

## Программное обеспечение «МЭ104»

Инструкция по установке и настройке

РОФ.АПЦБ.00104-01 90 01

Листов 32

Инв. № подл.	Подп. и дата	Взам. инв. №	Инв. № дубл.	Подп. и дата

**АННОТАЦИЯ**

Настоящий документ представляет собой инструкцию по установке и настройке экземпляра Программного обеспечения «МЭ104», десятичный номер – РОФ.АПЦБ.00104-01 (далее ПО «МЭ104», Программа), предоставленного для проведения экспертной проверки.

**ОГЛАВЛЕНИЕ**

1	ВВЕДЕНИЕ .....	4
1.1	Назначение Программы.....	4
1.2	Назначение документа.....	4
1.3	Требования к квалификации персонала .....	4
1.4	Необходимые права пользователя для установки Программы.....	5
1.5	Требования к оборудованию и системному программному обеспечению 5	
1.6	Меры безопасности.....	5
1.7	Антивирусная защита .....	5
2	КОМПЛЕКТ ПОСТАВКИ .....	5
3	УСТАНОВКА ПРОГРАММЫ .....	6
3.1	Подготовка к установке.....	6
3.2	Установка Программы.....	10
3.3	Запуск Программы.....	11
3.4	Проверка работоспособности Программы .....	12
4	НАСТРОЙКА ПРОГРАММЫ.....	13
4.1	Настройка сетевых интерфейсов .....	15
4.2	Настройка маршрутизации .....	18
4.3	Настройка протоколов Syslog и SNMP .....	19
4.4	Настройка правил фильтрации протокола МЭК 60870-5-104.....	22
4.5	Настройка межсетевого экрана .....	27
4.6	Журнал событий.....	29
5	ОБНОВЛЕНИЕ ПРОГРАММЫ .....	29
6	УДАЛЕНИЕ ПРОГРАММЫ .....	30
	ПЕРЕЧЕНЬ ПРИНЯТЫХ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ .....	31

## **1 ВВЕДЕНИЕ**

### **1.1 Назначение Программы**

Программа служит, для решения следующих задач:

- Инспекция соединений серверов АСДУ с устройствами телемеханики по протоколу МЭК 60870-5-104;
- Прием данных протокола МЭК 60870-5-104 по сети;
- Анализ принятых сообщений протокола МЭК 60870-5-104 (APDU) в IP-пакетах на предмет наличия команд телеуправления;
- Фильтрация APDU, содержащих команды телеуправления, в соответствии с действующими правилами фильтрации;
- Управление правилами фильтрации трафика протокола МЭК 60870-5-104 в соответствии с командами, полученными от Сервера управления;
- Оповещение Сервера управления о результатах фильтрации и смене состояний в правилах фильтрации (Извещение);
- Загрузка актуального списка контролируемых устройств телемеханики с Сервера управления;
- Предоставление пользовательского интерфейса, с помощью которого может выполняться первоначальная настройка МЭ104.

### **1.2 Назначение документа**

Настоящий документ применяется для установки и первичной настройки МЭ104.

### **1.3 Требования к квалификации персонала**

Персонал, занимающийся установкой Программы, должен обладать необходимой квалификацией и опытом установки серверных приложений, а также должен иметь опыт администрирования ОС семейства Linux.

## **1.4 Необходимые права пользователя для установки Программы**

Установка и настройка Программы выполняется лицом, обладающим правами администратора на выбранных для установки системы серверах.

## **1.5 Требования к оборудованию и системному программному обеспечению**

Для корректной работы Программы необходим ПК или сервер с ОЗУ объемом не менее 4 ГБ, центральным процессором как минимум с двумя ядрами.

Для работы Программы требуется ОС Astra Linux SE 1.7.3 редакции «Смоленск», которая не входит в комплект поставки и приобретается отдельно. Установка ОС должна производиться в соответствии с технической документацией, поставляемой производителем.

## **1.6 Меры безопасности**

Программа спроектирована и разработана таким образом, чтобы при условии корректной установки избежать, насколько это возможно, риска случайного поражения электрическим током при нормальном использовании и в состоянии одиночной неисправности.

## **1.7 Антивирусная защита**

Компания-производитель гарантирует отсутствие вирусов и иных вредоносных программных элементов в структуре данной Программы при поставке пользователям. Каждая сборка программного обеспечения перед выпуском проходит дополнительное тестирование на вредоносное программное обеспечение.

## **2 КОМПЛЕКТ ПОСТАВКИ**

В комплект поставки ПО входит:

- дистрибутив ПО «МЭ104» для устройства контроля и анализа управляющих команд МЭ104 (далее – устройство МЭ104).

**Внимание!** ОС Astra Linux и Сервер управления не входят в комплект поставки ПО «МЭ104» и поставляются отдельно.

### 3 УСТАНОВКА ПРОГРАММЫ

Общая последовательность установки программы:

- 1 Подготовка к установке;
- 2 Установка ПО «МЭ104»;
- 3 Запуск ПО «МЭ104»;
- 4 Проверка работоспособности ПО «МЭ104».

#### 3.1 Подготовка к установке

Установка ПО «МЭ104» производится компьютер или сервер с процессорной архитектурой x86-64 с заранее установленной ОС Astra Linux (не входит в комплект поставки ПО «МЭ104»!).

Также перед установкой прикладного ПО произвести установку дополнительных пакетов ОС Astra Linux с локального (идущего в комплекте поставки ОС Astra Linux) либо удаленного репозитория. Для обеспечения стабильности работы системы должна использоваться (**исключительно!**) «frozen» ветка репозитория base и extended.

Для подключения удаленного репозитория необходимо в файл `/etc/apt/sources.list` добавить следующие строки:

```
deb https://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-base/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-extended/ 1.7_x86-64 main contrib non-free
```

После чего необходимо выполнить команды:

```
$ apt update
$ apt list -upgradable
$ astra-update -A -r -T
```

Для создания локального репозитория прежде всего необходимо с помощью команды `apt-mirror` создать зеркала репозитория. Для этого нужно установить пакет `apt-mirror` с помощью команды:

```
$ sudo apt install apt-mirror
```

При установке этого пакета автоматически создается конфигурационный файл `/etc/apt/mirror.list`. В этом файле необходимо указать репозиторий, который необходимо скопировать. Пример файла для копирования репозитория ОС Astra Linux 1.7.3 base и extended:

```
##### config #####
#
# set base_path /var/spool/apt-mirror
#
# set mirror_path $base_path/mirror
# set skel_path $base_path/skel
# set var_path $base_path/var
# set cleanscript $var_path/clean.sh
# set defaultarch <running host architecture>
# set postmirror_script $var_path/postmirror.sh
# set run_postmirror 0
set nthreads 20
set _tilde 0
#
##### end config #####
deb https://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-base/ 1.7_x86-64 main contrib non-free
deb https://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-extended/ 1.7_x86-64 main contrib non-free

clean http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-base/
clean http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.3/repository-extended/
```

После необходимо выполнить команду:

```
$ apt-mirror
```

Далее необходимо создать iso-образы из полученных репозиториях. Для создания iso-образа ОС Astra Linux 1.7.3 base используется следующая команда:

```
$ sudo genisoimage -V 1.7_x86-64 -r -o /home/user/iso/1.7.3/1.7.4-base.iso
/var/spool/apt-mirror/mirror/download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.4/repository-base/
```

Для создания iso-образа ОС Astra Linux 1.7.3 extended используется команда:

```
$ sudo genisoimage -V 1.7_x86-64 -r -o /home/user/iso/1.7.3/1.7.3-extended.iso
/var/spool/apt-mirror/mirror/download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.1/repository-extended/
```

Далее находимо создать локальные репозитории для каждого из образов.

