



23 окт 2021 в 17:22

Прошивка OpenWRT для роутеров

Настройка Linux*, Сетевые технологии*

Ожидает приглашения

Введение

Данная статья может быть полезна продвинутым пользователям, которые хотят улучшить работу своего домашнего роутера, а также системным администраторам предприятий, перед которым стоит задача повысить надежность и безопасность удаленной работы сотрудников.

Как вы скорее всего знаете, ваш роутер – это маленький компьютер и него есть программное обеспечение, так называемая “прошивка” или “firmware”. Прошивку разрабатывает производитель роутера, однако существуют также альтернативные решения – проекты с открытым исходным кодом: OpenWRT, DD-WRT, Tomato.

Что нам даёт использование OpenWRT?

- Обновления (безопасность и новые фишки) выпускаются в разы чаще и поддержка сохраняется в разы дольше, чем у большинства производителей. Особенно актуально это стало в условиях карантина. Уязвимая “прошивка” роутера – одна из наиболее частых причин инцидентов при удаленной работе.
- “Родные” прошивки бывают нестабильными, особенно у дешевых роутеров. Так многие модели TP-Link зависали после нескольких дней непрерывной работы.
- Вы привыкаете к одному интерфейсу пользователя и при последующей смене/апгрейде роутера, даже от другого производителя, чувствуете себя “как дома”.
- Вам не обязательно покупать дорогой роутер для реализации продвинутых “фишек”, таких как IPv6, родительский контроль, блокировка рекламы, VPN, гостевой WiFi, DNS шифрование, динамический DNS (DDNS) и т. д.
- Есть активное сообщество, которое поможет оперативнее, чем даже поддержка крупного производителя, да и многое уже описано.
- Преимущества открытого решения на базе Linux: возможность подключаться через SSH, автоматизировать настройку и управлять роутером с помощью скриптов, настройки хранятся в текстовых файлах (автоматизация, контроль версий), можно использовать роутер для других задач (умный дом, SFTP/Web сервер, загрузка торрентов и т.п.).

Подробнее эти и другие причины описаны на сайте проекта.

Базовая настройка OpenWRT

Данная статья поможет вам настроить базовые функции OpenWRT, благодаря чему вы сможете быстро и безболезненно перейти на это решение. Вот перечень этих функций:

1. Установить пароль пользователя root.
2. Ограничить доступ по SSH только для интерфейса LAN.
3. Настроить PPPoE подключение по WAN.
4. Настроить WiFi.
5. Добавить гостевой WiFi (без доступа в локальную сеть).
6. Настроить динамический DNS NoIP.
7. Настроить переадресацию портов (port forwarding).
8. Сохранить конфигурацию в архивный файл.

Пункты 6 и 7 нужны, например, для того, чтобы подключаться из Интернета к домашнему компьютеру по SSH или SFTP (например, для синхронизация файлов с ноутбуком), а также для прямого подключения по Anydesk, которое работает быстрее, чем обычное.

Процесс “перепрошивки” на OpenWRT зависит от модели вашего роутера. Следует найти его в списке поддерживаемых устройств и следовать приведенным там рекомендациям.

Настройки можно делать с помощью SSH-подключения и скриптов, однако мы рассмотрим веб-интерфейс (который называется LuCI) как более наглядный и устойчивый к изменениям вариант.

1. Установить пароль пользователя root

Перейти в меню [System > Administration](#).

Router Password

SSH Access

SSH-Keys

Router Password

Changes the administrator password for accessing the device

Password

Confirmation

Save

Powered by LuCI openwrt-21.02 branch (git-21.231.26241-422c175) / OpenWrt 21.02.0 r16279-5cc0535800

2. Ограничить доступ по SSH только для интерфейса LAN

Перейти в меню [System](#) > [Administration](#) > [SSH Access](#).

Interface = lan

Router Password

SSH Access

SSH-Keys

SSH Access

Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server

Dropbear Instance

Delete

Interface

🔍 Listen only on the given interface or, if unspecified, on all

Port

22

Password authentication



🔍 Allow [SSH](#) password authentication

Allow root logins with
password



🔍 Allow the *root* user to login with password

Gateway Ports



🔍 Allow remote hosts to connect to local SSH forwarded ports

Add instance

Save & Apply ▾

Save

Reset

Powered by LuCI openwrt-21.02 branch (git-21.231.26241-422c175) / OpenWrt 21.02.0 r16279-5cc0535800

После этого шага имеет смысл сделать Logout и залогиниться снова, чтобы убрать предупреждение в верхней части экрана.

