



[Главная](#) >> [Инструкции](#) >> Простая настройка WireGuard Linux

Простая настройка WireGuard Linux

Опубликовано: 24 августа, 2022 от [admin](#), 7 комментариев, время чтения: 6 минут

WireGuard – это набирающий популярность VPN сервер, который работает на уровне ядра Linux. Это позволяет ему обрабатывать пакеты намного быстрее по сравнению с OpenVPN. С помощью WireGuard вы можете создать частную виртуальную сеть и объединить компьютеры, которые находятся в разных домах или даже городах, точно так же как и с помощью OpenVPN.

В большинстве инструкций предлагается всё делать вручную, устанавливать программу, генерировать конфигурационные файлы, однако если вы не хотите в этом разбираться и вам достаточно стандартных настроек, то всё можно сделать гораздо проще. В этой статье будет рассмотрена простая установка WireGuard на примере Ubuntu.

Содержание статьи:

- [Настройка WireGuard сервера в Linux](#)
- [Настройка клиента WireGuard](#)
- [Выходы](#)

Настройка WireGuard сервера в Linux

Существует скрипт для быстрого развертывания WireGuard. Он поддерживает не только Ubuntu, но и Debian, Fedora, CentOS, Arch Linux и Oracle Linux. Этот скрип

Privacy

работает аналогично скрипту для [простого развертывания OpenVPN](#). Программа задаст несколько вопросов, установит WireGuard и сгенерирует конфигурационные файлы для сервера и клиента. После установки с помощью скрипта можно добавлять новых клиентов, ограничивать доступ для старых или полностью удалить WireGuard. Таким образом, можно детально не разбираться самому как настроить WireGuard.

Выполните следующую команду для того чтобы скачать последнюю версию скрипта с GitHub:

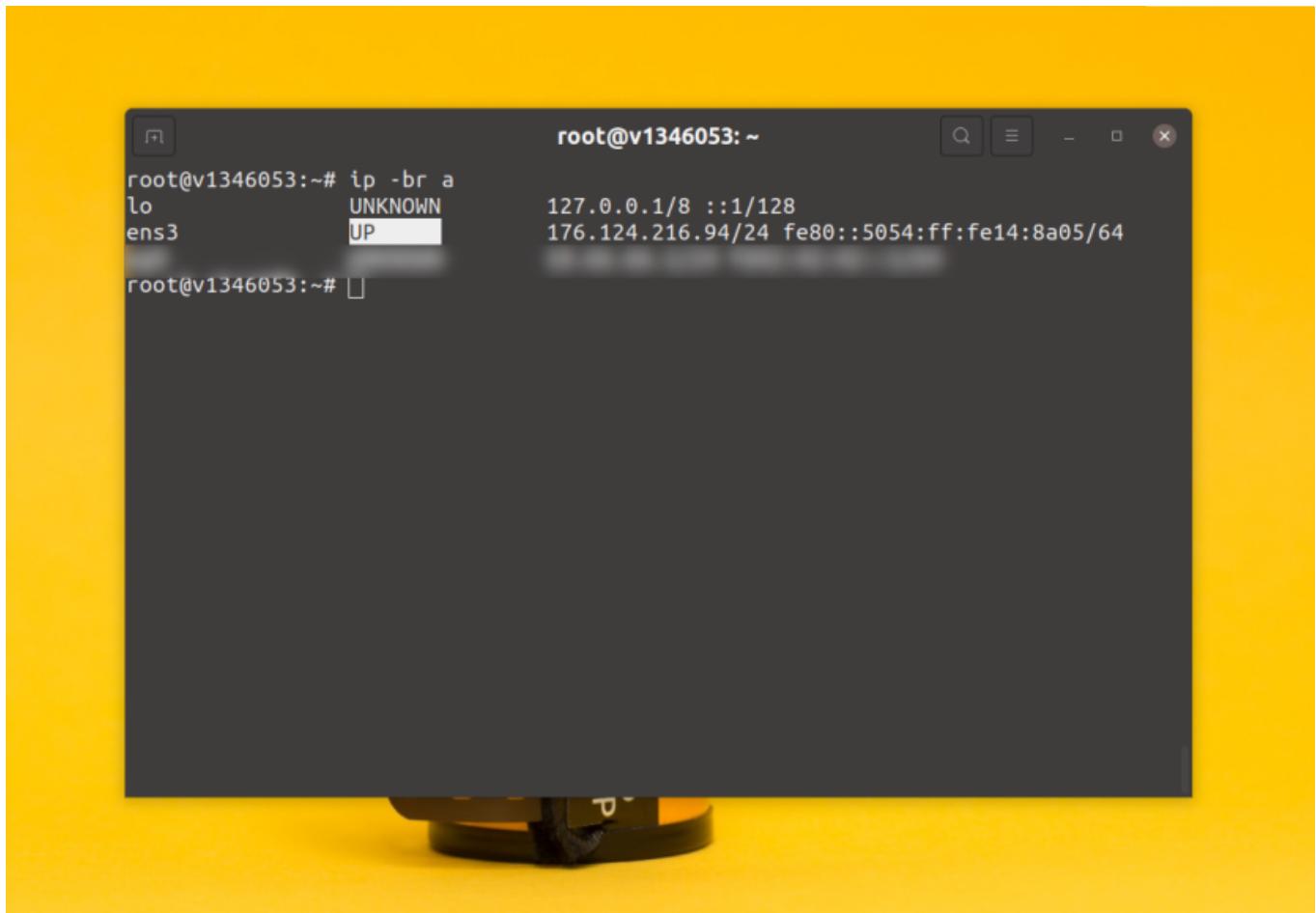
```
$ curl -O https://raw.githubusercontent.com/angristan/wireguard-install/master/wireguard-install.sh
```

Затем дайте файлу скрипта права на выполнение:

```
$ chmod +x wireguard-install.sh
```

Прежде чем запускать скрипт желательно посмотреть публичный IP вашего сервера. Для этого можно воспользоваться командой:

```
$ ip -br a
```



Команда отобразит список сетевых интерфейсов и их IP адреса. Как правило, реальный сетевой интерфейс имеет состояние UP. В данном случае это `ens0`. Если вы хотите подключаться к VPN серверу из интернет или обойти блокировки, вам необходимо установить его на VPS или другой сервер в сети. Список VPS для VPN можно найти [здесь](#).

