

Программное обеспечение «МЭ104»

Руководство оператора

РОФ.АПЦБ.00104-01 34 01

Листов 16

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

РОФ.АПЦБ.00104-01 34 01

### АННОТАЦИЯ

Настоящий документ представляет собой руководство оператора Программного обеспечения «МЭ104», десятичный номер – РОФ.АПЦБ.00104-01 (далее ПО «МЭ104»).

## Содержание

1 Общие сведения.....	4
1.1 Назначение Изделия.....	4
1.2 Меры безопасности .....	5
1.3 Антивирусная защита .....	5
2 Условия выполнения программы .....	6
2.1 Требования к квалификации персонала.....	6
2.2 Требования к оборудованию .....	6
2.3 Установка и настройка Изделия .....	6
3 Выполнение программы .....	7
4 Сообщения оператору .....	15
Перечень обозначений и сокращений .....	16

## 1 ОБЩИЕ СВЕДЕНИЯ

## 1.1 Назначение Изделия

Изделие 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.

Изделие соответствует «Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утв. приказом № 76 ФСТЭК России от 02 июня 2020 г.) – по 4-му уровню доверия и требованиям документа РОФ.АПЦБ.00104-01 ТУ.

Изделие при выполнении указаний по эксплуатации может применяться в автоматизированных системах управления до 1 класса защищенности включительно в соответствии с Приказом ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах,

представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», а также в значимых объектах критической информационной инфраструктуры Российской Федерации до 1 категории значимости включительно в соответствии с Приказом ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Изделие не является полнофункциональным межсетевым экраном, т.к. осуществляет анализ и контроль только трафика специализированного протокола прикладного уровня МЭК-60870-104. Для обеспечения информационной безопасности электронного периметра объекта Изделие необходимо использовать совместно с сертифицированными межсетевыми экранами типа «А», «Б» или «Д» соответствующего класса.

### 1.2 Меры безопасности

Система 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.

### 1.3 Антивирусная защита

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

## 2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

### 2.1 Требования к квалификации персонала

Персонал, занимающийся установкой Системы, должен обладать необходимой квалификацией и опытом установки серверных приложений: необходим опыт администрирования ОС Linux.

Порядок проверки знаний персонала и допуска его к работе устанавливается внутренними регламентами Заказчика.

### 2.2 Требования к оборудованию

Изделие может быть установлено как на физическом сервере, так и в виртуальной среде.

Аппаратные требования для работы Изделия могут меняться в зависимости от желаемой производительности Изделия, от требуемого количества сетевых портов и от планируемой нагрузки.

Минимальные аппаратные требования представлены в Таблице 1.

Таблица 1 – Минимальные аппаратные требования для МЭ104

Параметр	Значение
Архитектура процессора	x86-64
Количество ядер процессора	2
Объем ОЗУ	4 Гбайт
Свободное место на жестком диске или твердотельном накопителе	32 Гбайт
Сетевой интерфейс Ethernet	3

Требования к системному ПО представлены в Таблице 2.

Таблица 2 – Требования к системному ПО для МЭ104

Параметр	Значение
Операционная система	AstraLinux Special Edition v.1.6 и выше
Веб-браузер для удаленного управления	Google Chrome v.99 и выше

### 2.3 Установка и настройка Изделия

Порядок действий по установке и настройке Изделия, действий по реализации функций безопасности среды функционирования, действий по обновлению и удалению ПО приведен в документе «РОФ.АПЦБ.00104-01 90 01 Руководство по установке и настройке».

