

Подключение к серверу по ssh

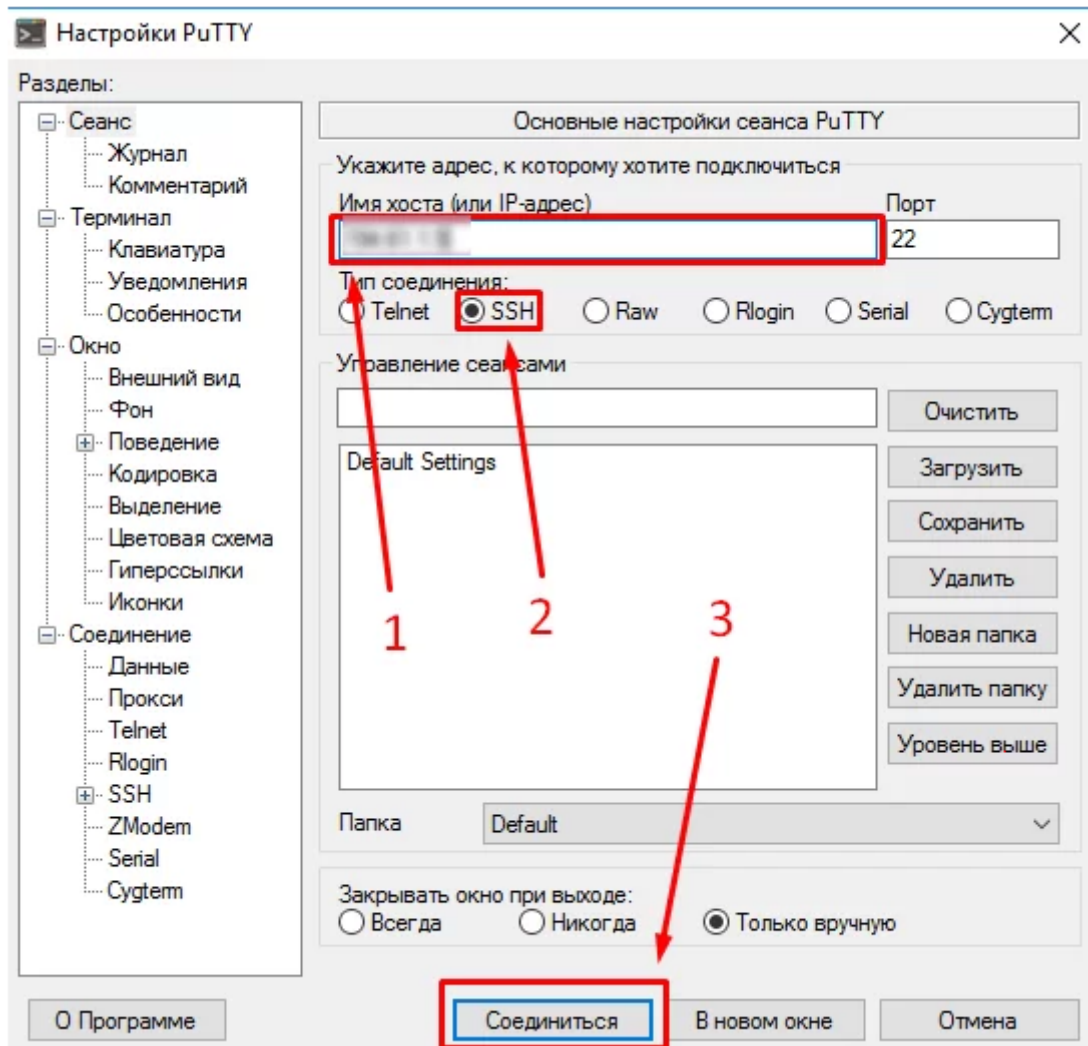
SSH — сетевой протокол, позволяющий создать безопасное удалённое подключение к серверам на базе ОС Linux.