Для репозитория ОС Astra Linux 1.7.3. base необходимо выполнить следующую последовательность действий:

1. Создать каталог:

```
$ sudo mkdir -p /srv/repo/1.7.3/base
```

2. Смонтировать образ:

```
$ sudo mount /путь_к_ISO-образу /media/cdrom
```

3. Скопировать файлы из iso-образа в каталог репозитория:

```
$ sudo cp -a /media/cdrom/* /srv/repo/1.7.3/base
```

4. Отмонтировать образ:

```
$ sudo umount /media/cdrom
```

Для репозитория ОС Astra Linux 1.7.3. extended необходимо выполнить следующую последовательность действий:

1. Создать каталог:

```
$ sudo mkdir -p /srv/repo/1.7.3/extended
```

2. Смонтировать образ:

```
$ sudo mount /путь_к_ISO-образу /media/cdrom
```

3. Скопировать файлы из iso-образа в каталог репозитория:

```
$ sudo cp -a /media/cdrom/* /srv/repo/1.7.3/extended
```

4. Отмонтировать образ:

```
$ sudo umount /media/cdrom
```

Далее для добавления всех созданных файлов необходимо привести файл `/etc/apt/sources.list` к виду:

```
deb file:/srv/repo/1.7.1/base 1.7_x86-64 main non-free contrib
deb file:/srv/repo/1.7.1/extended 1.7_x86-64 main contrib non-free
```

Далее необходимо выполнить следующие команды:

```
$ apt update
$ apt list -upgradable
$ astra-update -A -r -T
```



Перед установкой ПО «МЭ104» необходимо выполнить следующие команды для установки недостающих пакетов (здесь и далее имеется в виду, что администратор использует консоль ОС):

```
$ sudo apt install apache2
$ sudo apt install libmosquitto1 libsnmp30
```

Результат выполнения этих команд выглядит следующим образом:

```
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service
→ /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service
→ /lib/systemd/system/apache-htcacheclean.service.
Обрабатываются триггеры для xserver-xorg-core (2:1.20.14-1ubuntu1astra.se17)
...
update exec ids due to /usr/bin changed
Обрабатываются триггеры для systemd (241-7~deb10u8astra.se30) ...
Обрабатываются триггеры для man-db (2.8.5-2) ...
Обрабатываются триггеры для libc-bin (2.28-10+deb10u1+ci202207192202+astra
4) ...

Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Уже установлен пакет libsnmp30 самой новой версии (5.7.3+dfsg-5+deb10u3).
libsnmp30 помечен как установленный вручную.
Следующие НОВЫЕ пакеты будут установлены:
  libmosquitto1
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0
пакетов, и 0 пакетов не обновлено.
Необходимо скачать 64,2 кВ архивов.
После данной операции объём занятого дискового пространства возрастёт на 1
34 кВ.
Хотите продолжить? [Д/н] y
Пол:1      https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-
extended 1.7_x86-64/main amd64 libmosquitto1 amd64 1.5.7-1+deb10u1 [64,2 кВ]
Получено 64,2 кВ за 0с (998 кВ/с)
Выбор ранее не выбранного пакета libmosquitto1:amd64.
(Чтение базы данных ... на данный момент установлено 169748 файлов и
каталогов.)
Подготовка к распаковке .../libmosquitto1_1.5.7-1+deb10u1_amd64.deb ...
Распаковывается libmosquitto1:amd64 (1.5.7-1+deb10u1) ...
Настраивается пакет libmosquitto1:amd64 (1.5.7-1+deb10u1) ...
Обрабатываются триггеры для libc-bin (2.28-10+deb10u1+ci202207192202+astra
4) ...
```

Далее необходимо установить следующую группу недостающих пакетов командой:

```
$ sudo apt install libfcgi0ldbl ifenslave ipset bridge-utils keepalived
rsyslog
```

Результат выполнения этой команды выглядит следующим образом:

```
...
Настраивается пакет ipvsadm (1:1.29-1) ...
Настраивается пакет libfcgi0ldbl:amd64 (2.4.0-10) ...
Настраивается пакет keepalived (1:2.1.5-0.2~bpo10+1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/keepalived.service → /lib/systemd/system/keepalived.service.
Настраивается пакет libestr0:amd64 (0.1.10-2.1) ...
Настраивается пакет libfastjson4:amd64 (0.99.8-2) ...
Настраивается пакет libfcgi-bin (2.4.0-10) ...
Настраивается пакет bridge-utils (1.6-2) ...
Настраивается пакет liblognorm5:amd64 (2.0.5-1) ...
Настраивается пакет libipset11:amd64 (6.38-1.2) ...
Настраивается пакет ipset (6.38-1.2) ...
Настраивается пакет ifenslave (2.9) ...
Настраивается пакет rsyslog (8.1901.0-1+deb10u2+ci202209161614) ...
Created symlink /etc/systemd/system/syslog.service → /lib/systemd/system/rsyslog.service.
Created symlink /etc/systemd/system/multi-user.target.wants/rsyslog.service → /lib/systemd/system/rsyslog.service.
Обрабатываются триггеры для systemd (241-7~deb10u8astra.se30) ...
Обрабатываются триггеры для man-db (2.8.5-2) ...
Обрабатываются триггеры для dbus (1.12.20-2+astra.se7+ci7) ...
Обрабатываются триггеры для desktop-file-utils (0.26-1astral) ...
Обрабатываются триггеры для mime-support (3.62) ...
Обрабатываются триггеры для hicolor-icon-theme (0.17-2) ...
Обрабатываются триггеры для libc-bin (2.28-10+deb10u1+ci202207192202+astra4) ...
...
Обрабатываются триггеры для xserver-xorg-core (2:1.20.14-1ubuntu1astra.se17) ...
```

## 3.2 Установка Программы

Дистрибутив ПО «МЭ104» содержит в своём составе два установочных файла для ОС семейства Astra Linux (deb-пакеты «iec104fw-2.1.6.x86\_64.deb» и «iec104fcgi-1.5.1.x86\_64.deb») и tar-архив («iec104-frontend.tgz»).

Установка пакета iec104fw-2.1.6.x86\_64.deb производится с помощью следующей команды:

```
$ sudo dpkg -i iec104fw-2.1.6.x86_64.deb
```

Ниже приведен результат выполнения указанной команды:

```
Выбор ранее не выбранного пакета iec104fw.
(Чтение базы данных ... на данный момент установлено 169753 файла и каталога
.)
Подготовка к распаковке iec104fw-2.1.6.x86_64.deb ...
Распаковывается iec104fw (2.1.6) ...
```

```
Настраивается пакет iec104fw (2.1.6) ...  
Created symlink /etc/systemd/system/multi-  
user.target.wants/iec104fw.service → /lib/systemd/system/iec104fw.service.  
Обрабатываются триггеры для man-db (2.8.5-2)
```

Установка пакета `iec104fcgi-1.5.1.x86_64.deb` производится с помощью следующей команды:

```
$ sudo dpkg -i iec104fcgi-1.5.1.x86_64.deb
```

Выполнение команды выглядит примерно следующим образом:

```
Выбор ранее не выбранного пакета iec104fcgi.  
(Чтение базы данных ... на данный момент установлено 169430 файлов и каталог  
ов.)  
Подготовка к распаковке iec104fcgi-1.5.1.x86_64.deb ...  
Распаковывается iec104fcgi (1.5.1) ...  
Настраивается пакет iec104fcgi (1.5.1) ...  
Обрабатываются триггеры для rsyslog (8.1901.0-1+deb10u2+ci202209161614) ...
```

### 3.3 Запуск Программы

После установки ПО «МЭ104» необходимо настроить автозапуск службы, а также запустить её с помощью следующих команд:

```
$ sudo systemctl enable iec104fcgi.service  
$ sudo systemctl start iec104fcgi.service
```

Далее необходимо выполнить настройку веб-интерфейса МЭ104 с помощью следующих команд:

```
$ sudo a2enmod auth_basic authn_core authn_file proxy proxy_fcgi rewrite ssl  
headers
```

Результат выполнения данной команды выглядит следующим образом:

```
Considering dependency authn_core for auth_basic:  
Module authn_core already enabled  
Module auth_basic already enabled  
Module authn_core already enabled  
Module authn_file already enabled  
Module proxy already enabled  
Considering dependency proxy for proxy_fcgi:  
Module proxy already enabled  
Module proxy_fcgi already enabled  
Module rewrite already enabled  
Considering dependency setenvif for ssl:  
Module setenvif already enabled  
Considering dependency mime for ssl:  
Module mime already enabled
```

```
Considering dependency socache_shmcb for ssl:  
Module socache_shmcb already enabled  
Module ssl already enabled  
Enabling module headers.  
To activate the new configuration, you need to run:  
systemctl restart apache2
```

Распаковка tar-архива производится следующей командой:

```
$ tar xvf iec104-frontend.tgz ; cd iec104-frontend
```

Далее необходимо скопировать файлы из каталога «./apache2» в каталог «/etc/apache» следующей командой:

```
$ sudo cp -r apache2/* /etc/apache2/
```

Далее необходимо скопировать файлы из каталога «./var/www/html/» в каталог «/var/www/html/» следующей командой:

```
$ sudo cp -r var/www/html/* /var/www/html/
```

Далее необходимо выполнить следующие команды:

```
$ sudo a2ensite 0000-iec104fw.conf  
$ sudo a2ensite 0001-iec104fw-ssl.conf  
$ sudo a2dissite 000-default.conf  
$ sudo systemctl reload apache2
```

### 3.4 Проверка работоспособности Программы

Проверка статуса работы ПО «МЭ104» производится с помощью следующей команды:

```
$ sudo iec104fw --status  
iec104fw запущен  
systemctl status iec104fcgi  
iec104fcgi.service - IEC104 Fast CGI agent  
Loaded: loaded (/lib/systemd/system/iec104fcgi.service; enabled; vendor  
Active: active (running) since Mon 2023-04-24 13:59:49 MSK; 1h 51min ag  
Main PID: 7460 (iec104fcgi)  
Tasks: 2 (limit: 4637)  
Memory: 1.6M  
CGroup: /system.slice/iec104fcgi.service  
└─7460 /usr/sbin/iec104fcgi --config /usr/share/iec104fcgi/conf
```

Дальнейшие действия по настройке требуемого функционала системы и ПО «МЭ104» необходимо производить с помощью веб-интерфейса устройства.

