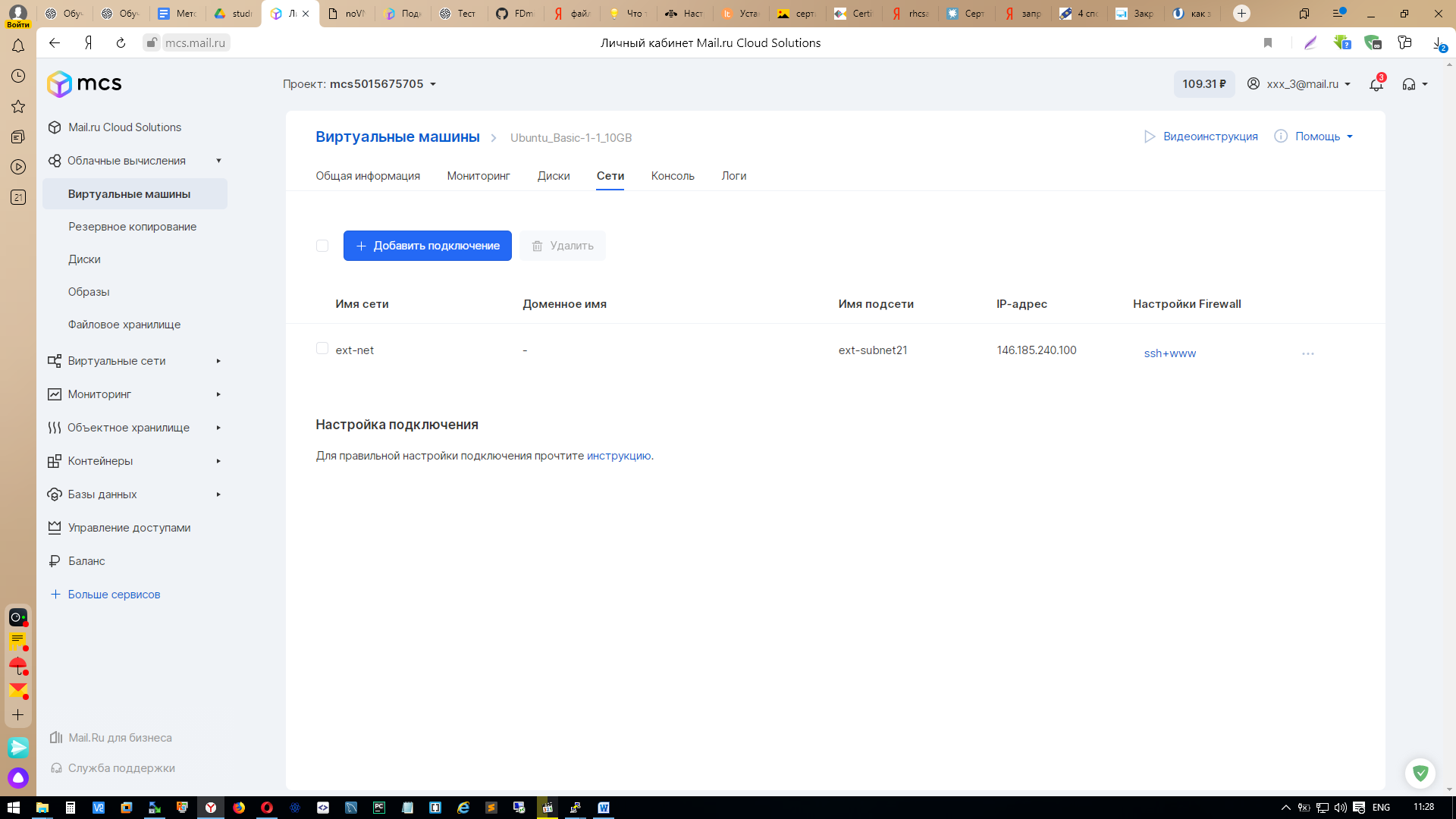
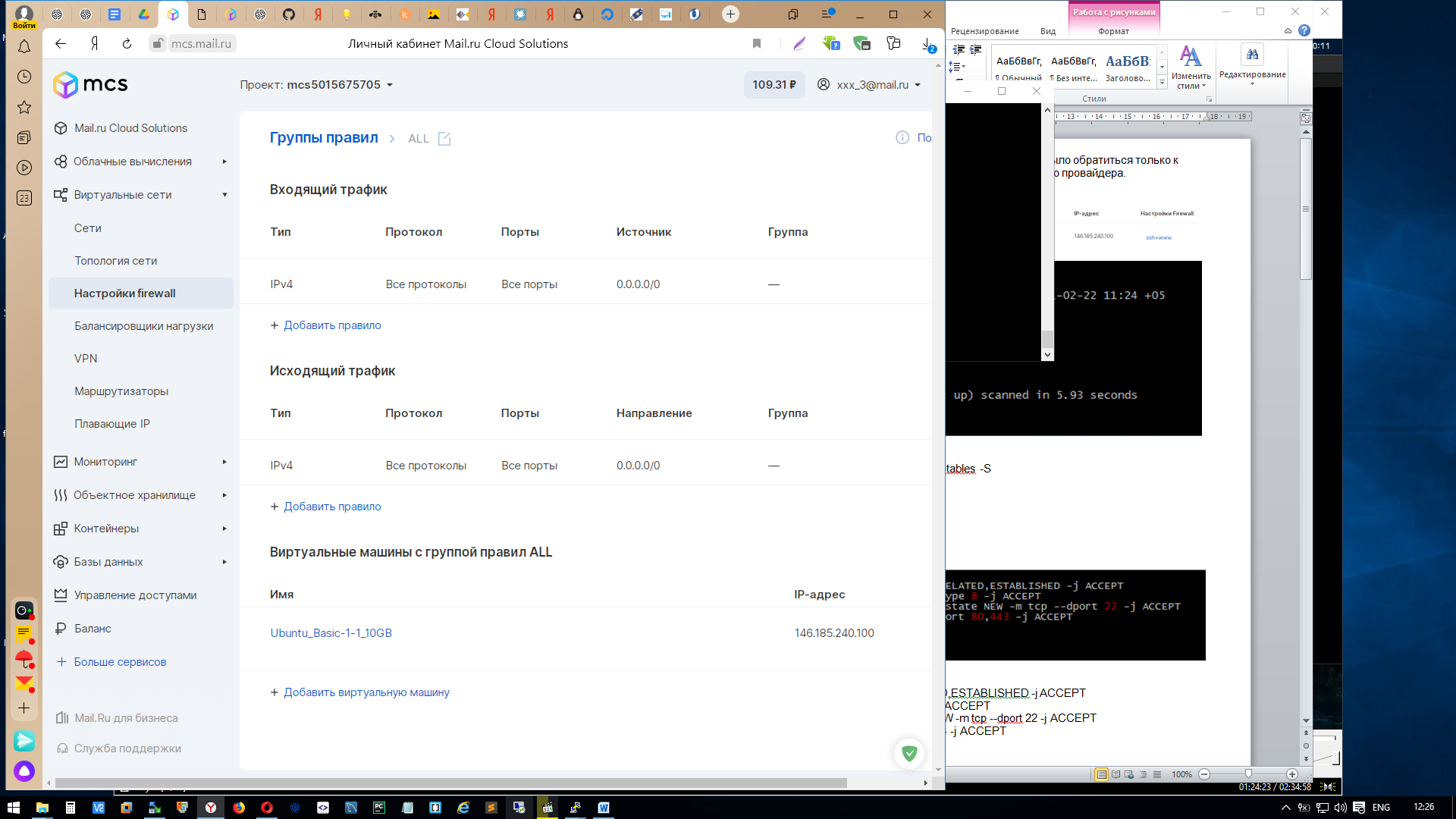
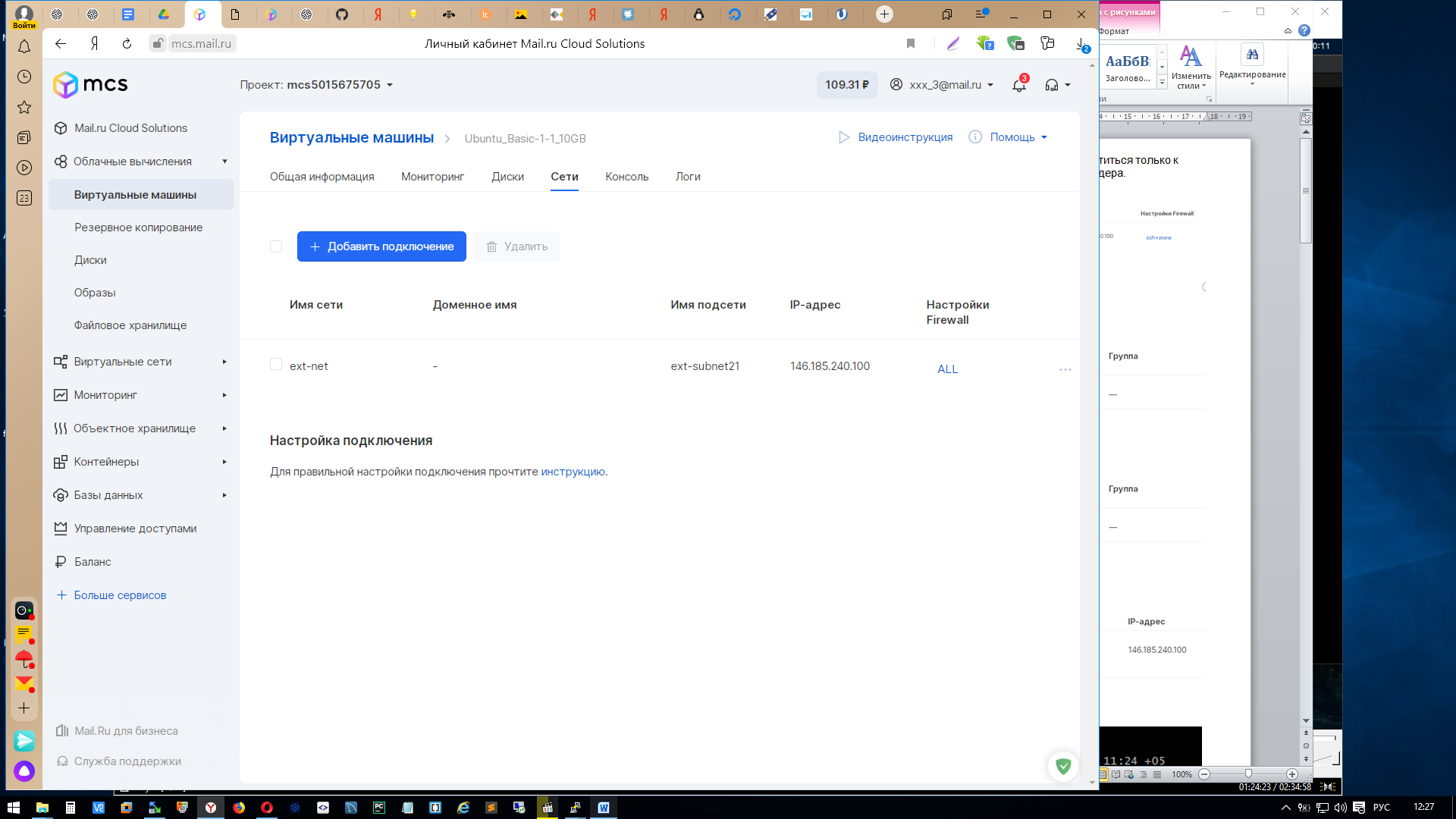
1. Настроить сетевой фильтр, чтобы из внешней сети можно было обратиться только к сервисам http (80 и 443) и ssh. Отключить фаервол облачного провайдера.

