

[КАК СТАТЬ АВТОРОМ](#)[Питчи недели аналитиков](#)[Поехали в гик-трип по Кал...](#)**MiraclePtr**

25 апр в 21:58

Bleeding-edge обход блокировок с полной маскировкой: настраиваем сервер и клиент XRay с XTLS-Reality быстро и просто

Простой

8 мин

133К

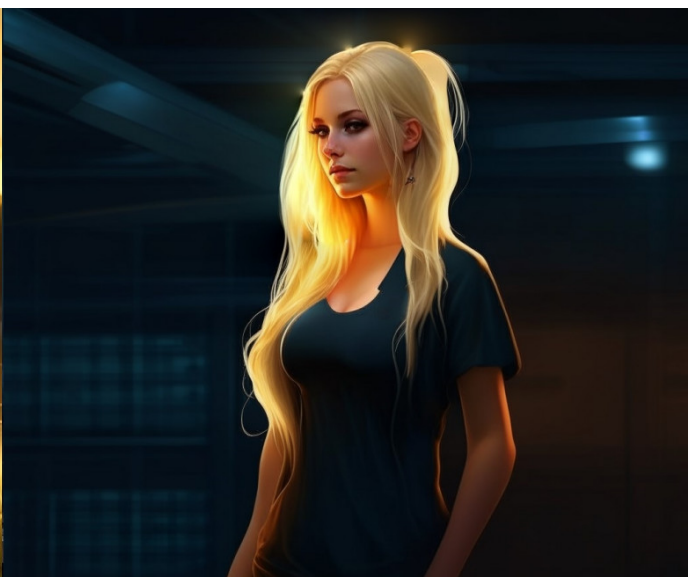
Настройка Linux*, Информационная безопасность*, Системное администрирование*, Сетевые технологии*

[Тutorial](#)

В серии предыдущих статей я описывал, почему повсеместно используемые VPN- и прокси-протоколы такие как Wireguard и L2TP очень уязвимы к выявлению и могут быть легко заблокированы цензорами при желании, обзревал [существующие гораздо более надежные протоколы](#) обхода блокировок, [клиенты для них](#), а также [описывал настройку сервера](#) для всего этого.

Но кое о чем мы не поговорили. Во второй статье я вскользь упомянул самую передовую и недетектируемую технологию обхода блокировок под названием **XTLS-Reality**, и пришло время рассказать о ней поподробнее, а именно - как настроить клиент и сервер для нее.

Кроме того, что этот протокол еще более устойчив к выявлению, приятным фактом будет и то, что настройка сервера XRay для XTLS-Reality гораздо проще, чем описанные ранее варианты - после предыдущих статей я получил довольно много комментариев типа "А что так сложно, нужен домен, нужны сертификаты, и куча всего" - теперь все будет гораздо проще.



+37

697



261

XTLS-Reality

Коротко про **XTLS-Reality**. Это самое новое изобретение от авторов XRay. Про XRay (и его прородителя V2Ray, он же V2Fly) я рассказывал в предыдущей статье. XTLS-Reality поддерживается в последних релизах XRay, Sing-box и многих клиентах.

Он предназначен для защиты от выявления методом **active probing**. В отличие от старых протоколов (Shadowsocks, VMess, VLESS, и транспорта XTLS-Vision), определение “свой/чужой” здесь происходит еще на этапе TLS-хендшейка в момент чтения ClientHello. Если клиент опознан как “свой”, сервер работает как прокси, а если нет - вжух! - и TLS подключение передается на какой-нибудь другой абсолютно реальный хост с TLS (например, google.com или gosuslugi.ru), и таким образом клиент (или цензор, желающий методом active probing проверить, а что же прячется на том конце) получит настоящий TLS-сертификат от google.com или gosuslugi.ru и настоящие данные с этого сервера. Полное соответствие. Механизм определения “свой/чужой” во многом схож с механизмом работы Cloak, и позволяет достоверно определить подлинность клиента, но вместе с тем не вызывает подозрения у цензоров и устойчив к replay-атакам - со стороны систем анализа трафика это выглядит как подключение к настоящему популярному сайту, сервер отдает настоящий TLS-сертификат этого сайта, и вообще все (включая TLS fingerprint сервера) выглядит до предела аутентично и не вызывает подозрений. Еще XTLS-Reality может оказаться вариантом для обхода суровых корпоративных прокси с Man-in-the-Middle, которые перешифровывают весь трафик из сети своим сертификатом (нередко подобные прокси имеют список исключений для ресурсов с HSTS и certificate pinning, либо для экономии ресурсом, и подобрав правильный домен можно пролезть во внешнюю сеть без расшифровки трафика). Бонусом еще XTLS-Reality обычно используется в паре с XTLS-Vision, то есть мы имеем очень достоверно выглядящие паттерны трафика из-за отсутствия двойного шифрования TLS-in-TLS (и заодно еще очень высокую производительность, у меня между хостами в Москве и в центральной Европе XRay легко выдает >100 мегабит).

