Алтайский государственный технический университет им. И.И. Ползунова,
г. Барнаул, Россия
Факультет информационных технологий
Кафедра прикладной математики

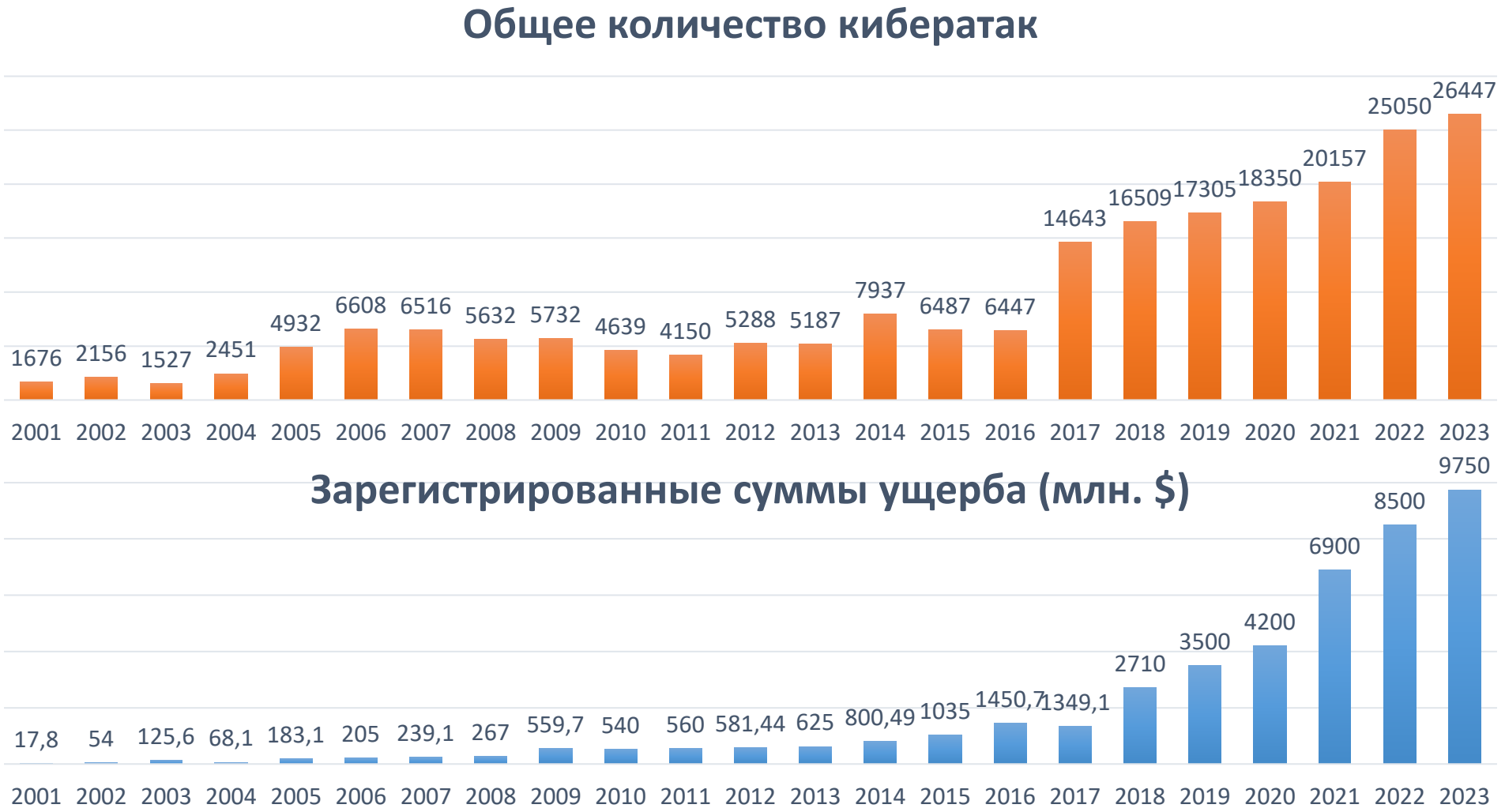
Проектирование и разработка программного комплекса для администрирования и анализа сетевой инфраструктуры на базе оборудования MikroTik

Выполнил: Голиков Е. В. (ПИ-01)

Научный руководитель: Боровцов Е.Г.

