Отчёт по лабораторной работе №13

Фильтр пакетов

Турсунов Мухамметназар

Содержание

1 Цель работы **5**

2 Выполнение **6**
2.1 Управление брандмауэром с помощью firewall-cmd 6
2.1.1 Добавление порта 2022 (TCP) 10
2.2 Управление брандмауэром с помощью firewall-config (GUI) 11
2.3 Самостоятельная работа 14

3 Контрольные вопросы **16**

4 Заключение **18**

Список иллюстраций

2.1 Определение зоны по умолчанию 6
2.2 Список доступных служб 7
2.3 Сравнение конфигурации зоны 8
2.4 Добавление vnc-server во время выполнения 9
2.5 Постоянное добавление vnc-server 10
2.6 Порт 2022 добавлен 11
2.7 Добавление сервисов GUI 12
2.8 Добавление порта GUI 13
2.9 Изменения применены 14
2.10 Итоговая конфигурация 15

Список таблиц

1 Цель работы

Получить навыки настройки пакетного фильтра в Linux.

2 Выполнение

2.1 Управление брандмауэром с помощью firewall-cmd

1. Сначала были получены права суперпользователя командой **su -**.

2. Для определения зоны брандмауэра, используемой по умолчанию, была выполнена команда `firewall-cmd --get-default-zone`.
   В результате отображена зона **public**.

```
mtursunov@mtursunov:~$ su
Password:
root@mtursunov:/home/mtursunov#
root@mtursunov:/home/mtursunov# firewall-cmd --get-default-zone
public
root@mtursunov:/home/mtursunov# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@mtursunov:/home/mtursunov# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet
audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet
 bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit coll
ectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls d
ocker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4
freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-av
ailability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kde
connect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-cont
roller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kube
let-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve ma
trix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-spe
ed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconso
le ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dh
cp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd
rtsp salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp
 snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris
stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog
syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp war
pinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd w
sdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-tra
pper zabbix-web-service zero-k zerotier
root@mtursunov:/home/mtursunov# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@mtursunov:/home/mtursunov#
```

Рис. 2.1: Определение зоны по умолчанию

3. Затем был получен список доступных зон (`firewall-cmd --get-zones`). Брандмауэр поддерживает несколько зон, среди которых *public, home, work, trusted* и другие.

4. Для просмотра всех доступных системных служб использовалась команда `firewall-cmd --get-services`.

   На экране был выведен длинный перечень известных сервисов.

```
mtursunov@mtursunov:~$ su
Password:
root@mtursunov:/home/mtursunov#
root@mtursunov:/home/mtursunov# firewall-cmd --get-default-zone
public
root@mtursunov:/home/mtursunov# firewall-cmd --get-zones
block dmz drop external home internal nm-shared public trusted work
root@mtursunov:/home/mtursunov# firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-k5-client amqp amqps anno-1602 anno-1800 apcupsd aseqnet
audit ausweisapp2 bacula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet
 bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit coll
ectd condor-collector cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls d
ocker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server factorio finger foreman foreman-proxy freeipa-4
freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-av
ailability http http3 https ident imap imaps iperf2 iperf3 ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin kde
connect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-secure kube-cont
roller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-secure kube-worker kubelet kube
let-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr llmnr-client llmnr-tcp llmnr-udp managesieve ma
trix mdns memcache minecraft minidlna mndp mongodb mosh mountd mpd mqtt mqtt-tls ms-wbt mssql murmur mysql nbd nebula need-for-spe
ed-most-wanted netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut opentelemetry openvpn ovirt-imageio ovirt-storageconso
le ovirt-vmconsole plex pmcd pmproxy pmwebapi pmwebapis pop3 pop3s postgresql privoxy prometheus prometheus-node-exporter proxy-dh
cp ps2link ps3netsrv ptp pulseaudio puppetmaster quassel radius radsec rdp redis redis-sentinel rootd rpc-bind rquotad rsh rsyncd
rtsp salt-master samba samba-client samba-dc sane settlers-history-collection sip sips slimevr slp smtp smtp-submission smtps snmp
 snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid ssdp ssh statsrv steam-lan-transfer steam-streaming stellaris
stronghold-crusader stun stuns submission supertuxkart svdrp svn syncthing syncthing-gui syncthing-relay synergy syscomlan syslog
syslog-tls telnet tentacle terraria tftp tile38 tinc tor-socks transmission-client turn turns upnp-client vdsm vnc-server vrrp war
pinator wbem-http wbem-https wireguard ws-discovery ws-discovery-client ws-discovery-host ws-discovery-tcp ws-discovery-udp wsdd w
sdd-http wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent zabbix-java-gateway zabbix-server zabbix-tra
pper zabbix-web-service zero-k zerotier
root@mtursunov:/home/mtursunov# firewall-cmd --list-services
cockpit dhcpv6-client ssh
root@mtursunov:/home/mtursunov#
```

Рис. 2.2: Список доступных служб

5. Далее был определён список активных служб, разрешённых в текущей зоне (`firewall-cmd --list-services`).