РОФ.АПЦБ.00104-01 34 01

## 3 ВЫПОЛНЕНИЕ ПРОГРАММЫ

Все действия с программой оператор производит с помощью веб-интерфейса, который после установки ОС и первичной настройки ПО «МЭ104» будет доступен по IP адресу устройства, 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:*

*Имя пользователя: user104;*

*Пароль: Power-On.*

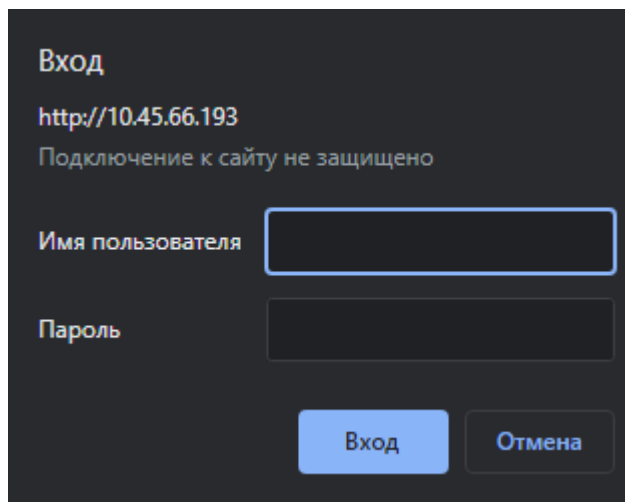
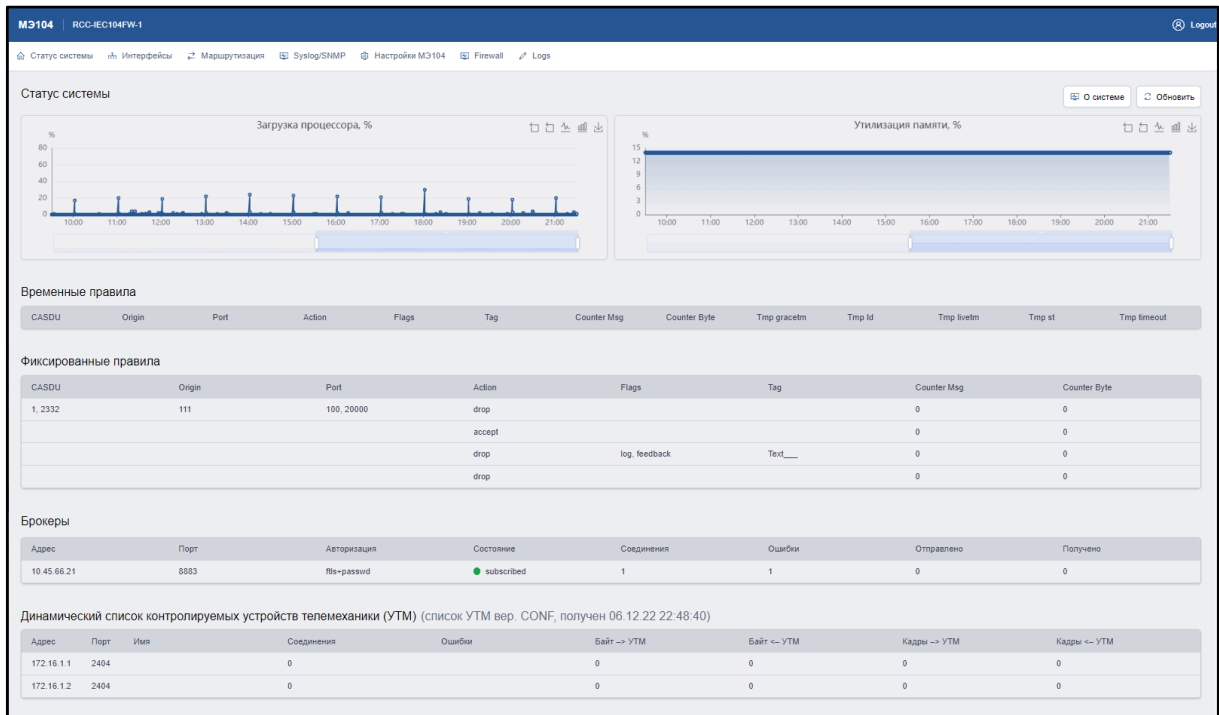


Рисунок 1 – Окно аутентификации веб-интерфейса устройства МЭ104

После успешной аутентификации становится доступен веб-интерфейс управления (Рисунок 2), на главной странице («Статус системы») представлены следующие сведения:

- краткая сводка о системе;
- графики, показывающие процент загрузки процессора и памяти.
- брокеры с состояниями и счётчиками статусов («Соединения», «Ошибки», «Отправлено», «Получено»).