Барнаул 2024

Увеличение количества кибератак



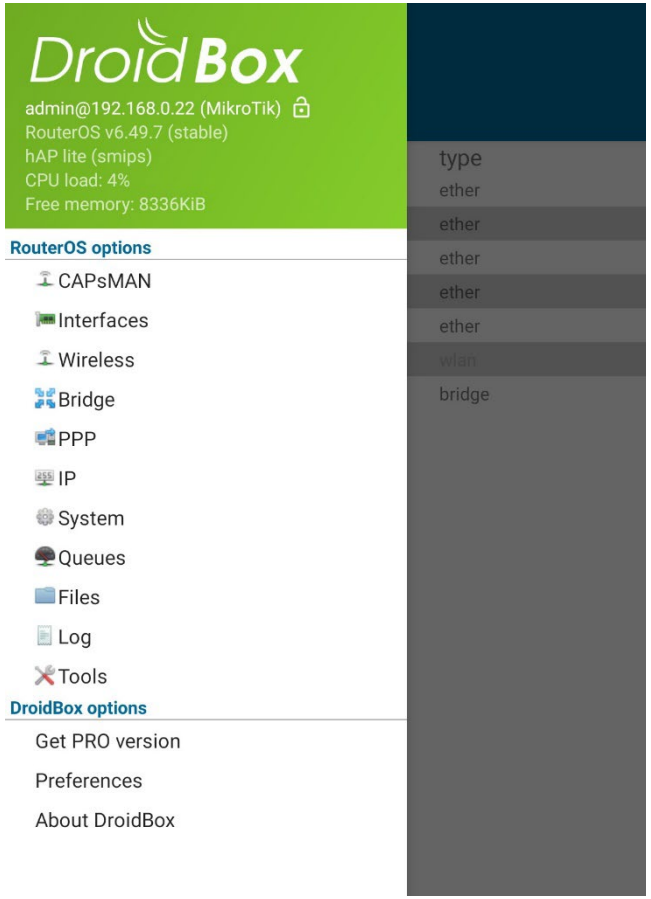
MikroTik и RouterOS

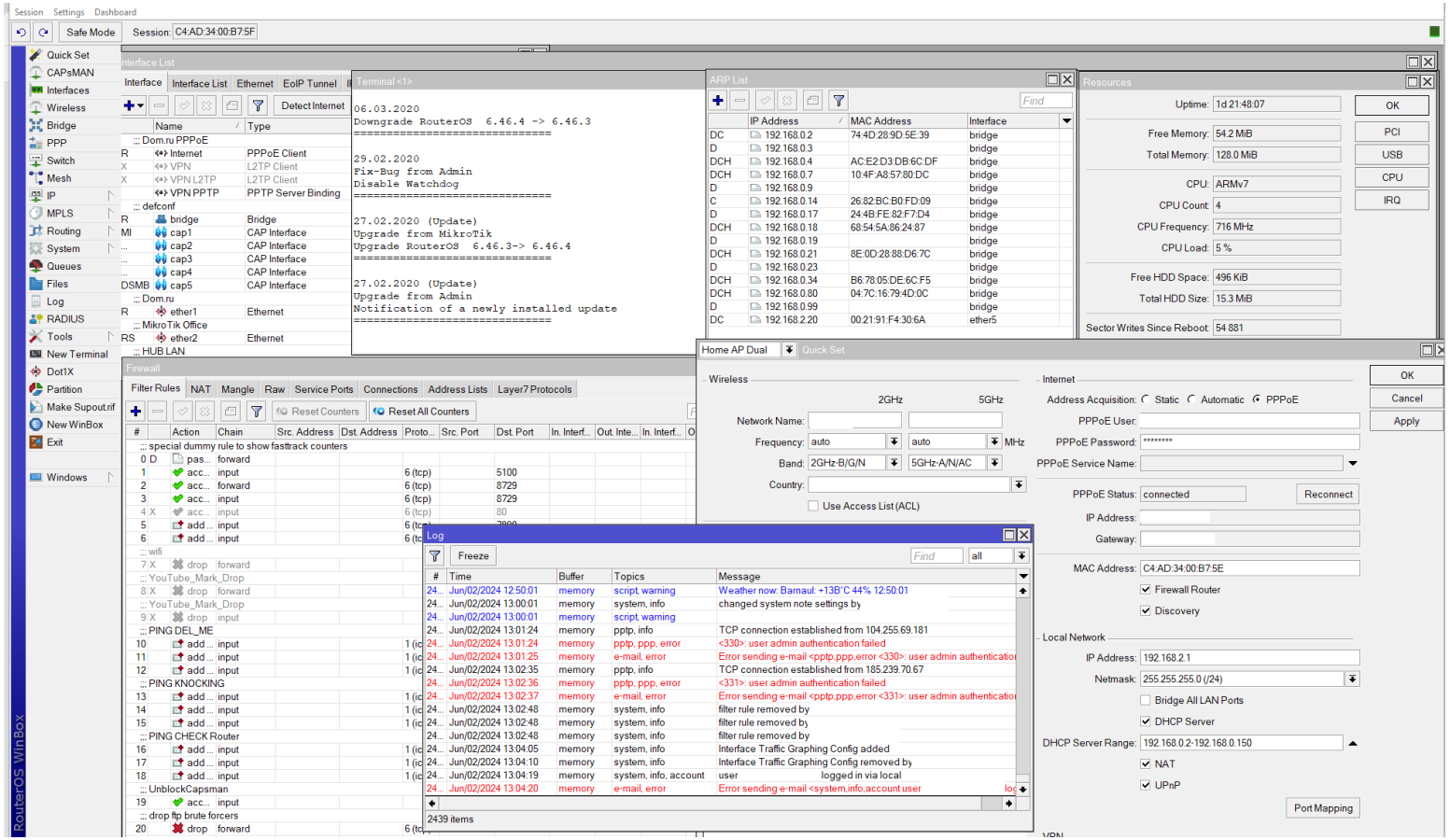
Оборудование MikroTik поставляется с предустановленной операционной системой RouterOS.

Основные достоинства RouterOS:

- Гибко конфигурируемая ОС
- Надежность и стабильная работа
- Высокая производительность
- Широкий спектр функциональности
- Активное сообщество
- Масштабируемость
- Пожизненное обновление ПО
- Хорошая совместимость между версиями

Обзор имеющихся продуктов на рынке





DroidBox

Winbox

Цель и задачи ВКР

Цель: Создание программного комплекса для удаленного анализа используемых ресурсов оборудования и администрирования

Задачи:

- Исследование предметной области
- Выбор средств для разработки
- Разработка интуитивно понятного интерфейса программы
- Опытное внедрение программного продукта

Введение в предметную область

РАБОТА API

Action	Chain	In interface	Protocol
drop	input		
add-src-to-addre...	input	Internet	icmp
add-src-to-addre...	input	Internet	icmp
add-src-to-addre...	input	Internet	icmp
add-src-to-addre...	input	Internet	icmp
add-src-to-addre...	input	Internet	icmp
add-src-to-addre...	input	Internet	icmp

