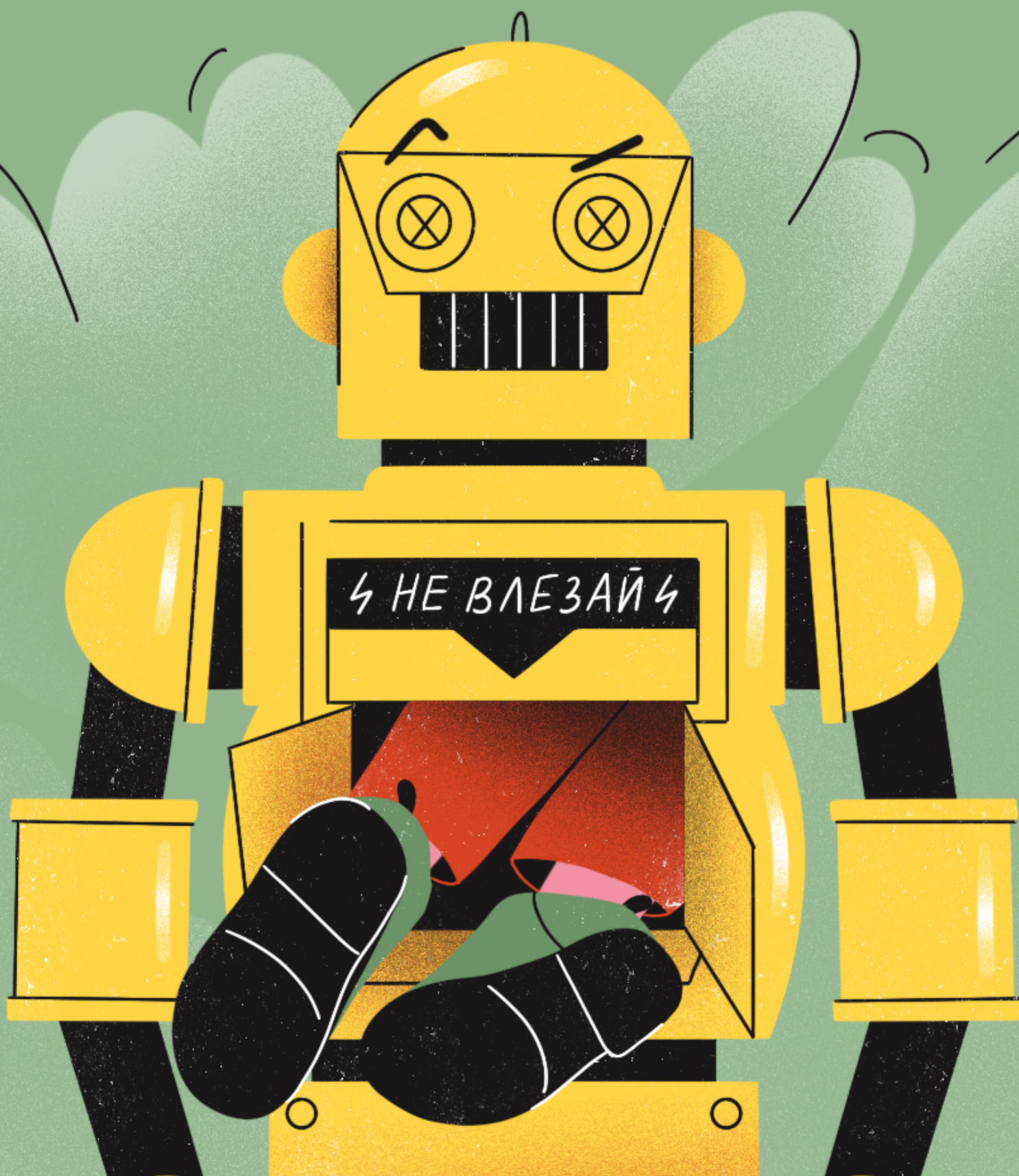


Как уберечь себя и не сломать учебное
окружение: виртуальную машину, Yandex
Cloud, Jenkins, Grafana и другое



На практике вы будете использовать различные инструменты, которые, как и все вещи в мире, можно сломать, например, погасить sshd-сервис. Также можно случайно предоставить доступ злоумышленнику, чтобы майнить биткойны на ваших ресурсах. Поэтому мы решили предостеречь вас и составили короткую Инструкцию по технике безопасности DevOps, написанную болтою предыдущих потоков.

