

## NAT

JSP & Servlets  
8 уровень, 4 лекция

ОТКРЫТА

### 5.1 Знакомство в NAT

Еще одна очень интересная тема – это NAT. NAT расшифровывается как **Network Address Translation** и обычно присутствует в каждом роутере как некий сервис. Так что же это такое и зачем оно нужно?

**NAT** – это точка, с помощью которой локальные сети можно подключать к глобальным сетям, таким как интернет, например.

Как ты уже знаешь, в локальных сетях у всех компьютеров (и других устройств, подключенных к сети) есть свои собственные локальные IP-адреса. А чтобы обмениваться данными с сервером в интернете, надо чтобы наш компьютер мог послать запрос к серверу и сервер мог прислать нам ответ. А куда ему присылать ответ, если наш IP-адрес неизвестен за рамками нашей локальной сети?

Представь, что ты пишешь бумажное письмо Дональду Трампу. Трамп – это публичная фигура, он такой один – это наш публичный сервер. А в качестве обратного адреса в письме вы указываете Машу. Маш много. Какой именно Маше нужно прислать ответ?

Поэтому ты отправляешь письмо своему знакомому из Вашингтона, тоже публичной фигуре, со строгим указанием выслать его Трампу. Твой знакомый получает письмо, шлет его Трампу, а в качестве обратного адреса указывает свой адрес в Вашингтоне.

Затем, получив ответ от Трампа, знакомый пересылает его тебе. Так же и с IP-пакетами...

Чтобы позволить устройству с приватным IPv4-адресом обращаться к устройствам и ресурсам за пределами локальной сети, приватный адрес сначала должен быть изменен на общедоступный публичный адрес.

Как раз NAT переводит приватные адреса в общедоступные. Это позволяет устройству с локальным IP-адресом обращаться к ресурсам за пределами его частной сети. NAT в сочетании с локальными IP-адресами оказался полезным методом сохранения общедоступных IPv4-адресов.

В мире живет 8 миллиардов человек, а сетевых устройств уже в разы больше: телефоны, ноутбуки, смарт-часы, сервера, любые умные устройства. А IP-адресов всего 4 миллиарда. Раньше казалось, что это много, но с быстрым ростом интернета всем стало понятно, что этого недостаточно.

Тут нам на помощь приходит NAT: один публичный IPv4-адрес может быть использован сотнями, даже тысячами устройств, каждый из которых имеет локальный IPv4-адрес. NAT имеет дополнительное преимущество, заключающееся в добавлении степени конфиденциальности и безопасности в сеть, поскольку он скрывает внутренние IPv4-адреса из внешних сетей.