Структура программного комплекса

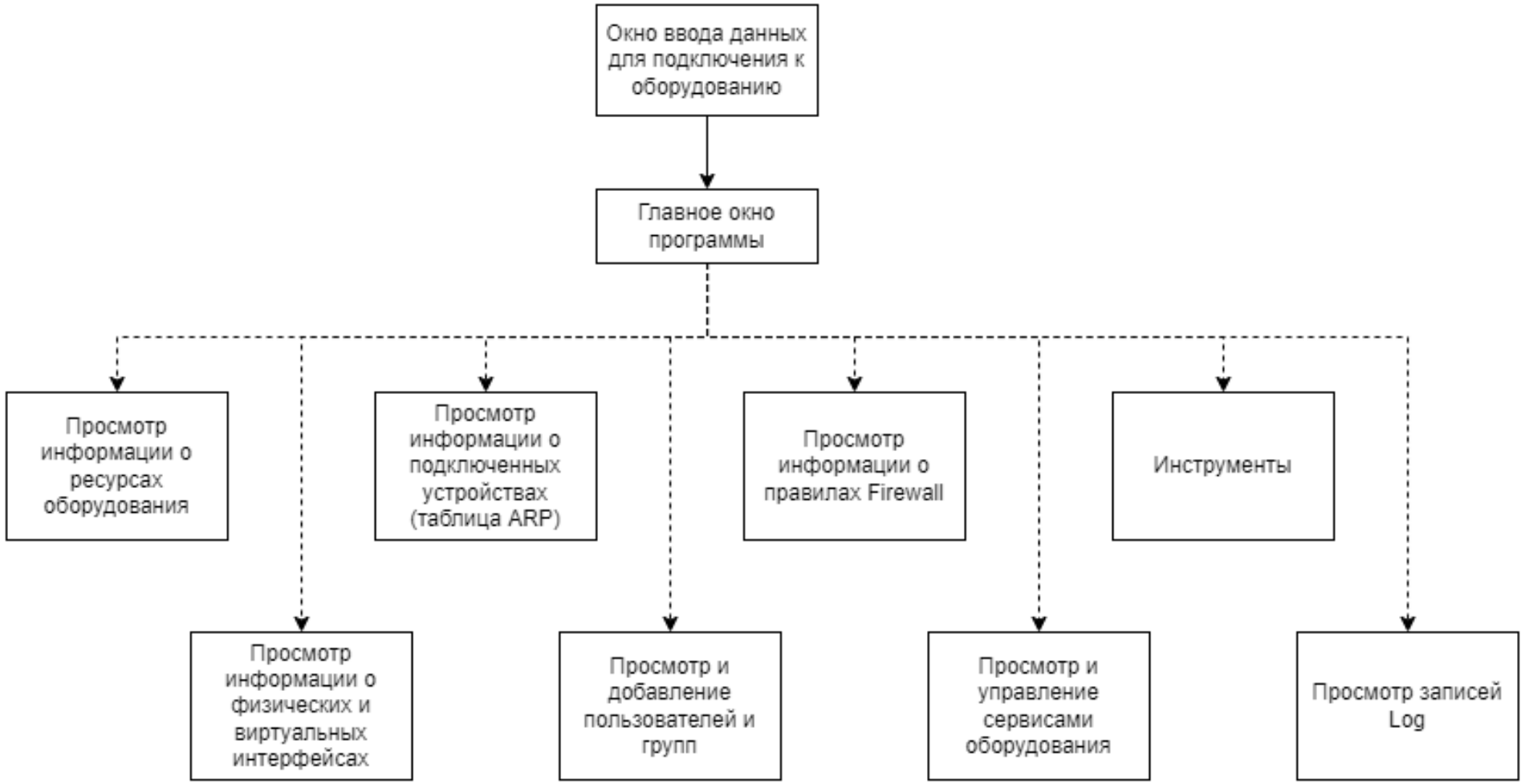
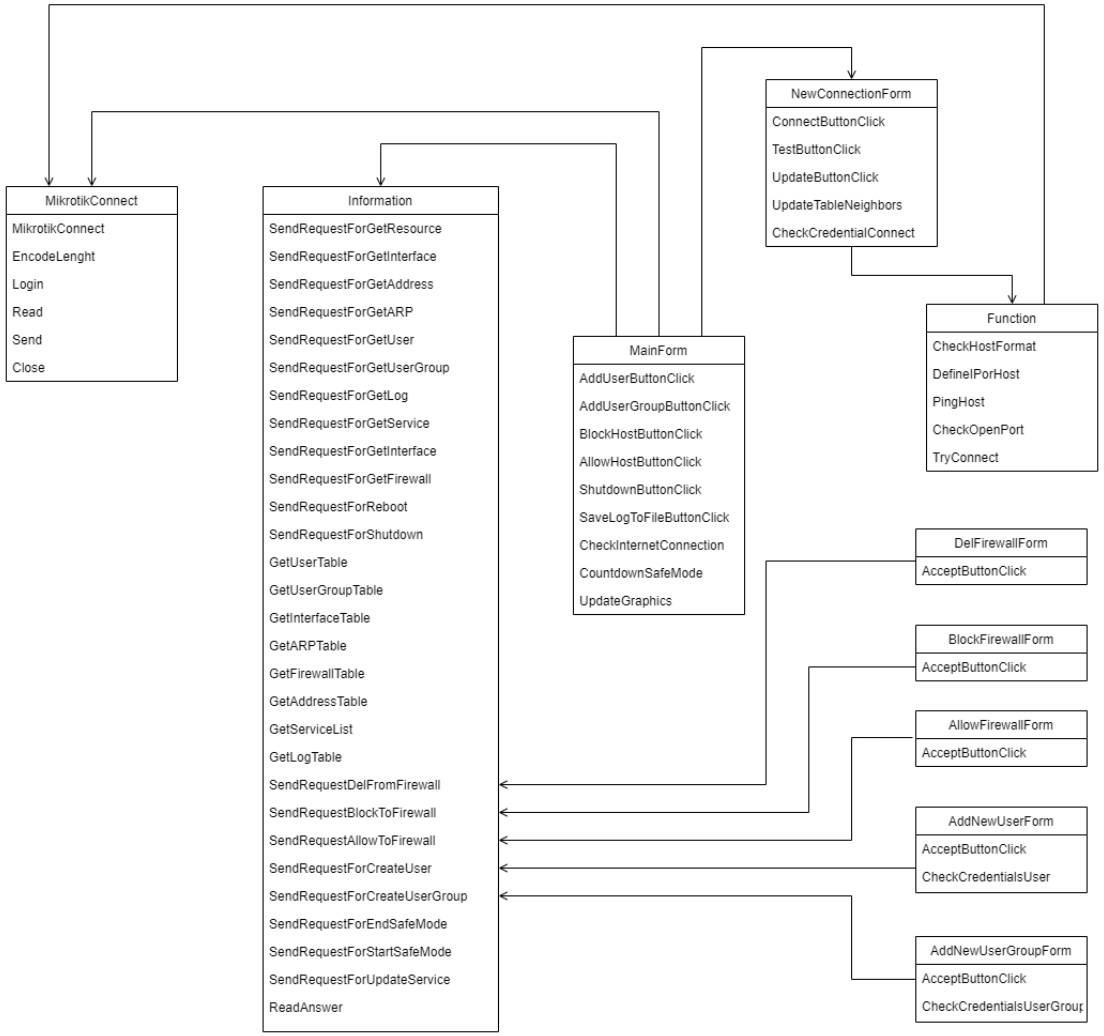
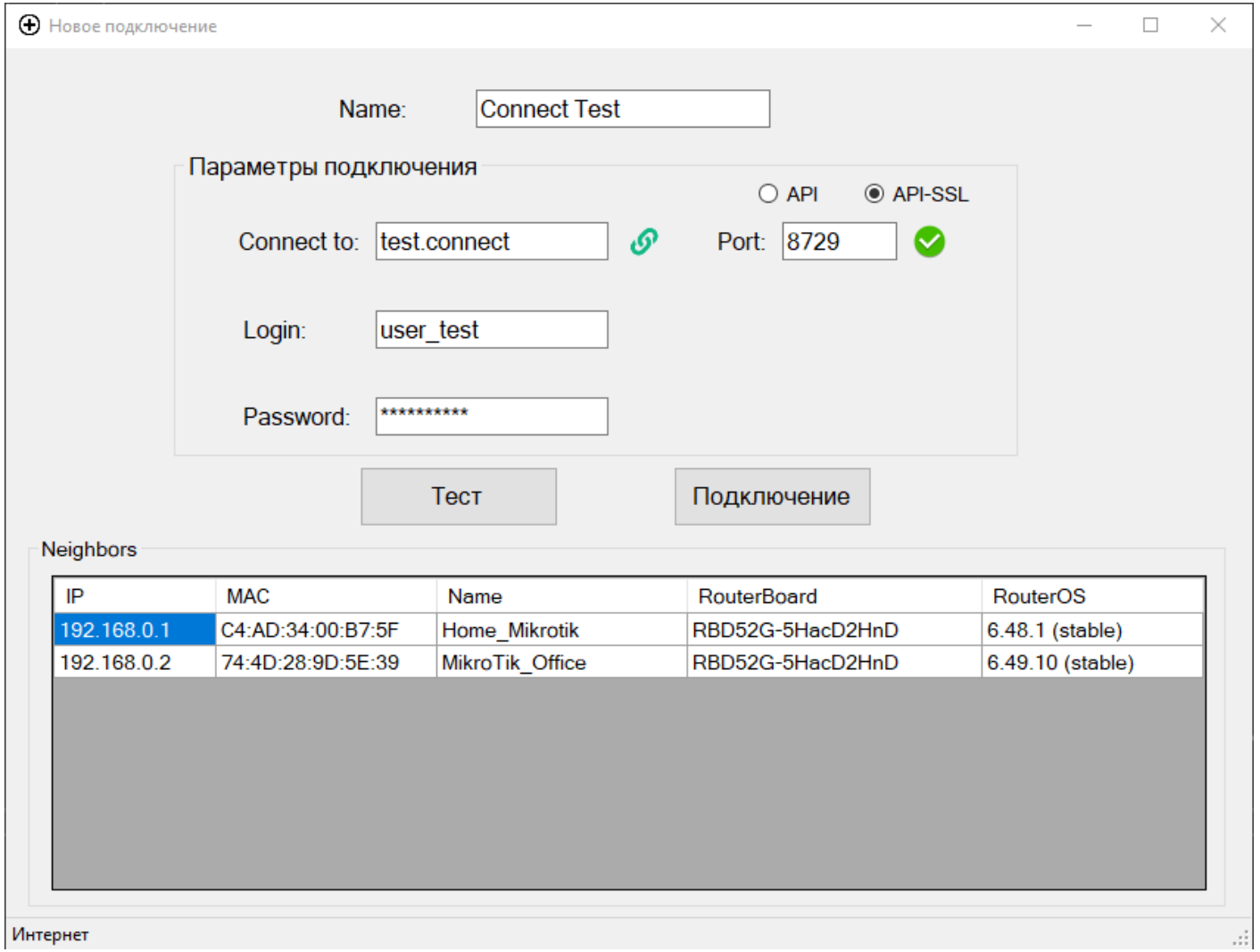