Как подключиться с ОС Windows по SSH

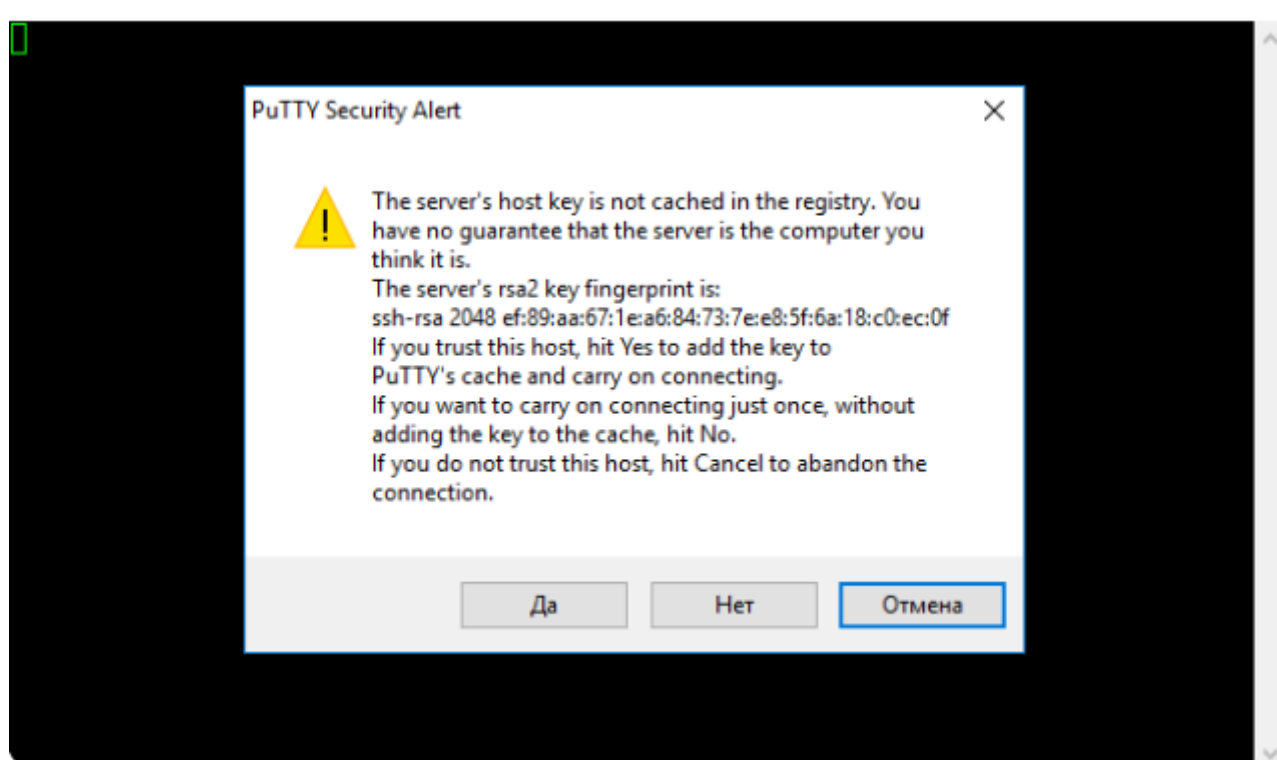
Если на вашем компьютере установлена ОС Windows, а на сервере — UNIX-подобная система (например, Ubuntu, Debian, CentOS и др.), то для установки SSH-соединения можно использовать PuTTY. Это бесплатная программа под Windows состоит из одного запускаемого файла и не требует установки. Скачать её можно с официального сайта по [ссылке](#)

Чтобы установить соединение при помощи PuTTY, необходимо проделать следующие действия:

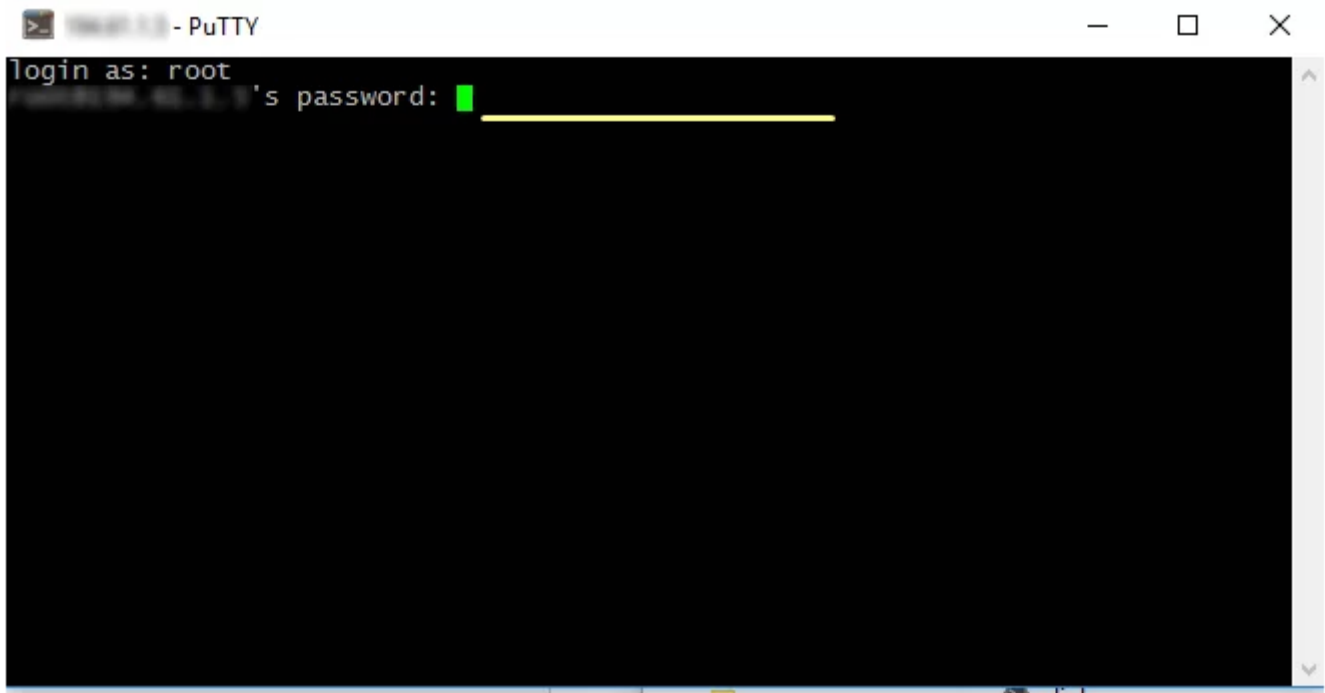
1. Скачайте нужную версию PuTTY по [ссылке](#).
2. Запустите файл `putty.exe`. Откроется окно программы. Вводим IP-адрес сервера в графу «Имя хоста». Проверяем графу «Тип соединения» — должен быть выбран пункт «SSH». Нажимаем «Соединиться».