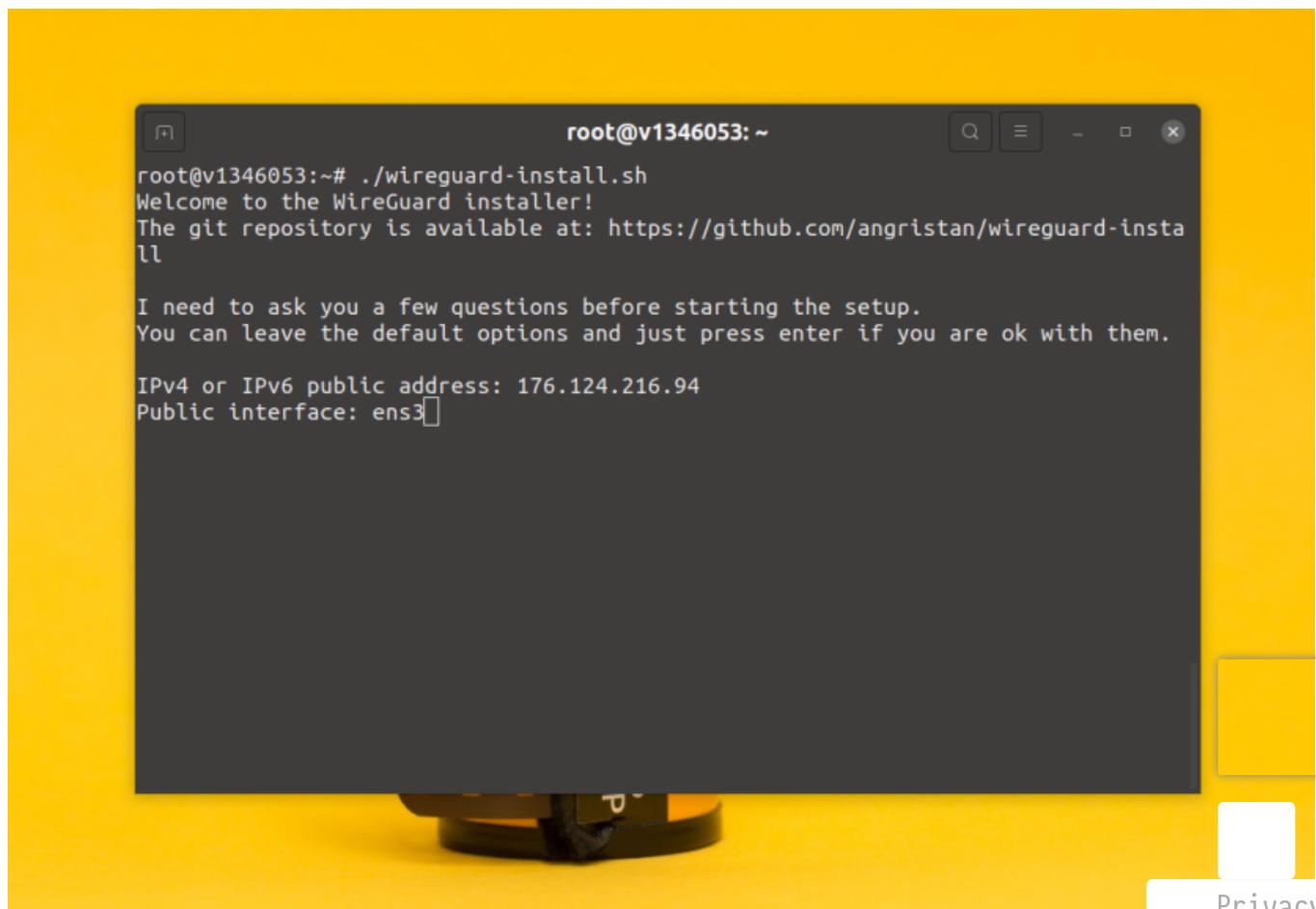
Для запуска скрипта выполните команду:

```
$ ./wireguard-install.sh
```

Первые два вопроса будут о внешнем IP адресе и сетевом интерфейсе, которые вы посмотрели ранее. Если у вас только один интерфейс, скорее всего, программа определит их верно. Если же несколько, возможно придется поправить:

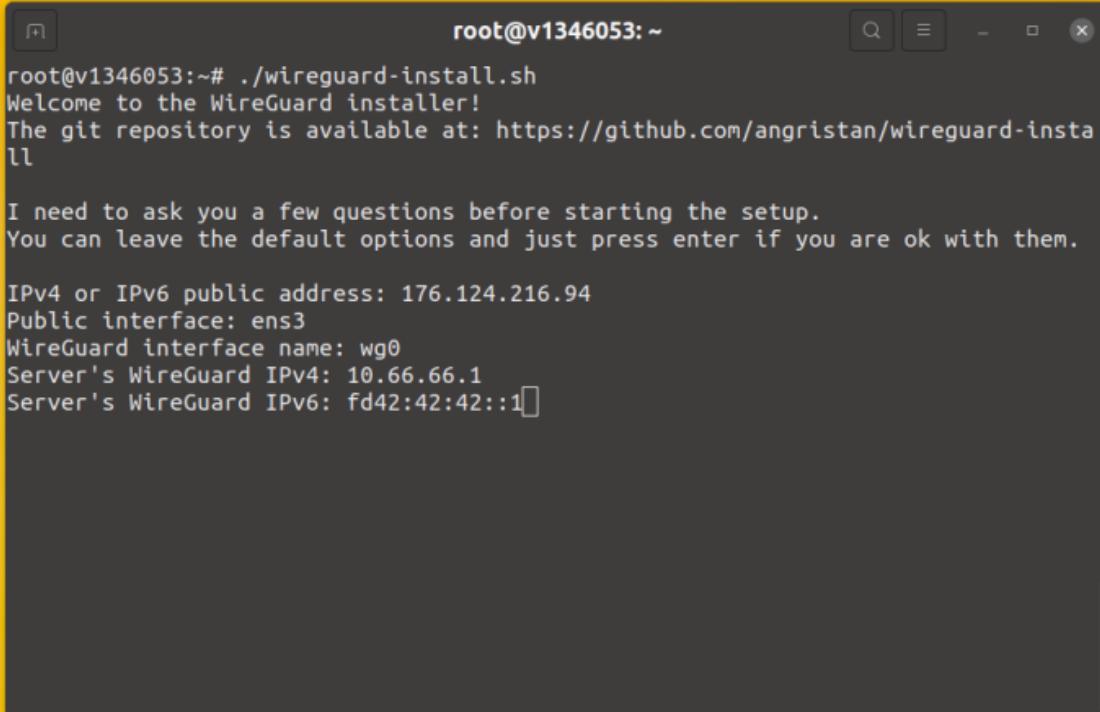


Далее нужно выбрать имя сетевого интерфейса для WireGuard, можно оставить по умолчанию:



Privacy

Следующие два вопроса – желаемый IP адрес сервера WireGuard в создаваемой виртуальной сети для IPv4 и IPv6. По умолчанию скрипт предлагает использовать 10.66.66.1:



```
root@v1346053:~# ./wireguard-install.sh
Welcome to the WireGuard installer!
The git repository is available at: https://github.com/angristan/wireguard-installer

I need to ask you a few questions before starting the setup.
You can leave the default options and just press enter if you are ok with them.

IPv4 or IPv6 public address: 176.124.216.94
Public interface: ens3
WireGuard interface name: wg0
Server's WireGuard IPv4: 10.66.66.1
Server's WireGuard IPv6: fd42:42:42::1
```

На следующем шаге нужно настроить порт, на котором будет доступен WireGuard:

```
root@v1346053:~# ./wireguard-install.sh
Welcome to the WireGuard installer!
The git repository is available at: https://github.com/angristan/wireguard-install

I need to ask you a few questions before starting the setup.
You can leave the default options and just press enter if you are ok with them.

IPv4 or IPv6 public address: 176.124.216.94
Public interface: ens3
WireGuard interface name: wg0
Server's WireGuard IPv4: 10.66.66.1
Server's WireGuard IPv6: fd42:42:42::1
Server's WireGuard port [1-65535]: 57397
```



WireGuard умеет менять настройки DNS клиентов при подключении. На этом шаге можно указать DNS серверы, которые следует использовать:

```
root@v1346053:~# ./wireguard-install.sh
Welcome to the WireGuard installer!
The git repository is available at: https://github.com/angristan/wireguard-install

I need to ask you a few questions before starting the setup.
You can leave the default options and just press enter if you are ok with them.

IPv4 or IPv6 public address: 176.124.216.94
Public interface: ens3
WireGuard interface name: wg0
Server's WireGuard IPv4: 10.66.66.1
Server's WireGuard IPv6: fd42:42:42::1
Server's WireGuard port [1-65535]: 57397
First DNS resolver to use for the clients: 8.8.8.8
Second DNS resolver to use for the clients (optional): 94.140.15.15
```

После этого нажмите любую клавишу для того чтобы запустить установку необходимых пакетов и создание конфигурационных файлов:

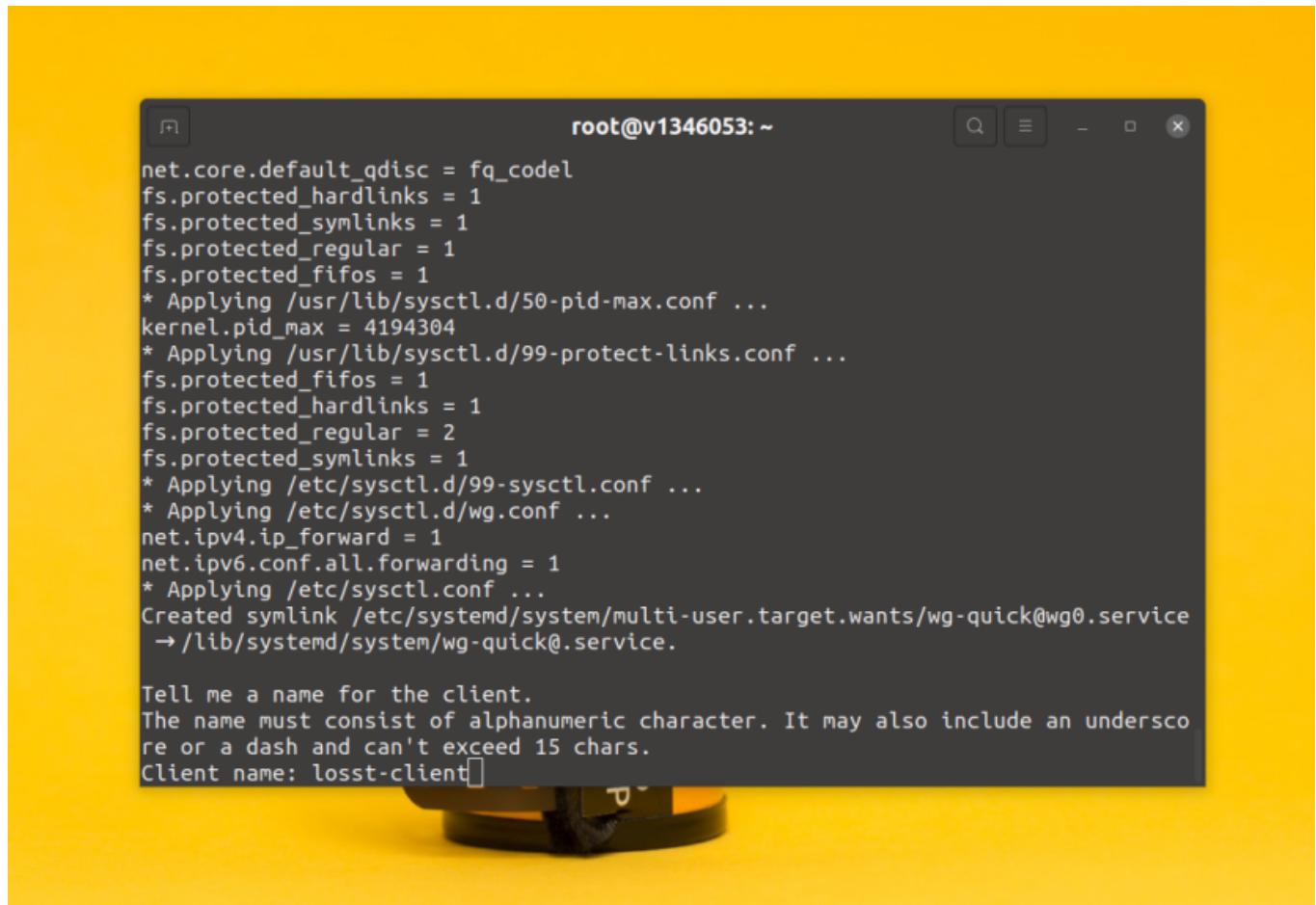
```
root@v1346053:~# ./wireguard-install.sh
Welcome to the WireGuard installer!
The git repository is available at: https://github.com/angristan/wireguard-install

I need to ask you a few questions before starting the setup.
You can leave the default options and just press enter if you are ok with them.

IPv4 or IPv6 public address: 176.124.216.94
Public interface: ens3
WireGuard interface name: wg0
Server's WireGuard IPv4: 10.66.66.1
Server's WireGuard IPv6: fd42:42:42::1
Server's WireGuard port [1-65535]: 57397
First DNS resolver to use for the clients: 8.8.8.8
Second DNS resolver to use for the clients (optional): 94.140.15.15

Okay, that was all I needed. We are ready to setup your WireGuard server now.
You will be able to generate a client at the end of the installation.
Press any key to continue...
```

После того как установка завершится скрипт предложит создать конфигурацию для первого клиента. Достаточно ввести имя. Оно не должно быть длиннее 15 символов:



```
root@v1346053: ~
net.core.default_qdisc = fq_codel
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
fs.protected_regular = 1
fs.protected_fifos = 1
* Applying /usr/lib/sysctl.d/50-pid-max.conf ...
kernel.pid_max = 4194304
* Applying /usr/lib/sysctl.d/99-protect-links.conf ...
fs.protected_fifos = 1
fs.protected_hardlinks = 1
fs.protected_regular = 2
fs.protected_symlinks = 1
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.d/wg.conf ...
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding = 1
* Applying /etc/sysctl.conf ...
Created symlink /etc/systemd/system/multi-user.target.wants/wg-quick@wg0.service
→ /lib/systemd/system/wg-quick@.service.

Tell me a name for the client.
The name must consist of alphanumeric character. It may also include an underscore or a dash and can't exceed 15 chars.
Client name: losst-client
```

Далее надо указать желаемый IP адрес клиента IPv4 и IPv6. Здесь IP адрес задается при создании конфигурации и для каждого клиента всегда будет статическим:



```
root@v1346053:~  
fs.protected_symlinks = 1  
fs.protected_regular = 1  
fs.protected_fifos = 1  
* Applying /usr/lib/sysctl.d/50-pid-max.conf ...  
kernel.pid_max = 4194304  
* Applying /usr/lib/sysctl.d/99-protect-links.conf ...  
fs.protected_fifos = 1  
fs.protected_hardlinks = 1  
fs.protected_regular = 2  
fs.protected_symlinks = 1  
* Applying /etc/sysctl.d/99-sysctl.conf ...  
* Applying /etc/sysctl.d/wg.conf ...  
net.ipv4.ip_forward = 1  
net.ipv6.conf.all.forwarding = 1  
* Applying /etc/sysctl.conf ...  
Created symlink /etc/systemd/system/multi-user.target.wants/wg-quick@wg0.service  
→ /lib/systemd/system/wg-quick@.service.  
  
Tell me a name for the client.  
The name must consist of alphanumeric character. It may also include an underscore or a dash and can't exceed 15 chars.  
Client name: losst-client  
Client's WireGuard IPv4: 10.66.66.2  
Client's WireGuard IPv6: fd42:42:42::2
```

После этого скрипт сообщит что конфигурация создана и вы можете скачать её на свой компьютер или отсканировать QR код на телефоне:



```
root@v1346053:~  
  
It is also available in /root/wg0-client-losst-client.conf  
If you want to add more clients, you simply need to run this script another time  
!  
root@v1346053:~#
```

Privacy

Настройка сервера WireGuard завершена. Теперь можно переходить к настройке клиента.