Диаграмма классов

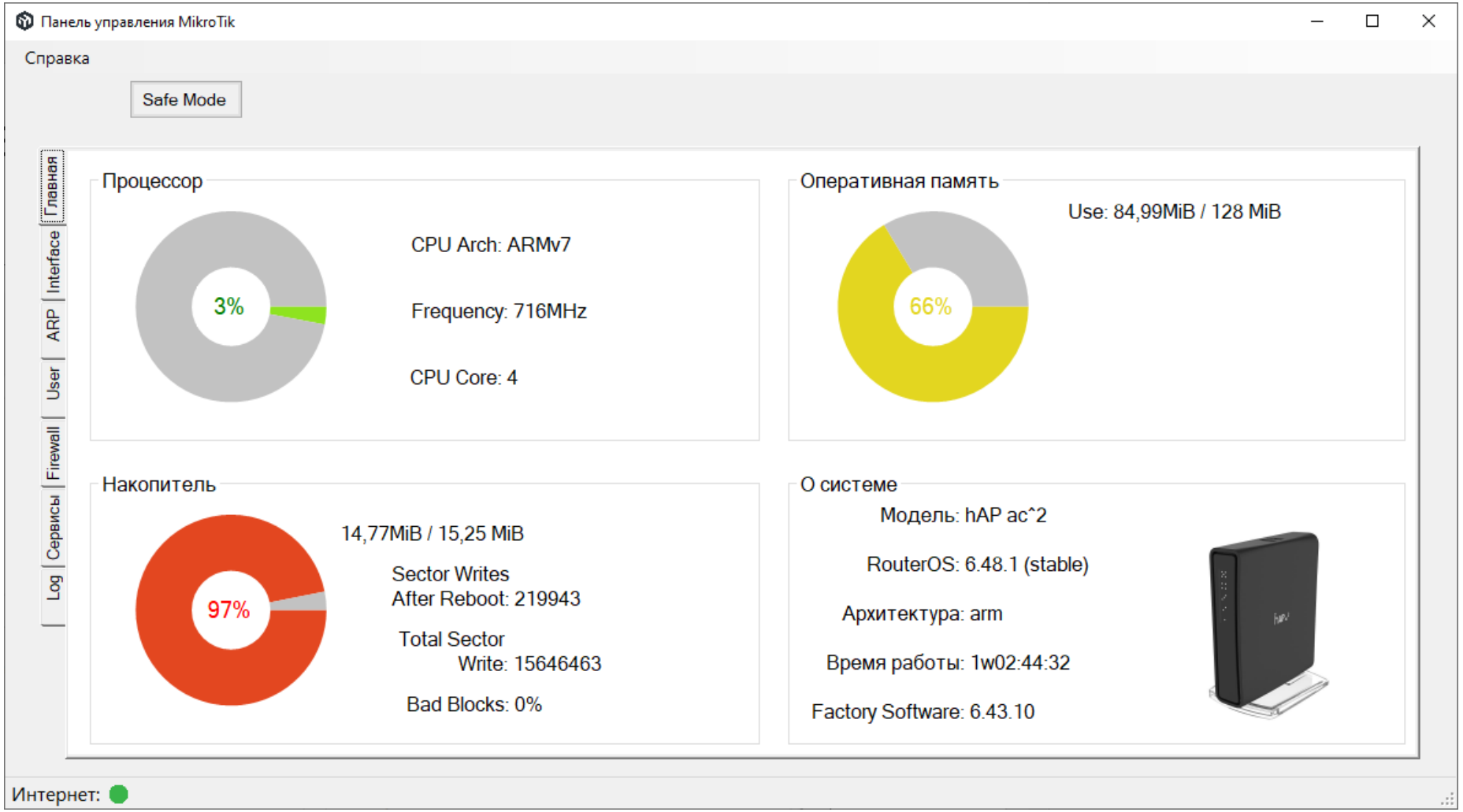


Реализация интерфейса подключения



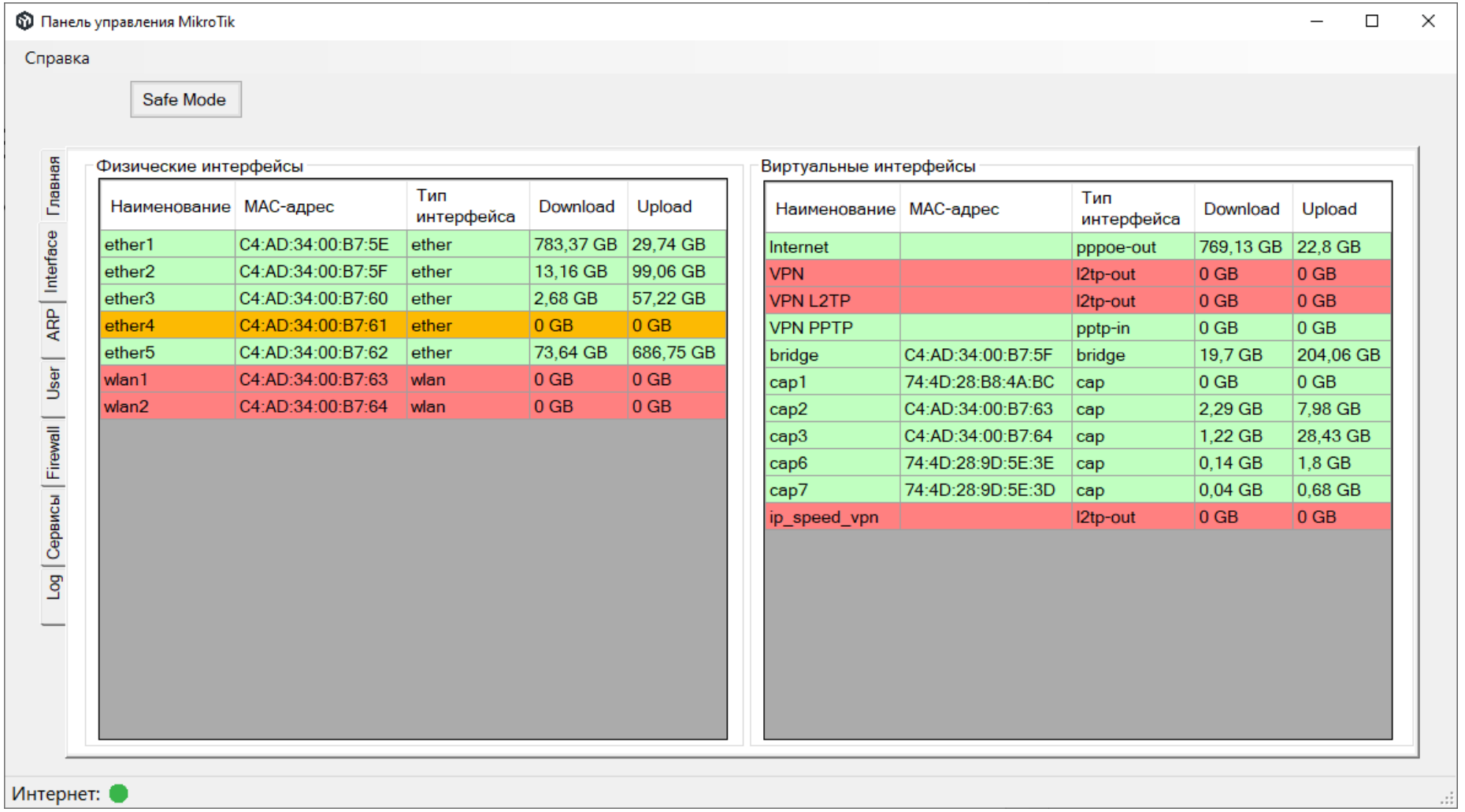
Интерфейс главного окна панели управления:

Анализ использования ресурсов оборудования



Интерфейс главного окна панели управления:

Просмотр списка физических и виртуальных интерфейсов

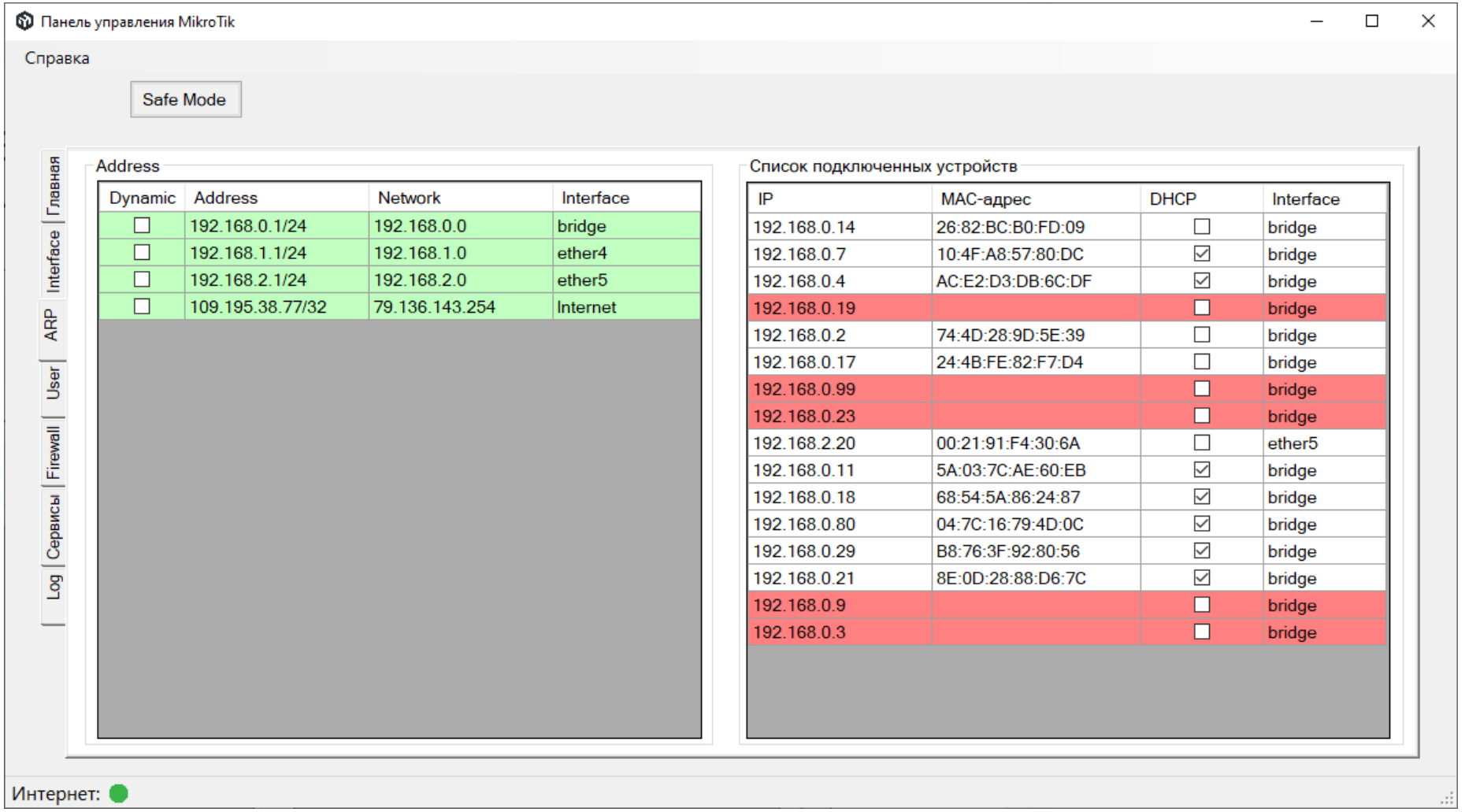


Наименование	MAC-адрес	Тип интерфейса	Download	Upload
ether1	C4:AD:34:00:B7:5E	ether	783,37 GB	29,74 GB
ether2	C4:AD:34:00:B7:5F	ether	13,16 GB	99,06 GB
ether3	C4:AD:34:00:B7:60	ether	2,68 GB	57,22 GB
ether4	C4:AD:34:00:B7:61	ether	0 GB	0 GB
ether5	C4:AD:34:00:B7:62	ether	73,64 GB	686,75 GB
wlan1	C4:AD:34:00:B7:63	wlan	0 GB	0 GB
wlan2	C4:AD:34:00:B7:64	wlan	0 GB	0 GB

Наименование	MAC-адрес	Тип интерфейса	Download	Upload
Internet		pppoe-out	769,13 GB	22,8 GB
VPN		l2tp-out	0 GB	0 GB
VPN L2TP		l2tp-out	0 GB	0 GB
VPN PPTP		pptp-in	0 GB	0 GB
bridge	C4:AD:34:00:B7:5F	bridge	19,7 GB	204,06 GB
cap1	74:4D:28:B8:4A:BC	cap	0 GB	0 GB
cap2	C4:AD:34:00:B7:63	cap	2,29 GB	7,98 GB
cap3	C4:AD:34:00:B7:64	cap	1,22 GB	28,43 GB
cap6	74:4D:28:9D:5E:3E	cap	0,14 GB	1,8 GB
cap7	74:4D:28:9D:5E:3D	cap	0,04 GB	0,68 GB
ip_speed_vpn		l2tp-out	0 GB	0 GB

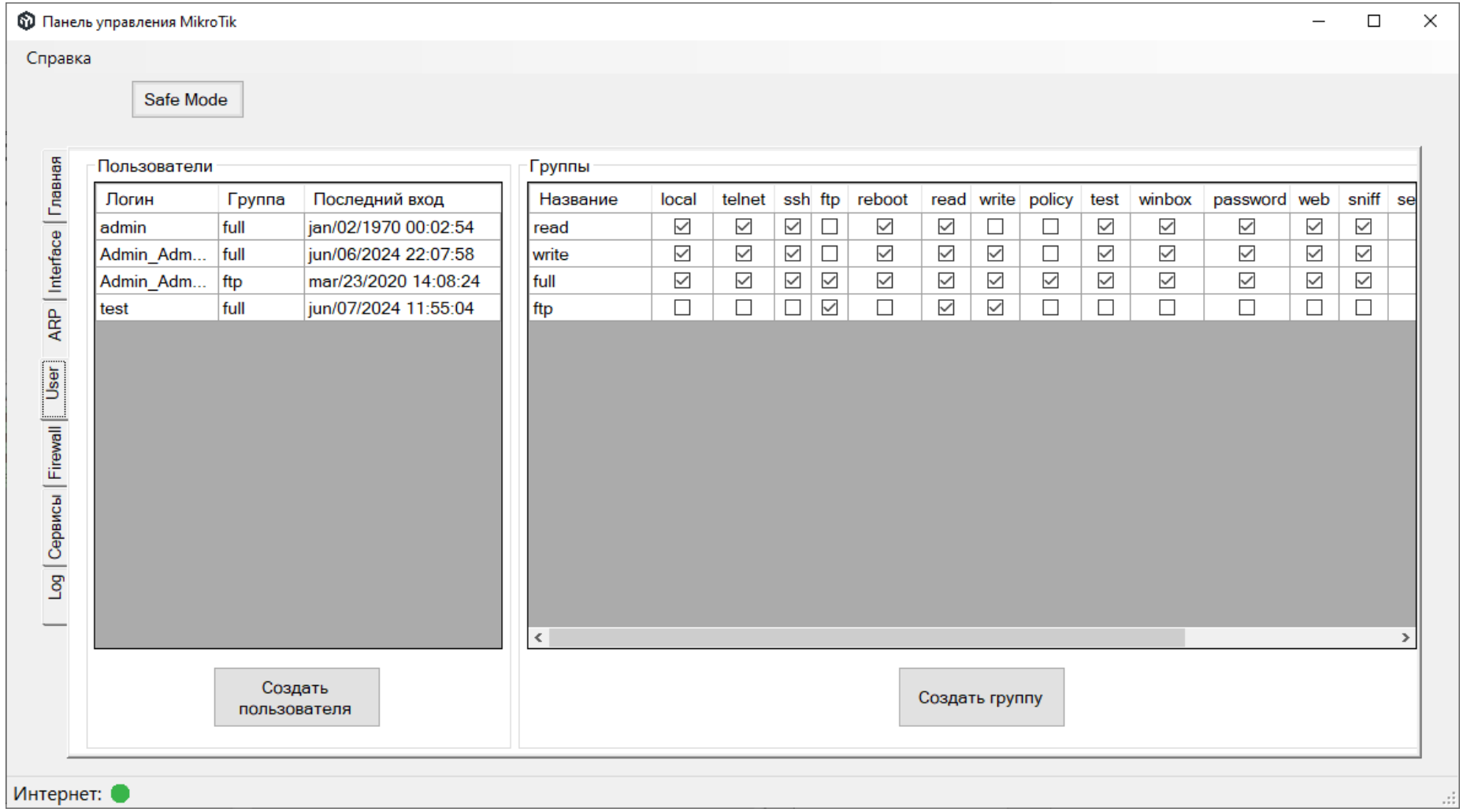
Интерфейс главного окна панели управления

