

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

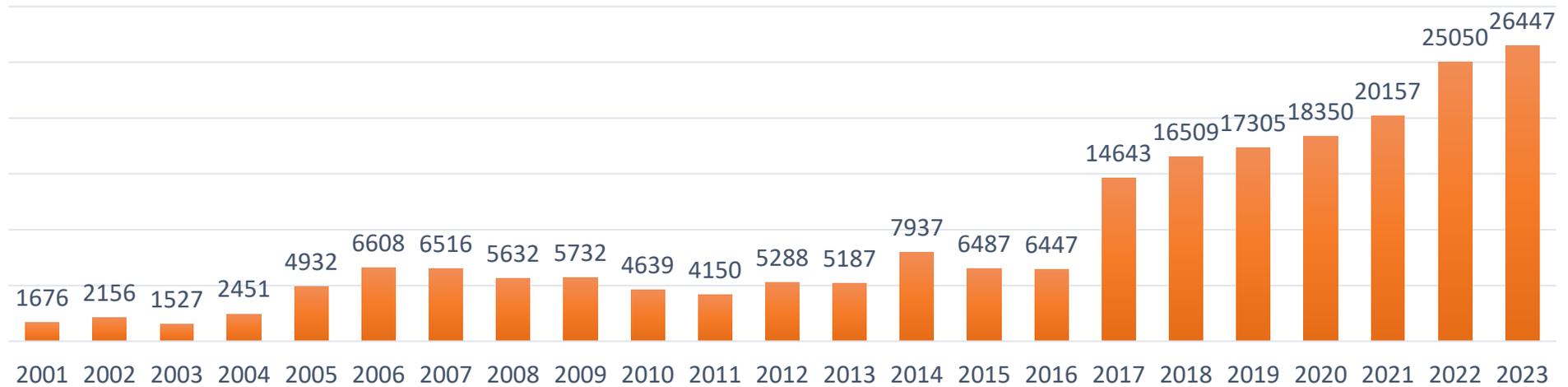
Выполнил: Голиков Е. В. (ПИ-01)

Научный руководитель: Боровцов Е.Г.

Барнаул 2024

Увеличение количества кибератак

Общее количество кибератак



Зарегистрированные суммы ущерба (млн. \$)



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

admin@192.168.0.22 (MikroTik)

RouterOS v6.49.7 (stable)

hAP lite (smips)

CPU load: 4%

Free memory: 8336KiB

- RouterOS options
 - CAPsMAN
 - Interfaces
 - Wireless
 - Bridge
 - PPP
 - IP
 - System
 - Queues
 - Files
 - Log
 - Tools
- DroidBox options
 - Get PRO version
 - Preferences
 - About DroidBox

type

ether

ether

ether

ether

ether

ether

bridge

The screenshot displays the WinBox interface for RouterOS. The main window is divided into several panes:

- Interface List:** Shows a table of network interfaces with columns for Name, Type, and Status. It lists interfaces like eth1, eth2, and HUB LAN.
- Terminal:** Displays system logs and messages, including updates and network events.
- ARP List:** Shows a table of IP addresses and their corresponding MAC addresses.
- Resources:** Displays system statistics such as Uptime (1d 21:48:07), Free Memory (54.2 MB), Total Memory (128.0 MB), CPU (ARMv7), CPU Frequency (716 MHz), CPU Load (5%), Free HDD Space (496 KiB), and Total HDD Size (15.3 MB).
- Firewall:** Shows a table of firewall rules with columns for Action, Chain, Src Address, Dst Address, Proto, Src Port, Dst Port, In. Interf., and Out. Interf.
- Log:** A detailed log window showing system events, errors, and messages with columns for Time, Buffer, Topics, and Message.
- Configuration Panels:** On the right, there are configuration panels for Wireless (Network Name, Frequency, Band, Country) and Internet (Address Acquisition, PPPoE User/Password, Service Name, Status, IP Address, Gateway, MAC Address, Local Network, DHCP Server Range, NAT, UPnP).