Единственный минус подобного решения - в отличие от более старых протоколов (VLESS без XTLS) нет возможности работать через websocket-транспорт, и, соответственно, через CDN типа Cloudflare. **Upd**: такая возможность есть если использовать многоуровневую схему с SNI-проху (типа haproxy), при необходимости расскажу в комментариях.

Установка сервера XRay

А теперь настало время все это настроить. Дано: VPS на Linux (Debian или Ubuntu, на других дистрибутивах плюс-минус то же самое) с IPv4 или IPv6-адресом.

Установку XRay и уже описывал [в предыдущей статье](#), поэтому здесь буду краток.

Можно установить XRay руками:

```
wget https://github.com/XTLS/Xray-core/releases/download/v1.8.1/Xray-linux-64
mkdir /opt/xray
unzip ./Xray-linux-64.zip -d /opt/xray
chmod +x /opt/xray/xray
nano /usr/lib/systemd/system/xray.service
systemctl enable xray
```

▸ [xray.service](#)

А можно установить скриптом от разработчиков (почему-то по умолчанию он ставит старую версию 1.7.5, которая не поддерживает Reality, поэтому нужно явно указать более свежую):

```
bash -c "$(curl -L https://raw.githubusercontent.com/XTLS/Xray-install/046d9a
```

Скрипт установит XRay и создаст для него systemd-юнит.

Настройка сервера XRay

Для настройки нам понадобится ряд параметров. Часть из них нам может сгенерировать сам XRay:

```
/usr/local/bin/xray uuid # /opt/xray/xray если устанавливали вручную
/usr/local/bin/xray x25519 # /opt/xray/xray если устанавливали вручную
```

На выходе вы получите UUID (идентификатор пользователя для протокола аутентификации VLESS), а также приватный и публичный ключи - запишите их, они вам понадобятся.

Еще один параметр, который нужен - short ID, он представляет собой просто шестнадцатиричное число (символы 0-9, a-g) длиной до 8 байт (16 символов) - можно набрать любую абракадабру типа "aabbccdd" или запустить `openssl rand -hex 8`

А вот дальше начинается самое интересное. Нам нужно найти сайт, под который мы будем маскироваться.

Требования довольно простые:

это должен быть иностранный сервер (вне РФ), не забаненный по домену Роскомнадзором, поддерживающий подключения по TLSv1.3 и HTTP/2, имеющий заглавную страницу, которая *не* переадресовывает на какой-нибудь другой домен. Если совсем упарываться, то неплохо было бы если бы IP-адрес был из диапазона того же облачного хостера, что и у вас, и чтобы сервер поддерживал Online Certificate Status Protocol (OCSP). Если вы не знаете, что вся эта фигня значит - не заморачивайтесь, выбирайте что-нибудь простое, например

- `www.samsung.com:443`
- `www.googletagmanager.com:443`
- `www.asus.com:443`
- `www.amd.com:443`
- `www.cisco.com:443`
- `www.microsoft.com:443`
- `dl.google.com:443`
- `www.linksys.com:443`
- `www.nvidia.com:443`

и т.д.

Сервер выбрали, настало время редактировать конфиг. Если вы ставили XRay вручную то он будет лежать в `/opt/xray/config.json`, если скриптом - то в `/usr/local/etc/xray/config.json`.

