



itdog

14 окт 2023 в 14:39

# Поднимаем на OpenWrt клиент прокси VLESS, Shadowsocks, Shadowsocks2022. Настройка sing-box и tun2socks

Средний

10 мин

98K

Настройка Linux\*, Системное администрирование\*, Сетевые технологии\*

Тutorial

Обучающее руководство описывающее, как поднять на роутере Shadowsocks, VMess, VLESS, Trojan и даже SOCKS5 проху и ходить к нему через сетевой интерфейс.

Трафиком на роутере удобно управлять, когда у туннеля есть свой интерфейс. С одной стороны, есть Wireguard и OpenVPN, которые предоставляют сетевые интерфейсы. С другой стороны есть, например, SOCKS5 прокси и вытекший из него Shadowsocks, которые работают на другом уровне. Настраивая их мы получаем порт, а не интерфейс.

Здесь разобраны два инструмента, которые могут предоставить сетевой интерфейс на роутере и пересылать трафик с него во всевозможные прокси.

Sing-box умеет всё то, что умеет tun2socks и даже больше. Но вероятно, по каким-то причинам (размер пакета) вам может не подойти sing-box, поэтому также рассматривается tun2socks.

Настройка технологий сокрытия туннеля отличается от настройки стандартных туннелей. Она сложнее, пакеты занимают много места, информации меньше или она вообще отсутствует. Поэтому если у вас работают стандартные WG и OpenVPN, то рекомендую остановиться на них.

Всё производится в консоли, для tun2socks и sing-box нет специальных пакетов для настройки через LuCi.

## tun2socks

<https://github.com/xjasonlyu/tun2socks>

Поддерживает следующие типы прокси:

- HTTP

- SOCKS4/SOCKS5
- Shadowsocks ("старая" версия)

Объем распакованного пакета 8.8М.

Он цепляется к сетевому интерфейсу tun и переводит трафик в прокси. Что только не сделаешь, чтобы обойти китайский firewall.

## Установка

Пакета tun2socks нет в репозиториях OpenWrt, поэтому его нужно скачивать с [гитхаба](#) проекта. Благо он собирается под множество архитектур, в том числе MIPS и ARM.

Глянуть архитектуру процессора на вашем роутере

```
opkg print-architecture
```

Вывод Xioami mi3g v1 для примера:

```
arch all 1
arch noarch 1
arch mipsel_24kc 10
```

Это архитектура mipsle. На роутерах в большинстве случаев будет либо mips, либо mipsle.

Скачиваем архив с нужной архитектурой на компьютер, разархивируем и перекидываем на роутер в /tmp.

Пример для mipsle:

```
wget https://github.com/xjasonlyu/tun2socks/releases/download/v2.5.1/tun2socks-linux-mi
unzip tun2socks-linux-mipsle-softfloat.zip
scp tun2socks-linux-mipsle-softfloat root@192.168.1.1:/tmp/
```

После этого заходим на роутер и проверяем, что точно скачали подходящий под вашу архитектуру бинарник

```
root@OpenWrt:~# /tmp/tun2socks-linux-mipsle-softfloat --help
Usage of ./tun2socks-linux-mipsle-softfloat:
  -config string
```

Help вывелся, значит, всё ок. Но если выводится такая ошибка

```
/tmp/tun2socks-linux-mips-softfloat: line 1: syntax error: unexpected "("
```

значит, архитектура выбрана неверно.

Перекидываем в `/usr/bin/` и заодно переименовываем

```
mv tun2socks-linux-mipsle-softfloat /usr/bin/tun2socks
```

Для работы tun интерфейса понадобится пакет `kmod-tun`

```
opkg update && opkg install kmod-tun
```

Настройка интерфейса и firewall

`tun2socks` не создаёт интерфейс сам, поэтому нужно самим создать интерфейс и присвоить ему ip.