   Отображены службы:

   - cockpit
   - dhcpv6-client
   - ssh

6. Для сравнения выводов была просмотрена конфигурация текущей зоны:

   - `firewall-cmd --list-all`
   - `firewall-cmd --list-all --zone=public`

   Оба вывода совпали, так как текущей зоной стоит **public**.

```
root@mtursunov:/home/mtursunov# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mtursunov:/home/mtursunov# firewall-cmd --list-all --zone=public
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mtursunov:/home/mtursunov#
```

Рис. 2.3: Сравнение конфигурации зоны

7. В конфигурацию была добавлена служба **vnc-server** (временная конфигурация времени выполнения).

8. Повторный вывод конфигурации (`firewall-cmd --list-all`) показал, что vnc-server добавлен.

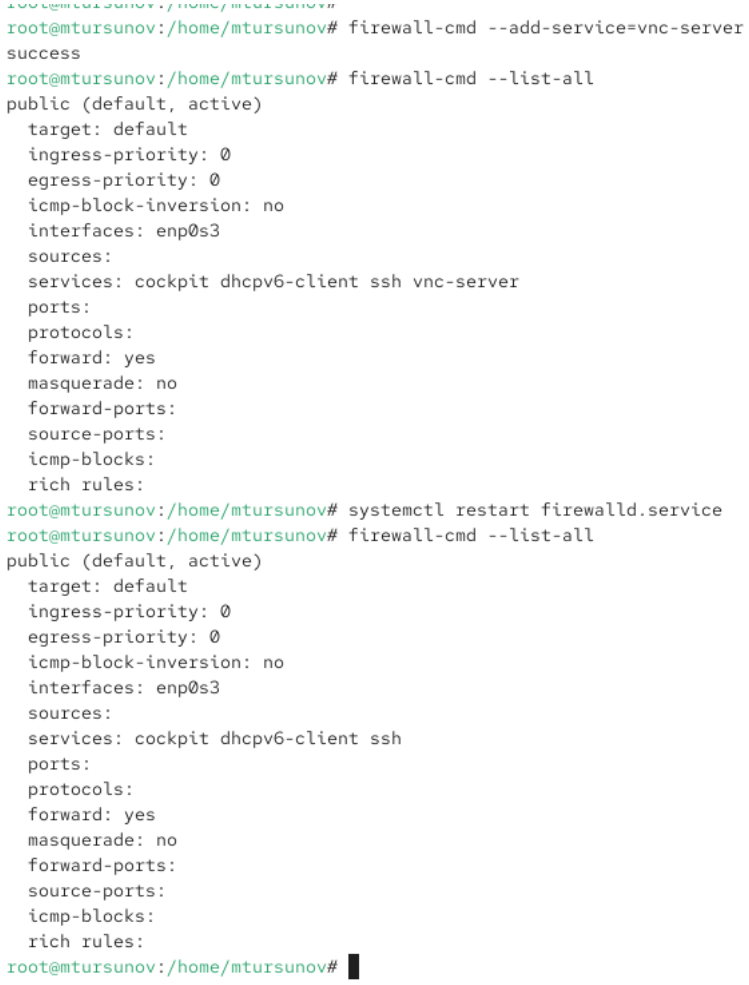

Рис. 2.4: Добавление vnc-server во время выполнения

9. После перезапуска службы firewalld (`systemctl restart firewalld`) служба исчезла из вывода.

10. Это произошло потому, что добавление было выполнено *во время выполнения* (runtime), а не записано в постоянную конфигурацию на диск. После перезапуска runtime-настройки сбрасываются.

11. Затем vnc-server был добавлен как постоянная конфигурация (`--permanent`).

12. Повторный вывод конфигурации пока не показал изменений — постоянные настройки не применяются автоматически.

13. После перезагрузки конфигурации (`firewall-cmd --reload`) vnc-server появился в списке активных.

```
root@mtursunov:/home/mtursunov# firewall-cmd --add-service=vnc-server --permanent
success
root@mtursunov:/home/mtursunov# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mtursunov:/home/mtursunov# firewall-cmd --reload
success
root@mtursunov:/home/mtursunov# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mtursunov:/home/mtursunov#
```

Рис. 2.5: Постоянное добавление vnc-server

2.1.1 Добавление порта 2022 (TCP)

1. В конфигурацию был добавлен порт **2022/tcp** как постоянный.

