

Работа с серверами и протокол удалённого управления SSH

Владислав Шевченко

Ведущий инженер разработки и внедрения моделей машинного обучения Альфа-Банке

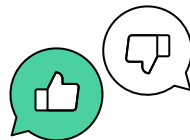


Проверка связи





Если у вас нет звука:

- убедитесь, что на вашем устройстве и на колонках включён звук
- обновите страницу вебинара (или закройте страницу и заново присоединитесь к вебинару)
- откройте вебинар в другом браузере
- перезагрузите компьютер (ноутбук) и заново попытайтесь зайти



Поставьте в чат:

-  если меня видно и слышно
-  если нет

Владислав Шевченко

О спикере:

- ментор программы «Инженерия данных»
- ведущий инженер разработки и внедрения моделей машинного обучения в Альфа-Банке
- преподаватель дисциплины «Семинар наставника»



Правила участия

- 1 Приготовьте блокнот и ручку, чтобы записывать важные мысли и идеи
- 2 Продолжительность вебинара — 80 минут
- 3 Вы можете писать свои вопросы в чате
- 4 Запись вебинара будет доступна в LMS
- 5 Обсуждения можно продолжить в Telegram



Цели занятия

- 1 Отработаем практические навыки по работе с SSH
- 2 Изучим методы поднятия сетевых сервисов
- 3 Узнаем на практике как работает SSH



План занятия

- 1 Что такое OpenSSH
- 2 Развёртывание и настройка тестовых стендов



Что такое OpenSSH



1

Введение в OpenSSH

OpenSSH (Open Secure Shell) — это программное обеспечение с открытым исходным кодом, реализующее протокол **SSH (Secure Shell)**.

SSH используется для безопасного доступа к удалённым компьютерам, передачи файлов, а также для выполнения команд на удалённых системах.

[Источник](#)



История создания OpenSSH

Идея и разработка

OpenSSH был создан как открытая альтернатива проприетарной версии SSH, разработанной Тату Юлоненом в 1995 году.

В 1999 году проект OpenSSH был запущен разработчиками OpenBSD во главе с Тео де Раадтом.

История создания OpenSSH

Первая версия OpenSSH

Первая версия **OpenSSH** была выпущена в декабре 1999 года как часть операционной системы OpenBSD.

С тех пор OpenSSH стал доступен для большинства Unix-подобных операционных систем, таких как Linux, FreeBSD, macOS, а также Windows.

Зачем был создан OpenSSH

OpenSSH обеспечивает:

- Безопасность
- Открытость и доступность
- Интеграцию с OpenBSD

Как работает OpenSSH

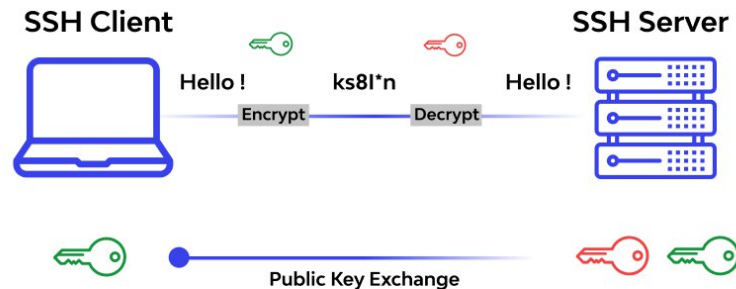
1. Как клиент-серверная архитектура

2. Как утилентификация

- Парольная аутентификация
- Аутентификация по ключам SSH
- Многофакторная аутентификация

3. Как шифрование

4. Как портфорвардинг (туннелирование)



[Источник](#)

Где применяется OpenSSH

- Администрирование серверов
- Передача файлов
- Туннелирование и прокси
- Автоматизация задач

Преимущества OpenSSH

- Безопасность
- Открытый исходный код
- Широкая поддержка

Текущее состояние и популярность OpenSSH

- Использование в корпоративной среде
- Поддержка новых стандартов
- Интеграция с другими инструментами



Ваши вопросы?



Развёртывание и настройка тестовых стендов



2

Для mac

- Устанавливаем:

Docker

- Запускаем через команду:

docker run -p 2222:22 -it --platform linux/x86_64 ubuntu bash

- После попадания внутрь контейнера, выполняем настройку:

apt update

apt install nano

apt install -y openssh-server

mkdir /var/run/sshd

echo 'root:root' | chpasswd

Для mac

- Редактируем конфигурационный файл:

nano /etc/ssh/sshd_config

- Убираем комментирование порта:

22

- Убираем комментирование и прописываем:

yes в **PermitRootLogin**

- Далее выполняем запуск **ssh** сервера с помощью команды:

/usr/sbin/sshd

Для Windows

- Открываем командную строку или **PowerShell** с правами администратора
- Запускаем SSH-сервер с помощью команды:

net start sshd

- Чтобы настроить автозапуск SSH-сервера при загрузке системы, выполняем:

Set-Service -Name sshd -StartupType 'Automatic'

Для Windows

- Открываем wsl или образ unix-системы в Virtual Box
- Выполняем следующие команды:

sudo apt update

sudo apt install -y openssh-server

- Настраиваем SSH-сервер, открыв конфигурационный файл:

sudo nano /etc/ssh/sshd_config

- Проверяем, что параметр **PermitRootLogin** установлен в **yes**, а также порт указан **22**

Для Windows

- WSL использует динамический IP-адрес, который может изменяться при каждом запуске. Узнаём текущий IP-адрес, выполнив команду:

ip addr show eth0

- Находим строку **inet**, содержащую IP-адрес (например, 172.20.224.1)
- Выполняем подключение с помощью PowerShell, ранее запущенным администратором, с помощью команды:

ssh user@172.20.224.1



Ваши вопросы?

Итоги занятия

- Отработали практические навыки по работе с SSH
- Изучили методы поднятия сетевых сервисов
- Узнали на практике как работает SSH



Рефлексия

- Что изменилось? «Раньше я думал(а), что..., а теперь...»
- Какие вопросы у меня остались?



Следующий вебинар

→ Практика по работе с SSH



Работа с серверами и протокол удалённого управления SSH

Владислав Шевченко

Ведущий инженер разработки и внедрения моделей машинного обучения Альфа-Банке

