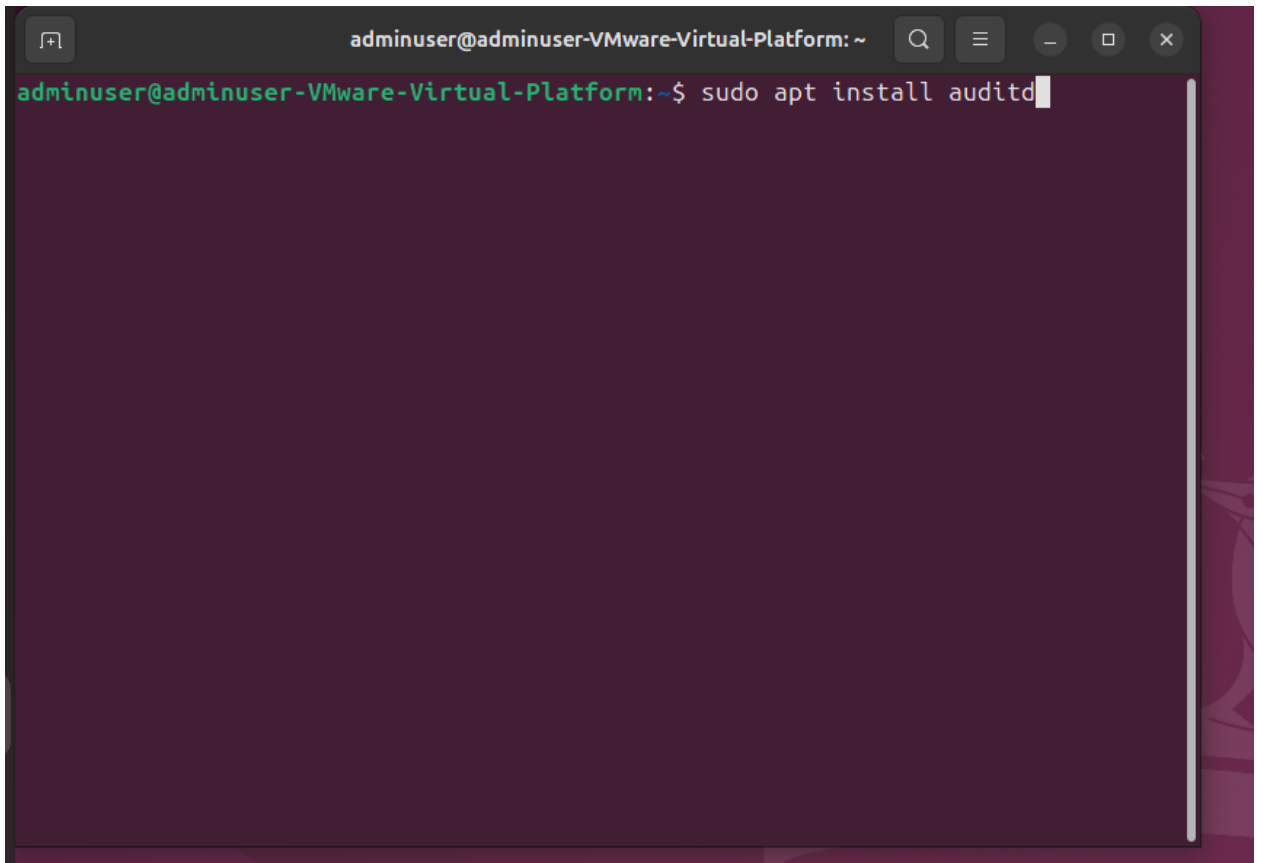
Рисунок 6 – Подтверждение шифрования раздела диска

2.4. После подтверждения введите кодовую фразу.

2.5. После шифрования раздел можно будет открыть с помощью команды
`sudo cryptsetup luksOpen /dev/sdX my_encrypted_volume`

3. Аудит системы

3.1. Установите пакет командой `sudo apt install auditd`

A terminal window with a dark purple background. The title bar at the top shows the user 'adminuser' and the host 'adminuser-VMware-Virtual-Platform'. The terminal prompt is 'adminuser@adminuser-VMware-Virtual-Platform:~\$'. The command 'sudo apt install auditd' is entered in white text, with a white cursor at the end of the line. The window has standard Linux window controls (minimize, maximize, close) on the right side of the title bar.

```
adminuser@adminuser-VMware-Virtual-Platform:~$ sudo apt install auditd
```

Рисунок 7 – Команда установки пакета auditd

3.2. После установки проверьте командой `sudo systemctl status auditd`

```

adminuser@adminuser-VMware-Virtual-Platform:~$ sudo systemctl status auditd
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: e>
   Active: active (running) since Sat 2025-11-01 00:31:28 +05; 1min 22s ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 14130 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
   Process: 14134 ExecStartPost=/sbin/augenrules --load (code=exited, status=0>
  Main PID: 14131 (auditd)
    Tasks: 2 (limit: 4545)
   Memory: 468.0K (peak: 2.2M)
      CPU: 46ms
   CGroup: /system.slice/auditd.service
           └─14131 /sbin/auditd

ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: enabled 1
ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: failure 1
ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: pid 14131
ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: rate_limit>
ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: backlog_li>
ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: lost 0
ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: backlog 4
ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: backlog_wa>
ноя 01 00:31:28 adminuser-VMware-Virtual-Platform augenrules[14145]: backlog_wa>
lines 1-23...skipping...
● auditd.service - Security Auditing Service
   Loaded: loaded (/usr/lib/systemd/system/auditd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2025-11-01 00:31:28 +05; 1min 22s ago
     Docs: man:auditd(8)
           https://github.com/linux-audit/audit-documentation
   Process: 14130 ExecStart=/sbin/auditd (code=exited, status=0/SUCCESS)
   Process: 14134 ExecStartPost=/sbin/augenrules --load (code=exited, status=0/SUCCESS)
  Main PID: 14131 (auditd)
    Tasks: 2 (limit: 4545)

```

Рисунок 8 – Результат проверки работы сервиса auditd

3.3. Добавьте файл в список отслеживания через редактирование конфиг файла

`-w /etc/passwd -p wa -k passwd_changes`

```

adminuser@adminuser-VMware-Virtual-Platform: ~
GNU nano 7.2 /etc/audit/rules.d/audit.rules *
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## This determine how long to wait in burst of events
--backlog_wait_time 60000

## Set failure mode to syslog
-f 1

-w /etc/passwd -p wa -k passwd_change

```

Рисунок 9 – Редактирование файла конфигурации

3.4. После редактирования перезапустите командой `sudo systemctl restart auditd` для применения настроек