3. Настроить PPPoE подключение по WAN

Перейти в меню **Network > Interfaces**.

Нажать кнопку "Edit" в строке "WAN".

Protocol = PPPoE + нажмите кнопку "Switch protocol"

PAP/CHAP username = ваш_логин_у_провайдера

PAP/CHAP password = ваш_пароль_у_провайдера

The screenshot shows the OpenWrt web interface with the 'Interfaces » WAN' configuration page. The 'General Settings' tab is selected. The configuration includes:

- Status: Device: pppoe-wan, Uptime: 1d 0h 18m 13s, RX: 1.36 GB (1831894 Pkts.), TX: 452.33 MB (1277578 Pkts.), IPv4: 37.25.119.113/32, IPv6: fe80::b845:cb27:b0c3:13a4/128
- Protocol: PPPoE (highlighted with a green circle)
- Device: wan
- Bring up on boot: ☒
- PAP/CHAP username: buld (highlighted with a green circle)
- PAP/CHAP password: masked with dots and an eye icon (highlighted with a green circle)
- Access Concentrator: auto, with a link to 'Leave empty to autodetect'
- Service Name: auto, with a link to 'Leave empty to autodetect'
- Buttons: Dismiss, Save (highlighted with a green circle)

At the bottom, there is a 'Save & Apply' dropdown, 'Save', and 'Reset' buttons. The footer indicates the system is powered by LuCI openwrt-21.02 branch (git-21.231.26241-422c175) / OpenWrt 21.02.0 r16279-5cc0535800.

4. Настроить WiFi

Перейти в меню **Network > Wireless**.

4.1 Нажать на кнопку “Edit” под “radio0 802.11nac”.

OpenWrt

StatusSystemServicesNetworkLogout

REFRESHING

Wireless Overview

radio0

MediaTek MT76x2E 802.11nac

Channel: 40 (5.200 GHz) | Bitrate: 433.3 Mbit/s

RestartScanAdd

-51 dBm

SSID: MVD5G | Mode: Master

BSSID: 00:16:FB:C6:A9:7C | Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)

DisableEditRemove

radio1

MediaTek MT76x2E 802.11bgn

Channel: 6 (2.437 GHz) | Bitrate: ? Mbit/s

RestartScanAdd

--- dBm

SSID: MVD2_4G | Mode: Master

BSSID: 00:16:FB:C6:99:7C | Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)

DisableEditRemove

--- dBm

SSID: MVD-guest | Mode: Master

BSSID: 02:16:FB:C6:99:7C | Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)

DisableEditRemove

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate	
<div>Master "MVD5G" (wlan0)</div>	2A:16:50:E4:40:2B	192.168.1.195	<div>-51 dBm</div>	6.0 Mbit/s, 20 MHz 433.3 Mbit/s, 80 MHz, VHT-MCS 9, VHT-NSS 1, Short GI	Disconnect

Save & Apply

Save

Reset

Powered by LuCI openwrt-21.02 branch (git-21.231.26241-422c175) / OpenWrt 21.02.0 r16279-5cc0535800

Channel = Auto

ESSID = имя_вашего_wifi_5GHz

Channel = Auto
ESSID = имя_вашего_wifi_5GHz

OpenWrt Status System Services Network Logout REFRESH

Wireless Network: Master "MVD5G" (wlan0)

Device Configuration

General Setup Advanced Settings

Status **Mode:** Master | **SSID:** MVD5G
BSSID: 00:16:FB:C6:A9:7C
Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)
Channel: 40 (5.200 GHz)
Tx-Power: 20 dBm
Signal: -51 dBm | **Noise:** 0 dBm
Bitrate: 433.3 Mbit/s | **Country:** 00

Wireless network is enabled Disable

Operating frequency **Mode:** AC **Channel:** auto **Width:** 80 MHz

Maximum transmit power **driver default** - Current power: 20 dBm
? Specifies the maximum transmit power the wireless radio may use. Depending on regulatory requirements and wireless usage, the actual transmit power may be reduced by the driver.

Interface Configuration

General Setup **Wireless Security** MAC-Filter Advanced Settings

Mode: Access Point

ESSID: MVD5G

Network: lan:

? Choose the network(s) you want to attach to this wireless interface or fill out the custom field to define a new network.