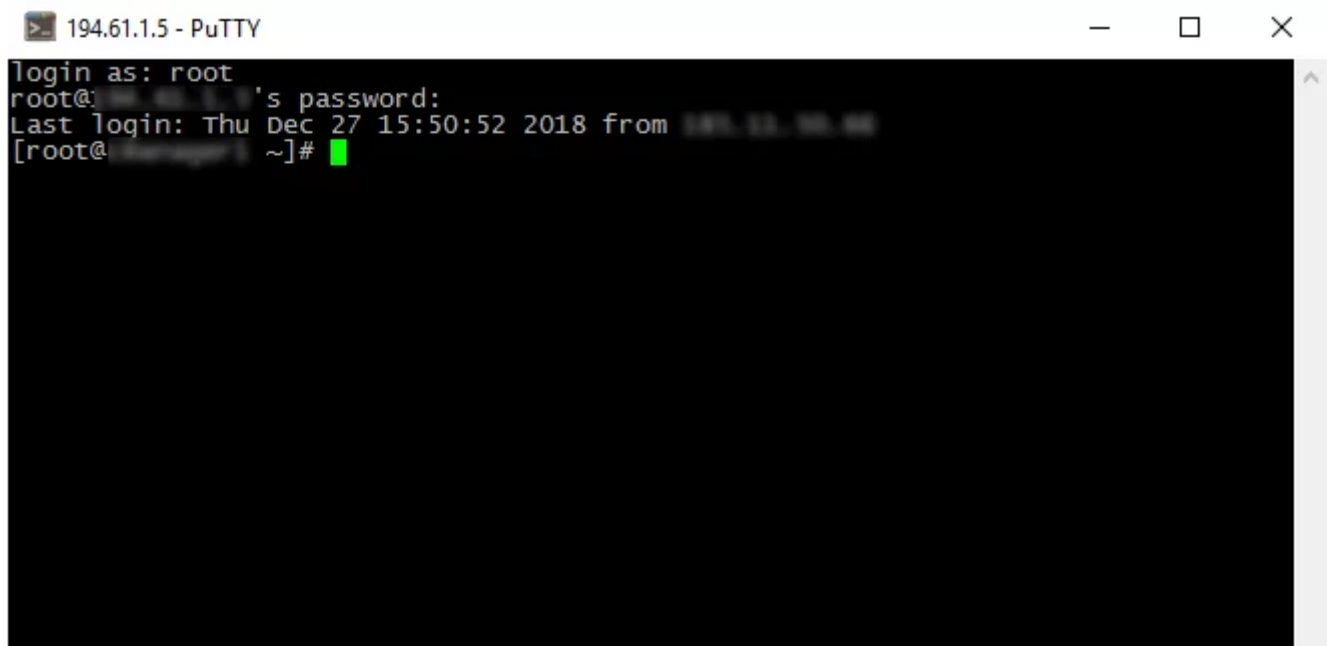
Может появиться предупреждение системы безопасности PuTTY — оно срабатывает при подключении к новому серверу. Нажмите Да — и соединение продолжится.



3. Вводим логин и нажимаем "Enter". Затем вводим пароль и снова нажимаем "Enter"



4. Готово. Мы подключились к серверу по SSH



Как подключиться с ОС Linux по SSH

Для подключения используем SSH-клиент Terminal, который встроен в ОС на основе Linux. При вводе команд нужно помнить, что в Linux-образных ОС они вводятся только в нижнем регистре (с маленькой буквы).

1. Открываем приложение. Вводим команду вида «ssh логин@IP-адрес» . Нажимаем «Enter».

Файл Правка Вид Поиск Терминал Помощь

```
kirill@kirill-pc:~$ ssh root@62.173.138.20
```

2. Если пользователь использует SSH-соединение первый раз, ему потребуется ввести команду подтверждения («Yes»)