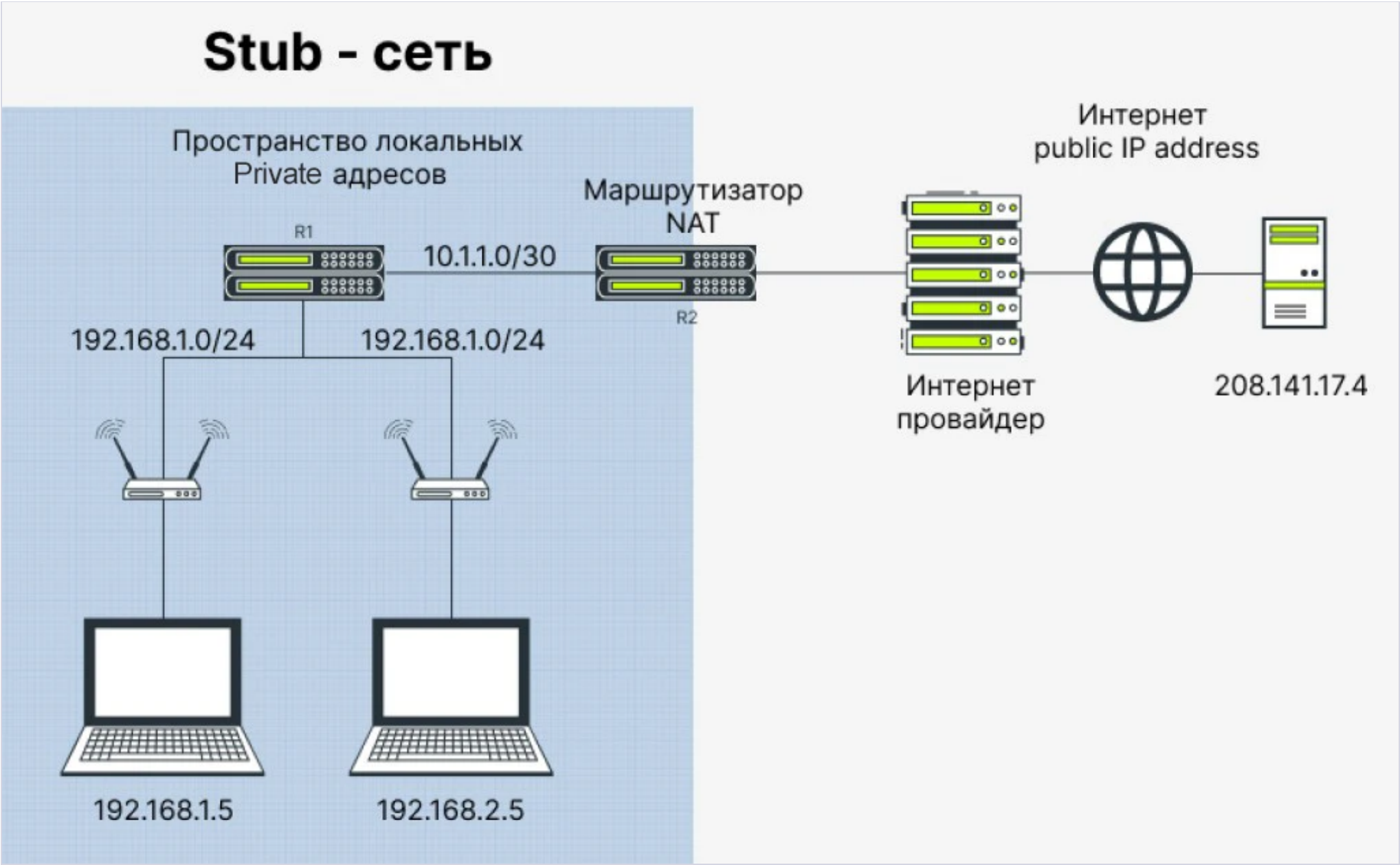
### 5.2 Подсети в NAT

Локальные сети обычно проектируются с использованием частных IP-адресов. Это адреса из приватных подсетей `10.0.0.0/8`, `172.16.0.0/12` и `192.168.0.0/16`. Эти IP-адреса используются внутри организации или площадки, чтобы позволить устройствам общаться локально, они не маршрутизируются в интернете.

Роутеры с поддержкой NAT могут быть настроены с одним или несколькими действительными общедоступными IPv4-адресами. Эти общедоступные адреса называются пулом NAT.

Когда устройство из внутренней сети отправляет трафик из сети наружу, то роутер с поддержкой NAT переводит внутренний IP-адрес устройства на публичный IP-адрес из пула NAT. Для внешних устройств весь трафик, входящий и исходящий из сети, выглядит имеющим общедоступный IP-адрес.

Маршрутизатор NAT обычно работает на границе Stub-сети. Stub-сеть – это термин из теории сетей: тупиковая сеть, которая имеет одно соединение с соседней сетью, один вход и выход из сети.



Когда устройство внутри Stub-сети хочет связываться с устройством за пределами своей сети, пакет пересылается роутеру и он выполняет NAT-процесс, переводя внутренний частный адрес устройства на публичный, внешний, маршрутизируемый адрес.

### 5.3 Терминология NAT

Если углубиться в теорию сетей, то NAT — это внутренняя сеть, которая представляет собой набор подсетей, подлежащих переводу. Внешняя сеть относится ко всем другим сетям.