Приводим его к следующему виду:

```
{
  "log": {
    "loglevel": "info"
  },

```

```
"routing": {
  "rules": [],
  "domainStrategy": "AsIs"
},
"inbounds": [
  {
    "port": 23,
    "tag": "ss",
    "protocol": "shadowsocks",
    "settings": {
      "method": "2022-blake3-aes-128-gcm",
      "password": "aaaaaaaaaaaaaabbbbbbbbbbbbbbbbbb",
      "network": "tcp,udp"
    }
  },
  {
    "port": 443,
    "protocol": "vless",
    "tag": "vless_tls",
    "settings": {
      "clients": [
        {
          "id": "4c3fe585-ac09-41df-b284-70d3fbe18884",
          "email": "user1@myserver",
          "flow": "xtls-rprx-vision"
        }
      ],
      "decryption": "none"
    },
    "streamSettings": {
      "network": "tcp",
      "security": "reality",
      "realitySettings": {
        "show": false,
        "dest": "www.microsoft.com:443",
        "xver": 0,
        "serverNames": [
          "www.microsoft.com"
        ],
        "privateKey": "G0TPj_klK7_j_IvjxiCtyBL80RYotYS0dBBBSfFOMH4",
        "minClientVer": "",
        "maxClientVer": "",
        "maxTimeDiff": 0,
        "shortIds": [
          "aabbccdd"
        ]
      }
    }
  }
]
```

```
    }  
  },  
  "sniffing": {  
    "enabled": true,  
    "destOverride": [  
      "http",  
      "tls"  
    ]  
  }  
},  
],  
"outbounds": [  
  {  
    "protocol": "freedom",  
    "tag": "direct"  
  },  
  {  
    "protocol": "blackhole",  
    "tag": "block"  
  }  
]  
}
```

На что обратить внимание: в "serverNames" указан домен, под сервер которого вы маскируетесь (в данном случае `www.microsoft.com`), "id" в секции "clients" - это тот самый UUID, что мы сгенерировали выше. "privateKey" и первый элемент в массиве "shortIds" - это приватный ключ и short ID, что мы тоже сгенерировали выше. Публичный ключ не теряйте, он будет нужен на клиенте.

В этом конфиге так же на 23 порту настроен Shadowsocks-2022, на всякий случай, вдруг пригодится. Если не надо, или хочется полной маскировки - можно удалить этот элемент из "inbounds".

Перезапускаем еще раз xray:

```
$ systemctl restart xray
```

Проверяем что все нормально запустилось:

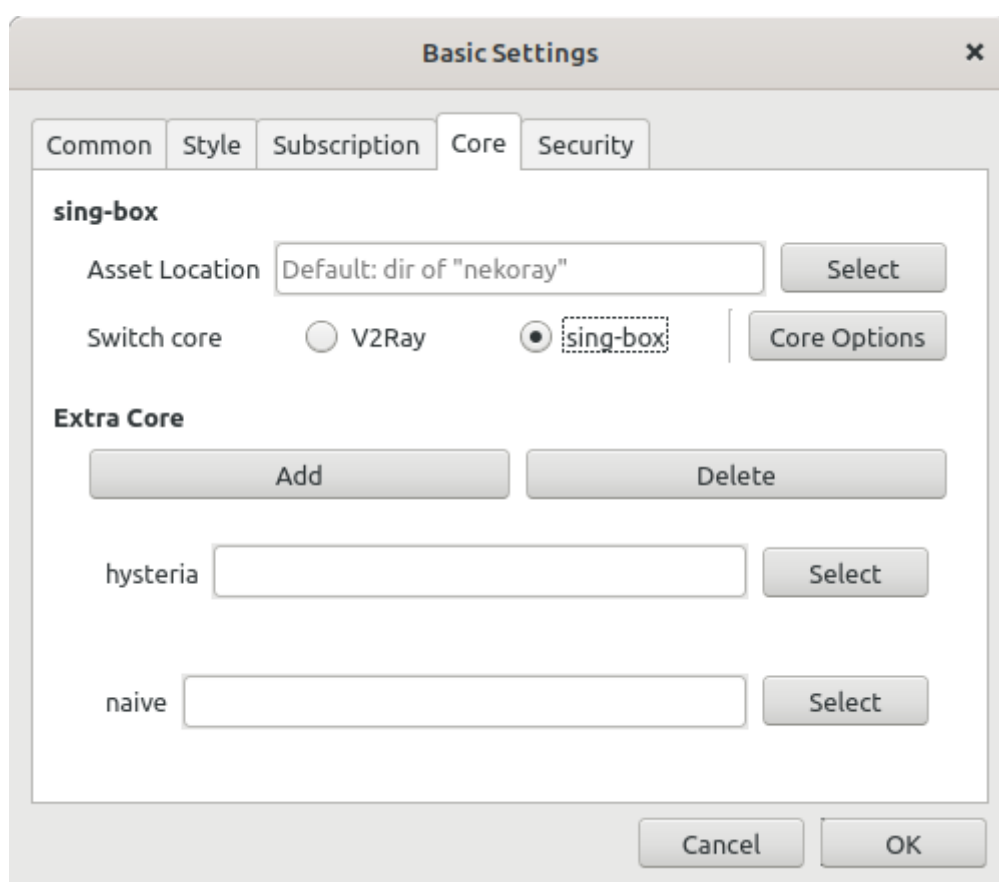
```
$ journalctl -u xray
```

Например, XRay может ругнуться что не удастся распарсить JSON-файл, обычно это связано с лишними запятыми в конце `}` блока, в этом случае он укажет, на какой строке ошибка. Исправляем ошибки, перезапускаем еще раз, и переходим к настройке клиентов.

Настройка клиентов

Сначала **Nekobox** на десктопе (Windows, Linux, и есть неофициальные билды под MacOS).

Если вы раньше им не пользовались, нужно переключить его на использование движка sing-box, Preferences -> Basic Settings -> Core:



Идем в Server -> New profile и заполняем все вот так:

Edit

Common

Name: VLESS West

Address: 6.2

Port: 443

VLESS

UUID: 4c3fe585-ac09-41df-b284-70d3fbe18884

Flow: xtls-rprx-vision

Custom Json Settings

Not set

Settings

Network*: tcp

Security*: tls

Packet Encoding*: xudp

Network Settings (tcp)

Path*:

Host*:

TLS Security Settings

☐ Allow insecure* Certificate: Not set

SNI*: www.microsoft.com

ALPN*: h2

TLS Camouflage Settings

uTLS: chrome

Reality Pbk*: kbITkINkTdFvB6e3xy97pTV7gjl3Z3irv246oRZ5

Reality Sid: aabbccdd


Cancel OK

Address - IP-адрес вашего сервера, UUID - соответственно, UUID, SNI должен соответствовать домену, под который вы маскируетесь (один из списка "serverNames" из конфига сервера), uTLS - я выбираю Chrome (это маскировка клиента под обычный браузер), Reality Pbk - публичный ключ (не приватный, а второй, публичный), Reality Sid - shortId из конфига выше.

Сохраняем, кликаем правой кнопкой мыши на новый сервер в списке, жмем Start, и проверяем подключение выбрав там же Current Select -> URL test.

Если все нормально, то галочками "VPN Mode" или "System proxy" можно завернуть трафик всех приложений на прокси.

Настройка v2rayN под Windows аналогична, набор параметров тот же, вот скриншот (не мой, из гугла):

 VLESS

Servers

Xray

Alias (remarks)

REALITY

Address

165.22.12.227

Port

443

UUID(id)

9f2b4b10-6818-492e-a157-d5131d450c7b

Generate

Flow

xtls-rprx-vision

Encryption

none

Transport

Transport protocol(network)

tcp

*Default value tcp

Camouflage type

none

*tcp camouflage type

Camouflage domain(host)

*http host Separated by com

Path

TLS

reality

SNI

www.microsoft.com

Fingerprint

chrome

PublicKey

ioE61VC3V30U7IdRmQ3bjhOq2ij9tPhVlgAD4JZ4YRY

ShortId

b1

SpiderX

/

Confirm

Cancel

Автор Nekobox перестал собирать версии под macOS, поэтому я рекомендую использовать Wings X / FoXray. Настройки точно такие же.

Если вдруг вам нравятся Clash-based клиенты (например, Clash Verge под Windows, Linux, MacOS или для мобильных устройств), то нужно использовать ядро Clash.Meta и специальны конфиг для Clash. В случае с Clash Verge можно сделать так:

1. Settings -> Clash Core -> Выбрать Meta
2. Сохранить конфиг в какой-нибудь локальный файл:

► [clash-reality.yml](#)

3. Profiles -> New - Type : Local -> выбрать ваш файл и кликнуть по нему в окне Clash
4. Proxies -> выбрать ваш новый прокси на вкладке Global -> кликнуть по полю справа чтобы протестировать подключение, должно появиться значение пинга
5. Settings -> System proxy: вкл - после этого трафик всей системы пойдет через прокси. Можно использовать и TUN, но для этого надо запускать Clash Verge от рута.