Добавляем в `/etc/config/network`

```
config interface 'tun0'
    option device 'tun0'
    option proto 'static'
    option ipaddr '172.16.250.1'
    option netmask '255.255.255.0'
```

Имейте в виду, что `ip a` покажет его только при запуске `tun2socks`.

Учтите, что если у вас настроен какой-нибудь VPN, то tun0 может быть занят. Можно поменять на tun1 тут и далее.

Создаём зону и правило в /etc/config/firewall

```
config zone
    option name 'tun'
    option forward 'REJECT'
    option output 'ACCEPT'
    option input 'REJECT'
    option masq '1'
    option mtu_fix '1'
    option device 'tun0'
    option family 'ipv4'

config forwarding
    option name 'lan-tun'
    option dest 'tun'
    option src 'lan'
    option family 'ipv4'
```

Обратите внимание, что требуется указывать device , а не network .

Рестартуем сеть

```
service network restart
```

## Автозапуск

Накидал простой сценарий, кладём его в /etc/init.d/tun2socks

```
#!/bin/sh /etc/rc.common

USE_PROCD=1

# starts after network starts
START=40

# stops before networking stops
STOP=89
```

```
PROG=/usr/bin/tun2socks
IF="tun0"
PROTO="$PROTO"
METHOD_USER="$METHOD_USER"
PASS="$PASS"
HOST="$HOST"
PORT="$PORT"

start_service() {
    procd_open_instance
    procd_set_param command "$PROG" -device "$IF" -proxy "$PROTO://" "$METHOD_USER":
    procd_set_param stdout 1
    procd_set_param stderr 1
    procd_set_param respawn ${respawn_threshold:-3600} ${respawn_timeout:-5} ${respawn_delay:-5}
    procd_close_instance
}
```

Надо подставить свои переменные, примеры:

### Shadowsocks

```
METHOD_USER="aes-256-gcm"
PASS="ochslozniyparol"
HOST="domain.com"
PORT="8388"
```

### Socks5 прокси без пароля

```
PROTO="socks5"
#METHOD_USER="aes-256-gcm"
#PASS="ochslozniyparol"
HOST="domain.com"
PORT="46202"
```

### Socks5 прокси с логином и паролем

```
PROTO="socks5"
METHOD_USER="user"
```

```
PASS="ochslozniyparol"  
HOST="domain.com"  
PORT="1080"
```

Переменную METHOD\_USER назвал так, потому что для SS - это метод шифрования, а в socks5 - это логин.

Для HTTP и SOCKS4 логика та же.

Не советую использовать бесплатные публичные прокси. Перенаправлять даже часть своего трафика на такие прокси опасно.

Делаем исполняемым, помещаем в автозапуск и запускаем

```
chmod +x /etc/init.d/tun2socks  
ln -s ../init.d/tun2socks /etc/rc.d/S40tun2socks  
service tun2socks start
```

## Тестирование работоспособности и поиск ошибок

Глянуть логи приложения

```
logread -f -e tun2socks
```

Потестить без сценария инициализации можно так

```
tun2socks -device tun0 -proxy ss://aes-256-gcm:ochslozniyparol@domain.com:8388 -loglevel
```

При `-loglevel debug` выводится трафик, который ходит через tun2socks. Но показывается только TCP и UDP. loglevel можно и в сценарий закинуть.

Если будет кушать много памяти, то у проекта есть [целая страница](#) с описанием флагов, которые можно подкрутить.

`ping -I` ничего не скажет о работоспособности. Пакеты будут "ходить" (по итогу до хоста они не доходят) даже если соединение не установлено.

Для проверки прокси лучше всего использовать curl и какой-нибудь сервис, определяющий IP-адрес.

Curl умеет направлять запрос через сетевой интерфейс.

```
curl --interface tun0 ifconfig.me
```

Curl должен отдать IP-адрес вашего прокси-сервера.

## Sing-box

В OpenWrt 23.05 добавлен пакет sing-box. Он умеет работать с tun интерфейсом. Поддерживает кучу протоколов:

- SOCKS5 proxy
- HTTP proxy
- Shadowsocks версии 2022-\* и старые aes-\*
- VMess и VLESS
- Trojan И другие

Объем распакованного пакета 21.5MB.