DroidBox

Winbox

Цель и задачи ВКР

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

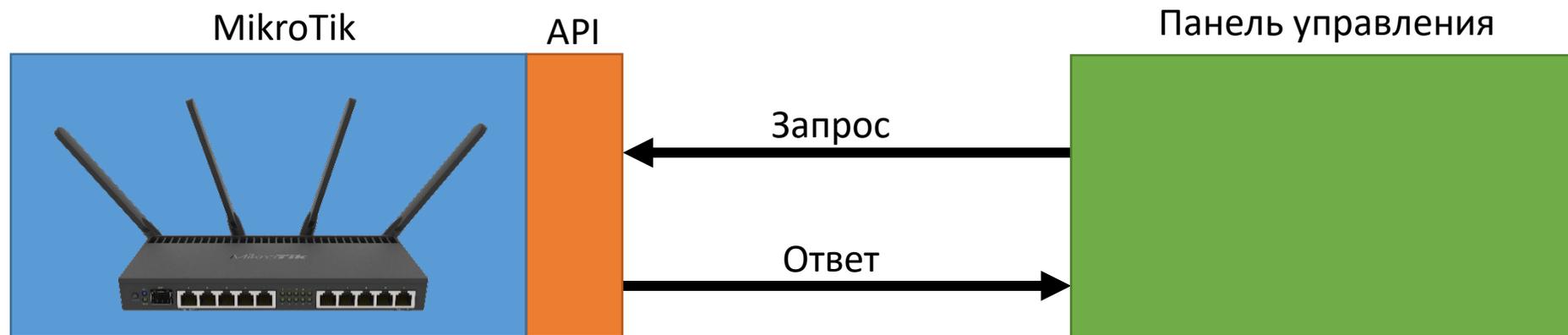
Задачи:

- 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

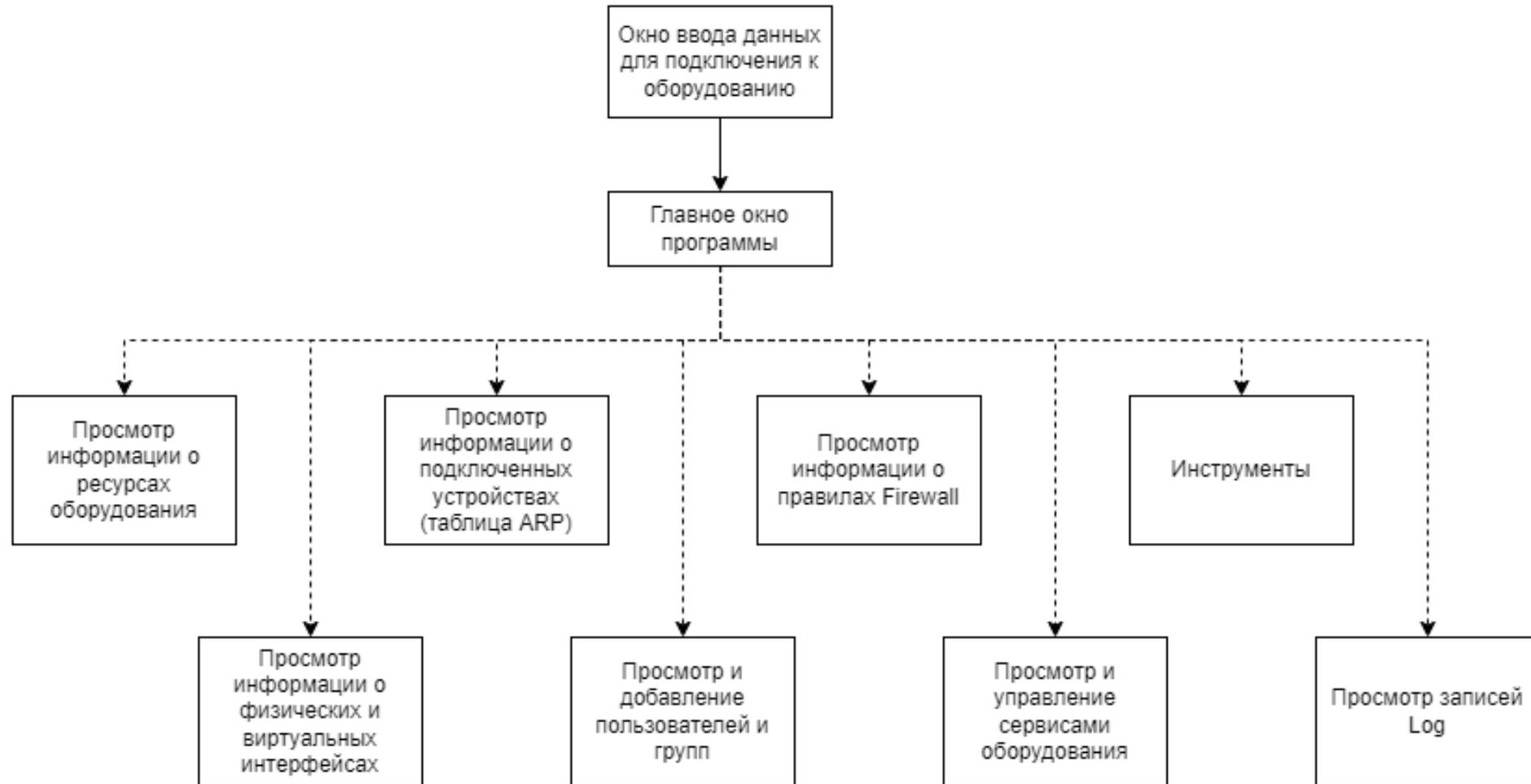
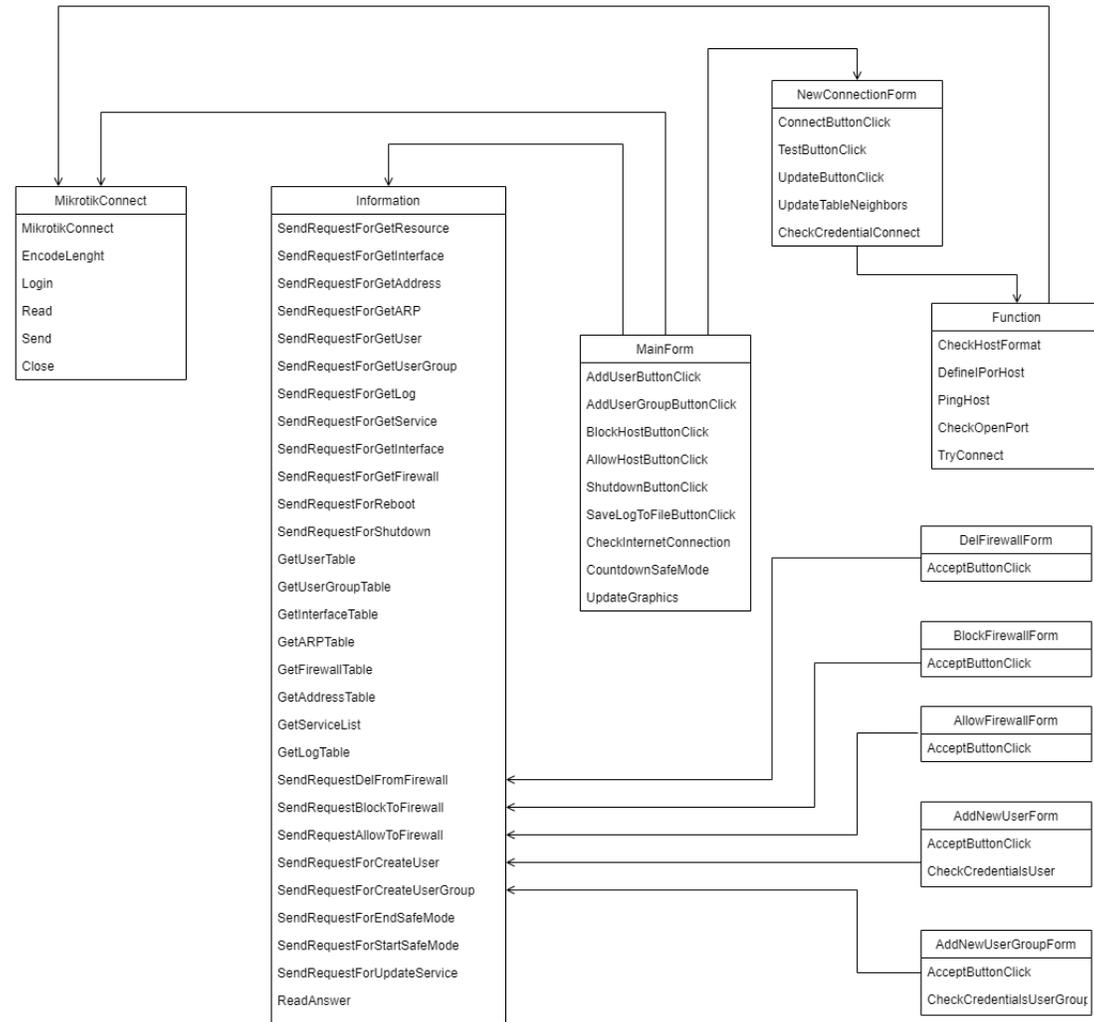


Диаграмма классов



Реализация интерфейса подключения

Новое подключение

Name:

Параметры подключения

API API-SSL

Connect to:  Port: 

Login:

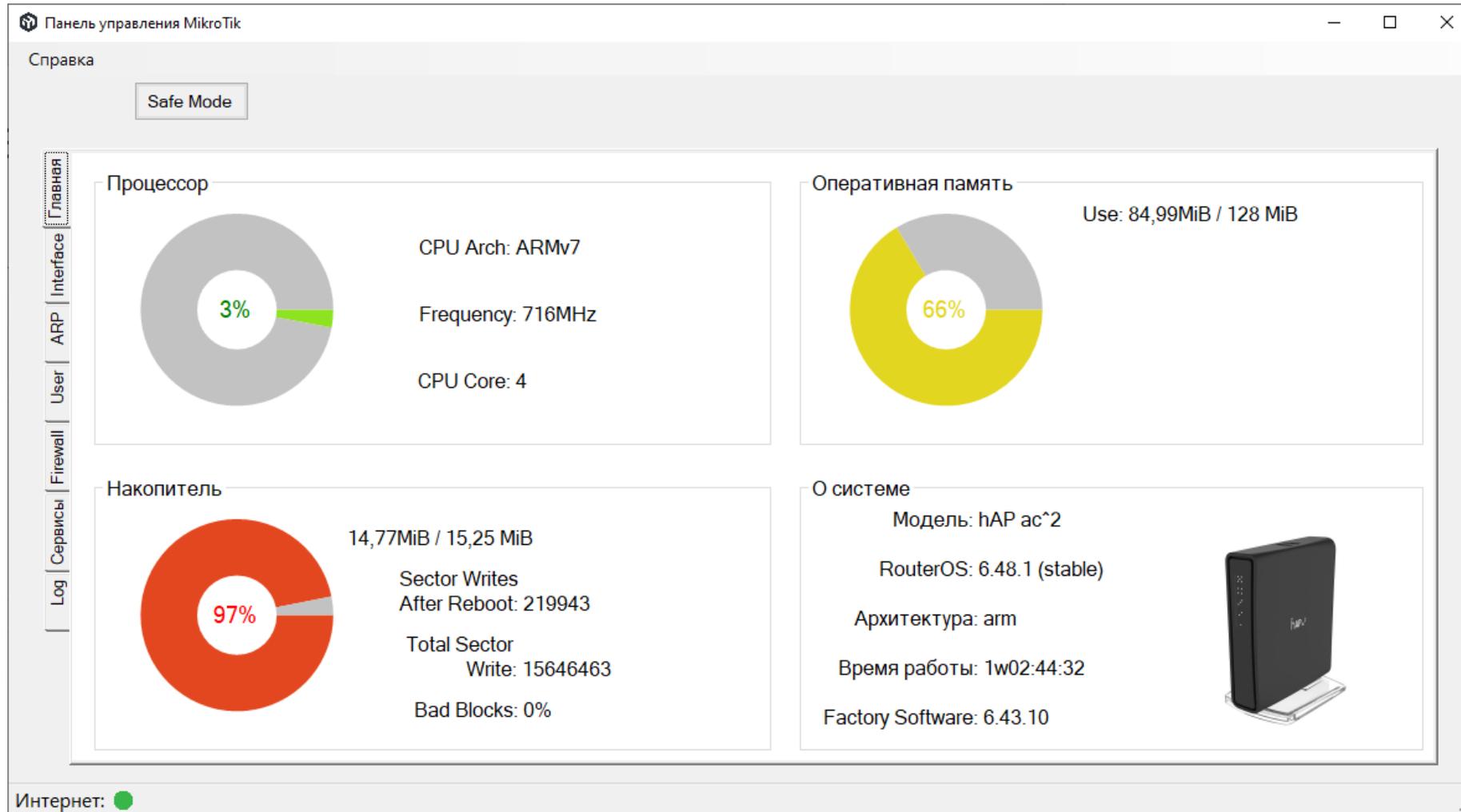
Password:

Neighbors

IP	MAC	Name	RouterBoard	RouterOS
192.168.0.1	C4:AD:34:00:B7:5F	Home_Mikrotik	RBD52G-5HacD2HnD	6.48.1 (stable)
192.168.0.2	74:4D:28:9D:5E:39	MikroTik_Office	RBD52G-5HacD2HnD	6.49.10 (stable)

Интернет

Интерфейс главного окна панели управления: Анализ использования ресурсов оборудования



Интерфейс главного окна панели управления: Просмотр списка физических и виртуальных интерфейсов