Далее, мобильные клиенты. Вариант раз: в Nekobox или в v2ray кликнуть правой кнопкой мыши на ваш сервер из списка, выбрать Share -> QR code или Link, и получить ссылку или QR-код, которые потом можно отсканировать/вставить в мобильные клиенты. Либо вбить все те же данные руками, вот как это выглядит в андроидовском v2rayNG (версия из Google Play еще не обновилась и не умеет работать с Reality, скачиваем APK с Гитхаба):

► [скриншоты](#)

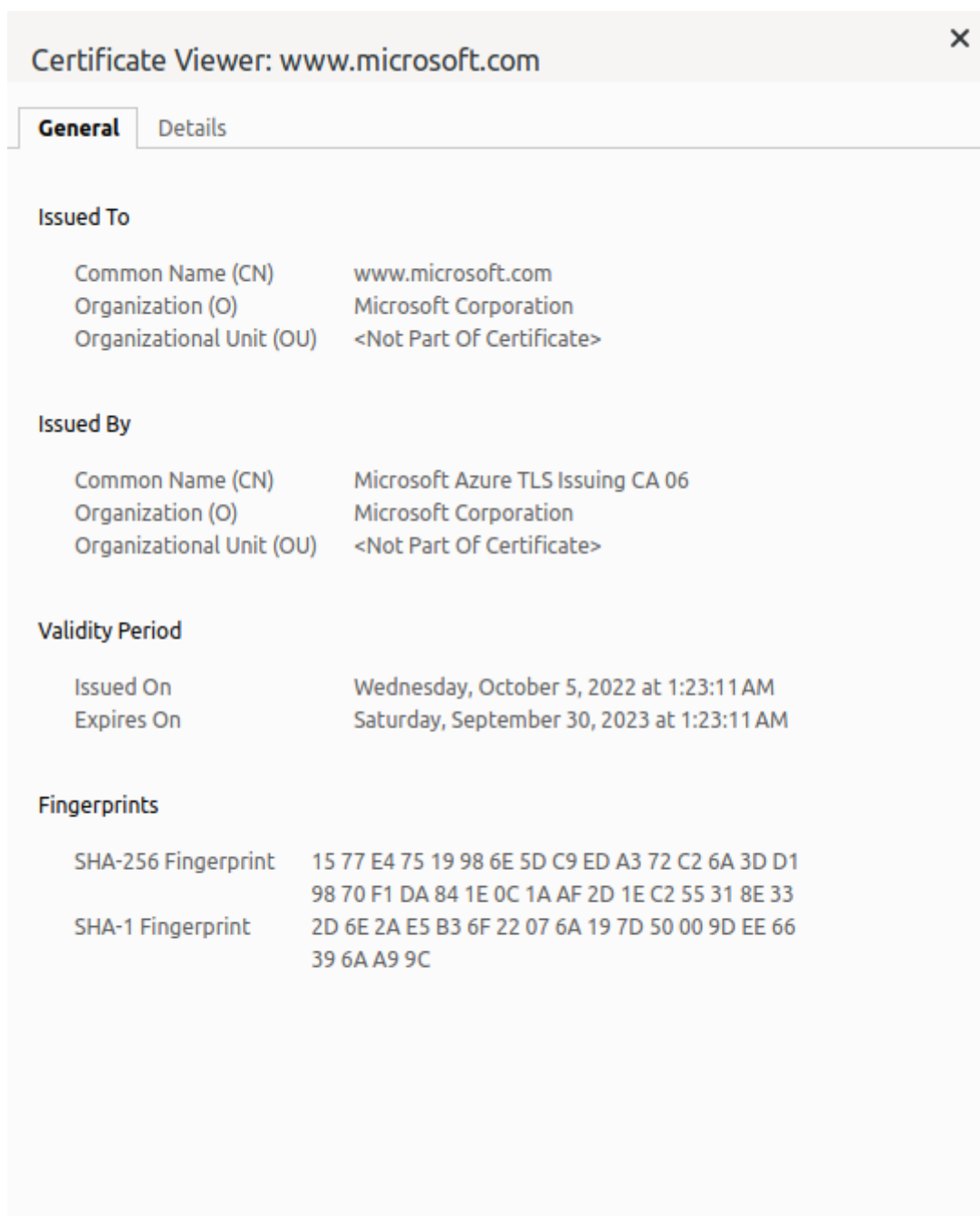
Под iOS я рекомендую использовать Shadowrocket (3\$) или Wings X / FoXray (он бесплатный). Настройки подключения полностью аналогичны описанному выше.

