УТВЕРЖДЕН

ФРПС.466259.001 РЭ-ЛУ

Межсетевой экран ССПТ-4А1

Руководство по эксплуатации

ФРПС.466259.001 РЭ

2022

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

Аннотация

Настоящий документ “*Межсетевой экран ССПТ-4А1. Руководство по эксплуатации” ФРПС.466259.001 РЭ* является частью эксплуатационной документации на программно-техническое изделие “*Межсетевой экран ССПТ-4А1” ФРПС.466259.001* (далее – МЭ ССПТ-4А1).

Настоящий документ описывает функциональные возможности, общие принципы функционирования, порядок настройки и управления МЭ ССПТ-4А1 версии 1.0.0, его конструктивные особенности и основные технические характеристики. Документ предназначен для специалистов в области сетевой безопасности и администраторов сетей, использующих МЭ ССПТ-4А1 для решения вопросов, связанных с разграничением доступа к информационным и сетевым ресурсам в компьютерных сетях, использующих технологию Ethernet.

МЭ ССПТ-4А1 может использоваться в локальных вычислительных сетях (далее – ЛВС), построенных на базе технологии Ethernet с пропускной способностью 10/100/1000 Мбит/с, а также 10 Гбит/с.

Назначение и организация документа. Данный документ представляет собой руководство администратора МЭ ССПТ-4А1, состоящее из следующих глав.

1) **Основные технические особенности и функциональные возможности**. Назначение, область применения и основные функциональные характеристики МЭ ССПТ-4А1.
2) **Подготовка к работе и первое включение**. Описание комплекта поставки, надписей и условных обозначений устройства, руководство по выполнению начальных настроек после первого включения устройства.
3) **Принципы функционирования.** Подробное описание принципов функционирования и порядка настройки подсистем МЭ ССПТ-4А1.
4) **WEB-интерфейс администратора**. Подробное руководство по использованию WEB-интерфейса администратора как полнофункционального средства для управления, настройки и администрирования МЭ ССПТ-4А1.
5) **SNMP-интерфейс администратора**. Подробное руководство по использованию SNMP-интерфейса администратора как средства для контроля состояния и мониторинга функционирования МЭ ССПТ-4А1.

6) **Регламентное тестирование**. Описание штатных процедур регламентного тестирования для проверки работоспособности и выявления нарушений в работе и неисправностей в аппаратной части и программных подсистемах МЭ ССПТ-4А1.

7) **Средство обновления и восстановления (СОВа-4)**. Руководство по восстановлению работоспособности МЭ ССПТ-4А1 после сбоев и отказов силами обслуживающего персонала без участия представителей предприятия-изготовителя.

8) Приложения.

8.1) **Требования к форматам данных и ограничения параметров конфигурации**. Перечень соглашений о форматах и допустимых значениях различных именуемых элементов определений политик доступа (правила фильтрации и справочник объектов), параметров конфигурации и командного языка МЭ ССПТ-4А1.

8.2) **Перечень регистрируемых событий**. Полный список и описание событий, регистрируемых подсистемой регистрации в процессе настройки и функционирования МЭ ССПТ-4А1.

8.3) **Перечень диагностических сообщений.** Полный список и описание диагностических сообщений программных модулей, которые могут быть получены администратором в процессе настройки и управления МЭ ССПТ-4А1.

8.4) **Командный язык**. Перечень всех команд командного интерфейса МЭ ССПТ-4А1 с описанием синтаксиса, назначения и привилегий администратора, требуемых для их выполнения.

8.5) **Определения правил фильтрации**. Синтаксис и подробное описание всех типов правил фильтрации МЭ ССПТ-4А1.

8.6) **Определения объектов справочника**. Синтаксис и подробное описание всех типов объектов справочника, применяемых в правилах фильтрации МЭ ССПТ-4А1.

8.7) **Дерево MIB-переменных SNMP-интерфейса.** Подробное описание групп и объектов дерева MIB-переменных, используемых для настройки, управления и мониторинга МЭ ССПТ-4А1 по протоколу SNMP, с указанием назначения, типа данных, прав доступа и установленных ограничений.

8.8) **Утилита аутентификации сетевого пользователя**. Руководство по использованию утилиты аутентификации сетевого пользователя, необходимой для работы пользователей через МЭ ССПТ-4А1 при включенной функции аутентификации сетевых пользователей.

8.9) **Протокол FNPCP**. Описание протокола FNPCP, предназначенного для уделенного управления МЭ ССПТ-4А1: назначение, форматы запросов и ответов протокола;

8.10) **Перечень диагностических сообщений ПО СОВа-4**. Полный список и описание диагностических сообщений и статусов выполнения процедуры обновления с использованием средства обновления и восстановления СОВа-4.

Принятые обозначения. В данном документе действуют следующие соглашения о шрифтовом оформлении:

- *курсив* – применяется для выделения в основном тексте новых терминов или важной для понимания излагаемого материала информации;
- `моноширинный шрифт` – применяется для выделения в основном тексте имен переменных, команд или файлов;
- **`моноширинный шрифт`** – обозначает в примерах и в основном тексте данные, вводимые пользователем.

Особо выделяемые фрагменты текста:

	Советы, подсказки и другая полезная дополнительная информация
	Предупреждения и предостережения
	Строгие ограничения и запреты

Настоящий документ соответствует версии программного обеспечения (далее – ПО) МЭ ССПТ-4А1 1.0.0.

Информация о документе. Общая выходная информация о данном документе представлена в таблице 1, стр. 5.

Таблица 1: Сведения о документе

Наименование документа:	Межсетевой экран ССПТ-4А1. Руководство по эксплуатации
Номер документа:	ФРПС.466259.001 РЭ
Версия документа:	1.0.0.2 (последнее обновление 01.12.2022)
Всего листов:	589
Версия ПО МЭ ССПТ-4А1:	1.0.0
Организация-производитель:	© ООО "НПО "ФРАКТЕЛ", 2019-2022
Юридический адрес:	Ул. Курчатова, д. 10. Санкт-Петербург. 194223. Российская Федерация
Адрес производства:	Ул. Курчатова, д. 10. Санкт-Петербург. 194223. Российская Федерация
Телефон/Факс:	+7 812 406-83-92
Электронная почта:	info@fractel.ru
WWW:	http://www.fractel.ru

Содержание

Аннотация....3

Содержание....6

Список сокращений....13

1. Основные технические особенности и функциональные возможности....15

1.1. Назначение и область применения....15

1.2. Аппаратная платформа....16

1.3. Технология скрытной фильтрации....16

1.4. Основные функциональные характеристики МЭ ССПТ-4А1....16

1.4.1. Режим пакетной фильтрации....17
1.4.2. Режим управления сессиями....19
1.4.3. Функция трансляции сетевых адресов....21
1.4.4. Приоритетная обработка трафика....22
1.4.5. HTTP-посредник....23
1.4.6. Регистрация....24
1.4.7. Идентификация, аутентификация и разграничение доступа....27
1.4.8. Горячее резервирование....28
1.4.9. Контроль целостности....28
1.4.10. Агрегирование портов управляющего интерфейса....29

1.5. Управление МЭ ССПТ-4А1....29

1.5.1. Средства администрирования....29
1.5.2. Права доступа администраторов, идентификация и аутентификация....30
1.5.3. Управление конфигурациями....31
1.5.4. Управление политиками доступа....33
1.5.5. Средство обновления и восстановления....37

2. Подготовка к работе и первое включение....39

2.1. Комплект поставки....39

2.2. Маркировка и назначение разъемов, светодиодов и элементов управления. .39

2.3. Жидкокристаллический индикатор....41

2.4. Требования к управляющему компьютеру....45

2.5. Системная консоль....47

2.6. Первое включение....48

2.7. Подключение через управляющий Ethernet-интерфейс....51

2.7.1. Подключение к командному интерфейсу....52

2.7.2. Подключение к WEB-интерфейсу....53
2.8. Штатное выключение устройства....54
3. Принципы функционирования МЭ ССПТ-4А1....55
3.1. Основы использования командного интерфейса....55
3.1.1. Структура команды....55
3.1.2. Редактирование командной строки....56
3.1.3. Использование специальных символов в параметрах команд....57
3.1.4. Буфер истории команд....57
3.1.5. Получение контекстной справки....58
3.1.6. Режим автодополнения....59
3.1.7. Сеанс работы администратора....61
3.1.8. Настройка режима просмотра данных....62
3.1.9. Диагностические сообщения командного интерфейса....66
3.2. Режимы фильтрации МЭ ССПТ-4А1....66
3.2.1. Режим управления сессиями....67
3.2.2. Режим пакетной фильтрации....84
3.2.3. Функции трансляции сетевых адресов и аутентификации сетевых пользователей....87
3.2.4. Функция приоритетной обработки трафика....108
3.3. Контроль целостности....109
3.4. Разграничение прав доступа, идентификация и аутентификация....111
3.4.1. Идентификация и аутентификация администраторов и сетевых пользователей через RADIUS-сервер....111
3.5. Система фильтрации с резервированием на основе МЭ ССПТ-4А1....116
3.5.1. Резервирование МЭ ССПТ-4А1....116
3.5.2. Резервирование “активный-резервный” в режиме Master/Slave....117
3.5.3. Резервирование “активный-активный” в режиме Sync/Sync....124
3.5.4. Резервирование “активный-активный” в режиме Balance/Balance....129
3.5.5. Синхронизация текущей политики доступа....135
3.6. Политики доступа....137
3.7. Правила фильтрации....140
3.7.1. TMP-правила....141
3.7.2. Общие правила....142
3.7.3. AP-правила....147
3.7.4. Статистика использования правил фильтрации....150
3.8. Справочник объектов....153
3.9. HTTP-посредник МЭ ССПТ-4А1....159
3.9.1. Использование HTTP-посредника без NAT....160
3.9.2. Использование HTTP-посредника совместно с NAT....164

3.9.3. Использование PROXY-правил....169
3.9.4. Использование списка доступа (ACL) для ограничения доступа к HTTP-посреднику....170
3.10. Управление администраторами....171
3.11. Управление регистрацией....173
3.11.1. Регистрация событий....174
3.11.2. Регистрация трафика....177
3.11.3. Регистрация системных сообщений....184
3.11.4. Выгрузка журналов регистрации на FTP-сервер....185
3.11.5. Выгрузка записей регистрации на SYSLOG-сервер....187
3.12. Управление конфигурациями....188
3.13. Системные настройки....194
3.13.1. Настройки командного интерфейса....194
3.13.2. Просмотр системной информации....196
3.13.3. Просмотр информации о состоянии ресурсов УОС....198
3.13.4. Системные дата и время....199
3.13.5. Настройки управляющего интерфейса....202
3.13.6. Настройки фильтрующих интерфейсов....206
3.13.7. Установка списка DNS-серверов....210
3.13.8. Маршрутная таблица....211
3.13.9. Настройки использования интерфейсов удаленного администрирования....213
3.13.10. Перезагрузка и выключение устройства....214
3.13.11. Сброс настроек устройства....216
3.13.12. Просмотр ключевой информации....217
3.14. Агрегирование портов управляющего интерфейса....218
4. WEB-интерфейс администратора....223
4.1. Состояние....224
4.1.1. Состояние: Устройство....224
4.1.2. Состояние: Фильтрация....227
4.1.3. Состояние: Целостность....229
4.2. Настройки....230
4.2.1. Настройки: Устройство....231
4.2.2. Настройки: Администраторы....240
4.2.3. Настройки: Интерфейсы....244
4.2.4. Настройки: NAT....252
4.2.5. Настройки: Сетевые пользователи....267
4.2.6. Настройки: Регистрация....273
4.2.7. Настройки: Резервирование....277
4.2.8. Настройки: RADIUS....279
4.2.9. Настройки: Маршруты....281

4.2.10. Настройки: HTTP-посредник....283
4.3. Управление политиками доступа....287
4.3.1. Политика: Управление....288
4.3.2. Политика: Справочник....294
4.3.3. Политика: Правила....300
4.3.4. Политика: Статистика....324
4.4. Управление сессиями....325
4.4.1. Сессии: Настройки....326
4.4.2. Сессии: Таблица сессий....329
4.5. Регистрация....336
4.5.1. Регистрация: События....337
4.5.2. Регистрация: Пакеты....340
4.5.3. Регистрация: Сессии....347
4.6. Отладка....352
5. SNMP-интерфейс администратора....355
5.1. Предварительная настройка MIB-браузера snmpb....356
5.2. Работа с МЭ ССПТ-4А1. Примеры использования MIB-браузера snmpb....363
5.2.1. Авторизация администратора МЭ ССПТ-4А1....363
5.2.2. Вывод таблицы....367
5.2.3. Запрос значений всех переменных некоторого узла....369
5.2.4. Завершение сеанса работы администратора....371
6. Регламентное тестирование....375
7. Средство обновления и восстановления....394
7.1. Устройство....396
7.2. Восстановление....399
7.2.1. Проверка файловой системы носителя МЭ ССПТ-4А1....401
7.2.2. Восстановление ПО МЭ ССПТ-4А1....403
7.2.3. Функции сброса....405
7.3. Обновление....407
7.3.1. Получение файла обновления от производителя....408
7.3.2. Выполнение процедуры обновления ПО МЭ ССПТ-4А1....410
7.3.3. Журнал обновлений....413
7.3.4. Описание ошибок обновления....415
7.3.5. Отмена обновления....416
7.3.6. Подтверждение обновления....418
Приложение А. Требования к форматам данных и ограничения параметров конфигурации....423
А.1. Требования к форматам данных....423

А.2. Ограничения параметров конфигурации....428
Приложение Б. Перечень регистрируемых событий....431
Б.1. Информационные события МЭ ССПТ-4А1....431
Б.2. События категории предупреждений МЭ ССПТ-4А1....439
Б.3. События категории ошибок МЭ ССПТ-4А1....441
Приложение В. Перечень диагностических сообщений ПО МЭ ССПТ-4А1....443
В.1. Формат диагностических сообщений ПО МЭ ССПТ-4А1....443
В.2. Диагностические сообщения библиотеки сервисных функций ПО МЭ ССПТ-4А1....444
В.2.1. Сообщения об ошибках....444
В.2.2. Предупреждающие сообщения....457
В.3. Диагностические сообщения командного интерпретатора МЭ ССПТ-4А1....457
В.3.1. Сообщения об ошибках....457
В.3.2. Предупреждающие сообщения....482
В.3.3. Информационные сообщения....486
В.4. Диагностические сообщения командного сервера МЭ ССПТ-4А1....498
В.4.1. Сообщения об ошибках....498
Приложение Г. Командный язык МЭ ССПТ-4А1....501
Г.1. Группа команд “config”....501
Г.2. Группа команд “directory”....501
Г.3. Группа команд “filter”....502
Г.4. Группа команд “interface”....502
Г.5. Группа команд “log”....503
Г.6. Группа команд “nat”....504
Г.7. Группа команд “policy”....507
Г.8. Группа команд “reserv”....507
Г.9. Группа команд “rule”....508
Г.10. Группа команд “session”....509
Г.11. Группа команд “system”....511
Г.12. Группа команд “user”....512
Приложение Д. Определения правил фильтрации....514
Д.1. Определение общего правила....514

Д.1.1. Конфликты значений параметров общего правила....521
Д.1.2. Конфликты по адресам IPv4, IPv6, MAC....523
Д.1.3. Конфликты по остальным параметрам общего правила....525
Д.2. Определение AP-правила....527
Д.2.1. Дополнительные параметры AP-правила для протокола HTTP (protocol=http)....531
Д.2.2. Дополнительные параметры AP-правила для протокола FTP (protocol=ftp)....532
Д.2.3. Дополнительные параметры AP-правила для протокола SMTP (protocol=smtp)....533
Д.2.4. Дополнительные параметры AP-правила для SQL-сервисов (protocol=sql)....533
Д.2.5. Дополнительные параметры AP-правила для протокола DNS (protocol=dns либо protocol=domain)....533
Д.3. Определение TMP-правила....534
Д.4. Определение PRI-правила (правила приоритизации)....536
Д.5. Определение PROXY-правила (правила HTTP-посредника)....537
Д.6. Комментарий к группе правил....538
Приложение Е. Определения объектов справочника....540
Е.1. Определение объекта "Узел сети" (host)....540
Е.2. Определение объекта "Сеть" (net)....541
Е.3. Определение объекта "Группа сетевых объектов" (net-group)....542
Е.4. Определение объекта "Сервис" (service)....542
Е.5. Определение объекта "Ресурс" (resource)....543
Е.6. Определение объекта "Интервал времени" (time)....544
Е.7. Определение объекта "Группа доменных имён" (domain-group)....545
Е.8. Определение объекта "Группа VLAN" (vlan-group)....546
Приложение Ж. Дерево MIB-переменных SNMP-интерфейса МЭ ССПТ-4А1....547
Ж.1. Группа auth....547
Ж.2. Группа filter....548
Ж.3. Группа rulesStats....551
Ж.4. Группа system....555
Ж.4.1. Группа sysCpuStatus....559
Ж.4.2. Группа sysRamStatus....560

Ж.5. Группа user....561

Приложение З. Утилита аутентификации сетевого пользователя....565

З.1. Параметры командной строки....567

З.2. Переменные окружения....569

З.3. Примеры использования....569

З.4. Графическая оболочка утилиты аутентификации сетевого пользователя....570

З.4.1. Главное окно графической оболочки....570

З.4.2. Отправка запросов удаленному МЭ ССПТ-4А1....573

З.4.3. Использование конфигураций графической оболочки....575

Приложение И. Протокол управления МЭ ССПТ-4А1 FNPCP....578

И.1. Формат запросов к командному серверу МЭ ССПТ-4А1....578

И.2. Формат ответов от командного сервера МЭ ССПТ-4А1....579

И.3. Ответ командного сервера МЭ ССПТ-4А1 на запрос авторизации....580

И.4. Ответ командного сервера МЭ ССПТ-4А1 на запрос выполнения команд....581

Приложение К. Перечень диагностических сообщений ПО СОВа-4....583

К.1. Формат диагностических сообщений ПО СОВа-4....583

К.2. Диагностические сообщения ПО СОВа-4....584

К.2.1. Сообщения об ошибках....584

К.2.2. Предупреждающие сообщения....586

К.3. Статусы выполнения процедуры обновления ПО МЭ ССПТ-4А1....587

Список сокращений

АС – автоматизированная система

АСУ – автоматизированная система управления

ГИС – государственная информационная система

ЖКИ – жидкокристаллический индикатор

ИСПДн – информационная система персональных данных

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ПО – программное обеспечение

СОВа – средство обновления и восстановления

УК – управляющий компьютер

УОС – управляющая операционная система

ЦПУ – центральное процессорное устройство

ARP – Address Resolution Protocol

CSS – Cascading Style Sheets

DNS – Domain Name System

FNPCP – FNP Control Protocol

FTP – File Transfer Protocol

GRE – Generic Routing Encapsulation

HTML – HyperText Markup Language

HTTP – HyperText Transfer Protocol

ICMP – Internet Control Message Protocol

IP – Internet Protocol

MIB – Management Information Base

NAT – Network Address Translation

OSI – Open System Interconnection

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

SSH – Secure Shell

SQL – Structured Query Language

TCP – Transmission Control Protocol

TLS – Transport Layer Security

TTL – Time To Live

UDP – User Datagram Protocol

URL – Uniform Resource Locator

1. Основные технические особенности и функциональные возможности

1.1. Назначение и область применения

Межсетевой экран ССПТ-4А1 (далее – МЭ ССПТ-4А1) выполнен в виде локального (однокомпонентного) устройства, реализующего контроль за информацией, которая циркулирует между отдельными подсистемами обработки информации внутри автоматизированной системы (далее – АС) и/или между АС. МЭ ССПТ-4А1 обеспечивает защиту информации в АС посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения об ее распространении в/из АС. МЭ ССПТ-4А1 используется для защиты АС, в которых обрабатывается информация одинакового предельно допустимого уровня конфиденциальности или секретности.

МЭ ССПТ-4А1 применяется для разделения сегментов информационной сети внутри или между ГИС 1 класса защищенности, АСУ 1 класса защищенности, ИСПДн 1 уровня защищенности, информационных системах общего пользования II класса, с целью обеспечения защиты информации от несанкционированного доступа (далее – НСД) посредством:

- **фильтрации сетевых пакетов**, передаваемых в ЛВС внутри АС или между АС. Фильтрация пакетов (передача пакета в защищаемую ЛВС или из неё, или запрет передачи – удаление пакета) осуществляется на основе анализа параметров заголовков пакета по совокупности критериев, устанавливаемых правилами фильтрации для разных уровней модели взаимодействия открытых систем (*OSI – Open System Interconnection*);
- **управления виртуальными транспортными соединениями** между отдельными узлами ЛВС внутри или между АС. Управление виртуальными транспортными соединениями (разрешение или запрет соединения) осуществляется на основе результатов анализа параметров соединений и/или запросов на установление соединений;
- **контроля данных**, передаваемых на прикладном уровне модели OSI. Контроль данных (анализ данных и их передача или запрет передачи) осуществляется по заданным критериям, в том числе, с учетом направления потока данных.

Реализация МЭ ССПТ-4А1 предусмотрена на ряде аппаратных средств, в виде исполнений, отличающихся друг от друга типоразмерами корпуса, количеством и пропускной способностью фильтрующих интерфейсов.

МЭ ССПТ-4А1 может использоваться в ЛВС, построенных на базе технологии Ethernet (IEEE802.3) с пропускной способностью 10/100/1000 Мбит/с и 10 Гбит/с.

1.2. Аппаратная платформа

МЭ ССПТ-4А1 является программно-аппаратным комплексом, реализованном на базе вычислительной архитектуры, совместимой с семейством 64-битных процессоров (x86_64, EMT64T) Intel® Core®.

В зависимости от варианта исполнения МЭ ССПТ-4А1 может быть оснащен от **5** до **15** фильтрующими сетевыми интерфейсами, поддерживающими технологию Ethernet со скоростями передачи 10/100/1000 Мбит/с или 10 Гбит/с.

1.3. Технология скрытной фильтрации

Эффективность применения МЭ ССПТ-4А1 достигается за счет использования *технологии скрытной фильтрации* (режим “*stealth*”) – инновационного решения, защищенного Патентом РФ № 2214623, позволяющего скрывать для средств удаленного сетевого мониторинга место расположения МЭ ССПТ-4А1, что повышает надежность функционирования и позволяет эффективно наращивать производительность системы информационной безопасности.

Основная особенность применения режима *полного скрытного контроля трафика* (*full stealth inspection*) состоит в том, что фильтрующим интерфейсам межсетевого экрана не назначаются логические (IP) адреса, а в процессе обработки пакетов не используются физические (MAC) адреса этих интерфейсов.

В результате, в этом режиме МЭ ССПТ-4А1:

- не изменяет параметров проходящих через него пакетов и не требует при своей установке специальной настройки других сетевых устройств;
- не подвержен воздействию компьютерных атак;
- может использоваться для реализации политики безопасности на основе комбинации правил фильтрации и контроля сетевых соединений.

1.4. Основные функциональные характеристики МЭ ССПТ-4А1

МЭ ССПТ-4А1 обеспечивает реализацию двух основных режимов фильтрации сетевых пакетов:

1) режим **пакетной фильтрации**;
2) режим **управления сессиями**.

МЭ ССПТ-4А1 реализует следующие функциональные возможности:

- трансляция сетевых адресов (функция NAT);
- аутентификация сетевых пользователей;
- приоритетная обработка трафика;
- HTTP-посредник;
- регистрация событий, трафика и системных сообщений;
- идентификация, аутентификация и разграничение доступа администраторов;
- горячее резервирование;
- контроль целостности программных компонентов МЭ ССПТ-4А1;
- агрегирование портов управляющего интерфейса.

1.4.1. Режим пакетной фильтрации

В режиме пакетной фильтрации МЭ ССПТ-4А1 реализует процедуру независимого анализа каждого принятого сетевого пакета по совокупности критериев и принятие решения о разрешении или запрете передачи пакета в защищаемый сегмент сети или из него на основе заданной политики доступа.

Пакетная фильтрация осуществляется на различных уровнях сетевого взаимодействия по полям заголовков сетевых пакетов следующих типов:

- кадры Ethernet следующих форматов:
  - ✔ Ethernet II;
  - ✔ IEEE 802.2/LLC;
  - ✔ IEEE-802.2/SNAP;
  - ✔ IEEE 802.3-raw;
- пакетов IPv4 и IPv6, инкапсулированных в кадры Ethernet форматов Ethernet II или IEEE-802.2/SNAP;
- пакетов ICMPv4 и ICMPv6, инкапсулированных в кадры Ethernet форматов Ethernet II или IEEE-802.2/SNAP;
- дейтаграмм UDP, инкапсулированных в пакеты IPv4 или IPv6;
- сегментов TCP, инкапсулированных в пакеты IPv4 или IPv6.

В правилах фильтрации предусмотрены следующие действия над обработанным пакетом:

1) **удалить** пакет (действие “**drop**”) – пакет не будет передан ни на один из фильтрующих интерфейсов МЭ ССПТ-4А1;
2) **удалить с уведомлением** (действие “**deny**”) – удаление пакета с отправкой клиенту пакета-уведомления (TCP-сегмента с флагом RST для протокола TCP, ICMP-сообщения – для

остальных протоколов);

3) **пропустить пакет** (действие “**accept**”) – пакет будет передан на фильтрующие интерфейсы МЭ ССПТ-4А1 в соответствии с маской выходных интерфейсов, определяемой правилами фильтрации, которые были применены к данному пакету;

4) **перейти к правилу** (действие “**goto**”) – пакет будет передан на обработку общему правилу с указанным номером (номер правила, которому передается пакет, должен быть больше, чем номер данного правила с действием “goto”).

Правила фильтрации хранятся в МЭ ССПТ-4А1 в виде таблиц и **однозначно идентифицируются своим номером**.

При фильтрации каждого пакета правила фильтрации просматриваются **в порядке возрастания их номеров** до выполнения одного из следующих условий:

- найдено правило фильтрации, параметры которого соответствуют заголовку пакета. В этом случае просмотр правил прекращается и указанное правило применяется к данному пакету (действие правила должно быть отличным от “**goto**”);
- достигнут конец таблицы правил фильтрации. В этом случае к данному пакету применяется **глобальное правило фильтрации**.

Канальный уровень. На канальном уровне сетевого взаимодействия обеспечивается фильтрация по следующим полям заголовков пакетов:

- для кадров Ethernet форматов **Ethernet II**, **IEEE 802.3-LLC**, **IEEE 802.3-SNAP**, **IEEE 802.3-raw**:
  - ✔ MAC-адреса отправителя/получателя;
  - ✔ код протокола, инкапсулированного в кадр Ethernet (*кроме IEEE 802.3-raw*);
- для стандарта **IEEE 802.1p/Q** (VLAN):
  - ✔ идентификатор VLAN.

Сетевой уровень. На сетевом уровне взаимодействия обеспечивается фильтрация по следующим полям заголовков пакетов:

- для протокола **IPv4**:
  - ✔ IP-адреса отправителя/получателя;
  - ✔ поле флагов TOS;
  - ✔ длина IP-пакета;
  - ✔ фрагментация пакета (*разрешена/запрещена*, *используется/не используется* для данного пакета);
  - ✔ время жизни пакета (*TTL – Time To Live*);
  - ✔ код протокола верхнего уровня;
- для протокола **IPv6**:
  - ✔ IP-адреса отправителя/получателя;
  - ✔ поле “Traffic Class”;

✔ поле “Hop Limit” (аналог TTL в IPv4);

✔ фрагментация пакета (*разрешена/запрещена*, *используется/не используется* для данного пакета);

✔ наличие/отсутствие дополнительных заголовков IPv6;

✔ код протокола верхнего уровня;

- для протокола **ICMP** (**ICMPv4** и **ICMPv6**):

✔ тип ICMP-сообщения;

✔ код ICMP-сообщения.

Транспортный уровень. Обеспечивается фильтрация следующих протоколов транспортного уровня, использующих на сетевом уровне протокол IPv4 или IPv6:

- для протокола **TCP**:

✔ номер порта источника;

✔ номер порта назначения;

✔ флаги управления потоком (*фильтрация по инициатору соединения*);

- для протокола **UDP**:

✔ номер порта источника;

✔ номер порта назначения.

1.4.2. Режим управления сессиями

В режиме управления сессиями МЭ ССПТ-4А1 реализует процедуры выявления в общем сетевом трафике виртуальных соединений между парами адресатов (*клиент* – инициатор соединения, *сервер* – второй участник виртуального соединения) и контроля корректности последовательностей пакетов в пределах данного виртуального соединения (*контроль сессий*).

В режиме управления сессиями по правилам фильтрации проверяется **только первый пакет каждого виртуального соединения**. Если он не отбрасывается, то создаётся виртуальная сессия и последующие пакеты проверяются на принадлежность этой сессии и на соответствие текущему состоянию сессии.

Контроль сессий поддерживается для следующих протоколов:

- для протоколов **ICMPv4**, **ICMPv6** (для режима утилиты ping “*echo-запрос/echo-ответ*”):

✔ контроль неизменности параметров (адреса, идентификатор в заголовке ICMP) клиента и сервера на протяжении всей сессии;

Механизм контроля сессий поддерживает следующие комбинации типов и кодов ICMP-сообщений:

- для ICMPv4:
  - ✔ тип: 8, код: 0 (echo-запрос);
  - ✔ тип: 0, код: 0 (echo-ответ);
- для ICMPv6:
  - ✔ тип: 128, код: 0 (echo-запрос);
  - ✔ тип: 129, код: 0 (echo-ответ);
  - ✔ тип: 135, код: 0 (neighbor solicitation);
  - ✔ тип: 136, код: 0 (neighbor advertisement);
  - ✔ тип: 137, код: 0 (redirect message).

- для протокола **UDP**:
  - ✔ контроль неизменности параметров (адреса, порты, интерфейсы) клиента и сервера на протяжении всей сессии;
- для протокола **TCP**:
  - ✔ контроль неизменности параметров (адреса, порты, интерфейсы) клиента и сервера на протяжении всей сессии;
  - ✔ контроль корректности переходов между состояниями виртуального TCP-соединения в соответствии с флагами управления;
  - ✔ контроль корректности номеров последовательностей;
- **TRACEROUTE** (трассировка маршрутов на базе протоколов ICMP, UDP или TCP):
  - ✔ контроль неизменности параметров (адреса, идентификатор в заголовке ICMP) клиента и сервера на протяжении всей сессии (для протокола ICMP);
  - ✔ контроль неизменности параметров (адреса, порты, интерфейсы) клиента и сервера на протяжении всей сессии (для протоколов UDP или TCP);
- **GRE** (туннелирование сетевых пакетов):
  - ✔ контроль неизменности параметров (адреса, интерфейсы) клиента и сервера на протяжении всей сессии;
- для **остальных протоколов**, работающих поверх протоколов IPv4 или IPv6, реализуется контроль неизменности IP-адресов и фильтрующих интерфейсов клиента и сервера.

В зависимости от заданных настроек режима управления сессиями для всех типов сессий может выполняться контроль неизменности *MAC-адреса* клиента и сервера, а также *номера VLAN*.

В режиме управления сессиями МЭ ССПТ-4А1 реализует процедуру контроля данных, передаваемых на прикладном уровне стека протоколов TCP/IP, с учетом критериев фильтрации на основе значений полей заголовков следующих прикладных протоколов:

- для протокола **HTTP**:
  - ✔ фильтрация по адресам и фрагментам URL;
  - ✔ фильтрация по именам и фрагментам имен передаваемых файлов;

✔ фильтрация по данным заголовка протокола HTTP;

- для протокола **FTP**:

✔ фильтрация по командам протокола FTP – GET, PUT;

✔ фильтрация по идентификатору и паролю пользователя;

✔ фильтрация по именам и фрагментам имен передаваемых файлов;

✔ фильтрация по данным заголовка протокола FTP;

- для протокола **SMTP**:

✔ фильтрация по почтовым адресам отправителя/получателя;

✔ фильтрация по данным заголовка протокола SMTP;

- для протокола службы **DNS**:

✔ фильтрация по запрашиваемым доменным именам;

- для протоколов передачи **SQL**-запросов (SQL*Net, MS-SQL, PostgreSQL, MySQL):

✔ фильтрация по SQL-запросам или их фрагментам.

В режиме управления сессиями МЭ ССПТ-4А1 дополнительно реализует следующие функциональные возможности:

- выявление и блокирование ряда **DoS-атак**, таких как:

✔ удаленная сетевая атака типа ICMP-flood;

✔ удаленная сетевая атака типа UDP-flood;

✔ атака с помощью переполнения SYN-пакетами в рамках протокола TCP (SYN-flood);

- функция **трансляции сетевых адресов** (*NAT – Network Address Translation*).

1.4.3. Функция трансляции сетевых адресов

Функция трансляции сетевых адресов NAT в МЭ ССПТ-4А1 обеспечивает следующие возможности:

- реализация обратимого преобразования (трансляции) сетевых адресов с целью сокрытия адресов и топологии защищаемых сегментов сети;
- реализация переадресации внешних сетевых запросов к сервисам, расположенным в сегментах внутренней сети;
- аутентификация сетевых пользователей;
- поддержка динамического ARP (*ARP – Address Resolution Protocol*);
- поддержка статических маршрутов для сетевого протокола IPv4.

Работа NAT возможна только при **включенном режиме управления сессиями**.

Существуют следующие ограничения на работу NAT в МЭ ССПТ-4А1:
- на сетевом уровне модели OSI NAT поддерживает только протоколы IPv4, ARP и ICMP;
- на внешние интерфейсы возможна передача только TCP, UDP и ICMP пакетов с типом 8;
- запрещена передача фрагментированных пакетов при использовании функции NAT.

Для поддержки NAT в МЭ ССПТ-4А1 используются понятие *виртуального контейнера NAT*, представляющего собой совокупность настроек и параметров NAT, применяемых к выделенному набору фильтрующих интерфейсов МЭ. Контейнер NAT может содержать следующие параметры:

- имя контейнера;
- список внешних интерфейсов NAT с назначенными на них IP-адресами;
- список внутренних интерфейсов NAT с назначенными на них IP-адресами;
- таблица статических маршрутов;
- правила трансляции;
- правила переадресации.

IP-адреса внутренних и внешних интерфейсов физически не привязаны к фильтрующим интерфейсам, а являются виртуальными и используются для реализации NAT только на уровне ПО МЭ ССПТ-4А1.

Правила трансляции предоставляют возможность выбора сегментов защищенной сети, которым разрешено обращение во внешнюю сеть, а так же назначения IP-адреса отправителя для подобных обращений.

Правила переадресации предоставляют возможность доступа к публичным ресурсам, расположенным в защищенном сегменте сети.

В случае достаточного количества фильтрующих интерфейсов существует возможность создания несколько контейнеров NAT, позволяющих реализовать независимые политики NAT в рамках одного устройства МЭ ССПТ-4А1. Также существует возможность настройки контейнера NAT для части фильтрующих интерфейсов, в то время, как для оставшейся части интерфейсов функция NAT будет отключена.

1.4.4. Приоритетная обработка трафика

Настройка приоритизации трафика позволяет по некоторым параметрам выделять приоритетный трафик и обеспечивать его передачу с более высокой скоростью, или же, напротив, замедлять передачу трафика, скорость которого некритична.

Приоритетная обработка реализована посредством алгоритма взвешенных очередей, что подразумевает предоставление определенного минимума пропускной способности для всех

классов трафика, включая трафик с низким приоритетом. Весовые коэффициенты для каждого из приоритетов фиксированы, их значения приведены в разделе 3.2.4, стр. 108.

Включение приоритетной обработки трафика имеет смысл в случае, если предполагается высокая нагрузка на МЭ ССПТ-4А1. В случае низкой нагрузки, высока вероятность неравномерной загрузки ядер процессора устройства МЭ ССПТ-4А1, что снизит эффект от использования приоритетной обработки трафика.

Настройка приоритетной обработки трафика возможна только при **включенном режиме управления сессиями**.

Существуют следующие ограничения на приоритетную обработку трафика в МЭ ССПТ-4А1:
- приоритетная обработка возможна только для пакетов IPv4 и IPv6;
- приоритетная обработка не применима к фрагментированному трафику.

Поддерживается возможность назначения следующих трех значений приоритета для обрабатываемого трафика:

- высокий приоритет;
- базовый приоритет;
- низкий приоритет.

По умолчанию для всего трафика используется базовый приоритет. Задать другое значение приоритета для части трафика можно путем добавления правил в список правил приоритизации. Правила приоритизации могут содержать следующие параметры:

- входной интерфейс;
- IP-адрес источника;
- IP-адрес приемника;
- порт источника;
- порт приемника;
- номер протокола, инкапсулированного в IP;
- значение приоритета;
- номер правила приоритизации.

Так как базовый приоритет назначается для всего трафика по умолчанию, в правилах приоритетной обработки возможно задавать только *высокий* и *низкий приоритет* для выбранного трафика.

1.4.5. HTTP-посредник

HTTP-посредник МЭ ССПТ-4А1 представляет собой прокси-сервер для протоколов HTTP и HTTPs.

HTTP-посредник позволяет пользователям корпоративной сети выполнять косвенные запросы к Web-серверам, тем самым обеспечивая анонимность пользователей. Сначала Web-браузер пользователя подключается к HTTP-посреднику и запрашивает Web-страницу, расположенную на Web-сервере в корпоративной сети или в сети Интернет. Затем HTTP-посредник подключается к указанному Web-серверу (открывает новое соединение, в котором выступает клиентом), получает от него Web-страницу и возвращает ее Web-браузеру в рамках соединения, открытого пользователем корпоративной сети.

Конфигурация по умолчанию HTTP-посредника обеспечивает доступ клиента ко всем Web-сайтам, доступным при прямом подключении клиента к ним, и не модифицирует ответы Web-серверов.

Основные возможности HTTP-посредника МЭ ССПТ-4А1:

- блокировка доступа клиентов к определенным Web-страницам по доменным именам;
- удаление сценариев JavaScript, VBScript для определенных Web-страниц с заданными доменным именами;
- ограничение доступа клиентов к HTTP-посреднику на основе списка доступа (ACL).

HTTP-посредник МЭ ССПТ-4А1 может использоваться как с выключенной, так и с включенной функцией NAT.

1.4.6. Регистрация

В МЭ ССПТ-4А1 реализована подсистема регистрации, обеспечивающая хранение регистрационной информации следующих категорий:

- события;
- трафик;
- системные сообщения.

Обеспечивается возможность выгрузки на удаленный FTP-сервер следующих файлов:

- журнала регистрации событий;
- журнала регистрации трафика (пакеты и сессии).

Обеспечивается возможность выгрузки на удаленный SYSLOG-сервер записей регистрации (текстовых сообщений) следующих категорий:

- события;
- пакеты;
- сессии.

Регистрация событий. Событие отражает факт изменения состояния, конфигурационных параметров либо режима функционирования МЭ ССПТ-4А1, произошедших в результате действий администраторов или вследствие возникновения сбоев или ошибок в работе МЭ ССПТ-4А1. Подсистема регистрации МЭ ССПТ-4А1 обеспечивает регистрацию следующих событий:

- вход/выход администратора;
- загрузка и инициализация УОС МЭ ССПТ-4А1 и ее останов;
- действия администратора по изменению и загрузке политик доступа;
- действия администратора по изменению конфигурационных параметров МЭ ССПТ-4А1;
- действия администратора по управлению МЭ ССПТ-4А1 (запуск/останов пакетного фильтра, сброс файлов регистрации и т. д.).

При регистрации события указывается:

- дата и время регистрируемого события с учетом часового пояса;
- код и описание события;
- идентификатор администратора МЭ ССПТ-4А1, действия которого привели к регистрации данного события;
- IP-адрес управляющего компьютера в случае удаленного администрирования.

Регистрируемые в МЭ ССПТ-4А1 события подразделяются на три категории:

1) **информационные события** – события извещающие об успешных действиях администраторов МЭ ССПТ-4А1, других стандартных событиях, характерных для текущего режима работы МЭ ССПТ-4А1;
2) **предупреждения** – события, не нарушающие нормального функционирования ПО МЭ ССПТ-4А1, однако являющихся нестандартными или некорректными;
3) **ошибки** – события, являющиеся критическими и нарушающие работу ПО МЭ ССПТ-4А1.

Формат представления событий и их полный перечень с описанием приводится в Приложении Б, стр 431.

МЭ ССПТ-4А1 может одновременно хранить до **6000** записей о зарегистрированных событиях.

В МЭ ССПТ-4А1 производится циклическое обновление записей о зарегистрированных событиях. Таким образом, наиболее старые записи переписываются вновь регистрируемыми.

Интерфейсы администратора, такие как командный интерфейс и WEB-интерфейс, при выводе сообщений предоставляют возможность отбора записей по установленным критериям, а также их сортировки по времени регистрации события. Могут использоваться следующие критерии отбора регистрационных записей:

- категория события;
- код события;
- интервал времени регистрации события;
- порядок сортировки при выводе списка событий в зависимости от времени регистрации события.

Регистрация трафика. Информация о трафике подразделяется на следующие категории:

- **пакеты** – информация о сетевых пакетах, обработанных МЭ ССПТ-4А1 в соответствии с действующей политикой доступа. Информация о каждом зарегистрированном пакете представляется в виде иерархической структуры, включающей информацию от канального до прикладного уровня;
- **сессии** – информация о сессиях, обработанных МЭ ССПТ-4А1.

Подсистема регистрации обеспечивает регистрацию трафика с сохранением следующих основных параметров:

- время регистрации пакета или сессии с точностью до микросекунды;
- номер входного и выходного фильтрующих интерфейсов МЭ ССПТ-4А1;
- цепочка правил фильтрации, по которым был обработан пакет (*при регистрации пакета*) или идентификатор сессии (*при регистрация сессии*);
- действие, выполненное над пакетом в результате его обработки;
- протокольные заголовки всех уровней, присутствующих в пакете (*при регистрации пакета*);
- данные о параметрах сессии (*при регистрации сессии*).

МЭ ССПТ-4А1 может одновременно хранить до **10000** записей о зарегистрированных пакетах/сессиях.

В МЭ ССПТ-4А1 производится циклическое обновление записей о зарегистрированных пакетах/сессиях. Таким образом, наиболее старые записи переписываются вновь регистрируемыми.

Регистрация системных сообщений. МЭ ССПТ-4А1 имеют возможность регистрации сообщений, используя службу системных сообщений (SYSLOG) УОС МЭ ССПТ-4А1. Зарегистрированные сообщения помещаются в файлы системных журналов УОС, возможность просмотра содержимого которых предоставляют средства администрирования.

Контроль размеров и управление ротацией файлов системных журналов осуществляет УОС МЭ ССПТ-4А1

Максимальный размер файла системного журнала для хранения системных сообщений, поступающих от подсистем ПО МЭ ССПТ-4А1, составляет **100 Мбайт**.

В файле системного журнала УОС МЭ ССПТ-4А1 каждое сообщение занимает отдельную текстовую строку. Например:

```
Dec 23 11:37:35 fnp4 fnp4[1266]: fnp4_filtd: Пакетный фильтр готов к работе (PID 1266)
```

Строка системного сообщения в общем случае состоит из следующих элементов:

- дата и время регистрации системного сообщения (`Dec 23 11:37:35`);
- префикс системного сообщения. Все системные сообщения, отправляемые подсистемами ПО МЭ ССПТ-4А1, имеют префикс `fnp4`;
- номер прикладного процесса УОС МЭ ССПТ-4А1, отправившего данное сообщение (`1266`);
- имя подсистемы ПО МЭ ССПТ-4А1, отправившей данное сообщение (`fnp4_filtd` – процесс пакетного фильтра МЭ ССПТ-4А1);
- текст сообщения.

1.4.7. Идентификация, аутентификация и разграничение доступа

В МЭ ССПТ-4А1 реализована подсистема авторизации, обеспечивающая идентификацию и аутентификацию администраторов МЭ ССПТ-4А1 при локальных и удаленных запросах.

Каждый администратор МЭ ССПТ-4А1 имеет личный идентификатор, на основании которого определяются его права по управлению изделием. Права администратора определяются уровнем прав доступа, хранящимся в его учетной записи.

Подсистема авторизации обеспечивает два способа аутентификации администраторов МЭ ССПТ-4А1:

1) локальная аутентификация, использующая информацию из файла учетных записей администраторов, хранящегося на файловой системе устройства;
2) удаленная аутентификация с обращением к удаленному серверу аутентификации с использованием протокола RADIUS.

При использовании средств удаленного администрирования поддерживаются списки доступа на основе IP-адресов управляющих компьютеров.

Дополнительно подсистема авторизации реализует обработку запросов на аутентификацию сетевых пользователей, используя перечисленные выше способы.

1.4.8. Горячее резервирование

В МЭ ССПТ-4А1 реализована подсистема резервирования, позволяющая повысить надежность выполнения функций по защите информации и разграничению доступа к информационным ресурсам.

В схеме резервирования используется два устройства МЭ ССПТ-4А1, работающих в одном из следующих режимов:

- режим **Master** – роль “Активный” в схеме “Активный-Резервный”: все фильтрующие интерфейсы МЭ ССПТ-4А1 устанавливаются в активное состояние;
- режим **Slave** – роль “Резервный” в схеме “Активный-Резервный”: все фильтрующие интерфейсы МЭ ССПТ-4А1 устанавливаются в заблокированное состояние;
- режим **Sync** – роль МЭ ССПТ-4А1 в схеме “Активный-Резервный” определяется настройками протоколов STP/RSTP на коммутаторах, к которым подключены фильтрующие интерфейсы МЭ ССПТ-4А1;
- режим **Balanace** – режим, используемый для схемы “Балансировка нагрузки”: на коммутаторах, к которым подключены фильтрующие интерфейсы МЭ ССПТ-4А1, должны быть выполнены соответствующие настройки по агрегированию портов.

В подсистеме резервирования МЭ ССПТ-4А1 реализована возможность выполнения процедуры синхронизации действующей политики доступа как в автоматическом, так и в ручном режимах.

1.4.9. Контроль целостности

В МЭ ССПТ-4А1 реализована подсистема контроля целостности основных компонентов УОС МЭ ССПТ-4А1, подсистем ПО МЭ ССПТ-4А1 и всех конфигурационных файлов. Контроль целостности осуществляется на основе периодической проверки контрольных сумм файлов, содержащих перечисленные выше компоненты. Таким образом, подсистема контроля целостности выявляет попытки несанкционированного изменения исполняемых файлов (и библиотек) подсистем МЭ ССПТ-4А1 и конфигурационных файлов путем прямого редактирования, минуя использование штатных средств администрирования МЭ ССПТ-4А1.

При обнаружении нарушения контрольной суммы подсистема контроля целостности выполнит следующие действия:

1) останов пакетного фильтра МЭ ССПТ-4А1;

2) регистрация события о нарушении контрольной суммы с указанием имени файла;

3) перевод подсистемы авторизации в однопользовательский режим работы – доступ администратора к МЭ ССПТ-4А1 будет возможен только для администратора с идентификатором “`admin`”.

1.4.10. Агрегирование портов управляющего интерфейса

МЭ ССПТ-4А1 поддерживает функцию **агрегирования портов управляющего интерфейса**. Данная функция позволяет организовать **агрегат**, включающий в себя управляющий интерфейс и один из фильтрующих интерфейсов. Агрегирование портов управляющего интерфейса обеспечивает резервирование управляющего интерфейса МЭ ССПТ-4А1: если выходит из строя один из интерфейсов, входящих в состав агрегата, то будет использоваться второй интерфейс. Поддерживается возможность совместного использования обоих интерфейсов в составе агрегата. Режим использования интерфейсов в составе агрегата определяется **протоколом агрегирования**, который может быть изменен администратором МЭ ССПТ-4А1.

Поддерживаются следующие протоколы агрегирования:

- **`failover`**: трафик передается только через активный порт (основной (master) порт - первый порт в агрегате). **Протокол агрегирования по умолчанию**;
- **`broadcast`**: отправляет кадры на все порты агрегата и принимает кадры на любой порт агрегата;
- **`lacp`**: поддерживает IEEE 802.1AX (ранее 802.3ad) Link Aggregation Control Protocol (LACP), а также Marker Protocol;
- **`loadbalance`**: балансировка исходящего трафика на основе хеширования заголовков пакетов и прием входящего трафика на любой из активных портов агрегата;
- **`roundrobin`**: распределение исходящего трафика между всеми активными портами, используя планировщик типа round-robin и прием входящего трафика на любой из активных портов агрегата.

1.5. Управление МЭ ССПТ-4А1

1.5.1. Средства администрирования

Администратору МЭ ССПТ-4А1 предоставляются следующие средства администрирования:

- **командный интерфейс администратора** как для локального (с *системной консоли* МЭ ССПТ-4А1), так и для удаленного администрирования в режиме командной строки;

- **WEB-интерфейс администратора** для удаленного администрирования МЭ ССПТ-4А1 с использованием стандартного WEB-браузера, поддерживающего протокол HTTPS;
- **SNMP-интерфейс администратора** для удаленного мониторинга состояния МЭ ССПТ-4А1 с использованием специального программного обеспечения на стороне управляющего компьютера, например, относящегося к классу SNMP MIB-браузеров, поддерживающих протокол SNMP версии 3;
- **FNPCP-интерфейс администратора** для удаленного администрирования с использованием клиентских приложений, функционирующих на стороне управляющего компьютера или других средств защиты информации и поддерживающих прикладной протокол FNPCP. Описание протокола FNPCP приведено в Приложении И, стр. 578.

В зависимости от исполнения в качестве системной консоли может использоваться:
1) **VGA монитор / клавиатура** – к МЭ ССПТ-4А1 необходимо подключить VGA-совместимый монитор и USB-клавиатуру к разъемам **VGA** (15-контактный гнездовой разъем D-SUB) и **USB** (разъем USB тип A) соответственно;
2) **управляющий компьютер** – к COM-порту МЭ ССПТ-4А1 необходимо подключить управляющий компьютер, используя нуль-модемный кабель (входит в комплект поставки). В этом случае управляющий компьютер взаимодействует с МЭ ССПТ-4А1 по последовательному порту RS-232 с использованием *программы-эмулятора терминала*.

Требования к управляющему компьютеру, используемому для управления МЭ ССПТ-4А1, изложены в разделе 2.4, стр. 45.

1.5.2. Права доступа администраторов, идентификация и аутентификация

МЭ ССПТ-4А1 обеспечивает разграничение прав доступа администраторов по управлению настройками и функционированием устройства. При этом, для каждой учетной записи администратора предусматриваются следующие уровни прав доступа:

- `admin` – обеспечивает возможности просмотра и управления параметрами, ресурсами, состоянием, учетными записями, политиками доступа и регистрационной информацией МЭ ССПТ-4А1;

Уровень прав доступа `admin` по умолчанию может быть назначен только администратору с идентификатором `admin`.

Возможность назначения данного уровня доступа администраторам с другими идентификаторами заблокирована.

- `full` – обеспечивает возможности, аналогичные уровню прав доступа `admin`, за исключением возможности управления учетными записями других администраторов. Для своей учетной записи уровень прав доступа `full` позволяет выполнять только изменение пароля;

- `read` – обеспечивает возможности просмотра параметров, ресурсов и регистрационной информации МЭ ССПТ-4А1. Для своей учетной записи уровень прав доступа `read` позволяет выполнять только изменение пароля.

МЭ ССПТ-4А1 обеспечивает идентификацию и аутентификацию администратора при его локальных (*командный интерфейс администратора с системной консоли*) и удаленных запросах (все средства администрирования, перечисленные в разделе 1.5.1, стр. 29) на доступ по идентификатору и паролю условно-постоянного действия.

Каждый администратор имеет личный идентификатор, на основании которого определяются его права по администрированию МЭ ССПТ-4А1. Права администратора определяются уровнем прав доступа, хранящимся в его учетной записи.

В МЭ ССПТ-4А1 предусмотрены два типа идентификации и аутентификации администраторов:

1) локальная аутентификация;
2) удаленная аутентификации с использованием удаленного RADIUS-сервера.

МЭ ССПТ-4А1 обеспечивает возможность управления учетными записями администраторов МЭ ССПТ-4А1. В *файле учетных записей администраторов* МЭ ССПТ-4А1 определена учетная запись администратора с идентификатором `admin`, *которая не может быть удалена*.

Администратору с идентификатором `admin` назначены права доступа `admin`, которые не могут быть изменены.

При использовании средств удаленного администрирования в МЭ ССПТ-4А1 поддерживаются списки доступа на основе IP-адресов управляющих компьютеров.

Идентификация и аутентификация администраторов при использовании удаленного доступа через SNMP-интерфейс имеет свои особенности и рассматривается отдельно (раздел 5, стр. 355).

1.5.3. Управление конфигурациями

Параметры настройки и функционирования МЭ ССПТ-4А1 (далее – параметры конфигурации) хранятся в *конфигурациях*. В МЭ ССПТ-4А1 существует два типа конфигураций:

1) **текущая конфигурация** – набор параметров настройки и функционирования МЭ ССПТ-4А1, которые в данный момент задействованы в процессе функционирования программных

компонентов ПО и УОС МЭ ССПТ-4А1;

2) **дополнительные конфигурации** – именованные наборы параметров настройки и функционирования, которые хранятся в МЭ ССПТ-4А1 и могут быть использованы для резервного копирования текущей конфигурации с возможностью *выгрузки/загрузки дополнительных конфигураций на управляющий компьютер*. Каждой дополнительной конфигурации присваивается *символическое имя, уникальное для данного устройства МЭ ССПТ-4А1*.

В МЭ ССПТ-4А1 существуют следующие ограничения при работе с дополнительными конфигурациями:

- МЭ ССПТ-4А1 может хранить не более **16** дополнительных конфигураций;
- имя дополнительной конфигурации должно отвечать следующим требованиям:
  - ✔ длина имени – от **1** до **251** символа;
  - ✔ допустимые символы в имени – **латинские буквы** (**`a-z`**, **`A-Z`**), **цифры** (**`0-9`**), символы '_' (подчеркивание), '**`-`**' (дефис) и '**`.`**' (точка);
  - ✔ имя дополнительной конфигурации *должно начинаться с латинской буквы, либо с цифры*;
  - ✔ в имени дополнительной конфигурации *не допускается наличие двух символов '`.`' (точка) подряд*;

МЭ ССПТ-4А1 обеспечивает следующие возможности по управлению конфигурациями:

- просмотр текущей или дополнительной конфигурации;
- сохранение текущей конфигурации в дополнительную;
- загрузка выбранной дополнительной конфигурации в текущую (далее – *применение дополнительной конфигурации*);
- удаление дополнительной конфигурации;
- загрузка с управляющего компьютера на МЭ ССПТ-4А1 дополнительной конфигурации;
- выгрузка с МЭ ССПТ-4А1 на управляющий компьютер текущей или дополнительной конфигурации;
- изменение имени и комментария дополнительной конфигурации (далее – *переименование дополнительной конфигурации*);
- отображение списка существующих на МЭ ССПТ-4А1 дополнительных конфигураций;
- применение конфигурации по умолчанию.

Дополнительные конфигурации, выгружаемые на управляющий компьютер, хранятся в текстовых файлах в формате XML.

МЭ ССПТ-4А1 осуществляет контроль корректности дополнительной конфигурации, загружаемой с управляющего компьютера. В случае обнаружения ошибок загрузка дополнительной конфигурации блокируется с выдачей соответствующего диагностического

сообщения. По каждой ошибке, обнаруженной в дополнительной конфигурации, выводится следующая информация:

- **для синтаксической ошибки** – номер строки в загружаемом XML-файле дополнительной конфигурации, в которой была обнаружена синтаксическая ошибка, имя атрибута (XML-тега) и значение атрибута, в случае его неверного или недопустимого значения;
- **для семантической ошибки** – описание семантической ошибки с указанием номера строки в XML-файле дополнительной конфигурации, в которой была обнаружена семантическая ошибка, с возможным указанием имени и значения атрибута (XML-тега).

Загрузка/выгрузка дополнительных конфигураций на управляющий компьютер возможна только с применением следующих средств администрирования:
- WEB-интерфейс администратора;
- FNPCP-интерфейс администратора.

При управлении конфигурациями администраторам МЭ ССПТ-4А1 в зависимости от прав доступа разрешены следующие действия:

- для администраторов с уровнем прав доступа `read`:
  - ✔ просмотр текущей или дополнительной конфигурации;
  - ✔ выгрузка с МЭ ССПТ-4А1 на управляющий компьютер дополнительной конфигурации;
  - ✔ отображение списка существующих на МЭ ССПТ-4А1 дополнительных конфигураций;
- для администраторов с уровнем прав доступа `full` или `admin`:
  - ✔ просмотр текущей или дополнительной конфигурации;
  - ✔ сохранение текущей конфигурации в дополнительную;
  - ✔ применение дополнительной конфигурации;
  - ✔ удаление дополнительной конфигурации;
  - ✔ загрузка с управляющего компьютера на МЭ ССПТ-4А1 дополнительной конфигурации;
  - ✔ выгрузка с МЭ ССПТ-4А1 на управляющий компьютер дополнительной конфигурации;
  - ✔ переименование дополнительной конфигурации;
  - ✔ отображение списка существующих на МЭ ССПТ-4А1 дополнительных конфигураций;
  - ✔ применение конфигурации по умолчанию.

1.5.4. Управление политиками доступа

Политика доступа – это используемый в МЭ ССПТ-4А1 согласованный набор определений правил фильтрации и определений объектов справочника, используемых в этих правилах фильтрации. В МЭ ССПТ-4А1 существует два типа политик доступа:

1) **текущая политика доступа** – набор определений правил фильтрации и определений объектов справочника, которые в данный момент задействованы в процессе

функционирования МЭ ССПТ-4А1;

2) **дополнительные политики доступа** – именованные согласованные наборы определений правил фильтрации и определений объектов справочника, которые хранятся в МЭ ССПТ-4А1 и могут быть использованы для резервного копирования текущей политики доступа с возможностью *выгрузки/загрузки дополнительных политик доступа на управляющий компьютер*. Каждой дополнительной конфигурации присваивается *символическое имя, уникальное для данного экземпляра МЭ ССПТ-4А1*.

В МЭ ССПТ-4А1 существуют следующие ограничения при работе с дополнительными политиками доступа:

- МЭ ССПТ-4А1 может хранить не более **32** дополнительных политик доступа;
- имя дополнительной политики доступа должно отвечать следующим требованиям:
  - ✔ длина имени – от **1** до **251** символа;
  - ✔ допустимые символы в имени – **латинские буквы** (**a-z**, **A-Z**), **цифры** (**0-9**), символы '_' (подчеркивание), '**-**' (дефис) и '**.**' (точка);
  - ✔ имя дополнительной конфигурации *должно начинаться с латинской буквы, либо с цифры*;
  - ✔ в имени дополнительной конфигурации *не допускается наличие двух символов '.' (точка) подряд*;

МЭ ССПТ-4А1 обеспечивает следующие возможности по управлению политиками доступа:

- просмотр текущей или дополнительной политики доступа;
- сохранение текущей политики доступа в дополнительную;
- загрузка выбранной дополнительной политики доступа в текущую (далее – *применение дополнительной политики доступа*);
- удаление дополнительной политики доступа;
- загрузка с управляющего компьютера на МЭ ССПТ-4А1 дополнительной политики доступа;
- выгрузка с МЭ ССПТ-4А1 на управляющий компьютер текущей или дополнительной политики доступа;
- изменение имени и комментария дополнительной политики доступа (далее – *переименование дополнительной политики доступа*);
- отображение списка существующих на МЭ ССПТ-4А1 дополнительных политик доступа;
- возврат текущей политики доступа в состояние до последнего изменения;
- применение политики доступа по умолчанию.

Дополнительные политики доступа, выгружаемые на управляющий компьютер, хранятся в виде единого для каждой из выгружаемых политик текстового файла, содержащего согласованные между собой справочник объектов и набор правил фильтрации.

МЭ ССПТ-4А1 обеспечивает возможность добавления, редактирования, удаления, копирования и перемещения правил фильтрации, как из основной политики доступа, так и из дополнительных.

Загрузка на МЭ ССПТ-4А1 дополнительных политик доступа и выгрузка на управляющий компьютер текущей и дополнительных политик доступа возможны только с применением следующих средств администрирования:
- WEB-интерфейс администратора;
- FNPCP-интерфейс администратора.

При управлении политиками доступа администраторам МЭ ССПТ-4А1 в зависимости от прав доступа разрешены следующие действия:

- для администраторов с уровнем прав доступа `read`:
  - ✔ просмотр текущей или дополнительной политики доступа;
  - ✔ выгрузка с МЭ ССПТ-4А1 на управляющий компьютер текущей или дополнительной политики доступа;
  - ✔ отображение списка существующих на МЭ ССПТ-4А1 дополнительных политик доступа;
- для администраторов с уровнем прав доступа `full` или `admin`:
  - ✔ просмотр текущей или дополнительной политики доступа;
  - ✔ сохранение текущей политики доступа в дополнительную;
  - ✔ применение дополнительной политики доступа;
  - ✔ удаление дополнительной политики доступа;
  - ✔ загрузка с управляющего компьютера на МЭ ССПТ-4А1 дополнительной политики доступа;
  - ✔ выгрузка с МЭ ССПТ-4А1 на управляющий компьютер текущей или дополнительной политики доступа;
  - ✔ переименование дополнительной политики доступа;
  - ✔ отображение списка существующих на МЭ ССПТ-4А1 дополнительных политик доступа;
  - ✔ возврат текущей политики доступа в состояние до последнего изменения;
  - ✔ применение политики доступа по умолчанию.

Управление справочниками объектов. Справочник объектов – это набор соответствий между символическими именами и идентифицированными объектами (хостами, сетями, сервисами и т. д.), имеющими определенные атрибуты. После добавления объекта в справочник его символическое имя можно использовать *как в правилах фильтрации, так и в других объектах для организации ссылки на данный объект*.

Символическое имя объекта справочника **должно быть уникальным** среди имен всех объектов, определенных в том же справочнике.

В МЭ ССПТ-4А1 поддерживаются следующие типы объектов:

- `host` (*хост*, *узел*) – объект для определения хоста/узла сети со следующими атрибутами:
  - ✔ символическое имя объекта `host`;

✔ перечисление IPv4-адресов;

✔ перечисление IPv6-адресов;

✔ перечисление MAC-адресов;

✔ VLAN;

✔ список фильтрующих интерфейсов МЭ ССПТ-4А1;

✔ строка комментария к экземпляру объекта `host`;

- `net` (*сеть*) – объект для определения IP-сети со следующими атрибутами:

  ✔ символическое имя объекта `net`;

  ✔ перечисление IPv4-адресов;

  ✔ перечисление IPv6-адресов;

  ✔ VLAN;

  ✔ фильтрующий интерфейс МЭ ССПТ-4А1;

  ✔ строка комментария к экземпляру объекта `net`;

- `net-group` (*группа сетевых объектов*) – объект, предназначенный для объединения объектов `host` и/или `net`. Объект `net-group` обладает следующими атрибутами:

  ✔ символическое имя объекта `net-group`;

  ✔ список имен объектов `host` (*не более 8 объектов*);

  ✔ список имен объектов `net` (*не более 8 объектов*);

  ✔ строка комментария к экземпляру объекта `net-group`;

- `service` (*сервис*) – объект для определения сетевого приложения со следующими атрибутами:

  ✔ символическое имя объекта `service`;

  ✔ код транспортного протокола;

  ✔ перечисление номеров портов (*для протоколов TCP, UDP*);

  ✔ перечисление типа/кода сообщения (*для протокола ICMP*);

  ✔ строка комментария к экземпляру объекта `service`;

- `resource` (*ресурс*) – объект для определения совокупности объектов `host` (`net`) и `service`. Объект `resource` обладает следующими атрибутами:

  ✔ символическое имя объекта `resource`;

  ✔ список имен объектов `host` (*не более 8 объектов*);

  ✔ список имен объектов `net` (*не более 8 объектов*);

  ✔ имя объекта `net-group`;

  ✔ имя объекта `service`;

  ✔ строка комментария к экземпляру объекта `resource`;

- `time` (*интервал времени*) – объект для определения объединения промежутков времени. Объект `time` обладает следующими атрибутами:
  - ✔ символическое имя объекта `time`;
  - ✔ набор месяцев года;
  - ✔ набор дней месяца;
  - ✔ набор дней недели;
  - ✔ время суток начала промежутка времени (*включительно*);
  - ✔ время суток окончания промежутка времени (*включительно*);
  - ✔ строка комментария к экземпляру объекта `time`;
- `vlan-group` (*группа VLAN*) – объект для определения объединения сетевых узлов (*хостов*) по признаку принадлежности к VLAN. Объект `vlan-group` обладает следующими атрибутами:
  - ✔ символическое имя объекта `vlan-group`;
  - ✔ перечисление номеров VLAN;
  - ✔ фильтрующий интерфейс МЭ ССПТ-4А1;
  - ✔ строка комментария к экземпляру объекта `vlan-group`;
- `domain-group` (*группа доменных имен*) – объект для определения перечня доменных имен, используемых в прикладных правилах фильтрации DNS и HTTP. Объект `domain-group` обладает следующими атрибутами:
  - ✔ символическое имя объекта `domain-group`;
  - ✔ перечисление доменных имен;
  - ✔ строка комментария к экземпляру объекта `domain-group`.

1.5.5. Средство обновления и восстановления

В комплект поставки МЭ ССПТ-4А1 входит Средство обновления и восстановления (далее – СОВа-4), которое поставляется на USB-носителе и привязано к экземпляру МЭ ССПТ-4А1. Основные функциональные возможности СОВа-4:

- сброс текущей конфигурации в состояние по умолчанию;
- сброс текущей политики доступа в состояние по умолчанию;
- сброс пароля системного пользователя `fnpsh`;
- сброс пароля администратора `admin`;
- восстановление файловой системы носителя данных МЭ ССПТ-4А1 в состояние по умолчанию (восстанавливаются все файлы и каталоги к состоянию на момент поставки или последнего обновления);
- проверка файловой системы носителя данных МЭ ССПТ-4А1 на наличие ошибок;

- просмотр информации об аппаратном и программном обеспечении данного экземпляра МЭ ССПТ-4А1;
- обновление ПО МЭ ССПТ-4А1 из файлов обновлений, предварительно записанных администратором на FAT-раздел USB-носителя данных СОВа-4.

2. Подготовка к работе и первое включение

Данная глава, описывающая порядок начала работы с МЭ ССПТ-4А1, содержит следующую информацию:

- описание комплекта поставки, надписей и условных обозначений устройства МЭ ССПТ-4А1 (раздел 2.1, стр. 39);
- порядок выполнения начальных настроек МЭ ССПТ-4А1 после первого включения устройства (раздел 2.6, стр. 48).

2.1. Комплект поставки

МЭ ССПТ-4А1 поставляется в комплекте согласно таблице 2.1.

Таблица 2.1: Комплект поставки МЭ ССПТ-4А1

№	Обозначение	Наименование	Количество	Примечание
1	ФРПС.466259.001-XX	Программно-аппаратный комплекс межсетевого экранирования с предустановленным ПО МЭ ССПТ-4А1	1	XX – исполнение [01...11]
2	ФРПС.467669.001	Средство обновления и восстановления с предустановленным ПО СОВа-4	1	Носитель USB-флэш
3	ФРПС.466259.001 ПС	Межсетевой экран ССПТ-4А1. Паспорт	1	Формат А4
4	ФРПС.466259.001 РЭ	Межсетевой экран ССПТ-4А1. Руководство по эксплуатации	1	На компакт-диске
5		Утилиты МЭ ССПТ-4А1	1	На компакт-диске
6		Заверенная копия выданного ФСБ РФ сертификата соответствия Системы сертификации средств защиты информации по требованиям безопасности информации №РОСС RU.0003.01БИ00	1	Формат А4
7		Шнур питания 220 В / 50 Гц	1	
8		Консольный кабель	1	
9		Монтажные скобы с комплектом крепежа	2	
10		Упаковка	1	

2.2. Маркировка и назначение разъемов, светодиодов и элементов управления

Разъемы и элементы управления, расположенные на лицевой панели МЭ ССПТ-4А1, имеют следующие маркировку и назначение:

- **Eth0**, **Eth1**, **Eth2**, … , **Eth15** – разъемы фильтрующих интерфейсов Ethernet, к которым подключаются защищаемые сегменты локальной сети. Общее количество и компоновка разъемов (количество разъемов типа RJ-45, наличие разъемов типов SFP и SFP+ и их

количество) зависит от варианта исполнения МЭ ССПТ-4А1. Таблица вариантов исполнения МЭ ССПТ-4А1 приведена в документе *“Межсетевой экран ССПТ-4А1. Паспорт” ФРПС.466259.001 ПС*;

- **EthC** – разъем управляющего интерфейса Ethernet. Используемый тип кабеля – “витая пара”, тип разъема – RJ-45;
- **COM** – разъем последовательного интерфейса RS-232, к которому подключается управляющий компьютер при помощи консольного кабеля (входит в комплект поставки). Используемый тип кабеля – “витая пара”, тип разъема – RJ-45;
- **USB** – разъем для подключения USB-носителя СОВа-4 (входит в комплект поставки), а также для подключения USB-клавиатуры при управлении МЭ ССПТ-4А1 через системную консоль, использующую разъем **VGA** устройства;
- **RESET** – кнопка перезагрузки устройства по питанию.

Маркировка и назначение светодиодных индикаторов, расположенных на лицевой панели МЭ ССПТ-4А1, представлены в таблице 2.2.

Таблица 2.2: Маркировка и назначение светодиодных индикаторов

Маркировка		***Назначение***
Исполнения 01 – 08	***Исполнения 09 – 11***	
⏻	**POWER**	Питание
∿	**–**	Не используется
🛢	**HDD**	Операции чтения/записи на носитель данных
L/A	**LINK ACT**	Наличие несущей и активность для интерфейсов SFP и SFP+ (в зависимости от исполнения могут отсутствовать)

Разъемы и элементы управления, расположенные на задней панели МЭ ССПТ-4А1, имеют следующие маркировку и назначение:

- **VGA** – разъем типа DSUB-15 для подключения к МЭ ССПТ-4А1 VGA-монитора (только в вариантах исполнений ФРПС.466259.001-09 – ФРПС.466259.001-11);
- кнопка включения/отключения питания (только в вариантах исполнений ФРПС.466259.001-01 – ФРПС.466259.001-08);
- разъем питания для подключения шнура питания 220 В / 50 Гц (входит в комплект поставки).

2.3. Жидкокристаллический индикатор

МЭ ССПТ-4А1 в исполнениях ФРПС.466259.001-01 – ФРПС.466259.001-08 оснащен жидкокристаллическим индикатором (далее – *ЖКИ*), позволяющим администратору просматривать следующую информацию об экземпляре МЭ ССПТ-4А1:

- модель устройства, имя экземпляра устройства;
- IP-адрес и маска на управляющем интерфейсе, IP-адрес шлюза в маршруте по умолчанию;
- состояние основных подсистем;
- статистика использования центрального процессора устройства;
- информация об использовании оперативной памяти устройства;
- имя выпуска, версия и дата сборки ПО МЭ ССПТ-4А1.

ЖКИ расположен в левой части лицевой панели МЭ ССПТ-4А1 и включает в себя помимо дисплея, четыре кнопки. Схематическое изображение ЖКИ приведено на рисунке 2.1, стр. 41. Назначение кнопок поясняется ниже в соответствии с их маркировкой.

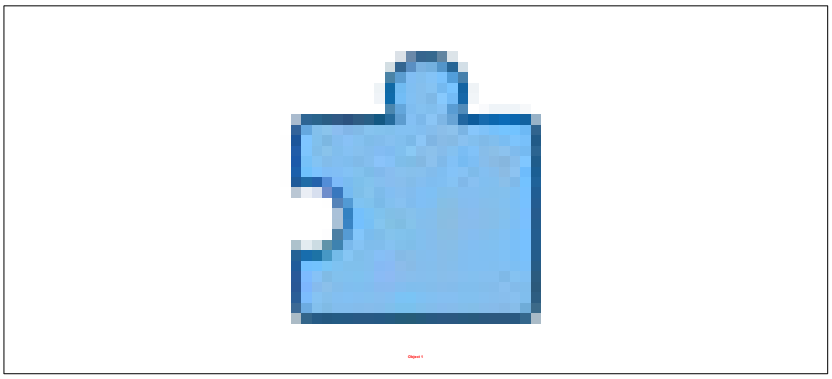


Рисунок 2.1: ЖКИ МЭ ССПТ-4А1

Дисплей ЖКИ содержит 2 строки для вывода текстовой информации. В каждой строке может быть выведено до 20 символов. В ПО МЭ ССПТ-4А1 версии 1.0.0 поддерживается вывод на ЖКИ только с использованием символов латинского алфавита.

Для выбора информации, выводимой на ЖКИ, используются кнопки клавиатуры ЖКИ (рис. 2.1, стр. 41). Комбинацию из двух текстовых строк, выводимых на ЖКИ одновременно, далее называется *экран ЖКИ*. Каждый экран ЖКИ содержит определенный набор информации об экземпляре МЭ ССПТ-4А1. Клавиатура ЖКИ, включающая в себя 4 кнопки, позволяет выбирать экран ЖКИ для отображения. Назначение кнопок в соответствии с приведенной маркировкой (рис. 2.1, стр. 41) следующее:

- **<** – перейти к первому экрану ЖКИ;
- ∧ – перейти к предыдущему экрану ЖКИ;
- ∨ – перейти к следующему экрану ЖКИ;
- **>** – перейти к последнему экрану ЖКИ.

Первый экран ЖКИ отображается по умолчанию. В ПО МЭ ССПТ-4А1 версии 1.0.0 имеется 9 экранов ЖКИ, между которыми можно переключаться с помощью кнопок ЖКИ. Далее приводится описание информации, выводимой на каждом из экранов ЖКИ в порядке увеличения их нумерации (порядок отображения экранов при переключении их по кнопке с маркировкой: `V`).

Через **20** секунд после последнего нажатия любой кнопки клавиатуры ЖКИ автоматически выполняется переход к первому экрану ЖКИ.

Первый экран ЖКИ. Пример первого экрана ЖКИ приведен на рисунке 2.2, стр. 42.

```
Model: SSPT-4A1
fnp4
```

Рисунок 2.2: Первый экран ЖКИ

В первой строке экрана ЖКИ выводится модель устройства (`SSPT-4A1`). Таким образом вид первой строки – общий для всех экземпляров МЭ ССПТ-4А1. Во второй строке экрана ЖКИ выводится имя устройства из текущей конфигурации МЭ ССПТ-4А1 (по умолчанию – `fnp4`).

Если выявлено нарушение контрольной суммы какого-либо из контролируемых файлов МЭ ССПТ-4А1, то в первой строке первого экрана ЖКИ выводится оповещение о данной нештатной ситуации в виде восклицательного знака, заключенного в круглые скобки. Пример оповещения о нарушении контрольных сумм приведен на рисунке 2.3, стр. 42.

```
Model: SSPT-4A1 (!)
fnp4
```

Рисунок 2.3: Первый экран ЖКИ: нарушение контрольных сумм

Второй экран ЖКИ. Пример второго экрана ЖКИ приведен на рисунке 2.4, стр. 42.

```
IP: 10.234.28.71/16
GW: not set
```

Рисунок 2.4: Второй экран ЖКИ: маршрут по умолчанию не задан

В первой строке выводится IP-адрес и маска, назначенные на управляющем интерфейсе МЭ ССПТ-4А1. Маска выводится в кратком формате (CIDR). В примере (см. рис. 2.4, стр. 42), маска имеет значение `16`, что тождественно 255.255.0.0.

Во второй строке выводится IP-адрес шлюза в маршруте по умолчанию. В случае, если маршрут по умолчанию не установлен, во второй строке выводится `not set`.

Пример второго экрана ЖКИ при наличии маршрута по умолчанию приведен на рисунке 2.5, стр. 43.

```
IP:  10.234.28.71/16
GW:  10.234.28.254
```

Рисунок 2.5: Второй экран ЖКИ: маршрут по умолчанию задан

Третий экран ЖКИ. Пример третьего экрана ЖКИ приведен на рисунке 2.6, стр. 43.

```
Filter:    avail
Integrity: avail
```

Рисунок 2.6: Третий экран ЖКИ

В первой строке третьего экрана ЖКИ выводится состояние процесса пакетного фильтра (`Filter`). Во второй строке – состояние процесса сервера проверки контрольных сумм (`Integrity`).

Процессы подсистем МЭ ССПТ-4А1 могут находиться в следующих состояниях:

- **avail** — процесс запущен и отвечает на запросы в течение тайм-аута, предусмотренного для данной подсистемы;
- **unavail** — процесс запущен, но не отвечает на запросы в течение тайм-аута, предусмотренного для данной подсистемы;
- **stopped** – процесс остановлен.

Если процесс не ответил на запрос в течение **1** секунды, то на экран ЖКИ выводится следующая информация, извещающая администратора об ожидании ответа процесса:

```
waiting for reply
please wait...
```

По истечении тайм-аута, предусмотренного для данной подсистемы (для сервера авторизации – до **60** секунд, для остальных подсистем – до **10** секунд), состояние процесса будет установлено в `unavail`.

Четвертый экран ЖКИ. Пример четвертого экрана ЖКИ приведен на рисунке 2.7, стр. 43

```
Auth:    avail
Logging: avail
```

Рисунок 2.7: Четвертый экран ЖКИ

В первой строке четвертого экрана ЖКИ выводится состояние процесса сервера авторизации (`Auth`). Во второй строке – состояние процесса сервера регистрации (`Logging`).

Пятый экран ЖКИ. Пример пятого экрана ЖКИ приведен на рисунке 2.8, стр. 44

```
Reserve:    avail
Cmd server: avail
```

Рисунок 2.8: Пятый экран ЖКИ

В первой строке пятого экрана ЖКИ выводится состояние процесса сервера резервирования (`Reserve`). Во второй строке – состояние процесса командного сервера (`Cmd server`).

Шестой экран ЖКИ. Пример шестого экрана ЖКИ приведен на рисунке 2.9, стр. 44

```
WEB:  avail
SNMP: avail
```

Рисунок 2.9: Шестой экран ЖКИ

В первой строке шестого экрана ЖКИ выводится состояние процесса Web-сервера, реализующего WEB-интерфейс (`WEB`). Во второй строке – состояние процесса SNMP-сервера, реализующего SNMP-интерфейс (`SNMP`).

Седьмой экран ЖКИ. Пример седьмого экрана ЖКИ приведен на рисунке 2.10, стр. 44

```
FNP4 1.0.0-RELEASE
Nov 28 2019
```

Рисунок 2.10: Седьмой экран ЖКИ

В первой строке седьмого экрана ЖКИ выводится имя выпуска, включающее в себя версию ПО МЭ ССПТ-4А1 (1.0.0). Во второй строке – дата сборки ПО МЭ ССПТ-4А1.

Восьмой экран ЖКИ. Пример восьмого экрана ЖКИ приведен на рисунке 2.11, стр. 44

```
Usr:0.0% Sys:0.2%
Int:0.2% Idle:96.6%
```

Рисунок 2.11: Восьмой экран ЖКИ

На восьмом экране ЖКИ приводится статистика использования центрального процессор устройства. Выводится процент времени, проведенный процессором в определенном состоянии.

В первой строке выводятся:

- процент времени, проведенный процессором в состоянии “`user`” (`Usr`);
- процент времени, проведенный процессором в состоянии “`system`” (`Sys`).

Во второй строке выводятся:

- процент времени, проведенный процессором в состоянии “`interrupt`” (`Int`);
- процент времени, проведенный процессором в состоянии “`idle`” (`Idle`).

При переходе к восьмому экрану ЖКИ (по нажатию одной из кнопок ЖКИ) вывод экрана осуществляется с задержкой в **1** секунду, в течении которой формируется статистика использования центрального процессора устройства.

Девятый экран ЖКИ. Пример девятого экрана ЖКИ приведен на рисунке 2.12, стр. 45

```
Act: 6M Ina: 54M
Fr: 7400M Tot: 8138M
```

Рисунок 2.12: Девятый экран ЖКИ

На девятом экране ЖКИ приводится информация об использовании оперативной памяти устройства.

В первой строке выводятся:

- объем активной памяти в мегабайтах (`Act`);
- объем неактивной памяти в мегабайтах (`Ina`).

Во второй строке выводятся:

- объем свободной памяти в мегабайтах (`Fr`);
- суммарный объем памяти в мегабайтах (`Tot`).

2.4. Требования к управляющему компьютеру

Управляющий компьютер – это персональный компьютер общего назначения, который используется для управления и настройки параметров функционирования МЭ ССПТ-4А1, как при работе через системную консоль, так и при работе через управляющий Ethernet-интерфейс. УК должен работать под управлением одной из следующих операционных систем:

- Microsoft Windows® XP/Vista/7/8/10;
- FreeBSD версий 10.x, 11.x;
- на базе ядра Linux версий не ниже 2.4.x.

Управляющий компьютер должен быть оснащен адаптером Ethernet для подключения к МЭ ССПТ-4А1 через управляющий Ethernet-интерфейс и/или последовательным портом RS-232 для подключения к МЭ ССПТ-4А1 через COM-порт по нуль-модемному кабелю.

Операционная система, под управлением которой функционирует управляющий компьютер, должна обеспечивать возможность работы в компьютерных сетях, использующих семейство протоколов TCP/IP на основе протокола IPv4.

На управляющем компьютере должно быть установлено следующее прикладное программное обеспечение:

- **SSH-клиент** – приложение для управления МЭ ССПТ-4А1 с использованием командного интерфейса администратора. SSH-клиент, устанавливаемый на управляющий компьютер, должен поддерживать протокол *SSH версии 2*. Рекомендуется использование следующих SSH-клиентов:
  - ✔ SSH-клиент, входящий в состав пакета программ **PuTTY** (*только для операционных систем MS Windows® Vista/7/8/10*);
  - ✔ SSH-клиент, входящий в состав пакета программ OpenSSH. Данный SSH-клиент входит в состав большинства дистрибутивов UNIX-подобных операционных систем (FreeBSD, OpenBSD, операционные системы на базе ядра Linux и др.);
- **WEB-браузер** – приложение для управления МЭ ССПТ-4А1 с использованием WEB-интерфейса администратора. WEB-браузер, устанавливаемый на управляющий компьютер, должен обладать следующими возможностями:
  - ✔ поддержка протокола **HTTP версии 1.1**;
  - ✔ поддержка протокола **HTTPS** (Secure HTTP);
  - ✔ возможность работы с **HTTP Cookies**;
  - ✔ возможность обработки сценариев языка JavaScript, соответствующего спецификациям ECMAScript 6 стандарта ECMA-262, передаваемых в составе WEB-документов;
  - ✔ возможность обработки формального языка описания внешнего вида WEB-документа CSS (*CSS – Cascading Style Sheets*) версии 2.1;

  Рекомендуется использование следующих WEB-браузеров:
  - ✔ **Mozilla Firefox** – начиная с версии **44.0**;
  - ✔ **Google Chrome** – начиная с версии **40.0**;
  - ✔ **Microsoft Internet Explorer** (*только для операционных систем MS Windows® Vista/7/8*) – версии **8.0.7601** (*только для операционной системы MS Windows® 7 SP1*), **9.x**, **10.x**;
  - ✔ **Microsoft Edge** (*только для операционной системы MS Windows® 10*);
- **MIB-браузер** – приложение для взаимодействия с МЭ ССПТ-4А1 с использованием SNMP-интерфейса администратора. MIB-браузер, устанавливаемый на управляющий компьютер, должен поддерживать протокол *SNMP версии 3*. Рекомендуется использование следующих MIB-браузеров:
  - ✔ **SnmpB** версии **0.8**. Страница загрузки – https://sourceforge.net/projects/snmpb;

✔ **iReasoning MIB Browser** версии **11 Build 4010**. Страница загрузки – http://ireasoning.com/download.shtml.

2.5. Системная консоль

Системная консоль является средством локального управления МЭ ССПТ-4А1. Подключение к системной консоли МЭ ССПТ-4А1 осуществляется через COM-порт изделия. Для подключения необходим консольный кабель (входит в комплект поставки). С одной стороны консольный кабель подключается к разъему **COM** МЭ ССПТ-4А1, с другой стороны – к COM-порту УК (разъем DB-9).

При отсутствии на УК COM-порта можно воспользоваться конвертером RS-232 в USB.

Для исполнений ФРПС.466259.001-09 – ФРПС.466259.001-11 МЭ ССПТ-4А1 управление через системную консоль также может быть организовано путем подключения VGA-монитора к разъему **VGA** (тип разъема – DSUB-15) и USB-клавиатуры к разъему **USB** устройства.

Связь УК с системной консолью МЭ ССПТ-4А1 осуществляется через программу-эмулятор удаленного терминала. При подключении к системной консоли обеспечивается управление устройством только посредством командного интерфейса администратора. Рекомендованные программы-эмуляторы удаленного терминала приведены в подразделе 2.4, стр. 45.

Для подключения к системной консоли МЭ ССПТ-4А1 необходимо настроить COM-порт УК, участвующий в соединении, следующим образом:

- скорость передачи данных – **115200** бит/с;
- биты данных – **8** бит;
- четность – **не проверяется**;
- стоповые биты – **1** бит;
- управление потоком – **аппаратное (CTS/RTS)**;

Краткая запись настроек COM-порта: **115200 8N1 CTS/RTS**.

Настройка COM-порта УК выполняется, как правило, непосредственно в программе-эмуляторе удаленного терминала.

При подключении к работающему устройству в некоторых программах-эмуляторах удаленного терминала для получения системного приглашения может потребоваться нажатие клавиши **`<Enter>`** на клавиатуре УК.

2.6. Первое включение

При первом включении МЭ ССПТ-4А1 администратору рекомендуется выполнить следующую последовательность действий:

1) **Подключить УК к COM-порту МЭ ССПТ-4А1**:

1.1) соединить при помощи консольного кабеля, входящего в комплект поставки, COM-порт экземпляра устройства МЭ ССПТ-4А1 (**COM**) и свободный COM-порт УК;

1.1) на УК запустить и настроить программу-эмулятор удаленного терминала согласно подразделу 2.5, стр. 47).

2) **Включить экземпляр устройства МЭ ССПТ-4А1**:

2.1) подключить шнур питания к разъему питания на задней панели изделия и розетке 220 В /50 Гц;

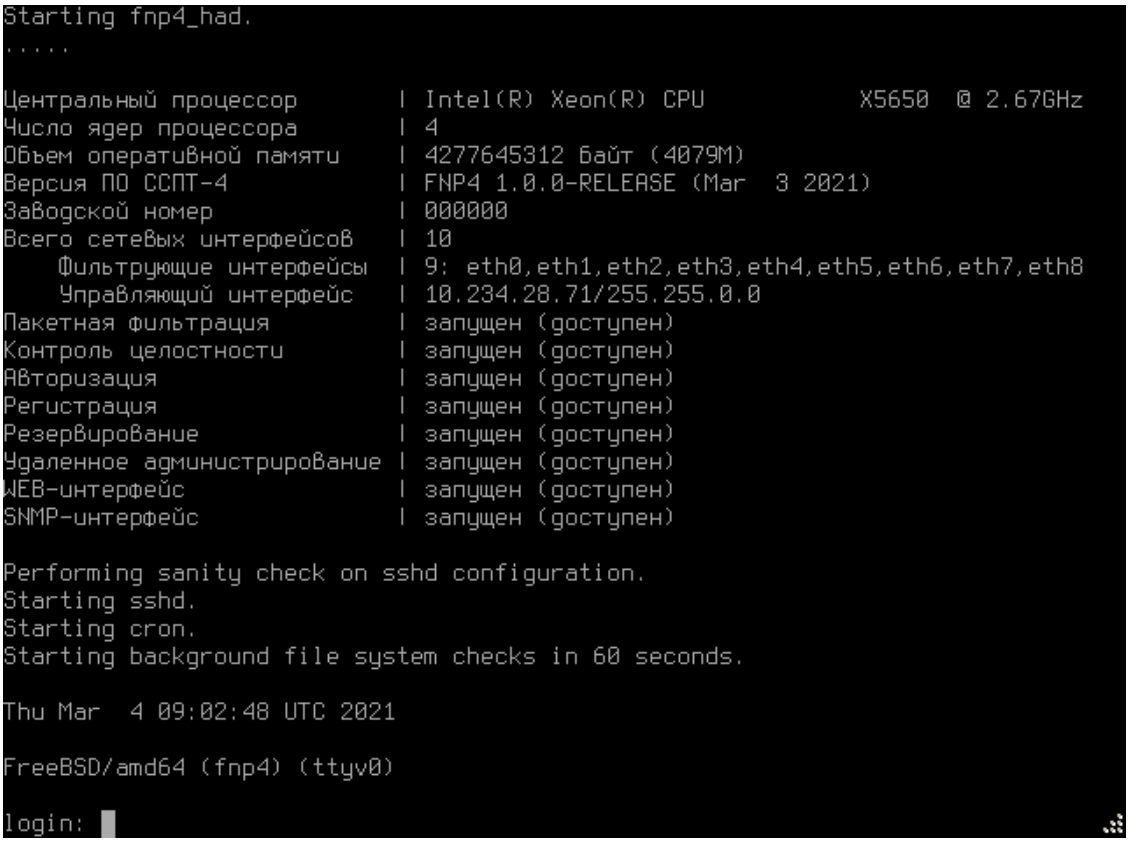


Рисунок 2.13: Вывод системной консоли при первом включении МЭ ССПТ-4А1

2.2) подать питание на изделие, нажав на кнопку питания на задней панели. Должен загореться световой индикатор “POWER” на передней панели изделия и появиться характерный звук работающих вентиляторов. Если этого не произошло, следует нажать кнопку “RESET” на передней панели изделия, после чего изделие начнет загрузку. В программе-эмуляторе удаленного терминала должна появиться информация о ходе загрузки УОС и подсистем ПО МЭ ССПТ-4А1, после чего должно быть выведено приглашение на

ввод учетных данных “`login:`”. Пример информации на системной консоли после успешной загрузки УОС и ПО МЭ ССПТ-4А1 представлен на рисунке 2.13, стр. 48;

3) **Последовательно ввести учетные данные** системного пользователя **`fnpsh`** и администратора МЭ ССПТ-4А1 **`admin`**. Пароль по умолчанию для обеих учетных записей – общий – **`FilterD`**. Данный шаг считается успешно пройденным, если получено диагностическое сообщение командного интерфейса МЭ ССПТ-4А1:

```
FNPSH-I-007.02.3001-Успешная авторизация администратора (admin)
```

> Пароль по умолчанию для системного пользователя **`fnpsh`** и администратора **`admin`** общий – **`FilterD`**.
>
> Настоятельно рекомендуется при первом включении сменить пароли обеих учетных записей.

4) **Убедиться, что все подсистемы МЭ ССПТ-4А1 запущены и доступны**, выполнив команду **`system show`**. Пример вывода команды представлен на рис. 2.14, стр. 49. Все подсистемы МЭ ССПТ-4А1, перечисленные в выводе команды **`system show`**, должны иметь состояние запущен (доступен), как в приведенном примере. Данное состояние означает, что подсистема запущена и работает в штатном режиме.

```
Имя администратора: admin
Пароль:

FNPSH-I-007.02.3001-Успешная авторизация администратора (admin)
fnp4> system show
Центральный процессор                | Intel(R) Xeon(R) CPU           X5650  @ 2
.67GHz
Число ядер процессора                | 4
Объем оперативной памяти             | 4277645312 байт (4079M)
Версия ПО ССПТ-4                     | FNP4 1.0.0-RELEASE (Mar  3 2021)
Заводской номер                      | 000000
Всего сетевых интерфейсов            | 10
    Фильтрующие интерфейсы           | 9: eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth
7,eth8
    Управляющий интерфейс            | Включен, 10.234.28.71/255.255.0.0
Пакетная фильтрация                  | запущен (доступен)
Контроль целостности                 | запущен (доступен)
Авторизация                          | запущен (доступен)
Регистрация                          | запущен (доступен)
Резервирование                       | запущен (доступен)
Удаленное администрирование          | запущен (доступен)
WEB-интерфейс                        | запущен (доступен)
SNMP-интерфейс                       | запущен (доступен)
Тайм-аут неактивности администратора | 600 секунд
Просмотрщик по умолчанию FNPSH       | Внутренний (internal)
Имя устройства                       | fnp4
Комментарий к устройству             |
fnp4>
```

Рисунок 2.14: Проверка функционирования и доступности подсистем МЭ ССПТ-4А1

5) **Убедиться в отсутствии нарушений контрольных сумм файлов, контролируемых МЭ ССПТ-4А1,** выполнив команду **`system icheck`**. Пример вывода команды представлен на рис. 2.15, стр. 50. В каждой строке вывода команды, содержащей имя контролируемого файла и его контрольную сумму, в столбце “`Результат`” должен быть знак “+”, свидетельствующий о том, что контрольная сумма файла не нарушена.

```
 09:08:38                    Проверка целостности                    04.03.2021
Имя файла                 Результат Контрольная сумма
------------------------------------------------------------------------------
rc.conf                     +         9A3B132AFBB383118215FD21D9B0F7ABFB32499B1ECB
fnp4                        +         17DAA971AB004FDEB708681F3403BEF3F89980206B19
fnp4eth                     +         145DC0CA9D7E982AAF4B1A972CCF2880840990F1E577
fnp4proxy                   +         2BAE035CD04A4D37295A253A8618575050589C1CF8FF
fnp4snmp                    +         20A48D7F6B496EE8757C7ACF1041D0C216BAB41A52B5
fnp4tmp                     +         B72AB6C48FF6221AAEC8885CD803937CBCF86C076077
fnp4web                     +         08ED2029B4544EF034CDE780288181D169AB3FEAA12B
kernel                      +         5B060E5BE88CDBA21303FFADB070CD70C942B647323F
libc.so.7                   +         2A5252E11888619A66E403ECE496131DA4D7465068A8
libkvm.so.7                 +         E47577DA165D2B22FEC2F25DA5D9C4E8B02AC21493BD
libcrypto.so.8              +         CF91396F03E1E5269D82F9D2BE6660128014DB3A2D66
libssl.so.8                 +         93BEBE43AE3FD211F6FB9849F5C384034EC078ED2151
libxml2.so.2.9.10           +         7377CEB9B830476830F04FDC573A8FBC10146A4593C2
libfnpcrypt2_ssl.so.2.1.0 +           B8CA6738CCB739AC51BE692A04E988B4E45507C382C1
login                       +         081956FC5FC4D4066C0304F5566049A1CDE0EC14F9BE
ntpdate                     +         83DB8416220B9509A68096B7B3DDC84A284A580C8A3E
httpd                       +         D0926F7952B34A8110009273FEDCE026108A75BB9852
snmpd                       +         7F376BE4D9CD576780AAB5A6DBCC6D570B40747C966C
openssl                     +         3F080C4279F8F3B02833F8368F5EF90093DA0710D2FC
fnp4sh                      +         4A12F8CBD286FFB438A6032AA035B044B993B1ADB272
fnp4_info                   +         58ACA9213F03921DB4B7CFADA93AC2485BB8170339E4
fnp4_authd                  +         2270CCAAB577BE25F6DE65A179430D54EB9E940CAAF6
fnp4_csd                    +         DCB0C596AC0D360F7DD67F016ADD1455C15F0284131F
fnp4_filtd                  +         AB3954705AF0C20AFCA4A11B5CBCEC0020F0BD448EAF
fnp4_had                    +         964FA3ED6AD8932CCE23DB4578CA5569301018 4D14F7
fnp4_lcmd                   +         21E658CE4BFE663ADC2ACA8293335317512B8C3B0D89
 Строки: 1-28 из 62                Столбцы: 1-80    H - справка  Q, F10 - Выход
```

Рисунок 2.15: Результат проверки целостности

6) **Сменить пароль системного пользователя `fnpsh`**, выполнив команду **`system fnpsh password`**. Новый пароль будет запрошен дважды, чтобы исключить ошибку при его вводе:

```
fnp4> system fnpsh password
Новый пароль:
Новый пароль повторно:
FNPSH-I-007.02.30C1-Пароль системного пользователя изменен
fnp4>
```

7) **Сменить пароль администратора `admin`** (администратора с привилегиями суперпользователя), выполнив команду **`user password`**. Будет запрошен текущий пароль администратора `admin`, который при первом запуске соответствует паролю по умолчанию. Далее новый пароль будет запрошен дважды, чтобы исключить ошибку при его вводе:

```
fnp4> user password
Старый пароль:
Новый пароль:
Новый пароль повторно:
FNPSH-I-007.02.300A-Пароль администратора изменен (admin)
fnp4>
```

8) При первом включении через системную консоль рекомендуется (при необходимости) **изменить IP-адрес управляющего интерфейса**. Для этого служит команда **`interface control set`**, например:

```
fnp4> interface control set address=10.2.1.157/255.255.255.224
Изменить параметры управляющего интерфейса? (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (10.2.1.157)
fnp4>
```

После выполнения указанной процедуры МЭ ССПТ-4А1 может быть настроен в соответствии с требованиями политики безопасности организации и инфраструктурой корпоративной сети. Настройка МЭ на примере командного интерфейса администратора рассматривается в главе 3, стр 55.

Политика доступа по умолчанию запрещает прохождение какого-либо трафика через МЭ ССПТ-4А1. В связи с этим, рекомендуется выполнять первый запуск МЭ ССПТ-4А1, а также последующую настройку параметров функционирования и текущей политики доступа до включения МЭ ССПТ-4А1 в существующую сетевую инфраструктуру организации.

9) В целях обеспечения безопасного использования МЭ ССПТ-4А1 **доступ к управляющему Ethernet-интерфейсу изделия должен быть ограничен** IP-адресом управляющего компьютера. Порядок внесения IP-адреса в список контроля доступа к управляющему Ethernet-интерфейсу см. в п. 3.13.5 настоящего документа.

В целях обеспечения безопасного использования МЭ ССПТ-4А1 **доступ к управляющему Ethernet-интерфейсу изделия должен быть ограничен** IP-адресом управляющего компьютера.

10) **Завершение работы МЭ ССПТ-4А1 и отключение УК.** Для корректного выключения МЭ ССПТ-4А1 необходимо ввести команду **`system halt`** и подтвердить действие, нажав «**Y**»:

```
fnp4> system halt
Выключить устройство? (Y/N) [N]: Y
```

После останова устройства отключить консольный кабель от COM-порта МЭ ССПТ-4А1.

2.7. Подключение через управляющий Ethernet-интерфейс

В целях обеспечения безопасного использования МЭ ССПТ-4А1 управляющий сегмент Ethernet, подключенный к управляющему Ethernet-интерфейсу изделия, должен быть:

- **физически изолирован** от остальных сегментов сети, включая сегменты, подключенные к фильтрующим интерфейсам;
- **защищен** от несанкционированного доступа **организационными мерами**.

Для подключения к МЭ ССПТ-4А1 через управляющий Ethernet-интерфейс необходим кабель “витая пара” категорий 5, 5E, 6.

По умолчанию установлены следующие параметры управляющего Ethernet-интерфейса МЭ ССПТ-4А1:

- автоопределение скорости (поддерживается 10/100/1000 Мбит/с);
- полный дуплекс;
- IP-адрес **10.234.28.71,** маска **255.255.0.0**.

Управление МЭ ССПТ-4А1 через управляющий Ethernet-интерфейс может осуществляться с использованием командного интерфейса и WEB-интерфейс а администратора.

2.7.1. Подключение к командному интерфейсу

Доступ к командному интерфейсу МЭ ССПТ-4А1 осуществляется с УК с использованием программы – SSH-клиента (требования к УК изложены в подразделе 2.4, стр. 45). В ОС FreeBSD и ОС на базе ядра Linux SSH-клиент предустановлен. Для подключения к МЭ ССПТ-4А1 достаточно в консоли выполнить команду **ssh** с указанием имени системного пользователя **fnpsh** и IP-адреса управляющего Ethernet-интерфейса МЭ ССПТ-4А1, например:

```
$ ssh fnpsh@10.2.1.1
```

Если IP-адрес управляющего Ethernet-интерфейса МЭ ССПТ-4А1 доступен с УК, то в консоли будет выведено приглашение ввода пароля системного пользователя **fnpsh**:

```
Password for fnpsh@10.2.1.1:
```

Далее выполняется последовательная авторизация системным пользователем **fnpsh** и администратором **admin**, аналогично тому, как это делается при подключении через системную консоль.

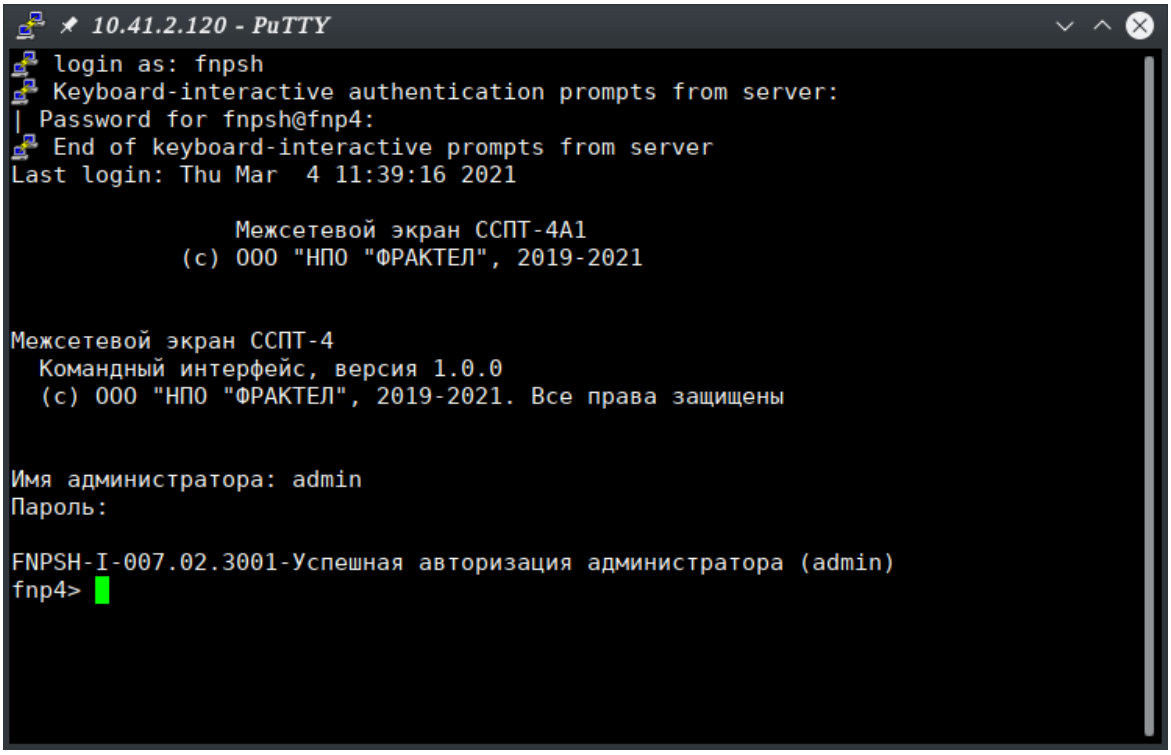


Рисунок 2.16: Подключение к командному интерфейсу МЭ ССПТ-4А1 через программу PuTTy

Если УК работает под управлением ОС семейства Windows, то для подключения к МЭ через командный интерфейс необходима установка стороннего SSH-клиента, например **PuTTy**. При подключении необходимо указать IP-адрес управляющего Ethernet-интерфейса МЭ ССПТ-4А1 и использовать порт 22 (порт SSH по умолчанию). Пример подключения с помощью программы **PuTTy** приведен на рисунке 2.16, стр 53.

Для подключения к МЭ ССПТ-4А1 через управляющий Ethernet-интерфейс IP-адреса УК и управляющего Ethernet-интерфейса МЭ ССПТ-4А1 должны принадлежать одной подсети. В противном случае на УК и МЭ ССПТ-4А1 администратором должны быть добавлены статические маршруты, обеспечивающие их связность.

Использование командного интерфейса администратора МЭ ССПТ-4А1 рассматривается в главе 3, стр. 55.

2.7.2. Подключение к WEB-интерфейсу

Доступ к WEB-интерфейсу МЭ ССПТ-4А1 осуществляется с УК с использованием WEB-браузера (требования к УК изложены в подразделе 2.4, стр. 45). Для доступа к WEB-интерфейсу необходимо в адресной строке WEB-бразуера ввести URL, включающий протокол доступа (https), IP-адрес управляющего Ethernet-интерфейса (например, https://10.2.1.157) и нажать **<Enter>**. В результате должна быть загружена страница авторизации МЭ ССПТ-4А1. Пример подключения к WEB-интерфейсу МЭ ССПТ-4А1 приведен на рисунке 2.17, стр. 54.

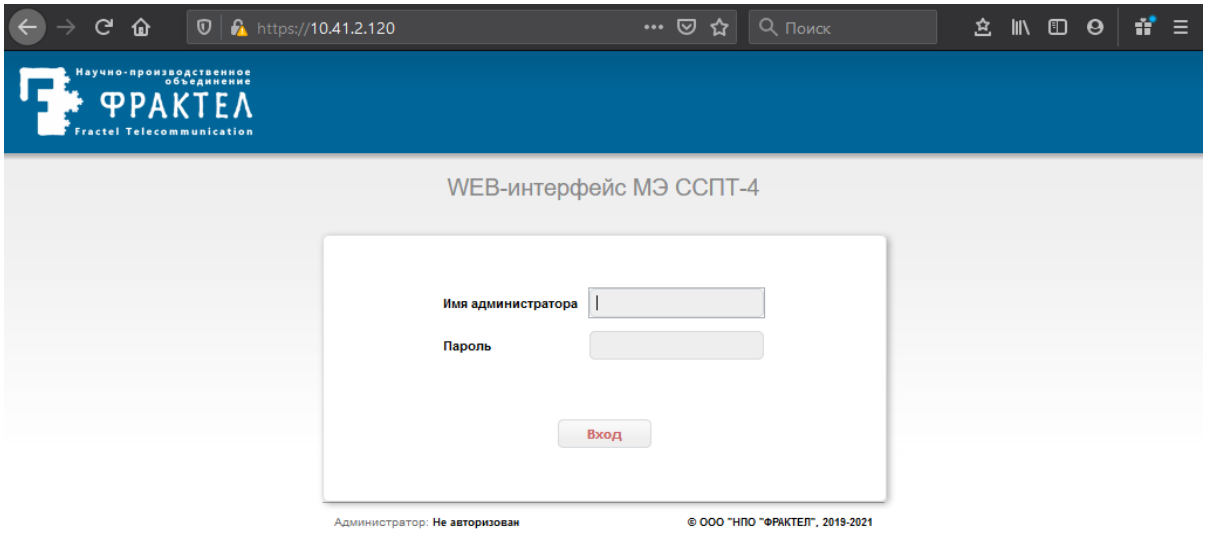


Рисунок 2.17: Подключение к WEB-интерфейсу МЭ ССПТ-4А1

Использование WEB-интерфейса для администрирования МЭ ССПТ-4А1 рассматривается в главе 4, стр. 223.

2.8. Штатное выключение устройства

Настоятельно рекомендуется выполнять процедуру штатного выключения устройства МЭ ССПТ-4А1. Для штатного выключения можно воспользоваться командным интерфейсом либо WEB-интерфейсом администратора.

В командном интерфейсе администратора для штатного выключения устройства необходимо выполнить команду **`system halt`**.

В WEB-интерфейсе администратора необходимо, находясь на странице **Состояние→Устройство**, нажать кнопку **Выключить** и в появившемся диалоговом окне также нажать кнопку **Выключить**.

В обоих случаях для штатного выключения устройства МЭ ССПТ-4А1 администратор должен иметь привилегии `admin` или `full`. В результате процедуры штатного выключения питание устройства будет автоматически выключено в течение одной минуты со старта процедуры, после чего кабель питания может быть отсоединен от устройства.

3. Принципы функционирования МЭ ССПТ-4А1

3.1. Основы использования командного интерфейса

Командный интерфейс администратора может быть использован как для локального (с системной консоли МЭ ССПТ-4А1), так и для удаленного администрирования в интерактивном режиме командной строки.

3.1.1. Структура команды

Команда имеет следующий синтаксис:

```
ключевое_слово [...] [параметр=[<значение>]]
```

где:

- `ключевое_слово` – ключевое слово командного языка. Ввод команды всегда начинается с одного или более ключевых слов;
- `параметр` – параметр команды. После последовательности ключевых слов в команде может быть указан один или более параметров. Каждый параметр должен иметь значение, которое отделяется от параметра знаком “**=**” (равно).

Формат значения параметра зависит от того, в контексте какой команды он используется.

> В командной строке ключевые слова и параметры должны отделяться друг от друга одним или несколькими символами пробела.
> Последовательность символов, отделенная символами пробела, называется *лексемой*.

Например, в команде **`policy apply name=default_accept`** имеется три лексемы: **`policy`**, **`apply`** и **`name=default_accept`**, из которых:

- **`policy`** и **`apply`** – ключевые слова команды **`policy apply`**;
- **`name`** – обязательный параметр команды **`policy apply`**;
- **`default_accept`** – значение параметра **`name`** команды, являющееся именем дополнительной политики доступа.

Основные группы команд. Весь набор команд делится на следующие основные группы:

- **`config`** – управление конфигурациями устройства;

- **filter** – управление пакетным фильтром (подсистемой фильтрации);
- **directory** – управление объектами справочника;
- **interface** – управление сетевыми интерфейсами (управляющим и фильтрующими);
- **log** – управление подсистемой регистрации;
- **nat** – управление функцией трансляции сетевых адресов (NAT);
- **policy** – управление политиками доступа;
- **rule** – управление правилами фильтрации;
- **reserv** – управление подсистемой резервирования;
- **session** – управление параметрами режима управления сессиями;
- **system** – управление параметрами функционирования УОС МЭ ССПТ-4А1;
- **user** – управление учетными записями администраторов МЭ ССПТ-4А1;
- **exit** – завершение сеанса работы администратора МЭ ССПТ-4А1.

Полный перечень команд командного языка МЭ ССПТ-4А1 с описанием назначения команд приводится в Приложении Г, стр 501. Информация по назначению конкретных параметров команд и форматам их значений доступна посредством функции контекстной справки командного интерфейса администратора.

3.1.2. Редактирование командной строки

В командном интерфейсе администратора МЭ ССПТ-4А1 ввод команд осуществляется с клавиатуры, при этом имеется возможность редактирования командной строки и перехода к ранее введенным командам, используя клавиши управления курсором и различные управляющие последовательности.

Ввод управляющей последовательности осуществляется одновременным нажатием клавиши **<Ctrl>** и одной из буквенных клавиш клавиатуры и обозначается как “**<Ctrl+буква>**”. Например, **<Ctrl+A>** обозначает одновременное нажатие клавиши **<Ctrl>** и клавиши **<A>**.
Для клавиш управления курсором используются следующие обозначения:
- **<↑>** – клавиша “стрелка вверх”;
- **<↓>** – клавиша “стрелка вниз”;
- **<←>** – клавиша “стрелка влево”;
- **<→>** – клавиша “стрелка вправо”.

Возможности по редактированию командной строки и вводу команд в командном интерфейсе администратора МЭ ССПТ-4А1 представлены в таблице 3.1, стр. 56.

Таблица 3.1: Возможности редактирования командной строки

Управление	*Назначение*
<↑>	Переход к предыдущей команде в списке ранее введенных команд
<↓>	Переход к следующей команде в списке ранее введенных команд
<←>, **<Ctrl+B>**	Перемещение курсора на одну позицию влево

Управление	Назначение
<→>, **<Ctrl+F>**	Перемещение курсора на одну позицию вправо
<Ctrl+A>	Перемещение курсора в начало командной строки (*в позицию первого символа командной строки*)
<Ctrl+E>	Перемещение курсора в конец командной строки (*в позицию за последним символом командной строки*)
<Ctrl+D>	Удаление символа в позиции курсора
<Backspace>, **<Ctrl+H>**	Удаление символа слева от позиции курсора
<Ctrl+W>	Удаление всех символов от позиции курсора до начала командной строки
<Ctrl+K>	Удаление всех символов от позиции курсора до конца командной строки
<Ctrl+U>	Удаление всех символов в командной строке
<Ctrl+T>	Смена местами символа в позиции курсора и символа слева от позиции курсора
<?>	Получение контекстной справки (раздел 3.1.5, стр. 58)
<Enter>	Передача набранной команды на выполнение

3.1.3. Использование специальных символов в параметрах команд

В командном языке МЭ ССПТ-4А1 некоторые символы имеют специальное назначение:

- '**?**' (знак вопроса) – получение контекстной справки;
- ' ' (пробел) – символ-разделитель лексем в командной строке.

Если указанные специальные символы используются в строках, определяющих значения параметров команд, то такие строки необходимо заключать в двойные кавычки ('**"**').

Строка значения параметра, заключенная в двойные кавычки, обрабатывается как единая лексема. Знак вопроса ('**?**') при этом отображается в составе командной строки, в отличие от случая использования его для получения контекстной справки.

Например:

```
fnp4> config save name=Config1 comment="Is it my config #1?"
FNPSH-I-007.02.300B-Дополнительная конфигурация сохранена (Config1)
fnp4> config list
Список дополнительных конфигураций:
    Имя     Последнее изменение                Комментарий
    Config1 05.03.2021 10:27:04 UTC+0000 (UTC) Is it my config #1?
Занято: 1       Свободно: 15
```

3.1.4. Буфер истории команд

После нажатия клавиши **<Enter>** набранная команда передается на выполнение командному интерпретатору МЭ ССПТ-4А1 и одновременно с этим запоминается в *буфере истории команд*. Таким образом формируется список ранее введенных команд, которые можно

повторно выполнять и редактировать, используя клавиши управления курсором и управляющие последовательности, перечисленные в таблице 3.1, стр. 56.

В буфере истории команд может храниться не более **100** ранее введенных команд.

Командный интерфейс администратора МЭ ССПТ-4А1 предоставляет следующие команды для управления буфером истории команд:

- **`system fnpsh history clear`** – очистка буфера истории команд;
- **`system fnpsh history show`** – просмотр содержимого буфера истории команд.

Например:

- просмотр содержимого буфера истории команд:

```
fnp4> system fnpsh history show
Буфер истории команд:
   1 - system show
   2 - log event show
   3 - log syslog show
   4 - system reboot
   5 - system show
   6 - system icheck
   7 - config save
   8 - config list
   9 - policy save
  10 - policy list
  11 - interface control set address=10.41.0.120/255.255.255.128

. . .

  43 - config default
  44 - system reboot
  45 - interface control set address=10.41.2.120/25
  46 - system route add dst-address=0.0.0.0 gateway=10.41.2.126
  47 - exit
  48 - config save name=Config1 comment="Is it my config #1?"
  49 - config list
  50 - system fnpsh history show
```

- очистка буфера истории команд (требуется подтверждение действия):

```
fnp4> system fnpsh history clear
Очистить буфер истории команд? (Y/N) [N]: Y
FNPSH-I-007.02.30BF-Буфер истории команд очищен
```

3.1.5. Получение контекстной справки

Командный интерфейс администратора МЭ ССПТ-4А1 предоставляет возможность получения контекстной справки по введенной команде.

Для получения контекстной справки в качестве последней лексемы в командной строке необходимо ввести символ '**?**' (знак вопроса). При этом введенный символ '**?**' *не отображается в командной строке*.

Контекстную справку можно получить для любого уровня лексического разбора команды. Например, для того чтобы получить справку по всем командам, предназначенным для работы с политиками доступа, следует ввести **`policy ?`**:

```
fnp4> policy
  apply    : К : применить дополнительную политику
  default  : К : сбросить политику в состояние по умолчанию
  list     : К : вывести список дополнительных политик
  remove   : К : удалить дополнительную политику
  rename   : К : переименовать дополнительную политику, изменить комментарий к ней
  rollback : К : возврат к предыдущему состоянию текущей политики
  save     : К : сохранить текущую политику как дополнительную
```

Чтобы получить справку по команде применения дополнительной политики доступа, следует ввести **`policy apply ?`**:

```
fnp4> policy apply
  name : П : имя дополнительной политики
  type : П : тип данных для применения из политики
```

Для получения краткой справки по всем группам команд следует ввести символ '?' непосредственно в первой позиции командной строки:

```
fnp4>
  config    : К : конфигурации устройства
  filter    : К : пакетный фильтр
  directory : К : объекты справочника (host, net и т.д.)
  interface : К : сетевые интерфейсы устройства
  log       : К : подсистема регистрации
  nat       : К : NAT
  policy    : К : действия над политиками доступа
  rule      : К : правила фильтрации
  reserv    : К : резервирование
  session   : К : механизм управления сессиями
  system    : К : параметры операционной системы
  user      : К : база данных администраторов
  exit      : К : выход из интерфейса командной строки
```

В строках вывода контекстной справки используются следующие условные обозначения:

- **К** – в данной строке вывода контекстной справки приводится описание *ключевого слова* командного языка МЭ ССПТ-4А1;
- **П** – в данной строке вывода контекстной справки приводится описание *параметра команды*, по которой была запрошена справочная информация;
- **З** – в данной строке вывода контекстной справки приводится описание *значения параметра команды* (конкретное значение либо последовательность символов, обозначающая допустимый формат значений).

3.1.6. Режим автодополнения

Командный интерфейс администратора МЭ ССПТ-4А1 предоставляет возможность автодополнения лексем в командной строке (далее – функция *автодополнения командного интерфейса*). Функция автодополнения действует для следующих типов лексем:

- ключевые слова командного языка МЭ ССПТ-4А1;
- имена параметров команды;

- значения параметров (*если значение параметра совпадает с ключевым словом и перечень допустимых значений параметра ограничен*).

Автодополнение или *краткая контекстная подсказка* выполняется по нажатию клавиши **<Tab>**, когда курсор располагается *в конце командной строки*.

В зависимости от текущего содержимого командной строки возможен один из следующих вариантов обработки нажатия клавиши **<Tab>**:

- если введенным начальным символам однозначно соответствует какое-либо из ключевых слов командного языка МЭ ССПТ-4А1, то последняя лексема в командной строке автоматически заменяется полным ключевым словом, т. е. выполняется *автодополнение*;
- если введенным начальным символам может соответствовать несколько ключевых слов командного языка МЭ ССПТ-4А1, то в качестве справочной информации выводятся *все ключевые слова*, начинающиеся с последовательности символов, составляющих последнюю лексему командной строки;
- если введенным начальным символам не соответствует ни одного ключевого слова, то выводится *соответствующее диагностическое сообщение*;
- если в текущей позиции курсора ожидается значение параметра (IP-адрес, MAC-адрес, число, строка) то в качестве справочной информации выводится строка, поясняющая формат значения параметра, либо перечень допустимых значений параметра, если он ограничен;
- если в текущей позиции курсора должен быть первый символ очередного ключевого слова команды, то в качестве справочной информации выводится перечень ключевых слов, допустимых в данном контексте.

Ниже приводятся примеры вариантов использования функции автодополнения.

- автодополнение ключевого слова команды:

  ✔ ввод в командной строке:

```
fnp4> policy app<Tab>
```

  ✔ результат:

```
fnp4> policy apply
```

- автодополнение параметра команды:

  ✔ ввод в командной строке:

```
fnp4> policy apply na<Tab>
```

  ✔ результат:

```
fnp4> policy apply name=
```

- вывод ключевых слов, допустимых для данного контекста:

  ✔ ввод в командной строке:

```
fnp4> policy <Tab>
```

✔ результат:

```
  apply        default      list         remove
  rename       rollback     save
fnp4> policy
```

- вывод формата значения параметра:

✔ ввод в командной строке:

```
fnp4> policy apply name=<Tab>
```

✔ результат:

```
  <name>
fnp4> policy apply name=
```

- вывод перечня допустимых значений параметра команды:

✔ ввод в командной строке:

```
fnp4> system time ntp set state=<Tab>
```

✔ результат:

```
  disable     enable
fnp4> system time ntp set state=
```

Перед выполнением команды все ее ключевые слова (в том числе параметры) должны быть введены полностью: вручную или с использованием функции автодополнения.

3.1.7. Сеанс работы администратора

Пройдя оба уровня авторизации (раздел 2.7.1, стр. 52), администратор получает доступ к командному интерфейсу МЭ ССПТ-4А1. Появление на экране терминала подсказки командной строки **fnp4>** означает, что командный интерфейс готов к работе и ожидает ввода команд. С этого момента начинается сеанс работы администратора.

Сеанс работы администратора завершается в одном из следующих случаев:

- администратор выполнил команду **exit**:

```
fnp4> exit
FNPSH-I-007.02.3003-Завершение работы администратора (admin)
```

- превышен лимит времени неактивности администратора – тайм-аут неактивности. Если администратор не производит выполнение команд в течение этого времени, то сеанс работы администратора автоматически завершается:

```
fnp4>
FNPSH-I-007.02.3005-Выход администратора по тайм-ауту неактивности (admin)
```

По умолчанию тайм-аут неактивности администратора составляет **600 секунд (10 минут)**.

Для изменения значения тайм-аута неактивности администратора используется команда **`system fnpsh set`** с параметром **`timeout`**. Значение параметра – новое значение тайм-аута неактивности в секундах:

```
fnp4> system fnpsh set timeout=180
FNPSH-I-007.02.30BE-Тайм-аут неактивности командного интерфейса изменен
fnp4>
```

Тайм-аут неактивности администратора может быть изменен только в ограниченных пределах:

- минимальное значение – **10 секунд**;
- максимальное значение – **6000 секунд (100 минут)**.

Для просмотра текущего значения тайм-аута неактивности администратора используется команда **`system show`** (строка вывода – “**`Тайм-аут неактивности администратора`**”):

```
fnp4> system show
Центральный процессор                | Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
Число ядер процессора                | 4
Объем оперативной памяти             | 4277645312 байт (4079M)
Версия ПО ССПТ-4                     | FNP4 1.0.0-RELEASE (Mar  3 2021)
Заводской номер                      | 000000
Всего сетевых интерфейсов            | 10
    Фильтрующие интерфейсы           | 9: eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8
    Управляющий интерфейс            | включен, 10.41.2.120/255.255.255.128
Пакетная фильтрация                  | запущен (доступен)
Контроль целостности                 | запущен (доступен)
Авторизация                          | запущен (доступен)
Регистрация                          | запущен (доступен)
Резервирование                       | запущен (доступен)
Удаленное администрирование          | запущен (доступен)
WEB-интерфейс                        | запущен (доступен)
SNMP-интерфейс                       | запущен (доступен)
Тайм-аут неактивности администратора | 600 секунд
Просмотрщик по умолчанию FNPSH       | внутренний (internal)
Имя устройства                       | fnp4
Комментарий к устройству             |
```

3.1.8. Настройка режима просмотра данных

Для удобства просмотра больших объемов данных, таких, как правила фильтрации, журналы регистрации, в КИА предусмотрены следующие режимы просмотра:

- `internal` – полноэкранный просмотр данных с использованием внутреннего просмотрщика. В этом режиме реализован как построчный, так и постраничный просмотр данных с возможностью перемещения вперед и назад;
- `more` – упрощенный постраничный просмотр данных с возможностью перемещения вперед и назад;
- `no` – сплошной вывод данных на экран без возможности построчного и постраничного просмотра. Возможно частичное исчезновение строк вверху терминала при выводе больших объемов данных, превышающих по количеству строк размер экрана терминала.

Для выбора режима просмотра служит параметр **viewer=<значение>**. Данный параметр можно использовать в любой команде, предусматривающей вывод большого объема данных.

По умолчанию используется полноэкранный режим просмотра данных – **internal**.

При использовании полноэкранного режима просмотра данных **минимально допустимый** размер окна терминала составляет **80x16** (80 символов в строке, 16 строк). В случае, если размер окна используемого терминала окажется меньше указанного значения, будет выведено соответствующее сообщение об ошибке.

Рекомендуемый минимальный размер окна терминала **80x24** (80 символов в строке, 24 строки). При меньшем размере окна некоторые данные могут быть выведены с искажением или не выведены вовсе.

Полноэкранный режим просмотра данных. В этом режиме пользователь имеет возможность просмотра данных, используя клавиши управления курсором и управляющие последовательности, перечисленные в таблице 3.2, стр. 63.

Таблица 3.2: Управление в полноэкранном режиме просмотра данных

Управление	*Назначение*
<↑>	Перемещение на одну строку вверх
<↓>	Перемещение на одну строку вниз
<←>	Перемещение на одну позицию влево
<→>	Перемещение на одну позицию вправо
<Home>	Перемещение к первой позиции в строке
<End>	Перемещение к последней позиции самой длинной строки
<Page Up>	Перемещение на один экран вверх
<Page Down>	Перемещение на один экран вниз
<Ctrl+B>	Перемещение к первой строке данных
<Ctrl+E>	Перемещение к последней строке данных
<H>	Вывод подсказки по клавишам управления просмотром данных
<F10>, <Q>	Завершение просмотра данных

Для иллюстрации работы полноэкранного режима на рисунке 3.1, стр. 64 представлен вывод параметров конфигурации МЭ ССПТ-4А1, выполненный по команде **config show viewer=internal**. Если терминал не поддерживает ANSI-цвета, будет автоматически использоваться *монохромный режим* работы терминала.

Режим постраничного просмотра данных. В этом режиме администратор имеет возможность построчного и постраничного просмотра данных, используя клавиши управления курсором и управляющие последовательности, перечисленные в таблице 3.3, стр. 63.

Таблица 3.3: Управление в режиме постраничного просмотра данных

Управление	*Назначение*
<↑>	Перемещение на одну строку вверх
<↓>	Перемещение на одну строку вниз

Управление	*Назначение*
<Page Up>	Перемещение на один экран вверх
<Page Down>	Перемещение на один экран вниз
<Q>	Завершение просмотра данных

Для иллюстрации работы режима постраничного просмотра данных на рисунке 3.2, стр. 65 представлен вывод параметров конфигурации МЭ ССПТ-4А1, выполненный по команде **`config show viewer=more`**. Используется только монохромный режим работы терминала. Просмотр автоматически завершается после вывода на экран терминала последней строки данных.

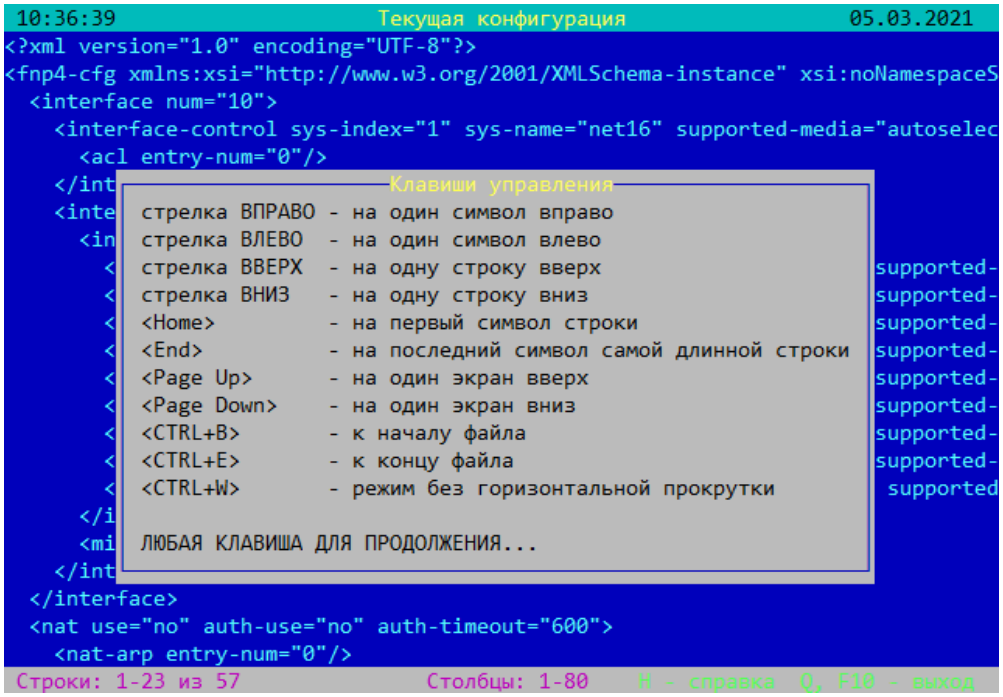


Рисунок 3.1: Полноэкранный режим просмотра данных

```
Текущая конфигурация:

<?xml version="1.0" encoding="UTF-8"?>
<fnp4-cfg xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceS
chemaLocation="fnp4_cf.xsd" version="1.0.0" device-name="fnp4" device-comment=""
>
  <interface num="10">
    <interface-control sys-index="1" sys-name="net16" supported-media="autoselec
t" min-mtu="72" max-mtu="9000" address="10.41.2.120" mask="255.255.255.128" use=
"yes" media="autoselect" duplex="" mtu="1500" lagg-use="no" lagg-proto="failover
" lagg-if-num="0">
      <acl entry-num="0"/>
    </interface-control>
    <interface-filter>
      <interface-filter-list entry-num="9">
        <interface-filter-entry num="0" sys-index="2" sys-name="net0" supported-
media="autoselect" min-mtu="72" max-mtu="9000" adm-name="eth0" media="autoselect
" duplex="" status="up" mtu="1500"/>
        <interface-filter-entry num="1" sys-index="3" sys-name="net1" supported-
media="autoselect" min-mtu="72" max-mtu="9000" adm-name="eth1" media="autoselect
" duplex="" status="up" mtu="1500"/>
        <interface-filter-entry num="2" sys-index="4" sys-name="net2" supported-
media="autoselect" min-mtu="72" max-mtu="9000" adm-name="eth2" media="autoselect
" duplex="" status="up" mtu="1500"/>
<Enter> - Далее...       <Q> - Выход
```

Рисунок 3.2: Режим постраничного просмотра данных

Режим сплошного вывода данных. В этом режиме администратор не имеет возможности управления просмотром данных. Данные выводятся на экран терминала построчно. Если количество строк данных превышает размер терминального окна по вертикали, то вывод строк будет частично потерян за счет автоматической прокрутки (*scrolling*) терминала.

Для установки режима просмотра данных по умолчанию используется команда **`system fnpsh set`** с параметром **`viewer`**:

- **`system fnpsh set viewer=internal`** – установка полноэкранного режима просмотра данных;
- **`system fnpsh set viewer=more`** – установка режима постраничного просмотра данных;
- **`system fnpsh set viewer=no`** – установка режима сплошного просмотра данных.

Изменение режима просмотра данных действует только на время текущего сеанса работы администратора.

Следующий пример иллюстрирует установку режима постраничного просмотра данных:

```
fnp4> system fnpsh set viewer=more
FNPSH-I-007.02.30BD-Режим просмотра изменен
```

3.1.9. Диагностические сообщения командного интерфейса

Выполнение команд в командном интерфейсе завершается выводом диагностического сообщения на экран терминала. Диагностическое сообщение имеет следующий формат:

```
<ПРЕФИКС_ПОДСИСТЕМЫ>-{E|W|I}-XXX.YY.ZZZZ-<текст_сообщения>[ (<системная_ошибка>)]
```

где:

- `<ПРЕФИКС_ПОДСИСТЕМЫ>` – идентификатор подсистемы, от которой получено сообщение:
  - ✔ `FNPAPI` – сообщения библиотеки сервисных функций ПО МЭ ССПТ-4А1;
  - ✔ `FNPSH` – сообщения командного интерпретатора МЭ ССПТ-4А1;
  - ✔ `FNPSHD` – сообщения командного сервера МЭ ССПТ-4А1;
- `{E|W|I}` – класс (категория) сообщения:
  - ✔ `E` – сообщение об ошибке;
  - ✔ `W` – предупреждающее сообщение;
  - ✔ `I` - информационное сообщение;
- `XXX.YY.ZZZZ` – составной код сообщения (`XXX`, `YY`, `ZZZZ` - шестнадцатеричные числа):
  - ✔ `XXX` – код продукта. Для ПО МЭ ССПТ-4А1 код продукта – `007`;
  - ✔ `YY` – код подсистемы ПО МЭ ССПТ-4А1:
    - ◆ `01` – библиотека сервисных функций ПО МЭ ССПТ-4А1;
    - ◆ `02` – командный интерпретатор МЭ ССПТ-4А1;
    - ◆ `03` – командный сервер МЭ ССПТ-4А1;
  - ✔ `ZZZZ` – код диагностического сообщения данной подсистемы ПО МЭ ССПТ-4А1:
    - ◆ `1ZZZ` – диапазон кодов для сообщений об ошибках;
    - ◆ `2ZZZ` – диапазон кодов для предупреждающих сообщений;
    - ◆ `3ZZZ` – диапазон кодов для информационных сообщений;
- `<текст_сообщения>` – текстовая интерпретация кода диагностического сообщения. Текст сообщения выводится на русском языке в кодировке UTF-8;
- `<системная_ошибка>` – необязательное сообщение, включаемое в строку диагностического сообщения, если при выполнении команды произошла системная ошибка. Сообщения о системных ошибках являются стандартными для УОС МЭ ССПТ-4А1.

Полный список кодов диагностических сообщений приводится в приложении В, стр. 443.

3.2. Режимы фильтрации МЭ ССПТ-4А1

МЭ ССПТ-4А1 реализует два основных режима фильтрации сетевых пакетов:

1) режим **пакетной фильтрации**;

2) режим **управления сессиями**.

Основным режимом фильтрации, установленным по умолчанию и обеспечивающим наиболее полный функционал, является режим управления сессиями. Включенный режим управления сессиями обеспечивает использование следующих функциональных возможностей:

1) трансляция сетевых адресов (функция *NAT*);

2) аутентификация сетевых пользователей при использовании функции NAT;

3) обнаружение и блокировка *flood-атак;*

4) приоритетная обработка трафика.

3.2.1. Режим управления сессиями

Общая информация. В режиме управления сессиями реализована следующая последовательность действий:

1) проверка поступившего пакета на принадлежность к одной из существующих сессий;

2) в случае нахождения подходящей сессии – контроль непротиворечивости параметрам сессии;

3) в случае отсутствия подходящей сессии – фильтрация первого пакета виртуального соединения по правилам фильтрации;

4) выявление параметров виртуального соединения между парой адресатов в случае, если принято решение пропустить пакет;

5) создание виртуальной сессии по выявленным параметрам.

Таким образом, в режиме управления сессиями фильтрация по общим правилам осуществляется для первого пакета виртуальной сессии, в то время как остальные пакеты проверяются только на соответствие контексту сессии.

Фильтрация по общим правилам (в режиме управления сессиями) также выполняется **при изменении текущей политики доступа** для первого пакета, поступившего от клиента с момента изменения политики доступа. Данная обработка выполняется при всех изменениях текущей политики доступа, за исключением следующих:

- применение дополнительной политики доступа;
- сброс политики доступа в состояние по умолчанию;
- отмена последнего изменения политики доступа.

Максимальное количество одновременно обслуживаемых сессий – **200 000**.

Основным параметром, идентифицирующим сессию, является ее идентификатор. Идентификатор сессии состоит из двух чисел, разделенных точкой. Первое число является номером программного потока фильтрации, обрабатывающего пакеты в рамках данной сессии. Второе число является порядковым номером сессии в данном потоке фильтрации. Таким

образом, идентификатор является уникальным для каждой сессии и позволяет делать выводы о равномерности нагрузки на МЭ ССПТ-4А1 при просмотре таблицы сессий.

> В МЭ ССПТ-4А1 для повышения быстродействия используется многопоточная обработка трафика.
>
> Количество потоков фильтрации находится в прямой зависимости от количества ядер ЦП МЭ ССПТ-4А1.
>
> Распределение трафика зависит от параметров пакетов и осуществляется автоматически. В случае N ядер, оптимальной считается такая загрузка, при которой в таблице сессий примерно равное количество сессий с идентификаторами, начинающимися с 0 до N-1.

Сессии с протоколом TCP подразумевают более сложную обработку пакета, так как помимо общих параметров (адреса, порты) контролируются флаги в пакетах, соответствие номеров последовательностей и подтверждений, а также корректность переходов между состояниями виртуального TCP-соединения. При необходимости осуществлять обработку TCP-пакетов быстрее можно отключить опцию “*Глубокий контроль TCP-сессий*”. В этом случае не будет производиться контроль флагов и номеров последовательностей и подтверждений пакетов, а также будет исключена часть проверок корректности переходов между состояниями TCP-соединения.

Включение режима управления сессиями. Для включения режима управления сессиями используется команда **`session enable`**:

```
fnp4> session enable
FNPSH-I-007.02.3085-Режим управления сессиями включен
```

Проверить, установлен ли режим управления сессиями в текущей конфигурации МЭ ССПТ-4А1 можно, воспользовавшись командой **`session show`**:

```
fnp4> session show
Управление сессиями:                                включено
Регистрация отброшенных пакетов:                    выключено
Использование AP-правил:                            выключено
Использование данных канального уровня:             включено
Глубокий контроль TCP:                              включено
Поддержка traceroute-сессий:                        включено
Тайм-ауты неактивности сессий (сек):
    TCP: инициализация (SYN, SYNACK):               5 (по умолчанию)
    TCP: установлено (ESTABLISHED):                 3600 (по умолчанию)
    TCP: завершение (FIN, FINACK, FINFINACK):       600 (по умолчанию)
    UDP: инициализация (SYN):                       5 (по умолчанию)
    UDP: установлено (ESTABLISHED):                 60 (по умолчанию)
    ICMP: инициализация (SYN):                      5 (по умолчанию)
    ICMP: установлено (ESTABLISHED):                20 (по умолчанию)
    Остальные протоколы: инициализация (SYN):       5 (по умолчанию)
    Остальные протоколы: установлено (ESTABLISHED): 30 (по умолчанию)
Обнаружение flood-атак:                             выключено
    Генерация сообщения alarm:                      выключено
    Пороговое значение для TCP (пакеты/сек):        1000 (по умолчанию)
    Пороговое значение для UDP (пакеты/сек):        500 (по умолчанию)
    Пороговое значение для ICMP (пакеты/сек):       300 (по умолчанию)
    Время жизни TMP-правила (сек):                  60 (по умолчанию)
    Регистрации пакетов для TMP-правила:            выключено
    Комментарий к TMP-правилу:                      Blocked flood attack
```

Помимо состояния режима управления сессиями данная команда выводит общие для всех сессий параметры. Кроме того, проверить основные функциональные возможности МЭ ССПТ-4А1, используемые в текущей конфигурации, можно, выполнив команду **`system show type=config`**:

```
fnp4> system show type=config
Управление сессиями                  | включено
Трансляция адресов (NAT)             | выключено
Аутентификация сетевых пользователей | выключено
HTTP-посредник                       | выключено
Агрегирование портов                 | выключено
Использование прикладных правил      | выключено
Использование правил приоритизации   | выключено
Регистрация пакетов                  | выключено
Резервирование                       | выключено
RADIUS-авторизация                   | выключено
```

При включенном режиме управления сессиями по умолчанию сессии будут созданы для всех соединений поддерживаемых протоколов, если первый пакет устанавливаемого соединения пропущен правилами фильтрации. В случае необходимости можно отключить создание сессий для отдельных правил фильтрации путем настройки в правиле фильтрации параметра **`session=disable`**, например:

```
fnp4> rule edit rule:10 session=disable
Изменить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3047-Общее правило изменено (10)
```

При включенном **режиме управления сессиями** пакеты от сервера к клиенту не проверяются на соответствие общим правилам фильтрации. Вместо этого они обрабатываются в таблице сессий на соответствие контексту сессии. Необходимо это учитывать при формировании политики доступа.

Настройка режима управления сессиями. Помимо команд включения/выключения режима управления сессиями, командный интерфейс МЭ ССПТ-4А1 предоставляет возможности настройки режима управления сессиями и контроля за их состоянием:

- команды настройки контролируемых параметров сессии;
- команды регистрации;
- команды просмотра и управления таблицей сессий;
- команды управления тайм-аутами для сессий;
- команды настройки обнаружения flood-атак;

Команды настройки контролируемых параметров сессии. По умолчанию для TCP-пакетов включена опция *глубокий контроль TCP*. Для включения и выключения опции *глубокий контроль TCP* используются команды **`session deeptcp enable`** и **`session deeptcp disable`** соответственно. Пример команды включения опции:

```
fnp4> session deeptcp enable
FNPSH-I-007.02.3094-Глубокий контроль TCP включен
```

При включенной опции глубокого контроля TCP для каждого пакета проверяются следующие параметры в отношении соответствующей ему TCP-сессии:

- корректность номеров последовательностей и подтверждений;
- корректность набора TCP-флагов и соответствие их текущему состоянию сессии.

При выключенной опции глубокого контроля TCP данные проверки не выполняются. Кроме того, в зависимости от использования опции глубокого контроля TCP сессия имеет разный перечень возможных состояний. Перечень состояний при включенной опции глубокого контроля TCP приведен в таблице 3.4, стр. 74, при выключенной – в таблице 3.5, стр. 75.

В режиме управления сессиями, помимо контроля соответствия параметров сетевого уровня, существует возможность включения контроля данных канального уровня для пакетов при отнесении их к сессии. В этом случае при проверке принадлежности пакета к сессии дополнительно проверяется соответствие *MAC-адреса* источника и назначения, а также *VLAN-идентификатор*. Для включения и выключения контроля параметров канального уровня используются команды **`session mac enable`** и **`session mac disable`** соответственно. Пример команды включения контроля параметров канального уровня:

```
fnp4> session mac enable
FNPSH-I-007.02.3092-Использование данных канального уровня включено
```

В режиме управления сессиями возможна поддержка *traceroute-сессий* – соотнесение ответных *ICMP*-сообщений с породившими их *TCP* или *UDP*-сессиями. Включение и выключение поддержки *traceroute-сессий* осуществляется с использованием команд **`session trace enable`** и **`session trace disable`** соответственно. Пример команды включения поддержки traceroute-сессий:

```
fnp4> session trace enable
FNPSH-I-007.02.3124-Поддержка traceroute-сессий включена
```

В режиме управления сессиями существует возможность фильтрации прикладных данных. Для того, чтобы иметь возможность фильтрации прикладных данных, необходимо включить поддержку фильтрации прикладных данных, создать прикладные правила фильтрации (*AP-правила*), и привязать их к общим правилам фильтрации. Более подробную информацию об этом можно найти в разделе 3.7.3, стр. 147. Для включения и выключения возможности фильтрации прикладных данных используются команды **`session ap enable`** и **`session ap disable`** соответственно. Пример команды включения фильтрации прикладных данных:

```
fnp4> session ap enable
FNPSH-I-007.02.3087-Использование AP-правил включено
```

Команды регистрации. Регистрация сессий включена по умолчанию для всех сессий. В случае, если необходимо выключить регистрацию для каких-либо сессий, можно изменить

настройки параметра **log** в соответствующем правиле фильтрации, отключив регистрацию всех сессий (и пакетов), созданных по данному правилу фильтрации:

```
fnp4> rule edit rule:10 log=disable
Изменить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3047-Общее правило изменено (10)
```

При использовании режима управления сессиями пакеты могут быть отброшены *модулем управления сессиями* в следующих случаях:

- пакет имеет некорректный набор флагов TCP для создания сессии (при включенном глубоком контроле TCP);
- пакет не соответствует контексту сессии.

При этом такие пакеты могут быть зарегистрированы в журнале регистрации трафика. Для управления данной опцией предназначена функция регистрации пакетов, отброшенных механизмом управления сессиями. По умолчанию данная функция выключена в текущей конфигурации. Для ее включения используется команда **session invalid log enable**, например:

```
fnp4> session invalid log enable
FNPSH-I-007.02.3052-Регистрация IP-пакетов, отброшенных механизмом управления сессиями,
включена
```

При включении данной функции, если включена функция регистрации пакетов (команда **log packet enable**), в журнале регистрации пакетов будут регистрироваться пакеты, отброшенные модулем управления сессиями. В детальной информации записи регистрации такого пакета доступна информация о причине его удаления. Полный перечень возможных причин удаления пакета модулем управления сессиями доступен в приложении Б.3, стр. 441 (коды соответствующих ошибок: **3006**, **3009-300F** и **3121**).

Команды просмотра и управления таблицей сессий. Для просмотра таблицы сессий служит команда **session table show**. По умолчанию при выполнении данной команды выводится вся таблица сессий с сортировкой записей по скорости. Пример вывода данной команды представлен на рис. 3.3, стр. 72 и на рис. 3.4, стр. 72.

```
11:50:04                          Таблица сессий                          09.03.2021
Номер Правило Удаление VLAN            Клиент          Сервер Протокол   Состоян
  1.3       0     3600   -1 2:10.10.1.1:32390 1:10.10.0.1:22  tcp/ssh ESTABLISH
  3.4       0       20   -1       2:10.10.1.1    1:10.10.0.1  icmp(1) ESTABLISH

123456789 Авто | Сессий: 2                                   Страница: 1 из 1
                          H - справка  Q, F10 - выход
```

Рисунок 3.3: Таблица сессий

```
11:57:12                          Таблица сессий                          09.03.2021
   Клиент          Сервер Протокол   Состояние Пакеты     Байты Пакеты/с Байты/с
.1.1:14051 1:10.10.0.1:22  tcp/ssh ESTABLISHED  33-29  2,5K-10K        0     411
:10.10.1.1    1:10.10.0.1  icmp(1) ESTABLISHED  34-34 2,1K-2,1K        2     128

123456789 Авто | Сессий: 2                                   Страница: 1 из 1
                          H - справка  Q, F10 - выход
```

Рисунок 3.4: Таблица сессий после горизонтальной прокрутки вправо

Каждая строка вывода содержит следующую информацию о сессии:

- номер сессии, состоящий из двух чисел, разделенных точкой (столбец “**Номер**”);
- номер общего правила, на основе которого создана сессия (столбец “**Правило**”);
- число секунд до удаления сессии, время создания сессии, время неактивности сессии (столбцы “**Удаление**”, “**Старт**” и “**Тайм-аут**” соответственно) – в соответствующей позиции выводится один из перечисленных столбцов, по умолчанию – “**Удаление**”;

- идентификатор VLAN, к которой принадлежат пакеты данной сессии (значение -1 означает, что VLAN не используется) (столбец “**VLAN**”);
- атрибуты клиента – номер фильтрующего интерфейса МЭ ССПТ-4А1, IPv4- либо IPv6-адрес клиента и номер порта (для протоколов TCP и UDP) (столбец “**Клиент**”);
- атрибуты сервера – номер фильтрующего интерфейса МЭ ССПТ-4А1, IPv4- либо IPv6-адрес сервера и номер порта (для протоколов TCP и UDP) (столбец “**Сервер**”);
- протоколы сессии: протокол, инкапсулированный в IP, и протокол прикладного уровня в случае TCP или UDP (столбец “**Протоколы**”);
- текущее состояние сессии (столбец “**Состояние**”);
- количество пакетов, переданных в контексте данной сессии (столбец “**Пакеты**”);
- количество байт в пакетах, переданных в контексте данной сессии (столбец “**Байты**”);
- скорость передачи трафика в контексте данной сессии в числе пакетов в секунду (столбец “**Пакеты/с**”);
- скорость передачи трафика в контексте данной сессии в числе байтов в секунду (столбец “**Байты/с**”).

Команда **session table show** при отсутствии параметров:
- выводит все записи из таблицы сессий;
- записи сортируются в порядке убывания скорости передачи трафика в числе байтов в секунду.

При подсчете скорости передачи трафика в контексте данной сессии в числе пакетов в секунду и в числе байтов в секунду используются суммарные значения (от клиента к серверу и в обратном направлении) пакетов и байтов соответственно.

Время создания сессии выводится в формате:

`ЧЧ:ММ:СС`

где:

- ЧЧ – часы в 24-часовом формате;
- ММ – минуты;
- СС – секунды.

Число секунд до удаления сессии показывает количество секунд, оставшихся до удаления сессии в том случае, если не будет принято ни одного пакета в контексте данной сессии.

При просмотре таблицы сессий возможны случаи, когда для некоторых сессий число секунд до удаления сессии является отрицательным значением. Это означает, что сессия будет автоматически удалена модулем управления сессиями, как устаревшая, на следующем цикле обработки таблицы сессий.

Время неактивности сессии показывает количество секунд, прошедших с момента времени, когда был принят последний пакет в контексте данной сессии.

Каждая сессия отражает сетевое взаимодействие между двумя узлами сети. Инициатор сетевого взаимодействия называется *клиентом*, противоположная сторона – *сервером*. Атрибуты клиента и сервера выводятся в формате:

`<интерфейс>:<IP_адрес>[:<порт>]`

где:

- `<интерфейс>` – номер фильтрующего интерфейса МЭ ССПТ-4А1, на который принимаются пакеты, входящие в контекст сессии, от данной стороны сетевого взаимодействия – клиента или сервера;
- `<IP_адрес>` – IPv4-адрес или IPv6-адрес стороны сетевого взаимодействия;
- `<порт>` – номер порта стороны сетевого взаимодействия (только для сессий, базирующихся на транспортных протоколах TCP и UDP).

Столбец протоколов содержит имена протоколов транспортного и прикладного уровней, которые используются в данной сессии. Протоколы прикладного уровня указываются только для сессий, использующих транспортные протоколы TCP и UDP.

По мере обработки пакетов каждая сессия может последовательно находиться в нескольких состояниях. Набор возможных состояний для сессий, базирующихся на разных протоколах (TCP, UDP, ICMP и других), различный. Перечень состояний и их описание для протокола TCP при включенной опции *глубокого контроля TCP* (по умолчанию – включена) приводится в таблице 3.4. Перечень состояний и их описание для протоколов UDP, ICMP и других протоколов, непосредственно использующих протокол IP, а также для протокола TCP при отключенной опции *глубокого контроля TCP*, приводится в таблице 3.5.