Наименование	Текущее значение
Версия ОС	1.7.2
МЭ104 – процесс Web-сервера (iecs104fcgi)	1.5.1 [a4666c3]
МЭ104 – процесс анализа и контроля протокола МЭК-104 (iecs104fw)	2.1.6 [d13b6b3]
Имя устройства	iecs-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 устройства МЭ104

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

Оператору также доступны следующие вкладки (Рисунок 3):

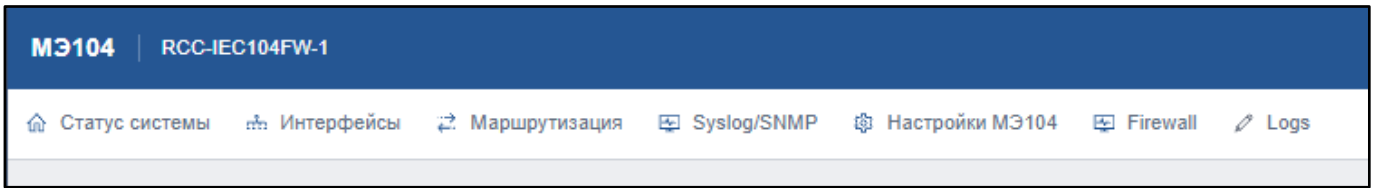


Рисунок 3 – Доступные вкладки

На вкладке «Интерфейсы» оператор может ознакомиться с текущими настройками сетевых интерфейсов и при необходимости может произвести их изменение с помощью кнопки «Редактировать» после выделения необходимого интерфейса (Рисунок 4):

Интерфейсы									
Bond		Vlan		Bridge		Редактировать		Удалить	
						Обновить		Применить	
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

На вкладке «Маршрутизация» (Рисунок 5) оператор может ознакомиться с текущими настройками маршрутизации. На данной странице отображаются текущие статические маршруты.

**M3104 | RCC-IEC104FW-1** Logout

Статус системы | Интерфейсы | **Маршрутизация** | Syslog/SNMP | Настройки M3104 | Firewall | Logs

### Настроенные в M3104 статические маршруты

Добавить | Редактировать | Удалить | Обновить | Применить

Адрес сети/Маска	Шлюз
<input type="checkbox"/> 5.5.15.0/32	10.45.66.22
<input type="checkbox"/> 34.34.0.0/16	10.45.66.1
<input type="checkbox"/> 10.99.99.1/32	10.45.66.77
<input type="checkbox"/> 15.43.4.0/24	10.45.66.1

### Актуальная таблица маршрутизации (данные из операционной системы)

Адрес сети/Маска	Шлюз	Протокол	Интерфейс	Обл. действия	Src. addr	Метрика
2.3.4.0/24		kernel	eth7	link	2.3.4.5	
5.5.15.0	10.45.66.22		eth0			
10.45.66.0/24		kernel	eth0	link	10.45.66.29	
10.99.99.1	10.45.66.77		eth0			
15.43.4.0/24	10.45.66.1		eth0			
34.34.0.0/16	10.45.66.1		eth0			

Рисунок 5 – Настройка маршрутизации

**На вкладке «Syslog/SNMP» оператор может ознакомиться с текущими настройками протокола SNMP (Рисунок 6).**

The screenshot displays the configuration page for MЭ104 (RCC-IEC104FW-1) with the following sections:

**Syslog**

Program Name	Facility	Level	Targets
iec104fw	*	*	remote:10.44.68.21:514:udp, file:ttt.log
	local4	*	remote:10.5.4.8:544:udp