Настройка клиента WireGuard

На компьютере с которого вы хотите подключиться к WireGuard его тоже необходимо установить. В Ubuntu и Debian команда установки будет выглядеть следующим образом:

```
$ sudo apt install wireguard
```

Кроме того, если в системе не установлены пакеты resolvconf и iptables их надо установить:

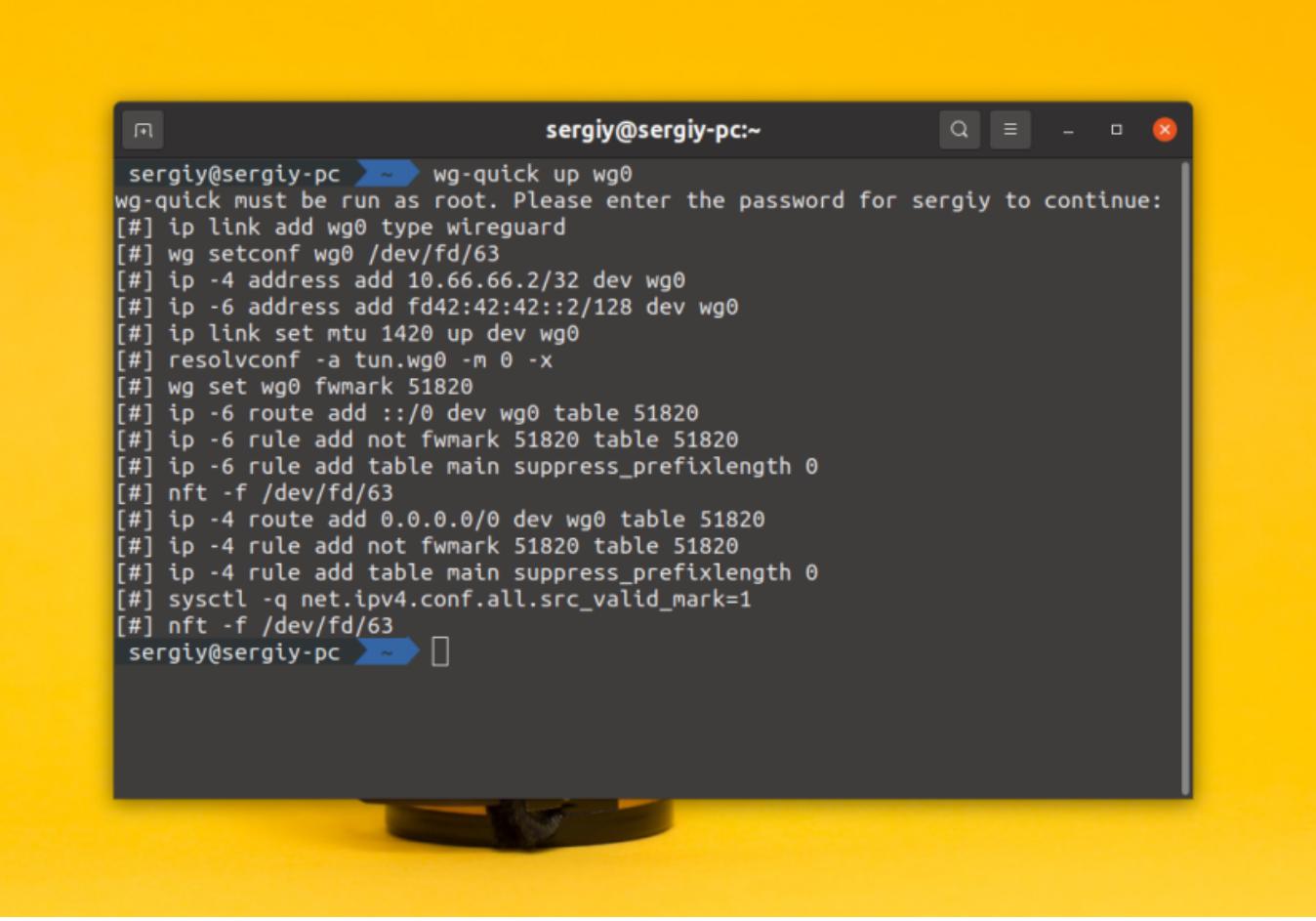
```
$ sudo apt install resolvconf iptables
```

После этого переместите скачанный конфигурационный файл клиента WireGuard в папку **/etc/wireguard** и переименуйте в **wg0.conf**. Имя конфигурационного файла должно соответствовать имени сетевого интерфейса, который будет создан WireGuard. Например:

```
$ sudo mv ~/wg0-client-losst.conf /etc/wireguard/wg0.conf
```