#### 4 НАСТРОЙКА ПРОГРАММЫ

Действия по настройке ПО «МЭ104» необходимо производить с помощью веб-интерфейса, который после установки ОС и первичной настройки ПО «МЭ104» будет доступен по IP адресу, выбранному при настройке ОС.

Общий вид окна аутентификации веб-интерфейса приведен на рисунке ниже (Рисунок 1). Вид окна зависит от используемого браузера.

Данные для аутентификации (по умолчанию):

*Имя пользователя: user104*

*Пароль: Power-On*

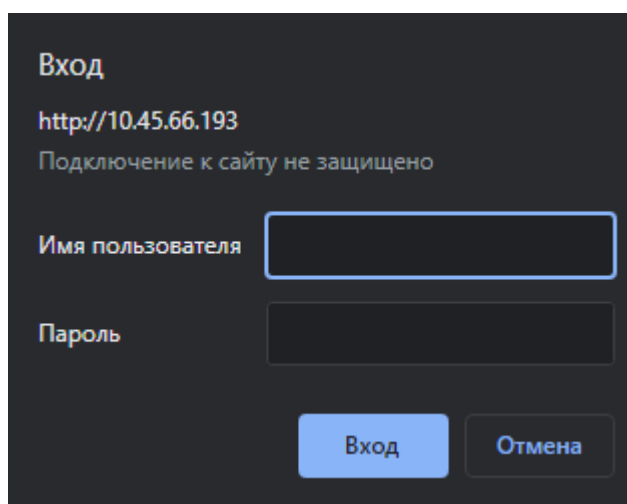
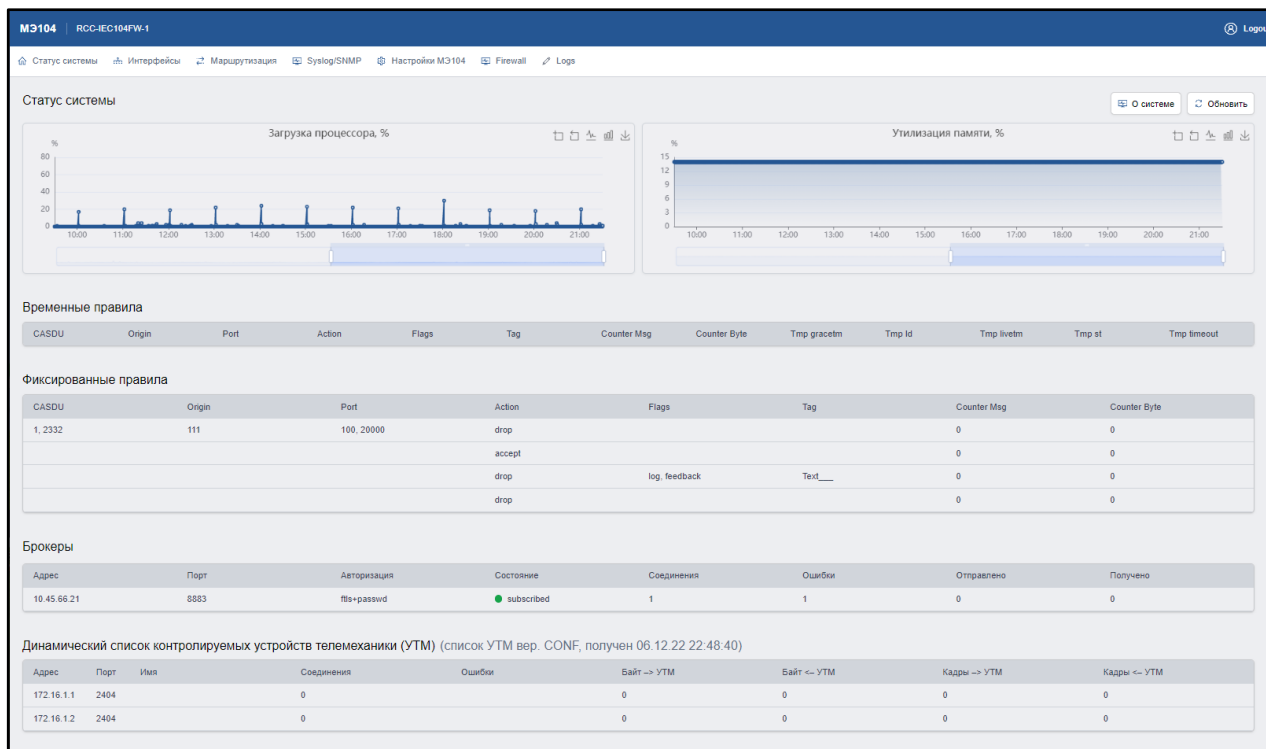


Рисунок 1 – Окно аутентификации веб-интерфейса ПО «МЭ104»

После успешной аутентификации становится доступен веб-интерфейс управления (см. Рисунок 2). На главной странице представлена краткая сводка о системе. Графики указывают процент загрузки центрального процессора и оперативной памяти. Показанные временные и фиксированные правила отображают политику действия устройства для трафика, подпадающего под описание в правилах. Указаны брокеры с состояниями и счётчиками («соединения», «ошибки», «отправлено», «получено») статусов. Динамический список контролируемых устройств телемеханики отображает действующие объекты управления и автоматически обновляется.

Получить краткую справку о программе можно нажав на кнопку «О системе». Во всплывающем окне будут указаны основные параметры программного обеспечения.



Наименование	Текущее значение
Версия ОС	1.7.2
МЭ104 – процесс Web-сервера (ies104fcgi)	1.5.1 [a4666c3]
МЭ104 – процесс анализа и контроля протокола МЭК-104 (ies104fw)	2.1.6 [d13b6b3]
Имя устройства	ies-front17
Номер версии ядра ОС	5.10.0-1057-generic
Архитектура ОС	x86_64
Номер сборки ОС	1.7.2.5
Обновления ОС	
Текущая дата	12.12.2022
Местное время	21:38:10
Временная зона	MSK

Рисунок 2 – Главная страница веб-интерфейса и справка ПО «МЭ104»

## 4.1 Настройка сетевых интерфейсов

Настройка сетевых интерфейсов производится на вкладке «Интерфейсы» (Рисунок 3)

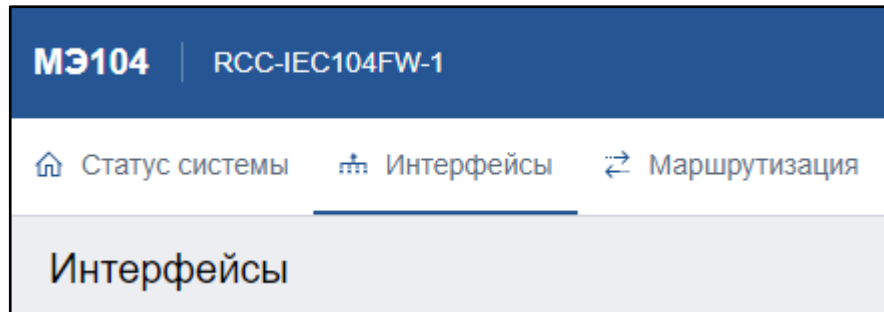
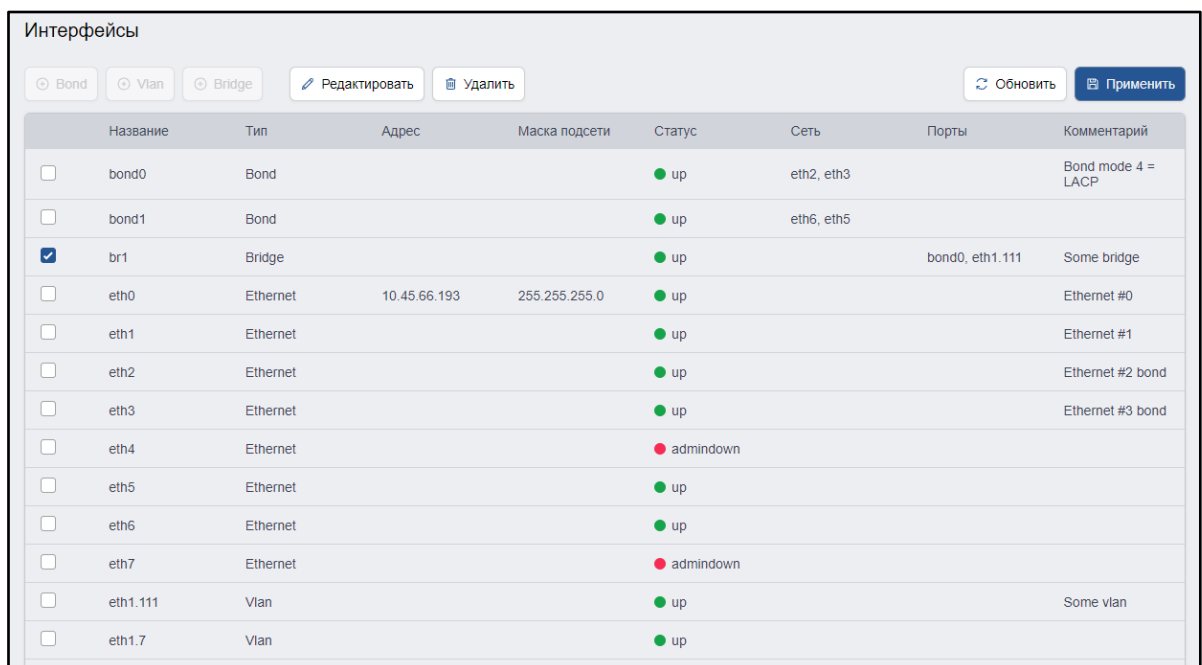