## Установка

Для OpenWrt 23.05 всё просто

```
opkg update && opkg install sing-box
```

Для версии 22.03 можно установить пакет вручную:

- Узнать архитектуру роутера `opkg print-architecture`
- Найти её в <https://downloads.openwrt.org/releases/23.05.0/packages/>
- Перейти в каталог packages, найти пакет sing-box
- Скачать в /tmp

- Установить `opkg install sing-box_1.3.0-1_mips_24kc.ipk`

На 21.02 установить не получится, пакет зависит от модуля ядра `kmod-netlink-diag`, которого в 21.02 нет.

```
* pkg_hash_check_unresolved: cannot find dependency kmod-inet-diag for sing-box
```

## Настройка

Если до этого вы использовали интерфейс `tun0` (например, OpenVPN использует `tun`), то остановите сначала другой туннель, либо используйте `tun1` в конфигурации.

По дефолту сервис `sing-box` запускается от юзера `sing-box`. Но у этого юзера нет прав для управления `/dev/net/tun`. Поэтому запускать `sing-box` надо от `root`.

Без `root` получите такую ошибку

```
Fri Jun  9 06:43:41 2023 daemon.err sing-box[9272]: FATAL[0000] start service: initiali
```

Настраивается это в `/etc/config/sing-box`. Там же сервис надо включить, проставив 1 параметру `enabled`. Этот параметр проверяется при старте сервиса в `../init.d/sing-box`, при 0 сервис не запускается.

По итогу должно выглядеть так:

```
config sing-box 'main'
    option enabled '1'
    option user 'root'
    option conffile '/etc/sing-box/config.json'
    option workdir '/usr/share/sing-box'
```

Сам файл конфигурации находится в `/etc/sing-box/config.json`. Нам от `sing-box` нужен `tun` интерфейс, который будет перенаправлять трафик, например, в `shadowsocks`:

```
{
  "log": {
```



```

    "level": "debug"
  },
  "inbounds": [
    {
      "type": "tun",
      "interface_name": "tun0",
      "domain_strategy": "ipv4_only",
      "inet4_address": "172.16.250.1/30",
      "auto_route": false,
      "strict_route": false,
      "sniff": true
    }
  ],
  "outbounds": [
    {
      "type": "shadowsocks",
      "server": "$HOST",
      "server_port": $PORT,
      "method": "2022-blake3-aes-128-gcm",
      "password": "$PASS"
    }
  ],
  "route": {
    "auto_detect_interface": true
  }
}

```

## VLESS (xtls-rprx-vision, reality)

```

{
  "log": {
    "level": "debug"
  },
  "inbounds": [
    {
      "type": "tun",
      "interface_name": "tun0",
      "domain_strategy": "ipv4_only",
      "inet4_address": "172.16.250.1/30",
      "auto_route": false,
      "strict_route": false,
      "sniff": true
    }
  ],

```

```

"outbounds": [
  {
    "type": "vless",
    "server": "$HOST",
    "server_port": $PORT,
    "uuid": "$UUID",
    "flow": "xtls-rprx-vision",
    "tls": {
      "enabled": true,
      "insecure": false,
      "server_name": "$FAKE_SERVER",
      "utls": {
        "enabled": true,
        "fingerprint": "chrome"
      },
      "reality": {
        "enabled": true,
        "public_key": "$PUBLIC_KEY",
        "short_id": "$SHORT_ID"
      }
    }
  }
],
"route": {
  "auto_detect_interface": true
}
}

```

"Обычный" Shadowsocks, разница только в методе шифрования

```

{
  "log": {
    "level": "debug"
  },
  "inbounds": [
    {
      "type": "tun",
      "interface_name": "tun0",
      "domain_strategy": "ipv4_only",
      "inet4_address": "172.16.250.1/30",
      "auto_route": false,
      "strict_route": false,
      "sniff": true
    }
  ]
}

```

```
],
"outbounds": [
  {
    "type": "shadowsocks",
    "server": "$HOST",
    "server_port": $PORT,
    "method": "aes-256-gcm",
    "password": "$PASS"
  }
],
"route": {
  "auto_detect_interface": true
}
}
```

**Важное про Shadowsocks2022:** Если у вас многопользовательский сервер, то в конфигурации необходимо указывать два пароля общий и юзера через :.