2. После перезагрузки конфигурации (`firewall-cmd --reload`) порт появился в списке.

```
root@mtursunov:/home/mtursunov#
root@mtursunov:/home/mtursunov# firewall-cmd --add-port=2022/tcp --permanent
success
root@mtursunov:/home/mtursunov# firewall-cmd --reload
success
root@mtursunov:/home/mtursunov# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mtursunov:/home/mtursunov#
```

Рис. 2.6: Порт 2022 добавлен

2.2 Управление брандмауэром с помощью firewall-config (GUI)

1. Была запущена утилита **firewall-config**.
2. В меню *Configuration* выбрано значение **Permanent**, чтобы изменения сохранялись на диск.
3. В зоне **public** были включены службы:
   - http
   - https
   - ftp

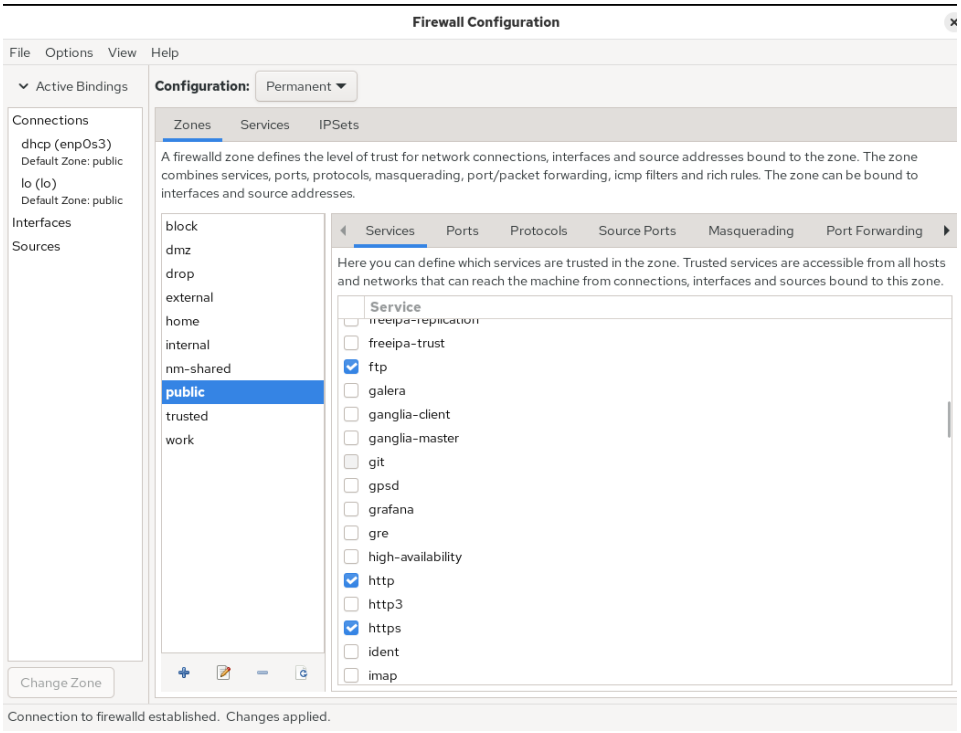

Рис. 2.7: Добавление сервисов GUI

4. На вкладке **Ports** был добавлен порт **2022/udp**.

