**Руководство пользователя по установке и использованию антивируса ClamAV в операционной системе Ubuntu**

### 1. ВВЕДЕНИЕ

#### 1.1 Область применения

Настоящее руководство предназначено для пользователей операционной системы Ubuntu, осуществляющих установку, настройку и эксплуатацию антивирусного программного обеспечения ClamAV.

#### 1.2 Назначение программного средства

ClamAV — антивирус с открытым исходным кодом, предназначен для обнаружения и удаления вредоносных программ в среде GNU/Linux.

#### 1.3 Уровень подготовки пользователя

Для работы с программой необходимы базовые знания командной строки и наличие прав администратора (sudo).

#### 1.4 Условия эксплуатации

* Операционная система: Ubuntu 20.04 и выше
* Доступ в интернет для обновления сигнатур
* Права суперпользователя (sudo)

### 2. ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

* Название: ClamAV
* Тип: консольное приложение
* Поддержка обновления баз: да
* Поддержка демона: да (clamd)
* Распространение: свободное (open-source)

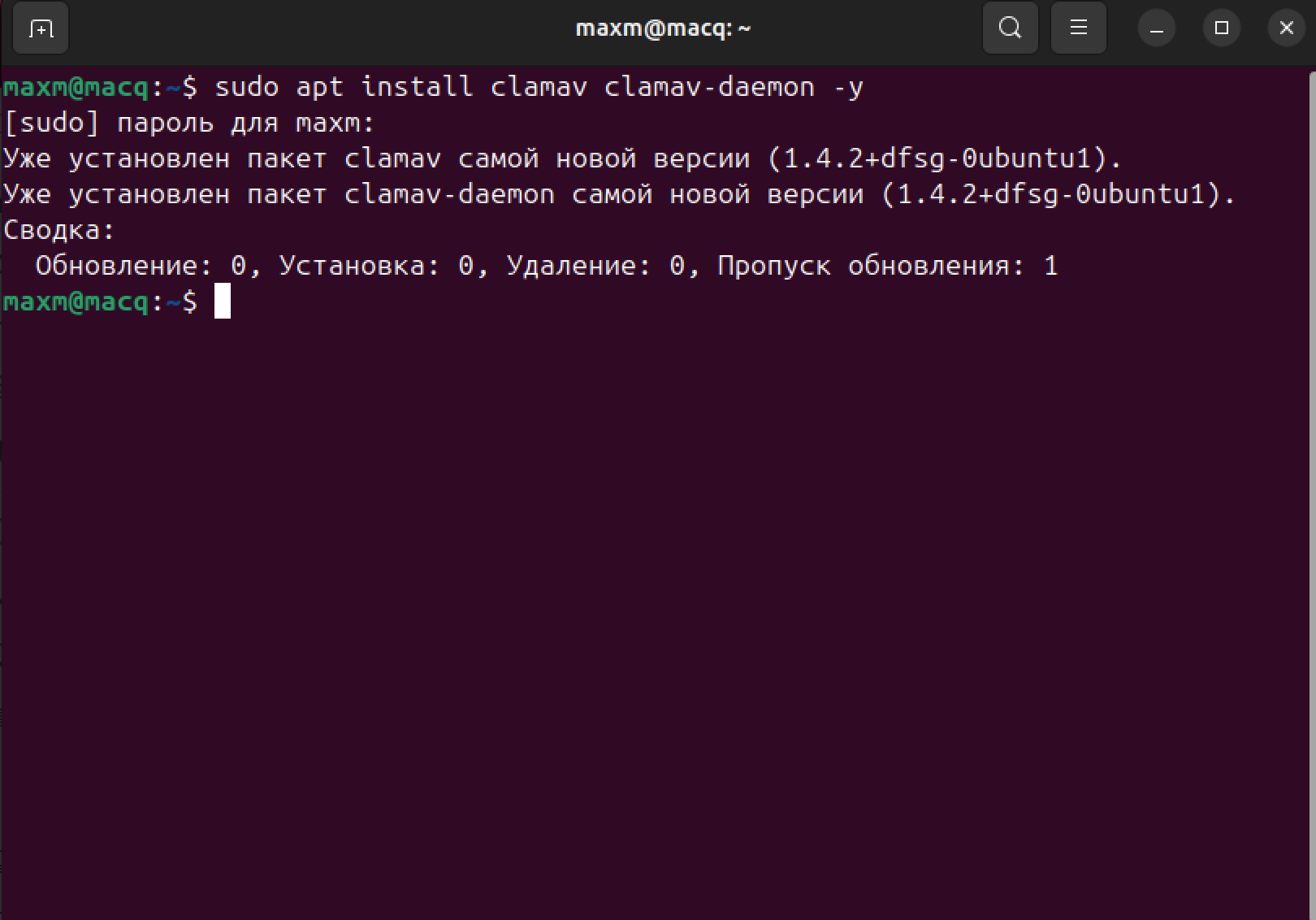
### 3. ПОДГОТОВКА К РАБОТЕ

#### 3.1 Установка программы

Откройте терминал и выполните следующие команды:

sudo apt update

sudo apt install clamav clamav-daemon -y

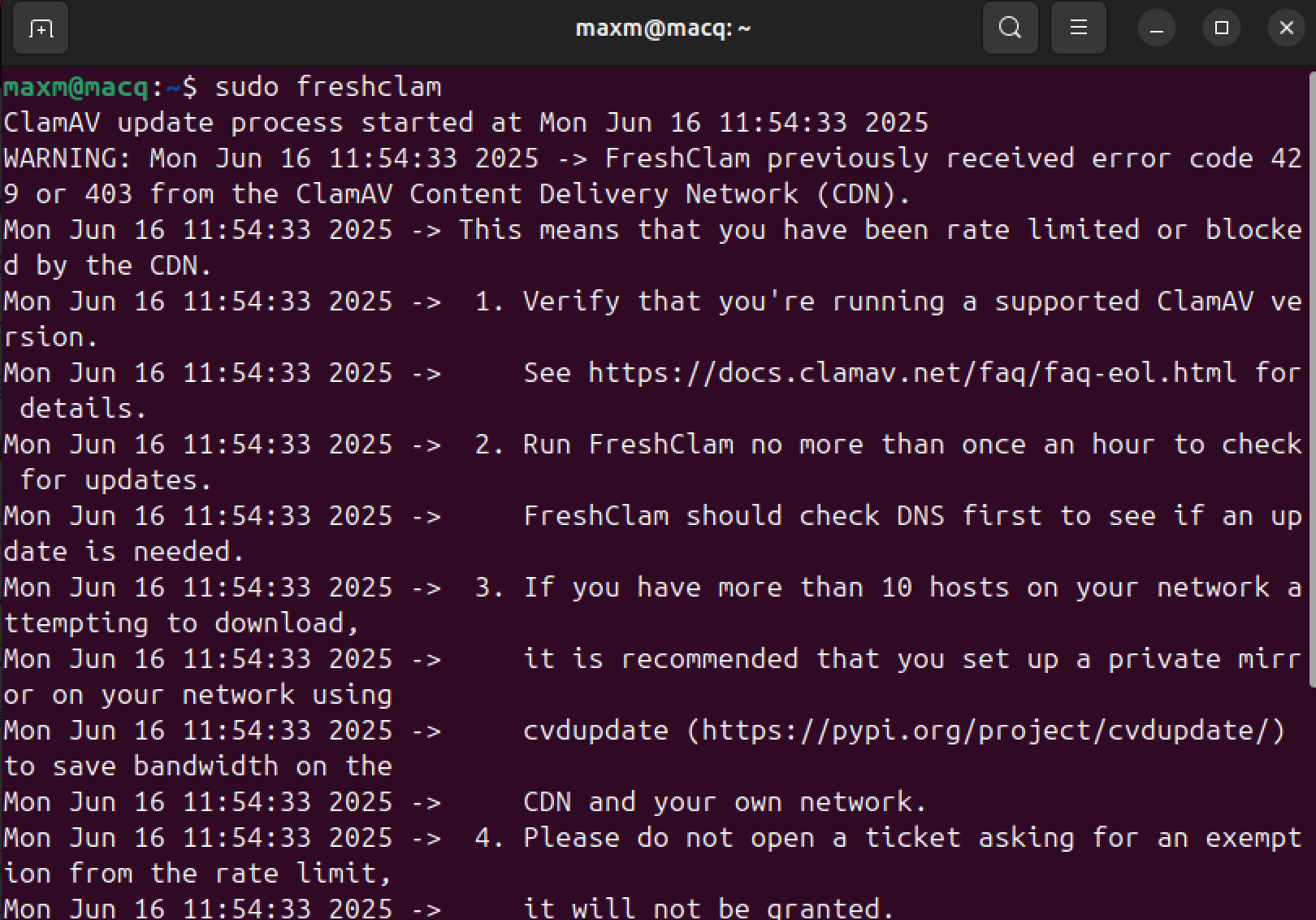


### 4. ОБНОВЛЕНИЕ АНТИВИРУСНЫХ БАЗ

Перед началом использования необходимо обновить базы данных вирусов.