**inbounds** - здесь это то, что поднято на роутере. Эта часть отвечает за "входящий" трафик. Вы можете поднять сервер с SS, например. Но в вашем случае роутер является клиентом. Нам нужно, чтобы роутер отправлял часть трафика в сетевой интерфейс. Поэтому здесь описываем интерфейс **tun**.

Важное про параметр `auto_route`, его включение перенаправляет весь трафик в `tun`. В данной конфигурации он работать не будет, плюс автор `sing-box` рекомендует не использовать его на роутерах, а использовать для этого стандартные средства роутера. Он должен быть `false`. Как перенаправлять весь трафик через `tun` описано в конце статьи.

`Sing-box` также поддерживает TLS DNS, но работает это только с включенным `auto_route`. Если вам нужно шифровать DNS трафик, то используйте `dnscrypt-proxy2` или `stubby`.

**outbounds** - это "исходящий" трафик. Здесь как раз настраивается клиент с нужным типом прокси или туннеля. В примере это `shadowsocks2022`. Описывается протокол, сервер, порт сервера, метод шифрования и пароль. В общем, всё стандартно, но можно ещё подкрутить другими параметрами.

Настройка других протоколов описана в [Outbound](#) разделе документации.

Чтобы трафик ходил, нужно настроить `firewall`. Настраиваем зону и `forwading` для неё в `/etc/config/firewall`

```
config zone
    option name 'tun'
```

```
option forward 'ACCEPT'
option output 'ACCEPT'
option input 'ACCEPT'
option masq '1'
option mtu_fix '1'
option device 'tun0'
option family 'ipv4'

config forwarding
option name 'lan-tun'
option dest 'tun'
option src 'lan'
option family 'ipv4'
```

Здесь следует обратить внимание на то, что разрешён не только output трафик, как у всех других туннелей, но и весь остальной. Без полного разрешения туннель не заработает.

Осталось рестартануть firewall и запустить sing-box

```
service firewall restart
service sing-box start
```

При рестарте роутера туннель будет подниматься автоматически: при установке пакета автоматически проставляется симлинк в `/etc/rc.d/`.

## Тестирование работоспособности и поиск ошибок

Глянуть логи приложения

```
logread -f -e sing-box
```

После этого в соседнем терминале

```
service sing-box restart
```

Если есть какая-то грубая ошибка в конфигурации, то sing-box просто не запустится и интерфейс через `ip a` не будет видно. Ошибку будет видно в логге.

Проверить хождение трафика через интерфейс здесь можно точно так же, как для tun2socks.

`ping -I` ничего не скажет о работоспособности. Пакеты будут "ходить" (по итогу до хоста они не доходят) даже если соединение не установлено.

Для проверки прокси лучше всего использовать `curl` и какой-нибудь сервис, определяющий IP-адрес.

Curl умеет направлять запрос через сетевой интерфейс.

```
curl --interface tun0 ifconfig.me
```

Curl должен отдать IP-адрес вашего прокси-сервера.

## Применение на роутерах

После настройки туннеля его нужно как-то использовать. Приведу самые востребованные примеры.