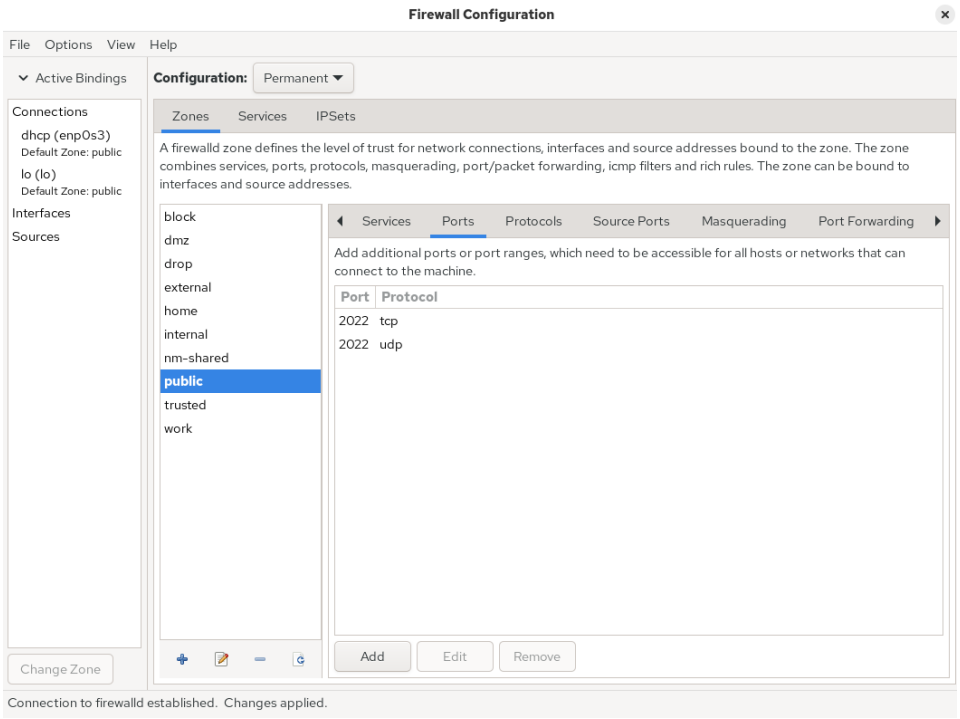

Рис. 2.8: Добавление порта GUI

5. После закрытия интерфейса и проверки в терминале изменения ещё не были применены — они записаны как постоянные.

6. После выполнения `firewall-cmd --reload` изменения вступили в силу.

```
root@mtursunov:/home/mtursunov# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ssh vnc-server
  ports: 2022/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mtursunov:/home/mtursunov# firewall-cmd --reload
success
root@mtursunov:/home/mtursunov# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ftp http https ssh vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mtursunov:/home/mtursunov#
```

Рис. 2.9: Изменения применены

2.3 Самостоятельная работа

1. Служба **telnet** была добавлена в постоянную конфигурацию через командную строку.
2. Службы **imap**, **pop3**, **smtp** были разрешены через GUI firewall-config.
3. После перезагрузки конфигурации firewall все службы присутствуют в списке.

```
root@mtursunov:/home/mtursunov# firewall-cmd --add-service=telnet --permanent
success
root@mtursunov:/home/mtursunov# firewall-cmd --reload
success
root@mtursunov:/home/mtursunov# firewall-cmd --list-all
public (default, active)
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces: enp0s3
  sources:
  services: cockpit dhcpv6-client ftp http https imap pop3 smtp ssh telnet vnc-server
  ports: 2022/tcp 2022/udp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
root@mtursunov:/home/mtursunov#
```

Рис. 2.10: Итоговая конфигурация

3 Контрольные вопросы

1. **Какая служба должна быть запущена перед началом работы с менеджером конфигурации брандмауэра firewall-config?**
   firewalld.service

2. **Какая команда позволяет добавить UDP-порт 2355 в конфигурацию брандмауэра в зоне по умолчанию?**
   firewall-cmd –add-port=2355/udp –permanent

3. **Какая команда позволяет показать всю конфигурацию брандмауэра во всех зонах?**
   firewall-cmd –list-all-zones

4. **Какая команда позволяет удалить службу vnc-server из текущей конфигурации брандмауэра?**
   firewall-cmd –remove-service=vnc-server

5. **Какая команда firewall-cmd позволяет активировать новую конфигурацию, добавленную опцией –permanent?**
   firewall-cmd –reload

6. **Какой параметр firewall-cmd позволяет проверить, что новая конфигурация была добавлена в текущую зону и теперь активна?**
   firewall-cmd –list-all

7. **Какая команда позволяет добавить интерфейс eno1 в зону public?**
   firewall-cmd –zone=public –change-interface=eno1

8. **Если добавить новый интерфейс в конфигурацию брандмауэра, пока не указана зона, в какую зону он будет добавлен?**

   В зону по умолчанию (обычно — public).

4 Заключение

В выполненной работе были освоены основные методы администрирования брандмауэра в Linux с использованием системы **firewalld** и инструмента **firewall-cmd**, а также графического интерфейса **firewall-config**.

Были изучены зоны безопасности, просмотр доступных служб и портов, добавление и удаление сервисов, отличие временной конфигурации (runtime) от постоянной (permanent), а также применение изменений через перезагрузку конфигурации.

Работа позволила на практике понять, как управлять сетевым доступом, открывать и блокировать порты, назначать службы и интерфейсы сетевым зонам, что является важной частью обеспечения безопасности операционной системы.