В данный момент включен файрвол на сервисе.



Выключаем файрвол на сервисе





Создаем правила на сервере

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo iptables -S

-P INPUT ACCEPT

-P FORWARD ACCEPT

-P OUTPUT ACCEPT

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo iptables -A INPUT -i lo -j ACCEPT

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo iptables -A INPUT -p tcp -m conntrack --ctstate NEW -m tcp --dport 22 -j ACCEPT

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo iptables -A INPUT -j DROP

ubuntu@ubuntu-basic-1-1-10gb:~$

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo netfilter-persistent save

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo iptables -S

-P INPUT ACCEPT

-P FORWARD ACCEPT

-P OUTPUT ACCEPT

-A INPUT -i lo -j ACCEPT

-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT

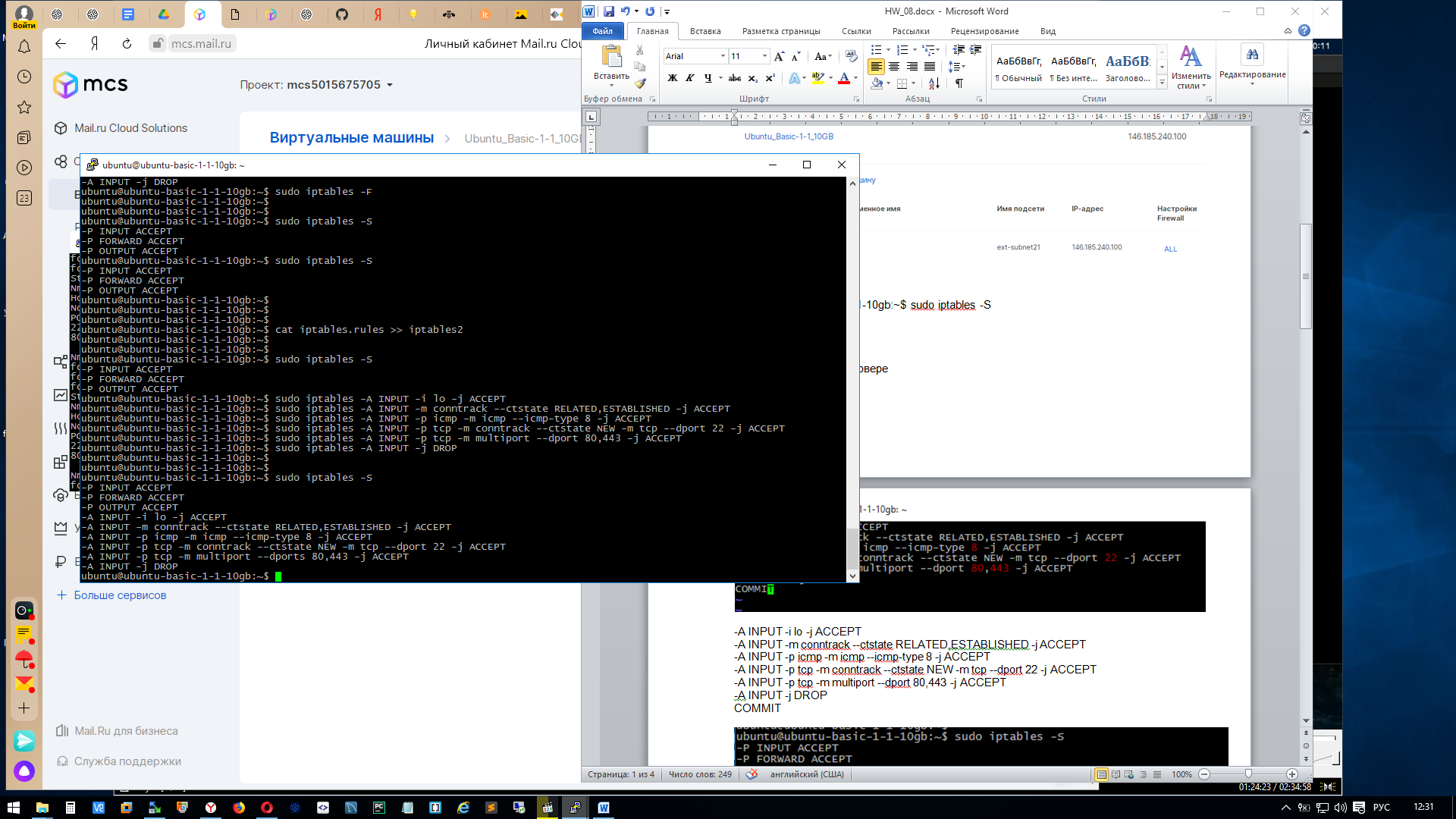
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT