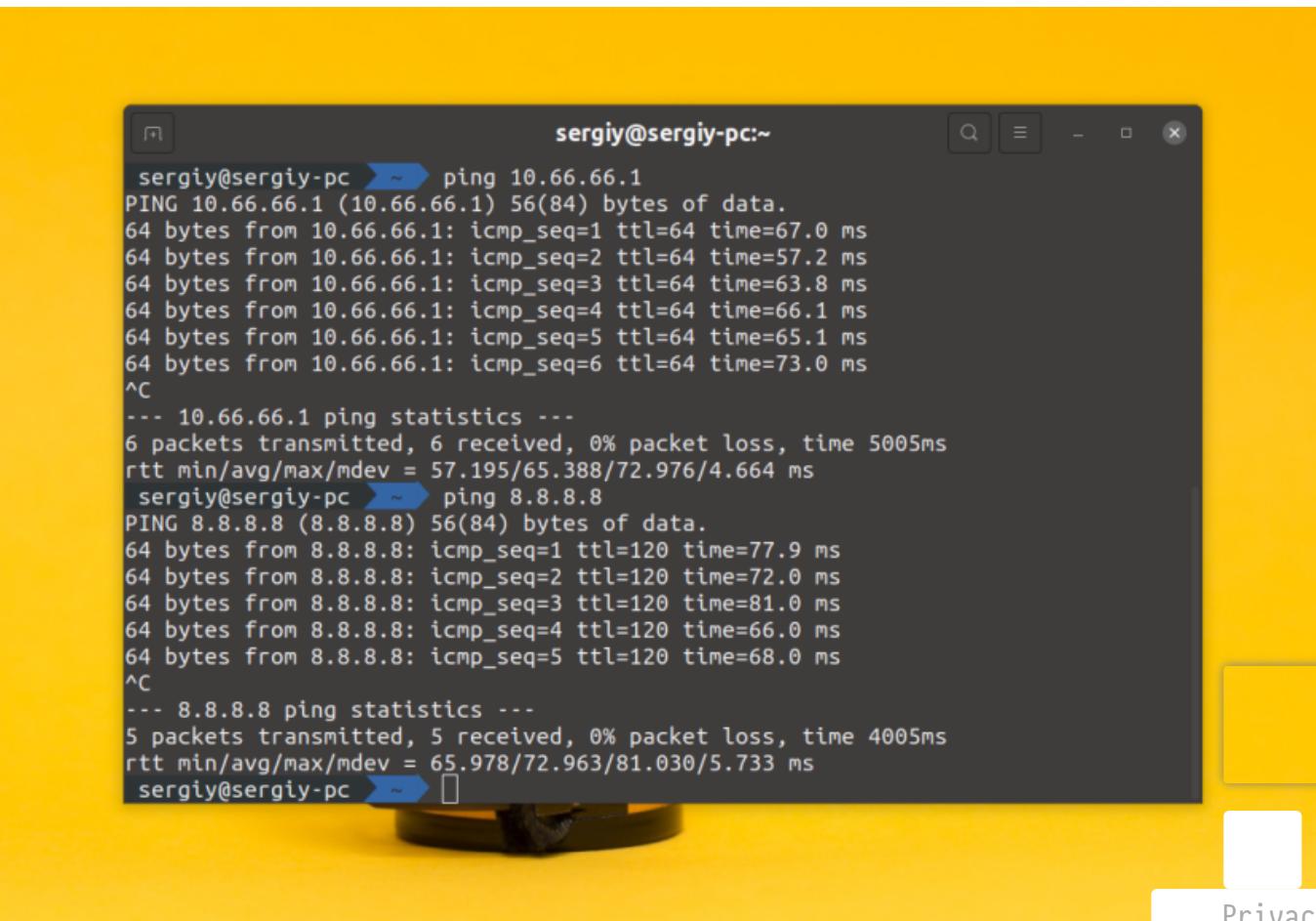
Или вы можете просто скопировать содержимое файла на сервере и вставить его в локальный **/etc/wireguard/wg0.conf**. Файл довольно небольшой, в отличии от OpenVPN. Теперь вы можете подключится к серверу используя команду **wg-quick**:

```
$ wg-quick up wg0
```



```
sergiy@sergiy-pc ➤ wg-quick up wg0
wg-quick must be run as root. Please enter the password for sergiy to continue:
[#] ip link add wg0 type wireguard
[#] wg setconf wg0 /dev/fd/63
[#] ip -4 address add 10.66.66.2/32 dev wg0
[#] ip -6 address add fd42:42:42::2/128 dev wg0
[#] ip link set mtu 1420 up dev wg0
[#] resolvconf -a tun.wg0 -m 0 -x
[#] wg set wg0 fwmark 51820
[#] ip -6 route add ::/0 dev wg0 table 51820
[#] ip -6 rule add not fwmark 51820 table 51820
[#] ip -6 rule add table main suppress_prefixlength 0
[#] nft -f /dev/fd/63
[#] ip -4 route add 0.0.0.0/0 dev wg0 table 51820
[#] ip -4 rule add not fwmark 51820 table 51820
[#] ip -4 rule add table main suppress_prefixlength 0
[#] sysctl -q net.ipv4.conf.all.src_valid_mark=1
[#] nft -f /dev/fd/63
sergiy@sergiy-pc ➤
```

Вы можете убедится что виртуальная сеть работает, попробовав пинговать VPN сервер по внутреннему адресу 10.66.66.1. Также можно проверить что интернет тоже работает:



```
sergiy@sergiy-pc ➤ ping 10.66.66.1
PING 10.66.66.1 (10.66.66.1) 56(84) bytes of data.
64 bytes from 10.66.66.1: icmp_seq=1 ttl=64 time=67.0 ms
64 bytes from 10.66.66.1: icmp_seq=2 ttl=64 time=57.2 ms
64 bytes from 10.66.66.1: icmp_seq=3 ttl=64 time=63.8 ms
64 bytes from 10.66.66.1: icmp_seq=4 ttl=64 time=66.1 ms
64 bytes from 10.66.66.1: icmp_seq=5 ttl=64 time=65.1 ms
64 bytes from 10.66.66.1: icmp_seq=6 ttl=64 time=73.0 ms
^C
--- 10.66.66.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 57.195/65.388/72.976/4.664 ms
sergiy@sergiy-pc ➤ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=120 time=77.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=120 time=72.0 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=120 time=81.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=120 time=66.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=120 time=68.0 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 65.978/72.963/81.030/5.733 ms
sergiy@sergiy-pc ➤
```

По умолчанию весь трафик клиента перенаправляется через VPN сервер. Это настроено в конфигурационном файле клиента с помощью директивы **AllowedIPs**. Здесь указано **0.0.0.0**, что означает все адреса, однако вы можете изменить эти настройки и перенаправлять только нужный трафик, или вообще не перенаправлять. Посмотреть состояние подключения WireGuard можно командой:

```
$ wg-quick status
```

```
sergiy@sergiy-pc ~ $ sudo wg show
interface: wg0
  public key: [REDACTED]
  private key: (hidden)
  listening port: 45728
  fwmark: 0xcab6c

peer:
  preshared key: (hidden)
  endpoint: 176.124.216.94:57397
  allowed ips: 0.0.0.0/0, ::/0
  latest handshake: 1 minute, 13 seconds ago
  transfer: 687.38 KiB received, 665.93 KiB sent
sergiy@sergiy-pc ~ $
```

Если вы хотите чтобы WireGuard подключался к серверу автоматически после загрузки системы можно добавить его в автозагрузку systemctl:

```
$ sudo systemctl enable wg-quick@wg0.service
```

Для запуска используйте:

```
$ sudo systemctl start wg-quick@wg0.service
```

А состояние можно проверить с помощью команды status:

Privacy

```
$ sudo systemctl status wg-quick@wg0.service
```

```
● wg-quick@wg0.service - WireGuard via wg-quick(8) for wg0
   Loaded: loaded (/lib/systemd/system/wg-quick@.service; enabled; vendor pre>
   Active: active (exited) since Mon 2022-08-22 21:38:54 EEST; 7s ago
     Docs: man:wg-quick(8)
           man:wg(8)
           https://www.wireguard.com/
           https://www.wireguard.com/quickstart/
           https://git.zx2c4.com/wireguard-tools/about/src/man/wg-quick.8
           https://git.zx2c4.com/wireguard-tools/about/src/man/wg.8
   Process: 507777 ExecStart=/usr/bin/wg-quick up wg0 (code=exited, status=0/S>
 Main PID: 507777 (code=exited, status=0/SUCCESS)

авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] ip -6 route add ::/0 dev wg0 ta>
авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] ip -6 rule add not fwmark 51820>
авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] ip -6 rule add table main suppr>
авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] nft -f /dev/fd/63
авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] ip -4 route add 0.0.0.0/0 dev w>
авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] ip -4 rule add not fwmark 51820>
авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] ip -4 rule add table main suppr>
авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] sysctl -q net.ipv4.conf.all.src>
авг 22 21:38:54 sergiy-pc wg-quick[507777]: [#] nft -f /dev/fd/63
авг 22 21:38:54 sergiy-pc systemd[1]: Finished WireGuard via wg-quick(8) for wg>
lines 1-22/22 (END)
```

Теперь вы знаете как выполняется настройка клиента WireGuard.

Выводы

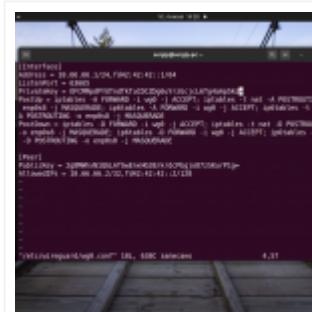
В этой статье мы рассмотрели как выполняется простая настройка WireGuard в Linux. Как видите, не обязательно разбираться в тонкостях работы с программой для того чтобы установить её на сервер. По моим субъективным ощущениям интернет с WireGuard быстрее по сравнению с OpenVPN. А каким VPN вы пользуетесь? Напишите в комментариях!

Обнаружили ошибку в тексте? Сообщите мне об этом. Выделите текст с ошибкой и нажмите Ctrl+Enter.

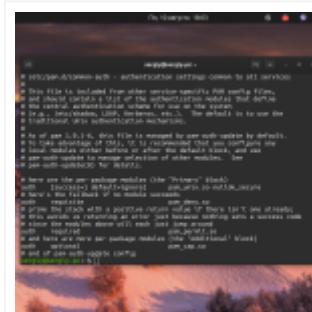
Похожие записи



Простая настройка
OpenVPN Linux



Установка
WireGuard в Ubuntu



Настройка РАМ в
Linux



Настройка веб-
камеры Linux

Оцените статью

(5 оценок, среднее: 4,20 из 5)



Статья распространяется под лицензией Creative Commons ShareAlike 4.0 при копировании материала ссылка на источник обязательна .

[Инструкции](#)

Об авторе



ADMIN

Основатель и администратор сайта losst.ru, увлекаюсь открытым программным обеспечением и операционной системой Linux. В качестве основной ОС сейчас использую Ubuntu. Кроме Linux, интересуюсь всем, что связано с информационными технологиями и современной наукой.

[Privacy](#)

7 комментариев к “Простая настройка WireGuard Linux”



Ave

24 августа, 2022 в 1:35 пп

Вот почему они не сделают нормальный GUI клиент для Линуксов?
Под виндой и андроидом все предельно просто – установил клиент, в несколько кликов добавил конфиг – все, готово.
Под линуком же сплошное трахомозгие, степень которого зависит от того, на каком дистрибутиве вы решили осесть. =\

[Ответить](#)



admin

24 августа, 2022 в 7:26 пп

Есть NetworkManager. Вроде там можно управлять и OpenVPN и WireGuard.

[Ответить](#)



Сергей

24 августа, 2022 в 3:20 пп

Главный вопрос не то какой vpn сервер выбрать и как его настроить, а то как найти безопасный хостинг для сервера и как оплатить его.

[Ответить](#)

[Privacy](#)

**Арсений**25 августа, 2022 в 8:57 дп

Из самых простых советую aeza. Компания российская, чтобы есть за границей. Сейчас можно взять простейший сервер в Амстердаме за 99р в месяц. Я там разворачивал сервера, vpn нормально работает, блокировок нет. Если есть желание заморачиваться то тогда free tier от амazona AWS, но надо карту делать и пополнять её долларами.

Ответить**UINREG00**26 августа, 2022 в 10:14 дп

только все сервисы проверки ip адресов показывают, что их сервера находятся не в Амстердаме, а в России, тп говорит, что данные скоро обновятся и будет показывать Амстердам, но спустя два месяца тестирования ничего не поменялось и сайты которые блокируют загрузку с ip адресов России и дальше продолжают это делать.

Ответить**Andrey**28 августа, 2022 в 3:36 пп

И всё же самая простая настройка – это докер-контейнер:
<https://github.com/WeeJewel/wg-easy>

Ответить**Николай**17 октября, 2022 в 6:44 дп[Privacy](#)

Докер медленнее работает.