1. Точечный роутинг по доменам. Вся настройка описана там, есть скрипт для автоматической настройки. В маршруте нужно указать интерфейс `tun0`
2. Временный вариант. Весь трафик (и с роутера, и с клиентов роутера), который идёт к подсети `172.64.195.0/24`, будет идти через туннель.  
Может пригодиться для тестов туннеля, для проверки доступности ресурса через туннель или если провайдер что-то вытворяет

```
ip route add 172.64.195.0/24 via 172.16.250.1 dev tun0
```

3. Постоянный вариант. Если нужно:

- Направить **весь** трафик клиентов роутера в туннель
- Направить трафик в туннель только для одного клиента роутера (Вашей приставке или холодильнику надо прикинуться иностранцем)
- Направлять трафик в туннель только для определенного IP-адреса или подсети

Для этого нужно маркировать пакеты. Это можно реализовать вручную или через пакет pbr.

## Pbr

Пакет pbr создаёт правила маркировки сам. У него даже есть интерфейс для LuCi.

```
opkg update && opkg install pbr luci-app-pbr
```

Я лично пакет не использовал, но видел неоднократное его упоминание. Поэтому на его счёт больше ничего сказать не могу.

## Ручная настройка

Ну а если вы хотите настроить всё вручную без лишних пакетов, всё точно так же как [раньше](#).

Если у вас уже настроена маркировка пакетов, то пропустите эту часть и переходите к правилам firewall.

Добавляем новую таблицу в конец файла /etc/iproute2/rt\_tables

```
99 vpn
```

Делаем маршрут в /etc/config/network . Все маркированные пакеты слать в таблицу VPN

```
config rule
    option priority '100'
    option lookup 'vpn'
    option mark '0x1'
```

Там же создаём маршрут: всё, что попадает в таблицу vpn, отправляется в интерфейс tun0.

Создаём файл /etc/hotplug.d/iface/30-vpnroute со скриптом внутри:

```
#!/bin/sh
```

```
sleep 5
ip route add table vpn default dev tun0
```

Требуется рестарт сети

```
service network restart
```

Теперь всё готово, чтобы создавать необходимые правила в firewall. Для этого нужно лишь предоставлять этим правилам `set_mark '0x1'`.

Пару примеров:

1. Весь трафик с клиента роутера с IP-адресом 192.168.56.242 отправлять в туннель

```
config rule
    option name 'From IP through tun'
    option src 'lan'
    option dest '*'
    option proto 'all'
    option set_mark '0x1'
    option target 'MARK'
    option family 'ipv4'
    option src_ip '192.168.56.242'
```

2. Трафик от **всех** клиентов роутера отправляется в туннель

```
config rule
    option name 'All lan through tun'
    option src 'lan'
    option dest '*'
    option proto 'all'
    option set_mark '0x1'
    option target 'MARK'
    option family 'ipv4'
```

3. Всё, что идёт к IP-адресу 1.1.1.1, отправлять в туннель

```
config rule
    option name 'To IP through tun'
    option src 'lan'
    option dest '*'
    option proto 'all'
    option set_mark '0x1'
    option target 'MARK'
    option family 'ipv4'
    option dest_ip '1.1.1.1'
```

4. То же самое, но уже загоняем целую подсеть. Используется также `dest_ip`

```
config rule
    option name 'To subnet through tun'
    option src 'lan'
    option dest '*'
    option proto 'all'
    option set_mark '0x1'
    option target 'MARK'
    option family 'ipv4'
    option dest_ip '172.64.194.0/24'
```

5. Весь трафик с клиента пускать через провайдера. Будто на роутере ничего не настроено

```
config rule
    option name 'From IP through tun'
    option src 'lan'
    option dest '*'
    option proto 'all'
    option set_mark '0x0'
    option target 'MARK'
    option family 'ipv4'
    option src_ip '192.168.56.242'
```

**После всех примеров необходимо рестартить `firewall service firewall restart`.**

Все обновления и новые статьи публикую в моём телеграм-канале.