Таблица 3.4: Состояния TCP-сессии при включенной опции глубокого контроля TCP

Состояние	***Описание***
SYN	Виртуальное TCP-соединение устанавливается – получен SYN-пакет от клиента.
SYNACK	Виртуальное TCP-соединение устанавливается – получен ответный SYN-пакет от сервера.
ESTABLISHED	Виртуальное TCP-соединение установлено. В этом состоянии происходит передача данных прикладного уровня между клиентом и сервером.
FIN	Одна из сторон соединения прекратила передачу данных – от нее получен FIN-пакет
FINFIN	Обе стороны соединения прекратили передачу данных – получены FIN-пакеты от обеих сторон, но еще ни один из них не подтвержден.
FINACK	Одна из сторон соединения прекратила передачу данных и другая сторона это подтвердила – от нее получен ACK-пакет.
FINFINACK	Обе стороны соединения прекратили передачу данных – получены FIN-пакеты от обеих сторон и от одной из сторон соединения получено подтверждение – ACK-пакет.
TIMEWAIT	Обе стороны соединения прекратили передачу данных и подтвердили это. Ожидание запоздавших пакетов.
RESET	Одна из сторон сбросила соединение, отправив другой стороне RST-пакет Ожидание серии RST-пакетов (*характерно для некоторых приложений*).

Состояние	Описание
CLOSED	Сессия закрыта.

Таблица 3.5: Состояния сессий для протоколов UDP, ICMP и других, а также TCP при отключенной опции глубокого контроля TCP

Состояние	Описание
SYN	Сессия устанавливается – получен пакет от клиента (для ICMP – эхо-запрос)
ESTABLISHED	Сессия установлена – получен пакет от сервера (для ICMP – эхо-ответ)

Количество пакетов/байтов, переданных в контексте сессии, выводится в формате:

`<клиент>-<сервер>`

где:

- `<клиент>` – количество пакетов/байтов, переданных в направлении от клиента к серверу;
- `<сервер>` – количество пакетов/байтов, переданных в направлении от сервера к клиенту.

При подсчете скорости передачи трафика в контексте данной сессии в числе пакетов в секунду и в числе байтов в секунду используются суммарные значения (от клиента к серверу и в обратном направлении) пакетов и байтов соответственно.

Информация, выводимая в таблице сессий, обновляется каждые **5** секунд. Автоматическое обновление информации может быть выключено (включено) однократным нажатием клавиши **<F>** во время просмотра таблицы сессий.

Для просмотра таблицы сессий используются клавиши и управляющие последовательности, перечисленные в таблице 3.6, стр. 75.

Таблица 3.6: Управление просмотром таблицы сессий

Управление	Назначение
<↑>	Перемещение на одну строку таблицы сессий вверх
<↓>	Перемещение на одну строку таблицы сессий вниз
<←>	Перемещение влево на одну позицию
<→>	Перемещение вправо на одну позицию
<Home>	Перемещение к первой позиции строк таблицы сессий
<End>	Перемещение к последней позиции строк таблицы сессий
<Page Up>	Переход к предыдущей странице вывода таблицы сессий
<Page Down>	Переход к следующей странице вывода таблицы сессий
<R>	Обновление информации о таблице сессий
<F>	Выключение/включение автоматического обновления информации в таблице сессий
1	Скрыть/показать столбец “Правило” таблицы сессий
2	Последовательно скрыть/показать столбцы “Удаление”, “Старт” и “Тайм-аут” таблицы сессий
3	Скрыть/показать столбец “VLAN” таблицы сессий
4	Скрыть/показать столбец “Клиент” таблицы сессий
5	Скрыть/показать столбец “Сервер” таблицы сессий
6	Скрыть/показать столбец “Протоколы” таблицы сессий
7	Скрыть/показать столбец “Состояние” таблицы сессий

Управление	Назначение
8	Скрыть/показать столбец “Пакеты” таблицы сессий
9	Скрыть/показать столбец “Байты” таблицы сессий
<H>	Вывод подсказки по клавишам управления просмотром таблицы сессий
<F10>, <Q>	Завершение выполнения команды

Сортировка записей таблицы сессий. Выше было указано, что по умолчанию (при отсутствии параметров команды **`session table show`**) записи таблицы сортируются в порядке убывания скорости передачи трафика в числе байтов в секунду. Порядок сортировки может быть явно задан с помощью параметра **`order`** (по возрастанию или по убыванию), а критерий сортировки – с помощью параметра **`sort`**.

Порядок сортировки записей таблицы сессий по умолчанию – **по убыванию** значения критерия сортировки.

Например, для сортировки записей таблицы в порядке возрастания номера порта сервера необходимо выполнить команду:

```
fnp4> session table show order=asc sort=portsrv
```

Полный перечень допустимых критериев сортировки записей представлен ниже:

- **`sid`** – сортировка по идентификатору сессии;
- **`ipcl`** – сортировка по IP-адресу клиента;
- **`ipsrv`** – сортировка по IP-адресу сервера;
- **`portcl`** – сортировка по порту клиента;
- **`portsrv`** – сортировка по порту сервера;
- **`tproto`** – сортировка по протоколу, инкапсулированному в IP;
- **`aproto`** – сортировка по прикладному протоколу;
- **`state`** – сортировка по состоянию сессии;
- **`rule`** – сортировка по номеру общего правила, на основе которого создана сессия;
- **`traffic-pkts`** – сортировка по количеству пакетов, переданных в контексте сессии;
- **`traffic-bytes`** – сортировка по количеству байт, переданных в контексте сессии;
- **`speed-pkts`** – сортировка по скорости передачи трафика в числе пакетов в секунду;
- **`speed-bytes`** – сортировка по скорости передачи трафика в числе байт в секунду.

Выборка записей таблицы сессий. Команда **`session table show`** также позволяет выводить в таблице сессий только записи, удовлетворяющие комбинации критериев отбора. Критерии отбора задаются через необязательные параметры команды **`session table show`**. Например, для выбора записей с портом сервера 22 протокола TCP необходимо выполнить следующую команду:

```
fnp4> session table show tproto=tcp portsrv=22
```

Полный перечень допустимых критериев отбора записей представлен ниже:

- **sid** – отбор по идентификатору (sid) сессии (поскольку идентификатор – уникальный параметр сессии, то по данному критерию всегда выводится не более одной сессии);
- **vlan** – отбор по идентификатору VLAN;
- **ifcl** – отбор по фильтрующему интерфейсу МЭ ССПТ-4А1 клиента;
- **ifsrv** – отбор по фильтрующему интерфейсу МЭ ССПТ-4А1 сервера;
- **ipcl4** – отбор по IPv4-адресам клиента;
- **ipsrv4** – отбор по IPv4-адресам сервера;
- **ip4** – отбор по IPv4-адресам (клиента или сервера);
- **ipcl6** – отбор по IPv6-адресам клиента;
- **ipsrv6** – отбор по IPv6-адресам сервера;
- **ip6** – отбор по IPv6-адресам (клиента или сервера);
- **portcl** – отбор по порту клиента;
- **portsrv** – отбор по порту сервера
- **port** – отбор по порту (клиента или сервера);
- **tproto** – отбор по протоколу, инкапсулированному в IP;
- **aproto** – отбор по протоколу прикладного уровня;
- **state** – отбор по состоянию сессии;
- **rule** – отбор по номеру общего правила, на основе которого создана сессия.

Следующие пары критериев отбора не допустимы к указанию в команде **session table show**:

- ipcl4 и ip4;
- ipsrv4 и ip4;
- ipcl4 и ipcl6, ipsrv6, ip6;
- ipsrv4 и ipsrv6, ipcl6, ip6;
- ipcl6 и ip6;
- ipsrv6 и ip6;
- ipcl6 и ipcl4, ipsrv4, ip4;
- ipsrv6 и ipsrv4, ipcl4, ip4;
- port и portsrv;
- port и portcl.

В случае указания недопустимой пары критериев будет выведено предупреждение:

```
FNPSH-E-007.02.1136-Совместное использование параметров недопустимо
(имя_параметра_1, имя_параметра_2)
```

Ограничение числа выводимых записей. При большом числе записей в таблице сессий полезным может оказаться параметр **number** команды **session table show**, который ограничивает максимальное число сессий, выводимых по команде: будет выведено сессий не более значения параметра **number**, с учетом порядка и критерия сортировки. Например:

```
fnp4> session table show number=100
```

Удаление сессий. Администратор имеет возможность удалить любую запись таблицы сессий по ее идентификатору. Для этого необходимо выполнить команду **`session table delete`**, указав параметр **`sid`** со значением соответствующего идентификатора сессии. Например:

```
fnp4> session table delete sid=1.3
Удалить сессии? (Y/N) [N]: y
FNPSH-I-007.02.305E-Выбранные сессии удалены
```

Удаление сессии администратором сопровождается регистрацией соответствующего события в **журнале регистрации событий**. Например:

```
27.06.2017 11:16:41 UTC+0300 (MSK) | I-1302: Удаление выбранных сессий
(admin,10.98.100.250)
```

Поскольку регистрация сессий в **журнале регистрации трафика** производится по факту завершения сессий, то при удалении сессии администратором также регистрируется запись в журнале регистрации трафика. При этом в детальной информации по сессии указывается:

```
Причина закрытия: удалена администратором
```

В случае указания идентификатора несуществующей сессии выводится соответствующая диагностика, например:

```
fnp4> session table delete sid=3.3
Удалить сессии? (Y/N) [N]: y
FNPSH-E-007.02.10B7-Не найдено подходящей сессии
```

КИА также предоставляет администратору возможность удаления всех сессий, удовлетворяющих заданным критериям отбора. Критерии отбора указываются в команде **`session table delete`** с помощью параметров. Например, можно удалить все сессии с заданным IP-адресом клиента:

```
fnp4> session table delete ipcl=10.2.253.242
Удалить сессии? (Y/N) [N]: y
FNPSH-I-007.02.305E-Выбранные сессии удалены
```

Ниже приводится полный перечень критериев отбора для удаления сессий из таблицы сессий:

- **`sid`** – идентификатор сессии;
- **`ipcl`** – IPv4- или IPv6-адрес клиента;
- **`ipsrv`** – IPv4- или IPv6-адрес сервера;
- **`ip`** – IPv4- или IPv6-адрес клиента или сервера;
- **`portcl`** – порт клиента;
- **`portsrv`** – порт сервера;
- **`port`** – порт клиента или сервера;
- **`tproto`** – протокол, инкапсулированный в IP;
- **`aproto`** – протокол прикладного уровня;

- **`state`** – состояние сессии;
- **`rule`** – номер общего правила, по которому была создана сессия.

Следующие пары критериев отбора не допустимы к указанию в команде **session table delete**:

- ipcl и ip;
- ipsrv и ip;
- portcl и port;
- portsrv и port;.

В случае указания недопустимой пары критериев будет выведено предупреждение:

```
FNPSH-E-007.02.1136-Совместное использование параметров недопустимо
(имя_параметра_1, имя_параметра_2)
```

Очистка таблицы сессий. Администратор имеет возможность очистить таблицу сессий, выполнив команду **`session table clear`**. При этом из таблицы сессий будут удалены все записи. Например:

```
fnp4> session table clear
Очистить таблицу сессий? (Y/N) [N]: y
FNPSH-I-007.02.304A-Таблица сессий очищена
```

В результате выполнения команды **session table clear** в журнале регистрации сессий могут быть зарегистрированы все сессии, находившиеся в таблице на момент выполнения данной команды (в том случае, если это предписано соответствующей опцией в правилах фильтрации, по которым создавались сессии).

В случае большого количества сессий в таблице это может привести к временному замедлению работы МЭ ССПТ-4А1 вследствие выполнения множественных операций записи в журнал регистрации сессий. Чтобы избежать данной ситуации, рекомендуется очищать таблицу сессий без регистрации удаляемых сессий, используя команду **session table clear nolog**.

Пример очистки таблицы сессий без регистрации удаляемых сессий:

```
fnp4> session table clear nolog
Очистить таблицу сессий без регистрации? (Y/N) [N]: y
FNPSH-I-007.02.304A-Таблица сессий очищена без регистрации
```

Команды управления тайм-аутами сессий. КИА предоставляет возможность изменить тайм-ауты неактивности различных состояний сессий для различных протоколов. Тайм-аут неактивности определяет период времени, после которого сессия, находящаяся в данном состоянии, будет автоматически удалена из таблицы сессий. Ниже приводится сводная таблица протоколов, состояний сессий для данных протоколов, граничные значения тайм-аутов неактивности для каждого из состояний и значения тайм-аутов по умолчанию (таблица 3.7, стр. 79). Значения тайм-аутов указаны в секундах.

Таблица 3.7: Тайм-ауты состояний сессий для различных протоколов

Протокол	*SYN*	*ESTABLISHED*	*FIN*
TCP	1-20 (5)	0-200000000 (3600)	0-20000 (600)
UDP	1-20 (5)	1-360 (60)	Не поддерживается
ICMP	1-20 (5)	1-360 (20)	Не поддерживается

Протокол	SYN	ESTABLISHED	FIN
Остальные протоколы	1-60 (5)	1-300 (30)	Не поддерживается

В скобках указаны значения тайм-аутов по умолчанию. “Не поддерживается” означает, что данное состояние не поддерживается для данного протокола. Нулевое значение (минимальное значение тайм-аута для состояний SYN и ESTABLISHED для протокола TCP) означает отключение проверки на тайм-аут. TCP-соединение в этом случае должно само корректно завершиться взаимодействующими сторонами.

В случае, если включена опция *глубокого контроля TCP*, то для протокола TCP в таблице 3.7 столбец SYN включает состояния SYN и SYNACK, столбец FIN – состояния FIN, FINFIN, FINACK, FINFINACK (см. состояния протокола TCP, таблица 3.4).

Для установки тайм-аутов неактивности состояний сессий служит команда **`session timeout set`**. В одной команде можно установить тайм-ауты всех поддерживаемых состояний сессий заданного протокола.

Например, для установки тайм-аутов неактивности всех поддерживаемых состояний протокола TCP можно выполнить следующую команду:

```
fnp4> session timeout protocol=tcp syn=10 established=1800 fin=300
FNPSH-I-007.02.3089-Тайм-аут неактивности TCP-сессии изменен (SYN)
FNPSH-I-007.02.3089-Тайм-аут неактивности TCP-сессии изменен (ESTABLISHED)
FNPSH-I-007.02.3089-Тайм-аут неактивности TCP-сессии изменен (FIN)
```

Просмотреть текущие значения тайм-аутов неактивности сессий можно, выполнив команду **`session show`**. Например:

```
fnp4> session show
Управление сессиями:                                включено
Регистрация отброшенных пакетов:                    включено
Использование AP-правил:                            включено
Использование данных канального уровня:             включено
Глубокий контроль TCP:                              включено
Поддержка traceroute-сессий:                        включено
Тайм-ауты неактивности сессий (сек):
    TCP: инициализация (SYN, SYNACK):               10
    TCP: установлено (ESTABLISHED):                 1800
    TCP: завершение (FIN, FINACK, FINFINACK):       300
    UDP: инициализация (SYN):                       5 (по умолчанию)
    UDP: установлено (ESTABLISHED):                 60 (по умолчанию)
    ICMP: инициализация (SYN):                      5 (по умолчанию)
    ICMP: установлено (ESTABLISHED):                20 (по умолчанию)
    Остальные протоколы: инициализация (SYN):       5 (по умолчанию)
    Остальные протоколы: установлено (ESTABLISHED): 30 (по умолчанию)
Обнаружение flood-атак:                             выключено
    Генерация сообщения alarm:                      выключено
    Пороговое значение для TCP (пакеты/сек):        1000 (по умолчанию)
    Пороговое значение для UDP (пакеты/сек):        500 (по умолчанию)
    Пороговое значение для ICMP (пакеты/сек):       300 (по умолчанию)
    Время жизни TMP-правила (сек):                  60 (по умолчанию)
    Регистрации пакетов для TMP-правила:            выключено
    Комментарий к TMP-правилу:                      Заблокирована flood-атака
```

Команда **`session timeout default`** устанавливает все тайм-ауты неактивности сессий в значения по умолчанию:

```
fnp4> session timeout default
Установить тайм-ауты сессий в значения по умолчанию? (Y/N) [N]: y
FNPSH-I-007.02.308D-Тайм-аут неактивности сессий установлен по умолчанию
```

Убедиться в том, что тайм-ауты были установлены в значения по умолчанию можно, вновь выполнив команду **`session show`**:

```
fnp4> session show
Управление сессиями:                                  включено
Регистрация отброшенных пакетов:                      включено
Использование AP-правил:                              включено
Использование данных канального уровня:               включено
Глубокий контроль TCP:                                включено
Поддержка traceroute-сессий:                          включено
Тайм-ауты неактивности сессий (сек):
    TCP: инициализация (SYN, SYNACK):                 5 (по умолчанию)
    TCP: установлено (ESTABLISHED):                   3600 (по умолчанию)
    TCP: завершение (FIN, FINACK, FINFINACK):         600 (по умолчанию)
    UDP: инициализация (SYN):                         5 (по умолчанию)
    UDP: установлено (ESTABLISHED):                   60 (по умолчанию)
    ICMP: инициализация (SYN):                        5 (по умолчанию)
    ICMP: установлено (ESTABLISHED):                  20 (по умолчанию)
    Остальные протоколы: инициализация (SYN):         5 (по умолчанию)
    Остальные протоколы: установлено (ESTABLISHED):   30 (по умолчанию)
Обнаружение flood-атак:                               выключено
    Генерация сообщения alarm:                        выключено
    Пороговое значение для TCP (пакеты/сек):          1000 (по умолчанию)
    Пороговое значение для UDP (пакеты/сек):          500 (по умолчанию)
    Пороговое значение для ICMP (пакеты/сек):         300 (по умолчанию)
    Время жизни TMP-правила (сек):                    60 (по умолчанию)
    Регистрации пакетов для TMP-правила:              выключено
    Комментарий к TMP-правилу:                        Заблокирована flood-атака
```

Команды настройки обнаружения flood-атак. Функция обнаружения flood-атак позволяет пакетному фильтру выявлять flood-атаки на основе превышения пороговых значений интенсивности (числа пакетов в секунду) для каждой сессии и, в случае выявления, блокировать пакеты, относящиеся к flood-атаке. Дополнительно для протоколов TCP, UDP и ICMP контролируется интенсивность появления новых сессий. Пороговые значения могут быть скорректированы администратором в определенных пределах. Данные пределы (граничные значения) для пороговых значений обнаружения flood-атак приведены в таблице 3.8, стр. 81. Для каждого порогового значения также указано значение по умолчанию. Все значения указываются в числе пакетов в секунду.

Таблица 3.8: Пороговые значения обнаружения flood-атак

Протокол	*Граничные значения*	*Значение по умолчанию*
TCP	10-200000	1000
UDP	10-200000	500
ICMP	10-200000	300

Обнаружение flood-атак по умолчанию выключено в текущей конфигурации МЭ ССПТ-4А1.

Для использования функции обнаружения flood-атак **режим управления сессиями** должен быть включен в текущей конфигурации МЭ ССПТ-4А1 (по умолчанию - включен).

Для включения обнаружения flood-атак служит команда **`session flood enable`**:

```
fnp4> session flood enable
FNPSH-I-007.02.3060-Обнаружение flood-атак включено
```

Пороговые значения обнаружения flood-атак могут быть установлены с помощью команды **session flood threshold**. В одной команде можно указать пороговые значения для всех поддерживаемых протоколов (см. таблица 3.8, стр. 81). Например:

```
fnp4> session flood threshold icmp=100 udp=400 tcp=2000
FNPSH-I-007.02.3064-Пороговое значение изменено (TCP)
FNPSH-I-007.02.3064-Пороговое значение изменено (UDP)
FNPSH-I-007.02.3064-Пороговое значение изменено (ICMP)
```

Текущие пороговые значения можно просмотреть с помощью команды **session show**:

```
fnp4> session show
Управление сессиями:                                включено
Регистрация отброшенных пакетов:                    включено
Использование AP-правил:                            включено
Использование данных канального уровня:             включено
Глубокий контроль TCP:                              включено
Поддержка traceroute-сессий:                        включено
Тайм-ауты неактивности сессий (сек):
    TCP: инициализация (SYN, SYNACK):               5 (по умолчанию)
    TCP: установлено (ESTABLISHED):                 3600 (по умолчанию)
    TCP: завершение (FIN, FINACK, FINFINACK):       600 (по умолчанию)
    UDP: инициализация (SYN):                       5 (по умолчанию)
    UDP: установлено (ESTABLISHED):                 60 (по умолчанию)
    ICMP: инициализация (SYN):                      5 (по умолчанию)
    ICMP: установлено (ESTABLISHED):                20 (по умолчанию)
    Остальные протоколы: инициализация (SYN):       5 (по умолчанию)
    Остальные протоколы: установлено (ESTABLISHED): 30 (по умолчанию)
Обнаружение flood-атак:                             включено
    Генерация сообщения alarm:                      выключено
    Пороговое значение для TCP (пакеты/сек):        2000
    Пороговое значение для UDP (пакеты/сек):        400
    Пороговое значение для ICMP (пакеты/сек):       100
    Время жизни TMP-правила (сек):                  60 (по умолчанию)
    Регистрации пакетов для TMP-правила:            выключено
    Комментарий к TMP-правилу:                      Заблокирована flood-атака
```

Пороговые значения по умолчанию могут быть восстановлены по команде **session flood threshold default**:

```
fnp4> session flood threshold default
Установить пороговые значения по умолчанию? (Y/N) [N]: y
FNPSH-I-007.02.3064-Пороговое значение изменено
```

Убедиться, что пороговые значения были установлены в значения по умолчанию можно, вновь выполнив команду **session show**:

```
fnp4> session show
Управление сессиями:                                включено
Регистрация отброшенных пакетов:                    включено
Использование AP-правил:                            включено
Использование данных канального уровня:             включено
Глубокий контроль TCP:                              включено
Поддержка traceroute-сессий:                        включено
Тайм-ауты неактивности сессий (сек):
    TCP: инициализация (SYN, SYNACK):               5 (по умолчанию)
    TCP: установлено (ESTABLISHED):                 3600 (по умолчанию)
    TCP: завершение (FIN, FINACK, FINFINACK):       600 (по умолчанию)
    UDP: инициализация (SYN):                       5 (по умолчанию)
    UDP: установлено (ESTABLISHED):                 60 (по умолчанию)
    ICMP: инициализация (SYN):                      5 (по умолчанию)
    ICMP: установлено (ESTABLISHED):                20 (по умолчанию)
```

```
    Остальные протоколы: инициализация (SYN):       5 (по умолчанию)
    Остальные протоколы: установлено (ESTABLISHED): 30 (по умолчанию)
Обнаружение flood-атак:                             включено
    Генерация сообщения alarm:                      выключено
    Пороговое значение для TCP (пакеты/сек):        1000 (по умолчанию)
    Пороговое значение для UDP (пакеты/сек):        500 (по умолчанию)
    Пороговое значение для ICMP (пакеты/сек):       300 (по умолчанию)
    Время жизни TMP-правила (сек):                  60 (по умолчанию)
    Регистрации пакетов для TMP-правила:            выключено
    Комментарий к TMP-правилу:                      Заблокирована flood-атака
```

При обнаружении flood-атаки пакетный фильтр автоматически создает TMP-правило (временное) в соответствии с которым удаляются пакеты, относящиеся к flood-атаке. Администратор может установить следующие параметры TMP-правила, которые будут использоваться при добавлении каждого нового TMP-правила в ответ на flood-атаку:

- время жизни TMP-правила — интервал времени в секундах, по истечению которого TMP-правило будет автоматически удалено;
- комментарий к TMP-правилу – строка комментария к правилу: администратор может просмотреть данный комментарий вместе с остальными параметрами правила по команде r**ule show**;
- параметр регистрации пакетов по данному TMP-правилу.

Для установки данных параметров TMP-правила служит команда **session flood rule**. В одной команде могут быть указаны все три параметра, например:

```
fnp4> session flood rule lifetime=120 log=enable comment="блокировка flood-атаки"
FNPSH-I-007.02.3062-Регистрация обнаружения flood-атак включена
FNPSH-I-007.02.3090-Комментарий TMP-правила изменен
FNPSH-I-007.02.3091-Время жизни TMP-правила изменено
```

Просмотреть текущие значения параметров TMP-правила, блокирующего flood-атаку, можно выполнив команду **session show**:

```
fnp4> session show
Управление сессиями:                                включено
Регистрация отброшенных пакетов:                    включено
Использование AP-правил:                            включено
Использование данных канального уровня:             включено
Глубокий контроль TCP:                              включено
Поддержка traceroute-сессий:                        включено
Тайм-ауты неактивности сессий (сек):
    TCP: инициализация (SYN, SYNACK):               5 (по умолчанию)
    TCP: установлено (ESTABLISHED):                 3600 (по умолчанию)
    TCP: завершение (FIN, FINACK, FINFINACK):       600 (по умолчанию)
    UDP: инициализация (SYN):                       5 (по умолчанию)
    UDP: установлено (ESTABLISHED):                 60 (по умолчанию)
    ICMP: инициализация (SYN):                      5 (по умолчанию)
    ICMP: установлено (ESTABLISHED):                20 (по умолчанию)
    Остальные протоколы: инициализация (SYN):       5 (по умолчанию)
    Остальные протоколы: установлено (ESTABLISHED): 30 (по умолчанию)
Обнаружение flood-атак:                             включено
    Генерация сообщения alarm:                      выключено
    Пороговое значение для TCP (пакеты/сек):        1000 (по умолчанию)
    Пороговое значение для UDP (пакеты/сек):        500 (по умолчанию)
    Пороговое значение для ICMP (пакеты/сек):       300 (по умолчанию)
    Время жизни TMP-правила (сек):                  120
    Регистрации пакетов для TMP-правила:            включено
    Комментарий к TMP-правилу:                      блокировка flood-атаки
```

МЭ ССПТ-4А1 обеспечивает регистрацию факта обнаружения flood-атаки в журнале регистрации событий, а также возможность регистрации факта обнаружения flood-атаки в журнале регистрации системных сообщений (опция *Генерация сообщения alarm* в выводе команды **`session show`**). По умолчанию данная возможность выключена. Для включения сигнализации обнаружения flood-атак служит команда **`session flood alarm enable`**, для выключения – **`session flood alarm disable`**. Например:

```
fnp4> session flood alarm enable
Включить сигнализацию обнаружения flood-атак? (Y/N) [N]: y
FNPSH-I-007.02.308E-Сигнализация обнаружения flood-атак включена
```

В случае, когда наблюдается высокая интенсивность flood-атак и включена сигнализация обнаружения flood-атак, регистрация flood-атак может быть временно приостановлена во избежание переполнения журналов регистрации.

Если в течение **1** секунды было заблокировано не менее **10** любых flood-атак, запись соответствующих событий в **журнал регистрации событий** и в **журнал регистрации системных сообщений** блокируется на **300** секунд. По истечению данного тайм-аута, возможность регистрировать информацию о flood-атаках будет восстановлена.

Для выключения обнаружения flood-атак служит команда **`session flood disable`**:

```
fnp4> session flood disable
FNPSH-I-007.02.3061-Обнаружение flood-атак выключено
```

3.2.2. Режим пакетной фильтрации

В режиме пакетной фильтрации каждый пакет, поступающий на какой-либо фильтрующий интерфейс МЭ ССПТ-4А1, проверяется по временным правилам фильтрации, если они есть, и по общим правилам фильтрации. Работа с правилами фильтрации данных типов рассматривается в разделе 3.7.1, стр. 141 и 3.7.2, стр. 142 соответственно. Таким образом, решение об удалении пакета или о передаче на выходные интерфейсы принимается на основании действия правила, которому соответствует пакет. При этом модуль управления сессиями не задействован, и, таким образом, проверки на соответствие пакета контексту сессии не выполняются. Обработка трафика при использовании режима пакетной фильтрации медленнее, чем при использовании режима управления сессиями. Кроме того, требуется добавление большего количества правил фильтрации для реализации той же самой политики доступа, по сравнению с режимом управления сессиями, т. к. требуется отдельное разрешающее правило для каждого направления передачи трафика: одно правило – для передачи пакетов от клиента к серверу, другое правило – для передачи пакетов от сервера к клиенту.

Управление пакетным фильтром. При включении МЭ ССПТ-4А1 процесс пакетного фильтра всегда стартует автоматически (при отсутствии нарушения целостности файловой системы МЭ ССПТ-4А1 и при неизменности аппаратной конфигурации устройства). Пакетный фильтр может быть остановлен, перезапущен и запущен из остановленного состояния

администратором МЭ ССПТ-4А1. Для останова пакетного фильтра служит команда **filter stop**. Например:

```
fnp4> filter stop
Остановить пакетный фильтр? (Y/N) [N]: y
FNPSH-I-007.02.3056-Пакетный фильтр остановлен
```

Останов пакетного фильтра влечет за собой прекращение передачи пакетов через фильтрующие интерфейсы МЭ ССПТ-4А1.

Если на момент выполнения команды **filter stop** пакетный фильтр уже остановлен, то его состояние остается без изменения.

Пример выполнения команды **filter stop**, когда пакетный фильтр уже остановлен:

```
fnp4> filter stop
FNPSH-W-007.02.2003-Пакетный фильтр выключен
```

Для запуска пакетного фильтра из остановленного состояния служит команда **filter start**. Например:

```
fnp4> filter start
FNPSH-I-007.02.3054-Пакетный фильтр запущен
```

Если на момент выполнения команды **filter start** пакетный фильтр уже запущен, то его состояние остается без изменения.

Пример выполнения команды **fitler start,** когда пакетный фильтр уже запущен:

```
fnp4> filter start
FNPSH-W-007.02.201F-Пакетный фильтр уже работает
```

Для перезапуска пакетного фильтра служит команда **filter restart**. Например:

```
fnp4> filter restart
Перезапустить пакетный фильтр? (Y/N) [N]: y
FNPSH-I-007.02.3112-Пакетный фильтр перезапущен
```

При перезапуске пакетного фильтра обнуляется статистика трафика по правилам фильтрации текущей политики доступа, статистика трафика по фильтрующим интерфейсам устройства, а также очищается таблица сессий.

Очистка таблицы сессий приводит к разрыву сетевых соединений, которые были в таблице сессий на момент перезапуска пакетного фильтра.

Для вывода информации о состоянии пакетного фильтра и о статистике по фильтрующим интерфейсам служит команда **filter show**. Информация выводится только в том случае, если пакетный фильтр находится в активном состоянии (запущен). В противном случае командный интерфейс МЭ ССПТ-4А1 выведет предупреждающее сообщение:

```
FNPSH-W-007.02.2003-Пакетный фильтр выключен
```

Пример вывода команды **filter show** представлен на рис. 3.5, стр. 86.

```
Фильтр В РАБОТЕ 5 дней 22 минуты 49 секунд, с 04.03.2021 11:38:55 (UTC)
                    Статистика трафика: Весь трафик

  Пакеты          eth0          eth1          eth2
    Получено         0           447           377
  Отправлено        32           389           384
     Удалено         0            75             0
  Повреждено         0             0             0

   Байты          eth0          eth1          eth2
    Получено         0        100717         32732
  Отправлено      1780         33284         96342
     Удалено         0          4927             0
  Повреждено         0             0             0

TCP <-- Весь трафик --> Ethernet II
H - справка  Q, F10 - выход
```

Рисунок 3.5: Состояние пакетного фильтра и статистика трафика

Информация о состоянии пакетного фильтра выводится в верхней строке экрана терминала и включает следующие данные:

- время наработки пакетного фильтра с момента последнего запуска;
- время последнего запуска пакетного фильтра.

По каждому фильтрующему интерфейсу выводится следующая информация о статистике трафика:

- количество **принятых** пакетов/байтов;
- количество **переданных** пакетов/байтов;
- количество **удаленных** пакетов/байтов из числа принятых. Пакет может быть удален в соответствии с применяемыми правилами фильтрации, либо в результате работы подсистемы управления сессиями или трансляции сетевых адресов (NAT).

Имеется возможность просмотра как суммарной статистики трафика (рис. 3.5, стр. 86), так и статистики трафика по отдельным типам кадров Ethernet и протоколам:

- кадры Ethernet: Ethernet II, IEEE 802.3-LLC, IEEE 802.3-SNAP, IEEE 802.3-RAW;
- протоколы: ARP, Reverse ARP, IP, IPv6, ICMP, ICMPv6, UPD, TCP.

В нижних строках экрана терминала выводится подсказка (рис. 3.5, стр. 86):

- текущая страница статистики трафика и переходы к предыдущей и следующей страницам;
- краткая справка по управлению просмотром.

В процессе выполнения команды информация о состоянии пакетного фильтра и статистике трафика автоматически обновляется с периодом в **5** секунд.

Для просмотра статистики трафика используются клавиши и управляющие последовательности, перечисленные в таблице 3.9, стр. 87.

Таблица 3.9: Управление просмотром статистики трафика

Управление	***Назначение***
<↑>	Переход к предыдущей странице статистики
<↓>	Переход к следующей странице статистики
<←>	Перемещение к предыдущему фильтрующему интерфейсу
<→>	Перемещение к следующему фильтрующему интерфейсу
<Home>	Перемещение к первому фильтрующему интерфейсу
<End>	Перемещение к последнему фильтрующему интерфейсу
<Page Up>	Переход к первой странице статистики (суммарный трафик)
<Page Down>	Переход к последней странице статистики (TCP-трафик)
<R>	Немедленное обновление информации о состоянии пакетного фильтра и статистики трафика
<H>	Вывод подсказки по клавишам управления просмотром статистики
<F10>, <Q>	Завершение выполнения команды

3.2.3. Функции трансляции сетевых адресов и аутентификации сетевых пользователей

Настройка функции трансляции сетевых адресов состоит из следующей последовательности действий:

1) Создание *контейнера NAT* (определение см. ниже в настоящем пункте);

2) Настройка параметров контейнера NAT;

3) Включение функции трансляции сетевых адресов.

В случае неполной или некорректной настройки контейнера NAT результаты работы МЭ ССПТ-4А1 могут не соответствовать ожидаемым. Для уменьшения вероятности возникновения подобных ситуаций рекомендуется соблюдать указанный порядок действий, и включать функцию трансляции сетевых адресов после настройки и проверки параметров контейнера NAT.

Перед настройкой функции NAT рекомендуется выбрать и назначить виртуальные MAC-адреса для фильтрующих интерфейсов, используемых в контейнере NAT. Для этого необходимо воспользоваться командой **`nat mac set`**.

В случае, если настроенный на МЭ ССПТ-4А1 контейнер NAT использует не все фильтрующие интерфейсы, трафик через оставшуюся часть фильтрующих интерфейсов

обрабатывается в режиме сессий без использования функции трансляции сетевых адресов. При этом выходными интерфейсами для такого трафика не могут быть интерфейсы, задействованные в контейнере NAT.

В случае редактирования настроек в контейнере NAT большая часть производимых операций (добавление и удаление правил трансляции, статических маршрутов, и т. п.) повлечет за собой полное очищение таблицы сессий для того, чтобы таблица сессий всегда находилась в консистентном состоянии и не противоречила правилам фильтрации и настройкам NAT.

Помимо настроек, касающихся конкретного контейнера NAT, следующие настройки являются общими для всех контейнеров NAT:

- управление статическими и динамическими записями в ARP-таблице;
- управление аутентификацией сетевых пользователей.

Отметим, что если на МЭ ССПТ-4А1 используется политика доступа, отвечающая принципу «запрещено всё, что явно не разрешено», то для обеспечения сетевого взаимодействия узлов сети через МЭ в текущую политику доступа должно быть добавлено общее правило, явно разрешающее прохождение через МЭ пакетов протокола ARP.

Пример добавления правила, разрешающего прохождение через МЭ трафика протокола ARP для любых фильтрующих интерфейсов МЭ:

```
fnp4> rule add rule:15 action=accept frame=eth2 ethproto=0x0806
FNPSH-I-007.02.3046-Общее правило добавлено (15)
```

В случае использования политики доступа по умолчанию, которая запрещает прохождение через МЭ ССПТ-4А1 любого трафика, для обеспечения сетевого взаимодействия через МЭ должны быть добавлены следующие общие правила:

- правило, разрешающее прохождение трафика протокола ARP;
- правило, разрешающее прохождение трафика на уровне IP (для протоколов из числа: ICMP, TCP, UDP) в соответствии с требованиями политики доступа (взаимодействие между конкретными узлами внутренней и внешней сети NAT).

Создание контейнера NAT. Контейнер NAT представляет собой структуру данных, содержащую ограниченный набор *внешних* и *внутренних интерфейсов NAT*, а также совокупность настроек и параметров, применяемым к данным интерфейсам.

Для создания контейнера NAT используется команда **`nat case add`** с заданием обязательного параметра **`name`**:

```
fnp4> nat case add name=nat1
FNPSH-I-007.02.3113-Контейнер NAT добавлен
```

Выполнение данной команды приведет к созданию пустого контейнера NAT, который требует дальнейшей настройки. Убедиться, что контейнер NAT создан, можно с помощью команды **`nat case show`**, которая выводит список существующих на данном устройстве контейнеров и их параметры. Пример отображения пустого контейнера NAT приведен ниже:

```
fnp4> nat case show viewer=no
Контейнеры NAT:

Контейнер NAT: nat1
  Внутренние интерфейсы NAT
  Внешние интерфейсы NAT
  Правила трансляции NAT
  Правила переадресации NAT (переадресация включена)
  Таблица маршрутов NAT
```

Настройка параметров контейнера NAT. Настройка параметров контейнера NAT состоит из последовательности следующих действий:

1) настройка внешних и внутренних интерфейсов контейнера NAT;

2) настройка демилитаризованной зоны (*DMZ*) в контейнере NAT;

3) настройка правил трансляции контейнера NAT;

4) настройка статических маршрутов контейнера NAT;

5) настройка правил переадресации контейнера NAT;

Для возможности включения функции NAT должен существовать по меньшей мере один контейнер NAT, в котором определены как минимум один *внутренний интерфейс NAT* и один *внешний интерфейс NAT*,

При этом для *реального функционирования NAT* требуется также наличие в контейнере NAT по меньшей мере:

- одного правила трансляции;
- маршрута по умолчанию.

Настройка внешних и внутренних интерфейсов контейнера NAT. Основной функцией NAT является сокрытие топологии и защита сегментов внутренней сети. Поэтому, прежде чем начинать настройку контейнера NAT, следует выделить сегменты сети, которые будут являться внутренними сетями NAT, и выделить для них фильтрующие интерфейсы МЭ ССПТ-4А1. Необходимо также определить фильтрующие интерфейсы для выхода в незащищенную сеть, являющиеся внешними для NAT.

Для включения функции трансляции сетевых адресов минимально необходима настройка внешнего и внутреннего интерфейсов в контейнере NAT, выбранных из списка фильтрующих интерфейсов МЭ ССПТ-4А1.

В качестве внешнего или внутреннего интерфейса NAT может использоваться *агрегированный интерфейс* – именованный в пределах контейнера NAT внешний или внутренний интерфейс, состоящий из нескольких физических фильтрующих интерфейсов МЭ ССПТ-4А1. IP-адреса, назначенные на агрегированный интерфейс, относятся одинаково ко всем физическим фильтрующим интерфейсам, входящим в него. С помощью такого интерфейса, можно, к примеру, настроить одну подсеть, части которой будут видеть друг друга только через данный интерфейс межсетевого экрана. В этом случае часть фильтрующих интерфейсов МЭ ССПТ-4А1 будет выступать в роли повторителя (хаба).

Для добавления внешнего и внутреннего интерфейсов в контейнер NAT используются соответственно команды **`nat public add`** и **`nat private add`** с заданием следующих параметров:

- **`case`** – имя контейнера NAT, для которого добавляется внешний/внутренний интерфейс;
- **`name`** – имя внешнего/внутреннего интерфейса в контейнере NAT;
- **`interface`** – имя или номер физического фильтрующего интерфейса, который добавляется в качестве внешнего/внутреннего для контейнера NAT;
- **`address`** – IP-адрес, назначаемый на интерфейс контейнера NAT в формате <IP-адрес/маска>.

В случае, если необходимо добавить агрегированный интерфейс в качестве внешнего или внутреннего, в параметре **`interface`** через запятую перечисляются имена или номера физических фильтрующих интерфейсов МЭ ССПТ-4А1, объединяемых в агрегированный интерфейс.

Ниже представлен пример добавления внешнего агрегированного интерфейса в контейнер NAT:

```
fnp4> nat public add case=nat1 name=pub_if interface=5,6 address=10.2.253.22/24
FNPSH-I-007.02.3115-Интерфейс NAT добавлен
```

При настройке интерфейсов контейнера NAT необходимо учитывать следующие ограничения :

- IP-адреса, назначенные на внешние интерфейсы контейнера NAT уникальны. Ни один IP-адрес внешнего интерфейса не может повторяться дважды – ни в разных контейнерах NAT, ни в пределах одного, за исключением ситуации агрегирования физических фильтрующих интерфейсов в одном внешнем интерфейсе контейнера NAT;
- внешние физические фильтрующие интерфейсы контейнера NAT не могут быть в составе внутренних интерфейсов любого контейнера, но могут быть в составе внешних интерфейсов другого контейнера с другим назначенным на него IP-адресом (внешний физический интерфейс с двумя различными IP-адресами может входить в два контейнера NAT);
- внутренний физический интерфейс не может использоваться одновременно в двух контейнерах NAT;
- IP-адреса, назначенные на внутренние интерфейсы контейнера NAT, не являются уникальными, и могут повторяться в других контейнерах NAT.

Не допускается использовать в составе внешних и внутренних интерфейсов NAT фильтрующие интерфейсы, используемые в качестве:

- зеркалирующего интерфейса (см. раздел 3.13.6, стр. 206);
- интерфейса HTTP-посредника (см. раздел 3.9, стр. 159);
- интерфейса, входящий в агрегат управляющего интерфейса (см. раздел 3.14, стр. 218).

При необходимости можно изменять настройки внешних и внутренних интерфейсов контейнера NAT, используя команды **`nat public edit`** и **`nat private edit`**, соответственно, указывая обязательные параметры **`case`** и **`name`**, а также другие параметры, которые подлежат изменению.

Ниже представлен пример изменения IP-адреса, назначенного на внешний интерфейс контейнера NAT:

```
fnp4> nat public edit case=nat1 name=pub_if address=10.2.253.23/24
Изменить интерфейс NAT? (Y/N) [N]: y
FNPSH-I-007.02.3116-Интерфейс NAT изменен
```

Для удаления внешнего или внутреннего интерфейса используются команды **`nat public delete`** и **`nat private delete`** соответственно:

```
fnp4> nat public delete case=nat1 name=pub_if
Удалить интерфейс NAT? (Y/N) [N]: y
FNPSH-I-007.02.3117-Интерфейс NAT удален
```

Возможность удаления или редактирования внешних и внутренних интерфейсов контейнера NAT есть только в том случае, если данный интерфейс не используется правилами трансляции, маршрутизации и переадресации. В противном случае удаление и редактирование настроек внешнего или внутреннего интерфейса доступно только после удаления правил контейнера NAT (трансляции, маршрутизации, переадресации), в которых используется данный интерфейс.

Для просмотра настроек внешних и внутренних интерфейсов контейнера NAT можно использовать команды **`nat public show`** и **`nat private show`** с указанием обязательного параметра **`case`**:

```
fnp4> nat public show case=nat1
Интерфейс NAT:          pub_if
Фильтрующие интерфейсы: eth5,eth6
IP-адреса:              10.2.253.23/255.255.255.0
```

Настройка демилитаризованной зоны (DMZ) в контейнере NAT. Для настройки DMZ в контейнере NAT не предусмотрено отдельных интерфейсов. Предполагается что DMZ – это часть внешней сети, настроенной в контейнере NAT.

Трафик, который проходит из внешней сети в DMZ, проходит этап фильтрации, однако по отношению к нему не производится преобразования адресов.

Настроить DMZ во внешней сети контейнера NAT возможно следующим образом:

- необходимо создать агрегированный внешний интерфейс с назначением на него одного IP-адреса;
- за одним из физических интерфейсов, входящих в агрегированный интерфейс, расположить выход в незащищенную сеть;
- за другим физическим интерфейсом, входящим в агрегированный интерфейс, расположить подсеть узлов DMZ.

При необходимости настроить DMZ в защищенном сегменте внутренней сети, необходимо использовать правила передаресации.

Настройка правил трансляции контейнера NAT. Добавление правил трансляции в контейнер NAT позволяет:

- вводить ограничения на обращения во внешнюю сеть для сегментов или узлов внутренней сети;
- настроить виртуальные IP-адреса отправителя при обращениях во внешнюю сеть для конкретных узлов или сегментов внутренней сети.

Если для IP-пакета, принятого на внутренний интерфейс NAT, в контейнере NAT нет подходящего правила трансляции, то такой IP-пакет **не будет передан** на внешний интерфейс NAT данного контейнера, а будет **удален**.

Если при этом в текущей конфигурации МЭ ССПТ-4А1 включена регистрация пакетов, отброшенных NAT, то такой пакет будет зарегистрирован с диагностикой:

```
Ошибка E-3010: NAT - соответствующее правило трансляции не найдено
```

Добавленные правила трансляции располагаются и просматриваются в порядке их добавления администратором.

Для добавления правила трансляции используется команда **`nat translate add`** со следующими параметрами :

- **`case`** – имя контейнера NAT, для которого добавляется правило трансляции;
- **`number`** – номер правила трансляции в контейнере NAT;
- **`interface`** – имя внешнего интерфейса, для которого добавляется правило трансляции;
- **`prv-address`** – IP-адрес внутреннего сегмента сети, узла или диапазона узлов внутренней сети, для которых действует данное правило трансляции. IP-адрес может быть задан в одном из следующих форматов:
  - ✔ `<X.X.X.X>` – для отдельного узла;
  - ✔ `<X.X.X.X>-<Y.Y.Y.Y>` – для диапазона узлов;
  - ✔ `<X.X.X.X>/<N>` – для подсети с маской в формате CIDR;
  - ✔ `<X.X.X.X>/<Y.Y.Y.Y>` – для подсети с маской в десятично-точечном формате;
- **`pub-address`** – виртуальный IP-адрес отправителя при обращениях во внешнюю сеть:
  - ✔ адрес отправителя должен быть выбран из списка IP-адресов указанного внешнего интерфейса;
  - ✔ параметр может содержать список IP-адресов. В этом случае при обращении во внешнюю сеть используется круговой цикл выборки IP-адресов из заданного списка и назначение его в качестве IP-адреса отправителя для каждой новой сессии;
  - ✔ IP-адрес может быть задан в формате `<X.X.X.X>`, при задании списка IP-адресов, они перечисляются через запятую;
- **`dst-address`** – IP-адрес узла или сети назначения, является необязательным параметром. IP-адрес может быть задан в одном из следующих форматов:
  - ✔ `<X.X.X.X>` – для отдельного узла;

✔ <X.X.X.X>-<Y.Y.Y.Y> – для диапазона узлов;

✔ <X.X.X.X>/<N> – для подсети с маской в формате CIDR;

✔ <X.X.X.X>/<Y.Y.Y.Y> – для подсети с маской в десятично-точечном формате;

- **protocol** – имя или номер протокола, инкапсулированного в IP-пакет, для которого задается правило трансляции. Является необязательным параметром, по умолчанию имеет значение **any** (любой протокол).

Ниже приведен пример добавления правила трансляции в контейнер NAT для случая настройки сети, представленного в таблице 3.10, стр. 93.

Таблица 3.10: Пример добавления правила трансляции в контейнер NAT

Параметр	*Значение*
Внешняя сеть	10.2.100.0/24
Внутренняя сеть	10.2.200.0/24
IP-адрес внешнего интерфейса	10.2.100.20, 10.2.100.21, 10.2.100.22
IP-адрес внутреннего интерфейса	10.2.200.30
IP-адрес внутреннего сегмента сети	10.2.200.1 — 10.2.200.10
Выбранный адрес отправителя	10.2.100.21, 10.2.100.22
Выбранный протокол	UDP
Выбранный адрес назначения	Любой

Команда добавления такого правила трансляции в контейнер NAT выглядит следующим образом:

```
fnp4> nat translate add case=nat1 number=1 prv-address=10.2.200.1-10.2.200.10  pub-
address=10.2.100.21,10.2.100.22 interface=pub_if protocol=udp
FNPSH-I-007.02.3118-Правило трансляции NAT добавлено
```

В приведенном примере сегменту внутренней сети с IP-адресами с **10.2.200.1** по **10.2.200.10** разрешены обращения на любой IP-адрес во внешней сети по протоколу UDP, при этом исходящие пакеты будут иметь IP-адрес отправителя **10.2.100.21** либо **10.2.100.22**. Контейнер NAT при добавлении данного правила трансляции и соответственно настроенных внешних и внутренних интерфейсах будет выглядеть так, как представлено ниже:

```
fnp4> nat case show viewer=no
Контейнеры NAT:

Контейнер NAT: nat1
  Внутренние интерфейсы NAT
    Интерфейс NAT: prv_if
      Фильтрующие интерфейсы: eth3
      IP-адреса: 10.2.200.30/255.255.255.0
  Внешние интерфейсы NAT
    Интерфейс NAT: pub_if
      Фильтрующие интерфейсы: eth5,eth6
      IP-адреса:
10.2.100.20/255.255.255.0,10.2.100.21/255.255.255.0,10.2.100.22/255.255.255.0
  Правила трансляции NAT
    number=1 prv-address=10.2.200.1-10.2.200.10 pub-address=10.2.100.21,10.2.100.22
interface=pub_if dst-address=any protocol=udp
```

```
Правила переадресации NAT (переадресация включена)
Таблица маршрутов NAT
  dst-address=10.2.200.0/255.255.255.0 interface=prv_if
  dst-address=10.2.100.0/255.255.255.0 interface=pub_if
```

Правила трансляции контейнера NAT можно редактировать и удалять с помощью команд **`nat translate edit`** и **`nat translate delete`** с указанием обязательных параметров **`case`** и **`number`**:

```
fnp4> nat translate delete case=nat1 number=1
Удалить правило трансляции NAT? (Y/N) [N]: y
FNPSH-I-007.02.311A-Правило трансляции NAT удалено
```

Просмотреть правила трансляции для определенного контейнера NAT можно с помощью команды **`nat translate show`** с указанием обязательного параметра **`case`**.

Настройка статических маршрутов контейнера NAT. Контейнер NAT содержит таблицу статических маршрутов, в которой могут присутствовать:

- маршруты на IP-адреса узлов или сетей;
- маршруты на интерфейсы контейнера NAT;
- маршрут на шлюз по умолчанию.

Маршруты на интерфейсы контейнера NAT формируются автоматически при добавлении внешних и внутренних интерфейсов в контейнер NAT. Остальные типы маршрутов настраиваются вручную администратором МЭ ССПТ-4А1.

Внутреннее представление маршрутной таблицы представляет собой отсортированный список, который формируется по следующему принципу:

- маршруты располагаются в списке в порядке возрастания IP-адресов назначения. При этом, более специфичные маршруты из одной подсети располагаются перед менее специфичными (маршрут на узел из подсети будет располагаться перед маршрутом на подсеть);
- маршруты на интерфейсы контейнера NAT располагаются в конце списка таблицы маршрутизации;
- маршрут на шлюз по умолчанию, в случае его присутствия в таблице маршрутизации, всегда располагается в начале списка и имеет порядковый номер **1**.

Отображение таблицы маршрутизации отличается от ее внутреннего представления – первыми всегда отображаются маршруты на интерфейсы контейнера NAT, затем маршрут по умолчанию, далее статические маршруты в порядке их добавления (при добавлении маршрута ему присваивается порядковый номер, который впоследствии используется при необходимости удаления данного маршрута).

Поиск подходящего маршрута всегда начинается с начала таблицы маршрутизации, и продолжается до первого найденного маршрута. В случае присутствия в таблице маршрута на

шлюз по умолчанию, он всегда применяется в последнюю очередь, при отсутствии других подходящих маршрутов.

Для добавления нового статического маршрута используется команда **nat route add** со следующими параметрами:

- **case** – имя контейнера NAT, для которого добавляется статический маршрут;
- **dst-address** – IP-адрес узла или сети назначения. IP-адрес может быть задан в одном из следующих форматов:
  - ✔ <X.X.X.X> – для отдельного узла;
  - ✔ <X.X.X.X>/<N> – для подсети с маской в формате CIDR;
  - ✔ <X.X.X.X>/<Y.Y.Y.Y> – для подсети с маской в десятично-точечном формате;
- **gateway** – IP-адрес шлюза в формате <X.X.X.X>.

Маршрут на шлюз по умолчанию задается аналогично любому статическому маршруту, но при этом параметр **dst-address** устанавливается в значение **0.0.0.0**. Ниже представлен пример добавления статического маршрута на подсеть и на узел из данной подсети:

```
fnp4> nat route add case=nat1 dst-address=10.3.100.20 gateway=10.2.100.31
FNPSH-I-007.02.311E-Маршрут NAT добавлен
fnp4> nat route add case=nat1 dst-address=10.3.100.0/24 gateway=10.2.100.30
FNPSH-I-007.02.311E-Маршрут NAT добавлен
```

Ниже представлено отображение контейнера NAT после выполнения команд добавления данных статических маршрутов:

```
fnp4> nat case show viewer=no
Контейнеры NAT:

Контейнер NAT: nat1
  Внутренние интерфейсы NAT
    Интерфейс NAT: prv_if
      Фильтрующие интерфейсы: eth3
      IP-адреса: 10.2.200.30/255.255.255.0
  Внешние интерфейсы NAT
    Интерфейс NAT: pub_if
      Фильтрующие интерфейсы: eth5,eth6
      IP-адреса:
10.2.100.20/255.255.255.0,10.2.100.21/255.255.255.0,10.2.100.22/255.255.255.0
  Правила трансляции NAT
  Правила переадресации NAT (переадресация включена)
  Таблица маршрутов NAT
    dst-address=10.2.200.0/255.255.255.0 interface=prv_if
    dst-address=10.2.100.0/255.255.255.0 interface=pub_if
    number=1 dst-address=10.3.100.20 gateway=10.2.100.31 interface=pub_if
    number=2 dst-address=10.3.100.0/255.255.255.0 gateway=10.2.100.30 interface=pub_if
```

Статические маршруты контейнера NAT можно редактировать и удалять с помощью команд **nat route edit** и **nat route delete** с указанием обязательных параметров **case** и **number**:

```
fnp4> nat route delete case=nat1 number=1
Удалить маршрут NAT? (Y/N) [N]: y
FNPSH-I-007.02.3120-Маршрут NAT удален
```

Просмотреть статические маршруты определенного контейнера NAT можно с помощью команды **`nat route show`** с указанием обязательного параметра **`case`**.

Настройка правил переадресации контейнера NAT. Настройка правил переадресации необходима в случае, когда пользователей, расположенных во внешней сети, требуется предоставить доступ к публичным ресурсам, находящимся в пределах защищенного сегмента сети (внутренняя сеть NAT).

Для добавления правила переадресации используется команда **`nat redirect add`** со следующими параметрами:

- **`case`** – имя контейнера NAT, для которого добавляется правило переадресации;
- **`interface`** – имя внешнего интерфейса контейнера NAT, для которого добавляется правило переадресации;
- **`pub-address`** – IP-адрес внешнего интерфейса контейнера NAT, обращения на который переадресуются. IP-адрес задается в формате `<X.X.X.X>`;
- **`pub-port`** — номер внешнего порта, обращения на который переадресуются во внутреннюю сеть. Может быть задан либо одиночный номер порта, либо диапазон номеров портов;
- **`prv-address`** – IP-адрес узла из внутренней сети контейнера NAT, на который будет отправляться переадресованный трафик. IP-адрес задается в формате `<X.X.X.X>`;
- **`prv-port`** – номер порта узла из внутренней сети контейнера NAT, на который будет отправляться переадресованный трафик. Является необязательным параметром, по умолчанию принимается равным значению параметра **`pub-port`**. Может быть задан либо одиночный номер порта, либо диапазон номеров портов, аналогичный размеру диапазона номеров портов для параметра **`pub-port`**;
- **`src-address`** – IP-адрес узла или диапазона узлов из внешней сети, для которых применимо данное правило переадресации. Является необязательным параметром, по умолчанию правило применимо к любым IP-адресам. IP-адрес может быть задан в одном из следующих форматов:
  - ✔ `<X.X.X.X>` – для отдельного узла;
  - ✔ `<X.X.X.X>-<Y.Y.Y.Y>` – для диапазона узлов;
  - ✔ `<X.X.X.X>/<N>` – для подсети с маской в формате CIDR;
  - ✔ `<X.X.X.X>/<Y.Y.Y.Y>` – для подсети с маской в десятично-точечном формате.
- **`protocol`** – имя или номер протокола, инкапсулированного в IP-пакет, для которого задается правило переадресации. Является необязательным параметром, по умолчанию имеет значение **`any`** (любой протокол).

Правила переадресации располагаются и просматриваются в порядке их добавления администратором МЭ ССПТ-4А1.

Ниже приведен пример добавления правила переадресации в контейнер NAT для случая настройки сети, представленного в таблице 3.11, стр. 97.

Таблица 3.11: Пример добавления правила переадресации в контейнер NAT

Параметр	*Значение*
Внешняя сеть	10.2.100.0/24
Внутренняя сеть	10.2.200.0/24
IP адрес и порт внешнего интерфейса для переадресации	10.2.100.20, port 22
IP адрес пользователя во внешней сети	10.3.100.10
IP адрес хоста с публичными ресурсами во внутренней сети	10.2.200.20
Протокол взаимодействия	UDP

Команда добавления такого правила переадресации в контейнер NAT выглядит следующим образом:

```
fnp4> nat redirect add case=nat1 interface=pub_if pub-address=10.2.100.20 pub-port=22 prv-
address=10.2.200.20 protocol=udp src-address=10.3.100.10
FNPSH-I-007.02.311B-Правило переадресации NAT добавлено
```

Контейнер NAT при добавлении данного правила переадресации и соответствующим образом настроенными внешними и внутренними интерфейсами контейнера NAT будет выглядеть так, как представлено ниже:

```
fnp4> nat case show viewer=no
Контейнеры NAT:

Контейнер NAT: nat1
  Внутренние интерфейсы NAT
    Интерфейс NAT: prv_if
      Фильтрующие интерфейсы: eth3
      IP-адреса: 10.2.200.30/255.255.255.0
  Внешние интерфейсы NAT
    Интерфейс NAT: pub_if
      Фильтрующие интерфейсы: eth5,eth6
      IP-адреса:
10.2.100.20/255.255.255.0,10.2.100.21/255.255.255.0,10.2.100.22/255.255.255.0
  Правила трансляции NAT
  Правила переадресации NAT (переадресация включена)
    number=1 interface=pub_if pub-address=10.2.100.20 prv-address=10.2.200.20 pub-port=22
prv-port=22 src-address=10.3.100.10 protocol=udp
  Таблица маршрутов NAT
    dst-address=10.2.200.0/255.255.255.0 interface=prv_if
    dst-address=10.2.100.0/255.255.255.0 interface=pub_if
```

Правила переадресации контейнера NAT можно редактировать и удалять с помощью команд **`nat redirect edit`** и **`nat redirect delete`** с указанием обязательных параметров **`case`** и **`number`**:

```
fnp4> nat redirect delete case=nat1 number=1
Удалить правило трансляции NAT? (Y/N) [N]: y
```

```
FNPSH-I-007.02.311D-Правило переадресации NAT удалено
```

Просмотреть правила переадресации для контейнера NAT можно с помощью команды **nat redirect show** с указанием обязательного параметра **case**.

Также для правил переадресации существует команда **nat redirect set** с обязательными параметрами **case** и **state**, позволяющая запретить или разрешить использование переадресации. По умолчанию переадресация разрешена. При необходимости запретить переадресацию необходимо выполнить команду **nat redirect set,** установив параметр **state** в значение **disable**:

```
fnp4> nat redirect set case=nat1 state=disable
FNPSH-I-007.02.3123-Переадресация для контейнера NAT выключена
```

Включение функции трансляции сетевых адресов. Включение функции трансляции сетевых адресов осуществляется с помощью команды **nat enable**, выключение – с помощью команды **nat disable**:

```
fnp4> nat enable
FNPSH-I-007.02.3027-NAT включен
```

Для проверки состояния функции трансляции сетевых адресов можно воспользоваться командой **nat show**:

```
fnp4> nat show
Состояние NAT:                                    включено
Регистрация отброшенных пакетов:                  выключено
Аутентификация сетевых пользователей:             выключено
Тайм-аут неактивности сетевых пользователей(сек) 600
MAC-адреса:
    eth0:                                         02:01:01:01:00:3a
    eth1:                                         02:01:01:01:00:00
    eth2:                                         02:01:01:01:00:16
    eth3:                                         02:01:01:01:00:1c
    eth4:                                         02:01:01:01:00:62
    eth5:                                         02:01:01:01:00:68
    eth6:                                         02:01:01:01:00:7e
    eth7:                                         02:01:01:01:00:44
Контейнеры NAT:                                   nat1
```

Управление состоянием ARP-таблицы. ARP-таблица МЭ ССПТ-4А1 используется только при включенной функции NAT. Рассмотрим работу с ARP-таблицей на примере следующего контейнера NAT (создание контейнера NAT и настройка его параметров описаны выше в данном разделе):

```
fnp4> nat case show viewer=no
Контейнеры NAT:

Контейнер NAT: nat1
  Внутренние интерфейсы NAT
    Интерфейс NAT: prv
      Фильтрующие интерфейсы: eth1
      IP-адреса: 10.2.253.246/255.255.255.248
  Внешние интерфейсы NAT
    Интерфейс NAT: pub
      Фильтрующие интерфейсы: eth2
      IP-адреса: 10.2.253.253/255.255.255.248
```

```
  Правила трансляции NAT
    number=1 prv-address=10.2.253.240/255.255.255.248 pub-address=10.2.253.253
interface=pub dst-address=any protocol=any
  Правила переадресации NAT (переадресация включена)
  Таблица маршрутов NAT
    dst-address=10.2.253.240/255.255.255.248 interface=prv
    dst-address=10.2.253.248/255.255.255.248 interface=pub
    number=1 dst-address=0.0.0.0 gateway=10.2.253.254 interface=pub
```

ARP-таблица МЭ ССПТ-4А1 может включать в себя записи двух типов:

- динамические;
- статические;

Динамические ARP-записи добавляются в таблицу автоматически в результате работы протокола ARP, реализованной в МЭ ССПТ-4А1, при обращении к узлу во внутренней или внешней сети NAT. Например, в результате ICMP-запроса (команда ping) с узла внутренней сети с IP-адресом 10.2.253.242 к шлюзу по умолчанию, расположенному во внешней сети NAT с IP-адресом 10.2.253.254, будет добавлена динамическая ARP-запись, содержащая IP- и MAC-адреса шлюза по умолчанию. Для просмотра ARP-таблицы служит команда **`nat arp show`**. Вывод данной команды, содержащей динамическую ARP-запись для шлюза по умолчанию, представлен на рис. 3.6, стр. 100.

Из рисунка видно, что динамическая ARP-запись имеет следующие атрибуты:

- **`Интерфейс`** – фильтрующий интерфейс МЭ ССПТ-4А1, через который сетевые пакеты доставляются данному узлу сети;
- **`IP-адрес`** – IP-адрес данного узла сети;
- **`MAC-адрес`** – MAC-адрес данного узла сети, полученный автоматически с помощью протокола ARP;
- **`Тип`** – тип данной ARP-записи (динамическая);
- **`Состояние`** – состояние динамической ARP-записи (в приведенном примере ARP-запись – полная, т. к. содержит MAC-адрес узла сети);
- **`До удаления`** – интервал времени, оставшийся до автоматического удаления данной динамической записи. На момент добавлении ARP-записи составляет 1200 с.

Статические ARP-записи добавляются администратором по команде **`nat arp add`**. Например:

```
fnp4> nat arp add interface=2 ip=10.2.253.249 mac=aa:bb:cc:dd:ee:ff
FNPSH-I-007.02.3033-Новая запись добавлена в ARP-таблицу
```

Пример вывода ARP-таблицы с учетом динамической ARP-записи, добавленной ранее, и статической ARP-записи, добавленной по команде выше, представлен на рис. 3.7, стр. 100.

```
14:10:50                          ARP-таблица                          27.06.2017
Интерфейс IP-адрес        MAC-адрес         Тип  Состояние До удаления
eth2      10.2.253.254    00:0c:29:62:84:6b дин  полная    1144 сек

                                   Автообновление: включено | Страница: 1 из 1
                              H - справка    Q, F10 - выход
```

Рисунок 3.6: ARP-таблица: динамическая ARP-запись

```
14:14:41                          ARP-таблица                          27.06.2017
Интерфейс IP-адрес        MAC-адрес         Тип  Состояние До удаления
eth2      10.2.253.249    aa:bb:cc:dd:ee:ff стат
eth2      10.2.253.254    00:0c:29:62:84:6b дин  полная    913 сек

                                   Автообновление: включено | Страница: 1 из 1
                              H - справка    Q, F10 - выход
```

Рисунок 3.7: ARP-таблица: динамическая и статическая ARP-записи

Из рисунка видно, что атрибуты “**Состояние**” и “**До удаления**” для статической ARP-записи не имеют значений, поскольку статическая ARP-запись всегда несет в себе всю необходимую информацию (обязательные параметры команды **nat arp add**), и статическая ARP-запись может быть удалена только администратором МЭ ССПТ-4А1.

Для просмотра ARP-таблицы используются клавиши и управляющие последовательности, перечисленные в таблице 3.12, стр. 101.

Таблица 3.12: Управление просмотром ARP-таблицы

Управление	*Назначение*
<↑>	Перемещение на одну строку таблицы сессий вверх
<↓>	Перемещение на одну строку таблицы сессий вниз
<←>	Перемещение влево на одну позицию
<→>	Перемещение вправо на одну позицию
<Page Up>	Переход к предыдущей странице вывода ARP-таблицы
<Page Down>	Переход к следующей странице вывода ARP-таблицы
<R>	Обновление выводимой информации
<F>	Выключение/включение автоматического обновления выводимой информации
<H>	Вывод подсказки по клавишам управления просмотром ARP-таблицы
<F10>, <Q>	Завершение выполнения команды

Информация, выводимая в ARP-таблице, обновляется каждые **5** секунд. Автоматическое обновление информации может быть выключено (включено) однократным нажатием клавиши **<F>** во время просмотра ARP-таблицы.

Для удаления ARP-записей служит команда **`nat arp delete`**. При этом должен быть указан тип удаляемых записей (параметр **`type`**) и один из следующих параметров удаляемых ARP-записей:

- **`ip`** – IP-адрес узла сети;
- **`mac`** – MAC-адрес узла сети;
- **`interface`** – фильтрующий интерфейс МЭ ССПТ-4А1.

Например, удаление ранее добавленной статической ARP-записи:

```
fnp4> nat arp delete ip=10.2.253.249 type=static
1 Будут удалены ARP-записи NAT:
<eth2  10.2.253.249  aa:bb:cc:dd:ee:ff (s)>
Удалить записи выше? (Y/N) [N]: y
FNPSH-I-007.02.3032-Запись удалена из ARP-таблицы (1)
```

Для удаления всех ARP-записей одного типа служит команда **`nat arp clear`** с параметром **`type`**. В случае, если параметр **`type`** не использован, будут удалены динамические ARP-записи, например:

```
fnp4> nat arp clear
Удалить динамические ARP-записи NAT? (Y/N) [N]: y
FNPSH-I-007.02.3034-ARP-таблица очищена (динамические записи)
```

По команде **nat arp clear** без указания параметра **type** удаляются только динамические ARP-записи.

Указание параметра **`type=static`** в команде **`nat arp clear`** позволяет удалить все статические ARP-записи из таблицы.

Настройка аутентификации сетевых пользователей. МЭ ССПТ-4А1 поддерживает функцию аутентификации сетевых пользователей, работающих во внутренней или внешней сети NAT, для ограничения доступа к сетевым ресурсам пользователей, не прошедших процедуру аутентификации. Данная функция поддерживается только при включенной функции NAT.

При включенной функции аутентификации сетевых пользователей каждый сетевой пакет, полученный на одном из внутренних или внешних интерфейсов NAT, проверяется на принадлежность одному из активных сетевых пользователей. Если такое соответствие установлено, пакет обрабатывается в соответствии с режимом фильтрации. Если соответствия не установлено, то пакет отбрасывается с соответствующей диагностикой.

Для использования функции аутентификации сетевых пользователей администратору МЭ ССПТ-4А1 необходимо выполнить следующую последовательность действий (на примере одного сетевого пользователя):

1) Включить функцию аутентификации сетевых пользователей.
2) Добавить пользователя в базу данных сетевых пользователей.
3) Сформировать открытый и закрытый ключи аутентификации с привязкой к IP-адресу персонального компьютера, с которого будет осуществляться доступ через МЭ ССПТ-4А1.
4) С помощью WEB-интерфейса МЭ ССПТ-4А1 выгрузить с МЭ ССПТ-4А1 следующие файлы:
   - ✔ открытый ключ Диффи-Хеллман устройства МЭ ССПТ-4А1;
   - ✔ файл параметров Диффи-Хеллмана;
   - ✔ закрытый ключ аутентификации для IP-адреса пользователя;
   - ✔ открытый ключ аутентификации для IP-адреса пользователя.

Процедура аутентификации выполняется с помощью утилиты аутентификации сетевого пользователя МЭ ССПТ-4А1, запускаемой на компьютере пользователя. Использование данной утилиты рассматривается в приложении 3, стр. 565.

По умолчанию процедура аутентификации сетевого пользователя выполняется локально, с использованием базы данных сетевых пользователей МЭ ССПТ-4А1. Дополнительно поддерживается возможность выполнять процедуру аутентификации на RADIUS-сервере (см. раздел 3.4.1, стр. 111).

Далее приводится пример настройки МЭ ССПТ-4А1 для использования функции аутентификации сетевых пользователей.

Предполагается, что к моменту начала настройки МЭ ССПТ-4А1 для использования функции аутентификации сетевых пользователей включена **функция трансляции сетевых адресов (NAT)** с использованием следующего контейнера NAT:

```
fnp4> nat case show viewer=no
Контейнеры NAT:

Контейнер NAT: nat1
  Внутренние интерфейсы NAT
    Интерфейс NAT: prv
      Фильтрующие интерфейсы: eth1
      IP-адреса: 10.2.253.246/255.255.255.248
  Внешние интерфейсы NAT
    Интерфейс NAT: pub
      Фильтрующие интерфейсы: eth2
      IP-адреса: 10.2.253.253/255.255.255.248
  Правила трансляции NAT
    number=1 prv-address=10.2.253.240/255.255.255.248 pub-address=10.2.253.253
interface=pub dst-address=any protocol=any
  Правила переадресации NAT (переадресация включена)
  Таблица маршрутов NAT
    dst-address=10.2.253.240/255.255.255.248 interface=prv
    dst-address=10.2.253.248/255.255.255.248 interface=pub
    number=1 dst-address=0.0.0.0 gateway=10.2.253.254 interface=pub
```

Включение функции аутентификации сетевых пользователей. Для этого служит команда **`nat authentication set`**. Например:

```
fnp4> nat authentication set state=enable
FNPSH-I-007.02.3071-Аутентификация сетевых пользователей включена
```

Команда **`nat authentication set`** также позволяет изменить тайм-аут неактивности сетевых пользователей, по истечению которого сетевому пользователю необходимо снова выполнить процедуру аутентификации для дальнейшей работы через МЭ ССПТ-4А1. Например:

```
fnp4> nat authentication set timeout=1200
FNPSH-I-007.02.307A-Тайм-аут неактивности сетевых пользователей изменен
```

Тайм-аут неактивности сетевых пользователей по умолчанию составляет **600** секунд.

Добавление сетевого пользователя в базу данных сетевых пользователей. Для этого служит команда **`nat authentication user add`**. Например:

```
fnp4> nat authentication user add name=netuser1
Новый пароль:
Новый пароль повторно:
Параметры сетевого пользователя:
  Имя сетевого пользователя: netuser1 ()
  Ограничения доступа:
    MAC-адрес: any
    IP-адрес: any
    Фильтрующие интерфейсы: any
FNPSH-I-007.02.3073-Новый сетевой пользователь добавлен (netuser1)
```

Команда **nat authentication user add** также позволяет с помощью необязательных параметров задать ряд ограничений для добавляемого сетевого пользователя:

- **address** – IP-адрес компьютера, с которого разрешена аутентификация для данного сетевого пользователя;
- **mac** – MAC-адрес компьютера, с которого разрешена аутентификация для данного сетевого пользователя;
- **interface** – фильтрующие интерфейсы МЭ ССПТ-4А1, с которых разрешены запросы аутентификации от данного сетевого пользователя.

Параметры учетной записи сетевого пользователя могут быть изменены с помощью команды **nat authentication user edit**. Например учетная запись сетевого пользователя может быть выключена или включена:

```
fnp4> nat authentication user edit name=netuser1 state=disable
Параметры сетевого пользователя:
  Имя сетевого пользователя: netuser1 ()
  Состояние: выключено
  Ограничения доступа:
    MAC-адрес: any
    IP-адрес: any
    Фильтрующие интерфейсы: any

Изменить параметры сетевого пользователя? (Y/N) [N]: y
FNPSH-I-007.02.3075-Сетевой пользователь выключен (netuser1)
fnp4> nat authentication user edit name=netuser1 state=enable
Параметры сетевого пользователя:
  Имя сетевого пользователя: netuser1 ()
  Состояние: включено
  Ограничения доступа:
    MAC-адрес: any
    IP-адрес: any
    Фильтрующие интерфейсы: any

Изменить параметры сетевого пользователя? (Y/N) [N]: y
FNPSH-I-007.02.3076-Сетевой пользователь включен (netuser1)
```

Для смены пароля учетной записи сетевого пользователя служит команда **nat authentication user password**. Например:

```
fnp4> nat authentication user password name=netuser1
Новый пароль:
Новый пароль повторно:
FNPSH-I-007.02.3077-Пароль сетевого пользователя изменен (netuser1)
```

Для удаления учетной записи сетевого пользователя служит команда **nat authentication user delete**. Например (предполагается, что ранее была добавлена учетная запись сетевого пользователя **netuser2**):

```
fnp4> nat authentication user delete name=netuser2
Удалить сетевого пользователя? (Y/N) [N]: y
FNPSH-I-007.02.3074-Сетевой пользователь удален (netuser2)
```

Для просмотра списка учетных записей сетевых пользователей служит команда **nat authentication user list**. Например:

```
fnp4> nat authentication user list
Всего сетевых пользователей: 1

Пользователь IP-адрес MAC-адрес    Интерфейс Состояние Комментарий
netuser1     любой    любой        0,1,2,3,4,5,6,7 включен
```

Формирование открытого и закрытого ключей аутентификации сетевого пользователя. Для формирования данной пары ключей с привязкой к IP-адресу персонального компьютера, с которого будет осуществляться доступ через МЭ ССПТ-4А1, служит команда **`nat key add`**. Например, предполагается что сетевой пользователь будет осуществлять доступ с компьютера с IP-адресом **`10.2.253.242`**, принадлежащего внутренней сети NAT (см. настройки контейнера NAT выше). В этом случае необходимо выполнить команду:

```
fnp4> nat authentication key add address=10.2.253.242
FNPSH-I-007.02.307C-Новая запись добавлена в файл ключей аутентификации (10.2.253.242)
```

Ранее добавленные ключи аутентификации сетевых пользователей могут быть заново сформированы с сохранением привязки к IP-адресу компьютера сетевого пользователя. Для этого служит команда **`nat authentication key update`**. Например:

```
fnp4> nat authentication key update address=10.2.253.242
Обновить запись? (Y/N) [N]: y
FNPSH-I-007.02.307E-Запись изменена в файле ключей аутентификации (10.2.253.242)
```

Для удаления ключа аутентификации служит команда **`nat authentication key delete`**, при этом должен быть указан IP-адрес, к которому привязан ключ. Пример добавления и удаления ключа аутентификации:

```
fnp4> nat authentication key add address=10.3.4.5
FNPSH-I-007.02.307C-Новая запись добавлена в файл ключей аутентификации (10.3.4.5)
fnp4> nat authentication key delete address=10.3.4.5
Удалить запись? (Y/N) [N]: y
FNPSH-I-007.02.307D-Запись удалена из файла ключей аутентификации (10.3.4.5)
```

Для просмотра ранее добавленных ключей аутентификации служит команда **`nat authentication key show`**. Пример вывода команды представлен на рис. 3.8, стр 106.

```
18:11:36                    Файл ключей аутентификации                29.06.2017

Всего записей: 1

-------------------------------------------------------------
IP-адрес: 10.2.253.242

Закрытый ключ: 4FDAC326649C86621F25B2648598362100708CBE3800C18A12F980D459300C4CA

Открытый ключ: 2E3EE4D9FC1338AC0857DA921065CE1F10AC05D3875A8DBA792BB757CCA70C5BE

Строки: 1-9 из 9                Столбцы: 1-80    H - справка  Q, F10 - выход
```

Рисунок 3.8: Просмотр ключей аутентификации сетевых пользователей

Выгрузка с МЭ ССПТ-4А1 файлов, необходимых для выполнения процедуры аутентификации. Выгрузка осуществляется через WEB-интерфейс МЭ ССПТ-4А1. Должны быть выгружены следующие файлы:

- открытый ключ Диффи-Хеллман устройства МЭ ССПТ-4А1;
- файл параметров Диффи-Хеллмана;
- закрытый ключ аутентификации IP-адреса пользователя;
- открытый ключ аутентификации IP-адреса пользователя.

Выгрузка данных файлов посредством WEB-интерфейса администратора рассмотрена в разделе 4.2.5, стр. 267.

Процедура аутентификации выполняется с помощью утилиты аутентификации сетевого пользователя МЭ ССПТ-4А1, запускаемой на компьютере пользователя. Использование данной утилиты рассматривается в приложении 3, стр. 565.

Далее, при приведении примеров выполнения команд подразумевается, что аутентификация сетевого пользователя **`netuser1`** была успешно выполнена, сетевой пользователь **`netuser1`** активен, тайм-аут неактивности пользователя не истек на момент выполнения команд, приводимых в примерах.

Просмотр списка активных сетевых пользователей. Для просмотра списка активных сетевых пользователей, т. е. пользователей, успешно прошедших процедуру аутентификации и чей тайм-аут неактивности еще не истек, служит команда **`nat authentication user show`**. Например:

```
fnp4> nat authentication user show
Активных сетевых пользователей: 1  Системное время: 30.06.2017 17:11:56 (MSK)

Пользователь Время входа         Откуда                           Неактивность
netuser1     30.06.2017 17:11:38 1,00:0c:29:b7:34:ec,10.2.253.242 18с
```

Из вывода команды **nat authentication user show** можно получить следующую информацию об активном сетевом пользователе:

- идентификатор (имя) сетевого пользователя (поле “Пользователь”);
- дата и время входа пользователя (прохождения процедуры аутентификации пользователем) (поле “Время входа”);
- информация от том, откуда работает сетевой пользователь (поле “Откуда”):
  - ✔ номер фильтрующего интерфейса, на который получен запрос аутентификации (в приведенном примере: интерфейс с номером 1, являющийся внутренним интерфейсом NAT в соответствии с используемым контейнером NAT);
  - ✔ MAC-адрес сетевого интерфейса компьютера сетевого пользователя, с которого был отправлен запрос аутентификации;
  - ✔ IP-адрес сетевого интерфейса компьютера сетевого пользователя, с которого был отправлен запрос аутентификации;
- время неактивности сетевого пользователя в секундах, т. е. интервал времени с момента получения на фильтрующий интерфейс МЭ ССПТ-4А1 последнего пакета с компьютера сетевого пользователя (поле “Неактивность”).

По завершению тайм-аута неактивности, который по умолчанию составляет **600 секунд**, запись сетевого пользователя будет автоматически удалена из **списка активных сетевых пользователей,** и для продолжения работы через МЭ ССПТ-4А1 потребуется снова выполнить процедуру аутентификации.

Сеанс работы активного сетевого пользователя может быть принудительно завершен администратором. Для этого служит команда **nat authentication user clear** с указанием параметра **name**. Например:

```
fnp4> nat authentication user show
Активных сетевых пользователей: 1  Системное время: 30.06.2017 17:55:47 (MSK)

Пользователь Время входа         Откуда                           Неактивность
netuser1     30.06.2017 17:51:45 1,00:0c:29:b7:34:ec,10.2.253.242 4м2с
fnp4> nat authentication user clear name=netuser1
Завершить сеанс сетевого пользователя? (Y/N) [N]: y
FNPSH-I-007.02.3078-Сеанс сетевого пользователя завершен (netuser1)
fnp4> nat authentication user show
FNPSH-I-007.02.3079-Нет активных сетевых пользователей
```

Из приведенного вывода видно, что в результате выполнения команды **nat authentication user clear** запись сетевого пользователя **netuser1** была удалена из списка активных пользователей.

Если в команде **`nat authentication user clear`** отсутствует параметр **`name`**, то в результате ее выполнения будут завершены сеансы всех активных сетевых пользователей.

3.2.4. Функция приоритетной обработки трафика

Функция приоритетной обработки трафика обеспечивает возможность ускорения или замедления в обработке трафика заданного типа, выделенного по параметрам, задаваемым в правилах приоритизации.

Реализованный в МЭ ССПТ-4А1 алгоритм приоритетной обработки подразумевает наличие взвешенных очередей, каждой из которых соответствует некоторое значение приоритета и фиксированный весовой коэффициент. Весовой коэффициент определяет соотношение максимального количества пакетов с определенным приоритетом, которое поток фильтрации имеет право принять на обработку за один рабочий цикл. Значения весовых коэффициентов для различных типов приоритетов представлены в таблице 3.13, стр. 108.

Таблица 3.13: Значения весовых коэффициентов для очередей с разными приоритетами

Приоритет	***Максимальное количество пакетов за один рабочий цикл***	***Доля пропускной способности, %***
Высокий приоритет	10	63
Базовый приоритет	5	31
Низкий приоритет	1	6

Выборка трафика из очередей происходит в порядке от высокого приоритета к низкому. В течение рабочего цикла принимается на обработку доступное количества пакетов, но не более установленного максимального количества для данной очереди, после чего осуществляется переход к менее приоритетной очереди.

Для включения и выключения функции приоритетной обработки трафика используются команды **`rule priority enable`** и **`rule priority disable`** соответственно. Например:

```
fnp4> rule priority enable
FNPSH-I-007.02.312B-Использование PRI-правил включено
```

Для настройки приоритетной обработки трафика необходимо добавить правила приоритизации, воспользовавшись командой **`rule add pri`** со следующими параметрами:

- **`priority`** – приоритет, назначаемый подходящим под правило пакетам. Возможна установка двух значений:
  - ✔ **`high`** – высокий приоритет;
  - ✔ **`low`** – низкий приоритет;
- **`srcif`** – номер или имя фильтрующего интерфейса, на котором ожидается прием пакетов;
- **`srcip4`**/**`srcip6`** – IPv4- или IPv6-адрес источника пакета. Может быть задан диапазон адресов;

- **dstip4/dstip6** – IPv4- или IPv6-адрес приемника пакета. Может быть задан диапазон адресов;
- **srcport** – номер порта источника пакета. Может быть задан список номеров портов;
- **dstport** – номер порта приемника пакета. Может быть задан список номеров портов;
- **ipproto** – код или имя протокола, инкапсулированного в IPv4 -или IPv6-пакет;
- **comment** – комментарий к правилу приоритизации.

> Определение правила приоритизации (полный перечень параметров и форматы их значений) приведены в приложении Д.4, стр. 536.

Для того, чтобы задать приоритет для всех пакетов конкретной сессии, необходимо добавить два правила приоритизации, которые будут отличаться “*переставленными*” значениями IP-адресов и номеров портов источника и приемника. Например:

```
fnp4> rule add pri:1 priority=high srcip4=10.2.100.10 dstip4=10.2.200.10 srcport=4000
dstport=4001
FNPSH-I-007.02.3126-PRI-правило добавлено (1)
fnp4> rule add pri:2 priority=high dstip4=10.2.100.10 srcip4=10.2.200.10 dstport=4000
srcport=4001
FNPSH-I-007.02.3126-PRI-правило добавлено (2)
```

Проверить, что правила приоритизации добавлены, можно, используя команду **rule show.** Правила приоритизации для приведенного примера представлены ниже:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=accept log=enable
ap:0 action=drop
pri:1 priority=high srcip4=10.2.100.10 srcport=4000 dstip4=10.2.200.10 dstport=4001
pri:2 priority=high srcip4=10.2.200.10 srcport=4001 dstip4=10.2.100.10 dstport=4000
```

Помимо добавления для правил приоритизации доступны те же операции, что и для общих правил фильтрации:

- **rule delete pri** – удаление правила приоритизации;
- **rule edit pri** – редактирование правила приоритизации;
- **rule copy pri** – копирование правила приоритизации;
- **rule show type=pri** – просмотр правил приоритизации.

3.3. Контроль целостности

В составе ПО МЭ ССПТ-4А1 реализована подсистема контроля целостности основных компонентов УОС МЭ ССПТ-4А1, подсистем ПО МЭ ССПТ-4А1 и всех конфигурационных файлов. Контроль целостности осуществляется на основе периодической проверки контрольных сумм файлов, содержащих перечисленные выше компоненты.

Период проверки контрольных сумм файлов составляет: **14400 секунд (4 часа)**.

Таким образом, подсистема контроля целостности предотвращает попытки несанкционированного изменения исполняемых файлов и библиотек подсистем МЭ ССПТ-4А1, а также конфигурационных файлов путем прямого редактирования, минуя использование штатных средств администрирования МЭ ССПТ-4А1.

При обнаружении нарушения контрольной суммы подсистема контроля целостности выполнит следующие действия:

1) останов пакетного фильтра МЭ ССПТ-4А1;
2) регистрация события о нарушении контрольной суммы с указанием имени файла;
3) перевод подсистемы авторизации в однопользовательский режим работы – доступ к интерфейсу управления будет возможен только для администратора с идентификатором “**`admin`**”.

Изделие будет принудительно выключено подсистемой контроля целостности в случае появления **следующих критических ошибок**:

- ошибка чтения текущего файла параметров конфигурации МЭ ССПТ-4А1;
- ошибка чтения файла контрольных сумм МЭ ССПТ-4А1.

Контроль целостности также может быть выполнен администратором в произвольный момент времени. Для выполнения контроля целостности в КИА необходимо выполнить команду **`system icheck`** (рисунок 3.9, стр. 111).

В результате в полноэкранном режиме (раздел 3.1.8, стр. 62) построчно будет выведена таблица, в каждой строке которой указывается:

- имя контролируемого исполняемого файла, библиотеки или конфигурационного файла МЭ ССПТ-4А1;
- результат проверки целостности данного файла:
  - ✔ **+** – целостность файла не нарушена;
  - ✔ **-** – целостность файла нарушена;
- вычисленная во время выполнения команды **`system icheck`** контрольная сумма файла.

```
09:08:38                    Проверка целостности                    04.03.2021
Имя файла                  Результат Контрольная сумма
-----------------------------------------------------------------------------
rc.conf                       +        9A3B132AFBB383118215FD21D9B0F7ABFB32499B1ECB
fnp4                          +        17DAA971AB004FDEB708681F3403BEF3F89980206B19
fnp4eth                       +        145DC0CA9D7E982AAF4B1A972CCF2880840990F1E577
fnp4proxy                     +        2BAE035CD04A4D37295A253A8618575050589C1CF8FF
fnp4snmp                      +        20A48D7F6B496EE8757C7ACF1041D0C216BAB41A52B5
fnp4tmp                       +        B72AB6C48FF6221AAEC8885CD803937CBCF86C076077
fnp4web                       +        08ED2029B4544EF034CDE780288181D169AB3FEAA12B
kernel                        +        5B060E5BE88CDBA21303FFADB070CD70C942B647323F
libc.so.7                     +        2A5252E11888619A66E403ECE496131DA4D7465068A8
libkvm.so.7                   +        E47577DA165D2B22FEC2F25DA5D9C4E8B02AC21493BD
libcrypto.so.8                +        CF91396F03E1E5269D82F9D2BE6660128014DB3A2D66
libssl.so.8                   +        93BEBE43AE3FD211F6FB9849F5C384034EC078ED2151
libxml2.so.2.9.10             +        7377CEB9B830476830F04FDC573A8FBC10146A4593C2
libfnpcrypt2_ssl.so.2.1.0     +        B8CA6738CCB739AC51BE692A04E988B4E45507C382C1
login                         +        081956FC5FC4D4066C0304F5566049A1CDE0EC14F9BE
ntpdate                       +        83DB8416220B9509A68096B7B3DDC84A284A580C8A3E
httpd                         +        D0926F7952B34A8110009273FEDCE026108A75BB9852
snmpd                         +        7F376BE4D9CD576780AAB5A6DBCC6D570B40747C966C
openssl                       +        3F080C4279F8F3B02833F8368F5EF90093DA0710D2FC
fnp4sh                        +        4A12F8CBD286FFB438A6032AA035B044B993B1ADB272
fnp4_info                     +        58ACA9213F03921DB4B7CFADA93AC2485BB8170339E4
fnp4_authd                    +        2270CCAAB577BE25F6DE65A179430D54EB9E940CAAF6
fnp4_csd                      +        DCB0C596AC0D360F7DD67F016ADD1455C15F0284131F
fnp4_filtd                    +        AB3954705AF0C20AFCA4A11B5CBCEC0020F0BD448EAF
fnp4_had                      +        964FA3ED6AD8932CCE23DB4578CA55693010184D14F7
fnp4_lcmd                     +        21E658CE4BFE663ADC2ACA82933335317512B8C3B0D89
 Строки: 1-28 из 62                Столбцы: 1-80    H - справка  Q, F10 - Выход
```

Рисунок 3.9: Вывод команды проверки целостности

Выполнение контроля целостности также доступно через WEB-интерфейс администратора (раздел 4.1.3, стр. 229).

3.4. Разграничение прав доступа, идентификация и аутентификация

3.4.1. Идентификация и аутентификация администраторов и сетевых пользователей через RADIUS-сервер.

МЭ ССПТ-4А1 обеспечивает возможность идентификации и аутентификации администраторов и сетевых пользователей через RADIUS-сервер в дополнение к идентификации и аутентификации с использованием локальных файлов учетных записей.

Для использования функции идентификации и аутентификации через RADIUS-сервер требуется выполнить следующие шаги:

1) сконфигурировать ПО RADIUS-сервера;

2) подключить сконфигурированный RADIUS-сервер к управляющей сети МЭ ССПТ-4А1

3) настроить параметры идентификации и аутентификации через RADIUS-сервер с помощью КИА или WEB-интерфейс администратора.

Ниже в данном разделе описываются шаги настройки функции идентификации и аутентификации через RADIUS-сервер.

Настройка RADIUS-сервера. Данный этап будет рассмотрен на примере настройки программного пакета `freeradius3-3.0.12`. Настройка данного ПО сводится к внесению изменений в конфигурационные файлы ПО и добавлению файла словаря `dictionary.nportc` с VSA-атрибутами (`Vendor Specific Attributes`) МЭ ССПТ-4А1 в соответствующий каталог данного ПО. Рассмотрим процесс настройка RADIUS-сервера:

1) Добавить в файл `/usr/local/etc/raddb/clients.conf` запись, содержащую:

- ✔ произвольное символическое имя (указывается после ключевого слова `client`);
- ✔ IP-адрес управляющего интерфейса МЭ ССПТ-4А1 (параметр `ipaddr`);
- ✔ секретный ключ (параметр `secret`).

Например:

```
client fnp4-dc7 {
    ipaddr = 10.98.3.7
    secret = parisdakar
}
```

2) Создать в каталоге RADIUS-сервера `/usr/local/etc/raddb/` файл словаря `dictionary.nportc` со следующим содержимым (строки, начинающиеся с символа # являются комментариями):

```
# dictionary файл для ССПТ-4А1

VENDOR NPORTC 32907

BEGIN-VENDOR NPORTC

# атрибуты:
# 1: тип учетной записи
# 2: IP-адрес сетевого пользователя
# 3: MAC-адрес сетевого пользователя
# для простоты указания MAC-адреса в файле users лучше использовать
# тип string, а не octets
# 4: номер фильтрующего интерфейса сетевого пользователя
# для атрибута Interface используем тип string, т.к. необходима проверка
# по р.в., т.к. пользователю может быть разрешен вход с нескольких
# интерфейсов
# 5: привилегии обычного пользователя (администратора МЭ)

ATTRIBUTE NPORTC-User-Type            1 integer
ATTRIBUTE NPORTC-Net-User-IP-Address  2 ipaddr
ATTRIBUTE NPORTC-Net-User-MAC-Address 3 string
ATTRIBUTE NPORTC-Net-User-Interface   4 string
ATTRIBUTE NPORTC-User-Privilege       5 integer

# строки для значений integer атрибутов:
# NPORTC-User-Type: тип учетной записи
# NPORTC-User-Privilege: привилегии учетной записи

VALUE NPORTC-User-Type       Local 1
```

```
VALUE NPORTC-User-Type       Network 2
VALUE NPORTC-User-Privilege  Read 0
VALUE NPORTC-User-Privilege  Full 1

END-VENDOR NPORTC
```

3) Включить файл `dictionary.nportc` в основной файл словаря `/usr/local/etc/raddb/dictionary`, добавив в него строку:

```
$INCLUDE dictionary.nportc
```

4) Добавить учетные записи в файл `/usr/local/etc/raddb/users` пользователей для аутентификации через RADIUS-сервер. Например, запись для администратора `reader`, и запись для сетевого пользователя `nuser1`:

```
reader Cleartext-Password := "reader123", NPORTC-User-Type == Local
         NPORTC-User-Privilege = Read
nuser1 Cleartext-Password := "netuser1", NPORTC-User-Type == Network, NPORTC-Net-User-IP-
Address == 10.98.31.33
```

Учетная запись администратора МЭ ССПТ-4А1 в файле **users** должна содержать следующие **VSA-атрибуты**, определенные в файле **dictionary.nportc**:

- **NPORTC-User-Type** в первой строке записи (строка проверяемых атрибутов) со значением **Local**;
- **NPORTC-User-Privilege** во второй строке (или одной из последующих строк) записи (атрибут ответа Access-Accept) с одним из следующих значений:
  - ✔ read;
  - ✔ full;

Учетная запись сетевого пользователя МЭ ССПТ-4А1 в файле **users** должна иметь **VSA-атрибут NPORTC-User-Type**, определенный в файле **dictionary.nportc**, со значением **Network**.

Учетная запись сетевого пользователя МЭ ССПТ-4А1 в файле **users** может содержать следующие необязательные **VSA-атрибуты**, определенные в файле **dictionary.nportc**:

- **NPORTC-Net-User-IP-Address**: если учетная запись сетевого пользователя привязана к IP-адресу узла сети;
- **NPORTC-Net-User-MAC-Address**: если учетная запись сетевого пользователя привязана к MAC-адресу сетевого интерфейса узла сети;
- **NPORTC-Net-User-Interface**: если учетная запись сетевого пользователя привязана к конкретным фильтрующим интерфейсам МЭ ССПТ-4А1.

5) Перезапустить ПО `freeradius` для применения обновленной конфигурации ПО, выполнив в терминале команду: **`service radiusd restart`** (либо: **`service radiusd onerestart`**), либо запустить ПО `freeradius` (если не было запущено ранее), выполнив команду: **`service radiusd start`** (либо: **`service radiusd onestart`**).

На этом этап конфигурации RADIUS-сервера завершен.

Подключение сконфигурированного RADIUS-сервера к управляющей сети МЭ ССПТ-4А1. RADIUS-сервер может быть подключен как к управляющей IP-сети МЭ ССПТ-4А1, например через коммутатор, так и к другой IP-сети. В последнем случае на МЭ ССПТ-4А1 необходимо настроить маршрут по умолчанию, через который будет осуществляться доступ к IP-сети, в которой находится RADIUS-сервер. Настройка маршрута по умолчанию может быть выполнена как через командный интерфейс администратора, так и через WEB-интерфейс.

Ниже приводится пример настройки маршрута по умолчанию через командный интерфейс администратора МЭ ССПТ-4А1:

```
fnp4> system route add dst-address=0.0.0.0 gateway=10.2.1.126
FNPSH-I-007.02.312F-Маршрут добавлен
```

Во избежание потери связности с МЭ ССПТ-4А1 рекомендуется выполнять установку маршрута по умолчанию при локальном подключении к МЭ ССПТ-4А1.

В доступности RADIUS-сервера с управляющего интерфейса МЭ ССПТ-4А1 можно убедиться, выполнив команду **`interface control ping host=<IP-адрес_RADIUS-сервера>`**. Например:

```
fnp4> interface control ping host=10.98.3.1
PING 10.98.3.1: 56 data bytes
64 bytes from 10.98.3.1: seq=0, ttl=64, rtt=1,013 ms
64 bytes from 10.98.3.1: seq=1, ttl=64, rtt=0,199 ms
64 bytes from 10.98.3.1: seq=2, ttl=64, rtt=0,268 ms

--- 10.98.3.1 ping statistics ---
3 packets transmitted, 3 packets received,
round-trip min/avg/max/stddev = 0,199/0,493/1,013/0,369 ms
fnp4>
```

Настройка параметров идентификации и аутентификации через RADIUS-сервер. Подразумевается, что в локальные файлы учетных записей администраторов и сетевых пользователей МЭ ССПТ-4А1 добавлены все учетные записи, которые были добавлены в файл `users` RADIUS-сервера. Ниже приводится пример команды настройки параметров идентификации и аутентификации администраторов и сетевых пользователей МЭ ССПТ-4А1 через RADIUS-сервер (подразумевается что настройка RADIUS-сервера уже выполнена):

```
fnp4> user radius set master-server=10.98.3.1 master-key=parisdakar state=enable
FNPSH-I-007.02.3080-RADIUS-авторизация включена
FNPSH-I-007.02.307F-Конфигурация RADIUS-сервера изменена
```

В результате выполнения данной команды идентификация и аутентификация через RADIUS-сервер включена и используется как для администраторов, так и для сетевых пользователей МЭ ССПТ-4А1.

Посредством установки соответствующего параметра конфигурации можно выбрать категорию учетных записей, для которой будет использоваться идентификация и аутентификация через RADIUS-сервер:

- только администраторы МЭ ССПТ-4А1;
- только сетевые пользователи МЭ ССПТ-4А1;
- администраторы и сетевые пользователи МЭ ССПТ-4А1 (**значение по умолчанию**).

Изменить категорию учетных записей МЭ ССПТ-4А1, для которых используется идентификация и аутентификация через RADIUS-сервер, можно с помощью параметра **`type`** использованной выше команды **`user radius set`**.

При настройке параметров идентификации и аутентификации администраторов и/или сетевых пользователей МЭ ССПТ-4А1 через RADIUS-сервер могут быть также заданы следующие необязательные параметры:

- **`retry`** – количество обращений к RADIUS-серверу: определяет количество повторных обращений к RADIUS-серверу в том случае, если за заданный тайм-аут ожидания не был получен ответ от RADIUS-сервера;
- **`timeout`** – тайм-аут ожидания ответа от RADIUS-сервера: определяет интервал ожидания ответа от RADIUS-сервера на запрос аутентификации.

Параметр **retry** по умолчанию имеет значение **3**. Допустимый диапазон значений **1..10**.
Параметр **timeout** по умолчанию имеет значение **5** секунд. Допустимый диапазон значений **0..10** секунд.

Кроме того, допускается использование запасного RADIUS-сервера, обращение к которому производится в случае недоступности основного RADIUS-сервера. Для возможности использования запасного RADIUS-серевера в команде **`user radius set`** должны быть указаны параметры запасного RADIUS-сервера:

- **`slave-server`** – IP-адрес запасного RADIUS-сервера;
- **`slave-key`** – секретный ключ запасного RADIUS-сервера.

Секретные ключи основного и запасного RADIUS-серверов (параметры **master-key** и **slave-key** соответственно) могут иметь длину от **1** до **127** символов. Допускается использование любых печатаемых символов, но при этом секретный ключ должен удовлетворять требованиям к формату секретного ключа в используемом ПО RADIUS-сервера.

Задание параметров **master-port** (порт основного RADIUS-сервера) и **slave-port** (порт запасного RADIUS-сервера) необязательно. По умолчанию используется порт **1812**.

Идентификация и аутентификация администратора МЭ ССПТ-4А1 с именем **admin** всегда выполняется с использованием локального файла учетных записей администраторов МЭ ССПТ-4А1.

Иначе говоря, для администратора **admin** идентификация и аутентификация через RADIUS-сервер **не применима**.

Если в конфигурации МЭ ССПТ-4А1 включена идентификация и аутентификация через RADIUS-сервер, то процедура идентификации и аутентификации учетной записи (администратор и/или сетевой пользователь) выполняется в следующем порядке:

- идентификация и аутентификация через основной RADIUS-сервер;
- идентификация и аутентификация через запасной RADIUS-сервер (если основной RADIUS-сервер недоступен и запасной RADIUS-сервер определен в конфигурации);
- идентификация и аутентификация через локальный файл учетных записей (если авторизация через RADIUS-сервер(ы) не была выполнена).

3.5. Система фильтрации с резервированием на основе МЭ ССПТ-4А1

3.5.1. Резервирование МЭ ССПТ-4А1

На основе МЭ ССПТ-4А1 может быть создана система фильтрации с резервированием для обеспечения отказоустойчивости процесса фильтрации. Система фильтрации с резервированием может использовать одну из двух логических схем подключения (далее “схема резервирования”):

- схема “**активный-резервный**” реализуется путем установки на парных устройствах режимов **Master**/**Slave**;
- схема “**активный-активный**” реализуется путем установки на парных устройствах режимов **Sync**/**Sync** или **Balance**/**Balance**.

Режим резервирования — параметр конфигурации МЭ ССПТ-4А1, определяющий основную роль данного устройства в схеме резервирования. Режимы резервирования, устанавливаемые на устройствах, определяются требуемой схемой резервирования.

Состояние резервирования — текущая (актуальная) роль данного устройства в схеме резервирования, которая определяется:

- режимом резервирования, заданным для данного устройства;
- состоянием парного устройства в схеме резервирования.

Состояния резервирования делятся на две группы:

- **рабочее состояние** – состояние, в котором устройство работоспособно и выполняет соответствующие функции в схеме резервирования;
- **состояние отказа** – состояние, в котором устройство неработоспособно и не может выполнять фильтрацию трафика.

Рабочие состояния:

- для режима **Master** – единственное рабочее состояние **Master**;
- для режима **Slave** – основное рабочее состояние **Slave**, также допускается рабочее состояние **Master** в случае отказа парного МЭ ССПТ-4А1, работавшего в режиме **Master**;
- для режима **Sync** – единственное рабочее состояние **Sync**;
- для режима **Balance** – единственное рабочее состояние **Balance**.

Состояния отказа:

- **программный отказ** возникает в случае, когда вследствие штатного останова либо аварийного завершения оказывается неработоспособным процесс пакетного фильтра. МЭ ССПТ-4А1, на котором возникла такая ситуация, оповещает парный МЭ ССПТ-4А1 о переходе в данное состояние;
- **аппаратный отказ** парного МЭ ССПТ-4А1 определяется в случае, когда парный МЭ ССПТ-4А1 не отвечает на запросы в течение 3 с.

Конфигурация обоих изделий схемы резервирования должна быть одинакова, за исключением настроек подсистемы резервирования и адресов управляющего интерфейса.

Управление и настройка параметров МЭ ССПТ-4А1 в системе фильтрации с резервированием осуществляется из командного интерфейса администратора либо WEB-интерфейса администратора. Порядок настройки системы фильтрации с резервированием, ее запуска и останова, а также описание используемых при этом команд, представлены ниже.

3.5.2. Резервирование “активный-резервный” в режиме Master/Slave

Схема резервирования **“активный-резервный”** предполагает работу двух МЭ ССПТ-4А1, один из которых находится в режиме **Master**, другой – в режиме **Slave**. Данная схема строится на основе принципа “горячего” резервирования: два МЭ ССПТ-4А1 подключаются к сегментам локальной сети параллельно и работают как единая логическая система фильтрации (см. рисунок 3.10, стр. 118). При этом один МЭ ССПТ-4А1 является активным (режим **Master**) и производит фильтрацию трафика, а второй – резервным (режим **Slave**) и находится в “горячем” резерве, не пропуская пакеты, которые достигают его фильтрующих интерфейсов. Синхронизация и обмен сообщениями между парными МЭ ССПТ-4А1, находящимися в режимах **Master** и **Slave** с целью выявления отказов и переключения состояний, происходит через управляющие Ethernet-интерфейсы (EthC) устройств.

Логическая система фильтрации, построенная на МЭ ССПТ-4А1 в схеме резервирования “активный-резервный”, обеспечивает бесперебойное функционирование системы фильтрации при любом отказе аппаратных или программных компонентов устройства, работающего в режиме **Master**, если такой отказ приводит к прекращению работы пакетного фильтра (подсистемы фильтрации) устройства. При выявлении отказа МЭ ССПТ-4А1, работающего в режиме **Master**, МЭ ССПТ-4А1, работающий в режиме **Slave**, сменит свое состояние на **Master**. Если далее МЭ ССПТ-4А1, работавший в режиме **Master**, восстановится (преодолеет состояние отказа), то состояния обоих МЭ ССПТ-4А1 сменятся и снова будут соответствовать их режимам, настроенным при конфигурации.

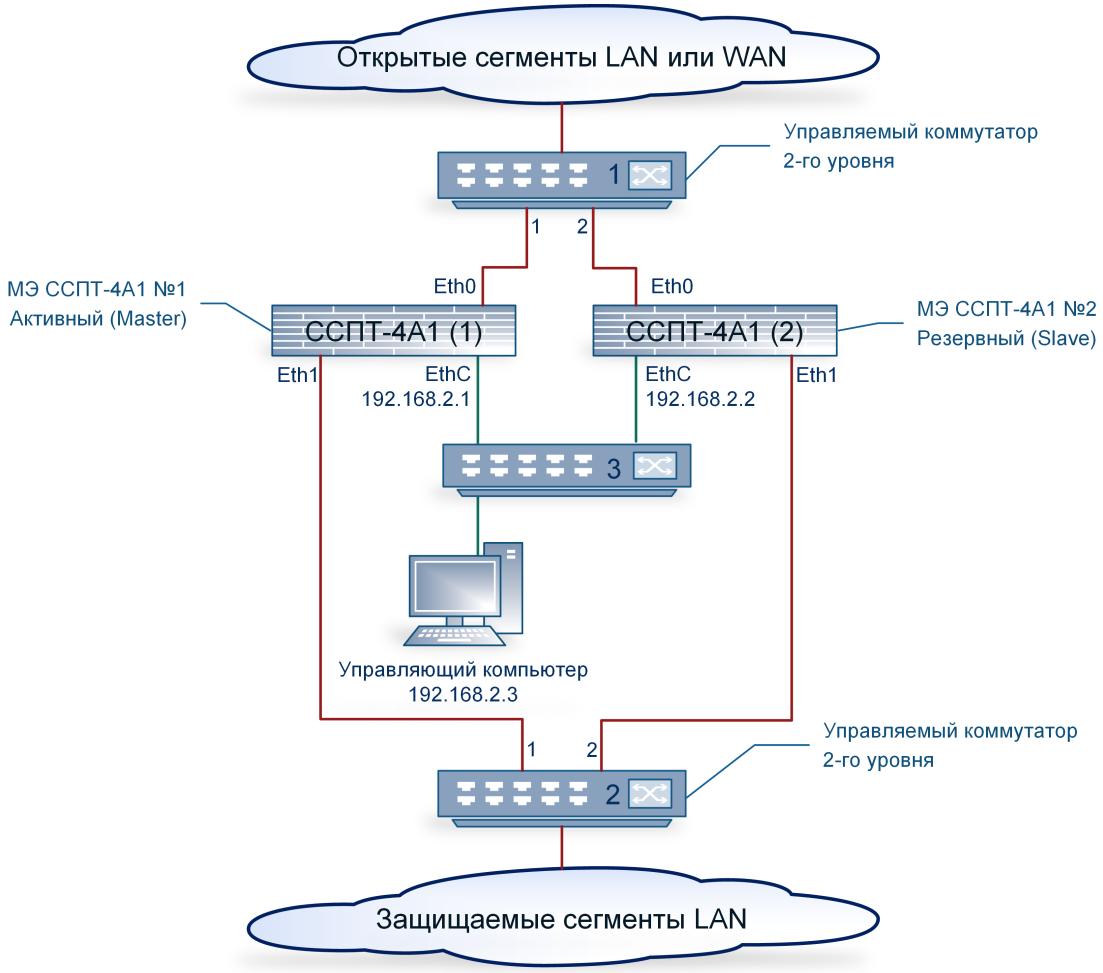


Рисунок 3.10: Схема резервирования “Активный-резервный” в режиме Master/Slave.

Особенности схемы **“активный-резервный”** в режиме **Master/Slave**:

- возможна автоматическая или ручная синхронизация политики доступа между двумя МЭ ССПТ-4А1 (см. раздел 3.5.5)
- в случае отказа МЭ ССПТ-4А1, работающего в режиме **Master**, происходит обрыв установленных сеансов связи, работавших через схему фильтрации. После перехода на резервный МЭ ССПТ-4А1 пользователи должны восстановить свои сеансы связи;
- в данном режиме могут использоваться только исполнения МЭ ССПТ-4А1, у которых все фильтрующие интерфейсы имеют идентичные типы, например, 5 фильтрующих интерфейсов Ethernet 1 Гбит/с (исполнение 01);
- требуется настройка коммутаторов, к которым подключены МЭ ССПТ-4А1:
  - ✔ установка параметров скорости/дуплекса портов коммутаторов, подключенных к фильтрующим интерфейсам МЭ ССПТ-4А1.

Доступность МЭ ССПТ-4А1 для передачи трафика в состояниях **Master** и **Slave** обеспечивается специальным режимом работы фильтрующих интерфейсов. В состоянии **Master** фильтрующие интерфейсы МЭ ССПТ-4А1 **активны**, т.е. несущая между интерфейсами МЭ ССПТ-4А1 и портами коммутатора поднята. В состоянии **Slave**, а также в случае штатного или аварийного останова пакетного фильтра фильтрующие интерфейсы МЭ ССПТ-4А1 **заблокированы**, т.е. несущая между интерфейсами МЭ ССПТ-4А1 и портами коммутатора отсутствует. Такой характер работы обеспечивается соответствующим согласованием портов коммутаторов и фильтрующих интерфейсов МЭ ССПТ-4А1:

- на портах коммутаторов, к которым подключены фильтрующие интерфейсы МЭ ССПТ-4А1, должно быть отключено автосогласование скоростей и принудительно установлен режим скорости/дуплекса, соответствующий максимальной пропускной способности, поддерживаемой фильтрующими интерфейсами МЭ ССПТ-4А1, например, **`1000BaseTX/full-duplex`**;
- на фильтрующих интерфейса МЭ ССПТ-4А1 при включении резервирования в режиме **Master/Slave** автоматически устанавливается скорость/дуплекс, соответствующий режиму данного устройства в системе фильтрации: для устройства в режиме **Master** устанавливается скорость/дуплекс **активного** состояния; для устройства в режиме **Slave** устанавливается скорость/дуплекс **заблокированного** состояния (порядок настройки см. ниже).

В приведенном примере показан порядок настройки системы фильтрации с резервированием в схеме “активный-резервный” для режимов **Master/Slave**. Предполагается, что используются МЭ ССПТ-4А1 и коммутаторы, поддерживающие скорости 10/100/1000 Мбит/с.

В схеме **“активный-резервный”** для режимов **Master** и **Slave** могут использоваться исполнения МЭ ССПТ-4А1, у которых все фильтрующие интерфейсы имеют идентичные списки поддерживаемых скоростей передачи. В противном случае в установке режимов **Master** и **Slave** будет отказано, при этом параметры “*Фильтрующие интерфейсы в активном состоянии*” и “*Фильтрующие интерфейсы в заблокированном состоянии*” не будут иметь значений по умолчанию, поскольку в этом случае данные настройки не используются.

Необходимое оборудование и материалы. Для организации схемы резервирования “**активный-резервный”** в режиме **Master/Slave** (рисунок 3.10, стр. 118) необходимо:

- два межсетевых экрана МЭ ССПТ-4А1;
- два управляемых коммутатора 2-го уровня, поддерживающих функцию принудительной установки скорости на портах;
- один коммутатор для организации взаимодействия между двумя МЭ ССПТ-4А1 через управляющие Ethernet-интерфейсы, а также между УК и двумя МЭ ССПТ-4А1;
- семь кабелей типа “витая пара” категории 5е и выше для соединения по схеме согласно рисунок 3.10, стр. 118.

Настройка МЭ ССПТ-4А1 и дополнительного оборудования. Для настройки схемы резервирования “**активный-резервный”** в режиме **Master/Slave** (рисунок 3.10, стр. 118) необходимо проделать следующие шаги:

1) Настройка коммутаторов. На управляемых коммутаторах 1 и 2 для портов 1 и 2 выключить свойство **`autonegotiation`** и установить максимальную скорость, поддерживаемую и портами коммутатора, и фильтрующими интерфейсами МЭ ССПТ-4А1 (в нашем случае - **`1000BaseTX/full-duplex`**). Выключить протокол **Spanning Tree** на портах 1 и 2 коммутаторов

1 и 2. Порядок настройки коммутаторов описан в соответствующих руководствах.

2) Подключение МЭ ССПТ-4А1. Подключить управляющие Ethernet-интерфейсы МЭ ССПТ-4А1 к коммутатору 3 с помощью двух кабелей “витая пара”. Подключить УК к коммутатору 3 с помощью кабеля “витая пара”.

3) Настройка МЭ ССПТ-4А1 №1 в режиме **Master**:

3.1) Получить доступ к командному интерфейсу администратора через системную консоль согласно подразделу Ошибка: источник перекрёстной ссылки не найден.

3.2) Настроить управляющий Ethernet-интерфейс:

```
fnp4> interface control set address=192.168.2.1/255.255.255.0
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (192.168.2.1)
```

3.3) Завершить работу в системной консоли командой `exit`.

3.4) Получить доступ к командному интерфейсу администратора через управляющий Ethernet-интерфейс согласно подразделу Ошибка: источник перекрёстной ссылки не найден.

3.5) Получить списки допустимых скоростей передачи (media) для фильтрующих интерфейсов МЭ ССПТ-4А1, выполнив команду:

```
fnp4> interface filter media list
Поддерживаемая скорость передачи:
eth0 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth1 : autoselect,1000baseT,100baseTX,10baseT/UTP
fnp4>
```

Вывод команды **“interface filter media list”** может отличаться в зависимости от варианта исполнения МЭ ССПТ-4А1 (число и тип фильтрующих интерфейсов).

3.6) Произвести следующие настройки резервирования:

- установить IP-адрес смежного устройства – 192.168.2.2;
- установить режим **Master** (активный режим работы) данного устройства в схеме резервирования;
- установить скорости передачи фильтрующих интерфейсов для **активного** и **заблокированного** состояний.

Указанные настройки резервирования допустимо произвести одной командой:

```
fnp4> reserv set neighbour=192.168.2.2 mode=master media-active=1000baseT media-
blocked=10baseT/UTP
FNPSH-I-007.02.30C6-Режим резервирования изменен
FNPSH-I-007.02.30C9-IP-адрес смежного устройства изменен
FNPSH-I-007.02.30D2-Скорость фильтрующих интерфейсов для функции резервирования изменена
FNPSH-I-007.02.30D2-Скорость фильтрующих интерфейсов для функции резервирования изменена
fnp4>
```

При установке скоростей передачи фильтрующих интерфейсов для **активного** и **заблокированного** состояний необходимо следовать следующим правилам:

- для **активного состояния** интерфейсов устанавливается значение параметра media, соответствующее **максимальной скорости**, поддерживаемой МЭ ССПТ-4А1 и коммутаторами;
- для **заблокированного состояния** устанавливается значение параметра media, соответствующее **минимальной скорости**, поддерживаемой МЭ ССПТ-4А1.

Режим передачи для **активного** и **заблокированного** состояний фильтрующих интерфейсов МЭ ССПТ-4А1 устанавливается автоматически:

- для **активного состояния** предпринимается попытка установить режим передачи **“full-duplex”**, в случае если данный режим передачи не поддерживается интерфейсом: предпринимается попытка установить режим передачи **“half-duplex”**;
- для **заблокированного состояния** предпринимается попытка установить режим передачи **“half-duplex”**, в случае если данный режим передачи не поддерживается интерфейсом: предпринимается попытка установить режим передачи **“full-duplex”**.

4) Настройка МЭ ССПТ-4А1 (№2) в режиме **Slave**:

4.1) Получить доступ к командному интерфейсу администратора через системную консоль согласно подразделу Ошибка: источник перекрёстной ссылки не найден.

4.2) Настроить управляющий Ethernet-интерфейс:

```
fnp4> interface control set address=192.168.2.2/255.255.255.0
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (192.168.2.2)
```

4.3) Завершить работу в системной консоли командой `exit`.

4.4) Получить доступ к командному интерфейсу администратора через управляющий Ethernet-интерфейс согласно подразделу Ошибка: источник перекрёстной ссылки не найден.

4.5) Получить списки допустимых скоростей передачи (media) для фильтрующих интерфейсов МЭ ССПТ-4А1, выполнив команду:

```
fnp4> interface filter media list
Поддерживаемая скорость передачи:
eth0 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth1 : autoselect,1000baseT,100baseTX,10baseT/UTP
fnp4>
```

Вывод команды **“interface filter media list”** может отличаться в зависимости от варианта исполнения МЭ ССПТ-4А1 (число и тип фильтрующих интерфейсов).

4.6) Произвести следующие настройки резервирования:

- установить IP-адрес смежного устройства – 192.168.2.1;
- установить режим **Slave** (резервный режим работы) данного устройства в схеме резервирования;
- установить параметры фильтрующих интерфейсов для активного и заблокированного состояний.

При установке скоростей передачи фильтрующих интерфейсов для **активного** и **заблокированного** состояний необходимо следовать следующим правилам:

- для **активного состояния** интерфейсов устанавливается значение параметра media, соответствующее **максимальной скорости**, поддерживаемой МЭ ССПТ-4А1 и коммутаторами;
- для **заблокированного состояния** устанавливается значение параметра media, соответствующее **минимальной скорости**, поддерживаемой МЭ ССПТ-4А1.

Режим передачи для **активного** и **заблокированного** состояний фильтрующих интерфейсов МЭ ССПТ-4А1 устанавливается автоматически:

- для **активного состояния** предпринимается попытка установить режим передачи **“full-duplex”**, в случае если данный режим передачи не поддерживается интерфейсом: предпринимается попытка установить режим передачи **“half-duplex”**;
- для **заблокированного состояния** предпринимается попытка установить режим передачи **“half-duplex”**, в случае если данный режим передачи не поддерживается интерфейсом: предпринимается попытка установить режим передачи **“full-duplex”**.

Значения скоростей передачи (media) для **активного** и **заблокированного** состояний фильтрующих интерфейсов должны быть идентичны на обоих МЭ ССПТ-4А1 схемы резервирования **“активный-резервный”** для режимов **Master** и **Slave**.

Указанные настройки резервирования допустимо произвести одной командой:

```
fnp4> reserv set neighbour=192.168.2.1 mode=slave media-active=1000baseT media-
blocked=10baseT/UTP
FNPSH-I-007.02.30C6-Режим резервирования изменен
FNPSH-I-007.02.30C9-IP-адрес смежного устройства изменен
FNPSH-I-007.02.30D2-Скорость фильтрующих интерфейсов для функции резервирования изменена
FNPSH-I-007.02.30D2-Скорость фильтрующих интерфейсов для функции резервирования изменена
fnp4>
```

После выполнения указанных схема резервирования “активный-резервный” в режиме **Master/Slave** готова к включению.

Включение и останов схемы резервирования “активный-резервный” в режиме Master/Slave. Включение системы фильтрации с резервированием осуществляется следующим образом.

1) Включить резервирование на МЭ ССПТ-4А1 №1:

```
fnp4> reserv enable
FNPSH-I-007.02.30C7-Резервирование включено
fnp4>
```

2) Проконтролировать включение резервирования на МЭ ССПТ-4А1 №1:

```
fnp4> reserv show
Состояние резервирования:                          включено
Режим устройства:                                  MASTER (активный)
Состояние устройства:                              MASTER (активный)
Смежное устройство:
    IP-адрес:                                      192.168.2.2
    Состояние:                                     Аппаратный отказ (недоступно)
Автоматическая синхронизация текущей политики:     включено (Временно заблокировано)
Фильтрующие интерфейсы в активном состоянии:       1000baseT
Фильтрующие интерфейсы в заблокированном состоянии: 10baseT/UTP
fnp4>
```

После включения резервирования на **МЭ ССПТ-4А1** в режиме **Master** для фильтрующих интерфейсов автоматически устанавливается скорость передачи, заданная параметром **“Фильтрующие интерфейсы в активном состоянии”**.

При включении резервирования, если **автоматическая синхронизация текущей политики** включена в конфигурации устройства (по умолчанию – включена), то данная функция **временно блокируется**. Условия включения и выключения временной блокировки автоматической синхронизации описаны в разделе 3.5.5, стр. 135.

Состояние смежного устройства (МЭ ССПТ-4А1 №2) выводится как **“Аппаратный отказ (недоступно)”**, потому что резервирование на нем еще не включено.

3) Включить резервирование на МЭ ССПТ-4А1 №2:

```
fnp4> reserv enable
FNPSH-I-007.02.30C7-Резервирование включено
fnp4>
```

4) Проконтролировать включение функции резервирования на МЭ ССПТ-4А1 №2:

```
fnp4> reserv show
Состояние резервирования:                          включено
Режим устройства:                                  SLAVE (резервный)
Состояние устройства:                              SLAVE (резервный)
Смежное устройство:
    IP-адрес:                                      192.168.2.1
    Состояние:                                     master (активный)
Автоматическая синхронизация текущей политики:     включено (Временно заблокировано)
Фильтрующие интерфейсы в активном состоянии:       1000baseT
Фильтрующие интерфейсы в заблокированном состоянии: 10baseT/UTP
fnp4>
```

После включения резервирования на **МЭ ССПТ-4А1** в режиме **Slave** для фильтрующих интерфейсов автоматически устанавливается скорость передачи, заданная параметром **“Фильтрующие интерфейсы в заблокированном состоянии”**.

Если **автоматическая синхронизация текущей политики** включена в конфигурации устройства (по умолчанию – включена), то при включении резервирования данная функция **временно блокируется**. Условия включения и выключения временной блокировки автоматической синхронизации описаны в разделе 3.5.5, стр. 135.

5) Подключить МЭ ССПТ-4А1 №1 и МЭ ССПТ-4А1 №2 к коммутаторам 1 и 2 (рисунок 3.10, стр. 118):

✔ интерфейс eth0 МЭ ССПТ-4А1 №1 к порту 1 коммутатора 1;

✔ интерфейс eth1 МЭ ССПТ-4А1 №1 к порту 1 коммутатора 2;

✔ интерфейс eth0 МЭ ССПТ-4А1 №2 к порту 2 коммутатора 1;

✔ интерфейс eth1 МЭ ССПТ-4А1 №2 к порту 2 коммутатора 2.

6) Проконтролировать наличие несущей по светодиодам “Link” на интерфейсах eth0 и eth1 МЭ ССПТ-4А1 №1, работающего в режиме **Master**, и отсутствие несущей по светодиодам “Link” на интерфейсах eth0 и eth1 МЭ ССПТ-4А1 №2, работающего в режиме **Slave**.

После проделанных шагов схема резервирования “активный-резервный” в режиме **Master**/**Slave** готова к работе.

Для корректного останова схемы резервирования “активный-резервный” в режиме **Master**/**Slave** необходимо проделать следующие шаги:

1) Выключить МЭ ССПТ-4А1 №2 (**Slave**) следующим образом:

1.1) отсоединить интерфейсы eth0 и eth1 устройства МЭ ССПТ-4А1 №2 (**Slave**) от портов коммутатора 1 и 2:

1.2) выключить резервирование на МЭ ССПТ-4А1 №2 (**Slave**):

```
fnp4> reserv disable
Выключить резервирование? (Y/N) [N]: y
FNPSH-I-007.02.30C8-Резервирование выключено
fnp4>
```

После выключения резервирования на МЭ ССПТ-4А1 №2 фильтрующие интерфейсы автоматически переводятся в состояние, в котором они находились до включения резервирования.

2) Выключить резервирование на МЭ ССПТ-4А1 №1 (**Master**) :

```
fnp4> reserv disable
Выключить резервирование? (Y/N) [N]: y
FNPSH-I-007.02.30C8-Резервирование выключено
fnp4>
```

После выключения резервирования на МЭ ССПТ-4А1 №1 фильтрующие интерфейсы автоматически переводятся в состояние, в котором они находились до включения резервирования. После проделанных шагов МЭ ССПТ-4А1 №1 останется в схеме и продолжит работу, как межсетевой экран без резервирования.

3.5.3. Резервирование “активный-активный” в режиме Sync/Sync

Схема резервирования **“активный-активный”** в режиме **Sync/Sync** основана на схеме соединения двух коммутаторов двумя физическими каналами, при этом функция обнаружения резервной связи и ее блокировка возлагается на реализованный в ПО коммутаторов протокол семейства **Spanning Tree (STP)**, предназначенный для выявления и устранения петель в физической структуре коммутируемой сети. Коммутаторы, поддерживающие протокол **Spanning Tree**, обмениваясь служебными сообщениями, блокируют избыточные связи в топологии сети, тем самым гарантируя наличие единственного пути из одной точки сети в другую.

В этой системе два МЭ ССПТ-4А1 подключаются в разрыв физических каналов между коммутаторами и работают как одна логическая система фильтрации (рисунок 3.11, стр. 125). При этом на обоих МЭ ССПТ-4А1 настроен режим резервирования **Sync**, оба устройства являются активными, но фильтрацию трафика производит только одно устройство, так как одновременно задействован только один физический канал. Переключение каналов осуществляется коммутаторами в случае обнаружения разрыва в активном канале связи. Синхронизация и обмен сообщениями между МЭ ССПТ-4А1 с целью выявления программных отказов и переключения режимов работы, происходит через управляющие Ethernet-интерфейсы

(EthC). В случае, если в такой схеме откажет (по причине программного или аппаратного сбоя) одно из устройств МЭ ССПТ-4А1, коммутаторы обнаружат отказ по отсутствию служебных сообщений **Spanning Tree** и включат в работу резервную связь. Таким образом, система фильтрации остается работоспособной.

Особенности схемы “активный-активный“ в режиме **Sync/Sync**:

- возможна автоматическая или ручная синхронизация политики доступа между двумя МЭ ССПТ-4А1 (см. раздел 3.5.5)
- в случае переключения схемы на резервную связь происходит обрыв установленных сеансов, работавших через схему фильтрации. После такого переключения пользователи должны восстановить свои сеансы связи;
- требуется настройка коммутаторов, к которым подключены МЭ ССПТ-4А1:
  - ✔ включение протоколов STP (RSTP) на портах коммутаторов, подключенных к фильтрующим интерфейсам МЭ ССПТ-4А1.

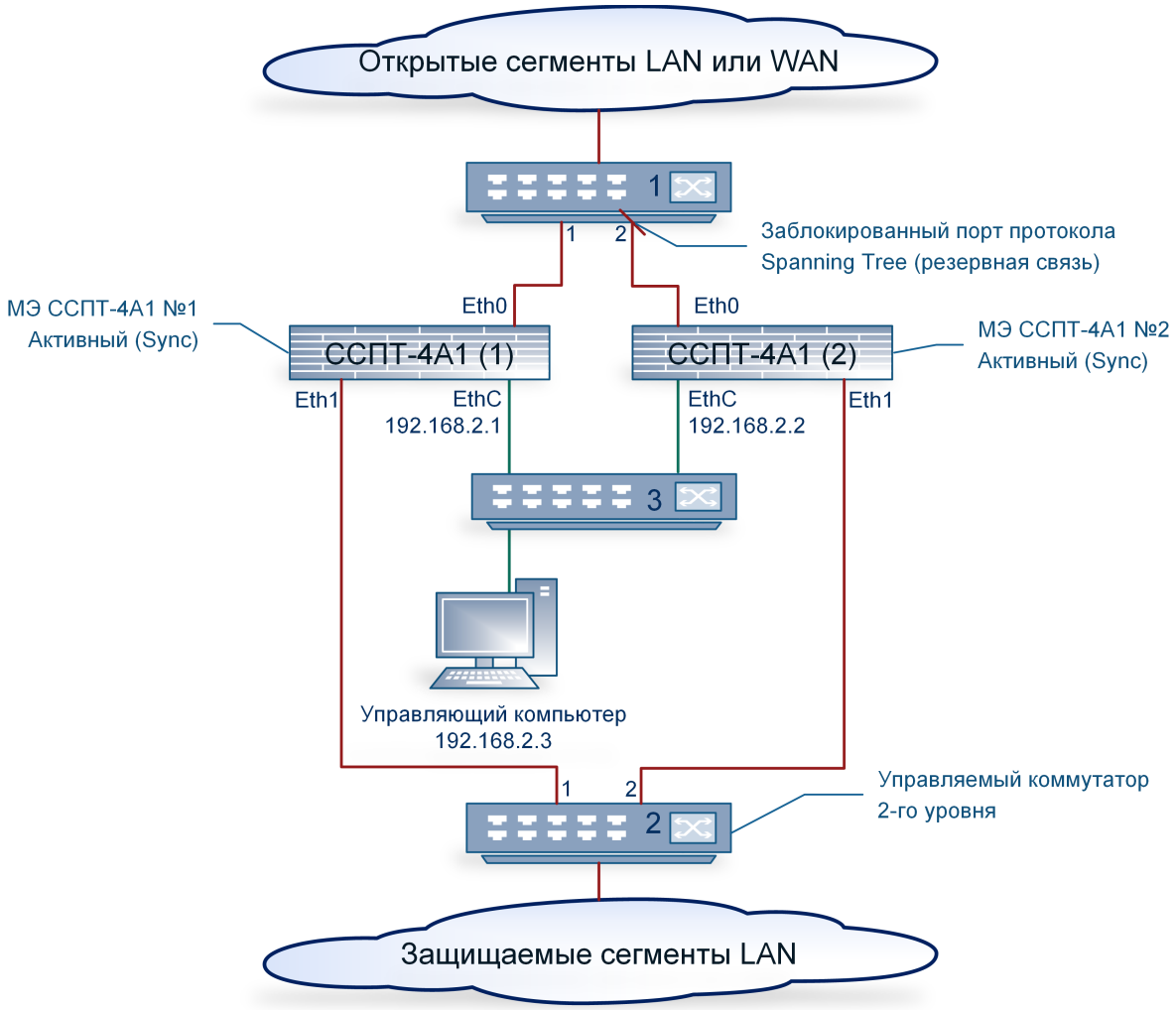


Рисунок 3.11: Схема резервирования “активный-активный”, режим Sync/Sync

Необходимое оборудование и материалы. Для организации резервирования “**активный-активный**” в режиме **Sync/Sync** (рисунок 3.11) необходимо:

- два МЭ ССПТ-4А1;

- два управляемых коммутатора 2-го уровня, поддерживающих стандарт IEEE 802.1d (Spanning Tree) или IEEE 802.1w (Rapid Spanning Tree);
- один коммутатор для организации взаимодействия между двумя МЭ ССПТ-4А1 через управляющие Ethernet-интерфейсы, а также между УК и двумя МЭ ССПТ-4А1;
- семь кабелей типа “витая пара” категории 5е и выше для соединения по схеме согласно рисунку 3.11.

Настройка МЭ ССПТ-4А1 и дополнительного оборудования. Для настройки схемы резервирования “активный-активный” в режиме **Sync/Sync** необходимо проделать следующие шаги:

1) Настройка коммутаторов. На управляемых коммутаторах 1 и 2 для портов 1 и 2 включить использование протокола Spanning Tree или Rapid Spanning Tree. Порядок настройки коммутаторов описан в соответствующих руководствах.
2) Подключение МЭ ССПТ-4А1. Подключить управляющие Ethernet-интерфейсы МЭ ССПТ-4А1 к коммутатору 3 с помощью двух кабелей “витая пара”. Подключить УК к коммутатору 3 с помощью кабеля “витая пара”.
3) Настройка МЭ ССПТ-4А1 №1 в режиме **Sync**:
   3.1) Получить доступ к командному интерфейсу администратора через системную консоль согласно подразделу Ошибка: источник перекрёстной ссылки не найден.
   3.2) Настроить управляющий Ethernet-интерфейс:

```
fnp4> interface control set address=192.168.2.1/255.255.255.0
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (192.168.2.1)
```

   3.3) Завершить работу в системной консоли командой `exit`.
   3.4) Получить доступ к командному интерфейсу администратора через управляющий Ethernet-интерфейс согласно подразделу Ошибка: источник перекрёстной ссылки не найден.
   3.5) Произвести следующие настройки резервирования:

- установить IP-адрес смежного устройства – 192.168.2.2;
- установить режим **Sync** (активный режим работы) данного устройства в схеме резервирования.

Указанные настройки резервирования допустимо произвести одной командой:

```
fnp4> reserv set neighbour=192.168.2.2 mode=sync
FNPSH-I-007.02.30C6-Режим резервирования изменен
FNPSH-I-007.02.30C9-IP-адрес смежного устройства изменен
fnp4>
```

4) Настройка МЭ ССПТ-4А1 №2 в режиме **Sync**:

4.1) Получить доступ к командному интерфейсу администратора через системную консоль согласно подразделу Ошибка: источник перекрёстной ссылки не найден.

4.2) Настроить управляющий Ethernet-интерфейс:

```
fnp4> interface control set address=192.168.2.2/255.255.255.0
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (192.168.2.2)
```

4.3) Завершить работу в системной консоли командой `exit`.

4.4) Получить доступ к командному интерфейсу администратора через управляющий Ethernet-интерфейс согласно подразделу Ошибка: источник перекрёстной ссылки не найден.

4.5) Произвести следующие настройки резервирования:

- установить IP-адрес смежного устройства;
- установить режим **Sync** (активный режим работы) данного устройства в схеме резервирования.

Указанные настройки резервирования допустимо произвести одной командой:

```
fnp4> reserv set neighbour=192.168.2.1 mode=sync
FNPSH-I-007.02.30C6-Режим резервирования изменен
FNPSH-I-007.02.30C9-IP-адрес смежного устройства изменен
fnp4>
```

После выполнения указанных настроек схема резервирования “активный-активный” в режиме **Sync/Sync** готова к включению.

Включение и останов схемы резервирования “активный-активный” в режиме Sync/Sync. Включение схемы резервирования “активный-активный” в режиме **Sync/Sync** осуществляется следующим образом.

1) Включить резервирование на МЭ ССПТ-4А1 №1:

```
fnp4> reserv enable
FNPSH-I-007.02.30C7-Резервирование включено
fnp4>
```

2) Проконтролировать включение функции резервирования на МЭ ССПТ-4А1 №1:

```
fnp4> reserv show
Состояние резервирования:                          включено
Режим устройства:                                  SYNC (синхронизация)
Состояние устройства:                              SYNC (синхронизация)
Смежное устройство:
    IP-адрес:                                      192.168.2.2
    Состояние:                                     Аппаратный отказ (недоступно)
Автоматическая синхронизация текущей политики:     включено (Временно заблокировано)
Фильтрующие интерфейсы в активном состоянии:       1000baseT
Фильтрующие интерфейсы в заблокированном состоянии: 10baseT/UTP
fnp4>
```

Если **автоматическая синхронизация текущей политики** включена в конфигурации устройства (по умолчанию – включена), то при включении резервирования данная функция **временно блокируется**. Условия включения и выключения временной блокировки автоматической синхронизации описаны в разделе 3.5.5, стр. 135.

3) Включить резервирование на на МЭ ССПТ-4А1 №2:

```
fnp4> reserv enable
FNPSH-I-007.02.30C7-Резервирование включено
fnp4>
```

4) Проконтролировать включение функции резервирования на МЭ ССПТ-4А1 №2:

```
fnp4> reserv show
Состояние резервирования:                          включено
Режим устройства:                                  SYNC (синхронизация)
Состояние устройства:                              SYNC (синхронизация)
Смежное устройство:
    IP-адрес:                                      192.168.2.1
    Состояние:                                     sync (синхронизация)
Автоматическая синхронизация текущей политики:     включено (Временно заблокировано)
Фильтрующие интерфейсы в активном состоянии:       1000baseT
Фильтрующие интерфейсы в заблокированном состоянии: 10baseT/UTP
fnp4>
```

5) Подключить МЭ ССПТ-4А1 №1 и на МЭ ССПТ-4А1 №2 к коммутаторам 1 и 2 (рисунок 3.11, стр. 125):

✔ интерфейс eth0 МЭ ССПТ-4А1 №1 к порту 1 коммутатора 1;

✔ интерфейс eth1 МЭ ССПТ-4А1 №1 к порту 1 коммутатора 2;

✔ интерфейс eth0 МЭ ССПТ-4А1 №2 к порту 2 коммутатора 1;

✔ интерфейс eth1 МЭ ССПТ-4А1 №2 к порту 2 коммутатора 2.

6) Проконтролировать наличие несущей по светодиодам “Link” на подключенных интерфейсах устройств.

После проделанных шагов схема резервирования “активный-активный” в режиме **Sync/Sync** готова к работе.

Для корректного останова схема резервирования “активный-активный” в режиме **Sync/Sync** необходимо проделать следующие шаги:

1) Выключить МЭ ССПТ-4А1 №2 следующим образом:

1.1) отсоединить интерфейсы eth0 и eth1 устройства МЭ ССПТ-4А1 №2 от портов коммутатора 1 и 2;

1.2) выключить резервирование на МЭ ССПТ-4А1 №2:

```
fnp4> reserv disable
Выключить резервирование? (Y/N) [N]: y
FNPSH-I-007.02.30C8-Резервирование выключено
fnp4>
```

2) Выключить резервирование на МЭ ССПТ-4А1 №2 следующим образом:

```
fnp4> reserv disable
Выключить резервирование? (Y/N) [N]: y
FNPSH-I-007.02.30C8-Резервирование выключено
fnp4>
```

После проделанных шагов МЭ ССПТ-4А1 №1 останется в схеме и продолжит работу, как межсетевой экран без резервирования.

3.5.4. Резервирование “активный-активный” в режиме Balance/Balance

Схема резервирования “**активный-активный**” в режиме **Balance/Balance** основана на объединении двух физических каналов между коммутаторами в один логический канал, называемый транком (например, стандарт IEEE 802.3ad Link Aggregation). В такой системе два МЭ ССПТ-4А1 подключаются в разрыв физических каналов между коммутаторами и работают как одна логическая система фильтрации (рисунок 3.12, стр. 130). При этом на обоих устройствах настроен режим резервирования **Balance**, оба устройства является активными и производят фильтрацию трафика. Распределение нагрузки на физические каналы осуществляют коммутаторы, настроенные соответствующим образом. Синхронизация и обмен сообщениями между МЭ ССПТ-4А1 с целью выявления аппаратных и программных отказов и переключения режимов работы происходит через управляющие Ethernet-интерфейсы (EthC). В случае, если в такой схеме откажет (по причине программного или аппаратного сбоя) одно из устройств МЭ ССПТ-4А1, коммутаторы перераспределят трафик на доступные физические каналы и, таким образом, система фильтрации останется работоспособной.

Особенности схемы **“активный-активный”** в режиме **Balance/Balance**:

- возможна автоматическая или ручная синхронизация политики доступа между двумя МЭ ССПТ-4А1 (см. раздел 3.5.5)
- пакетный фильтр может работать в следующих режимах:
  - ✔ в режиме управления сессиями при отключенной функции глубокого контроля TCP;
  - ✔ в режиме пакетной фильтрации (режим управления сессиями отключен);
- могут использоваться только исполнения МЭ ССПТ-4А1, у которых все фильтрующие интерфейсы имеют идентичные типы (например, исполнение 01 – 5 фильтрующих интерфейсов Ethernet 1 Гбит/с);
- требуется настройка коммутаторов, к которым подключены МЭ ССПТ-4А1:
  - ✔ установка параметров скорости/дуплекса портов коммутаторов, подключенных к фильтрующим интерфейсам МЭ ССПТ-4А1;
  - ✔ включение функции агрегирования портов коммутаторов, подключенных к фильтрующим интерфейсам МЭ ССПТ-4А1.

Доступность МЭ ССПТ-4А1 для передачи трафика в режиме **Balance/Balance** обеспечивается специальным режимом работы фильтрующих интерфейсов. При штатном функционировании в этом режиме фильтрующие интерфейсы обоих МЭ ССПТ-4А1 активны, т. е. несущая между интерфейсами МЭ ССПТ-4А1 и портами коммутаторов поднята. В случае штатного или аварийного останова пакетного фильтра (подсистемы МЭ ССПТ-4А1, отвечающей за передачу пакетов между интерфейсам) фильтрующие интерфейсы МЭ ССПТ-4А1, на котором это произошло, блокируются, т.е. несущая между интерфейсами данного МЭ ССПТ-4А1 и портами коммутатора отсутствует. Такой характер работы обеспечивается

соответствующими настройками портов коммутаторов и фильтрующих интерфейсов МЭ ССПТ-4А1:

- на портах коммутаторов, к которым подключены фильтрующие интерфейсы МЭ ССПТ-4А1, должно быть отключено автосогласование скоростей и принудительно установлен режим скорости/дуплекса, соответствующий максимальной пропускной способности, поддерживаемой фильтрующими интерфейсами МЭ ССПТ-4А1, например, **`1000BaseTX/full-duplex`**;
- на фильтрующих интерфейса МЭ ССПТ-4А1 при включении резервирования в режиме **Balance/Balance** автоматически устанавливается скорость/дуплекс, соответствующий режиму данного устройства в системе фильтрации: для устройства в режиме **Balance** устанавливается скорость/дуплекс **активного** состояния; в случае обнаруженного программного отказа устанавливается скорость/дуплекс **заблокированного** состояния (порядок настройки см. ниже).

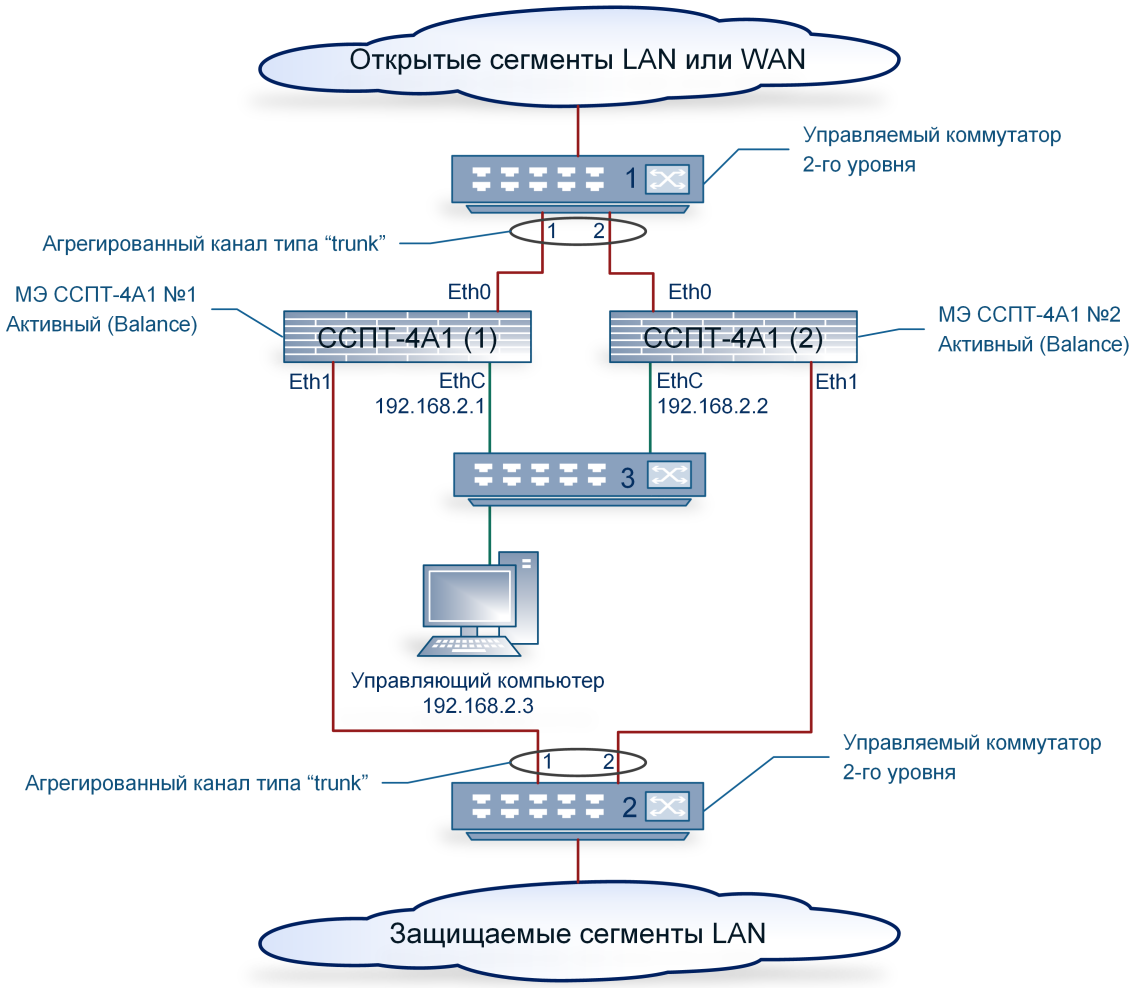


Рисунок 3.12: Схема резервирования “активный-активный”, режим Balance/Balance

В приведенном ниже примере показан порядок настройки системы фильтрации с резервированием в режиме **Balance/Balance**.

Предполагается, что используются МЭ ССПТ-4А1 и коммутаторы, поддерживающие скорости 10/100/1000 Мбит/с.

В схеме **“Балансировка нагрузки”** могут использоваться только МЭ ССПТ-4А1, у которых все фильтрующие интерфейсы имеют идентичные списки поддерживаемых скоростей передачи. В противном случае в установке режимов **Master** и **Slave** будет отказано, при этом параметры “*Фильтрующие интерфейсы в активном состоянии*” и “*Фильтрующие интерфейсы в заблокированном состоянии*” не будут иметь значений по умолчанию, поскольку в этом случае данные настройки не используются.

Необходимое оборудование и материалы. Для организации резервирования “**активный-активный**” в режиме **Balance/Balance** (рисунок 3.12, стр. 130), необходимо:

- два МЭ ССПТ-4А1;
- два управляемых коммутатора 2-го уровня, поддерживающих стандарт IEEE 802.3ad;
- один коммутатор для организации взаимодействия между двумя МЭ ССПТ-4А1 через управляющие Ethernet-интерфейсы, а также между УК и двумя МЭ ССПТ-4А1;
- семь кабелей типа “витая пара” категории 5е и выше для соединения по схеме согласно рисунку 3.12.

Настройка МЭ ССПТ-4А1 и дополнительного оборудования. Для настройки через интерфейс командной строки необходимо проделать следующие шаги:

1) Настройка коммутаторов. На управляемых коммутаторах 1 и 2 для портов 1 и 2 выключить свойство autonegotiation и установить скорости, соответствующие максимальным скоростям фильтрующих интерфейсов МЭ ССПТ-4А1 eth0 и eth1 (в нашем случае - 1000BaseTX/full-duplex). Настроить агрегирование каналов (транк) для портов 1 и 2 коммутаторов 1 и 2. Порядок настройки коммутаторов описан в соответствующих руководствах.
2) Подключение МЭ ССПТ-4А1. Подключить управляющие Ethernet-интерфейсы МЭ ССПТ-4А1 к коммутатору 3 с помощью двух кабелей “витая пара”. Подключить УК к коммутатору 3 с помощью кабеля “витая пара”.
3) Настройка через интерфейс командной строки МЭ ССПТ-4А1 №1:

   3.1) Настроить управляющий Ethernet-интерфейс:

```
fnp4> interface control set address=192.168.2.1/255.255.255.0
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (192.168.2.1)
FNPSH-I-007.02.3003-Завершение работы администратора (admin)
```

   3.2) Получить списки допустимых скоростей передачи (media) для фильтрующих интерфейсов МЭ ССПТ-4А1, выполнив команду:

```
fnp4> interface filter media list
Поддерживаемая скорость передачи:
eth0 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth1 : autoselect,1000baseT,100baseTX,10baseT/UTP
fnp4>
```

Вывод команды **“interface filter media list”** может отличаться в зависимости от варианта исполнения МЭ ССПТ-4А1 (число фильтрующих интерфейсов и их модели).

3.3) Произвести следующие настройки резервирования:

3.3.1) Установить IP-адрес смежного устройства;

3.3.2) Установить режим “Balance” (балансировка нагрузки) данного устройства в схеме резервирования;

3.3.3) Установить скорости передачи фильтрующих интерфейсов для активного и заблокированного состояний.

При установке скоростей передачи фильтрующих интерфейсов для **активного** и **заблокированного** состояний необходимо следовать следующим правилам:

- для **активного состояния** интерфейсов устанавливается значение параметра media, соответствующее **максимальной скорости**, поддерживаемой МЭ ССПТ-4А1 и коммутаторами;
- для **заблокированного состояния** устанавливается значение параметра media, соответствующее **минимальной скорости**, поддерживаемой МЭ ССПТ-4А1.

Настройки для **активного состояния** интерфейсов будут использоваться при штатном функционировании системы фильтрации в режиме **Balance/Balance**.

Настройки для **заблокированного состояния** интерфейсов будут использоваться в случае штатного (по команде администратора) или аварийного останова пакетного фильтра, отвечающего за передачу пакетов между интерфейсам.

Режим передачи для **активного** и **заблокированного** состояний фильтрующих интерфейсов МЭ ССПТ-4А1 устанавливается автоматически:

- для **активного состояния** предпринимается попытка установить режим передачи **“full-duplex”**, в случае если данный режим передачи не поддерживается интерфейсом: предпринимается попытка установить режим передачи **“half-duplex”**;
- для **заблокированного состояния** предпринимается попытка установить режим передачи **“half-duplex”**, в случае если данный режим передачи не поддерживается интерфейсом: предпринимается попытка установить режим передачи **“full-duplex”**.

Описанные выше настройки резервирования можно произвести выполнением одной команды. В нашем случае необходимо выполнить команду:

```
fnp4> reserv set neighbour=192.168.2.2 mode=balance media-active=1000baseT media-
blocked=10baseT/UTP
FNPSH-I-007.02.30C6-Режим резервирования изменен
FNPSH-I-007.02.30C9-IP-адрес смежного устройства изменен
FNPSH-I-007.02.30D2-Скорость фильтрующих интерфейсов в режиме резервирования изменена
FNPSH-I-007.02.30D2-Скорость фильтрующих интерфейсов в режиме резервирования изменена
fnp4>
```

4) Настройка через интерфейс командной строки МЭ ССПТ-4А1 №2:

4.1) Настроить управляющий Ethernet-интерфейс:

```
fnp4> interface control set address=192.168.2.2/255.255.255.0
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (192.168.2.2)
FNPSH-I-007.02.3003-Завершение работы администратора (admin)
```

4.2) Получить списки допустимых скоростей передачи (media) для фильтрующих интерфейсов МЭ ССПТ-4А1, выполнив команду:

```
fnp4> interface filter media list
Поддерживаемая скорость передачи:
```

```
eth0 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth1 : autoselect,1000baseT,100baseTX,10baseT/UTP
fnp4>
```

Вывод команды **“interface filter media list”** может отличаться в зависимости от варианта поставки МЭ ССПТ-4А1 (число фильтрующих интерфейсов и их модели).

4.3) Произвести следующие настройки резервирования:

4.3.1) Установить IP-адрес смежного устройства;

4.4) Установить режим работы “Balance” (балансировка нагрузки) данного устройства в схеме резервирования;

4.5) Установить параметры фильтрующих интерфейсов для активного и заблокированного состояния.

При установке скоростей передачи фильтрующих интерфейсов для **активного** и **заблокированного** состояний необходимо следовать следующим правилам:

- для **активного состояния** интерфейсов устанавливается значение параметра media, соответствующее **максимальной скорости**, поддерживаемой МЭ ССПТ-4А1 и коммутаторами;
- для **заблокированного состояния** устанавливается значение параметра media, соответствующие **минимальной скорости**, поддерживаемой МЭ ССПТ-4А1.

Настройки для **активного состояния** интерфейсов будут использоваться при штатном функционировании системы фильтрации в режиме **Balance/Balance**.

Настройки для **заблокированного состояния** интерфейсов будут использоваться в случае штатного (по команде администратора) или аварийного останова пакетного фильтра, отвечающего за передачу пакетов между интерфейсам.

Режим передачи для **активного** и **заблокированного** состояний фильтрующих интерфейсов МЭ ССПТ-4А1 устанавливается автоматически:

- для **активного состояния** предпринимается попытка установить режим передачи **“full-duplex”**, в случае если данный режим передачи не поддерживается интерфейсом: предпринимается попытка установить режим передачи **“half-duplex”**;
- для **заблокированного состояния** предпринимается попытка установить режим передачи **“half-duplex”**, в случае если данный режим передачи не поддерживается интерфейсом: предпринимается попытка установить режим передачи **“full-duplex”**.

Описанные выше настройки резервирования можно произвести выполнением одной команды. В нашем случае необходимо выполнить команду:

```
fnp4> reserv set neighbour=192.168.2.1 mode=balance media-active=1000baseT media-
blocked=10baseT/UTP
FNPSH-I-007.02.30C6-Режим резервирования изменен
FNPSH-I-007.02.30C9-IP-адрес смежного устройства изменен
FNPSH-I-007.02.30D2-Скорость фильтрующих интерфейсов в режиме резервирования изменена
FNPSH-I-007.02.30D2-Скорость фильтрующих интерфейсов в режиме резервирования изменена
fnp4>
```

Включение и останов системы фильтрации с резервированием в режиме Balance/Balance. Включение системы фильтрации через интерфейс командной строки осуществляется следующим образом:

1) Включить резервирование на МЭ ССПТ-4А1 №1:

```
fnp4> reserv enable
FNPSH-I-007.02.30C7-Резервирование включено
```

```
fnp4>
```

2) Проконтролировать включение резервирования на МЭ ССПТ-4А1 №1:

```
fnp4> reserv show
Состояние резервирования:                              включено
Режим устройства:                                      BALANCE (балансировка)
Состояние устройства:                                  BALANCE (балансировка)
Смежное устройство:
    IP-адрес:                                          192.168.2.2
    Состояние:                                         Аппаратный отказ (недоступно)
Автоматическая синхронизация текущей политики:         включено (Временно заблокировано)
Фильтрующие интерфейсы в активном состоянии:           1000baseT
Фильтрующие интерфейсы в заблокированном состоянии: 10baseT/UTP
fnp4>
```

После включения резервирования на МЭ ССПТ-4А1 в режиме **“Balance”** фильтрующие интерфейсы автоматически переводятся в состояние, заданное параметром **“Фильтрующие интерфейсы в активном состоянии”**.

При включении резервирования, если **автоматическая синхронизация текущей политики** включена в конфигурации устройства (по умолчанию – включена), то данная функция **временно блокируется**. Условия включения и выключения временной блокировки автоматической синхронизации описаны в разделе 3.5.5, стр. 135.

3) Включить резервирование на МЭ ССПТ-4А1 №2:

```
fnp4> reserv enable
FNPSH-I-007.02.30C7-Резервирование включено
fnp4>
```

4) Проконтролировать включение резервирования на МЭ ССПТ-4А1 №2:

```
fnp4> reserv show
Состояние резервирования:                              включено
Режим устройства:                                      BALANCE (балансировка)
Состояние устройства:                                  BALANCE (балансировка)
Смежное устройство:
    IP-адрес:                                          192.168.2.1
    Состояние:                                         balance (балансировка)
Автоматическая синхронизация текущей политики:         включено (Временно заблокировано)
Фильтрующие интерфейсы в активном состоянии:           1000baseT
Фильтрующие интерфейсы в заблокированном состоянии: 10baseT/UTP
fnp4>
```

После включения резервирования на МЭ ССПТ-4А1 №2 фильтрующие интерфейсы автоматически переводятся в состояние, заданное параметром “Фильтрующие интерфейсы в активном состоянии”.

5) Подключить МЭ ССПТ-4А1 №1 и МЭ ССПТ-4А1 №2 к коммутаторам 1 и 2 как показано на рисунке 6.12:

- ✔ интерфейс eth0 МЭ ССПТ-4А1 №1 к порту 1 коммутатора 1;
- ✔ интерфейс eth1 МЭ ССПТ-4А1 №1 к порту 1 коммутатора 2;
- ✔ интерфейс eth0 МЭ ССПТ-4А1 №2 к порту 2 коммутатора 1;
- ✔ интерфейс eth1 МЭ ССПТ-4А1 №2 к порту 2 коммутатора 2;

6) Проконтролировать наличие несущей по светодиодам “Link” на интерфейсах eth0 и eth1 устройства МЭ ССПТ-4А1 и на интерфейсах eth0 и eth1 устройства МЭ ССПТ-4А1 №2.

После проделанных шагов система фильтрации с резервированием в режиме **Balance/Balance** приступает к работе.

Для корректного останова через интерфейс командной строки системы фильтрации с резервированием в режиме **Balance/Balance** необходимо проделать следующие шаги:

1) Выключить МЭ ССПТ-4А1 №2 следующим образом:

1.1) отсоединить интерфейсы eth0 и eth1 устройства МЭ ССПТ-4А1 №2 от портов коммутатора 1 и 2.

1.2) выключить резервирование на МЭ ССПТ-4А1 №2:

```
fnp4> reserv disable
Выключить резервирование? (Y/N) [N]: y
FNPSH-I-007.02.30C8-Резервирование выключено
fnp4>
```

После выключения резервирования на МЭ ССПТ-4А1 №2 фильтрующие интерфейсы автоматически переводятся в состояние, в котором они находились до включения резервирования.

2) Выключить резервирование МЭ ССПТ-4А1 №2 следующим образом:

```
fnp4> reserv disable
Выключить резервирование? (Y/N) [N]: y
FNPSH-I-007.02.30C8-Резервирование выключено
fnp4>
```

После выключения резервирования на МЭ ССПТ-4А1 №2 фильтрующие интерфейсы автоматически переводятся в состояние, в котором они находились до включения резервирования.

После проделанных шагов МЭ ССПТ-4А1 №1 останется в схеме и продолжит работу, как межсетевой экран без резервирования.

3.5.5. Синхронизация текущей политики доступа

Автоматическая синхронизация текущей политики. Функция автоматической синхронизации текущей политики между устройствами в схеме резервирования призвана обеспечивать идентичность текущих политик доступа на паре устройств за счет автоматической синхронизации (передачи смежному устройству в схеме) текущей политики доступа при любом действии администратора, приводящем к ее изменению (добавление правила, удаление объекта справочника и т. д.).

По умолчанию данная функция включена в конфигурации МЭ ССПТ-4А1. Если данная функция была выключена администратором, то для ее включения необходимо выполнить команду:

```
fnp4> reserv set sync=enable
FNPSH-I-007.02.30CE-Синхронизация политики включена
fnp4>
```

В процессе работы системы фильтрации с резервированием **функция автоматической синхронизации текущей политики доступа может временно блокироваться** в следующих случаях:

- отказ (аппаратный или программный) смежного устройства;
- текущие политики пары устройств схемы резервирования отличаются по результатам процедуры проверки идентичности текущих политик устройств схемы резервирования;
- временная блокировка функции автоматической синхронизации текущей политики изначально включена при включении резервирования на устройстве.

После того как резервирование будет включено на втором устройстве схемы резервирования первым устройством будет инициирована **процедура проверки идентичности текущих политик устройств схемы резервирования** (здесь подразумевается, что первое устройство схемы — то, на котором резервирование было включено раньше, второе — позже). Если в результате этой процедуры окажется, что текущие политики на устройствах **идентичны**, то **временная блокировка функции автоматической синхронизации текущей политики** будет **выключена** на обоих устройствах схемы резервирования.

Если текущие политики устройств схемы отличаются, то функция автоматической синхронизации текущей политики доступа **останется временно заблокированной** и для ее разблокировки необходимо будет выполнить **команду ручной (принудительной) синхронизации текущей политики доступа** на одном из устройств схемы, выполнив команду:

```
fnp4> reserv sync
Немедленно синхронизировать текущую политику? (Y/N) [N]: y
FNPSH-I-007.02.30D0-Синхронизация политики инициирована
fnp4>
```

Команда ручной (принудительной) синхронизации текущей политики доступа может быть выполнена независимо от того, включена ли в конфигурации устройства **функция автоматической синхронизации текущей политики доступа**.

Команда ручной синхронизации текущей политики доступа может быть выполнена только если смежное устройство доступно (не находится в состоянии аппаратного отказа), при этом режим и состояние данного устройства отвечают следующим требованиям:

- для режима **Master/Slave** команда ручной синхронизации может быть выполнена только на устройстве в состоянии **Master**;
- для режима **Sync/Sync** команда ручной синхронизации может быть выполнена на любом из устройств схемы;
- для режима **Balance/Balance** команда ручной синхронизации может быть выполнена на любом из устройств схемы.
- независимо от схемы резервирования команда может быть выполнена на устройстве в состоянии **“Программный отказ”**.

После успешного выполнения ручной синхронизации текущей политики доступа также выполняется **процедура проверки идентичности политик на устройствах**. Если в результате ручной синхронизации текущие политики стали **идентичны** на устройствах схемы, то **временная блокировка автоматической синхронизации выключится**.

При **включении/выключении временной блокировки** автоматической синхронизации текущей политики в журнале событий регистрируются соответствующие **события**.

Ручная и автоматическая синхронизация текущей политики доступа **недоступны в случае конфликта режимов устройств схемы резервирования**. Корректными являются только перечисленные ниже комбинации режимов на парных устройствах в схеме резервирования:

- **Master** и **Slave**;
- **Sync** и **Sync**;
- **Balance** и **Balance**.

3.6. Политики доступа

Политика доступа МЭ ССПТ-4А1 содержит в себе правила фильтрации, используемые пакетным фильтром для фильтрации трафика:

- общие правила;
- АР-правила (прикладные правила);

Кроме того политика доступа может содержать:

- PRI-правила (правила приоритизации);
- PROXY-правила (правила HTTP-посредника);
- объекты справочника (для использования в правилах фильтрации).

Политики доступа МЭ ССПТ-4А1 могут быть двух типов:

- текущая политика доступа;
- дополнительная политика доступа.

По умолчанию текущая политика доступа содержит лишь два правила:

- глобальное общее правило;
- глобальное АР-правило.

При этом оба глобальных правила изначально имеют действие **“drop”**, т.е. текущая политика по умолчанию запрещает весь трафик.

Текущая политика может быть сохранена в дополнительную политику доступа для последующего применения в качестве текущей политики доступа. Для сохранения текущей политики в дополнительную используется команда **`policy save`**.

Пример сохранения текущей политики в дополнительную с автоматически сгенерированным именем дополнительной политики:

```
fnp4> policy save
Имя дополнительной политики не указано. Сохранить со сгенерированным именем? (Y/N) [N]: y
FNPSH-I-007.02.30FD-Дополнительная политика сохранена (fnp4-fnp4-20170525-152609)
```

Пример сохранения текущей политики в дополнительную с явным указанием имени и комментария к политике:

```
fnp4> policy save name=pol1 comment="комментарий к политике доступа"
FNPSH-I-007.02.30FD-Дополнительная политика сохранена (pol1)
```

МЭ ССПТ-4А1 позволяет хранить до **32** дополнительных политик.

Просмотреть список дополнительных политик доступа на данном устройстве МЭ ССПТ-4А1 можно, выполнив команду **policy list**:

```
fnp4> policy list
Список дополнительных политик:
    Имя                          Последнее изменение                Комментарий
    fnp4-fnp4-20170525-152609    25.05.2017 15:26:09 UTC+0300 (MSK)
    pol1                         25.05.2017 15:32:00 UTC+0300 (MSK) комментарий к политике
    policy_accept                25.05.2017 13:09:23 UTC+0300 (MSK) всё разрешено
    policy_drop                  25.05.2017 13:09:23 UTC+0300 (MSK) всё запрещено
    proxy_1                      17.04.2017 11:39:51 UTC+0300 (MSK)
Занято: 5       Свободно: 27
```

Дополнительные политики policy_accept и policy_drop присутствуют на МЭ ССПТ-4А1 изначально.

- **policy_accept** — разрешает прохождение любого трафика через устройство, если в конфигурации МЭ ССПТ-4А1 выключено использование АР-правил (по умолчанию);
- **policy_drop** - запрещает прохождение любого трафика через устройство и соответствует текущей политике доступа по умолчанию.

Данные политики доступа могут быть удалены администратором, но это делать не рекомендуется.

Дополнительная политика может быть переименована, может быть изменен или удален комментарий к ней. Для этого служит команда **`policy rename`**, например:

```
fnp4> policy rename srcname=pol1 dstname=policy1 comment="новый комментарий"
FNPSH-I-007.02.3107-Комментарий к дополнительной политике изменен (pol1)
FNPSH-I-007.02.3108-Дополнительная политика переименована (pol1, policy1)
```

Убедиться в переименовании политики доступа и изменении комментария к ней можно, снова выполнив команду **`policy list`**:

```
fnp4> policy list
Список дополнительных политик:
    Имя                          Последнее изменение                Комментарий
    fnp4-fnp4-20170525-152609    25.05.2017 15:26:09 UTC+0300 (MSK)
    policy1                      25.05.2017 15:51:02 UTC+0300 (MSK) новый комментарий
    policy_accept                25.05.2017 13:09:23 UTC+0300 (MSK) всё разрешено
    policy_drop                  25.05.2017 13:09:23 UTC+0300 (MSK) всё запрещено
    proxy_1                      17.04.2017 11:39:51 UTC+0300 (MSK)
Занято: 5       Свободно: 27
```

Допустим, текущая политика была изменена администратором МЭ ССПТ-4А1 (например, добавлены или удалены правила фильтрации) и возникла необходимость применить в качестве текущей политики ранее сохраненную дополнительную политику. Для применения дополнительной политики служит команда **`policy apply`**, например:

```
fnp4> policy apply name=policy1
Применить дополнительную политику (режим управления сессиями)? (Y/N) [N]: y
FNPSH-I-007.02.30FC-Дополнительная политика применена (правила и справочник)
```

При применении дополнительной политики пакетный фильтр МЭ ССПТ-4А1 очищает таблицу сессий.

Дополнительная политика может быть удалена. Для этого служит команда **policy remove**, например:

```
fnp4> policy remove name=fnp4-fnp4-20170525-152609
Удалить дополнительную политику? (Y/N) [N]: y
FNPSH-I-007.02.30FE-Дополнительная политика удалена
```

Отмена последнего изменения текущей политики доступа

Допустим, текущая политика соответствует политике по умолчанию:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
ap:0 action=drop
```

Далее администратор по ошибке добавил синтаксически правильное, но логически некорректное правило:

```
fnp4> rule add rule:10 action=accept
FNPSH-I-007.02.3046-Общее правило добавлено (10)
```

В результате изменился состав текущей политики:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
rule:10 action=accept apr=no
ap:0 action=drop
```

Отменить последнее изменение политики доступа (в данном примере — добавление общего правила с номером 10) можно, выполнив команду **policy rollback**:

```
fnp4> policy rollback
Выполнить возврат к предыдущему состоянию политики (режим управления сессиями)? (Y/N) [N]:
y
FNPSH-I-007.02.304E-Возврат к предыдущему состоянию текущей политики выполнен
```

В результате текущая политика вернулась к состоянию до последнего изменения в ней:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
ap:0 action=drop
```

МЭ ССПТ-4А1 хранит до **пяти** последних состояний текущей политики доступа. Таким образом, повторным выполнением команды **policy rollback** можно отменить до **пяти** последних изменений текущей политики доступа.