Список активных физических и виртуальных интерфейсов



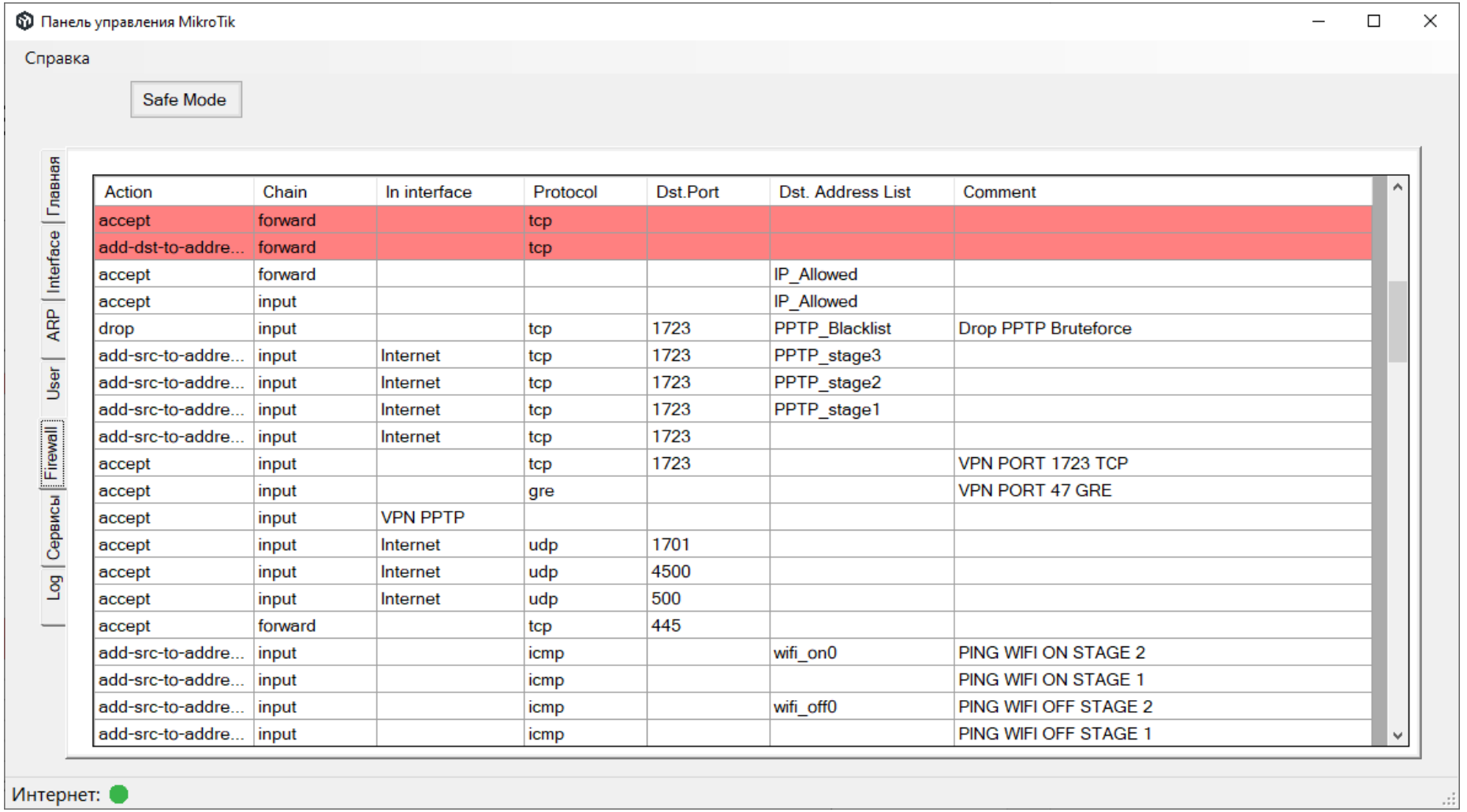
Интерфейс главного окна панели управления