Рисунок 3 – Настройка сетевых интерфейсов

Доступные сетевые интерфейсы системы отображаются на панели данной страницы. Изменение настроек сетевых интерфейсов производится кнопкой «Редактировать» после выделения необходимого интерфейса (Рисунок 4).

The image shows a table of network interfaces. At the top of the table, there are buttons for 'Bond', 'Vlan', and 'Bridge', along with 'Редактировать' and 'Удалить'. On the right side, there are buttons for 'Обновить' and 'Применить'. The table has the following columns: 'Название', 'Тип', 'Адрес', 'Маска подсети', 'Статус', 'Сеть', 'Порты', and 'Комментарий'. The 'br1' interface is selected with a checked checkbox. The 'eth4' and 'eth7' interfaces have a status of 'admindown' (red dot), while others are 'up' (green dot).

	Название	Тип	Адрес	Маска подсети	Статус	Сеть	Порты	Комментарий
<input type="checkbox"/>	bond0	Bond			● up	eth2, eth3		Bond mode 4 = LACP
<input type="checkbox"/>	bond1	Bond			● up	eth6, eth5		
<input checked="" type="checkbox"/>	br1	Bridge			● up		bond0, eth1.111	Some bridge
<input type="checkbox"/>	eth0	Ethernet	10.45.66.193	255.255.255.0	● up			Ethernet #0
<input type="checkbox"/>	eth1	Ethernet			● up			Ethernet #1
<input type="checkbox"/>	eth2	Ethernet			● up			Ethernet #2 bond
<input type="checkbox"/>	eth3	Ethernet			● up			Ethernet #3 bond
<input type="checkbox"/>	eth4	Ethernet			● admin-down			
<input type="checkbox"/>	eth5	Ethernet			● up			
<input type="checkbox"/>	eth6	Ethernet			● up			
<input type="checkbox"/>	eth7	Ethernet			● admin-down			
<input type="checkbox"/>	eth1.111	Vlan			● up			Some vlan
<input type="checkbox"/>	eth1.7	Vlan			● up			

Рисунок 4 – Выбор сетевого интерфейса для настройки

Интерфейсы устройства различаются по типу: физические интерфейсы (Ethernet), агрегированные интерфейсы (Bond), мостовые интерфейсы (Bridge).

В зависимости от типа интерфейса настройки его параметров отличаются.

Для управления устройством обычно выделяют отдельный интерфейс, не предназначенный для передачи другого трафика, кроме веб-трафика управления, трафика мониторинга и трафика журналов событий.

В ПО «МЭ104» возможно добавление агрегированных интерфейсов типа Active-Backup и LACP (802.3ad). Для агрегации доступны только физические интерфейсы (Ethernet). При настройке необходимо задать номер группы агрегации, выбрать требуемые интерфейсы и тип агрегации. Дополнительно задается MTU, интервалы мониторинга дочерних интерфейсов и основной интерфейс при настройке Active-backup агрегации (Рисунок 5).

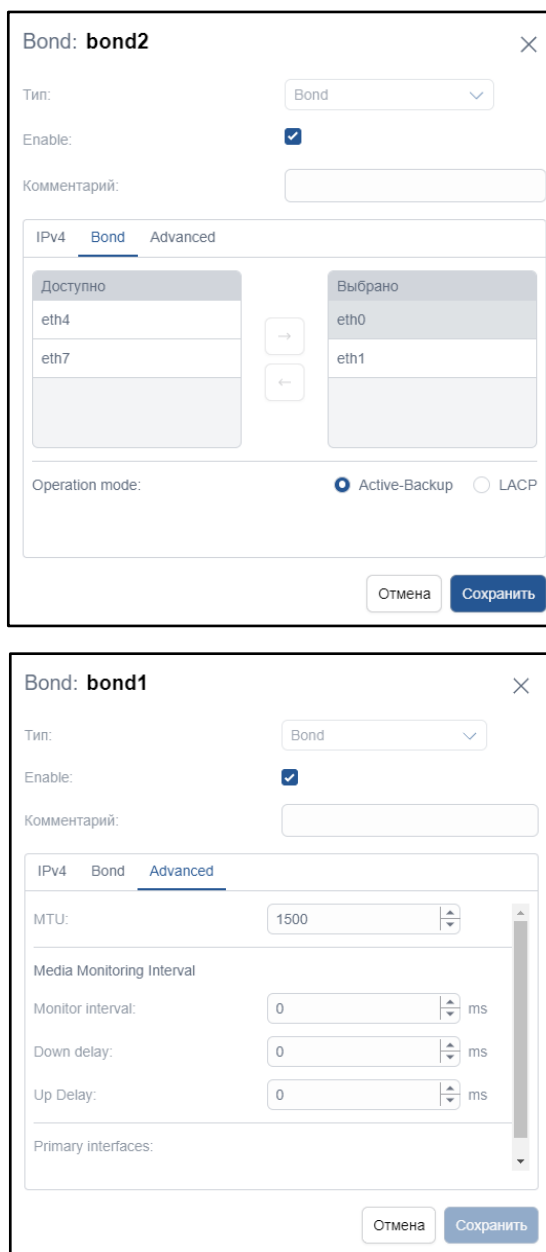


Рисунок 5 – Настройка агрегированного интерфейса



В ПО «МЭ104» возможно добавление мостовых интерфейсов (Bridge). Для объединения в Bridge доступны физические интерфейсы (Ethernet) и агрегированные интерфейсы (Bonding).

При настройке выбрать требуемые интерфейсы, входящие в состав моста (Рисунок 6).