[Ответить](#)

Оставьте комментарий

Имя *

Email

Я прочитал и принимаю политику конфиденциальности. Подробнее [Политика конфиденциальности](#) *

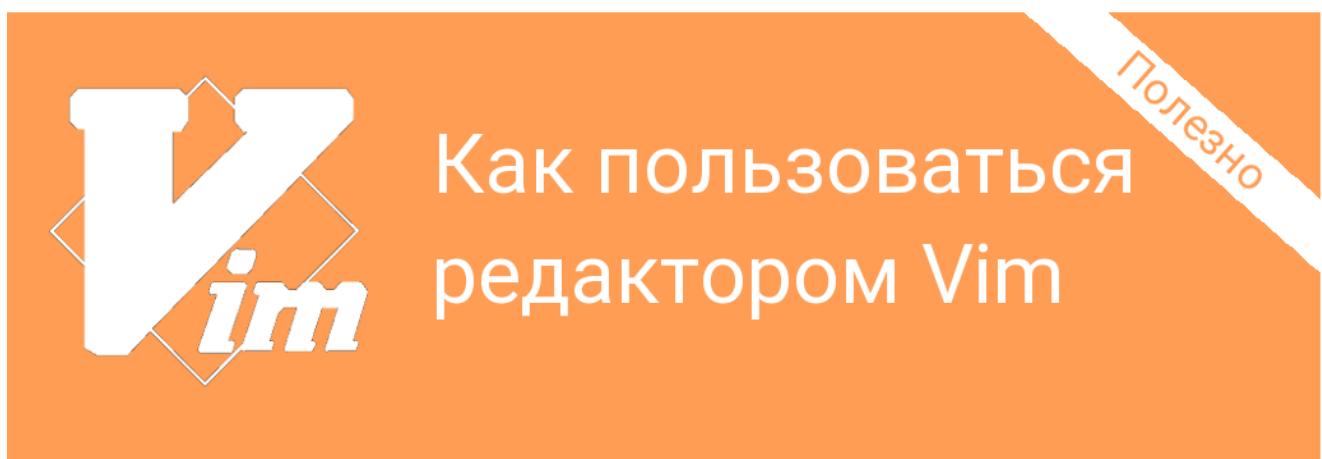
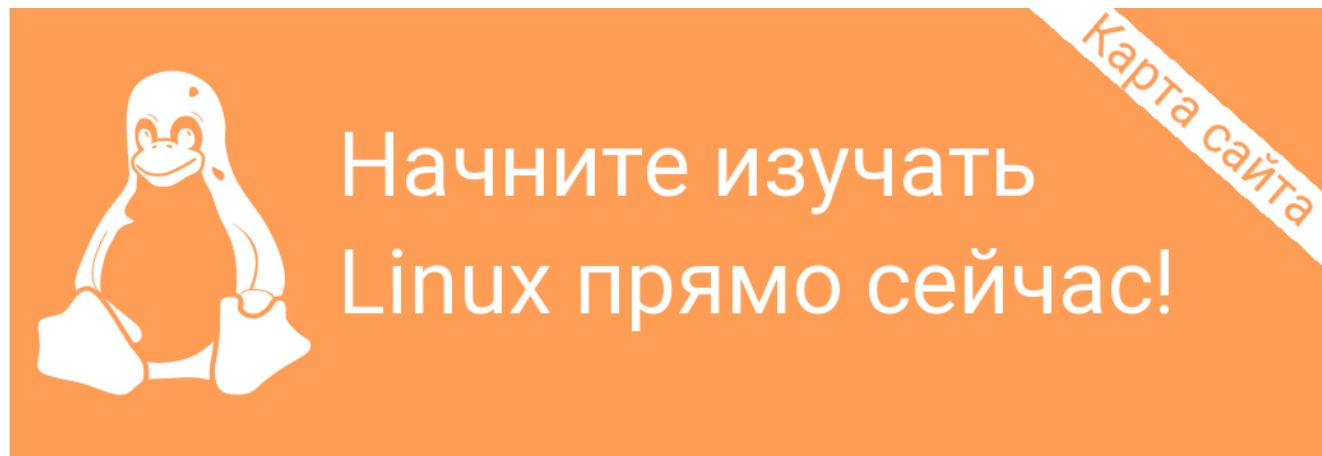
Комментировать

Русский

Privacy

Поиск

ПОИСК ПО КОМАНДАМ

 Начните вводить команду Поиск Лучшие Свежие Теги Privacy



Команда find в Linux

2021-10-17



Команда chmod Linux

2020-04-13



Права доступа к файлам в Linux

2020-10-09



Настройка Cron

2021-10-01



Копирование файлов в Linux

2023-03-03

РАССЫЛКА

Ваш E-Mail адрес

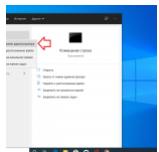
Я прочитал(а) и принимаю политику конфиденциальности

Sign up

Windows

Списки

Privacy



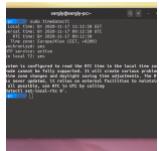
Восстановление Grub после установки Windows 10

2023-05-04



Ошибка Ubuntu не видит сеть Windows

2023-02-19



Сбивается время в Ubuntu и Windows

2023-02-19



Подключение ext4 в Windows

2023-02-19

[Смотреть ещё](#)

ОБНАРУЖИЛИ ОШИБКУ?

Сообщите мне об этом. Выделите текст с ошибкой и нажмите Ctrl+Enter.

ВКОНТАКТЕ



>< komYounity

Мы создаём комьюнити, комьюнити создаёт
Linux.

13 973 подписчика



[Подписаться на новости](#)

[Privacy](#)

МЕТА

[Регистрация](#)

[Войти](#)

[Лента записей](#)

[Лента комментариев](#)

СЛЕДИТЕ ЗА НАМИ В СОЦИАЛЬНЫХ СЕТЯХ



ИНТЕРЕСНОЕ



[Шпаргалка по journalctl в Linux](#)

2019-03-22



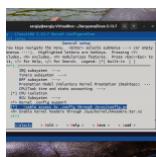
[Полезные утилиты для Linux](#)

2021-10-13



[Шпаргалка по tmux](#)

2021-10-01



[Сборка ядра Linux](#)

2021-08-14

[Privacy](#)

©Losst 2023 CC-BY-SA [Политика конфиденциальности](#)



Privacy