Панель управления MikroTik

Справка

Safe Mode

Главная | Interface | ARP | User | Firewall | Сервисы | Log

Физические интерфейсы

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

Виртуальные интерфейсы

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

Интернет: ●

Интерфейс главного окна панели управления

Список активных физических и виртуальных интерфейсов

Панель управления MikroTik

Справка

Safe Mode

Главная | Interface | ARP | User | Firewall | Сервисы | Log

Address

Dynamic	Address	Network	Interface
<input type="checkbox"/>	192.168.0.1/24	192.168.0.0	bridge
<input type="checkbox"/>	192.168.1.1/24	192.168.1.0	ether4
<input type="checkbox"/>	192.168.2.1/24	192.168.2.0	ether5
<input type="checkbox"/>	109.195.38.77/32	79.136.143.254	Internet

Список подключенных устройств

IP	MAC-адрес	DHCP	Interface
192.168.0.14	26:82:BC:B0:FD:09	<input type="checkbox"/>	bridge
192.168.0.7	10:4F:A8:57:80:DC	<input checked="" type="checkbox"/>	bridge
192.168.0.4	AC:E2:D3:DB:6C:DF	<input checked="" type="checkbox"/>	bridge
192.168.0.19		<input type="checkbox"/>	bridge
192.168.0.2	74:4D:28:9D:5E:39	<input type="checkbox"/>	bridge
192.168.0.17	24:4B:FE:82:F7:D4	<input type="checkbox"/>	bridge
192.168.0.99		<input type="checkbox"/>	bridge
192.168.0.23		<input type="checkbox"/>	bridge
192.168.2.20	00:21:91:F4:30:6A	<input type="checkbox"/>	ether5
192.168.0.11	5A:03:7C:AE:60:EB	<input checked="" type="checkbox"/>	bridge
192.168.0.18	68:54:5A:86:24:87	<input checked="" type="checkbox"/>	bridge
192.168.0.80	04:7C:16:79:4D:0C	<input checked="" type="checkbox"/>	bridge
192.168.0.29	B8:76:3F:92:80:56	<input checked="" type="checkbox"/>	bridge
192.168.0.21	8E:0D:28:88:D6:7C	<input checked="" type="checkbox"/>	bridge
192.168.0.9		<input type="checkbox"/>	bridge
192.168.0.3		<input type="checkbox"/>	bridge

Интернет: ●

Интерфейс главного окна панели управления

Список пользователей и групп

Панель управления MikroTik

Справка

Safe Mode

Главная | Interface | ARP | **User** | Firewall | Сервисы | Log

Пользователи

Логин	Группа	Последний вход
admin	full	jan/02/1970 00:02:54
Admin_Adm...	full	jun/06/2024 22:07:58
Admin_Adm...	ftp	mar/23/2020 14:08:24
test	full	jun/07/2024 11:55:04

Создать пользователя

Группы

Название	local	telnet	ssh	ftp	reboot	read	write	policy	test	winbox	password	web	sniff	se
read	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
write	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
full	<input checked="" type="checkbox"/>													
ftp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Создать группу