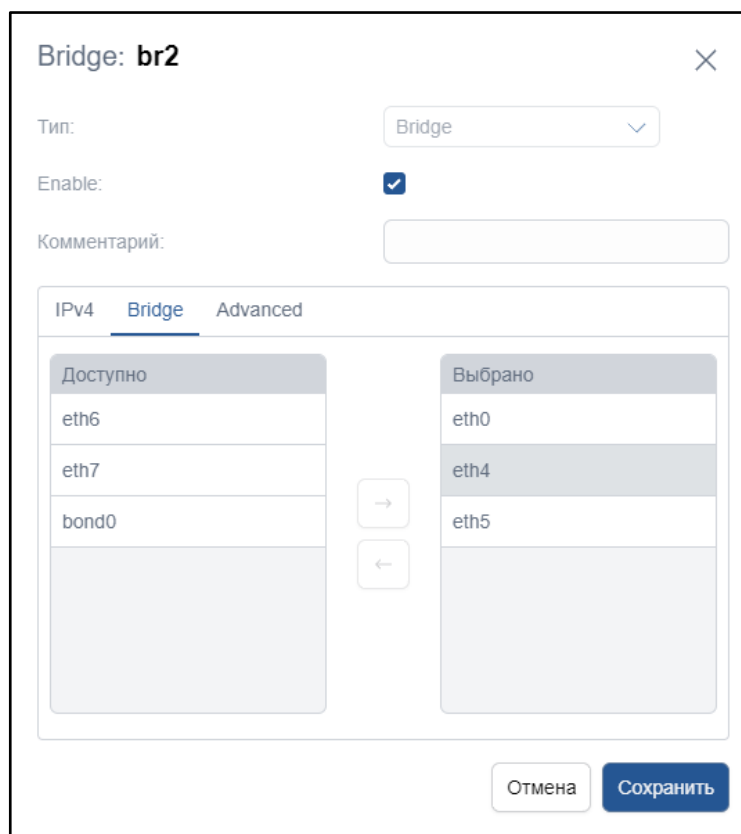
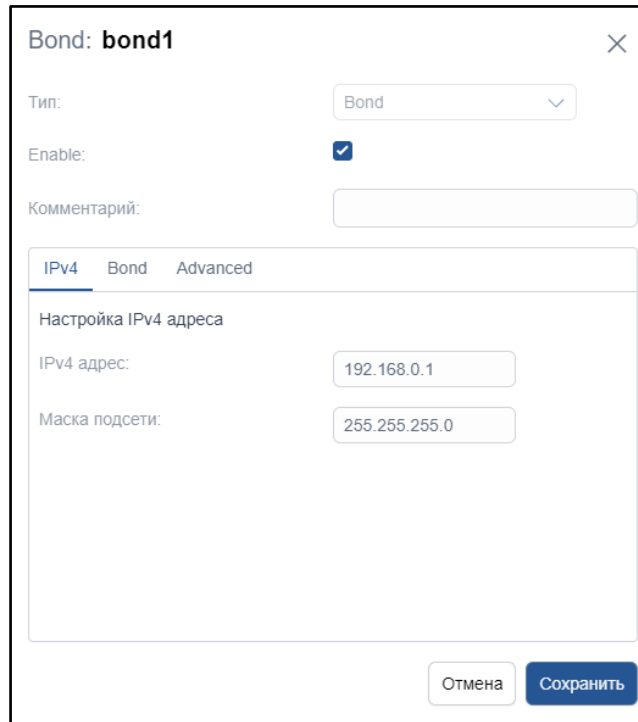


Рисунок 6 – Настройка мостового интерфейса

Настройка IP адреса производится в настройках при добавлении или редактировании любого интерфейса на вкладке IPv4 (Рисунок 7).

**Внимание: IP адрес может быть не задан!**

Кроме этого, IP адрес не должен быть настроен на отдельных интерфейсах, входящих в агрегированный интерфейс (bond) или в мостовой интерфейс (bridge).



The image shows a configuration window titled "Bond: bond1" with a close button (X) in the top right corner. The window contains the following fields and controls:

- Тип:** A dropdown menu set to "Bond".
- Enable:** A checked checkbox.
- Комментарий:** An empty text input field.
- IPv4 Bond Advanced:** A tabbed interface with three tabs: "IPv4" (selected), "Bond", and "Advanced".
- Настройка IPv4 адреса:** A section header for the IPv4 configuration.
- IPv4 адрес:** A text input field containing "192.168.0.1".
- Маска подсети:** A text input field containing "255.255.255.0".
- Buttons:** "Отмена" (Cancel) and "Сохранить" (Save) buttons at the bottom right.

Рисунок 7 – Настройка IP адреса

## 4.2 Настройка маршрутизации

Настройка маршрутизации производится на вкладке «Маршрутизация» (Рисунок 8).

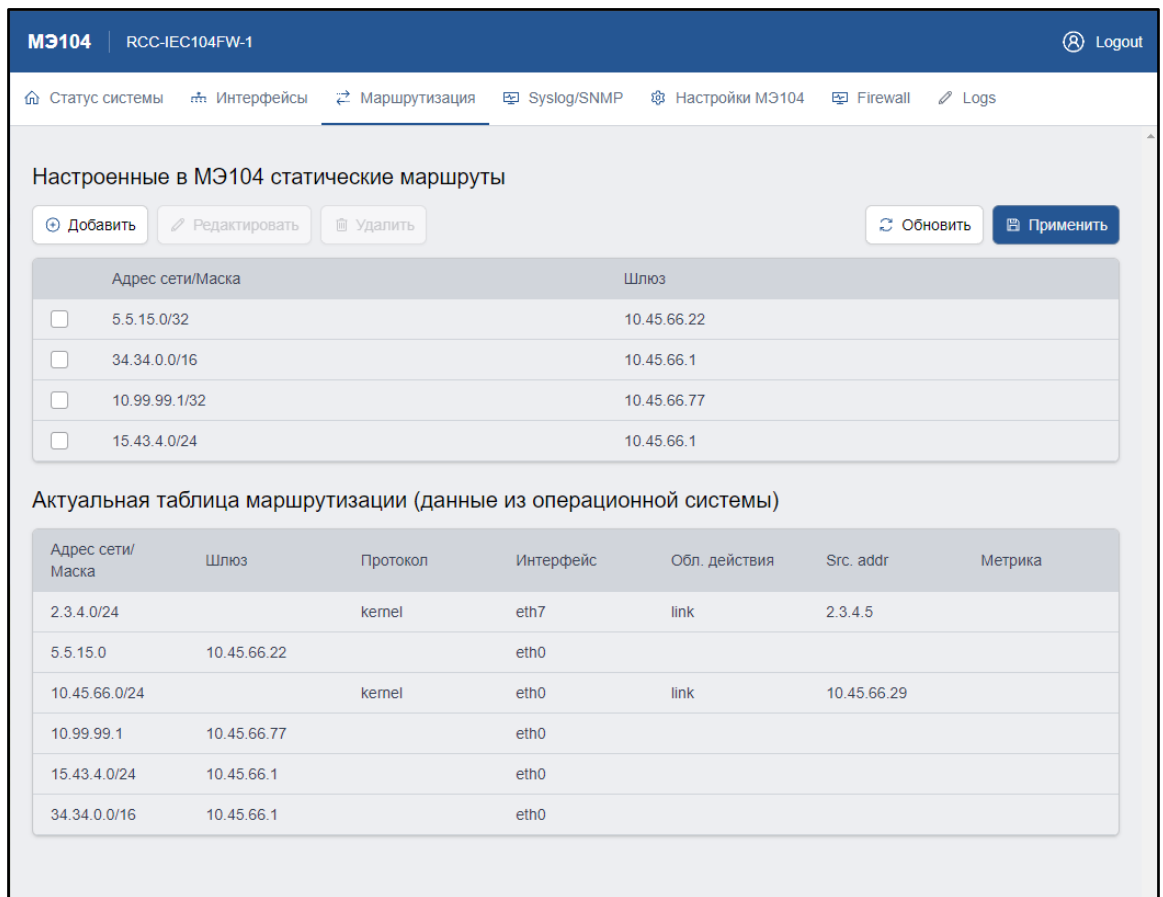


Рисунок 8 – Настройка маршрутизации

Текущие статические маршруты отображаются на данной странице (Рисунок 9). Добавление и изменение маршрутов производится по нажатию на соответствующую кнопку.

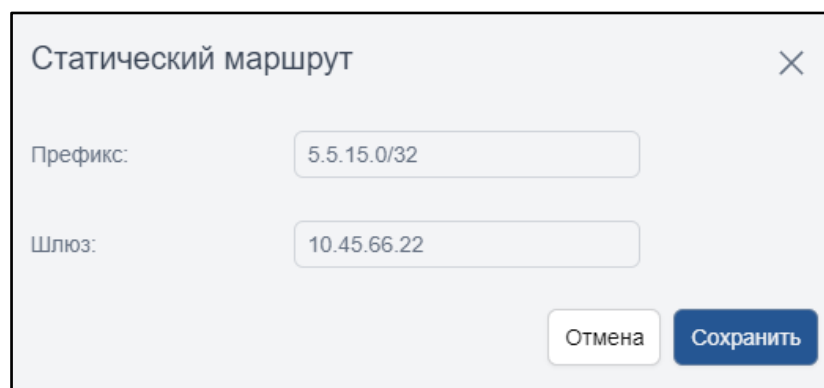


Рисунок 9 – Добавление статического маршрута

### 4.3 Настройка протоколов Syslog и SNMP

Настройка SNMP производится на вкладке «Syslog/SNMP» (Рисунок 10).