-A INPUT -p tcp -m conntrack --ctstate NEW -m tcp --dport 22 -j ACCEPT

-A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT

-A INPUT -j DROP

ubuntu@ubuntu-basic-1-1-10gb:~$



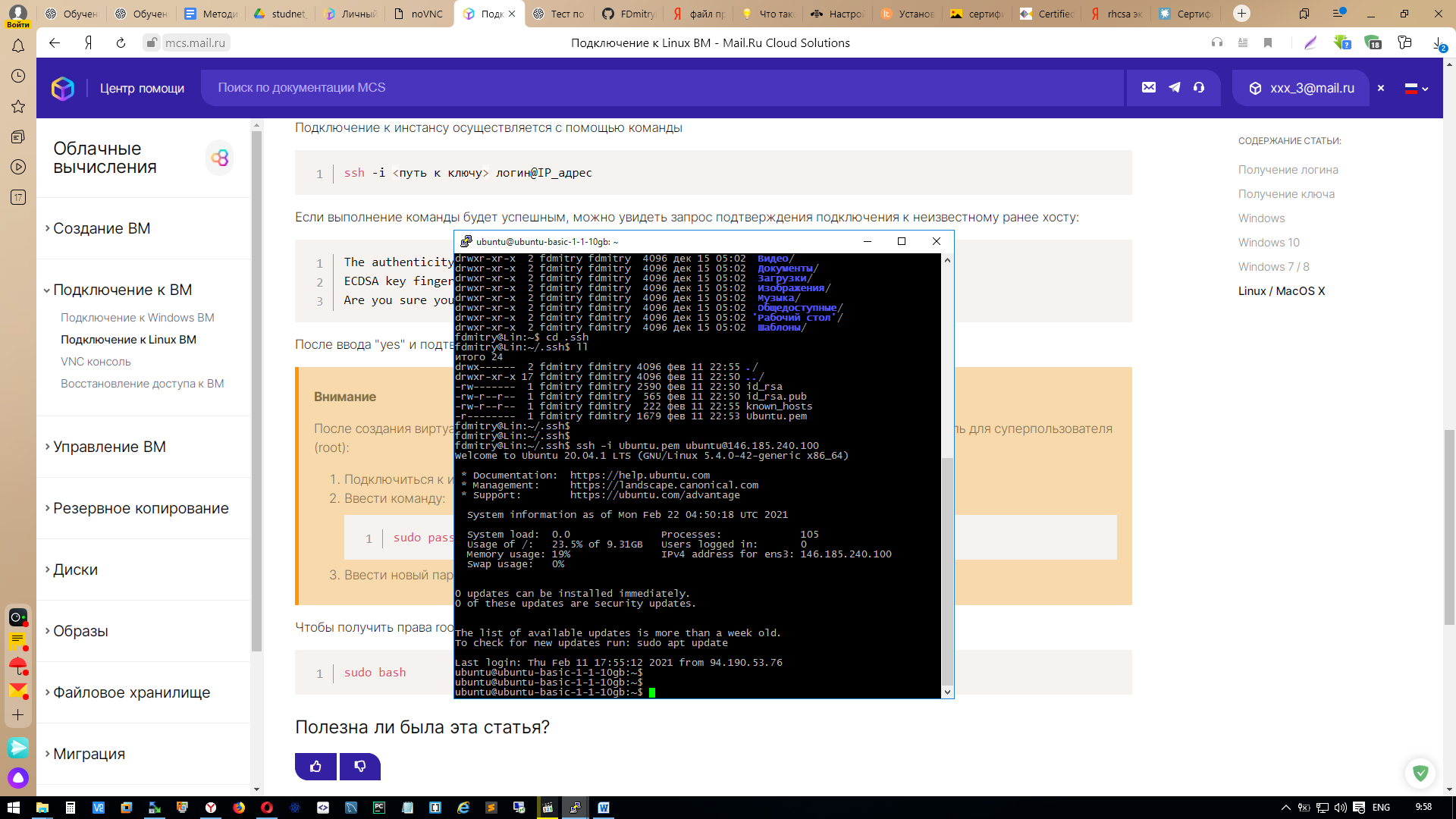
1. Настроить SSH аутентификацию только по ключу, отключить парольную аутентификацию, запретить логин под root