При использовании NAT, IP адреса имеют разные обозначения, основанные на том, находятся ли они в частной сети или в общедоступной сети (в интернете) и является ли трафик входящим или исходящим.

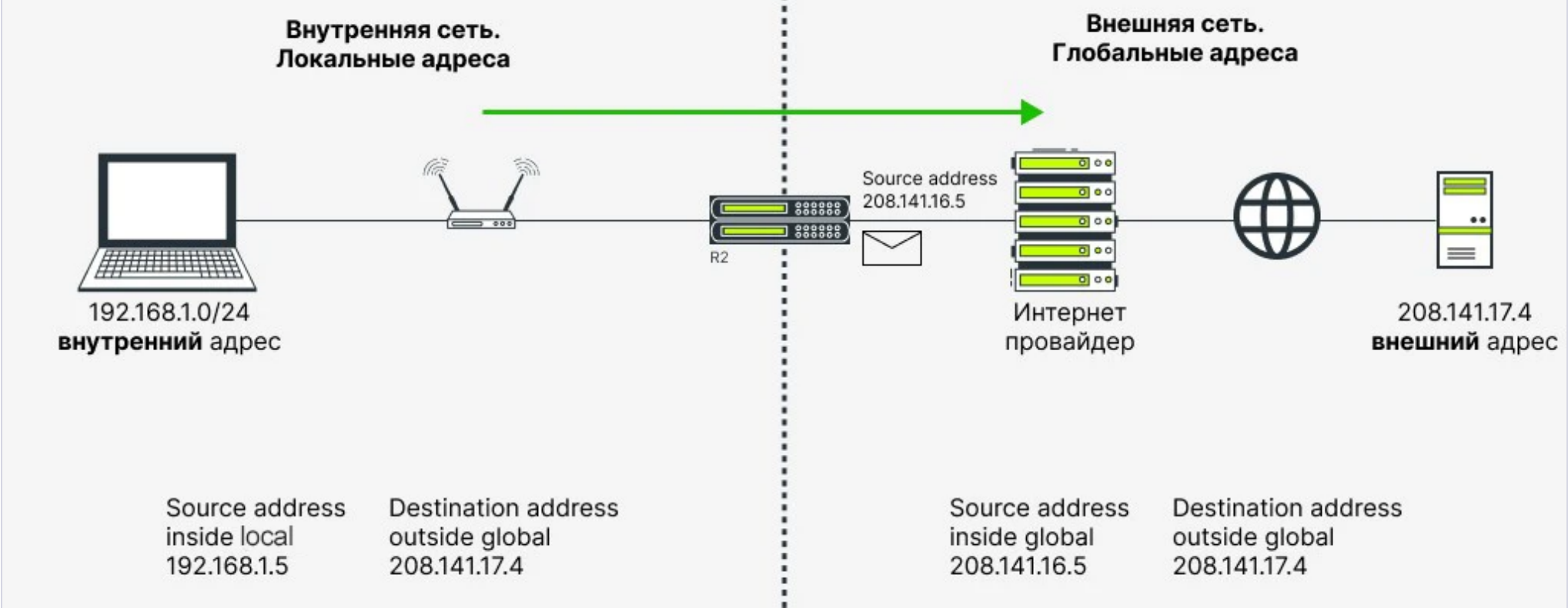
NAT включает в себя четыре типа адресов:

- **Внутренний локальный адрес** (Inside local address);
- **Внутренний глобальный адрес** (Inside global address);
- **Внешний местный адрес** (Outside local address);
- **Внешний глобальный адрес** (Outside global address);

При определении того, какой тип адреса используется, важно помнить, что терминология NAT всегда применяется с точки зрения устройства с транслированным адресом:

- **Внутренний адрес** (Inside address) – адрес устройства, которое транслируется NAT;
- **Внешний адрес** (Outside address) – адрес устройства назначения;
- **Локальный адрес** (Local address) – это любой адрес, который отображается во внутренней части сети;
- **Глобальный адрес** (Global address) – это любой адрес, который отображается во внешней части сети.