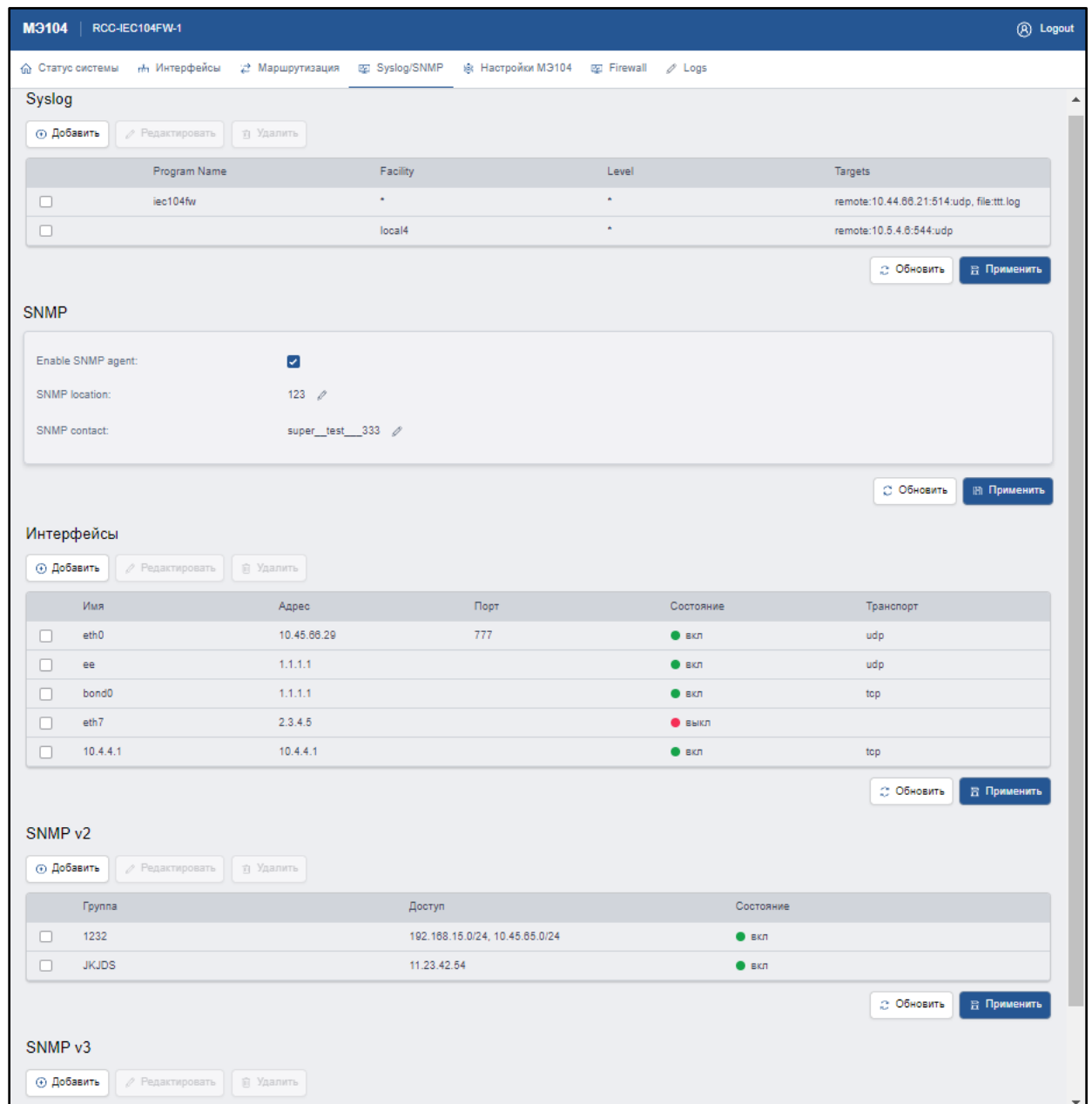


Рисунок 10 – Настройка SNMP

На данной вкладке включается SNMP-интерфейс для мониторинга системы, задаются параметры хоста (contact, location), интерфейсы, на которых будет доступен протокол SNMP, а также производится настройка параметров протокола Syslog.

Для SNMP v2 задаются параметры community, для SNMP v3 параметры USM (userbased security model) (Рисунок 11).

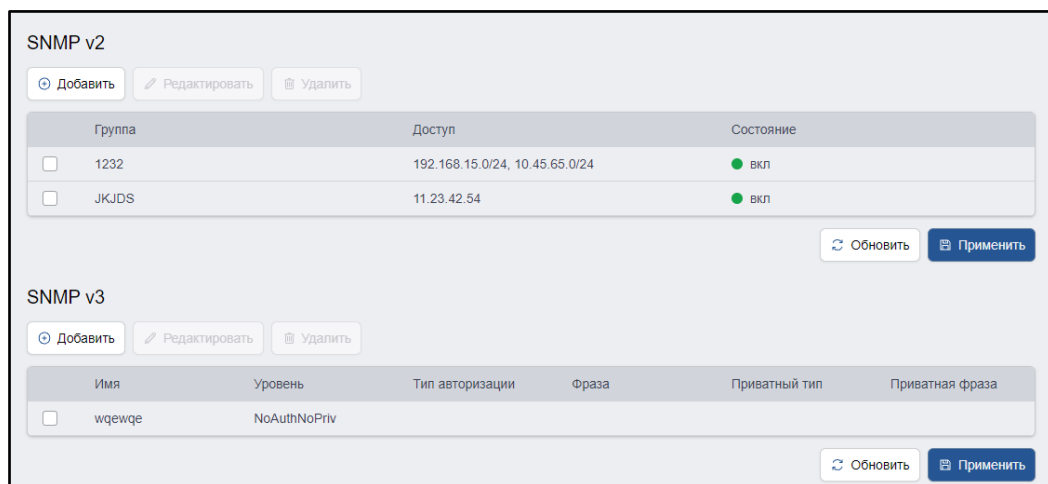


Рисунок 11 – Настройки v2 community, v3 USM

При добавлении пользователя необходимо задать его имя, уровень SNMPv3 (authPriv, authNoPriv), алгоритмы для аутентификации и шифрования, а также соответствующие пароли (Рисунок 12).

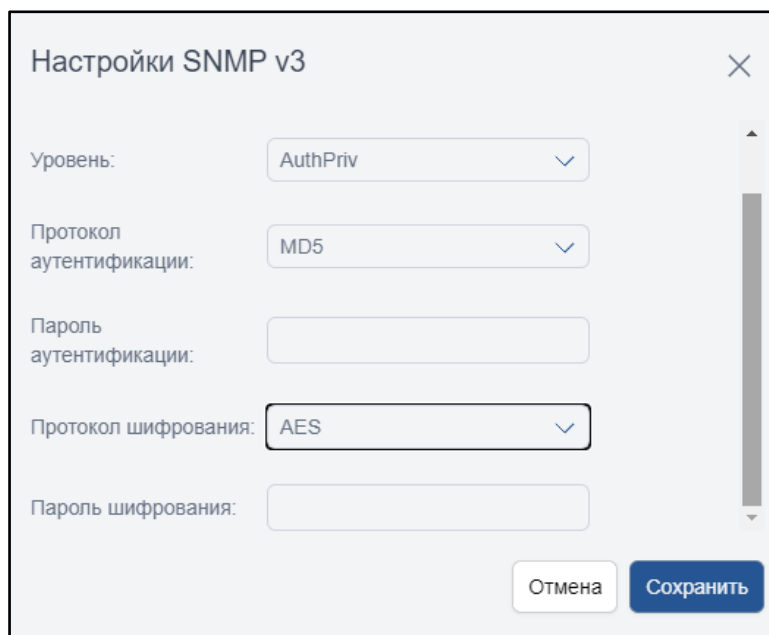
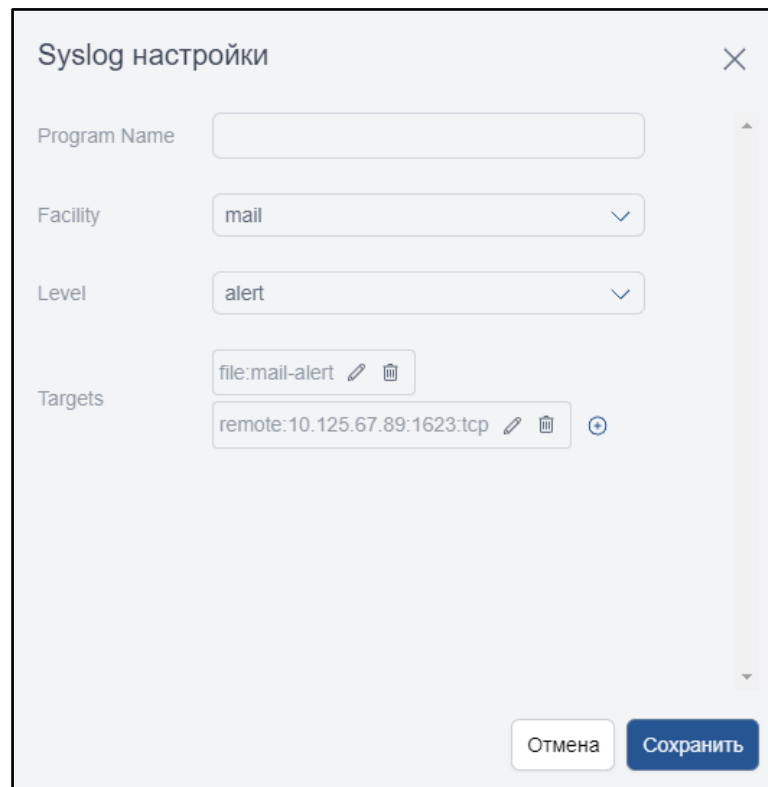


Рисунок 12 – Настройка параметров SNMPv3

При настройке Syslog пользователь должен указать источник сообщения, уровень серьёзности и адресатов сообщений (файл или адрес с протоколом передачи) (Рисунок 13).