Hide ESSID: ☐
? Where the ESSID is hidden, clients may fail to roam and airtime efficiency may be significantly reduced.

WMM Mode: ☒
? Where Wi-Fi Multimedia (WMM) Mode QoS is disabled, clients may be limited to 802.11a/802.11g rates.

Dismiss Save

Перейти на вкладку Wireless Security.

Encryption = WPA2-PSK/WPA3-SAE Mixed Mode
Key = пароль_вашего_wifi_5GHz

Interface Configuration

General Setup **Wireless Security** MAC-Filter Advanced Settings

Encryption

WPA2-PSK/WPA3-SAE Mixed M ▼

Key

.....*

802.11r Fast Transition

☐

?

 Enables fast roaming among access points that belong to the same Mobility Domain

802.11w Management Frame Protection

Optional ▼

?

 Note: Some wireless drivers do not fully support 802.11w. E.g. mwlwifi may have problems

802.11w maximum timeout

1000

?

 802.11w Association SA Query maximum timeout

802.11w retry timeout

201

?

 802.11w Association SA Query retry timeout

Enable key reinstallation (KRACK) countermeasures

☐

?

 Complicates key reinstallation attacks on the client side by disabling retransmission of EAPOL-Key frames that are used to install keys. This workaround might cause interoperability issues and reduced robustness of key negotiation especially in environments with heavy traffic load.

Dismiss

Save

4.2 Нажать на кнопку “Edit” под “radio1 802.11bgn”.

```
Channel = Auto
ESSID = имя_вашего_wifi_2.4GHz
```

Перейти на вкладку Wireless Security.

```
Encryption = WPA2-PSK/WPA3-SAE Mixed Mode
Key = пароль_вашего_wifi_2.4GHz
```

Нажать кнопки “Enable” (слева от “Edit”) на обоих подключениях.

5. Добавить гостевой WiFi

Взято [отсюда](#), плюс ужато и обновлено под новый интерфейс.

Делаем для 2.4 ГГц, но аналогично можно сделать и для 5ГГц.

5.1 Перейти в меню **Network > Wireless**.

5.1.1 Нажать кнопку “Add” в “radio1 802.11bgn”.

OpenWrt

StatusSystemServicesNetworkLogout

REFRESHING

Wireless Overview

radio0

MediaTek MT76x2E 802.11nac

Channel: 40 (5.200 GHz) | Bitrate: 13 Mbit/s

RestartScanAdd

-55 dBm

SSID: MVD5G | Mode: Master

BSSID: 00:16:FB:C6:A9:7C | Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)

DisableEditRemove

radio1

MediaTek MT76x2E 802.11bgn

Channel: 6 (2.437 GHz) | Bitrate: ? Mbit/s

RestartScanAdd

--- dBm

SSID: MVD2_4G | Mode: Master

BSSID: 00:16:FB:C6:99:7C | Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)

DisableEditRemove

--- dBm

SSID: MVD-guest | Mode: Master

BSSID: 02:16:FB:C6:99:7C | Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)

DisableEditRemove

Associated Stations

Network	MAC address	Host	Signal / Noise	RX Rate / TX Rate	
<div>Master "MVD5G" (wlan0)</div>	2A:16:50:E4:40:2B	192.168.1.195	<div>-51 dBm</div>	6.0 Mbit/s, 20 MHz 433.3 Mbit/s, 80 MHz, VHT-MCS 9, VHT-NSS 1, Short GI	Disconnect

Save & Apply

Save

Reset

Powered by LuCI openwrt-21.02 branch (git-21.231.26241-422c175) / OpenWrt 21.02.0 r16279-5cc0535800

Channel = Auto

ESSID = имя_вашего_гостевого_wifi

network = выбрать "-- custom --" и ввести "guest"

OpenWrt Status System Services Network Logout REFRESH

Wireless Network: Master "MVD-guest" (wlan1-1)

Device Configuration

General Setup Advanced Settings

Status Mode: Master | SSID: MVD-guest
BSSID: 02:16:FB:C6:99:7C
Encryption: mixed WPA2/WPA3 PSK, SAE (CCMP)
Channel: 6 (2.437 GHz)
Tx-Power: 20 dBm
Signal: 0 dBm | Noise: 0 dBm
Bitrate: 0.0 Mbit/s | Country: 00

Wireless network is enabled Disable

Operating frequency Mode Channel Width
N auto 20 MHz

Allow legacy 802.11b rates ☐
Legacy or badly behaving devices may require legacy 802.11b rates to interoperate. Airtime efficiency may be significantly reduced where these are used. It is recommended to not allow 802.11b rates where possible.