Статьи от @Andrevich , в которых он идёт другим путём:

- Обход блокировок на OpenWRT с помощью Passwall (v2ray, xray, trojan) и tun2socks
- Обход блокировок на OpenWRT с помощью Sing-box (vless, vmess, trojan, ss)
- Скрипт для хранения tun2socks в RAM. Настраиваем клиент Outline на OpenWRT за 5 минут с помощью tun2socks

**Теги:** sing-box, shadowsocks, tun2socks, tun0, vless, shadowsocks2022, openwrt

**Хабы:** Настройка Linux, Системное администрирование, Сетевые технологии

◆ +16

📖 223



💬 15

## Редакторский дайджест



Присылаем лучшие статьи раз в месяц

Электронная почта



154

0

Карма

Рейтинг

@itdog

Пользователь

Подписаться



## Комментарии 15



Nicorn

14 окт 2023 в 16:58

Ура, новая статья, могу попросить подсказку!

Роутер Xiaomi AX3600, OpenWRT 23.05 релиз.

Постоянно у sing-box в логах такое:

```
ERROR [495998350 82ms] inbound/tun[0]: x509: certificate is not valid for any names, but wanted to match dl.google.com
```

При этом, через homerоху или luci-app-xray подключается, но летит в туннель вообще всё, да и тяжеловесное и слишком китайское оно.

С ПК через curl проверял - ошибок по сертификату нет. Куда ещё можно посмотреть?

↑  ↓ Ответить



itdog  
14 окт 2023 в 17:08

Через sing-box можно разное поднять, что используется для прокси? И какой конфиг sing-box. Видимо, используется маскировка под сайт [dl.google.com](https://dl.google.com) и она не работает.

↑  ↓ Ответить



Nicorn  
14 окт 2023 в 17:14

Прошу прощения, в пылу борьбы конфигами забыл. VPS с X-UI, Vless, Reality, маскировка действительно под [dl.google.com](https://dl.google.com).

↑  ↓ Ответить



itdog  
14 окт 2023 в 17:59

Видимо, нужно настраивать sing-box под это дело, если он вообще это умеет. Я не настраивал это, не вижу на данный момент в этом никакого смысла.

Могу лишь посоветовать посмотреть документацию <https://sing-box.sagernet.org/> и issues на гитхабе проекта.

↑  ↓ Ответить



Nicorn  
15 окт 2023 в 11:38

В общем, что-то не работает.

Упорно не нравится сертификат, при том что Curl говорит "SSL certificate verify ok."

Сдался, подключил shadowsocks2022 с полпинка, спасибо за статью

↑  ↓ Ответить



Nicorn  
19 окт 2023 в 00:25

UPD

Разобрался, я упорно в конфиге писал IP своего VPS, а надо было свой домен, ссылающийся на него. Всё заработало.

↑  ↓ Ответить



itdog  
4 ноя 2023 в 13:49

Теперь есть смысл. Добавил пример конфигурации для VLESS.



Ответить



**zyxmon**

24 янв в 14:27

Мои 2 копейки на тему sing-box - <https://forum.keenetic.com/topic/17455-sing-box-универсальный-набор-прокси-инструментов-shadowsocks-vmess-vless-trojan/>

Собрал sing-box для entware и описал, как делать клиентские конфиги.



Ответить



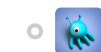
**rexen**

21 июл в 22:14

"You do not have permission to view this topic"



Ответить



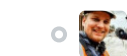
**zyxmon**

22 июл в 16:19

Никаких геоблоков у форума кинетиков нет. Все заходит без vpn.



Ответить



**rexen**

22 июл в 20:08

Да нет же, сам форум открывается (другие темы), но как я понял, там не игнор по айпи, а просто скрыта тема от незарегистрированных. Хз зачем - может чтобы РКН не возбуждался?



Ответить



**SantaClaus16**

26 янв в 21:14

Столкнулся с проблемой. Предыстория - дачный роутер перестал подключаться по Wireguard к городу. Решил завернуть трафик WG в VLESS. Поставил sing-box на роутер, поднял VLESS - тут ок, никаких проблем. Пытаюсь поднять WG через tun от sing-box, все по мануалам выше. Коннекта нет. Почему то tun ни в какую не пропускает udp. Решения не нашел.