Syslog настройки

Program Name

Facility

Level

Targets

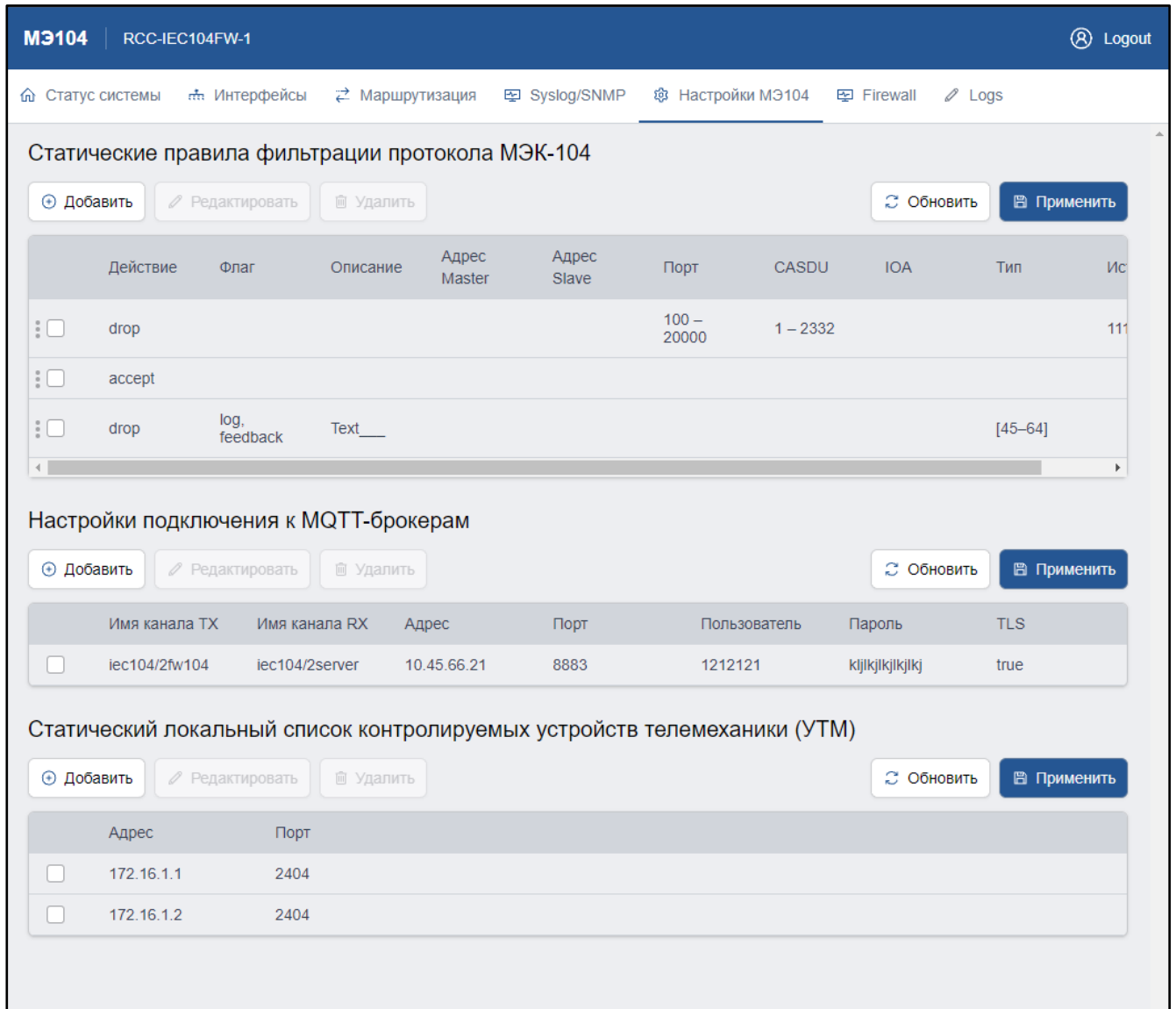
- file:mail-alert  
- remote:10.125.67.89:1623:tcp   

Отмена Сохранить

Рисунок 13 – Настройка параметров Syslog

#### 4.4 Настройка правил фильтрации протокола МЭК 60870-5-104

Настройка правил фильтрации протокола МЭК 60870-5-104 производится на соответствующей вкладке (Рисунок 14). В данном разделе настраиваются общие правила фильтрации, статический список устройств телеметрии (УТМ), брокеры сообщений MQTT.



The screenshot displays the configuration page for MЭ104 (RCC-IEC104FW-1). The interface includes a top navigation bar with the device name and a 'Logout' button. Below the navigation bar, there are links for 'Статус системы', 'Интерфейсы', 'Маршрутизация', 'Syslog/SNMP', 'Настройки МЭ104', 'Firewall', and 'Logs'. The main content area is divided into three sections:

- Статические правила фильтрации протокола МЭК-104**: This section contains a table of static filtering rules. The table has columns for 'Действие', 'Флаг', 'Описание', 'Адрес Master', 'Адрес Slave', 'Порт', 'CASDU', 'IOA', 'Тип', and 'Ис'. Three rules are visible: a 'drop' rule with port 100-20000 and CASDU 1-2332; an 'accept' rule; and another 'drop' rule with 'log, feedback' flag and 'Text' description, with IOA [45-64].
- Настройки подключения к MQTT-брокерам**: This section contains a table of MQTT broker connection settings. The table has columns for 'Имя канала TX', 'Имя канала RX', 'Адрес', 'Порт', 'Пользователь', 'Пароль', and 'TLS'. One entry is shown with channel names 'iec104/2fw104' and 'iec104/2server', address '10.45.66.21', port '8883', user '1212121', password 'kjjkjjkjjkjj', and TLS 'true'.
- Статический локальный список контролируемых устройств телемеханики (УТМ)**: This section contains a table of static local telemechanics devices. The table has columns for 'Адрес' and 'Порт'. Two entries are shown: '172.16.1.1' on port '2404' and '172.16.1.2' on port '2404'.

Рисунок 14 – Настройка параметров МЭ104

Добавление или редактирование настроек MQTT-брокера производится в соответствующем модальном окне (Рисунок 15).

Брокер сообщений

Имя канала TX: ies104/2fw104

Имя канала RX: ies104/2server

Адрес:

Обязательное поле

Порт: 1883

Пользователь:

Пароль:

TLS:  True  False

Отмена Сохранить

Рисунок 15 – Настройка параметров брокера сообщений

Статические правила работы ПО «МЭ104» редактируются в соответствующем модальном окне.

Статические правила, как правило, не должны использовать сложные критерии соответствия, т. к. более специфичные настройки задаются с использованием внешнего приложения, имеющего актуальную информацию о конфигурации объектов управления.

Статические правила служат для:

- разрешения передачи кадров синхронизации;
- общего опроса;
- получения телеизмерений (ТИ) и телесигналов (ТС);
- запрещения кадров управления (ТУ).

Более приоритетные правила для конкретных УТМ задаются через Сервер управления с помощью сообщений, получаемых по протоколу MQTT.

При добавлении и редактировании статического правила могут быть заданы следующие параметры (Рисунок 16):

- тип действия данного правила по заданным критериям;



- указание на необходимость записывать события по данному правилу в журнал событий (log, feedback);
- описание статического правила;
- адреса клиентов и мастеров (slaves, masters);
- порт устройства;
- диапазон CASDU;
- диапазон адресов IOA;
- диапазон типов ASDU (в численном виде);
- адрес источника и порт.