В облаке Mail.ru при создании Виртуальной машины сразу генерируется ключ

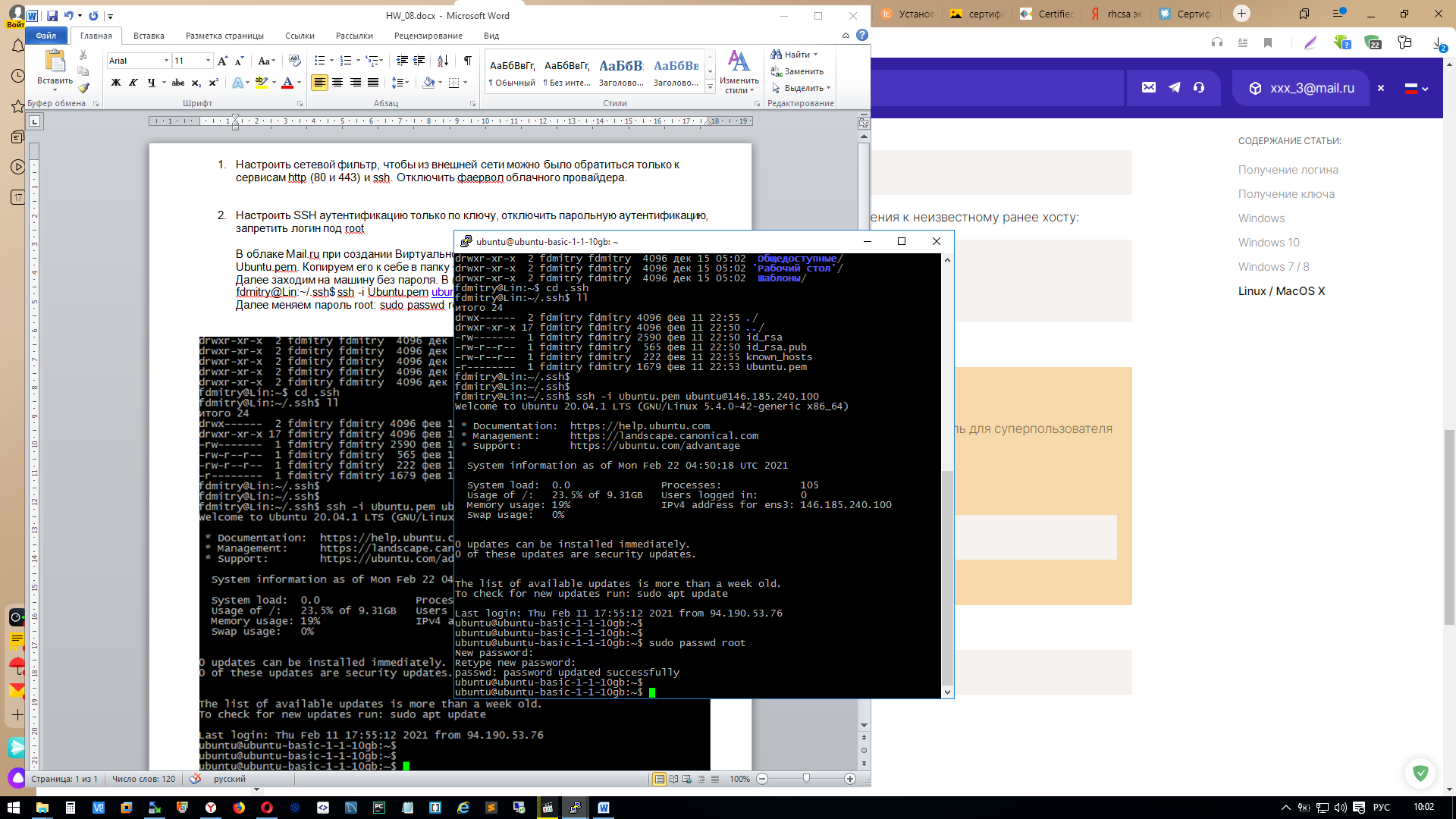
Ubuntu.pem. С личного кабинета сохраняем его и копируем к себе на машину в папку ~/.ssh/

Далее заходим на машину без пароля. В моем случае:

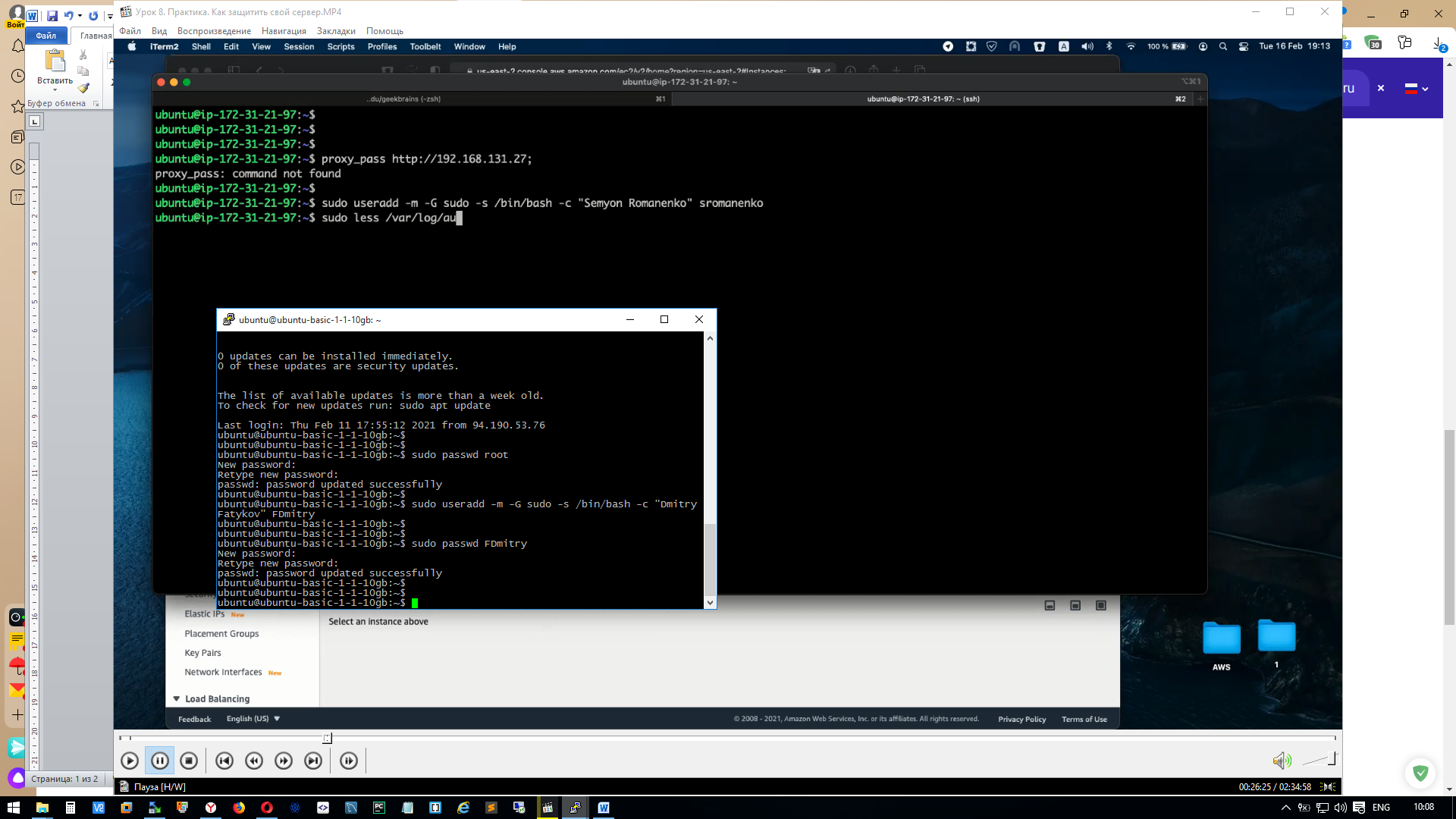
fdmitry@Lin:~/.ssh$ ssh -i Ubuntu.pem [ubuntu@146.185.240.100](mailto:ubuntu@146.185.240.100)