1. Не делитесь вашей персональной информацией

Иногда возникает соблазн поделиться со сторонними людьми вашими IP-адресами, логинами и паролями к ним, секретными токенами для доступа к сервисам типа Kubernetes, Nexus, Yandex Cloud. Не надо этого делать.

Если вам кажется, что ваш репозиторий на GitHub — это надёжное место для хранения логинов и паролей, то рекомендуем развернуть свой собственный сервер с публичным IP-адресом, а креды от `root` выложить в репозиторий и посчитать до трёхсот. Именно столько в среднем требуется ботам-парсерам, чтобы найти «конфиденциальную» информацию и выполнить подключение на ваш (или уже не только ваш) сервер.

В этом правиле может быть только одно исключение — ваши наставники, которым иногда нужно увидеть ситуацию вашими глазами, чтобы помочь. Однако не спешите бросаться в них учётками, только по просьбе наставника.

2. Ваш сервис должен быть запаролен

Как вы знаете по первому пункту, не стоит разбрасываться кредами налево-направо. Но также не стоит забывать, что необходимо включать авторизацию на том, что вы установили (особенно веб-приложении).

В нашем курсе есть Jenkins и Grafana, для которых нужно поставить логин и пароль, иначе каждый на просторах интернета сможет начать использовать их в своё удовольствие, вопреки вашему. Если сервис больше не нужен — не забудьте его выключить. Вы получите больше ресурсов, а мы — меньше точек проникновения злоумышленников.

3. Прежде чем вносить системные изменения, обдумайте, не сломаете ли

Бывало ли с вами такое, что после удаления папки Windows компьютер перестал запускаться? Нет? Ну и правильно, давайте не повторять этих ошибок и в Linux.

Прежде чем вносить изменения в какой-либо файл, не поленитесь сделать его бэкап. Всего одна команда `cp <имя-файла> <имя-файла>_bkr` — зато сколько спасённых нервных клеток! Вот список самых частых файлов, которые ломают на курсе:

`/etc/sudoers`

`/etc/sudoers.d/<название нового файла>`

`/etc/fstab`

и другие

Если сломаете такой или аналогичный файл, не произойдёт конец света, но резко возрастет дополнительная нагрузка на ваших наставников. Вместо того чтобы рассказать вам, как, например, в Kubernetes переиспользовать `secrets` из другого `namespace`, они будут чинить вам доступ по ssh на виртуальную машину. Инженерам курса также достанутся лишние тикеты. А ведь всего этого можно легко избежать.

4. Скачивать что-то из непроверенных источников

Несмотря на то что мы собрались здесь ради познания чего-то нового, не стоит скачивать и устанавливать на ваш сервер все пакеты из интернета без разбора. Вам могут достаться «паразиты», сильно замедляющие виртуальную машину или делающие работу с ней невозможной.

По всему курсу вы будете находить ссылки и команды — пожалуйста, ограничьтесь только ими. Так надёжнее.

5. Yandex Cloud общий для всей группы


В каталоге Yandex Cloud вам предоставлены внушительные права. Но, как мы знаем, чем больше сила, тем больше и ответственность! Поэтому постарайтесь не уничтожить работу ваших коллег. А если проводите какие-то манипуляции с виртуальными машинами, проверьте ещё один раз.

Ведь никому не хочется, чтобы почти выполненное домашнее задание случайно исчезло, правда?

6. Вход на VM только по доменному имени

Виртуальные машины на курсе раз в сутки попадают в сказку о Золушке и превращаются в тыкву — они перезагружаются. Бывает, что на перезагрузку уходит до 10 минут, поэтому не спешите паниковать, если VM недоступна, просто подождите. Но здесь есть парочка нюансов:

- При каждой перезагрузке виртуальная машина получает новый IP-адрес, поэтому подключаться к ней нужно только по доменному имени.
- Приложения без автозапуска не будут самостоятельно запускаться после перезагрузки VM.



Продолжение
следует...