Файл Правка Вид Поиск Терминал Помощь

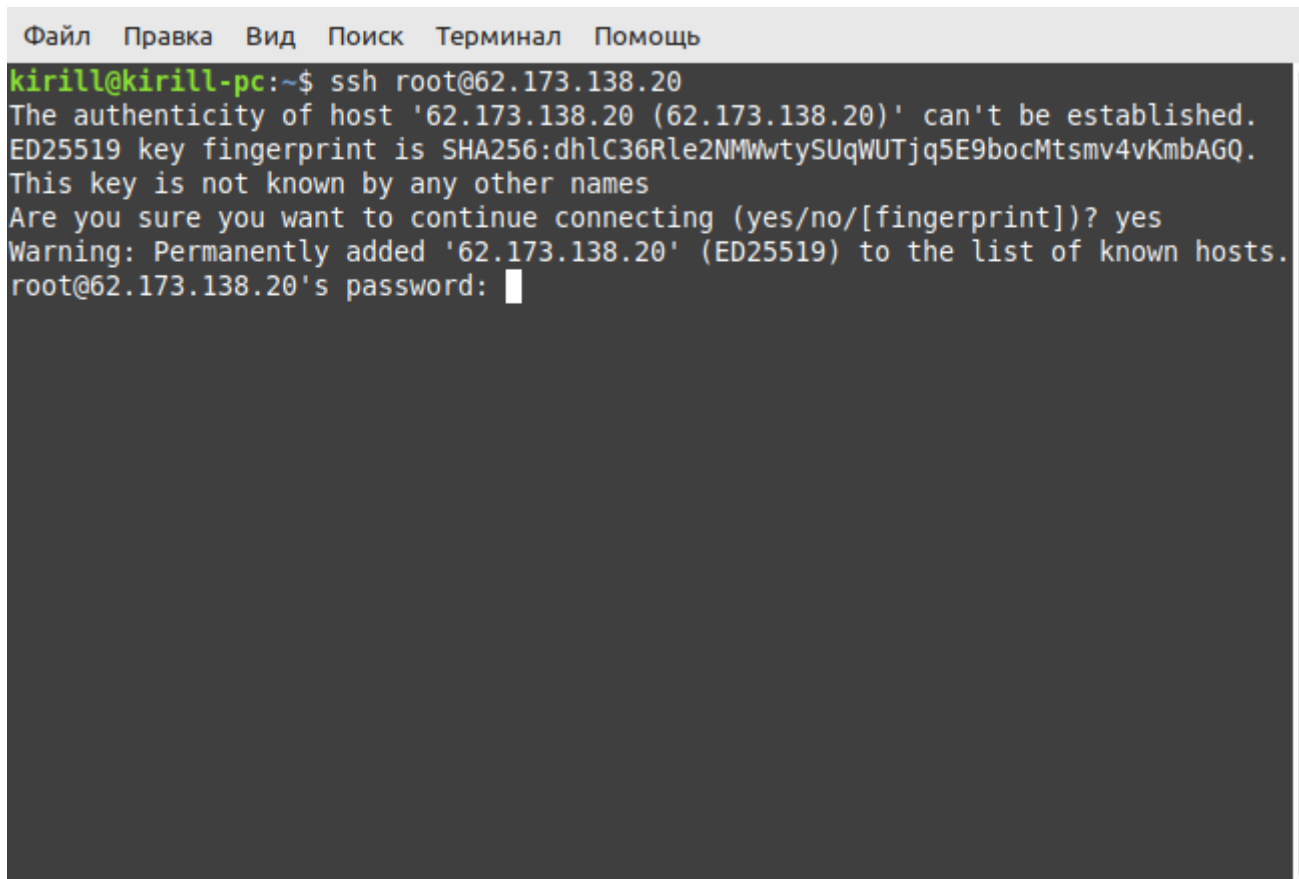
```
kirill@kirill-pc:~$ ssh root@62.173.138.20
```

```
The authenticity of host '62.173.138.20 (62.173.138.20)' can't be established.  
ED25519 key fingerprint is SHA256:dhlC36Rle2NMWwtySUqWUTjq5E9bocMtsmv4vKmbAGQ.
```

```
This key is not known by any other names
```

```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
```

3. Вводим пароль от виртуального сервера и нажимаем "Enter".

A screenshot of a terminal window with a light gray title bar containing menu items: 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Помощь'. The terminal background is dark gray. The text displayed is as follows:
kirill@kirill-pc:~\$ ssh root@62.173.138.20
The authenticity of host '62.173.138.20 (62.173.138.20)' can't be established.
ED25519 key fingerprint is SHA256:dhlC36Rle2NMWwtySUqWUTjq5E9bocMtsmv4vKmbAGQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '62.173.138.20' (ED25519) to the list of known hosts.
root@62.173.138.20's password: [redacted]
The terminal shows a vertical scrollbar on the right side.