Maximum transmit power driver default - Current power: 20 dBm
Specifies the maximum transmit power the wireless radio may use. Depending on regulatory requirements and wireless usage, the actual transmit power may be reduced by the driver.

Interface Configuration

General Setup Wireless Security MAC-Filter Advanced Settings

Mode Access Point

ESSID MVD-guest

Network guest:

Choose the network(s) you want to attach to this wireless interface or fill out the custom field to define a new network.

Hide ESSID ☐
Where the ESSID is hidden, clients may fail to roam and airtime efficiency may be significantly reduced.

WMM Mode ☒
Where Wi-Fi Multimedia (WMM) Mode QoS is disabled, clients may be limited to 802.11a/802.11g rates.

Dismiss Save

5.1.2 Перейти на вкладку Wireless Security.

Encryption = WPA2-PSK/WPA3-SAE Mixed Mode
Key = пароль_вашего_гостевого_wifi

5.2 Перейти в меню Network > Interfaces.

5.2.1 Нажать на кнопку “Edit” в интерфейсе “GUEST”.

Protocol=Static address + нажать кнопку “Switch protocol”

IPv4 address = 192.168.3.1

IPv4 netmask = 255.255.255.0

OpenWrt Status System Services Network Logout REFRESH

Interfaces » GUEST

General Settings Advanced Settings Firewall Settings DHCP Server

Status **Device:** Master "MVD-guest"
Uptime: 1d 0h 36m 9s
MAC: 02:16:FB:C6:99:7C
RX: 6.51 MB (16662 Pkts.)
TX: 43.09 MB (28898 Pkts.)
IPv4: 192.168.3.1/24

Protocol Static address ▼

Device unspecified ▼

Bring up on boot ☒

IPv4 address 192.168.3.1 ...

IPv4 netmask 255.255.255.0 ▼

IPv4 gateway 217.77.208.254 (wan)

IPv4 broadcast 192.168.3.255

IPv6 address Add IPv6 address... +

IPv6 gateway

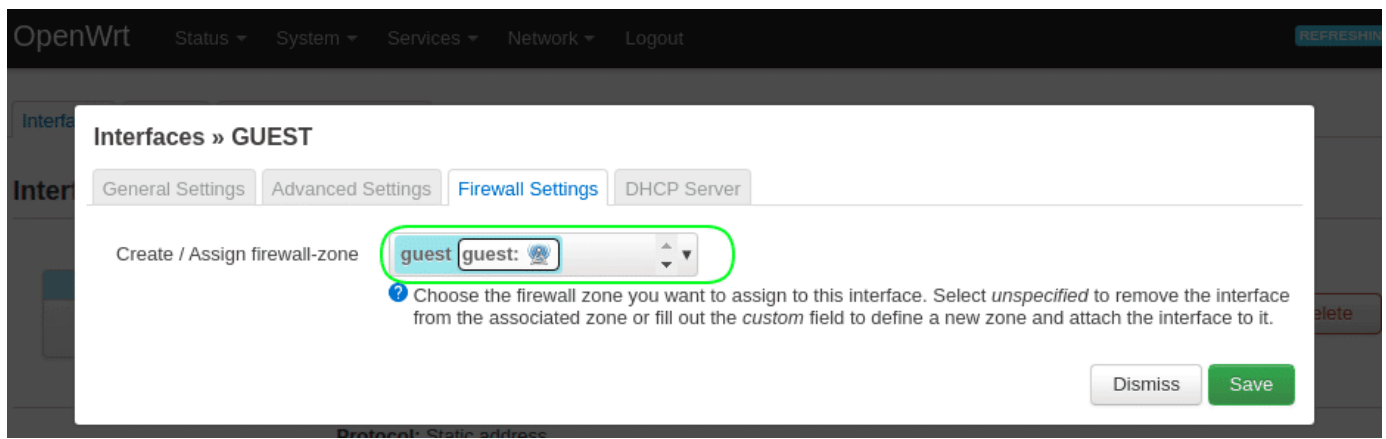
IPv6 routed prefix

Public prefix routed to this device for distribution to clients.

Dismiss Save

5.2.2 Перейти на вкладку “Firewall settings”.