Список пользователей и групп



Интерфейс главного окна панели управления

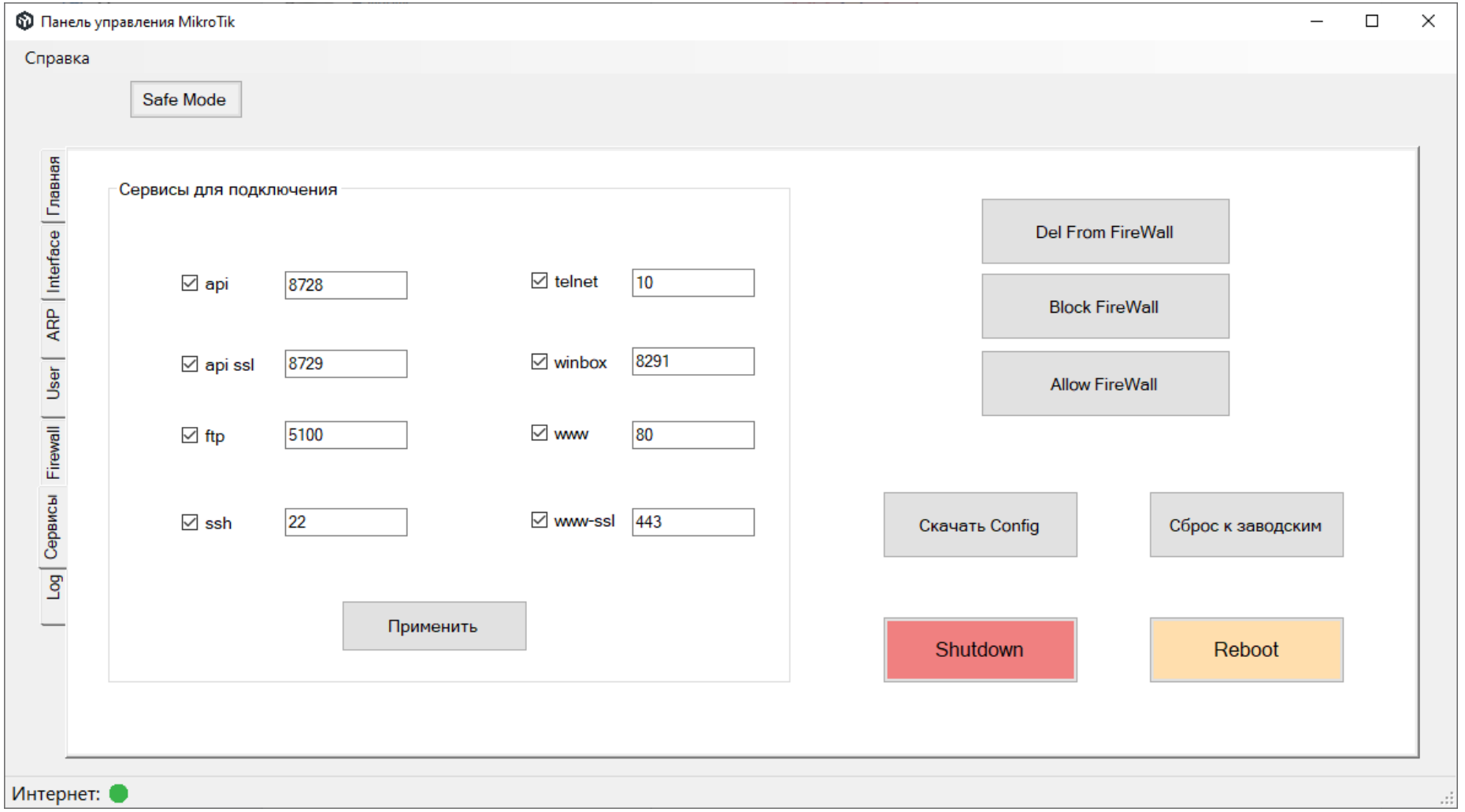
Список правил Firewall



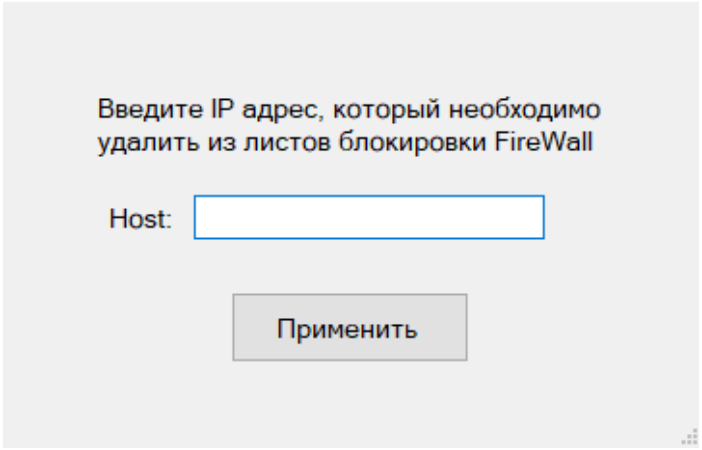
Action	Chain	In interface	Protocol	Dst.Port	Dst. Address List	Comment
accept	forward		tcp			
add-dst-to-addre...	forward		tcp			
accept	forward				IP_Allowed	
accept	input				IP_Allowed	
drop	input		tcp	1723	PPTP_Blacklist	Drop PPTP Bruteforce
add-src-to-addre...	input	Internet	tcp	1723	PPTP_stage3	
add-src-to-addre...	input	Internet	tcp	1723	PPTP_stage2	
add-src-to-addre...	input	Internet	tcp	1723	PPTP_stage1	
add-src-to-addre...	input	Internet	tcp	1723		
accept	input		tcp	1723		VPN PORT 1723 TCP
accept	input		gre			VPN PORT 47 GRE
accept	input	VPN PPTP				
accept	input	Internet	udp	1701		
accept	input	Internet	udp	4500		
accept	input	Internet	udp	500		
accept	forward		tcp	445		
add-src-to-addre...	input		icmp		wifi_on0	PING WIFI ON STAGE 2
add-src-to-addre...	input		icmp			PING WIFI ON STAGE 1
add-src-to-addre...	input		icmp		wifi_off0	PING WIFI OFF STAGE 2
add-src-to-addre...	input		icmp			PING WIFI OFF STAGE 1

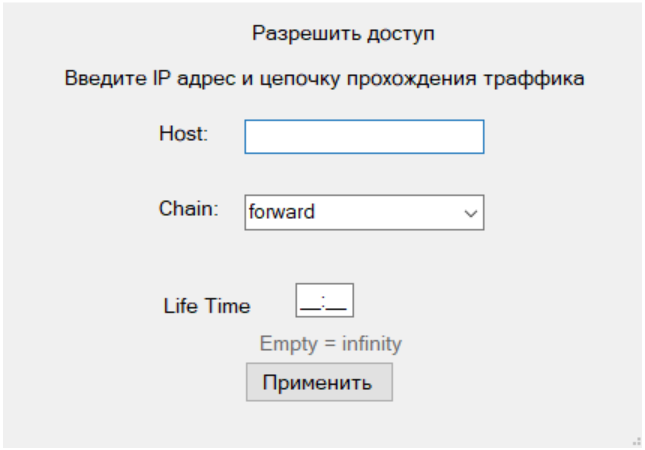
Интерфейс главного окна панели управления:

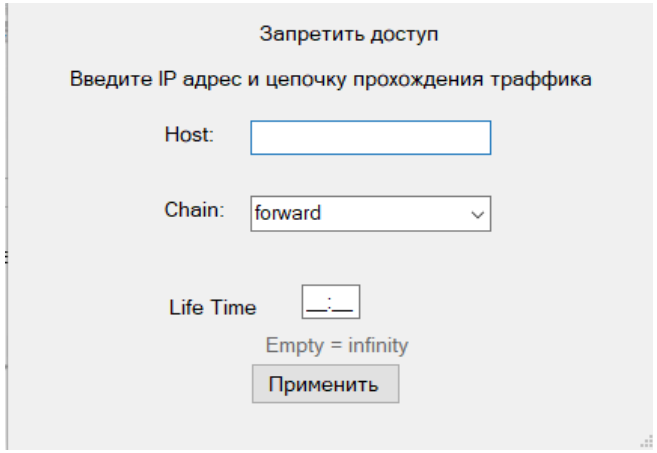
Управление сервисами оборудования и дополнительные инструменты