Интернет: ●

Интерфейс главного окна панели управления

Список правил Firewall

Панель управления MikroTik

Справка

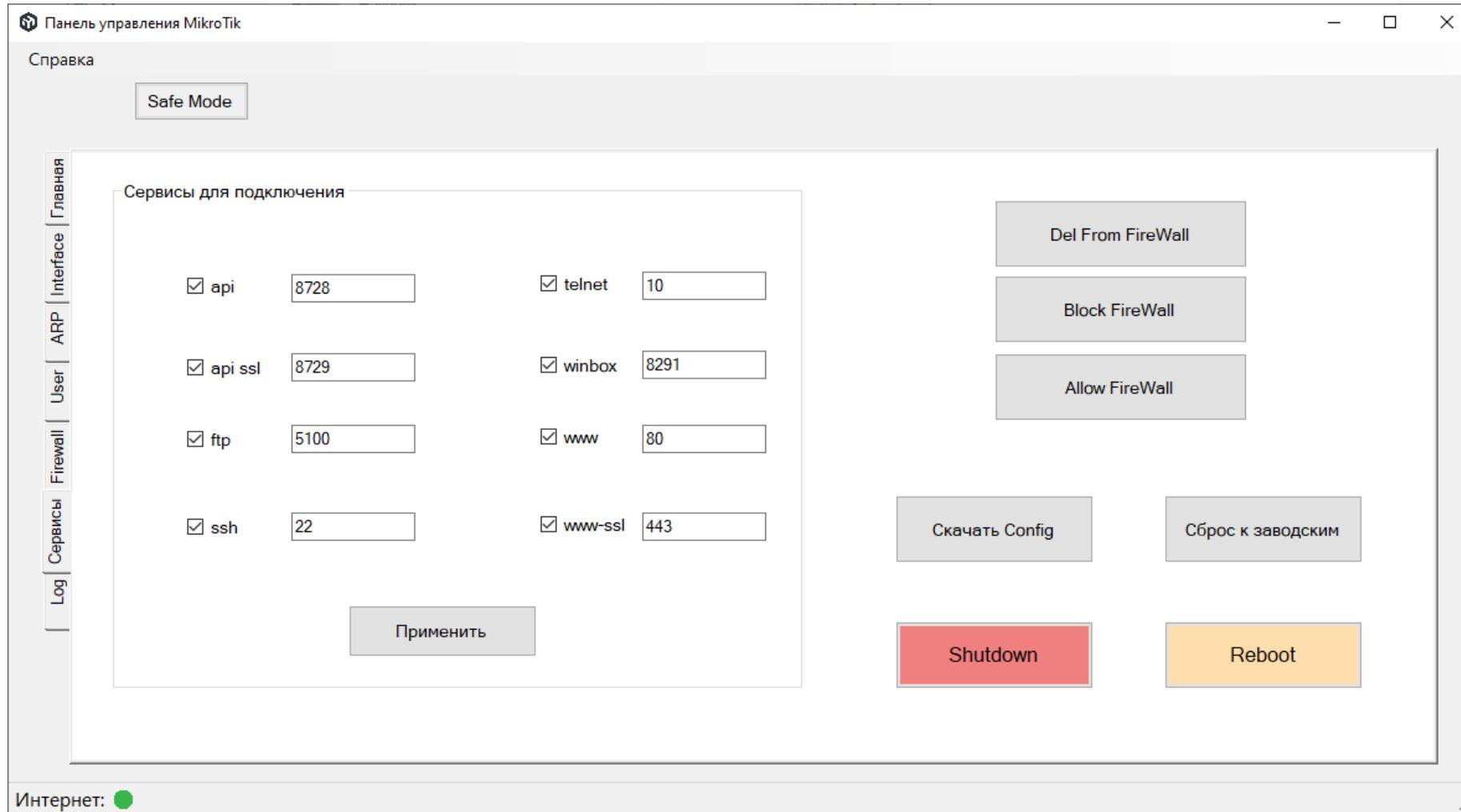
Safe Mode

Главная | Interface | ARP | User | Firewall | Сервисы | Log

Action	Chain	In interface	Protocol	Dst.Port	Dst. Address List	Comment
accept	forward		tcp			
add-dst-to-address...	forward		tcp			
accept	forward				IP_Allowed	
accept	input				IP_Allowed	
drop	input		tcp	1723	PPTP_Blacklist	Drop PPTP Bruteforce
add-src-to-address...	input	Internet	tcp	1723	PPTP_stage3	
add-src-to-address...	input	Internet	tcp	1723	PPTP_stage2	
add-src-to-address...	input	Internet	tcp	1723	PPTP_stage1	
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-address...	input		icmp		wifi_on0	PING WIFI ON STAGE 2
add-src-to-address...	input		icmp			PING WIFI ON STAGE 1
add-src-to-address...	input		icmp		wifi_off0	PING WIFI OFF STAGE 2
add-src-to-address...	input		icmp			PING WIFI OFF STAGE 1

Интернет: ●

Интерфейс главного окна панели управления: Управление сервисами оборудования и дополнительные инструменты



Инструменты для ручного управления доступом

Введите IP адрес, который необходимо удалить из листов блокировки FireWall

Host:

Разрешить доступ

Введите IP адрес и цепочку прохождения траффика

Host:

Chain:

Life Time

Empty = infinity

Запретить доступ

Введите IP адрес и цепочку прохождения траффика

Host:

Chain:

Life Time

Empty = infinity

Интерфейс главного окна панели управления: Просмотр журнала событий (log)

Панель управления MikroTik

Справка

Safe Mode

Update Save To File

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:...

Интернет: ●

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 Сбербанк г. Барнаул
ОГРН 1102225011811 656011, Алтайский край, г. Барнаул, пр. Калинина, 15в

АКТ О ВНЕДРЕНИИ РЕЗУЛЬТАТОВ КВАЛИФИКАЦИОННОЙ 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.



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