Ответить



**SantaClaus16**

28 янв в 15:12

Хоть и решение завернуть wg в vless может показаться странным на первый взгляд, на это есть свои причины... По итогу удалось сделать следующим образом:

Взял проект <https://github.com/rfc1036/udptunnel>. Скопировал бинарники для сервера и роутера.

Может показаться что, зачем? Есть ведь есть socat (очень сильно режется скорость,



буквально до кбит), есть `udptunnel` в официальных репозиториях `openwrt` (это не то, хоть и имеет такое же название. Более того, `udptunnel` из репозитория `openwrt` у меня не заработал и судя по форуму `openwrt`, не только у меня).

На сервере: [tcp который будем слушать] [ip и udp куда нам надо переадресовать]  
`udptunnel -S --server -v 0.0.0.0:12345 127.0.0.1:51820`

На клиенте: [udp в который будем ломиться] [адрес сервера с tcp портом]  
`udptunnel -S -v 0.0.0.0:12345 example.com:12345`

По итогу такая связка заработала. Wireguard кстати на `openwrt` капризный, если указывать в endpoint - localhost, wg отказывается у меня запускаться. 127.0.0.1 работает. Скорость получилась 50/20 мбит против эталонных - 110/200, что мало конечно, но лично меня устраивает.

↑  ↓ Ответить  

○  **Cancer**  
6 сен в 21:52 

А кто-то смог заставить эту связку (sing-box-vless ну с маркировкой пакетов и роутингом в виртуальный интерфейс) работать со звонками в whatsapp и telegram?

↑  ↓ Ответить  

○  **LabEG**  
5 окт в 23:31


Сделал по инструкции, но столкнулся с проблемой что после рестарта железки сеть перестает работать. Лечиться рестартом network сервиса. Подскажите как полечить? Делать рестарт сервиса через 10 секунд после загрузки не вариант.

↑  ↓ Ответить  

Зарегистрируйтесь на Хабре, чтобы оставить комментарий

## Публикации

ЛУЧШИЕ ЗА СУТКИ    ПОХОЖИЕ

 **BabayMazay**  
7 часов назад

**Lampwork — декоративная стеклодувная техника. Часть 2.**  
**Основные приёмы, работы заключительные**

 Средний  9 мин  894

Тutorial

 +50

 7

 6

7 часов назад

## Всероссийский рейтинг IT-брендов работодателей 2024

 9 мин  18K

 +36

 18

 11



qertis

7 часов назад

## Как я отправился покорять Эльбрус и не дошел до вершины 71 метр

 10 мин  3.9K

 +28

 6

 7



Bright\_Translate

3 часа назад

## Небезопасный Rust сложнее C

 Средний  19 мин  1.9K

Обзор

Перевод

 +25

 11

 7



MaFrance351

8 часов назад

## Сенсорный пин-пад и как он работает

 Простой  9 мин  2.2K

Обзор

 +22

 7

 19



OlegSivchenko

19 часов назад

## Как гравитационная линза стала космическим телескопом

 11 мин  3.1K

 +21

 10

 37



Seleditor

6 часов назад

## Стоять или сидеть? Развенчиваем мифы о здоровом образе работы



3 мин



2.8K



+20



10



4



artemmoscow

6 часов назад

## Циничные заметки о карьере в IT от «гейткипера»



4 мин



2K

Мнение



+19



12



27



klimensky

6 часов назад

## AD-X2: присадка для аккумуляторов, взбудоражившая Америку



Простой



11 мин



2.4K

Ретроспектива



+19



2



8



mitradir

3 часа назад

## Nearly Stateless L4 Balancer: алгоритм и патч на GitHub. Доклад Яндекса



10 мин



482



+16



4



0

Для каких задач можно использовать Evolution Free Tier от Cloud.ru: истории юзеров