Create / Assign firewall-zone = выбрать "-- custom --" и ввести "guest"



5.2.3 Перейти на вкладку “DHCP server”.

Нажать на кнопку "Setup DHCP server" и далее Save

5.3 Перейти в меню **Network > Firewall**.

5.3.1 Нажать на кнопку “Edit” в зоне “guest”.

Input = reject
Allow forward to destination zones = WAN

Firewall - Zone Settings

General Settings | Advanced Settings | Conntrack Settings | Extra iptables arguments

This section defines common properties of "guest". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name:

Input:

Output:

Forward:

Masquerading: ☐

MSS clamping: ☐

Covered networks:

The options below control the forwarding policies between this zone (guest) and other zones. *Destination zones* cover forwarded traffic **originating from guest**. *Source zones* match forwarded traffic from other zones **targeted at guest**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to destination zones:

Allow forward from source zones:

Dismiss Save

5.3.2 Перейти на вкладку **Traffic rules**.

Нажать на кнопку "Add" внизу.

```
Name = Guest DNS
Protocol = TCP+UDP
Source zone = guest
Destination zone = Device(input)
Destination port = 53
Save
```

Нажать на кнопку "Add" внизу.

```
Name = Guest DHCP
Protocol = UDP
Source zone = guest
Destination zone = Device(input)
```

Destination port = 67

Save

Firewall - Traffic Rules - guest DNS

[General Settings](#) [Advanced Settings](#) [Time Restrictions](#)

Name

Protocol

Source zone

Source address

Source port

Destination zone

Destination address

Destination port

Action

[Dismiss](#) [Save](#)

6. Настроить динамический DNS NoIP

6.1 Перейти в меню [System](#) > [Software](#).

Нажать кнопку “Update lists...”

Набрать “ddns” в поле “Filter”.

Установить пакеты “ddns-scripts”, “ddns-scripts-noip”, “luci-app-ddns”.

Сделать Logout и потом залогиниться снова.

OpenWrt
Status
System
Services
Network
Logout

Software

Free space:

94% (10.1 MB)

Filter:
Clear

Download and install package:
OK

Actions:

«
Displaying 1-46 of 46
»

Package name	Version	Size (.ipk)	Description	
<u>ddns-scripts</u>	2.8.2-11	24.8 KB	Dynamic DNS Client scripts (with IPv6 support)...	<input type="button" value="Installed"/>
<u>ddns-scripts-cloudflare</u>	2.8.2-11	4.0 KB	Dynamic DNS Client scripts extension for cloudflare.com API v4 (require curl)	<input type="button" value="Install..."/>
<u>ddns-scripts-cnkuai</u>	2.8.2-11	2.2 KB	Dynamic DNS Client scripts extension for "cnkuai.cn"....	<input type="button" value="Install..."/>
<u>ddns-scripts-digitalocean</u>	2.8.2-11	2.4 KB	Dynamic DNS Client scripts extension for "digitalocean.com API v2"....	<input type="button" value="Install..."/>
<u>ddns-scripts-freedns</u>	2.8.2-11	1.8 KB	Dynamic DNS Client scripts extension for "freedns.42.pl".	<input type="button" value="Install..."/>
<u>ddns-scripts-gandi</u>	2.8.2-11	1.6 KB	Dynamic DNS Client scripts extension for "gandi.net"....	<input type="button" value="Install..."/>
<u>ddns-scripts-godaddy</u>	2.8.2-11	3.6 KB	Dynamic DNS Client scripts extension for "godaddy.com API v1".	<input type="button" value="Install..."/>
<u>ddns-scripts-noip</u>	2.8.2-11	2.0 KB	Dynamic DNS Client scripts extension for "no-ip.com".	<input type="button" value="Installed"/>

6.2 Перейти в меню Services > Dynamic DNS.

6.2.1 Нажать кнопку "Edit" в строке "myddns_ipv4".

```

Lookup Hostname = your.dyndns.domain.com
DDNS Service provider = no-ip.com + нажать кнопку "Switch service"
Domain = your.dyndns.domain.com
Username = your_username
Password = your_password

```

DDns Service » myddns_ipv4

Basic Settings Advanced Settings Timer Settings Log File Viewer

Enabled ☒

? If this service section is disabled it could not be started. Neither from LuCI interface nor from console.