Далее меняем пароль root: sudo passwd root



Создаю своего пользователя

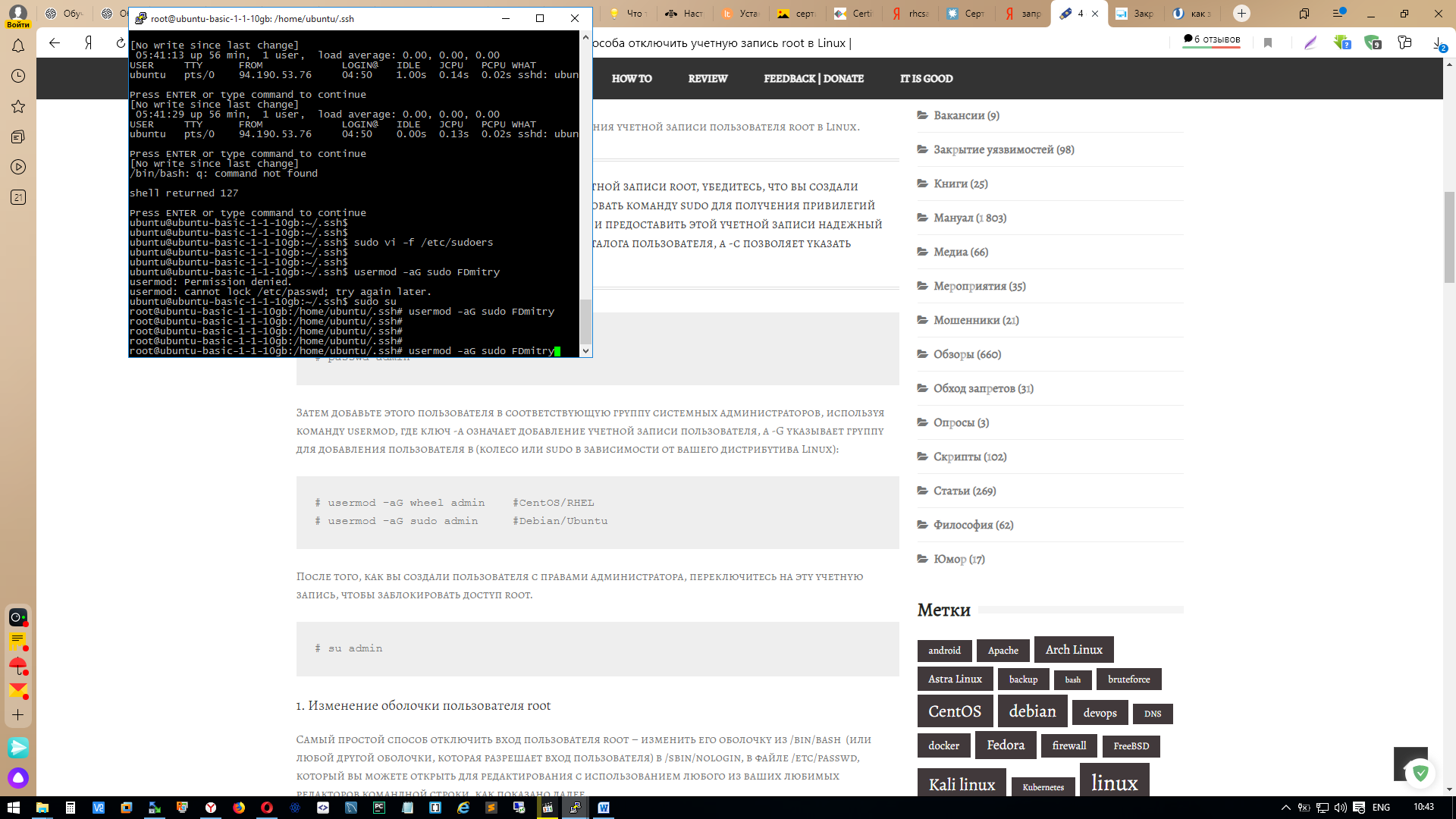


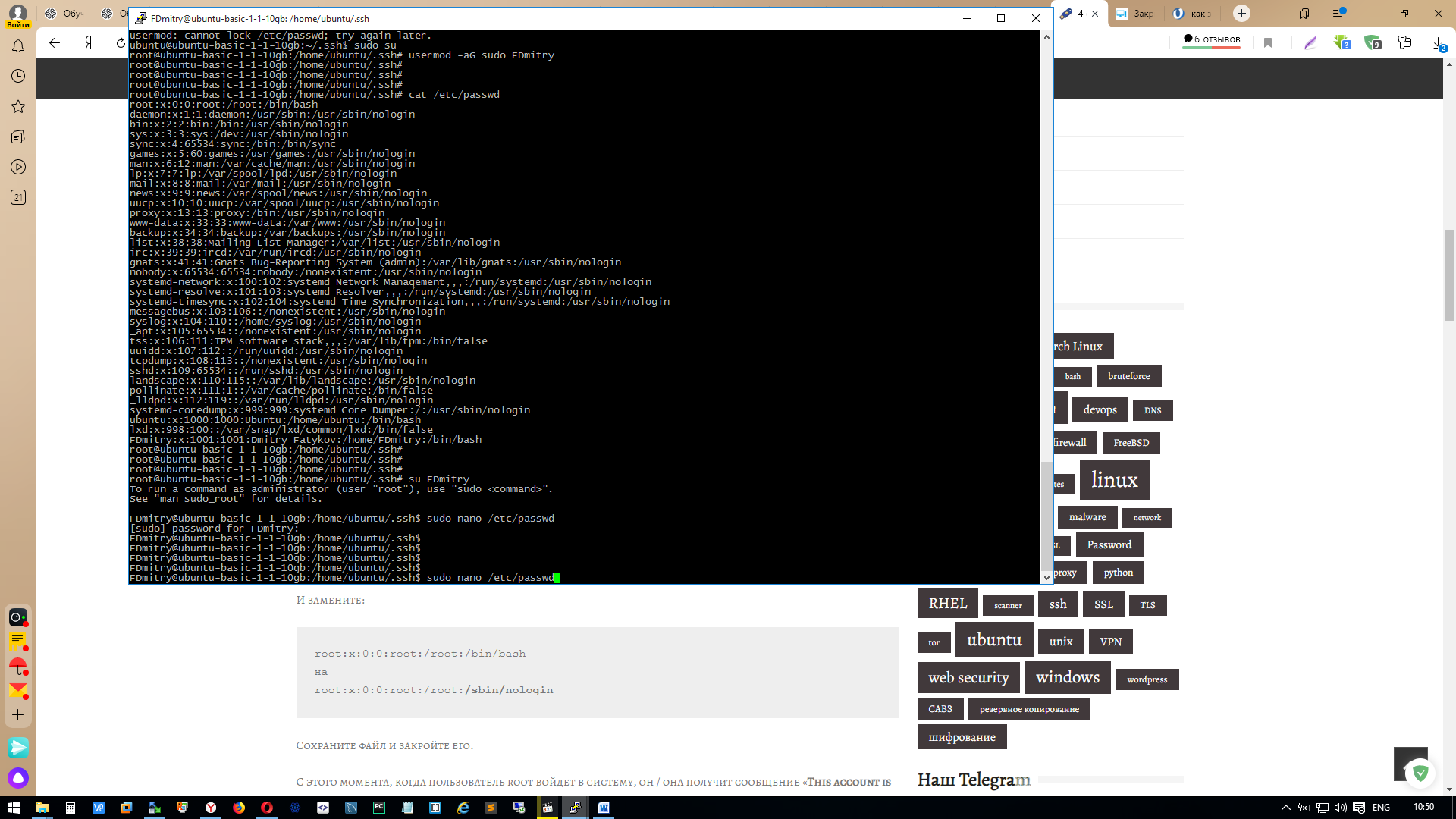
Запрет под логином ROOT

Прежде чем блокировать “root” надо другому пользователю дать Админские права, в моем случае это “FDmitry”

sudo usermod -aG sudo FDmitry

sudo usermod -aG admin FDmitry





Меняем root:x:0:0:root:/root:/bin/bash

На root:x:0:0:root:/root:/sbin/nologin

1. Поставить и настроить fail2ban на блокировку SSH запросов с неверным паролем/ключом. Проверить работу fail2ban

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo apt install fail2ban

Reading package lists... Done

Building dependency tree

Reading state information... Done

fail2ban is already the newest version (0.11.1-1).

0 upgraded, 0 newly installed, 0 to remove and 188 not upgraded.

ubuntu@ubuntu-basic-1-1-10gb:~$

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo vim /etc/fail2ban/jail.d/defaults-debian.conf

[sshd]