Изменением текущей политики доступа, которое можно отменить, является любое изменение, относящееся к правилу фильтрации или к объекту справочника.

В том случае, если политика доступа **policy_drop**, изначально присутствующая на МЭ ССПТ-4А1, была удалена администратором, вернуть текущую политику к состоянию по умолчанию можно, выполнив команду **policy default**:

```
fnp4> policy default
Применить политику по умолчанию? (удаление всех пакетов и очистка справочника) (Y/N) [N]: y
FNPSH-I-007.02.30FF-Политика установлена в состояние по умолчанию (правила и справочник)
```

В результате из текущей политики доступа будут удалены все объекты справочника (если присутствовали) и текущая политика будет содержать следующие правила фильтрации:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
ap:0 action=drop
```

Выгрузка политики доступа. Как текущая, такая и дополнительная политика доступа может быть выгружена с МЭ ССПТ-4А1 на управляющий компьютер администратора для резервного копирования и/или последующей загрузки на другое устройство МЭ ССПТ-4А1.

Функция выгрузки политик доступа с МЭ на УК доступна с применением следующих средств администрирования:

- WEB-интерфейс администратора;
- FNPCP-интерфейс администратора.

Пример выгрузки текущей политики доступа на УК администратора с использованием WEB-интерфейса администратора приведен в разделе 4.3.1, стр. 290. Выгрузка дополнительной политики доступа выполняется аналогичным образом.

Загрузка политики доступа. Ранее выгруженную политику доступа можно загрузить на МЭ ССПТ-4А1 и впоследствии применить как дополнительную политику доступа.

Функция загрузки политики доступа с УК на МЭ доступна с применением следующих средств администрирования:

- WEB-интерфейс администратора;
- FNPCP-интерфейс администратора.

Пример загрузки политики доступа с УК администратора на МЭ с использованием WEB-интерфейса администратора приведен в разделе 4.3.1, стр. 291.

3.7. Правила фильтрации

В МЭ ССПТ-4А1 используются правила фильтрации трех типов:

- TMP-правила (временные правила);
- общие правила;
- AP-правила (прикладные правила).

3.7.1. TMP-правила

TMP-правила (временные правила) служат для временного запрета определенного трафика. TMP-правило имеет параметр **Время жизни**, который определяет временной отрезок от создания TMP-правила до автоматического удаления TMP-правила.

> В отличие от **общих правил** и **AP-правил**, **TMP-правила** не сохраняются в политике доступа МЭ ССПТ-4А1. Таким образом, после перезапуска пакетного фильтра или перезагрузки МЭ ССПТ-4А1 все ранее добавленные TMP-правила будут удалены.

Синтаксис TMP-правил представлен в приложении Д.3, стр. 534.

Типовая задача применения TMP-правил. Требуется временно запретить доступ некоторой группе узлов сети, находящейся за одним из фильтрующих интерфейсов МЭ ССПТ-4А1, к другому узлу сети, например некоторому серверу.

Например, есть три узла сети, находящиеся за фильтрующим интерфейсом с номером **1**, каждый из которых доступен как по IPv4-адресу, так и по IPv6-адресу:

1) *IPv4: 10.99.1.1, IPv6: 2001:0db8::0010:0099:0001:0001*;
2) *IPv4: 10.99.1.2, IPv6: 2001:0db8::0010:0099:0001:0002*;
3) *IPv4: 10.99.1.3, IPv6: 2001:0db8::0010:0099:0001:0003*.

Есть сервер, к которому необходимо временно запретить доступ трем узлам сети, указанным выше. Сервер также доступен по IPv4-адресу и по IPv6-адресу:

IPv4: 192.168.99.1, IPv6:2001:0db8::0192:0168:0099:0001

Доступ узлов сети к серверу должен быть запрещен только для TCP-трафика, для портов: 80, 443, 8080.

Например, изначально на устройстве были следующие правила фильтрации:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=accept
ap:0 action=drop
```

Для решения этой задачи необходимо добавить два TMP-правила. Первое правило запрещает доступ для IPv4-трафика:

```
fnp4> rule add tmp:1 srcif=1 srcip4=10.99.1.1,10.99.1.2,10.99.1.3 dstip4=192.168.99.1
ipproto=tcp dstport=80,443,8080
FNPSH-I-007.02.3096-TMP-правило добавлено (1)
```

Второе правило запрещает доступ для IPv6-трафика:

```
fnp4> rule add tmp:2 srcif=1
srcip6=2001:0db8::0010:0099:0001:0001,2001:0db8::0010:0099:0001:0002,2001:0db8::0010:0099:0
001:0003 dstip6=2001:0db8::0192:0168:0099:0001 ipproto=tcp dstport=80,443,8080
FNPSH-I-007.02.3096-TMP-правило добавлено (2)
```

В итоге политика доступа будет содержать следующие правила фильтрации:

```
fnp4> rule show viewer=no
Правила текущей политики:

tmp:1 srcif=1 srcip6=2001:db8::10:99:1:1,2001:db8::10:99:1:2,2001:db8::10:99:1:3
dstip6=2001:db8::192:168:99:1 dstport=80,443,8080 ipproto=tcp time=3600
tmp:2 srcif=1 srcip6=2001:db8::10:99:1:1,2001:db8::10:99:1:2,2001:db8::10:99:1:3
dstip6=2001:db8::192:168:99:1 dstport=80,443,8080 ipproto=tcp time=3600
rule:0 action=accept
ap:0 action=drop
```

В отличие от **общего правила** и **АР-правила** в **ТМР-правиле** не допускается одновременное использование IPv4-адресов и IPv6-адресов. Это означает, что в **ТМР-правиле** не допускается, чтобы параметры **srcip4 (dstip4)** и **srcip6 (dstip6)** одновременно были в значениях отличных от **"any"**.

Изменение параметров существующего **ТМР-правила** не предусмотрено.

ТМР-правила могут автоматически добавляться пакетным фильтром МЭ ССПТ-4А1 в ответ на обнаруженную **flood-атаку**.

ТМР-правило может быть удалено администратором до окончания его **времени жизни**. Например, чтобы удалить ранее добавленное ТМР-правило с номером 2, необходимо выполнить команду **`rule delete`**:

```
fnp4> rule delete tmp:2
Удалить ТМР-правило? (Y/N) [N]: y
FNPSH-I-007.02.30BC-TMP-правило удалено (2)
```

3.7.2. Общие правила

Общие правила позволяют фильтровать сетевой трафик на основе параметров канального и сетевого уровней. Синтаксис общих правил представлен в приложении Д.1, стр. 514.

Например, на МЭ ССПТ-4А1 используется политика доступа, отвечающая принципу “*Запрещено все, что явно не разрешено*”. Для формирования политики доступа, отвечающей данному принципу, удобно использовать политику доступа по умолчанию, содержащую глобальное общее правило и глобальное АР-правило – оба с действием **`drop`**:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
ap:0 action=drop
```

Для принципиальной возможности передачи IP-пакетов протокола IP версии 4 через МЭ ССПТ-4А1 при данной исходной политике доступа необходимо добавить общие правила, разрешающие передачу ARP-трафика, например между фильтрующими интерфейсами **0** и **1**:

```
fnp4> rule add rule:1 action=accept frame=eth2 ethproto=0x0806 srcif=0 dstif=1 comment="ARP
с eth0 на eth1"
FNPSH-I-007.02.3046-Общее правило добавлено (1)
fnp4> rule add rule:2 action=accept frame=eth2 ethproto=0x0806 srcif=1 dstif=0 comment="ARP
с eth1 на eth0"
FNPSH-I-007.02.3046-Общее правило добавлено (2)
```

Для принципиальной возможности передачи IP-пакетов протокола IP версии 6 через МЭ ССПТ-4А1 при данной исходной политике доступа необходимо добавить общие правила, разрешающие передачу ICMPv6-сообщений протокола NDP (*NDP – Neighbor Discovery Protocol*), например между фильтрующими интерфейсами **0** и **1**:

```
fnp4> rule add rule:6 action=accept log=enable srcif=0 dstif=1 version=6 ipproto=icmp6
icmp6=135/0
FNPSH-I-007.02.3046-Общее правило добавлено (6)
fnp4> rule add rule:7 action=accept log=enable srcif=1 dstif=0 version=6 ipproto=icmp6
icmp6=135/0
FNPSH-I-007.02.3046-Общее правило добавлено (7)
```

Данная пара правил разрешает прохождение через МЭ ССПТ-4А1 ICMPv6 сообщений типа *Neighbor Solicitation* (тип `135`, код `0`). Ответные ICMPv6 сообщения от опрашиваемого узла типа *Neighbor Advertisement* (тип `136`, код `0`) будут пропущены за счет работы режима управления сессиями (по умолчанию данный режим включен).

Теперь можно разрешить определенный IP-трафик между фильтрующими интерфейсами **0** и **1**. Например, требуется разрешить любой TCP и UDP трафик между IP-сетью 192.168.1.0/24 и сервером с IP-адресом 10.1.1.1

В том случае, если **режим управления сессиями** включен (по умолчанию включен), достаточно добавить одно общее правило, в котором источником является клиент, а приемником – сервер. Ответные пакеты от сервера к клиенту в этом случае будут доставлены за счет **режима управления сессиями**. Для добавления такого правила необходимо выполнить команду **`rule add`**:

```
fnp4> rule add rule:10 action=accept ipproto=tcp,udp srcif=0 dstif=1 srcip4=192.168.1.0/24
dstip4=10.1.1.1
FNPSH-I-007.02.3046-Общее правило добавлено (10)
```

Допустим, требуется также разрешить ICMP-трафик между указанными выше клиентом и сервером. Для этого достаточно изменить уже существующее правило, выполнив команду **`rule edit`**:

```
fnp4> rule edit rule:10 ipproto=tcp,udp,icmp
Изменить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3047-Общее правило изменено (10)
```

Параметр **ipproto** общего правила по умолчанию имеет значение **any** (любой протокол, инкапсулированный в IP). Если при этом в правиле не заданы параметры **srcport**, **dstport**, **icmp4** или **icmp6**, то данному правилу будут удовлетворять сообщения любых протоколов, инкапсулированных в IP-пакет (tcp, udp, icmp и т. д.).

Если **ipproto** имеет значение **any** и при этом:

- задан параметр **srcport** (и/или **dstport**), то правило будет применено только к TCP-сообщениям и UDP-дейтаграммам с указанными портами;
- задан параметр **icmp4**, то правило будет применено только к ICMPv4-сообщениям с указанными типом и кодами ICMPv4;
- задан параметр **icmp6**, то правило будет применено только к ICMPv6-сообщениям с указанными типом и кодами ICMPv6.

Если **ipproto** имеет значение **any** и при этом задана комбинация из числа перечисленных параметров (**srcport/dstport**, **icmp4**, **icmp6**), то общее правило будет применено только к тем протоколам, чьи параметры заданы.

Параметр **ipproto** также может быть задан явно списком конкретных протоколов.

При выключенном **режиме управления сессиями** для решения той же задачи потребуется добавить отдельное правило, разрешающее трафик протоколов TCP, UDP и ICMP в направлении от сервера к клиенту:

```
fnp4> rule add rule:11 action=accept srcif=1 srcip4=10.1.1.1 dstif=0
dstip4=192.168.1.0/255.255.255.0 ipproto=tcp,udp,icmp
FNPSH-I-007.02.3046-Общее правило добавлено (11)
```

В общем правиле можно использовать комбинации адресов **источника** и **приемника** следующих типов:

- MAC-адреса;
- IPv4-адреса;
- IPv6-адреса.

Пример добавления общего правила, использующего комбинацию всех трех типов адресов:

```
fnp4> rule add rule:100 action=accept srcmac=aa:bb:cc:dd:ee:01 srcip4=192.168.1.1
srcip6=2001:0db8::0192:0168:0001:0001 dstmac=aa:bb:cc:dd:ee:02 dstip4=192.168.1.2
dstip6=2001:0db8::0192:0168:0001:0002
FNPSH-I-007.02.3046-Общее правило добавлено (100)
```

Добавленному правилу буду соответствовать Ethernet-кадр с MAC-адресом источника **`aa:bb:cc:dd:ee:01`** и MAC-адресом приемника **`aa:bb:cc:dd:ee:02`**, если в данный Ethernet-кадр инкарсулирован один из следующих пакетов:

- IPv4-пакет с IP-адресом источника **`192.168.1.1`** и IP-адресом приемника **`192.168.1.2`**;
- IPv6-пакет с IPv6-адресом источника **`2001:0db8::0192:0168:0001:0001`** и IPv6-адресом приемника **`2001:0db8::0192:0168:0001:0002`**.

Одно общее правило может использоваться, как для фильтрации **IPv4-трафика**, так и для фильтрации **IPv6-трафика** при соответствующей комбинации адресных параметров правила.

Действия общего правила.

Общее правило допускает четыре действия в отношении пакета (и сессии):

- **accept** – пропуск пакета на выходные интерфейсы или передача на уровень прикладной фильтрации;
- **drop** – удаление пакета;
- **deny** – удаление пакета и корректное завершение сессии: клиент получает уведомление от МЭ ССПТ-4А1 от имени сервера, к которому производился запрос;
- **goto** – переход на другое общее правило с большим номером.

Действие **deny** является альтернативой действию **drop**. Оба действия обеспечивают один и тот же результат – запрет прохождения трафика через МЭ ССПТ-4А1, но отличаются формой представления результата конечному пользователю.

Поясним это на примере. Имеется задача – запретить взаимодействие клиента и сервера через МЭ ССПТ-4А1, где:

- IP-адресом клиента является **10.2.253.241**;
- IP-адресом сервера является **10.2.253.242**.

Первое решение – добавить правило с действием **drop**:

```
fnp4> rule add rule:20 action=drop srcip4=10.2.253.241 dstip4=10.2.253.242
FNPSH-I-007.02.3046-Общее правило добавлено (20)
```

Для проверки действия правила будем использовать взаимодействие клиента и севера по протоколу SSH. Попытка клиента обратиться к серверу:

```
$ ssh 10.2.253.242
ssh: connect to host 10.2.253.242 port 22: Operation timed out
```

SSH-клиент многократно повторяет запросы к серверу, которые удаляет МЭ ССПТ-4А1 в соответствии с правилом **20**, до тех пор, пока не наступит тайм-аут (конкретная диагностика может отличаться от ОС, используемой клиентом).

Второе решение – использовать правило с действием **deny**. Чтобы не добавлять отдельное правило изменим действие в ранее добавленном правиле с номером **20**:

```
fnp4> rule edit rule:20 action=deny
Изменить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3047-Общее правило изменено (20)
```

Попытка клиента обратиться к серверу:

```
$ ssh 10.2.253.242
ssh: connect to host 10.2.253.242 port 22: Connection refused
```

Клиент получил ответ от МЭ ССПТ-4А1 об отказе в соединении, выполненный от имени сервера. В результате программа SSH-клиент завершилась после получения ответа, не предпринимая повторных попыток соединения.

Действие **goto** позволяет выполнить условный переход при проверке пакета по списку общих правил и тем самым исключить часть правил из рассмотрения. Рассмотрим применение действия **goto** на примере. Допустим, в текущей политике доступа следующие правила:

```
fnp4> rule show viewer=no
Правила текущей политики:
rule:0 action=drop
rule:1 action=accept comment="ARP с eth0 на eth1" frame=eth2 ethproto=0x0806 srcif=0
dstif=1 apr=no
rule:2 action=accept comment="ARP с eth1 на eth0" frame=eth2 ethproto=0x0806 srcif=1
dstif=0 apr=no
rule:10 action=accept srcif=0 srcip4=192.168.1.0/255.255.255.0 dstif=1 dstip4=10.1.1.1
ipproto=tcp,udp,icmp apr=no
rule:11 action=accept srcif=1 srcip4=10.1.1.1 dstif=0 dstip4=192.168.1.0/255.255.255.0
ipproto=tcp,udp,icmp apr=no
rule:20 action=deny srcip4=10.2.253.241 dstip4=10.2.253.242 apr=no
rule:100 action=accept srcmac=aa:bb:cc:dd:ee:01 srcip4=192.168.1.1
srcip6=2001:db8::192:168:1:1 dstmac=aa:bb:cc:dd:ee:01 dstip4=192.168.1.2
dstip6=2001:db8::192:168:1:2 apr=no
```

Правило номер **20** запрещает любые взаимодействия между клиентом **10.2.253.241** и сервером **10.2.253.242**. Требуется изменить политику доступа так, чтобы SSH-соединения к серверу **10.2.253.242** разрешались от любых клиентов, в том числе от **10.2.253.241**, а соединения других протоколов от клиента **10.2.253.241** запрещались.

Для решения этой задачи достаточно добавить два правила. Вначале необходимо добавить правило, разрешающее SSH-соединения к серверу **10.2.253.242** от любых клиентов:

```
fnp4> rule add rule:21 action=accept dstip4=10.2.253.242 ipproto=tcp dstport=22
FNPSH-I-007.02.3046-Общее правило добавлено (21)
```

Далее, до правила с номером **20**, необходимо добавить правило, осуществляющее переход к правилу с номером **21** в том случае, если IP-адресом клиента является **10.2.253.241**, а IP-адресом сервера является **10.2.253.242** и обращение к серверу на порт SSH (**22**):

```
fnp4> rule add rule:19 action=goto:21 srcip4=10.2.253.241 dstip4=10.2.253.242 ipproto=tcp
dstport=22
FNPSH-I-007.02.3046-Общее правило добавлено (19)
```

Проверим, работу сформированной политики доступа. Соединение клиента **10.2.253.241** к серверу **10.2.253.242** по протоколу SSH:

```
$ ssh 10.2.253.242
The authenticity of host '10.2.253.242 (10.2.253.242)' can't be established.
ECDSA key fingerprint is SHA256:uOyvQx+gXkWRO5oMVmoaOC1xfXruP1ndtq4ayEwalNo.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)?
```

Вывод подтверждает, что TCP-соединение успешно установлено.

Попытка отправить ICMP-запрос от клиента **10.2.253.241** серверу **10.2.253.242**:

```
PING 10.2.253.242 (10.2.253.242): 56 data bytes
92 bytes from 10.2.253.242: Dest Unreachable, Bad Code: 9
Vr HL TOS  Len   ID Flg  off TTL Pro  cks      Src      Dst
 4  5  00 0054 1729   0 0000  40  01 5398 10.2.253.241  10.2.253.242
```

ICMP-запрос подпадает под действие правила **20** с действием **deny**, о чем свидетельствует ответ “*Dest Unreachable*”, отправленный МЭ ССПТ-4А1 от имени сервера.

Отметим, что данная задача могла быть решена без использования действия **goto** за счет размещения правила, разрешающего доступ к серверу по протоколу SSH для всех клиентов, до правила **20**, запрещающего весь трафик между клиентом **10.2.253.241** и сервером **10.2.253.242**.

3.7.3. АР-правила

АР-правила (прикладные правила) предоставляют возможность фильтрации трафика на прикладном уровне.

По умолчанию использование АР-правил выключено в конфигурации МЭ ССПТ-4А1.

АР-правила могут иметь следующие действия:

- **accept** – пропуск пакета на выходные интерфейсы;
- **drop** – удаление пакета.

Действие **accept** служит для регистрации и сбора статистики трафика, отвечающего параметрам данного АР-правила.

В политике доступа по умолчанию присутствует только глобальное запрещающее АР-правило (с действием **drop)**. Таким образом, при использовании АР-правил необходимо изменить политику доступа, чтобы в ней было хотя бы одно разрешающее АР-правило с действием (**accept**).

Для использования АР-правил в политике доступа, помимо включения использования АР-правил в конфигурации МЭ ССПТ-4А1, необходимо явно разрешить использование **АР-правил**, хотя бы в одном из общих правил политики доступа.

АР-правила МЭ ССПТ-4А1 имеют набор общих параметров, использование которых доступно независимо от прикладного протокола, заданного в АР-правиле (параметр **protocol**), а также наборы параметров, возможность использования которых определятся значением параметра прикладного протокола.

Синтаксис АР-правил, в том числе перечни допустимых параметров фильтрации в зависимости от прикладного протокола, представлены в приложении Д.2, стр. 527.

Рассмотрим пример настройки МЭ ССПТ-4А1 для использования АР-правил, предполагая, что устройство имеет текущие конфигурацию и политику доступа по умолчанию.

Включение использования АР-правил в конфигурации устройства:

```
fnp4> session ap enable
FNPSH-I-007.02.3087-Использование AP-правил включено
```

Правила текущей политики доступа:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
ap:0 action=drop
```

Добавление общего правила, разрешающего любой сетевой трафик с интерфейса **0** на интерфейс **1** и предписывающего обработку на прикладном уровне:

```
fnp4> rule add rule:1 action=accept srcif=0 dstif=1 apr=yes comment="использование AP-
правил"
FNPSH-I-007.02.3046-Общее правило добавлено (1)
```

Под данное правило попадает, в том числе, и ARP-трафик с интерфейса **0** на интерфейс **1**. Для передачи ARP-трафика в обратном направлении (с интерфейса **1** на интерфейс **0**) необходимо добавить отдельное правило:

```
fnp4> rule add rule:2 action=accept srcif=1 dstif=0 frame=eth2 ethproto=0x0806 comment="ARP
1->0"
FNPSH-I-007.02.3046-Общее правило добавлено (2)
```

Допустим, что обработка на прикладном уровне должна отвечать принципу “*Разрешено все, что явно не запрещено*”. Для этого, во-первых, нужно изменить действие глобального AP-правила:

```
fnp4> rule edit ap:0 action=accept
Изменить AP-правило? (Y/N) [N]: FNPSH-I-007.02.3049-AP-правило изменено (0)
```

Допустим, необходимо запретить запросы по протоколу HTTP к WEB-серверам с определенными адресами:

```
fnp4> rule add ap:1 action=drop protocol=http hostname="a*c.priv,xyz?.server.priv"
FNPSH-I-007.02.3048-AP-правило добавлено (1)
```

В соответствии с добавленным AP-правилом будут запрещены HTTP-запросы к WEB-серверам с доменными именами:

- **`ac.priv, abc.priv, aaaaac.priv`** и т. д.;
- **`xyzz.server.priv, xyz1.server.priv`** и т. д.

Полный перечень специальных символов, допустимых к использованию, а также других параметров AP-правил для поиска текстовых данных приведен в Д.2, стр. 527.

В итоге, в текущей политике доступа содержатся следующие правила:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop log=enable
rule:1 action=accept log=enable comment="использование AP-правил" srcif=0 dstif=1 apr=yes
rule:2 action=accept comment="ARP 1->0" frame=eth2 ethproto=0x0806 srcif=1 dstif=0 apr=no
ap:0 action=accept
ap:1 action=drop protocol=http hostname="a*c.priv,xyz?.server.priv"
```

В приведенном примере для общего правила с номером **1** была задана фильтрация на прикладном уровне (**apr=enable**). При этом трафик прикладного протокола проверяется на соответствие всем АР-правилам текущей политики доступа, отвечающим данному прикладному протоколу (до первого подходящего правила).

Синтаксис общих правил позволяет ограничить набор АР-правил политики доступа, по которым будет выполняться фильтрация на прикладном уровне для данного общего правила, явно указав список существующих АР-правил в значении параметра **apr** общего правила.

АР-правила, привязываемые к общему правилу за счет указания списка их номеров в значении параметра **apr,** должны быть добавлены в политику доступа заранее.
Это означает, что общее правило может быть привязано только к списку уже существующих АР-правил.

Приведем пример привязки общего правила к некоторому списку АР-правил. Как было сказано выше, вначале должны быть добавлены все АР-правила используемые в привязке к общему правилу.

Допустим необходимо, чтобы узлу сети с IP-адресом **10.2.253.241** запрещался доступ к WEB-серверам с доменными именами в соответствии с АР-правилом **1**, а узлу сети с IP-адресом **10.2.253.249** запрещался доступ к WEB-серверам с другими доменными именами. Для этого, во-первых, требуется добавить еще одно АР-правило:

```
fnp4> rule add ap:2 action=drop protocol=http hostname="first.server.priv"
FNPSH-I-007.02.3048-АР-правило добавлено (2)
```

Во-вторых, необходимо изменить общее правило **1** следующим образом:

```
fnp4> rule edit rule:1 srcip4=10.2.253.241 apr=1 comment="привязка к АР#1"
Изменить общее правило? (Y/N) [N]: FNPSH-I-007.02.3047-Общее правило изменено (1)
```

Теперь, в соответствии с общим правилом номер **1**, трафик клиента с IP-адресом **10.2.253.241** будет проверяться только на соответствие АР-правилу с номером **1**, а в случае несоответствия будет применено глобальное АР-правило.

В третьих, необходимо добавить общее правило для клиента с IP-адресом **10.2.253.249**, привязав его к АР-правилу с номером **2**:

```
fnp4> rule add rule:3 action=accept srcif=0 srcip4=10.2.253.249 dstif=1 apr=2
comment="привязка к АР#2"
FNPSH-I-007.02.3046-Общее правило добавлено (3)
```

В результате, текущая политика доступа содержит следующие правила:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop log=enable
rule:1 action=accept log=enable comment="привязка к АР#1" srcif=0 srcip4=10.2.253.241
dstif=1 apr=1
rule:2 action=accept comment="ARP 1->0" frame=eth2 ethproto=0x0806 srcif=1 dstif=0 apr=no
rule:3 action=accept comment="привязка к АР#2" srcif=0 srcip4=10.2.253.249 dstif=1 apr=2
```

```
ap:0 action=accept
ap:1 action=drop protocol=http hostname="a*c.priv,xyz?.server.priv"
ap:2 action=drop protocol=http hostname="first.server.priv"
```

Отметим, что данную задачу (фильтрация данных прикладного протокола в зависимости от IP-адреса клиента) можно решить более простым способом – без привязки конкретных АР-правил к общим правилам. Для этого необходимо в АР-правилах указать IP-адрес клиента (параметр **ipcl4**). При этом достаточно одного общего правила, разрешающего фильтрацию на прикладном уровне. Таким образом, следующие правила фильтрации предоставляют альтернативное решение данной задачи:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop log=enable
rule:1 action=accept log=enable comment="привязка к АР#1" srcif=0 dstif=1 apr=yes
rule:2 action=accept comment="ARP 1->0" frame=eth2 ethproto=0x0806 srcif=1 dstif=0 apr=no
ap:0 action=accept
ap:1 action=drop protocol=http ipcl4=10.2.253.241 hostname="a*c.priv,xyz?.server.priv"
ap:2 action=drop protocol=http ipcl4=10.2.253.249 hostname="first.server.priv"
```

При использовании АР-правил для фильтрации прикладных данных в рамках TCP-сессии, в в которой после установления соединения (первые три пакета), четвертым пакетом является пакет с установленными флагами PUSH, ACK необходимо добавление отдельного АР-правила, разрешающего пропуск данного пакета через МЭ ССПТ-4А1 (*в том случае, если глобальное АР-правило имеет действие “**drop**”*).

3.7.4. Статистика использования правил фильтрации

Администратор имеет возможность просмотреть статистику использования правил фильтрации текущей политики доступа.

Рассмотрим использование данной функции на примере политики доступа, содержащей следующие правила фильтрации:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
rule:1 action=accept comment="ARP с eth0 на eth1" frame=eth2 ethproto=0x0806 srcif=0
dstif=1 apr=no
rule:2 action=accept comment="ARP с eth1 на eth0" frame=eth2 ethproto=0x0806 srcif=1
dstif=0 apr=no
rule:10 action=accept comment="ssh с eth0 на eth1" srcif=0 dstif=1 dstport=22 ipproto=tcp
apr=yes
rule:11 action=accept comment="ICMP с eth0 на eth1" srcif=0 dstif=1 ipproto=icmp apr=no
ap:0 action=accept
```

Пояснение к правилам фильтрации, представленным выше:

- глобальное общее правило, запрещающее передачу трафика;
- общие правила 1 и 2 разрешают передачу ARP-трафикас фильтрующего интерфейса с номером 0 на интерфейс с номером 1 и в обратном порядке соответственно;
- общее правило с номером 10 разрешает передачу трафика протокола SSH между клиентом, находящимся за интерфейсом 0 и сервером, находящимся за интерфейсом 1 (подразумевается

что управление сессиями включено в конфигурации, поэтому достаточно одного правила в направлении от клиента к серверу). Кроме того, данное правило предписывает обработку на прикладном уровне (параметр **apr=yes**);

- общее правило с номером 11 разрешает передачу трафика протокола ICMP между клиентом, находящимся за интерфейсом 0 и сервером, находящимся за интерфейсом 1;
- глобальное AP-правило разрешает передачу данных независимо от протокола прикладного уровня .

Статистика использования правил фильтрации. Для вывода статистики использования правил фильтрации служит команда **rule stats show**. Пример вывода данной команды в случае текущей политики, приведенной ранее, представлен на рис. 3.13, стр. 151.

```
 16:47:01                          Статистика правил                          24.05.2018
Правила      Последняя активность  Пакеты    Байты     Комментарий
rule:0       24.05.2018, 16:45:00  3         132
rule:1       24.05.2018, 16:45:14  1         46        ARP с eth0 на eth1
rule:2       24.05.2018, 16:46:20  5         230       ARP с eth1 на eth0
rule:10      24.05.2018, 16:46:35  137       60K       ssh с eth0 на eth1
rule:11      24.05.2018, 16:46:19  198       12K       ICMP с eth0 на eth1
ap:0         24.05.2018, 16:46:35  95        56K

Правила:6                          Автообновление: включено | Страница: 1 из 1
                                   H - справка  Q, F10 - выход
```

Рисунок 3.13: Статистика использования правил фильтрации

В выводе команды каждая строка содержит статистику использования одного правила фильтрации. Строка статистики содержит следующие данные:

- Тип и номер правила фильтрации (столбец “Правила”);
- Дата и время последнего срабатывания правила фильтрации (столбец “Последняя активность”);
- Количество протокольных единиц (Ethernet-кадров, IP-пакетов), к которым было применено данное правило (столбец “Пакеты”);
- Суммарное количество байт данных в протокольных единицах, к которым было применено данное правило (столбец “Байты”);
- Комментарий к правилу (столбец “Комментарий”). В случае отсутствия комментария к правилу – пустая строка).

В выводе команды используются следующие суффиксы для сокращения числа знаков в численных значениях:

- `к` – Килобайт (1024 Байта);
- `м` — Мегабайт (1024 Килобайта);
- `г` – Гигабайт (1024 Мегабайта).

Для просмотра статистики использования правил фильтрации применяются клавиши и управляющие последовательности, перечисленные в таблице 3.14, стр. 152.

Таблица 3.14: Управление просмотром статистики использования правил фильтрации

Управление	***Назначение***
<↑>	Перемещение на одну строку вверх
<↓>	Перемещение на одну строку вниз
<←>	Перемещение влево на одну позицию
<→>	Перемещение вправо на одну позицию
<Page Up>	Переход к предыдущей странице
<Page Down>	Переход к следующей странице
<R>	Обновление выводимой информации
<F>	Выключение/включение автоматического обновления выводимой информации
<H>	Вывод подсказки по клавишам управления просмотром статистики использования правил фильтрации
<F10>, <Q>	Завершение выполнения команды

Статистика использования правил фильтрации может быть обнулена администратором в любой момент времени. Для этого служит команда r**`ule stats clear`**. Статистика использования правил фильтрации может быть обнулена полностью либо только для заданного типа правил фильтрации.

Вывод статистики использования правил фильтрации обновляется каждые **5** секунд. Автоматическое обновление информации может быть выключено (включено) однократным нажатием клавиши **<F>** во время просмотра статистики использования правил фильтрации.

При любом изменении в текущей политике доступа МЭ ССПТ-4А1, а также при перезапуске пакетного фильтра МЭ ССПТ-4А1 статистика использования правил фильтрации обнуляется.

Пример обнуления статистики только АР-правил фильтрации:

```
fnp4> rule stats clear ap
Очистить статистику правил? (Y/N) [N]: y
FNPSH-I-007.02.305F-Статистика правил очищена
```

Пример обнуления статистики правил фильтрации всех типов (общих-правил, АР-правил, ТМР-правил):

```
fnp4> rule stats clear
Очистить статистику правил? (Y/N) [N]: y
FNPSH-I-007.02.305F-Статистика правил очищена
```

3.8. Справочник объектов

Справочник объектов входит в состав политики доступа (текущей и дополнительной). Объекты справочника призваны облегчить задачи по формированию политики доступа. Это достигается за счет использования объектов справочника в качестве параметров правил фильтрации. Каждый объект может использоваться в неограниченном числе правил фильтрации при условии соблюдения синтаксиса и семантики.

Синтаксис объектов справочника приведен в приложении Е, стр. 540. Семантика определяется правилами использования объектов в правилах фильтрации, данная информация представлена в приложении Д.1, стр. 521.

МЭ ССПТ-4А1 поддерживает следующие типы объектов справочника:

- `host` – узел сети;
- `net` – сеть;
- `net-group` – группа сетевых объектов;
- `service` – сервис;
- `resource` – ресурс;
- `vlan-group` – группа VLAN;
- `time` – интервал времени;
- `domain-group` – группа доменных имен;

Объекты типа **группа доменных имен** могут использоваться только в **АР-правилах**, объекты остальных типов могут использоваться только в **общих правилах**.

Объект host (узел сети) может использоваться в общем правиле для задания адресной информации правила для источника и/или приемника.

Рассмотрим следующую задачу. Есть два узла сети, которым нужно обеспечить доступ к третьему узлу сети (серверу) по протоколу SSH. Каждый узел имеет IP-адрес, MAC-адрес и подключен к определенному фильтрующему интерфейсу МЭ ССПТ-4А1. Эту задачу можно решить с использованием трех объектов **`host`**.

Добавляем первый объект **`host`**:

```
fnp4> directory add host name=host1 ip4=10.2.253.241 mac=00:0c:29:26:d0:5d interface=0
FNPSH-I-007.02.30D3-Объект справочника добавлен (узел сети "host1")
```

Добавляем второй объект **`host`**:

```
fnp4> directory add host name=host2 ip4=10.2.253.243 mac=00:0c:29:26:d0:5f interface=0
FNPSH-I-007.02.30D3-Объект справочника добавлен (узел сети "host2")
```

Добавляем третий объект **host** (сервер):

```
fnp4> directory add host name=server ip4=10.2.253.242 mac=00:0c:29:b7:34:ec interface=1
FNPSH-I-007.02.30D3-Объект справочника добавлен (узел сети "server")
```

Добавляем общее правило, обеспечивающее доступ объектов **host1** и **host2** к объекту **server** по протоколам SSH и ICMP:

```
fnp4> rule add rule:1 action=accept srcobject=host1,host2 dstobject=server ipproto=tcp,icmp
dstport=22 comment="ssh и icmp"
FNPSH-I-007.02.3046-Общее правило добавлено (1)
```

Объект **host** может иметь как IPv4, так и IPv6-адрес. Добавим в каждый из созданных объектов IPv6-адреса. Тогда уже имеющееся общее правило **1** будет обеспечивать доступ как по протоколу IPv4, так и по протоколу IPv6:

```
fnp4> directory edit host name=host1 ip6=2001:db8::241
Изменить объект справочника? (Y/N) [N]: y
FNPSH-I-007.02.30D4-Объект справочника изменен (узел сети "host1")
fnp4> directory edit host name=host2 ip6=2001:db8::243
Изменить объект справочника? (Y/N) [N]: y
FNPSH-I-007.02.30D4-Объект справочника изменен (узел сети "host2")
fnp4> directory edit host name=server ip6=2001:db8::242
Изменить объект справочника? (Y/N) [N]: y
FNPSH-I-007.02.30D4-Объект справочника изменен (узел сети "server")
```

Объекты **host1** и **host2** можно объединить в один объект **net-group** (*группа сетевых объектов*) для более лаконичного использования данного списка объектов в общих правилах:

```
fnp4> directory add net-group name=net_group_1 host=host1,host2 comment="host1 и host2"
FNPSH-I-007.02.30D3-Объект справочника добавлен (группа сетевых объектов "net_group_1")
```

Воспользуемся созданным объектом **net-group** для того, чтобы разрешить доступ данным узлам сети по протоколу HTTPS к WEB-серверу с любым IP-адресом:

```
fnp4> rule add rule:2 action=accept srcobject=net_group_1 ipproto=tcp dstport=443
comment="доступ по HTTPs"
FNPSH-I-007.02.3046-Общее правило добавлено (2)
```

Объект net (сеть) удобно использовать в общем правиле, когда источником или приемником выступает не список узлов сети, а некоторая IP-подсеть целиком. Добавим объект **net**:

```
fnp4> directory add net name=net1 ip4=10.2.253.240/29 comment="сеть 241-247"
FNPSH-I-007.02.30D3-Объект справочника добавлен (сеть "net1")
```

Объект **net** также, как и объект **host** может использоваться в общем правиле как в качестве источника, так и в качестве приемника. Например:

```
fnp4> rule add rule:3 action=accept srcobject=net1 dstip4=192.168.1.1
FNPSH-I-007.02.3046-Общее правило добавлено (3)
```

Объект service (сервис) позволяет определить сервис для использования в общих правилах политики доступа. Использование объекта **service** является альтернативой задания

сервиса посредством параметров **ipproto** и **dstport**. Это особенно актуально, когда несколько правил задают доступ к одним и тем же сервисам.

В качестве примера добавим три объекта **service**, для описания сервисов, которые уже используются в ранее добавленных правилах.

Добавим сервис протокола SSH:

```
fnp4> directory add service name=service_ssh protocol=tcp port=22 comment=ssh
FNPSH-I-007.02.30D3-Объект справочника добавлен (сервис "service_ssh")
```

Добавим сервис протокола ICMP (ICMPv4):

```
fnp4> directory add service name=service_icmp4 protocol=icmp
FNPSH-I-007.02.30D3-Объект справочника добавлен (сервис "service_icmp4")
```

Добавим сервис протокола HTTPs:

```
fnp4> directory add service name=service_https protocol=tcp port=443 comment=https
FNPSH-I-007.02.30D3-Объект справочника добавлен (сервис "service_https")
```

Изменим ранее добавленные правила фильтрации так, чтобы они использовали объекты **service**:

```
fnp4> rule edit rule:1 dstservice=service_ssh,service_icmp4 ipproto=any dstport=any
Изменить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3047-Общее правило изменено (1)
fnp4> rule edit rule:2 dstservice=service_https ipproto=any dstport=any
Изменить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3047-Общее правило изменено (2)
```

В итоге, текущая политика доступа содержит правила:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
rule:1 action=accept comment="ssh и icmp" srcobject=host1,host2 dstobject=server
dstservice=service_ssh,service_icmp4 apr=no
rule:2 action=accept comment="доступ по HTTPs" srcobject=net_group_1
dstservice=service_https apr=no
rule:3 action=accept srcobject=net1 dstip4=192.168.1.1 apr=no
ap:0 action=drop
```

Запись правил стала лаконичнее, при этом новые правила тождественны старым по своему действию.

Сервер, имеющий постоянный IP-адрес и предоставляющий некоторый сервис, удобно описывать с помощью объекта **resource** для использования в общих правилах. Ресурс объединяет в себе сетевые объекты (узел сети, сеть, группа сетевых объектов) и сервис.

Например, добавим объекта **resource**, описывающий сервер с доступом по протоколу SSH:

```
fnp4> directory add resource name=resource_ssh host=server service=service_ssh
FNPSH-I-007.02.30D3-Объект справочника добавлен (ресурс "resource_ssh")
```

Перепишем правило с номером 1, чтобы оно использовало объект **resource_ssh**:

```
fnp4> rule edit rule:1 dstresource=resource_ssh dstservice=none dstobject=none
Изменить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3047-Общее правило изменено (1)
```

После изменения правило осталось тождественно предыдущей версии по своему действию.

Объект vlan-group (группа VLAN) используется для хранения списка идентификаторов VLAN (vid) для использования в общих правилах. Объект **`vlan-group`** может быть указан либо непосредственно в общем правиле, либо в объектах **`host`** и **`net`**.

Добавим объект **`vlan-group`**:

```
fnp4> directory add vlan-group name=vlan1 vid=10,55,177
FNPSH-I-007.02.30D3-Объект справочника добавлен (группа VLAN "vlan1")
```

В качестве примера непосредственного использования группы VLAN в общем правиле добавим использование объекта **`vlan1`** в общем правиле номер 3:

```
fnp4> rule edit rule:3 vlan=vlan1
Изменить общее правило? (Y/N) [N]: FNPSH-I-007.02.3047-Общее правило изменено (3)
```

Теперь правилу 3 будут соответствовать только Ethernet-кадры с тэгом VLAN, содержащим один из идентификаторов: 10, 55, 177.

В качестве примера использования группы VLAN в общем правиле посредством сетевого объекта выполним команду:

```
fnp4> directory edit host name=host1 vlan=vlan1
Изменить объект справочника? (Y/N) [N]: y
FNPSH-I-007.02.30D4-Объект справочника изменен (узел сети "host1")
```

Теперь идентификаторы, заданные в объекте **`vlan1`**, будут учитываться во всех общих правилах, в которых используется объект **`host1`**. Ethernet-кадры от объекта **`host2`** не будут проверяться на наличие тэга VLAN с идентификатором из списка, определенного в **`vlan1`**, поскольку для объекта **`host2`** параметр **`vlan`** не устанавливался.

Объект time (интервал времени) служат для введения временных ограничений на действие общих правил, в которых они используются. По умолчанию общее правило действует без временных ограничений: с момента создания до момента удаления.

Добавим интервал времени:

```
fnp4> directory add time name=weekends wdays=sat,sun
FNPSH-I-007.02.30D3-Объект справочника добавлен (интервал времени "weekends")
```

Данный интервал времени задает время действия каждые субботу и воскресенье.

Добавим еще один интервал времени:

```
fnp4> directory add time name=worktime wdays=mon,tue,wed,thu,fri dtime=10:00:00-19:00:00
FNPSH-I-007.02.30D3-Объект справочника добавлен (интервал времени "worktime")
```

Данный интервал времени задает время действия в течение рабочей недели: каждый день с 10 до 19 часов.

К каждому общему правилу можно привязать один или несколько объектов **time**, например:

```
fnp4> rule add rule:4 action=accept srcobject=net1 ipproto=tcp dstport=80
time=weekends,worktime
FNPSH-I-007.02.3046-Общее правило добавлено (4)
```

Объект domain-group (группа доменных имен), как было сказано в начале данного раздела, может использоваться только в АР-правилах. При этом параметр **protocol** должен иметь значение **http** (протокол HTTP) или **domain** (**dns**) (протокол DNS). Объект **domain-group** хранит в себе список доменных имен и их фрагментов.

Добавим объект **domain-group**:

```
fnp4> directory add domain-group name=domain1 hostname=*.yandex.ru,*.google.com
FNPSH-I-007.02.30D3-Объект справочника добавлен (группа доменных имен "domain1")
```

Добавим АР-правило, использующее объект **domain1**:

```
fnp4> rule add ap:1 protocol=http domain-group=domain1 action=drop
FNPSH-I-007.02.3048-АР-правило добавлено (1)
```

В одном АР-правиле можно одновременно использовать объект **domain-group**, а также установить параметр правила **hostname**. В итоге, при проверке сообщения прикладного протокола (HTTP или DNS) на соответствие данному АР-правилу будут учитываться как доменные имена, определенные в используемом объекте **domain-group**, так и доменные имена, заданные через параметр **hostname**. В качестве примера добавим дополнительные доменные имена в АР-правило с номером 1:

```
fnp4> rule edit ap:1 protocol=http hostname=mail.ru,www.mail.ru
Изменить АР-правило? (Y/N) [N]: y
FNPSH-I-007.02.3049-АР-правило изменено (1)
```

Использование объектов **domain-group** в АР-правилах для протокола DNS полностью аналогично использованию для протокола HTTP:

```
fnp4> rule add ap:2 protocol=domain hostname=*.zzz.org,www.abcdef.edu domain-group=domain1
action=drop
FNPSH-I-007.02.3048-АР-правило добавлено (2)
```

Просмотр правил фильтрации в режиме пакетного фильтра может оказаться полезным для администратора при использовании в правилах фильтрации объектов справочника. Он позволяет администратору увидеть правила политики доступа в альтернативном представлении, отражающем то, как правила фильтрации используются в пакетном фильтре, т.е. без ссылок на объекты справочника, но со всеми необходимыми параметрами, скопированными из объектов.

В качестве примера рассмотрим текущую политику доступа, которая была сформирована в результате выполнения всех команд, приведенных в данном разделе.

Объекты справочника текущей политики доступа:

```
fnp4> directory show viewer=no
Справочник текущей политики:

time name=weekends months=any mdays=any wdays=sat,sun
time name=worktime months=any mdays=any wdays=mon,tue,wed,thu,fri dtime=10:00:00-19:00:00
domain-group name=domain1 hostname="*.yandex.ru,*.google.com"
vlan-group name=vlan1 vid=10,55,177
host name=host1 ip4=10.2.253.241 ip6=2001:db8::241 mac=00:0c:29:26:d0:5d vlan=vlan1
interface=0
host name=host2 ip4=10.2.253.243 ip6=2001:db8::243 mac=00:0c:29:26:d0:5f interface=0
host name=server ip4=10.2.253.242 ip6=2001:db8::242 mac=00:0c:29:b7:34:ec interface=1
net name=net1 ip4=10.2.253.240/255.255.255.248 comment="сеть 241-247"
net-group name=net_group_1 host=host1,host2 comment="host1 и host2"
service name=service_ssh protocol=tcp port=22 comment=ssh
service name=service_icmp4 protocol=icmp
service name=service_https protocol=tcp port=443 comment=https
resource name=resource_ssh host=server service=service_ssh
```

Правила фильтрации текущей политики доступа, использующие объекты справочника:

```
fnp4> rule show viewer=no
Правила текущей политики:

rule:0 action=drop
rule:1 action=accept comment="ssh и icmp" srcobject=host1,host2 dstresource=resource_ssh
apr=no
rule:2 action=accept comment="доступ по HTTPs" srcobject=net_group_1
dstservice=service_https apr=no
rule:3 action=accept srcobject=net1 dstip4=192.168.1.1 vlan=vlan1 apr=no
rule:4 action=accept srcobject=net1 dstport=80 ipproto=tcp time=weekends,worktime apr=no
ap:0 action=drop
ap:1 action=drop protocol=http hostname="mail.ru,www.mail.ru" domain-group=domain1
ap:2 action=drop protocol=domain hostname="*.zzz.org,www.abcdef.edu" domain-group=domain1
```

Просмотр правил фильтрации текущей политики доступа **в режиме пакетного фильтра**:

```
fnp4> rule show viewer=no format=filter
Правила текущей политики:

rule:0:0 action=drop
rule:1:0 action=accept srcif=0 srcmac=00:0c:29:26:d0:5d srcip4=10.2.253.241
srcip6=2001:db8::241 dstif=1 dstmac=00:0c:29:b7:34:ec dstip4=10.2.253.242
dstip6=2001:db8::242 dstport=22 ipproto=tcp vlan=10,55,177 apr=no
rule:1:1 action=accept srcif=0 srcmac=00:0c:29:26:d0:5f srcip4=10.2.253.243
srcip6=2001:db8::243 dstif=1 dstmac=00:0c:29:b7:34:ec dstip4=10.2.253.242
dstip6=2001:db8::242 dstport=22 ipproto=tcp apr=no
rule:2:0 action=accept srcif=0 srcmac=00:0c:29:26:d0:5d srcip4=10.2.253.241
srcip6=2001:db8::241 dstport=443 ipproto=tcp vlan=10,55,177 apr=no
rule:2:1 action=accept srcif=0 srcmac=00:0c:29:26:d0:5f srcip4=10.2.253.243
srcip6=2001:db8::243 dstport=443 ipproto=tcp apr=no
rule:3:0 action=accept version=4 srcip4=10.2.253.240/255.255.255.248 dstip4=192.168.1.1
vlan=10,55,177 apr=no
rule:4:0 action=accept version=4 srcip4=10.2.253.240/255.255.255.248 dstport=80 ipproto=tcp
time="months=any mdays=any wdays=sat,sun;months=any mdays=any wdays=mon,tue,wed,thu,fri
time=10:00:00-19:00:00" apr=no
ap:0 action=drop
ap:1 action=drop protocol=http hostname="mail.ru,www.mail.ru,*.yandex.ru,*.google.com"
ap:2 action=drop protocol=domain
hostname="*.zzz.org,www.abcdef.edu,*.yandex.ru,*.google.com"
```

Просмотр правил фильтрации **в режиме пакетного фильтра** доступен только через командный интерфейс администратора МЭ ССПТ-4А1

Можно заметить, что число правил, выводимых в режиме пакетного фильтра, больше, чем в представлении с объектами справочника. Это является результатом работы алгоритма по преобразованию правил, использующих сетевые объекты (**`host`**, **`net`**, **`net-group`**) в альтернативное представление для применения пакетным фильтром.

3.9. HTTP-посредник МЭ ССПТ-4А1

HTTP-посредник МЭ ССПТ-4А1 представляет собой прокси-сервер для протоколов HTTP и HTTPs.

HTTP-посредник позволяет клиентам корпоративной сети выполнять косвенные запросы к WEB-серверам. Сначала клиент подключается к HTTP-посреднику и запрашивает WEB-страницу, расположенную на WEB-сервере в корпоративной сети или в сети Интернет. Затем HTTP-посредник подключается к указанному WEB-серверу (открывает новое соединение, в котором выступает клиентом), получает от него WEB-страницу и возвращает ее клиенту в рамках соединения, открытого клиентом из корпоративной сети. HTTP-посредник предоставляет возможность изменять ответ WEB-сервера в определённых целях. Эта функция подробно рассмотрена далее в данном разделе. HTTP-посредник позволяет защищать компьютер клиента от некоторых сетевых атак и помогает сохранять анонимность клиента.

При конфигурации по умолчанию HTTP-посредник обеспечивает доступ клиента ко всем WEB-страницам, доступным при прямом подключении клиента, и не модифицирует ответы WEB-серверов (HTTP-ответы).

Основные возможности HTTP-посредника МЭ ССПТ-4А1:

- блокировка доступа клиентов к определенным WEB-страницам (по доменным именам);
- удаление сценариев JavaScript, VBScript для определенных WEB-страниц (с заданными доменным именами);
- ограничение доступа клиентов к HTTP-посреднику на основе списка доступа (ACL);

HTTP-посредник МЭ ССПТ-4А1 может использоваться в двух схемах подключения:

- с выключенным NAT (МЭ ССПТ-4А1 работает в прозрачном режиме, IP-адреса в пакетах не изменяются);
- с включенным NAT (IP-адрес источника пакета, которым является IP-адрес HTTP-посредника, меняется перед отправкой пакета с внешнего интерфейса NAT).

3.9.1. Использование HTTP-посредника без NAT

Схема подключения для использования HTTP-посредника, когда функция NAT выключена в конфигурации МЭ ССПТ-4А1 приведена на рисунке 3.14, стр. 160. Пояснения к схеме:

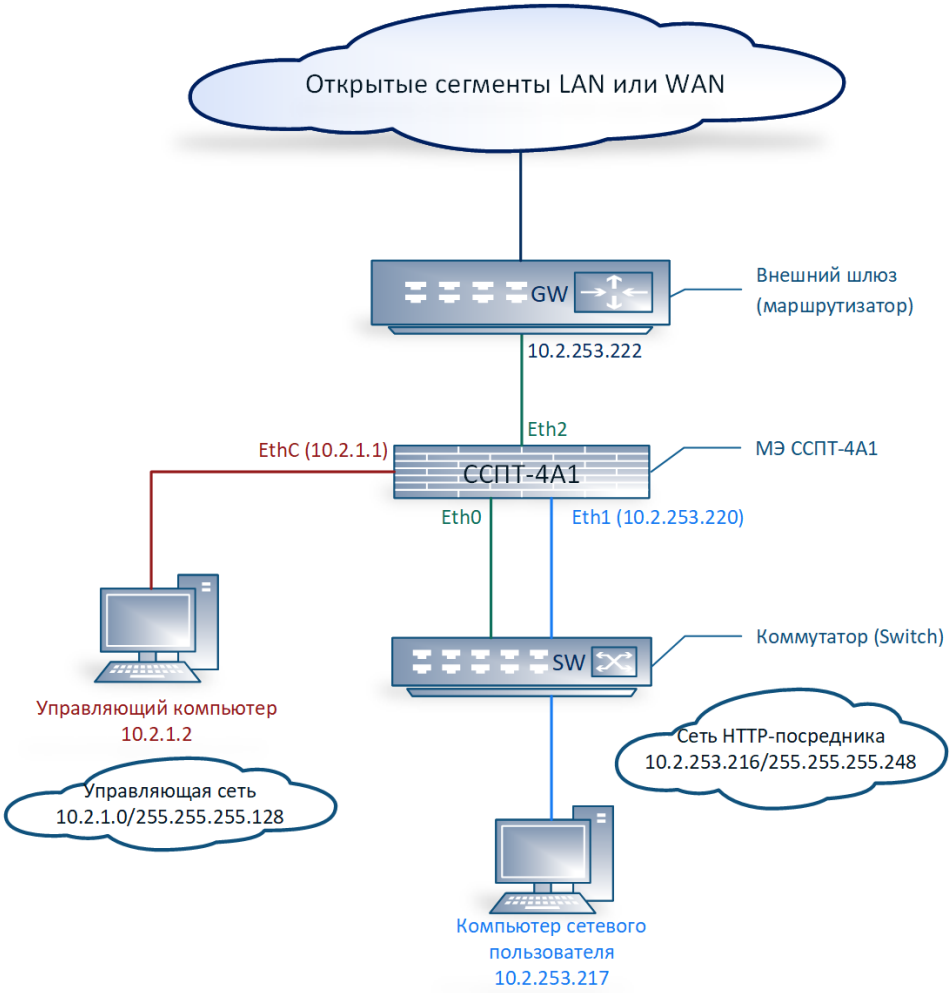


Рисунок 3.14: HTTP-посредник. Схема подключения без использования NAT

- GW – шлюз по умолчанию, используемый HTTP-посредником;
- SW – коммутатор;
- МЭ – устройство МЭ ССПТ-4А1 (функция NAT выключена):
  - ✔ Eth0 — интерфейс, на который поступают HTTP-запросы, адресованные WEB-серверу, от имени HTTP-посредника, и с которого отправляются ответы от WEB-сервера, адресованные HTTP-посреднику (соединен с интерфейсом HTTP-посредника и клиентом через коммутатор SW);
  - ✔ Eth1 – интерфейс HTTP-посредника;

✔ Eth2 – интерфейс для взаимодействия с WEB-сервером в сети Интернет, посредством шлюза (GW).

Конфигурация клиента, работающего через HTTP-посредник

Для использования HTTP-посредника МЭ ССПТ-4А1 каждый клиентский ПК должен быть настроен в соответствии со следующим алгоритмом, в котором IP-адреса соответствуют схеме на рисунке 3.14, стр. 160Ошибка: источник перекрёстной ссылки не найден:

- на ПК клиента должны быть установлены IP-адрес и адрес шлюза по умолчанию, соответствующие схеме подключения. Для представленной схемы подключения:
  - ✔ IP-адрес 10.2.253.217;
  - ✔ IP-адрес шлюза по умолчанию 10.2.253.222;
- должны быть заданы IP-адреса DNS-серверов;
- в настройках WEB-браузера клиента должны быть заданы IP-адрес и TCP-порт HTTP-посредника для протоколов HTTP и HTTPs (HTTP over SSL), соответствующие настройкам HTTP-посредника МЭ ССПТ-4А1:
  - ✔ IP-адрес HTTP-посредника: 10.2.253.220;
  - ✔ TCP-порт HTTP-посредника: 8118.

Конфигурация МЭ ССПТ-4А1 для использования HTTP-посредника должна включать в себя следующие этапы:

- установка IP-адреса EthC (если не установлен или требует изменения);
- добавление статического маршрута для связности EthC и узлов вне управляющей сети (необязательный этап, определяется потребностями администрирования);
- установка DNS-серверов для разрешения (resolve) доменных имен WEB-страниц, запрашиваемых клиентами;
- добавление общих правил фильтрации, обеспечивающих передачу ARP-трафика между интерфейсами Eth0 и Eth2;
- добавление общих правил фильтрации, обеспечивающих передачу трафика между интерфейсами Eth0 и Eth2;
- настройка HTTP-посредника МЭ ССПТ-4А1:
  - ✔ IP-адрес на интерфейсе HTTP-посредника;
  - ✔ TCP-порт HTTP-посредника;
  - ✔ фильтрующий интерфейс МЭ, используемый в качестве интерфейса HTTP-посредника;
- включение HTTP-посредника;
- добавление маршрута по умолчанию на интерфейсе HTTP-посредника.

В зависимости от требований политик доступа дополнительные этапы конфигурации HTTP-посредника могут включать:

- добавление PROXY-правил, управляющих работой HTTP-посредника (необязательный этап, определяется требованиями политики доступа);
- создание ACL (списка доступа) для ограничения доступа к HTTP-посреднику.

Поскольку указанные дополнительные этапы конфигурации HTTP-посредника не зависят от схемы подключения (без использования NAT или с использованием NAT), то они рассматриваются отдельно в разделах 3.9.3, стр. 169 и 3.9.4, стр. 170 соответственно.

Ниже рассматривается пример настройки МЭ ССПТ-4А1 для использования HTTP-посредника через командный интерфейс в соответствии с алгоритмом, описанным выше.

Настоятельно рекомендуется использовать **HTTP-посредник** при включенном **механизме контроля сессий** (по умолчанию механизм контроля сессий включен).

Во избежание потери связности управляющего ПК администратора с МЭ ССПТ-4А1 следующие действия рекомендуется выполнять из локальной консоли:

- установка IP-адреса EthC;
- добавление статического маршрута для связности EthC и узлов в сети Интернет.

Установка IP-адреса EthC

```
fnp4> interface control set address=10.2.1.1/255.255.255.128
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (10.2.1.1)
FNPSH-I-007.02.3003-Завершение работы администратора (admin)
```

В примере команда была выполнена удаленно, поэтому выводится предупреждение и принудительно завершается сеанс работы администратора.

Добавление статического маршрута для связности EthC и некоторой IP-сети

На рис. 3.14, стр. 160 сетевой интерфейс УК непосредственно подключен к управляющему интерфейсу (EthC) МЭ, поэтому добавления статического маршрута (для обеспечения связности УК и EthC) не требуется. Если бы УК располагался вне управляющей сети МЭ, то потребовалось бы добавление статического маршрута посредством выполнения команды **`system route add`**.

Установка DNS-серверов для разрешения (resolve) доменных имен WEB-страниц, запрашиваемых клиентами

```
fnp4> system dns set address=10.2.1.53,10.2.1.54
Установить список DNS-серверов? (Y/N) [N]: y
FNPSH-I-007.02.312D-Список DNS-серверов установлен
```

DNS-серверы не указаны на схеме, подразумевается, что они доступны HTTP-посреднику.

Добавление общих правил фильтрации, обеспечивающих передачу ARP-трафика между интерфейсами Eth0 и Eth2. В том случае, если в текущей политике доступа глобальное общее правило запрещает пропуск пакетов (действие “drop” или “deny”), должны быть добавлены два правила, обеспечивающие передачу ARP-трафика между интерфейсами Eth0 и Eth2 (каждое правило для ARP-пакетов действует только в одном направлении):

```
fnp4> rule add rule:1 action=accept log=enable comment=ARP_LAN->WAN frame=eth2
ethproto=0x0806 srcif=0 dstif=2
FNPSH-I-007.02.3046-Общее правило добавлено (1)
fnp4> rule add rule:2 action=accept log=enable comment=ARP_WAN->LAN frame=eth2
ethproto=0x0806 srcif=2 dstif=0
FNPSH-I-007.02.3046-Общее правило добавлено (2)
```

Добавление общих правил фильтрации, обеспечивающих передачу трафика между интерфейсами Eth0 и Eth2

```
fnp4> rule add rule:10 action=accept srcif=0 dstif=2 comment=proxy
FNPSH-I-007.02.3046-Общее правило добавлено (10)
```

Правило, добавленное выше, обеспечивает передачу любого трафика с Eth0 на Eth2 и ответных пакетов от серверов для TCP и UDP трафика (режим управления сессиями). Возможно, конкретная политика доступа потребует ограничений на трафик, передаваемый между интерфейсами Eth0 и Eth2, тогда потребуется добавление другого общего правила, отвечающего требованиям политики доступа.

Настройка параметров HTTP-посредника

```
fnp4> system proxy set interface=1 address=10.2.253.220/255.255.255.248
FNPSH-I-007.02.3112-Пакетный фильтр перезапущен
FNPSH-I-007.02.3134-Параметры HTTP-посредника установлены
```

Команда выше устанавливает все необходимые параметры HTTP-посредника. HTTP-посредник может быть включен одновременно с установкой его параметров в случае указания в команде выше **`state=enable`**, но в данном разделе включение HTTP-посредника выполняется за счет выполнения отдельной команды (оба варианта допустимы).

Включение HTTP-посредника

```
fnp4> system proxy set state=enable
FNPSH-I-007.02.3112-Пакетный фильтр перезапущен
FNPSH-I-007.02.3132-HTTP-посредник включен
```

Добавление маршрута по умолчанию

```
fnp4> system route add dst-address=0.0.0.0 gateway=10.2.253.222
FNPSH-I-007.02.312F-Маршрут добавлен
```

В соответствии со схемой маршрут по умолчанию должен использовать адрес шлюза 10.2.253.222, чтобы HTTP-запросы от HTTP-посредника достигали сети Интернет.

Установка TCP-порта HTTP-посредника необязательна, если предполагается использовать значение TCP-порта HTTP-посредника по умолчанию: **8118**.

Все маршруты должны добавляться после установки IP-адреса на соответствующем сетевом интерфейсе МЭ ССПТ-4А1.
Следует учитывать, что IP-адрес на интерфейсе HTTP-посредника устанавливается только при включении HTTP-посредника, либо при изменении IP-адреса HTTP-посредника, когда он находится во включенном состоянии.

3.9.2. Использование HTTP-посредника совместно с NAT

Схема подключения для использования HTTP-посредника, когда функция NAT включена в конфигурации МЭ ССПТ-4А1, приведена на рисунке 3.15, стр. 164. Пояснения к схеме:

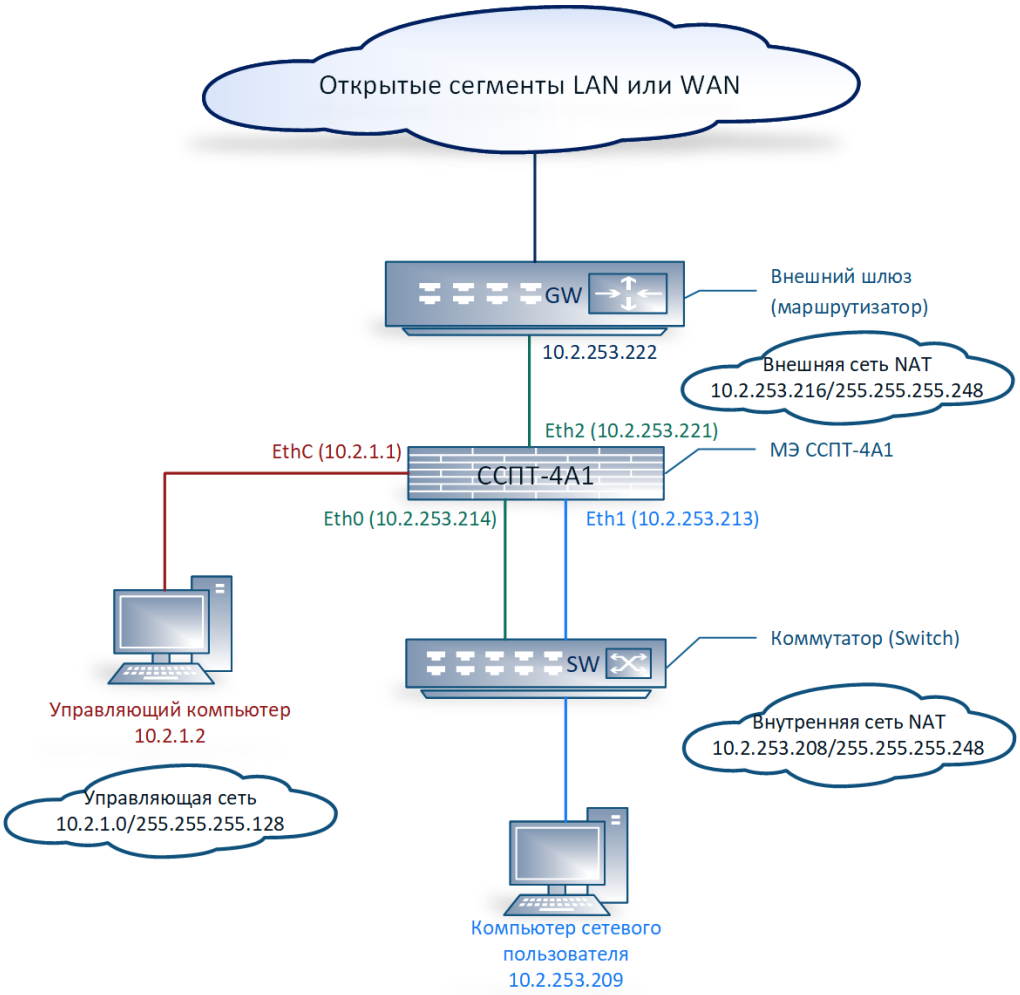


Рисунок 3.15: HTTP-посредник. Схема подключения с использованием NAT

- GW – шлюз по умолчанию, используемый HTTP-посредником;
- SW – коммутатор;

- устройство МЭ ССПТ-4А1 (функция NAT включена):
  - ✔ Eth1 – интерфейс HTTP-посредника: не входит в состав контейнера NAT, но имеет IP-адрес, принадлежащий внутренней сети NAT. Внутрення сеть NAT на схеме имеет IP-адрес 10.2.253.208/29, ей принадлежат IP-адреса: 10.2.253.214 (Eth0), 10.2.253.213 (Eth1) и 10.2.253.209 (IP-адрес клиента);
  - ✔ Eth0 – внутренний интерфейс NA, на который поступают HTTP-запросы, адресованные WEB-серверам от имени HTTP-посредника, и с которого отправляются ответы от WEB-серверов, адресованные HTTP-посреднику;
  - ✔ Eth2 – внешний интерфейс NAT, с которого отправляются HTTP-запросы WEB-серверам от имени внешнего IP-адреса NAT и на который принимаются HTTP-ответы от WEB-серверов из Интернет.

Конфигурация клиента, работающего через HTTP-посредник. Для использования HTTP-посредника МЭ ССПТ-4А1 каждый клиентский ПК должен быть настроен в соответствии со следующим алгоритмом, в котором IP-адреса соответствуют схеме на рисунке 3.15, стр. 164:

- на ПК клиента должны быть установлены IP-адрес и адрес шлюза по умолчанию, соответствующие схеме подключения:
  - ✔ IP-адрес 10.2.253.209;
  - ✔ IP-адрес шлюза по умолчанию 10.2.253.214 (IP-адрес внутреннего интерфейса NAT);
- должны быть заданы IP-адреса DNS-серверов;
- в настройках WEB-браузера клиента должны быть заданы IP-адрес и TCP-порт HTTP-посредника для протоколов HTTP и HTTPs (HTTP over SSL), соответствующие настройкам HTTP-посредника МЭ ССПТ-4А1:
  - ✔ IP-адрес HTTP-посредника: 10.2.253.213;
  - ✔ TCP-порт HTTP-посредника: 8118.

Конфигурация МЭ ССПТ-4А1 для использования HTTP-посредника должна включать в себя следующие этапы:

- установка IP-адреса EthC (если не установлен или требует изменения);
- добавление статического маршрута для связности EthC и узлов вне управляющей сети (необязательный этап, определяется потребностями администрирования);
- установка DNS-серверов для разрешения (resolve) доменных имен WEB-страниц, запрашиваемых клиентами;
- добавление общих правил фильтрации, обеспечивающих передачу ARP-трафика между интерфейсами Eth0 и Eth2;

- добавление общих правил фильтрации, обеспечивающих передачу трафика между интерфейсами Eth0 и Eth2;
- настройка NAT;
- настройка HTTP-посредника МЭ ССПТ-4А1:
  - ✔ IP-адрес на интерфейсе HTTP-посредника;
  - ✔ TCP-порт HTTP-посредника;
  - ✔ фильтрующий интерфейс МЭ, используемый в качестве интерфейса HTTP-посредника;
- включение HTTP-посредника;
- добавление маршрута по умолчанию на интерфейсе HTTP-посредника.

В зависимости от требований политики доступа дополнительные этапы конфигурации HTTP-посредника могут включать:

- добавление PROXY-правил, управляющих работой HTTP-посредника;
- создание ACL (списка доступа) для ограничения доступа к HTTP-посреднику.

Поскольку указанные дополнительные этапы конфигурации HTTP-посредника не зависят от схемы подключения (без использования NAT или с использованием NAT), то они рассматриваются отдельно в разделах: 3.9.3, стр. 169 и 3.9.4, стр. 170 соответственно.

Ниже рассматривается пример настройки МЭ ССПТ-4А1 через КИА для использования HTTP-посредника в соответствии с алгоритмом, описанным выше.

Во избежании потери связности управляющего ПК администратора с МЭ ССПТ-4А1 следующие действия рекомендуется выполнять с локальной консоли:
- Установку IP-адреса EthC;
- Добавление статического маршрута для связности EthC и узлов в сети Интернет.

Установка IP-адреса EthC

```
fnp4> interface control set address=10.2.1.1/255.255.255.128
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (10.2.1.1)
FNPSH-I-007.02.3003-Завершение работы администратора (admin)
```

В примере команда была выполнена удаленно, поэтому выводится предупреждение и принудительно завершается сеанс работы администратора.

Добавление статического маршрута для связности EthC и некоторой IP-сети

На рис. 3.15, стр. 164 сетевой интерфейс УК непосредственно подключен к управляющему интерфейсу (EthC) МЭ, поэтому добавления статического маршрута (для обеспечения связности УК и EthC) не требуется. Если бы УК располагался вне управляющей сети МЭ, то потребовалось бы добавление статического маршрута посредством выполнения команды **`system route add`**.

Установка DNS-серверов для разрешения доменных имен WEB-страниц, запрашиваемых клиентами

```
fnp4> system dns set address=10.2.1.53,10.2.1.54
Установить список DNS-серверов? (Y/N) [N]: y
FNPSH-I-007.02.312D-Список DNS-серверов установлен
```

DNS-серверы не показаны на схеме, подразумевается, что они доступны через интерфейс HTTP-посредника.

Добавление общих правил фильтрации, обеспечивающих передачу ARP-трафика между интерфейсами Eth0 и Eth2. В том случае, если в текущей политике доступа глобальное общее правило запрещает пропуск пакетов (действие “drop” или “deny”), должны быть добавлены два правила, обеспечивающие передачу ARP-трафика между интерфейсами Eth0 и Eth2 (каждое правило для ARP-пакетов действует только в одном направлении):

```
fnp4> rule add rule:1 action=accept log=enable comment=ARP_LAN->WAN frame=eth2
ethproto=0x0806 srcif=0 dstif=2
FNPSH-I-007.02.3046-Общее правило добавлено (1)
fnp4> rule add rule:2 action=accept log=enable comment=ARP_WAN->LAN frame=eth2
ethproto=0x0806 srcif=2 dstif=0
FNPSH-I-007.02.3046-Общее правило добавлено (2)
```

Добавление общего правила фильтрации, обеспечивающего передачу трафика между интерфейсами Eth0 и Eth2

```
fnp4> rule add rule:10 action=accept srcif=0 dstif=2 comment=proxy
FNPSH-I-007.02.3046-Общее правило добавлено (10)
```

Правило, добавленное выше, обеспечивает передачу TCP и UDP трафика между интерфейсами Eth0 на Eth2. Возможно, конкретная политика доступа потребует ограничений на трафик, передаваемый между интерфейсами Eth0 и Eth2, тогда потребуется добавление других общих правил, отвечающих требованиям политики доступа.

Настройка NAT. Настройка функции трансляции сетевых адресов (NAT) подробно рассматривается в разделе 3.2.3, стр. 87. Здесь приводится простейший пример настройки NAT для совместного использования с HTTP-посредником в соответствии со схемой подключения, представленной на рис. 3.15, стр. 164. Настройка NAT включает в себя следующие шаги:

- добавление контейнера NAT;
- добавление в контейнер и настройка внутреннего интерфейса NAT;
- добавление в контейнер и настройка внешнего интерфейса NAT;
- добавление в контейнер правила трансляции для замены IP-адресов узлов внутренней сети NAT (10.2.253.208/29) на IP-адрес внешнего интерфейса NAT (10.2.253.221);
- добавление маршрута NAT по умолчанию для того, чтобы пакеты из внутренней сети NAT достигали WEB-серверов из сети Интернет;
- включение функции NAT.

Добавление контейнера NAT

```
fnp4> nat case add name=c1
FNPSH-I-007.02.3113-Контейнер NAT добавлен
```

Добавление в контейнер и настройка внутреннего интерфейса NAT

```
fnp4> nat private add case=c1 name=prv interface=0 address=10.2.253.214/255.255.255.248
FNPSH-I-007.02.3115-Интерфейс NAT добавлен
```

Добавление в контейнер и настройка внешнего интерфейса NAT

```
fnp4> nat public add case=c1 name=pub interface=2 address=10.2.253.221/255.255.255.248
FNPSH-I-007.02.3115-Интерфейс NAT добавлен
```

Добавление в контейнер правила трансляции для замены IP-адресов узлов внутренней сети NAT (10.2.253.208/29) на IP-адрес внешнего интерфейса NAT (10.2.253.221)

```
fnp4> nat translate add case=c1 number=1 prv-address=10.2.253.208/255.255.255.248 pub-
address=10.2.253.221 interface=pub
FNPSH-I-007.02.3118-Правило трансляции NAT добавлено
```

Добавление маршрута NAT по умолчанию для того, чтобы пакеты из внутренней сети NAT достигали WEB-серверов из сети Интернет

```
fnp4> nat route add case=c1 dst-address=0.0.0.0 gateway=10.2.253.222
FNPSH-I-007.02.311E-Маршрут NAT добавлен
```

Включение функции NAT

```
fnp4> nat enable
FNPSH-I-007.02.3027-NAT включен
```

Настройка HTTP-посредника МЭ ССПТ-4А1

```
fnp4> system proxy set interface=1 address=10.2.253.213/255.255.255.248
FNPSH-I-007.02.3112-Пакетный фильтр перезапущен
FNPSH-I-007.02.3134-Параметры HTTP-посредника установлены
```

Команда выше устанавливает все необходимые параметры HTTP-посредника. HTTP-посредник может быть включен одновременно с установкой его параметров в случае указания в команде выше: **`state=enable`**, но в данном разделе включение HTTP-посредника выполняется за счет выполнения отдельной команды (оба варианта допустимы).

> Установка TCP-порта HTTP-посредника необязательна, если предполагается использовать значение TCP-порта HTTP-посредника по умолчанию: **8118**.

Включение HTTP-посредника

```
fnp4> system proxy set state=enable
FNPSH-I-007.02.3112-Пакетный фильтр перезапущен
FNPSH-I-007.02.3132-HTTP-посредник включен
```

Добавление маршрута по умолчанию на интерфейсе HTTP-посредника

```
fnp4> system route add dst-address=0.0.0.0 gateway=10.2.253.214
FNPSH-I-007.02.312F-Маршрут добавлен
```

В соответствии со схемой подключения (рис. 3.15, стр. 164) маршрут по умолчанию должен использовать адрес шлюза 10.2.253.214 (IP-адрес внутреннего интерфейса NAT), чтобы HTTP-запросы от HTTP-посредника отправлялись на внутренний интерфейс NAT, и далее посредством правила трансляции NAT отправлялись с внешнего интерфейса NAT.

Все маршруты должны добавляться после установки IP-адреса на соответствующем сетевом интерфейсе МЭ ССПТ-4А1.

Следует учитывать, что IP-адрес на интерфейсе HTTP-посредника, устанавливается только при включении HTTP-посредника, либо при изменении IP-адреса HTTP-посредника, когда он находится во включенном состоянии.

При совместном использовании функций **HTTP-посредника** и **NAT** не допускается использование одного и того же фильтрующего интерфейса в качестве интерфейса HTTP-посредника и в составе интерфейса внутреннего либо внешнего интерфейса NAT.

При совместном использовании функций **HTTP-посредника** и **зеркалирования сетевых интерфейсов** не допускается использование одного и того же фильтрующего интерфейса в качестве интерфейса HTTP-посредника и в качестве зеркалируемого либо зеркалирующего интерфейса.

При совместном использовании функций **HTTP-посредника** и **агрегировании портов управляющего интерфейса** не допускается использование одного и того же фильтрующего интерфейса в качестве интерфейса HTTP-посредника и в качестве интерфейса агрегата.

3.9.3. Использование PROXY-правил

Использование PROXY-правил позволяет решать следующие задачи:

- запрет доступа к WEB-страницам с определенными доменными именами;
- запрет выполнения сценариев JavaScript и VBScript на компьютерах клиентов HTTP-посредника за счет удаления соответствующих сценариев HTTP-посредником из WEB-страниц.

HTTP-посредник обеспечивает запрет выполнения сценариев **JavaScript** и **VBScript** только для WEB-страниц, доступ к которым осуществляется по протоколу **HTTP**.
Для WEB-страниц, доступ к которым осуществляется по протоколу **HTTPs**, запрет выполнения сценариев **JavaScript** и **VBScript** невозможен.

Синтаксис PROXY-правил представлен в приложении Д.5, стр. 537.

Ниже рассматриваются примеры типовых задач, решаемых с помощью PROXY-правил.

Задача: запретить сценарии JavaScript на WEB-страницах со следующими доменными именами:

- доменное имя "заканчивается" доменом **`qwerty12345.org`**, например: **`abc.qwerty12345.org`**, **`def.qwerty12345.org`** и т. д.;
- доменное имя – **`xyz123.net`**.

Решение:

```
fnp4> rule add proxy:1 action=edit filter=javascript hostname=.qwerty12345.org,xyz123.net
FNPSH-I-007.02.3135-PROXY-правило добавлено (1)
```

В добавленном PROXY-правиле:

- **`action=edit`** – действие PROXY-правила: изменять HTTP-сообщения в соответствии со значением параметра filter;
- **`filter=javascript`** – фильтр, применяемый для действия **`edit`**: удалить с WEB-страницы сценарии JavasScript;
- **`hostname`** – список доменных имен и их фрагментов, для которых будет применяться данное правило, т.е. из WEB-страниц, URL которых включает данные доменные имена, HTTP-посредником будут удалены JavaScript.

Если полное доменное имя узла сети (FQDN), доступ к которому должен осуществляться в соответствии с некоторым PROXY-правилом, неизвестно, или же PROXY-правило должно быть применено к множеству доменных имен (FQDN), с общим “окончанием”, то рекомендуется в параметре **hostname** указывать это общее “окончание” множества доменных имен, предваренное символом “точка”.

Например, в случае **hostname=.qwerty12345.org** PROXY-правило будет применено при обращении к следующим доменным именам:

- news.qwerty12345.org;
- mail.qwerty12345.org;
- dl.qwerty12345.org;
- и т.д.

Задача: запретить доступ клиентам к WEB-страницам, доменные имена которых "заканчиваются" на .aaabbbccc-xyz.com.

Решение:

```
fnp4> rule add proxy:2 action=deny hostname=.aaabbbccc-xyz.com
FNPSH-I-007.02.3135-PROXY-правило добавлено (2)
```

Задача: разрешить доступ клиентам к WEB-страницам с доменным именем news.aaabbbccc-xyz.com, т.е. сделать исключение из ранее добавленного PROXY-правила с номером 2.

Решение:

```
fnp4> rule add proxy:1 action=accept hostname=news.aaabbbccc-xyz.com
FNPSH-I-007.02.3135-PROXY-правило добавлено (1)
```

3.9.4. Использование списка доступа (ACL) для ограничения доступа к HTTP-посреднику

Список доступа (ACL) для ограничения доступа клиентов к HTTP-посреднику относится к категории «белый список» («white list»), т. е. в нем указываются IP-адреса клиентов, которым разрешена работа через HTTP-посредника.

По умолчанию ACL пустой, и работа через HTTP-посредник разрешена всем клиентам.

Рассмотрим типовую задачу по ограничению доступа к к HTTP-посреднику.

Задача: требуется ограничить доступ клиентов к HTTP-посреднику таким образом, чтобы доступ имели только клиенты с IP-адресами из подсети: 10.2.253.216/255.255.255.248

Решение:

```
fnp4> system proxy acl add address=10.2.253.216/255.255.255.248
FNPSH-I-007.02.313A-Новая запись добавлена в список доступа HTTP-посредника
```

Таким образом, клиенты с IP-адресами, не принадлежащими сети 10.2.253.216/255.255.255.248, не будут иметь возможности работать (иметь доступ к WEB-страницам) через HTTP-посредник.

3.10. Управление администраторами

По умолчанию в базе данных администраторов существует единственная учетная запись `admin` с привилегиями `admin`. Учетная запись `admin` – единственная, которой допускается:

- добавлять учетные записи администраторов;
- удалять учетные записи администраторов;
- изменять параметры других учетных записей администраторов:
  - ✔ пароль учетной записи;
  - ✔ привилегии учетной записи;
  - ✔ состояние учетной записи (включено/выключено).

Рассмотрим пример добавления учетной записи:

```
fnp4> user add name=reader
Новый пароль:
Новый пароль повторно:
FNPSH-I-007.02.3006-Администратор добавлен (reader)
```

По умолчанию учетная запись добавляется с привилегиями **`read`** и с состоянием **“включено”**. В этом можно убедиться, выполнив команду **`user list`** вывода всех существующих на устройстве учетных записей администраторов:

```
fnp4> user list
Всего администраторов: 2

Администратор Привилегии Состояние
admin         admin      включено
reader        read       включено
```

Все параметры учетной записи можно задать явно при добавлении:

```
fnp4> user add name=writer privilege=full state=enable
Новый пароль:
Новый пароль повторно:
FNPSH-I-007.02.3006-Администратор добавлен (writer)
```

Администраторы с привилегиями **`read`** и **`full`** могут менять собственные пароли, например:

```
Имя администратора: reader
Пароль:

FNPSH-I-007.02.3001-Успешная авторизация администратора (read)
fnp4> user password
Старый пароль:
Новый пароль:
Новый пароль повторно:
FNPSH-I-007.02.300A-Пароль администратора изменен (reader)
```

Привилегии **admin** необходимы для выполнения следующих команд:

- user add
- user edit
- user delete
- user password (в случае смены пароля администратору admin либо любому другому администратору)
- system snmp password
- system fnpsh password
- system default

Для выполнения всех остальных команд достаточно привилегий **full**.

Привилегии **read** позволяют:

- изменять пароль собственной учетной записи;
- просматривать параметры конфигураций и политик доступа (текущих и дополнительных);
- выгружать дополнительные конфигурации с МЭ ССПТ-4А1 на управляющий компьютер администратора;
- выгружать текущую и дополнительные политики доступа с МЭ ССПТ-4А1 на управляющий компьютер администратора.

При совместном использовании МЭ ССПТ-4А1 несколькими администраторами может возникать ситуация, когда администратор с привилегиями **`full`** или **`admin`** не использует МЭ, но сеанс администратора продолжает существовать до истечения тайм-аута неактивности администратора. В этом случае другой администратор с надлежащими привилегиями не может администрировать МЭ ССПТ-4А1 до тех пор, пока по тайм-ауту не завершится сеанс работы первого администратора. Команда **`user clear`** позволяет принудительно завершить все сеансы администраторов, кроме данного, тем самым позволяя данному администратору получить эффективные привилегии **`admin`** или **`full`** после выхода и повторной авторизации.

Проиллюстрируем сказанное примером:

```
Имя администратора: writer
Пароль:

FNPSH-W-007.02.2002-Вход администратора с ограниченными привилегиями (read)
fnp4> user show
Активных администраторов: 2    Системное время: 30.05.2017 18:36:46 (MSK)

Администратор Время входа                        Откуда            Привилегии Неактивность
admin         30.05.2017 18:35:49 UTC+0300 (MSK) WEB:10.98.100.250 admin      56c
writer        30.05.2017 18:36:32 UTC+0300 (MSK) CLI:10.98.100.250 read       14c
fnp4> user clear
```

```
Удалить все сессии работы администраторов кроме данной? (Y/N) [N]: y
FNPSH-I-007.02.3109-Сеансы работы администраторов сброшены
fnp4> user show
Активных администраторов: 1    Системное время: 30.05.2017 18:36:59 (MSK)

Администратор Время входа                        Откуда            Привилегии Неактивность
writer        30.05.2017 18:36:32 UTC+0300 (MSK) CLI:10.98.100.250 read       3c
fnp4> exit
FNPSH-I-007.02.3003-Завершение работы администратора (writer)
```

Администратор **writer** получил эффективные привилегии **read** вместо привилегий **full** из его учетной записи, поскольку на момент авторизации уже существовал сеанс администратора **admin** с эффективными привилегиями **admin**, об этом свидетельствует вывод команды **user show**, отображающий список активных администраторов МЭ ССПТ-4А1.

Далее администратор **writer** выполнил команду **user clear**, тем самым принудительно завершив сеанс работы администратора **admin**.

После этого администратор **writer** снова авторизовался и на этот раз получил эффективные привилегии **full**, соответствующие его учетной записи, т. к. эффективные привилегии **full** и **admin** на этот раз не были заняты другими администраторами.

3.11. Управление регистрацией

В МЭ ССПТ-4А1 реализована подсистема регистрации, обеспечивающая обработку запросов на регистрацию и хранение регистрационной информации следующих категорий:

- события;
- трафик;
- системные сообщения.

Также МЭ ССПТ-4А1 предоставляет возможность выгрузки на удаленный FTP либо SYSLOG-сервер регистрационной информации следующих категорий:

- события;
- трафик.

Вывод параметров подсистемы регистрации доступен по команде **log show,** например:

```
fnp4> log show
Регистрация пакетов:                        выключено
Регистрация пакетов, отброшенных сессиями: выключено
Регистрация пакетов, отброшенных NAT:      выключено
Регистрация синхронизации по NTP           выключено
Выгрузка файлов регистрации по FTP:        выключено
    IP-адрес FTP-сервера:                  не определено
    Порт FTP-сервера:                      21
    Путь на FTP-сервере:                   не определено
    Имя пользователя:                      не определено
Выгрузка записей регистрации по SYSLOG:    выключено
    IP-адрес SYSLOG-сервера:               не определено
    Порт SYSLOG-сервера:                   514
    Выгружаемые записи:                    события
```

По умолчанию регистрация пакетов, к которым применены правила фильтрации, не выполняется. Также по умолчанию не регистрируются пакеты, отброшенные режимом управления сессиями и функцией NAT.

3.11.1. Регистрация событий

Событие отражает факт изменения состояния, конфигурационных параметров либо режима функционирования МЭ ССПТ-4А1, произошедших в результате действий администраторов или вследствие возникновения штатных событий, сбоев или ошибок в работе МЭ ССПТ-4А1. Подсистема регистрации МЭ ССПТ-4А1 обеспечивает регистрацию следующих событий:

- вход/выход администратора;
- загрузка и инициализация УОС МЭ ССПТ-4А1 и ее останов;
- действия администратора по изменению и загрузке политик доступа;
- действия администратора по изменению конфигурационных параметров МЭ ССПТ-4А1;
- действия администратора по управлению МЭ ССПТ-4А1 (запуск/останов пакетного фильтра, сброс файлов регистрации и т. д.).

При регистрации события указываются:

- дата и время регистрируемого события с учетом часового пояса;
- код и описание события;
- идентификатор администратора МЭ ССПТ-4А1, действия которого привели к регистрации данного события (если применимо);
- IP-адрес управляющего компьютера в случае удаленного администрирования (если применимо);
- наименование подсистемы, являющейся источником события (если применимо).

Регистрируемые в МЭ ССПТ-4А1 записи подразделяются на три категории:

1) **информационные события** – сообщения, извещающие об успешных действиях администраторов МЭ ССПТ-4А1, других стандартных событиях, характерных для текущего режима работы МЭ ССПТ-4А1;
2) **предупреждения** – сообщения о событиях, не нарушающих нормального функционирования ПО МЭ ССПТ-4А1, однако являющихся нестандартными или некорректными;
3) **ошибки** – сообщения о событиях, являющихся критическими и способными нарушить работу ПО МЭ ССПТ-4А1.

Формат представления событий и их полный перечень с описанием приводится в приложении Б, стр 431.

МЭ ССПТ-4А1 может одновременно хранить до **6000** записей о зарегистрированных событиях.

В МЭ ССПТ-4А1 производится циклическое обновление записей о зарегистрированных событиях. Таким образом, наиболее старые записи переписываются вновь регистрируемыми.

Для просмотра зарегистрированных событий служит команда **`log event show`**. По умолчанию используется режим вывода **`internal`** (вывод с использованием внутреннего просмотрщика), обеспечивающий наиболее удобный способ просмотра большого числа записей. Вывод команды **`log event show`** представлен на рис. 3.16, стр. 175.

```
12:18:36                    Журнал регистрации событий                    09.03.2021
  1| 09.03.2021 11:32:14 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
  2| 09.03.2021 09:29:44 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
  3| 09.03.2021 09:26:53 UTC+0000 (UTC) | I-151D: Применение дополнительной пол
  4| 09.03.2021 09:26:03 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
  5| 05.03.2021 10:55:08 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
  6| 05.03.2021 10:27:04 UTC+0000 (UTC) | I-1024: Сохранение дополнительной кон
  7| 05.03.2021 10:26:47 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
  8| 05.03.2021 10:01:56 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
  9| 05.03.2021 10:00:04 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
 10| 04.03.2021 11:42:42 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
 11| 04.03.2021 11:42:38 UTC+0000 (UTC) | I-1556: Добавление маршрута - 0.0.0.0
 12| 04.03.2021 11:42:15 UTC+0000 (UTC) | I-101B: Установка IP-адреса управляющ
 13| 04.03.2021 11:39:23 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
 14| 04.03.2021 11:38:55 UTC+0000 (UTC) | I-1300: Запуск пакетного фильтра - за
 15| 04.03.2021 11:38:08 UTC+0000 (UTC) | I-1002: Перезагрузка устройства (admi
 16| 04.03.2021 11:37:59 UTC+0000 (UTC) | I-1301: Перезапуск пакетного фильтра
 17| 04.03.2021 11:37:55 UTC+0000 (UTC) | I-1040: Применение конфигурации по ум
 18| 04.03.2021 11:37:47 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
 19| 04.03.2021 10:29:44 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
 20| 04.03.2021 10:28:31 UTC+0000 (UTC) | I-151E: Удаление дополнительной полит
 21| 04.03.2021 10:26:46 UTC+0000 (UTC) | I-1022: Удаление дополнительной конфи
 22| 04.03.2021 10:24:23 UTC+0000 (UTC) | I-151D: Применение дополнительной пол
 23| 04.03.2021 10:21:38 UTC+0000 (UTC) | I-1301: Перезапуск пакетного фильтра
Строки: 1-23 из 58              Столбцы: 1-80    H - справка  Q, F10 - выход
```

Рисунок 3.16: Журнал регистрации событий

Интерфейсы администратора, такие как командный интерфейс и WEB-интерфейс, при выводе сообщений предоставляют возможность отбора записей по установленным критериям, а также их сортировки по времени регистрации события. Могут использоваться следующие **критерии отбора** регистрационных записей:

- категория события;
- код события;
- интервал времени регистрации события.

В случае отсутствия зарегистрированных событий, удовлетворяющих критериям отбора, на экран терминала будет выведено предупреждение:

`FNPSH-W-007.02.201C-Нет заданных регистрационных записей`

Также, команда **`log event show`** допускает явное задание **порядка сортировки** при выводе списка событий в зависимости от времени регистрации события и **режим просмотра** записей.

Таким образом, необязательные параметры команды **`log event show`** могут использоваться для задания:

- критериев отбора;
- порядка сортировки записей;
- режима просмотра.

Синтаксис команды **`log event show`** представлен в приложении Г, стр. 501.

> По умолчанию при выводе события сортируются по убыванию времени регистрации (**order=desc**).
>
> По умолчанию вывод событий осуществляется с использованием внутреннего **просмотрщика (viewer=internal)**.

Приведем пример вывода журнала регистрации событий с использованием постраничного просмотрщика в качестве альтернативы внутреннему просмотрщику. Данный режим просмотра при использовании неполноэкранного терминала удобен тем, что позволяет копировать строки записей регистрации для вставки в текстовый документ, почтовое сообщение и т. д. Вывод с использованием постраничного просмотрщика осуществляется командой **`log event show viewer=more`**:

```
Журнал регистрации событий:

   1| 09.03.2021 11:32:14 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
ый интерфейс; admin; локальная аутентификация (admin,10.41.255.2)
   2| 09.03.2021 09:29:44 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
ный интерфейс; admin;  (admin,10.41.0.129)
   3| 09.03.2021 09:26:53 UTC+0000 (UTC) | I-151D: Применение дополнительной пол
итики - policy_accept (admin,10.41.0.129)
   4| 09.03.2021 09:26:03 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
ый интерфейс; admin; локальная аутентификация (admin,10.41.0.129)
   5| 05.03.2021 10:55:08 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
ный интерфейс; admin;  (admin,10.41.2.31)
   6| 05.03.2021 10:27:04 UTC+0000 (UTC) | I-1024: Сохранение дополнительной кон
фигурации - Config1 (admin,10.41.2.31)
   7| 05.03.2021 10:26:47 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
ый интерфейс; admin; локальная аутентификация (admin,10.41.2.31)
   8| 05.03.2021 10:01:56 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
ный интерфейс; admin;  (admin,10.41.0.129)
   9| 05.03.2021 10:00:04 UTC+0000 (UTC) | I-1003: Вход администратора - Командн
ый интерфейс; admin; локальная аутентификация (admin,10.41.0.129)
  10| 04.03.2021 11:42:42 UTC+0000 (UTC) | I-1004: Выход администратора - Команд
ный интерфейс; admin;  (admin,Console)
  11| 04.03.2021 11:42:38 UTC+0000 (UTC) | I-1556: Добавление маршрута - 0.0.0.0
/0.0.0.0 (admin,Console)
<Enter> - Далее...       <Q> - Выход
```

3.11.2. Регистрация трафика

Регистрация трафика. Информация о зарегистрированном трафике подразделяется на следующие категории:

- **пакеты** – информация о сетевых пакетах, обработанных пакетным фильтром МЭ ССПТ-4А1 в соответствии с действующей политикой доступа. Информация о каждом зарегистрированном пакете представляется в виде иерархической последовательности записей от канального до прикладного уровня включительно;
- **сессии** – информация о сессиях, обработанных подсистемой управления сессиями пакетного фильтра МЭ ССПТ-4А1.

Подсистема регистрации обеспечивает регистрацию трафика с сохранением следующих основных параметров:

- время регистрации пакета или сессии с точностью до микросекунды;
- номер входного и выходного фильтрующих интерфейсов МЭ ССПТ-4А1;
- цепочка правил фильтрации, по которым был обработан пакет (*при регистрации пакета*) или идентификатор сессии (*при регистрация сессии*);
- действие, выполненное над пакетом, в результате его обработки в пакетном фильтре;
- протокольные заголовки всех уровней, присутствующих в пакете (*при регистрации пакета*);
- данные о параметрах сессии (*при регистрации сессии*).

МЭ ССПТ-4А1 может одновременно хранить до **10000** записей о зарегистрированных пакетах/сессиях.

В МЭ ССПТ-4А1 производится циклическое обновление записей о зарегистрированных пакетах/сессиях. Таким образом, наиболее старые записи переписываются вновь регистрируемыми.

По умолчанию функция **регистрации пакетов** выключена в конфигурации МЭ ССПТ-4А1. Для включения функции регистрации пакетов необходимо выполнить команду **`log packet enable`**:

```
fnp4> log packet enable
FNPSH-I-007.02.303D-Регистрация пакетов включена
```

При выключенной функции регистрации пакетов пакеты не будут регистрироваться, даже если в правилах фильтрации будет установлен флаг регистрации пакетов (**log=packet**).

Для просмотра **журнала регистрации пакетов** служит команда **`log packet show`**. Пример вывода команды представлен на рис. 3.17, стр. 178.

В выводе информации о зарегистрированных пакетах для **удаленных** пакетов (действие **drop**) список выходных интерфейсов будет отсутствовать.

В выводе информации о пакете для обозначения фильтрующих интерфейсов используются их символические имена.

По каждой записи регистрации можно просмотреть детальную информацию, которая логически разделена на несколько групп. Для выбора записи регистрации можно использовать клавиши **<↑>**, **<↓>**, **<Page Up>** и **<Page Down>**. Для просмотра детальной информации по выбранной записи регистрации пакета необходимо нажать **<Enter>**. В результате будет выведено меню, в котором с помощью клавиш **<↑>** и **<↓>** можно выбрать желаемую группу детальной информации для вывода. Вывод детальной информации выбранной группы осуществляется в отдельном окне по клавише **<Enter>**. Пример вывода общей информации по зарегистрированному пакету представлен на рис. 3.18, стр. 179.

Время	Действие	Правила	Интерфейсы	Протокол	Источник	
11:35:15.619205	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.619016	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.619009	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.618312	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.618145	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.618143	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.618134	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.617753	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.617637	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.617385	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.616248	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.615902	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.509883	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.408468	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.407787	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.328920	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.328592	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.200661	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:15.097364	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:15.096910	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:14.856797	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:14.753939	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.
11:35:14.753389	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:13.669811	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:13.563281	accept	rule:11	eth1->eth0	IPv4/TCP	10.2.253.242:38464	
11:35:13.563082	accept	rule:11	eth0->eth1	IPv4/TCP	10.2.253.241:22	10.

Пакеты: 1-26 из 352 Текущий: 1 H - справка Q, F10 - выход

Рисунок 3.17: Журнал регистрации пакетов

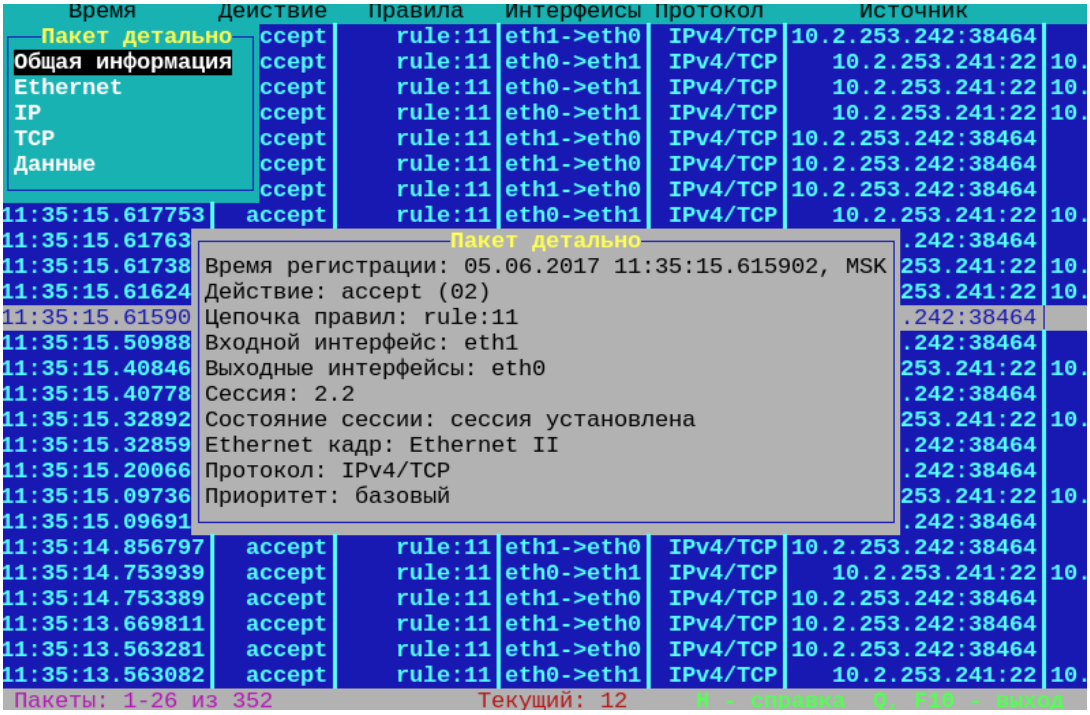


Рисунок 3.18: Детальная информация по пакету

При просмотре журнала регистрации пакетов могут использоваться следующие **критерии отбора** регистрационных записей:

- действие правила, примененного к пакету;
- входной фильтрующий интерфейс МЭ ССПТ-4А1;
- выходной фильтрующий интерфейс МЭ ССПТ-4А1;
- тип и номер правила фильтрации, примененного к пакету;
- тип кадра Ethernet, в который инкапсулирован пакет;
- список протоколов пакета и/или сообщения, инкапсулированного в пакет;
- идентификатор сессии, к которой относится пакет;
- MAC-адрес источника в Ethernet кадре;
- MAC-адрес приемника в Ethernet кадре;
- MAC-адрес источника или приемника в Ethernet кадре;
- IPv4-адрес источника;
- IPv4-адрес приемника;
- IPv4-адрес источника или приемника
- IPv6-адрес источника;
- IPv6-адрес приемника;
- IPv6-адрес источника или приемника;
- номер порта источника;
- номер порта приемника;

- номер порта источника или приемника;
- код ошибки для пакета, признанного ошибочным модулем контроля сессий или NAT;
- интервал времени регистрации пакета.

В случае отсутствия зарегистрированных пакетов, удовлетворяющих критериям отбора, на экран будет выведено предупреждение:

```
FNPSH-W-007.02.201C-Нет заданных регистрационных записей
```

Следующие пары критериев отбора не допустимы к указанию в команде **log packet show**, т. к. возникает логическое противоречие:

- srcip4 и ip4;
- dstip4 и ip4;
- srcip4 и srcip6, dstip6, ip6;
- dstip4 и dstip6, dstip6, ip6;
- srcip6 и ip6;
- dstip6 и ip6;
- srcip6 и srcip4, dstip4, ip4;
- dstip6 и dstip4, srcip4, ip4;
- mac и srcmac;
- mac и dstmac;
- port и srcport;
- port и dstport.

В случае указания недопустимой пары критериев на экран будет выведено предупреждение:

```
FNPSH-E-007.02.1136-Совместное использование параметров недопустимо
(имя_параметра_1, имя_параметра_2)
```

Также, команда **`log packet show`** допускает явное задание **порядка сортировки** при выводе списка пакетов (в зависимости от времени регистрации пакета) и **режим просмотра** записей.

Таким образом, необязательные параметры команды **`log packet show`** могут использоваться для задания:

- критериев отбора;
- порядка сортировки записей;
- режима просмотра.

Синтаксис команды **`log packet show`** представлен в приложении Г, стр. 501.

При выводе, по умолчанию пакеты сортируются по убыванию времени регистрации **(order=desc)**.

По умолчанию вывод зарегистрированных пакетов осуществляется с использованием **внутреннего просмотрщика (viewer=internal)**.

Приведем пример использования критерия отбора. Выведем все зарегистрированные пакеты, в которые инкапсулированы сообщения протокола ICMPv4, используя команду **`log packet show protocol=icmp`**. Вывод зарегистрированных пакетов с учетом данного критерия отбора представлен на рис. 3.19, стр. 181.

Время	Действие	Правила	Интерфейсы	Протокол	Источник	Приемник
11:34:38.750234	accept	rule:11	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
11:34:38.749708	accept	rule:11	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
11:34:37.737501	accept	rule:11	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
11:34:37.736872	accept	rule:11	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
11:34:36.674200	accept	rule:11	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
11:34:36.673649	accept	rule:11	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
11:11:47.696831	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
11:11:47.696581	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
11:11:46.637078	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
11:11:46.636570	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
11:11:45.579495	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
11:11:45.579196	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
15:28:33.080157	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
15:28:33.079699	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
15:21:58.819017	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
15:21:58.818403	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
15:20:07.766550	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
15:20:07.766044	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
15:19:24.678328	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
15:19:24.677971	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
15:19:23.629611	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
15:19:23.629266	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
13:09:12.425075	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
13:09:12.424735	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24
13:09:11.396854	accept	rule:1	eth1->eth0	IPv4/ICMP	10.2.253.242	10.2.253.24
13:09:11.396628	accept	rule:1	eth0->eth1	IPv4/ICMP	10.2.253.241	10.2.253.24

Пакеты: 1-26 из 35 Текущий: 1 H - справка Q, F10 - выход

Рисунок 3.19: Отбор пакетов протокола ICMP

Журнал регистрации пакетов может быть очищен с помощью команды **`log packet clear`**:

```
fnp4> log packet clear
Очистить журнал регистрации пакетов? (Y/N) [N]: y
FNPSH-I-007.02.303E-Регистрация пакетов очищена
```

Для просмотра **журнала регистрации сессий** служит команда **`log session show`**. Пример вывода команды представлен на рис. 3.20, стр. 182. Вывод содержит только основные характеристики сессии. По каждой из зарегистрированных сессий имеется возможность просмотра всей имеющейся информации. Для этого необходимо выделить нужную сессию, используя клавиши управления **<↑>**, **<↓>**, **<Page Up>** и **<Page Down>**, а затем нажать клавишу **<Enter>** для вывода на экран терминала подробной информации о сессии. Пример вывода подробной информации о сессии представлен на рис. 3.21, стр. 183.

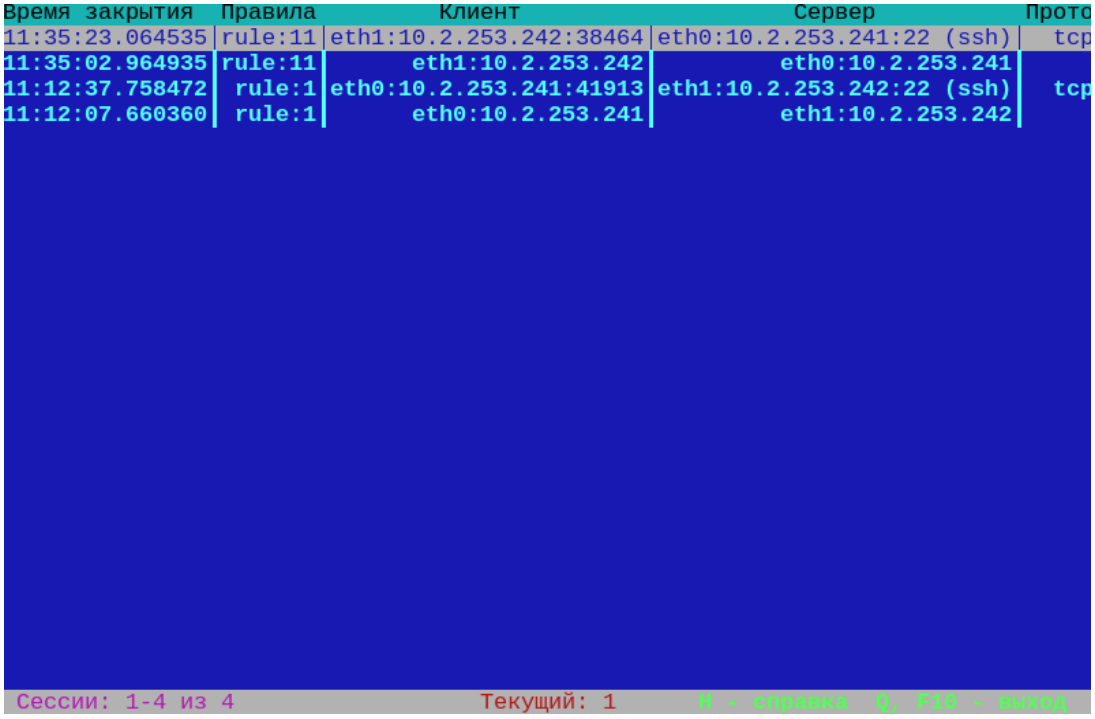


Рисунок 3.20: Журнал регистрации сессий

При просмотре журнала регистрации сессий могут использоваться следующие **критерии отбора** регистрационных записей:

- фильтрующие интерфейсы клиента;
- фильтрующие интерфейсы сервера;
- IPv4-адреса клиента
- IPv4-адреса сервера;
- IPv4-адреса как клиента или сервера;
- IPv6-адреса клиента;
- IPv6-адреса сервера;
- IPv6-адреса клиента или сервера;
- номера портов клиента;
- номера портов сервера;
- номера портов клиента или сервера;
- протокол, инкапсулированный в IP;
- протокол прикладного уровня;
- идентификатор сессии;
- время создания сессии;
- время завершения сессии (то же самое, что и время регистрации сессии).

```
Время закрытия  Правила        Клиент                     Сервер            Прото
11:35:23.064535 rule:11 eth1:10.2.253.242:38464 eth0:10.2.253.241:22 (ssh)  tcp
11:35:02.964935 rule:11      eth1:10.2.253.242          eth0:10.2.253.241
11:12:37.758472  rule:1 eth0:10.2.253.241:41913 eth1:10.2.253.242:22 (ssh)  tcp
11:12:07.660360  rule:1      eth0:10.2.253.241          eth1:10.2.253.242

                    Сессия детально
Номер сессии: 2.2
Время создания: 05.06.2017 11:35:06.614179, MSK
Время закрытия: 05.06.2017 11:35:23.064535, MSK
Причина закрытия: тайм-аут неактивности
Состояние сессии: завершение - ожидание завершающих пакетов
Цепочка правил: rule:11
Интерфейс клиента: eth1
Интерфейс сервера: eth0
Адрес клиента: 10.2.253.242
Адрес сервера: 10.2.253.241
Протокол, инкапсулированный в IP: TCP (6)
Порт клиента: 38464
Порт сервера: 22 (ssh)
Прикладной протокол: ssh
Счетчик пакетов (от клиента/от сервера): 72/70
Счетчик байт (от клиента/от сервера): 3222/7838

Сессии: 1-4 из 4          Текущий: 1      H - справка  Q, F10 - выход
```

Рисунок 3.21: Подробная информация о сессии

В случае отсутствия зарегистрированных сессий, удовлетворяющих критериям отбора, на экран терминала будет выведено предупреждение:

`FNPSH-W-007.02.201C-Нет заданных регистрационных записей`

Следующие пары критериев отбора не допустимы к указанию в команде **log session show**, т. к. возникает логическое противоречие:

- ipcl4 и ip4;
- ipsrv4 и ip4;
- ipcl4 и ipcl6, ipsrv6, ip6;
- ipsrv4 и ipcl6, ipsrv6, ip6;
- ipcl6 и ip6;
- ipsrv6 и ip6;
- ipcl6 и ipcl4, ipsrv4, ip4;
- ipsrv6 и ipcl4, ipsrv4, ip4;
- port и portcl;
- port и portsrv.

В случае указания недопустимой пары критериев на экран терминала будет выведено предупреждение:

```
FNPSH-E-007.02.1136-Совместное использование параметров недопустимо
(имя_параметра_1, имя_параметра_2)
```

Также, команда **`log session show`** допускает явное задание **порядка сортировки** при выводе списка сессий (в зависимости от времени регистрации сессии) и **режим просмотра** записей.

Таким образом, необязательные параметры команды **`log session show`** могут использоваться для задания:

- критериев отбора;

- порядка сортировки записей;
- режима просмотра.

Синтаксис команды **`log session show`** представлен в приложении Г, стр. 501.

По умолчанию при выводе сессии сортируются по убыванию времени регистрации **(order=desc)**.

По умолчанию вывод зарегистрированных сессий осуществляется с использованием **внутреннего просмотрщика (viewer=internal)**.

Журнал регистрации сессий может быть очищен с помощью команды **`log session clear`**:

```
fnp4> log session clear
Очистить журнал регистрации сессий? (Y/N) [N]: y
FNPSH-I-007.02.3043-Регистрация сессий очищена
```

3.11.3. Регистрация системных сообщений

МЭ ССПТ-4А1 обеспечивает возможность регистрации сообщений, используя службу системных сообщений (SYSLOG) УОС МЭ ССПТ-4А1. Зарегистрированные сообщения помещаются в файлы системных журналов УОС МЭ ССПТ-4А1, просмотр содержимого которых возможен с использованием средств администрирования МЭ ССПТ-4А1.

Контроль размеров и управление ротацией файлов системных журналов осуществляет УОС МЭ ССПТ-4А1
Максимальный размер файла системного журнала для хранения системных сообщений, поступающих от подсистем ПО МЭ ССПТ-4А1, составляет **100 Мбайт**.

В файле системного журнала УОС МЭ ССПТ-4А1 каждое сообщение занимает отдельную текстовую строку. Например:

```
Dec 23 11:37:35 fnp4 fnp4[1266]: fnp4_filtd: Пакетный фильтр готов к работе (PID 1266)
```

Строка системного сообщения в общем случае состоит из следующих элементов:

- дата и время регистрации системного сообщения (`Dec 23 11:37:35`);
- префикс системного сообщения. Все системные сообщения, отправляемые подсистемами ПО МЭ ССПТ-4А1, имеют префикс `fnp4`;
- номер прикладного процесса УОС МЭ ССПТ-4А1, отправившего данное сообщение (`fnp4[1266]`);
- имя подсистемы ПО МЭ ССПТ-4А1, отправившей данное сообщение (`fnp4_filtd` – процесс пакетного фильтра МЭ ССПТ-4А1);
- текст сообщения.

Системные сообщения выводятся в порядке возрастания времени их регистрации. Обратный порядок вывода не доступен для системных сообщений.

Для просмотра **журнала регистрации системных сообщений** служит команда **`log syslog show`**. Пример вывода данной команды представлен на рис. 3.22, стр. 185.

```
 12:28:30            Журнал регистрации системных сообщений          09.03.2021
Mar  3 14:35:15 fnp4 newsyslog[91119]: logfile first created
Mar  3 14:35:15 fnp4 syslogd: kernel boot file is /boot/kernel/kernel
Mar  3 14:35:15 fnp4 kernel: Copyright (c) 1992-2020 The FreeBSD Project.
Mar  3 14:35:15 fnp4 kernel: Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1
Mar  3 14:35:15 fnp4 kernel:    The Regents of the University of California. All
Mar  3 14:35:15 fnp4 kernel: FreeBSD is a registered trademark of The FreeBSD Fo
Mar  3 14:35:15 fnp4 kernel: FreeBSD 11.4-RELEASE-p8  r369361M amd64
Mar  3 14:35:15 fnp4 kernel: FreeBSD clang version 10.0.0 (git@github.com:llvm/l
Mar  3 14:35:15 fnp4 kernel: VT(efifb): resolution 1024x768
Mar  3 14:35:15 fnp4 kernel: CPU: Intel(R) Xeon(R) CPU           X5650  @ 2.67GH
Mar  3 14:35:15 fnp4 kernel:   Origin="GenuineIntel"  Id=0x206c2  Family=0x6  Mo
Mar  3 14:35:15 fnp4 kernel:   Features=0x1f83fbff<FPU,VME,DE,PSE,TSC,MSR,PAE,MC
Mar  3 14:35:15 fnp4 kernel:   Features2=0x81b82201<SSE3,SSSE3,CX16,SSE4.1,SSE4.
Mar  3 14:35:15 fnp4 kernel:   AMD Features=0x28100800<SYSCALL,NX,RDTSCP,LM>
Mar  3 14:35:15 fnp4 kernel:   AMD Features2=0x1<LAHF>
Mar  3 14:35:15 fnp4 kernel:   Structured Extended Features=0x2<TSCADJ>
Mar  3 14:35:15 fnp4 kernel:   Structured Extended Features3=0xbc000000<IBPB,STI
Mar  3 14:35:15 fnp4 kernel:   IA32_ARCH_CAPS=0xc<RSBA,SKIP_L1DFL_VME>
Mar  3 14:35:15 fnp4 kernel:   TSC: P-state invariant
Mar  3 14:35:15 fnp4 kernel: Hypervisor: Origin = "VMwareVMware"
Mar  3 14:35:15 fnp4 kernel: real memory  = 4294967296 (4096 MB)
Mar  3 14:35:15 fnp4 kernel: avail memory = 4108480512 (3918 MB)
Mar  3 14:35:15 fnp4 kernel: Event timer "LAPIC" quality 600
Строки: 1-23 из 1297          Столбцы: 1-80    H - справка  Q, F10 - выход
```

Рисунок 3.22: Журнал регистрации системных сообщений

3.11.4. Выгрузка журналов регистрации на FTP-сервер

Функция **выгрузки журналов регистрации на FTP-сервер** позволяет выгружать журналы регистрации в виде файлов:

- событий;
- трафика (пакетов и сессий).

Для просмотра настроек подсистемы регистрации, в том числе настроек выгрузки журналов регистрации на FTP-сервер, служит команда **`log export ftp`**. По умолчанию настройки выгрузки журналов регистрации на FTP-сервер следующие:

```
Выгрузка файлов регистрации по FTP:        выключено
    IP-адрес FTP-сервера:                  не определено
    Порт FTP-сервера:                      21
    Путь на FTP-сервере:                   не определено
    Имя пользователя:                      не определено
```

Для настройки выгрузки журналов регистрации на FTP-сервер служит команда **`log export ftp set`**. Рассмотрим пример ее использования:

```
fnp4> log export ftp set server=10.98.100.250 user=ftpuser path=/usr1/home/ftpuser
state=enable
FTP пароль:
FTP пароль повторно:
FNPSH-I-007.02.3042-Параметры выгрузки файлов регистрации по FTP определены
FNPSH-I-007.02.3040-Выгрузка файлов регистрации по FTP включена
```

Как видно из примера, команда **`log export ftp set`** позволяет задать все необходимые параметры, а также включить или выключить использование выгрузки журналов регистрации на FTP-сервер. В примере выгрузка была включена.

В том случае, если IP-адрес FTP-сервера не принадлежит сети управляющего интерфейса (**EthC**), администратор должен добавить соответствующий маршрут с использованием командного или WEB-интерфейса администратора

Выведем настройки подсистемы регистрации, чтобы увидеть новые значения параметров:

```
fnp4> log show
Регистрация пакетов:                        включено
Регистрация пакетов, отброшенных сессиями: выключено
Регистрация пакетов, отброшенных NAT:      выключено
Регистрация синхронизации по NTP           выключено
Выгрузка файлов регистрации по FTP:        включено
    IP-адрес FTP-сервера:                  10.98.100.250
    Порт FTP-сервера:                      21
    Путь на FTP-сервере:                   /usr1/home/ftpuser
    Имя пользователя:                      ftpuser
Выгрузка записей регистрации по SYSLOG:    выключено
    IP-адрес SYSLOG-сервера:               не определено
    Порт SYSLOG-сервера:                   514
    Выгружаемые записи:                    события
```

Выгрузка осуществляется каждый раз по достижению числа записей, кратного 1000. При этом в выгружаемый файл записывается последняя 1000 записей.

Регистрационные записи пакетов и сессий считаются суммарно и выгружаются в едином файле.

Для имен выгружаемых файлов регистрации используются следующие шаблоны:

- **logd_evn.XXXX** – файл записей регистрации событий;
- **logd_pkt.XXXX** – файл записей регистрации пакетов и сессий;

Формат выгружаемых файлов записей регистрации — **бинарный**, поэтому для их просмотра необходимо дополнительное программное обеспечение.

Настройки выгрузки могут быть сброшены командой **`log export ftp clear`**:

```
fnp4> log export ftp clear
Удалить параметры выгрузки по FTP? (Y/N) [N]: y
FNPSH-I-007.02.303F-Параметры выгрузки файлов регистрации по FTP сброшены
```

При этом также выключается использование выгрузки журналов регистрации на FTP-сервер, что соответствует настройкам по умолчанию:

```
fnp4> log show
Регистрация пакетов:                        включено
Регистрация пакетов, отброшенных сессиями: выключено
Регистрация пакетов, отброшенных NAT:      выключено
```

```
Регистрация синхронизации по NTP           выключено
Выгрузка файлов регистрации по FTP:        выключено
    IP-адрес FTP-сервера:                  не определено
    Порт FTP-сервера:                      21
    Путь на FTP-сервере:                   не определено
    Имя пользователя:                      не определено
Выгрузка записей регистрации по SYSLOG:    выключено
    IP-адрес SYSLOG-сервера:               не определено
    Порт SYSLOG-сервера:                   514
    Выгружаемые записи:                    события
```

3.11.5. Выгрузка записей регистрации на SYSLOG-сервер

Функция **выгрузки записей регистрации на SYSLOG-сервер** позволяет записывать текстовое представления записей регистрации в файл(ы) на удаленном сервере с использованием протокола SYSLOG.

Настройки выгрузки записей регистрации на SYSLOG-сервер позволят задать перечень типов выгружаемых записей регистрации из следующего списка:

- записи регистрации событий;
- записи регистрации пакетов;
- записи регистрации сессий.

По умолчанию, в конфигурации МЭ ССПТ-4А1, перечень типов записей регистрации, выгружаемых на SYSLOG-сервер, состоит из единственного значения, соответствующего *записям регистрации событий*.

Параметры выгрузки записей регистрации на SYSLOG-сервер доступны по команде **`log show`**:

```
fnp4> log show
Регистрация пакетов:                       включено
Регистрация пакетов, отброшенных сессиями: выключено
Регистрация пакетов, отброшенных NAT:      выключено
Регистрация синхронизации по NTP           выключено
Выгрузка файлов регистрации по FTP:        выключено
    IP-адрес FTP-сервера:                  не определено
    Порт FTP-сервера:                      21
    Путь на FTP-сервере:                   не определено
    Имя пользователя:                      не определено
Выгрузка записей регистрации по SYSLOG:    выключено
    IP-адрес SYSLOG-сервера:               не определено
    Порт SYSLOG-сервера:                   514
    Выгружаемые записи:                    события
```

Для настройки параметров выгрузки на SYSLOG-сервер необходимо задать параметр “`IP-адрес SYSLOG-сервера`” (параметры “`Порт SYSLOG-сервера`” и “`Выгружаемые записи`” имеют значения по умолчанию и их переназначение не обязательно). Включить использование выгрузки можно вместе с заданием параметров, выполнив команду **`log export syslog set`**. Например:

```
fnp4> log export syslog set server=10.98.100.250 type=event,packet,session state=enable
FNPSH-I-007.02.306F-Параметры выгрузки системных сообщений на SYSLOG-сервер изменены
```

```
FNPSH-I-007.02.306E-Выгрузка записей регистрации на SYSLOG-сервер включена
```

Настройка SYSLOG-сервера выходит за рамки данного руководства. Приведем примеры выгруженных записей регистрации.

Запись регистрации события:

```
Jun  2 14:43:04 <local0.notice> esxi2-gw.***.ru fnp4.esxi2.fractel.priv: I-1038: Включение
регистрации пакетов, отброшенных механизмом управления сессиями|admin,10.98.100.250
```

Запись регистрации пакета:

```
Jun  2 15:28:32 <local1.notice> esxi2-gw.***.ru fnp4.esxi2.fractel.priv: 02.06.2017
15:28:33.079699, MSK|02|rule:1|eth0|eth1|0.4|||установление соединения - принят первый
пакет|Ethernet II|IPv4/ICMP||0|00:0c:29:26:d0:5d|00:0c:29:b7:34:ec|00000000|84|0x33ca|0|0|
0|64|1 (icmp)|0x36f7|10.2.253.241|10.2.253.242|8|0
```

Данная запись регистрации – ICMP-запрос, зарегистрированный в соответствии с общим правилом номер 1.

Запись регистрации сессии:

```
Jun  2 15:28:55 <local2.notice> esxi2-gw.***.ru fnp4.esxi2.fractel.priv: 0.4|02.06.2017
15:28:33.079699, MSK|02.06.2017 15:28:56.090603, MSK|0002|сессия установлена|rule:1|eth0|
eth1||10.2.253.241|10.2.253.242|ICMP (1)|||||1|1|64|64
```

Данная запись регистрации – сессия протокола ICMPv4.

Параметры выгрузки записей регистрации на SYSLOG-сервер могут быть сброшены в значения по умолчанию с помощью команды **`log export syslog clear`**:

```
fnp4> log export syslog clear
Установить настройки выгрузки на SYSLOG-сервер по умолчанию? (Y/N) [N]: y
FNPSH-I-007.02.3111-Параметры выгрузки на SYSLOG-сервер сброшены
```

В результате: параметры выгрузки имеют значения по умолчанию, выгрузка выключена:

```
fnp4> log show
Регистрация пакетов:                        включено
Регистрация пакетов, отброшенных сессиями: включено
Регистрация пакетов, отброшенных NAT:      выключено
Регистрация синхронизации по NTP           выключено
Выгрузка файлов регистрации по FTP:        выключено
    IP-адрес FTP-сервера:                  не определено
    Порт FTP-сервера:                      21
    Путь на FTP-сервере:                   не определено
    Имя пользователя:                      не определено
Выгрузка записей регистрации по SYSLOG:    выключено
    IP-адрес SYSLOG-сервера:               не определено
    Порт SYSLOG-сервера:                   514
    Выгружаемые записи:                    события
```

3.12. Управление конфигурациями

Параметры настройки и функционирования МЭ ССПТ-4А1 (далее – параметры конфигурации) хранятся в *конфигурациях*. В МЭ ССПТ-4А1 существует два типа конфигураций:

1) **текущая конфигурация** – набор параметров настройки и функционирования МЭ ССПТ-4А1, которые в данный момент задействованы в процессе функционирования программных компонентов ПО и УОС МЭ ССПТ-4А1;
2) **дополнительные конфигурации** – именованные наборы параметров настройки и функционирования, которые хранятся в МЭ ССПТ-4А1 и могут быть использованы для резервного копирования текущей конфигурации с возможностью *выгрузки/загрузки* на управляющий компьютер. Каждой дополнительной конфигурации присваивается *символическое имя*, уникальное для данного устройства МЭ ССПТ-4А1.

МЭ ССПТ-4А1 обеспечивает следующие возможности по управлению конфигурациями:

- просмотр текущей или дополнительной конфигурации;
- сохранение текущей конфигурации в дополнительную;
- загрузка выбранной дополнительной конфигурации в текущую (далее – *применение дополнительной конфигурации*);
- удаление дополнительной конфигурации;
- загрузка с управляющего компьютера на МЭ ССПТ-4А1 дополнительной конфигурации;
- выгрузка с МЭ ССПТ-4А1 на управляющий компьютер дополнительной конфигурации;
- изменение имени и комментария дополнительной конфигурации (далее – *переименование дополнительной конфигурации*);
- отображение списка существующих на МЭ ССПТ-4А1 дополнительных конфигураций;
- применение конфигурации по умолчанию.

Дополнительные конфигурации, выгружаемые на управляющий компьютер, хранятся в текстовых файлах в формате XML.

МЭ ССПТ-4А1 осуществляет контроль корректности дополнительной конфигурации, загружаемой с управляющего компьютера. В случае обнаружения ошибок загрузка дополнительной конфигурации блокируется с выдачей соответствующего диагностического сообщения. По каждой ошибке, обнаруженной в дополнительной конфигурации, выводится следующая информация:

- **для синтаксической ошибки** – номер строки в загружаемом XML-файле дополнительной конфигурации, в которой была обнаружена синтаксическая ошибка, имя атрибута (XML-тега) и значение атрибута, в случае его неверного или недопустимого значения;
- **для семантической ошибки** – описание семантической ошибки с указанием номера строки в XML-файле дополнительной конфигурации, в которой была обнаружена семантическая ошибка, с возможным указанием имени и значения атрибута (XML-тега).

Загрузка/выгрузка дополнительных конфигураций на управляющий компьютер возможна только с применением следующих средств администрирования:
- WEB-интерфейс администратора;
- FNPCP-интерфейс администратора.

При управлении конфигурациями администраторам в зависимости от прав доступа разрешены следующие действия:

- для администраторов с уровнем прав доступа `read`:
  - ✔ просмотр текущей или дополнительной конфигурации;
  - ✔ выгрузка с МЭ ССПТ-4А1 на управляющий компьютер дополнительной конфигурации;
  - ✔ отображение списка существующих на МЭ ССПТ-4А1 дополнительных конфигураций;
- для администраторов с уровнем прав доступа `full` или `admin`:
  - ✔ просмотр текущей или дополнительной конфигурации;
  - ✔ сохранение текущей конфигурации в дополнительную;
  - ✔ применение дополнительной конфигурации;
  - ✔ откат текущей конфигурации;
  - ✔ удаление дополнительной конфигурации;
  - ✔ загрузка с управляющего компьютера на МЭ ССПТ-4А1 дополнительной конфигурации;
  - ✔ выгрузка с МЭ ССПТ-4А1 на управляющий компьютер дополнительной конфигурации;
  - ✔ переименование дополнительной конфигурации;
  - ✔ отображение списка существующих на МЭ ССПТ-4А1 дополнительных конфигураций;
  - ✔ применение конфигурации по умолчанию.

Для просмотра текущей или дополнительной конфигурации служит команда **`config show`**. Возможен вывод конфигураций в двух форматах:

- в формате XML;
- виде списка команд командного интерфейса МЭ ССПТ-4А1, выполнив которые можно получить данную конфигурацию.

По умолчанию конфигурации выводятся в формате XML.

Пример вывода текущей конфигурации в формате XML представлен на рис. 3.23, стр. 191. Для вывода текущей конфигурации в виде списка команд необходимо выполнить команду **`config show format=command`**. Пример вывода данной команды представлен на рис. 3.24, стр. 191.