Lookup Hostname

? Hostname/FQDN to validate, if IP update happen or necessary

IP address version

? Defines which IP address 'IPv4/IPv6' is send to the DDNS provider

DDNS Service provider

Domain

? Replaces [USERNAME] in Update-URL (URL-encoded)

Username

? Replaces [USERNAME] in Update-URL (URL-encoded)

Password

? Replaces [PASSWORD] in Update-URL (URL-encoded)

Optional Encoded Parameter

? Optional: Replaces [PARAMENC] in Update-URL (URL-encoded)

Optional Parameter

? Optional: Replaces [PARAMOPT] in Update-URL (NOT URL-encoded)

Use HTTP Secure ☐

? Enable secure communication with DDNS provider

Dismiss Save

6.2.2 Нажать кнопку “Reload” в строке “myddns_ipv4”.

6.2.3 Нажать кнопку “Delete” в строке “myddns_ipv6” — если вам достаточно IPv4.

7. Настроить переадресацию портов (port forwarding)

Перейти в меню Network > Firewall > Port Forwards.

Нажать кнопку “Add” внизу:

Name = SSH
Protocol = TCP+UDP
External port = 22
Internal IP address = 192.168.1.2
Save

Нажать кнопку “Add” внизу:

Name = Anydesk
Protocol = TCP+UDP
External port = 7070
Internal IP address = 192.168.1.2
Save

Firewall - Port Forwards - Anydesk

[General Settings](#) [Advanced Settings](#)

Name: Anydesk

Protocol: TCP+UDP

Source zone: wan

External port: 7070

Destination zone: lan

Internal IP address: 192.168.1.2 (drew-desktop.lan)

Internal port: any

Match incoming traffic directed at the given destination port or port range on this host

Redirect matched incoming traffic to the specified internal host

Redirect matched incoming traffic to the given port on the internal host

Dismiss Save

8. Сохранить конфигурацию в архивный файл.

Перейти в меню [System > Backup](#).

Нажать на кнопку “Generate archive”.

Сохранить скачанный файл в надёжном месте.

В этом же пункте меню можно загружать обновления прошивки – кнопка “Flash image...”.

Заключение

Таким образом, мы рассмотрели недорогие в применении меры повышения безопасности и стабильности работы домашних роутеров с помощью прошивки OpenWRT. В то же время, следует заметить, что ни одна разовая мера безопасности, включая внедрение дорогого оборудования и программного обеспечения, не даст гарантий отсутствия инцидентов безопасности. Если вам нужен действительно высокий уровень защищённости, то необходим комплексный системный подход, начиная с аудита вашей ИТ-инфраструктуры, в том числе, домашнего окружения.

Теги: router, openwrt, linux

Хабы: Настройка Linux, Сетевые технологии

Данная статья не подлежит комментированию, поскольку её автор ещё не является полноправным участником сообщества. Вы сможете связаться с автором только после того, как он получит приглашение от кого-либо из участников сообщества. До этого момента его username будет скрыт псевдонимом.

О ПЕСОЧНИЦЕ

Это [«Песочница»](#) — раздел, в который попадают дебютные публикации пользователей, желающих стать полноправными участниками сообщества.

Если у вас есть [приглашение](#), отправьте его автору понравившейся публикации — тогда её смогут прочитать и обсудить все остальные пользователи Хабра.

Чтобы исключить предвзятость при оценке, все публикации анонимны, псевдонимы показываются случайным образом.

О МОДЕРАЦИИ

Точно не пройдут модерацию:

- новости, анонсы и пресс-релизы;
- материалы рекламного характера;

- вакансии (для этого предназначена [«Хабр Карьера»](#))
- вопросы (используйте [«Хабр Q&A»](#));
- просьбы о помощи в решении задач (используйте [«Хабр Фриланс»](#));
- жалобы на компании и предоставляемые услуги;
- куски программного кода без подробных пояснений;
- публикации, ранее опубликованные на других сайтах;
- односложные материалы (пара абзацев или видеоролик);
- статьи, слабо относящиеся к IT-тематике или не относящиеся к ней вовсе;
- публикации, нарушающие [правила](#) сайта.

С большой вероятностью не пройдут модерацию (или будут отправлены на доработку):

- материалы с низким (менее 75%) показателем уникального текста;
- публикации без правильно расставленных знаков препинания, со смайликами, с обилием восклицательных знаков, неоправданным выделением слов и предложений;
- плохо оформленные публикации ([подробнее](#));

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



Настройка языка

Техническая поддержка