**SNMP**

Enable SNMP agent:

SNMP location: 123

SNMP contact: super\_test\_333

**Интерфейсы**

Имя	Адрес	Порт	Состояние	Транспорт
eth0	10.45.68.29	777	● вкл	udp
ee	1.1.1.1		● вкл	udp
bond0	1.1.1.1		● вкл	tcp
eth7	2.3.4.5		● выкл	
10.4.4.1	10.4.4.1		● вкл	tcp

**SNMP v2**

Группа	Доступ	Состояние
1232	192.168.15.0/24, 10.45.65.0/24	● вкл
JKJDS	11.23.42.54	● вкл

**SNMP v3**

Рисунок 6 – Настройка SNMP

На вкладке «МЭ104» оператор может ознакомиться с текущими настройками МЭ104 (Рисунок 7): общие правила фильтрации, статический список устройств телеметрии (УТМ), брокеры сообщений MQTT.

**МЭ104** | RCC-IEC104FW-1 Logout

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

### Статические правила фильтрации протокола МЭК-104

Добавить | Редактировать | Удалить Обновить | Применить

Действие	Флаг	Описание	Адрес Master	Адрес Slave	Порт	CASDU	IOA	Тип	Ис
<input type="checkbox"/>	drop				100 – 20000	1 – 2332			111
<input type="checkbox"/>	accept								
<input type="checkbox"/>	drop	log, feedback	Text					[45-64]	

### Настройки подключения к MQTT-брокерам

Добавить | Редактировать | Удалить Обновить | Применить

Имя канала TX	Имя канала RX	Адрес	Порт	Пользователь	Пароль	TLS	
<input type="checkbox"/>	iec104/2fw104	iec104/2server	10.45.66.21	8883	1212121	kjlkjlkjlkj	true

### Статический локальный список контролируемых устройств телемеханики (УТМ)

Добавить | Редактировать | Удалить Обновить | Применить

Адрес	Порт
<input type="checkbox"/>	172.16.1.1 2404
<input type="checkbox"/>	172.16.1.2 2404

Рисунок 7 – Настройка параметров МЭ104

На вкладке «**Firewall**» оператор может ознакомиться с текущими настройками функций межсетевого экрана (Рисунок 8). 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).

**Forward Firewall**

Action	Bytes	Description	Hitcount	State	Protocol	Source	Destination	DPort	SPort	Log
DROP	0	No invalid connections	0	INVALID						
ACCEPT	0	pass immediately	0	RELATED, ESTABLISHED						
ACCEPT	0	Zabbix	0	NEW	TCP	10.3.2.20/30		10051		
ACCEPT	0	NTP and DNS server	0		UDP		10.8.3.11, 10.8.3.15	53, 123, 53		
ACCEPT	0	AD server	0		TCP		10.8.3.11, 10.8.3.15, 10.7.7.7	[88-90], 139, [443-445], 8080		
ACCEPT	0	TEST__TEST	0	NEW	ICMP					

**Input Firewall**

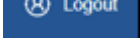
Action	Bytes	Description	Hitcount	State	Protocol	Source	Destination	DPort	SPort	Log
ACCEPT	2286063		5715							
ACCEPT	0	TCP input connections	0	NEW	TCP			80, 443		
ACCEPT	0	connections	0	RELATED, ESTABLISHED	TCP					

Рисунок 8 – Настройка параметров Firewall

На вкладке «Logs» (Рисунок 9) оператор может ознакомиться с текущими записями 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).

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 9 – Вкладка журнала событий

Для прекращения работы с Системой нажмите кнопку  в правом верхнем углу экрана.

4 СООБЩЕНИЯ ОПЕРАТОРУ

При работе с Системой отправка каких-либо сообщений оператору не предусмотрена.

## ПЕРЕЧЕНЬ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

Обозначение	Описание
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