```
 12:31:28                    Текущая конфигурация                    09.03.2021
<?xml version="1.0" encoding="UTF-8"?>
<fnp4-cfg xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceS
  <interface num="10">
    <interface-control sys-index="1" sys-name="net16" supported-media="autoselec
      <acl entry-num="0"/>
    </interface-control>
    <interface-filter>
      <interface-filter-list entry-num="9">
        <interface-filter-entry num="0" sys-index="2" sys-name="net0" supported-
        <interface-filter-entry num="1" sys-index="3" sys-name="net1" supported-
        <interface-filter-entry num="2" sys-index="4" sys-name="net2" supported-
        <interface-filter-entry num="3" sys-index="5" sys-name="net3" supported-
        <interface-filter-entry num="4" sys-index="6" sys-name="net4" supported-
        <interface-filter-entry num="5" sys-index="7" sys-name="net5" supported-
        <interface-filter-entry num="6" sys-index="8" sys-name="net6" supported-
        <interface-filter-entry num="7" sys-index="9" sys-name="net7" supported-
        <interface-filter-entry num="8" sys-index="10" sys-name="net8" supported
      </interface-filter-list>
      <mirroring use="no" from="0" to="0" dir="both"/>
    </interface-filter>
  </interface>
  <nat use="no" auth-use="no" auth-timeout="600">
    <nat-arp entry-num="0"/>
 Строки: 1-23 из 57              Столбцы: 1-80     H - справка  Q, F10 - выход
```

Рисунок 3.23: Просмотр текущей конфигурации в формате XML

```
 12:33:23                    Текущая конфигурация                    09.03.2021
interface control set state=enable address=10.41.2.120/255.255.255.128 media=aut
 mtu=1500
interface control acl clear
interface filter set interface=eth0 state=enable media=autoselect mtu=1500
interface filter set interface=eth1 state=enable media=autoselect mtu=1500
interface filter set interface=eth2 state=enable media=autoselect mtu=1500
interface filter set interface=eth3 state=enable media=autoselect mtu=1500
interface filter set interface=eth4 state=enable media=autoselect mtu=1500
interface filter set interface=eth5 state=enable media=autoselect mtu=1500
interface filter set interface=eth6 state=enable media=autoselect mtu=1500
interface filter set interface=eth7 state=enable media=autoselect mtu=1500
interface filter set interface=eth8 state=enable media=autoselect mtu=1500
interface filter mirror state=disable srcif=eth0 dstif=eth0 direction=all
session enable
session ap disable
session invalid log disable
session mac enable
session deeptcp enable
session trace enable
session timeout protocol=tcp syn=5 established=3600 fin=600
session timeout protocol=udp syn=5 established=60
session timeout protocol=icmp syn=5 established=20
session timeout protocol=other syn=5 established=30
 Строки: 1-23 из 44              Столбцы: 1-80     H - справка  Q, F10 - выход
```

Рисунок 3.24: Просмотр текущей конфигурации в виде списка команд

При просмотре конфигурации может быть выбран режим вывода из следующего списка:

- внутренний (**`internal`**);
- постраничный (**`more`**);
- без использования просмотрщика (**`no`**).

По умолчанию при выводе конфигурации используется внутренний просмотрщик **(viewer=internal)**.

Последние два режима вывода удобно использовать, когда необходимо скопировать отдельные строки вывода конфигурации для вставки в текстовый документ, сообщение электронной почты и т. д.

Например, для просмотра текущей конфигурации с использованием постраничного режима вывода необходимо выполнить команду **`config show viewer=more`**:

```
Текущая конфигурация:

<?xml version="1.0" encoding="UTF-8"?>
<fnp4-cfg xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceS
chemaLocation="fnp4_cf.xsd" version="1.0.0" device-name="fnp4" device-comment=""
>
  <interface num="10">
    <interface-control sys-index="1" sys-name="net16" supported-media="autoselec
t" min-mtu="72" max-mtu="9000" address="10.41.2.120" mask="255.255.255.128" use=
"yes" media="autoselect" duplex="" mtu="1500" lagg-use="no" lagg-proto="failover
" lagg-if-num="0">
      <acl entry-num="0"/>
    </interface-control>
    <interface-filter>
      <interface-filter-list entry-num="9">
        <interface-filter-entry num="0" sys-index="2" sys-name="net0" supported-
media="autoselect" min-mtu="72" max-mtu="9000" adm-name="eth0" media="autoselect
" duplex="" status="up" mtu="1500"/>
        <interface-filter-entry num="1" sys-index="3" sys-name="net1" supported-
media="autoselect" min-mtu="72" max-mtu="9000" adm-name="eth1" media="autoselect
" duplex="" status="up" mtu="1500"/>
        <interface-filter-entry num="2" sys-index="4" sys-name="net2" supported-
media="autoselect" min-mtu="72" max-mtu="9000" adm-name="eth2" media="autoselect
" duplex="" status="up" mtu="1500"/>
<Enter> - Далее...       <Q> - Выход
```

Для сохранения текущей конфигурации в дополнительную используется команда **`config save`**.

Пример сохранения текущей конфигурации в дополнительную с автоматически сгенерированным именем дополнительной конфигурации:

```
fnp4> config save
Имя конфигурации не задано. Сохранить со сгенерированным именем? (Y/N) [N]: y
FNPSH-I-007.02.300B-Дополнительная конфигурация сохранена (fnp4-fnp4-20170606-154718)
```

Пример сохранения текущей конфигурации в дополнительную с явным указанием имени и комментария к конфигурации:

```
fnp4> config save name=cfg1 comment="комментарий к конфигурации"
FNPSH-I-007.02.300B-Дополнительная конфигурация сохранена (cfg1)
```

МЭ ССПТ-4А1 позволяет хранить до **16** дополнительных конфигураций.

Изначально на устройстве МЭ ССПТ-4А1 дополнительные конфигурации отсутствуют.

Просмотреть список дополнительных конфигураций на данном устройстве МЭ ССПТ-4А1 можно, выполнив команду config list:

```
fnp4> config list
Список дополнительных конфигураций:
    Имя                       Последнее изменение                Комментарий
    Config1                   05.03.2021 10:27:04 UTC+0000 (UTC) Is it my config #1?
    fnp4-fnp4-20210309-123745 09.03.2021 12:37:45 UTC+0000 (UTC)
Занято: 2       Свободно: 14
```

Дополнительная конфигурация может быть переименована, кроме того может быть изменен или удален комментарий к ней. Для этого служит команда **`config rename`**, например:

```
fnp4> config rename srcname=Config1 dstname=cfg1 comment="новый комментарий"
FNPSH-I-007.02.3102-Комментарий к дополнительной конфигурации изменен (Config1)
FNPSH-I-007.02.3103-Дополнительная конфигурация переименована (Config1, cfg1)
```

Убедиться в переименовании конфигурации и изменении комментария к ней можно, снова выполнив команду **`config list`**:

```
fnp4> config list
Список дополнительных конфигураций:
    Имя                       Последнее изменение                Комментарий
    cfg1                      09.03.2021 12:40:01 UTC+0000 (UTC) новый комментарий
    fnp4-fnp4-20210309-123745 09.03.2021 12:37:45 UTC+0000 (UTC)
Занято: 2       Свободно: 14
```

Для применения ранее сохраненной дополнительной конфигурации в качестве текущей конфигурации служит команда **`config apply`**, например:

```
fnp4> config apply name=cfg1
Применить дополнительную конфигурацию? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.3112-Пакетный фильтр перезапущен
FNPSH-I-007.02.3024-Дополнительная конфигурация применена (cfg1)
```

При применении дополнительной конфигурации пакетный фильтр МЭ ССПТ-4А1 перезапускается.

При применении **дополнительной конфигурации** в том случае, если IP-адрес управляющего интерфейса в дополнительной конфигурации отличается от IP-адреса в текущей конфигурации, завершаются все сеансы работы администраторов МЭ ССПТ-4А1, в том числе сеанс администратора, выполнившего данную операцию.

Эта особенность позволяет администратору получить привилегии **admin** или **full** при следующем входе на МЭ с управляющего компьютера (сетевое администрирование).

Дополнительная конфигурация может быть удалена с устройства МЭ ССПТ-4А1. Для этого служит команда **`config remove`**, например:

```
fnp4> config remove name=fnp4-fnp4-20210309-123745
Удалить дополнительную конфигурацию? (Y/N) [N]: Y
FNPSH-I-007.02.3023-Дополнительная конфигурация удалена (fnp4-fnp4-20210309-123745)
```

В процессе администрирования МЭ ССПТ-4А1 может возникнуть необходимость в применении конфигурации по умолчанию (возврат текущей конфигурации в состояние по умолчанию). Для этого служит команда **`config default`**.

При применении **конфигурации по умолчанию** завершаются все сеансы работы администраторов МЭ ССПТ-4А1, в том числе сеанс администратора, выполнившего данную операцию.

Эта особенность позволяет администратору получить привилегии **admin** или **full** при следующем входе на МЭ с управляющего компьютера (сетевое администрирование).

Выгрузка дополнительной конфигурации. Дополнительная конфигурация может быть выгружена с МЭ ССПТ-4А1 на управляющий компьютер администратора для резервного копирования и/или последующей загрузки на другое устройство МЭ ССПТ-4А1.

Функция выгрузки дополнительной конфигурации доступна через WEB-интерфейс администратора и FNPCP-интерфейс, но не доступна через КИА.

Возможность выгрузки **текущей конфигурации** МЭ ССПТ-4А1 **не предоставляется**, т. к. форматы текущей и дополнительной конфигурации отличаются: текущая конфигурация содержит параметры сетевых интерфейсов данного устройства МЭ, которые отсутствуют в дополнительной конфигурации.

Пример выгрузки дополнительной конфигурации с использованием в WEB-интерфейса администратора приведен в разделе 4.2.1, стр. 237.

Загрузка дополнительной конфигурации. Ранее выгруженную дополнительную конфигурацию можно загрузить на МЭ ССПТ-4А1. Загрузка дополнительной конфигурации доступна через WEB-интерфейс администратора и FNPCP-интерфейс, но не доступна через КИА.

Пример загрузки дополнительной конфигурации с использованием в WEB-интерфейса администратора приведен в разделе 4.2.1, стр. 235.

3.13. Системные настройки

3.13.1. Настройки командного интерфейса

К настройкам командного интерфейса относится следующее:

- буфер истории команд;
- пароль системного пользователя **`fnpsh`**;
- тайм-аут неактивности сеанса работы администратора ;
- режим просмотра по умолчанию.

Для каждого администратора в файловой системе УОС хранится буфер из максимум **100** последних команд, выполненных администратором в командном интерфейсе.

По завершению сеанса работы администратора его буфер команд сохраняется.

Для просмотра буфера истории команд служит команда **system fnpsh history show**, например:

```
fnp4> system fnpsh history show
Буфер истории команд:
   1 - log session show ifcl=0
   2 - log session show srbv=0
   3 - log session show ifsrv=0
   4 - log session show ifsrv=eth1
   5 - log session show ifsrv=eth0
…
```

Буфер истории команд может быть очищен администратором МЭ ССПТ-4А1, к которому он относится. Для этого администратору необходимо выполнить команду **system fnpsh history clear**:

```
fnp4> system fnpsh history clear
Очистить буфер истории команд? (Y/N) [N]: y
FNPSH-I-007.02.30BF-Буфер истории команд очищен
```

Если следом за очисткой буфера истории команд вывести буфер, то вывод будет следующим (содержать единственную команду):

```
fnp4> system fnpsh history show
Буфер истории команд:
   1 - system fnpsh history show
```

Пароль системного пользователя **fnpsh** для уровня системной авторизации, используемой для командного интерфейса МЭ ССПТ-4А1, может быть изменен. Для этого служит команда **system fnpsh password**, например:

```
fnp4> system fnpsh password
Новый пароль:
Новый пароль повторно:
FNPSH-I-007.02.30C1-Пароль системного пользователя изменен
```

Требования к формату пароля системного пользователя **fnpsh** приведены в приложении А, стр. 423.

Изменение пароля системного пользователя **fnpsh** доступно только администратору **admin**.

Тайм-аут неактивности сеанса работы администратора может быть изменен. Для этого служит команда **system fnpsh set**, например:

```
fnp4> system fnpsh set timeout=1800
FNPSH-I-007.02.30BE-Тайм-аут неактивности командного интерфейса изменен
```

Установка режима просмотра данных в КИА действует только до окончания данного сеанса работы администратора.

В начале каждого сеанса работы администратора через КИА режим просмотра данных установлен в значение **internal** (полноэкранный режим просмотра данных).

Тайм-аут неактивности сеанса работы администратора может быть изменен в пределах от **60** до **6000** секунд.

Режим просмотра данных в командном интерфейсе может быть изменен для данного сеанса работы администратора. Поддерживаются следующие режимы просмотра данных:

- **`internal`** — полноэкранный режим просмотра данных;
- **`more`** — упрощенный режим постраничного просмотра данных;
- **`no`** — режим сплошного вывода данных на экран терминала без возможности постраничного и построчного просмотра.

Для изменения режима просмотра данных в командном интерфейсе МЭ ССПТ-4А1 служит команда **`system fnpsh set`**, например:

```
fnp4> system fnpsh set viewer=no
FNPSH-I-007.02.30BD-Режим просмотра изменен
```

В результате установки данного режима просмотра (**`no`**) такие команды, как: **`log packet show`**, **`log session show`**, **`log event show`** и т. д. будут использовать данный режим просмотра данных, если требуемый режим просмотра данных не задан непосредственно в команде, например:

```
fnp4> log session show
Журнал регистрации сессий:

13:19:09.456661|rule:11|eth1:10.2.253.242|eth0:10.2.253.241|icmp
18:37:48.367413|rule:11|eth1:10.2.253.242|eth0:10.2.253.241|icmp
18:37:28.298044|rule:11|eth1:10.2.253.242:65485|eth0:10.2.253.241:22 (ssh)|tcp/ssh
```

Установка режима просмотра данных в командном интерфейсе МЭ ССПТ-4А1 действует только до окончания данного сеанса работы администратора, поскольку не сохраняется в текущую конфигурацию устройства.

В начале каждого сеанса работы администратора через командный интерфейс МЭ ССПТ-4А1 режим просмотра данных установлен в значение **internal** (полноэкранный режим просмотра данных).

При использовании полноэкранного режима просмотра данных **минимально допустимый** размер окна терминала составляет: **80x16** (80 символов в строке, 16 строк). В противном случае будет выведено сообщение об ошибке, а данные выведены не будут.

Рекомендуемый размер окна терминала: **80x24** (80 символов в строке, 24 строки). При меньшем размере окна некоторые данные могут быть выведены с искажением или не выведены вовсе.

3.13.2. Просмотр системной информации

Системная информация, доступная для просмотра, делится на две категории:

- системная информация по аппаратному и программному обеспечению данного устройства МЭ ССПТ-4А1;

- основные параметры конфигурации МЭ ССПТ-4А1 (функции, используемые в текущей конфигурации и т. д.).

Для просмотра системной информации обеих категорий служит команда **system show**. По умолчанию (при отсутствии параметров команды) выводится системная информация по аппаратному и программному обеспечению данного устройства МЭ ССПТ-4А1. Например:

```
fnp4> system show
Центральный процессор                | Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
Число ядер процессора                | 4
Объем оперативной памяти             | 4277645312 байт (4079M)
Версия ПО ССПТ-4                     | FNP4 1.0.0-RELEASE (Mar  3 2021)
Заводской номер                      | 000000
Всего сетевых интерфейсов            | 10
    Фильтрующие интерфейсы           | 9: eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8
    Управляющий интерфейс            | включен, 10.41.2.120/255.255.255.128
Пакетная фильтрация                  | запущен (доступен)
Контроль целостности                 | запущен (доступен)
Авторизация                          | запущен (доступен)
Регистрация                          | запущен (доступен)
Резервирование                       | запущен (доступен)
Удаленное администрирование          | запущен (доступен)
WEB-интерфейс                        | запущен (доступен)
SNMP-интерфейс                       | запущен (доступен)
Тайм-аут неактивности администратора | 600 секунд
Просмотрщик по умолчанию FNPSH       | внутренний (internal)
Имя устройства                       | fnp4
Комментарий к устройству             |
```

В приведенном выводе отображается следующая информация:

- модель и частота центрального процессора;
- число ядер центрального процессора;
- объем оперативной памяти;
- версия ПО МЭ ССПТ-4А1;
- общее число сетевых интерфейсов;
- число фильтрующих интерфейса и список назначенных имен фильтрующих интерфейсов;
- IP-адрес, назначенный на управляющем интерфейсе, и состояние управляющего интерфейса;
- перечень подсистем МЭ ССПТ-4А1 и их состояний. Для каждой подсистемы указывается, запущена она или нет. В том случае, если подсистема запущена, указывается результат проверки доступности подсистемы;
- тайм-аут неактивности сеанса работы администратора;
- режим просмотра данных, используемый в данном сеансе работы администратора;
- назначенное имя устройства МЭ ССПТ-4А1 (FQDN);
- комментарий к устройству МЭ ССПТ-4А1.

Просмотр основных параметров конфигурации МЭ ССПТ-4А1 доступен в случае указания параметра **type=config** в команде **system show**, например:

```
fnp4> system show type=config
Управление сессиями                  | включено
```

```
Трансляция адресов (NAT)              | выключено
Аутентификация сетевых пользователей | выключено
HTTP-посредник                        | выключено
Использование прикладных правил       | включено
Использование правил приоритизации    | выключено
Регистрация пакетов                   | включено
Резервирование                        | выключено
RADIUS-авторизация                    | выключено
```

3.13.3. Просмотр информации о состоянии ресурсов УОС

Для просмотра информации о состоянии и характеристиках ресурсов УОС МЭ ССПТ-4А1 служит команда **`system status`**. Пример вывода данной команды представлен ниже:

```
fnp4> system status
Использование центрального процессора:
    Пользовательские процессы: 0,2%
    Приоритетные процессы:     0,0%
    Системные процессы:        0,2%
    Прерывания:                0,0%
    Простой:                   99,6%
Использование оперативной памяти:
    Активная:                  7,0M
    Неактивная:                138,0M
    Свободно:                  3615,0M
    Всего:                     4079M
Состояние разделов:
  Раздел:         0
    Использовано: 193M (21%)
    Свободно:     719M (79%)
    Всего:        991M
  Раздел:         1
    Использовано: 1,0K (100%)
    Свободно:     0B (0%)
    Всего:        1,0K
  Раздел:         2
    Использовано: 4,0K (0%)
    Свободно:     3,5G (100%)
    Всего:        3,5G
```

Пояснения к строкам вывода команды **`system status`** приведены в таблице 3.15, стр. 198.

Таблица 3.15: Информация, выводимая по команде "system status"

Строка вывода	***Описание***
Использование центрального процессора	Соотношение времени использования центрального процессора между различными активными процессами: пользовательскими, высокоприоритетными, системными и процессами обработки прерываний
Использование оперативной памяти	Распределение объема оперативной памяти: в активных страницах, в неактивных страницах, свободная память, всего установлено.
Состояние разделов	Информация о разделах файловых систем: занятое пространство, свободное пространство, общий объем раздела: • Раздел 0 – основной раздел на дисковом накопителе; • Раздел 1 – специальная файловая система устройств (devfs – Device File System), используется только УОС МЭ ССПТ-4А1; • Раздел 2 — файловая система в оперативной памяти (RAM-диск), используется для хранения временных файлов.

3.13.4. Системные дата и время

Для просмотра системной даты и времени, часового пояса, а также параметров синхронизации системного времени служит команда **system time show**, например:

```
fnp4> system time show
Настройки системного времени:
    Дата:                       09.03.2021, вторник
    Время:                      12:45:42
    Часовой пояс:               UTC, UTC+0000
    NTP:                        выключено
    NTP-сервер:                 не определено
    Регистрация сообщений NTP:  выключено
    Тайм-аут опроса NTP:        3600
```

Системная дата и время могут быть установлены администратором МЭ ССПТ-4А1 по команде **system time set**, например:

```
fnp4> system time set time=12:59:30
FNPSH-I-007.02.300F-Системное время изменено (09.03.2021 12:59:30 UTC+0000 (UTC))
```

Допустима установка только системного времени:

```
fnp4> system time set time=17:02:30
FNPSH-I-007.02.300F-Системное время изменено (22.06.2017 17:02:30 UTC+0300 (MSK))
```

Аналогично, допустима установка только системной даты:

```
fnp4> system time set date=09.03.2021
FNPSH-I-007.02.300F-Системное время изменено (09.03.2021 13:00:08 UTC+0000 (UTC))
```

Установка часового пояса. Для установки часового пояса служит команда **system time zone**. Команда запрашивает в интерактивном режиме и устанавливает новое значение часового пояса.

Выбор часового пояса осуществляется на основе многоуровневого меню, выводимого на экран терминала. Выбор пункта меню осуществляется путем ввода с клавиатуры номера пункта меню из предлагаемого списка и нажатия клавиши **<Enter>**.

Меню имеет следующие уровни:

1) континент/регион – выбор континента или географического региона Земли;
2) страна/регион – выбор страны или географического региона, расположенных на выбранном континенте/регионе;
3) часовой пояс – выбор часового пояса, проходящего через выбранную страну/регион.

> Отменить установку часового пояса можно на любом уровне меню, нажав клавишу **<Enter>**.
>
> Просмотреть текущие настройки часового пояса можно, используя команду **system time show**.

Ниже приводится пример установки Московского времени (часовой пояс MSK):

```
fnp4> system time zone
  [1] Africa
  [2] America - North and South
  [3] Antarctica
  [4] Arctic Ocean
  [5] Asia
  [6] Atlantic Ocean
  [7] Australia
  [8] Europe
  [9] Indian Ocean
  [10] Pacific Ocean
  [11] UTC
Выберите континент/регион (Отмена - <Enter>): 8
 [1] Albania             [18] Holy See           [35] Poland
 [2] Andorra             [19] Hungary            [36] Portugal
 [3] Austria             [20] Ireland            [37] Romania
 [4] Belarus             [21] Isle of Man        [38] Russian Federation
 [5] Belgium             [22] Italy              [39] San Marino
 [6] Bosnia and Herzegov [23] Jersey             [40] Serbia
 [7] Bulgaria            [24] Latvia             [41] Slovakia
 [8] Croatia             [25] Liechtenstein      [42] Slovenia
 [9] Czech Republic      [26] Lithuania          [43] Spain
 [10] Denmark            [27] Luxembourg         [44] Sweden
 [11] Estonia            [28] Macedonia (the for [45] Switzerland
 [12] Finland            [29] Malta              [46] Turkey
 [13] France             [30] Moldova (Republic  [47] Ukraine
 [14] Germany            [31] Monaco             [48] United Kingdom of
 [15] Gibraltar          [32] Montenegro         [49] Åland Islands
 [16] Greece             [33] Netherlands
 [17] Guernsey           [34] Norway
Выберите страну/регион (Отмена - <Enter>): 38
 [1] MSK-01 - Kaliningrad
 [2] MSK+00 - Moscow area
 [3] MSK+00 - Kirov
 [4] MSK+00 - Volgograd
 [5] MSK+01 - Astrakhan
 [6] MSK+01 - Saratov
 [7] MSK+01 - Ulyanovsk
 [8] MSK+01 - Samara, Udmurtia
 [9] MSK+02 - Urals
 [10] MSK+03 - Omsk
 [11] MSK+04 - Novosibirsk
 [12] MSK+04 - Altai
 [13] MSK+04 - Tomsk
 [14] MSK+04 - Kemerovo
 [15] MSK+04 - Krasnoyarsk area
 [16] MSK+05 - Irkutsk, Buryatia
 [17] MSK+06 - Zabaykalsky
 [18] MSK+06 - Lena River
 [19] MSK+06 - Tomponsky, Ust-Maysky
 [20] MSK+07 - Amur River
 [21] MSK+07 - Oymyakonsky
 [22] MSK+08 - Magadan
 [23] MSK+08 - Sakhalin Island
 [24] MSK+08 - Sakha (E); North Kuril Is
 [25] MSK+09 - Kamchatka
 [26] MSK+09 - Bering Sea
Выберите часовой пояс (Отмена - <Enter>): 2
FNPSH-I-007.02.3010-Часовой пояс изменен (MSK)
```

Настройки синхронизации времени по NTP. Функция синхронизация времени по NTP обеспечивает автоматическую синхронизацию системной даты и времени по протоколу NTP с заданным периодом. Синхронизация производится с удаленным NTP-сервером.

Для установки параметров синхронизации по NTP, а также включения или выключения синхронизации времени по NTP служит команда **`system time ntp set`**.

Ниже приводится пример минимально необходимой настройки синхронизации времени по NTP и включение синхронизации по NTP:

```
fnp4> system time ntp set server=10.41.0.242 state=enable
FNPSH-I-007.02.3014-Адрес NTP-сервера изменен
FNPSH-I-007.02.3011-NTP включен
```

Просмотреть параметры синхронизации по NTP и состояние синхронизации (включено/выключено) можно, выполнив команду **`system time show`**, например:

```
fnp4> system time show
Настройки системного времени:
    Дата:                       09.03.2021, вторник
    Время:                      16:03:14
    Часовой пояс:               MSK, UTC+0300
    NTP:                        включено
    NTP-сервер:                 10.41.0.242
    Регистрация сообщений NTP:  выключено
    Тайм-аут опроса NTP:        3600
```

Также по команде **`system time ntp set`** могут быть установлены следующие параметры синхронизации системного времени по NTP:

- Регистрация сообщений NTP – регистрация запросов синхронизации к NTP-серверу (включено/выключено);
- Тайм-аут опроса NTP – период синхронизации по NTP в секундах.

По умолчанию в текущей конфигурации МЭ ССПТ-4А1 выключены:
- синхронизация системного времени по протоколу NTP;
- регистрация запросов синхронизации времени к NTP-серверу в журнале регистрации системных сообщений.

Для успешного выполнения запросов NTP-сервер должен быть доступен через управляющий Ethernet-интерфейс МЭ ССПТ-4А1.

Если IP-адрес NTP-сервера не принадлежит подсети управляющего Ethernet-интерфейса, администратором должен быть добавлен соответствующий маршрут с помощью команды **system route add**.

Доступность NTP-сервера по его IP-адресу можно проверить, используя команду **interface control ping**

IP-адрес NTP-сервера должен быть установлен до включения синхронизации по NTP либо одновременно с включением синхронизации по NTP (посредством указания параметра **server** в команде **system time ntp set**).

По команде **`system time ntp set`** также может быть включена (или выключена) регистрация NTP-запросов, например:

```
fnp4> system time ntp set log=enable
FNPSH-I-007.02.3015-Регистрация сообщений NTP включена
```

Регистрация NTP-запросов заключается в регистрации системного сообщения при каждом обращении к NTP-серверу. Например:

```
Jun 22 19:10:03 fnp4 fnp4[12679]: fnp4_csd: I-1013: Синхронизация времени по NTP
- 192.168.1.254, -0.053047 sec
```

Просмотр системных сообщений выполняется по команде **log syslog show**

Параметры синхронизации времени по NTP могут быть удалены из текущей конфигурации МЭ ССПТ-4А1 по команде **`system time ntp delete`**.

В результате выполнения команды **system time ntp delete** параметры синхронизации системного времени по NTP будут установлены в значения по умолчанию. Синхронизация системного времени по NTP будет выключена.

Если параметр **server** не указан в команде **system time ntp update**, то будет использован IP-адрес NTP-сервера, установленный в текущей конфигурации МЭ ССПТ-4А1 по команде **system time ntp set**.

Например:

```
fnp4> system time ntp delete
Удалить параметры NTP? (Y/N) [N]: Y
FNPSH-I-007.02.3013-Параметры NTP удалены
fnp4> system time show
Настройки системного времени:
    Дата:                       09.03.2021, вторник
    Время:                      15:54:38
    Часовой пояс:               MSK, UTC+0300
    NTP:                        выключено
    NTP-сервер:                 не определено
    Регистрация сообщений NTP:  выключено
    Тайм-аут опроса NTP:        3600
```

МЭ ССПТ-4А1 позволяет выполнять немедленную синхронизацию времени с NTP-сервером. Для этого служит команда **`system time ntp update`**, например:

```
fnp4> system time ntp update
FNPSH-I-007.02.3018-Системное время изменено по NTP (offset -0.000809 sec)
```

При выполнении немедленной синхронизации времени с NTP-сервером в журнале регистрации событий регистрируется соответствующее событие:

```
22.06.2017 18:03:35 UTC+0300 (MSK) | I-1013: Синхронизация времени по NTP -
192.168.1.254, -0.021475 sec (admin,10.98.100.250)
```

3.13.5. Настройки управляющего интерфейса

Установка параметров управляющего интерфейса. Для установки параметров управляющего Ethernet-интерфейса МЭ ССПТ-4А1 служит команда **`interface control set`**. Данная команда позволяет установить следующие параметры управляющего Ethernet-интерфейса МЭ ССПТ-4А1:

- **`address`** – IP-адрес и маска подсети;
- **`duplex`** – режим передачи;
- **`media`** – скорость передачи;

- **`mtu`** – MTU (Maximum transmission unit);
- **`state`** – состояние управляющего интерфейса (включен/выключен).

По умолчанию управляющему Ethernet-интерфейсу МЭ ССПТ-4А1 назначен IP-адрес **10.234.28.71** с сетевой маской **255.255.0.0**.

В команде **`interface control set`** должен быть указан, как минимум, один из перечисленных параметров. Ниже представлен пример команды, устанавливающей IP-адрес, скорость передачи и MTU:

```
fnp4> interface control set address=10.2.1.1/255.255.255.128 media=autoselect mtu=2000
Изменить параметры управляющего интерфейса? (Возможна потеря соединения) (Y/N) [N]: y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (10.2.1.1)
FNPSH-I-007.02.306B-Скорость передачи управляющего интерфейса изменена (autoselect)
FNPSH-I-007.02.3104-MTU управляющего интерфейса изменено (2000)
FNPSH-I-007.02.3003-Завершение работы администратора (admin)
```

При установке IP-адреса управляющего Ethernet-интерфейса МЭ ССПТ-4А1 сеанс администратора автоматически завершается в случае удаленного администрирования во избежание ситуации, когда привилегии администратора на запись (admin или full) окажутся временно занятыми в случае потери связности между управляющим компьютером администратора и экземпляром МЭ ССПТ-4А1

Если новый IP-адрес управляющего Ethernet-интерфейса принадлежит другой подсети, то маршрут по умолчанию на управляющем интерфейсе, в случае его наличия, удаляется из маршрутной таблицы и администратору потребуется добавить его заново с помощью команды **system route add** (см. раздел 3.13.8 Маршрутная таблица, стр. 211).

Просмотр настроек управляющего интерфейса. Для просмотра настроек управляющего Ethernet-интерфейса МЭ ССПТ-4А1 служит команда **`interface control show`**. Например:

```
fnp4> interface control show
Интерфейс:                      управляющий
    Настроено:
        Состояние:              включено
        IP-адрес:               10.41.2.120
        IP-маска:               255.255.255.128
        Шлюз по умолчанию:      10.41.2.126
        Скорость передачи:      autoselect
        MTU:                    1500 (72-9000)
        Агрегирование портов:   выключено
        Протокол агрегирования: failover
        Интерфейс агрегата:     eth0
        Список доступа:         любой
    Определено:
        Состояние:              включено
        IP-адрес:               10.41.2.120
        IP-маска:               255.255.255.128
        Шлюз по умолчанию:      10.41.2.126
        Скорость передачи:      autoselect
        MTU:                    1500
        Несущая:                активна
```

Настройки управляющего Ethernet-интерфейса определяются по двум источникам;

- **`Настроено`** – настройки управляющего Ethernet-интерфейса в текущей конфигурации МЭ ССПТ-4А1;

- **Определено** – текущие системные настройки и состояние управляющего Ethernet-интерфейса.

В группе настроек “**Настроено**” строка “**MTU**” позволяет узнать диапазон допустимых значений MTU для управляющего Ethernet-интерфейса, который указывается в скобках после значения, установленного в текущей конфигурации.. В приведенном примере: **72-9000**.

Просмотр допустимых скоростей передачи. Для просмотра перечня допустимых скоростей передачи (значение параметра **media** команды **interface control set**) служит команда interface control media list. Например:

```
fnp4> interface control media list
Поддерживаемая скорость передачи:
autoselect
```

В приведенном примере управляющий Ethernet-интерфейс поддерживает единственное значение скорости передачи: **autoselect**. Как правило, поддерживается несколько скоростей передачи.

Проверка доступности узла сети. Для проверки доступности узла сети с управляющего интерфейса служит команда **interface control ping**. Доступность проверяется на основе отправки эхо-запросов и ожидания эхо-ответов по протоколу ICMP по аналогии с утилитой **ping**. Например:

```
fnp4> interface control ping host=10.41.2.126
PING 10.41.2.126: 56 байт данных
64 bytes from 10.41.2.126: seq=0, ttl=64, rtt=0,266 ms
64 bytes from 10.41.2.126: seq=1, ttl=64, rtt=0,494 ms
64 bytes from 10.41.2.126: seq=2, ttl=64, rtt=0,697 ms

--- 10.41.2.126 ping statistics ---
3 packets transmitted, 3 packets received,
round-trip min/avg/max/stddev = 0,266/0,486/0,697/0,176 ms
```

По умолчанию команда **interface control ping** выполняет **3** эхо-запроса. Можно явно указать число эхо-запросов в команде с помощью параметра **number**.

Отправку эхо-запросов можно прервать в любой момент комбинацией клавиш **<Ctrl+C>**.

Перед использованием команды **interface control ping** необходимо назначить IP-адрес управляющему Ethenet-интерфейсу МЭ ССПТ-4А1 и включить его.

Для проверки доступности узла сети извне управляющей сети в маршрутной таблице МЭ ССПТ-4А1 должен присутствовать соответствующий маршрут. Работа с маршрутной таблицей МЭ ССПТ-4А1 рассматривается в разделе “Маршрутная таблица“ (раздел 3.13.8, стр. 211).

Список доступа к управляющему интерфейсу. МЭ ССПТ-4А1 поддерживает возможность ограничения доступа к управляющему Ethernet-интерфейсу на основе списка доступа. В случае наличия записей в списке доступа удаленное управление МЭ ССПТ-4А1 возможно только с адресов, включенных в этот список. В противном случае удаленное управление возможно с любого адреса.

Для добавления новой записи в список доступа служит команда **`interface control acl add`**.

Каждая запись списка доступа должна содержать информацию об IP-адресах, с которых разрешен доступ. Допускаются следующие варианты задания IP-адресов:

- одиночный IP-адрес;
- IP-подсеть;
- диапазон IP-адресов.

Пример добавления одиночного IP-адреса:

```
fnp4> interface control acl add address=10.98.100.250
Добавить первую запись в список доступа? (Возможна потеря соединения и доступа) (Y/N) [N]:
y
FNPSH-I-007.02.3019-Новая запись добавлена в список доступа
```

Пример добавления IP-подсети:

```
fnp4> interface control acl add address=10.2.1.1/255.255.255.128
FNPSH-I-007.02.3019-Новая запись добавлена в список доступа
```

Пример добавления диапазона IP-адресов:

```
fnp4> interface control acl add address=192.168.1.2-192.168.1.5
FNPSH-I-007.02.3019-Новая запись добавлена в список доступа
```

Перед добавлением **первой записи** в список доступа выводится соответствующее предупреждение, чтобы администратор мог убедиться, что IP-адрес управляющего компьютера удовлетворяет добавляемой записи, в противном случае возникнет мгновенная потеря соединения и доступа к управлению МЭ ССПТ-4А1.

Перед добавлением последующих записей предупреждение не выводится. Предполагается, что соответствующая запись уже была добавлена администратором МЭ ССПТ-4А1 в список доступа.

Список доступа может содержать не более **16** элементов.

Если список доступа не пустой, то доступ к управлению МЭ ССПТ-4А1 разрешается только с IP-адресов, удовлетворяющих какому-либо из элементов списка.

Для просмотра списка доступа к управляющему Ethernet-интерфейсу служит команда **`interface control acl show`**. Например:

```
fnp4> interface control acl show
Список доступа:
 1  10.98.100.250
 2  10.2.1.0/255.255.255.128
 3  192.168.1.2-192.168.1.5
Занято: 3       Свободно: 13
```

Для удаления элемента из списка доступа служит команда **`interface control acl delete`**. В данной команде посредством параметра **`number`** должен быть указан номер удаляемой записи, доступный в выводе команды **`interface control acl show`**, например:

```
fnp4> interface control acl delete number=3
Удалить запись из списка доступа? (Возможна потеря соединения и доступа) (Y/N) [N]: y
```

```
FNPSH-I-007.02.301B-Запись удалена из списка доступа
```

Перед удалением записи из списка доступа выводится предупреждение, чтобы администратор мог убедиться, что удаление данной записи не повлечет за собой потерею соединения и доступа к управлению МЭ ССПТ-4А1.

После выполнения команды **interface control acl clear** доступ к управлению МЭ ССПТ-4А1 будет разрешен с любого IP-адреса.

Для очистки списка доступа служит команда **`interface control acl clear`**. Например:

```
fnp4> interface control acl clear
Очистить списка доступа? (Y/N) [N]: y
FNPSH-I-007.02.301A-Список доступа очищен
```

3.13.6. Настройки фильтрующих интерфейсов

Установка параметров фильтрующих интерфейсов. Для установки параметров фильтрующих Ethernet-интерфейсов МЭ ССПТ-4А1 служит команда **`interface filter set`**. Данная команда позволяет установить следующие параметры фильтрующих Ethernet-интерфейсов:

- **`duplex`** – режим передачи;
- **`media`** – скорость передачи;
- **`mtu`** – MTU (Maximum transmission unit);
- **`state`** – состояние управляющего интерфейса (включен/выключен).

В команде **`interface filter set`** должен быть указан, как минимум, один из перечисленных параметров. Параметр **`interface`** позволяет указать конкретный фильтрующий Ethernet-интерфейс, для которого будут установлены параметры, указанные в команде. В том случае если, параметр **`interface`** не указан в команде, установка параметров выполняется для всех фильтрующих Ethernet-интерфейсов МЭ ССПТ-4А1.

Пример включения и установки скорости передачи на всех фильтрующих Ethernet-интерфейсах:

```
fnp4> interface filter set state=enable media=autoselect
Изменить параметры всех фильтрующих интерфейсов? (Y/N) [N]: y
FNPSH-I-007.02.3068-Скорость передачи фильтрующего интерфейса изменена (Интерфейс: eth0,
autoselect)
FNPSH-I-007.02.301F-Фильтрующий интерфейс включен (eth0)
FNPSH-I-007.02.3068-Скорость передачи фильтрующего интерфейса изменена (Интерфейс: eth1,
autoselect)
FNPSH-I-007.02.301F-Фильтрующий интерфейс включен (eth1)
FNPSH-I-007.02.3068-Скорость передачи фильтрующего интерфейса изменена (Интерфейс: eth2,
autoselect)
```

Из приведенного фрагмента вывода видно, что для каждого установленного параметра каждого интерфейса выводится отдельное информационное сообщение.

Пример установки MTU для фильтрующих интерфейсов eth0 и eth1 соответственно:

```
fnp4> interface filter set interface=0 mtu=3000
Изменить параметры фильтрующего интерфейса? (Y/N) [N]: y
FNPSH-I-007.02.3105-MTU фильтрующего интерфейса изменено (Интерфейс: eth0, 3000)
fnp4> interface filter set interface=1 mtu=3000
Изменить параметры фильтрующего интерфейса? (Y/N) [N]: y
FNPSH-I-007.02.3105-MTU фильтрующего интерфейса изменено (Интерфейс: eth1, 3000)
```

Если необходимо установить MTU для всех фильтрующих интерфейсов, то удобно воспользоваться одним из следующих специальных значений параметр **mtu** команды **inteface filter set**:

- **align** – устанавливает максимальное общее значение MTU (допустимое для всех фильтрующих интерфейсов);
- **max** – устанавливает для каждого интерфейса максимальное значение MTU, поддерживаемое им (в этом случае установленные значения MTU могут отличаться для интерфейсов).

Просмотр настроек и текущего состояния фильтрующих интерфейсов. Для просмотра настроек и текущего состояния фильтрующих интерфейсов МЭ ССПТ-4А1 служит команда **`interface filter show`**. Если в команде указан параметр **`interface`**, то информации выводится только по выбранному интерфейсу. Параметр **`viewer`** позволяет выбрать режим просмотра для вывода. Например:

```
fnp4> interface filter show interface=0 viewer=no
Фильтрующие интерфейсы:

Интерфейс:                  0:eth0
    Настроено:
        Состояние:          включено
        Скорость передачи:  autoselect
        MTU:                3000 (72-16110)
        Зеркалирование      выключено
    Определено:
        Состояние:          включено
        Скорость передачи:  1000baseT/half-duplex
        MTU:                3000
        Несущая:            активна
```

При отсутствии в команде параметра **`interface`** выводится информация по всем фильтрующим интерфейсам.

Настройки фильтрующего интерфейса в выводе команды определяются по двум источникам:

- Настроено – настройки фильтрующего интерфейса в текущей конфигурации МЭ ССПТ-4А1:
  - ✔ состояние интерфейса – включен/выключен;
  - ✔ скорость и режим передачи;
  - ✔ MTU (Maximum Transmission Unit);
  - ✔ параметры зеркалирования;
- Определено – текущие системные настройки и состояние фильтрующего интерфейса:
  - ✔ состояние интерфейса – включен/выключен;
  - ✔ скорость и режим передачи;
  - ✔ MTU (Maximum Transmission Unit);
  - ✔ наличие несущей.

В группе настроек “**Настроено**” в строке “**MTU**” выводится диапазон допустимых значений MTU для интерфейса. В приведенном выводе: **72-16110**.

Просмотр допустимых скоростей передачи. Для просмотра перечня допустимых скоростей передачи (значение параметра **media** команды **interface filter set**) служит команда **interface filter media list**. Например:

```
fnp4> interface filter media list
Поддерживаемая скорость передачи:
eth0 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth1 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth2 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth3 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth4 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth5 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth6 : autoselect,1000baseT,100baseTX,10baseT/UTP
eth7 : autoselect,1000baseT,100baseTX,10baseT/UTP
```

С помощью параметра **interface** можно вывести перечень поддерживаемых скоростей конкретного фильтрующего интерфейса. Например:

```
fnp4> interface filter media list interface=1
Поддерживаемая скорость передачи:
eth1 : autoselect,1000baseT,100baseTX,10baseT/UTP
```

Если во время использования МЭ ССПТ-4А1 (устройство включено) выполняется установка (смена) SFP-модулей, то после установки (смены) SFP-модулей **необходимо** выполнить команду **“filter restart”**. В результате выполнения данной команды перечни допустимых скоростей передачи фильтрующих интерфейсов будут актуализированы в текущей конфигурации МЭ ССПТ-4А1.

Переименование фильтрующих интерфейсов. Изначально каждому фильтрующему интерфейсу назначено имя, соответствующее его номеру. Например, интерфейсу с номером 0 – **eth0**, интерфейсу с номером 1 – **eth1** и т. д.

Данные назначенные имена фильтрующих интерфейсов могут быть изменены администратором. Для этого служит команда **interface filter rename**. Например:

```
fnp4> interface filter rename interface=0 name=LAN_1
FNPSH-I-007.02.3022-Интерфейс переименован
```

Отметим, что назначенные имена интерфейсов выводятся по команде **interface filter show**, рассмотренной ранее в данном разделе. Например:

```
fnp4> interface filter show interface=0 viewer=no
Фильтрующие интерфейсы:

Интерфейс:                  0:LAN_1
    Настроено:
        Состояние:          включено
        Скорость передачи:  autoselect
        MTU:                1500 (72-16110)
        Зеркалирование      выключено
    Определено:
        Состояние:          включено
        Скорость передачи:  1000baseT/half-duplex
        MTU:                1500
        Несущая:            активна
```

Зеркалирование фильтрующих интерфейсов. В МЭ ССПТ-4А1 предусмотрена функция зеркалирования трафика, позволяющая перенаправлять копии пакетов на заданный фильтрующий интерфейс независимо от действия общего правила фильтрации, которым обработан пакет. Данная функция может быть полезна при необходимости отслеживания всего трафика, проходящего через какой-либо фильтрующий интерфейс, дополнительным средствами анализа, например, системой обнаружения вторжений или системой регистрации пакетов.

Зеркалируемый интерфейс – фильтрующий интерфейс, копии пакетов с которого требуется перенаправлять на другой, **зеркалирующий,** интерфейс.

Если в правилах фильтрации **зеркалирующий** интерфейс указывается в качестве выходного, то, в соответствии с таким правилом, на этот интерфейс будут передаваться пакеты, что при определенных условиях может привести к возникновению дублирующих пакетов на **зеркалирующем** интерфейсе.

Зеркалирующий интерфейс не может использоваться во **внутренних** и **внешних интерфейсах NAT** при использовании функции трансляции сетевых адресов (NAT).

Зеркалирующий и зеркалируемый интерфейсы не допускается использовать в качестве интерфейса **HTTP-посредника** и в качестве **интерфейса агрегата**.

Не допускается перенаправлять зеркалируемый трафик на используемый фильтрующий интерфейс.
Интерфейс, на который производится **зеркалирование** (**зеркалирующий**), перестает работать в режиме фильтрации, т.е. все пакеты, пришедшие на этот интерфейс из подключенного к нему сетевого сегмента, удаляются без обработки.

Для настройки параметров зеркалирования фильтрующих интерфейсов и включения функции зеркалирования служит команда **`interface filter mirror`**. Выполнив одну команду, можно установить параметры зеркалирования и включить либо выключить функцию зеркалирования. Например:

```
fnp4> interface filter mirror srcif=3 dstif=4 direction=in state=enable
Внимание! Зеркалирующий интерфейс не может использоваться, как фильтрующий!
Включить зеркалирование? (Y/N) [N]: y
FNPSH-I-007.02.3110-Настройки зеркалирования интерфейсов изменены (зеркалируемый интерфейс)
FNPSH-I-007.02.3110-Настройки зеркалирования интерфейсов изменены (зеркалирующий интерфейс)
FNPSH-I-007.02.3110-Настройки зеркалирования интерфейсов изменены (направление трафика)
FNPSH-I-007.02.3021-Зеркалирование интерфейсов включено
```

В результате выполнения приведенной команды:

- интерфейс с номером 3 назначается **зеркалируемым интерфейсом**;
- интерфейс с номером 4 назначается **зеркалирующим интерфейсом**;
- задается направление зеркалируемого трафика: зеркалировать только **входящий трафик** (**`direction=in`**);
- включается функция зеркалирования (**`state=enable`**).

Параметр **direction** (направление зеркалирования) команды **interface filter mirror** может принимать следующие значения:

- **all** – на зеркалирующий интерфейс будут передаваться копии входящих и исходящих пакетов зеркалируемого интерфейса;
- **in** – на зеркалирующий интерфейс будут передаваться копии только входящих пакетов зеркалируемого интерфейса;
- **out** – на зеркалирующий интерфейс будут передаваться копии только исходящих пакетов зеркалируемого интерфейса.

Настройки зеркалирования можно просмотреть по команде **`interface filter show`**, рассмотренной ранее в данном разделе. Например, в результате выполнения команды **`interface filter mirror`**, приведенной выше, настройки зеркалирования будут следующие (указываются среди параметров **зеркалирумого** и **зеркалирующего** интерфейсов):

```
Интерфейс:                  3:eth3
    Настроено:
        Состояние:          включено
        Скорость передачи: autoselect
        MTU:                1500 (72-16110)
        Зеркалирование      входящий в 4
    Определено:
        Состояние:          включено
        Скорость передачи: 1000baseT/half-duplex
        MTU:                1500
        Несущая:            активна

Интерфейс:                  4:eth4
    Настроено:
        Состояние:          включено
        Скорость передачи: autoselect
        MTU:                1500 (72-16110)
        Зеркалирование      входящий из 3
    Определено:
        Состояние:          включено
        Скорость передачи: 1000baseT/half-duplex
        MTU:                1500
        Несущая:            активна
```

Пример выключения функции зеркалирования:

```
fnp4> interface filter mirror state=disable
Выключить зеркалирование интерфейсов? (Y/N) [N]: y
FNPSH-I-007.02.3020-Зеркалирование интерфейсов выключено
```

3.13.7. Установка списка DNS-серверов

Для установки списка DNS-серверов служит команда **`system dns set`**, например:

```
fnp4> system dns set address=192.168.1.134,192.168.2.53
Установить список DNS-серверов? (Y/N) [N]: y
FNPSH-I-007.02.312D-Список DNS-серверов установлен
```

Список DNS-серверов должен быть установлен для работы HTTP-посредника МЭ ССПТ-4А1. Если использование HTTP-посредника не требуется, то список DNS-серверов может быть пустым (значение по умолчанию в текущей конфигурации МЭ ССПТ-4А1).

Просмотреть список DNS-серверов установленных, в текущей конфигурации МЭ ССПТ-4А1, можно по команде **`system dns show`**, например:

```
fnp4> system dns show
DNS-серверы
    1: 195.208.115.134
    2: 195.208.113.53
```

Список DNS-серверов может быть очищен по команде **`system dns clear`**, в результате которой список DNS-серверов станет пустым.

Список DNS-серверов может включать в себя не более **3 IP-адресов**.

Например:

```
fnp4> system dns clear
Очистить список DNS-серверов? (Y/N) [N]: y
FNPSH-I-007.02.312E-Список DNS-серверов очищен
fnp4> system dns show
DNS-серверы
```

3.13.8. Маршрутная таблица

Маршрутная таблица МЭ ССПТ-4А1 позволяет администратору задавать статические маршруты для:

- доступа управляющего Ethernet-интерфейса к различным сервисам (RADIUS, NTP, FTP и SYSLOG), находящимся вне управляющей сети МЭ ССПТ-4А1;
- доступа Ethernet-интерфейса HTTP-посредника к сети Интернет.

По умолчанию маршрутная таблица МЭ ССПТ-4А1 - пустая.

Максимальное число маршрутов в таблице – **1024**.

Маршрутная таблица МЭ ССПТ-4А1 может включать в себя не более одного маршрута по умолчанию. Данный маршрут применяется, если это единственный маршрут в таблице или если IP-адрес назначения в остальных маршрутах не соответствует IP-адресу назначения в пакете, который система УОС должна передать адресату.

Для добавления, как маршрута по умолчанию, так и обычного маршрута, служит команда **`system route add`**. В случае добавления маршрута по умолчанию параметр **`dst-address`** команды должен иметь значение **`0.0.0.0`**.

Например:

```
fnp4> system route add dst-address=0.0.0.0 gateway=10.2.1.126
FNPSH-I-007.02.312F-Маршрут добавлен
```

Для обычного маршрута в качестве значения параметра **`dst-address`** должен быть указан IP-адрес сети или узла сети, например:

```
fnp4> system route add dst-address=10.98.100.0/255.255.255.0 gateway=10.2.1.125
FNPSH-I-007.02.312F-Маршрут добавлен
```

Просмотреть маршрутную таблицу можно по команде **`system route show`**, например:

```
fnp4> system route show viewer=no
Таблица маршрутов:

number=1 dst-address=0.0.0.0 gateway=10.2.1.126 interface=ethc
number=2 dst-address=10.98.100.0/255.255.255.0 gateway=10.2.1.125 interface=ethc
```

В каждой записи маршрутной таблицы, помимо параметров **`dst-address`** (IP-адрес назначения) и **`gateway`** (IP-адрес шлюза), задаваемых через команду **`system route add`**, выводятся следующие параметры информационного характера:

- **`number`** – номер записи таблицы: используется для изменения или удаления существующей записи таблицы;
- **`interface`** – Ethernet-интерфейс МЭ ССПТ-4А1, через который будет отправлен IP-пакет в соответствии с данным маршрутом;

Маршрут по умолчанию, если он присутствует, при выводе маршрутной таблицы всегда имеет номер **1** (параметр **number**).

Параметр **interface** может иметь одно из следующих значений:
- ethc – маршрут использует управляющий Ethernet-интерфейс МЭ ССПТ-4А1;
- назначенное имя фильтрующего интерфейса МЭ ССПТ-4А1, используемого в качестве интерфейса HTTP-посредника;

При добавлении маршрута каждый раз производится сортировка маршрутов в таблице по возрастанию IP-адресов назначения (параметр **dst-address**).

При добавлении маршрута IP-адрес шлюза (параметр **gateway**) должен принадлежать либо сети управляющего Ethernet-интерфейса, либо сети Ethernet-интерфейса HTTP-посредника.

Таким образом, до добавления маршрута на соответствующем Ethernet-интерфейсе должен быть установлен IP-адрес.

В ранее добавленном маршруте может быть изменен IP-адрес шлюза (параметр **`gateway`**). Для этого служит команда **`system route edit`**, например:

```
fnp4> system route edit number=2 gateway=10.2.1.124
Изменить маршрут? (Y/N) [N]: y
FNPSH-I-007.02.3130-Маршрут изменен
fnp4> system route show viewer=no
Таблица маршрутов:

number=1 dst-address=0.0.0.0 gateway=10.2.1.126 interface=ethc
number=2 dst-address=10.98.100.0/255.255.255.0 gateway=10.2.1.124 interface=ethc
```

Для удаления маршрута служит команда **`system route delete`**, с указанием номера удаляемого маршрута (параметр **`number`**). Например:

```
fnp4> system route delete number=2
Удалить маршрут? (Y/N) [N]: y
FNPSH-I-007.02.3131-Маршрут удален
fnp4> system route show viewer=no
Таблица маршрутов:

number=1 dst-address=0.0.0.0 gateway=10.2.1.126 interface=ethc
```

Для удаления всех маршрутов из таблицы используется команда **`system route delete`** без параметра **`number`**.

> При удалении маршрута, использующего управляющий Ethernet-интерфейс, следует иметь в виду, что в случае удаленного администрирования извне управляющей сети произойдет потеря связности УК администратора и МЭ ССПТ-4А1.
>
> В связи с этим рекомендуется модифицировать маршрутную таблицу при администрировании через локальное подключение к МЭ.

Например:

```
fnp4> system route delete
Удалить все маршруты? (Y/N) [N]: y
FNPSH-I-007.02.3131-Маршрут удален
fnp4> system route show viewer=no
FNPSH-W-007.02.2018-Отсутствуют данные для вывода
```

Последнее диагностическое сообщение в примере свидетельствует о том, что маршрутная таблица – пустая.

3.13.9. Настройки использования интерфейсов удаленного администрирования

Использование WEB-интерфейса и SNMP-интерфейса администратора может быть включено или выключено администратором. Соответствующие параметры хранятся в текущей конфигурации, поэтому состояние использования интерфейса администрирования сохраняется после перезагрузки устройства.

> По умолчанию использование WEB-интерфейса и SNMP-интерфейса администратора включено в текущей конфигурации МЭ ССПТ-4А1.

WEB-интерфейс. Для выключения WEB-интерфейса администратора МЭ ССПТ-4А1 служит команда **`system web disable`**. Например:

```
fnp4> system web disable
FNPSH-I-007.02.30C3-WEB-интерфейс выключен
```

Проверить состояние использования WEB-итерфейса (и SNMP-интерфейса) можно, выполнив команду **`system show`**. Например:

```
fnp4> system show
Центральный процессор                | Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
Число ядер процессора                | 4
Объем оперативной памяти             | 4277645312 байт (4079M)
Версия ПО ССПТ-4                     | FNP4 1.0.0-RELEASE (Mar  3 2021)
Заводской номер                      | 000000
Всего сетевых интерфейсов            | 10
    Фильтрующие интерфейсы           | 9: eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8
    Управляющий интерфейс            | включен, 10.41.2.120/255.255.255.128
Пакетная фильтрация                  | запущен (доступен)
Контроль целостности                 | запущен (доступен)
Авторизация                          | запущен (доступен)
```

```
Регистрация                          | запущен (доступен)
Резервирование                       | запущен (доступен)
Удаленное администрирование          | запущен (доступен)
WEB-интерфейс                        | запущен (доступен)
SNMP-интерфейс                       | запущен (доступен)
Тайм-аут неактивности администратора | 600 секунд
Просмотрщик по умолчанию FNPSH       | внутренний (internal)
Имя устройства                       | fnp4
Комментарий к устройству             |
```

Из вывода видно, что WEB-интерфейс остановлен, т. к. до этого была выполнена команда **`system web disable`**.

Для включения WEB-интерфейса администратора МЭ ССПТ-4А1 служит команда **`system web enable`**. Например:

```
fnp4> system web enable
FNPSH-I-007.02.30C2-WEB-интерфейс включен
```

SNMP-интерфейс. Управление использованием SNMP-интерфейсом аналогично управлению использованием WEB-интерфейса. Для выключения SNMP-интерфейса служит команда **`system snmp disable`**, например:

```
fnp4> system snmp disable
FNPSH-I-007.02.30C5-SNMP-интерфейс выключен
```

Для включения SNMP-интерфейса служит команда **`system snmp enable`**, например:

```
fnp4> system snmp enable
FNPSH-I-007.02.30C4-SNMP-интерфейс включен
```

Кроме того, администратор может сменить пароль пользователя `fnpsnmp` SNMP-интерфейса. Для этого служит команда **`system snmp password`**.

Команда **system snmp password** может быть выполнена только администратором МЭ ССПТ-4А1 с идентификатором **admin**.

Например:

```
fnp4> system snmp password
Новый пароль:
Новый пароль повторно:
FNPSH-I-007.02.3065-Пароль пользователя SNMP-интерфейса изменен
```

При этом запрашивается двукратный ввод нового пароля пользователя SNMP-интерфейса.

3.13.10. Перезагрузка и выключение устройства

Для перезагрузки УОС МЭ ССПТ-4А1 служит команда **`system reboot`**, например:

```
fnp4> system reboot
Перезагрузить устройство? (Y/N) [N]: y
FNPSH-I-007.02.300E-Устройство будет перезагружено через две минуты. Выход ...
```

Не рекомендуется перезагружать МЭ ССПТ-4А1, используя кнопку аппаратного сброса (Reset), поскольку это может привести к серьезным нарушениям целостности файловой системы МЭ ССПТ-4А1.

МЭ ССПТ-4А1 также обеспечивает функцию **отложенной перезагрузки**. Данная функция позволяет осуществить перезагрузку МЭ ССПТ-4А1 через заданный интервал времени, при этом после перезагрузки автоматически будут применены заданная дополнительная конфигурация и/или заданная дополнительная политика доступа. Данная функция может быть полезна, например, для восстановления связности УК администратора с МЭ ССПТ-4А1 в том случае, если связность будет потеряна в результате некорректных действий администратора по конфигурированию МЭ ССПТ-4А1. Подразумевается, что администратор в инициирует отложенную перезагрузку до начала действий по конфигурированию МЭ ССПТ-4А1, которые могут повлечь потерю связности УК администратора с МЭ ССПТ-4А1.

Пример выполнения отложенной перезагрузки с применением дополнительной конфигурации и дополнительной политики:

```
fnp4> system reboot timeout=00:40:00 config=cfg1 policy=policy1
Инициировать отложенную перезагрузку? (Y/N) [N]: y
FNPSH-I-007.02.3141-Отложенная перезагрузка инициирована
```

В результате выполнения указанной команды была инициирована отложенная перезагрузка со следующими параметрами:

- интервал времени до отложенной перезагрузки: **`40`** минут;
- дополнительная конфигурация для применения: **`cfg1`**;
- дополнительная политика для применения: **`policy1`**.

Для выполнения отложенной перезагрузки в команде **system reboot** должен быть указан параметр **timeout** и хотя бы один из параметров: **config** и **policy**.

Отложенная перезагрузка может быть отменена администратором до момента ее выполнения. Время, оставшееся до выполнения отложенной перезагрузки, можно узнать, выполнив команду **`system show`**. Например:

```
fnp4> system show
Центральный процессор                | Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
Число ядер процессора                | 4
Объем оперативной памяти             | 4277645312 байт (4079M)
Версия ПО ССПТ-4                     | FNP4 1.0.0-RELEASE (Mar  3 2021)
Заводской номер                      | 000000
Всего сетевых интерфейсов            | 10
    Фильтрующие интерфейсы           | 9: eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8
    Управляющий интерфейс            | включен, 10.41.2.120/255.255.255.128
Пакетная фильтрация                  | запущен (доступен)
Контроль целостности                 | запущен (доступен)
Авторизация                          | запущен (доступен)
```

```
Регистрация                          | запущен (доступен)
Резервирование                       | запущен (доступен)
Удаленное администрирование          | запущен (доступен)
WEB-интерфейс                        | запущен (доступен)
SNMP-интерфейс                       | запущен (доступен)
Тайм-аут неактивности администратора | 600 секунд
Просмотрщик по умолчанию FNPSH       | внутренний (internal)
Имя устройства                       | fnp4
Комментарий к устройству             |
Отложенная перезагрузка              | 00:34:35
```

В том случае, если администратором была инициирована отложенная перезагрузка, то в выводе команды присутствует дополнительная строка (последняя), в которой указано количество времени, оставшееся до выполнения отложенной перезагрузки.

Для отмены ранее инициированной отложенной перезагрузки администратору необходимо выполнить команду **`system reboot`** с параметром **`timeout`**, установленным в специальное значение **`disable`**. Например:

```
fnp4> system reboot timeout=disable
Отменить отложенную перезагрузку? (Y/N) [N]: y
FNPSH-I-007.02.3142-Отложенная перезагрузка отменена
```

В журнале событий МЭ ССПТ-4А1 регистрируется, как событие об *инициировании отложенной перезагрузки*, так и событие о ее *отмене*. Для первого события указываются также интервал времени до перезагрузки, имя дополнительной конфигурации и/или дополнительной политики.

Останов УОС МЭ ССПТ-4А1 и выключение питания МЭ ССПТ-4А1 выполняется по команде **`system halt`**. Например:

```
fnp4> system halt
Выключить устройство? (Y/N) [N]: y
FNPSH-I-007.02.300D-Устройство будет выключено через две минуты. Выход ...
FNPSH-I-007.02.3003-Завершение работы администратора (admin)
```

Не рекомендуется выключать МЭ ССПТ-4А1 без останова УОС, используя выключатель питания на корпусе МЭ ССПТ-4А1, поскольку это может привести к серьезным нарушениям целостности файловой системы МЭ ССПТ-4А1.

3.13.11. Сброс настроек устройства

МЭ ССПТ-4А1 предоставляет возможность сброса настроек устройства, который включает в себя следующие действия:

- сброс текущей конфигурации МЭ ССПТ-4А1 в состояние по умолчанию;
- сброс текущей политики доступа МЭ ССПТ-4А1 в состояние по умолчанию;
- сброс базы данных учетных записей администраторов МЭ ССПТ-4А1 в состояние по умолчанию (остается единственная учетная запись `admin` с паролем по умолчанию);
- сброс базы данных учетных записей сетевых пользователей МЭ ССПТ-4А1 в состояние по умолчанию (отсутствие сетевых пользователей);

- сброс пароля системного пользователя `fnpsh` УОС МЭ ССПТ-4А1 в состояние по умолчанию;
- сброс пароля пользователя `fnpsnmp` SNMP-интерфейса МЭ ССПТ-4А1 в состояние по умолчанию;
- сброс таблицы маршрутизации в состояние по умолчанию (пустая таблица);
- сброс списка DNS-серверов (пустой список);
- удаление с устройства всех дополнительных конфигураций;
- удаление с устройства всех дополнительных политик доступа, за исключением политик: `policy_drop` и `policy_accept`.

Таким образом, изделие приводится к состоянию на момент первого включения.

Перед выполнением сброса настроек устройства рекомендуется выгрузить с МЭ ССПТ-4А1 все необходимые дополнительные конфигурации и политики доступа, так как они будут удалены из файловой системы устройства.

Все необходимые учетные записи администраторов и сетевых пользователей МЭ ССПТ-4А1 после сброса настроек должны быть добавлены заново администратором **admin**.

Для сброса настроек устройства служит команда **`system default`**. Например:

```
fnp4> system default
Сбросить настройки устройства? (Возможна потеря соединения) (Y/N) [N]: y
```

В приведенном примере на терминал не было выведено диагностическое сообщение о сбросе настроек изделия, т. к. команда была выполнена в рамках сеанса удаленного администрирования, по причине чего произошла потеря связности между УК и МЭ ССПТ-4А1.

В случае успешного сброса всех настроек МЭ ССПТ-4А1 в журнале регистрации событий будет зарегистрировано соответствующее сообщение:

```
23.06.2017 13:45:33 UTC+0000 (UTC) | I-152C: Сброс настроек устройства
(admin,10.2.1.2)
```

В случае ошибки при выполнении какого-либо действия по сбросу настроек МЭ ССПТ-4А1 (перечень действий перечислен выше) будет зарегистрировано соответствующее сообщение с информацией о невыполненных действиях. Например:

```
23.06.2017 13:55:01 UTC+0000 (UTC) | W-2015: Настройки устройства сброшены
частично - Ошибки при сбросе: дополнительные конфигурации и политики, пароль
системного пользователя (admin,10.2.1.2)
```

3.13.12. Просмотр ключевой информации

Для просмотра ключевой информации (ключи и сертификаты) данного экземпляра МЭ ССПТ-4А1 служит команда **`system key show`**. По команде выводится следующая ключевая информация в указанном порядке:

- сертификат удостоверяющего центра;
- сертификат экземпляра МЭ ССПТ-4А1;

- параметры Диффи-Хеллман (Diffie-Hellman) экземпляра МЭ ССПТ-4А1;
- открытий ключ Диффи-Хеллман (Diffie-Hellman) экземпляра МЭ ССПТ-4А1.

Сертификат удостоверяющего центра и экземпляра МЭ ССПТ-4А1 используются при управлении МЭ ССПТ-4А1 через WEB-интерфейс администратора и через интерфейс FNPCP. Данные сертификаты доступны к выгрузке на УК администратора посредством WEB-интерфейса.

Файл параметров и открытий ключ Диффи-Хеллман (Diffie-Hellman) экземпляра МЭ ССПТ-4А1 используются при аутентификации сетевых пользователей. Они также доступны к выгрузке посредством WEB-интерфейса.

Команда **`system key show`** использует внутренний просмотрщик (полноэкранный режим просмотра данных) для вывода ключевой информации, описанной выше. Соответственно, для вертикальной и горизонтальной прокрутки выводимых данных доступны стандартные клавиши внутреннего просмотрщика (раздел 3.1.8, стр. 62). Фрагмент вывода команды **`system key show`** приведен на рисунке 3.25, стр. 218.

```
16:02:19                    Сертификаты и ключи                    09.03.2021

-----------------------------------------------------------------
Сертификат Удостоверяющего Центра (SSL):
        Version: 3 (0x2)
        Serial Number: 68736385026 (0x1001020002)
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: C=RU, ST=Russian Federation, L=Saint-Petersburg, O=NPO Fractel,
        Validity
            Not Before: Nov  8 16:27:07 2019 GMT
            Not After : Dec 31 23:59:59 2039 GMT
        Subject: C=RU, ST=Russian Federation, L=Saint-Petersburg, O=NPO Fractel,
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:f1:bc:d2:bc:c8:3e:c8:d6:98:ea:e9:18:96:69:
                    a4:ee:35:11:d6:68:bc:a0:60:1a:cb:64:51:c0:09:
                    85:cb:ae:33:2f:7c:70:93:ed:2e:bf:21:02:d0:52:
                    f4:89:0e:da:cd:8b:cf:5b:ba:38:0f:a3:61:c8:13:
                    aa:00:b2:27:2e:43:05:53:8f:b8:a7:05:06:84:ff:
                    ff:02:fc:a6:45:e5:1d:7e:8a:12:5d:8e:ef:92:82:
                    12:66:06:f0:2c:5f:75:a4:7e:4c:2d:44:33:66:31:
                    38:d0:71:9a:37:ed:80:21:f5:44:66:2e:e6:f6:b0:
Строки: 1-23 из 178          Столбцы: 1-80    H - справка  Q, F10 - выход
```

Рисунок 3.25: Фрагмент вывода ключевой информации МЭ ССПТ-4А1

3.14. Агрегирование портов управляющего интерфейса

МЭ ССПТ-4А1 поддерживает функцию **агрегирования портов управляющего интерфейса**. Данная функция позволяет организовать **агрегат**, включающий в себя управляющий интерфейс и один из фильтрующих интерфейсов. Агрегирование портов

управляющего интерфейса обеспечивает резервирование управляющего интерфейса МЭ ССПТ-4А1: если выходит из строя один из интерфейсов, входящих в состав агрегата, то будет использоваться второй интерфейс. Кроме того, допускается совместное использование обоих интерфейсов в составе агрегата. Режим использования интерфейсов в составе агрегата определяется **протоколом агрегирования**, который может быть изменен администратором.

По умолчанию функция агрегирования портов управляющего интерфейса выключена в текущей конфигурации МЭ ССПТ-4А1.

Для включения функции агрегирования портов управляющего интерфейса служит команда **`interface control lagg`**, например:

```
fnp4> interface control lagg state=enable
Включить агрегирование портов управляющего интерфейса? (Y/N) [N]: y
FNPSH-I-007.02.313D-Агрегирование портов управляющего интерфейса включено
```

Убедиться в том, что агрегирование было включено, можно, воспользовавшись командой **`interface control show`**. Например:

```
fnp4> interface control show
Интерфейс:                      управляющий
    Настроено:
        Состояние:              включено
        IP-адрес:               10.41.2.120
        IP-маска:               255.255.255.128
        Шлюз по умолчанию:      10.41.2.126
        Скорость передачи:      autoselect
        MTU:                    1500 (72-9000)
        Агрегирование портов:   включено
        Протокол агрегирования: failover
        Интерфейс агрегата:     eth0
        Список доступа:         любой
    Определено:
        Состояние:              включено
        IP-адрес:               10.41.2.120
        IP-маска:               255.255.255.128
        Шлюз по умолчанию:      10.41.2.126
        Скорость передачи:      ethC autoselect
                                eth0 autoselect
        MTU:                    ethC 1500
                                eth0 1500
        Несущая:                ethC активна
                                eth0 активна
```

В приведенном выводе команды в секции “`Настроено`” строка “`Агрегирование портов`” свидетельствует о том, что функция агрегирования включена. Следующая строка предоставляет информацию об установленном протоколе агрегирования — `failover` (значение по умолчанию). Следующая строка – фильтрующий интерфейс, используемый в составе агрегата. Поскольку протокол агрегирования и фильтрующий интерфейс в составе агрегата являются параметрами текущей конфигурации, то строки с их значениями отображаются как при включенном, так и при выключенном агрегировании портов. В секции “`Определено`”

предоставляется информация об IP-адресе, назначенном на агрегат, и о состоянии интерфейсов в составе агрегата:

- скорость передачи и режим передачи (если доступен);
- значение MTU (должно быть одинаковым у обоих интерфейсов в составе агрегата);
- наличие несущей на интерфейсе.

При первом включении функции **агрегирования портов управляющего интерфейса**, если явно не указано в команде, в составе агрегата будет использован фильтрующий интерфейс с нулевым номером **(Eth0)**.

Администратор имеет возможность сменить выбор фильтрующего интерфейса для использования в агрегате, но для этого функция **агрегирования портов управляющего интерфейса** должна быть вначале **выключена**.

При включении функции **агрегирования портов управляющего интерфейса** на агрегате автоматически устанавливается IP-адрес управляющего интерфейса из текущей конфигурации МЭ ССПТ-4А1. Также автоматически корректируются маршруты, использовавшие управляющий интерфейс: данные маршруты будут использовать **агрегат**.

При включении функции **агрегирования портов управляющего интерфейса** фильтрующий интерфейс, используемый в агрегате, перестает выполнять роль фильтрующего, т. е.:

- не используется в правилах фильтрации ни в качестве входного, ни выходного;
- не используется в резервировании (если резервирование включено);
- не может использоваться в зеркалировании интерфейсов;
- не может использоваться в интерфейсах NAT;
- не может использоваться в качестве интерфейса HTTP-посредника;

Если на момент включения функции агрегирования фильтрующий интерфейс агрегата уже используется в **зеркалировании**, **NAT** или **HTTP-посреднике**, то включение функции агрегирования не будет произведено с выводом соответствующего предупреждающего сообщения.

Для включения функции **агрегирования портов управляющего интерфейса** MTU управляющего интерфейса и фильтрующего интерфейса, предназначенного для использования в агрегате, должны иметь одинаковые значения.

При включении функции **агрегирования портов управляющего интерфейса** скорости передачи обоих интерфейсов в составе агрегата автоматически устанавливаются в **autoselect**.

Как было сказано выше, администратор МЭ ССПТ-4А1 может изменить протокол агрегирования. Поддерживаются следующие протоколы агрегирования:

- **`failover`**: трафик передается только через активный порт (основной (master) порт - первый порт в агрегате). **Протокол агрегирования по умолчанию**;
- **`broadcast`**: отправляет кадры на все порты агрегата и принимает кадры на любой порт агрегата;
- **`lacp`**: поддерживает IEEE 802.1AX (ранее 802.3ad) Link Aggregation Control Protocol (LACP), а также Marker Protocol;
- **`loadbalance`**: балансировка исходящего трафика на основе хеширования заголовков пакетов и прием входящего трафика на любой из активных портов агрегата;

- **roundrobin**: распределение исходящего трафика между всеми активными портами, используя планировщик типа round-robin и прием входящего трафика на любой из активных портов агрегата.

Для установки протокола агрегирования служит команда **interface control lagg** с указанием параметра **protocol**. Например:

```
fnp4> interface control lagg protocol=roundrobin
FNPSH-I-007.02.313F-Протокол агрегирования портов управляющего интерфейса изменен
```

Для смены фильтрующего интерфейса в составе агрегата предназначен параметр **interface** команды **interface control lagg**, но перед сменой интерфейса в составе агрегата функция агрегирования портов управляющего интерфейса должна быть выключена. Например:

```
fnp4> interface control lagg interface=5
FNPSH-W-007.02.204B-Необходимо выключить агрегирование портов управляющего интерфейса
fnp4> interface control lagg state=disable
Выключить агрегирование портов управляющего интерфейса? (Y/N) [N]: y
FNPSH-I-007.02.313E-Агрегирование портов управляющего интерфейса выключено
fnp4> interface control lagg interface=5
FNPSH-I-007.02.3140-Интерфейс агрегата изменен
fnp4> interface control lagg state=enable
Включить агрегирование портов управляющего интерфейса? (Y/N) [N]: y
FNPSH-I-007.02.313D-Агрегирование портов управляющего интерфейса включено
```

При включении функции **агрегирования портов управляющего интерфейса**, а также при смене **протокола агрегирования**, когда функции агрегирования уже включена, возможна потеря связности УК с МЭ ССПТ-4А1. В связи с этим данные операции рекомендуется производить при управлении через системную консоль (подключение через COM-порт).

Выше было отмечено, что при включении функции агрегирования портов управляющего интерфейса фильтрующий интерфейс в составе агрегата перестает выполнять функции фильтрующего интерфейса. В связи с этим данный фильтрующий интерфейс исключается из числа интерфейсов, выводимых по командам **inteface filter show** и **filter show**. Кроме того, при включенном агрегировании запрещается изменять параметры фильтрующего интерфейса, используемого в агрегате. Например, если интерфейс **eth5** используется в агрегате, то указанная команда завершится с ошибкой::

```
fnp4> interface filter set interface=eth5 media=1000baseT
FNPSH-E-007.02.105E-Фильтрующий интерфейс с заданным именем не найден
```

Информация об использовании функции агрегирования также отражается в выводе команды **system show**, например:

```
fnp4> system show
Центральный процессор                | Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
Число ядер процессора                | 4
Объем оперативной памяти             | 4277645312 байт (4079M)
Версия ПО ССПТ-4                     | FNP4 1.0.0-RELEASE (Mar  3 2021)
Заводской номер                      | 000000
Всего сетевых интерфейсов            | 10
    Фильтрующие интерфейсы           | 9: eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8
    Управляющий интерфейс            | включен, 10.41.2.120/255.255.255.128
                                     | агрегирование включено, failover, eth5
Пакетная фильтрация                  | запущен (доступен)
```

```
Контроль целостности                  | запущен (доступен)
Авторизация                           | запущен (доступен)
Регистрация                           | запущен (доступен)
Резервирование                        | запущен (доступен)
Удаленное администрирование           | запущен (доступен)
WEB-интерфейс                         | запущен (доступен)
SNMP-интерфейс                        | запущен (доступен)
Тайм-аут неактивности администратора  | 600 секунд
Просмотрщик по умолчанию FNPSH        | внутренний (internal)
Имя устройства                        | fnp4
Комментарий к устройству              |
```

Из приведенного вывода видно, что общее число сетевых интерфейсов данного экземпляра МЭ ССПТ-4А1 – 8, а число фильтрующих – 6, а не 7, т. к. eth5 используется в агрегате. Также данный интерфейс не выводится в списке фильтрующих. В случае использования функции агрегирования в выводе команды **`system show`** присутствует дополнительная строка, информирующая о том, что:

- функция агрегирования включена;
- использует указанный протокол агрегирования (в приведенном выводе – `failover`);
- использует в составе агрегата указанный фильтрующий интерфейс (в приведенном выводе – `eth5`).

4. WEB-интерфейс администратора

Стартовой страница WEB-интерфейса администратора содержит форму авторизации администратора. После прохождения процедуры авторизации (ввода имени администратора и пароля в соответствующие поля WEB-формы) открывается страница `Состояние: Устройство`. Страница `Состояние: Устройство` подробно рассматривается далее в разделе 4.1.1, стр. 224.

В верхней части любой страницы WEB-интерфейса (за исключением форм редактирования настроек и страниц вывода записей регистрации) содержится основное меню WEB-интерфейса, пункты которого расположены горизонтально в одну строку, и кнопка `Выход`.

Нажатие кнопки `Выход` приводит к выходу из WEB-интерфейса, то есть завершению сеанса работы администратора.

Нажатие некоторых кнопок WEB-интерфейса, требующих выполнения какого-либо действия, приводит к появлению диалогового окна с кнопками подтверждения этого действия или его отмены.

Кнопка *Справка* имеется внизу каждой страницы WEB-интерфейса, ее нажатие приводит к выводу справочной информации по соответствующей странице.

Основное меню WEB-интерфейса состоит из следующих пунктов:

- `Состояние`: просмотр состояния МЭ ССПТ-4А1. Состояние основных подсистем, информация об аппаратном и программном обеспечении, информация о настройках управляющего интерфейса и т.д.;
- `Настройки`: настройки функциональных возможностей МЭ ССПТ-4А1. Изменение параметров текущей конфигурации МЭ ССПТ-4А1;
- `Политика`: действия над текущей и дополнительными политиками доступа МЭ ССПТ-4А1;
- `Сессии`: настройки режима управления сессиями, просмотр и модификация таблицы сессий;
- `Регистрация`: просмотр регистрационной информации (события, пакеты, сессии, системные сообщения SYSLOG);
- `Отладка`: ввод команд МЭ ССПТ-4А1 без их интерпретации WEB-интерфейсом с целью отладки.

Ввод данных в WEB-интерфейсе для изменения параметров конфигурации МЭ ССПТ-4А1, добавления или редактирования сущностей (правила фильтрации, объекты справочника, учетные записи администраторов и т. д.) осуществляется через модальные окна, содержащие в себе формы. Далее в тексте используется термин *форма*, при этом подразумевается модальное окно с формой, например: форма добавления учетной записи администратора.

Каждая форма WEB-интерфейса имеет как минимум две кнопки:

- кнопка, находящаяся левее остальных, служит для применения изменений в форме, ее название может отличаться в зависимости от конкретной формы (при этом в зависимости от формы выполняется синтаксическая и/или семантическая проверка введенных данных);
- кнопка **Отмена** служит для закрытия формы без применения изменений.

В случае успешного применения данных, введенных в форму, выводится диалоговое окно без заголовка с соответствующим информационным сообщением командного интерпретатора МЭ ССПТ-4А1. Например:

```
FNPSH-I-007.02.3106-Имя устройства и/или комментарий к нему изменено
```

4.1. Состояние

Пункт меню `Состояние` содержит подменю, включающее в себя пункты:

- `Устройство` – управление устройством и информация о программном и аппаратном обеспечении устройства;
- `Фильтрация` – статистика обработки трафика;
- `Целостность` – информация о целостности компонентов операционной системы и программного обеспечения МЭ ССПТ-4А1;

Страницы, относящиеся к пункту `Состояние` основного меню, объединяет то, что все они предназначены для информирования администратора о текущем состоянии МЭ ССПТ-4А1 и не содержат элементов управления для изменения его текущей конфигурации.

4.1.1. Состояние: Устройство

Страница `Состояние: Устройство` приведена на рисунке 4.1, стр. 225.

На странице `Состояние: Устройство` выводится следующая информация:

- информация об устройстве:
- имя устройства (значение по умолчанию: **`fnp4`**),
- комментарий (значение по умолчанию: пустая строка);
- системная информация — информация о процессоре, объёме памяти, версии ПО МЭ, заводском номере экземпляра устройства, числе фильтрующих интерфейсов, системной дате и времени, установленном тайм-ауте неактивности администратора, при достижении которого происходит автоматическое завершение сеанса его работы;
- управляющий интерфейс – информация об управляющем интерфейсе (EthC):
  - ✔ IP адрес/маска;
  - ✔ наличие несущей, скорость передачи и режим работы;
  - ✔ состояние функции агрегирования портов управляющего интерфейсе (если агрегирование включено, то также протокол агрегирования и фильтрующий интерфейс в составе агрегата).

- состояние процессов — информация о состоянии основных процессов. Состояние процесса отображается индикатором, который может принимать следующий вид (цвет):
  - ✔ – процесс запущен и доступен (ответил на тестовое воздействие);
  - ✔ – процесс запущен, но не доступен (не ответил на тестовое воздействие);
  - ✔ – процесс остановлен.

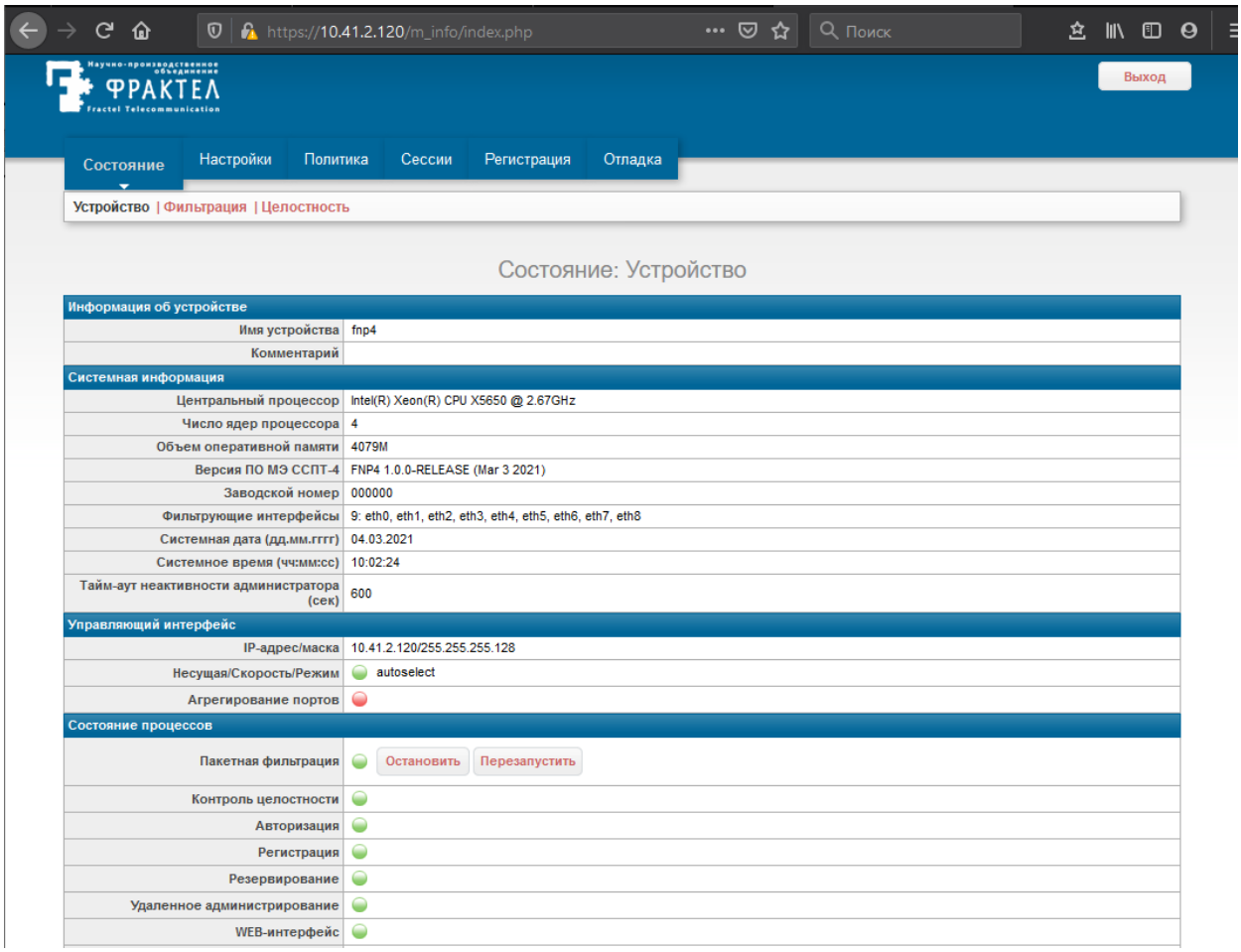


Рисунок 4.1: Страница Состояние: Устройство

Администратор может повлиять на состояние процесса `Пакетная фильтрация` при помощи кнопок:

- `Перезапустить`: останов процесса и его повторный запуск, при этом перечитываются файлы текущей конфигурации и текущей политики и сбрасывается текущая информация, используемая процессом (таблица сессий, статистика использования правил фильтрации, статистика трафика по фильтрующим интерфейсам).
- `Выключить`: останов процесса. В этом случае цветовой индикатор состояния процесса меняет цвет на красный, а вместо кнопок `Выключить` и `Перезапустить` появляется кнопка `Запустить` (нажатие которой приводит к запуску процесса).

Запуск и останов процессов: *WEB-интерфейс* и *SNMP-интерфейс* доступен только через командный интерфейс администратора и только для администратора *admin*.

Остальные процессы не могут быть остановлены администратором МЭ ССПТ-4А1 и должны функционировать всегда (зеленый индикатор).

В нижней части страницы `Состояние: Устройство` расположена секция `Управление`. Во второй строке секции расположены две кнопки:

- `Перезагрузить`: перезагрузка УОС МЭ ССПТ-4А1;
- `Выключить`: плановый останов УОС МЭ ССПТ-4А1 и выключение питания устройства.

В первой строке секции отображается состояние **функции отложенной перезагрузки устройства** в виде цветового индикатора:

- – отложенная перезагрузка была инициирована администратором (ожидается ее выполнение);
- – отложенная перезагрузка не инициирована администратором в настоящий момент (по умолчанию).

Справа, в той же строке, расположена кнопка `Редактировать`, по нажатию на которую открывается форма редактирования настроек отложенной перезагрузки. Форма, со значениями элементов ввода по умолчанию, приведена на рисунке 4.2, стр. 226.

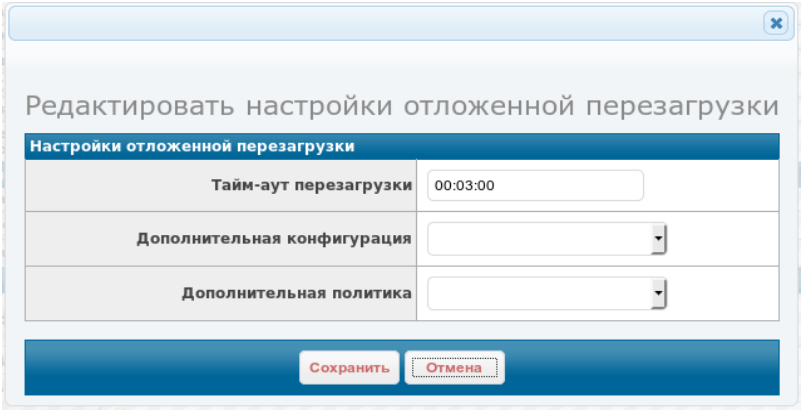


Рисунок 4.2: Форма редактирования настроек отложенной перезагрузки

Форма редактирования настроек отложенной перезагрузки содержит следующие элементы ввода данных:

- `Тайм-аут перезагрузки`: интервал времени до перезагрузки устройства (по умолчанию: **3 минуты**);
- `Дополнительная конфигурация`: список выбора дополнительной конфигурации для применения при отложенной перезагрузке (по умолчанию: **не выбрано**);

- Дополнительная политика: список выбора дополнительной политики для применения при отложенной перезагрузке (по умолчанию: **не выбрано**).

> Для того чтобы инициировать отложенную перезагрузку администратору необходимо выбрать *дополнительную конфигурацию* либо *дополнительную политику*. Допустим выбор обеих сущностей.
>
> Тайм-аут до выполнения перезагрузки устройства может быть установлен в диапазоне от **3** минут до **23** часов **59** минут **59** секунд.
>
> Интервал времени, оставшийся до перезагрузки устройства, не обновляется автоматически. Соответственно, чтобы увидеть актуальное значение данного интервала времени необходимо обновить страницу средствами WEB-браузера.

По нажатию на кнопку Сохранить инициируется отложенная перезагрузка устройства с указанными параметрами. При этом индикатор состояния отложенной перезагрузки меняет цвет с красного на зеленый и справа от него отображается интервал времени, оставшийся до перезагрузки устройства. Вместо кнопки Редактировать отображается кнопка Отменить, служащая для отмены отложенной перезагрузки устройства. Пример секции Управление устройством, после того как отложенная перезагрузка была инициирована администратором, приведен на рисунке 4.3, стр. 227.

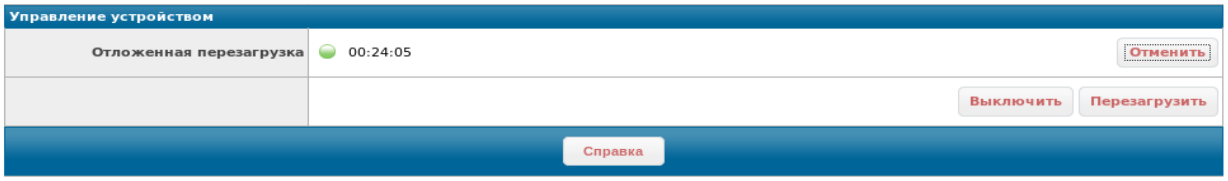


Рисунок 4.3: Управление устройством при инициированной отложенной перезагрузке

4.1.2. Состояние: Фильтрация

На странице Состояние: Фильтрация представлена информация о длительности процесса фильтрации, состоянии фильтрующих интерфейсов и статистические данные об обработанном трафике (по интерфейсам, типам кадров, протоколам).

Пример страницы Состояние: Фильтрация приведен на рисунке 4.4, стр. 228.

Страница Состояние: Фильтрация состоит из двух секций:

- Состояние фильтрации – текущее состояние пакетного фильтра МЭ ССПТ-4А1;
- Информация о трафике – состояние фильтрующих интерфейсов и общая статистика трафика.

В секции Состояние фильтрации расположены две строки:

- Фильтрация включена: дата и время запуска пакетного фильтра МЭ ССПТ-4А1
- Фильтрация продолжается: продолжительность работы пакетного фильтра МЭ ССПТ-4А1 с момента запуска.

В секции Информация о трафике расположена таблица, столбцами которой являются фильтрующие интерфейсы МЭ ССПТ-4А1, а в строках располагается следующая информация:

- Состояние: состояние несущей (есть/нет), скорость передачи и режим передачи, если доступен)
- Кадров/байт получено: общее количество кадров Ethernet/суммарный объем трафика, принятый на фильтрующих интерфейсах. *Далее следуют строки с количеством полученных кадров, пакетов, сообщений, дейтаграмм и т. д., а также суммарного объема трафика в них для различных протоколов различных уровней сетевого взаимодействия*.

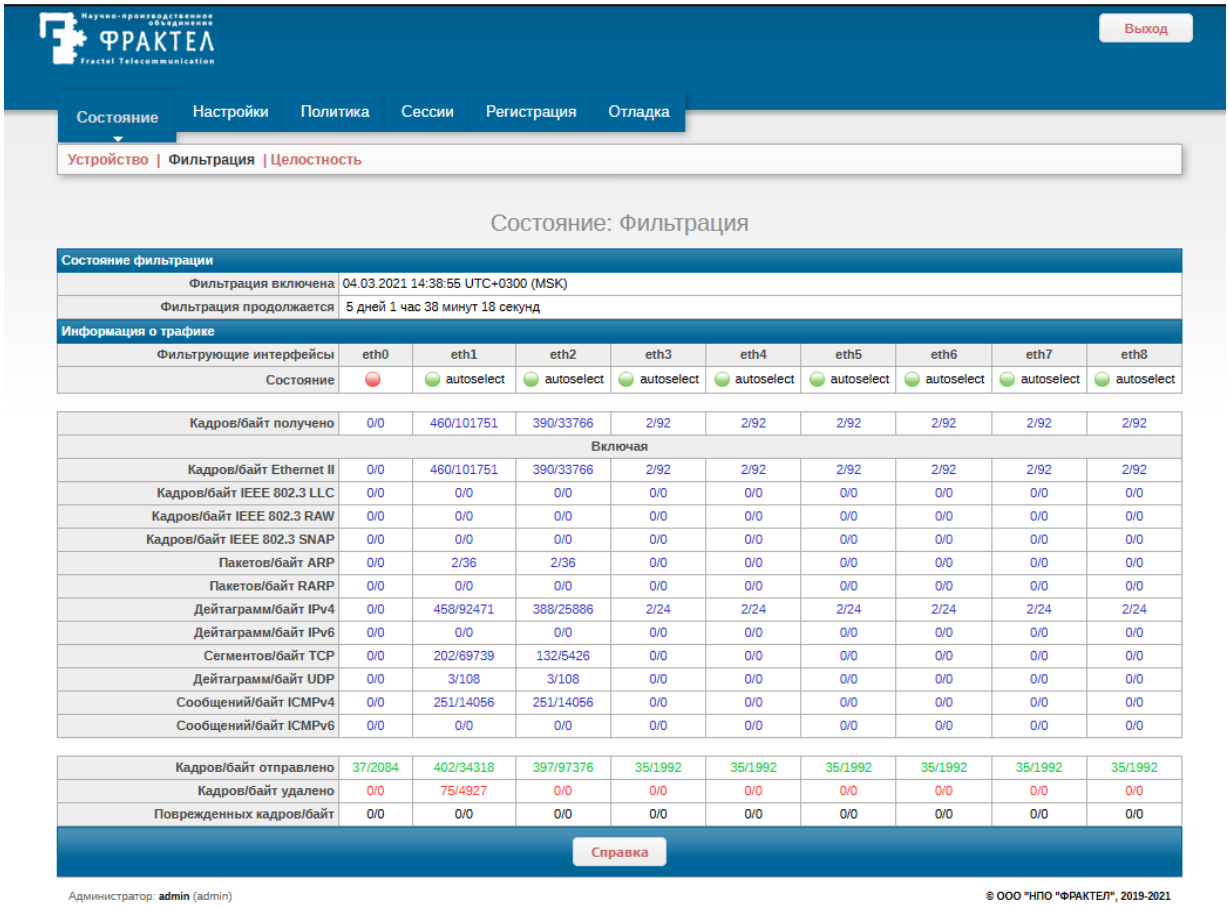


Рисунок 4.4: Страница Состояние: Фильтрация

Таблица завершается следующими тремя строками:

- Кадров/байт отправлено – общее количество кадров Ethernet/суммарный объем трафика, переданный на фильтрующие интерфейсы;
- Кадров/байт удалено – общее количество кадров Ethernet/суммарный объем трафика, удаленный пакетным фильтром МЭ ССПТ-4А1;
- Кадров/байт повреждено – общее количество кадров Ethernet/суммарный объем трафика с нарушенной внутренней структурой.

Информация на странице “*Состояние: Фильтрация*” не обновляется автоматически. Соответственно, чтобы увидеть актуальные данные необходимо обновить страницу средствами WEB-браузера.

Если пакетный фильтр выключен, то на странице *Состояние: Фильтрация* вместо информации о пакетном фильтре и таблицы со статистикой обработки трафика выводится диагностическое сообщение:

`FNPSH-W-007.02.2003-Пакетный фильтр выключен`

4.1.3. Состояние: Целостность

На странице “Состояние: Целостность” представлена информация о результате проверки целостности контролируемых файлов:

- цветовой индикатор;
- имя файла;
- контрольная сумма.

Перечень всех контролируемых файлов приведен в документе “*Программное обеспечение межсетевого экрана ССПТ-4А1. Описание программы. ФРПС.00014-01 13*” (раздел 3.3.8). Пример фрагмента страницы “Состояние: Целостность” приведен на рисунке 4.5, стр. 230.

В нормальном состоянии МЭ ССПТ-4А1 все цветовые индикаторы – зеленые. Появление одного или нескольких красных индикаторов свидетельствует о нарушении целостности соответствующих файлов. В этом случае процесс фильтрации автоматически останавливается, то есть пакеты перестают проходить через устройство. Администратору необходимо выключить устройство и принять меры, связанные с его восстановлением (ремонтом).

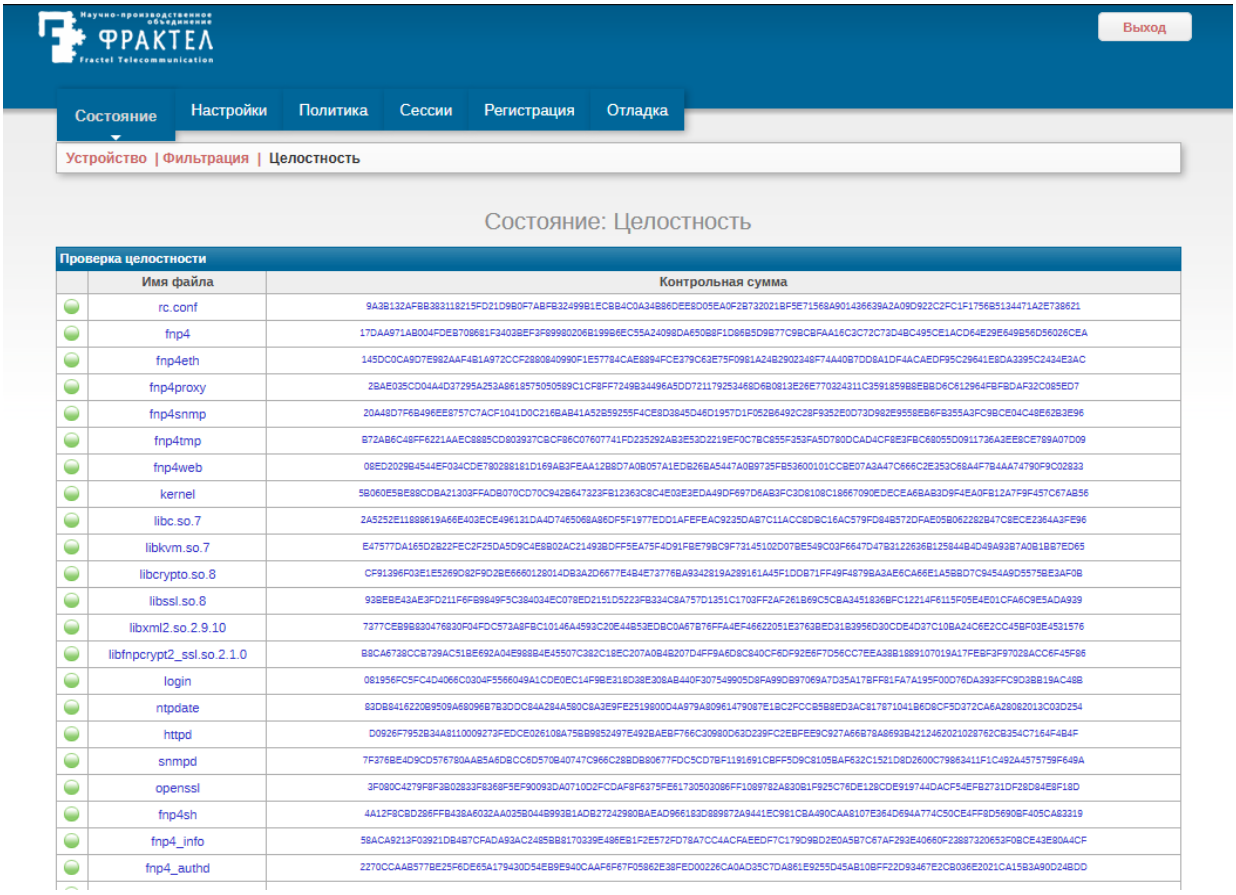


Рисунок 4.5: Фрагмент страницы “Состояние: Целостность”

4.2. Настройки

Страницы, относящиеся к пункту `Настройки` основного меню WEB-интерфейса, предназначены для настройки различных функциональных возможностей МЭ ССПТ-4А1 и соответственно для изменения параметров текущей конфигурации МЭ ССПТ-4А1.

Пункт меню `Настройки` включает в себя следующие подпункты, отвечающие за различные группы настроек МЭ ССПТ-4А1:

- `Устройство`: управление конфигурациями МЭ ССПТ-4А1, настройка системной даты, времени и часового пояса;
- `Администраторы`: управление учетными записями и сеансами работы администраторов МЭ ССПТ-4А1;
- `Интерфейсы`: управление настройками управляющего и фильтрующих интерфейсов;
- `NAT`: управление настройками функции трансляции сетевых адресов (NAT);
- `Сетевые пользователи`: управление учетными записями и сеансами работы сетевых пользователей МЭ ССПТ-4А1;
- `Регистрация`: управление настройками подсистемы регистрации;
- `Резервирование`: управление настройками работы подсистемы резервирования;

- RADIUS: настройка аутентификации администраторов и сетевых пользователей МЭ ССПТ-4А1 через RADIUS-сервер.

4.2.1. Настройки: Устройство

Страница Настройки: Устройство разделена на четыре секции. Ниже приведены данные секции и их предназначение:

- Устройство:
  - ✔ выгрузка файлов сертификатов УЦ и МЭ ССПТ-4А1 на управляющий компьютер;
  - ✔ установка символического имени и комментария для устройства МЭ ССПТ-4А1;
- Текущая конфигурация: управление текущей конфигурацией МЭ ССПТ-4А1;
- Дополнительные конфигурации: вывод информации и управление дополнительными конфигурациями МЭ ССПТ-4А1;
- Системная дата время: управление настройками системных даты и времени устройства МЭ ССПТ-4А1.

Секция “Устройство”. Пример секции Устройство представлен на рисунке 4.6, стр. 232.

В секции “Устройство” выводятся следующие параметры текущей конфигурации:

- Имя устройства – имя данного экземпляра устройства (по умолчанию: **fnp4**);
- Комментарий – комментарий к данному экземпляру устройства (по умолчанию: пустая строка).

Также в секции расположены две кнопки:

- Сертификаты;
- Переименовать.

По нажатию по кнопке **Переименовать** (рисунок 4.6, стр. 232) открывается окно переименования устройства с формой (далее для краткости будет использовано: *открывается форма*) для смены имени устройства и комментария к нему. Форма переименования устройства представлена на рисунке 4.7, стр. 232.

Форма переименования устройства содержит два поля ввода:

- Имя устройства: используется для смены имени данного экземпляра устройства (в приведенном примере: значение по умолчанию – **fnp4**);
- Комментарий: используется для смены комментария к данному экземпляру устройства (в приведенном примере: пустая строка – значение по умолчанию).

Форма переименования устройства имеет две кнопки:

- `Переименовать`: применение данных введенных в форму: смена имени и/или комментария к устройству;
- `Отмена`: закрытие формы без применения введенных данных (стандартное действие для всех форм).

При нажатии по кнопке **`Сертификаты`** секции “Устройство” (рисунок 4.6, стр. 232) открывается форма выгрузки сертификатов, представленная на рисунке 4.8, стр. 232.

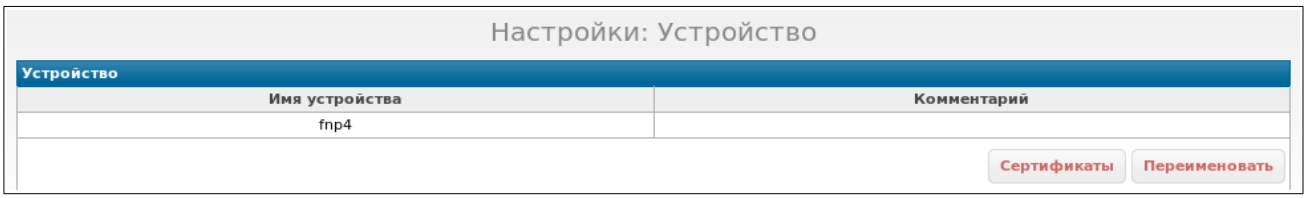


Рисунок 4.6: Секция “Устройство”

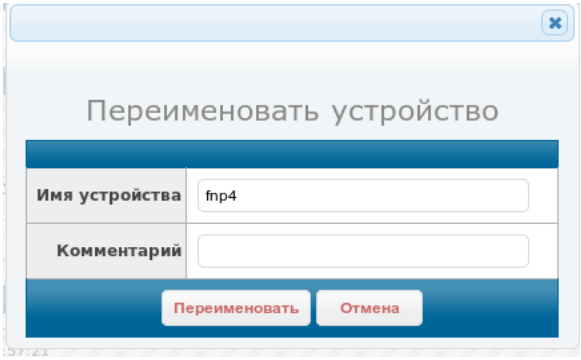


Рисунок 4.7: Форма переименования устройства

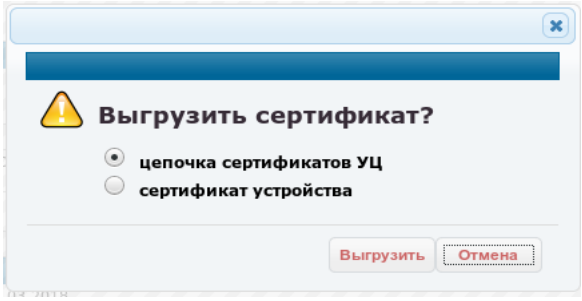


Рисунок 4.8: Форма выгрузки сертификатов

Предназначение формы выгрузки сертификатов ясно из ее названия – форма служит для выгрузки различных сертификатов с МЭ ССПТ-4А1 на УК администратора (далее – *УК*). Форма имеет переключатель (*radio button*) для выбора выгружаемых сертификатов:

- `цепочка сертификатов УЦ`: выгрузка файла цепочки сертификатов УЦ с именем `ca_chain.pem`;
- `сертификат устройства`: выгрузка файла сертификата устройства с именем `fnp4_cert.pem`.

По кнопке **`Выгрузить`** открывается стандартная форма WEB-браузера для сохранения файла на жесткий диск в соответствии со значением переключателя.

- Предназначение формы выгрузки сертификатов ясно из ее названия: форма служит для выгрузки различных сертификатов с МЭ ССПТ-4А1 на УК администратора (далее – *УК*). Форма имеет переключатель (*radio button*) для выбора выгружаемых сертификатов:

- `цепочка сертификатов УЦ`: выгрузка файла цепочки сертификатов УЦ с именем `ca_chain.pem`;
- `сертификат устройства`: выгрузка файла сертификата устройства с именем `fnp4_cert.pem`.

По кнопке **`Выгрузить`** открывается стандартная форма WEB-браузера для сохранения файла на жесткий диск в соответствии со значением переключателя.

Секция “Текущая конфигурация”, представленная на рисунке 4.9, стр. 233, содержит три кнопки:

- `Показать`: просмотр текущей конфигурации в выбранном представлении;
- `Сохранить`: сохранение текущей конфигурации в дополнительную;
- `Сбросить`: сброс текущей конфигурации в состояние по умолчанию.

При нажатии на кнопку **`Показать`** открывается окно просмотра текущей конфигурации. Окно просмотра текущей конфигурации приведено на рисунке 4.10, стр. 233.

Рисунок 4.9: Секция “Текущая конфигурация”

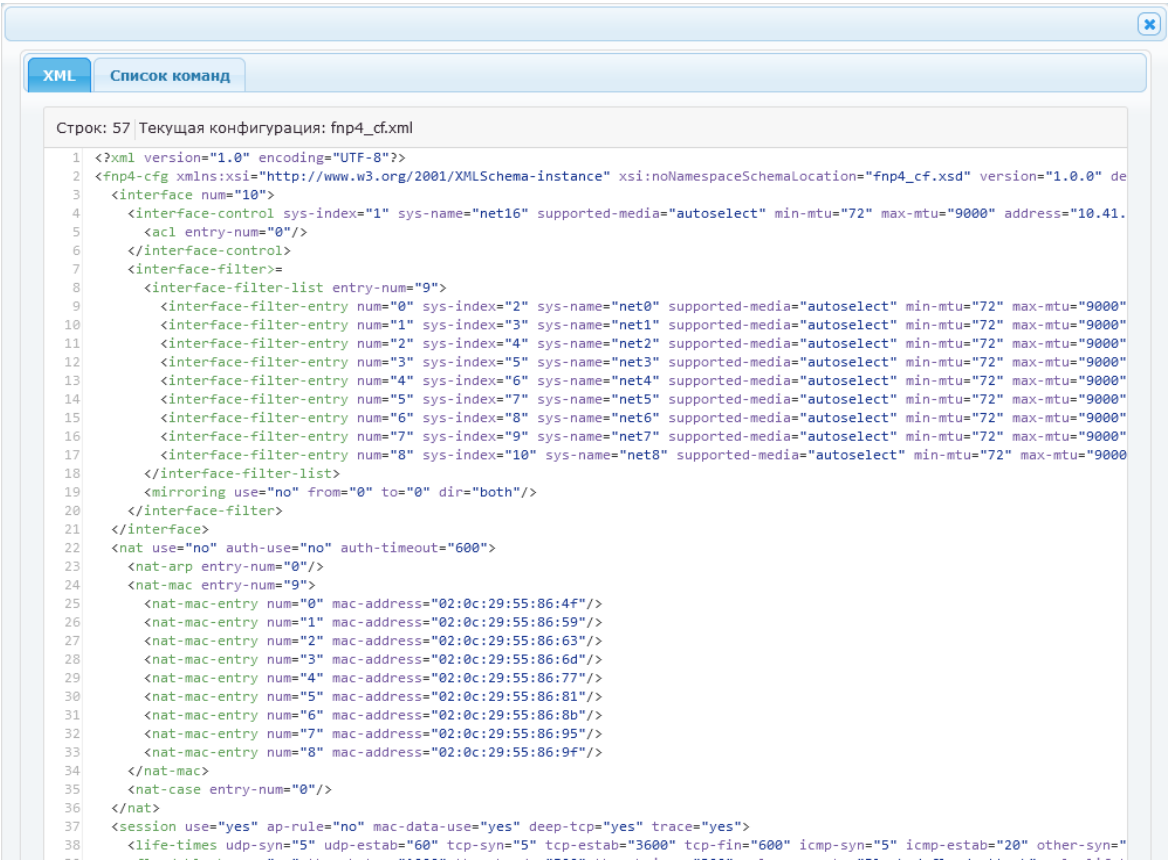


Рисунок 4.10: Окно просмотра текущей конфигурации

Окно просмотра текущей конфигурации содержит две вкладки:

- `XML` – вывод конфигурации в виде XML с подсветкой синтаксиса (файл конфигурации имеет формат XML), данная вкладка отображается по умолчанию;
- `Список команд` – вывод конфигурации в виде списка команд (командного интерфейса администратора), которые необходимо выполнить чтобы получить данное состояние конфигурации.

При нажатии на кнопку **`Сохранить`** открывается форма сохранения текущей конфигурации, представленная на рисунке 4.11, стр. .234.

Форма сохранения текущей конфигурации содержит следующие поля ввода:

- `Имя конфигурации` – имя дополнительной конфигурации, под которым будет сохранена текущая конфигурация;
- `Комментарий` – строка комментария к сохраняемой конфигурации (комментарий отображается в таблице дополнительных конфигураций, помогая администратору идентифицировать дополнительную конфигурацию).

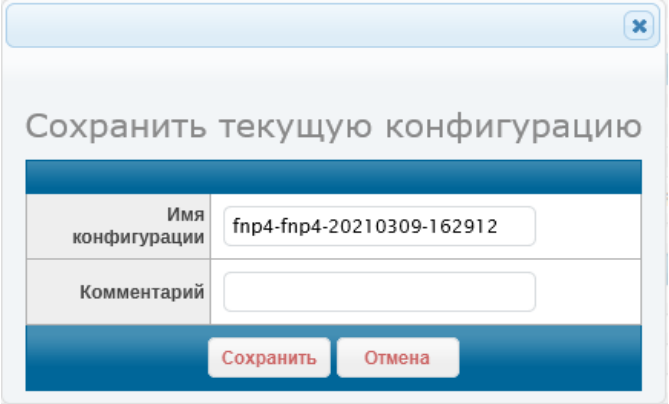


Рисунок 4.11: Форма сохранения текущей конфигурации

При открытии формы сохранения текущей конфигурации в поле `Имя конфигурации` всегда предварительно введено имя конфигурации, соответствующее следующему шаблону:

```
fnp4-<имя_устройства>-ГГГГММСС-ЧЧММСС
```

где:

- `<имя_устройства>` – параметр конфигурации “Имя устройства” (по умолчанию: **`fnp4`**);
- `ГГГГММСС` – текущая дата в указанном формате (например: **`20180327`**);
- `ЧЧММСС` – текущее время в указанном формате (например: **`132628`**).

Администратор может изменить значение поля `Имя конфигурации` на произвольное имя в соответствии с форматом *имени дополнительной конфигурации и дополнительной политики доступа* (приложение А, стр. 423).

Поле Комментарий не обязательно для заполнения. Комментарий должен удовлетворять формату *строки комментария* (приложение А, стр. 423).

Кнопка **Сохранить** формы сохранения текущей конфигурации проверяет введенные данные и в случае их корректности сохраняет текущую конфигурацию в дополнительную с указанным именем.

Кнопка **Сбросить** секции “Текущая конфигурация” (рисунок 4.10, стр. 233) предназначена для сброса текущей конфигурации в состояние по умолчанию. При нажатии на данную кнопку выводится диалоговое окно подтверждения действия, т. к. сброс текущей конфигурации приведет к потере связности УК с МЭ. Кроме того, если администратор заранее не сохранил текущую конфигурацию в дополнительную, то текущие настройки МЭ будут утеряны (может потребоваться их восстановление вручную).

Секция “Дополнительные конфигурации” предназначена для просмотра имеющихся дополнительных конфигураций и выполнения действий над ними. Изначально (на момент поставки) на МЭ ССПТ-4А1 отсутствуют дополнительные конфигурации поэтому секция Дополнительные конфигурации имеет вид, представленный на рисунке 4.12, стр. 235.

Загрузка дополнительной конфигурации. В первой строке секции Дополнительные конфигурации расположена кнопка Загрузить, которая служит для загрузки дополнительной конфигурации с УК на МЭ. По нажатию на кнопку Загрузить открывается форма загрузки дополнительной конфигурации, приведенная на рисунке 4.13, стр. 235. Пример формы загрузки дополнительной конфигурации после выбора файла приведен на рисунке 4.14, стр. 235.

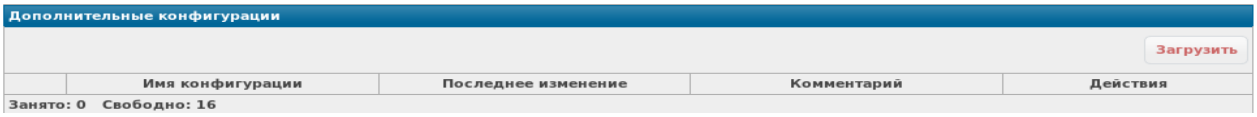


Рисунок 4.12: Секция “Дополнительные конфигурации” – конфигурации отсутствуют

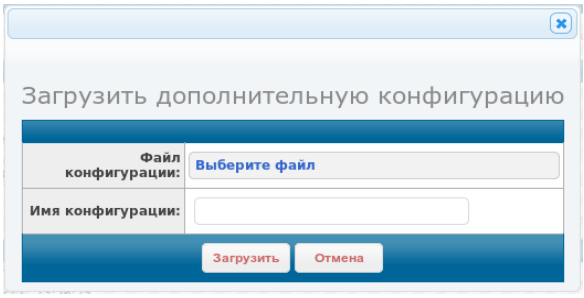


Рисунок 4.13: Форма загрузки дополнительной конфигурации

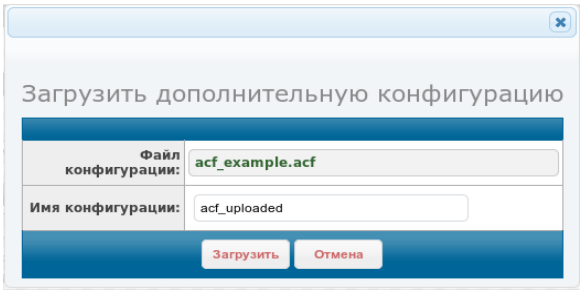


Рисунок 4.14: Форма загрузки дополнительной конфигурации – файл выбран

В строке Файл конфигурации располагается кнопка **Выберите файл** (рис. 4.13, стр. 235). По нажатию на данную кнопку открывается стандартное диалоговое окно WEB-браузера

выбора файла для загрузки на удаленный сервер. В данном случае должен быть выбран файл дополнительной конфигурации (расширение файла: acf) для загрузки на МЭ ССПТ-4А1. После успешного выбора файла надпись кнопки будет изменена с **Выберите файл** на имя выбранного файла (рис. 4.14, стр. 235).

Поле Имя конфигурации предназначено для ввода имени дополнительной конфигурации, под которым загруженная конфигурация будет сохранена на МЭ. В том случае если значение поля не задано, конфигурации будет сохранена на МЭ со своим исходным именем.

Кнопка **Загрузить** выполняет загрузку выбранного файла конфигурации с УК на МЭ и сохраняет его на МЭ, используя имя в соответствии со значением поля Имя конфигурации.

В секции “Дополнительные конфигурации” также располагается таблица дополнительных конфигураций. При наличии на МЭ ССПТ-4А1 дополнительных конфигураций выводится заполненная таблица дополнительных конфигураций. Пример секции с дополнительной конфигурацией, ранее загруженной с УК, приведен на рисунке 4.18, стр. 236.

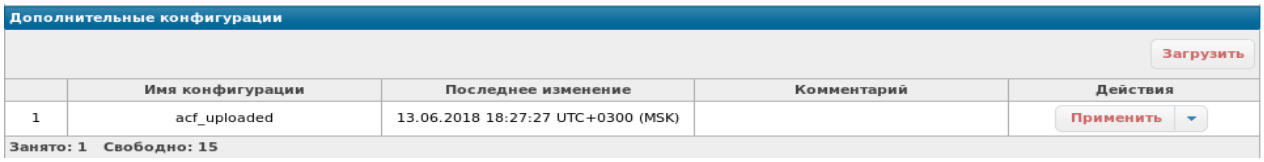


Рисунок 4.15: Секция Дополнительные конфигурации: присутствует конфигурация

Таблица имеет следующие поля:

- Первое (безымянное поле) – порядковый номер дополнительной конфигурации;
- Имя конфигурации – имя, под которым была сохранена дополнительная конфигурация;
- Последнее изменение – дата и время последнего изменения файла дополнительной конфигурации;
- Комментарий – комментарий к конфигурации (для удобства ее идентификации администратором среди других конфигураций, в дополнение к имени конфигурации);
- Действие – поле выбора действия для выполнения над конфигурацией.

В поле Действие располагаются кнопки:

- Применить;
- – кнопка выбора действия;

Кнопка **Применить** служит для применения данной дополнительной конфигурации.

При нажатии на кнопку *Применить* выбранная дополнительная конфигурация применяется без подтверждения от администратора. Это следует иметь в виду, так как возможна потеря связности УК с МЭ.

При нажатии на кнопку выбора действия отображается меню выбора действия над дополнительной конфигурацией. Пример данного меню приведен на рисунке 4.16, стр. 237.

Меню выбора действий содержит следующие элементы:

- `Показать` – просмотр конфигурации в виде XML либо списка команд (аналогично просмотру текущей конфигурации);
- `Переименовать` – смена имени и/или комментария к конфигурации. Форма переименования дополнительной конфигурации приведена на рисунке 4.17, стр. 237;
- `Удалить` – удаление файла конфигурации с носителя данных МЭ ССПТ-4А1.
- `Выгрузить` – выгрузка (сохранение) файла конфигурации на УК администратора.

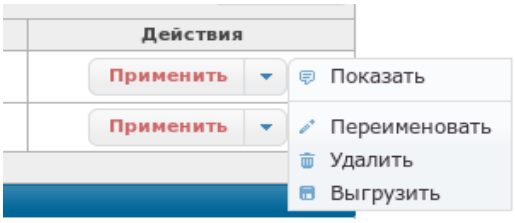


Рисунок 4.16: Выбор действия над конфигурацией

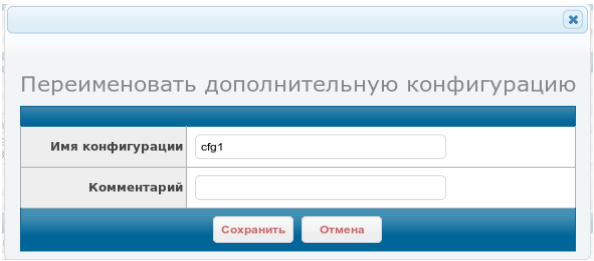


Рисунок 4.17: Форма переименования дополнительной конфигурации

Переименование дополнительной конфигурации. Форма переименования дополнительной конфигурации (рисунок 4.28, стр. 245) содержит два поля:

- `Имя конфигурации` – поле ввода нового имени для конфигурации. Изначально в поле ввода установлено текущее имя конфигурации;
- `Комментарий` — поле ввода комментария к конфигурации. Изначально в поле ввода установлен текущий комментарий к конфигурации (в приведенном примере поле ввода пустое, так как комментарий к данной конфигурации отсутствует).

При нажатии на кнопку `Сохранить` выполняется проверка введенных данных. Форматы имени конфигурации и общий формат комментария приведены в приложении А, стр. 423. Если данные корректны, то выполняется переименование файла конфигурации и/или смена комментария к ней.

Выгрузка дополнительной конфигурации. Для выгрузки дополнительной конфигурации необходимо выполнить следующие шаги (предполагается, что дополнительная

конфигурация, предназначенная для выгрузки, была предварительно сохранена из текущей конфигурации):

1) в меню выбора действия над конфигурацией нажать на пункт **Выгрузить** (рис. 4.18, стр. 238);
2) в результате выполнения пункта 1 откроется стандартное окне WEB-браузера для сохранения файла с WEB-сервера. В нем необходимо выбрать **Save File** (**Сохранить Файл**) и нажать кнопку **OK** (рис. 4.19, стр. 238).

В результате выполнения данных шагов файл дополнительной конфигурации будет сохранен в каталог загрузки, заданный в параметрах конфигурации WEB-бразуера.

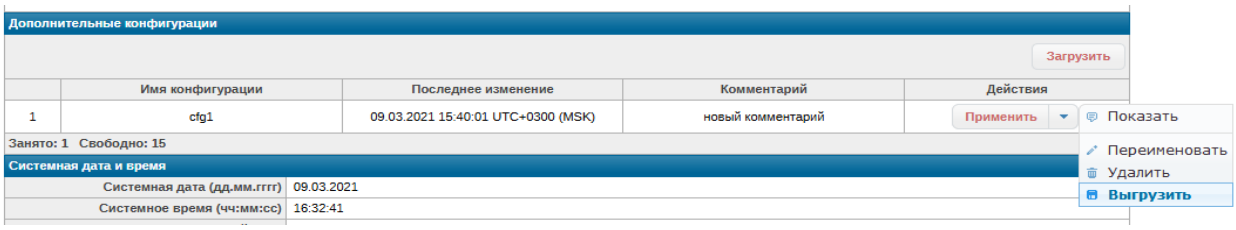


Рисунок 4.18: Меню выбора действия – Выгрузить

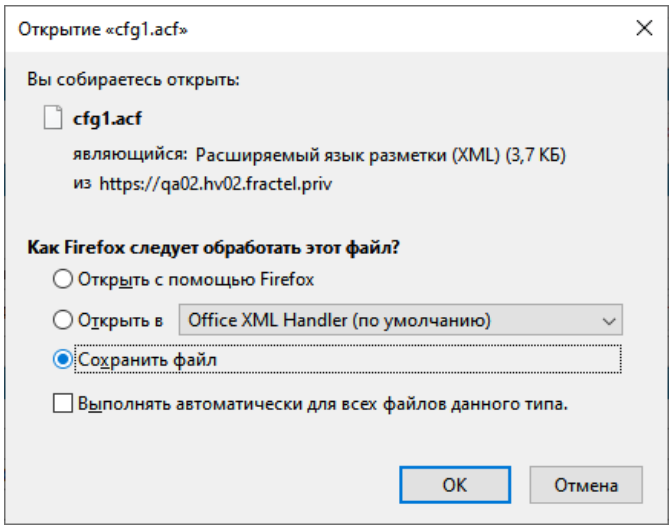


Рисунок 4.19: Стандартное окно WEB-браузера для сохранения файла

Секция “Системная дата и время” содержит следующую информацию:

- `Системная дата (дд.мм.гггг)`: системная дата в указанном формате;
- `Системное время (чч:мм:сс)`: системное время;
- `Часовой пояс`: установленный часовой пояс;
- `NTP`: использование функции обновления по NTP (**включено**/**выключено**);
- `IP-адрес NTP-сервера`: установленный IP-адрес NTP-сервера;
- `Регистрация сообщений NTP`: использование функции регистрации сообщений NTP в журнале системных сообщений (**включено**/**выключено**);

- `Тайм-аут опроса NTP (сек)`: тайм-аут (период) опроса NTP-сервера в секундах.

В последней строке секции – следующие кнопки:

- `Редактировать`: установка системных даты и времени, установка параметров обновления даты и времени по протоколу NTP;
- `Сбросить NTP`: сброс параметров обновления даты и времени по протоколу NTP в значения по умолчанию;
- `Обновить`: выполнить обновление системных даты и времени через NTP-сервер, заданный в конфигурации (кнопка появляется когда IP-адрес NTP-сервера задан в текущей конфигурации).

При нажатии на кнопку **`Редактировать`** открывается форма установки системного времени. Данная форма приведена на рисунке 4.20, стр. .239

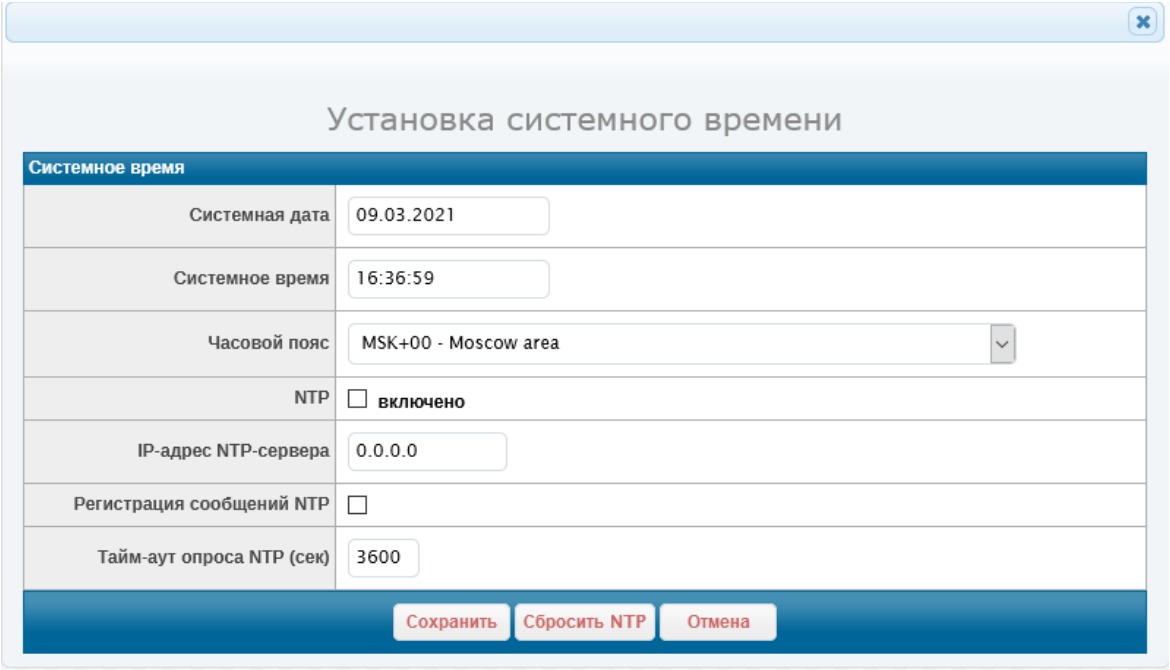


Рисунок 4.20: Форма установки системного времени

Форма содержит следующие элементы ввода данных:

- `Системная дата` – поле ввода системной даты. При выборе поля отображается *виджет* календаря для выбора даты. Дата также может быть введена с клавиатуры. В поле выводится текущая дата.
- `Системное время` – поле ввода системного времени. При выборе поля отображается виджет установки системного времени. Время также может быть введено с клавиатуры. В поле выводится текущая время.
- `Часовой пояс` – список выбора часового пояса. В списке выбран текущий часовой пояс. Значение по умолчанию: **`UTC`**.

- `NTP` – флажок использования функции обновления системных даты и времени по протоколу NTP. Значение по умолчанию: **выключено**;
- `IP-адрес NTP-сервера` – поле ввода IP-адреса NTP-сервера. Значение по умолчанию: **не определено**, что означает отсутствие IP-адреса NTP-сервера в текущей конфигурации.
- `Регистрация сообщений NTP` – флажок регистрации сообщений обновления по NTP в журнале системных сообщений. Значение по умолчанию: **выключено**;
- `Тайм-аут опроса NTP` – поле ввода тайм-аута (периода) обращений к NTP-серверу в секундах. Значение по умолчанию: **`3600`** с (1 час).

Форма имеет следующие кнопки:

- `Сохранить` – проверка корректности и применение данных, введенных в форму;
- `Сбросить NTP` – сброс параметров обновления по NTP в значения по умолчанию;
- `Отмена` – закрытие формы без применения изменений.

4.2.2. Настройки: Администраторы

Страница `Настройки: Администраторы` содержит три секции:

- `Список администраторов`;
- `Список активных администраторов`;
- `Пользователь SNMP-интерфейса`.

Секция “Список администраторов” содержит список учетных записей администраторов, представленный в виде таблицы. Изначально (на момент поставки) на МЭ ССПТ-4А1 присутствует единственная учетная запись: администратора `admin` с привилегиями суперпользователя. Список допустимых привилегий и их возможности описаны в разделе 3.10, стр. 171.

Исходный вид секции `Список администраторов` представлен на рисунке 4.21, стр. 240.

Список администраторов

	Имя администратора	Привилегии	Состояние	Действия
1	admin	admin	включено	

Рисунок 4.21: Секция Список администраторов: исходный вид

Таблица имеет следующие поля:

- порядковый номер учетной записи;
- `Имя администратора`;
- `Привилегии` – привилегии учетной записи (**`admin`**, **`full`** или **`read`**);
- `Состояние` – состояние учетной записи (**включено** или **выключено**);
- `Действия` – выполнение действий над учетной записью.

В таблице используются следующие управляющие иконки для выполнения действий над учетными записями:

- – добавление учетной записи администратора. При нажатии на иконку открывается форма добавления администратора. Форма приведена на рисунке 4.22, стр. 241.
- – изменение параметров учетной записи администратора. При нажатии на иконку открывается форма редактирования администратора. Вид формы редактирования зависит от того редактирует ли администратор собственную учетную запись или учетную запись другого администратора. Форма редактирования администратором собственной учетной записи приведена на рисунке 4.23, стр. 242. Форма редактирования администратором `admin` учетной записи другого администратора приведена рисунке 4.24, стр. 242.
- – удаление учетной записи администратора. При нажатии на иконку открывается стандартное окно подтверждения действия.

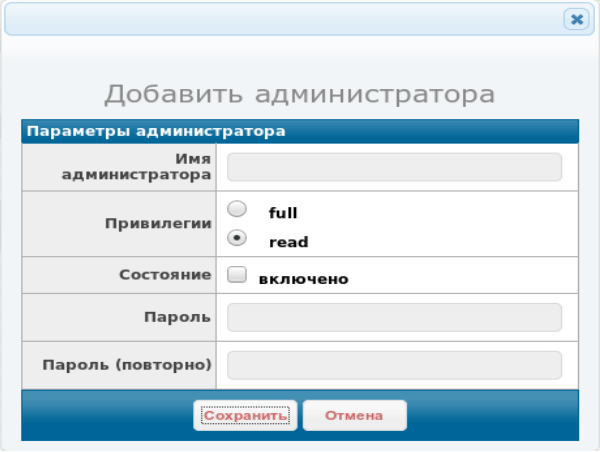


Рисунок 4.22: Форма добавления администратора

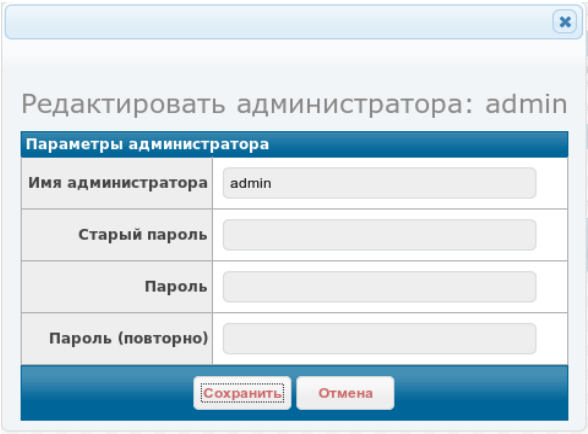


Рисунок 4.23: Форма редактирования параметров собственной учетной записи

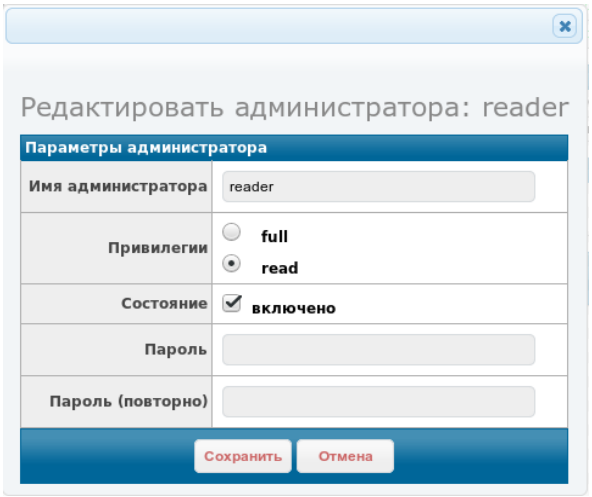


Рисунок 4.24: Форма редактирования параметров учетной записи другого администратора

В форме добавлении учетной записи следующие параметры имеют значения по умолчанию (рисунок 4.22, стр. 241):

- `Привилегии`: **`read`**;
- `Состояние`: **включено**.

Администратор `admin`, как и любой другой администратор, в собственной учетной записи может сменить только пароль (рисунок 4.23, стр. 242). Администратор `admin` имеет возможность изменить следующие параметры учетных записей остальных администраторов (рисунок 4.24, стр. 242):

- `Привилегии` (**`full`** или **`read`**);
- `Состояние` – состояние учетной записи (**включено** или **выключено**);
- `Пароль`.

Привилегии **admin** необходимы для выполнения следующих действий над учетными записями администраторов:

- добавление администратора;
- редактирование администратора;
- удаление администратора

Администраторы с привилегиями **read** и **full** имеют возможность только смены собственного пароля.

Таким образом администраторам с привилегиями **read** и **full** доступна только иконка изменения параметров собственной учетной записи (остальные иконки не отображаются в таблице).

Пример секции “Список администраторов”, которую может наблюдать `admin`, после добавления учетных записей приведен на рисунке 4.25, стр. 243.

Список администраторов				
	Имя администратора	Привилегии	Состояние	Действия
1	admin	admin	включено	
2	reader	read	включено	
3	tester	full	включено	

Рисунок 4.25: Секция Список администраторов: вид после добавления учетных записей

В данном случае в таблице администраторов присутствуют все управляющие иконки, описанные ранее.

Секция “Список активных администраторов” содержит таблицу активных администраторов, т. е. администраторов, которые выполнили вход (авторизовались на МЭ ССПТ-4А1) и сеанс работы которых продолжается в настоящий момент. Пример таблицы активных администраторов приведен на рисунке 4.26, стр. 243.

Список активных администраторов					
	Имя администратора	Время входа	Откуда	Привилегии	Время неактивности
1	admin	28.03.2018 14:40:25 UTC+0300 (MSK)	WEB:10.98.100.250	admin	0 секунд
2	tester	28.03.2018 14:47:38 UTC+0300 (MSK)	CLI:10.98.100.250	read	5 секунд

Рисунок 4.26: Секция Список активных администраторов

Таблица активных администраторов имеет следующие поля:

- порядковый номер активного сеанса администратора;
- `Имя администратора`;
- `Время входа`;
- `Откуда` – символьное обозначение интерфейса администратора (например: `WEB`, `CLI`, `SNMP`) и IP-адрес УК при удаленном подключении;
- `Привилегии` – текущие привилегии администратора;
- `Время неактивности` – интервал времени с момента последней активности администратора.

> Привилегии, выводимые в таблице активных администраторов, являются *текущими* (т. н. *эффективные привилегии*). Они могу отличаться от привилегий учетной записи администратора, т. к. только один администратор может обладать текущими привилегиями на запись (**admin** или **full**). Все администраторы, выполнившие вход позже, будут иметь привилегии **read**.
>
> Время неактивности исчисляется со времени выполнения администратором последней команды Следует иметь в виду, что открытие каждой страницы WEB-интерфейса приводит к выполнению определенного набора команд.

В таблице активных администраторов присутствует единственная управляющая иконка – завершение сеансов всех активных администраторов, кроме сеанса администратора, выполняющего данное действие. При нажатии по данной иконке выводится стандартное диалоговое окно подтверждения действия.

Секция “Пользователь SNMP-интерфейса” содержит в себе две кнопки:

- **Выключить** – выключение SNMP-интерфейса (при этом процесс SNMP-интерфейса будет остановлен и его состояние на странице **Состояние: Устройство** будет соответствующим образом изменено. После выключения SNMP-интерфейса данная кнопка заменяется на кнопку **Включить**, действие которой противоположно.
- **Сменить пароль** – смена пароля пользователя SNMP-интерфейса.

При нажатии по кнопке Сменить пароль открывается форма смены пароля пользователя SNMP-интерфейса. Форма приведена на рисунке 4.27, стр. 244.

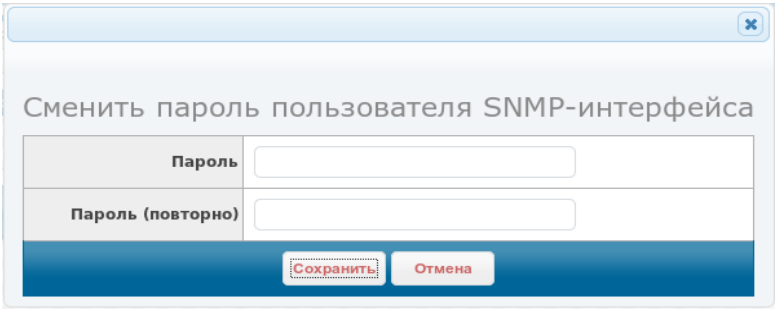


Рисунок 4.27: Форма смены пароля пользователя SNMP-интерфейса

Форма содержит два поля: для двукратного ввода нового пароля. Формат пароля пользователя SNMP-интерфейса приведен в приложении А, стр. 423.

4.2.3. Настройки: Интерфейсы

Страница “Настройки: Интерфейсы” предназначена для просмотра состояний сетевых интерфейсов МЭ ССПТ-4А1, а также изменения их настроек. Пример страницы “Настройки: Интерфейсы” приведен на рисунке 4.28, стр. 245.

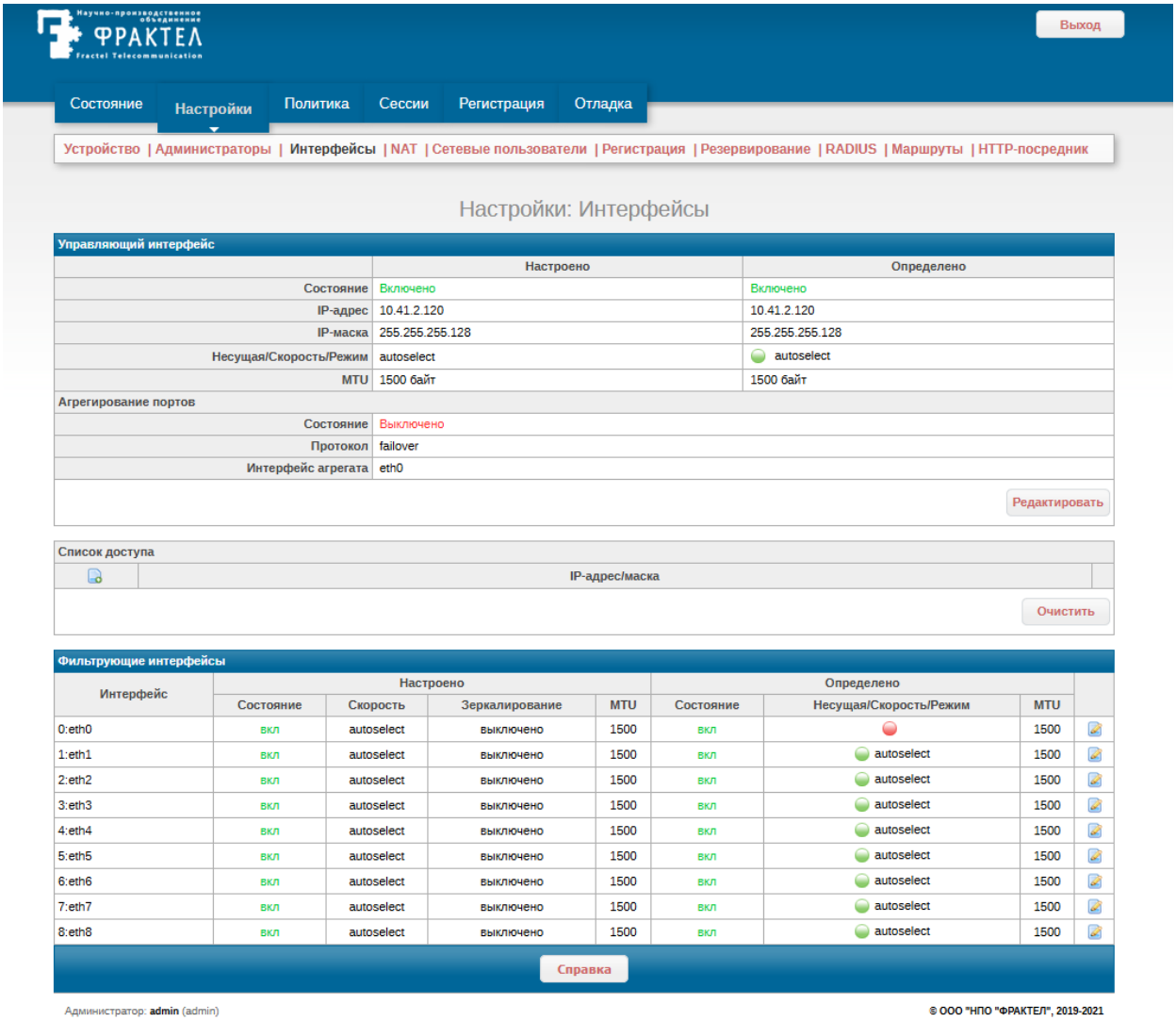


Рисунок 4.28: Пример страницы “Настройки: Интерфейсы”

Поскольку МЭ ССПТ-4А1 имеет интерфейсы двух типов (управляющий и фильтрующие), то страница разделена на две секции:

- `Управляющий интерфейс`: параметры управляющего интерфейса и список доступа (ACL) к нему;
- `Фильтрующие интерфейсы`: таблица фильтрующих интерфейсов.

Секция “Управляющий интерфейс”. В секции расположена таблица параметров управляющего интерфейса, организованная так, что для каждого параметра интерфейса (строка таблицы):

- в столбце `Настроено` располагается значение параметра, установленное в текущей конфигурации МЭ ССПТ-4А1;
- в столбце `Определено` располагается значение параметра, полученное от УОС МЭ ССПТ-4А1, т. е. фактическое значение параметра.

В таблице параметров управляющего интерфейса выводятся значения следующих параметров:

- Состояние – состояние интерфейса (включено/выключено);
- IP-адрес – IP-адрес, назначенный на интерфейс;
- IP-маска – IP-маска управляющей подсети;
- Несущая/Скорость/Режим:
  - ✔ в столбце Настроено выводится только скорость передачи и режим передачи (если доступен);
  - ✔ в столбце Определено: состояние несущей (зеленый цвет – несущая есть, красный – нет). При наличии несущей также выводится скорость передачи и режим передачи (если доступен).
- MTU – значение MTU (Maximum Transfer Unit), установленное на интерфейсе;
- Агрегирование портов:
  - ✔ Состояние – состояние функции агрегирования портов управляющего интерфейса (включено/выключено);
  - ✔ Протокол – протокол агрегирования;
  - ✔ Интерфейс агрегата – фильтрующий интерфейс, который будет использован в составе агрегата при включении функции агрегирования портов.

По нажатию на кнопку Редактировать открывается форма редактирования настроек управляющего интерфейса. Форма приведена на рисунке 4.29, стр. 247.

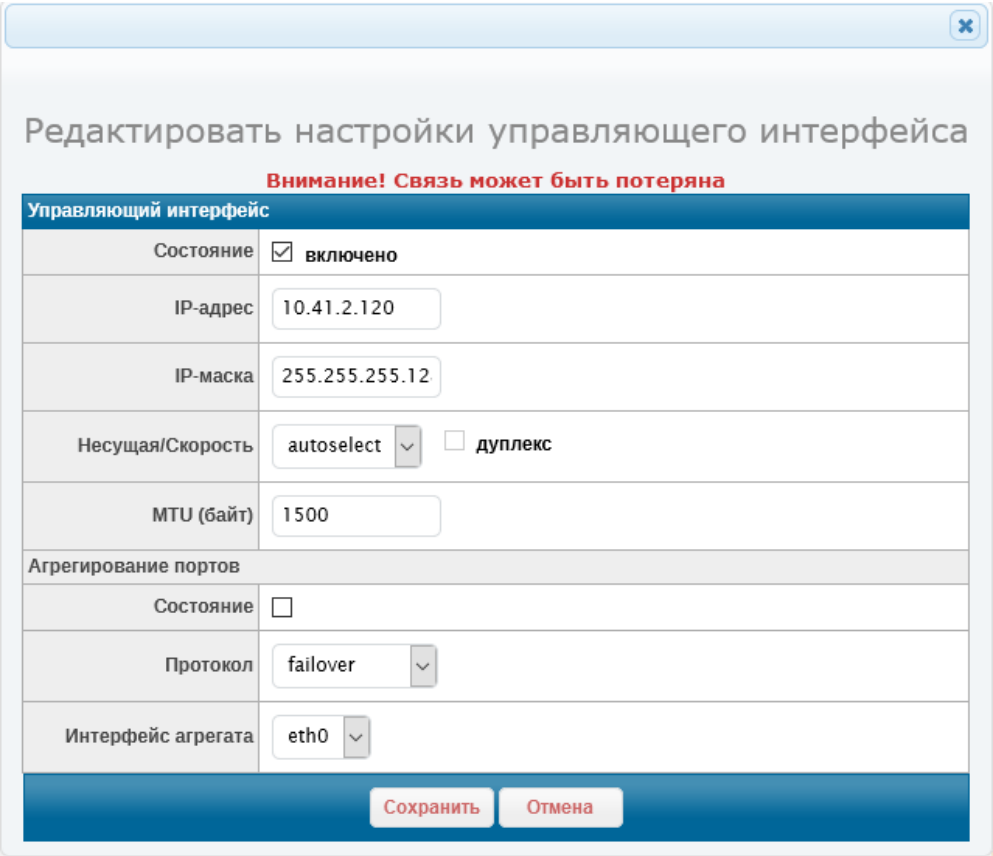


Рисунок 4.29: Форма редактирования настроек управляющего интерфейса

Назначение элементов ввода данных формы ясно из описания полей таблицы параметров управляющего интерфейса, приведенного выше. Отметим, что режим передачи задается кнопкой-флагом дуплекс:

- **включено** – полнодуплексный режим;
- **выключено** – полудуплексный режим.

Если на интерфейсе установлена скорость передачи **autoselect**, то параметр режим передачи не может быть установлен.

При установленном значении скорости **autoselect** фактическое значение скорости, выводимое в столбце *“Определено”*, как правило, будет отличным от **autoselect** и соответственно будет выводиться и режим передачи.

По умолчанию управляющему Ethernet-интерфейсу МЭ ССПТ-4А1 назначен IP-адрес *10.234.28.71* с сетевой маской *255.255.0.0*.

При установке IP-адреса управляющего Ethernet-интерфейса МЭ ССПТ-4А1 сеанс администратора автоматически завершается в случае удаленного администрирования, во избежание того что привилегии администратора МЭ ССПТ-4А1 на запись (**admin** или **full**) окажутся временно занятыми в случае потери связности между УК администратора МЭ ССПТ-4А1 и устройством МЭ ССПТ-4А1

Если новый IP-адрес управляющего Ethernet-интерфейса МЭ ССПТ-4А1 принадлежит другой подсети, то маршрут по умолчанию на управляющем интерфейсе, в случае его наличия, удаляется из маршрутной таблицы и администратору МЭ ССПТ-4А1 потребуется добавить корректный маршрут по умолчанию самостоятельно (см. раздел 4.2.9 Настройки: Маршруты, стр. 281).

Список выбора `Протокол` позволяет выбрать протокол агрегирования. Допустимы следующие протоколы:

- **`failover`**: трафик передается только через активный порт (основной (master) порт – первый порт в агрегате). Протокол по умолчанию;
- **`broadcast`**: отправляет кадры на все порты агрегата и принимает кадры на любой порт агрегата;
- **`lacp`**: поддерживает IEEE 802.1AX (ранее 802.3ad) Link Aggregation Control Protocol (LACP), а также Marker Protocol;
- **`loadbalance`**: балансировка исходящего трафика на основе хеширования заголовков пакетов и прием входящего трафика на любой из активных портов агрегата;
- **`roundrobin`**: распределение исходящего трафика между всеми активными портами, используя планировщик типа round-robin и прием входящего трафика на любой из активных портов агрегата.

При первом включении функции *агрегирования портов управляющего интерфейса*, если явно не указано в команде, в составе агрегата будет использован фильтрующий интерфейс с нулевым номером (**Eth0**).

Администратор имеет возможность сменить выбор фильтрующего интерфейса для использования в агрегате, но для этого функция *агрегирования портов управляющего интерфейса* должна быть вначале **выключена**.

При включении функции *агрегирования портов управляющего интерфейса* на *агрегате* автоматически устанавливается IP-адрес управляющего интерфейса из текущей конфигурации МЭ ССПТ-4А1. Также автоматически корректируются маршруты, использовавшие управляющий интерфейс: данные маршруты будут использовать *агрегат*.

При включении функции *агрегирования портов управляющего интерфейса* фильтрующий интерфейс, используемый в агрегате, перестает выполнять роль фильтрующего, т. е.:

- не используется в правилах фильтрации ни в качестве входного, ни выходного;
- не используется в резервировании (если резервирование включено);
- не может использоваться в зеркалировании интерфейсов;
- не может использоваться в интерфейсах NAT;
- не может использоваться в качестве интерфейса HTTP-посредника;

Если на момент включения функции агрегирования фильтрующий интерфейс агрегата уже используется в *зеркалировании*, *NAT* или *HTTP-посреднике*, то включение функции агрегирования не будет произведено с выводом соответствующего предупреждающего сообщения.

Для включения функции *агрегирования портов управляющего интерфейса* MTU управляющего интерфейса и фильтрующего интерфейса, предназначенного для использования в агрегате, должны иметь одинаковые значения.

При включении функции *агрегирования портов управляющего интерфейса* скорости передачи обоих интерфейсов в составе агрегата автоматически устанавливаются в **autoselect**.

Список доступа к управляющему интерфейсу. Список доступа (ACL) позволяет ограничить доступ к управляющему интерфейсу списком IP-адресов, которым разрешен доступ. По умолчанию доступ разрешен с любых IP-адресов, соответственно список доступа пуст.

Пустой список доступа приведен на рисунке 4.30, стр. 249. Пример списка доступа с единственной записью приведен на рисунке 4.31, стр. 249.

Для модификации списка доступа используются следующие иконки:

- – добавить запись в список доступа;
- – удалить запись из списка доступа.

По нажатию на кнопку **Очистить** удаляются все записи списка доступа: ограничение доступа к управляющему интерфейсу отменяется.

> Перед добавлением *первой записи* в список доступа администратору МЭ ССПТ-4А1 необходимо убедиться, что IP-адрес управляющего компьютера удовлетворяет добавляемой записи, в противном случае возникнет мгновенная потеря соединения и доступа к управлению МЭ ССПТ-4А1.

При нажатии на иконку добавления записи в список доступа открывается соответствующая форма, приведенная на рисунке 4.32, стр. 249.

Рисунок 4.30: Пример пустого списка доступа

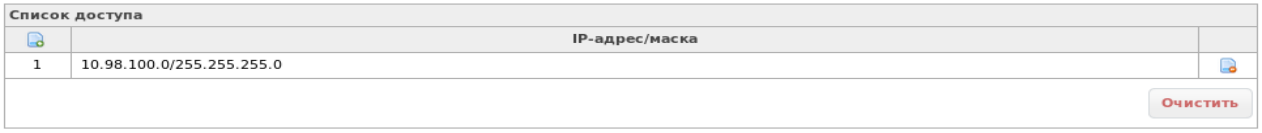


Рисунок 4.31: Пример списка доступа с единственной записью

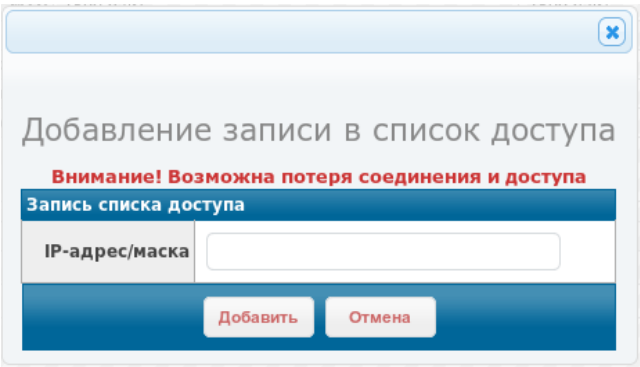


Рисунок 4.32: Форма добавления записи в список доступа

Форма добавления записи в список доступа имеет единственное поле ввода: `IP-адрес/маска`. Допускаются следующие варианты значений поля:

- одиночный IP-адрес (например: **`192.168.1.1`**);

- IP-подсеть (например: **192.168.1.0/24**);
- диапазон IP-адресов (например: **192.168.1.1-192.168.1.5**).

Секция “Фильтрующие интерфейсы” представляет собой таблицу фильтрующих интерфейсов. Пример таблицы фильтрующих интерфейсов приведен на рисунке 4.33, стр. 250.

Фильтрующие интерфейсы

Интерфейс	Настроено				Определено			
	Состояние	Скорость	Зеркалирование	MTU	Состояние	Несущая/Скорость/Режим	MTU	
0:eth0	вкл	autoselect	выключено	1500	вкл		1500	
1:eth1	вкл	autoselect	выключено	1500	вкл	autoselect	1500	
2:eth2	вкл	autoselect	выключено	1500	вкл	autoselect	1500	
3:eth3	вкл	autoselect	выключено	1500	вкл	autoselect	1500	
4:eth4	вкл	autoselect	выключено	1500	вкл	autoselect	1500	
5:eth5	вкл	autoselect	выключено	1500	вкл	autoselect	1500	
6:eth6	вкл	autoselect	выключено	1500	вкл	autoselect	1500	
7:eth7	вкл	autoselect	выключено	1500	вкл	autoselect	1500	
8:eth8	вкл	autoselect	выключено	1500	вкл	autoselect	1500	

Справка

Рисунок 4.33: Пример таблицы фильтрующих интерфейсов

Аналогично таблице параметров управляющего интерфейса для каждого параметра выводится два значения:

- в столбце `Настроено` – значение параметра, установленное в текущей конфигурации МЭ ССПТ-4А1;
- в столбце `Определено` – значение параметра, полученное от УОС МЭ ССПТ-4А1, т. е. фактическое значение параметра.

В таблице выводятся следующие поля:

- `Интерфейс`: индекс и назначенное имя интерфейса;
- `Состояние`: состояние интерфейса (включено/выключено);
- `Скорость`:
  - ✔ `Настроено`: скорость передачи и режим передачи (если доступен);
  - ✔ `Определено`: состояние несущей (зеленый цвет – несущая есть, красный – нет). При наличии несущей также выводится скорость передачи и режим передачи (если доступен);
- `Зеркалирование` (только в `Настроено`):
  - ✔ выключено, если функция зеркалирования выключена;
  - ✔ в противном случае для двух интерфейсов, используемых данной функций, выводится дополнительная информация об установленных параметрах зеркалирования;
- `MTU` – значение MTU (Maximum Transfer Unit), установленное на интерфейсе.

Если включена функция *агрегирования портов управляющего интерфейса* и/или функция *HTTP-посредника*, то фильтрующие интерфейсы, используемые данными функциями, не выводятся в таблице фильтрующих интерфейсов, поскольку не используются в качестве фильтрующих интерфейсов МЭ.

В последнем поле записи таблицы располагается иконка – редактировать настройки фильтрующего интерфейса. По нажатию на иконку открывается форма редактирования настроек фильтрующего интерфейса. Форма приведена на рисунке 4.34, стр. 251.

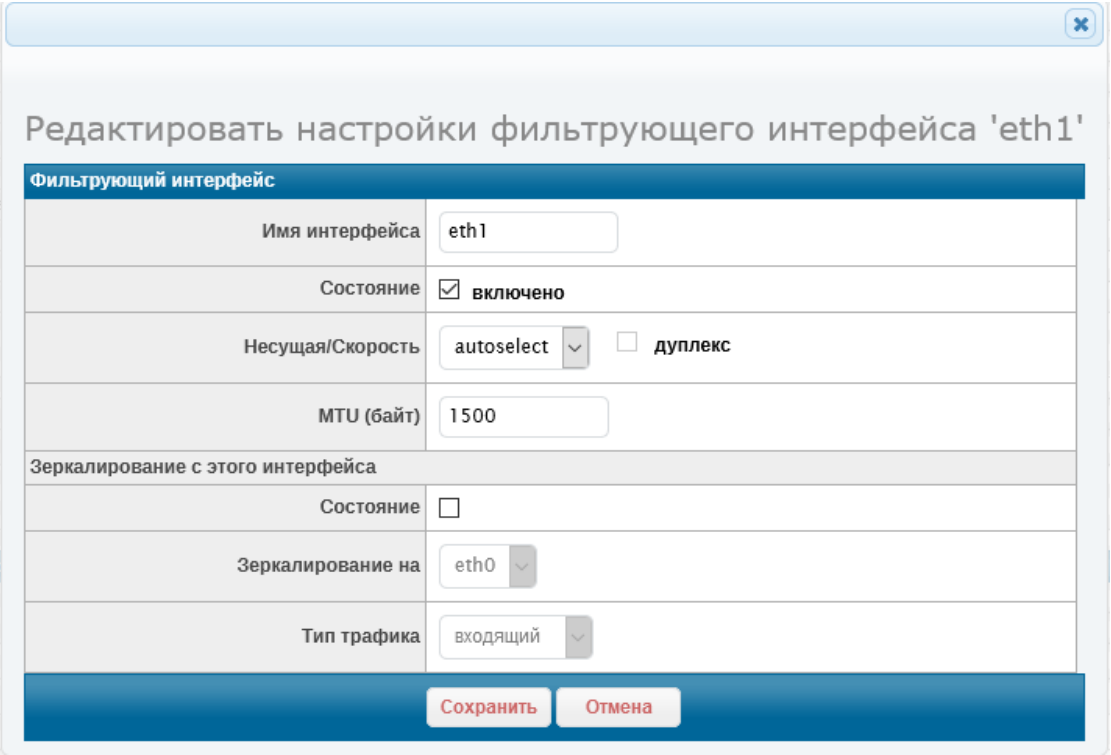


Рисунок 4.34: Форма редактирования настроек фильтрующего интерфейса

Форма содержит следующие элементы ввода данных:

- `Имя интерфейса` – назначенное имя интерфейса. Значение должно соответствовать формату *имени именованной сущности* (приложение А, стр. 423);
- `Состояние` – состояние интерфейса (включено/выключено);
- `Несущая/Скорость` – скорость передачи и режим передачи. Режим передачи устанавливается флагом-кнопкой дуплекс:
  - ✔ **включено** – полнодуплексный режим;
  - ✔ **выключено** – полудуплексный режим;
- `MTU` – значение MTU (Maximum Transfer Unit) интерфейса;
- `Зеркалирование с этого интерфейса` – настройки зеркалирования трафика с данного интерфейса:
  - ✔ `Состояние` – состояние функции зеркалирования (включено/выключено);
  - ✔ `Зеркалирование на` – выбор инетрфейса, на который будет зеркалироваться трафик с данного;
  - ✔ `Тип трафика` – выбор типа зеркалируемого трафика. Допустимые значение:
    - **входящий**;

- **исходящий**;
- **весь** (входящий и исходящий).

	Если на интерфейсе установлена скорость передачи **autoselect**, то режим передачи не может быть установлен. При установленном значении скорости **autoselect** фактическое значение скорости, выводимое в столбце *“Определено”*, как правило будет отличным от **autoselect** и соответственно будет выводиться и режим передачи.
	Если в правилах фильтрации *зеркалирующий интерфейс* указывается в качестве выходного, то, в соответствии с таким правилом, на этот интерфейс будут передаваться пакеты, что при определенных условиях может привести к возникновению дублирующих пакетов на *зеркалирующем интерфейсе*. *Зеркалирующий инетрфейс* не может использоваться во *внутренних* и *внешних интерфейсах NAT* при использовании функции трансляции сетевых адресов (NAT). *Зеркалирующий* и *зеркалируемый* инетрфейсы не допускается использовать в качестве интерфейса *HTTP-посредника* и *интерфейса агрегата*.
	Если во время использования МЭ ССПТ-4А1 (устройство включено) выполняется установка (смена) SFP-модулей, то после установки (смены) SFP-модулей **необходимо** перезапустить пакетный фильтр (см. раздел 4.1.1, стр. 224). В результате перезапуска пакетного фильтра перечни допустимых скоростей передачи фильтрующих интерфейсов будут актуализированы в текущей конфигурации МЭ ССПТ-4А1.
	Не допускается перенаправлять зеркалируемый трафик на используемый фильтрующий интерфейс. Интерфейс, на который производится *зеркалирование* (далее: *зеркалирующий интерфейс*), перестает работать в режиме фильтрации, т.е. все пакеты, пришедшие на этот интерфейс из подключенного к нему сетевого сегмента, удаляются без обработки.

4.2.4. Настройки: NAT

Страница “Настройки: NAT” предназначена для настроек функции NAT, включения/выключения ее использования. Исходный вид страницы (с настройками NAT по умолчанию) приведен на рисунке 4.35, стр. 252.

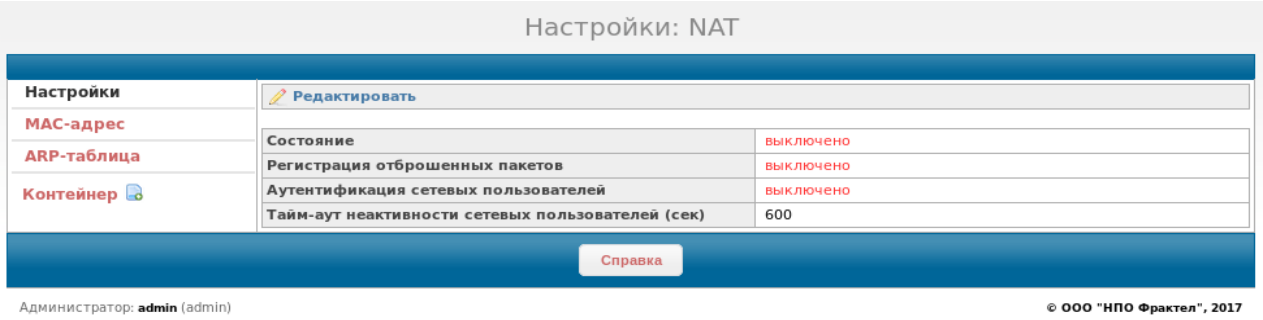


Рисунок 4.35: Исходный вид страницы “Настройки: NAT”

Страница организована таким образом, что слева находится меню, в котором сгруппированы различные настройки NAT:

- `Настройки` – общие настройки NAT;
- `MAC-адрес` – настройки псевдо MAC-адресов, используемых фильтрующими интерфейсами МЭ ССПТ-4А1 при включенной функции NAT;

- `ARP-таблица` – просмотр и редактирование ARP таблицы NAT;
- `Контейнер` – работа с контейнерами NAT и настройками, содержащимися в них.

Меню “Настройки” объединяет общие настройки NAT:

- `Состояние` – использование функции NAT (включено/выключено). Значение по умолчанию: **выключено**;
- `Регистрация отброшенных пакетов` – регистрация пакетов, отброшенных функцией NAT (включено/выключено). Значение по умолчанию: **выключено**;
- `Аутентификация сетевых пользователей` – использование функции аутентификации сетевых пользователей (включено/выключено). Значение по умолчанию: **выключено**;
- `Тайм-аут неактивности сетевых пользователей (сек)` – интервал времени с момента прохождения последнего сетевого пакета от данного сетевого пользователя, по истечении которого сеанс работы пользователя завершается и для дальнейшей работы пользователя через МЭ требуется повторная авторизация. Значение по умолчанию: **`600`** секунд.

Функция *аутентификации сетевых пользователей* может быть включена при выключенной функции NAT в конфигурации МЭ ССПТ-4А1, но ее реальное функционирование возможно только при включенной функции NAT.

Сетевой пакет может быть удален функцией NAT по различным причинам. При включенной *регистрации отброшенных пакетов* (функцией NAT) причина удаления пакета сохраняется в записи регистрации данного пакета и доступна администратору при просмотре зарегистрированных пакетов.

По нажатию на кнопку `Редактировать` открывается форма редактирования общих настроек NAT. Форма приведена на рисунке 4.36, стр. 253.

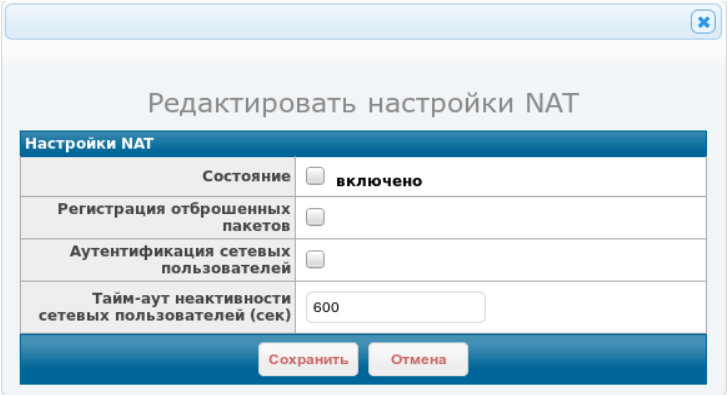


Рисунок 4.36: Форма редактирования общих настроек NAT

Форма позволяет изменить значения общих настроек NAT, описанных выше.

MAC-адрес. На данной странице можно просмотреть и изменить *псевдо* MAC-адреса, используемые фильтрующими интерфейсами МЭ при включенной функции NAT. Фрагмент страницы `MAC-адрес` приведен на рисунке 4.37, стр. 254.

На странице настроек MAC-адресов выводятся текущие значения псевдо MAC-адресов, закрепленных за фильтрующими интерфейсами МЭ. По умолчанию MAC-адреса сгенерированы так, что у них отличается только последний байт. Значения всех MAC-адересов могут быть изменены администратором.

По нажатию на кнопке `Редактировать` открывается форма редактирования MAC-адресов. Форма приведена на рисунке 4.38, стр. 255.

Форма позволяет изменить произвольное число MAC-адресов: от одного до всех. Очевидно, MAC-адреса не должны повторяться.

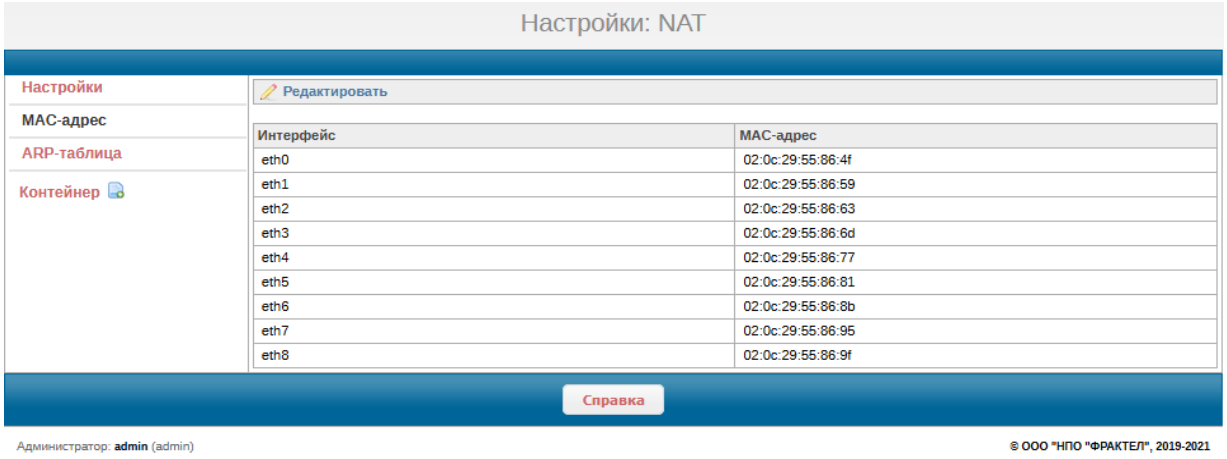


Рисунок 4.37: Настройки MAC-адресов

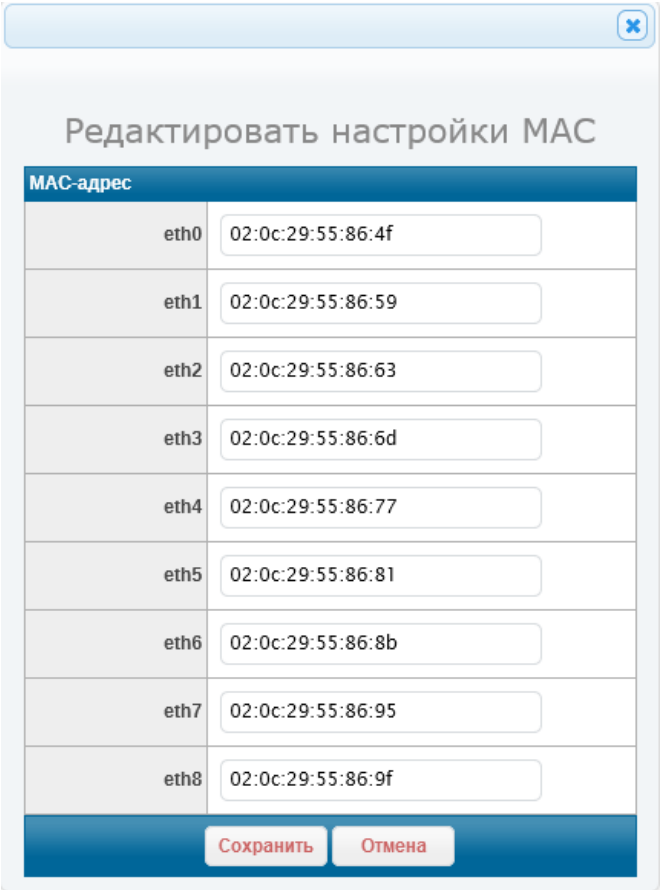


Рисунок 4.38: Форма редактирования MAC-адресов

ARP-таблица NAT. На данной странице выводится ARP-таблица и элементы для ее модификации. Исходный вид ARP-таблицы (записи отсутствуют) приведен на рисунке 4.39, стр. 255.

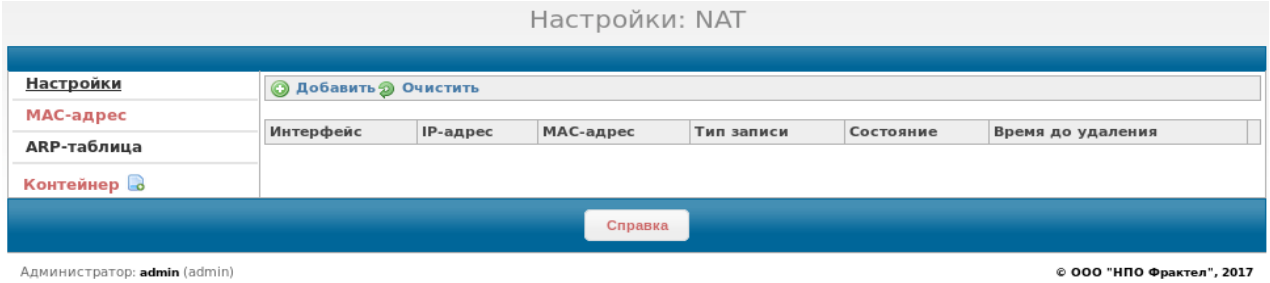


Рисунок 4.39: Исходный вид ARP-таблицы

ARP-таблица может включать в себя записи двух типов:

- *статическая* – добавляется администратором;
- *динамическая* – автоматически добавляется пакетным фильтром вследствие использования им протокола ARP для получения MAC-адреса узла сети, отправившего пакет на один из интерфейсов NAT.

ARP-таблица состоит из следующих полей:

- Интерфейс – назначенное имя фильтрующего интерфейса, через который отправляются сетевые пакеты, адресованный узлу сети в соответствии с данной ARP-записью;
- IP-адрес – IP-адрес узла сети, к которому относится данная ARP-запись;
- MAC-адрес – MAC-адрес, соответствующий IP-адресу узла сети в поле IP-адрес
- Тип записи – тип ARP-записи. Допустимые значения:
  - ✔ static – статическая;
  - ✔ dynamic – динамическая;
- Состояние – состояние **динамической** записи (для **статической** записи поле не заполняется). Допустимые значения:
  - ✔ полная – запись имеет все необходимые параметры для ее использования при отправке пакета, обработанного функцией NAT;
  - ✔ частичная – запись добавлена в ARP-таблицу, но MAC-адрес узла сети еще не определен;
- Время до удаления записи: интервал времени в секундах до удаления **динамической** записи пакетным фильтром (для **статической** записи поле не заполняется).

На странице ARP-таблица имеются два управляющих элемента:

- Добавить – добавление статической ARP-записи;
- Очистить – удаление всех записей выбранного типа из ARP-таблицы.

По нажатию на элемент Добавить открывается форма добавления статической ARP-записи. Форма приведена на рисунке 4.40, стр. 256.

По нажатию на элемент Очистить открывается диалоговое окно выбора типа удаляемых записей. Окно выбора типа записей приведено на рисунке 4.41, стр. 256.

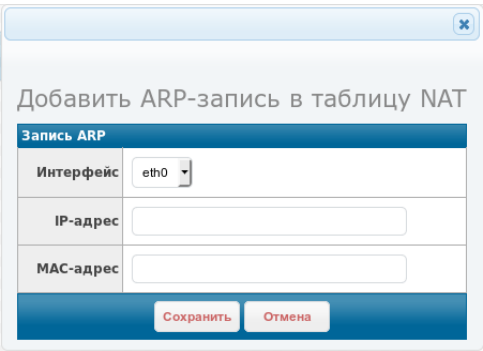


Рисунок 4.40: Форма добавление статической ARP-записи

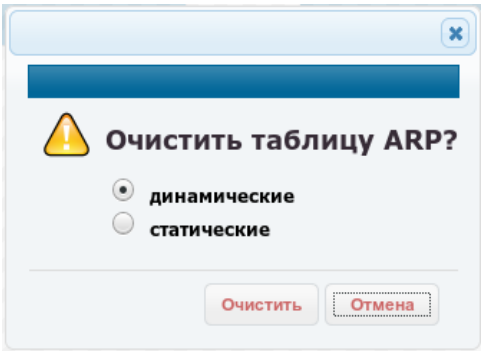


Рисунок 4.41: Окно выбора типа удаляемых ARP-записей

Форма добавления ARP-записи включает в себя следующие элементы ввода данных:

- Интерфейс – выпадающий список выбора фильтрующего интерфейса;
- IP-адрес – IP-адрес узла сети;

- `MAC-адрес` – MAC-адрес узла сети.

Поля `IP-адрес` и `MAC-адрес` обязательны к заполнению. Интерфейс должен быть выбран в соответствии с конфигурацией сети: запросы от узла сети должны поступать на данный интерфейс МЭ.

В результате нажатия кнопки `Очистить` в окне выбора типа удаляемых ARP-записей будут удалены все ARP-записи данного типа.

При наличии в ARP-таблице записей в строке каждой записи появляется иконка – удаление данной ARP-записи.

Пример ARP-таблицы с одной статической записью приведен на рисунке 4.42, стр. 257.

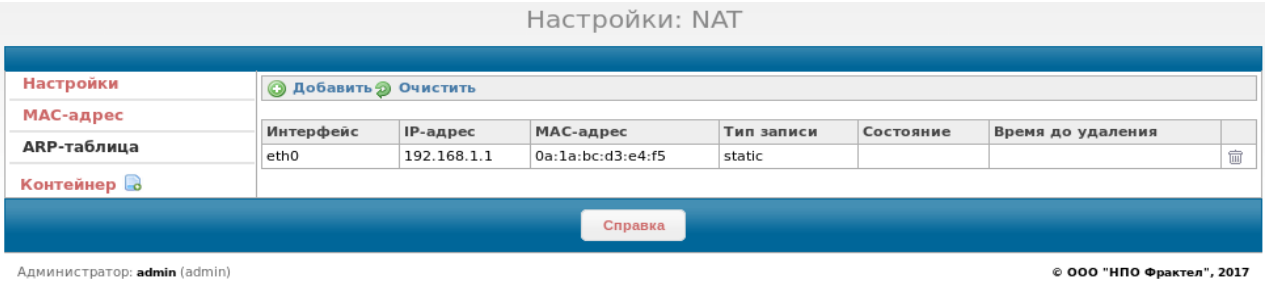


Рисунок 4.42: Пример ARP-таблицы со статической записью

Добавление контейнера NAT. Контейнер NAT служит для задания определенной конфигурации NAT. Параллельно могут существовать и использоваться несколько контейнеров NAT. Для возможности включения функции NAT должен существовать хотя бы один контейнер NAT, имеющий, по крайней мере, по одному внутреннему и одному внешнему интерфейсу NAT. В строке `Контейнер` (рис. 4.42, стр. 257) расположена иконка – добавление контейнера NAT.

По нажатию на данную иконку открывается форма добавления контейнера NAT. Форма приведена на рисунке 4.43, стр. 257.

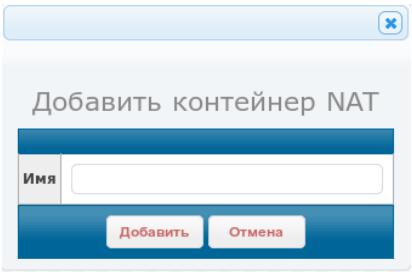


Рисунок 4.43: Форма добавления контейнера NAT

По нажатию на кнопку `Добавить` создается пустой (не сконфигурированный) контейнер NAT с указанным именем. Имя контейнера NAT должно удовлетворять формату *имени*

именованной сущности (приложение А, стр. 423). В результате создания контейнера Web-браузер осуществляет переход на страницу настроек контейнера NAT.

Настройки контейнера NAT. Фрагмент страницы настроек контейнера NAT (имя контейнера: **`case1`**) приведен на рисунке 4.44, стр. 258.

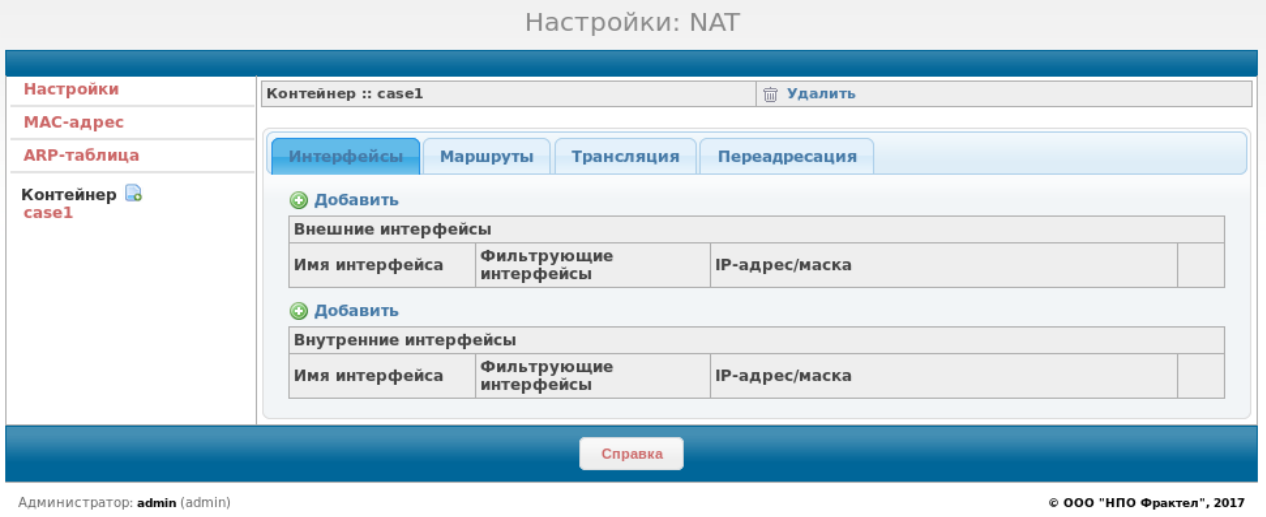


Рисунок 4.44: Фрагмент страницы настроек контейнера NAT. Вкладка “Интерфейсы”

В левой части страницы под строкой `Контейнер` выводится список существующих в конфигурации контейнеров (в приведенном примере – один контейнер: **`case1`**).

В правой части страницы – четыре вкладки:

- `Интерфейсы` – просмотр, добавление, изменение, удаление интерфейсов NAT;
- `Маршруты` – просмотр, добавление, изменение, удаление статических маршрутов NAT;
- `Трансляция` – просмотр, добавление, изменение, удаление правил трансляции;
- `Переадресация` – просмотр, добавление, изменение, удаление правил переадресации.

В верхней строке страницы располагается управляющий элемент Удалить – удаление данного контейнера NAT со всеми сущностями, входящими в его состав.

На каждой вкладке страницы настроек контейнера NAT присутствует управляющий элемент Добавить – добавить сущность, соответствующую выбранной вкладке настроек контейнера NAT (далее в тексте – элемент `Добавить`).

После добавления некоторой сущности NAT (интерфейс NAT, правило трансляции, правило переадресации, маршрут) в соответствующей ей записи таблицы появляются две управляющие иконки:

– редактировать запись;

– удалить запись.

Вкладка “Интерфейсы”. Настройка контейнера NAT должна начинаться с добавления интерфейсов NAT, т. к. остальные сущности контейнера NAT (правила трансляции и т. д.) имеют явные или неявные ссылки на интерфейсы NAT.

Для возможности включения функции NAT должен существовать по меньшей мере один контейнер NAT в котором определены как минимум один *внутренний интерфейс NAT* и один *внешний интерфейс NAT*,

При этом для *реального функционирования NAT* требуется также наличие в контейнере NAT по меньшей мере:

- одного правила трансляции;
- маршрута по умолчанию.

Для добавления внутреннего или внешнего интерфейса NAT необходимо нажать на соответствующий элемент `Добавить` (рис. 4.44, стр. 258). В результате откроется форма добавления интерфейса NAT. Формы добавления внешнего и внутреннего интерфейсов NAT приведены на рисунках 4.45 и 4.46, стр. 259, соответственно.

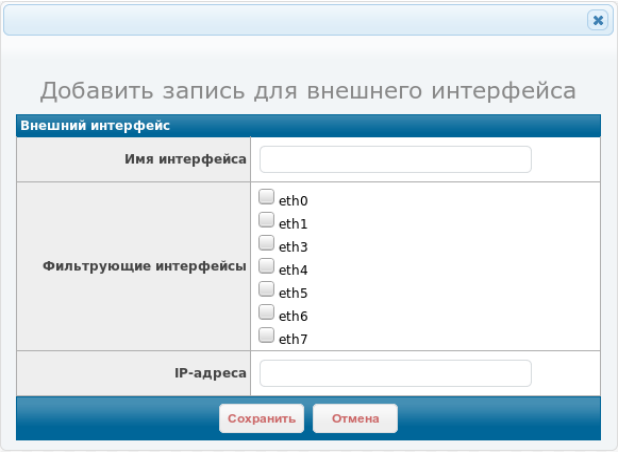


Рисунок 4.45: Форма добавления внешнего интерфейса

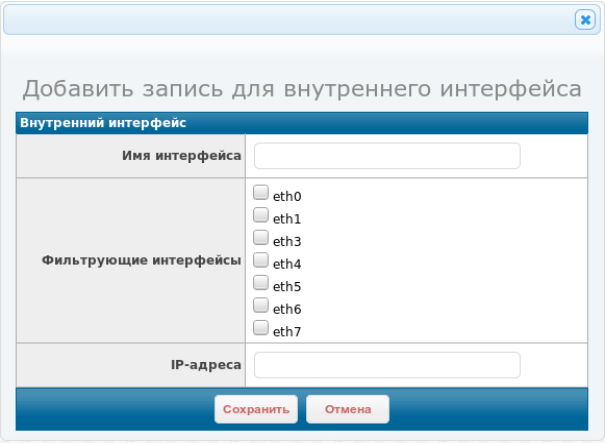


Рисунок 4.46: Форма добавления внутреннего интерфейса

Формы добавления внешнего и внутреннего интерфейсов NAT идентичны по своей структуре и включают следующие элементы ввода данных:

- `Имя интерфейса` – поле ввода имени интерфейса NAT. Имя интерфейса NAT должно быть уникально в рамках данного контейнера NAT и должно отвечать формату *имени именованной сущности* (приложение А, стр. 423);
- `Фильтрующие интерфейсы` – набор фильтрующих интерфейсов в составе данного интерфейса NAT (минимум: один интерфейс);
- `IP-адреса` – список IP-адресов, привязанных к данному интерфейсу NAT в формате: `<IP-адрес>/<IP-маска>`. Минимум один элемент в списке. Разделитель элементов в списке – символ запятой.

После добавления интерфейса NAT его запись добавляется в соответствующую таблицу интерфейсов. Пример таблицы интерфейсов NAT, при наличии в них записей, приведен на рисунке 4.47, стр. 260.

Из примера видно, что в обеих таблицах для каждой записи присутствует, упомянутая ранее, пара иконок для редактирования и удаления записи.

Пример формы редактирования записи внешнего интерфейса приведен на рисунке 4.48, стр. 260. Форма редактирования записи внутреннего интерфейса – идентична.

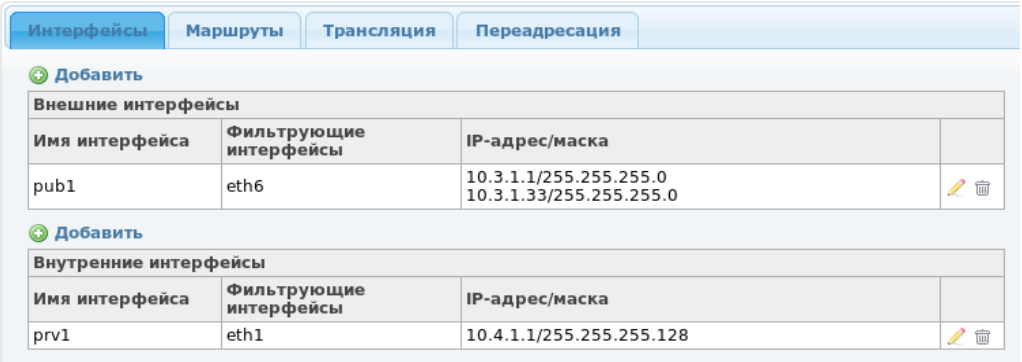


Рисунок 4.47: Пример таблицы интерфейсов NAT

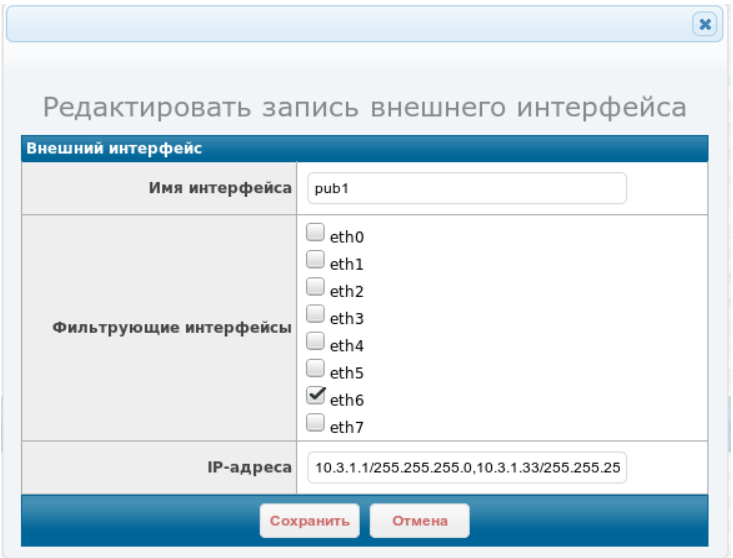


Рисунок 4.48: Примеры формы редактирования внешнего интерфейса

Форма позволяет менять значения всех параметров, кроме имени интерфейса.

Если *внутренний* или *внешний* интерфейс NAT используется в других сущностях контейнера (правилах трансляции, правилах переадресации или статических маршрутах), то изменение фильтрующих интерфейсов в его составе не допускается. При нажатии на кнопку **Сохранить** будет выведено сообщение об ошибке, в котором будут указаны все ссылки на данный интерфейс NAT. При этом изменения не будут сохранены.

Вкладка “Маршруты”. Данная вкладка предназначена для просмотра, добавления, редактирования и удаления статических маршрутов. Изначально, когда контейнер NAT пуст, вкладка имеет вид, приведенный на рисунке 4.49, стр. 261.

Во вкладке присутствуют две таблицы. Первая таблица содержит маршруты на подсети интерфейсов NAT и заполняется автоматически при наличии в контейнере интерфейсов NAT. Таблица имеет следующие поля:

- `IP-адрес приемника`: формируется автоматически как IP-адрес подсети на интерфейсе NAT
- `Имя интерфейса`: имя интерфейса NAT.

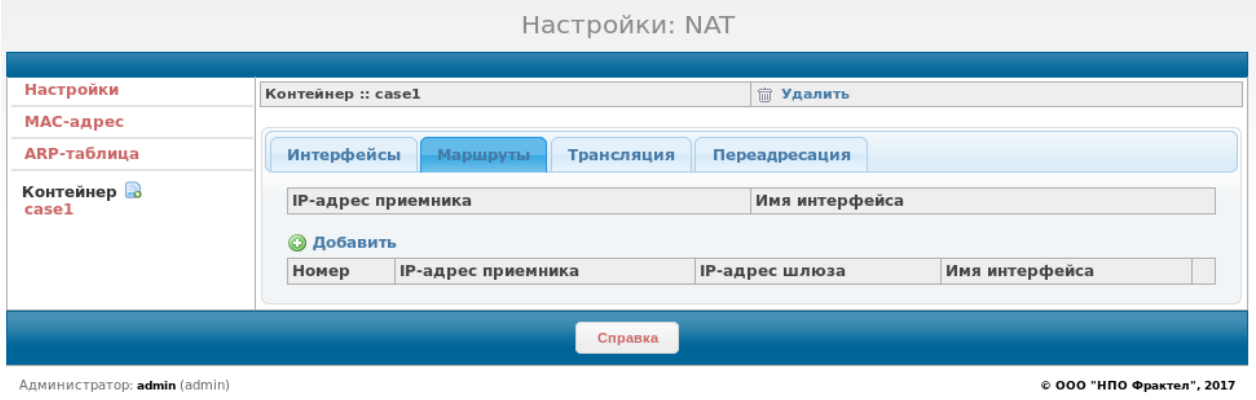


Рисунок 4.49: Вкладка “Маршруты”. Вид при пустом контейнере

Вторая таблица содержит статические маршруты, то есть те, которые были добавлены администратором. Поля таблицы:

- `Номер` – порядковый номер маршрута;
- `IP-адрес приемника` – IP-адрес назначения маршрута;
- `IP-адрес шлюза` – IP-адрес шлюза, находящегося в той же подсети, что и один из IP-адресов интерфейса NAT (внутреннего или внешнего);
- `Имя интерфейса` – имя интерфейса NAT, соответствующее указанному IP-адресу шлюза.

При нажатии по элементу `Добавить` открывается форма добавления маршрута. Форма приведена на рисунке 4.50, стр. 262.

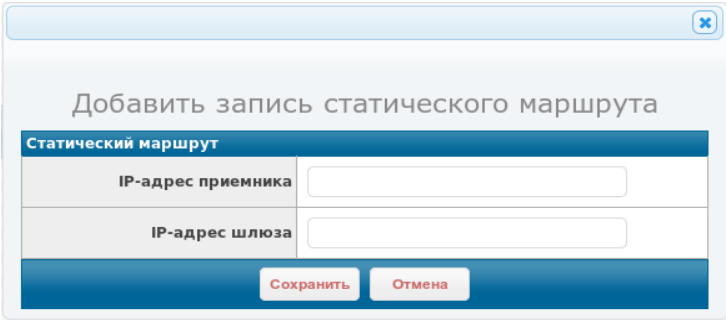


Рисунок 4.50: Форма добавления статического маршрута

Форма содержит два поля ввода:

- `IP-адрес приемника`: допустим ввод IP-адреса узла сети либо IP-адреса посети в формате: `<IP-адрес_сети>/<IP-маска>`. Например: **`192.168.1.0/24`**).
- `IP-адрес шлюза`.

> Для добавления *маршрута по умолчанию* в поле *IP-адрес приемника* должен быть введен IP-адрес: **0.0.0.0**. Маршрут по умолчанию всегда выводится в первой позиции таблицы статических маршрутов.

Администратор может удалить либо отредактировать статический маршрут. Для этого в каждой записи таблицы статических маршрутов присутствуют соответствующие иконки, описанные ранее в данном разделе. Пример вкладки `Маршруты` с записями в обеих таблицах приведен на рисунке 4.51, стр. 262.

Рисунок 4.51: Пример вкладки “Маршруты” при наличии маршрутов

Из таблицы маршрутов на подсети интерфейсов NAT (первая таблица) видно, что в контейнере `case1` один внутренний интерфейс – `prv1` и один внешний интерфейс – `pub1`, на каждый из которых назначено по одному IP-адресу.

Вкладка “Трансляция”. Данная вкладка предназначена для просмотра, добавления, редактирования и удаления правил трансляции. Изначально, когда контейнер NAT пуст, вкладка имеет вид, приведенный на рисунке 4.52, стр. 263 .

Во вкладке располагается таблица правил трансляции со следующими полями:

- `Номер` – порядковый номер правила;
- Внутренние IP-адреса – список внутренних IP-адресов;
- `Внешние IP-адреса` – список внешних IP-адресов;
- `Внешний интерфейс` – внешний интерфейс NAT, с которого оттранслированный пакет отправляется во внешнюю сеть;
- `IP-адрес приемника` – список IP-адресов назначения пакета, для которых должно применяться данное правило;
- `Протокол` – протокол, инкапсулированный в IP, для которого должно применяться данное правило.

При нажатии по элементу `Добавить` открывается форма добавления правила трансляции. Форма добавления правила приведена на рисунке 4.53, стр. 264. Правило трансляции допускает редактирование. Пример формы редактирования правила приведен на рисунке 4.54, стр. 264.

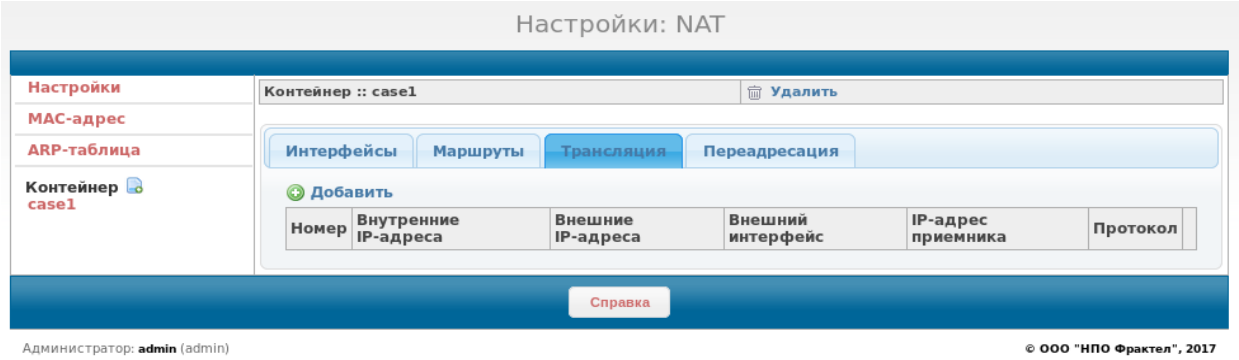


Рисунок 4.52: Вкладка “Трансляция”. Вид при пустом контейнере

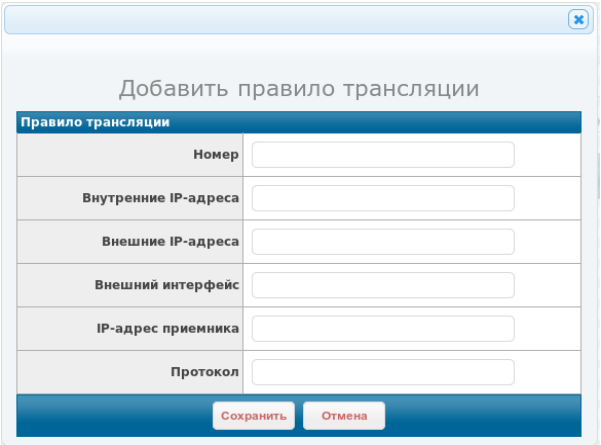


Рисунок 4.53: Форма добавления правила трансляции

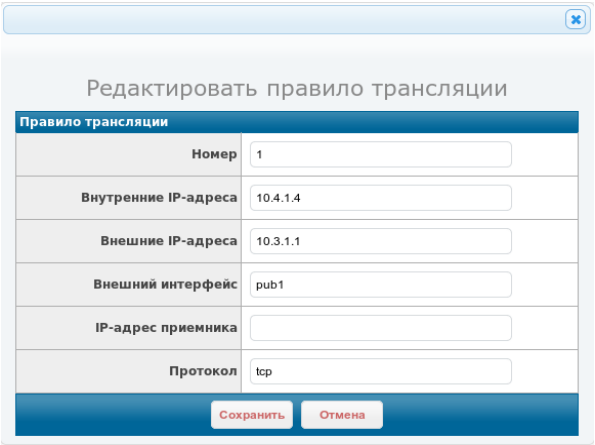


Рисунок 4.54: Пример формы редактирования правила трансляции

Формы добавления и редактирования правила трансляции идентичны по своей структуре и содержат одинаковый набор полей ввода:

- `Номер` – номер правила трансляции. Определяет очередность проверки пакета из внутренней сети на соответствие данному правилу трансляции (роль аналогична роли номера в правиле фильтрации). Допустимые значения: **`1..65535`**. Номер указывается при добавлении правила, изменение номера при редактировании правила не допускается (ввод заблокирован).
- `Внутренние IP-адреса` – список внутренних IP-адресов. Пакеты с IP-адресом источника, отвечающим указанному списку будут оттранслированы в соответствии с данным правилом. Список может содержать следующие элементы:
  - ✔ `<IP-адрес>` – IP-адрес узла сети (например: **`10.1.1.1`**);
  - ✔ `<IP-адрес_сети/IP-маска>` – IP-адрес сети с указанием маски сети (например: **`192.168.1.0/24`**);
  - ✔ `<IP-адрес_1>-<IP-адрес_2>` – диапазон IP-адресов узлов сети (например: **`10.1.1.1-10.1.1.32`**);
- `Внешние IP-адреса` – список IP-адресов, назначенных на один из внешних интерфейсов NAT данного контейнера. Список может содержать следующие элементы:
  - ✔ `<IP-адрес>` – IP-адрес, назначенный на внешний интерфейс NAT (например: **`192.168.1.1`**);
- `Внешний интерфейс` – внешний интерфейс NAT данного контейнера, через который МЭ должен отправлять пакеты, оттранслированные в соответствии с данным правилом. Формат значений: `<имя_внешнего_интерфейса_NAT>` (например: **`pub1`**). Значение поля должно соответствовать значению поля `Внешние IP-адреса`;
- `IP-адрес приемника` – список IP-адресов, которому должен отвечать IP-адрес назначения в транслируемом пакете. Значение по умолчанию: **`отсутствует`** (любой IP-адрес приемника).

Список может содержать следующие элементы:

✔ `<IP-адрес>` – IP-адрес узла сети (например: **`10.1.1.1`**);

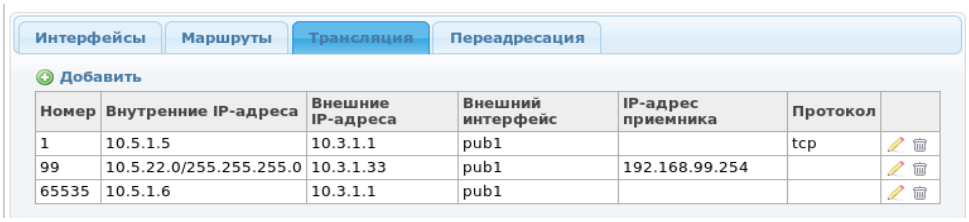
✔ `<IP-адрес_сети/IP-маска>` – IP-адрес сети с указанием маски сети (например: **`192.168.1.0/24`**);

✔ `<IP-адрес_1>-<IP-адрес_2>` – диапазон IP-адресов узлов сети (например: **`10.1.1.1-10.1.1.32`**);

- `Протокол` – протокол, инкапсулированный в IP, для которого должно применяться данное правило. Значение по умолчанию: **`отсутствует`** (любой протокол). Допустимые значения: **`tcp`**, **`udp`** или **`icmp`**.

В каждой записи таблицы правил трансляции присутствуют две стандартные иконки для редактирования и удаления записи. Пример таблицы правил трансляции приведен на рисунке 4.55, стр. 265.

Вкладка Переадресация. Данная вкладка предназначена для просмотра, добавления, редактирования и удаления правил переадресации. Изначально, когда контейнер NAT пуст, вкладка имеет вид, приведенный на рисунке 4.56, стр. 265.



Номер	Внутренние IP-адреса	Внешние IP-адреса	Внешний интерфейс	IP-адрес приемника	Протокол	
1	10.5.1.5	10.3.1.1	pub1		tcp	
99	10.5.22.0/255.255.255.0	10.3.1.33	pub1	192.168.99.254		
65535	10.5.1.6	10.3.1.1	pub1			

Рисунок 4.55: Пример таблицы правил трансляции

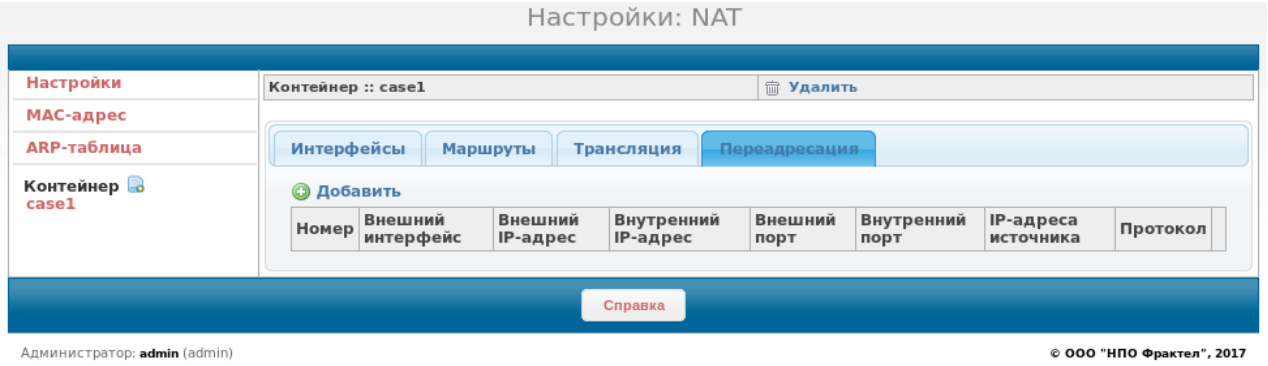


Рисунок 4.56: Вкладка “Переадресация”. Вид при пустом контейнере

Во вкладке располагается таблица правил переадресации со следующими полями:

- `Номер` – порядковый номер правила;
- `Внешний интерфейс` – внешний интерфейс NAT;

- Внешний IP-адрес – IP-адрес, назначенный на интерфейс, выводимый в поле Внешний интерфейс;
- Внутренний IP-адрес – IP-адрес, на который производиться переадресация с IP-адреса в поле Внешний IP-адрес;
- Внешний порт – список TCP или UDP-портов, для которых выполняется переадресация;
- Внутренний порт – список TCP или UDP-порто на которые выполняется переадресация с портов, указанных в поле Внешний порт;
- IP-адрес источника – список IP-адресов источника пакета, для которых применяется данное правило;
- Протокол – протокол, инкапсулированный в IP-пакет, для которого применяется данное правило.

При нажатии по элементу Добавить открывается форма добавления правила переадресации. Форма добавления правила приведена на рисунке 4.57, стр. 266. Правило переадресации допускает редактирование. Пример формы редактирования правила приведен на рисунке 4.58, стр. 266.

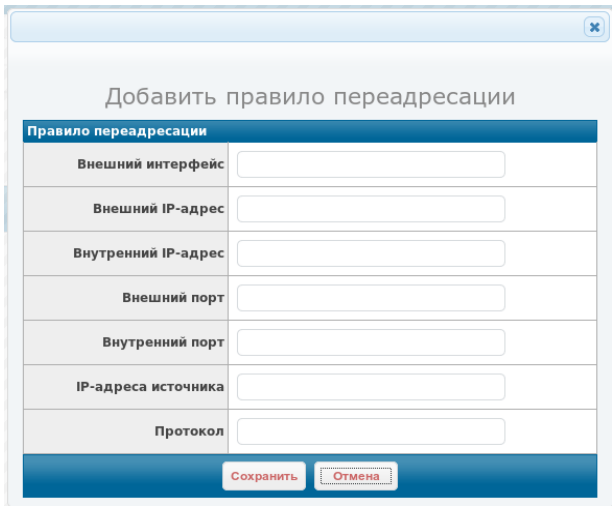


Рисунок 4.57: Форма добавления правила переадресации

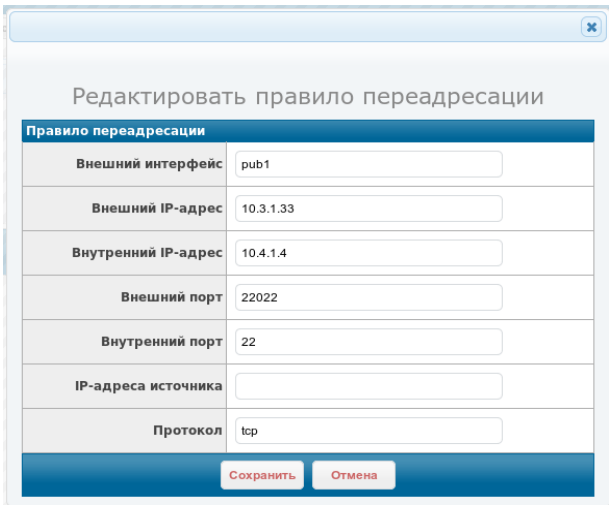


Рисунок 4.58: Пример формы редактирования правила переадресации

Формы добавления и редактирования правила переадресации идентичны по своей структуре и содержат одинаковый набор полей ввода:

- Внешний интерфейс – имя внешнего интерфейса NAT, на который должен поступить пакет для переадресации в соответствии с данным правилом.
- Внешний IP-адрес – IP-адрес из числа IP-адресов, назначенных на внешний интерфейс NAT, указанный в поле Внешний инетрфейс;
- Внутренний IP-адрес – IP-адрес узла сети, находящегося во внутренней сети. На данный IP-адрес выполняется переадресация пакета, поступившего из внутренней сети. Внутренний IP-

адрес не обязан принадлежать IP-подсети некоторого внутреннего интерфейса NAT, т. к. может находиться за маршрутизатором.

- `Внешний порт` – TCP или UDP-порт, запросы на который переадресуются на `Внутренний порт` (порт узла во внутренней сети);
- `Внутренний порт` – TCP или UDP-порт узла во внутренней сети, на который который переадресуются запросы, поступившие на `Внешний порт`;
- `IP-адрес источника` – список IP-адресов, которому должен отвечать IP-адрес источника в пакете, для которого должна выполниться переадресация. Значение по умолчанию: **`отсутствует`** (любой IP-адрес источника). Список может содержать следующие элементы:
  - ✔ `<IP-адрес>` – IP-адрес узла сети (например: **`10.1.1.1`**);
  - ✔ `<IP-адрес_сети/IP-маска>` – IP-адрес сети с указанием маски сети (например: **`192.168.1.0/24`**);
  - ✔ `<IP-адрес_1>-<IP-адрес_2>` – диапазон IP-адресов узлов сети (например: **`10.1.1.1-10.1.1.32`**);
- `Протокол` – протокол транспортного уровня. Значение по умолчанию: **`отсутствует`** (любой протокол из числа: tcp, udp). Допустимые значения: **`tcp`**, **`udp`**.

Поля *Внешний порт* и *Внутренний порт* форм добавления и редактирования правила переадресации допускают указание диапазонов портов. При этом длины диапазонов в обоих полях должны быть равны. Например, поле *Внешний порт* имеет значение: 20020-20021, поле *Внутренний порт*: 20-21. При этом переадресация по портам будет выполняться поэлементно (20020 в 20, 200021 в 21 и т. п.).

В каждой записи таблицы правил переадресации присутствуют две стандартные иконки для редактирования и удаления записи. Пример таблицы правил переадресации приведен на рисунке 4.59, стр 267.

Интерфейсы | Маршруты | Трансляция | Переадресация

Добавить

Номер	Внешний интерфейс	Внешний IP-адрес	Внутренний IP-адрес	Внешний порт	Внутренний порт	IP-адреса источника	Протокол	
1	pub1	10.3.1.33	10.4.1.4	22022	22		tcp	
2	pub1	10.3.1.1	192.168.1.1	8080	80	10.22.33.0/255.255.255.0		

Рисунок 4.59: Пример таблицы правил переадресации

4.2.5. Настройки: Сетевые пользователи

Страница “Настройки: Сетевые пользователи” предназначена для управления сетевыми пользователями.

Работа сетевых пользователей через МЭ ССПТ-4А1 возможна только при включенных функциях: *NAT* и *аутентификации сетевых пользователей*. Сетевой пользователь может находиться как во внешней сети (за внешним интерфейсом NAT), так и во внутренней сети (за внутренним интерфейсом NAT).

Страница разделена на следующие секции:

- Список сетевых пользователей;
- Список активных сетевых пользователей;
- Ключи аутентификации;
- Параметры и ключи Диффи-Хеллмана.

Изначально (на момент поставки МЭ ССПТ-4А1) станица Настройки: Сетевые пользователи имеет вид, приведенный на рисунке 4.60, стр. 268.

Список сетевых пользователей. Секция содержит таблицу учетных записей сетевых пользователей. Изначально (на момент поставки МЭ ССПТ-4А1) учетные записи сетевых пользователей отсутствуют, поэтому таблица – пустая (рисунок 4.60, стр. 268).

Пример таблицы сетевых пользователей, при наличии учетных записей, приведен на рисунке 4.61, стр. 268.

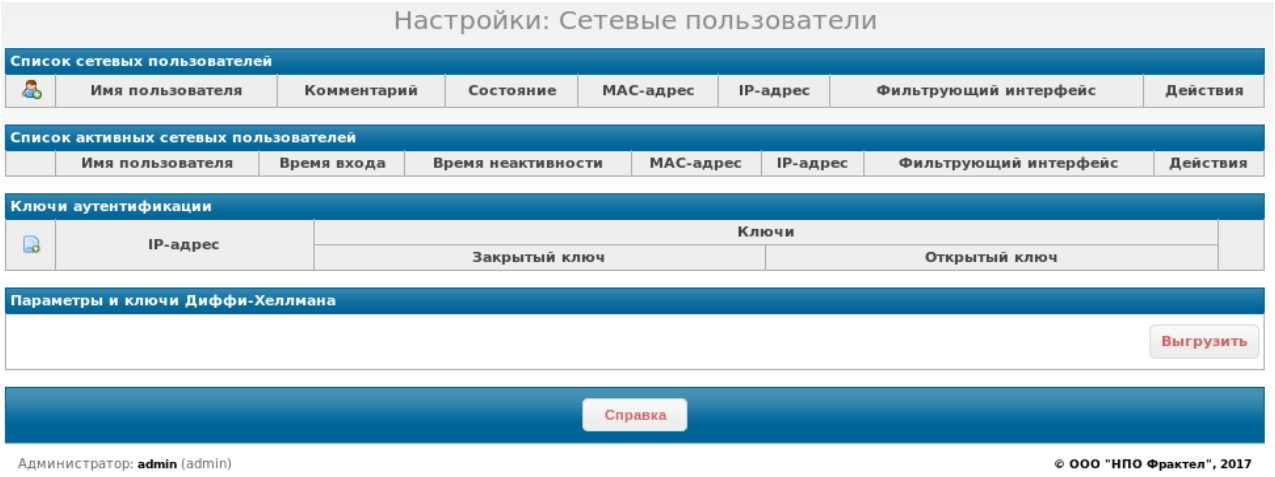
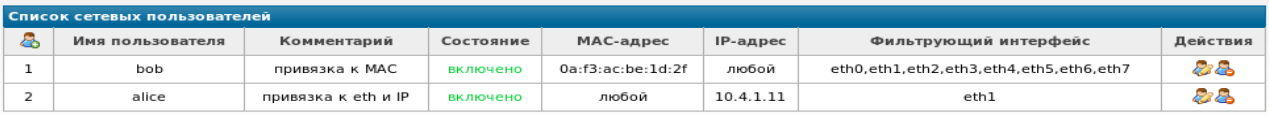


Рисунок 4.60: Исходный вид страницы “Настройки: Сетевые пользователи”



Список сетевых пользователей

	Имя пользователя	Комментарий	Состояние	MAC-адрес	IP-адрес	Фильтрующий интерфейс	Действия
1	bob	привязка к MAC	включено	0a:f3:ac:be:1d:2f	любой	eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth7	
2	alice	привязка к eth и IP	включено	любой	10.4.1.11	eth1	

Рисунок 4.61: Таблица учетных записей сетевых пользователей

Таблица учетных записей сетевых пользователей состоит из следующих полей:

- Поле порядкового номера учетной записи;
- Комментарий – строка комментария к учетной записи;
- Состояние –состояние учетной записи (включено/выключено);
- MAC-адрес – MAC-адрес привязки учетной записи. Аутентификация возможна только для пакетов (кадров) от данного сетевого пользователя с указанным MAC-адресом источника;

- `IP-адрес` – IP-адрес привязки учетной записи. Аутентификация возможна только для пакетов от данного сетевого пользователя с указанным IP-адресом источника;
- `Фильтрующий интерфейс` – список фильтрующих интерфейсов привязки учетной записи. Аутентификация возможна только для пакетов от данного сетевого пользователя, поступивших на один из указанных в списке интерфейсов МЭ;
- `Действия` – поле действий над учетной записью (редактирование и удаление).

В таблице используются следующие иконки для модификации содержимого таблицы:

- – добавление учетной записи;
- – редактирование учетной записи;
- – удаление учетной записи.

По нажатию на иконку добавления учетной записи открывается форма добавления сетевого пользователя, приведенная на рисунке 4.62, стр. 269. По нажатию на иконку редактирования учетной записи открывается форма редактирования сетевого пользователя, пример которой приведен на рисунке 4.63, стр. 269.

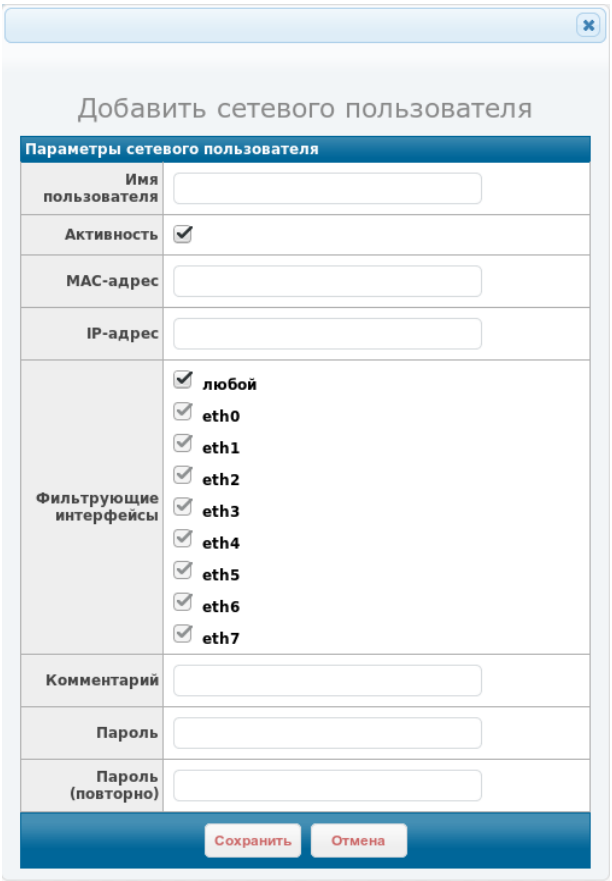


Рисунок 4.62: Форма добавления сетевого пользователя

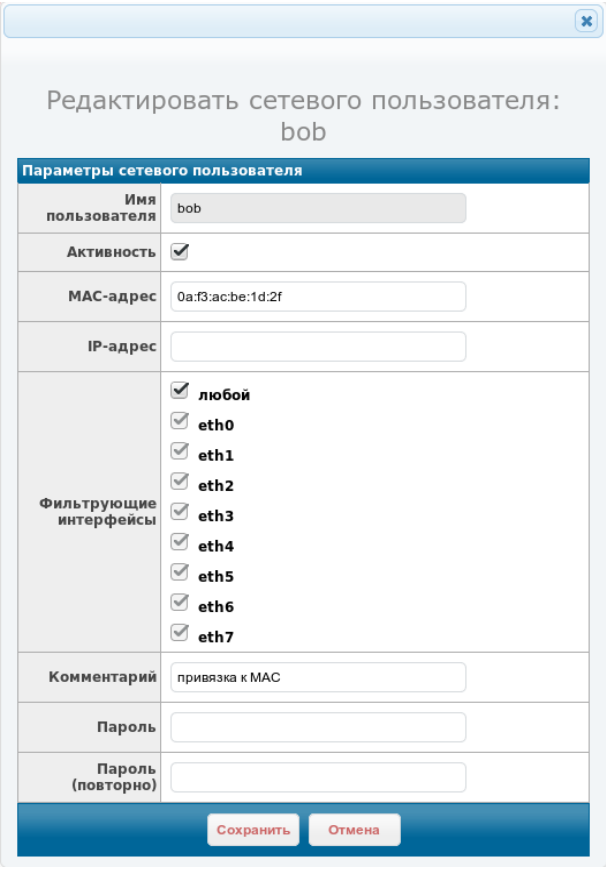


Рисунок 4.63: Пример формы редактирования сетевого пользователя

Формы идентичны по своей структуре, за тем исключением, что форма редактирования сетевого пользователя не позволяет изменить имя сетевого пользователя (поле заблокировано). Форма добавления сетевого пользователя содержат следующие элементы ввода данных:

- `Имя пользователя` – имя сетевого пользователя;
- `Активность` – состояние учетной записи (включено/выключено). Значение по умолчанию: **`включено`**;
- `MAC-адрес` – MAC-адрес привязки учетной записи. Значение по умолчанию: **`отсутствует`** (привязка отсутствует);
- `IP-адрес` – IP-адрес привязки учетной записи. Значение по умолчанию: **`отсутствует`** (привязка отсутствует);
- `Фильтрующие интерфейсы` – список фильтрующих интерфейсов привязки учетной записи. Значение по умолчанию: **`выбраны все интерфейсы`** (привязка отсутствует: доступ разрешен со всех фильтрующих интерфейсов МЭ);
- `Комментарий` – строка комментария к учетной записи. Значение по умолчанию: **`отсутствует`** (комментарий отсутствует);
- `Пароль` – поле ввода пароля учетной записи;
- `Пароль (повторно)` – поле повторного ввода пароля учетной записи.

Требования к форматам имени и пароля сетевого пользователя приведены в приложении А, стр. 423.

Список активных сетевых пользователей. Секция содержит таблицу активных сетевых пользователей, т. е. прошедших процедуру аутентификации и чей тайм-аут неактивности не истек к данному моменту. Процедура аутентификации сетевого пользователя выполняется с использованием утилит МЭ ССПТ-4А1 на ПК сетевого пользователя. Описание ее использования приводится в приложении 3, стр. 565.

Таблица активных сетевых пользователей (рисунок 4.60, стр. 268) состоит из следующих полей:

- `Имя пользователя` – имя сетевого пользователя;
- `Время входа` – дата и время входа (авторизации) сетевого пользователя;
- `Время неактивности` – интервал времени с момент получения на интерфейс МЭ последнего сетевого пакета от данного сетевого пользователя;
- `MAC-адрес` – MAC-адрес сетевого интерфейса ПК сетевого пользователя;
- `IP-адрес` – IP-адрес сетевого пользователя;
- `Фильтрующий интерфейс` – фильтрующий интерфейс МЭ, через который был авторизован сетевой пользователь;

- `Действия` – поле для размещения иконки завершения сеанса сетевого пользователя (других действий не предусмотрено).

В таблице активных сетевых пользователей используются следующие управляющие иконки:

- – завершить сеансы работы всех активных сетевых пользователей;
- – завершить сеанс работы данного сетевого пользователя.

Ключи аутентификации сетевых пользователей. Данная секция содержит таблицу ключей аутентификации сетевых пользователей. Изначально таблица – пустая (рисунок 4.60, стр. 268). Пример таблицы, при наличии записей, приведен на рисунке 4.64, стр. 271.

Ключи аутентификации

	IP-адрес	Ключи		
		Закрытый ключ	Открытый ключ	
1	10.4.1.11	59E7183998B200E302418B86AE70465B 75F0A28DB359A138FEDF89DFD6E4928E 76B1E81EA4F7D470B4750486BA12F4DF A8C151A72EC286C211B0801E2F676874 EAF5267E85221FB1C02CC567D1E26C5C 8F45AFFDED3C55B101D9531D20619B00 F4CAC61D317B53D721F74FE6C1AEFD61 A33E67AC3B142B7B4F4335FEF4892D62 150C2C3925863EF1DF108599797D2EAA AAD3B5B239CF6005BD14609040D2E4A1 D95FD843488713CE497BF1EE29F6F8AB 703E50F5B33375D425CCE2ECDA32C450 87B77A1C053497B95898FCEE6BD19BD6 E6F90C890DE1027D4F00826A2722C908 80E3AB4FFCA2E882D69B6610DFED101E E53675E75989A697F35E236384667AAD	0747235C571C7D60B96B9DC0CE6C5039 E89F93147CEFE3209B1DD372A2991483 866402D33CC7A0F27AA231B48D88A066 F2445DA151EB6F3A66CC8497F0592212 D70DCF8A4C89AF458D3E43BBAB2B68E0 80E6BB92404E0C033A5B0D42F3E78FA5 5D71A0B34534390FA82A64E75606E112 AACB366F5DC735A99F74ADD3A569CD4E BD1BC411574B1F2AC15CAE9C88F7E5BD E78906A137A141DC484ABDFF3849FE07 4DC82A8E87D7736B0DC5434F11CA46F7 2810782CEE98D170229319998413AA0A A7680FD86FBF0C6D2CB1408A81B67DDF F978CA2D4DDD9A1684366E205AB64282 395C5A9E6CA910011BD6110EB5BBCEF3 FCE63817ED0087937D64CF5F839F3ECE	

Рисунок 4.64: Пример таблицы ключей аутентификации сетевых пользователей

Таблица состоит из следующих полей:

- Поле порядкового номера записи;
- `IP-адрес` – IP-адрес, к которому привязана данная пара ключей;
- `Закрытый ключ` – закрытый ключ сетевого пользователя в шестнадцатеричном виде;
- `Открытый ключ` – закрытый ключ сетевого пользователя в шестнадцатеричном виде;
- Полей действий над данной парой ключей. Для модификации таблицы ключей аутентификации используются следующие иконки:
- – добавление (генерация) пары ключей аутентификации;
- – обновление (повторная генерация и замена) пары ключей для данного IP-адреса;
- – удаление пары ключей аутентификации;
- – выгрузка пары ключей аутентификации на УК администратора.

При нажатии на иконку добавления пары ключей аутентификации открывается соответствующая форма, которая приведена на рисунке 4.66, стр. 272. При нажатии на иконку

выгрузки пары ключей аутентификации открывается формы выбора ключа для выгрузки, приведенная на рисунке 4.66, стр. 272.

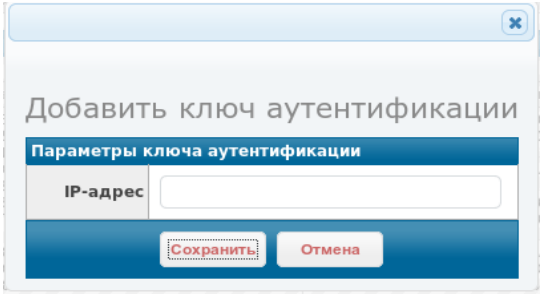


Рисунок 4.65: Форма добавления пары ключей аутентификации

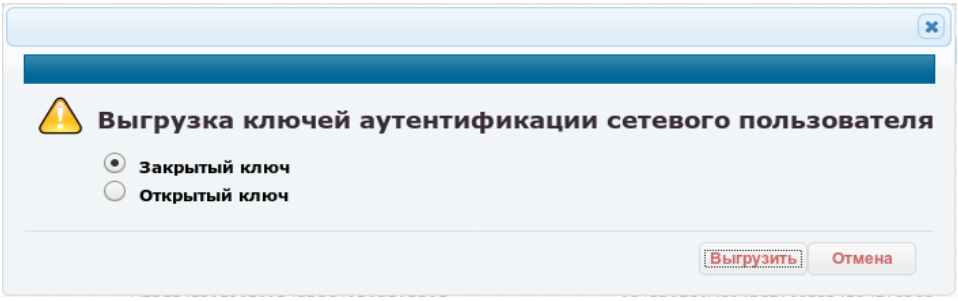


Рисунок 4.66: Форма выбора ключа для выгрузки

Форма добавления пары ключей аутентификации содержит единственное поле ввода: `IP-адрес`, предназначенное для ввода IP-адреса сетевого пользователя, к которому будет привязана пара ключей аутентификации. При нажатии на кнопку `Сохранить` для указанного IP-адреса будет сгенерирована пара ключей аутентификации, которая впоследствии будет выводиться в таблице ключей аутентификации (рисунок 4.64, стр. 271).

Для выполнения процедуры аутентификации требуется выгрузить оба ключа (открытый и закрытый) сетевого пользователя. Выгрузка выполняется последовательно: сначала выгружается один ключ, затем – другой. При нажатии кнопки **`Выгрузить`** (рисунок 4.66, стр. 272.) открывается стандартное окно WEB-браузера для сохранения файла, в котором необходимо выбрать **`Save File`** (**`Сохранить Файл`**) и нажать **`OK`**. Для файлов выгружаемых ключей используются следующие шаблоны имен:

- `<IP-адрес>_dhprvkey.bn` – файл закрытого ключа;
- `<IP-адрес>_dhpubkey.bn` – файл открытого ключа.

где IP-адрес – IP-адрес ПК сетевого пользователя, к которому привязана данная пара ключей.

Аутентификация сетевых пользователей использует двухключевую схему (пара открытый и закрытый ключ). Каждая пара ключей аутентификации привязана к IP-адресу сетевого пользователя. Соответственно для одного IP-адреса сетевого пользователя допускается единственная пара ключей аутентификации.

Для выполнения процедуры аутентификации сетевого пользователя средствами утилит МЭ ССПТ-4А1 пара ключей, соответствующая данному сетевому пользователю (IP-адрес) должна быть вначале выгружена на УК администратора и далее перенесена на ПК сетевого пользователя.

Параметры и ключи Диффи-Хеллмана. Данная секция предназначена для сохранения (выгрузки) параметров Диффи-Хеллмана и открытого ключа экземпляра МЭ ССПТ-4А1, также необходимых для выполнения процедуры аутентификации сетевых пользователей.

Секция содержит единственную кнопку `Выгрузить`, по нажатию на которую открывается диалоговое окно выбора выгружаемого файла. Диалоговое окно приведено на рисунке 4.67, стр 273.

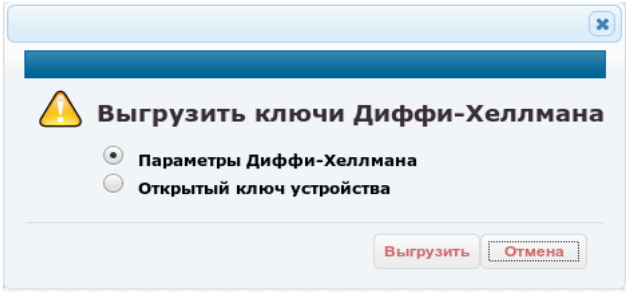


Рисунок 4.67: Диалоговое окно выбора выгружаемого файла

При нажатии на кнопку **`Выгрузить`** открывается стандартное окно WEB-браузера для сохранения файла. Допускается выгрузка следующих файлов:

- `Параметры Диффи-Хеллмана` – файл параметров Диффи-Хеллмана с именем: `fnp4_dhparam.pem`;
- `Открытый ключ устройства` – файл открытого ключа экземпляра МЭ ССПТ-4А1 с именем: `fnp4_dhpubkey.bn`.

Файлы параметров Диффи-Хеллмана и открытого ключа устройства должны быть выгружены на УК администратора и далее перенесены на ПК сетевого пользователя, для возможности выполнения процедуры аутентификации последним.

4.2.6. Настройки: Регистрация

На странице “Настройки: Регистрация” собраны настройки подсистемы регистрации. Фрагмент страницы приведен на рисунке 4.68, стр.274.

Страница “Настройки: Регистрация” разделена на три секции, каждая из которых объединяет логически связанные параметры:

- `Регистрация` – общие настройки подсистемы регистрации, управляющие регистрацией отдельных сущностей.
- `Выгрузка по FTP` – настройки выгрузки журналов регистрации на удаленный FTP-сервер;
- `Выгрузка по SYSLOG` – настройки выгрузки записей регистрации на удаленный SYSLOG-сервер.

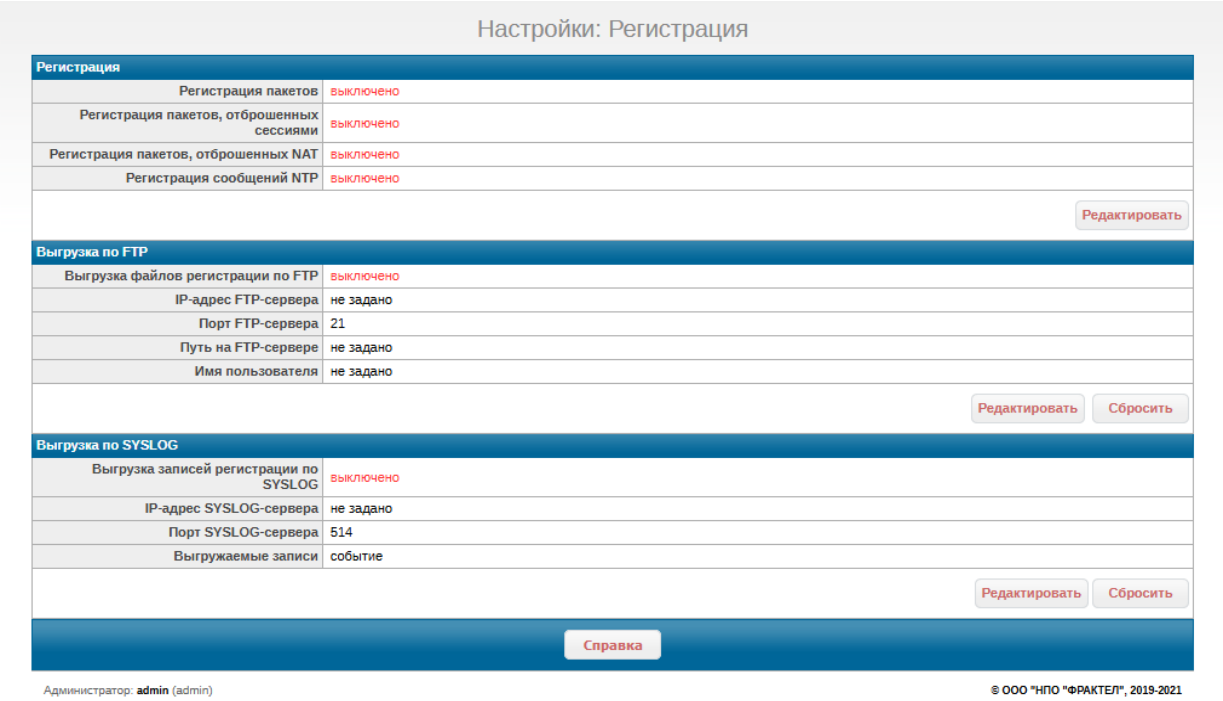


Рисунок 4.68: Фрагмент страницы “Настройки: Регистрация”

Секция “Регистрация” объединяет вывод следующих параметров подсистемы регистрации:

- `Регистрация пакетов`: использование функции регистрации пакетов (`включено` или `выключено`). Значение по умолчанию: **выключено**.
- `Регистрация пакетов, отброшенных сессиями`: использование функции регистрации пакетов, отброшенных сессиями (включено или выключено). Пакет может быть отброшен режимом управления сессиями в силу различных причин: их полный перечень доступен в приложении Б.3, стр. 441 (коды соответствующих ошибок: **`3006`**, **`3009-300F`**). Значение по умолчанию: **выключено**.
- `Регистрация пакетов, отброшенных NAT`: использование функции регистрации пакетов, отброшенных функцией NAT (включено или выключено). Пакет может быть отброшен функцией NAT в силу различных причин: их полный перечень доступен в приложении Б.3, стр. 441 (коды соответствующих ошибок: **`3102-3110`**, **`3112`**, **`3114`**, **`3116`**, **`3117`**). Значение по умолчанию: **выключено**.

- Регистрация сообщений NTP: использование функции регистрации сообщений обновления по NTP в журнал системных сообщений (включено или выключено). Значение по умолчанию: **выключено**.

Кнопка **Редактировать** служит для изменения параметров секции Регистрация. По нажатию на кнопку открывается форма редактирования настроек. Форма приведена на рисунке 4.69, стр. 275.

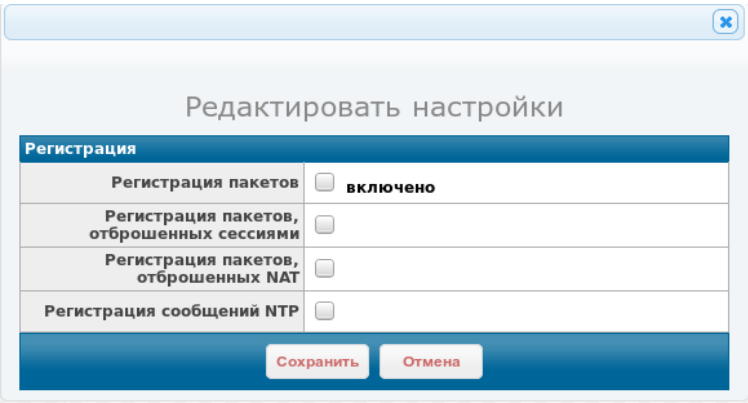


Рисунок 4.69: Форма редактирования настроек регистрации

Функция регистрации пакетов по умолчанию **выключена**. Для регистрации пакетов в соответствии с правилами фильтрации данная функция должна быть **включена**.

Секция "Выгрузка по FTP" объединяет параметры выгрузки журналов регистрации на удаленный FTP-сервер:

- Выгрузка файлов регистрации по FTP – использование функции выгрузки файлов (журналов) регистрации на удаленный FTP-сервер
- IP-адрес FTP-сервера. Значение по умолчанию – **не задано**;
- Порт FTP-сервера. Значение по умолчанию – **21**;
- Путь на FTP-сервере – путь на FTP-сервере для сохранения выгруженных с МЭ файлов регистрации. Значение по умолчанию – **не задано**;
- Имя пользователя. Значение по умолчанию – **не задано**;

Секция имеет две кнопки:

- Редактировать – изменение параметров выгрузки по FTP;
- Сбросить – сброс параметров выгрузки по FTP в значения по умолчанию.

По нажатию на кнопку Редактировать открывается форма редактирования настроек выгрузки по FTP. Форма приведена на рисунке 4.70, стр. 276.

Помимо, указанных выше параметров выгрузки по FTP, форма также позволяет изменить пароль пользователя для доступа к FTP-серверу.

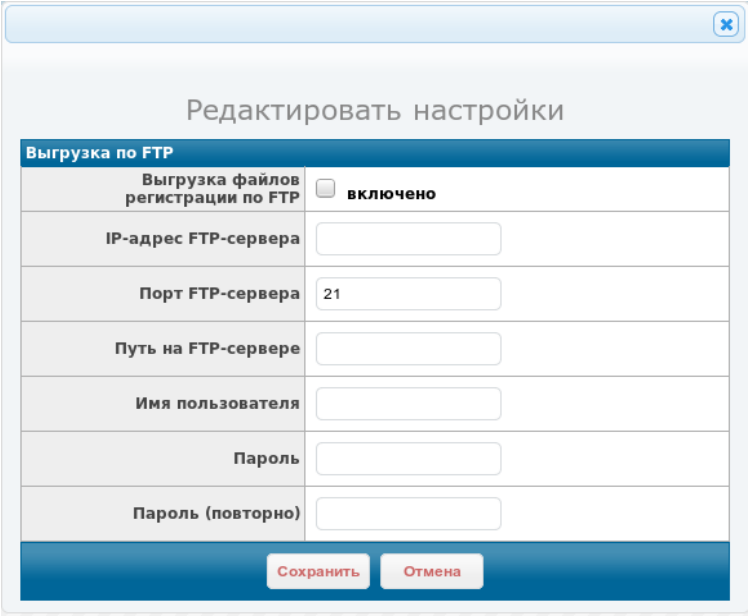


Рисунок 4.70: Форма редактирования настроек выгрузки по FTP

Секция Выгрузка по SYSLOG объединяет параметры выгрузки записей регистрации на удаленный SYSLOG-сервер:

- `Выгрузка записей регистрации по SYSLOG` – использование функции выгрузки записей регистрации на удаленный SYSLOG-сервер (включено/выключено). Значение по умолчанию: **выключено**.
- `IP-адрес SYSLOG-сервера`. Значение по умолчанию – **не задано**;
- `Порт SYSLOG-сервера`. Значение по умолчанию – **514**;
- `Выгружаемые записи` – типы выгружаемых записей регистрации из числа: **пакеты**, **сессии**, **события**. Допускается любая комбинация указанных типов. Значение по умолчанию – **события**.

Секция имеет две кнопки:

- `Редактировать` – изменение параметров выгрузки по SYSLOG;
- `Сбросить` – сброс параметров выгрузки по SYSLOG в значения по умолчанию;

По нажатию на кнопку **Редактировать** открывается форма редактирования настроек выгрузки по SYSLOG. Форма приведена на рисунке 4.71, стр. 277.

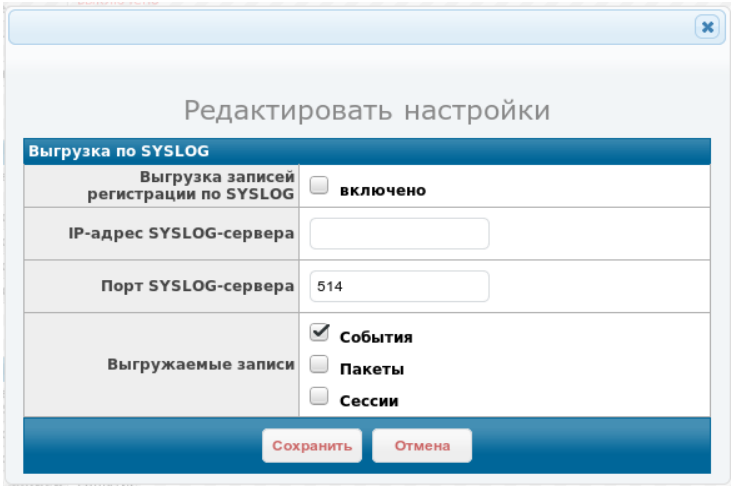


Рисунок 4.71: Форма редактирования настроек выгрузки по SYSLOG

Элементы ввода данных формы соответствуют параметрам выгрузки по SYSLOG, указанным выше.

4.2.7. Настройки: Резервирование

Страница “Настройки: Резервирование” предназначена для настроек функции резервирования МЭ ССПТ-4А1. Руководство по настройке и использованию функции резервирования приведено в разделе 3.5, стр. 116. Исходный вид (настройки резервирования имеют значения по умолчанию) страницы “Настройки: Резервирование” приведен на рисунке 4.72, стр. 277.

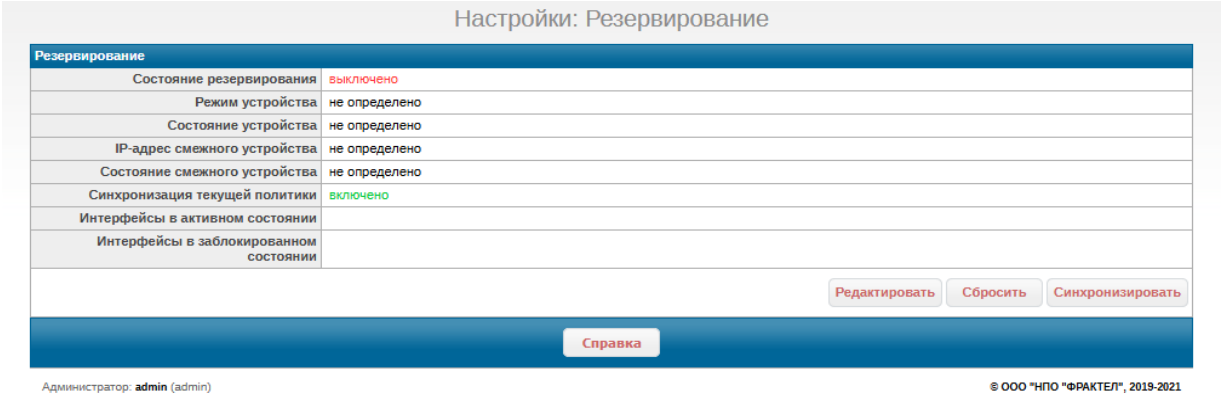


Рисунок 4.72: Исходный вид страницы “Настройки: Резервирование”

На странице выводится следующая информация:

- `Состояние резервирования` – использование функции резервирования (включено/выключено). Значение по умолчанию – **выключено**;
- `Режим устройства` – режим данного устройства в выбранной схеме резервирования. Допустимые значения: **`Balance`**, **`Master`**, **`Slave`**, **`Sync`**. Значение по умолчанию – **не**

определено.

- `Состояние устройства` – текущее состояние данного устройства в схеме резервирования. Имеет смысл только при включенной функции резервирования. Значение по умолчанию – не определено.
- `IP-адрес смежного устройства`. Значение по умолчанию – **не определено**;
- `Состояние смежного устройства` – состояние смежного устройства в схеме резервирования. Имеет смысл только при включенной функции резервирования. Значение по умолчанию – **не определено**;
- `Синхронизация текущей политики` – использование функции автоматической синхронизация текущей политики доступа. Значение по умолчанию – **не определено**;
- `Интерфейсы в активном состоянии` – скорость передачи всех фильтрующих интерфейсов в *активном состоянии* (раздел 3.5, стр. 116). Соответствует максимальной поддерживаемой скорости передачи фильтрующих интерфейсов МЭ. В приведенном примере – **`1000baseT`**;
- `Интерфейсы в заблокированном состоянии` – скорость передачи всех фильтрующих интерфейсов в *заблокированном состоянии* (раздел 3.5, стр. 116). Соответствует минимальной поддерживаемой скорости передачи фильтрующих интерфейсов МЭ. В приведенном примере – **`10baseT/UTP`**.

На странице “Настройки: Резервирование” присутствуют три кнопки:

- `Редактировать` – изменение параметров, включение/выключение функции резервирования;
- `Сбросить` – сброс параметров функции резервирования в значения по умолчанию, при этом, если функция резервирования включена, выполняется ее выключение.
- `Синхронизировать` – немедленная синхронизация текущей политики доступа. В результате текущая политика доступа данного устройства должна быть отправлена смежному устройству и применена на нем в качестве его текущей политики доступа.

По нажатию на кнопку **`Редактировать`** открывается форма редактирования настроек резервирования. Форма допускает изменение всех параметров функции резервирования, перечисленных выше. Форма приведена на рисунке 4.73, стр. 279.

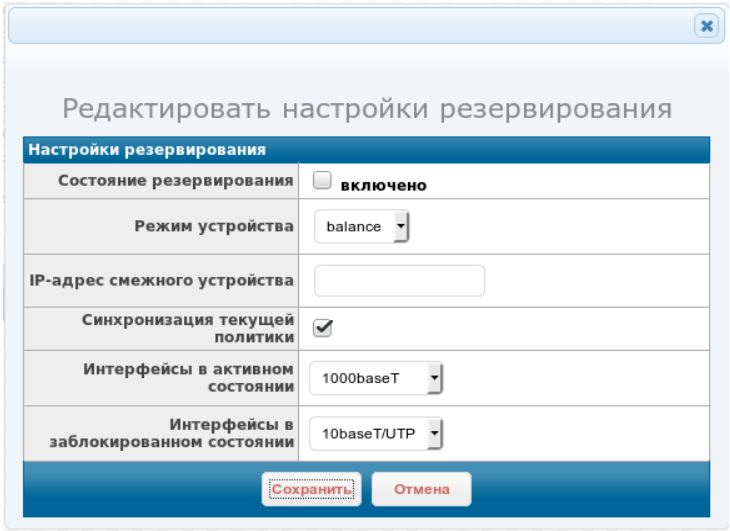


Рисунок 4.73: Форма редактирования настроек резервирования

Следует иметь в виду, что *Состояние устройства* и *Состояние смежного устройства* не являются параметрами конфигурации МЭ ССПТ-4А1 и соответственно не могут быть явно заданы администратором.

Изменение параметров резервирования возможно только когда функция резервирования **выключена**.

В том случае, если набор поддерживаемых скоростей передачи отличается для некоторых фильтрующих интерфейсов МЭ, допускается только использование режима резервирования **Sync**.

4.2.8. Настройки: RADIUS

Страница “Настройки: RADIUS” предназначена для настройки функции авторизации администраторов и/или сетевых пользователей через удаленный RADIUS-сервер. Пример настройки данной функции приведен в разделе 3.4.1, стр. 111. Исходный вид страницы “Настройки: RADIUS” (со значениями параметров по умолчанию) приведен на рисунке 4.74, стр. 280.

Рисунок 4.74: Исходный вид страницы “Настройки: RADIUS”

На странице выводятся следующие параметры авторизации через RADIUS-сервер:

- `Состояние` – использование функции авторизации через RADIUS-сервер (включено/выключено). Значение по умолчанию – **выключено**;
- `Использовать для` – типы учетны записей, для которых разрешена авторизации через RADIUS-сервер. Значение по умолчанию – **`администраторы и сетевые пользователи`**;
- `Тайм-аут ожидания` – тайм-аут ожидания ответа от RADIUS-сервер. Значение по умолчанию – **5** с;
- `Количество обращений к серверу` – максимальное количество обращений к RADIUS-серверу в случае если ответ не был получен в течение тайм-аута ожидания. Значение по умолчанию – **3**;
- `Основной RADIUS-сервер`: параметры основного RADIUS-сервера:
  - ✔ `IP-адрес`. Значение по умолчанию – **`не определено`**;
  - ✔ `Секретный ключ` – строка символов секретного ключа. Значение по умолчанию – **`не определено`**;
  - ✔ `Порт`. Значение по умолчанию – **1812**;
- `Запасной RADIUS-сервер` – параметры основного RADIUS-сервера:
  - ✔ `IP-адрес`. Значение по умолчанию – **`не определено`**;
  - ✔ `Секретный ключ` – строка символов секретного ключа. Значение по умолчанию – **`не определено`**;
  - ✔ `Порт`. Значение по умолчанию – **1812**.

Кнопка **`Редактировать`** предназначена для изменения параметров функции авторизации через RADIUS-сервер, включения или выключения данной функции. По нажатию на кнопку

открывается форма редактирования настроек RADIUS. Форма приведена на рисунке 4.75, стр. 281.

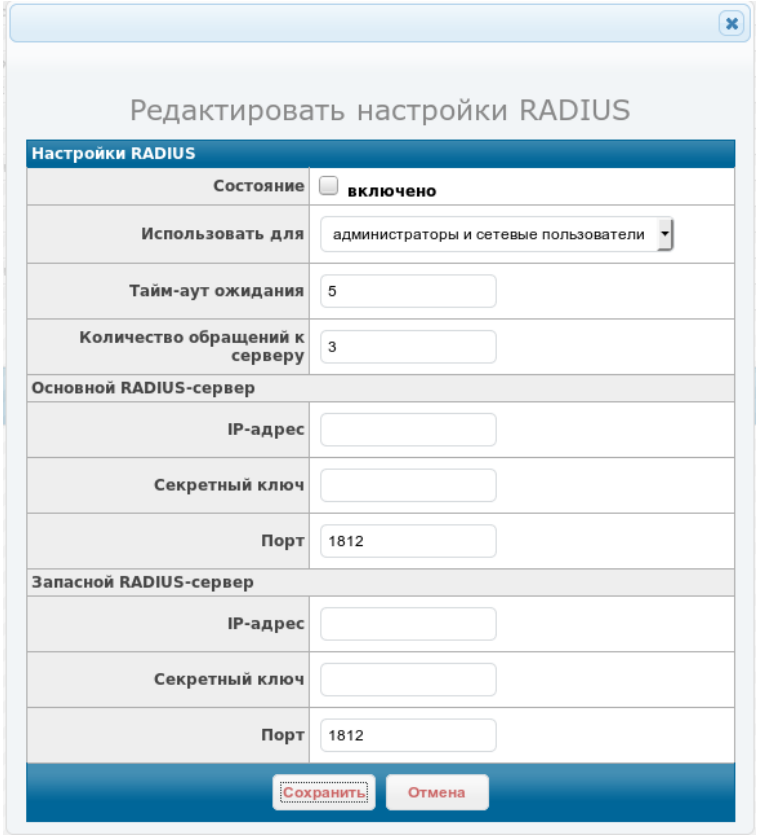


Рисунок 4.75: Форма редактирования настроек RADIUS

Параметры допустимые к изменению в форме полностью соответствуют параметрам выводимым на странице “Настройки: RADIUS”, которые описаны выше.

4.2.9. Настройки: Маршруты

Страница “Настройки: Маршруты” предназначена для работы с системной таблицей маршрутов. Страница состоит из единственной секции “Список маршрутов”, которая представляет собой таблицу маршрутов. Пример таблицы маршрутов, содержащей маршрут по умолчанию, приведен на рисунке 4.76, стр. 281.

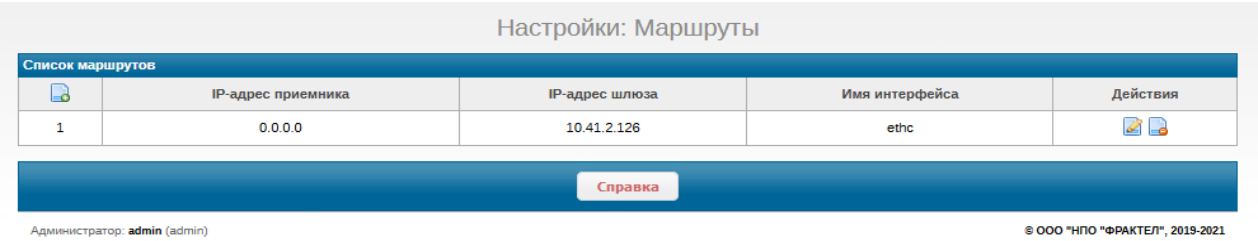


Рисунок 4.76: Пример таблицы маршрутов

Таблица `Список маршрутов` состоит из следующих полей:

- порядковый номер маршрута;
- `IP-адрес приемника` – содержит IP-адрес узла сети или сети назначения;
- `IP-адрес шлюза` – содержит IP-адрес шлюза, которому отправляются IP-пакеты, предназначенные для узла сети или сети, указанных в поле IP-адрес приемника;
- `Имя интерфейса` – имя интерфейса через который отправляются пакеты в соответствии с данным маршрутом;
- `Действия` – содержит управляющие иконки для редактирования и удаления маршрута соответственно.

Значение поля *Имя интерфейса* определяется тем, какой IP-сети принадлежит IP-адрес шлюза по умолчанию в данном маршруте.
Таким образом, поле *Имя интерфейса* может иметь следующие значения:
- **ethc**: маршрут использует управляющий интерфейс для отправки пакетов;
- ***eth<N>***: маршрут использует указанный фильтрующий интерфейс для отправки пакетов от имени HTTP-посредника (соответствующий интерфейс должен быть задан в настройках HTTP-посредника, например: *eth5*).

В таблице маршрутов используются следующие управляющие иконки:

- – добавление маршрута в таблицу;
- – редактирование маршрута;
- – удаление маршрута.

При нажатии на иконку добавления маршрута открывается форма добавления маршрута, приведенная на рисунке 4.77, стр. 282. При нажатии на кнопку редактирования маршрута – форма редактирования маршрута, приведенная на рисунке 4.78, стр 282.

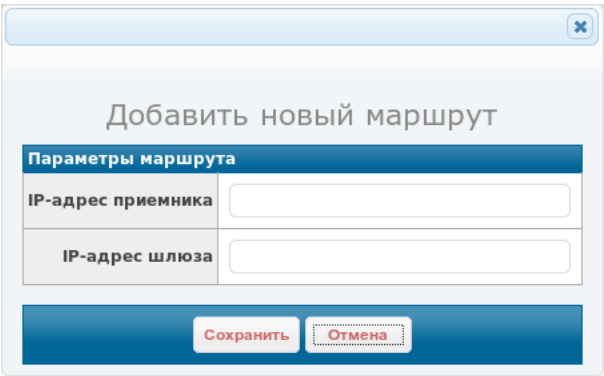


Рисунок 4.77: Форма добавления маршрута

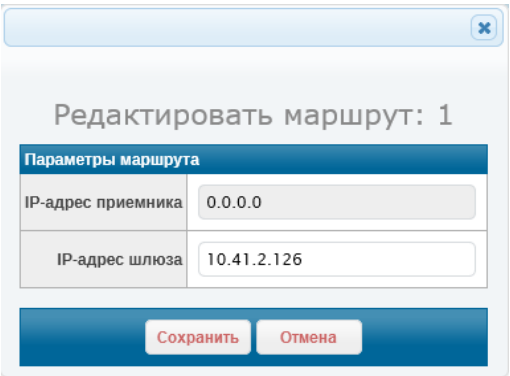


Рисунок 4.78: Форма редактирования маршрута

В поле ввода IP-адрес приемника в форме добавления маршрута допускается указание:

- IP-адреса узла сети. Например, **`192.168.1.1`**;
- IP-адреса сети. Например, **`192.168.1.0/24`**.

Поле ввода `IP-адрес приемника` в форме редактирования маршрута заблокировано, т. к. данный параметр не допускает изменения.

> Если необходимо добавить маршрут по умолчанию, то в поле *IP-адрес приемника* необходимо ввести значение: **0.0.0.0**.
>
> Если маршрут по умолчанию присутствует в таблице маршрутов, то он всегда имеет номер: **1** и соответственно располагается в первой записи таблицы.
>
> *IP-адрес шлюза* должен принадлежать либо IP-сети управляющего интерфейса, либо IP-сети HTTP-посредника. В последнем случае перед добавлением маршрута функция HTTP-посредника должна быть настроена и включена администратором МЭ ССПТ-4А1.

4.2.10. Настройки: HTTP-посредник

Страница “Настройки: HTTP-посредник” предназначена для настройки параметров конфигурации МЭ ССПТ-4А1, относящихся к функции HTTP-посредника. Исходный вид страницы (соответствующий конфигурации по умолчанию) приведен на рисунке 4.79, стр. 283.

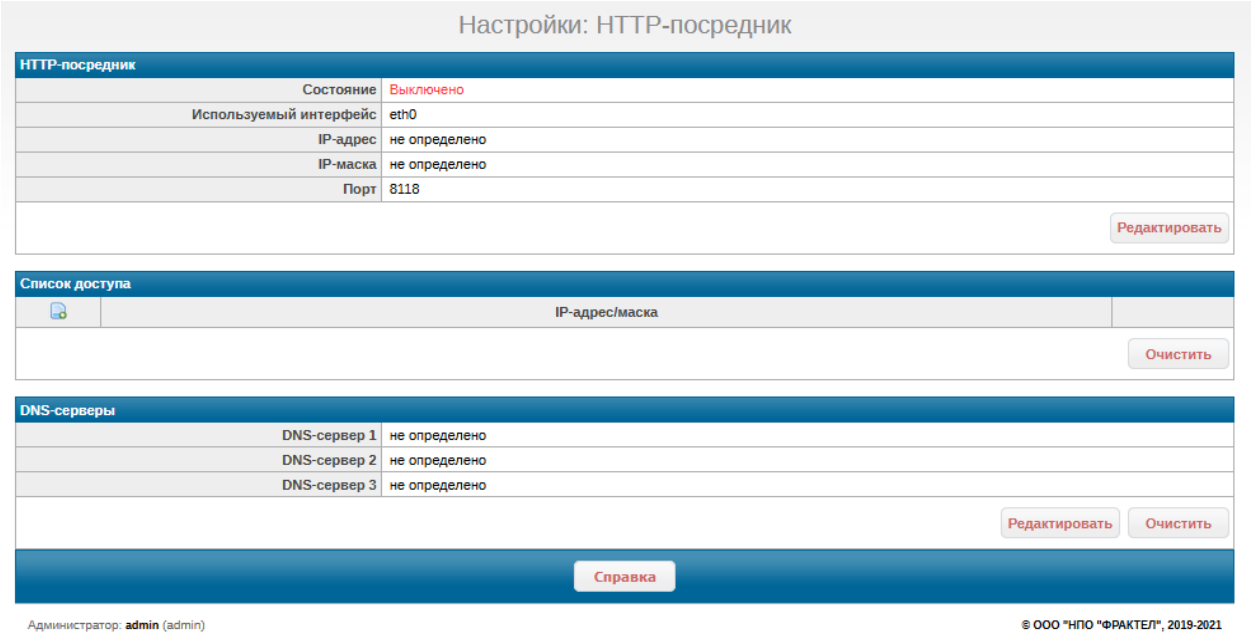


Рисунок 4.79: Исходный вид страницы “Настройки: HTTP-посредник”

Страница “Настройки: HTTP-посредник” состоит из трех секций:

- `HTTP-посредник` – основные параметры HTTP-посредника;
- `Список доступа` – список доступа к сетевому интерфейсу, используемому HTTP-посредником;
- `DNS-серверы` – список DNS-серверов для разрешения доменных имен WEB-страниц, доступ к которым осуществляется через HTTP-посредник.

Секция “HTTP-посредник” предназначена для настройки основных параметров HTTP-посредника. В секции выводится следующая информация:

- `Состояние`: использование функции HTTP-посредника (включено/выключено). Значение по умолчанию: **выключено**;
- `Используемый интерфейс`: фильтрующий интерфейс, предназначенный для использования HTTP-посредником (когда функция HTTP-посредника включена). Далее: *интерфейс HTTP-посредника*). Значение по умолчанию: **не определено**;
- `IP-адрес`: IP-адрес, назначаемый на интерфейс HTTP-посредника при включении функции HTTP-посредника. Значение по умолчанию: **`eth0`**;
- `Порт`: TCP-порт, используемый HTTP-посредником (когда функция HTTP-посредника включена). Значение по умолчанию: **`8118`**.

В секции расположена единственная кнопка `Редактировать`, по нажатию на которую открывается форма редактирования настроек HTTP-посредника. Форма приведена на рисунке 4.80, стр. 284.

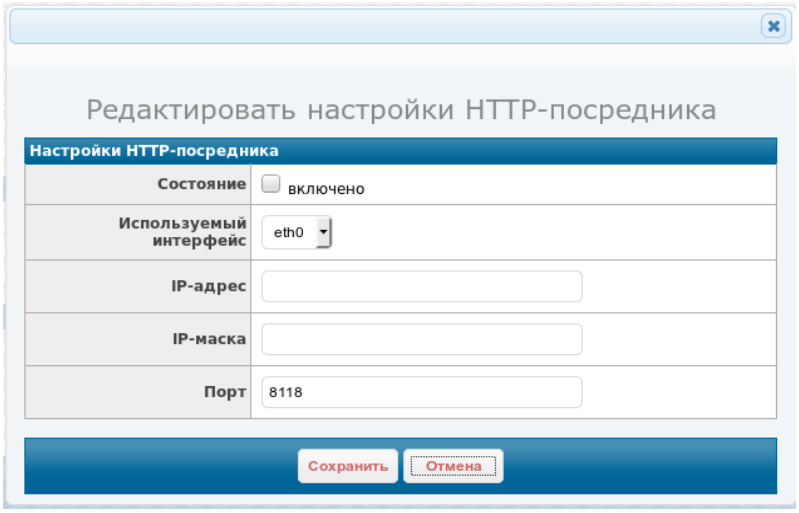


Рисунок 4.80: Форма редактирования настроек HTTP-посредника

Форма позволяет задать значения параметров HTTP-посредника, которые выводятся в секции `HTTP-посредник`. Их описание приведено выше.

Значения всех доступных параметров могут быть изменены как при выключенной, так и при включенной функции HTTP-посредника,

При включении функции HTTP-посредника фильтрующий интерфейс, выбранный в списке *Используемый интерфейс*, становится *интерфейсом HTTP-посредника* и перестает участвовать в фильтрации: пакеты, поступившие на данный интерфейс, не обрабатываются пакетным фильтром, и в то же время пакетный фильтр не передает пакеты на данный интерфейс, даже если общие правила фильтрации предписывают это.

Секция “Список доступа” позволяет ограничить доступ к интерфейсу HTTP-посредника, предоставив доступ только заданным узлам сети и IP-подсетям. Изначально список доступа к HTTP-посреднику – пуст, т. е. доступ разрешен любым узлам сети, независимо от их

IP-адресов. Исходный вид секции приведен на рисунке 4.81, стр. 285. Пример секции с заданным списком доступа приведен на рисунке 4.82, стр. 285.

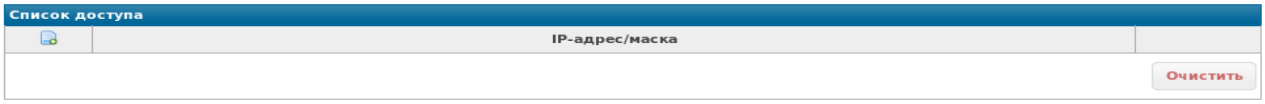


Рисунок 4.81: Пустой список доступа к HTTP-посреднику

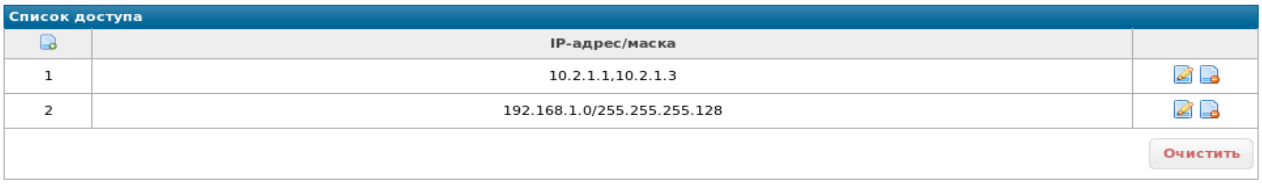


Рисунок 4.82: Пример списка доступа к HTTP-посреднику

Для модификации списка доступа используются следующие иконки:

- – добавить запись в список доступа;
- – редактировать запись списка доступа.
- – удалить запись из списка доступа.

По нажатию на кнопку `Очистить` удаляются все записи списка доступа: ограничение доступа к интерфейсу HTTP-посредника отменяется.

При нажатии на иконку добавления записи в список доступа открывается соответствующая форма, приведенная на рисунке 4.83, стр. 285.

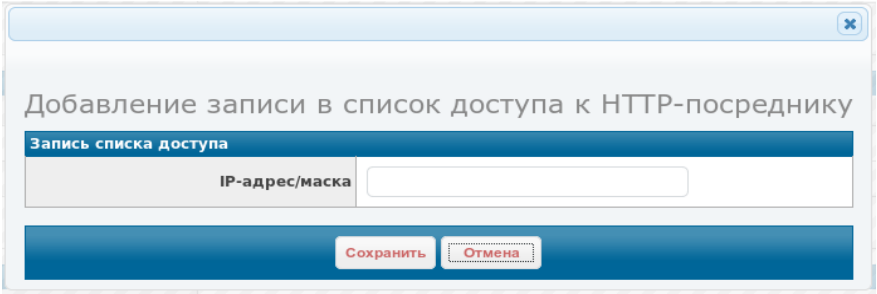


Рисунок 4.83: Форма добавления записи в список доступа к HTTP-посреднику

Форма добавления записи в список доступа имеет единственное поле ввода: `IP-адрес/маска`. Допускается задание списка, включающего в себя элементы следующих типов:

- одиночный IP-адрес (например, **`192.168.1.1`**);
- IP-подсеть (например, **`192.168.1.0/24`**).

Форма редактирования записи списка доступа к HTTP-посреднику идентична по своей структуре форме добавления, поэтому не нуждается в отдельном рассмотрении.

Секция “DNS-серверы” позволяет задать до трех DNS-серверов для разрешения доменных имен WEB-страниц, к которым ведется обращение через HTTP-посредник. В секции выводятся DNS-серверы, заданные в текущей конфигурации. По умолчанию DNS-серверы не заданы. Пример секции в отсутствие DNS-серверов приведен на рисунке 4.84, стр. 286. Пример секции, при наличии двух DNS-сервров приведен на рисунке 4.85, стр. 286.

Рисунок 4.84: DNS-серверы не заданы

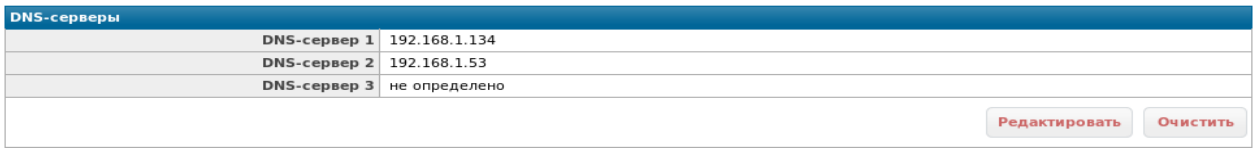


Рисунок 4.85: Задано два DNS-сервера

Если DNS-сервер не задан, то в соответствующей позиции выводится: **не определено**. При этом, если в конфигурации задано от одного до двух DNS-серверов включительно, то DNS-серверы выводятся подряд, начиная с первой позиции, а в оставшихся позициях выводится: **не определено**.

В секции имеются две кнопки:

- **`Редактировать`** – служит для редактирования набора DNS-серверов.
- **`Очистить`** – служит для очистки набора DNS-серверов. В результате очистки в конфигурации не будет задано ни одного DNS-сервера.

По нажатию на кнопку `Редактировать` открывается форма редактирования DNS-серверов, пример которой приведен рисунке 4.86, стр. 287.

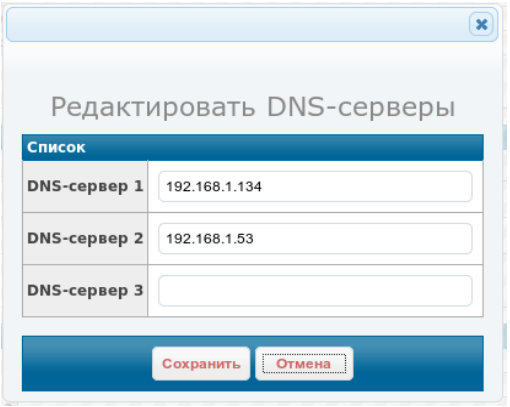


Рисунок 4.86: Пример формы редактирования DNS-серверов

Для возможности использования HTTP-посредника должен быть задан хотя бы один DNS-сервер, так как обращегние к WEB-страницам обычно производится через URL, включающий в себя доменное имя WEB-сервера, а не его IP-адрес.

В форме редактирования DNS-серверов администратору разрешается вводить IP-адреса в любых из имеющихся полей ввода, но хотя бы одно из полей ввода должно быть обязательно заполнено.

При нажатии кнопки *Сохранить* будет учтен порядок (приоритет) IP-адресов. Это означает, например, что если администратор заполнил поля *“DNS-сервер 1”* и *“DNS-сервер 3”*, то при следующем выводе страницы *Настройки: HTTP-посредник* в списке DNS-серверов окажутся заполненными позиции 1 и 2. Иначе говоря при заполнении формы, важен приоритет от 1 к 3, а не конкретная позиция.

4.3. Управление политиками доступа

Пункт `Политика` основного меню WEB-инетрфейса реализует доступ к группе страниц, предназначенных для выполнения действий над текущей и дополнительной политиками доступа. Эта группа включат в себя следующие страницы:

- `Политика: Управление` – действия над политиками доступа как над единым целым (сохранение, применение, загрузка, выгрузка).
- `Политика: Справочник` – действия над объектами справочника (добавление, изменение, удаление);
- `Политика: Правила` – действия над правилами фильтрации, правилами приоритизации, правилами HTTP-посредника;
- `Политика: Статистика` – статистика использования правил фильтрации текущей политики доступа.

При нажатии на пункт `Политика` основного меню WEB-интерфейса открывается страница “Политика: Управление”.

4.3.1. Политика: Управление

Страница “Политика: Управление” предназначена для выполнения действий над политиками доступа как над единым целым (без манипуляций с отдельными правилами и объектами справочника).

Исходный (с дополнительными политиками доступа по умолчанию) вид страницы “Политика: Управление” приведен на рисунке 4.87, стр. 288.

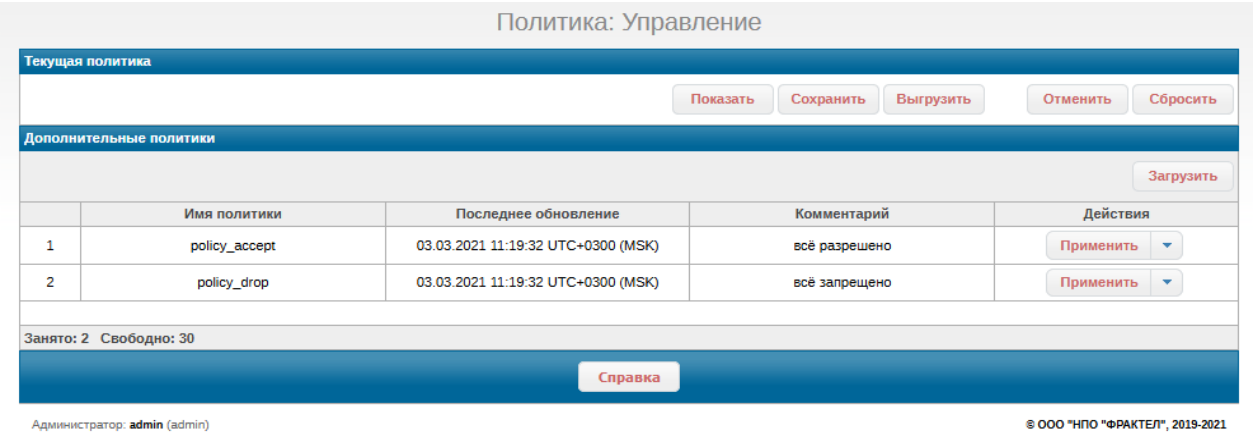


Рисунок 4.87: Исходный вид страницы “Политика: Управление”

Страница содержит две секции:

- `Текущая политика` – выполнение действий над текущей политикой;
- `Дополнительные политики` – просмотр списка дополнительных политик и выполнение действий над ними.

Секция “Текущая политика” содержит четыре кнопки:

- **`Показать`** – вывод справочника объектов и правил фильтрации текущей политики доступа;
- **`Сохранить`** – сохранение текущей политики доступа в дополнительную;
- **`Выгрузить`** – выгрузка текущей политики доступа на УК администратора;
- **`Отменить`** – отмена последнего изменения в текущей политике доступа;
- **`Сбросить`** – сброс текущей политики доступа в состояние по умолчанию.

По нажатию на кнопку `Показать` открывается окно просмотра справочника и правил текущей политики доступа. Окно содержит две вкладки:

- `Справочник` – просмотр файла справочника;
- `Правила` – просмотр файла правил.

Вкладка `Справочник` приведена на рисунке 4.88, стр. 289, вкладка `Правила` – на рисунке 4.89, стр. 289.

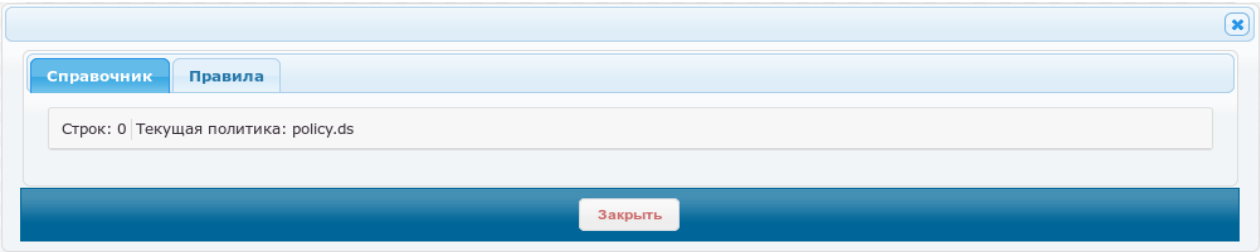


Рисунок 4.88: Просмотр файла справочника текущей политики доступа

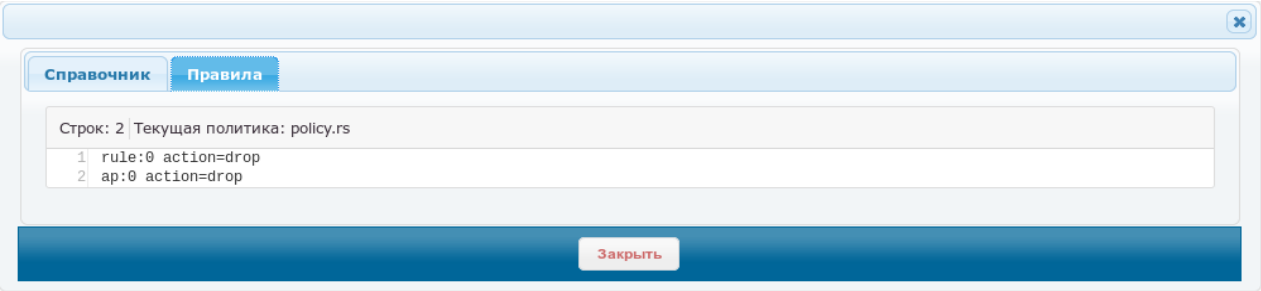


Рисунок 4.89: Просмотр файла правил текущей политики доступа

В приведенном примере – просмотр текущей политики доступа в состоянии по умолчанию:

- объекты справочника отсутствуют;
- глобальное общее правило с действием: удалить (`drop`);
- глобальное AP-правило с действием: удалить (`drop`).

По нажатию на кнопку `Сохранить` (рис. 4.87, стр. 288) открывается форма сохранения текущей политики доступа в дополнительную. Данная форма приведена на рисунке 4.90, стр. 289.

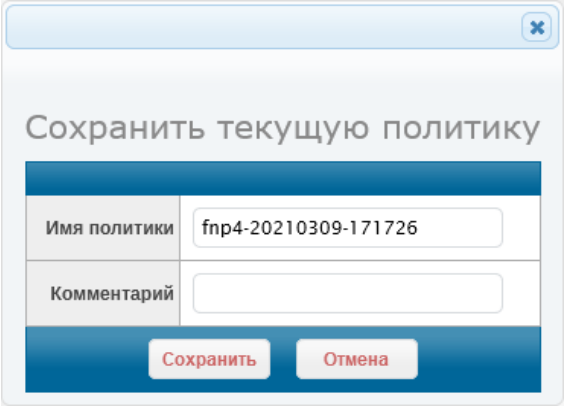


Рисунок 4.90: Форма сохранения текущей политики доступа

В форме сохранения текущей политик два поля ввода:

- `Имя политики` – имя дополнительной политики доступа. Значение поля должно соответствовать формату *имени дополнительной конфигурации и дополнительной политики*

доступа (приложение А, стр. 423). Значение по умолчанию соответствует шаблону `fnp4-<ГГГГММДД>-<ЧЧММСС>`.

- `Комментарий` – строка комментария к политике доступа. Значение поля должно соответствовать формату *строки комментария* (приложение А, стр. 423). Значение по умолчанию: пустая строка (комментарий отсутствует).

В результате сохранения текущей политики доступа она появится в списке дополнительных политик доступа в секции `Дополнительные политики`.

Выгрузка текущей политики доступа. Для выгрузки текущей политики доступа необходимо выполнить следующие шаги:

1) Нажать на кнопку **`Выгрузить`** в секции **`Текущая политика`** (рис. 4.91, стр. 290).
2) В результате выполнения пункта 1 откроется стандартное окно WEB-браузера для сохранения файла, в котором необходимо выбрать **`Save File`** (**`Сохранить Файл`**) и нажать кнопку **`OK`** (рис. 4.92, стр. 290).

В результате выполнения данных шагов файл текущей политики доступа будет сохранен в каталоге загрузки файлов, заданном в настройках WEB-браузера. Файл сохраняется с именем, соответствующим шаблону `fnp4-<ГГГГММДД>-<ЧЧММСС>.aps`.

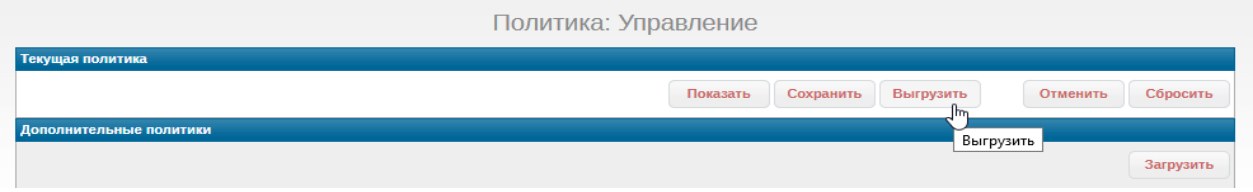


Рисунок 4.91: Выгрузка текущей политики доступа

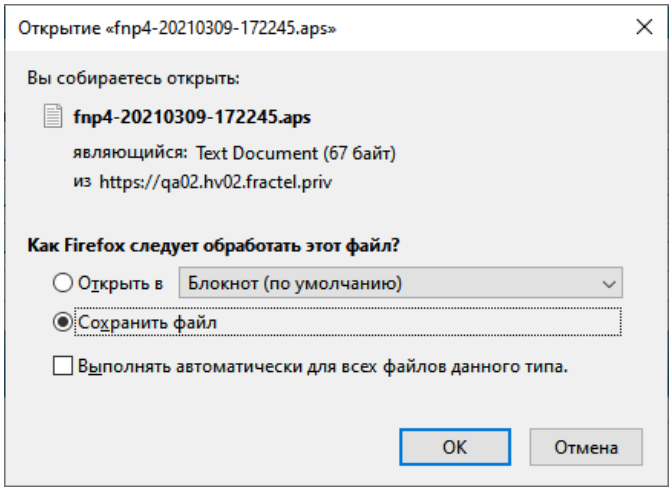


Рисунок 4.92: Сохранение текущей политики доступа на УК

При на нажатии на кнопку `Сбросить` (рис. 4.87, стр. 288) открывается диалоговое окно выбора компонент текущей политики доступа для сброса. Окно приведено на рисунке 4.93, стр 291.

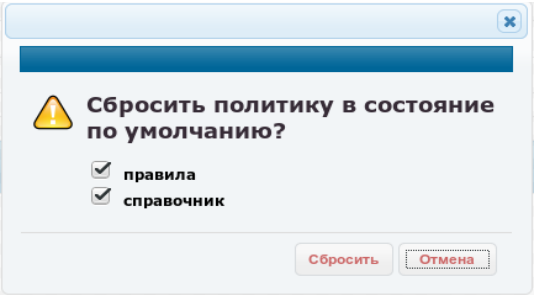


Рисунок 4.93: Окно сброса текущей политики доступа

Окно позволяет выбрать компоненты текущей политики доступа:

- **правила** – правила фильтрации будут сброшены в состояние по умолчанию;
- **справочник** – справочник будет сброшен в состояние по умолчанию.

По умолчанию выбраны обе компоненты политики для сброса. При выборе только справочника, возможен отказ в сбросе политики доступа, в том случае если объекты справочника используются в правилах фильтрации. В таком случае следует сбрасывать обе компоненты политики.

Секция “Дополнительные политики” организована следующим образом: справа вверху находится кнопка `Загрузить`, ниже – таблица дополнительных политик доступа (рис. 4.87, стр. 288).

Загрузка дополнительной политики доступа. По нажатию на кнопку `Загрузить` открывается форма загрузки дополнительной политики на МЭ ССПТ-4А1 с УК администратора. Форма приведена на рисунке 4.94, стр. 291. Пример формы загрузки дополнительной политики после выбора файла приведен на рисунке 4.95, стр. 291. Пример таблицы дополнительных политик, в котором присутствует политика, загруженная на МЭ с УК приведен на рисунке 4.96, стр. 292.

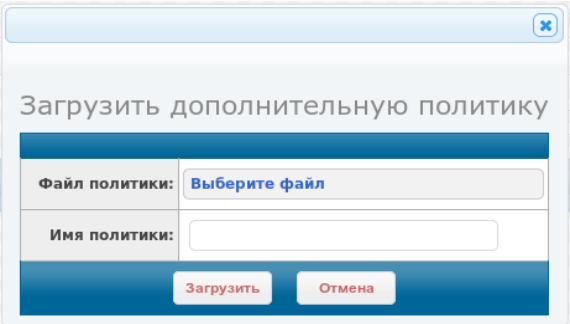


Рисунок 4.94: Форма загрузки дополнительной политики

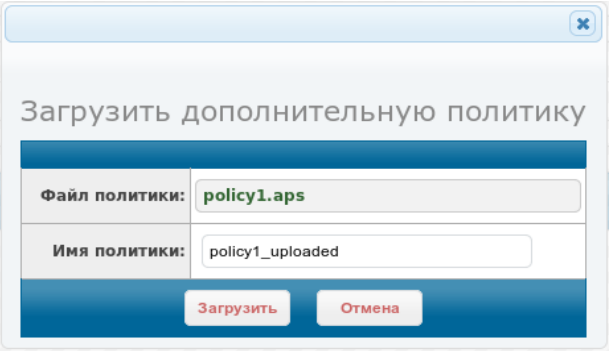
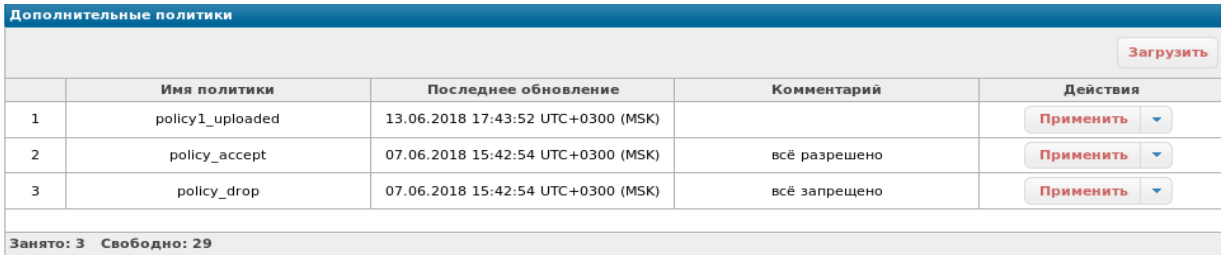


Рисунок 4.95: Форма загрузки дополнительной политики: файл выбран

Форма загрузки дополнительной политики (рис. 4.94, стр. 291) содержит следующие элементы ввода данных:

- Кнопка **Выберите файл** – выбор файла дополнительной политики для загрузки;
- Имя политики – поле ввода имени дополнительной политики;

По нажатию на кнопку Выберите файл открывается стандартное окно WEB-браузера



Дополнительные политики

Загрузить

	Имя политики	Последнее обновление	Комментарий	Действия
1	policy1_uploaded	13.06.2018 17:43:52 UTC+0300 (MSK)		Применить
2	policy_accept	07.06.2018 15:42:54 UTC+0300 (MSK)	всё разрешено	Применить
3	policy_drop	07.06.2018 15:42:54 UTC+0300 (MSK)	всё запрещено	Применить

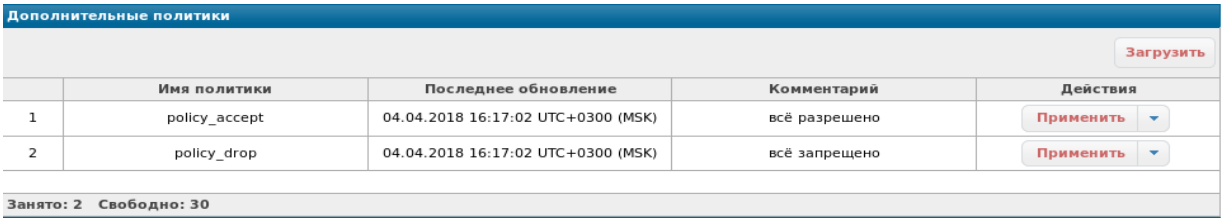
Занято: 3 Свободно: 29

Рисунок 4.96: Таблица дополнительных политик: после загрузки политики с УК

файла. В противном случае – имя, указанное в данном поле (рис. 4.95, стр. 291).

По нажатию на кнопку **Загрузить** выполняется загрузка выбранного файла дополнительной политики доступа. В результате – в таблицу дополнительных политик будет добавлена политика, загруженная с УК (рис. 4.96, стр. 292).

Таблица дополнительных политик доступа приведена на рисунке 4.97, стр. 292.



Дополнительные политики

Загрузить

	Имя политики	Последнее обновление	Комментарий	Действия
1	policy_accept	04.04.2018 16:17:02 UTC+0300 (MSK)	всё разрешено	Применить
2	policy_drop	04.04.2018 16:17:02 UTC+0300 (MSK)	всё запрещено	Применить

Занято: 2 Свободно: 30

Рисунок 4.97: Таблица дополнительных политик

Изначально (на момент поставки) на МЭ ССПТ-4А1 присутствуют две дополнительные политики (рис. 4.97, стр. 292):

- **policy_accept**: политика содержит:
  - ✔ глобальное общее правило с действием: пропустить (**accept**);
  - ✔ глобальное АР-правило с действием: удалить (**drop**);
- **policy_drop**:
  - ✔ глобальное общее правило с действием: пропустить (**drop**);
  - ✔ глобальное АР-правило с действием: удалить (**drop**);

Дополнительная политика **policy_accept** разрешает прохождение всех пакетов через МЭ ССПТ-4А1 в случае конфигурации по умолчанию, т. е. когда использование прикладных правил (АР-правил) выключено.

Дополнительная политика **policy_drop** соответствует текущей политики доступа по умолчанию.

МЭ ССПТ-4А1 позволяет хранить до **32** дополнительных политик.

Таблица дополнительных политик (рис. 4.97, стр. 292) состоит из следующих полей:

- порядковый номер политики;
- `Имя политики`;
- `Последнее обновление` – дата и время последнего обновления дополнительной политики с указанием часового пояса;
- `Комментарий` – строка комментария к дополнительной политике;
- `Действие` – выбор действия над дополнительной политикой.

В поле `Действие` располагаются кнопки:

- **`Применить`**;
- – кнопка выбора действия;

Кнопка `Применить` служит для применения данной дополнительной политики в качестве текущей политики доступа.

При нажатии на кнопку выбора действия отображается меню выбора действия над дополнительной политикой. Пример данного меню приведен на рисунке 4.98, стр. 294.

Меню выбора действий содержит следующие элементы:

- `Показать` – просмотр политики доступа в виде текстовых определений объектов справочника и правил (аналогично просмотру текущей политики доступа);
- `Переименовать` – смена имени и/или комментария к политике. Форма переименования дополнительной политики приведена на рисунке 4.99, стр. 294;
- `Удалить` – удаление файла политики с носителя данных МЭ ССПТ-4А1;
- `Выгрузить` – выгрузка (сохранение) файла политики на УК администратора. Выгрузка дополнительной политики на УК администратора выполняется аналогично выгрузке текущей политики, рассмотренной ранее в данном разделе. Единственное отличие — имя сохраняемого файла формируется по другому шаблону: `<имя_политики>.aps`

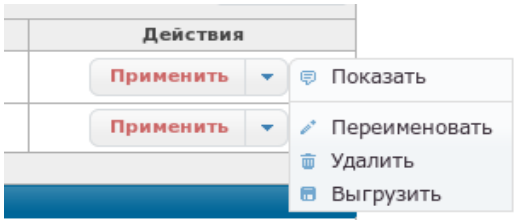


Рисунок 4.98: Выбор действия над политикой

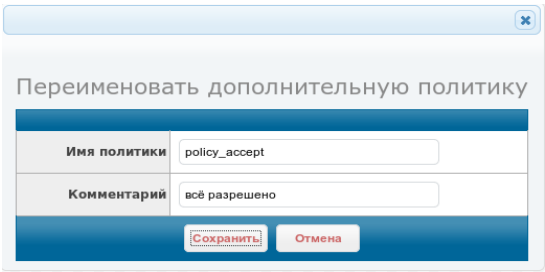


Рисунок 4.99: Форма переименования дополнительной политики

Форма переименования дополнительной политики (рисунок 4.99, стр. 294) содержит два поля ввода:

- `Имя политики` – поле ввода нового имени для политики. Изначально в поле ввода установлено текущее имя политики;
- `Комментарий` – поле ввода комментария к политике. Изначально в поле ввода установлен текущий комментарий к политике.

При нажатии на кнопку **`Сохранить`** выполняется проверка введенных данных. Форматы имени политики и общий формат комментария приведены в приложении А, стр. 423. Если данные корректны, то выполняется переименование файла политики и/или смена комментария к ней.

4.3.2. Политика: Справочник

Страница “Политика: Справочник” предназначена для просмотра и модификации справочника текущей политики доступа и дополнительных политик доступа (для дополнительных политик: только добавление объектов).

Страница “Политика: Справочник” приведена на рисунке 4.100, стр. 295.

Страница разделена на две части:

- слева – дерево объектов, в каждой ветви которого расположены объекты одного типа;
- справа выводится определение выбранного объекта (параметры и их значения).

В дереве объектов используются следующие управляющие элементы:

- – раскрыть соответствующий узел дерева объектов;

- ··· Добавить – открыть форму добавления объекта выбранного типа (элемент отображается после раскрытия узла).

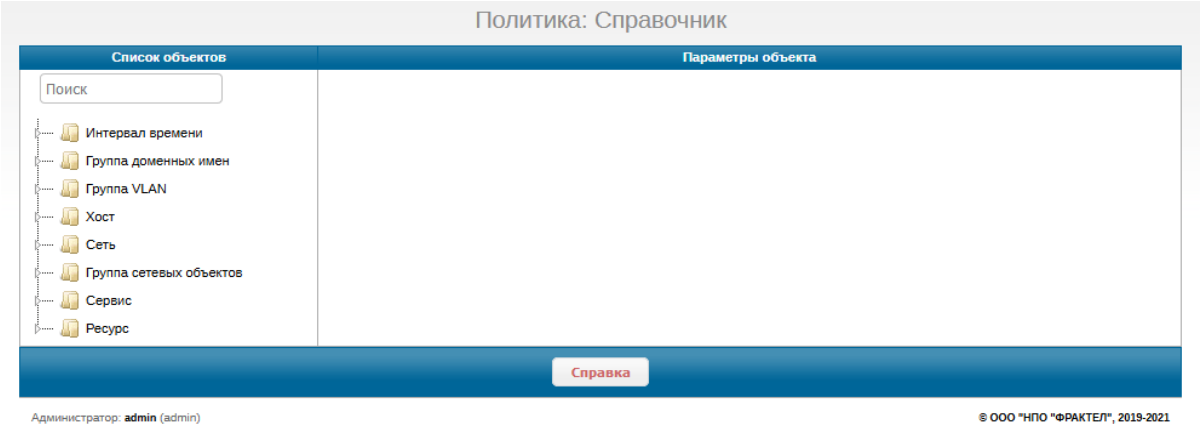


Рисунок 4.100: Страница Политика: Справочник

Если объекты выбранного типа были добавлены ранее, то они отображаются под элементом Добавить. По нажатию на имя объекта в правой части страницы выводится таблица с определением выбранного объекта (выводятся значения параметров объекта). Пример вывода определения объекта приведен на рисунке 4.101, стр. 295.

В правой части страницы (Параметры объекта) два управляющих элемента:

- Редактировать – открыть форму редактирования объекта;
- Удалить – удалить объект.

Далее приводится обзор форм добавления для объектов всех поддерживаемых типов. В формах добавления присутствует список выбора политики доступа, в которую следует добавить объект. По умолчанию объекты добавляются в текущую политику доступа.

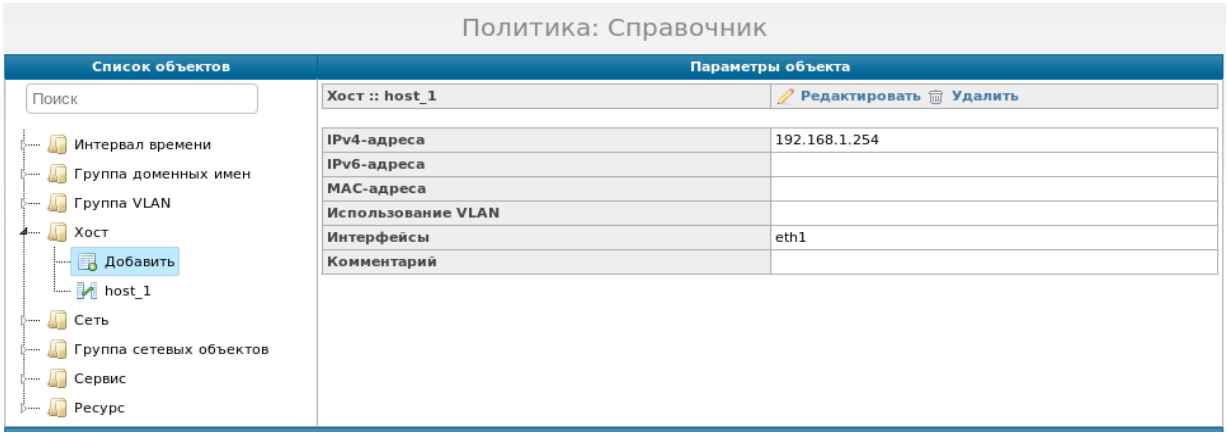


Рисунок 4.101: Пример вывода определения объекта справочника

Форма редактирования, как правило, полностью повторяет форму добавления для данного типа объектов, за тем исключением, что поля *Политика* и *Имя* заблокированы, так как редактирование объектов в дополнительных политиках и переименование объектов не поддерживаются.

Интервал времени. Форма добавления интервала времени приведена на рисунке 4.102, стр. 296.

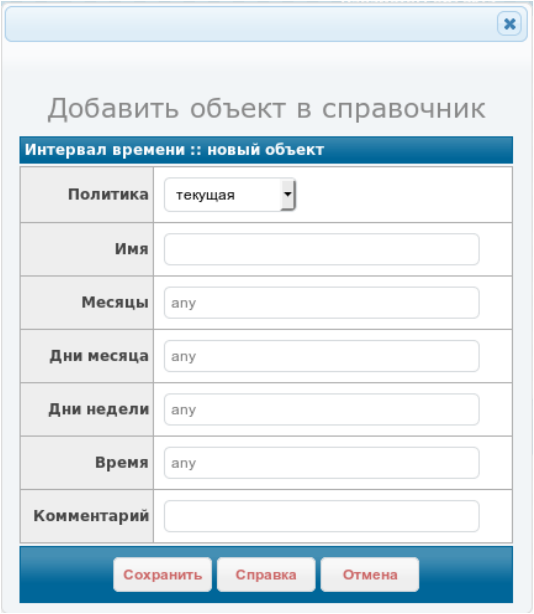


Рисунок 4.102: Форма добавления интервала времени

Описание параметров и форматы их значений для объекта "Интервал времени" приведены в приложении Е.6, стр. 544.

В определении объекта *“Интервал времени” (time)* по меньшей мере одно из следующих полей должно иметь значение отличное от **any**:

- Месяцы;
- Дни месяца;
- Дни недели;
- Время.

Группа доменных имен. Форма добавления группы доменных имен приведена на рисунке 4.103, стр. 296.

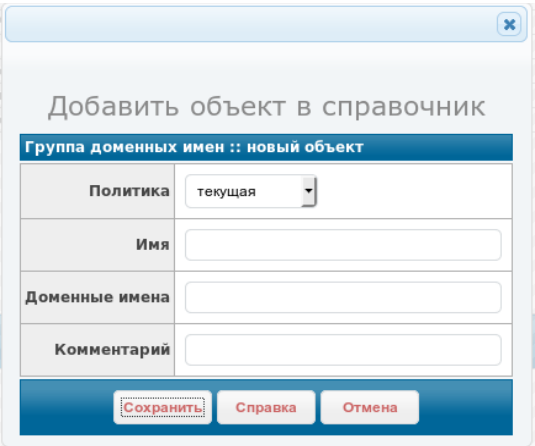


Рисунок 4.103: Форма добавления группы доменных имен

Описание параметров и форматы их значений для объекта "Группа доменных имен" приведены в приложении Е.7, стр. 545.

В определении объекта *“Группа доменных имён” (domain-group)* должен быть определено поле *Доменные имена*.

Группа VLAN. Форма добавления группы VLAN приведена на рисунке 4.104, стр. 297.

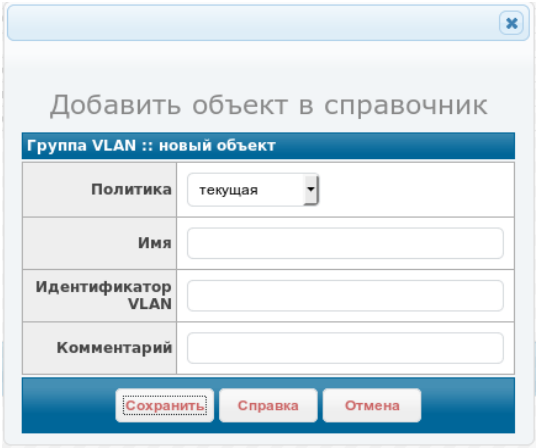


Рисунок 4.104: Форма добавления группы VLAN

Описание параметров и форматы их значений для объекта "Группа VLAN" приведены в приложении Е.8, стр. 546.

В определении объекта *“Группа VLAN” (vlan-group)* должно быть задано поле *Идентификатор VLAN*.

Хост. Форма добавления хоста (узла сети) приведена на рисунке 4.105, стр. 297.

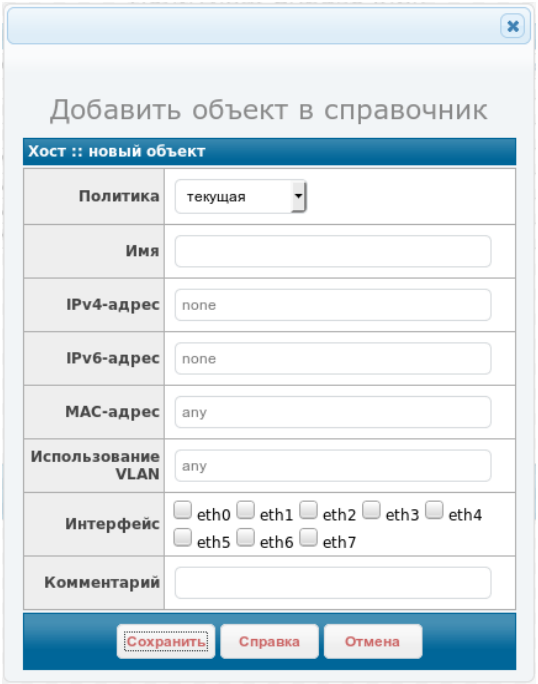


Рисунок 4.105: Форма добавления хоста (узла сети)

Описание параметров и форматы их значений для объекта "Хост" (узел сети) приведены в приложении Е.1, стр. 540.

В определении объекта **"*Узел сети" (host)*** по крайней мере одно из следующих полей должно быть определено, т.е иметь значение, отличное от значения по умолчанию:

- IPv4-адрес;
- IPv6-адрес;
- MAC-адрес.

Сеть. Форма добавления сети приведена на рисунке 4.106, стр. 298.

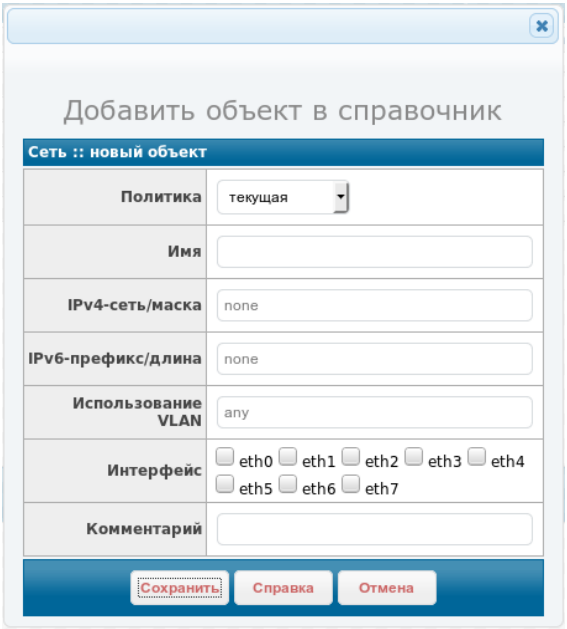


Рисунок 4.106: Форма добавления сети

Описание параметров и форматы их значений для объекта "Сеть" приведены в приложении Е.2, стр. 541.

В определении объекта *"Сеть" (net)* по крайней мере одно из следующих полей должно быть определено, т.е иметь значение, отличное от значения по умолчанию:

- IPv4-сеть/маска;
- IPv6-префикс/длина.

Группа сетевых объектов. Форма добавления группы сетевых объектов приведена на рисунке 4.107, стр. 299.

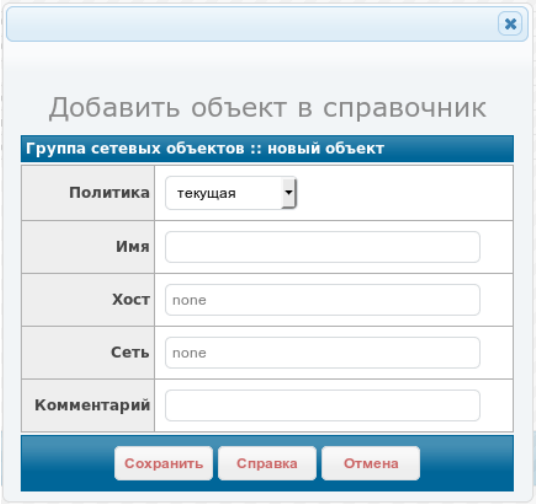


Рисунок 4.107: Форма добавления группы сетевых объектов

Описание параметров и форматы их значений для объекта "Группа сетевых объектов" приведены в приложении Е.3, стр. 542.

В определении объекта *"Группа сетевых объектов" (net-group)* по крайней мере одно из следующих полей должно быть определено, т.е иметь значение, отличное от значения по умолчанию:

- Хост;
- Сеть.

Сервис. Форма добавления сервиса приведена на рисунке 4.108, стр. 299.

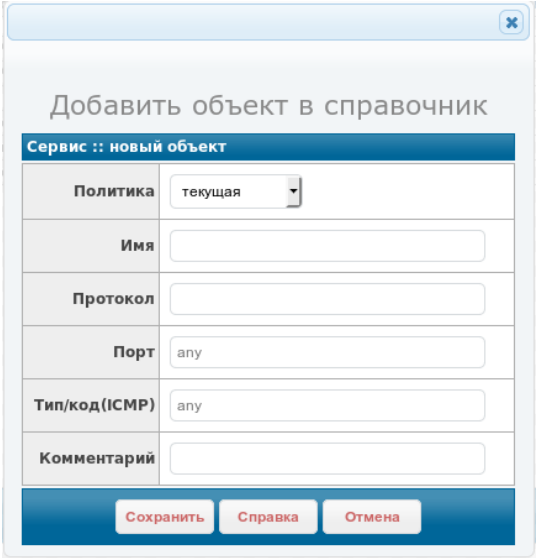


Рисунок 4.108: Форма добавления сервиса

Описание параметров и форматы их значений для объекта "Сервис" приведены в приложении Е.4, стр. 542.

Требования к определению объекта *"Сервис" (service)*:

- Должно быть определено поле *Протокол*;
- Поле *Порт* допустимо задавать только для протоколов *tcp* и *udp*;
- Поле *Тип/код (ICMP)* – только для протоколов *icmp* и *imcp6*.

Ресурс. Форма добавления ресурса приведена на рисунке 4.109, стр. 300.

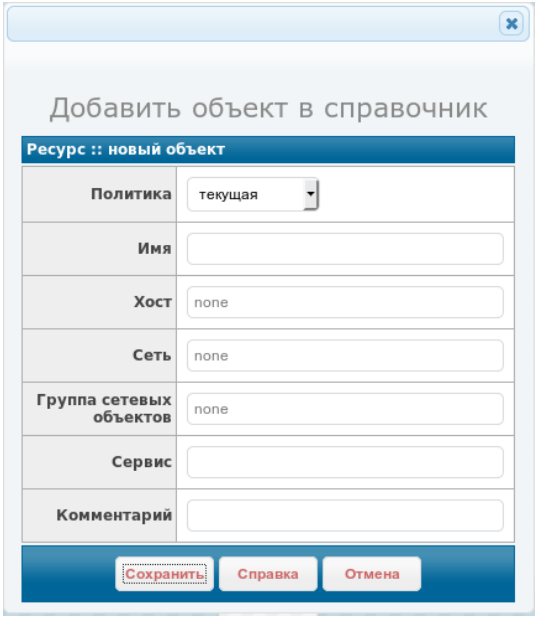


Рисунок 4.109: Форма добавления ресурса

Описание параметров и форматы их значений для объекта "Ресурс" приведены в приложении Е.5, стр. 543.

В определении объекта *“Ресурс” (resource)* должны быть определены следующие поля:

- по меньшей мере одно из полей: *Хост*, *Сеть* или *Группа сетевых объектов*;
- поле *Сервис*.

4.3.3. Политика: Правила

Страница “Политика: Правила” предназначена для просмотра и модификации правил текущей политики доступа и дополнительных политик доступа (для дополнительных политик: только добавление правил).

Страница “Политика: Правила” приведена на рисунке 4.110, стр. 300.

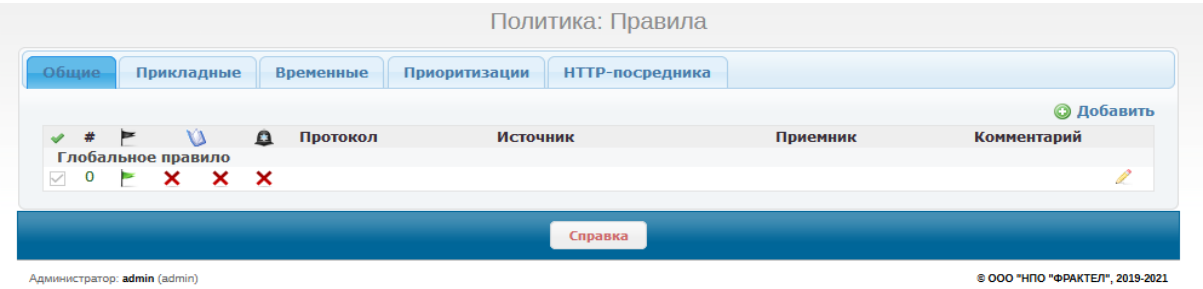


Рисунок 4.110: Страница Политика: Правила

Страница включает в себя вкладки:

- Общие – таблица общих правил;
- Прикладные – таблица прикладных правил (AP-правила);
- Временные – таблица временных правил (TMP-правила);
- Приоритизации – таблица правил приоритизации (PRI-правила);
- HTTP-посредника – таблица правил HTTP-посредника (PROXY-правила).

По умолчанию открыта вкладка “Общие”.

Общие. Во вкладке расположена таблица общих правил текущей политики доступа. Таблица состоит из следующих полей:

- – активность правила (активно/не активно);
- # – номер правила;
- – действие;
- – регистрация (пакеты и/или сессии либо выключено);
- – сигнализация: генерация сообщений сигнализации (включено/выключено):
- Протокол – список протоколов, инкапсулированных в IP-пакет;
- Источник – информация об IP-адресах и портах источника;
- Приемник – информация об IP-адресах и портах приемника;
- Комментарий – строка комментария к правилу.

Пример таблицы правил, в которой помимо глобального правила, присутствуют регулярные правила, приведен на рисунке 4.111, стр. 301.

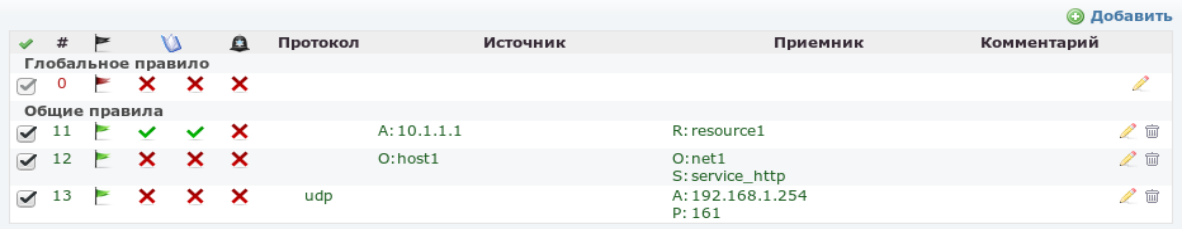


Рисунок 4.111: Пример таблицы общих правил

Из примера видно, что в полях Источник и Приемник может выводиться информация различного типа. Данные поля используют следующий формат вывода информации:

- A:<IP-адрес>, где <IP-адрес> – IP-адрес, заданный непосредственно в правиле;
- P:<порт>, где <порт> – TCP и/или UDP порт, заданный непосредственно в правиле;
- O:<имя_объекта>, где <имя_объекта> – имя сетевого объекта типа хост, сеть или группа сетевых объектов, посредством которого заданы IP-адреса и другие атрибуты пакета);

- `S:<имя_сервиса>`, где <имя_сервиса> – имя объекта типа сервис, посредством которого заданы: протокол инкапсулированный в IP, TCP или UDP-порты либо типы и коды ICMP;
- `R:<имя_ресурса>`, где где <имя_ресурса> – имя объекта типа ресурс, посредством которого заданы различные атрибуты пакета (IP-адреса, порты и т. д.).

Каждый из приведенных типов может содержать список элементов. В этом случае каждый элемент выводится в отдельной строке в один столбец.

Записи таблицы общих правил отличаются цветом текста, в зависимости от действия правила фильтрации:
- зеленый – действие *пропустить* (**accept**);
- желтый – действие *отклонить* (**deny**);
- красный – действие *удалить* (**drop**);
- синий – действие *перейти к правилу* (**goto**).

В таблице общих правил используются следующие управляющие иконки:

- – редактировать правило;
- – удалить правило.

Если в таблице общих правил курсор мыши навести на регулярное правило и при этом нажать правую кнопку мыши, до будет отображено контекстное меню действий над данным правилом. Пример вывода контекстного меню приведен на рисунке 4.112, стр. 302.

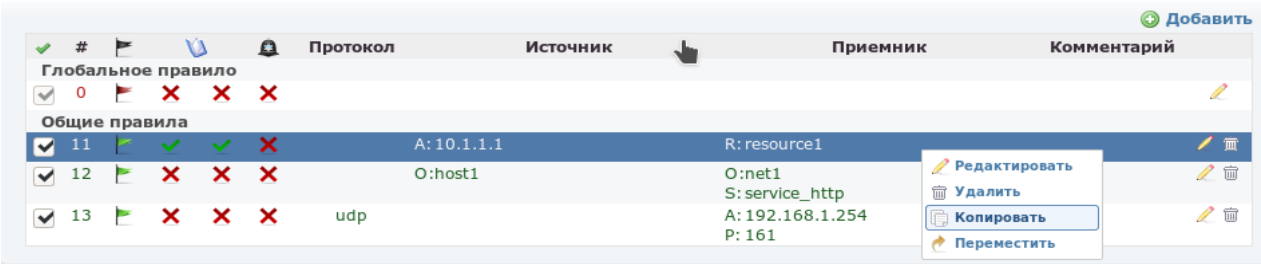


Рисунок 4.112: Контекстное меню действий над регулярным общим правилом

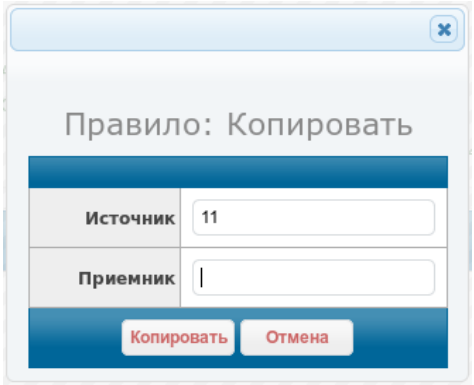


Рисунок 4.113: Форма копирования правила

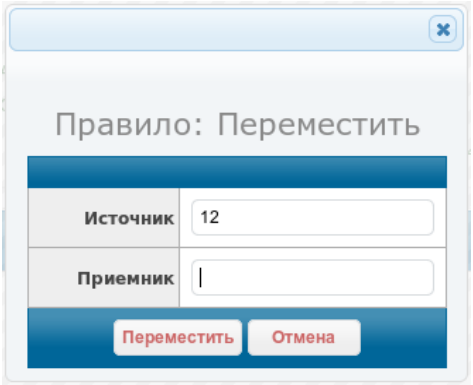


Рисунок 4.114: Форма перемещения правила

В контекстном меню доступны следующие действия над правилом:

- `Редактировать` – вывод формы редактирования данного правила;
- `Удалить` – удаление данного правила (перед удалением запрашивается подтверждение);
- `Копировать` – создание копии данного правила (в поле `Приемник` формы копирования правила, приведенной на рисунке 4.113, стр. 302, необходимо ввести номер правила-копии);
- `Переместить` – перемещение данного правила в пределах таблицы общих правил (эквивалентно смене номера правила, в поле `Приемник` формы перемещения правила, приведенной на рисунке 4.114, стр. 302, необходимо ввести новый номер для данного правила).

Функции копирования и перемещения правил аналогичным образом доступны для следующих типов правил:
- прикладные правила (AP-правила);
- правила приоритизации (PRI-правила);
- правила HTTP-посредника (PROXY-правила).

Если при копировании или перемещении правила в поле *Приемник* ввести номер существующего правила, то оно будет перезаписано.

По нажатию на кнопку **`Добавить`** открывается форма добавления общего правила. Форма приведена на рисунке 4.115, стр. 304. По умолчанию при открытии формы добавления общего правила выводятся `Основные настройки` – основные параметры общего правила. На рисунке 4.115. стр. 304 видны не все элементы формы, т. к. присутствует полоса прокрутки.

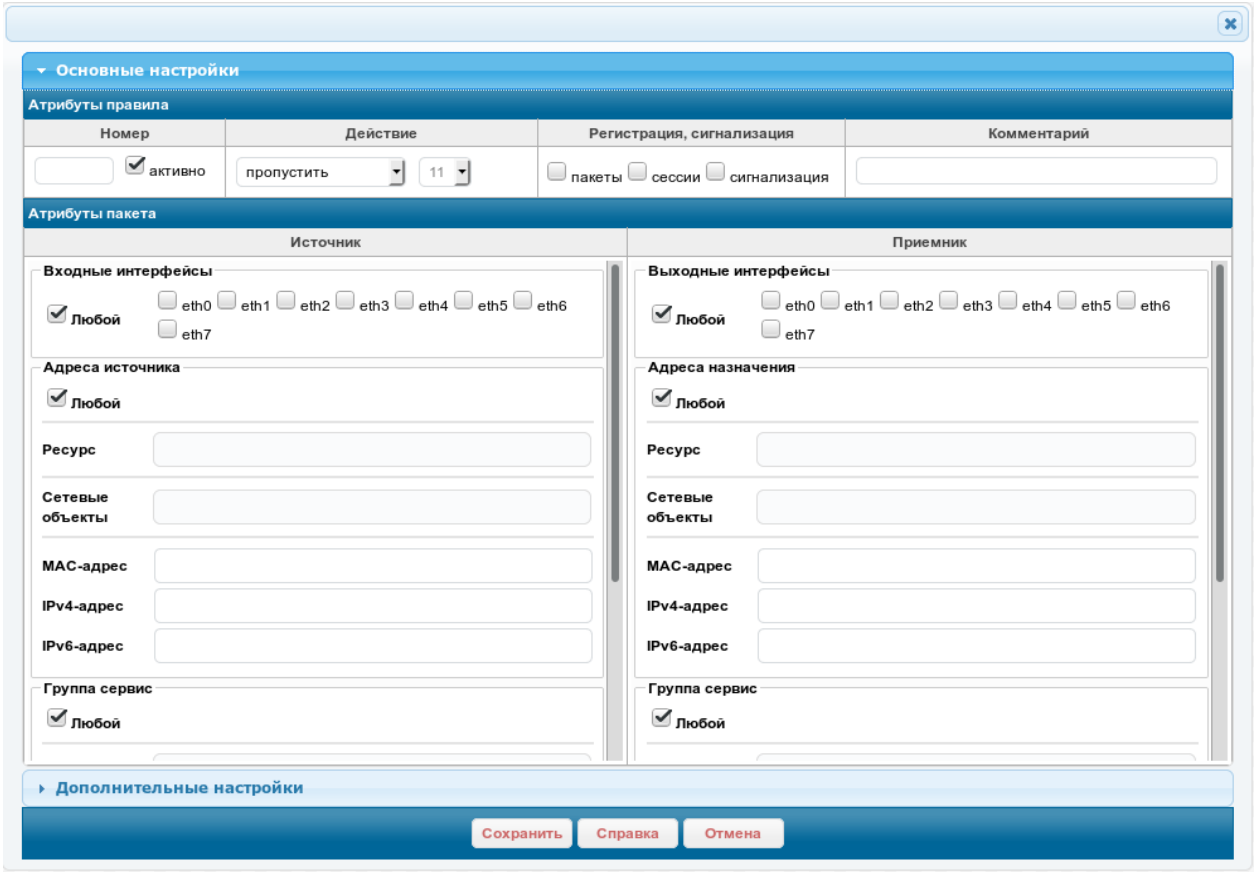


Рисунок 4.115: Форма добавления общего правила: основные настройки

Форма “Основные настройки” состоят из двух секций:

- Атрибуты правила – содержат элементы ввода данных для настройки атрибутов правила, не относящихся к полям пакета;
- Атрибуты пакета – содержат элементы ввода данных для настройки параметров пакета, которым должно соответствовать данное правило;

Атрибуты правила:

- Номер – номер правила;
- активно – флаг активности правила. Значения:
  - ✔ **включено** – правило активно;
  - ✔ **выключено** – правило неактивно;
- Действие – действие правила над пакетом. Допустимые значения:
  - ✔ **пропустить** – передача пакета на фильтрацию прикладного уровня (по АР-правилам фильтрации) либо на выходные интерфейсы (при отсутствии АР-правил);
  - ✔ **удалить** – удаление пакета;
  - ✔ **перейти к правилу** – безусловный переход к правилу с указанным номером в списке общих правил фильтрации;

✔ **отклонить** – удаление пакета с отправкой пакета-уведомления (TCP-сообщения с флагом RST для TCP и ICMP-сообщения для остальных протоколов).

- Регистрация, сигнализация – использование функций регистрации трафика и генерации сообщений сигнализации при срабатывании правила. По умолчанию регистрация и сигнализация выключены в правиле. Допустима комбинация из следующих значений:
  ✔ **пакеты** – регистрировать пакеты;
  ✔ **сессии** – регистрировать сессии;
  ✔ **сигнализация** – генерировать сообщения сигнализации;
- Комментарий – строка комментария к правилу.

Секция Атрибуты пакета разделена вертикально на две равные части:

- Источник – параметры источника пакета;
- Приемник – параметры приемника пакета;

Часть параметров является общей для источника и приемника, поэтому продублирована в обеих частях (Протокол, IMCPv4, ICMPv6).

Итак, Атрибуты пакета включают в себя:

- Источник:
  ✔ Входные интерфейсы – список входных интерфейсов;
  ✔ Адреса источника:
    ◆ Ресурс – список объектов типа ресурс;
    ◆ Сетевые объекты – список сетевых объектов (объекты типов: хост, сеть, группа сетевых объектов;
    ◆ MAC-адрес – список MAC-адресов;
    ◆ IPv4-адрес – список IPv4-адресов;
    ◆ IPv6-адрес – список IPv6-адресов;
  ✔ Группа Сервис:
    ◆ Сервис – список объектов типа сервис;
    ◆ Порт – список портов;
    ◆ Протокол – список протоколов, инкапсулированных в IP-пакет;
    ◆ ICMPv4 – тип и код протокола ICMP;
    ◆ ICMPv6 – тип и код протокола ICMPv6;
- Приемник:
  ✔ Выходные интерфейсы – список выходных интерфейсов;
  ✔ Адреса назначения:
    ◆ Ресурс – список объектов типа ресурс;

- Сетевые объекты – список сетевых объектов (объекты типов: хост, сеть, группа сетевых объектов;
- MAC-адрес – список MAC-адресов;
- IPv4-адрес – список IPv4-адресов;
- IPv6-адрес – список IPv6-адресов;

✔ Группа Сервис:

- Сервис – список объектов типа сервис;
- Порт – список портов;
- Протокол – список протоколов, инкапсулированных в IP-пакет;
- ICMPv4 – тип и код протокола ICMP;
- ICMPv6 – тип и код протокола ICMPv6.

Определение общего правила фильтрации (полный перечень параметров и форматы их значений) приведены в приложении Д.1, стр. 514.

Поля ввода основных настроек общего правила имеют правила взаимных блокировок для исключения *конфликтов параметров правила*. Описание возможных конфликтов параметров общего правила приведено в приложении Д.1.1, стр. 521.

При вводе имен объектов справочника в соответствующих полях формы добавления правила используется функция автодополнения. Предлагаемое автодополнением имя объекта необходимо выбрать, нажав по нему мышкой, тогда оно будет добавлено в соответствующее поле в виде блока с символом “**x**” справа от имени. При нажатии на данный символ объект будет удален из поле ввода.

Если же вводить произвольные имена объектов, не используя функцию автодополенения, то введеные имена будут проигнорированы при нажатии на кнопку “**Сохранить**” и указанные таким образом объекты не будут использоваться в правиле фильтрации.

При нажатии на заголовок Дополнительные настройки в форме добавления правила выводятся элементы ввода дополнительных параметров правила. Форма для задания дополнительных настроек правила приведена на рисунке 4.116, стр. 307.

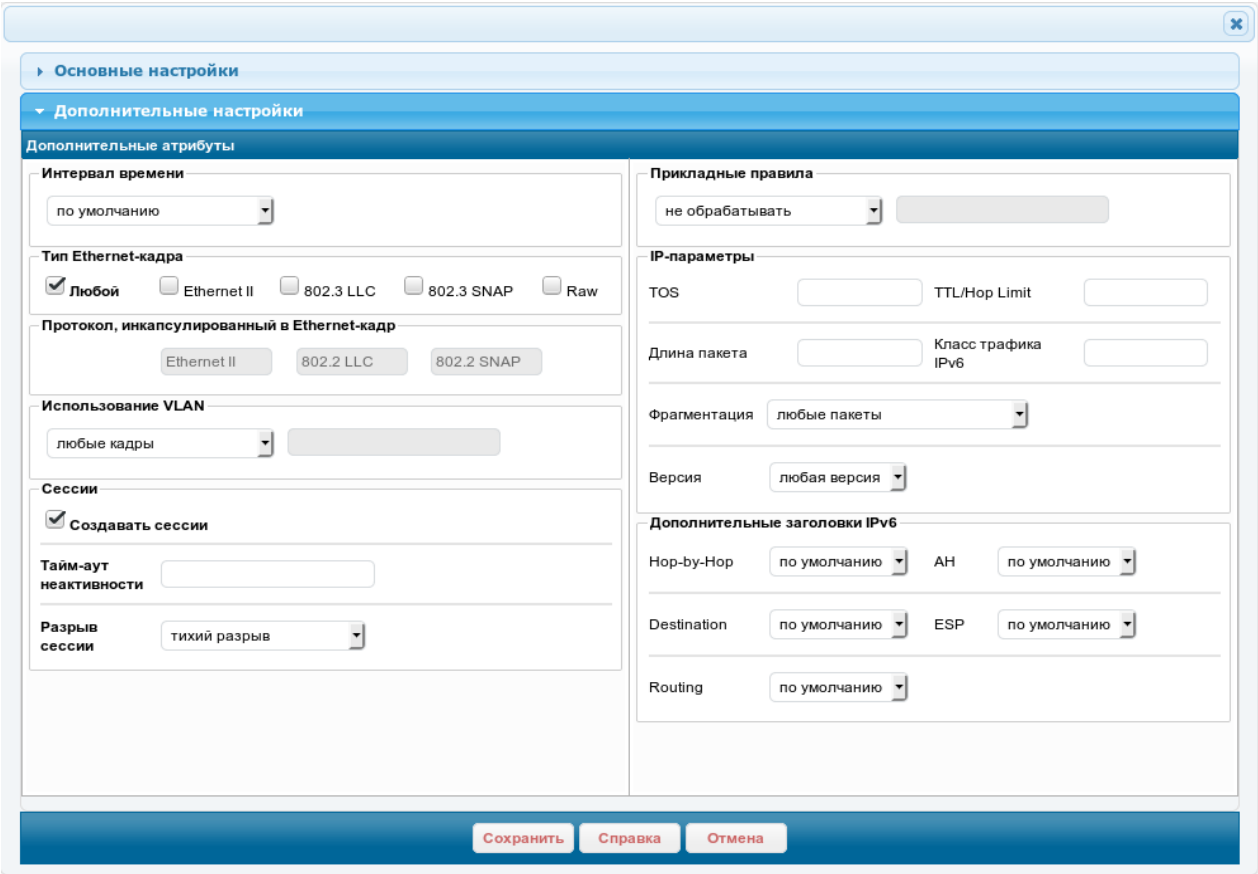


Рисунок 4.116: Форма добавления общего правила: дополнительные настройки

Форма “Дополнительные настройки” содержит следующие элементы ввода дополнительных атрибутов общего правила:

- Интервал времени – выбор объекта типа интервал времени. Выполняет привязку общего правила к интервалу времени: правило активно только в указанный интервал времени;
- Тип Ethernet-кадра – выбор типов Ethernet-кадров, в которые может быть инкапсулирован IP-пакет. Допускается комбинация следующих значений: **Ethernet II**, **802.3 LLC**, **802.3 SNAP**, **Raw**;
- Протокол, инкапсулированный в Ethernet-кадр – ввод списка кодов протоколов, инкапсулирвоанных в Ethernet-кадр. Ввод в соответствующее поле допустим только тогда, когда выбран один конкретный тип Ethernet-кадра;
- Использование VLAN – параметр использования тэга VLAN в Ethernet-кадре. Допустимые значения:
  - ✔ **любые кадры** – любой Ethernet -кадр (с тегом IEEE 802.1q или без него);
  - ✔ **только кадры с VLAN** – только Ethernet- кадры с тегом IEEE 802.1q;
  - ✔ **только кадры без VLAN** – только Ethernet- кадры без тега IEEE 802.1q;
  - ✔ **задать значения VLAN ID** – список идентификаторов и/или диапозонов идентификаторов VLAN. Правилу будут сопоставлены Ethernet-кадры, содержащие идентификатор VLAN из

списка;

- ✔ **имя группы VLAN** – имя группы VLAN из справочника. Правило будет действовать только для Ethernet-кадров, содержащих указанные в группе идентификаторы VLAN;

- Сессии – параметры создания сессии по данному правил:
  - ✔ Создавать сессии – создание сессии на основе пакетов, обработанных данным правилом:
    - **включено** – создавать сессии по пакетам, обработанным данным правилом;
    - **выключено** – не создавать сессии по пакетам, обработанным данным правилом;
  - ✔ Тайм-аут неактивности: – тайм-аут неактивности для сессий, созданных по данному правилу;
  - ✔ Разрыв сессии – корректность обработки TCP-сессии при сбросе инициирующего SYN-пакета, а так же при разрыве установившейся TCP-сессии:
    - **тихий разрыв** – сессия разрывается без уведомления взаимодействующих сторон;
    - **отправить флаг RESET** – сессия разрывается с уведомлением взаимодействующих сторон TCP-пакетами с установленным флагом RESET;
- Прикладные правила – список номеров прикладных правил, привязанных к данному общему правилу. Допустимые значения:
  - ✔ **не обрабатывать** – пакеты не будут обрабатываться на прикладном уровне;
  - ✔ **обрабатывать** – пакеты будут обрабатываться на прикладном уровне;
  - ✔ **обрабатывать по списку** – список номеров и/или диапазонов номеров прикладных правил;
- IP-параметры – параметры заголовка IP-пакета (помимо IP-адресов):
  - ✔ Значение TOS – значение битов TOS заголовка IPv4
  - ✔ Значение TTL – значение поля TTL заголовка IPv4 или заголовка HopLimit IPv6
  - ✔ Длина пакета – суммарная длина IP-пакета, включая IP-заголовок;
  - ✔ Класс трафика – значение битов поля "Traffic class" заголовка IPv6-пакета
  - ✔ Фрагментация – использование фрагментации в пакете. Допустимые значения:
    - **любые пакеты** – правило применяется применяется как к фрагментированным, так и к нефрагментированным пакетам
    - **только фрагментированные** – правило применяется только к фрагментированным пакетам
    - **только нефрагментированные** – правило применяется только к нефрагментированным пакетам;
  - ✔ Версия IP – версия протокола IP. Допустимые значения:
    - **IPv4** – протокол IP версии 4;
    - **IPv6** – протокол IP версии 6;

- `Дополнительные заголовки IPv6` – параметры использования в IPv6-пакете конкретных дополнительных заголовков: `Hop-by-Hop`, `AH`, `Destination`, `ESP`, `Routing`. Допустимые значения (для каждого из заголовков):
  - ✔ **`по умолчанию`** – для правила не важно наличие данного дополнительного заголовка;
  - ✔ **`присутствует`** – данный дополнительный заголовок должен присутствовать в пакете, чтобы правило сработало;
  - ✔ **`отсутствует`** – данный дополнительный заголовок должен отсутствовать в пакете, чтобы правило сработало.

> Форма редактирования общего правила по своей структуре полностью идентична форме добавления, поэтому отдельно не рассматривается. Форма, помимо прочего, позволяет изменить номер правила (аналогично команде *rule move*).

Прикладные. Во вкладке расположена таблица прикладных правил (АР-правил) текущей политики доступа. Пример таблицы прикладных правил приведен на рисунке 4.117, стр. 309.

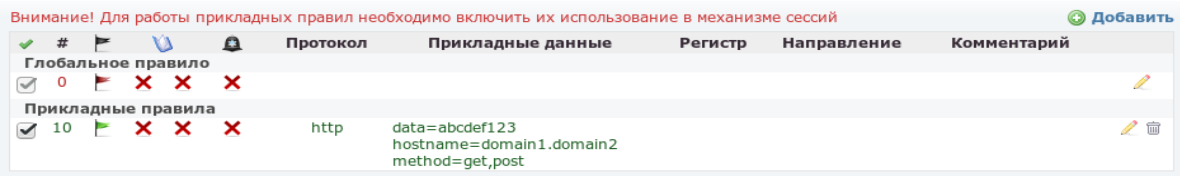


Рисунок 4.117: Пример таблицы прикладных правил

В приведенном примере, помимо глобального правила, присутствует регулярное правило. В текущей политике доступа по умолчанию присутствует только глобальное АР-правило с действием **`удалить`**.

Таблица прикладных правил состоит из следующих полей:

- – активность правила (активно/не активно);
- # – номер правила;
- – действие;
- – регистрация (пакеты и/или сессии либо выключено);
- – сигнализация: генерация сообщений сигнализации (включено/выключено):
- `Протокол` – прикладной протокол;
- `Прикладные данные` – параметры фильтрации по прикладным данным.
- `Регистр` – регистр искомых ASCII-символов в прикладных данных;

- Направление – направление поиска прикладных данных (от клиента, от сервера либо оба направления);
- Комментарий – строка комментария к правилу.

В поле “Прикладные данные” информация выводится в следующем формате:

<параметр_АР-правила>=<значение>, где <параметр_АР-правила> – один из параметров поиска прикладных данных, применимых для выбранного прикладного протокола. Перечень допустимых прикладных протоколов и соответствующих им параметров поиска приведен в приложении Д.2, стр. 527.

Записи таблицы прикладных правил отличаются цветом текста, в зависимости от действия правила фильтрации:
- зеленый – действие *пропустить* (**accept**);
- красный – действие *удалить* (**drop**).

В таблице прикладных правил используются следующие управляющие иконки:

- – редактировать правило;
- – удалить правило.

По нажатию на кнопку Добавить открывается форма добавления прикладного правила. Исходный вид формы приведен на рисунке 4.118, стр. 311. В исходном виде формы не выводятся поля поиска прикладных данных, состав которых зависит от выбранного прикладного протокола.

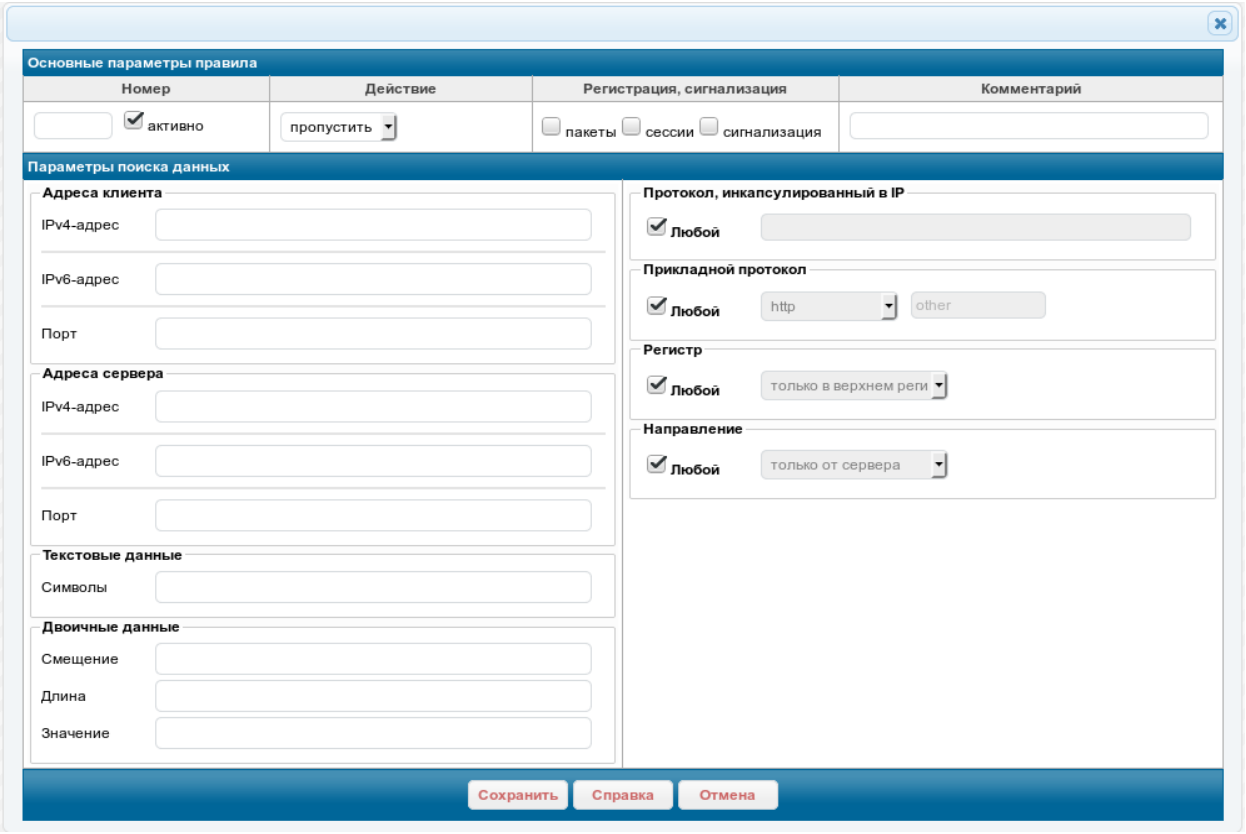


Рисунок 4.118: Форма добавления прикладного правила

Дополнительные элементы ввода, предназначенные для поиска прикладных данных конкретных протоколов, приведены на отдельных рисунках (данные элементы отображаются в форме добавления АР-правила при выборе соответствующего прикладного протокола в списке Прикладной протокол):

- **http** – рисунок 4.119, стр. 311;
- **ftp** – рисунок 4.120, стр. 311;
- **smtp** – рисунок 4.121, стр. 312;
- **sql** – рисунок 4.122, стр. 312;
- **dns** – рисунок 4.123, стр. 312.

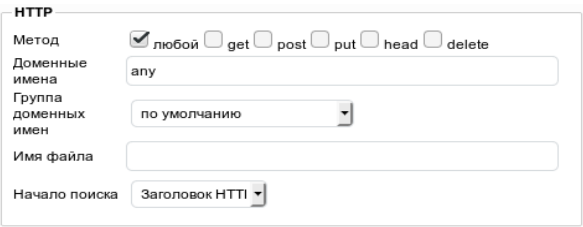


Рисунок 4.119: Дополнительные элементы протокола HTTP

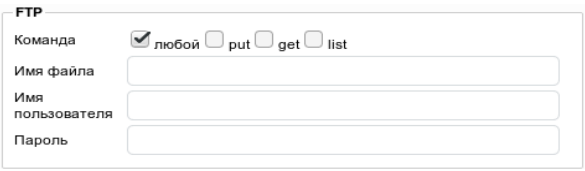


Рисунок 4.120: Дополнительные элементы протокола FTP

Рисунок 4.121: Дополнительные элементы протокола SMTP

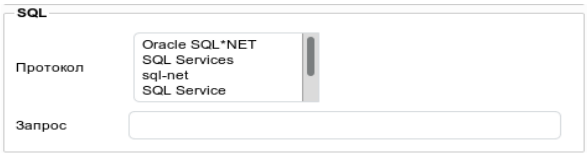


Рисунок 4.122: Дополнительные элементы SQL-сервисов

Рисунок 4.123: Дополнительные элементы протокола DNS

Форма добавления прикладного правила содержит следующие элементы ввода данных:

- `Номер`: номер прикладного правила;
- `активно` – флаг активности правила. Значения:
  - ✔ **включено** – правило активно;
  - ✔ **выключено** – правило неактивно;
- Действие – действие правила. Допустимые значения:
  - ✔ **пропустить** – передача пакета на выходной фильтрующий интерфейс;
  - ✔ **удалить** – удаление пакета;
- `Регистрация, сигнализация` – использование функций регистрации трафика и генерации сообщений сигнализации при срабатывании правила. По умолчанию регистрация и сигнализация выключены в правиле. Допустима комбинация из следующих значений:
  - ✔ **пакеты** – регистрировать пакеты;
  - ✔ **сессии** – регистрировать сессии;
  - ✔ **сигнализация** – генерировать сообщения сигнализации;
- `Комментарий` – строка комментария к правилу;
- `Адреса клиента`:
  - ✔ `IPv4-адрес` – список IPv4-адресов на стороне клиента;
  - ✔ `IPv6-адрес` – список IPv6-адресов на стороне клиента;
  - ✔ `Порт` – список TCP или UDP-портов клиента;
- `Адреса сервера`:
  - ✔ `IPv4-адрес` – список IPv4-адресов на стороне сервера;
  - ✔ `IPv6-адрес` – список IPv6-адресов на стороне сервера;
  - ✔ `Порт` – список TCP или UDP-портов сервера;
- `Текстовые данные: Символы` – последовательность печатных ASCII-символов;
- `Двоичные данные` – последовательность двоичных данных по указанному смещению:

- ✔ Смещение – смещение относительно начала прикладных данных в байтах к искомой последовательности;
- ✔ Длина – длина последовательности в байтах;
- ✔ Значение – значение двоичной последовательности в шестнадцатеричном виде;

- Протокол: протокол, инкапсулированный в IP – список номеров и/или имен протоколов;
- Прикладной протокол – протокол прикладного уровня. Допустимые значения: **http**, **ftp**, **smtp**, **sql**, **dns** либо код прикладного протокола;
- Регистр – регистр ASCII-символов в строках поиска (поле Текстовые данные: Символы и поля, состав которых зависит от значения поля Проткол: приведены далее). Допустимые значения:
  - ✔ **любой** – регистр не учитывается;
  - ✔ **только в верхнем регистре** – только символы в верхнем регистре;
  - ✔ **только в нижнем регистре** – только символы в нижнем регистре;
  - ✔ **регистр учитывается** – будет произведен поиск строки в том регистре, в котором строка указана в правиле;
- Направление – направление потока, в котором производится поиск. Допустимые значения:
  - ✔ **любое** – правило применяется к обоим потокам (от сервера к клиенту и от клиента к серверу);
  - ✔ **только от сервера** – правило применяется только к потоку от сервера к клиенту;
  - ✔ **только от клиента** – правило применяется только к потоку от клиента к серверу;
- HTTP – параметры протокола HTTP (значение **http** параметра Прикладной протокол):
  - ✔ Метод – идентификаторы метода запроса к HTTP-серверу. Допустима комбинация конкретных методов либо вариант – любой метод:
    - ◆ **любой** – любой метод запроса;
    - ◆ **get** – метод GET;
    - ◆ **put** – метод PUT;
    - ◆ **post** – метод POST;
    - ◆ **head** – метод HEAD;
    - ◆ **delete** – метод DELETE;
  - ✔ Доменные имена – список имен или фрагментов доменных имен HTTP-серверов;
  - ✔ Группа доменных имен – имя группы доменных имен из справочника объектов текущей политики;
  - ✔ Имя файла – список имен файлов (или их фрагментов), запрашиваемых у HTTP-сервера;
  - ✔ Начало поиска – указывает точку отсчета смещения для поиска параметра Двоичные данные. Допустимые значения:

- **Заголовок HTTP-сообщения** – поиск будет производиться от начала HTTP-заголовка (значение по умолчанию);
- **Тело HTTP-сообщения** – поиск будет производиться от начала тела HTTP-сообщения (заголовок не учитывается);

- FTP – параметры протокола FTP (значение **ftp** параметра Прикладной протокол):
  - ✔ Команда – команда клиента протокола FTP. Допустима комбинация конкретных команд, либо вариант **любая команда**:
    - **любая** – любая команда;
    - **put** – команда пересылки файла на FTP-сервер;
    - **get** – команда пересылки файла с FTP-сервера;
    - **list** – команда вывода содержимого каталога FTP-сервера;
  - ✔ Имя файла – список имен (или их фрагментов) файлов, передаваемых между FTP-клиентом и FTP-сервером;
  - ✔ Имя пользователя – список имен пользователей, предъявляемых при доступе к FTP-серверу;
  - ✔ Пароль – список паролей пользователей, предъявляемых при доступе к FTP-серверу;
- SMTP – параметры протокола SMTP (значение **smtp** параметра Прикладной протокол):
  - ✔ Отправитель – список почтовых адресов отправителей;
  - ✔ Получатель – список почтовых адресов получателей;
- SQL – параметры SQL-сервисов (значение **sql** параметра Прикладной протокол):
  - ✔ Протокол – список множественного выбора предназначен для выбора конкретных SQL-сервисов, пакеты которых должны обрабатываться по данному правилу. Допустима любая комбинация из следующих значений:
    - **Oracle SQL*NET** – порт 66;
    - **SQL Services** – порт 118;
    - **sql-net** – порт 150;
    - **SQL Service** – порт 156;
    - **Microsoft-SQL-Server** – порт 1433;
    - **Microsoft-SQL-Monitor** – порт 1434;
    - **watcom-sql** – порт 1498;
    - **mysql** – порт 3306;
    - **postgresql** – порт 5432.
  - ✔ Запрос – список SQL-запросов (или их фрагментов);
- DNS – параметры протокола DNS (значение **dns** параметра Прикладной протокол):
  - ✔ Доменые имена – список доменных имен (или их фрагментов);

✔ Группа доменных имен – имя группы доменных имен из справочника текущей политики доступа.

Определение прикладного правила фильтрации (полный перечень параметров и форматы их значений) приведены в приложении Д.2, стр. 527.

Если при добавлении АР-правила для SQL-сервисов (поле *Прикладной протокол* – в значении *sql*) в списке множественного выбора *Протокол* секции *SQL* не выбран ни один из SQL-сервисов, то на соответствие данному АР-правилу будут проверяться пакеты всех SQL-сервисов из следующего списка:

- Oracle SQL*NET (порт 66);
- SQL Services (порт 118);
- SQL Net (порт 150);
- SQL Service (порт 156);
- Microsoft-SQL-Server (порт 1433);
- Microsoft-SQL-Monitor (порт 1434);
- Watcom SQL (порт 1498);
- MySQL (порт 3306).
- PostgreSQL Database (порт 5432).

Для фильтрации пакетов конкретных SQL-сервисов в АР-правиле необходимо выбрать требуемые SQL-сервисы в списке множественного выбора *Протокол* секции *SQL*, при этом номера портов выбранных SQL-сервисов будут автоматически добавлены в поле ввода *Порт сервера* формы добавления АР-правила**.** Для выбора нескольких значений в списке *Протокол* следует удерживать клавишу <*Ctrl*> до окончания выбора.

Форма редактирования прикладного правила по своей структуре максимально близка форме добавления, поэтому отдельно не рассматривается. Форма, помимо прочего, позволяет изменить номер правила (аналогично команде *rule move*).

Изменение параметра *Прикладной протокол* не поддерживается.

Временные. Во вкладке расположена таблица временных правил (ТМР-правил). Пример таблицы временных правил приведен на рисунке 4.124, стр. 315.

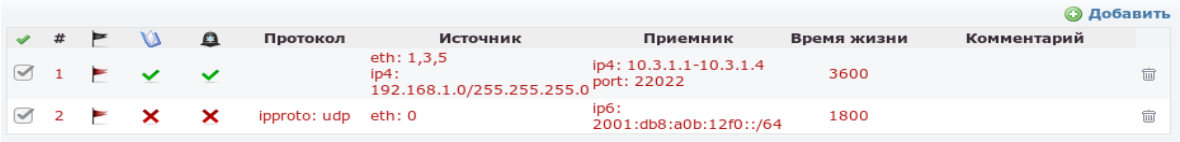


Рисунок 4.124: Пример таблицы прикладных временных правил

Изначально на МЭ ССПТ-4А1 отсутствуют временные правила. Временные правила могут быть добавлены администратором или автоматически пакетным фильтром при использовании функции обнаружения flood-атак.

Таблица временных правил состоит из следующих полей:

- – активность правила (активно в течение времени жизни);
- # – номер правила;
- – действие (единственное действие: удалить);

- – регистрация пакетов, удаленных правилом (включено/выключено);
- – сигнализация: генерация сообщений сигнализации (включено/выключено):
- `Протокол` – список протоколов, инкапсулированных в IP;
- `Источник` – адресная информация источника;
- `Приемник` – адресная информация приемника;
- `Время жизни` – интервал времени в секундах, в течении которого правило существует;
- `Комментарий` – строка комментария к правилу.

В поле `Источник` может быть выведена следующая информация:

- список входных интерфейсов в формате `eth:<список_интерфейсов>` (например, **`eth:1,3,5`**);
- список IPv4-адресов в формате `ip4:<список_IPv4>` (например, **`ip4:192.168.1.0/24`**);
- список IPv6-адресов в формате `ip6:<список_IPv6>` (например, **`ip6:2001:db8:a0b:12f0::/64`**);
- список TCP или UDP-портов в формате `port:<список_портов>` (например, **`port:32768`**).

В поле `Приемник` может быть выведена следующая информация:

- список IPv4-адресов в формате `ip4:<список_IPv4>` (например, **`ip4:10.3.1.1-10.3.1.4`**);
- список IPv6-адресов в формате `ip6:<список_IPv6>` (например, **`ip6:2001:db8:a0b:12f0::/64`**);
- список TCP или UDP-портов в формате `port:<список_портов>` (например, **`port:22022`**).

В таблице временных правил используется управляющая иконка – удалить правило.

По нажатию на кнопку `Добавить` открывается форма добавления временного правила. Форма приведена на рисунке 4.125, стр. 317.

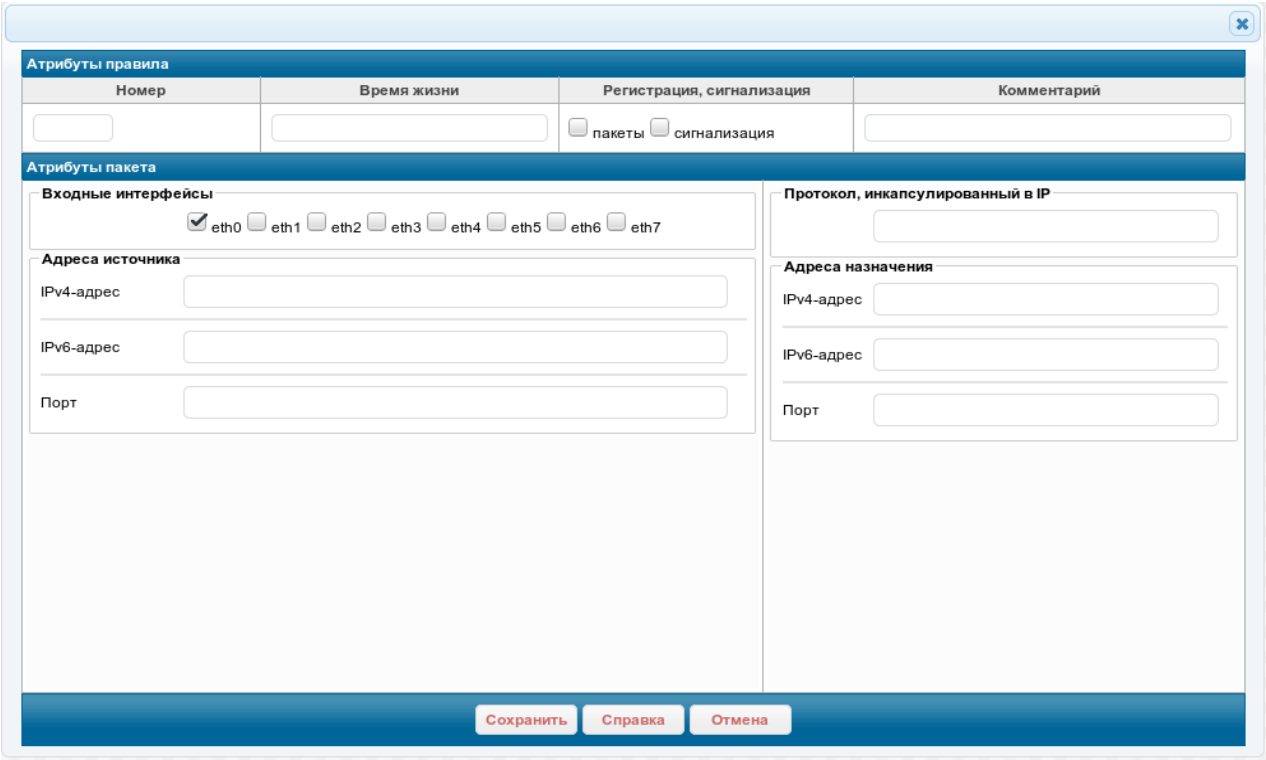


Рисунок 4.125: Форма добавления временного правила

Форма добавления временного правила содержит следующие элементы ввода данных:

- `Номер` – номер временного правила;
- `Время жизни` – интервал времени в секундах, по истечению которого правило будет автоматически удалено;
- `Регистрация, сигнализация` – использование функций регистрации пакетов и генерации сообщений сигнализации при срабатывании правила. По умолчанию регистрация и сигнализация выключены в правиле. Допустима комбинация из следующих значений:
  - ✔ **пакеты** – регистрировать пакеты, удаленные правилом;
  - ✔ **сигнализация** – генерировать сообщения сигнализации;
- `Комментарий` – строка комментария к правилу;
- `Входные интерфейсы` – список входных интерфейсов;
- `Протокол - протокол, инкапсулированный в IP`: список номеров и/или имен протоколов;
- `Адреса источника`:
  - ✔ `IPv4-адрес` – список IPv4-адресов источника;
  - ✔ `IPv6-адрес` – список IPv6-адресов источника;
  - ✔ `Порт` – список TCP или UDP-портов источника;
- `Адреса назначения`:

✔ `IPv4-адрес` – список IPv4-адресов назначения;

✔ `IPv6-адрес` – список IPv6-адресов назначения;

✔ `Порт` – список TCP или UDP-портов назначения.

Определение временного правила фильтрации (полный перечень параметров и форматы их значений) приведено в приложении Д.3, стр. 534.

В отличие от *общего правила* и *АР-правила* в *ТМР-правиле* не допускается одновременное использование IPv4-адресов и IPv6-адресов.
Т.е. в *ТМР-правиле* не допускается, чтобы параметры IPv4-адрес источника (IPv4-адрес назначения) и IPv6-адрес источника (IPv6-адрес назначения) одновременно были заданы администратором.

Редактирование *ТМР-правила* не поддерживается.

Приоритизации. Во вкладке расположена таблица *правил приоритизации* (PRI-правил), которые служат для приоритетной обработки трафика (в соответствии с заданными в правилах уровнями приоритета).

По умолчанию функция приоритетной обработки трафика выключена и правила приоритизации отсутствуют в политике доступа по умолчанию. Пример исходного вида вкладки правил приоритизации приведен на рисунке 4.126, стр. 318. Пример вкладки правил приоритизации, когда функция приоритетной обработки трафика включена и в политике доступа присутствуют правила приоритизации приведен на рисунке 4.127, стр. 318.

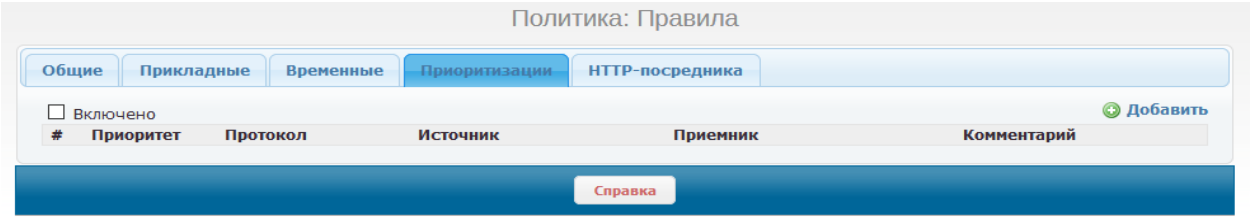


Рисунок 4.126: Пример исходного вида вкладки правил приоритизации

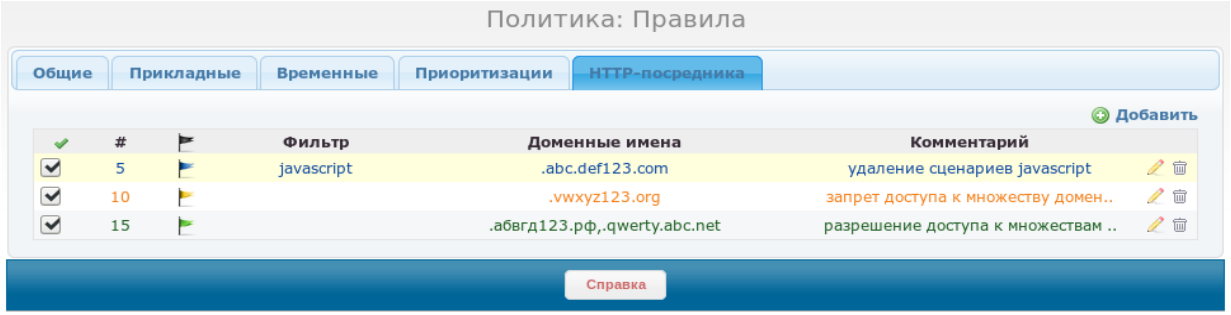


Рисунок 4.127: Пример вкладки правил приоритизации при наличии правил

На вкладке правил приоритизации расположены следующие управляющие элементы:

- кнопка-флаг `Включено` – управляет использованием функции приоритетной обработки трафика. Значение по умолчанию – **выключено**.
- `Добавить` – открывает форму добавления правила приоритизации.

Таблица правил приоритизации состоит из следующих полей:

- `#` – номер правила;
- `Приоритет` – значение приоритета, которое будет присвоено пакетам, подпадающим под данное правило;
- `Протокол` – протокол, инкапсулированный в IP-пакет;
- `Источник` – адресная информация источника;
- `Приемник` – адресная информация приемника;
- `Комментарий` – строка комментария к правилу.

Записи таблицы правил приоритизации выделяются цветом текста (рис. 4.127) в зависимости от значения поля `Приоритет`:

- *зеленый* – правила с высоким приоритетом обработки трафика;
- *красный* – правила с низким приоритетом обработки трафика.

В поле `Источник` может быть выведена следующая информация:

- список входных интерфейсов в формате `eth:<список_интерфейсов>` (например: **`eth:1,3,5`**);
- список IPv4-адресов в формате `ip4:<список_IPv4>` (например: **`ip4:192.168.1.0/24`**);
- список IPv6-адресов в формате `ip6:<список_IPv6>` (например: **`ip6:2001:db8:a0b:12f0::/64)`**;
- список TCP или UDP-портов в формате `port:<список_портов>` (например: **`port:32768`**).

В поле `Приемник` может быть выведена следующая информация:

- список IPv4-адресов в формате `ip4:<список_IPv4>` (например: **`ip4:10.3.1.1-10.3.1.4`**);
- список IPv6-адресов в формате `ip6:<список_IPv6>` (например: **`ip6:2001:db8:a0b:12f0::/64`**);
- список TCP или UDP-портов в формате `port:<список_портов>` (например: **`port:22022`**).

В таблице правил приоритизации используются следующие управляющие иконки:

- – редактировать правило;
- – удалить правило.

По нажатию на кнопку `Добавить` открывается форма добавления правила приоритизации. Форма приведена на рисунке 4.128, стр. 320.

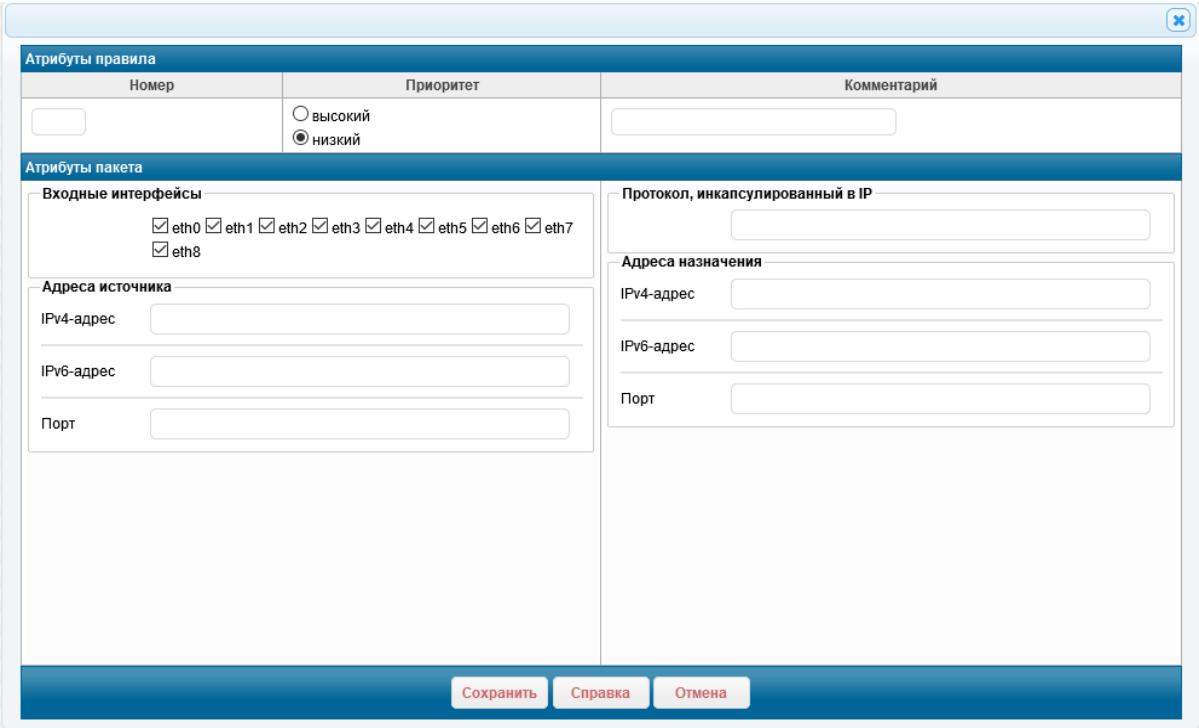


Рисунок 4.128: Форма добавления правила приоритизации

Форма добавления правила приоритизации содержит следующие элементы ввода данных:

- `Номер` – номер правила;
- `Приоритет` – значение приоритета, которое будет присвоено пакетам, подпадающим под данное правило. Пакеты будут обрабатываться с указанным приоритетом. Допустимые значения:
  - ✔ **высокий**;
  - ✔ **низкий** (по умолчанию);
- `Комментарий` – строка комментария к правилу;
- `Входные интерфейсы` – список входных интерфейсов (по умолчанию: выбраны все интерфейсы устройства, это значит, что правилу будут соответствовать IP-пакеты независимо от интерфейса МЭ, на который они поступят);
- `Протокол: протокол, инкапсулированный в IP` – список номеров и/или имен протоколов;
- `Адреса источника`:
  - ✔ `IPv4-адрес` – список IPv4-адресов источника;
  - ✔ `IPv6-адрес` – список IPv6-адресов источника;
  - ✔ `Порт` – список TCP или UDP-портов источника;
- `Адреса назначения`:
  - ✔ `IPv4-адрес` – список IPv4-адресов назначения;
  - ✔ `IPv6-адрес` – список IPv6-адресов назначения;

✔ Порт – список TCP или UDP-портов назначения.

При использовании *функции приоритетной обработки трафика*, сетевые пакеты, не подпадающие ни под одно из пправил приоритизации, имеют **базовый** приоритет обработки, который выше **низкого** и ниже **высокого**.

Записи таблицы правил приоритизации отличаются цветом текста, в зависимости от значения параметра *Приоритет*:

- зеленый – *высокий* приоритет (**high**);
- красный – *низкий* приоритет (**low**).

Форма редактирования *правила приоритизации* по своей структуре полностью идентична форме добавления, поэтому отдельно не рассматривается. Форма, помимо прочего, позволяет изменить номер правила (аналогично команде *rule move*).

Определение правила приоритизации (полный перечень параметров и форматы их значений) приведены в приложении Д.4, стр. 536.

В отличие от *общего правила* и *AP-правила* в *PRI-правиле* (приоритизации) не допускается одновременное использование IPv4-адресов и IPv6-адресов.
Т.е. в *PRI-правиле* не допускается, чтобы параметры IPv4-адрес источника (IPv4-адрес назначения) и IPv6-адрес источника (IPv6-адрес назначения) одновременно были заданы администратором.

Если *функция приоритетной обработки трафика* **выключена**, то пакеты не обрабатываются по правилам приоритизации.

HTTP-посредника. Во вкладке расположена таблица *правил HTTP-посредника* (PROXY-правил), которые управляют тем как HTTP-посредник обрабатывает трафик протоколов HTTP и HTTPs при обращении к различным WEB-серверам.

Правила HTTP-посредника отсутствуют в политике доступа по умолчанию. Пример исходного вида вкладки правил HTTP-посредника приведен на рисунке 4.129, стр. 321. Пример вкладки правил HTTP-посредника, при наличии правил, приведен на рисунке 4.130, стр. 322.

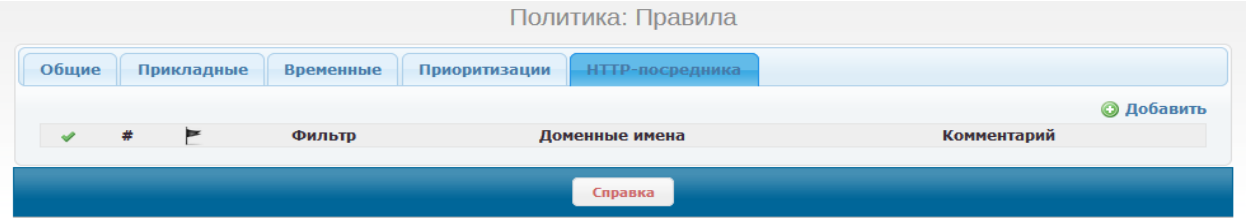


Рисунок 4.129: Пример исходного вида вкладки правил HTTP-посредника

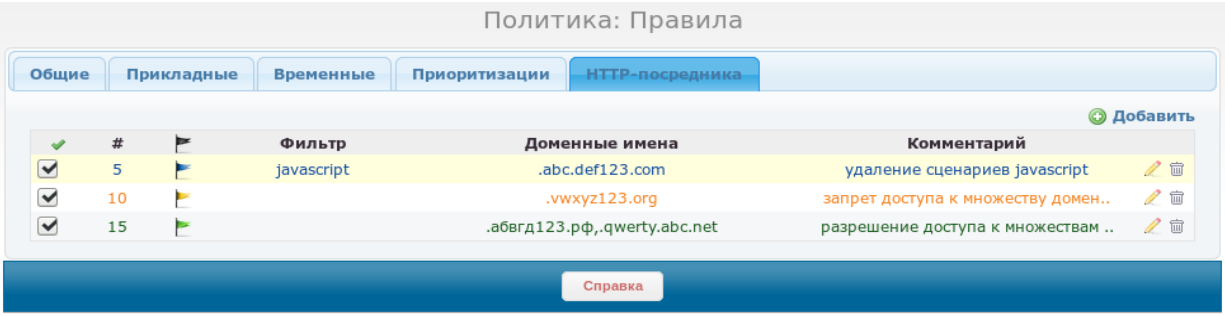


Рисунок 4.130: Пример вкладки правил HTTP-посредника при наличии правил

Таблица правил HTTP-посредника состоит из следующих полей:

- – активность правила (активно/не активно);
- # – номер правила;
- – действие;
- `Фильтр` – значение фильтра, в соответствии с которым HTTP-сообщения должны модифицироваться в случае действия **`изменить`** (**`edit`**);
- `Доменные имена` – список доменных имен, при обращении которым, должно применяться данное правило;
- `Комментарий` – строка комментария к правилу.

Записи таблицы правил HTTP-посредника выделяются цветом текста (рис. 4.130), в зависимости от действия правила:

- *зеленый* – действие **`принять`** (**`accept`**);
- *красный* – действие **`отклонить`** (**`deny`**);
- *синий* – действие **`изменить`** (**`edit`**).

В таблице правил HTTP-посредника используются следующие управляющие иконки:

- – редактировать правило;
- – удалить правило.

На вкладке правил HTTP-посредника расположена кнопка `Добавить`, по нажатию на которую открывается форма добавления правила HTTP-посредника. Форма приведена на рисунке 4.131, стр. 323.

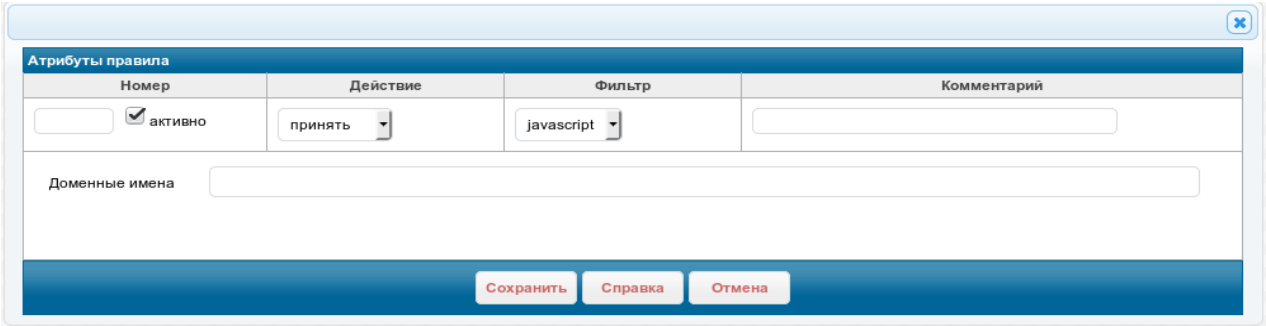


Рисунок 4.131: Форма добавления правила приоритизации

Форма добавления правила HTTP-посредника содержит следующие элементы ввода данных:

- `Номер` – номер правила;
- `активно` – флаг активности правила. Значения:
  - ✔ **включено** – правило активно;
  - ✔ **выключено** – правило неактивно;
- `Действие` – действие правила над пакетом с HTTP-сообщением. Допустимые значения:
  - ✔ **принять** – принять HTTP-сообщение (доступ по HTTP/HTTPs разрешен);
  - ✔ **отклонить** – отклонить HTTP-сообщение (доступ по HTTP/HTTPs запрещен);
  - ✔ **изменить** – изменить HTTP-сообщение в соответствии с фильтром, выбранным в списке `Фильтр`;
- Фильтр – фильтр, в соответствии с которым модифицируется HTTP-сообщение от WEB-сервера при выборе действия **изменить**. HTTP-посредник удаляет сценарии выбранного типа из WEB-страниц, перед формированием ответных HTTP-сообщений инициатору соединения с WEB-сервером В случае выбора действия, отличного от **изменить**, данный список блокируется. Допустимые значения:
  - ✔ **javascript** – запрет выполнения сценариев JavaScript;
  - ✔ **vbscript** – запрет выполнения сценариев VBScript (
- `Комментарий` – строка комментария к правилу;
- `Доменные имена` – список доменных имен, при обращении к которым должно применяться данное правило.

Определение правила HTTP-посредника (полный перечень параметров и форматы их значений) приведены в приложении Д.5, стр. 537.

Форма редактирования *правила HTTP-посредника* по своей структуре полностью идентична форме добавления, поэтому отдельно не рассматривается. Форма, помимо прочего, позволяет изменить номер правила (аналогично команде *rule move*).

Если полное доменное имя узла сети (FQDN), доступ к которому должен осуществляться в соответствии с некоторым PROXY-правилом, неизвестно или же PROXY-правило должно быть применено к множеству доменных имен (FQDN), с общим “окончанием”, то рекомендуется в параметре **hostname** указывать это общее “окончание” множества доменных имен, предваренное символом “точка”.

Например, в случае **hostname=.qwerty12345.org** PROXY-правило будет применено при обращении к следующим доменным именам:

- news.qwerty12345.org;
- mail.qwerty12345.org;
- dl.qwerty12345.org;
- и т.д.

HTTP-посредник обеспечивает запрет выполнения сценариев **JavaScript** и **VBScript** только для Web-станиц, доступ к которым осуществляется по протоколу **HTTP**.

Для Web-старниц, доступ к которым осуществляется по протоколу **HTTPs**, запрет выполнения сценариев **JavaScript** и **VBScript** не возможен.

Для обработки HTTP-трафика по правилам HTTP-посредника функция HTTP-посредника должна быть соответствующим образом настроена и включена (страница *Настройки: HTTP-посредник* WEB-интерфейса администратора).

4.3.4. Политика: Статистика

Страница “Политика: Статистика” предназначена для просмотра статистики использования правил фильтрации текущей политики доступа. Фрагмент страницы приведен на рисунке 4.132, стр. 324.

Правило	Последняя активность	Пакеты	Байты	Комментарий
rule:0	24.05.2018 17:45:00	11	484	
rule:1	24.05.2018 17:52:07	2	92	ARP с eth0 на eth1
rule:2	24.05.2018 17:52:07	24	1104	ARP с eth1 на eth0
rule:10	24.05.2018 16:46:35	137	61448	ssh с eth0 на eth1
rule:11	24.05.2018 17:52:26	238	15232	ICMP с eth0 на eth1
ap:0	24.05.2018 16:46:35	95	57048	

Рисунок 4.132: Фрагмент страницы Политика: Статистика

Статистика использования правил фильтрации отображается в табличной форме. Таблица состоит из следующих полей:

- `Правило` – тип и номер правила;
- `Последняя активность` – дата и время последнего срабатывания правила (когда правило в последний раз было применено к пакету);
- `Пакеты` – число пакетов, обработанных данным правилом;
- `Байты` – суммарное число байт в пакетах, обработанных данным правилом.
- `Комментарий` – строка комментария к правилу (поле предназначено для удобства идентификации правила администратором в дополнение к типу и номеру правила). Если

комментарий к правилу отсутствует, то поле выводится пустым. Комментарии длиннее 32 символов обрезаются для корректного вывода таблицы статистики.

Статистика в таблице выводится для правил следующих типов:

- `tmp` – TMP-правила (временные правила);
- `rule` – общие правила;
- `ap` – AP-правила (прикладные правила).

В приведенном примере (рис. 4.132, стр. 324) временные правила отсутствуют, но если бы они были добавлены администратором, то в таблице бы присутствовали соответствующие записи.

Если правило ни разу срабатывало за время работы пакетного фильтра (поля *Пакеты* и *Байты* имеют нулевые значения), то в поле *Последняя активность* выводится дата и время последнего чтения пакетным фильтром текущей политики доступа.

Статистика правил фильтрации сбрасывается при:
- перезапуске пакетного фильтра;
- любом изменении в текущей политике доступа (добавление правила и т. д.).

Записи таблицы отличаются цветом текста, в зависимости от действия правила фильтрации:
- зеленый – действие *пропустить* (**accept**);
- желтый – действие *отклонить* (**deny**);
- красный – действие *удалить* (**drop**);
  - синий – действие *перейти к правилу* (**goto**).

На странице `Политика: Статистика` присутствуют две кнопки:

- `Обновить` – обновление данных статистики;
- `Очистить` – сброс статистики.

При нажатии на кнопку `Обновить` происходит немедленное обновление статистики (запрос актуальных данных у пакетного фильтра и их вывод).

При нажатии на кнопку `Очистить` выполняется очистка статистики: для всех записей сбрасываются значения счетчиков `Пакеты` и `Байты`.

Имеется возможность автоматического обновления вывода статистики. Для этого на странице (рис. 4.132, стр. 324) используется кнопка-флаг `автообновление` (по умолчанию: **выключено**). Справа от кнопки-флага `автообновление` имеется список выбора периода обновления данных (по умолчанию: **5** секунд).

4.4. Управление сессиями

Пункт `Сессии` основного меню WEB-интерфейса позволяет перейти к следующим страницам, относящимся к *режиму управления сессиями*:

- `Сессии: Настройки` – просмотр и редактирование настроек режима управления сессиями;

- Сессии: Таблица сессий – просмотр таблицы сессий, удаление сессий в соответствии с критериями выборки, полная очистка таблицы сессий.

4.4.1. Сессии: Настройки

При выборе пункта “Сессии” основного меню WEB-интерфейса открывается страница Сессии: Настройки. Данная страница предназначена для настройки параметров режима управления сессиями МЭ ССПТ-4А1. Исходный вид (соответствует состоянию конфигурации МЭ ССПТ-4А1 по умолчанию) страницы “Сессии: Настройки” приведен на рисунке 4.133, стр. 327.

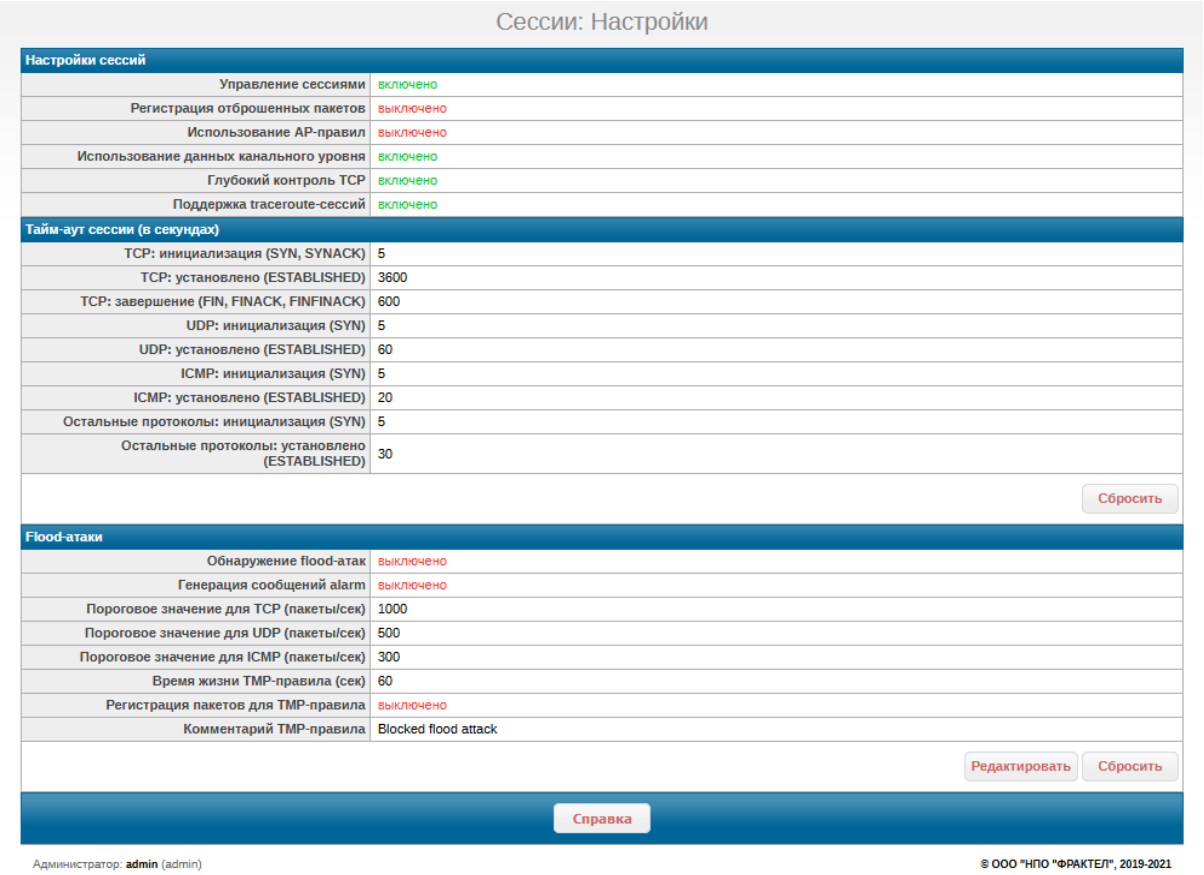
Страница разделена на три секции, в каждой из которых сгруппированы настройки в соответствии с их предназначением:

- Настройки сессий – общие настройки режима управления сессиями;
- Тайм-аут сессии (в секундах) – значения тайм-аутов различных состояний сессий для различных протоколов;
- Flood-атаки – параметры функции обнаружения Flood-атак.

Настройки сессий. В секции выводятся текущие значения следующих параметров:

- Управление сессиями – состояние режима управления сессиями;
- Регистрация отброшенных пакетов – регистрация пакетов, отброшенных режимом управления сессиями (например: пакет не соответствует контексту сессии);
- Использование АР-правил – использование АР-правил для фильтрации данных прикладного уровня;
- Использование данных канального уровня – использование данных канального уровня режимом управления сессиями;
- Глубокий контроль TCP – использование опции глубокого контроля TCP-сессий (контролируются номера последовательностей, подтверждений и другие параметры TCP-сессий);
- Поддержка traceroute-сессий – соотнесение ответных ICMP-сообщений с породившими их TCP или UDP-сессиями.

Тайм-аут сессии (в секундах). В секции указаны текущие значения тайм-аутов для различных состояний сессий применительно к различным протоколам. Если сессия некоторого протокола находится в определенном состоянии дольше чем значение соответствующего тайм-аута, то сессия будет автоматически удалена из *таблицы сессий*.



Сессии: Настройки

Настройки сессий	
Управление сессиями	включено
Регистрация отброшенных пакетов	выключено
Использование AP-правил	выключено
Использование данных канального уровня	включено
Глубокий контроль TCP	включено
Поддержка traceroute-сессий	включено
Тайм-аут сессии (в секундах)	
TCP: инициализация (SYN, SYNACK)	5
TCP: установлено (ESTABLISHED)	3600
TCP: завершение (FIN, FINACK, FINFINACK)	600
UDP: инициализация (SYN)	5
UDP: установлено (ESTABLISHED)	60
ICMP: инициализация (SYN)	5
ICMP: установлено (ESTABLISHED)	20
Остальные протоколы: инициализация (SYN)	5
Остальные протоколы: установлено (ESTABLISHED)	30
	Сбросить
Flood-атаки	
Обнаружение flood-атак	выключено
Генерация сообщений alarm	выключено
Пороговое значение для TCP (пакеты/сек)	1000
Пороговое значение для UDP (пакеты/сек)	500
Пороговое значение для ICMP (пакеты/сек)	300
Время жизни TMP-правила (сек)	60
Регистрация пакетов для TMP-правила	выключено
Комментарий TMP-правила	Blocked flood attack
	Редактировать Сбросить

Справка

Администратор: **admin** (admin)

© ООО "НПО "ФРАКТЕЛ", 2019-2021

Рисунок 4.133: Исходный вид страницы “Сессии: Настройки”

В секции имеется кнопка **`Сбросить`**, предназначенная для сброса всех тайм-аутов в значения по умолчанию.

Flood-атаки. В секции указаны текущие значения следующих параметров *функции обнаружения flood-атак*:

- `Обнаружение flood-атак` – использование функции обнаружения flood-атак.
- `Генерация сообщений alarm` – генерация сообщений сигнализации (alarm) при обнаружении flood-атак;
- `Пороговое значение для TCP (пакеты/сек)` – пороговое значение в числе пакетов в секунду, при превышении которого TCP-сессия будет расценена как flood-атака;
- `Пороговое значение для UDP (пакеты/сек)` – пороговое значение в числе пакетов в секунду, при превышении которого UDP-сессия будет расценена как flood-атака;
- `Пороговое значение для ICMP (пакеты/сек)` – пороговое значение в числе пакетов в секунду, при превышении которого ICMP-сессия будет расценена как flood-атака;

- `Время жизни TMP-правила (сек)` – интервал времени, по истечению которого TMP-правило, автоматически созданное пакетным фильтром в ответ на flood-атаку, будет удалено.
- `Регистрация пакетов для TMP-правила` – регистрация пакетов, отвечающих TMP-правилу, созданному в ответ на flood-атаку;
- `Комментарий TMP-правила` – строка комментария, которая будет использована в качестве значения параметра *Комментарий* при создании TMP-правила в ответ на flood-атаку.

В секции имеется две кнопки:

- **`Редактирование`** – изменение параметров функции управления сессиями;
- **`Сбросить`** – сброс пороговых значений обнаружения flood-атак в значения по умолчанию.

По нажатию кнопки **`Редактирование`** открывается общая форма редактирования настроек режима управления сессиями, посредством которой можно изменить значения всех параметров, выводимых на странице “Сессии: Настройки”. Пример формы с исходными значениями параметров (соответствующими конфигурации МЭ ССПТ-4А1 по умолчанию) приведен на рисунке 4.134, стр. 329.

Описание всех параметров, представленных в форме, приведено выше, при рассмотрении информации, выводимой на странице `Сессии: Настройки`. В случае ввода некорректного значения тайм-аута сессии или порогового значения обнаружения flood-атаки, будет выведено соответствующее сообщения об ошибке. Значения по умолчанию и граничные значения для тайма-аутов сессий и пороговых значений обнаружения flood-атак приведены в приложении А.2, стр. 428.

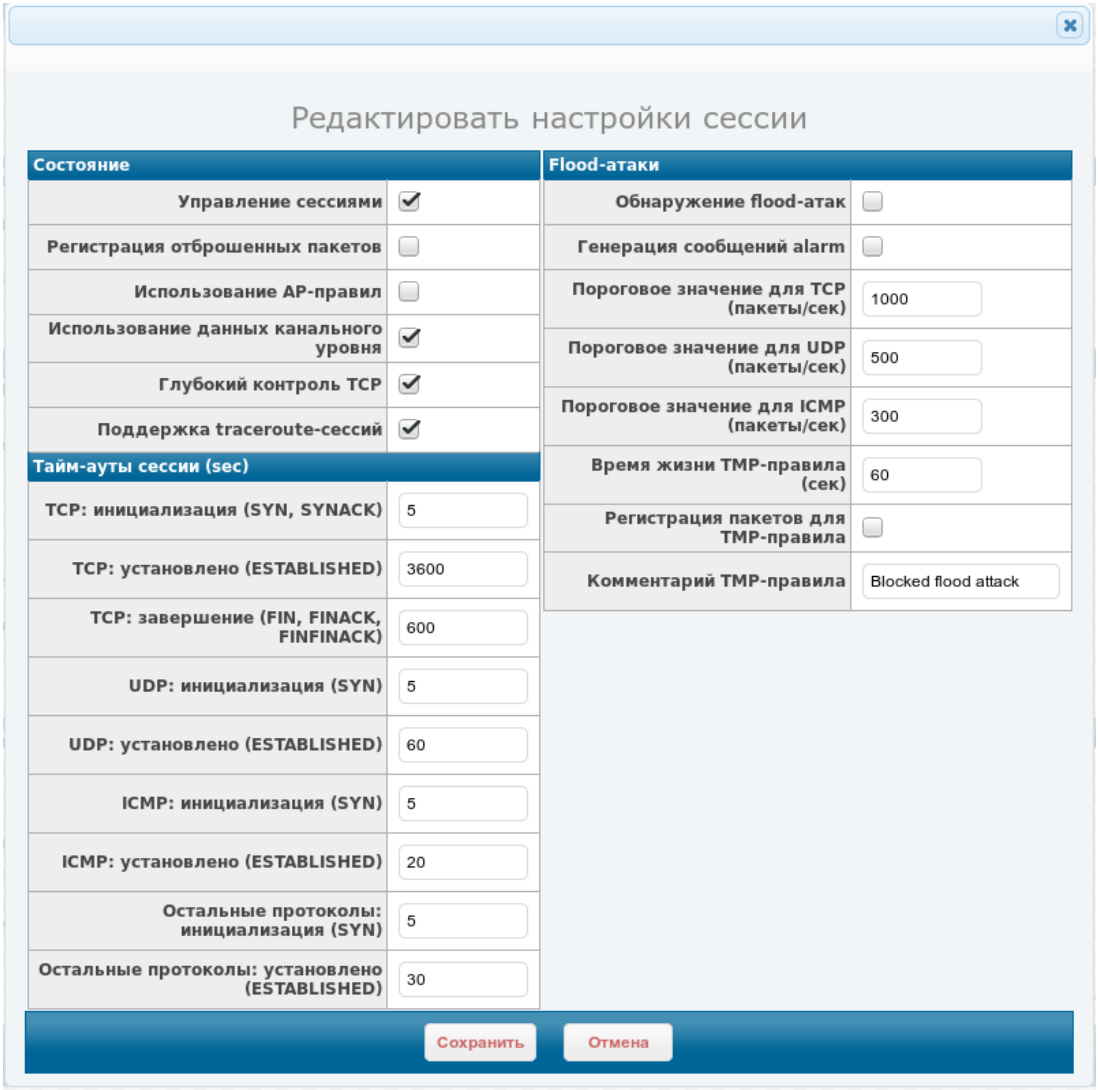


Рисунок 4.134: Форма редактирования настроек функции управления сессиями

4.4.2. Сессии: Таблица сессий

Страница “Сессии: Таблица сессий” предназначена для просмотра текущих сетевых соединений (сессий) через МЭ ССПТ-4А1. Страница также обеспечивает возможности:

- удаления сессий в соответствии с критериями выборки;
- полной очистки таблицы сессий.

Вид страницы “Сессии: Таблица сессий”, в отсутствие сетевых соединений, приведен на рисунке 4.135, стр. 330.

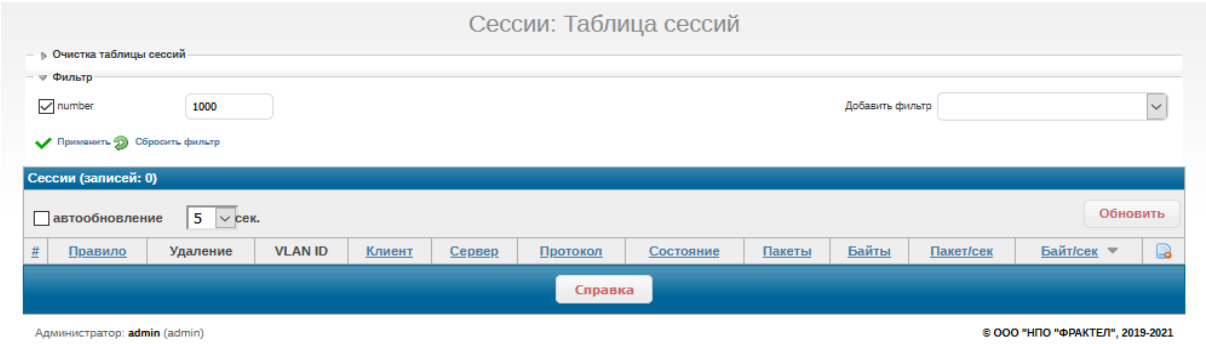


Рисунок 4.135: Страница Сессии: Таблица сессий при отсутствии сетевых соединений

Страница организована следующим образом:

Сверху находится раскрывающаяся секция “Очистка таблицы сессий”, которая по умолчанию – в свернутом состоянии. На рисунке 4.136, стр. 330 приведена данная секция в раскрытом состоянии.

Рисунок 4.136: Секция Очистка таблицы сессий в раскрытом виде

В секции присутствуют следующие управляющие элементы:

- кнопка-флаг `без регистрации сессий` – для выбора варианта очистки таблицы сессий. Значение по умолчанию: **включено**, т. е. при очистке таблицы сессий удаленные сессий не будут зарегистрированы в журнале регистрации сессий.
- `Очистить таблицу` – текстовая кнопка для выполнения очистки таблицы сессий в соответствии со значением кнопки-флага, описанной выше.

Под секцией “Очистка таблицы сессий” располагается раскрывающаяся секция `Фильтр`. По умолчанию данная секция выводится в раскрытом состоянии (рисунок 4.135, стр. 330). Секция служит для управления фильтрами вывода сессий. По умолчанию выбран фильтр `number` – вывод не более указанного числа сессий в соответствии с критерием сортировки таблицы сессий.

Выбор дополнительных фильтров осуществляется через выпадающий список `Добавить фильтр`. Содержимое списка приведено на рисунке 4.137, стр. 331.

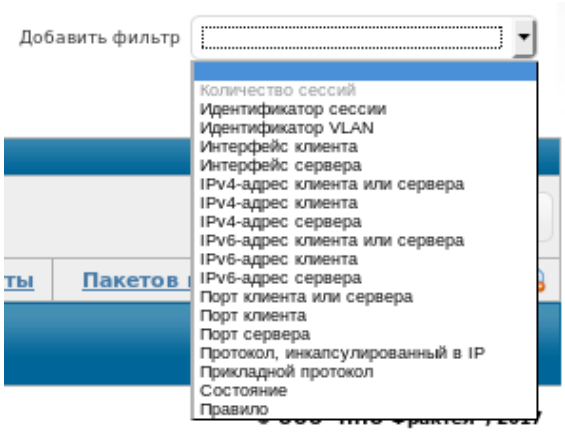


Рисунок 4.137: Список фильтров вывода сессий

Список включает в себя следующие фильтры (критерии выборки сессий):

- `Количество сессий (number)` – вывод не более указанного количества сессий (*выбран по умолчанию*);
- `Идентификатор сессии (sid)` – вывод сессии с указанным идентификатором;
- `Идентификатор VLAN (vlan)` – вывод сессий с указанным значением идентификатора VLAN;
- `Интерфейс клиента (ifcl)` – вывод сессий с указанным сетевым интерфейсом клиента;
- `Интерфейс сервера (ifsrv)` – вывод сессий с указанным сетевым интерфейсом сервера;
- `IPv4-адрес клиента или сервера (ip4)` – вывод сессий с указанным IP-адресом версии 4 клиента или сервера;
- `IPv4-адрес клиента (ipcl4)` – вывод сессий с указанным IP-адресом версии 4 клиента;
- `IPv4-адрес сервера (ipsrv4)` – вывод сессий с указанным IP-адресом версии 4 сервера;
- `IPv6-адрес клиента или сервера (ip6)` – вывод сессий с указанным IP-адресом версии 6 клиента или сервера;
- `IPv6-адрес клиента (ipcl6)` – вывод сессий с указанным IP-адресом версии 6клиента;
- `IPv6-адрес сервера (ipsrv6)` – вывод сессий с указанным IP-адресом версии 6 сервера;
- `Порт клиента или сервера (port)` – вывод сессий с указанным портом клиента или сервера;
- `Порт клиента (portcl)` – вывод сессий с указанным портом клиента;
- `Порт сервера (portsrv)` – вывод сессий с указанным портом сервера;
- `Протокол, инкапсулированным в IP (tproto)` – вывод сессий с указанным протоколом, инкапсулированным в IP;
- `Прикладной протокол (aproto)` – вывод сессий с указанным прикладным протоколом;
- `Состояние (state)` – вывод сессий, находящихся в указанном состоянии;
- `Правило (rule)` – вывод сессий, созданных по указанному общему правилу фильтрации.

Фильтр **vlan** допускает указание:

- идентификатора VLAN (например: 211);
- диапазона идентификаторов VLAN (например: 301-305);
- списка из указанных выше элементов (например: 211,301-305);

Фильтры **ip4**, **ipcl4**, **ipsrv4** допускают указание:

- IP-адреса узла сети (например: 192.168.1.1);
- IP-адреса сети с указанием маски (например: 192.168.2.0/24);
- диапазона IP-адресов (например: 10.1.1.1-10.1.1.9);
- списка из указанных выше элементов (например: 192.168.1.1,192.168.2.0/24,10.1.1.1-10.1.1.9);

Фильтры **ip6**, **ipcl6**, **ipsrv6** допускают указание:

- IPv6-адреса узла сети (например: 2001:db8:a1b:12f0::1);
- IPv6-адреса сети с указанием длины префикса (например: 2001:db8:a0b:12f0::0/64);
- списка из указанных выше элементов (например: 2001:db8:a1b:12f0::1,2001:db8:a0b:12f0::0/64);

Выбранные фильтры помещаются в секцию Фильтр для ввода значения фильтра. Пример вывода выбранных фильтров приведен на рисунке 4.138, стр. 332.

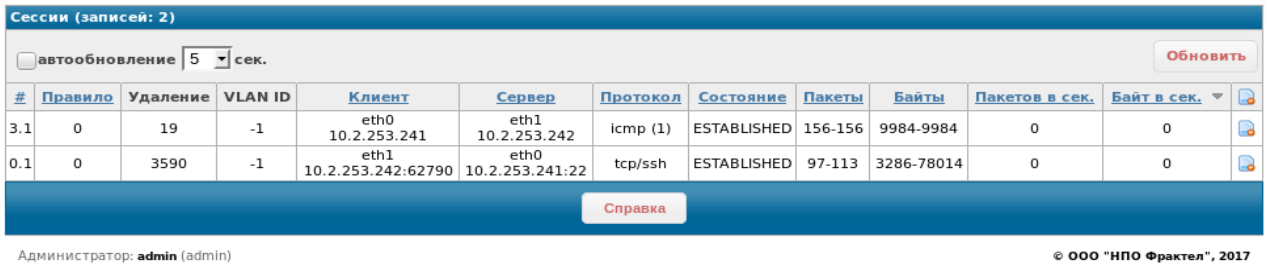
Рисунок 4.138: Пример задания фильтров вывода сессий

Перед именем каждого фильтра – кнопка-флаг, позволяющая не использовать добавленный фильтр при выборке сессий. В строке каждого фильтра – поле ввода его значения.

Под списком выбранных фильтров – управляющие элементы:

- `Применить` – применение выбранного набора фильтров. В итоге перезагружается вывод таблицы сессий с учетом выбранного набора фильтров.
- `Сбросить фильтр` – сброс набора фильтров в состояние по умолчанию (выбран фильтр `number` со значением **`1000`**).

Под секцией “Фильтры” располагается всегда видимая секция “Сессии”. Данная секция содержит таблицу сессий. Пример вывода таблицы сессий приведен на рисунке 4.139, стр. 332.



#	Правило	Удаление	VLAN ID	Клиент	Сервер	Протокол	Состояние	Пакеты	Байты	Пакетов в сек.	Байт в сек.
3.1	0	19	-1	eth0 10.2.253.241	eth1 10.2.253.242	icmp (1)	ESTABLISHED	156-156	9984-9984	0	0
0.1	0	3590	-1	eth1 10.2.253.242:62790	eth0 10.2.253.241:22	tcp/ssh	ESTABLISHED	97-113	3286-78014	0	0

Рисунок 4.139: Пример вывода таблицы сессий

В секции “Сессии” имеются следующие управляющие элементы:

- кнопка-флаг `автообновление` – использование автоматического обновления вывода таблицы сессий. Значение по умолчанию: **выключено**;
- выпадающий список выбора интервала автоматического обновления таблицы сессий. Значение по умолчанию: **5** секунд;
- кнопка `Обновить` – принудительное обновление вывода таблицы сессий.

Таблица сессий состоит из следующих полей:

- `#` – идентификатор сессии;
- `Правило` – номер общего правила фильтрации, в соответствии с которым была создана данная сессия;
- `Удаление` – количество секунд до удаления сессии из таблицы. Отрицательное значение говорит о том, что сессия будет удалена из таблицы в течение ближайших 10 секунд;
- `VLAN ID` – идентификатор VLAN, которой принадлежит данная сессия. Нулевое значение говорит о том, что VLAN-тегов в пакетах данной сессии нет;
- `Клиент` – адресные данные инициатора соединения, включающие в себя:
  - ✔ имя фильтрующего интерфейса;
  - ✔ IP-адрес;
  - ✔ порт – только для сессий протокола TCP и UDP;
- `Сервер` – адресные данные сервера, включающие в себя:
  - ✔ имя фильтрующего интерфейса;
  - ✔ IP-адрес;
  - ✔ порт – только для сессий протокола TCP и UDP;
- `Протокол` – протоколы данной сессии;
- `Состояние` – состояние сессии. Возможны следующие значения данного поля:
  - ✔ Для протокола TCP:
    - ◆ `SYN` – принят SYN-пакет от клиента;
    - ◆ `SYNACK` – принято подтверждение от сервера на SYN-пакет от клиента;
    - ◆ `ESTABLISH` – сессия установлена;
    - ◆ `FIN` – принят FIN-пакет от одного из участников соединения;
    - ◆ `FINACK` – принято подтверждение на первый FIN-пакет;
    - ◆ `FINFINACK` – стороны обменялись FIN-пакетами, один из FIN-пакетов подтвержден;
    - ◆ `FINFIN` – стороны обменялись FIN-пакетами, ни один из FIN-пакетов не подтвержден;
    - ◆ `TIMEWAIT` – стороны закрыли TCP-соединение, ожидание опоздавших пакетов;
    - ◆ `RESET` – произошел сброс соединения одной из сторон, ожидание серии RST-пакетов;
- Для протоколов UDP и ICMP:
  - ✔ `SYN` – принят первый пакет от клиента;

✔ ESTABLISH – сессия установлена; произошел как минимум один обмен пакетами между клиентом и сервером;

- Пакеты: количество пакетов, переданное в рамках данной сессии в формате: <от_клиента>-<от_сервера>;
- Байты: количество байт, переданное в рамках данной сессии в формате: <от_клиента>-<от_сервера>;
- Пакетов в сек. – суммарная (от клиента и от сервера) скорость передачи данных в рамках данной сессий в числе пакетов в секунду;
- Байт в сек. – суммарная (от клиента и от сервера) скорость передачи данных в рамках данной сессий в числе байт в секунду.

Записи в таблице сессий могут быть отсортированы по любому из перечисленных полей таблицы, за исключением полей: VLAN ID и Удаление. Также может быть выбран порядок сортировки: по возрастанию или по убыванию.

По умолчанию сортировка выполняется по возрастанию значений поля Байт в сек. (рис. 4.139, стр. 332). Поле, выбранное для сортировки записей таблицы, отмечается специальным символом, который указывается после заголовка поля:

- – сортировка по убыванию значений поля;
- – сортировка по возрастанию значений поля;

Для выбора поля, по которому выполняется сортировка записей, необходимо нажать на заголовок данного поля. При этом поле будет отмечено символом сортировки по возрастанию. Для смены порядка сортировки необходимо еще раз нажать на заголовок данного поля: в результате символ порядка сортировки будет изменен.

По умолчанию автоматическое обновление таблицы сессий **выключено**. При выключенном автоматическом обновлении после смены поля, используемого для сортировки записей либо смены порядка сортировки необходимо нажать кнопку *Обновить*.

При включенном автоматическое обновление таблицы сессий после смены поля, используемого для сортировки либо порядка сортировки, записи таблицы будут пересортированы автоматически при очередном обновлении данных таблицы.

В каждой записи таблицы, а также в заголовке таблицы присутствует иконка удаления записей. Назначение данной иконки:

- в записи таблицы – удаление данной сессии;
- в заголовке таблицы – удаление сессий в соответствии с заданными критериями выборки. При нажатии на иконку открывается форма задания критериев удаления сессий. Форма приведена на рисунке 4.140, стр. 335.

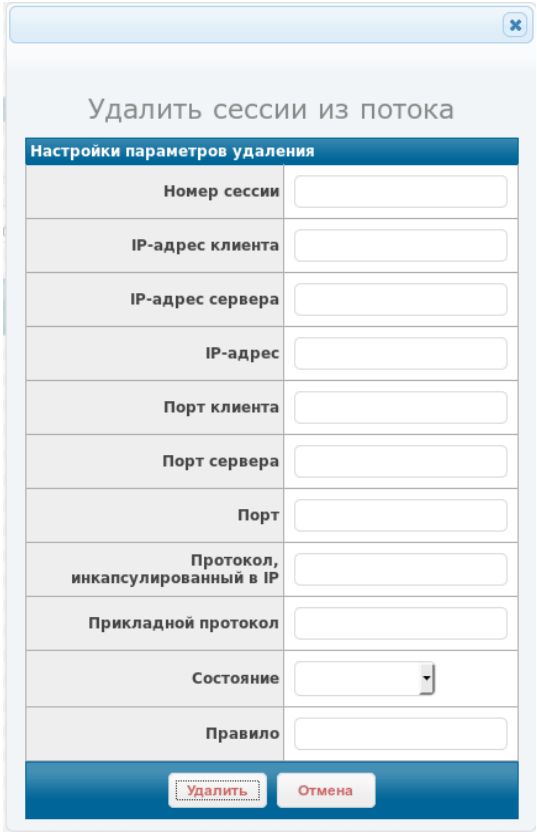


Рисунок 4.140: Форма задания критериев удаления сессий

Форма содержит следующие элементы ввода данных:

- `Номер сессии` – идентификатор сессии для удаления в формате `<X>.<Y>`, где `<X>` и `<Y>` – числа в десятичном виде;
- `IP-адрес клиента` – IP-адрес клиента (инициатора соединения);
- `IP-адрес сервера` – IP-адрес сервера;
- `IP-адрес` – IP-адрес клиента либо сервера;
- `Порт клиента` – TCP или UDP порт клиента;
- `Порт сервера` – TCP или UDP порт сервера;
- `Порт` – TCP или UDP порт клиента либо сервера;
- `Протокол, инкапсулированный в IP` – имя либо код протокола, инкапсулированного в IP. Например, **`tcp`** или **`6`**, **`udp`** или **`17`** или **`icmp`** или **`1`** и т. п.;
- `Прикладной протокол` – имя либо код прикладного протокола (код соответствует стандартному номера порта данного прикладного протокола). Например, **`http`** или **`80`**, **`ssh`** или **`22`** и т. п.;
- `Состояние` – выпадающий список выбора состояния сессий. Элементы списка соответствуют состояниям, выводимым в таблице сессий (см. описание поля `Состояние` таблицы сессий);
- `Правило` – номер общего правила, по которому были созданы сессии.

Следующие пары критериев выборки сессий для удаления не допустимы к использованию, т. к. возникает логическое противоречие:

- ipcl и ip;
- ipsrv и ip;
- portcl и port;
- portsrv и port;.

В случае указания недопустимой пары критериев при нажатии на кнопку Удалить формы будет выедено сообщение об ошибке:

```
FNPSH-E-007.02.1136-Совместное использование параметров недопустимо
(имя_параметра_1, имя_параметра_2)
```

4.5. Регистрация

Пункт `Регистрация` основного меню WEB-интерфейса позволяет через подменю перейти к группе страниц, предназначенных для просмотра журналов регистрации МЭ ССПТ-4А1. При выборе данного пункта основного меню открывается страница “Регистрация: События”.

В подменю доступны следующие пункты:

- `События` – переход к странице “Регистрация: События” (раздел 4.5.1, стр. 337);
- `Пакеты` – переход к странице “Регистрация: Пакеты” (раздел 4.5.2, стр. 340);
- `Сессии` – переход к странице “Регистрация: Сессии” (раздел 4.5.3, стр. 347);
- `Очистка файлов регистрации` – очистка журналов регистрации пакетов и/или сессий.

Пример страницы “Регистрация: Системные сообщения” приведен на рисунке 4.141, стр. 336.

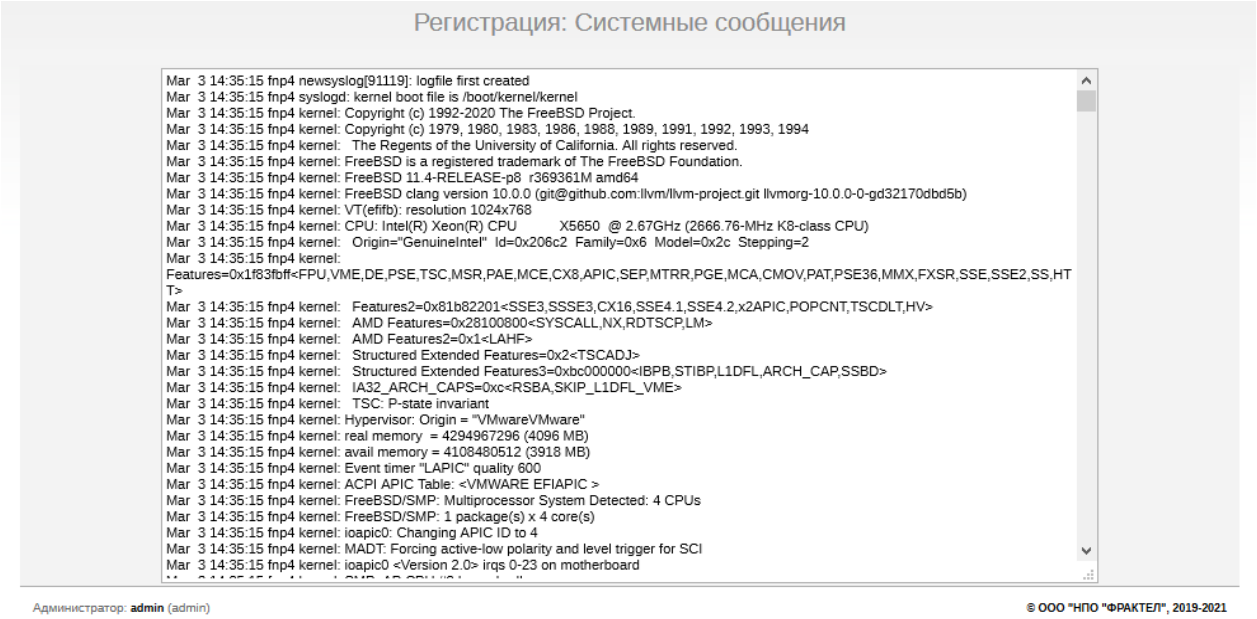


Рисунок 4.141: Пример страницы “Регистрация: Системные сообщения”

Системные сообщения выводятся в порядке возрастания даты и времени регистрации. Изменение порядка сортировки и выборка сообщений не предусмотрены.

По нажатию на кнопку **Очистка файлов регистрации** открывается диалоговое окно выбора журнала для очистки, которое приведено на рисунке 4.142, стр. 337.

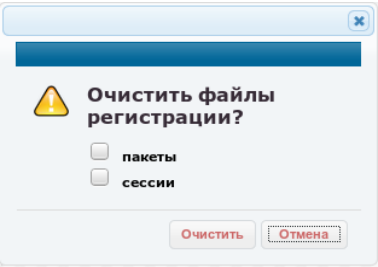


Рисунок 4.142: Окно выбора журналов регистрации для очистки

Возможен выбор одного или обоих вариантов:

- пакеты – очистка журнала регистрации пакетов;
- сессии – очистка журнала регистрации сессий.

На журналы регистрации пакетов и сессий в сумме отведено **10000** записей (позиций). По достижении этого числа записей начинается циклическая перезапись: новые записи регистрации заменяют старые.

4.5.1. Регистрация: События

Страница “Регистрация: События”, приведенная на рисунке 4.143, стр. 338, позволяет:

- задать критерии выборки событий для вывода;
- выбрать порядок сортировки событий;
- вывести события.

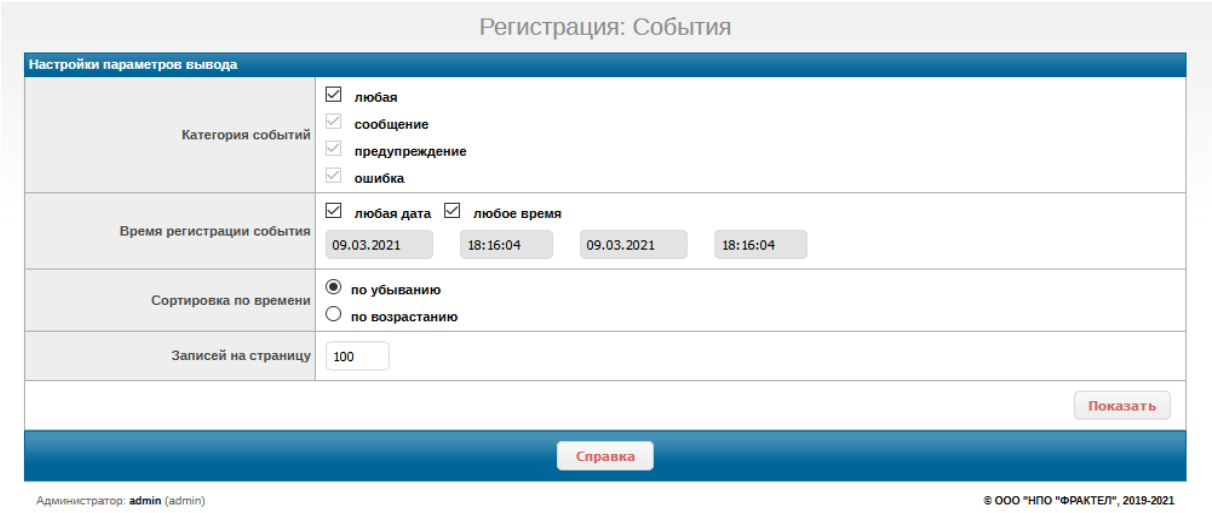


Рисунок 4.143: Страница “Регистрация: События”

События для вывода могут быть выбраны в соответствии со следующими критериями:

- Категория событий – выбор категорий событий для вывода. Допускается выбор комбинаций следующих значений:
  - ✔ **любая** – вывод событий всех категорий, указанных ниже (по умолчанию);
  - ✔ **сообщение** – вывод только информационных сообщений;
  - ✔ **предупреждение** – вывод только предупреждений;
  - ✔ **ошибка** – вывод только сообщений об ошибках;
- Время регистрации события – задание интервала времени регистрации событий. В результате будут выведены события, зарегистрированные за указанный интервал времени. Ожидается ввод даты и времени начала интервала, а также даты и времени конца интервала. Значения по умолчанию – **любая дата** и **любое время**. При значениях по умолчанию будут выбраны события, зарегистрированные за все время эксплуатации МЭ ССПТ-4А1.
- Сортировка по времени – выбор варианта сортировки событий по времени регистрации. Допустимые значения:
  - ✔ **по убыванию** – последнее зарегистрированное событие будет показано первым (от “новых” к “старым”). Значение по умолчанию;
  - ✔ **по возрастанию** – последнее зарегистрированное событие будет показано последним (от “старых” к “новым”);
- Записей на страницу – максимальное количество записей, выводимых на одной странице. Все записи, предназначенные для просмотра, разделяются на страницы, в каждой из которых содержится не более указанного количества записей.

Кнопка **Показать** служит для вывода событий в соответствии с:

- указанными критериями выборки;

- указанным порядком сортировки;
- указанным максимальным числом записей на одной странице.

> МЭ ССПТ-4А1 может одновременно хранить до **6000** записей о зарегистрированных событиях.
>
> В МЭ ССПТ-4А1 производится циклическое обновление записей о зарегистрированных событиях. Таким образом, наиболее старые записи переписываются вновь регистрируемыми.
>
> По умолчанию выводятся все записи регистрации событий, отсортированные по убыванию времени регистрации (последние – вначале). На одной странице выводится не более **100** записей.

По нажатию на кнопку **`Показать`** открывается модальное окно “Регистрация: Список событий”. Фрагмент такого окна приведен на рисунке 4.144, стр.340.

Записи выводятся в форме таблицы со следующими полями:

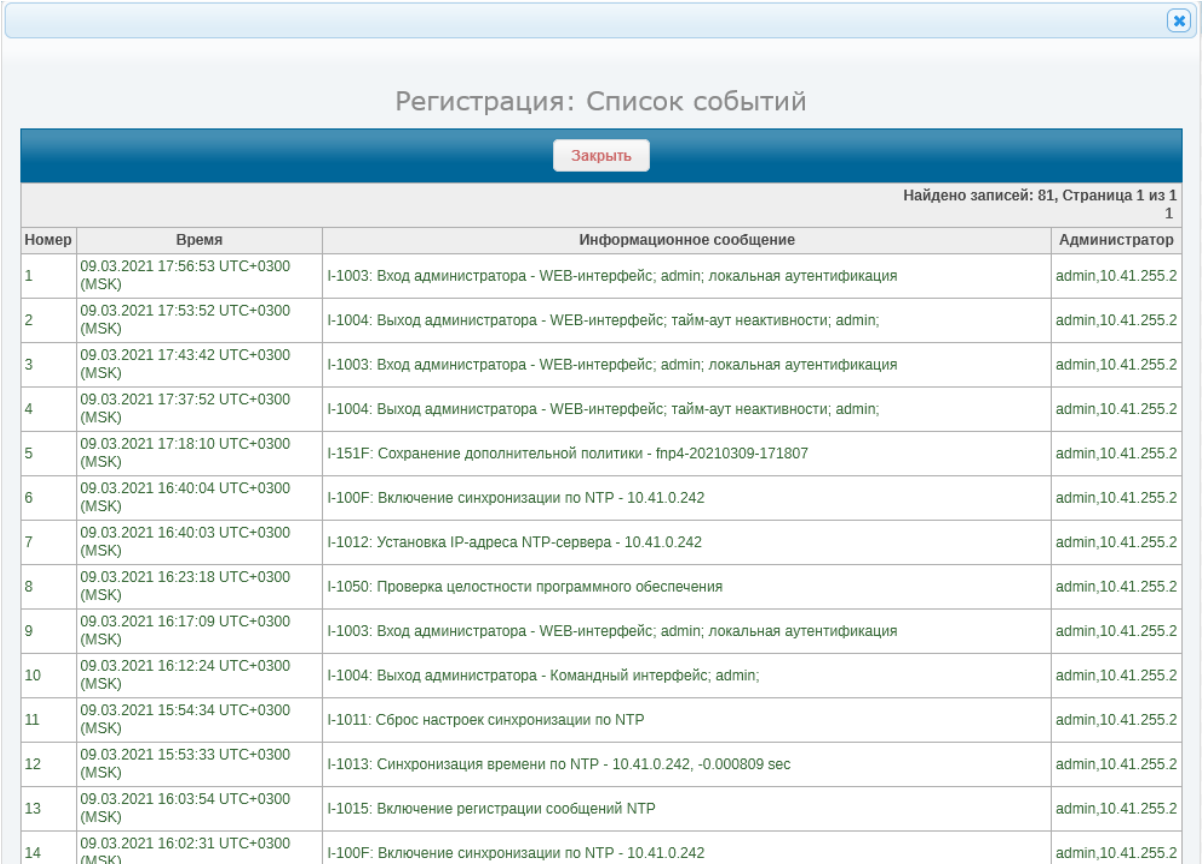
- `Номер`: порядковый номер при выбранном варианте сортировки;
- `Время`: дата и время регистрации события с указанием часового пояса;
- `Информационное сообщение`: категория события (I, W или E), шестнадцатеричный код события, текст сообщения события. Для событий входа и выхода администратора также указывается реальные привилегии, полученные при авторизации.
- `Администратор`: имя администратора, IP-адрес УК администратора при удаленном подключении либо `Console` при локальном подключении.

Записи, соответствующие событиям различных категорий, отличаются цветом текста:

- категория “сообщение” – зеленый;
- категория “предупреждение” – синий;
- категория “ошибка” – красный.

Вверху окна расположены:

- кнопка Закрыть для закрытия окна
- общее число выбранных записей;
- элементы навигации для переключения между страницами вывода записей регистрации.



Регистрация: Список событий

Закрыть

Найдено записей: 81, Страница 1 из 1
1

Номер	Время	Информационное сообщение	Администратор
1	09.03.2021 17:56:53 UTC+0300 (MSK)	I-1003: Вход администратора - WEB-интерфейс; admin; локальная аутентификация	admin,10.41.255.2
2	09.03.2021 17:53:52 UTC+0300 (MSK)	I-1004: Выход администратора - WEB-интерфейс; тайм-аут неактивности; admin;	admin,10.41.255.2
3	09.03.2021 17:43:42 UTC+0300 (MSK)	I-1003: Вход администратора - WEB-интерфейс; admin; локальная аутентификация	admin,10.41.255.2
4	09.03.2021 17:37:52 UTC+0300 (MSK)	I-1004: Выход администратора - WEB-интерфейс; тайм-аут неактивности; admin;	admin,10.41.255.2
5	09.03.2021 17:18:10 UTC+0300 (MSK)	I-151F: Сохранение дополнительной политики - fnp4-20210309-171807	admin,10.41.255.2
6	09.03.2021 16:40:04 UTC+0300 (MSK)	I-100F: Включение синхронизации по NTP - 10.41.0.242	admin,10.41.255.2
7	09.03.2021 16:40:03 UTC+0300 (MSK)	I-1012: Установка IP-адреса NTP-сервера - 10.41.0.242	admin,10.41.255.2
8	09.03.2021 16:23:18 UTC+0300 (MSK)	I-1050: Проверка целостности программного обеспечения	admin,10.41.255.2
9	09.03.2021 16:17:09 UTC+0300 (MSK)	I-1003: Вход администратора - WEB-интерфейс; admin; локальная аутентификация	admin,10.41.255.2
10	09.03.2021 16:12:24 UTC+0300 (MSK)	I-1004: Выход администратора - Командный интерфейс; admin;	admin,10.41.255.2
11	09.03.2021 15:54:34 UTC+0300 (MSK)	I-1011: Сброс настроек синхронизации по NTP	admin,10.41.255.2
12	09.03.2021 15:53:33 UTC+0300 (MSK)	I-1013: Синхронизация времени по NTP - 10.41.0.242, -0.000809 sec	admin,10.41.255.2
13	09.03.2021 16:03:54 UTC+0300 (MSK)	I-1015: Включение регистрации сообщений NTP	admin,10.41.255.2
14	09.03.2021 16:02:31 UTC+0300 (MSK)	I-100F: Включение синхронизации по NTP - 10.41.0.242	admin,10.41.255.2

Рисунок 4.144: Фрагмент окна “Регистрация: Список событий”

В нижней части окна (не показаны на рисунке 4.144, стр. 340) для удобства администратора продублированы:

- кнопка **Закрыть**;
- элементы навигации для переключения между страницами вывода записей регистрации.

4.5.2. Регистрация: Пакеты

Страница “Регистрация: Пакеты” представляет собой форму для задания критериев выборки записей регистрации пакетов, а также выбора других параметров вывода записей регистрации пакетов. Фрагмент страницы “Регистрация: Пакеты” приведен на рисунке 4.145, стр. 341.

Настройки параметров вывода

Показать

Действие	☑ пропустить ☑ удалить ☑ отклонить
Интерфейсы Вх.	☐ eth0 ☐ eth1 ☐ eth2 ☐ eth3 ☐ eth4 ☐ eth5 ☐ eth6 ☐ eth7
Интерфейсы Вых.	☐ eth0 ☐ eth1 ☐ eth2 ☐ eth3 ☐ eth4 ☐ eth5 ☐ eth6 ☐ eth7
Правило	
Тип кадра Ethernet	☑ Ethernet II ☑ IEEE 802.2 LLC ☑ IEEE 802.2 SNAP ☑ IEEE 802.3 Raw
Протокол	☑ ARP ☑ IPv4 ☑ IPv6 ☑ ICMPv4 ☑ ICMPv6 ☑ TCP ☑ UDP ☑ Другие
Номер сессии	
MAC-адрес источника	
MAC-адрес приемника	
MAC-адрес	
IPv4-адрес источника	
IPv4-адрес приемника	
IPv4-адрес	
IPv6-адрес источника	
IPv6-адрес приемника	
IPv6-адрес	
Порт источника	
Порт приемника	
Порт	
Время регистрации пакета	☑ любая дата ☑ любое время 12.10.2018 13:36:31 12.10.2018 13:36:31
Сортировка по времени	◉ по убыванию ○ по возрастанию
Записей на страницу	100

Рисунок 4.145: Фрагмент страницы “Регистрация: Пакеты”

Страница “Регистрация: Пакеты” содержит следующие элементы ввода данных:

- `Действие` – вывод пакет с указанными действиями. Допустимы действия – **`пропустить`**, **`удалить`**, **`отклонить`**;
- `Интерфейс Вх.` – вывод пакетов с указанным входным интерфейсом. Допускается множественный выбор;
- `Интерфейс Вых.` – вывод пакетов с указанным выходным интерфейсом. Допускается множественный выбор;
- `Правило` – тип и номер правила фильтрации, примененного к пакету. Формат `<тип_правила>:<номер_правила>`, где `<тип_правила>`:

  ✔ **`rule`** – общее правило

✔ **ap** – AP-правило;

✔ **tmp** – TMP-правило;

- `Тип кадра Ethernet` – вывод пакетов, инкапсулированных в кадры Ethernet указанных типов. Допустимы следующие типы кадров – **Ethernet II**, **IEEE 802.2 LLC**, **IEEE 802.2 SNAP**, **IEEE 802.3 Raw**;
- `Протокол` – вывод пакетов с указанными протоколами. Допустимы следующие значения протоколов – **ARP**, **IPv4**, **IPv6**, **ICMPv4**, **ICMPv6**, **TCP**, **UDP**, **Другие** (все остальные протоколы);
- `Номер сессии` – идентификатор сессии. Формат: `<номер>.<номер>`, где `<номер>` – десятичное число;
- `MAC-адрес источника` – вывод пакетов с указанным MAC-адресом источника. Формат: список следующих элементов (`X` – шестнадцатеричный знак, `<N>` – десятичное число байтов макси):

  ✔ `<XX:XX:XX:XX:XX:XX>` – MAC-адрес;

  ✔ `<XX:XX:XX:XX:XX:XX>/<N>` – MAC-адрес/маска;

  ✔ `<XX-XX-XX-XX-XX-XX>` – MAC-адрес;

  ✔ `<XX-XX-XX-XX-XX-XX>/<N>` – MAC-адрес/маска;

  ✔ `<XXXXXXXXXXXX>` – MAC-адрес;

  ✔ `<XXXXXXXXXXXX>/<N>` – MAC-адрес/маска;
- `MAC-адрес приемника` – вывод пакетов с указанным MAC-адресом приемника. Формат: список следующих элементов (`X` – шестнадцатеричный знак, `<N>` – десятичное число байтов макси):

  ✔ `<XX:XX:XX:XX:XX:XX>` – MAC-адрес;

  ✔ `<XX:XX:XX:XX:XX:XX>/<N>` – MAC-адрес/маска;

  ✔ `<XX-XX-XX-XX-XX-XX>` – MAC-адрес;

  ✔ `<XX-XX-XX-XX-XX-XX>/<N>` – MAC-адрес/маска;

  ✔ `<XXXXXXXXXXXX>` – MAC-адрес;

  ✔ `<XXXXXXXXXXXX>/<N>` – MAC-адрес/маска;
- `MAC-адрес` – вывод пакетов с указанным MAC-адресом источника или приемника. Формат: список следующих элементов:

  ✔ `<XX:XX:XX:XX:XX:XX>` – MAC-адрес;

  ✔ `<XX:XX:XX:XX:XX:XX>/<N>` – MAC-адрес/маска;

  ✔ `<XX-XX-XX-XX-XX-XX>` – MAC-адрес;

  ✔ `<XX-XX-XX-XX-XX-XX>/<N>` – MAC-адрес/маска;

  ✔ `<XXXXXXXXXXXX>` – MAC-адрес;

✔ <XXXXXXXXXXXX>/<N> – MAC-адрес/маска;

- IPv4-адрес источника – вывод пакетов с указанным IP-адресом источника. Формат: список следующих элементов:
  - ✔ <IP-адрес> – IPv4-адрес;
  - ✔ <IP-адрес>/<N> – IPv4-адрес/маска в виде префикса;
  - ✔ <IP-адрес>/<IP-маска> – IPv4-адрес/маска;
  - ✔ <IP-адрес_1>-<IP-адрес_2> – диапазон IPv4-адресов;
- IPv4-адрес приемника – вывод пакетов с указанным IP-адресом приемника. Формат: список следующих элементов:
  - ✔ <IP-адрес> – IPv4-адрес;
  - ✔ <IP-адрес>/<N> – IPv4-адрес/маска в виде префикса;
  - ✔ <IP-адрес>/<IP-маска> – IPv4-адрес/маска;
  - ✔ <IP-адрес_1>-<IP-адрес_2> – диапазон IPv4-адресов;
- IPv4-адрес – вывод пакетов с указанным IP-адресом источника или приемника. Формат: список следующих элементов:
  - ✔ <IP-адрес> – IPv4-адрес;
  - ✔ <IP-адрес>/<N> – IPv4-адрес/маска в виде префикса;
  - ✔ <IP-адрес>/<IP-маска> – IPv4-адрес/маска;
  - ✔ <IP-адрес_1>-<IP-адрес_2> – диапазон IPv4-адресов;
- IPv6-адрес источника – вывод пакетов с указанным IPv6-адресом источника. Формат: список следующих элементов:
  - ✔ <IPv6-адрес> – IPv6-адрес;
  - ✔ <IPv6-префикс>/<N> – IPv6-префикс сети, где <N> – длина префикса;
  - ✔ <IPv6-адрес_1>-<IPv6-адрес_2> – диапазон IPv6-адресов;
- IPv6-адрес приемника – вывод пакетов с указанным IPv6-адресом приемника. Формат: список следующих элементов:
  - ✔ <IPv6-адрес> – IPv6-адрес;
  - ✔ <IPv6-префикс>/<N> – IPv6- префикс сети, где <N> – длина префикса;
  - ✔ <IPv6-адрес_1>-<IPv6-адрес_2> – диапазон IPv6-адресов;
- IPv6-адрес – вывод пакетов с указанным IPv6-адресом источника или приемника. Формат: список следующих элементов:
  - ✔ <IPv6-адрес> – IPv6-адрес;
  - ✔ <IPv6-префикс>/<N> – IPv6- префикс сети, где <N> – длина префикса;
  - ✔ <IPv6-адрес_1>-<IPv6-адрес_2> – диапазон IPv6-адресов;

- `Порт источника` – вывод пакетов с указанным номером порта источника. Формат: список следующих элементов:
  - ✔ `<номер_порта>` – номер порта;
  - ✔ `<номер_порта_1>-<номер_порта_2>` – диапазон номеров портов;
- `Порт сервера` – вывод пакетов с указанным номером порта приемника. Формат: список следующих элементов:
  - ✔ `<номер_порта>` – номер порта;
  - ✔ `<номер_порта_1>-<номер_порта_2>` – диапазон номеров портов;
- `Порт` – вывод пакетов с указанным номером порта источника или приемника. Формат: список следующих элементов:
  - ✔ `<номер_порта>` – номер порта;
  - ✔ `<номер_порта_1>-<номер_порта_2>` – диапазон номеров портов;
- `Время регистрации пакета` – вывод пакетов, зарегистрированных в указанном интервале времени;
- `Сортировка по времени` – выбор порядка сортировки пакетов по времени их регистрации. Возможна следующая сортировка:
  - ✔ **по убыванию** – последний зарегистрированный пакет будет показана первым;
  - ✔ **по возрастанию** – последний зарегистрированный пакет будет показана последним;
- `Записей на страницу` – максимальное количество записей, выводимых на одной странице. Все записи, предназначенные для просмотра, разделяются на страницы, в каждой из которых содержится не более указанного количества записей.

Кнопка **Показать** служит для вывода записей регистрации сессий в соответствии с:

- указанными критериями выборки;
- указанным порядком сортировки;
- указанным максимальным числом записей на одной странице.

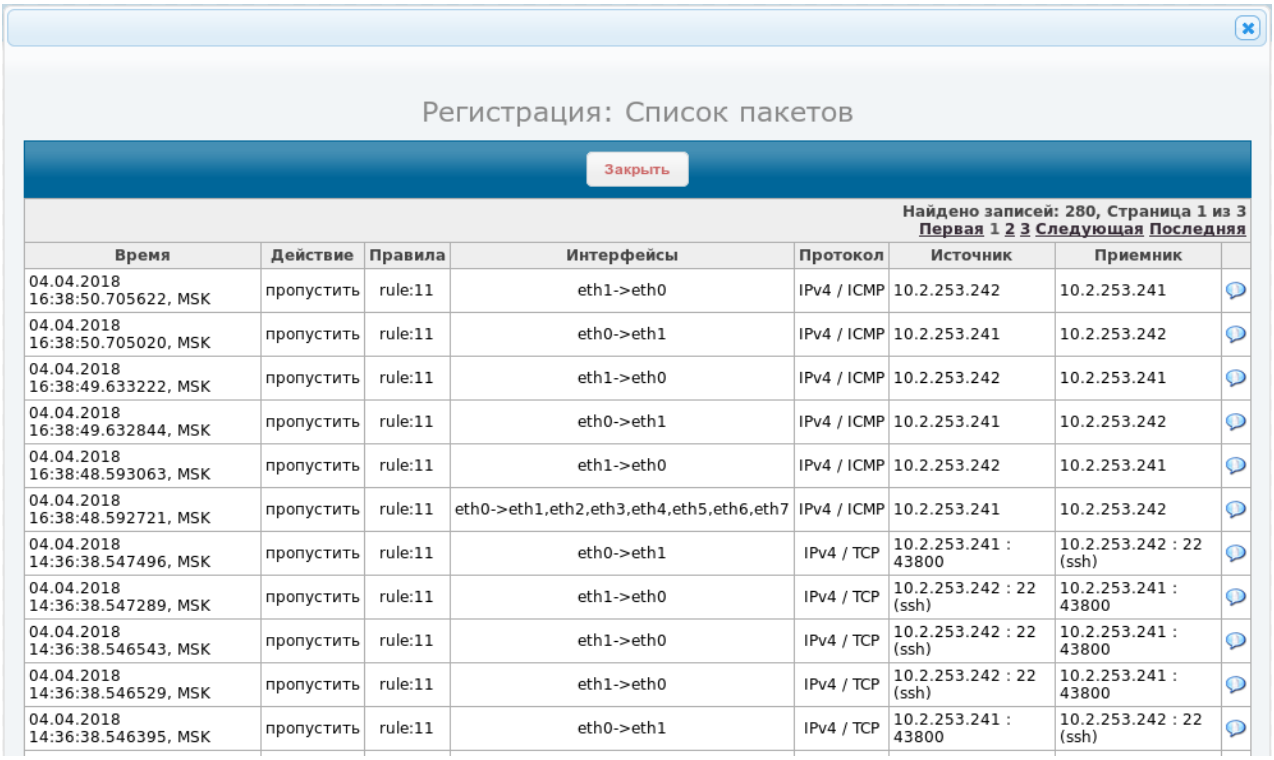
По умолчанию выводятся все записи регистрации пакетов, отсортированные по убыванию времени регистрации (последние – вначале). На одной странице выводится не более **100** записей.

Максимальное число записей регистрации пакетов – **10000**. Данное число записей выделено в сумме на пакеты и сессии (суммарное число записей регистрации пакетов и сессий не может превышать **10000**). По достижении этого числа записей начинается циклическая перезапись: новые записи регистрации заменяют старые.

Следующие пары критериев выборки записей регистрации пакетов являются запрещенными:

- любой из: **IPv4-адрес**, **IPv4-адрес источника**, **IPv4-адрес приемника** и любой из: **IPv6-адрес**, **IPv6-адрес источника**, **IPv6-адрес приемника**;
- **IPv4-адрес** и любой из: **IPv4-адрес источника**, **IPv4-адрес приемника**;
- **IPv6-адрес** и любой из: **IPv6-адрес источника**, **IPv6-адрес приемника**;
- **Порт** и любой из: **Порт источника**, **Порт приемника**.

По нажатию на кнопку **Показать** открывается модальное окно “Регистрация: Список пакетов”. Пример фрагмента такого окна приведен на рисунке 4.146, стр. 345.



Регистрация: Список пакетов

Закрыть

Найдено записей: 280, Страница 1 из 3
Первая 1 2 3 Следующая Последняя

Время	Действие	Правила	Интерфейсы	Протокол	Источник	Приемник	
04.04.2018 16:38:50.705622, MSK	пропустить	rule:11	eth1->eth0	IPv4 / ICMP	10.2.253.242	10.2.253.241	
04.04.2018 16:38:50.705020, MSK	пропустить	rule:11	eth0->eth1	IPv4 / ICMP	10.2.253.241	10.2.253.242	
04.04.2018 16:38:49.633222, MSK	пропустить	rule:11	eth1->eth0	IPv4 / ICMP	10.2.253.242	10.2.253.241	
04.04.2018 16:38:49.632844, MSK	пропустить	rule:11	eth0->eth1	IPv4 / ICMP	10.2.253.241	10.2.253.242	
04.04.2018 16:38:48.593063, MSK	пропустить	rule:11	eth1->eth0	IPv4 / ICMP	10.2.253.242	10.2.253.241	
04.04.2018 16:38:48.592721, MSK	пропустить	rule:11	eth0->eth1,eth2,eth3,eth4,eth5,eth6,eth7	IPv4 / ICMP	10.2.253.241	10.2.253.242	
04.04.2018 14:36:38.547496, MSK	пропустить	rule:11	eth0->eth1	IPv4 / TCP	10.2.253.241 : 43800	10.2.253.242 : 22 (ssh)	
04.04.2018 14:36:38.547289, MSK	пропустить	rule:11	eth1->eth0	IPv4 / TCP	10.2.253.242 : 22 (ssh)	10.2.253.241 : 43800	
04.04.2018 14:36:38.546543, MSK	пропустить	rule:11	eth1->eth0	IPv4 / TCP	10.2.253.242 : 22 (ssh)	10.2.253.241 : 43800	
04.04.2018 14:36:38.546529, MSK	пропустить	rule:11	eth1->eth0	IPv4 / TCP	10.2.253.242 : 22 (ssh)	10.2.253.241 : 43800	
04.04.2018 14:36:38.546395, MSK	пропустить	rule:11	eth0->eth1	IPv4 / TCP	10.2.253.241 : 43800	10.2.253.242 : 22 (ssh)	

Рисунок 4.146: Фрагмент окна “Регистрация: Список пакетов”

Вверху окна расположены:

- кнопка **Закрыть** для закрытия окна
- общее число выбранных записей;
- элементы навигации для переключения между страницами вывода записей регистрации.

В нижней части окна (не показаны на рисунке 4.146, стр. 345) для удобства администратора продублированы:

- кнопка **Закрыть**;
- элементы навигации для переключения между страницами вывода записей регистрации.

Записи регистрации пакетов выводятся в форме таблицы со следующими полями:

- Время – время регистрации пакета;
- Действие – действие, примененное к пакету;
- Правила – цепочка правил фильтрации, примененных к пакету;
- Интерфейсы – входной и выходной интерфейсы (выходной интерфейс – только в случае действия пропустить);
- Протокол – протокол пакета. В случае, если протокол сетевого уровня – IPv4 или IPv6, также указывается инкапсулированный в него протокол (например, **IPv4 / ICMP** или **IPv4 / TCP**);

- Источник – адресная информация источника:
  - ✔ IP-адрес источника;
  - ✔ порт – для протоколов TCP и UDP;
- Приемник: адресная информация приемника:
  - ✔ IP-адрес;
  - ✔ порт – для протоколов TCP и UDP;

Последним полем таблицы является безымянное поле, в котором для каждой записи размещена иконка – открытие окна детальной информации по записи регистрации пакета. Пример такого окна приведен на рисунке 4.150, стр. 352.

Регистрация: Подробная информация о пакете

Информация о пакете

Время	Действие	Правила	Интерфейсы	Номер сессии	Ошибка	Состояние сессии	Приоритет
04.04.2018 14:36:38.546008, MSK	пропустить	rule:11	eth1 -> eth0	2.3		сессия установлена	базовый

Заголовок Ethernet

Тип кадра	Протокол	VLAN ID	MAC-адрес источника	MAC-адрес приемника
Ethernet II	IPv4/TCP		00:0c:29:b7:34:ec	00:0c:29:26:d0:5d

Заголовок IPv4

TOS/DSCP	Длина сегмента	Идентификатор	Фрагментация (MF, DF, Offset)	TTL	Протокол	Контрольная сумма	IP-адрес источника	IP-адрес приемника
00010000	228	0xf0a4	0, 1, 0	64	6 (tcp)	0x3977	10.2.253.242	10.2.253.241

Заголовок TCP

Порт источника	Порт приемника	Номер последовательности	Номер подтверждения	Смещение данных	Флаги TCP	Окно TCP	Контрольная сумма
22 (ssh)	43800	2502713346	688285459	32	ACK,PUSH	1040	0x31e8

Прикладные данные

```
E5 6F E7 94 B9 0F 45 0E 65 04 1A 1C 2C 3C D0 1F
B5 02 E0 49 D0 AA FB 5D 2B A6 CA D1 FE 3D 75 44
BC B9 25 B3 14 5F 54 FF BD 1C 95 B4 83 68 4F 22
E8 59 44 EF BF 79 18 18 50 DB 0B 64 CF 48 9B F7
25 3A 9F F6 AD 0D 6F 92 04 15 2A 9D F6 38 59 AF
04 6E
```