Советы бывалых

1. Очень рекомендуется настраивать на клиентах правила маршрутизации ([пример в комментариях](#)), чтобы трафик до .ru-доменов и хостов с российскими IP шел напрямую, а не через прокси (в клиентах для такого поставляется GeoIP база данных).
2. Обязательно используйте uTLS на клиентах, выставляя правильный TLS fingerprint (например, Chrome).
Если при использовании XTLS вы почему-то не можете подключиться, в логах сервера видна ошибка типа "failed to use xtls-rprx-vision, found outer tls version 771", попробуйте сменить версию uTLS. У меня, например, при выборе "android" клиент не подключается, а при выборе "chrome" все okay.
3. Для увеличения производительности можно настроить на сервере Bottleneck Bandwidth и Round-trip propagation time (BBR) congestion control algorithm:

```
echo "net.core.default_qdisc=fq" >> /etc/sysctl.conf  
echo "net.ipv4.tcp_congestion_control=bbr" >> /etc/sysctl.conf  
sysctl -p
```

4. Чтобы проверить, что маскировка работает как надо, добавьте IP-адрес вашего сервера и домен, под который вы маскируетесь, в hosts-файл (на Linux это /etc/hosts, на Windows это c:\windows\system32\drivers\etc\hosts), например, "38.25.63.10 www.microsoft.com", и после этого попробуйте зайти на этот адрес браузером - должна открыться настоящая страница этого домена с настоящим TLS-сертификатом:



Другой вариант: использовать CURL.

```
curl -v --resolve www.microsoft.com:443:151.101.65.69
```

https://www.microsoft.com (вместо 151.101.xx.xx должен быть IP вашего сервера)

Теги: xtls, xtls-reality, v2ray, xray, обход блокировок, цензура

Хабы: Настройка Linux, Информационная безопасность, Системное администрирование, Сетевые технологии

Редакторский дайджест

Присылаем лучшие статьи раз в месяц

✕

Электронпочта



278

70

Карма


Рейтинг

Surrounded by idiots @MiraclePtr
В борделе на пианино играю

Комментарии 261

Публикации

ЛУЧШИЕ ЗА СУТКИ ПОХОЖИЕ

- 

andreybrylb

4 часа назад

Существование треугольника Шарыгина — это настоящее математическое чудо


👍 Простой

🕒 2 мин

👁 7.5K

💎 +47

🔖 31

💬 8
- 

igor_suhorukov

14 часов назад

Я бы не жил в Сочи в этих местах...


👍 Простой

🕒 6 мин

👁 14K

💎 +30

🔖 53

💬 59
- 

AndreyBolotov1989

13 часов назад

Как оптимизирован завод: вопросы оптимальной загрузки и «иридиевых чапельников»



Простой



9 мин



1.7K

[Обзор](#)

+29



23



3



orionII

5 часов назад

Вышла Java 21



Средний



18 мин



5K

[Обзор](#)

+28



20



14



AlexxIT

14 часов назад

Диалоги с кофеваркой, про Яндекс Алису и умный дом Home Assistant



Простой



6 мин



4.8K

+27



26



13



ravor84

13 часов назад

Перф-тесты VS аномалии. Вечная битва за производительность приложений на iOS



17 мин



1.5K

+22



9



5



Doctor_IT

7 часов назад

Платформа для анализа данных за вечер



11 мин



1.2K

[Кейс](#)

+21



35



0



angelov-iaroslav

8 часов назад

А теперь — поподробнее про флюс



Простой



12 мин



2.1K

Обзор



+21



19



3



SergeyAstanin

12 часов назад

Контроль состояния аккумулятора, если у вас стоит предпусковой подогреватель



Средний



8 мин



1.6K

Тutorial



+21



10



3



melnik909

11 часов назад

Очередной ответ на вопрос: «Зачем нужна семантика?»