Статические правила

Общие настройки | Адреса | CASDU / IOA / Типы / Origin

Действие: drop

Флаги: feedback × log ×

Описание:

Отмена Сохранить

Статические правила

Общие настройки | Адреса | CASDU / IOA / Типы / Origin

Masters: ○

Slaves: ○

Порт: [12-526] ✎ 🗑

Отмена Сохранить

Статические правила

Общие настройки | Адреса | CASDU / IOA / Типы / Origin

CASDU: [1231-4265] ✎ 🗑

IOA: [234-688] ✎ 🗑 ○

Тип: [2-34] ✎ 🗑 📄

Origin: [52-74] ✎ 🗑

Отмена Сохранить

Рисунок 16 – Создание статических правил

#### **4.5 Настройка межсетевого экрана**

Настройка функций межсетевого экрана производится на соответствующей вкладке (Рисунок 17). Доступные для настройки параметры: действие (Action), описание (Description), состояние файрволла (State), протокол трафика (Protocol), адрес источника (Source), адрес назначения (Destination), DPort, SPort, параметр ведения логов (Log).

Для добавления доступны два типа межсетевых экранов – для трафика, проходящего через устройство (Forward) и трафика, адресованного устройству (Input).

**МЭ104** | RCC-IEC104FW-1 Logout

Статус системы | Интерфейсы | Маршрутизация | Syslog/SNMP | Настройки МЭ104 | **Firewall** | Logs

### Forward Firewall

DROP

Action	Bytes	Description	Hitcount	State	Protocol	Source	Destination	DPort	SPort	Log
<input type="checkbox"/> DROP	0	No invalid connections	0	INVALID						
<input type="checkbox"/> ACCEPT	0	pass immediately	0	RELATED, ESTABLISHED						
<input type="checkbox"/> ACCEPT	0	Zabbix	0	NEW	TCP	10.3.2.20/30		10051		
<input type="checkbox"/> ACCEPT	0	NTP and DNS server	0		UDP		10.8.3.11, 10.6.3.15	53, 123, 53		
<input type="checkbox"/> ACCEPT	0	AD server	0		TCP		10.8.3.11, 10.6.3.15, 10.7.7.7	[88-90], 139, [443-445], 8080		
<input type="checkbox"/> ACCEPT	0	TEST__TEST	0	NEW	ICMP					

### Input Firewall

ACCEPT

Action	Bytes	Description	Hitcount	State	Protocol	Source	Destination	DPort	SPort	Log
<input type="checkbox"/> ACCEPT	2286063		5715							
<input type="checkbox"/> ACCEPT	0	TCP input connections	0	NEW	TCP			80, 443		
<input type="checkbox"/> ACCEPT	0	connections	0	RELATED, ESTABLISHED	TCP					

### Настройки фаервола

✕

Action:

Description:

State:

Protocol:   Auto

Source:

Destination:

DPort:

SPort:

Log:  Log

Рисунок 17 – Настройка параметров Firewall

## 4.6 Журнал событий

На вкладке Logs (Рисунок 18) отображены записи в журнале событий. Параметры записей, отображаемые на вкладке: время записи (Дата, время), название источника (Host), степень важности (Severity), категория записи (Facility), метка Syslog (Syslog tag), источник (Source), сообщение (Message). Записи с категорией «local4» вносятся в файл iec104fw.log. В файл all.log не попадают записи со степенью важности debug.

В качестве параметров фильтрации и поиска сообщений доступны: текст сообщения или метка Syslog (Message, Tag), степень важности (Severity), категория записи (Facility), источник (Source). Также можно изменять количество выводимых на странице сообщений.

Дата, время	Host	Severity	Facility	Syslog tag	Source	Message
05.12.2022 13:31:42	iec-front17	INFO	daemon	systemd[1]:	systemd	anacron service: Succeeded.
05.12.2022 13:31:42	iec-front17	NOTICE	cron	anacron[10858]:	anacron	Normal exit (0 jobs run)
05.12.2022 13:31:42	iec-front17	NOTICE	cron	anacron[10858]:	anacron	Anacron 2.3 started on 2022-12-05
05.12.2022 13:31:42	iec-front17	INFO	daemon	systemd[1]:	systemd	Started Run anacron jobs.
05.12.2022 13:30:01	iec-front17	INFO	authpriv	CRON[10856]:	CRON	pam_unix(cron:session): session closed for user root
05.12.2022 13:30:01	iec-front17	INFO	cron	CRON[10857]:	CRON	(root) CMD ([ -x /etc/init.d/anacron ] && if [ ! -d /run/systemd/system ]; then /usr/sbin/invoke-rc.d anacron start >/dev/null; fi)
05.12.2022 13:30:01	iec-front17	INFO	authpriv	CRON[10856]:	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
05.12.2022 13:30:01	iec-front17	NOTICE	authpriv	CRON[10856]:	CRON	pam_kiosk2(cron:session): need_continue: UID 0 detected, skipping. User: root
05.12.2022 13:17:01	iec-front17	INFO	authpriv	CRON[10851]:	CRON	pam_unix(cron:session): session closed for user root
05.12.2022 13:17:01	iec-front17	INFO	cron	CRON[10852]:	CRON	(root) CMD ( cd / && run-parts --report /etc/cron.hourly)
05.12.2022 13:17:01	iec-front17	INFO	authpriv	CRON[10851]:	CRON	pam_unix(cron:session): session opened for user root by (uid=0)
05.12.2022 13:17:01	iec-front17	NOTICE	authpriv	CRON[10851]:	CRON	pam_kiosk2(cron:session): need_continue: UID 0 detected, skipping. User: root
05.12.2022 13:02:02	iec-front17	INFO	authpriv	CRON[10767]:	CRON	pam_unix(cron:session): session closed for user logcheck
05.12.2022 13:02:01	iec-front17	INFO	cron	CRON[10768]:	CRON	(logcheck) CMD ( if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck; fi)

Рисунок 18 – Вкладка журнала событий

## 5 ОБНОВЛЕНИЕ ПРОГРАММЫ

Все обновления ПО Системы передаются специалистами компании производителя с инструкциями по их инсталляции.

## 6 УДАЛЕНИЕ ПРОГРАММЫ

**Осторожно, данные действия необратимы и после них потребуется переустановка ПО!**

Для полного удаления системы и приведения серверов в исходное состояние необходимо выполнить команду **sudo apt remove --purge iec104fw** и подтвердить полную остановку сервиса и удаление всех его файлов и конфигурации.

```
$ sudo apt remove --purge iec104fw
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Пакеты, которые будут УДАЛЕНЫ:
  iec104fw*
обновлено 0, установлено 0 новых пакетов, для удаления отмечено 1
пакетов, и 1 пакетов не обновлено.
После данной операции, объём занятого дискового пространства уменьшится
на 381 кВ.
Хотите продолжить? [Д/н]
```

После выполнения данной команды ПО «МЭ104» будет удалено.

**ПЕРЕЧЕНЬ ПРИНЯТЫХ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ**

<b>Обозначение</b>	<b>Описание</b>
ALD	(англ. Astra Linux Directory) – служба управления Единым пространством пользователей
APDU	(англ. Application Protocol Data Unit) – протокольный блок данных прикладного уровня
CASDU	(англ. Common Address of ASDU) – общий адрес для сообщений протокола МЭК 60870-5-104
FEP	(англ. Front-End Processor) – коммуникационный процессор
HDD	(англ. Hard (magnetic) Disk Drive) – запоминающее устройство произвольного доступа
IP	(англ. Internet Protocol) – межсетевой протокол
LACP	(англ. Link Aggregation Control Protocol) – протокол, предназначенный для объединения нескольких физических каналов в один логический в сетях Ethernet
MBR	(англ. Master Boot Record) – главная загрузочная запись
MQTT	(англ. Message Queuing Telemetry Transport) – упрощённый сетевой протокол, работающий поверх TCP/IP, ориентированный на обмен сообщениями между устройствами по принципу издатель-подписчик
NTP	(англ. Network Time Protocol) – протокол сетевого времени
RAID	(англ. Redundant Array of Independent Disks – избыточный массив независимых (самостоятельных) дисков) – технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности
SNMP	(англ. Simple Network Management Protocol) – простой протокол сетевого управления
TLS	(англ. Transport layer security) – протокол защиты транспортного уровня, обеспечивающий защищённую передачу данных между узлами в сети Интернет
АРМ	Автоматизированное рабочее место
БД	База данных

МЭ104	Устройство контроля и анализа управляющих команд МЭ104
МЭК	Международная электротехническая комиссия (МЭК) – международная некоммерческая организация по стандартизации в области электрических, электронных и смежных технологий
ОС	Операционная система
ПАО	Публичное акционерное общество
ПО	Программное обеспечение
ПТК	Программно-технический комплекс
РФ	Российская Федерация
СУБД	Система управления базами данных
ТЗ	Техническое задание
ТИ	Телеизмерения
ТМ	Телемеханика
ТС	Телесигнализация
ТУ	Телеуправление
УТМ	Устройство телемеханики