Турбо

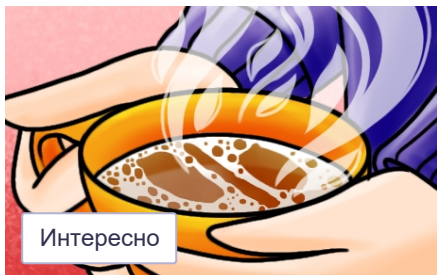
Показать еще

## МИНУТОЧКУ ВНИМАНИЯ



Турбо

Курс на автоматизацию и облака: о трендах DevOps в России



Интересно

Лучше горячего чая — горячие скидки. Бери, пока не остыли



Турбо

Будущее ИИ-контента к 2035 году: предсказания видеографа

## ЗАКАЗЫ

Помочь грамотно настроить Asterisk 22

3000 руб./за проект · 2 отклика · 28 просмотров

Организовать CI\CD для группы фрилансеров и настроить VLESS-сервер

1200 руб./в час · 8 откликов · 55 просмотров

Настройка 3X-UI панели

2000 руб./за проект · 1 отклик · 37 просмотров

Аудиомост на Ардуино

50000 руб./за проект · 13 откликов · 80 просмотров

Настроить инструменты на сервере

2000 руб./в час · 7 откликов · 107 просмотров

Больше заказов на Хабр Фрилансе

## ЧИТАЮТ СЕЙЧАС

Пользователи сообщили, что YouTube снова заработал в России без ограничений по замедлению у некоторых провайдеров

47K

59

Готовьтесь к росту цен

78K 145

Всероссийский рейтинг IT-брендов работодателей 2024

18K 11

Смартфон S24 Ultra – классический фейк, где все «железо» тоже ненастоящее

43K 129

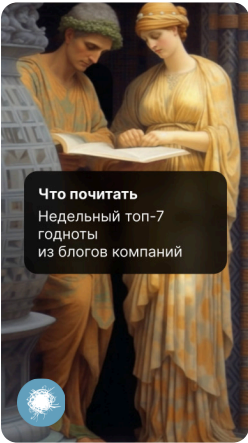
Нафига козе баян? (Мне не сдались такие программисты)

40K 225

Для каких задач можно использовать Evolution Free Tier от Cloud.ru: истории юзеров

Турбо

ИСТОРИИ



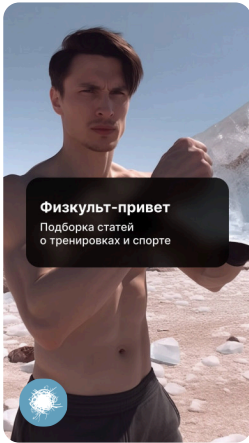
Топ-7 годноты из блогов компаний



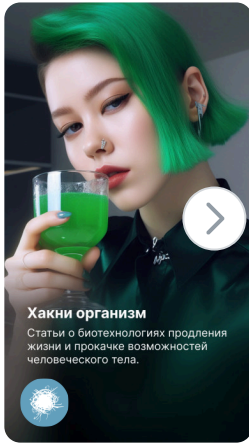
Tencent выпустила ИИ для генерации 3D



Сладость или гадость?



Физкульт-привет



Хакни организм

РАБОТА

DevOps инженер  
39 вакансий

Системный администратор  
91 вакансия



БЛИЖАЙШИЕ СОБЫТИЯ



8 октября – 4 декабря

ТурбоХакатон «Решения для электроэнергетики на базе искусственного интеллекта»

Онлайн

Разработка Другое

Больше событий в календаре



5 – 17 ноября

Вайб-чек для бэкендеров на Хабр Карьере

Онлайн

Разработка

Больше событий в календаре



15 – 16 ноября

IT-конференция Skolkovo

Москва

Разработка М

Другое

Больше событий в к

Ваш аккаунт

Войти

Регистрация

Разделы

Статьи

Новости

Хабы

Компании

Авторы

Песочница

Информация

Устройство сайта

Для авторов

Для компаний

Документы

Соглашение

Конфиденциальность

Услуги

Корпоративный блог

Медийная реклама

Нативные проекты

Образовательные

программы

Стартапам



[Настройка языка](#)

[Техническая поддержка](#)

© 2006–2024, Habr