Рассмотрим это на примере схемы.





ПК		Веб-сервер	
Insde Global	Inside Local	Outside Local	Outside Global
208.141.17.4	192.168.1.5	208.141.16.5	208.141.16.5

Внутренний локальный адрес (**Inside local address**) – адрес источника, видимый из внутренней сети. На рисунке адрес `192.168.1.5` присвоен компьютеру – это и есть его внутренний локальный адрес.

Внутренний глобальный адрес (Inside global address) – адрес источника, видимый из внешней сети. На рисунке, когда трафик с компа отправляется на веб-сервер по адресу `208.141.17.4`, роутер переводит внутренний локальный адрес (local address) на внутренний глобальный адрес (Inside global address). В этом случае роутер изменяет адрес источника **IPv4** с `192.168.1.5` на `208.141.16.5`.

Внешний глобальный адрес (Outside global address) – адрес адресата, видимый из внешней сети. Это глобально маршрутизируемый IP-адрес, назначенный хосту в интернете. На схеме веб-сервер доступен по адресу `208.141.17.4`. Чаще всего внешние локальные и внешние глобальные адреса одинаковы.

Внешний локальный адрес (Outside local address) – адрес получателя, видимый из внутренней сети. В этом примере комп отправляет трафик на веб-сервер по адресу `208.141.17.4`

Теперь давай рассмотрим весь путь прохождения пакета. Комп с адресом `192.168.1.5` пытается установить связь с веб-сервером `208.141.17.4`. Когда пакет прибывает в маршрутизатор с поддержкой NAT, он считывает IP-адрес назначения пакета, чтобы определить, соответствует ли пакет критериям, указанным для перевода. В этом примере исходный адрес соответствует критериям и переводится с `192.168.1.5` (Inside local address) на `208.141.16.5` (Inside global address).

Роутер добавляет это сопоставление локального в глобальный адрес в таблицу NAT и отправляет пакет с переведенным адресом источника в пункт назначения. Веб-сервер отвечает пакетом, адресованным внутреннему глобальному адресу ПК (`208.141.16.5`).

Роутер получает пакет с адресом назначения `208.141.16.5` и проверяет таблицу NAT, в которой находит запись для этого сопоставления. Он использует эту информацию и переводит обратно внутренний глобальный адрес (`208.141.16.5`) на внутренний локальный адрес (`192.168.1.5`), пакет перенаправляется в сторону ПК.

## 5.5 Преимущества и недостатки NAT

Сервис NAT – это очень мощное решение, которое используется повсеместно. NAT предоставляет **множество преимуществ**, в том числе:

- NAT сохраняет зарегистрированную схему адресации, обеспечивая гибкую работу локальных сетей. При NAT внутренние хосты могут совместно использовать один публичный IP-адрес для всех внешних коммуникаций. В этом типе конфигурации требуется очень мало внешних адресов для поддержки многих внутренних хостов.
- NAT повышает гибкость соединений с интернетом. Многочисленные пулы, пулы резервного копирования и пулы балансировки нагрузки могут быть реализованы для обеспечения надежных общедоступных сетевых подключений.
- NAT обеспечивает согласованность для внутренних схем адресации сети. В сети, не использующей частные IP-адреса и NAT, изменение общей схемы IP-адресов требует переадресации всех хостов в существующей сети. Стоимость переадресации хостов может быть значительной. NAT позволяет существующей частной адресной схеме IPv4 оставаться, позволяя легко изменять новую схему общедоступной адресации. Это означает, что организация может менять провайдеров и не нужно менять ни одного из своих внутренних клиентов.
- NAT **обеспечивает сетевую безопасность**. Поскольку частные сети не рекламируют свои адреса или внутреннюю топологию, они остаются достаточно надежными при использовании в сочетании с NAT для получения контролируемого внешнего доступа. Однако нужно понимать, что NAT не заменяет фаерволы

Но у NAT есть некоторые **недостатки**. Тот факт, что хосты в интернете, по-видимому, напрямую взаимодействуют с устройством с поддержкой NAT, а не с фактическим хостом внутри частной сети, создает ряд проблем:

- Один из недостатков использования NAT связан с производительностью сети, особенно для протоколов реального времени, таких как VoIP. NAT увеличивает задержки переключения, потому что перевод каждого IP-адреса в заголовках

пакетов требует времени.

