Шпаргалка: 8 правил безопасности VPS

Закроет 95% типовых атак.

VPS даёт полную свободу — и полную ответственность. Без этих 8 пунктов сервер взломают через недели после публикации.

01 **Отключить root-вход по SSH**
Создать обычного пользователя с sudo. В sshd_config: PermitRootLogin no. Отсекает большинство автоматических атак.

02 **SSH-ключи вместо паролей**
ssh-keygen на своём ПК, ssh-copy-id на сервер. PasswordAuthentication no в sshd_config. Подобрать ключ нельзя.

03 **Поменять порт SSH с 22**
На 2222, 7654 или любой другой. 90% сканеров ищут только 22 — отсекаются. Не забудьте открыть новый порт в брандмауэре.

04 **Настроить UFW (брандмауэр)**
ufw default deny + разрешить только нужные порты (SSH, 80, 443). Закрывает доступ к лишним сервисам.

05 **Установить fail2ban**
После 3 неудачных попыток входа IP блокируется на час. Автоматическая защита от brute-force.

06 **Регулярные обновления**
apt update && apt upgrade раз в неделю-две. Без обновлений уязвимости накапливаются.

07 **Автобэкапы + внешние копии**
Хостинг + облако (S3, Yandex Cloud). Не держите единственную копию на том же сервере.

08 **Мониторинг и алерты**
Логи доступа, UptimeRobot для проверки доступности, Wordfence/Sucuri для WP. Узнать о проблеме за час, а не за неделю.

> Подробный гайд:
> https://host.seoshnic.ru/osnovy/bezopasnost-vps-server/