Инструменты для ручного управления доступом

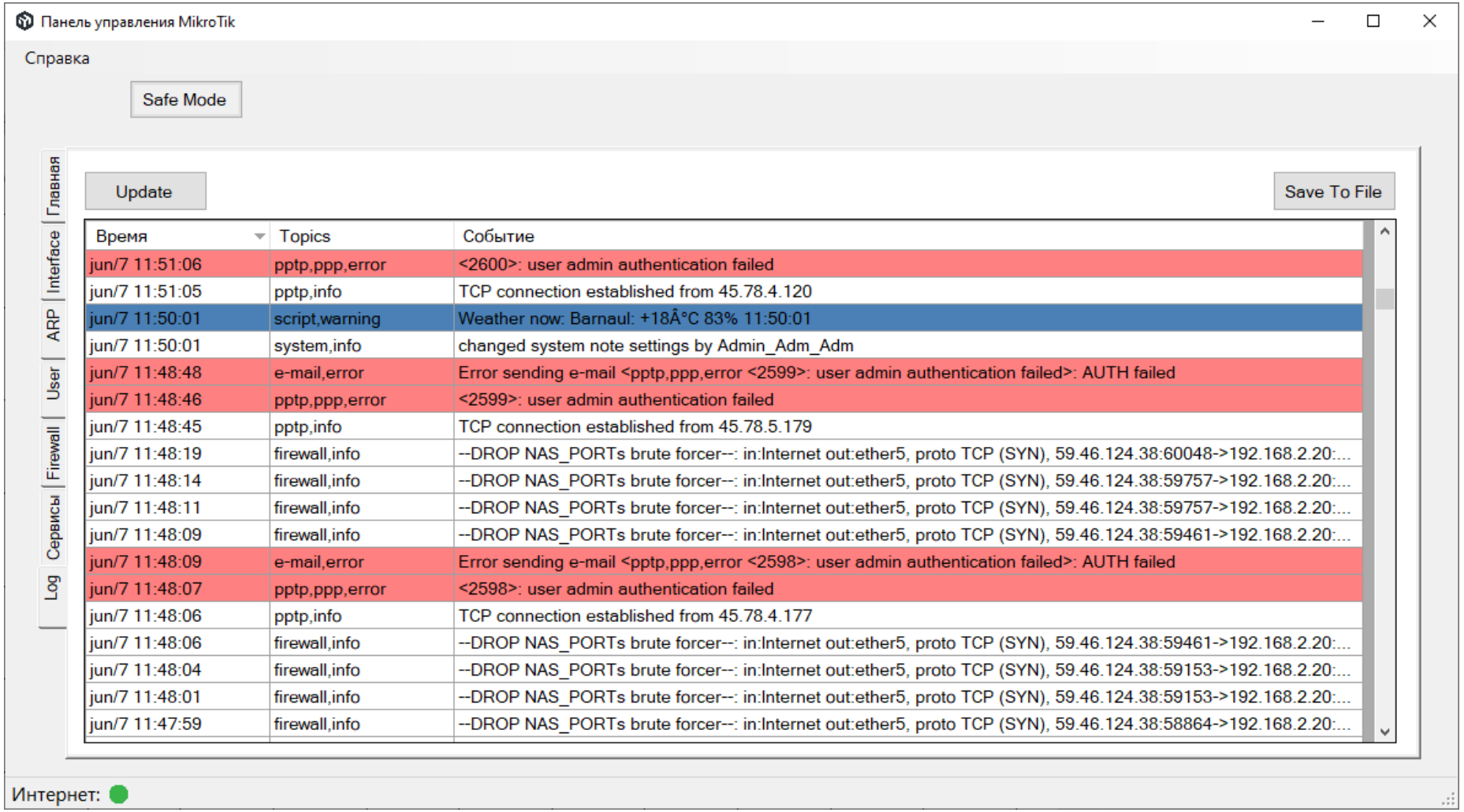






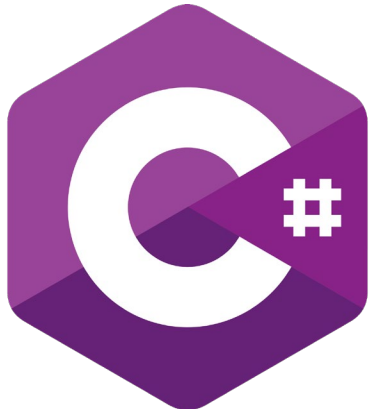
Интерфейс главного окна панели управления:

Просмотр журнала событий (log)



Время	Topics	Событие
jun/7 11:51:06	pptp,ppp,error	<2600>: user admin authentication failed
jun/7 11:51:05	pptp,info	TCP connection established from 45.78.4.120
jun/7 11:50:01	script,warning	Weather now: Barnaul: +18Â°C 83% 11:50:01
jun/7 11:50:01	system,info	changed system note settings by Admin_Adm_Adm
jun/7 11:48:48	e-mail,error	Error sending e-mail <pptp,ppp,error <2599>: user admin authentication failed>: AUTH failed
jun/7 11:48:46	pptp,ppp,error	<2599>: user admin authentication failed
jun/7 11:48:45	pptp,info	TCP connection established from 45.78.5.179
jun/7 11:48:19	firewall,info	--DROP NAS_PORTs brute forcer--: in:Internet out:ether5, proto TCP (SYN), 59.46.124.38:60048->192.168.2.20:...
jun/7 11:48:14	firewall,info	--DROP NAS_PORTs brute forcer--: in:Internet out:ether5, proto TCP (SYN), 59.46.124.38:59757->192.168.2.20:...
jun/7 11:48:11	firewall,info	--DROP NAS_PORTs brute forcer--: in:Internet out:ether5, proto TCP (SYN), 59.46.124.38:59757->192.168.2.20:...
jun/7 11:48:09	firewall,info	--DROP NAS_PORTs brute forcer--: in:Internet out:ether5, proto TCP (SYN), 59.46.124.38:59461->192.168.2.20:...
jun/7 11:48:09	e-mail,error	Error sending e-mail <pptp,ppp,error <2598>: user admin authentication failed>: AUTH failed
jun/7 11:48:07	pptp,ppp,error	<2598>: user admin authentication failed
jun/7 11:48:06	pptp,info	TCP connection established from 45.78.4.177
jun/7 11:48:06	firewall,info	--DROP NAS_PORTs brute forcer--: in:Internet out:ether5, proto TCP (SYN), 59.46.124.38:59461->192.168.2.20:...
jun/7 11:48:04	firewall,info	--DROP NAS_PORTs brute forcer--: in:Internet out:ether5, proto TCP (SYN), 59.46.124.38:59153->192.168.2.20:...
jun/7 11:48:01	firewall,info	--DROP NAS_PORTs brute forcer--: in:Internet out:ether5, proto TCP (SYN), 59.46.124.38:59153->192.168.2.20:...
jun/7 11:47:59	firewall,info	--DROP NAS_PORTs brute forcer--: in:Internet out:ether5, proto TCP (SYN), 59.46.124.38:58864->192.168.2.20:...

Стек технологий



Внедрение

Программный продукт

успешно внедрен в опытную эксплуатацию.

Общество с ограниченной ответственностью
«ВОСТОК»

ИНН/КПП 2221181920/222101001 р/с 40702810902140038335 в Отделении №8644 ПАО Сбербанка г. Барнаул
ОГРН 1102225011811 656011, Алтайский край, г. Барнаул, пр. Калинина, 15в

АКТ
О ВНЕДРЕНИИ РЕЗУЛЬТАТОВ КВАЛИФИКАЦИОНОЙ РАБОТЫ

Настоящим подтверждаю, что результаты выпускной квалификационной работы студента АлтГТУ им. И.И. Ползунова группы ПИ-01 очной формы обучения Голикова Е.В. на тему “Проектирование и разработка программного комплекса для администрирования и анализа сетевой инфраструктуры на базе оборудования MikroTik” обладают актуальностью, представляют практический интерес и были использованы в компании для удаленного управления оборудованием MikroTik

В процессе первичного тестирования и использования установлено, что предложенное решение обеспечивает надежное и безопасное подключение к оборудованию MikroTik с целью дальнейшего анализа ресурсов и администрирования оборудования.

Директор Дубинский А.В.

М.П.

Алтайский государственный технический университет им. И.И. Ползунова,
г. Барнаул, Россия
Факультет информационных технологий
Кафедра прикладной математики

Проектирование и разработка программного комплекса для администрирования и анализа сетевой инфраструктуры на базе оборудования MikroTik

Выполнил: Голиков Е. В. (ПИ-01)

Научный руководитель: Боровцов Е.Г.

Барнаул 2024