- Другим недостатком использования NAT является то, что сквозная адресация теряется. Многие интернет-протоколы и приложения зависят от сквозной адресации от источника до места назначения. Некоторые приложения не работают с NAT. Приложения, которые используют физические адреса, а не квалифицированное доменное имя, не доходят до адресатов, которые транслируются через NAT-маршрутизатор. Иногда этого можно избежать, реализуя статические сопоставления NAT.
- Также теряется сквозная трассировка IPv4. Сложнее трассировать пакеты, которые подвергаются многочисленным изменениям адресов пакетов в течение нескольких NAT-переходов, что затрудняет поиск и устранение неполадок.
- Использование NAT также затрудняет протоколы туннелирования, такие как IPsec, поскольку NAT изменяет значения в заголовках, которые мешают проверкам целостности, выполняемым IPsec и другими протоколами туннелирования.
- Службы, требующие инициирования TCP-соединений из внешней сети, или stateless протоколы, например, использующие UDP, могут быть нарушены. Если маршрутизатор NAT не настроен для поддержки таких протоколов, входящие пакеты не могут достичь своего адресата.

[← Предыдущая лекция](#)

Следующая лекция >

 **+17** 

### Комментарии (6)

## популярные

## НОВЫЕ

старые

**JavaCoder**

Введите текст комментария

**Gleb** Уровень 48

14 августа, 18:22 

## И Insight на Inside поправяте

Ответить

 **+2** 

**Anastasiya** Уровень 15

2 августа, 12:21

Долго вдупляла в локал и глобал адрес, потому что на картинках с пересылкой пакета и схеме адрес 192.168.1.5 подписан как Insight Global, в не **Insight Local**. А вот в тексте и таблице потом уже написано правильно. Поправьте, пожалуйста, на картинках, а то и так тема на абстрактное мышление, а с ошибками в материалах еще сложнее заходит

Ответить

 **+3** 

## Anastasiya Уровень 15

2 августа, 12:24 ⋮

И в тексте под таблицей: "...роутер переводит внутренний **локальный** адрес (**global** address) на внутренний глобальный адрес (Inside global address)"

Ответить

 **+2** 

Vladislav Shamshurin Уровень 1

3 августа, 11:56 ⋮

Да забей) Когда это тебе в реальной работе понадобится (если понадобится) - ты уже достаточно многое забудешь) Придётся заново вникать

Ответить

– +3 +

**Александр Ц.** System Engineer

15 сентября, 19:36 

"Privet"-адреса!

Ответить

 **+1** 

## Andrey Panchenko Моет полы в Яндекс

16 сентября, 19:08 ⋮

Смысл - понять суть вещей. Детали забываются, но суть в памяти сохраняется 📌 Так что всё правильно Anastasiya делает.

Ответить

 **+1** 

ОБУЧЕНИЕ

- Курсы программирования
- Курс Java
- Помощь по задачам
- Подписки
- Задачи-игры

СООБЩЕСТВО

- Пользователи
- Статьи
- Форум
- Чат
- Истории успеха
- Активности

КОМПАНИЯ

- О нас
- Контакты
- Отзывы
- FAQ
- Поддержка



JavaRush — это интерактивный онлайн-курс по изучению Java-программирования с нуля. Он содержит 1200 практических задач с проверкой решения в один клик, необходимый минимум теории по основам Java и мотивирующие фишки, которые помогут пройти курс до конца: игры, опросы, интересные проекты и статьи об эффективном обучении и карьере Java-девелопера.

ПОДПИСЫВАЙТЕСЬ

ЯЗЫК ИНТЕРФЕЙСА

Русский

СКАЧИВАЙТЕ НАШИ ПРИЛОЖЕНИЯ