4. Готово. Вы успешно подключились к серверу

```
Файл  Правка  Вид  Поиск  Терминал  Помощь
kirill@kirill-pc:~$ ssh root@62.173.138.20
The authenticity of host '62.173.138.20 (62.173.138.20)' can't be established.
ED25519 key fingerprint is SHA256:dhlC36Rle2NMMwtySUqWUTjq5E9bocMtsmv4vKmbAGQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '62.173.138.20' (ED25519) to the list of known hosts.
root@62.173.138.20's password:
Connection closed by 62.173.138.20 port 22
kirill@kirill-pc:~$ ssh root@62.173.138.20
root@62.173.138.20's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-169-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed 31 Jan 2024 12:55:34 PM MSK

System load:  0.0           Processes:      118
Usage of /:   6.7% of 39.28GB Users logged in: 0
Memory usage: 14%          IPv4 address for ens3: 62.173.138.20
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

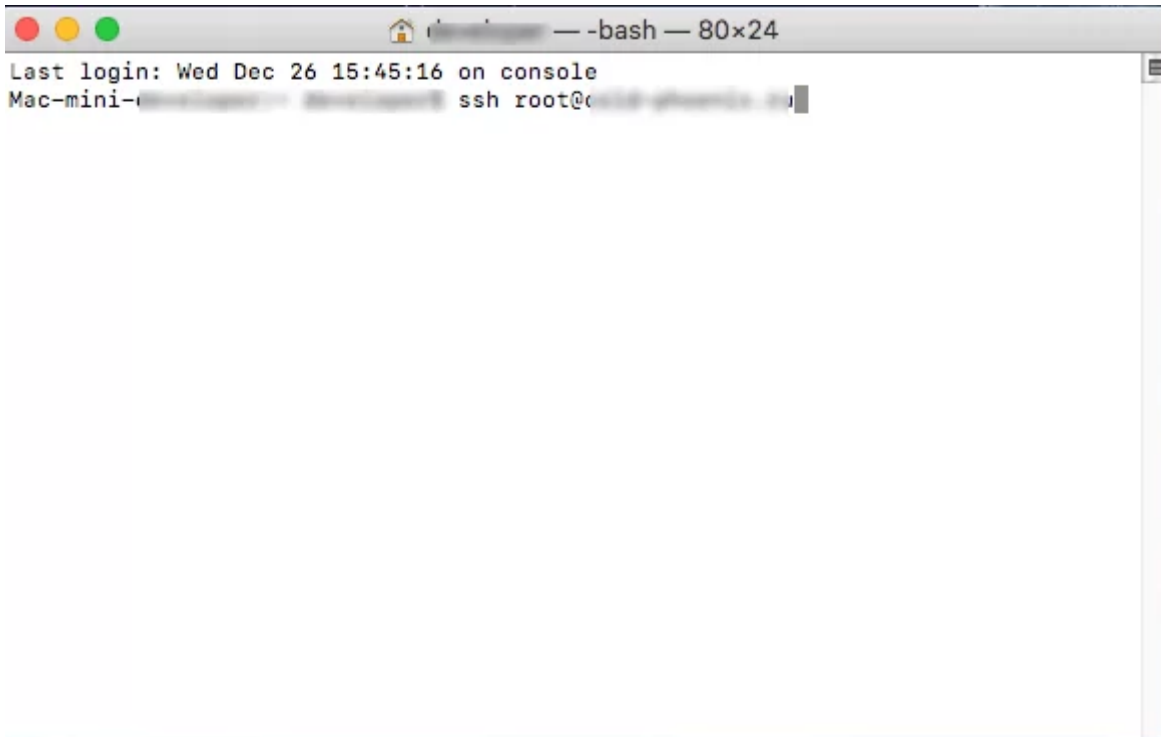
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Jan 31 11:54:47 2024 from 85.93.129.147
root@kirill:~#
```

Как подключиться с macOS и iOS по SSH

Для подключения к серверу по SSH с устройств на операционной системе macOS, также как и в предыдущем случае, используем встроенный клиент Terminal.

1. Открываем приложение. Вводим команду с данными сервера «ssh логин@IP-адрес». Нажимаем «Enter».



A terminal window titled "developer — -bash — 80x24". The window shows the output of an SSH command: "Last login: Wed Dec 26 15:45:16 on console" followed by "Mac-mini-... ssh root@...". The cursor is at the end of the second line.

```
Mac-mini-... ssh root@...
```

2. При первом входе подтверждаем свои действия соответствующей командой «Yes».



A terminal window titled "ssh -p 3110 root@... — 80x24". The window shows the output of an SSH command: "Mac-mini-...:~ developer\$ ssh -p 3110 root@...". This is followed by a warning message: "The authenticity of host '[...]:3110 ([...]):3110)' can't be established." and "ECDSA key fingerprint is SHA256:...". The prompt "Are you sure you want to continue connecting (yes/no)? yes" is shown with "yes" entered.

```
Mac-mini-...:~ developer$ ssh -p 3110 root@...
The authenticity of host '[...]:3110 ([...]):3110)' can't be established.
ECDSA key fingerprint is SHA256:...
Are you sure you want to continue connecting (yes/no)? yes
```

3. Вводим пароль от виртуального сервера.