Выполните обновление вручную:

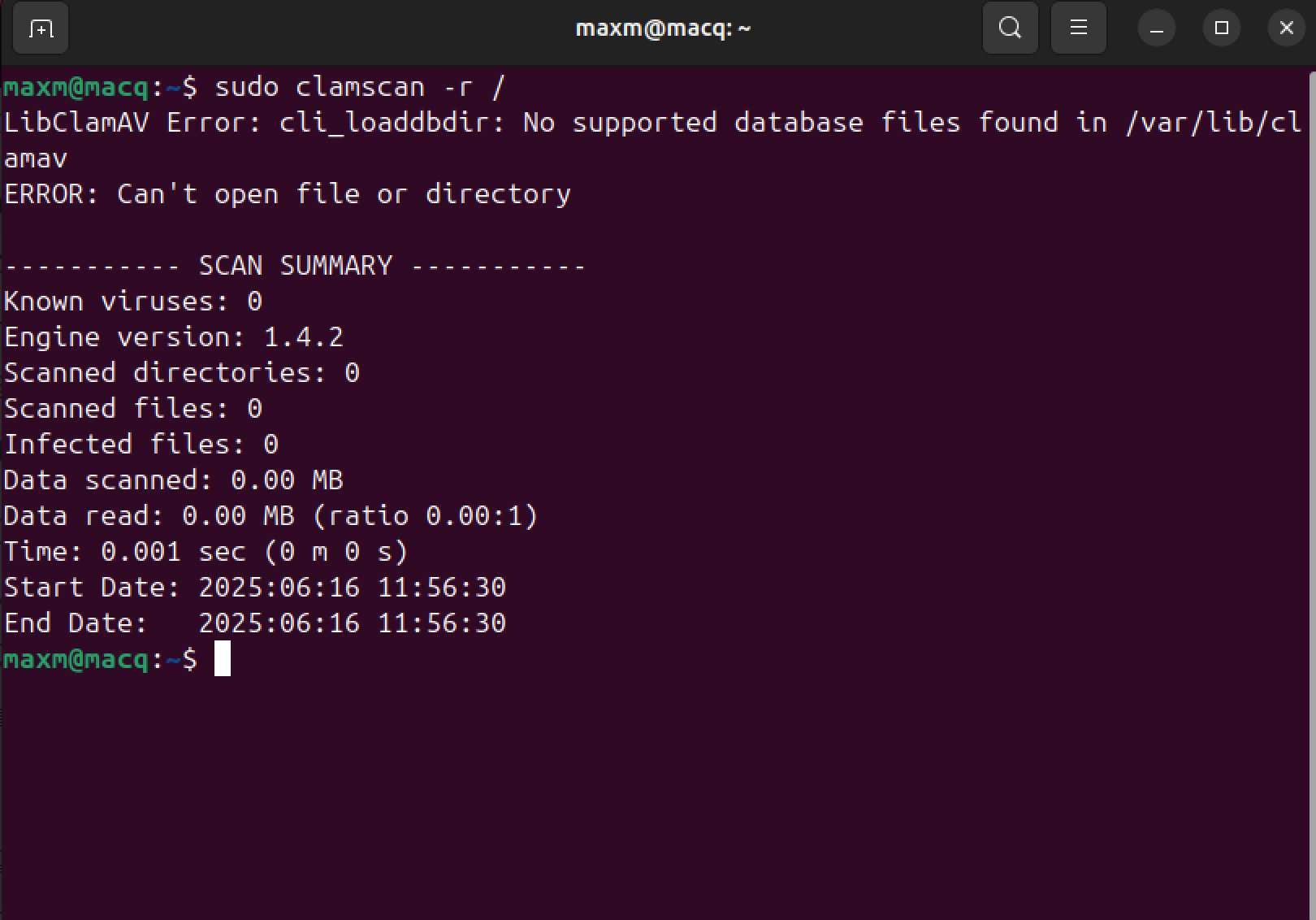
sudo freshclam



### 5. ПРОВЕДЕНИЕ СКАНИРОВАНИЯ

#### 5.1 Сканирование всей системы

sudo clamscan -r /



#### 5.2 Сканирование конкретной директории

clamscan -r /путь/к/папке

### 7. УПРАВЛЕНИЕ СЛУЖБОЙ CLAMAV-DAEMON

#### 7.1 Запуск

sudo systemctl start clamav-daemon

#### 7.2 Остановка

sudo systemctl stop clamav-daemon

#### 7.3 Проверка статуса

sudo systemctl status clamav-daemon

### 11. ЗАКЛЮЧЕНИЕ

ClamAV является надежным инструментом для базовой антивирусной защиты на Linux-системах. Рекомендуется регулярное обновление баз и сканирование системы.