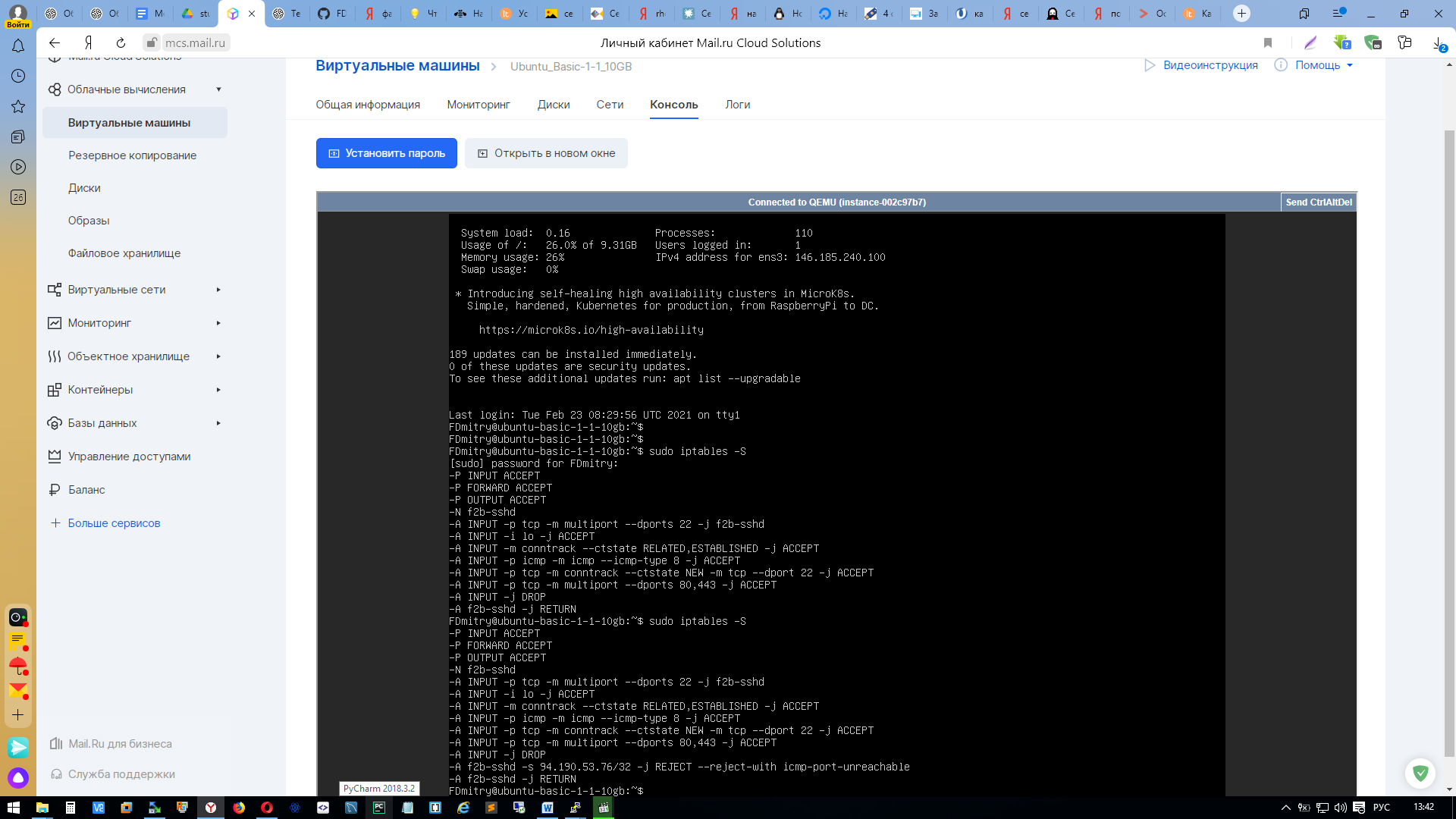
enabled = true

bantime = 30

maxretry = 3

ubuntu@ubuntu-basic-1-1-10gb:~$

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo systemctl restart fail2ban.service



1. \* Установить certbot и получить SSL сертификат для вашего домена

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo snap install core; sudo snap refresh core

core 16-2.48.2.1 from Canonical✓ installed

snap "core" has no updates available

ubuntu@ubuntu-basic-1-1-10gb:~$

ubuntu@ubuntu-basic-1-1-10gb:~$

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo snap install --classic certbot

certbot 1.12.0 from Certbot Project (certbot-eff✓) installed

ubuntu@ubuntu-basic-1-1-10gb:~$

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo certbot --nginx -d fdmitry.tk -d www.fdmitry.tk --register-unsafely-without-email

Saving debug log to /var/log/letsencrypt/letsencrypt.log

Plugins selected: Authenticator nginx, Installer nginx

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Please read the Terms of Service at

https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must

agree in order to register with the ACME server. Do you agree?

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

(Y)es/(N)o: y

Account registered.

Requesting a certificate for fdmitry.tk and www.fdmitry.tk

Performing the following challenges:

http-01 challenge for fdmitry.tk

http-01 challenge for www.fdmitry.tk

Waiting for verification...

Cleaning up challenges

Deploying Certificate to VirtualHost /etc/nginx/sites-enabled/default

Deploying Certificate to VirtualHost /etc/nginx/sites-enabled/default

Redirecting all traffic on port 80 to ssl in /etc/nginx/sites-enabled/default

Redirecting all traffic on port 80 to ssl in /etc/nginx/sites-enabled/default

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Congratulations! You have successfully enabled https://fdmitry.tk and

https://www.fdmitry.tk

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at:

/etc/letsencrypt/live/fdmitry.tk/fullchain.pem

Your key file has been saved at:

/etc/letsencrypt/live/fdmitry.tk/privkey.pem

Your certificate will expire on 2021-05-24. To obtain a new or

tweaked version of this certificate in the future, simply run

certbot again with the "certonly" option. To non-interactively

renew \*all\* of your certificates, run "certbot renew"

- If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate

Donating to EFF: <https://eff.org/donate-le>

ubuntu@ubuntu-basic-1-1-10gb:~$ sudo certbot renew --dry-run

Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Processing /etc/letsencrypt/renewal/fdmitry.tk.conf

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Cert not due for renewal, but simulating renewal for dry run

Plugins selected: Authenticator nginx, Installer nginx

Account registered.

Simulating renewal of an existing certificate for fdmitry.tk and www.fdmitry.tk

Performing the following challenges:

http-01 challenge for fdmitry.tk

http-01 challenge for www.fdmitry.tk

Waiting for verification...

Cleaning up challenges

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

new certificate deployed with reload of nginx server; fullchain is

/etc/letsencrypt/live/fdmitry.tk/fullchain.pem

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Congratulations, all simulated renewals succeeded:

/etc/letsencrypt/live/fdmitry.tk/fullchain.pem (success)

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

5. \* Настроить nginx на редирект запросов с 80 порта на 443 и подключить полученные SSL сертификаты