Средний



7 мин



1K

Аналитика



+20



24



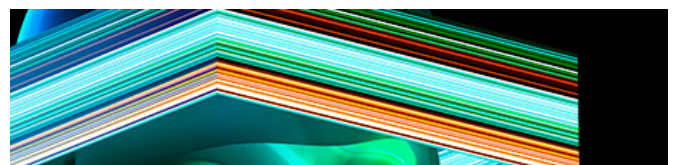
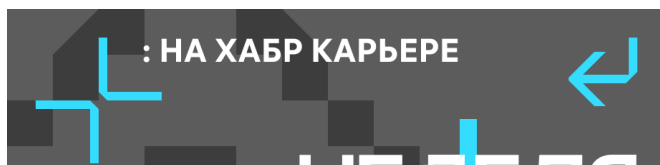
0

Боевые приемы и техники GitLab: что нужно знать Devops-инженеру

Турбо

Показать еще

МИНУТОЧКУ ВНИМАНИЯ





Это что, еще одна карьерная неделя для аналитиков?



Узнайте, что будет на SmartDev 2023

ВАКАНСИИ

Системный администратор Linux

до 300 000 ₽ · i7 LLC · Москва · Можно удаленно

Системный администратор Linux

от 150 000 до 200 000 ₽ · ИТЦ "ДЖЭТ" · Москва

Системный администратор Linux

до 200 000 ₽ · Notamedia · Москва · Можно удаленно

Инженер серверных платформ (ОС Linux)

до 120 000 ₽ · МегаФон · Москва · Можно удаленно

Python-разработчик (Платформа Linux)

от 250 000 до 350 000 ₽ · Сбер · Москва

Больше вакансий на Хабр Карьере

ЧИТАЮТ СЕЙЧАС

Блогер обнаружил в российском мониторе со 140 баллами локализации тайваньский чип от Realtek

👁 5.9K 💬 29

Существование треугольника Шарыгина — это настоящее математическое чудо

👁 7.6K 💬 8

Вышла Java 21

👁 5K 💬 14

«Подарил удочки и попрощался с друзьями на год»: как я стал Android-разработчиком, отказавшись даже от прогулок

26K

78

Химики придумали унитаз, к которому ничего не прилипает

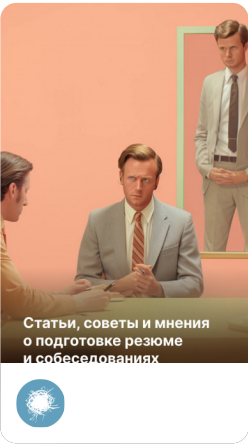
6.4K

48

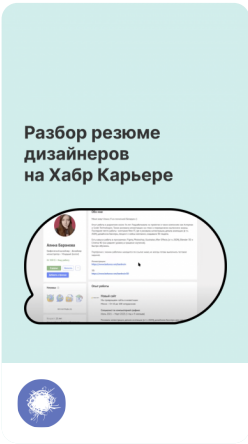
Боевые приемы и техники GitLab: что нужно знать Devops-инженеру

Турбо

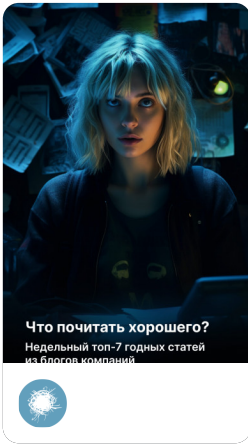
ИСТОРИИ



Полезная подборка о собеседованиях



Разбор резюме дизайнеров



Топ-7 годных статей из блогов компаний



Учиться хорошо



Золотая рыбка, хочу, чтоб у меня все было

РАБОТА

Специалист по информационной безопасности
109 вакансий

Системный администратор
119 вакансий

DevOps инженер
44 вакансии

Все вакансии

Ваш аккаунт	Разделы	Информация	Услуги
Войти	Статьи	Устройство сайта	Корпоративный блог
Регистрация	Новости	Для авторов	Медийная реклама
	Хабы	Для компаний	Нативные проекты
	Компании	Документы	Образовательные
	Авторы	Соглашение	программы
	Песочница	Конфиденциальность	Стартапам
			Спецпроекты



Настройка языка

Техническая поддержка

Вернуться на старую версию

© 2006–2023, Habr