```
. o . . . . E . e . . . , < . .
. . . I . . . ] + . . . . = u D
. . % . . _ T . . . . . . h O "
. Y D . . y . . P . . d . H . .
% : . . . . o . . . * . . 8 Y .
. n
```

Закрыть

Рисунок 4.147: Пример окна подробной информации о записи регистрации пакета

В окне подробной информации о пакете (на примере IPv4-пакета) доступны следующие дополнительные сведения, которые не выводятся в таблице пакетов:

- Заголовок Ethernet:
  - ✔ Тип кадра;
  - ✔ VLAN ID – идентификатор VLAN;
  - ✔ MAC-адрес источника;
  - ✔ MAC-адрес приемника;
- Заголовок IPv4:

- ✔ TOS/DSCP – значение поля флагов TOS/DSCP в двоичном формате;
- ✔ Длина сегмента;
- ✔ Идентификатор;
- ✔ Фрагментация (MF, DF, Offset) – значения полей, относящихся к фрагментации (MF, DF, Offset) соответственно;
- ✔ TTL;
- ✔ Контрольная сумма – контрольная сумма пакета;

- Заголовок TCP:
  - ✔ Номер последовательности;
  - ✔ Номер подтверждения;
  - ✔ Смещение данных;
  - ✔ Флаги TCP – список установленных флагов TCP;
  - ✔ Окно TCP – размер окна TCP;
  - ✔ Контрольная сумма – контрольная сумма TCP;
  - ✔ Прикладные данные – данные в TCP-сообщении (если данные нет, то столбцы поля не заполнены):
    - в левом столбце – последовательность байт поля данных TCP-сообщения в шестнадцатеричном виде;
    - в правом столбце – последовательность байт поля данных TCP-сообщения в виде последовательности ASCII-символов.

4.5.3. Регистрация: Сессии

Страница “Регистрация: Сессии” представляет собой форму для задания критериев выборки записей регистрации сессий, а также выбора других параметров вывода записей регистрации сессий. Фрагмент страницы “Регистрация: Сессии” приведен на рисунке 4.148, стр. 348.

Страница “Регистрация: Сессии” содержит следующие элементы ввода данных:

- Номер сессии – вывод сессии с указанным номером (идентификатором);
- Интерфейс клиента – вывод сессий с указанным интерфейсом клиента. Допускается множественный выбор;
- Интерфейс сервера – вывод сессий с указанным интерфейсом сервера. Допускается множественный выбор;
- IPv4-адрес клиента – вывод сессий с указанным IP-адресом клиента. Формат – список следующих элементов:

✔ <IP-адрес> – IPv4-адрес;

✔ <IP-адрес>/<N> – IPv4-адрес/маска в виде префикса;

✔ <IP-адрес>/<IP-маска> – IPv4-адрес/маска;

✔ <IP-адрес_1>-<IP-адрес_2> – диапазон IPv4-адресов;

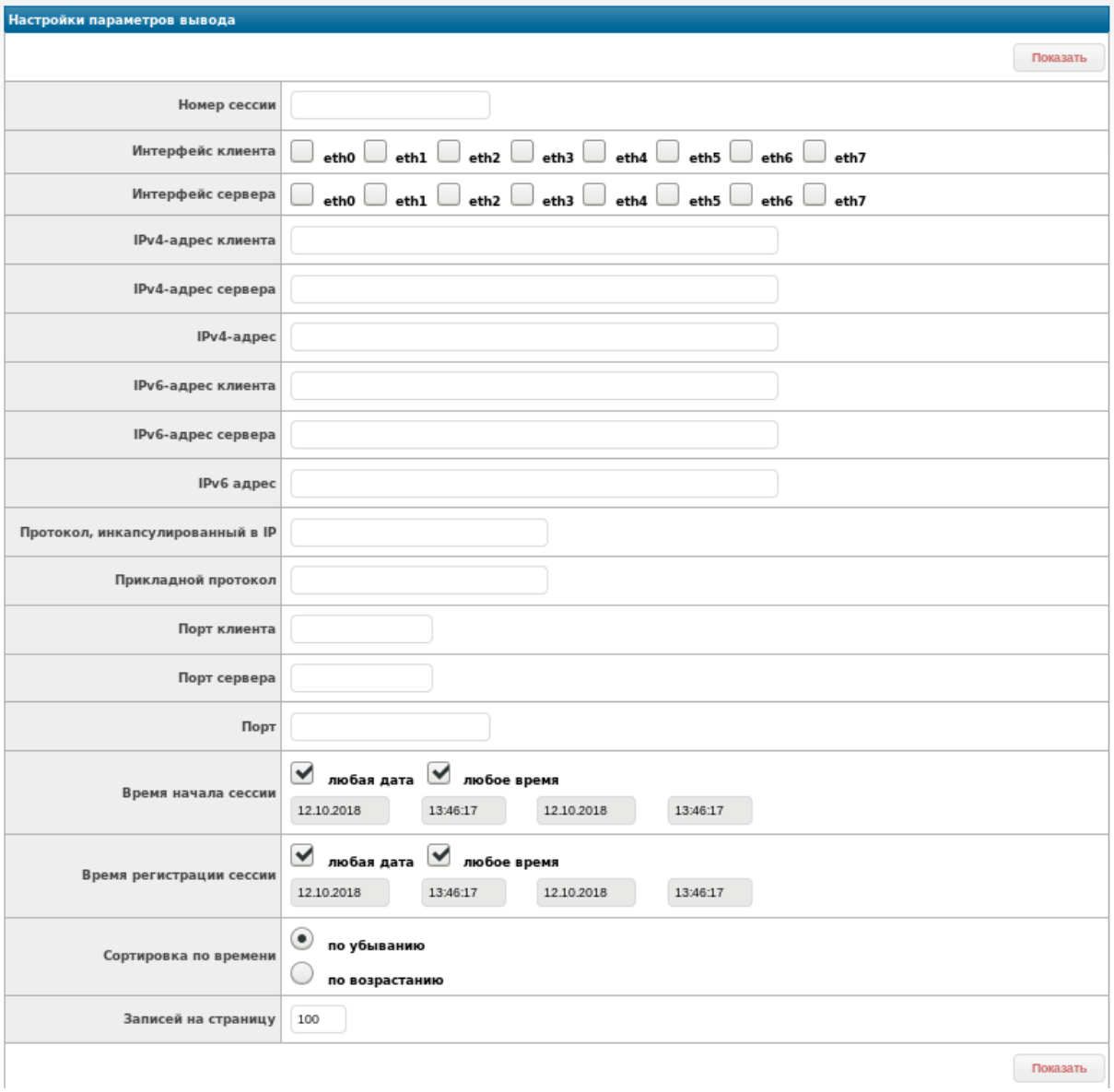


Рисунок 4.148: Фрагмент страницы “Регистрация: Сессии”

- IPv4-адрес сервера – вывод сессий с указанным IP-адресом сервера. Формат – список следующих элементов:

  ✔ <IP-адрес> – IPv4-адрес;

  ✔ <IP-адрес>/<N> – IPv4-адрес/маска в виде префикса;

  ✔ <IP-адрес>/<IP-маска> – IPv4-адрес/маска;

  ✔ <IP-адрес_1>-<IP-адрес_2> – диапазон IPv4-адресов;

- IPv4-адрес – вывод сессий с указанным IP-адресом клиента или сервера. Формат – список следующих элементов:
  - ✔ <IP-адрес> – IPv4-адрес;
  - ✔ <IP-адрес>/<N> – IPv4-адрес/маска в виде префикса;
  - ✔ <IP-адрес>/<IP-маска> – IPv4-адрес/маска;
  - ✔ <IP-адрес_1>-<IP-адрес_2> – диапазон IPv4-адресов;
- IPv6-адрес клиента – вывод сессий с указанным IPv6-адресом клиента. Формат – список следующих элементов:
  - ✔ <IPv6-адрес>: IPv6-адрес;
  - ✔ <IPv6-префикс>/<N>: IPv6-префикс сети, где <N> – длина префикса;
  - ✔ <IPv6-адрес_1>-<IPv6-адрес_2>: диапазон IPv6-адресов;
- IPv6-адрес сервера – вывод сессий с указанным IPv6-адресом сервера. Формат – список следующих элементов:
  - ✔ <IPv6-адрес> – IPv6-адрес;
  - ✔ <IPv6-префикс>/<N> – IPv6- префикс сети, где <N> – длина префикса;
  - ✔ <IPv6-адрес_1>-<IPv6-адрес_2> – диапазон IPv6-адресов;
- IPv6-адрес – вывод сессий с указанным IPv6-адресом клиента или сервера. Формат – список следующих элементов:
  - ✔ <IPv6-адрес> – IPv6-адрес;
  - ✔ <IPv6-префикс>/<N> – IPv6- префикс сети, где <N> – длина префикса;
  - ✔ <IPv6-адрес_1>-<IPv6-адрес_2> – диапазон IPv6-адресов;
- Протокол, инкапсулированный в IP: вывод сессий с указанным протоколом. Формат – <номер_протокола>|<имя_протокола>. Например, **tcp** или **6**.
- Прикладной протокол – вывод сессий с указанным прикладным протоколом. Формат – <номер_протокола>|<имя_протокола>. Например, **ssh** или **22**.
- Порт клиента – вывод сессий с указанным номером порта клиента. Формат – список следующих элементов:
  - ✔ <номер_порта> – номер порта;
  - ✔ <номер_порта_1>-<номер_порта_2> – диапазон номеров портов;
- Порт сервера – вывод сессий с указанным номером порта сервера. Формат – список следующих элементов:
  - ✔ <номер_порта> – номер порта;
  - ✔ <номер_порта_1>-<номер_порта_2> – диапазон номеров портов;
- Порт – вывод сессий с указанным номером порта клиента или сервера. Формат – список следующих элементов:

✔ <номер_порта> – номер порта;

✔ <номер_порта_1>-<номер_порта_2> – диапазон номеров портов;

- Время начала сессии – вывод сессий, созданных в указанном интервале времени;
- Время регистрации сессии – вывод сессий, зарегистрированных (завершившихся) в указанном интервале времени.
- Сортировка по времени – выбор порядка сортировки сессий по времени их регистрации. Возможна следующая сортировка:

  ✔ **по убыванию** – последняя зарегистрированная сессия будет показана первой;

  ✔ **по возрастанию** – последняя зарегистрированная сессия будет показана последней;
- Записей на страницу – максимальное количество записей, выводимых на одной странице. Все записи, предназначенные для просмотра, разделяются на страницы, в каждой из которых содержится не более указанного количества записей.

Кнопка **Показать** служит для вывода записей регистрации сессий в соответствии с:

- указанными критериями выборки;
- указанным порядком сортировки;
- указанным максимальным числом записей на одной странице.

По умолчанию выводятся все записи регистрации сессий, отсортированные по убыванию времени регистрации (последние – вначале). На одной странице выводится не более **100** записей.

Максимальное число записей регистрации сессий – **10000**. Данное число записей выделено в сумме на пакеты и сессии (суммарное число записей регистрации пакетов и сессий не может превышать **10000**). По достижении этого числа записей начинается циклическая перезапись: новые записи регистрации заменяют старые.

Следующие пары критериев выборки записей регистрации сессий являются запрещенными:

- любой из: **IPv4-адрес**, **IPv4-адрес клиента**, **IPv4-адрес сервера** и любой из: **IPv6-адрес**, **IPv6-адрес клиента**, **IPv6-адрес сервера**;
- **IPv4-адрес** и любой из: **IPv4-адрес клиента**, **IPv4-адрес сервера**;
- **IPv6-адрес** и любой из: **IPv6-адрес клиента**, **IPv6-адрес сервера**;
- **Порт** и любой из: **Порт клиента**, **Порт сервера**.

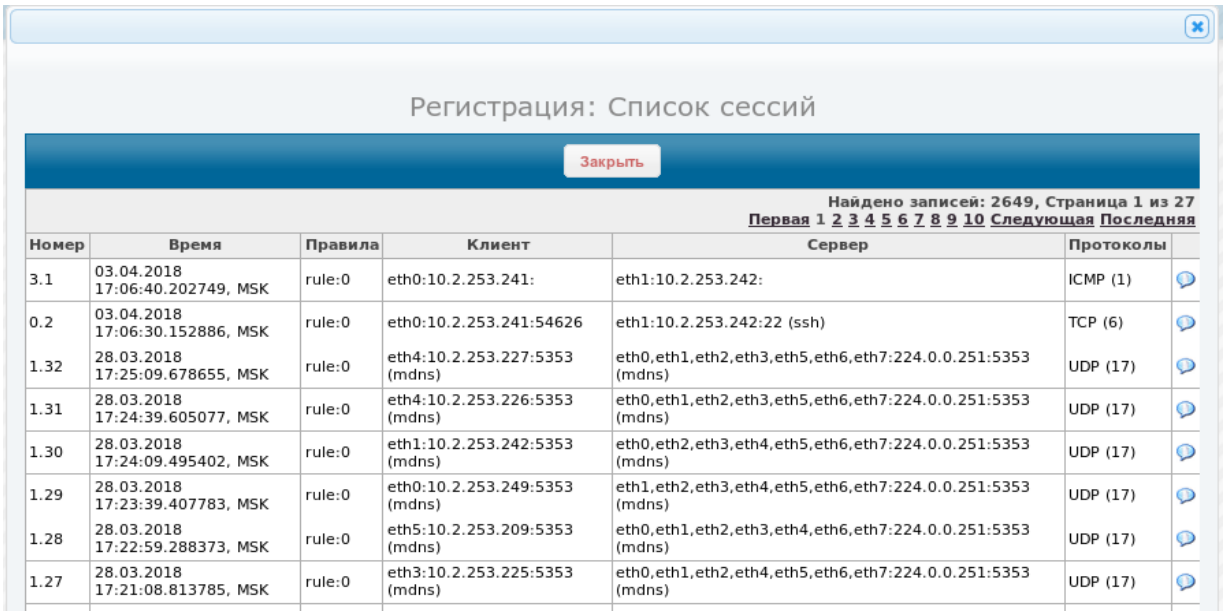
По нажатию на кнопку `Показать` открывается модальное окно `Регистрация: Список сессий`. Пример фрагмента такого окна приведен на рисунке 4.149, стр. 351.

Вверху окна расположены:

- кнопка **Закрыть** для закрытия окна
- общее число выбранных записей;
- элементы навигации для переключения между страницами вывода записей регистрации.

В нижней части окна (не показаны на рисунке 4.149, стр. 351) для удобства администратора продублированы:

- кнопка **Закрыть**;
- элементы навигации для переключения между страницами вывода записей регистрации.



Номер	Время	Правила	Клиент	Сервер	Протоколы
3.1	03.04.2018 17:06:40.202749, MSK	rule:0	eth0:10.2.253.241:	eth1:10.2.253.242:	ICMP (1)
0.2	03.04.2018 17:06:30.152886, MSK	rule:0	eth0:10.2.253.241:54626	eth1:10.2.253.242:22 (ssh)	TCP (6)
1.32	28.03.2018 17:25:09.678655, MSK	rule:0	eth4:10.2.253.227:5353 (mdns)	eth0,eth1,eth2,eth3,eth5,eth6,eth7:224.0.0.251:5353 (mdns)	UDP (17)
1.31	28.03.2018 17:24:39.605077, MSK	rule:0	eth4:10.2.253.226:5353 (mdns)	eth0,eth1,eth2,eth3,eth5,eth6,eth7:224.0.0.251:5353 (mdns)	UDP (17)
1.30	28.03.2018 17:24:09.495402, MSK	rule:0	eth1:10.2.253.242:5353 (mdns)	eth0,eth2,eth3,eth4,eth5,eth6,eth7:224.0.0.251:5353 (mdns)	UDP (17)
1.29	28.03.2018 17:23:39.407783, MSK	rule:0	eth0:10.2.253.249:5353 (mdns)	eth1,eth2,eth3,eth4,eth5,eth6,eth7:224.0.0.251:5353 (mdns)	UDP (17)
1.28	28.03.2018 17:22:59.288373, MSK	rule:0	eth5:10.2.253.209:5353 (mdns)	eth0,eth1,eth2,eth3,eth4,eth6,eth7:224.0.0.251:5353 (mdns)	UDP (17)
1.27	28.03.2018 17:21:08.813785, MSK	rule:0	eth3:10.2.253.225:5353 (mdns)	eth0,eth1,eth2,eth4,eth5,eth6,eth7:224.0.0.251:5353 (mdns)	UDP (17)

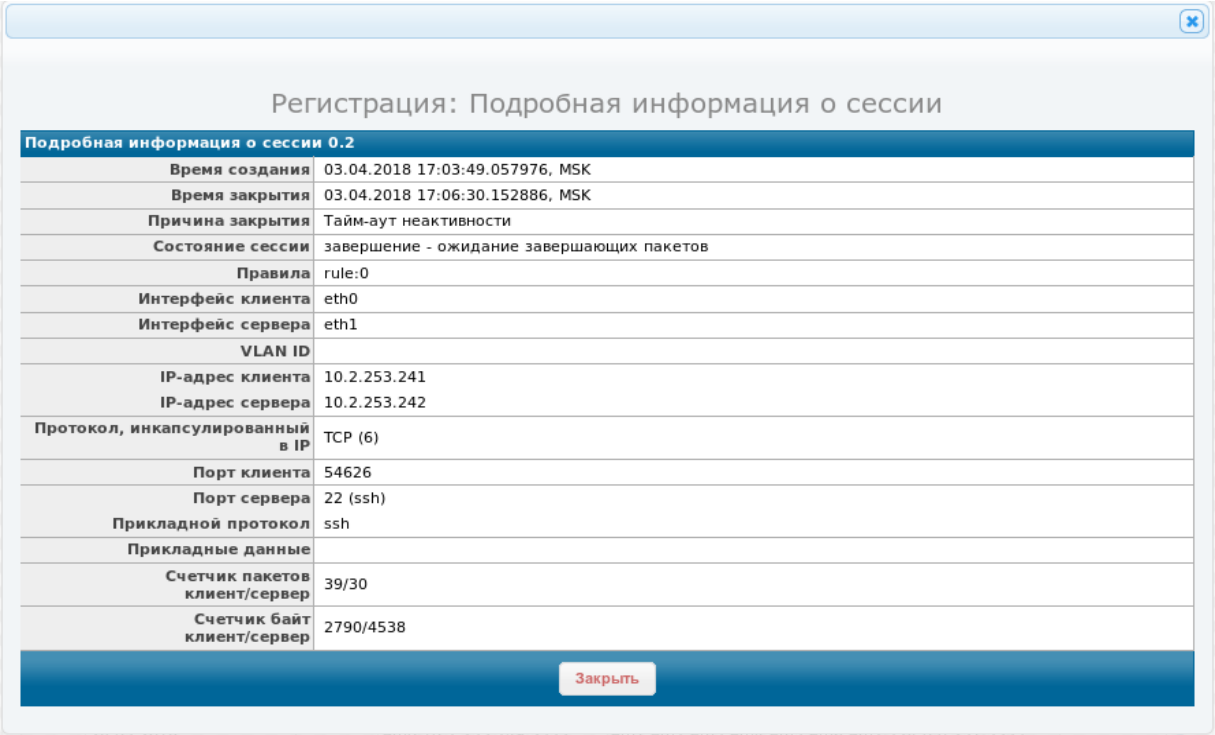
Рисунок 4.149: Фрагмент окна Регистрация: Список сессий

Записи регистрации сессий выводятся в форме таблицы со следующими полями:

- `Номер` – идентификатор сессии;
- `Время` – время регистрации (завершения) сессии;
- `Правила` – цепочка правил фильтрации, применявшихся к пакетам данной сессии (в приведенном примере цепочка состоит из одного правила: `rule:0` – глобальное общее правило, по которому была создана сессия);
- `Клиент` – адресная информация клиента (инициатора соединения):
  - ✔ фильтрующий интерфейс;
  - ✔ IP-адрес;
  - ✔ порт для протоколов TCP и UDP;

- `Сервер` – адресная информация сервера:
  - ✔ фильтрующий интерфейс (возможен список интерфейсов в случае если IP-адрес сервера — групповой);
  - ✔ IP-адрес;
  - ✔ порт для протоколов TCP и UDP;
- `Протоколы` – имя и код протокола, инкапсулированного в IP-пакет;

Последним полем таблицы является безымянное поле, в котором для каждой записи размещена иконка – открытие окна детальной информации по записи регистрации сессии. Пример такого окна приведен на рисунке 4.150, стр. 352.



Регистрация: Подробная информация о сессии

Подробная информация о сессии 0.2	
Время создания	03.04.2018 17:03:49.057976, MSK
Время закрытия	03.04.2018 17:06:30.152886, MSK
Причина закрытия	Тайм-аут неактивности
Состояние сессии	завершение - ожидание завершающих пакетов
Правила	rule:0
Интерфейс клиента	eth0
Интерфейс сервера	eth1
VLAN ID	
IP-адрес клиента	10.2.253.241
IP-адрес сервера	10.2.253.242
Протокол, инкапсулированный в IP	TCP (6)
Порт клиента	54626
Порт сервера	22 (ssh)
Прикладной протокол	ssh
Прикладные данные	
Счетчик пакетов клиент/сервер	39/30
Счетчик байт клиент/сервер	2790/4538

Закрыть

Рисунок 4.150: Пример окна подробной информации о записи регистрации сессии

В окне подробной информации о сессии доступны следующие дополнительные сведения:

- `Причина закрытия` – причина закрытия сессии;
- `Состояние сессии` – состояние, в котором сессия была закрыта;
- `VLAN ID` – идентификатор ID пакетов сессии (при отсутствии – пустая строка);
- `Прикладной протокол` – название прикладного протокола (при отсутствии – пустая строка);
- `Прикладные данные` – данные прикладного уровня (только для протоколов: HTTP, FTP и SMTP);
- `Счетчик пакетов клиент/сервер` – счетчики пакетов, отправленных клиентом и сервером в рамках данной сессии соответственно;

- Счетчик байт клиент/сервер – счетчики суммарного количества байт в пакетах, отправленных клиентом и сервером в рамках данной сессии соответственно.

4.6. Отладка

Пункт Отладка основного меню WEB-интерфейса позволяет перейти к странице Отладка: Командная строка. Данная страница предоставляет возможность выполнения команд командного языка МЭ ССПТ-4А1 без обработки их вывода WEB-интерфейсом. Эта возможность позволяет убедиться в корректности выполнения команд на основании результата выполнения команды в текстовой форме, содержащего как минимум одно диагностическое сообщение и, для некоторых команд, строки данных.

Пример страницы Отладка: Командная строка, в результате ввода и выполнения команды **policy list** (просмотр списка дополнительных политик доступа), приведен на рисунке 4.151, стр. 353.

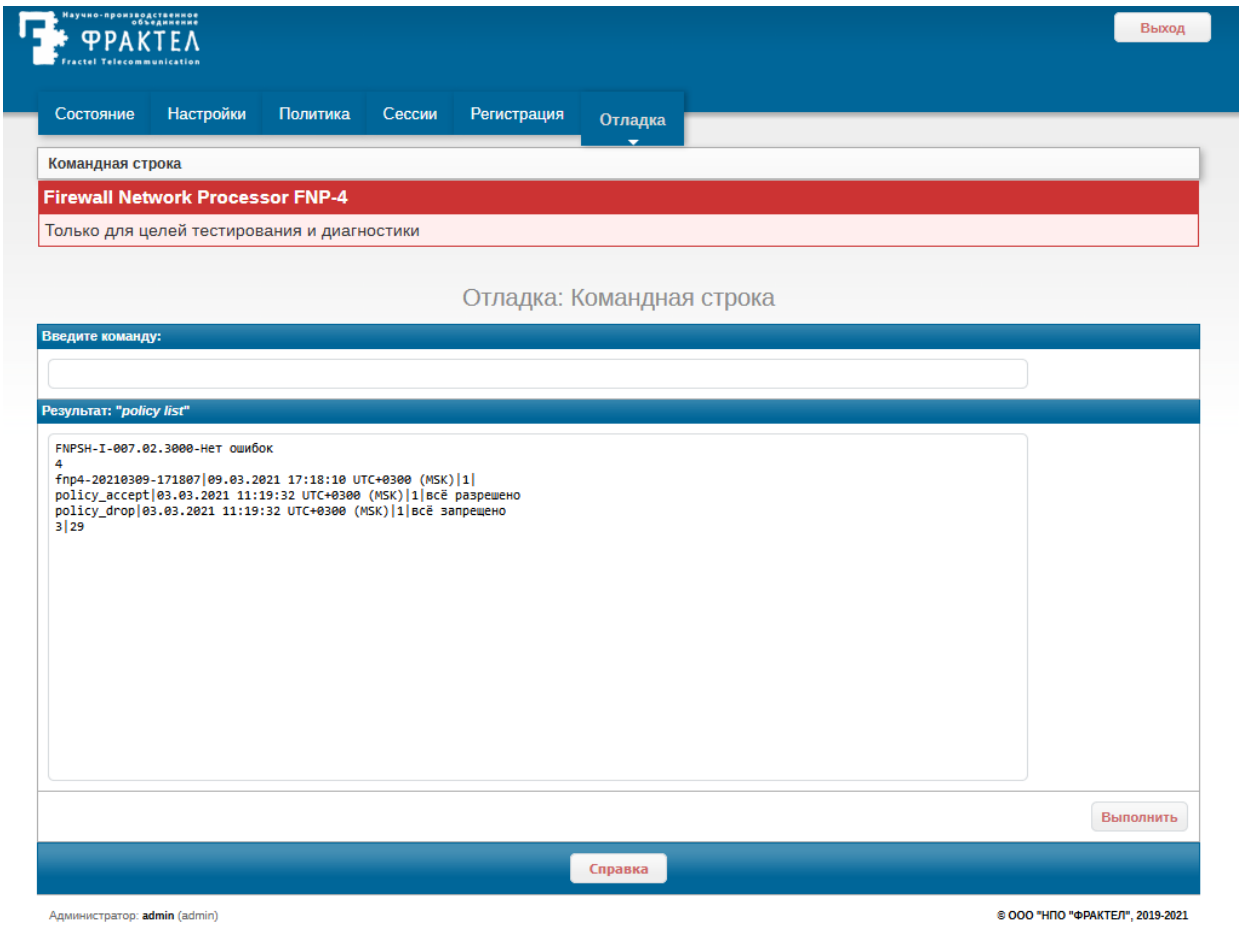


Рисунок 4.151: Пример страницы “Отладка: Командная строка”

Страница Отладка: Командная строка содержит:

- поле ввода команды командного языка МЭ ССПТ-4А1 (под надписью: Введите команду);

- поле вывода результата выполнения команды (под надписью: `Результат:`);
- кнопку `Выполнить`: по нажатию кнопки выполняется команда, введенная в поле ввода, результат выполнения команды выводится в поле вывода результата.

В приведенном примере (рисунок 4.151, стр. 353) результат выполнения команды **`policy list`** содержит:

- диагностическое сообщение об успешном выполнении команды;
- число строк данных, следующих ниже (`3`);
- три строки данных, предоставленных по команде.

5. SNMP-интерфейс администратора

SNMP-интерфейс администратора может быть использован для:

- просмотра значений переменных дерева объектов MIB через программу, относящуюся к категории MIB-браузеров;
- периодического удаленного “снятия” статистических показателей работы МЭ ССПТ-4А1, имеющихся в дереве объектов MIB (MIB-модуля) МЭ ССПТ-4А1.

Работа с МЭ ССПТ-4А1 через SNMP-интерфейс возможна только по протоколу SNMPv3 (третья версия протокола SNMP), так как только данная версия протокола, к моменту написания этой документации, обеспечивает надлежащий уровень безопасности за счет поддержки:

- аутентификации пользователей SNMP-агента на основе алгоритмов хеширования (без передачи паролей по сети в открытом виде).
- преобразования данных сообщений протокола SNMP (запросов и ответов).

Для работы с МЭ ССПТ-4А1 через SNMP-интерфейс необходимо ПО, относящееся к категории MIB-браузеров. MIB-браузер обеспечивает:

- навигацию по дереву объектов MIB.
- просмотр значений объектов MIB;
- установку значений объектов MIB, имеющих права доступа “чтение/запись”.

До начала использования любого MIB-браузера требуется выполнить процедуру его предварительной настройки, состоящей из следующих действий:

1) Копирование файла описания дерева объектов MIB (MIB-модуля) МЭ ССПТ-4А1 в один из каталогов поиска MIB-модулей, заданных в настройках MIB-бразуера.
2) Загрузка MIB-модуля, описывающего все объекты устройства, к которым можно обращаться по протоколу SNMP;
3) Создание учетной записи для аутентификации и преобразования SNMP-запросов от MIB-браузера к SNMP-агенту и ответов в обратном направлении;
4) Создание профиля SNMP-агента, функционирующего на целевом МЭ ССПТ-4А1:
   4.1) установка адресной информации SNMP-агента (IP-адрес, UDP-порт);
   4.2) установка атрибутов протокола SNMPv3 соответствующих настройкам SNMP-агента устройства;
   4.3) привязка ранее созданной учетной записи пользователя к профилю SNMP-агента.

Описание MIB-модуля МЭ ССПТ-4А1 (состав и назначение переменных в каждом узле дерева объектов MIB МЭ ССПТ-4А1) приведено в приложении Ж, стр. 547.

Далее в данном разделе будет описана процедура предварительной настройки MIB-браузера на примере программы `snmpb`. Данное приложение можно загрузить из Интернет по адресу: `http://sourceforge.net/projects/snmpb/`. Также будут пояснены принципы управления МЭ ССПТ-4А1 через SNMP-интерфейс на примере использования MIB-браузера `snmpb`.

5.1. Предварительная настройка MIB-браузера snmpb

Подразумевается что MIB-браузер `snmpb` установлен и запущен на управляющем ПК. Также подразумевается что не открыто никаких диалоговых окон настроек, только главное окно `snmpb`.

Процедура предварительной настройки MIB-браузера `snmb` требует выполнения следующей последовательности действий:

1) Скопировать файл MIB-модуля МЭ ССПТ-4А1 в один из каталогов поиска MIB-модулей, заданных в настройках `snmpb`. Для того чтобы посмотреть список каталогов поиска MIB-модулей необходимо в главном меню выбрать подменю **`Options`**, в нём пункт **`Preferences`**. В меню окна **`Preferences`** слева выбрать пункт **`Modules`**.
2) Загрузить MIB-модуль МЭ ССПТ-4А1: в главном окне выбрать вкладку **`Modules`**. В области **`Available MIB modules`** выбрать MIB-модуль МЭ ССПТ-4А1 и загрузить его нажав на кнопку со стрелкой вправо (рисунок 5.1, стр. 357).
3) Создать учетную запись пользователя протокола SNMPv3:
   3.1) В главном меню выбрать подменю **`Options`**, в нём пункт **`Manage SNMPv3 USM Profiles`** (рисунок 5.2, стр. 358).

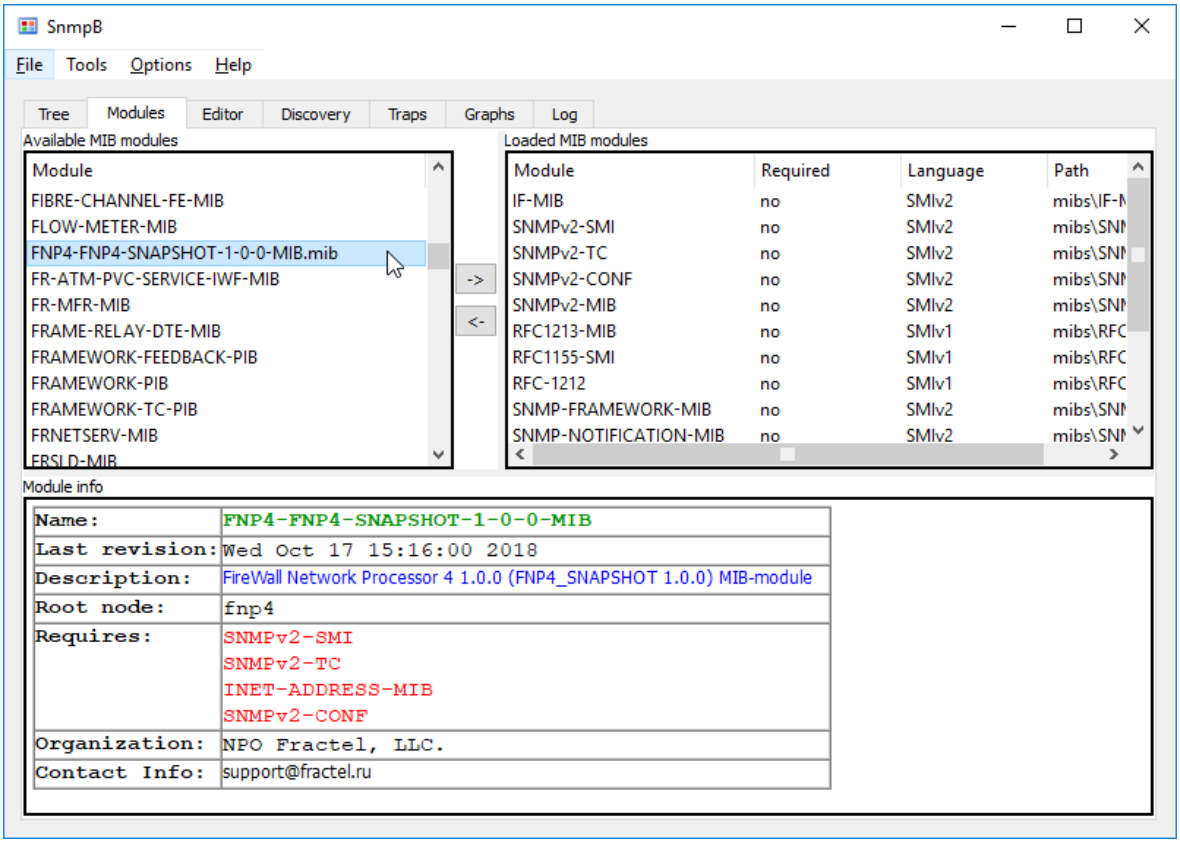


Рисунок 5.1: Загрузка MIB-модуля МЭ ССПТ-4А1

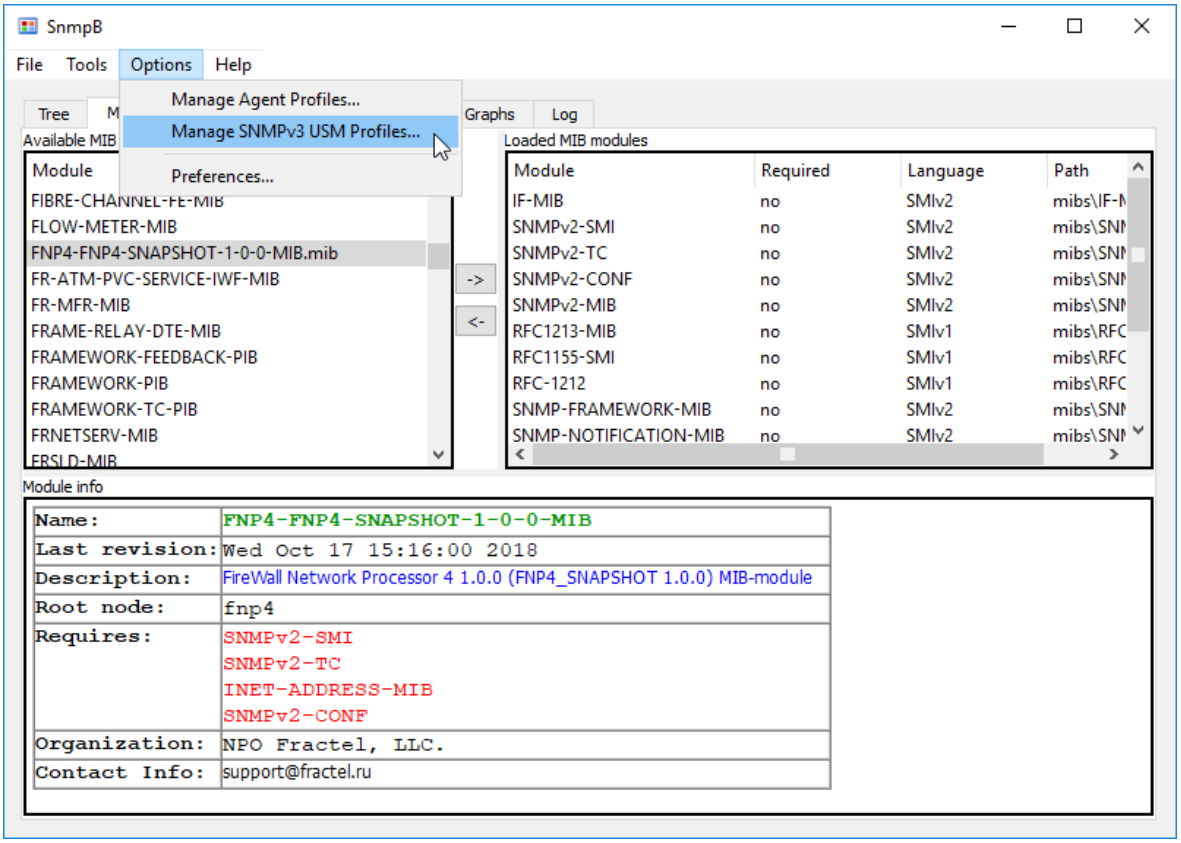


Рисунок 5.2: Открытие окна настроек учетных записей SNMPv3

3.2) В меню окна **`USM Profiles`** кликнуть правой кнопкой мыши по белой области в левой части окна: в появившемся контекстном меню выбрать пункт **`New USM Profile`** (рисунок 5.3, стр. 359).

3.3) Установить атрибуты учетной записи пользователя SNMPv3 (рисунок 5.4, стр. 359):

- `Security User Name` (имя пользователя) – в **`fnpsnmp`**;
- `Authentication Protocol` (протокол аутентификации) – в **`MD5`**;
- `Authentication Password` (пароль аутентификации) – в **`FnpsnmpD`** (пароль по умолчанию);
- `Privacy Protocol` (протокол преобразования) – в **`AES128`**.
- `Privacy Password` (пароль преобразования) – в **`FnpsnmpD`** (пароль по умолчанию);

3.4) Подтвердить создание учетной записи пользователя SNMPv3 с заданными значениями атрибутов, кликнув по кнопке OK в окне **`USM Profiles`** (рисунок 5.4, стр. 359).

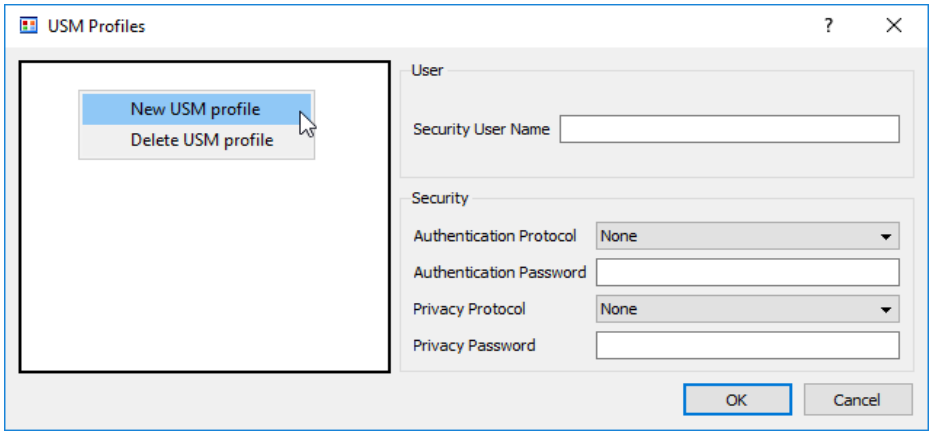


Рисунок 5.3: Добавление новой учетной записи

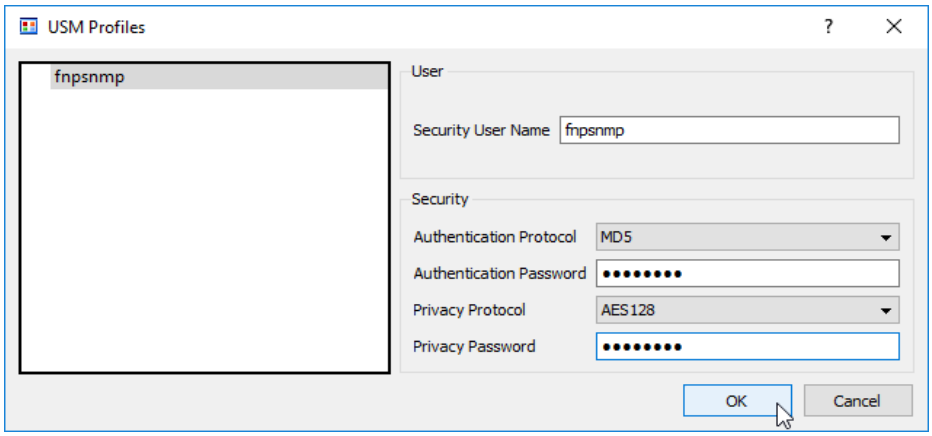


Рисунок 5.4: Установка атрибутов новой учетной записи

4) Создание профиля SNMP-агента, работающего на целевом устройстве:

4.1) В первой (основной) вкладке **`Tree`** главного окна кликнуть по кнопке с изображением инструментов (рисунок 5.5, стр. 360).

4.2) В открывшемся окне профилей SNMP-агентов кликнуть правой кнопкой мыши по белой области в левой части окна, в появившемся контекстном меню выбрать пункт **`New agent profile`** (рисунок 5.6, стр. 361).

4.3) В правой части окна профилей SNMP-агента установить атрибуты только что созданного профиля (рисунок 5.7, стр. 361):

- `Name` – имя для идентификации SNMP-агента (например: **`fnp4`**);
- `Agent Address/Name` – IP-адрес/доменное имя SNMP-агента;
- `Agent Port` – номер UDP-порта SNMP-агента (необходимо оставить значение по-умолчанию: **`161`**).
- `Retries` – число повторных запросов в том случае, если SNMP-агент не отвечает в течение тайм-аута (необходимо оставить значение по умолчанию: **`1`**).

- `Timeout` – тайм-аута ожидания ответа от SNMP-агента (рекомендуется установить значение: **`10`** для возможности получения статистики использования ЦП МЭ ССПТ-4А1: переменные узла `sysCpuStatus`).
- `Supported SNMP version` – версия протокола SNMP, поддерживаемая SNMP-агентом (необходимо установить флаг для значения SNMPv3, остальные флаги снять, если установлены).

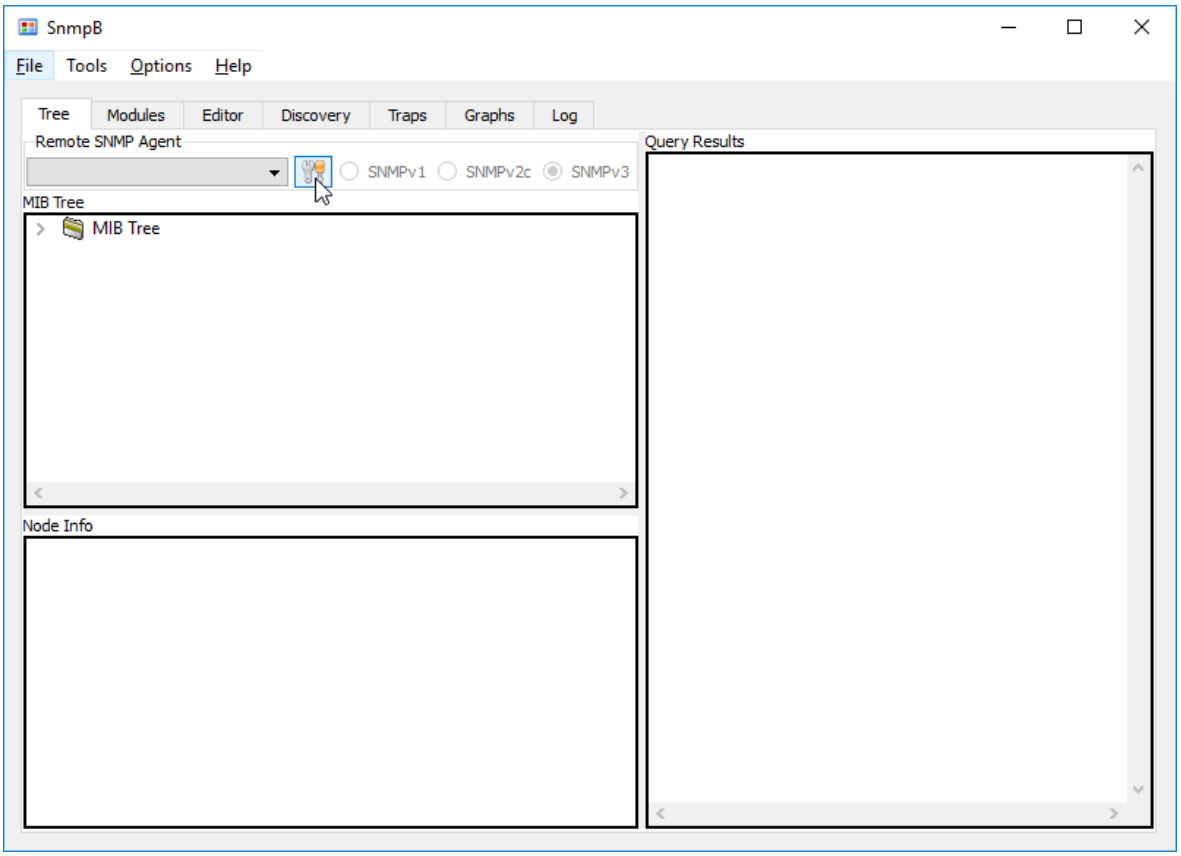


Рисунок 5.5: Открытие окна настроек профилей SNMP-агентов

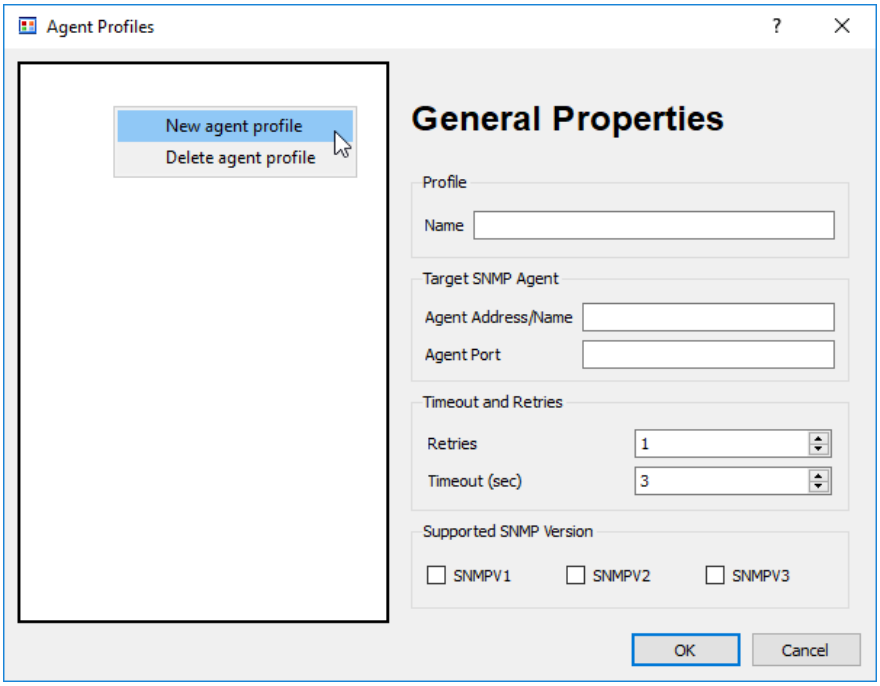


Рисунок 5.6: Создание нового профиля SNMP-агента

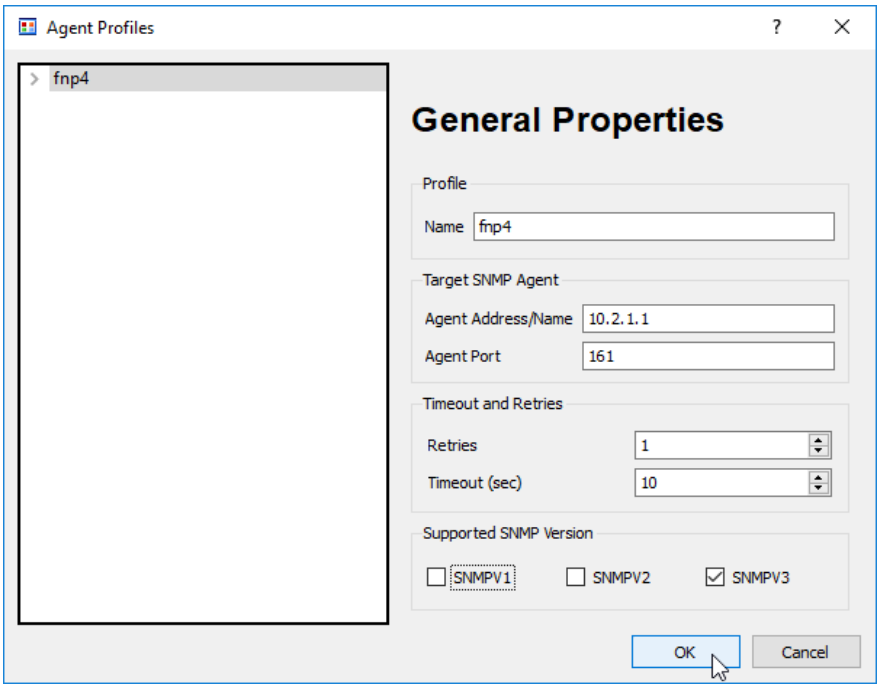


Рисунок 5.7: Установка атрибутов профиля SNMP-агента

5) Привязать созданную ранее учетную запись пользователя SNMPv3 к сконфигурированному выше профилю SNMP-агента:

5.1) Развернуть дерево в левой части окна **`Agent Profiles`**, корнем которого является имя профиля SNMP-агента (`fnp4`) (рисунок 5.8, стр. 362).

5.2) В дереве кликнуть по элементу с именем `SnmpV3`: в правой части окна отобразится форма свойств протокола SNMPv3 (рисунок 5.9, стр. 362), которые необходимо установить:

- В списке **`Security Name`** выбрать имя, ранее созданного пользователя SNMPv3: `fnpsnmp`.

- В списке **Security Level** выбрать значение authPriv (уровень безопасности: “аутентификация и преобразование”).

5.3) Кликнуть по кнопке OK в левом нижнем углу окна **Agent Profiles**, тем самым подтвердив создание нового профиля SNMP-агента со значениями атрибутов, определенными выше (рисунок 5.9, стр. 362).

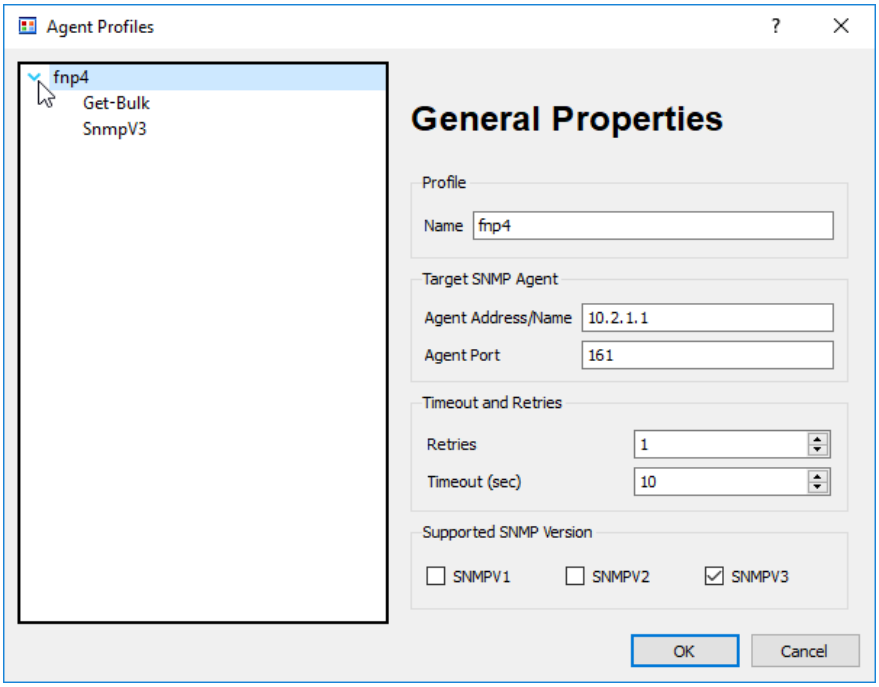


Рисунок 5.8: Переход к форме свойств SNMPv3 в профиле SNMP-агента

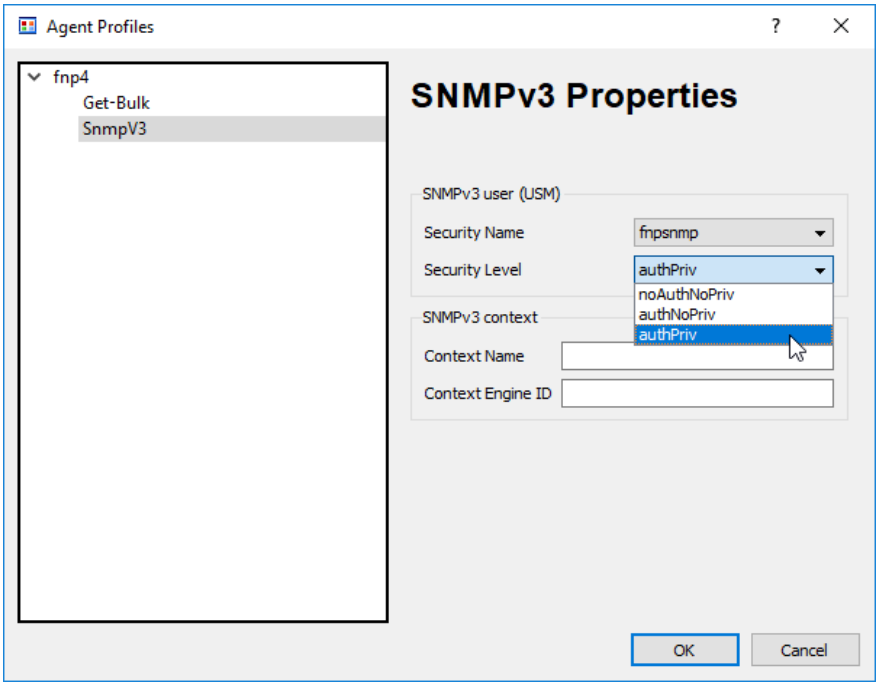


Рисунок 5.9: Настройка свойства протокола SNMPv3 в профиле SNMP-агента

Предварительная настройка MIB-браузера snmpb завершена, программа готова к использованию для работы с МЭ ССПТ-4А1 по протоколу SNMPv3.

5.2. Работа с МЭ ССПТ-4А1. Примеры использования MIB-браузера snmpb

В данном разделе приводятся примеры решения нескольких типовых задач по работе с МЭ ССПТ-4А1 с использованием MIB-браузера snmpb:

- авторизация администратора МЭ ССПТ-4А1 (раздел 5.2.1, стр. 363);
- работа с МЭ ССПТ-4А1:
  - ✔ вывод таблицы filterStatsTable: статистика трафика на фильтрующих интерфейсах МЭ ССПТ-4А1 (раздел 5.2.2, стр. 367);
  - ✔ получение значений всех переменных узла system.sysInfo: сведения об аппаратной конфигурации и версии ПО МЭ ССПТ-4А1 (раздел 5.2.3, стр. 369);
- завершение сеанса работы администратора МЭ ССПТ-4А1 (раздел 5.2.4, стр. 371).

Описание всех объектов MIB-модуля МЭ ССПТ-4А1 приведено в приложении Ж, стр. 547.

5.2.1. Авторизация администратора МЭ ССПТ-4А1

Предполагается, что к моменту выполнения данного этапа MIB-браузер snmpb соответствующим образом сконфигурирован (раздел 5.1, стр. 356).

1) Запустить snmpb.
2) В области MIB Tree развернуть узел (поддерево объектов MIB МЭ ССПТ-4А1) iso.org.dod.internet.private.enterprises.npoRTC.fnp4 (далее для краткости: узел fnp4) дерева объектов MIB и внутри него выбрать узел auth.
3) Кликнуть правой кнопкой мыши по переменной fnp4Uname: в контекстном меню кликнуть по пункту **Set...** (рисунок 5.10, стр. 364).

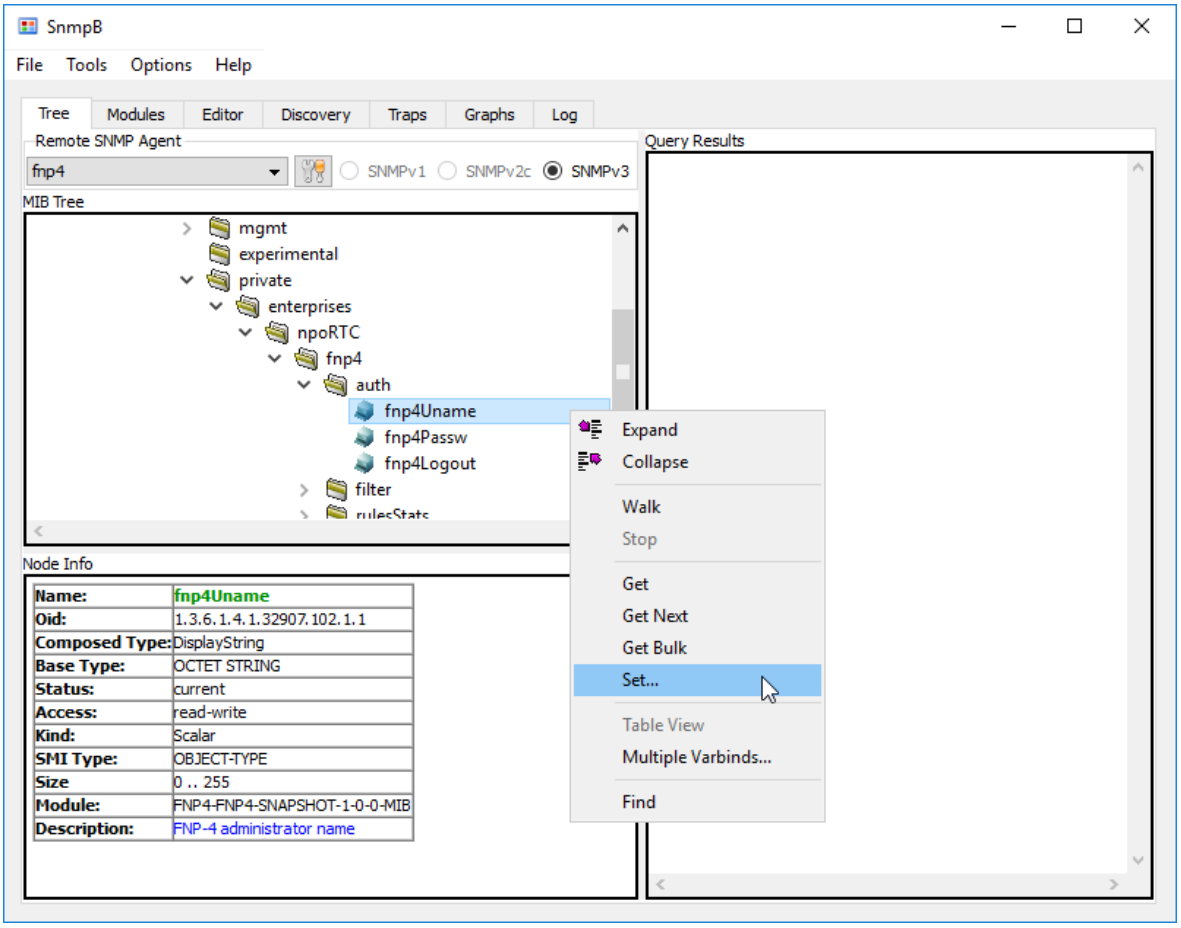


Рисунок 5.10: Контекстное меню переменной fnp4Uname

4) В открывшемся диалоговом окне **`Set`** в поле `Value` ввести значение переменной – имя администратора МЭ ССПТ-4А1, которого необходимо авторизовать. Например, администратор – **`admin`** (рисунок 5.11, стр. 365).
5) В диалоговом окне **`Set`** кликнуть по кнопке **`OK`** (рисунок 5.11, стр. 365). Убедиться, что переменная `fnp4Uname` была успешно установлена: в области **`Query Results`** главного окна должно быть выведено имя установленной переменной, ее новое значение и результат выполнения запроса: **`SNMP set finished`** (рисунок 5.12, стр. 365).
6) Кликнуть правой кнопкой мыши по переменной `fnp4Passw` (также внутри узла `auth`): в контекстном меню кликнуть по пункту **`Set...`** (рисунок 5.12, стр. 365).

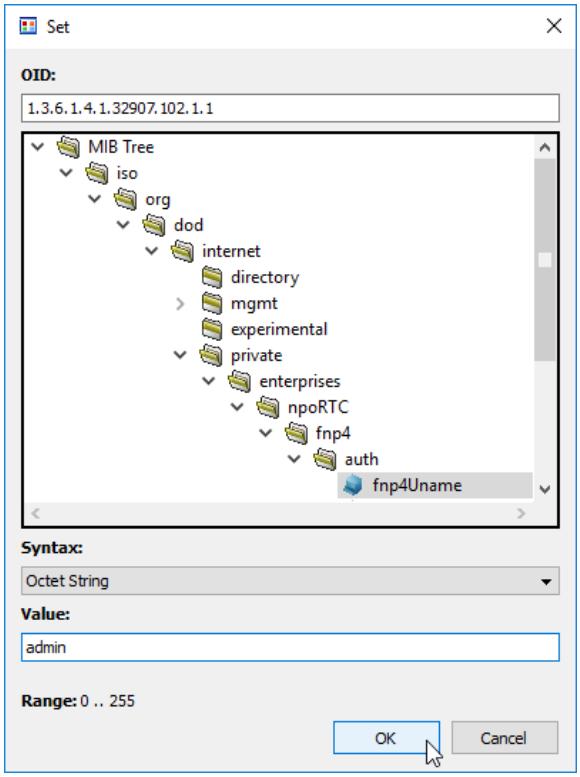


Рисунок 5.11: Диалоговое окно установки переменной fnp4Uname

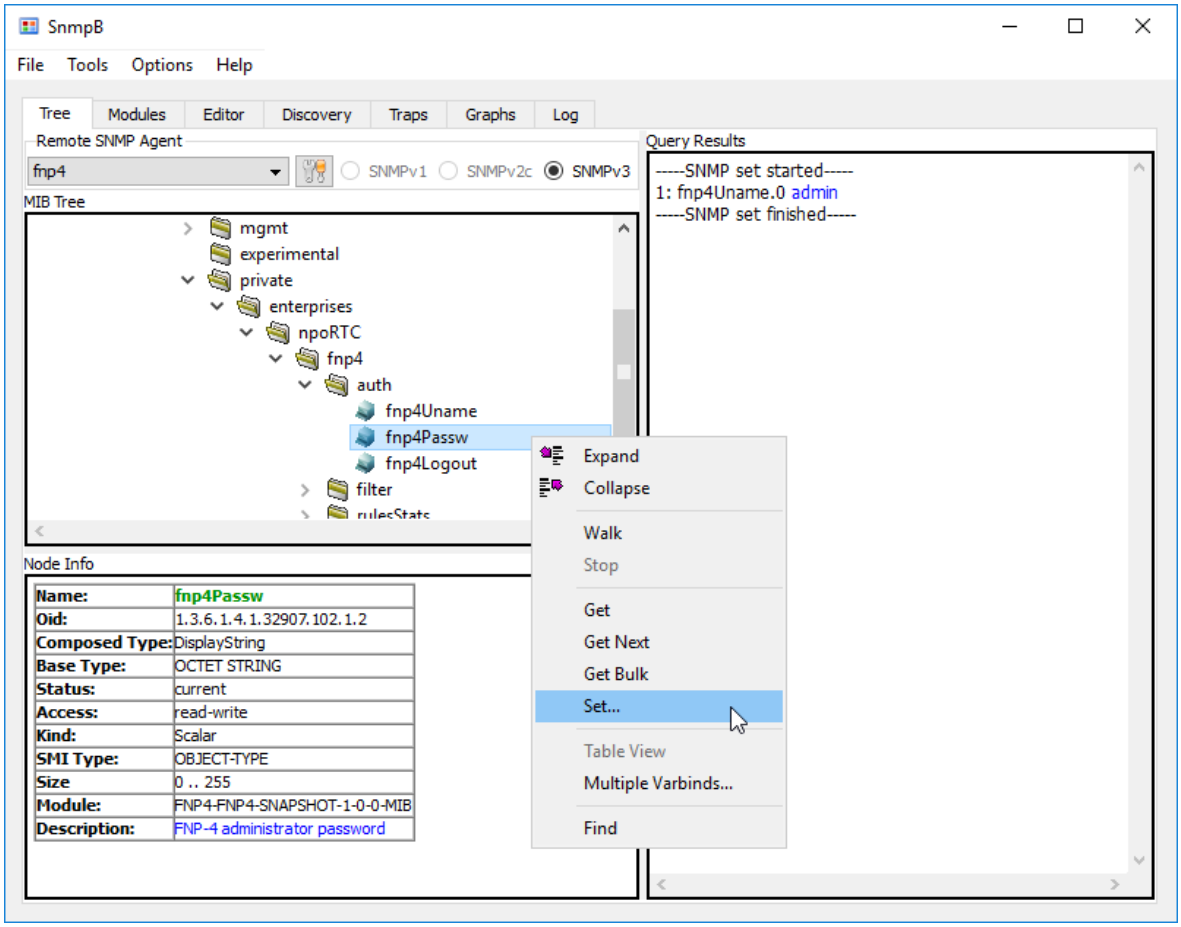


Рисунок 5.12: Результат установки переменной fnp4Uname и контекстное меню переменной fnp4Passw

7) В открывшемся диалоговом окне **`Set`** в поле `Value` ввести значение переменной – пароль администратора МЭ ССПТ-4А1, которого необходимо авторизовать (в примере – пароль по умолчанию администратора `admin`) (рисунок 5.13, стр. 366).

8) В диалоговом окне **`Set`** кликнуть по кнопке **`OK`** (рисунок 5.13, стр. 366). Убедиться, что переменная `fnp4Passw` была успешно установлена, то есть администратор был авторизован: в области **`Query Results`** главного окна должно быть выведено имя установленной переменной, ее новое значение и результат выполнения запроса: **`SNMP set finished`** (рисунок 5.14, стр. 367).

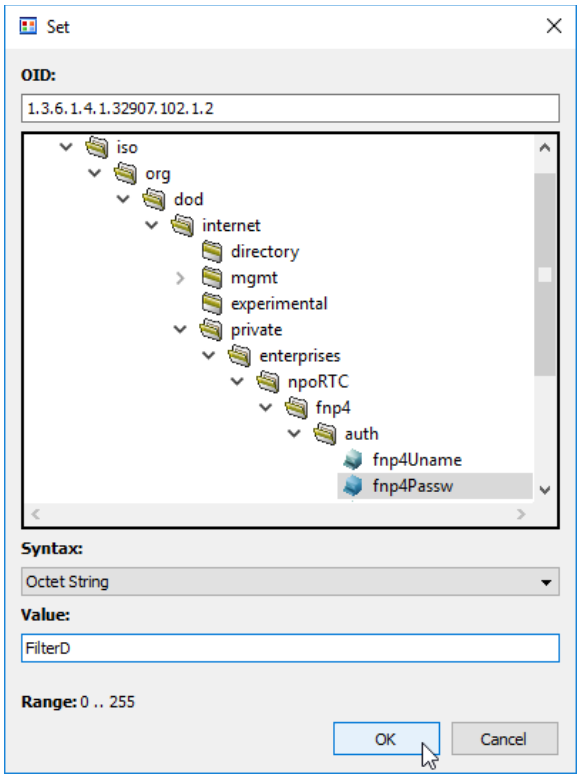


Рисунок 5.13: Диалоговое окно установки переменной fnp4Passw

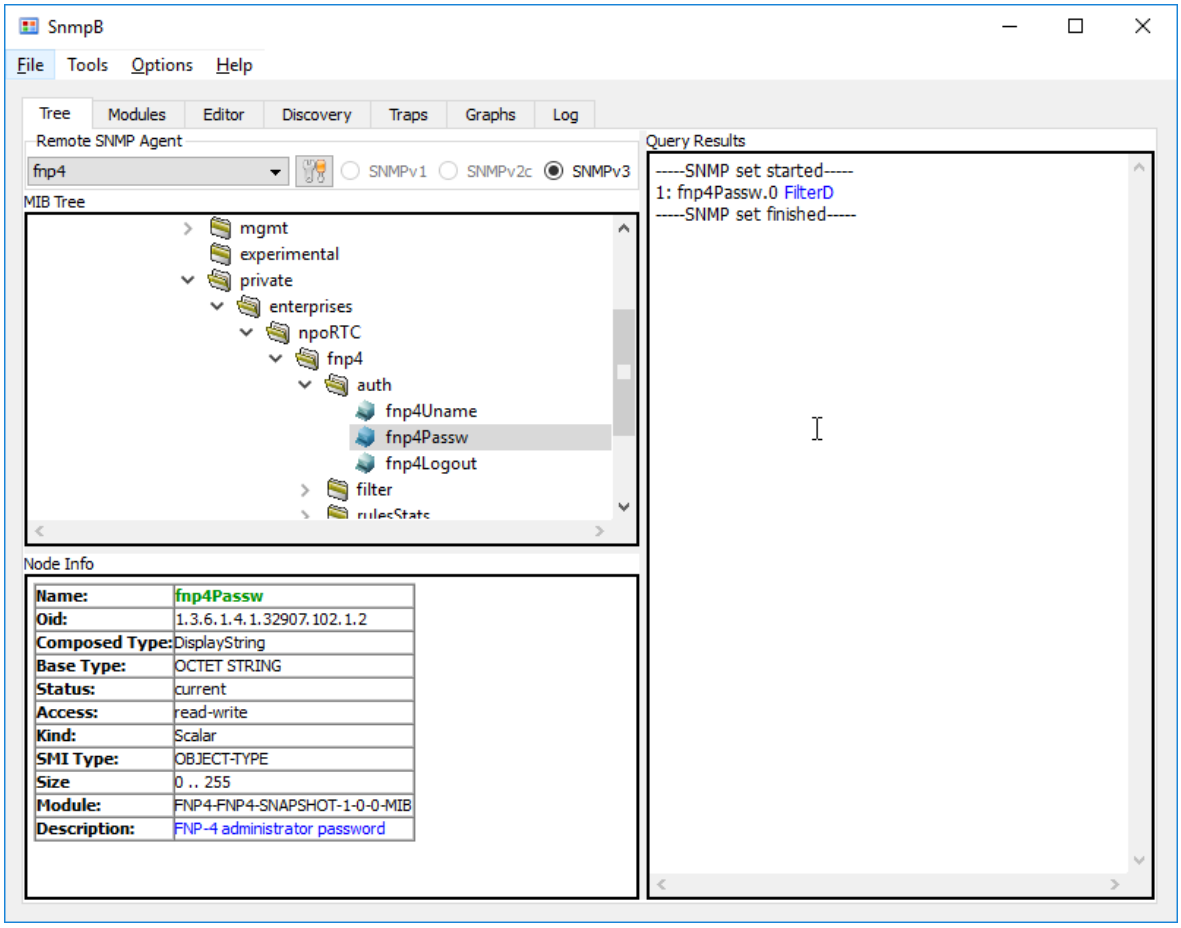


Рисунок 5.14: Результат установки переменной fnp4Passw

5.2.2. Вывод таблицы

MIB-браузер `snmpb` позволяет выводить табличные объекты дерева объектов MIB в табличной форме. Имена всех табличных объектов MIB-модуля МЭ ССПТ-4А1 заканчиваются подстрокой “`Table`”. Рассмотрим данную возможность на примере таблицы статистики трафика на фильтрующих интерфейсах МЭ ССПТ-4А1 - `filterStatsTable`. Подразумевается, что авторизация администратора МЭ ССПТ-4А1 уже выполнена (раздел 5.2.1, стр. 363). Для просмотра данной таблицы необходимо выполнить следующую последовательность действий:

1) Внутри узла `fnp4` дерева объектов MIB выбрать узел `filter`, развернуть его и выбрать целевой объект `filterStatsTable` (рисунок 5.15, стр. 368).
2) Кликнуть правой кнопкой мыши по объекту `filterStatsTable` и в появившемся контекстном меню выбрать пункт **`Table View`** (рисунок 5.15, стр. 368).
3) Убедиться, что в области **`Query Results`** выведена таблица `filterStatsTable` (рисунок 5.16, стр. 369).

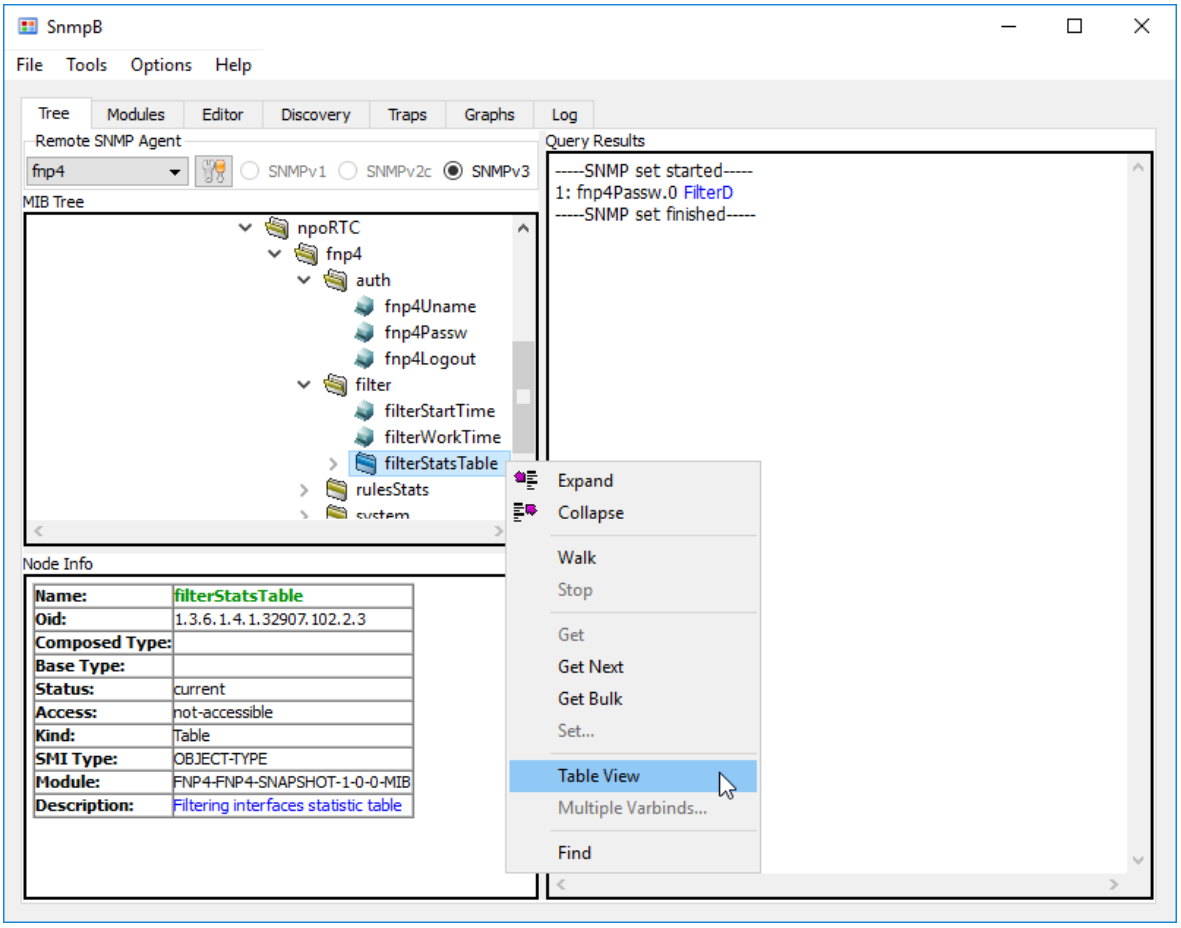


Рисунок 5.15: Контекстное меню таблицы filterStatsTable

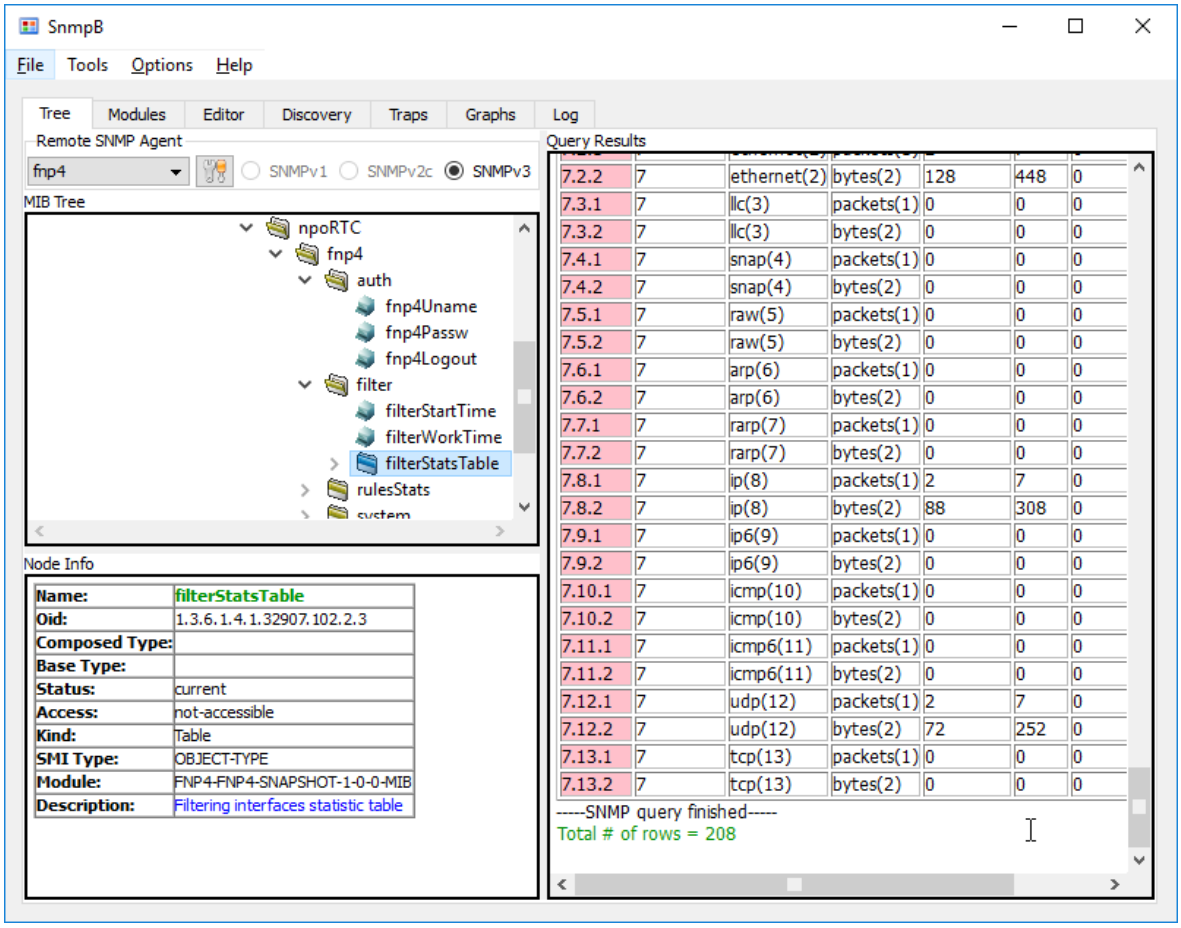


Рисунок 5.16: Вывод таблицы filterStatsTable

5.2.3. Запрос значений всех переменных некоторого узла

Протокол SNMP поддерживает специальный тип запроса - `walk`, позволяющий получить значения всех переменных, принадлежащих одному узлу, за один запрос. В данном разделе продемонстрируем выполнение запроса типа walk на примере получения всех значений узла `system.sysInfo`, содержащей сведения об аппаратной конфигурации и версии ПО МЭ ССПТ-4А1. Подразумевается, что до выполнения действий, изложенных ниже, была выполнена авторизация администратора МЭ ССПТ-4А1 (раздел 5.2.1, стр. 363).

1) Внутри узла `fnp4` дерева объектов MIB выбрать узел `system`, развернуть его и выбрать целевой узел `sysInfo` (рисунок 5.17, стр. 370).
2) Кликнуть правой кнопкой мыши по объекту `sysInfo` и в появившемся контекстном меню выбрать пункт **`Walk`** – в результате должен быть выполнен запрос типа `walk` к данному узлу (рисунок 5.17, стр. 370).
3) Убедиться, что в области **`Query Results`** выведены имена и значения всех объектов (переменных), находящихся внутри узла `sysInfo` (рисунок 5.18, стр. 371).

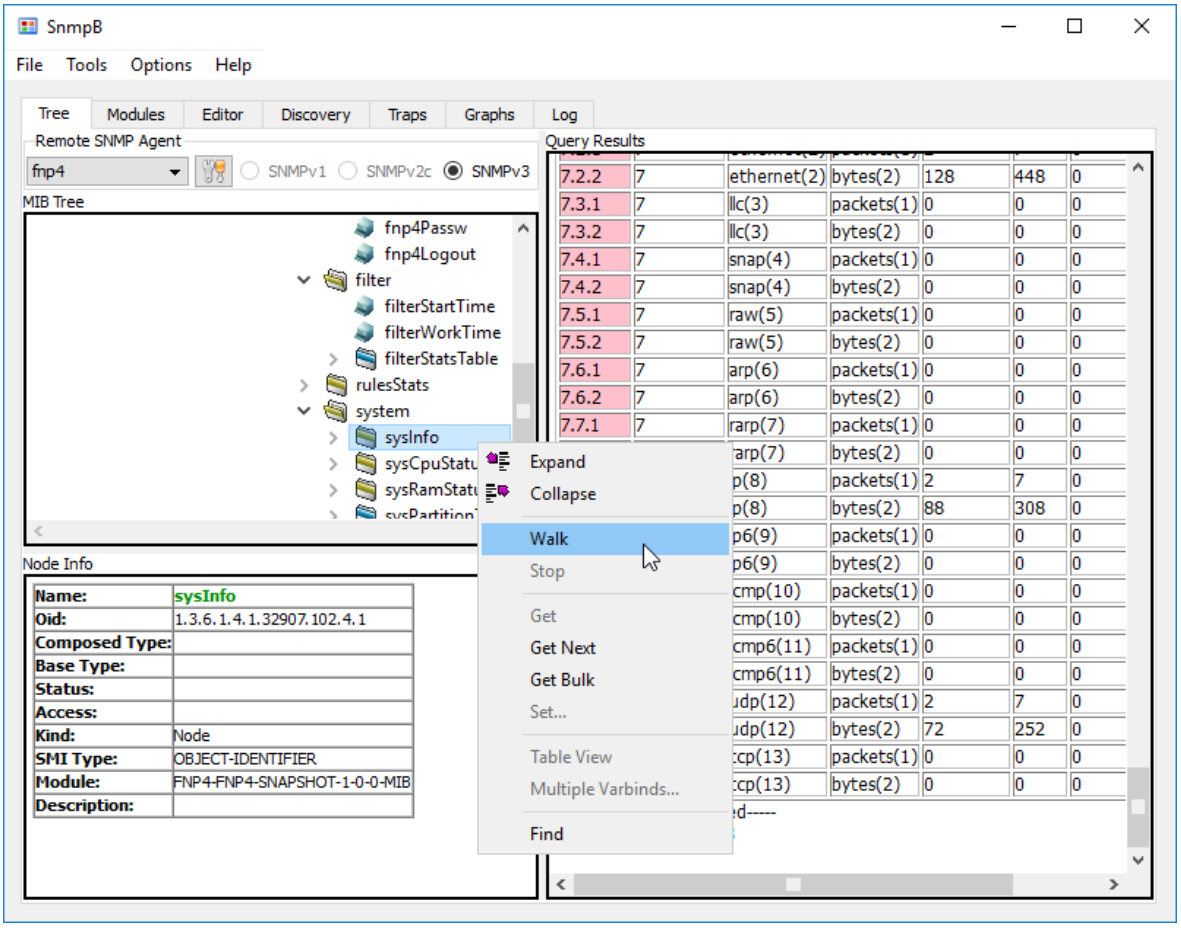


Рисунок 5.17: Запрос значений всех переменных узла system.sysInfo

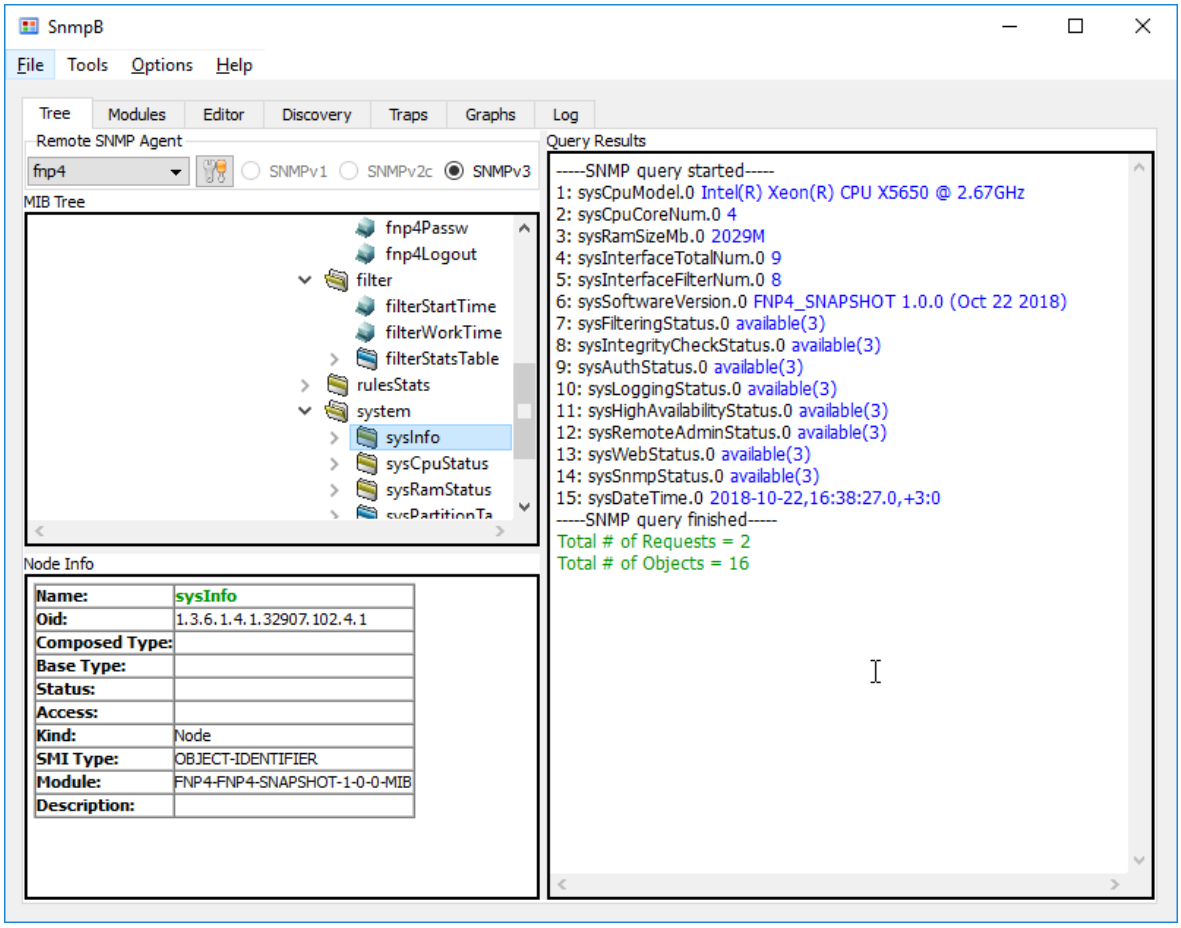


Рисунок 5.18: Вывод значений всех переменных узла system.sysInfo

5.2.4. Завершение сеанса работы администратора

После того, как работа с МЭ ССПТ-4А1 в MIB-браузере завершена, рекомендуется явно завершать сеанс работы администратора МЭ ССПТ-4А1, не дожидаясь его автоматического завершения по тайм-ауту неактивности администратора. Подразумевается, что до выполнения действий, изложенных ниже, была выполнена авторизация администратора МЭ ССПТ-4А1 (раздел 5.2.1, стр. 363).

Для завершения сеанса работы администратора МЭ ССПТ-4А1 в `snmpb` необходимо выполнить следующие действия:

1) Внутри узла `fnp4` дерева объекта MIB выбрать узел `auth`, развернуть его и выбрать целевой объект `fnp4Logout` (рисунок 5.19, стр. 372).
2) Кликнуть правой кнопкой мыши по объекту `fnp4Logout` и в появившемся контекстном меню выбрать пункт **`Set...`** (рисунок 5.19, стр. 372).
3) В открывшемся диалоговом окне **`Set`** в списке **`Value`**, под пустым полем ввода, выбрать значение **`logout (1)`** (рисунок 5.20, стр. 373).

4) Кликнуть по кнопке **OK** в диалоговом окне **Set**: в результате должен быть выполнен запрос на установку переменной `fnp4Logout` в значение **logout (1)** (рисунок 5.21, стр. 373).

5) По диагностике в области **Query Results** убедиться, что запрос был успешно выполнен, то есть сеанс работы администратора МЭ ССПТ-4А1 успешно завершен (рисунок 5.22, стр. 373).

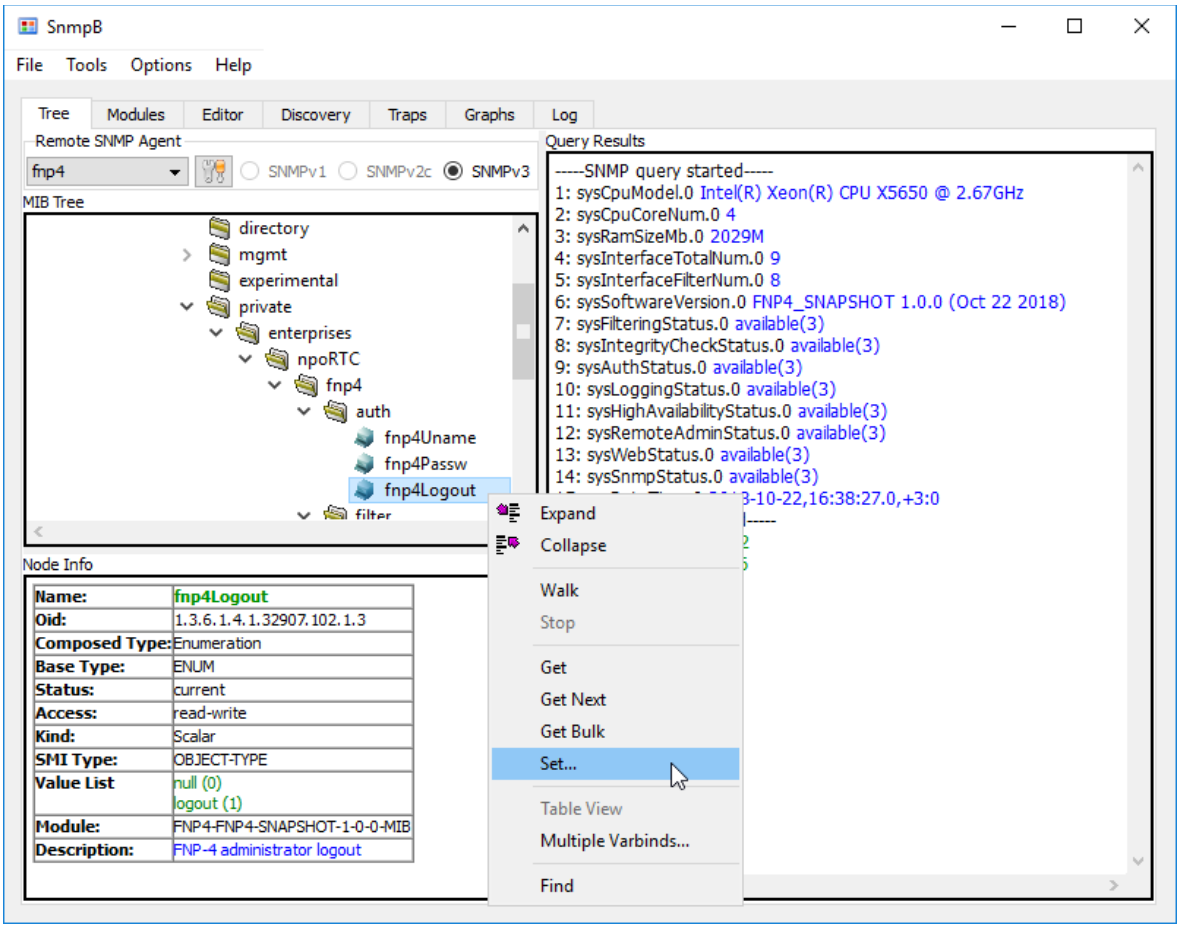


Рисунок 5.19: Контекстное меню переменной fnp4Logout

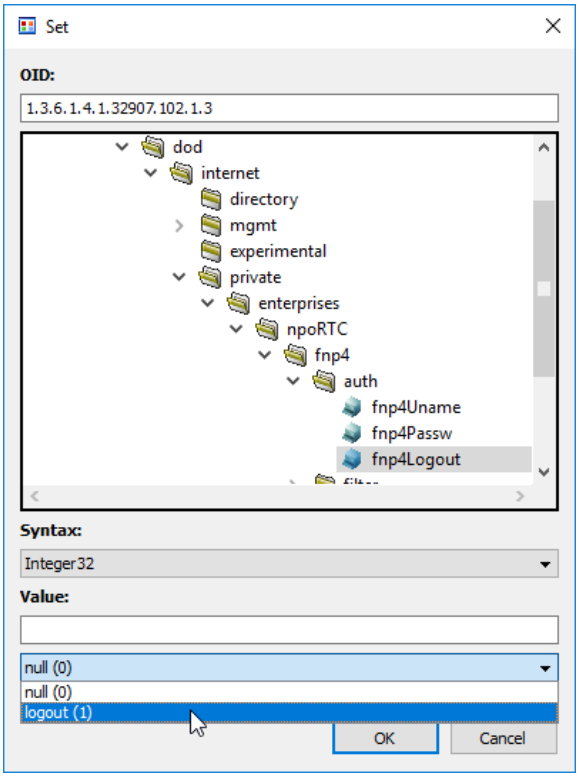


Рисунок 5.20: Выбор устанавливаемого значения переменной fnp4Logout

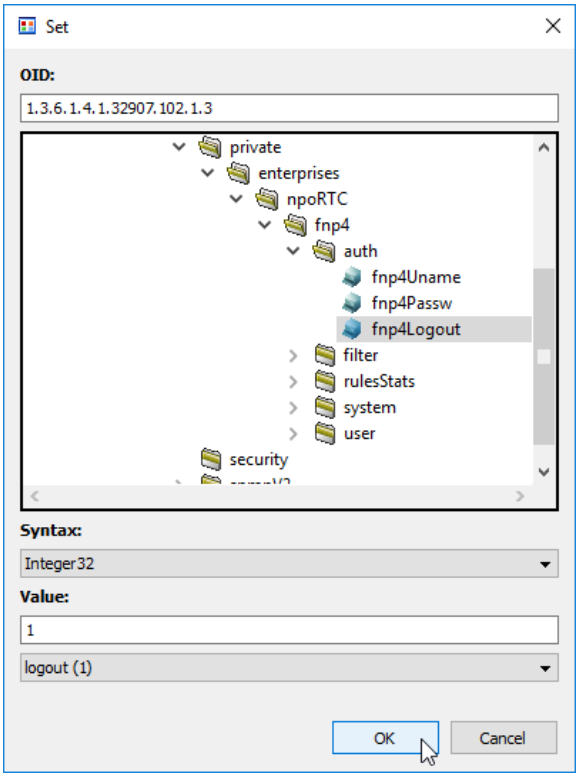


Рисунок 5.21: Установка переменной fnp4Logout

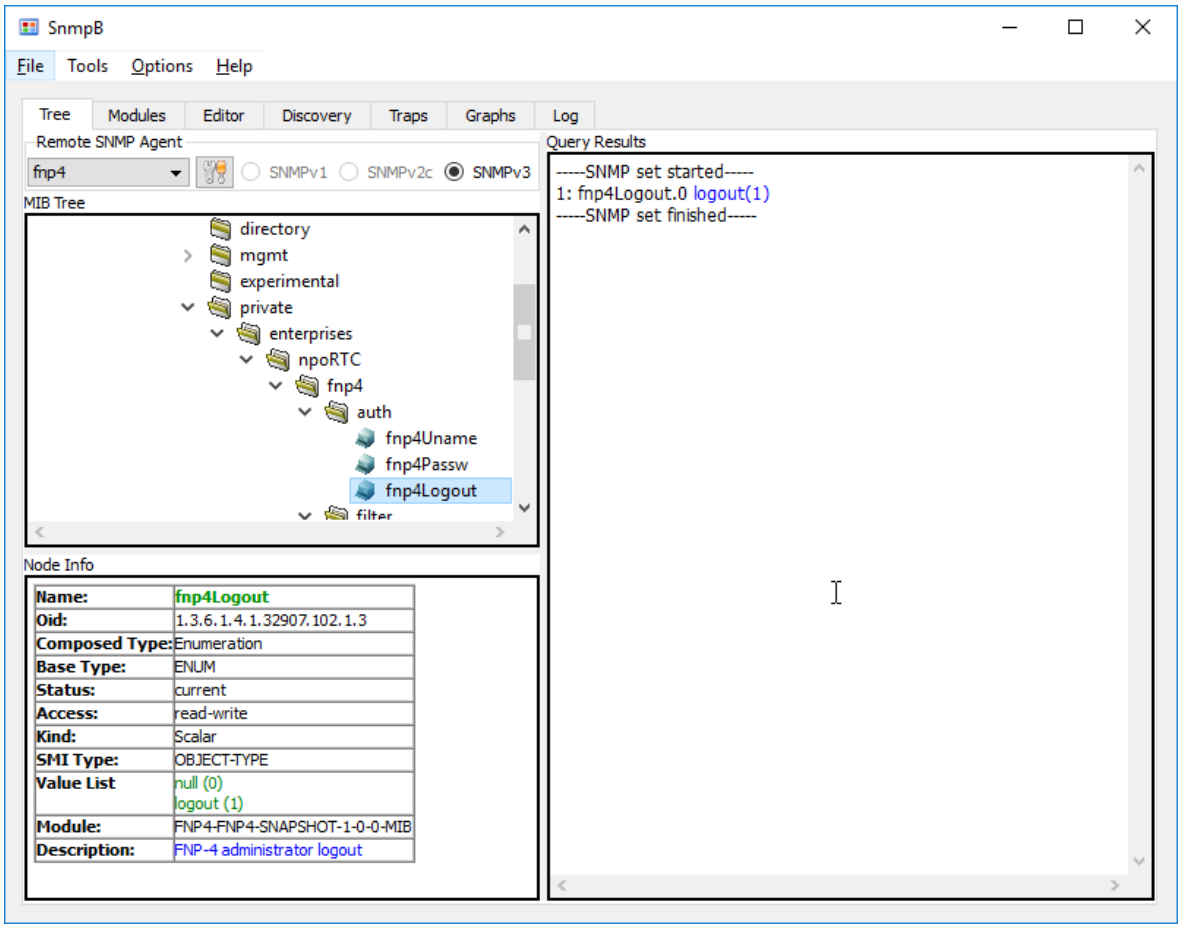


Рисунок 5.22: Диагностика об успешной установке переменной fnp4Logout

6. Регламентное тестирование

Объектом регламентного тестирования является экземпляр устройства МЭ ССПТ-4А1, изготовленный в соответствии с техническими условиями ФРПС.466259.001 ТУ, независимо от варианта исполнения.

При проведении регламентного тестирования необходимо наличие следующей документации:

- паспорт экземпляра устройства МЭ ССПТ-4А1 – *“Межсетевой экран ССПТ-4А1. Паспорт” ФРПС.466259.001 ПС*;
- настоящий документ – *“Межсетевой экран ССПТ-4А1. Руководство по эксплуатации” ФРПС.466259.001 РЭ*.

Целью регламентного тестирования является подтверждение работоспособности экземпляра устройства МЭ ССПТ-4А1. Успешное прохождение процедуры регламентного тестирования гарантирует исправность экземпляра устройства МЭ ССПТ-4А1.

В случае нарушений в работе экземпляра устройства МЭ ССПТ-4А1, выявленных при прохождении процедуры регламентного тестирования, необходимо обратиться в сервисный центр ООО "НПО "ФРАКТЕЛ" для его сервисного обслуживания и/или ремонта.

В УОС МЭ ССПТ-4А1 имеется учетная запись системного пользователя с именем **`fractel`**, которая может быть использована персоналом сервисного центра ООО "НПО "ФРАКТЕЛ" при проведении работ по техническому обслуживанию, восстановлению работоспособности и модернизации экземпляров устройств МЭ ССПТ-4А1, выполняемых как непосредственно в сервисном центре ООО "НПО "ФРАКТЕЛ", так и при выезде к заказчику.

В процессе регламентного тестирования экземпляра устройства МЭ ССПТ-4А1 выполняются следующие задачи:

- проверка корректности загрузки УОС и ПО МЭ ССПТ-4А1;
- проверка контрольных сумм контролируемых файлов УОС и ПО МЭ ССПТ-4А1 на соответствие контрольным суммам, указанным в паспорте экземпляра устройства МЭ ССПТ-4А1;
- проверка управления дополнительными конфигурациями и политиками доступа;
- проверка работоспособности управляющего интерфейса;
- проверка работоспособности фильтрующих интерфейсов;
- проверка реализации правил фильтрации;
- проверка процесса регистрации;
- проверка процесса идентификации и аутентификации администратора защиты;
- проверка доступности WEB-интерфейса администратора;
- проверка процесса формирования и поддержания изолированной программной среды;

- проверка процедуры восстановления (выполняется в соответствии с описанием, приведенным в разделе 7.2.2, стр. 403).

Процедура регламентного тестирования должна проводиться на специальном стенде, в состав которого входят следующие компоненты:

- экземпляр устройства МЭ ССПТ-4А1;
- управляющий компьютер. Требования, предъявляемые к управляющему компьютеру, приводятся в разделе Ошибка: источник перекрёстной ссылки не найден, стр. Ошибка: источник перекрёстной ссылки не найден;
- сетевой кабель типа «витая пара», соединители RJ-45 – RJ-45: 2 шт.;
- оптический сетевой кабель, соединители LC-LC: 2 шт.

Процедура регламентного тестирования должна выполняться пошагово. При выполнении каждого последующего шага используются настройки экземпляра устройства МЭ ССПТ-4А1, выполненные на предыдущем шаге.

Процедура регламентного тестирования представляет собой последовательность следующих шагов:

Подготовка к проведению регламентного тестирования

1) **Подключить УК к МЭ через системную консоль**. Все экземпляры устройств МЭ ССПТ-4А1 оснащаются последовательным портом стандарта RS-232 (далее – COM-порт). Этот COM-порт используется в качестве системной консоли экземпляра устройства МЭ ССПТ-4А1. Для подключения УК к МЭ через COM-порт необходимо выполнить следующую последовательность шагов:

   1.1) Соединить при помощи консольного кабеля, входящего в комплект поставки МЭ ССПТ-4А1, COM-порт (тип разъема RJ-45) экземпляра устройства МЭ ССПТ-4А1 и свободный COM-порт (тип разъема DB-9) УК (при отсутствии COM-порта на УК воспользоваться конвертером RS-232 в USB);

   1.2) Настроить COM-порт УК, участвующий в соединении, следующим образом (краткая запись настроек COM-порта: **115200 8N1 CTS/RTS**):

   - скорость передачи данных – **115200** бит/с;
   - биты данных – **8** бит;
   - четность – **не проверяется**;
   - стоповые биты – **1** бит;
   - управление потоком – **аппаратное (*CTS/RTS*)**;

   Настройка COM-порта УК выполняется, как правило, непосредственно в программах-эмуляторах терминала, которые будут использоваться для взаимодействия с экземпляром

устройства МЭ ССПТ-4А1.

2) **Включить экземпляр устройства МЭ ССПТ-4А1**, предварительно подключив шнур питания к розетке 220В/50Гц. Данный шаг считается успешно пройденным, если произошла загрузка УОС и информация на системной консоли выглядит так, как это показано на рисунке 6.1, стр. 377;

```
Starting fnp4_had.
.....

Центральный процессор       | Intel(R) Xeon(R) CPU           X5650  @ 2.67GHz
Число ядер процессора       | 4
Объем оперативной памяти    | 4277645312 Байт (4079M)
Версия ПО ССПТ-4            | FNP4 1.0.0-RELEASE (Mar  3 2021)
Заводской номер             | 000000
Всего сетевых интерфейсов   | 10
    Фильтрующие интерфейсы  | 9: eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth7,eth8
    Управляющий интерфейс   | 10.234.28.71/255.255.0.0
Пакетная фильтрация         | запущен (доступен)
Контроль целостности        | запущен (доступен)
Авторизация                 | запущен (доступен)
Регистрация                 | запущен (доступен)
Резервирование              | запущен (доступен)
Удаленное администрирование | запущен (доступен)
WEB-интерфейс               | запущен (доступен)
SNMP-интерфейс              | запущен (доступен)

Performing sanity check on sshd configuration.
Starting sshd.
Starting cron.
Starting background file system checks in 60 seconds.

Thu Mar  4 09:02:48 UTC 2021

FreeBSD/amd64 (fnp4) (ttyv0)

login:
```

Рисунок 6.1: Вид системной консоли после включения экземпляра устройства МЭ ССПТ-4А1

3) **Последовательно ввести учетные данные** системного пользователя **`fnpsh`** и администратора МЭ ССПТ-4А1 **`admin`**. Данный шаг считается успешно пройденным, если:

3.1) информация на системной консоли выглядит, как это показано на рисунке 6.2, стр. 378;

3.2) получено диагностическое сообщение командного интерфейса МЭ ССПТ-4А1

```
FNPSH-I-007.02.3001-Успешная авторизация администратора (admin)
```

В некоторых программах-эмуляторах терминала для получения системного приглашения может потребоваться нажатие клавиши **`<Enter>`** на клавиатуре УК.

Проверка корректности загрузки УОС и ПО МЭ ССПТ-4А1

4) **Проверить корректность загрузки** экземпляра устройства МЭ ССПТ-4А1, выполнив команду **`system show`**. Данный шаг считается успешно пройденным, если:

4.1) информация на системной консоли выглядит, как это показано на рисунке 6.3, стр. 379;

```
WEB-интерфейс                | запущен (доступен)
SNMP-интерфейс               | запущен (доступен)

Performing sanity check on sshd configuration.
Starting sshd.
Starting cron.
Starting background file system checks in 60 seconds.

Thu Mar  4 11:39:05 UTC 2021

FreeBSD/amd64 (fnp4) (ttyv0)

login: fnpsh
Password:
Last login: Thu Mar  4 11:37:40 on ttyv0

                МежсетеВой экран ССПТ-4А1
            (c) ООО "НПО "ФРАКТЕЛ", 2019-2021


МежсетеВой экран ССПТ-4
  Командный интерфейс, Версия 1.0.0
  (c) ООО "НПО "ФРАКТЕЛ", 2019-2021. Все права защищены


Имя администратора: admin
Пароль:

FNPSH-I-007.02.3001-Успешная авторизация администратора (admin)
fnp4>
```

Рисунок 6.2: Вид системной консоли после авторизации администратора МЭ ССПТ-4А1

4.2) количество физических сетевых интерфейсов Ethernet экземпляра устройства МЭ ССПТ-4А1 совпало с количеством, указанным в строке вывода команды **`system show`** “**`Всего сетевых интерфейсов`**”;

```
Имя администратора: admin
Пароль:

FNPSH-I-007.02.3001-Успешная авторизация администратора (admin)
fnp4> system show
Центральный процессор                | Intel(R) Xeon(R) CPU           X5650  @ 2
.67GHz
Число ядер процессора                | 4
Объем оперативной памяти             | 4277645312 байт (4079M)
Версия ПО ССПТ-4                     | FNP4 1.0.0-RELEASE (Mar  3 2021)
Заводской номер                      | 000000
Всего сетевых интерфейсов            | 10
    Фильтрующие интерфейсы           | 9: eth0,eth1,eth2,eth3,eth4,eth5,eth6,eth
7,eth8
    Управляющий интерфейс            | Включен, 10.234.28.71/255.255.0.0
Пакетная фильтрация                  | запущен (доступен)
Контроль целостности                 | запущен (доступен)
Авторизация                          | запущен (доступен)
Регистрация                          | запущен (доступен)
Резервирование                       | запущен (доступен)
Удаленное администрирование          | запущен (доступен)
WEB-интерфейс                        | запущен (доступен)
SNMP-интерфейс                       | запущен (доступен)
Тайм-аут неактивности администратора | 600 секунд
Просмотрщик по умолчанию FNPSH       | Внутренний (internal)
Имя устройства                       | fnp4
Комментарий к устройству             |
fnp4>
```

Рисунок 6.3: Проверка корректности загрузки экземпляра устройства МЭ ССПТ-4А1

4.3) состояние программных модулей в строках вывода команды **`system show`** “**`Пакетная фильтрация`**”, “**`Контроль целостности`**”, “**`Авторизация`**”, “**`Регистрация`**”, “**`Резервирование`**”, “**`Удаленное администрирование`**”, “**`WEB-интерфейс`**” и “**`SNMP-интерфейс`**” обозначено как “**`запущен (доступен)`**”;

Проверка контрольных сумм контролируемых файлов

5) **Проверить контрольные суммы** контролируемых файлов УОС и ПО МЭ ССПТ-4А1, выполнив команду **`system icheck`**. Данный шаг считается успешно пройденным, если:

5.1) информация на системной консоли выглядит, как это показано на рисунке 6.4, стр. 380;

5.2) контрольные суммы, полученные в результате выполнения команды **`system icheck`**, совпали с контрольными суммами, указанными в паспорте экземпляра устройства МЭ ССПТ-4А1;

Контрольные суммы файлов, зависящие от экземпляра устройства МЭ ССПТ-4А1, а также файлов, изменяемых в процессе его работы, не указываются в паспорте устройства. К таким файлам относятся:

- fnp4_dhparam.pem
- fnp4_dhkey.bn
- fnp4_dhpubkey.bn
- fnp4_key.pem
- fnp4_cert.pem
- master.passwd
- fnp4_cf.xml
- net_passwd
- fnp4_net.keys
- fnp4_passwd
- policy.ds
- policy.rs
- rc.conf.local
- proxy.config
- proxy.action
- resolv.conf

```
 09:08:38                    Проверка целостности                    04.03.2021
Имя файла                 Результат Контрольная сумма
-----------------------------------------------------------------------------
rc.conf                     +         9A3B132AFBB383118215FD21D9B0F7ABFB32499B1ECB
fnp4                        +         17DAA971AB004FDEB708681F3403BEF3F89980206B19
fnp4eth                     +         145DC0CA9D7E982AAF4B1A972CCF2880840990F1E577
fnp4proxy                   +         2BAE035CD04A4D37295A253A8618575050589C1CF8FF
fnp4snmp                    +         20A48D7F6B496EE8757C7ACF1041D0C216BAB41A52B5
fnp4tmp                     +         B72AB6C48FF6221AAEC8885CD803937CBCF86C076077
fnp4web                     +         08ED2029B4544EF034CDE780288181D169AB3FEAA12B
kernel                      +         5B060E5BE88CDBA21303FFADB070CD70C942B647323F
libc.so.7                   +         2A5252E11888619A66E403ECE496131DA4D7465068A8
libkvm.so.7                 +         E47577DA165D2B22FEC2F25DA5D9C4E8B02AC21493BD
libcrypto.so.8              +         CF91396F03E1E5269D82F9D2BE6660128014DB3A2D66
libssl.so.8                 +         93BEBE43AE3FD211F6FB9849F5C384034EC078ED2151
libxml2.so.2.9.10           +         7377CEB9B830476830F04FDC573A8FBC10146A4593C2
libfnpcrypt2_ssl.so.2.1.0   +         B8CA6738CCB739AC51BE692A04E988B4E45507C382C1
login                       +         081956FC5FC4D4066C0304F5566049A1CDE0EC14F9BE
ntpdate                     +         83DB8416220B9509A68096B7B3DDC84A284A580C8A3E
httpd                       +         D0926F7952B34A8110009273FEDCE026108A75BB9852
snmpd                       +         7F376BE4D9CD576780AAB5A6DBCC6D570B40747C966C
openssl                     +         3F080C4279F8F3B02833F8368F5EF90093DA0710D2FC
fnp4sh                      +         4A12F8CBD286FFB438A6032AA035B044B993B1ADB272
fnp4_info                   +         58ACA9213F03921DB4B7CFADA93AC2485BB8170339E4
fnp4_authd                  +         2270CCAAB577BE25F6DE65A179430D54EB9E940CAAF6
fnp4_csd                    +         DCB0C596AC0D360F7DD67F016ADD1455C15F0284131F
fnp4_filtd                  +         AB3954705AF0C20AFCA4A11B5CBCEC0020F0BD448EAF
fnp4_had                    +         964FA3ED6AD8932CCE23DB4578CA55693010184D14F7
fnp4_lcmd                   +         21E658CE4BFE663ADC2ACA8293335317512B8C3B0D89
 Строки: 1-28 из 62                 Столбцы: 1-80    H - справка  Q, F10 - Выход
```

Рисунок 6.4: Проверка контрольных сумм

Проверка управления дополнительными конфигурациями и политиками доступа (начало)

6) **Сохранить настройки экземпляра устройства МЭ ССПТ-4А1**, выполнив команду **`config save`**. В результате выполнения команды, будет сохранена дополнительная конфигурация с именем, сформированным автоматически по следующим правилам:

`fnp4-<имя_устройства>-YYYYMMDD-HHMMSS`

где:

- `<имя_устройства>` – доменное имя, назначенное экземпляру устройства по команде **`config device`**;
- `YYYYMMDD` – дата создания дополнительной конфигурации (`YYYY` – значение года, `MM` – значение месяца, `DD` – значение дня месяца);

- HHMMSS – время создания дополнительной конфигурации (HH – часы, MM – минуты, SS – секунды).

Для поверки правильности сохранения дополнительной конфигурации выполните команду **config list**. Если информация на системной консоли выглядит так, как это показано на рисунке 6.5, стр. 381, значит шаг был выполнен успешно.

```
fnp4> config save
Имя конфигурации не задано. Сохранить со сгенерированным именем? (Y/N) [N]: Y
FNPSH-I-007.02.300B-Дополнительная конфигурация сохранена (fnp4-fnp4-20210304-09
0949)
fnp4> config list
Список дополнительных конфигураций:
    Имя                        Последнее изменение                Комментарий
    fnp4-fnp4-20210304-090949 04.03.2021 09:09:49 UTC+0000 (UTC)
Занято: 1       Свободно: 15
fnp4>
```

Рисунок 6.5: Сохранение дополнительной конфигурации с именем по умолчанию

7) **Сохранить настройки политики доступа экземпляра устройства МЭ ССПТ-4А1**, выполнив команду **policy save**. В результате выполнения команды, будет сохранена дополнительная политика доступа с именем, сформированным автоматически по следующим правилам:

fnp4-<имя_устройства>-YYYYMMDD-HHMMSS

где:

- <имя_устройства> – доменное имя, назначенное экземпляру устройства по команде config device;
- YYYYMMDD – дата создания дополнительной конфигурации (YYYY – значение года, MM – значение месяца, DD – значение дня месяца;
- HHMMSS – время создания дополнительной конфигурации (HH – часы, MM – минуты, SS – секунды.

Для поверки правильности сохранения дополнительной политики доступа выполните команду **policy list**. Если информация на системной консоли выглядит так, как это показано на рисунке 6.6, стр. 382, значит шаг был выполнен успешно.

```
fnp4> policy save
Имя дополнительной политики не указано. Сохранить со сгенерированным именем? (Y/
N) [N]: Y
FNPSH-I-007.02.30FD-Дополнительная политика сохранена (fnp4-fnp4-20210304-091138
)
fnp4> policy list
Список дополнительных политик:
    Имя                        Последнее изменение                Комментарий
    fnp4-fnp4-20210304-091138 04.03.2021 09:11:38 UTC+0000 (UTC)
    policy_accept              03.03.2021 08:19:32 UTC+0000 (UTC) Всё разрешено
    policy_drop                03.03.2021 08:19:32 UTC+0000 (UTC) Всё запрещено
Занято: 3       Свободно: 29
fnp4>
```

Рисунок 6.6: Сохранение дополнительной политики доступа с именем по умолчанию

8) **Применить конфигурацию по умолчанию**, выполнив команду **`config default`**.

После применения конфигурации по умолчанию сеанс администратора будет завершен. Необходимо будет вновь выполнить авторизацию на экземпляре устройства МЭ ССПТ-4А1.

Для подтверждения выполнения команды необходимо нажать последовательность кнопок на клавиатуре **<Y>**,**<Enter>** (или **<y>**,**<Enter>**) как это показано на рисунке 6.7, стр. 382.

```
fnp4> config default
Применить конфигурацию по умолчанию? (Y/N) [N]: y
FNPSH-I-007.02.3112-Пакетный фильтр перезапущен
FNPSH-I-007.02.305D-Конфигурация по умолчанию применена
FNPSH-I-007.02.3003-Завершение работы администратора (admin)


FreeBSD/amd64 (fnp4) (ttyv0)

login:
```

Рисунок 6.7: Применение конфигурации по умолчанию для экземпляра устройства МЭ ССПТ-4А1

9) **Настроить управляющий интерфейс** экземпляра устройства МЭ ССПТ-4А1, выполнив команду **`interface control set address=10.41.2.120/255.255.255.128`**. Для подтверждения выполнения команды необходимо нажать последовательность кнопок на клавиатуре **<Y>**,**<Enter>** (или **<y>**,**<Enter>**) как это показано на рисунке 6.8, стр. 382. Проверить правильность настройки управляющего интерфейса, выполнив команду **`interface control show`** (рисунок 6.9, стр. 383);

```
fnp4> interface control set address=10.41.2.120/255.255.255.128
Изменить параметры управляющего интерфейса? (Y/N) [N]: Y
FNPSH-I-007.02.301D-IP-адрес управляющего интерфейса изменен (10.41.2.120)
fnp4>
```

Рисунок 6.8: Настройка управляющего интерфейса

```
fnp4> interface control show
Интерфейс:                        управляющий
    Настроено:
        Состояние:                Включено
        IP-адрес:                 10.41.2.120
        IP-маска:                 255.255.255.128
        Шлюз по умолчанию:        не определено
        Скорость передачи:        autoselect
        MTU:                      1500 (72-9000)
        Агрегирование портов:     Выключено
        Протокол агрегирования:   failover
        Интерфейс агрегата:       eth0
        Список доступа:           любой
    Определено:
        Состояние:                Включено
        IP-адрес:                 10.41.2.120
        IP-маска:                 255.255.255.128
        Шлюз по умолчанию:        не определено
        Скорость передачи:        autoselect
        MTU:                      1500
        Несущая:                  активна
fnp4>
```

Рисунок 6.9: Проверка настройки управляющего интерфейса

10) **Применить политику доступа по умолчанию**, выполнив команду **`policy default`**.

> Политика доступа по умолчанию предполагает полный запрет прохождения пакетов через фильтрующие интерфейсы экземпляра устройства МЭ ССПТ-4А1 и отсутствие каких бы то ни было определений в справочнике объектов.

Для подтверждения выполнения команды необходимо нажать последовательность кнопок на клавиатуре **`<Y>`**,**`<Enter>`** (или **`<y>`**,**`<Enter>`**) как это показано на рисунке 6.10, стр. 383. Для поверки правильности применения политики доступа по умолчанию необходимо выполнить команду **`rule show`**. Если информация на системной консоли выглядит так, как это показано на рисунке 6.11, стр. 383, значить шаг был выполнен успешно.

```
fnp4> policy default
Применить политику по умолчанию? (удаление всех пакетов и очистка справочника) (
Y/N) [N]: Y
FNPSH-I-007.02.30FF-Политика установлена в состояние по умолчанию (правила и спр
авочник)
fnp4>
```

Рисунок 6.10: Применение политики доступа по умолчанию

```
 09:26:44                    Правила текущей политики                    04.03.2021
rule:0 action=drop
ap:0 action=drop
```

Рисунок 6.11: Состав политики доступа по умолчанию (команда rule show)

11) **Применить дополнительную политику доступа**, выполнив команду **`policy apply name=policy_accept`**.

Дополнительная политика доступа с именем **policy_accept** является предустановленной политикой, разрешающей прохождение пакетов через фильтрующие интерфейсы экземпляра устройства МЭ ССПТ-4А1 и отсутствие каких бы то ни было определений в справочнике объектов.

Для подтверждения выполнения команды необходимо нажать последовательность кнопок на клавиатуре **<Y>**,**<Enter>** (или **<y>**,**<Enter>**) как это показано на рисунке 6.12, стр. 384. Для поверки правильности применения политики доступа по умолчанию, необходимо выполнить команду **rule show**. Если информация на системной консоли выглядит так, как это показано на рисунке 6.13, стр. 384, значит шаг был выполнен успешно.

```
fnp4> policy apply name=policy_accept
Применить дополнительную политику (режим управления сессиями)? (Y/N) [N]: Y
FNPSH-I-007.02.30FC-Дополнительная политика применена (правила и справочник)
fnp4>
```

Рисунок 6.12: Применение политики доступа policy_accept

```
09:29:36                    Правила текущей политики                    04.03.2021
rule:0 action=accept
ap:0 action=drop
```

Рисунок 6.13: Состав политики доступа policy_accept

Проверка работоспособности управляющего и фильтрующих интерфейсов

12) Проверить функционирование управляющего и фильтрующих интерфейсов следующим образом.

12.1) Подключить сетевым кабелем управляющий интерфейс `EthC` к фильтрующему интерфейсу `Eth0`;

12.2) на сетевом интерфейсе УК установить IP-адрес **10.41.2.121** с IP-маской **255.255.255.128**;

12.3) подключить сетевым кабелем сетевой интерфейс УК к фильтрующему интерфейсу `Eth1` экземпляра устройства МЭ ССПТ-4А1;

12.4) проверить доступность управляющего интерфейса экземпляра устройства МЭ ССПТ-4А1, выполнив на УК команду **ping -c 3 10.41.2.120**. Если информация, выводимая в терминальном окне УК, выглядит следующим образом

```
$ ping -c 3 10.41.2.120
PING 10.41.2.120 (10.41.2.120): 56 data bytes
64 bytes from 10.41.2.120: icmp_seq=0 ttl=64 time=0.525 ms
64 bytes from 10.41.2.120: icmp_seq=1 ttl=64 time=0.333 ms
64 bytes from 10.41.2.120: icmp_seq=2 ttl=64 time=0.287 ms

--- 10.41.2.120 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
```

```
round-trip min/avg/max/stddev = 0.287/0.382/0.525/0.103 ms
```

значит шаг был выполнен успешно.

12.5) Повторить шаги 12.3)-12.4), подключая УК ко всем остальным фильтрующим интерфейсам (с разъемом RJ-45) экземпляра устройства МЭ ССПТ-4А1.

12.6) В случае, если экземпляр МЭ ССПТ-4А1 снабжен оптическими фильтрующими интерфейсами (исполнения: 03, 04, 05, 06, 07, 08), проверить функционирование оптических фильтрующих интерфейсов следующим образом (на примере исполнения 03).

12.6.1) подключить сетевым кабелем сетевой интерфейс УК к фильтрующему интерфейсу `Eth1` экземпляра устройства МЭ ССПТ-4А1;

12.6.2) подключить оптическими сетевыми кабелями интерфейс `Eth5` к интерфейсу `Eth6`, соблюдая направление передачи (например, TX Eth5 замкнуть с RX Eth6, TX Eth6 замкнуть с RX Eth5);

12.6.3) добавить общее правило фильтрации, разрешающее пропуск любого трафика с интерфейса `Eth1` на интерфейс `Eth5`:

```
fnp4> rule add rule:1 srcif=1 dstif=5 action=accept
FNPSH-I-007.02.3046-Общее правило добавлено (1)
```

12.6.4) добавить общее правило фильтрации, разрешающее пропуск любого трафика с интерфейса `Eth6` на интерфейс `Eth0`:

```
fnp4> rule add rule:2 srcif=6 dstif=0 action=accept
FNPSH-I-007.02.3046-Общее правило добавлено (2)
```

12.6.5) проверить доступность управляющего интерфейса экземпляра устройства МЭ ССПТ-4А1, выполнив на УК команду **`ping -c 3 10.41.2.120`**. Если информация, выводимая в терминальном окне УК, выглядит примерно следующим образом

```
$ ping -c 3 10.41.2.120
PING 10.41.2.120 (10.41.2.120): 56 data bytes
64 bytes from 10.41.2.120: icmp_seq=0 ttl=64 time=0.525 ms
64 bytes from 10.41.2.120: icmp_seq=1 ttl=64 time=0.333 ms
64 bytes from 10.41.2.120: icmp_seq=2 ttl=64 time=0.287 ms

--- 10.41.2.120 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.287/0.382/0.525/0.103 ms
```

значит шаг был выполнен успешно.

12.6.6) удалить общие правила №1 и №2, выполнив команду **`rule delete`** с соответствующими параметрами:

```
fnp4> rule delete rule:1
Удалить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3050-Общее правило удалено (1)
fnp4> rule delete rule:2
Удалить общее правило? (Y/N) [N]: y
FNPSH-I-007.02.3050-Общее правило удалено (2)
```

12.7) Для исполнений МЭ ССПТ-4А1, имеющих более двух оптических интерфейсов (исполнения: 06, 07, 08) **повторить шаги 12.6.2)-12.6.6)**, подключая попарно оптические

интерфейсы друг к другу, и добавляя соответствующие пары общих правил, обеспечивающих передачу трафика между интерфейсом `Eth1` и первым оптическим интерфейсом пары, а также между вторым оптическим интерфейсом пары и интерфейсом `Eth0`. Например для исполнения 06 потребуется подключить оптический интерфейс `Eth7` к оптическому интерфейсу `Eth8`, и при этом добавить два правила, обеспечивающих: передачу трафика с интерфейса `Eth1` на интерфейс `Eth7` и с `Eth8` на `Eth0` соответственно.

Проверка реализации правил фильтрации

13) **Проверить реализацию правил фильтрации** на примере функционирования общего правила, разрешающего пропуск IP-пакетов, а затем на примере общего правила, предписывающего удаление IP-пакетов, следующим образом.

13.1) Убедиться, что управляющий интерфейс `EthC` подключен сетевым кабелем к фильтрующему интерфейсу `Eth0` экземпляру устройства МЭ ССПТ-4А1.

13.2) Подключить сетевым кабелем сетевой интерфейс УК к фильтрующему интерфейсу `Eth1` экземпляра устройства МЭ ССПТ-4А1.

13.3) Убедиться, что остальные фильтрующие интерфейсы экземпляра МЭ ССПТ-4А1 не задействованы в схеме.

13.4) Включить регистрацию пакетов, выполнив команду **`log packet enable`**:

```
fnp4> log packet enable
FNPSH-I-007.02.303D-Регистрация пакетов включена
```

13.5) Очистить журнал регистрации пакетов, выполнив команду **`log packet clear`**:

```
fnp4> log packet clear
Очистить журнал регистрации пакетов? (Y/N) [N]: y
FNPSH-I-007.02.303E-Регистрация пакетов очищена
```

13.6) Добавить общее правило, разрешающее пропуск IP-пакетов с IP-адресом источника: **`10.41.2.121`** (УК) и IP-адресом приемника: **`10.41.2.120`** (МЭ), входной интерфейс – **`eth1`**, выходной интерфейс – **`eth0`**:

```
fnp4> rule add rule:1 srcif=eth1 dstif=eth0 srcip4=10.41.2.121 dstip4=10.41.2.120
log=enable action=accept
FNPSH-I-007.02.3046-Общее правило добавлено (1)
```

13.7) На УК выполнить команду: **`ping -c 1 10.41.2.120`**, и убедиться, что УК получил ICMP-ответ. Например:

```
$ ping -c 1 10.41.2.120
PING 10.41.2.120 (10.41.2.120): 56 data bytes
64 bytes from 10.41.2.120: icmp_seq=0 ttl=64 time=1.252 ms

--- 10.41.2.120 ping statistics ---
1 packets transmitted, 1 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.252/1.252/1.252/0.000 ms
```

13.8) Выполнить команду **`log packet show viewer=no order=asc`** и убедиться, что две последние записи в выводе команды соответствуют приведенным ниже (дата и время

регистрации будут отличаться от приведенных):

```
15:01:16.479014|accept|rule:1|eth1→eth0|IPv4/ICMP|10.41.2.121|10.41.2.120
15:01:16.479722|accept|rule:1|eth0→eth1|IPv4/ICMP|10.41.2.120|10.41.2.121
```

13.9) Изменить общее правило №1, так чтобы оно запрещало пропуск IP-пакетов с IP-адресом источника: **10.41.2.121** (УК) и IP-адресом приемника: **10.41.2.120** (МЭ):

```
fnp4> rule edit rule:1 action=drop
FNPSH-I-007.02.3046-Общее правило изменено (1)
```

13.10) На УК выполнить команду: **ping -c 1 10.41.2.120** и убедиться, что УК не получил ICMP-ответ. Например:

```
$ ping -c 1 10.41.2.120
PING 10.41.2.120 (10.41.2.120): 56 data bytes

--- 10.41.2.120 ping statistics ---
1 packets transmitted, 0 packets received, 100.0% packet loss
```

13.11) Выполнить команду **log packet show viewer=no order=asc** и убедиться, что последняя запись в выводе команды соответствуют приведенной ниже (дата и время регистрации будет отличаться от приведенной):

```
15:03:47.090217|drop|rule:1|eth1→|IPv4/ICMP|10.41.2.121| 10.41.2.120
```

Проверка процесса регистрации

14) **Проверить процесс регистрации** действий администратора. (проверка регистрации трафика выполняется в рамках пункта 13)) следующим образом.

14.1) Выполнить команду **log event show viewer=no order=asc** и убедиться, что последние зарегистрированные события соответствуют приведенным ниже (номера и время регистрации событий будут отличаться от приведенных):

```
86| 04.03.2021 14:59:23 UTC+0000 (UTC) | I-1029: Включение регистрации пакетов
(admin,Console)
87| 04.03.2021 14:59:31 UTC+0000 (UTC) | I-102A: Очистка текущего файла регистрации пакетов
(admin,Console)
88| 04.03.2021 14:59:45 UTC+0000 (UTC) | I-1030: Добавление правила фильтрации - Общее
правило #1 (admin,Console)
89| 04.03.2021 15:02:39 UTC+0000 (UTC) | I-1031: Изменение правила фильтрации - Общее
правило #1 (action) (admin,Console)
```

Проверка процесса идентификации и аутентификации администратора защиты

15) **Проверить процесс идентификации и аутентификации администратора защиты** следующим образом.

15.1) Завершить текущий сеанс работы администратора, выполнив команду **exit**.

15.2) Последовательно ввести учетные данные системного пользователя fnpsh и администратора МЭ ССПТ-4А1 admin, при этом для администратора admin ввести некорректный пароль.

15.3) Убедиться в выводе сообщения об ошибке:

```
FNPSH-E-007.02.1005-Вход администратора не выполнен
```

15.4) Убедиться, что вместо приглашения ввода команды выведен запрос ввода имени администратора:

```
Имя администратора:
```

15.5) Последовательно ввести учетные данные системного пользователя `fnpsh` и администратора МЭ ССПТ-4А1 `admin` (ввести корректные пароли для обеих учетных записей).

15.6) Убедиться в выводе на консоль информационного сообщения и приглашения к вводу команды:

```
FNPSH-I-007.02.3001-Успешная авторизация администратора (admin)
fnp4>
```

15.7) Выполнить команду **`log event show viewer=no order=asc`** и убедиться, что три последних зарегистрированных события соответствуют приведенным ниже (номера записей, даты и времена регистрации событий будут отличаться от приведенных):

```
90| 04.03.2021 15:03:50 UTC+0000 (UTC) | I-1004: Выход администратора - Командный
интерфейс; admin;  (admin,Console)
91| 04.03.2021 15:04:30 UTC+0000 (UTC) | W-2005: Вход администратора не выполнен -
Командный интерфейс; локальная аутентификация (admin,Console)
92| 04.03.2021 15:05:36 UTC+0000 (UTC) | I-1003: Вход администратора - Командный интерфейс;
admin; локальная аутентификация (admin,Console)
```

Проверка доступности WEB-интерфейса администратора

16) **Проверить работоспособность WEB-интерфейса** администратора МЭ ССПТ-4А1 следующим образом.

16.1) Запустить на УК программу WEB-браузера (раздел Ошибка: источник перекрёстной ссылки не найден, стр. Ошибка: источник перекрёстной ссылки не найден) и обратиться из нее по IP-адресу, назначенному управляющему интерфейсу экземпляра устройства МЭ ССПТ-4А1: **`https://10.2.1.157`**. Если в окне WEB-браузера отобразилась страница аутентификации администратора МЭ ССПТ-4А1 (рисунок 6.14, стр. 389), значит шаг был выполнен успешно.

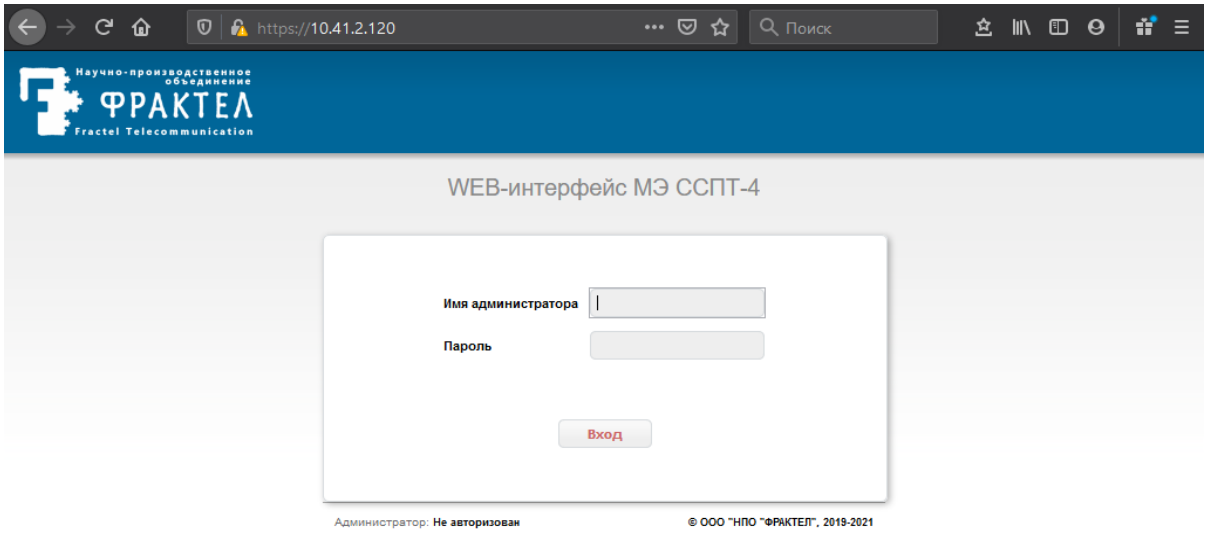


Рисунок 6.14: WEB-интерфейс. Страница аутентификации администратора

16.2) В поле ввода `Имя` администратора ввести: **`admin`**, в поле ввода `Пароль` ввести актуальный пароль данной учетной записи, нажать кнопку `Вход` (рисунок 6.15, стр. 389). Если аутентификация администратора выполнена, то будет загружена страница WEB-интерфейса: `Состояние: Устройство` (рисунок 6.16, стр. 390).

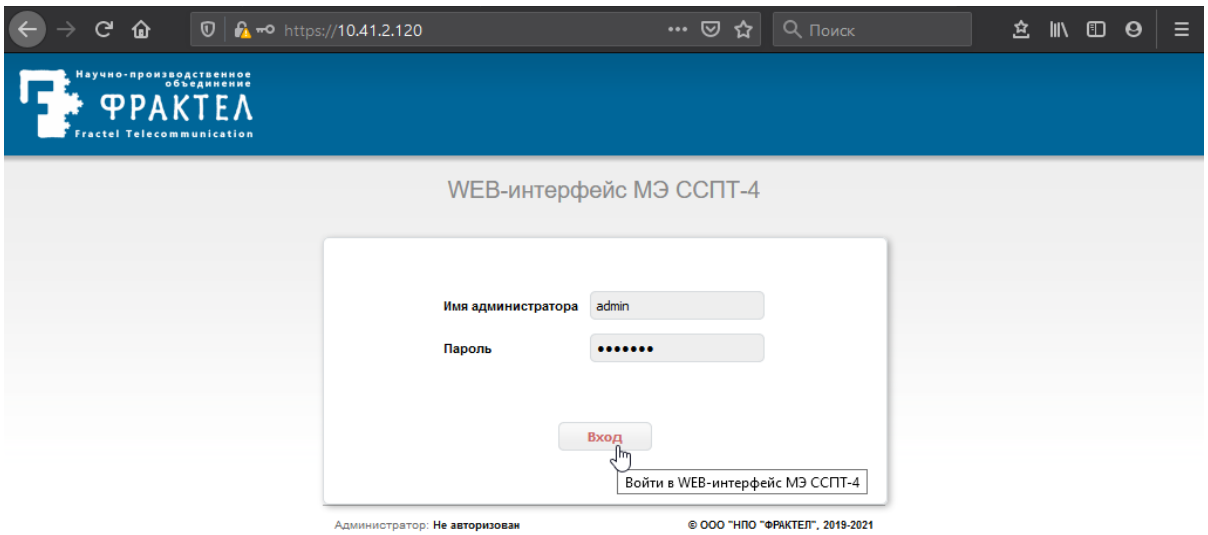


Рисунок 6.15: WEB-интерфейс. Ввод данных аутентификации администратора

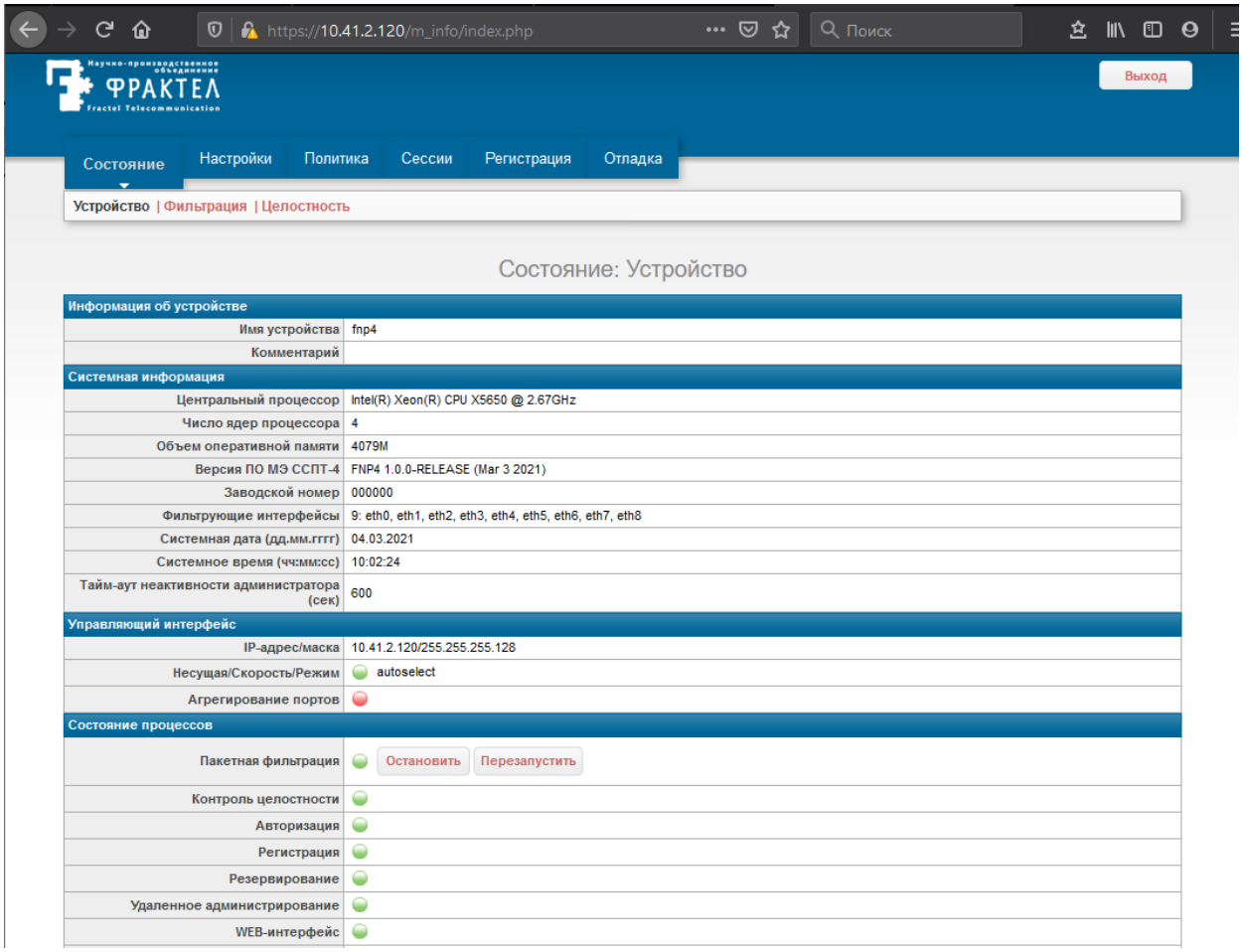


Рисунок 6.16: WEB-интерфейс. Результат успешной аутентификации

Проверка изолированности программной среды

17) **Проверить изолированность программной среды** следующим образом:

17.1) **Убедиться**, что в соответствии с требованиями раздела 2.7, стр. 51 настоящего Руководства управляющий сегмент Ethernet, подключенный к управляющему интерфейсу (`EthC`) МЭ ССПТ-4А1:

- физически изолирован от защищаемых сегментов;
- защищен от несанкционированного доступа организационными мерами.

17.2) **Убедиться в отсутствии доступа** к управляющему интерфейсу через фильтрующие интерфейсы следующим образом:

17.2.1) подключить сетевым кабелем сетевой интерфейс УК к управляющему интерфейсу (`EthC`) экземпляра устройства МЭ ССПТ-4А1;

17.2.2) проверить доступность управляющего интерфейса экземпляра устройства МЭ ССПТ-4А1, выполнив на УК команду **`ping -c 3 10.41.2.120`**. Если информация, выводимая в терминальном окне УК, выглядит следующим образом

```
$ ping -c 3 10.41.2.120
PING 10.41.2.120 (10.41.2.120): 56 data bytes
```

```
64 bytes from 10.41.2.120: icmp_seq=0 ttl=64 time=0.420 ms
64 bytes from 10.41.2.120: icmp_seq=1 ttl=64 time=0.326 ms
64 bytes from 10.41.2.120: icmp_seq=2 ttl=64 time=0.251 ms

--- 10.41.2.120 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.251/0.332/0.420/0.069 ms
```

значит шаг был выполнен успешно.

17.2.3) удалить ARP-запись с IP-адресом управляющего интерфейса МЭ ССПТ-4А1 (**`10.41.2.120`**) из ARP-таблицы УК средствами ОС, например, следующей командой:

```
# arp -d 10.41.2.120
10.41.2.120 (10.41.2.120) deleted
```

17.2.4) подключить сетевым кабелем сетевой интерфейс УК к фильтрующему интерфейсу `Eth0` экземпляра устройства МЭ ССПТ-4А1;

17.2.5) убедиться в отсутствии доступа к управляющему интерфейсу экземпляра устройства МЭ ССПТ-4А1, выполнив на УК команду **`ping -c 3 10.41.2.120`**. Если информация, выводимая в терминальном окне УК, выглядит следующим образом

```
$ ping -c 3 10.41.2.120
PING 10.41.2.120 (10.41.2.120): 56 data bytes

--- 10.41.2.120 ping statistics ---
3 packets transmitted, 0 packets received, 100.0% packet loss
```

значит шаг был выполнен успешно.

17.2.6) средствами ОС убедиться в отсутствии ARP-записи для IP-адреса **`10.41.2.120 в`** ARP-таблице УК, например, следующей командой:

```
$ arp 10.41.2.120
10.41.2.120 (10.41.2.120) -- no entry
```

17.3) Повторить шаги 17.2.4)-17.2.6) для всех остальных фильтрующих интерфейсов (с разъемом RJ-45) экземпляра устройства МЭ ССПТ-4А1.

Проверка управления дополнительными конфигурациями и политиками доступа (окончание)

18) **Проверить восстановление сохраненных настроек экземпляра МЭ ССПТ-4А1** путем последовательного применения предварительно сохраненной дополнительной конфигурации и дополнительной политики доступа следующим образом.

18.1) **Применить дополнительную конфигурацию** с помощью команды **`config apply`** следующим образом.

18.1.1) Уточнить имя сохраненной дополнительной конфигурации, выполнив команду **`config list`**:

```
fnp4> config list
Список дополнительных конфигураций:
    Имя                      Последнее изменение                Комментарий
    fnp4-fnp4-20210304-090949 04.03.2021 09:09:49 UTC+0000 (UTC)
Занято: 1       Свободно: 15
```

Имя дополнительной конфигурации: “**fnp4-fnp4-20210304-090949**”.

18.1.2) Применить дополнительную конфигурацию, выполнив команду **config apply**:

```
fnp4> config apply name=fnp4-fnp4-20210304-090949
Применить дополнительную конфигурацию? (Возможна потеря соединения) (Y/N) [N]: Y
FNPSH-I-007.02.3112-Пакетный фильтр перезапущен
FNPSH-I-007.02.3024-Дополнительная конфигурация применена (fnp4-fnp4-20210304-090949)
```

Если было получено диагностическое сообщение с кодом FNPSH-I-007.02.3024, значит дополнительная конфигурация была успешно применена.

18.2) **Применить дополнительную политику доступа** с помощью команды **policy apply**. следующим образом.

18.2.1) Уточнить имя сохраненной дополнительной политики доступа, выполнив команду **policy list**:

```
fnp4> policy list
Список дополнительных политик:
    Имя                      Последнее изменение                Комментарий
    fnp4-fnp4-20210304-091138 04.03.2021 09:11:38 UTC+0000 (UTC)
    policy_accept            03.03.2021 08:19:32 UTC+0000 (UTC) всё разрешено
    policy_drop              03.03.2021 08:19:32 UTC+0000 (UTC) всё запрещено
Занято: 3       Свободно: 29
```

Имя дополнительной политики доступа: “**fnp4-fnp4-20210304-091138**”.

18.2.2) Применить дополнительную политику доступа, выполнив команду **policy apply**:

```
fnp4> policy apply name=fnp4-fnp4-20210304-091138
Применить дополнительную политику (режим управления сессиями)? (Y/N) [N]: Y
FNPSH-I-007.02.30FC-Дополнительная политика применена (правила и справочник)
```

Если было получено диагностическое сообщение с кодом FNPSH-I-007.02.30FC, значит дополнительная политика доступа была успешно применена.

19) **Удалить дополнительную конфигурацию и дополнительную политику доступа**, созданные в процессе выполнения процедуры регламентного тестирования следующим образом:

19.1) Уточнить список имеющихся дополнительных конфигураций, выполнив команду **config list**:

```
fnp4> config list
Список дополнительных конфигураций:
    Имя                      Последнее изменение                Комментарий
    fnp4-fnp4-20210304-090949 04.03.2021 09:09:49 UTC+0000 (UTC)
Занято: 1       Свободно: 15
```

Дополнительная конфигурация для удаления: “**fnp4-fnp4-20210304-090949**”.

19.2) Удалить дополнительную конфигурацию, выполнив команду **config remove**:

```
fnp4> config remove name=fnp4-fnp4-20210304-090949
Удалить дополнительную конфигурацию? (Y/N) [N]: Y
FNPSH-I-007.02.3023-Дополнительная конфигурация удалена (fnp4-fnp4-20210304-090949)
```

Если было получено диагностическое сообщение с кодом FNPSH-I-007.02.3023, значит дополнительная конфигурация была успешно удалена.

19.3) Уточнить список имеющихся дополнительных политик доступа, выполнив команду **policy list**:

```
fnp4> policy list
Список дополнительных политик:
    Имя                     Последнее изменение                Комментарий
    fnp4-fnp4-20210304-091138 04.03.2021 09:11:38 UTC+0000 (UTC)
    policy_accept           03.03.2021 08:19:32 UTC+0000 (UTC) всё разрешено
    policy_drop             03.03.2021 08:19:32 UTC+0000 (UTC) всё запрещено
Занято: 3       Свободно: 29
```

Дополнительная политика доступа для удаления: “**fnp4-fnp4-20210304-091138**”.

19.4) Удалить дополнительную политику доступа, выполнив команду **policy remove**:

```
fnp4> policy remove name=fnp4-fnp4-20210304-091138
Удалить дополнительную политику? (Y/N) [N]: Y
FNPSH-I-007.02.30FE-Дополнительная политика удалена
```

Если было получено диагностическое сообщение с кодом `FNPSH-I-007.02.30FE`, значит дополнительная политика доступа была успешно удалена.

7. Средство обновления и восстановления

Средство обновления и восстановления МЭ ССПТ-4А1 предоставляет следующие основные возможности:

- восстановление файловой системы УОС МЭ ССПТ-4А1 или отдельных конфигурационных файлов МЭ ССПТ-4А1;
- обновление ПО МЭ ССПТ-4А1 с использованием предварительно записанного на USB-носитель файла обновлений.

СОВа-4 предоставляется на USB-носителе, входящем в комплект поставки МЭ ССПТ-4А1. Для использования СОВа-4 необходимо выполнить следующую последовательность действий.

При включенном МЭ ССПТ-4А1:

1) подключиться к МЭ ССПТ-4А1 через системную консоль (раздел 2.5, стр. 47);
2) вставить USB-носитель СОВа-4 в USB-разъем МЭ ССПТ-4А1;
3) выполнить перезагрузку МЭ ССПТ-4А1 через командный интерфейс.

При выключенном МЭ ССПТ-4А1:

1) подключиться к МЭ ССПТ-4А1 через системную консоль (раздел 2.5, стр. 47);
2) вставить USB-носитель СОВа-4 в USB-разъем МЭ ССПТ-4А1;
3) включить МЭ ССПТ-4А1, используя кнопку включения питания.

В результате выполнения указанных действий вместо УОС МЭ ССПТ-4А1 будет загружена УОС СОВа-4 с USB-носителя. При этом будет автоматически запущено ПО СОВа-4. При запуске СОВа-4 выводится приветственное окно “**О программе**”, в котором выводится версия ПО СОВа-4. Данное окно автоматически закрывается в течение нескольких секунд и становится доступным Главное меню ПО СОВа-4. Состав главного меню приведен на рисунке 7.1, стр. 395.

Главное меню включает в себя следующие пункты:

- **Устройство**: функции управления устройством (выключение, перезагрузка, вывод информации об экземпляре устройства);
- **Восстановление**: функции восстановления конфигурационных файлов и паролей учетных записей, используемых для администрирования МЭ ССПТ-4А1, а также полное восстановление всех файлов и каталогов на носителе данных МЭ ССПТ-4А1;
- **Обновление**: обновление ПО МЭ ССПТ-4А1 из файла обновления, предварительно записанного администратором на FAT-раздел USB-носителя СОВа-4;

- **О программе**: вывод версии ПО СОВа-4.

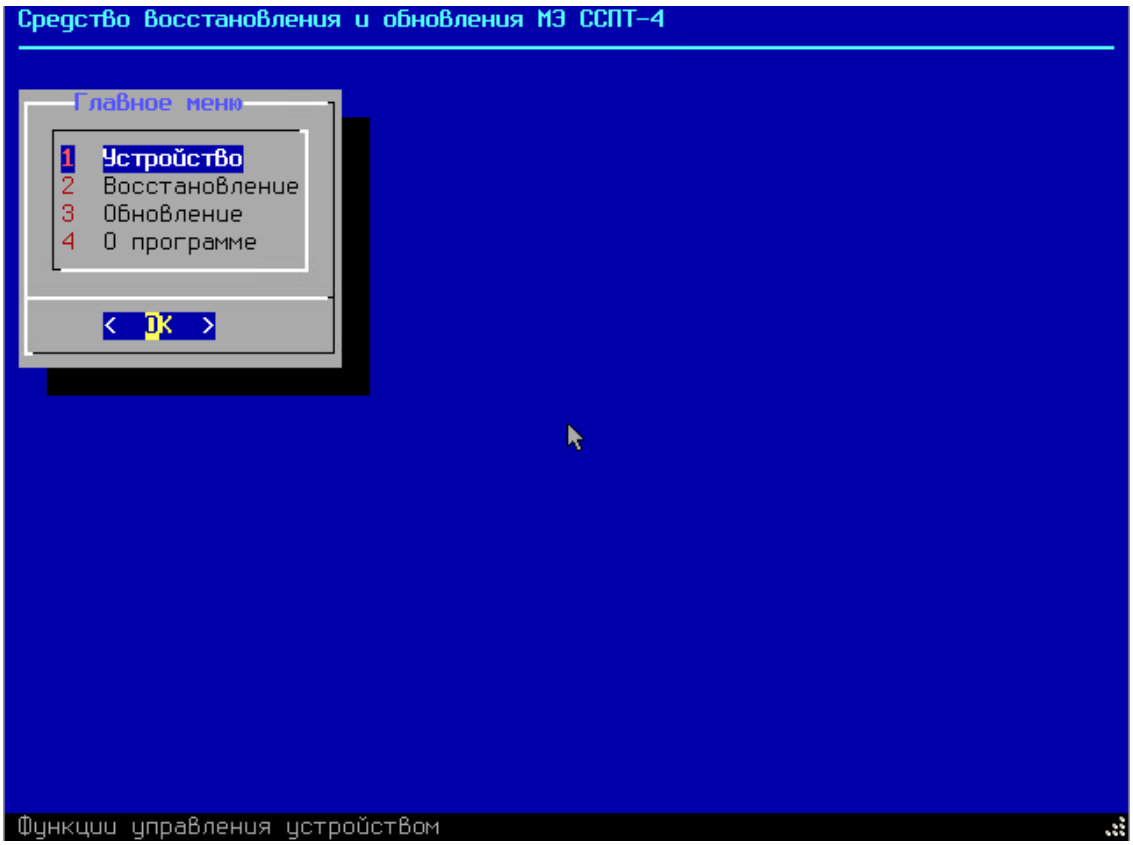


Рисунок 7.1: Главное меню СОВа-4

Для навигации в интерфейсе ПО СОВа-4 используются клавиши, представленные в таблице 7.1, стр. 395.

Таблица 7.1: Клавиши навигации в интерфейсе ПО *СОВа-4*

Управление	***Назначение***
<↑>	Переход к предыдущему пункту меню
<↓>	Переход к следующему пункту меню
<←>,	В диалоговом окне выделить кнопку слева от текущей выделенной кнопки
<→>	В диалоговом окне выделить кнопку справа от текущей выделенной кнопки
<Enter>	Выбор выделенного пункта меню. Подтверждение действия в диалоговом окне.
<Esc>	Возврат к меню предыдущего уровня
<Tab>	В диалоговом окне выделить следующую по порядку следования кнопку (Порядок следования: слева направо, сверху вниз. Переход выполняется циклически: если выделена последняя кнопка, то переход будет выполнен к первой.
1..N	Быстрый переход к пункту меню с соответствующим номером. Номер пункта меню всегда указывается перед названием пункта меню в той же строке.

ПО СОВа-4 запускается автоматически при загрузке с USB-носителя СОВа-4.

USB-носитель СОВа-4 из комплекта поставки МЭ ССПТ-4А1 предназначен для использования только в паре с данным экземпляром МЭ ССПТ-4А1. При попытке использования ПО СОВа-4 и МЭ ССПТ-4А1 из разных комплектов основной функционал ПО СОВа-4 будет заблокирован для использования. Администратору будут доступны лишь следующие функции ПО СОВа-4:

- перезагрузка МЭ;
- останов МЭ;
- просмотр информации об экземпляре МЭ ССПТ-4А1.

Для использования СОВа-4 в BIOS МЭ ССПТ-4А1 должна быть включена функция загрузки с USB-носителя. При этом USB-носитель должен быть указан первым устройством в списке устройств для загрузки.

7.1. Устройство

Для перехода к `Меню управления устройством` необходимо выбрать пункт **`Устройство`** главного меню ПО СОВа-4. Данный пункт главного меню выделен по умолчанию после запуска ПО СОВа-4, а также после возврата в главное меню из меню следующего за ним уровня.

Состав **`Меню управления устройством`** представлен на рисунке 7.2, стр. 396.

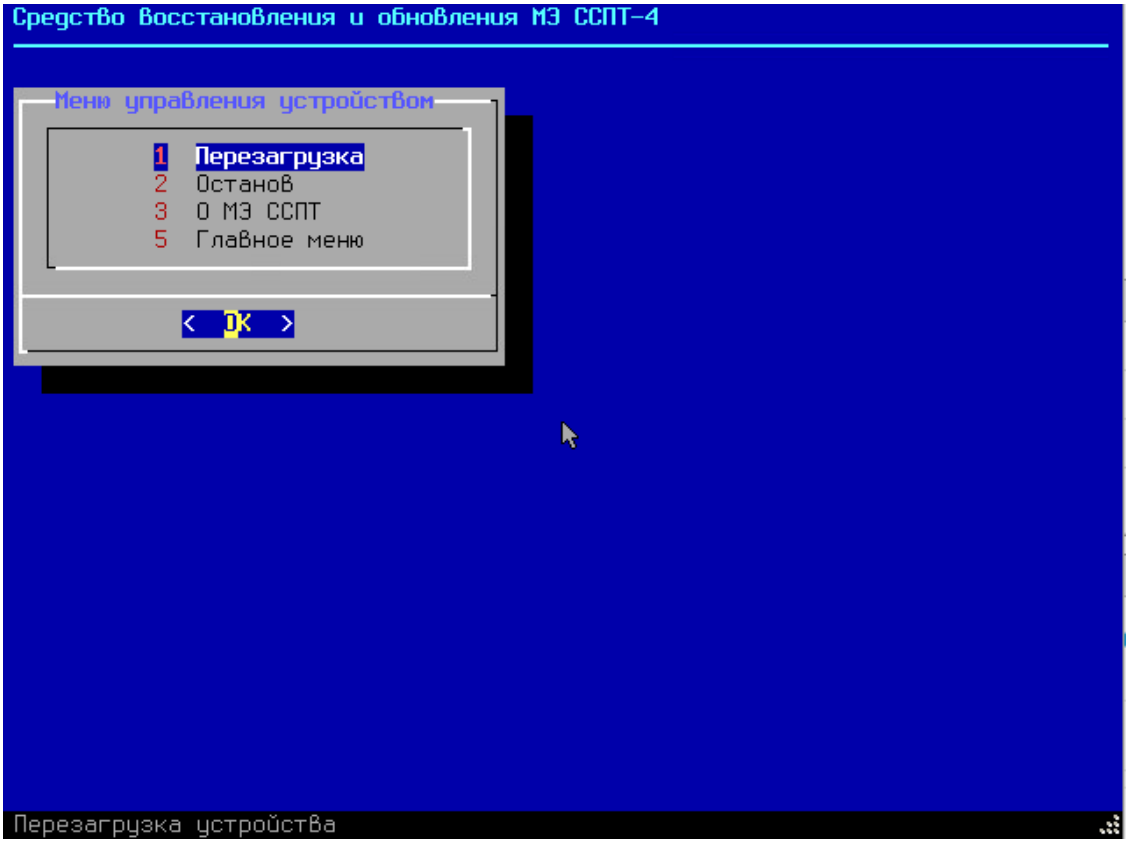


Рисунок 7.2: Меню управления устройством

`Меню управления устройством` содержит следующие пункты:

- **`Перезагрузка`**: выполняется перезагрузка МЭ ССПТ-4А1.
- **`Останов`**: выполняется останов УОС СОВа-4. При этом питание устройства будет выключено.
- **`О МЭ ССПТ`**: выводится информация о данном экземпляре МЭ ССПТ-4А1;

- **Главное меню**: осуществляется возврат в главное меню ПО СОВа-4 (возврат в главное меню также может быть выполнен по клавише **<Esc>**).

> Функция *Перезагрузка* служит для перезагрузки устройства МЭ ССПТ-4А1 с последующей загрузкой УОС МЭ ССПТ-4А1. Необходимо, чтобы USB-носитель СОВа-4 был вовремя извлечен из USB-разъема устройства (сразу после того как интерфейс ПО СОВа-4 исчезнет с консоли в результате старта процедуры перезагрузки). В противном случае будет выполнена повторная загрузка УОС СОВа-4.
>
> Функции управления устройством не вносят изменений в ФС МЭ ССПТ-4А1, поэтому доступны всегда, в том числе когда экземпляр ПО СОВа-4 не соответствует экземпляру МЭ ССПТ-4А1.

При выборе в Меню управления устройством пункта **Перезагрузка** или **Останов** выводится диалоговое окно подтверждения действия. Выбор по умолчанию для данных действий – кнопка **<Да>**: выполнить действие. Пример подтверждения перезагрузки устройства приведен на рисунке 7.3, стр. 397.

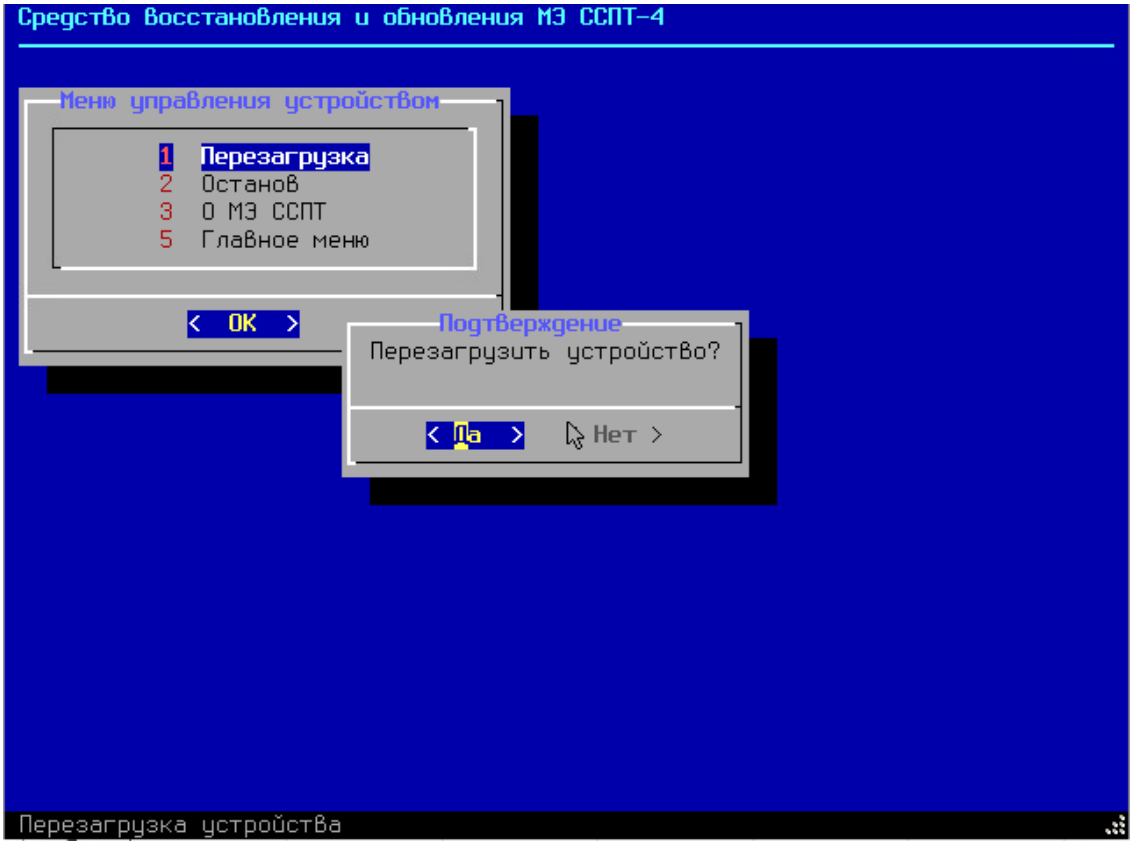


Рисунок 7.3: Подтверждение перезагрузки устройства

При выборе пункта **О МЭ ССПТ** открывается окно с информацией о данном экземпляре МЭ ССПТ-4А1. Пример вывода информации об экземпляре МЭ ССПТ-4А1 приведен на рисунке 7.4, стр 398.

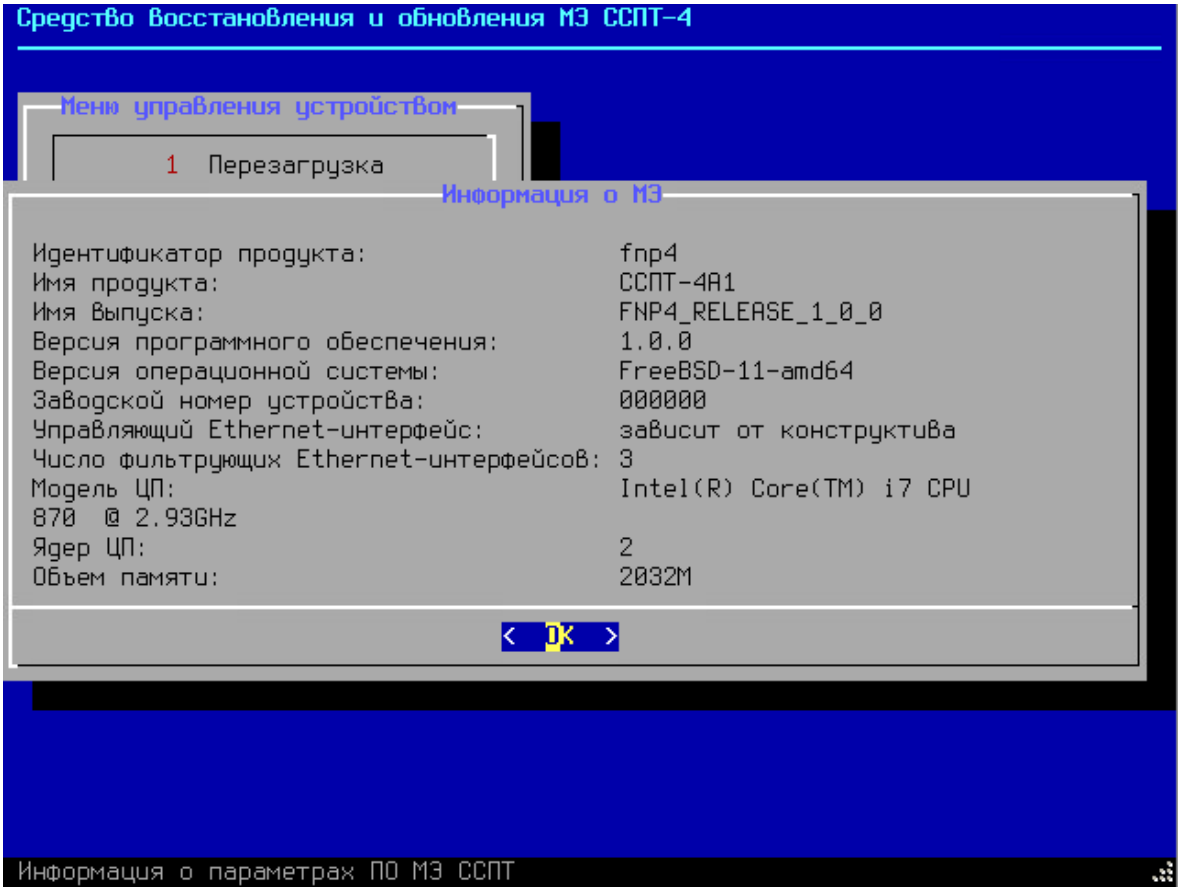


Рисунок 7.4: Пример вывода информации об экземпляре МЭ ССПТ-4А1

Информация об экземпляре МЭ ССПТ-4А1 включает в себя следующие данные:

- ✔ **Идентификатор продукта** – символьный идентификатор продукта, который состоит из символов латинского алфавита и числа (значение: `fnp4`);
- ✔ **Имя продукта** – официальное кириллическое имя продукта (значение: `ССПТ-4А1`);
- ✔ **Имя выпуска** – строка имени, присвоенного данному выпуску ПО МЭ ССПТ-4А1, состоящая из символов латинского алфавита и цифр. Содержит в себе также номер версии ПО МЭ ССПТ-4А1;
- ✔ **Версия программного обеспечения** – номер версии ПО МЭ ССПТ-4А1 в формате `X.X.X`, где `X` – десятичное число);
- ✔ **Версия операционной системы** – строка, содержащая версию и разрядность УОС МЭ (например: `FreeBSD-11-amd64`);
- ✔ **Заводской номер устройства** – шестизначный уникальный номер данного экземпляра МЭ;
- ✔ **Управляющий Ethernet-интерфейс** – вариант расположения управляющего Ethernet-интерфейса МЭ среди всех Ethernet-интерфейсов устройства (допустимые варианты: первый или последний);
- ✔ **Число фильтрующих Ethernet-интерфейсов**;

- ✔ **Модель ЦП** – строка, содержащая в себе название модели и тактовую частоту ЦП устройства;
- ✔ **Ядер ЦП** – число ядер ЦП устройства;
- ✔ **Объем памяти** – объем оперативной памяти устройства (RAM) в Мегабайтах.

7.2. Восстановление

Для перехода к Меню восстановления необходимо в главном меню ПО СОВа-4 выбрать пункт **Восстановление** (рисунок 7.5, стр. 399). Состав **Меню восстановления** представлен на рисунке 7.6, стр. 400.

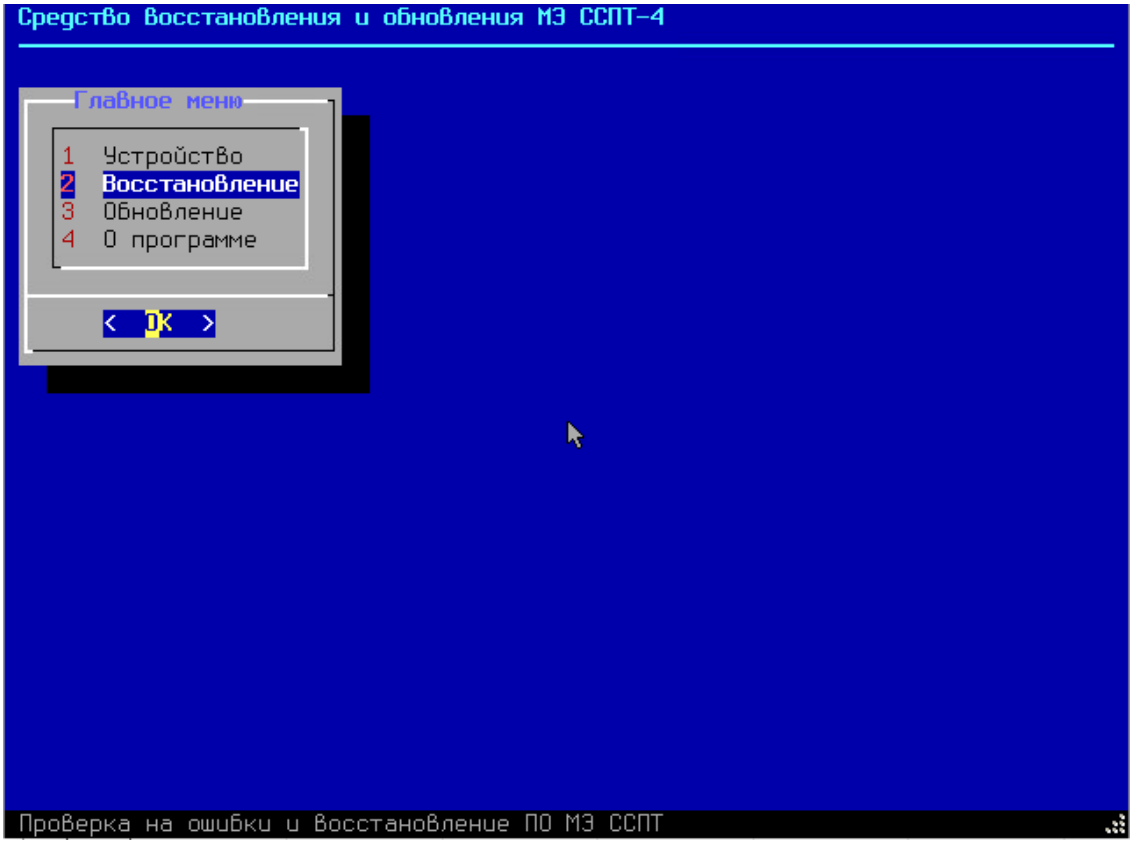


Рисунок 7.5: Переход к меню восстановления

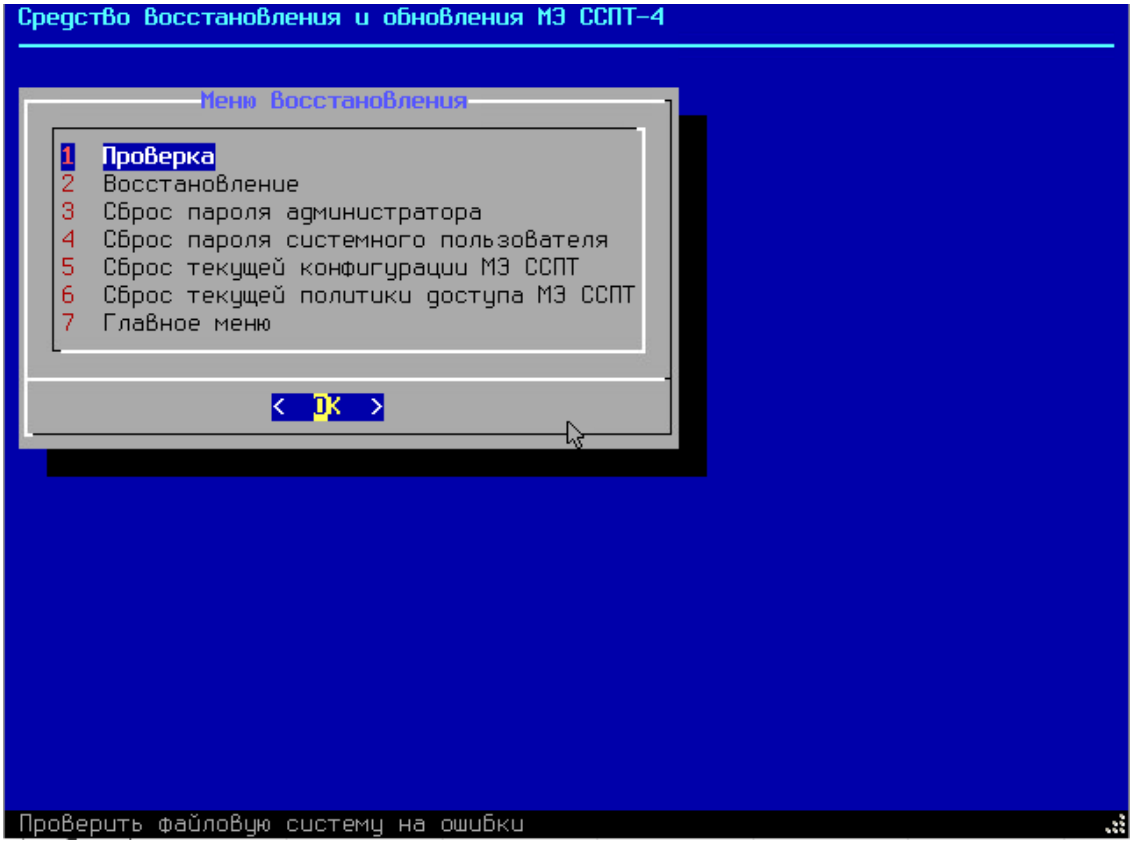


Рисунок 7.6: Меню восстановления

`Меню восстановления` содержит следующие пункты:

- **`Проверка`**: проверка носителя данных МЭ ССПТ-4А1 на наличие ошибок файловой системы;
- **`Восстановление`**: полное восстановление каталогов и файлов носителя данных МЭ ССПТ-4А1 из dump-образа;
- **`Сброс пароля администратора admin`**: сброс пароля администратора `admin` в значение по умолчанию;
- **`Сброс пароля системного пользователя`**: сброс пароля системного пользователя `fnpsh` в значение по умолчанию;
- **`Сброс текущей конфигурации МЭ ССПТ`**: сброс текущей конфигурации ССПТ-4А1 в состояние по умолчанию;
- **`Сброс текущей политики доступа МЭ ССПТ`**: сброс текущей политики доступа ССПТ-4А1 в состояние по умолчанию.
- **`Главное меню`**: возврат в главное меню ПО СОВа-4 (возврат в главное меню также может быть выполнен по клавише **`<Esc>`**).

Все пункты *Меню восстановления*, кроме пункта *Проверка*, в соответствующем диалоговом окне подтверждения действия имеют в качестве выбора по умолчанию кнопку <*Нет*>. Это связано с тем, что все действия по восстановлению вносят те или иные изменения в файлы носителя данных МЭ ССПТ-4А1, что в определенных случаях может привести к потере информации (например, в случае отсутствия необходимой дополнительной политики при сбросе текущей политики доступа).

7.2.1. Проверка файловой системы носителя МЭ ССПТ-4А1.

Пункт меню **Проверка** выполняет проверку целостности файловой системы носителя данных МЭ ССПТ-4А1. При нажатии **<Enter>** выводится диалоговое окно для подтверждения старта процедуры проверки. Пример приведен на рисунке 7.7, стр. 401.

В ходе процедуры проверки выводятся выполняемые действия, по завершении проверки выводится отчет о результате проверки. Пример отчета приведен на рисунке 7.8, стр. 402. По нажатию **<Enter>** выводится сообщение о том, что проверка файловой системы носителя данных МЭ ССПТ-4А1 завершена. Пример данного сообщения приведен на рисунке 7.9, стр. 402. По нажатию **<Enter>** происходит возврат к Меню восстановления.

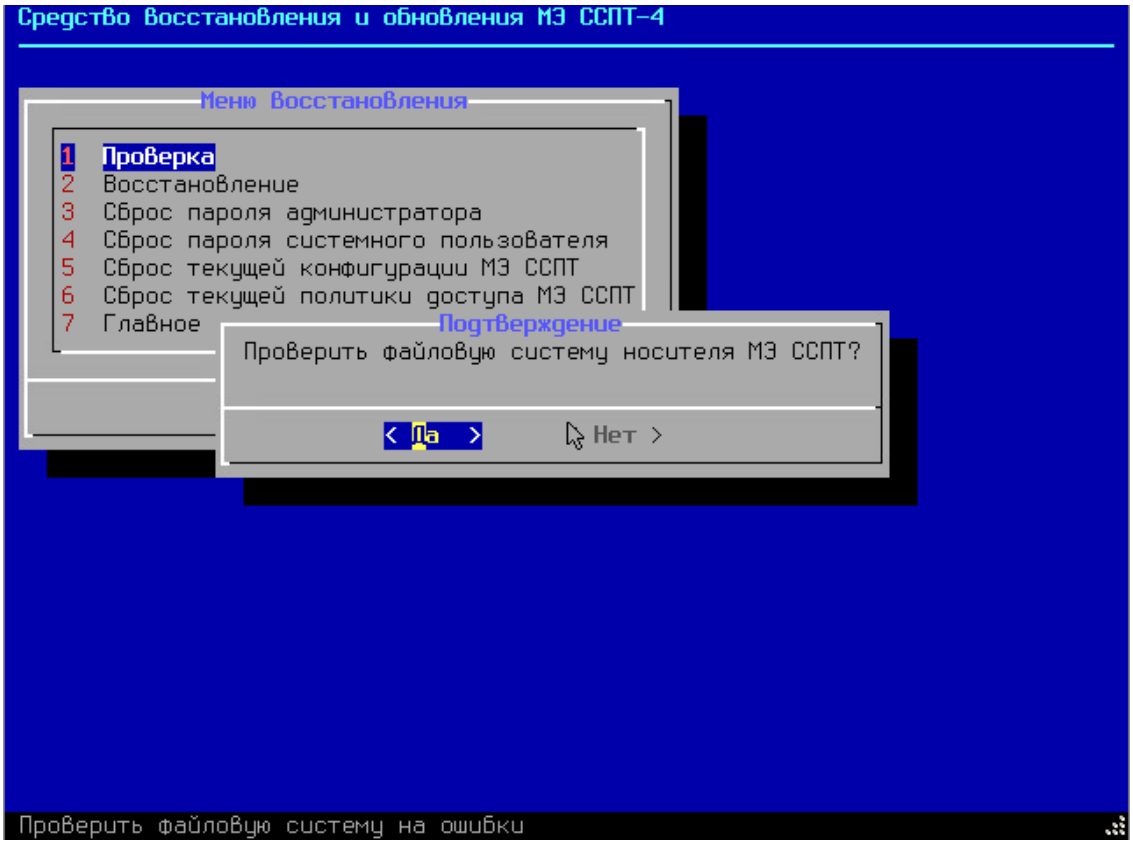


Рисунок 7.7: Подтверждение старта процедуры проверки файловой системы

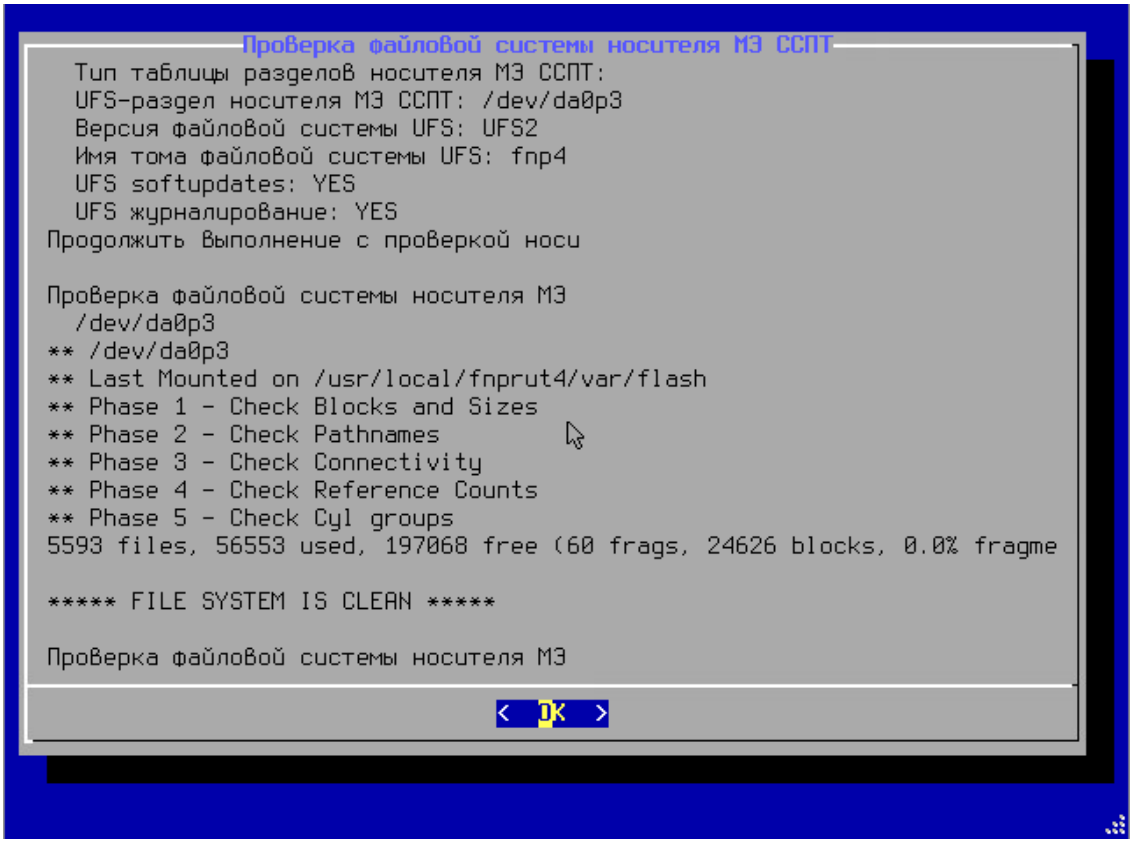


Рисунок 7.8: Отчет о результате проверки

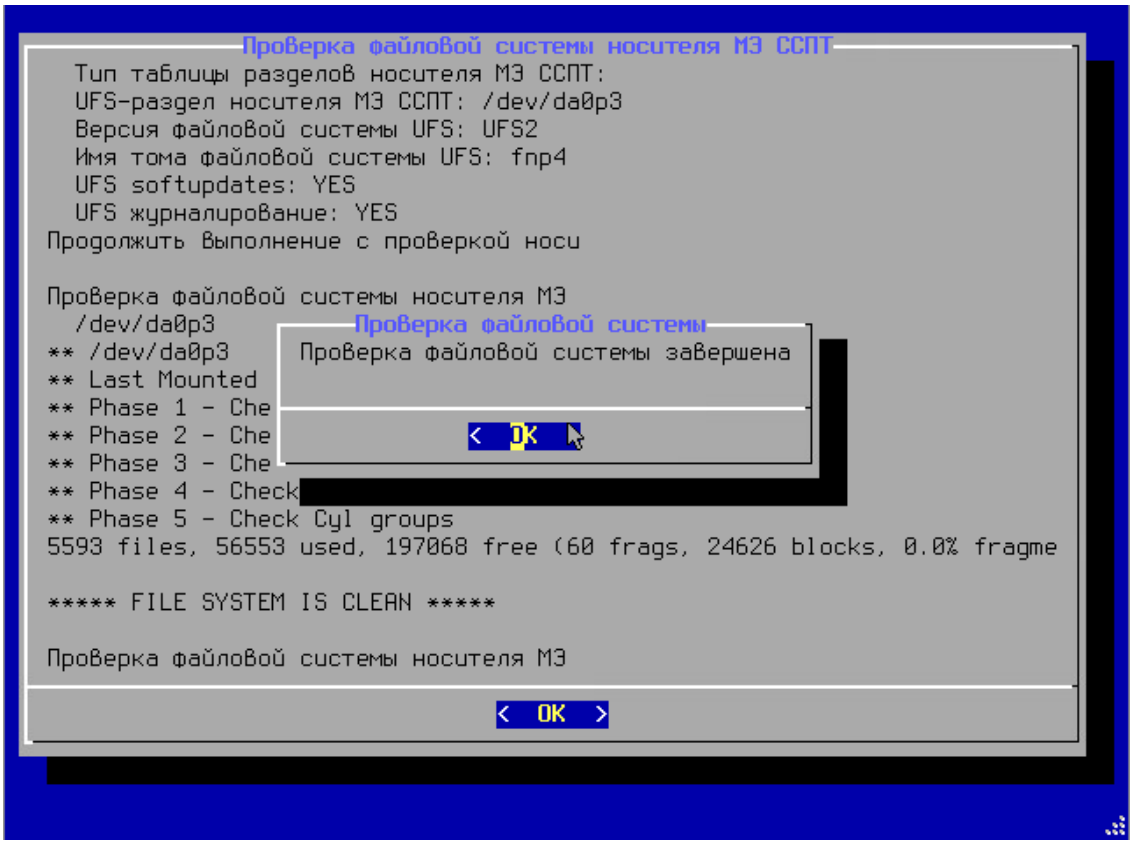


Рисунок 7.9: Сообщение о завершении процедуры проверки

7.2.2. Восстановление ПО МЭ ССПТ-4А1

Пункт **Восстановление** одноименного меню служит для восстановления всех файлов и каталогов МЭ ССПТ-4А1 из сохраненного на USB-носителе СОВа-4 dump-образа.

Если обновление ПО еще не выполнялось средствами ПО СОВа-4, то в результате выполнения функции *Восстановление* МЭ ССПТ-4А1 будет восстановлен к “заводскому” состоянию:

- текущая конфигурация будет сброшена в состояние по умолчанию;
- текущая политика доступа будет сброшена в состояние по умолчанию;
- все учетные записи, изначально имеющиеся на устройстве (администратор **admin**, системный пользователь **fnpsh**, пользователь SNMP-интерфейса **fnpsnmp**) будут иметь пароли по умолчанию;
- все дополнительно созданные учетные записи (администраторов и сетевых пользователей) будут утеряны;
- все созданные администратором дополнительные политики доступа и конфигурации будут утеряны (дополнительные политики **policy_accept** и **policy_drop** будут сброшены в состояние по умолчанию).

Если обновление ПО ранее уже выполнялось средствами ПО СОВа-4, то, в результате выполнения функции *Восстановление*, МЭ ССПТ-4А1 будет восстановлен к состоянию на момент завершения последней процедуры обновления. Все изменения (конфигурации, политики доступа, учетные записи и т.д,), произведенные после выполнения последней процедуры обновления, будут утеряны.

При выборе пункта **Восстановление** перед началом процедуры восстановления будет выведено стандартное окно подтверждения с выбором по умолчанию: **<Нет>**. В случае подтверждения действия (нажатие **<Enter>** по кнопке **<Да>**) начнется процедура восстановления ПО МЭ ССПТ-4А1. Во время процедуры восстановления в текстовой форме выводятся выполняемые действия. По завершении становится доступной кнопка **<OK>**. Пример вывода по завершении процедуры восстановления приведен на рисунке 7.10, стр 404. По нажатию на кнопку **<OK>** выводится сообщение об успешном завершении процедуры восстановления. Пример сообщения приведен на рисунке 7.11, стр. 404.

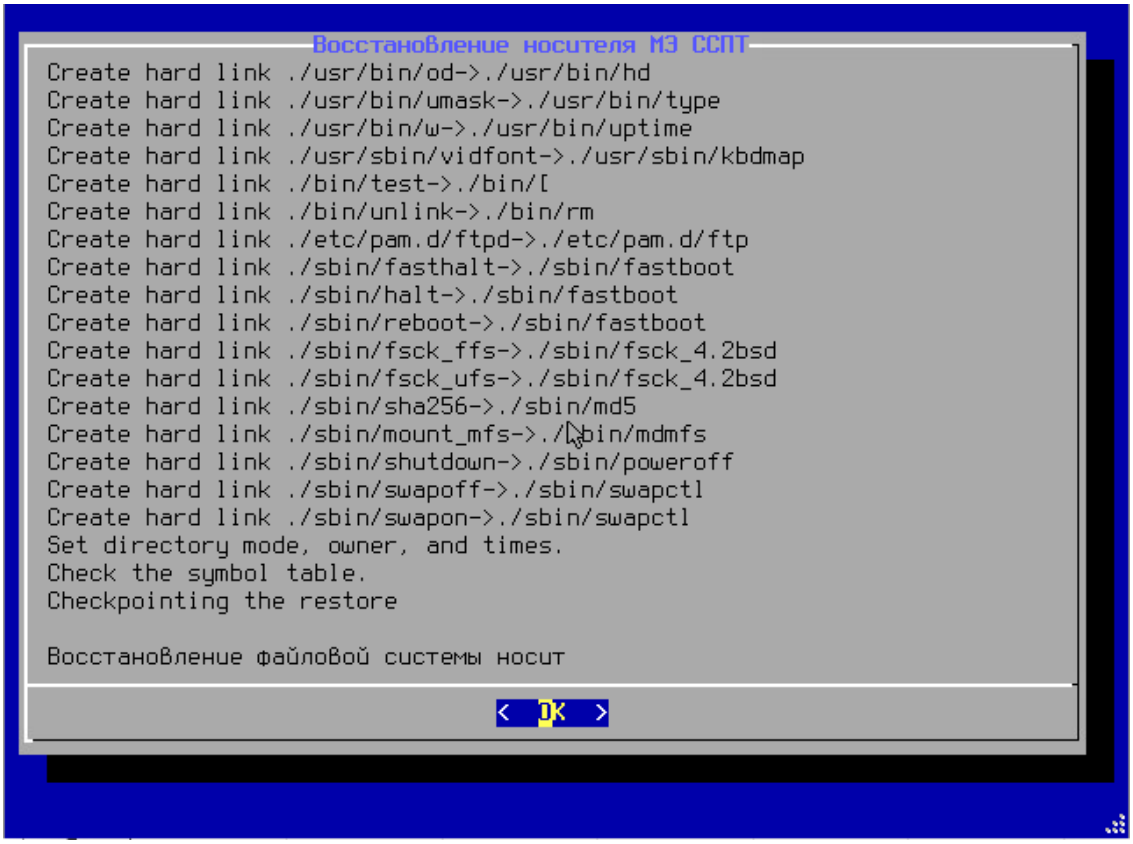


Рисунок 7.10: Пример вывода по завершении процедуры восстановления

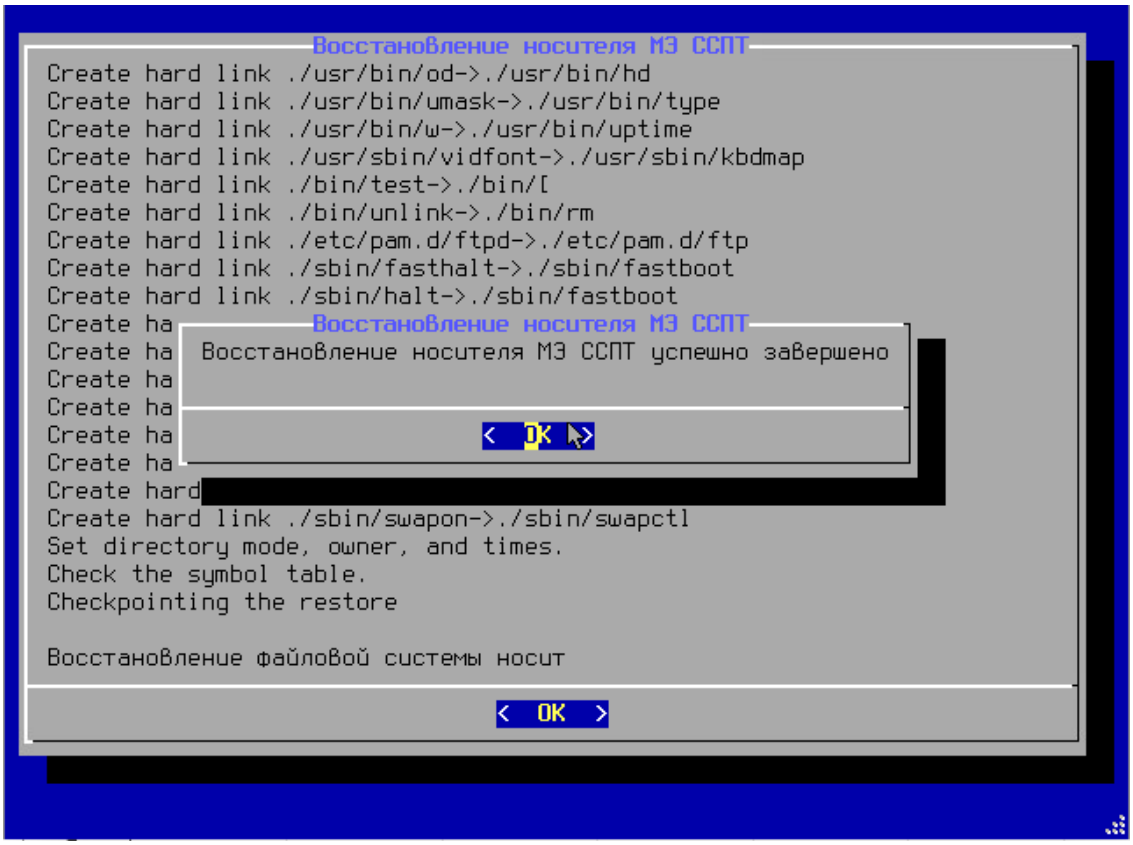


Рисунок 7.11: Сообщение об успешном завершении процедуры восстановления

7.2.3. Функции сброса

Меню восстановления предоставляет следующие функции сброса:

- **Сброс пароля администратора admin**: сброс пароля администратора admin в значение по умолчанию;
- **Сброс пароля системного пользователя**: сброс пароля системного пользователя fnpsh в значение по умолчанию;
- **Сброс текущей конфигурации МЭ ССПТ**: сброс текущей конфигурации МЭ ССПТ-4А1 в состояние по умолчанию;
- **Сброс текущей политики доступа МЭ ССПТ**: сброс текущей политики доступа МЭ ССПТ-4А1 в состояние по умолчанию.

Для каждого пункта меню, относящего к сбросу, выводится диалоговое окно подтверждения действия с выбором по умолчанию: **Нет**. При успешном выполнении сброса выбранной сущности выводится стандартное сообщение об успешном выполнении действия. Пример подтверждения сброса пароля администратора admin приведен на рисунке 7.12, стр. 405. Пример сообщения об успешном сбросе пароля администратора admin – на рисунке 7.13, стр. 406.

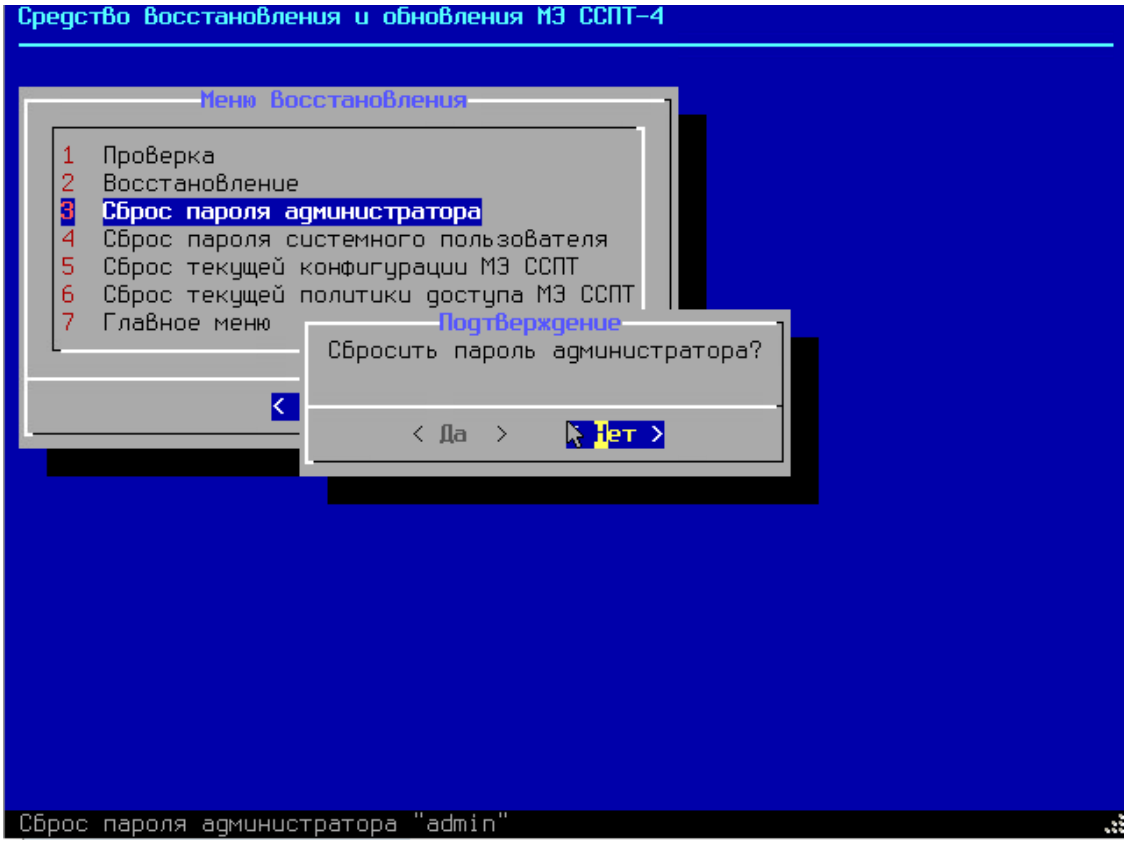


Рисунок 7.12: Подтверждение сброса пароля администратора admin

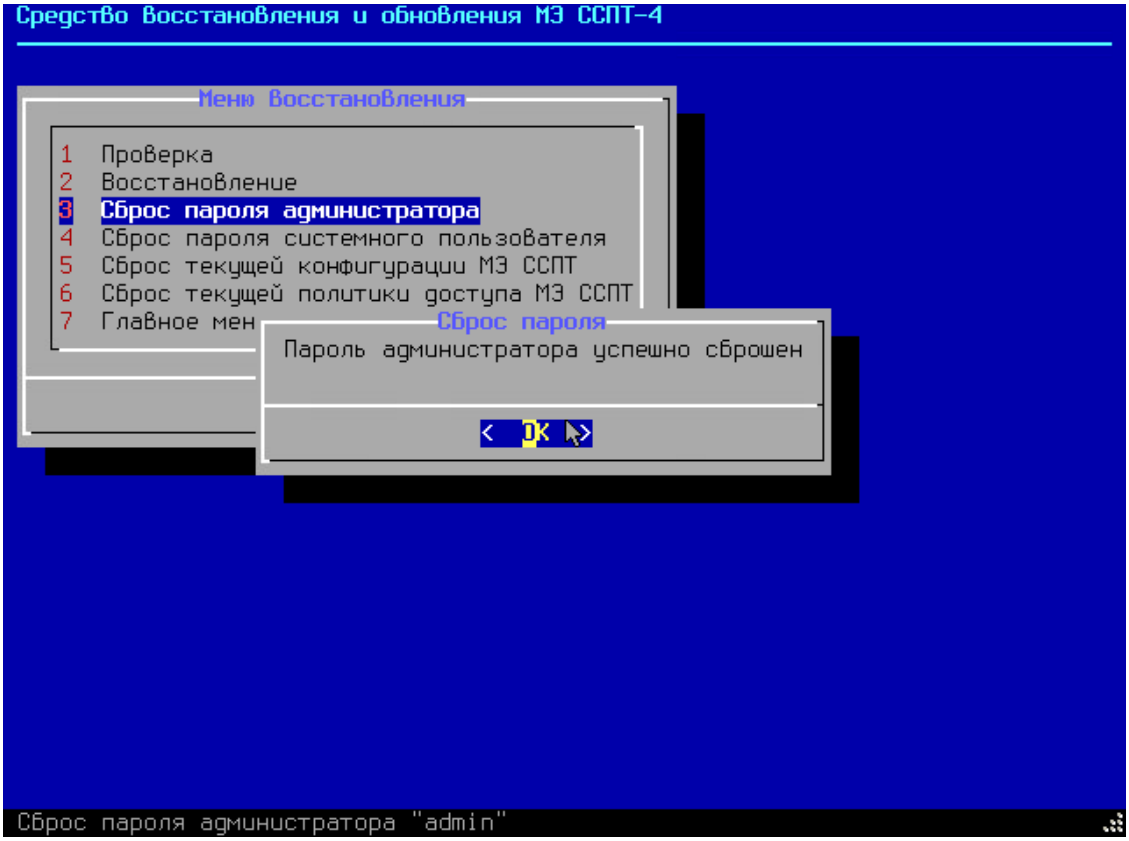


Рисунок 7.13: Сообщение об успешном сбросе пароля администратора admin

При сбросе текущей конфигурации или политики доступа МЭ ССПТ-4А1 в случае необходимости администратор должен сам заранее позаботиться об их сохранении в качестве дополнительных средствами командного интерфейса или WEB-интерфейса администратора МЭ ССПТ-4А1.

Сброс пароля пользователя SNMP-интерфейса **fnpsnmp** не доступен через ПО СОВа-4. Однако, установка нового пароля пользователя SNMP-интерфейса **fnpsnmp** доступна администратору **admin** через командный интерфейс или WEB-интерфейс администратора МЭ ССПТ-4А1 (при этом, ввод текущего значения пароля пользователя **fnpsnmp** не требуется). Сброс пароля администратора **admin** доступен средствами ПО СОВа-4.

7.3. Обновление

Меню обновления ПО МЭ ССПТ-4А1 приведено на рисунке 7.14, стр. 407.

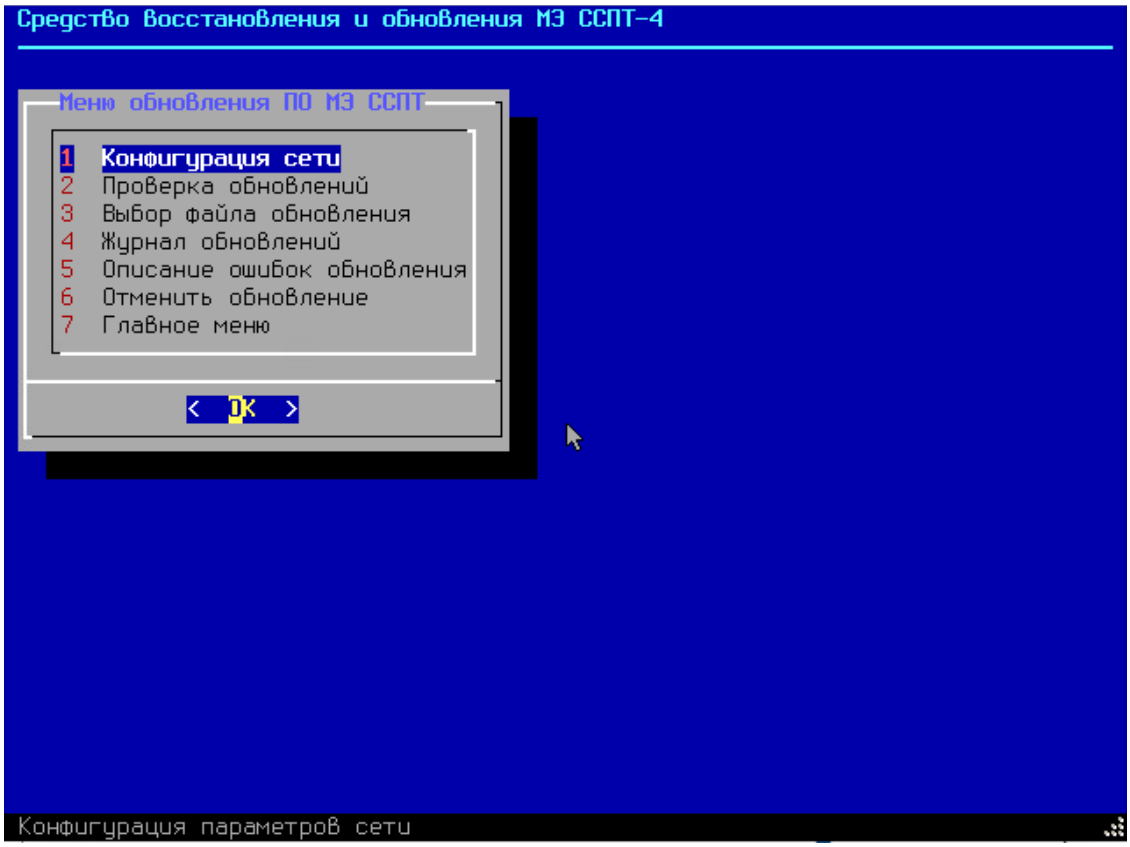


Рисунок 7.14: Меню обновления ПО МЭ ССПТ-4А1

Меню содержит следующие пункты:

1) **Конфигурация сети**: настройка параметров управляющего интерфейса МЭ ССПТ-4А1 для доступа к серверу обновлений в корпоративной сети или сети Интернет (*функция находится в разработке и не доступна в текущей версии ПО* СОВа-4);
2) **Проверка обновлений**: проверка наличия обновлений на сервере обновлений (*функция находится в разработке и не доступна в текущей версии ПО* СОВа-4);
3) **Выбор файла обновлений**: выбор файла обновления на FAT-разделе USB-носителя СОВа-4 и выполнение процедуры обновления ПО МЭ ССПТ-4А1 из выбранного файла;
4) **Журнал обновлений**: просмотр журнала обновлений;
5) **Описание ошибок обновления**: просмотр описания ошибок, которые могут возникнуть в ходе процедуры обновления;
6) **Отменить обновление**: отмена последнего выполненного обновления ПО МЭ ССПТ-4А1 (отмена последнего обновления возможна только если оно не было подтверждено администратором);
7) **Главное меню**: возврат в главное меню.

В текущей версии ПО СОВа-4 доступно обновление ПО МЭ ССПТ-4А1 только из файлов обновлений, предварительно записанных администратором на FAT-раздел USB-носителя данных СОВа-4 с использованием УК администратора.

При выборе пунктов **1** и **2** выводится предупреждение о том, что функция не доступна, так как находится в стадии разработки. Пример такого предупреждения приведен на рисунке 7.15, стр. 408.

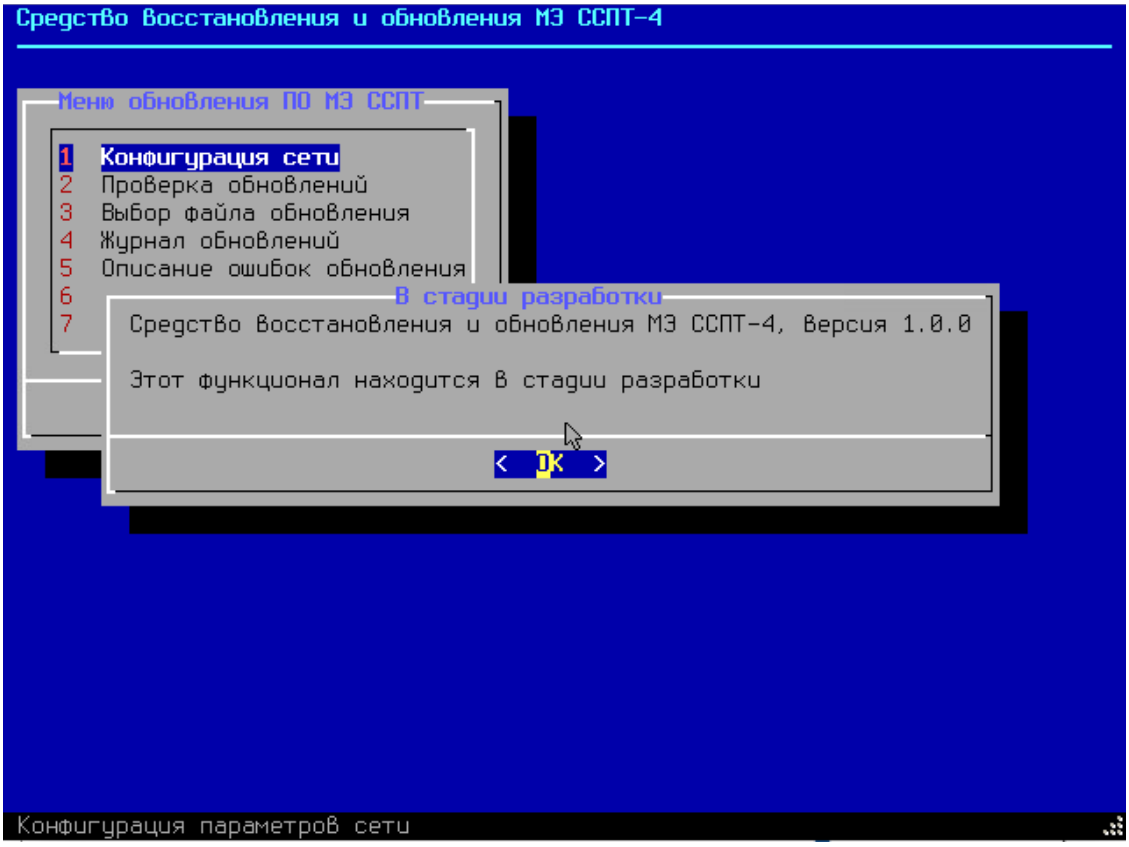


Рисунок 7.15: Пример предупреждения о функционале в стадии разработки

7.3.1. Получение файла обновления от производителя

Для выполнения процедуры обновления ПО потребителю МЭ ССПТ-4А1 необходимо получить файл обновления, сформированный для данного экземпляра МЭ ССПТ-4А1 предприятием-изготовителем. Ниже приводится алгоритм получения файла обновления:

1) Предприятие-изготовитель уведомляет организацию-потребителя МЭ ССПТ-4А1 о выпуске обновления следующими способами:
   - ✔ объявление на сайте производителя www.fractel.ru;
   - ✔ электронное письмо (E-mail) на контактный адрес потребителя;
   - ✔ по контактному телефону потребителя.
2) Потребитель скачивает по URL-ссылкам, содержащимся в уведомительном электронном письме (E-mail), файлы обновления для эксплуатируемых им экземпляров МЭ ССПТ-4А1;

3) Для каждого обновления потребителю в электронном сообщении пересылается две URL-ссылки для скачивания следующих файлов:

- непосредственно файла обновления. Имя данного файла имеет формат `fnp4-<версия>-<дата>-<номер>.img`. Полное описание формата имени файла обновления приводится в разделе 7.3.2 на стр. 411;
- файла, содержащего контрольную сумму файла обновления, подсчитанную по алгоритму SHA-512. Имя файла контрольной суммы имеет формат `fnp4-<версия>-<дата>-<номер>.sha512`.

4) Потребитель необходимо скачать указанные файлы по полученным URL-ссылкам.

5) Потребитель должен проверить целостность полученного файла обновления, для чего подсчитать его контрольную сумму и сравнить ее со значением, содержащемся в файле контрольной суммы.

- Для ОС Windows 10 подсчет контрольной суммы осуществляется в командной строке Windows командой `certutil` следующим образом:

  ```
  certutil -hashfile <имя_файла_обновления> SHA512
  ```

- Для ОС Linux подсчет контрольной суммы осуществляется командой `sha512sum` следующим образом:

  ```
  sha512sum <имя_файла_обновления>
  ```

- Для ОС FreeBSD подсчет контрольной суммы осуществляется командой `sha512` следующим образом:

  ```
  sha512 <имя_файла_обновления>
  ```

  Полученная в результате подсчета контрольная сумма должна совпадать с контрольной суммой, содержащейся в файле контрольной суммы. Если контрольные суммы не совпадают, потребитель должен обратиться к предприятию-изготовителю.

6) После проверки контрольной суммы файл обновления данного экземпляра МЭ ССПТ-4А1 (файл с расширением `.img`, имеющий номер, соответствующий номеру обновляемого устройства) записывается на FAT-раздел (метка раздела “msdosfs”) USB-носителя СОВа-4, входящего в комплект поставки данного экземпляра МЭ ССПТ-4А1.

После записи файла обновления на USB-носитель СОВа-4 экземпляр МЭ ССПТ-4А1 готов к проведению процедуры обновления ПО. Далее описываются шаги, которые необходимо выполнить в ПО СОВа-4 для установки обновления и подтверждения установленного обновления.

Уведомительное электронное письмо (e-mail) о выпуске обновления содержит следующую информацию:

- номер версии ПО МЭ ССПТ-4А1, соответствующей обновлению, и дату выпуска обновления;
- перечень уязвимостей и/или ошибок, устраняемых дынным обновлением;
- список URL-ссылок на файлы обновлений (для каждого экземпляра МЭ ССПТ-4А1, эксплуатируемого потребителем, отдельная ссылка на соответствующий ему файл обновления).

7.3.2. Выполнение процедуры обновления ПО МЭ ССПТ-4А1

Для того, чтобы начать процедуру обновления, необходимо в меню обновления выбрать пункт **Выбор файла обновления**. При выборе пункта **Выбор файла обновления**:

- в случае отсутствия файлов обновлений на FAT-разделе USB-носителя СОВа-4 выводится соответствующее предупреждение. Пример предупреждения приведен на рисунке 7.16, стр. 410;
- в случае наличия файлов обновлений выводится их список с возможностью выбора файла для выполнения процедуры обновления. Пример вывода доступных файлов обновлений приведен на рисунке 7.17, стр. 411.

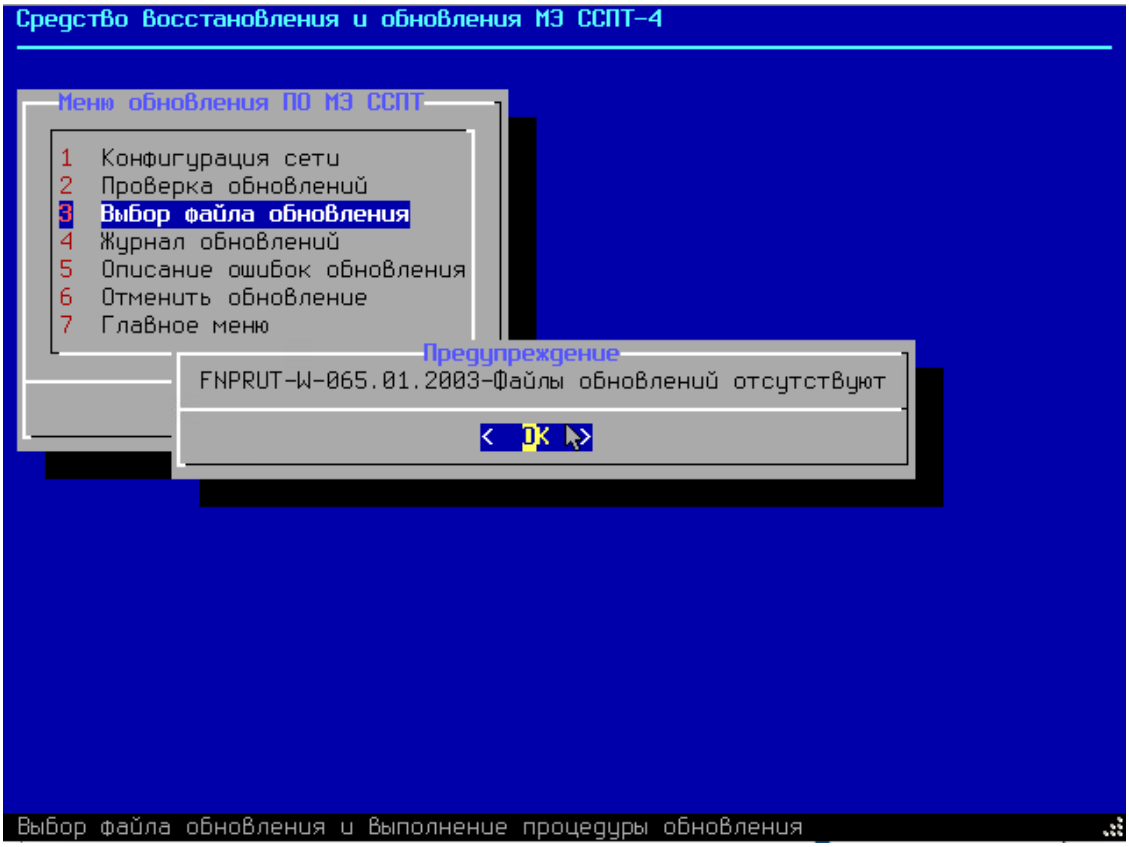


Рисунок 7.16: Отсутствие файлов обновлений на FAT-разделе носителя

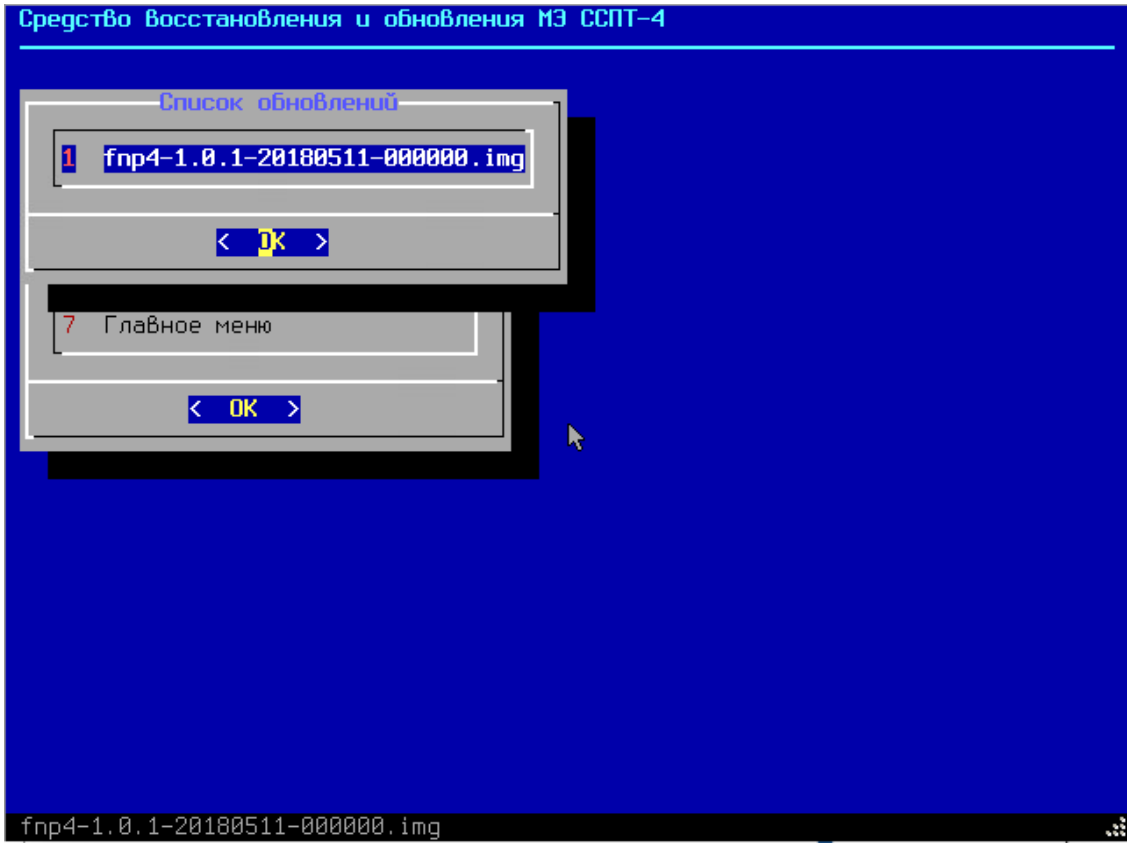


Рисунок 7.17: Пример вывода доступных файлов обновлений

Для возможности выполнения процедуры обновления файл обновления должен быть предварительно записан администратором МЭ ССПТ-4А1 на FAT-раздел USB-носителя СОВа-4. Для этого необходимо:

- подключить USB-носитель СОВа-4 к USB-порту УК администрртатора;
- скопировать файл обновления на FAT-раздел USB-носителя СОВа-4, имеющий символьную метку *“msdosfs”*, используя программу типа файловый менеджер.

Имя файла обновления имеет следующий формат – `fnp4-V.V.V-ГГГГММДД-NNNNNN.img`, где:

- `V.V.V` – номер версии ПО МЭ ССПТ-4А1 в данном обновлении (например: *1.0.1*);
- `ГГГГММДД` – дата выпуска обновления (например: *20180511*);
- `NNNNNN` – шестизначный заводской номер экземпляра МЭ ССПТ-4А1 (например: *000001*).

Файлы, находящиеся на FAT-разделе носителя и не являющиеся файлами обновлений, исключаются из вывода в меню *Список обновлений*.

Для возврата в меню обновления из списка файлов обновлений необходимо использовать клавишу **<Esc>**.

Контроль файлов обновлений средствами ПО МЭ ССПТ-4А1:

- Файлы обновлений специальным образом преобразованы, при этом каждый файл обновления привязан к конкретному экземпляру МЭ ССПТ-4А1. При попытке обновления другого экземпляра МЭ ССПТ-4А1 процедура обновления завершится с соответствующей диагностикой до замены файлов на носителе данных МЭ ССПТ-4А1.
- В ходе процедуры обновления проверяется целостность файла обновления. В случае нарушения целостности файла обновления процедура обновления завершится с соответствующей диагностикой до замены файлов на носителе данных МЭ ССПТ-4А1.
- Обновление ПО МЭ ССПТ-4А1 может быть выполнено только на версию ПО старше текущей версии ПО. Понижение версии ПО МЭ ССПТ-4А1 средствами ПО СОВа-4 не допускается.

При выборе файла обновления (нажатие **<Enter>** по выделенному имени файла) выводится диалоговое окно подтверждения старта процедуры обновления ПО МЭ ССПТ-4А1. Пример окна подтверждения приведен на рисунке 7.18, стр. 412.

Во время процедуры обновления выводится окно с ходом создания временного dump-образа носителя данных МЭ ССПТ-4А1, который необходим на тот случай, если администратор решит отменить данное обновление и вернуться к предыдущей версии ПО МЭ ССПТ-4А1. В случае возникновения какой-либо ошибки после перезаписи файлов на носителе МЭ ССПТ-4А1 данный dump-образ будет использован для автоматического восстановления к состоянию до начала процедуры обновления. По завершении создания dump-образа администратору необходимо нажать кнопку **<OK>** для продолжения процедуры обновления. Пример окна с ходом создания временного dump-образа приведен на рисунке 7.19, стр. 413.

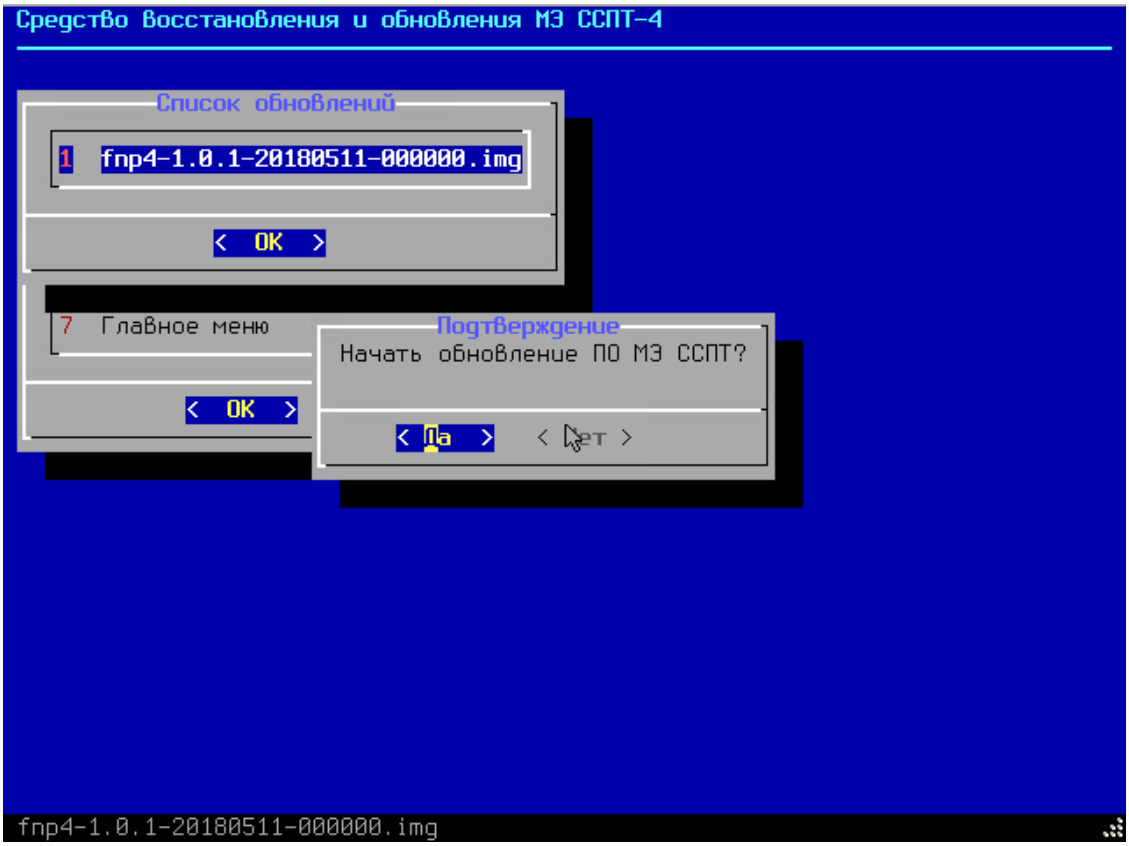


Рисунок 7.18: Подтверждение старта процедуры обновления ПО МЭ ССПТ-4А1

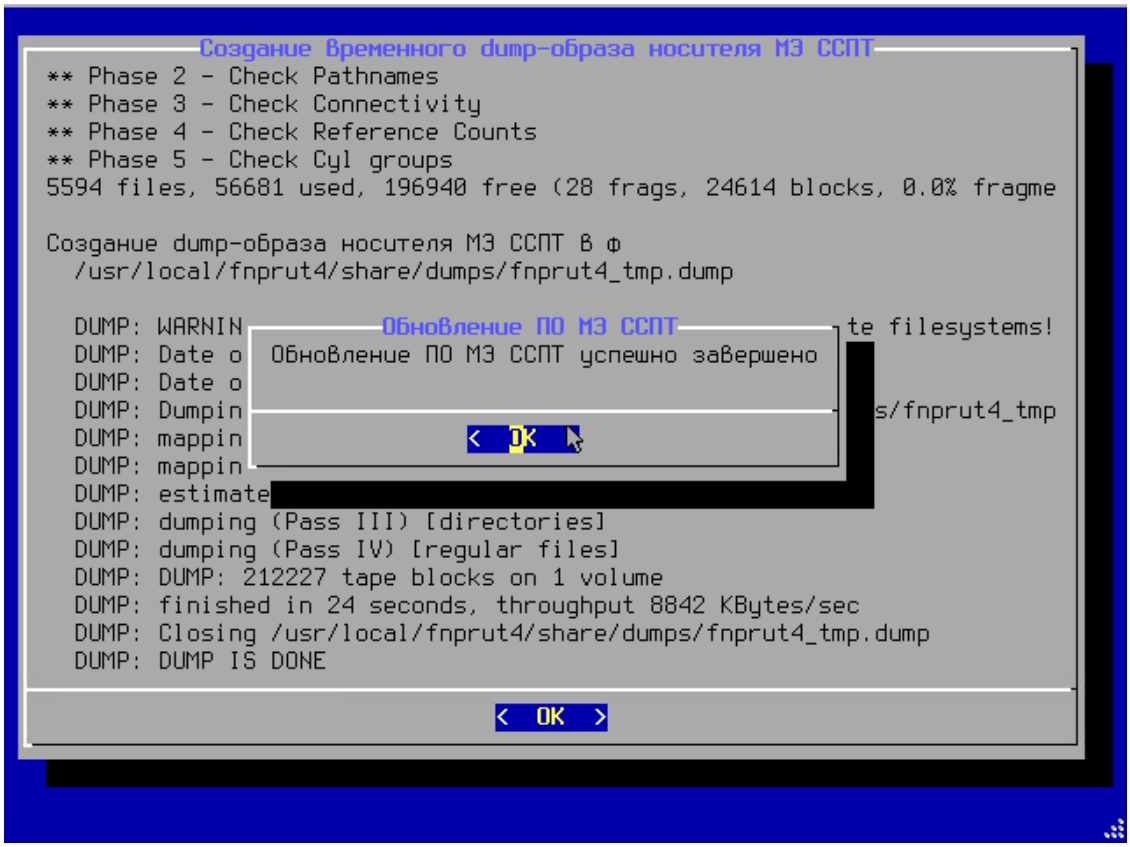


Рисунок 7.19: Ход создания временного dump-образа носителя данных МЭ ССПТ-4А1

При успешном завершении процедуры обновления ПО МЭ ССПТ-4А1 выводится соответствующее сообщение (7.19, стр. 413). При нажатии клавиши **<Enter>** во время отображения данного сообщения выполняется возврат в меню обновления.

7.3.3. Журнал обновлений

Процедура обновления ПО МЭ ССПТ-4А1 журналируется. Это значит, что для каждой начатой процедуры обновления в журнале обновлений будет сделана запись с информацией о статусе завершения процедуры обновления. В случае успешного завершения процедуры обновления в журнал также будет добавлена запись о подтверждении выполненного обновления или об его отмене (после того, как администратор выполнит соответствующее действие).

Для просмотра журнала обновлений необходимо выбрать пункт меню **Журнал обновлений**. Пример вывода журнала обновлений приведен на рисунке 7.20, стр. 414.

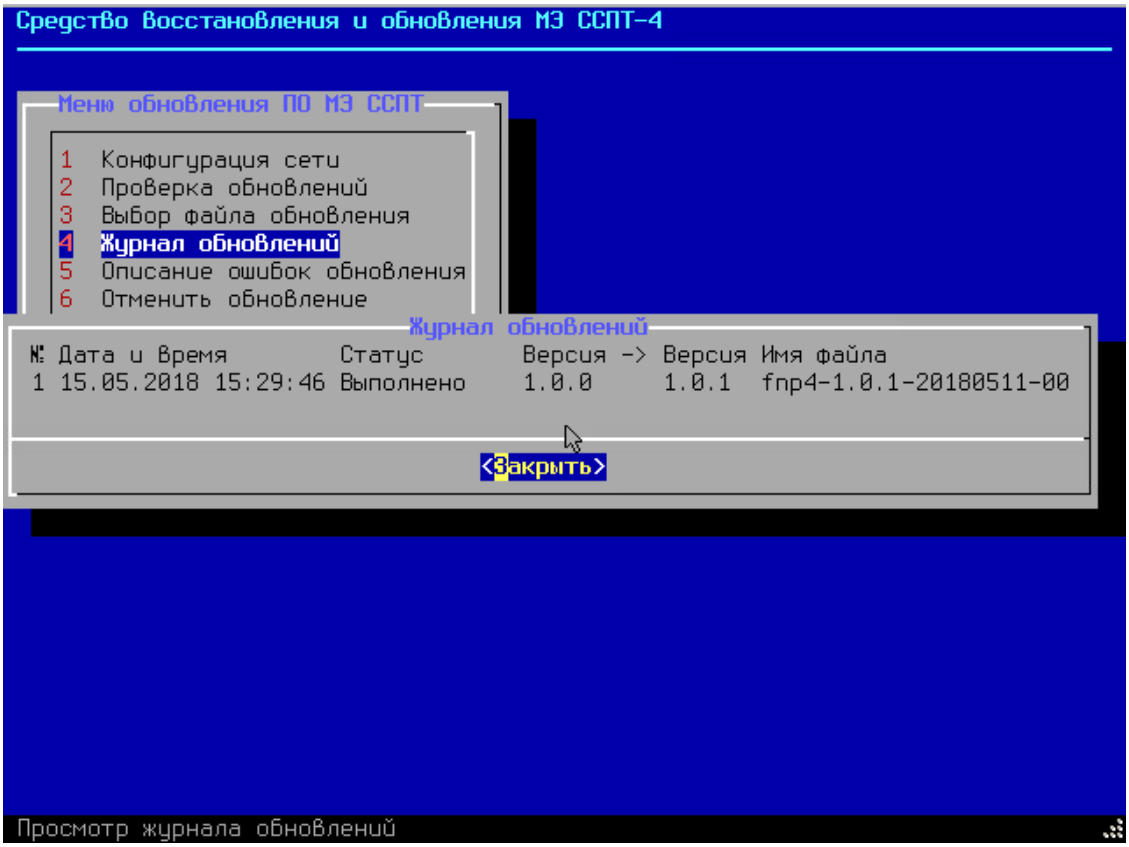


Рисунок 7.20: Пример вывода журнала обновлений

Запись журнала обновления содержит следующие поля:

- № – порядковый номер записи;
- Дата и время – дата и время завершения процедуры обновления, отмены или подтверждения обновления;
- Статус – статус завершения процедуры обновления, отмены или подтверждения обновления. Если процедура не была выполнена из-за ошибки, то в данном поле выводится соответствующий код ошибки. Описание кодов всех ошибок, которые могут отображаться в данном поле, доступно в пункте меню **Описание ошибок обновления**.
- Версия (первое поле) – текущая версия ПО МЭ ССПТ-4А1 (до обновления);
- Версия (второе поле) – версия обновления ПО МЭ ССПТ-4А1;
- Имя файла – базовое имя файла обновления (без указания расширения .img).

В случае ошибки в ходе выполнения процедуры обновления в поле *Статус* выводится код ошибки, например: *Ошибка 9*. В случае некоторых ошибок второе поле *Версия* может выводиться пустым, это значит, что на момент возникновения ошибки версия обновления была недоступна для ПО СОВа-4.

Записи журнала обновлений выводятся в порядке убывания даты и времени. То есть в первой строке – самая последняя по времени запись. Последняя запись журнала обновлений имеет максимальный *порядковый номер*.

При просмотре журнала доступна *горизонтальная* и *вертикальная* прокрутка с использованием клавиш *курсоров* (*стрелок*). Горизонтальная прокрутка позволяет увидеть имя файла обновления целиком. Вертикальная прокрутка позволяет увидеть более ранние записи журнала обновлений, которые не поместились в рабочую область окна журнала обновлений.

7.3.4. Описание ошибок обновления

В ходе процедуры обновления могут возникнуть различные ошибки. При первой ошибке процедура обновления завершается и в журнал обновлений добавляется запись с соответствующим кодом ошибки в поле `Статус`. Для просмотра описаний всех возможных ошибок процедуры обновления необходимо выбрать пункт **`Описание ошибок обновления`**. Пример окна с описанием ошибок обновления приведен на рисунке 7.21, стр. 416.

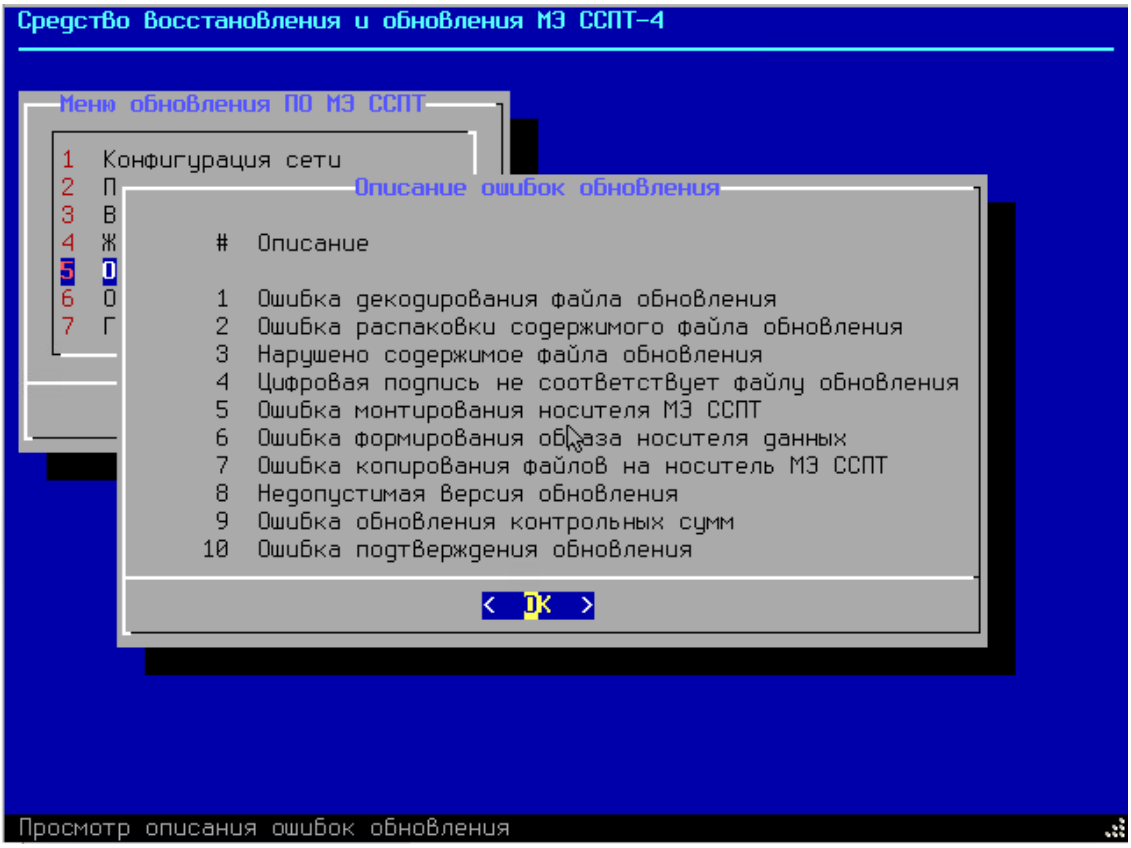


Рисунок 7.21: Просмотр описания ошибок процедуры обновления

7.3.5. Отмена обновления

Успешно выполненное обновление ПО МЭ ССПТ-4А1 может быть отменено администратором с целью возврата к версии ПО МЭ ССПТ-4А1 до выполнения последнего обновления. Для этого в меню обновления доступен пункт **Отмена обновления**. При выборе данного пункта выводится диалоговое окно подтверждения действия. Пример окна, с помощью которого администратор может начать процедуру отмены обновления или отказаться от ее выполнения, приведен на рисунке 7.22, стр. 417. Во время процедуры отмены обновления выводится ход восстановления данных на носителе МЭ ССПТ-4А1. По завершении процедуры восстановления данных выводится соответствующее сообщение. Пример окна с ходом процедуры восстановления носителя МЭ ССПТ-4А1 приведен на рисунке 7.23, стр. 417.

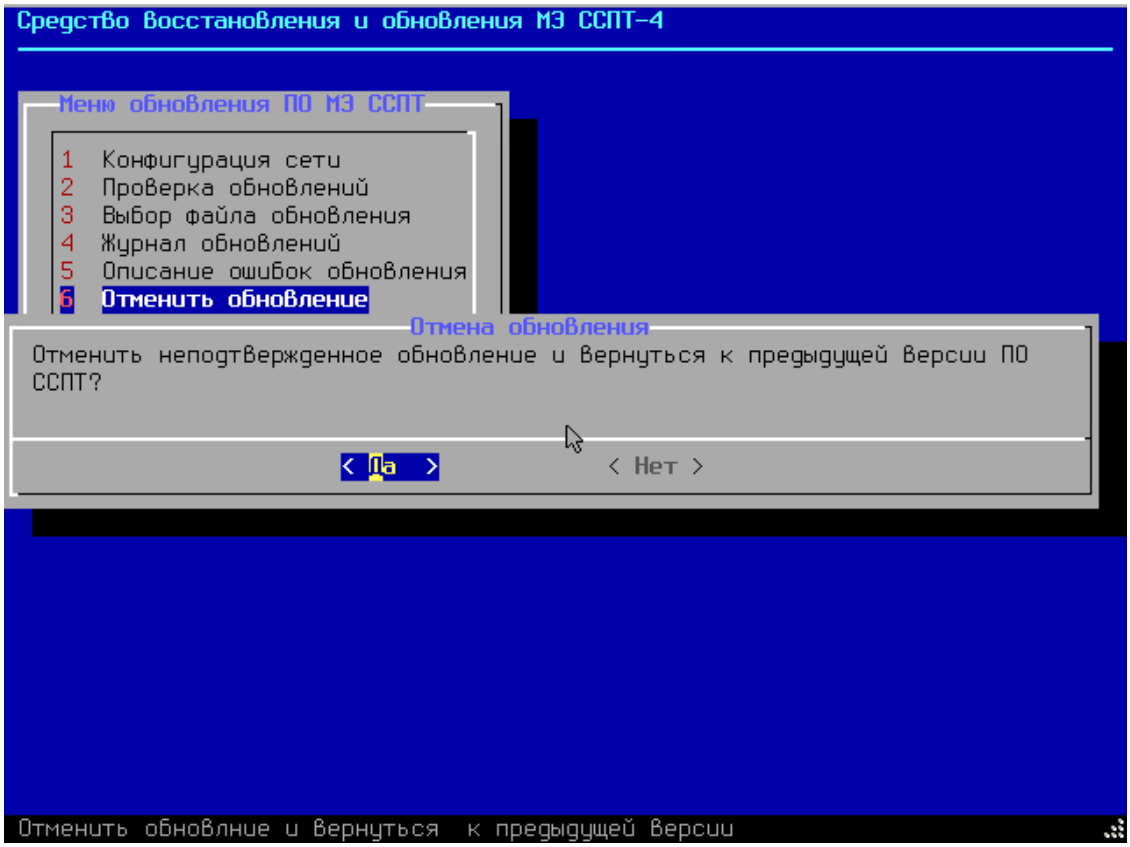


Рисунок 7.22: Подтверждение старта процедуры отмены обновления

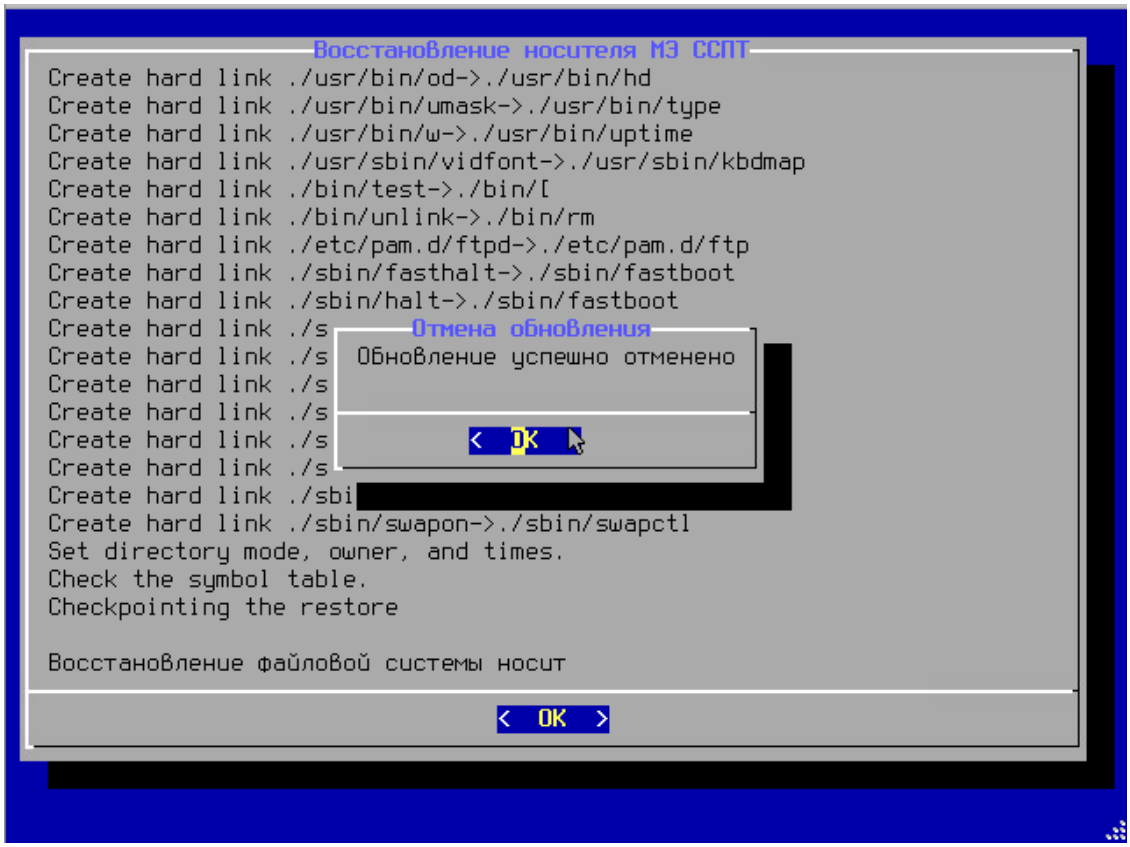


Рисунок 7.23: Ход процедуры восстановления данных на носителе МЭ ССПТ-4А1

По завершении процедуры отмены обновления выводится соответствующее сообщение (рисунок 7.23, стр. 417).

> Отмена обновления ПО МЭ ССПТ-4А1 доступна до тех пор, пока выполненное обновление не было подтверждено администратором.

В случае отмены обновления в журнал обновлений добавляется запись с соответствующим значением поля `Статус`. Пример записи об отмене обновления приведен на рисунке 7.24, стр. 418.

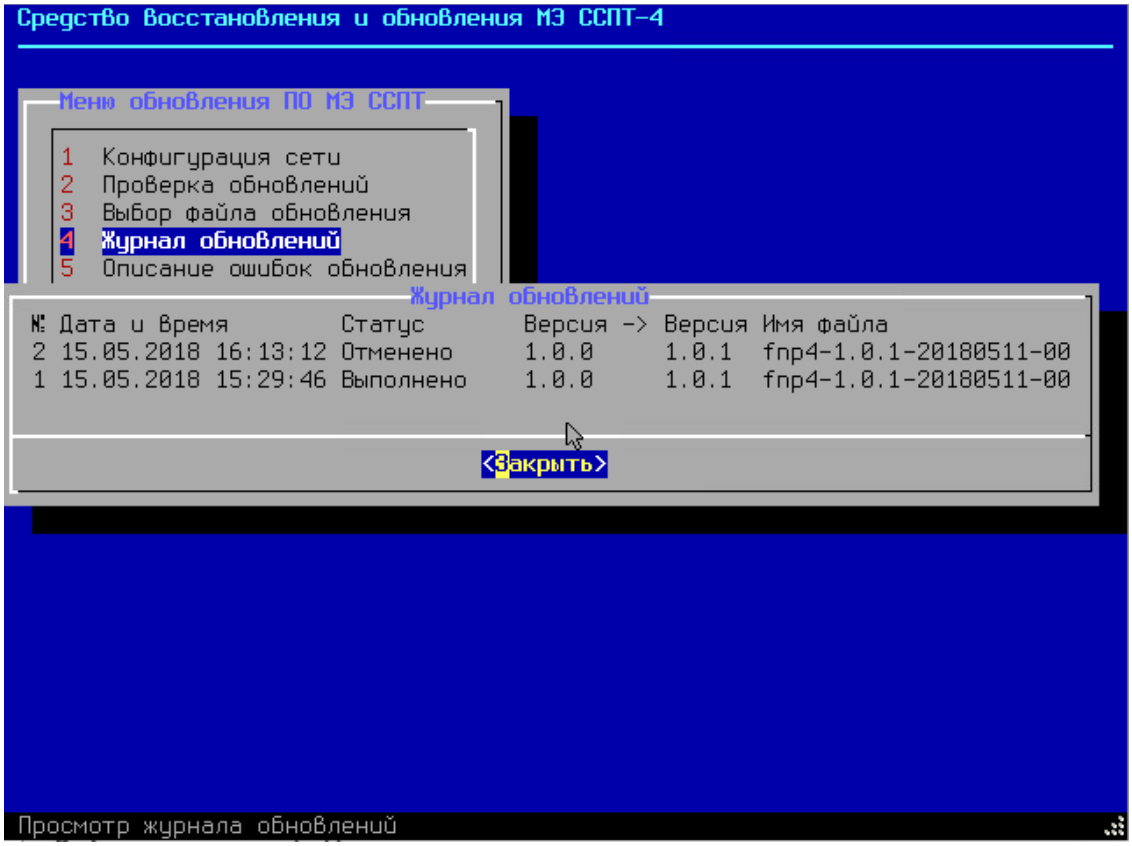


Рисунок 7.24: Запись отмены обновления в журнале

7.3.6. Подтверждение обновления

После выполнения обновления администратору МЭ ССПТ-4А1 предоставляется возможность убедиться, что все подсистемы МЭ ССПТ-4А1 успешно стартовали и доступны. Для этого после успешного завершения процедуры обновления администратору необходимо перезагрузить МЭ (**`Устройство`** → **`Перезагрузка`**) и выполнить загрузку УОС МЭ ССПТ-4А1 с носителя данных МЭ ССПТ-4А1. Для этого потребуется сразу после начала перезагрузки устройства извлечь USB-носитель СОВа-4 из USB-разъема устройства.

Далее выполнится загрузка УОС МЭ ССПТ-4А1 и администратор сможет через вывод на консоли и/или командный интерфейс убедиться в доступности всех подсистем МЭ ССПТ-4А1 (команда **`system show`**) и выполнить другие команды по своему усмотрению.

После того, как администратор принял решение, что работа новой версии ПО МЭ ССПТ-4А1 его устраивает, необходимо подтвердить ранее выполненное обновление. Для этого требуется выполнить следующую последовательность действий:

1) вставить USB-носитель СОВа-4 в USB-разъем устройства;
2) перезагрузить устройство (команда **`system reboot`**);
3) если в BIOS МЭ ССПТ-4А1 USB-носитель установлен не первым устройством в списке устройств для загрузки, то необходимо, не дожидаясь загрузки УОС МЭ ССПТ-4А1, зайти в BIOS и установить USB-носитель первым в списке устройств для загрузки.

В результате будет выполнена загрузка с USB-носителя СОВа-4 и сразу после приветственного окна будет выведено диалоговое окно подтверждения обновления. Пример диалогового окна подтверждения обновления приведен на рисунке 7.25, стр. 420. В ходе процедуры подтверждения обновления выполняется создание dump-образа носителя данных МЭ ССПТ-4А1, для использования функцией восстановления носителя данных (**Восстановление** → **Восстановление**). Таким образом, впоследствии, при необходимости восстановления, будет восстановлена текущая (обновленная) версия ПО МЭ ССПТ-4А1. Пример окна с ходом создания dump-образа приведен на рисунке 7.26, стр. 420.

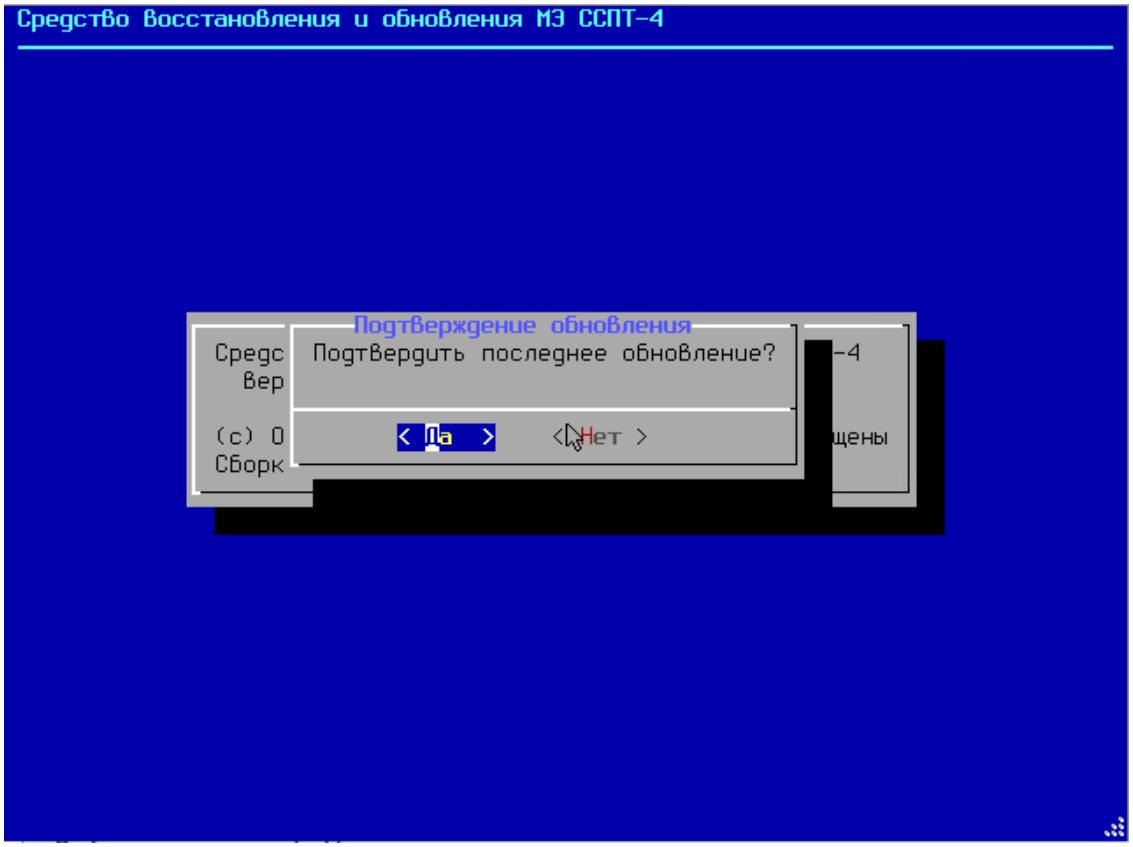


Рисунок 7.25: Диалоговое окно подтверждения обновления

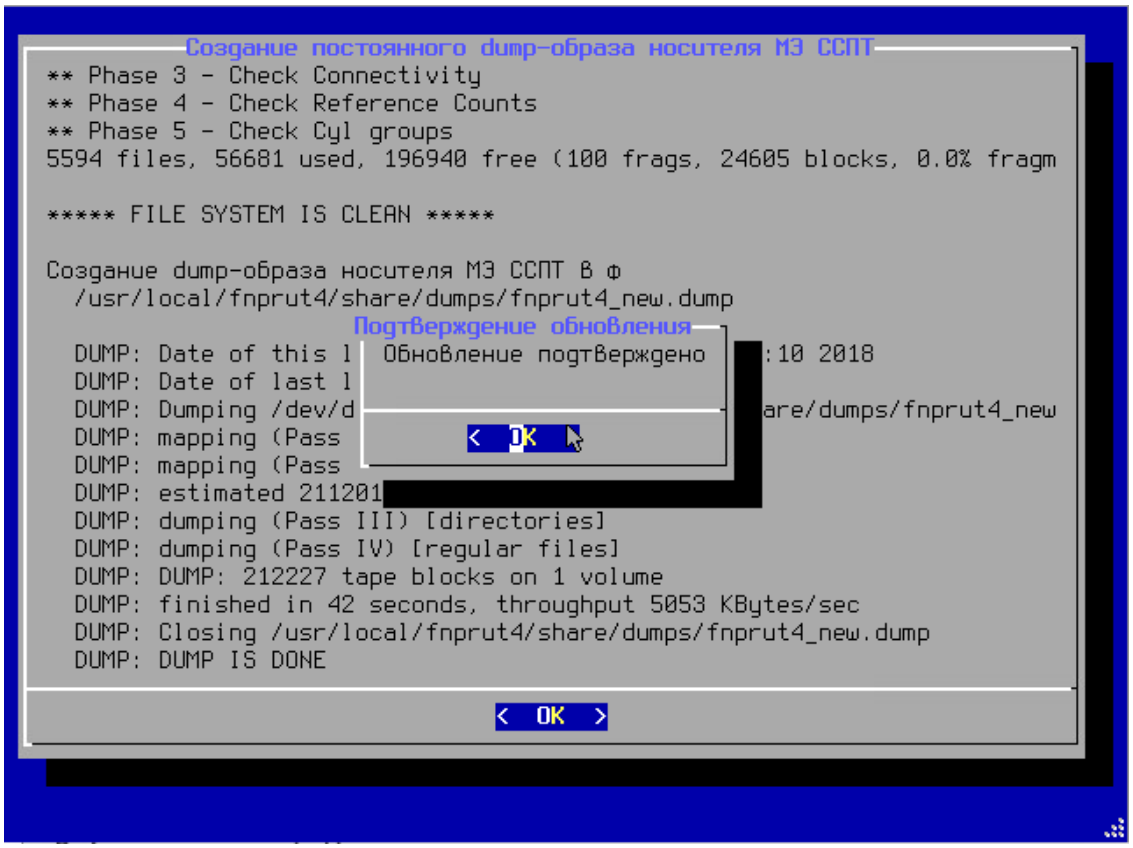


Рисунок 7.26: Окно хода создания dump-образа для функции восстановления

По завершении создания dump-образа станет доступна кнопка **<OK>**, на которую необходимо нажать (равносильно нажатию **<Enter>**). В результате будет выведено окно об успешном подтверждении обновления (рисунок 7.26, стр. 420). Для перехода к главному меню необходимо вновь нажать **<Enter>**.

В результате подтверждения обновления:

- в журнал обновлений будет добавлена запись с соответствующим значением поля `Статус`;
- в информации об устройстве (**Устройство → О МЭ ССПТ**) изменятся значения параметров `Имя выпуска` и `Версия программного обеспечения`.

После того, как администратор подтвердил обновление, выполненное ранее, отмена данного обновления средствами ПО СОВа-4 становится недоступна.

Администратор может не подтверждать обновление, выполненное ранее, нажав <*Нет*> в диалоговом окне подтверждения обновления. В этом случае администратор сможет отменить обновление (*Обновление → Отменить обновление*). Однако, в случае сбоя, при неподтвержденном обновлении, администратор сможет восстановить (*Восстановление → Восстановление*) только версию ПО МЭ ССПТ-4А1, которая использовалась до последнего обновления.

Впоследствии выполненное обновление ПО должно быть подтверждено для внесения соответствующих отметок в паспорт (формуляр) экземпляра МЭ ССПТ-4А1. Запрос на подтверждение обновления выводится при каждом запуске ПО СОВа-4 до тех пор, пока администратор не выполнил подтверждение либо отмену обновления ПО.

Пример записи журнала обновлений о подтверждении обновления приведен на рисунке 7.27, стр. 422. Пример вывода актуальных имени выпуска и версии ПО МЭ ССПТ-4А1 приведен на рисунке 7.28, стр. 422.

После подтверждения обновления необходимо внести соответствующую отметку в раздел “Сведения об изменениях” паспорта (формуляра).

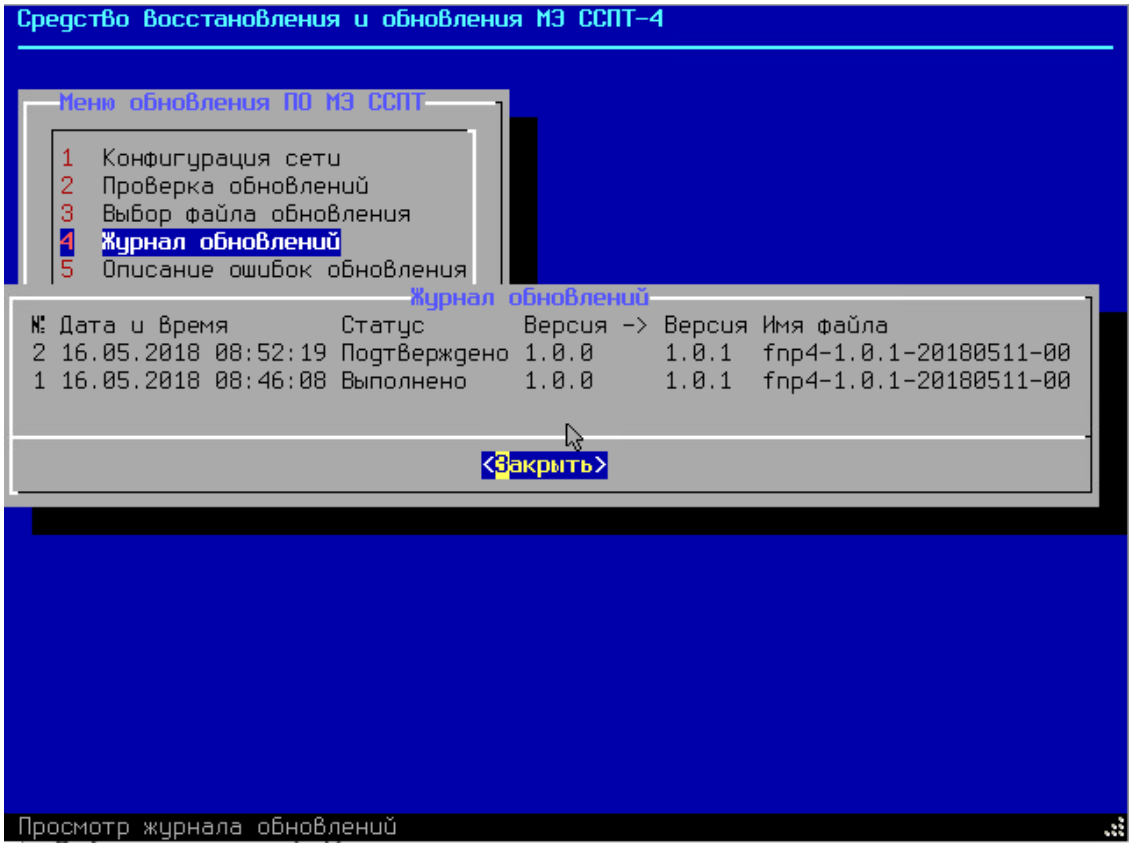


Рисунок 7.27: Запись журнала обновлений о подтверждении обновления

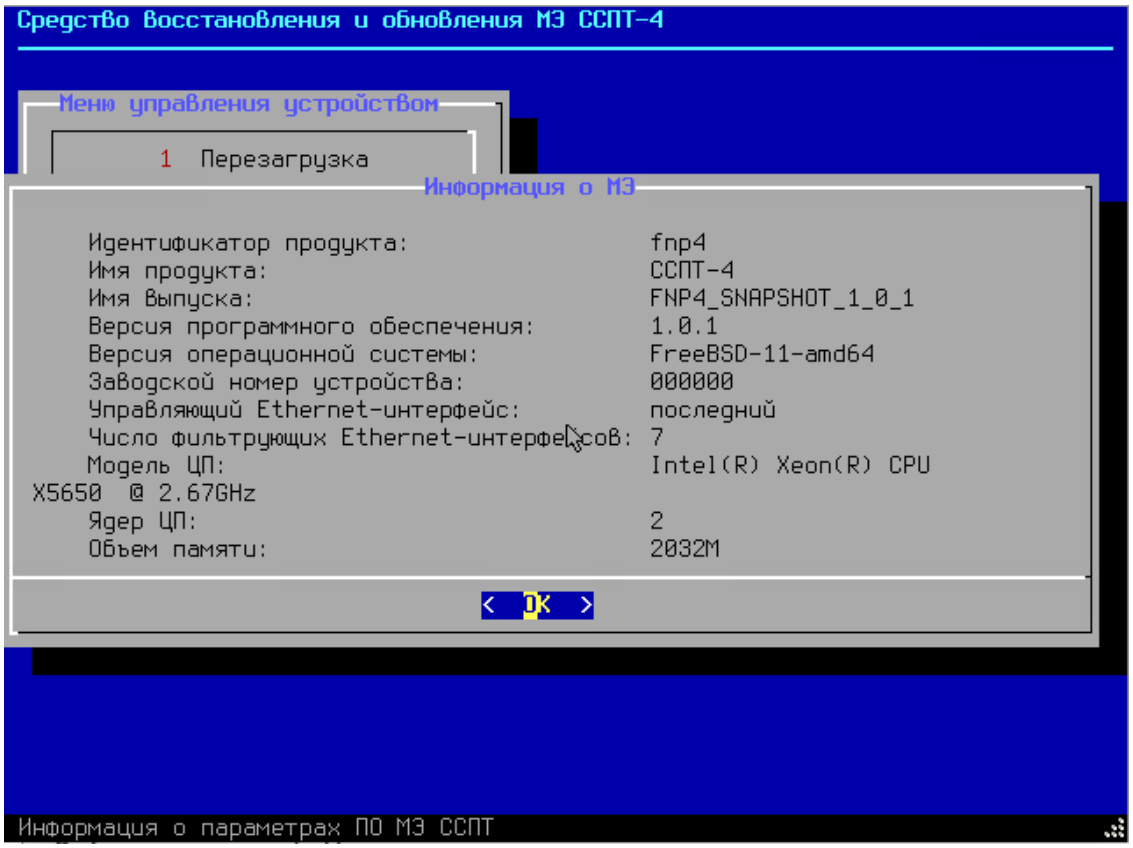


Рисунок 7.28: Вывод актуальных имени выпуска и версии ПО

Приложение А. Требования к форматам данных и ограничения параметров конфигурации

А.1. Требования к форматам данных

Идентификатор учетной записи должен отвечать требованиям, представленным в таблице А.1, стр. 423.

Таблица А.1: Идентификатор учетной записи

Тип	Текстовый
Длина	От **2** до **128** символов
Допустимые символы	• первый символ - строчные латинские символы **a-z** или цифры **0-9**; • последующие символы - строчные латинские символы **a-z**, цифры **0-9**, символ подчеркивания '_', точка '.', дефис '-', коммерческое at '@
Уникальность	Да
Значение по умолчанию	Отсутствует
Использование	• имя администратора; • имя сетевого пользователя; • имя пользователя FTP-сервера для выгрузки журналов регистрации.

Пароль учетной записи должен отвечать требованиям, представленным в таблице А.2, стр. 423.

Таблица А.2: Пароль учетной записи

Тип	Текстовый
Длина	От **6** до **128** символов
Допустимые символы	ASCII-символы от символа пробела и до тильды (**'~'**) включительно (цифры **0-9**, строчные латинские символы **a-z**, прописные латинские символы **A-Z** и остальные символы из данного диапазона ASCII-символов)
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	• пароль администратора; • пароль системного пользователя fnpsh; • пароль сетевого пользователя; • пароль пользователя FTP-сервера для выгрузки журналов регистрации.

Пароль учетной записи SNMP-пользователя должен отвечать требованиям, представленным в таблице А.3, стр. 423.

Таблица А.3: Пароль учетной записи SNMP-пользователя

Тип	Текстовый
Длина	От **8** до **128** символов

Тип	Текстовый
Допустимые символы	ASCII-символы от символа пробела и до тильды (**'~'**) включительно (цифры **0-9**, строчные латинские символы **a-z**, прописные латинские символы **A-Z** и остальные символы из данного диапазона ASCII-символов)
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	Пароль SNMP-пользователя

Строка даты должна отвечать требованиям, представленным в таблице А.4, стр. 424.

Таблица А.4: Строка даты

Тип	Текстовый
Синтаксис Формат представления	ДД.ММ.ГГГГ, где: • ДД — день месяца: число от 1 до 31; • ММ — номер месяца: число от 1 до 12; • ГГГГ — год: число от 1900 до 9999.
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	• установка системной даты; • критерии выборки записей регистрации событий. пакетов, сессий.

Строка даты и времени должна отвечать требованиям, представленным в таблице А.5, стр. 424.

Таблица А.5: Строка даты и времени

Тип	Текстовый
Допустимые символы	ДД.ММ.ГГГГ.ЧЧ:ММ:СС, где: • ДД — день месяца: число от 1 до 31; • ММ — номер месяца: число от 1 до 12; • ГГГГ — год: число от 1900 до 9999; • ЧЧ — часы: число от 0 до 23; • ММ — минуты: число от 0 до 59; • СС — секунды: число от 0 до 59.
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	Критерии выборки записей регистрации событий. пакетов, сессий;

Имя дополнительной конфигурации и дополнительной политики доступа должно отвечать требованиям, представленным в таблице А.6, стр. 424.

Таблица А.6: Имя дополнительной конфигурации и дополнительной политики доступа

Тип	Текстовый
Длина	От **1** до **251** символов

Тип	Текстовый
Допустимые символы	• первый символ (обязателен) – строчные латинские символы **a-z**, прописные латинские символы **A-Z**, цифры **0-9**; • серединная последовательность символов (не обязательна), допустимые символы: строчные латинские символы **a-z**, прописные латинские символы **A-Z**, цифры **0-9**, символ подчеркивания '_', дефис '-'; • конечная последовательность символов (не обязательна, может повторяться произвольное число раз с соблюдением общей длины строки): первый символ – **точка '.'**, далее: минимум один символ из числа следующих: строчные латинские символы **a-z**, прописные латинские символы **A-Z**, цифры **0-9**, символ подчеркивания '_', дефис '-'.
Уникальность	Да
Значение по умолчанию	**fnp4-имя_устройства-ГГГГММДД-ЧЧММСС** , где: • имя_устройства — имя устройства из текущей конфигурации (см. таблица А.9, стр. 426); • ГГГГММДД-ЧЧММСС — дата и время сохранения дополнительной конфигурации либо политики доступа с точностью до секунды.
Использование	• имя дополнительной конфигурации; • имя дополнительной политики доступа.

Строка комментария должна отвечать требованиям, представленным в таблице А.7, стр. 425.

Таблица А.7: Строка комментария

Тип	Текстовый
Длина	От **0** до **200** символов
Допустимые символы	• строчные латинские символы **a-z**; • прописные латинские символы **A-Z**; • строчные кириллические символы **а-я**; • прописные кириллические символы **А-Я**; • цифры **0-9**; • прочие печатаемые ASCII-символы;
Уникальность	Нет
Значение по умолчанию	Строка нулевой длины
Использование	• комментарий к правилу фильтрации; • комментарий к объекту справочника; • комментарий к группе правил фильтрации; • комментарий к группе объектов справочника; • комментарий к дополнительной конфигурации; • комментарий к дополнительной политике доступа; • комментарий к устройству;

Имя именованной сущности из конфигурации или политики доступа МЭ ССПТ-4А1 должно отвечать требованиям, представленным в таблице А.8, стр. 425.

Таблица А.8: Имя именованной сущности из конфигурации или политики доступа МЭ ССПТ-4А1

Тип	Текстовый
Длина	От **2** до **32** символов
Допустимые символы	• первый символ - строчные латинские символы **a-z**, прописные латинские символы **A-Z**; • последующие символы - строчные латинские символы **a-z**, прописные латинские символы **A-Z**, цифры **0-9**, символ подчеркивания '_', точка **'.'**, дефис '-'.

Тип	Текстовый
Уникальность	Среди сущностей одного типа
Значение по умолчанию	Отсутствует
Использование	Именованные сущности из конфигурации или политики доступа МЭ ССПТ-4А1: • назначенное имя фильтрующего интерфейса • имя объекта справочника; • имя контейнера NAT; • имя сетевого интерфейса NAT.

Полное доменное имя (FQDN) должно отвечать требованиям, представленным в таблице А.9, стр. 426.

Таблица А.9: Полное доменное имя (FQDN)

Тип	Текстовый
Длина	От **2** до **255** символов
Синтаксис	**имя_домена[.имя_домена[….]]** , где **имя_домена** должно отвечать следующим требованиям: • длина: от **2** до **63** символов; • первый символ и последний символ - строчные латинские символы **a-z**, прописные латинские символы **A-Z**, строчные кириллические символы **а-я**, прописные кириллические символы **А-Я**, цифры **0-9**; • символы, кроме первого и последнего (если есть) - строчные латинские символы **a-z**, прописные латинские символы **A-Z**, строчные кириллические символы **а-я**, прописные кириллические символы **А-Я**, цифры **0-9**, дефис '-'; • запрещается использование двух и более символов дефис '-' подряд;
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	• имя устройства (**запрещается использование кириллических символов**); • элемент списка в значении параметра **hostname** PROXY-правила.

Путь на FTP-сервере для сохранения выгруженных журналов регистрации должен отвечать требованиям, представленным в таблице А.10, стр. 426.

Таблица А.10: Путь на FTP-сервере для сохранения выгруженных журналов регистрации

Тип	Текстовый
Длина	От **1** до **1023** символов
Допустимые символы	• первый символ - слэш '/'**;**; • последующие символы - строчные латинские символы **a-z**, прописные латинские символы **A-Z**, цифры **0-9**, символ подчеркивания '_', точка **'.'**, слэш '/'.
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	Путь на FTP-сервере для сохранения выгруженных журналов регистрации

IPv4-адрес должен отвечать требованиям, представленным в таблице А.11, стр. 427.

Таблица A.11: IPv4-адрес

Тип	Текстовый
Синтаксис	**X.X.X.X** - четыре десятичных числа разделенных точками, где: • X — десятичное число от 0 до 255.
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	• параметры команд командного интерфейса МЭ ССПТ-4А1; • параметры правил фильтрации; • параметры объектов справочника.

IPv6-адрес должен отвечать требованиям, представленным в таблице A.12, стр. 427.

Таблица A.12: IPv6-адрес

Тип	Текстовый
Синтаксис	**XXXX::XXXX:XXXX** - восемь четырехзначных шестнадцатеричных чисел (то есть групп по четыре символа), разделенных двоеточием, где: • XXXX - четырехзначное шестнадцатеричных число. **Например:** *2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d* Если две и более групп подряд равны 0000, то они могут быть опущены и заменены на двойное двоеточие (::). Незначащие старшие нули в группах могут быть опущены. **Например:** *2001:0db8:0000:0000:0000:0000:ae21:ad12* может быть сокращён до: *2001:db8::ae21:ad12* *0000:0000:0000:0000:0000:0000:ae21:ad12* может быть сокращён до: *::ae21:ad12*
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	• параметры команд командного интерфейса МЭ ССПТ-4А1; • параметры правил фильтрации; • параметры объектов справочника.

MAC-адрес должен отвечать требованиям, представленным в таблице A.13, стр. 427.

Таблица A.13: MAC-адрес

Тип	Текстовый
Синтаксис	**XX:XX:XX:XX:XX:XX** - 48-разрядный (6 октетов) MAC-адрес, где: • XX — октет: две шестнадцатеричных цифры, допускается любой регистр для символов: **A..F**. Допустимы три формы записи MAC-адреса: • **XX:XX:XX:XX:XX:XX** — с использованием символа двоеточие ':' в качестве разделителя октетов; • **XX-XX-XX-XX-XX-XX** — с использованием символа дефис '-' в качестве разделителя октетов; • **XXXXXXXXXXXX -** — без использования разделителя октетов.
Уникальность	Нет
Значение по умолчанию	Отсутствует

Тип	Текстовый
Использование	• параметры команд командного интерфейса МЭ ССПТ-4А1; • параметры правил фильтрации; • параметры объектов справочника.

Шестнадцатеричный код должен отвечать требованиям, представленным в таблице А.14, стр. 428.

Таблица А.14: Шестнадцатеричный код

Тип	Текстовый
Синтаксис	0xXXXX...XX, где: • X — шестнадцатеричная цифра, допускается любой регистр для символов: **A..F**. Допустимое число шестнадцатеричных цифр зависит от контекста использования шестнадцатеричного кода
Уникальность	Нет
Значение по умолчанию	Отсутствует
Использование	• параметры команд командного интерфейса МЭ ССПТ-4А1; • параметры правил фильтрации.

А.2. Ограничения параметров конфигурации

В таблице А.15, стр. 428 приведены ограничения по всем численным параметрам конфигурации МЭ ССПТ-4А1.

Таблица А.15: Ограничения численных параметров конфигурации

Параметр	***Значение по умолчанию***	***Диапазон значений***	***Настройка параметра***	
			Командный интерфейс	***WEB-интерфейс***
Общие параметры NAT				
Тайм-аут неактивности сетевых пользователей (в секундах)	600	10..864000	Параметр **`timeout`** команды **`nat authentication set`**	`Настройки -> NAT -> Настройки -> Редактировать`
Параметры режима управления сессиями				
Тайм-ауты состояний сессий протокола TCP (в секундах)				
Тайм-аут состояния SYN	5	1..20	Параметр **`syn`** команды **`session timeout protocol=tcp`**	`Сессии -> Настройки -> Редактировать`
Тайм-аут состояния ESTABLISHED	3600	0..200000000	Параметр **`established`** команды **`session timeout protocol=tcp`**	`Сессии -> Настройки -> Редактировать`
Тайм-аут состояния FIN	600	0..20000	Параметр **`fin`** команды **`session timeout protocol=tcp`**	`Сессии -> Настройки -> Редактировать`
Тайм-ауты состояний сессий протокола UDP (в секундах)				
Тайм-аут состояния SYN	5	1..20	Параметр **`syn`** команды **`session timeout protocol=udp`**	`Сессии -> Настройки -> Редактировать`

Параметр	Значение по умолчанию	Диапазон значений	Настройка параметра	
			Командный интерфейс	WEB-интерфейс
Тайм-аут состояния ESTABLISHED	60	1..360	Параметр **established** команды **session timeout protocol=udp**	Сессии -> Настройки -> Редактировать
Тайм-ауты состояний сессий протокола ICMP (в секундах)				
Тайм-аут состояния SYN	5	1..20	Параметр **syn** команды **session timeout protocol=icmp**	Сессии -> Настройки -> Редактировать
Тайм-аут состояния ESTABLISHED	20	1..360	Параметр **established** команды **session timeout protocol=icmp**	Сессии -> Настройки -> Редактировать
Тайм-ауты состояний сессий остальных протоколов (в секундах)				
Тайм-аут состояния SYN	5	1..60	Параметр **syn** команды **session timeout protocol=other**	Сессии -> Настройки -> Редактировать
Тайм-аут состояния ESTABLISHED	30	1..300	Параметр **established** команды **session timeout protocol=other**	Сессии -> Настройки -> Редактировать
Параметры функции определения flood-атак				
Время жизни TMP-правила (в секундах)	60	10..3600	Параметр **lifetime** команды **session flood rule**	Сессии -> Настройки -> Редактировать
Пороговое значение для протокола TCP (в числе пакетов в секунду)	1000	10..200000	Параметр **tcp** команды **session flood threshold**	Сессии -> Настройки -> Редактировать
Пороговое значение для протокола UDP (в числе пакетов в секунду)	500	10..200000	Параметр **udp** команды **session flood threshold**	Сессии -> Настройки -> Редактировать
Пороговое значение для протокола ICMP (в числе пакетов в секунду)	300	10..200000	Параметр **icmp** команды **session flood threshold**	Сессии -> Настройки -> Редактировать
Параметры подсистемы регистрации				
Порт FTP-сервера для выгрузки файлов регистрации	21	0..65535	Параметр **port** команды **log export ftp set**	Настройки -> Регистрация -> Выгрузка по FTP -> Редактировать
Порт SYSLOG-сервера для выгрузки записей регистрации	514	0..65535	Параметр **port** команды **log export syslog set**	Настройки -> Регистрация -> Выгрузка по SYSLOG -> Редактировать
Параметры функции авторизации через RADIUS-сервер				
Порт основного RADIUS-сервера	1812	0..65535	Параметр **master-port** команды **user radius set**	Настройки -> RADIUS -> Редактировать

Параметр	Значение по умолчанию	Диапазон значений	Настройка параметра	
			Командный интерфейс	WEB-интерфейс
Порт запасного RADIUS-сервера	1812	0..65535	Параметр **slave-port** команды **user radius set**	Настройки -> RADIUS -> Редактировать
Тайм-аут ожидания ответа от RADIUS-сервера (в секундах)	5	0..10	Параметр **timeout** команды **user radius set**	Настройки -> RADIUS -> Редактировать
Количество обращений к RADIUS-серверу	3	1..10	Параметр **retry** команды **user radius set**	Настройки -> RADIUS -> Редактировать
Параметры синхронизации системных даты и времени по протоколу NTP				
Тайм-аут (период) опроса NTP-сервера (в секундах)	3600	600..86400	Параметр **timeout** команды **system time ntp set**	Настройки -> Устройство -> Системная дата и время -> Редактировать
Параметры сеанса работы администратора МЭ ССПТ-4А1				
Тайм-аут неактивности администратора (в секундах)	600	60..6000	Параметр **timeout** команды **system fnpsh set**	Не доступно
Параметры HTTP-посредника				
Порт HTTP-посредника	8118	0..65535	Параметр **port** команды **system proxy set**	Настройки -> HTTP-посредник -> Редактировать

Приложение Б. Перечень регистрируемых событий

Все регистрируемые события МЭ ССПТ-4А1 делятся на три категории:

- **информационные события** – генерируются в ответ на успешное выполнение команд по настройке МЭ ССПТ-4А1, при успешных входе и выходе администратора, а также при работе системы фильтрации с резервированием;
- **предупреждения** – генерируются различными подсистемами МЭ ССПТ-4А1 в ходе их работы (часть предупреждений, генерируемых пакетным фильтром, не регистрируются в журнале событий, но сохраняются в записи регистрации пакета и предоставляют информацию о причине удаления пакета);
- **ошибки** – могут генерироваться только пакетным фильтром и подсистемой контроля целостности МЭ ССПТ-4А1 в случае выявленных ошибок (часть ошибок, генерируемых пакетным фильтром, не регистрируются в журнале событий, но сохраняются в записи регистрации пакета и предоставляют информацию о причине удаления пакета).

При просмотре журнала событий для события независимо от его категории выводится:

- дата и время регистрируемого события с учетом часового пояса;
- буквенное обозначение категории события;
- код и описание события.

Для **информационного события** помимо также выводится:

- идентификатор (имя) администратора МЭ ССПТ-4А1, действия которого привели к регистрации данного события;
- IP-адрес управляющего компьютера в случае удаленного сетевого администрирования;
- дополнительная информация о событии (например: имя добавленного правила фильтрации, новое значение параметра конфигурации): указывается для некоторых событий.

Б.1. Информационные события МЭ ССПТ-4А1

Коды всех информационных событий МЭ ССПТ-4А1, их текстовая интерпретация и пояснения к некоторым из них представлены в таблице Б.1, стр. 431.

Таблица Б.1: Информационные события МЭ ССПТ-4А1

Код	*Описание события*	*Пояснение*
1001	Останов устройства	
1002	Перезагрузка устройства	
1003	Вход администратора	

Код	Описание события	Пояснение
1004	Выход администратора	
1005	Добавление администратора	
1006	Удаление администратора	
1007	Изменение пароля администратора	
1008	Изменение привилегий администратора	
1009	Выключение администратора	Учетная запись администратора МЭ ССПТ-4А1 не может быть использована для авторизации.
100A	Включение администратора	Учетная запись администратора МЭ ССПТ-4А1 может быть использована для авторизации.
100B	Останов пакетного фильтра	
100C	Очистка таблицы сессий	
100D	Изменение системного времени	
100E	Изменение часового пояса	
100F	Включение синхронизации по NTP	
1010	Выключение синхронизации по NTP	
1011	Сброс настроек синхронизации по NTP	
1012	Установка IP-адреса NTP-сервера	
1013	Синхронизация времени по NTP	
1015	Включение регистрации событий синхронизации по NTP	
1016	Выключение регистрации событий синхронизации по NTP	
1017	Изменение периода синхронизации по NTP	
1018	Добавление новой записи в список доступа	В список доступа к управляющему интерфейсу МЭ ССПТ-4А1 добавлена запись.
1019	Удаление записи из списка доступа	Из списка доступа к управляющему интерфейсу МЭ ССПТ-4А1 удалена запись.
101A	Очистка списка доступа	Из списка доступа к управляющему интерфейсу МЭ ССПТ-4А1 удалены все записи.
101B	Установка IP-адреса управляющего интерфейса	
101D	Выключение фильтрующего интерфейса	
101E	Включение фильтрующего интерфейса	
101F	Включение зеркалирования интерфейсов	
1020	Выключение зеркалирования интерфейсов	
1021	Переименование фильтрующего интерфейса	
1022	Удаление дополнительной конфигурации	
1023	Применение дополнительной конфигурации	

Код	Описание события	Пояснение
1024	Сохранение дополнительной конфигурации	
1026	Дополнительная конфигурация загружена с удаленного узла	Дополнительная конфигурация загружена на МЭ ССПТ-4А1 с управляющего компьютера администратора.
1028	Выключение регистрации пакетов	
1029	Включение регистрации пакетов	
102A	Очистка текущего файла регистрации пакетов	
102B	Сброс настроек выгрузки на FTP-сервер	
102C	Включение выгрузки на FTP-сервер	
102D	Выключение выгрузки на FTP-сервер	
102E	Изменение параметров выгрузки FTP-сервер	
102F	Очистка текущего файла регистрации сессий	
1030	Добавление правила фильтрации	
1031	Изменение правила фильтрации	
1035	Возврат к предыдущему состоянию текущей политики	
1037	Удаление правила фильтрации	
1038	Включение регистрации пакетов, отброшенных механизмом управления сессиями	Включена регистрация пакетов, отброшенных механизмом управления сессиями, при этом в записи регистрации пакета будет установлен соответствующий код предупреждения или ошибки (см. таблица Б.2, стр. 439 и таблица Б.3, стр. 441).
1039	Выключение регистрации пакетов, отброшенных механизмом управления сессиями	
103C	Общее правило скопировано	
103D	Общее правило перемещено	
103E	Прикладное правило скопировано	
103F	Прикладное правило перемещено	
1040	Применение конфигурации по умолчанию	
1041	Включение функции обнаружения flood-атак	
1042	Выключение функции обнаружения flood-атак	
1043	Включение регистрации обнаружения flood-атак	
1044	Выключение регистрации обнаружения flood-атак	
1045	Изменение порогового значения обнаружения flood-атаки	
1050	Проверка целостности программного обеспечения	

Код	Описание события	Пояснение
1051	Изменение пароля пользователя SNMP-интерфейса	
1052	Изменение пароля системного пользователя	
1053	Изменение тайм-аута неактивности администратора	
1054	Аутентификация сетевого пользователя	Аутентификация сетевого пользователя успешно выполнена: пользователь авторизован.
1055	Выход сетевого пользователя	Сетевой пользователь самостоятельно завершил свой сеанс работы через МЭ ССПТ-4А1.
1200	Включение NAT	
1201	Выключение NAT	
1207	Включение регистрации NAT	Включена регистрация пакетов, отброшенных NAT, при этом в записи регистрации пакета будет установлен соответствующий код предупреждения или ошибки (см. таблица Б.2, стр. 439 и таблица Б.3, стр. 441).
1208	Выключение регистрации NAT	
120B	Добавление записи в ARP-таблицу NAT	
120C	Удаление записей из ARP-таблицы NAT	
120D	Очистка ARP-таблицы NAT	
1217	Включение аутентификации сетевых пользователей	Аутентификация сетевых пользователей включена: работать через МЭ ССПТ-4А1 могут только авторизованные сетевые пользователи.
1218	Выключение аутентификации сетевых пользователей	Аутентификация сетевых пользователей выключена: через МЭ ССПТ-4А1 разрешена передача пакетов в соответствии с конфигурацией NAT и текущей политикой доступа.
1219	Добавление нового сетевого пользователя	
121A	Удаление сетевого пользователя	
121B	Включение сетевого пользователя	Учетная запись сетевого пользователя может быть использована для авторизации.
121C	Выключение сетевого пользователя	Учетная запись сетевого пользователя не может быть использована для авторизации.
121D	Сброс сетевого пользователя	Сеанс работы сетевого пользователя принудительно завершен администратором МЭ ССПТ-4А1.
121E	Смена пароля сетевого пользователя	
121F	Изменение тайм-аута неактивности сетевого пользователя	
1220	Изменение параметров сетевого пользователя	
1221	Добавление новой записи в файл ключей аутентификации	
1222	Удаление записи из файла ключей аутентификации	
1223	Обновление записи в файле ключей аутентификации	

Код	Описание события	Пояснение
1224	Включение WEB-интерфейса	
1225	Выключение WEB-интерфейса	
1226	Включение SNMP-интерфейса	
1227	Выключение SNMP-интерфейса	
1300	Запуск пакетного фильтра	
1301	Перезапуск пакетного фильтра	
1302	Удаление выбранных сессий	Из таблицы сессий удалены сессии в соответствии с критериями, указанными администратором МЭ ССПТ-4А1.
1303	Сброс статистики в правилах	
1310	Выключение управляющего интерфейса	
1311	Включение управляющего интерфейса	
1312	Изменение режима передачи управляющего интерфейса	
1313	Изменение скорости передачи управляющего интерфейса	
1314	Изменение скорости передачи фильтрующего интерфейса	
1315	Изменение режима передачи фильтрующего интерфейса	
1316	Включение выгрузки на SYSLOG-сервер	
1317	Выключение выгрузки на SYSLOG-сервер	
1318	Изменение параметров выгрузки на SYSLOG-сервер	
1319	Сброс настроек выгрузки на SYSLOG-сервер	
1400	Включение RADIUS-авторизации	
1401	Выключение RADIUS-авторизации	
1402	Изменение тайм-аута ожидания ответа от RADIUS-сервера	
1403	Изменение количества обращений к RADIUS-серверу	
1404	Изменение параметров RADIUS-сервера	
1405	Изменение типа учетной записи для RADIUS-авторизации	
1410	Включение управления сессиями	
1411	Выключение управления сессиями	
1412	Включение фильтрации на прикладном уровне	
1413	Выключение фильтрации на прикладном уровне	
1414	Включение поддержки traceroute-сессий	

Код	Описание события	Пояснение
1415	Выключение поддержки traceroute-сессий	
1416	Изменение тайм-аутов TCP	
1417	Изменение тайм-аутов UDP	
1418	Изменение тайм-аутов ICMP	
1419	Изменение тайм-аутов остальных протоколов	
141B	Установка тайм-аутов сессий в значения по умолчанию	
141C	Включение глубокого контроля TCP в сессиях	
141D	Выключение глубокого контроля TCP в сессиях	
141E	Включение использования данных канального уровня в сессиях	
141F	Выключение использования данных канального уровня в сессиях	
1420	Включение сигнализации обнаружения flood-атак	
1421	Выключение сигнализации обнаружения flood-атак	
1422	Изменение комментария TMP-правила для заблокированной flood-атаки	
1423	Изменение времени жизни TMP-правила для заблокированной flood-атаки	
1500	Изменение режима резервирования	
1501	Включение резервирования	
1502	Выключение резервирования	
1503	Изменение смежного резервного устройства	Изменен IP-адрес смежного устройства для резервирования.
1504	Установка параметров резервирования в значения по умолчанию	
1509	Включение автоматической синхронизации политики для функции резервирования	
150A	Выключение автоматической синхронизации политики для функции резервирования	
150B	Синхронизация текущей политики инициирована	Текущая политика доступа отправлена на смежное устройство для синхронизации
150C	Синхронизация текущей политики завершена	Данным устройством принята текущая политика смежного устройства и применена в качестве текущей политики данного устройства.
150D	Изменение скорости передачи интерфейсов для функции резервирования	Изменена скорость передачи фильтрующих интерфейсов для активного или заблокированного состояния интерфейсов при использовании функции резервирования.

Код	Описание события	Пояснение
1513	Добавление нового объекта справочника	
1514	Изменение объекта справочника	
1515	Удаление объекта справочника	
1516	Копирование объекта справочника	
1517	Перемещение объекта справочника	
1519	Добавление нового комментария к группе правил фильтрации	
151A	Изменение комментария к группе правил фильтрации	
151B	Удаление комментария к группе правил фильтрации	
151D	Применение дополнительной политики	
151E	Удаление дополнительного политики	
151F	Сохранение дополнительной политики	
1520	Политика установлена в состояние по умолчанию	
1521	Дополнительная политика загружена	Дополнительная политика доступа загружена на МЭ ССПТ-4А1 с управляющего компьютера администратора.
1524	Изменение комментария к дополнительной конфигурации	
1525	Переименование дополнительной конфигурации	
1526	Изменение MTU управляющего интерфейса	
1527	Изменение MTU фильтрующего интерфейса	
1528	Изменение имени устройства и/или комментария к нему	
1529	Изменение комментария к дополнительной политике	
152A	Переименование дополнительной политики	
152B	Завершение сеансов работы администраторов	
152C	Сброс настроек устройства	Настройки устройства (текущая конфигурация, текущая политика доступа, файл учетные записи администраторов и т. д.) установлены в состояния по умолчанию.
152E	Изменение параметров зеркалирования интерфейсов	
1530	Добавление нового комментария к группе объектов справочника	
1531	Изменение комментария к группе объектов справочника	
1532	Удаление комментария к группе объектов справочника	

Код	Описание события	Пояснение
1533	Добавление нового контейнера NAT	
1534	Удаление контейнера NAT	
1535	Добавление нового интерфейса NAT	
1536	Изменение параметров интерфейса NAT	
1537	Удаление интерфейса NAT	
1538	Добавление нового правила трансляции NAT	
1539	Изменение правила трансляции NAT	
153A	Удаление правила трансляции NAT	
153B	Добавление нового правила переадресации NAT	
153C	Изменение правила переадресации NAT	
153D	Удаление правила переадресации NAT	
153E	Добавление нового маршрута NAT	
153F	Изменение маршрута NAT	
1540	Удаление маршрута NAT	
1541	Установка MAC-адреса на интерфейсе в контексте NAT	
1542	Включение переадресации для контейнера NAT	Для данного контейнера NAT разрешено использование правила переадресации
1543	Выключение переадресации для контейнера NAT	Для данного контейнера NAT запрещено использование правил переадресации
1550	PRI-правило скопировано	
1551	PRI-правило перемещено	
1552	Включение использования правил приоритизации	Приоритизация трафика выполняется в соответствии с правилами приоритизации текущей политики доступа.
1553	Выключение использования правил приоритизации	Правила приоритизации не используются: приоритизация трафика не выполняется.
1554	Установка списка DNS-серверов	
1555	Очистка списка DNS-серверов	
1556	Добавление нового маршрута	
1557	Изменение маршрута	
1558	Удаление маршрута	
1559	Включение HTTP-посредника	Использование HTTP-посредника включено. На сетевом интерфейсе HTTP-посредника установлен IP-адрес. Фильтрующий интерфейс, используемый HTTP-посредником, не доступен для фильтрации трафика.
155A	Выключение HTTP-посредника	Использование HTTP-посредника выключено. Фильтрующий интерфейс, использовавшийся HTTP-посредником, снова доступен для фильтрации трафика.
155B	Изменение параметров HTTP-посредника	

Код	Описание события	Пояснение
155C	Добавление новой записи в список доступа HTTP-посредника	
155D	Изменение записи списка доступа HTTP-посредника	
155E	Удаление записи из списка доступа HTTP-посредника	Удалена запись списка доступа HTTP-посредника с указанным номером либо все записи списка доступа HTTP-посредника (если номер записи не указан).
155F	Включение агрегирования портов управляющего интерфейса	Использование агрегирования портов управляющего интерфейса включено. Соответствующий фильтрующий интерфейс добавлен в агрегат и не доступен для фильтрации трафика.
1560	Выключение агрегирования портов управляющего интерфейса	Использование агрегирования портов управляющего интерфейса выключено. Агрегат удален, фильтрующий интерфейс, входивший в состав агрегата, снова доступен для фильтрации трафика.
1561	Изменение протокола агрегирования	Изменен протокол агрегирования портов управляющего интерфейса.
1562	Изменение интерфейса агрегата	Изменен фильтрующий интерфейс, который будет использован в составе агрегата при включении агрегирования портов управляющего интерфейса.
1563	Запуск отложенной перезагрузки	Отложенная перезагрузка была инициирована администратором
1564	Отмена отложенной перезагрузки	Отложенная перезагрузка была отменена администратором
1565	PROXY-правило скопировано	
1566	PROXY-правило перенесено	

Б.2. События категории предупреждений МЭ ССПТ-4А1

Коды всех событий категории предупреждений МЭ ССПТ-4А1, их текстовая интерпретация и пояснения к ним представлены в таблице Б.2, стр. 439.

Таблица Б.2: События категории предупреждений МЭ ССПТ-4А1

Код	Описание события	Пояснение
2001	Доступ запрещен в соответствии со списком доступа	Попытка доступа к управляющему интерфейсу МЭ ССПТ-4А1 с узле сети, отсутствующего в списке доступа.
2002	Превышена интенсивность отказа в доступе в соответствии со списком доступа	События “Доступ запрещен в соответствии со списком доступа” (2001) временно не регистрируются в связи с их слишком частой регистрацией.
2003	Недостаточно привилегий для выполнения операции	Администратор МЭ ССПТ-4А1 попытался выполнить операцию, для которой у него недостаточно привилегий.

Код	Описание события	Пояснение
2004	Набор выходных интерфейсов пустой	Не является событием. Предупреждение, сохраняемое в записи регистрации пакета. В процессе обработки пакета пакетным фильтром из набора фильтрующих интерфейсов, на которые следовало отправить пакет, были исключены все интерфейсы. В этом случае в записи регистрации пакета фиксируется данное предупреждение.
2005	Вход администратора не выполнен	Авторизация администратора не выполнена по той или иной причине, во входе отказано.
2006	Попытка выхода незарегистрированного администратора	Выполнена попытка выхода администратора, сеанс работы которого был завершен ранее по тайм-ауту неактивности.
2007	Flood-атака обнаружена и заблокирована	Событие, регистрируемое пакетным фильтром. Предупреждение, сохраняемое в записи регистрации пакета, отнесенного к flood-атаке.
200A	Пакет вне окна приемника	Не является событием. Предупреждение, сохраняемое в записи регистрации пакета.
200B	Повторный пакет	Не является событием. Предупреждение, сохраняемое в записи регистрации пакета.
200C	Короткий тайм-аут неактивности сессии	Не является событием. Предупреждение, сохраняемое в записи регистрации пакета.
200D	Состояние резервирования изменено в связи с перевыбором	Состояние резервирования установлено равным режиму резервирования из текущей конфигурации данного устройства МЭ ССПТ-4А1, в связи с преодолением отказа смежным устройством,
200E	Состояние резервирования изменено в связи с отказом смежного устройства	Состояние резервирования данного устройства МЭ ССПТ-4А1 изменено в связи с отказом смежного устройства.
200F	Обнаружен конфликт режимов резервирования смежных устройств	Смежные устройства МЭ ССПТ-4А1 в схеме резервирования используют недопустимую комбинацию режимов резервирования: необходимо сменить режим резервирования в текущей конфигурации одного из устройств.
2010	Синхронизация текущей политики не завершена	Ошибка отправки текущей политики данного устройства МЭ ССПТ-4А1 смежному устройству. Ошибка сохранения принятой от смежного устройства МЭ ССПТ-4А1 политики доступа в качестве текущей политики доступа данного устройства.
2011	Текущая политика отличается от политики на смежном устройстве	Выявлено отличие текущих политик доступа на смежных устройствах МЭ ССПТ-4А1 в схеме резервирования.
2012	Автоматическая синхронизация текущей политики временно заблокирована	Автоматическая синхронизация текущей политики временно заблокирована. Для разблокировки функции необходимо вручную выполнить синхронизацию политик доступа.
2013	Автоматическая синхронизация текущей политики разблокирована	Автоматическая синхронизация текущей политики разблокирована в результате проверки идентичности политик доступа смежных устройств МЭ ССПТ-4А1.
2014	Неверный старый пароль	Введен неверный старый (текущий) пароль для учетной записи.

Код	Описание события	Пояснение
2015	Настройки устройства сброшены частично	В результате выполнения команды “system default” часть файлов не была сброшена в состояние по умолчанию из-за возникших ошибок: перечень файлов указывается следом за строкой описания события.
2016	Отказ в аутентификации сетевого пользователя	Неудачная попытка авторизации сетевого пользвателя.

Б.3. События категории ошибок МЭ ССПТ-4А1

Коды всех событий категории ошибок МЭ ССПТ-4А1, их текстовая интерпретация и пояснения к ним представлены в таблице Б.3, стр. 441.

Таблица Б.3: События категории ошибок МЭ ССПТ-4А1

Код	Описание события	Пояснение
3001	Нарушена целостность программного обеспечения ССПТ-4	Выявлено нарушение целостности программного обеспечения МЭ ССПТ-4А1: выполняются действия описанные в разделе 1.4.9, стр. 28.
3002	Ошибка операционной системы	Системная ошибка в пакетном фильтре.
3006	Сессия не добавлена - некорректный набор флагов	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3007	Сессия не добавлена - таблица переполнена	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3008	Сессия не добавлена - ошибка распределения памяти	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3009	Контекст сессии - неверный идентификатор VLAN	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
300A	Контекст сессии - неверный входной интерфейс	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
300C	Контекст сессии - неверный набор флагов	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
300D	Контекст сессии - неверный номер последовательности	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
300E	Контекст сессии - неверный номер подтверждения	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
300F	Контекст сессии - неизвестное состояние	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3102	NAT - неизвестный тип ARP-сообщения	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3103	NAT - неверный IP-адрес источника	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3104	NAT - неверный IP-адрес приемника	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3105	NAT - внутренний пакет	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3106	NAT - нет свободных портов	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3108	NAT - недопустимое ICMP-сообщение	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.

Код	Описание события	Пояснение
3109	NAT - недопустимый протокол	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
310A	NAT - сессия не создана по пакету	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
310B	NAT - неверный пакет на внешнем интерфейсе	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
310C	NAT - не найдена соответствующая сессия	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
310D	NAT - не найдена соответствующая запись в ARP-таблице	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
310E	NAT - соответствующий маршрут не найден	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3110	NAT - соответствующее правило трансляции не найдено	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3111	Неверная длина заголовка IP-пакета	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3112	NAT - фрагментированный пакет	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3113	Неверная длина IP-пакета	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3114	NAT - IP-пакет не аутентифицирован	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3115	Неверная длина TCP-заголовка	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3116	NAT - различные выходные интерфейсы в правиле и ARP-таблице	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3117	NAT - неверный MAC-адрес назначения	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3118	Фрагментация: нарушен порядок прихода пакетов	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3119	Фрагментация: некорректно установленные флаги	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3120	Фрагментация: таблица фрагментированных потоков переполнена	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.
3121	Требуется проверка сессии на соответствие измененной политике доступа	Не является событием. Ошибка, сохраняемая в записи регистрации пакета.

Приложение В. Перечень диагностических сообщений ПО МЭ ССПТ-4А1

В.1. Формат диагностических сообщений ПО МЭ ССПТ-4А1

Формализованные диагностические сообщения ПО МЭ ССПТ-4А1 имеют следующий формат:

```
<ПРЕФИКС_ПОДСИСТЕМЫ>-{E|W|I}-XXX.YY.ZZZZ-<текст_сообщения>[ (<системная_ошибка>)]
```

где:

- `<ПРЕФИКС_ПОДСИСТЕМЫ>` – идентификатор подсистемы, от которой получено сообщение:
  - ✔ `FNPAPI` – сообщения библиотеки сервисных функций ПО МЭ ССПТ-4А1;
  - ✔ `FNPSH` – сообщения командного интерпретатора МЭ ССПТ-4А1;
  - ✔ `FNPSHD` – сообщения командного сервера МЭ ССПТ-4А1;
- `{E|W|I}` – класс (категория) сообщения:
  - ✔ `E` – сообщение об ошибке;
  - ✔ `W` – предупреждающее сообщение;
  - ✔ `I` - информационное сообщение;
- `XXX.YY.ZZZZ` – составной код сообщения (`XXX`, `YY`, `ZZZZ` - шестнадцатеричные числа):
  - ✔ `XXX` – код продукта. Для ПО МЭ ССПТ-4А1 код продукта – `007`;
  - ✔ `YY` – код подсистемы ПО МЭ ССПТ-4А1:
    - ◆ `01` – библиотека сервисных функций ПО МЭ ССПТ-4А1;
    - ◆ `02` – командный интерпретатор МЭ ССПТ-4А1;
    - ◆ `03` – командный сервер МЭ ССПТ-4А1;
  - ✔ `ZZZZ` – код диагностического сообщения данной подсистемы ПО МЭ ССПТ-4А1:
    - ◆ `1ZZZ` – диапазон кодов для сообщений об ошибках;
    - ◆ `2ZZZ` – диапазон кодов для предупреждающих сообщений;
    - ◆ `3ZZZ` – диапазон кодов для информационных сообщений;
- `<текст_сообщения>` – текстовая интерпретация кода диагностического сообщения. Текст сообщения выводится на русском языке в кодировке UTF-8;
- `<системная_ошибка>` – необязательное сообщение, включаемое в строку диагностического сообщения, если при выполнении команды произошла системная ошибка. Сообщения о системных ошибках являются стандартными для УОС МЭ ССПТ-4А1.

Диагностические сообщения класса **информационных сообщений командного интерпретатора** МЭ ССПТ-4А1 выводятся в качестве подтверждения успешного выполнения команд по изменению параметров конфигурации МЭ ССПТ-4А1, команд по изменению политик доступа и т. д.

Диагностические сообщения класса **предупреждающих сообщений командного интерпретатора** МЭ ССПТ-4А1 выводятся в том случае, если команда не может быть выполнена по каким-либо причинам, не относящимся к ошибкам выполнения команд (например: недопустимые привилегии администратора для выполнения команд, отсутствие данных, вывод которых ожидается по команде и т. д.).

Диагностические сообщения класса **сообщений об ошибках командного интерпретатора** МЭ ССПТ-4А1 выводятся в случае ошибок выполнения команд (например: некорректный формат параметра команды, отсутствие обязательного параметра команды, отсутствие правила фильтрации, объекта справочника, на который ссылается команда).

Диагностические сообщения **библиотеки сервисных функций** ПО МЭ ССПТ-4А1 могут к одному из двух классов:

- **сообщения об ошибках**: выводятся в случае ошибок, выявленных при выполнении функций библиотеки при разборе политик доступа, конфигураций, выполнении команд и т.д.;
- **предупреждающие сообщения**: выводятся при положительных результатах проверок того, что подсистема уже включена (запущена), либо уже выключен (не запущена).

Диагностические сообщения **командного сервера** МЭ ССПТ-4А1 имеют единственный класс - класс **сообщений об ошибках** и выводятся в **журнал регистрации системных сообщений**, в случае ошибок, возникающих в ходе работы данной подсистемы (например при использовании средств удаленного администрирования и мониторинга МЭ ССПТ-4А1, таких как WEB-интерфейс, SNMP-интерфейс).

В.2. Диагностические сообщения библиотеки сервисных функций ПО МЭ ССПТ-4А1

В.2.1. Сообщения об ошибках

Коды всех сообщений об ошибках библиотеки сервисных функций ПО МЭ ССПТ-4А1, их текстовая интерпретация и описание представлены в таблице В.1.

Таблица В.1: Сообщения об ошибках библиотеки сервисных функций ПО МЭ ССПТ-4А1

Код	*Сообщение*	*Описание*
007.01.1000	Недопустимые параметры	Функции переданы недопустимые значения аргументов. **Действия**: Обратиться на предприятие-изготовитель.
007.01.1001	Системная ошибка	Системная ошибка. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1002	Нарушена структура системных данных интерфейсов	Ошибка получения от УОС МЭ ССПТ-4А1 информации по сетевым интерфейсам. **Действия**: Проверить целостность компонентов УОС МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1003	Ошибка инициализации файла	Ошибка инициализации файлов текущей политики доступа при первом запуске МЭ ССПТ-4А1. **Действия**: Обратиться на предприятие-изготовитель.
007.01.1004	Ошибка отправки запроса пакетному фильтру	Ошибка при отправке запроса пакетному фильтру МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли пакетный фильтр. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1005	Нет ответа от пакетного фильтра	Истекло время ожидания ответа от пакетного фильтра МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли пакетный фильтр.
007.01.1006	Ошибка получения ответа от пакетного фильтра	Ошибка выполнения запроса пакетным фильтром. **Действия**: Повторно выполнить запрос. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1008	Ошибка чтения файла конфигурации ССПТ-4А1	Системная ошибка чтения файла текущей конфигурации МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов операционной системы МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1009	Ошибка разбора файла конфигурации ССПТ-4А1	Файл текущей конфигурации МЭ ССПТ-4А1 имеет некорректный формат или содержит ошибки. **Действия**: Проверить целостность компонентов операционной системы МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.100A	Ошибка вычисления контрольной суммы файла	Ошибка вычисления контрольной суммы файла УОС МЭ ССПТ-4А1 или программного обеспечения МЭ ССПТ-4А1. **Действия**: Повторить выполнение команды. В случае повторения ошибки немедленно выключить МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.01.100B	Ошибка чтения файла контрольных сумм	Системная ошибка чтения файла контрольных сумм файлов УОС МЭ ССПТ-4А1 и программного обеспечения МЭ ССПТ-4А1. **Действия**: Немедленно выключить МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.01.100C	Нарушен размер файла контрольных сумм	Файл контрольных сумм имеет неправильный размер. **Действия**: Немедленно выключить МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.01.100D	Запись не найдена в файле контрольных сумм	Не удалось обновить файл контрольных сумм, так как не найдена соответствующая запись в файле контрольных сумм. **Действия**: Немедленно выключить МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.01.100E	Ошибка записи файла контрольных сумм	Не удалось обновить файл контрольных сумм, так как возникла ошибка записи в файл. **Действия**: Немедленно выключить МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.01.100F	Ошибка чтения PID-файла	Ошибка чтения PID-файла подсистемы МЭ ССПТ-4А1. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1010	Неверный формат PID файла	Неверный формат PID-файла подсистемы МЭ ССПТ-4А1. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1011	Ошибка отправки сигнала серверу проверки контрольных сумм	Ошибка отправки сигнала серверу проверки контрольных для перечитывания файла контрольных сумм. **Действия**: Убедиться, что сервер проверки контрольных сумм МЭ ССПТ-4А1 запущен. Если не запущен, то немедленно выключить МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.01.1012	Ошибка чтения временного файла данных	Системная ошибка чтения временного файла. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1013	Стартовый сценарий FNPWEB завершился неудачей	Ошибка при включении либо выключении WEB-интерфейса администратора МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки.
007.01.1014	Ошибка запуска стартового сценария FNPWEB	Ошибка при включении либо выключении WEB-интерфейса администратора МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки.

Код	Сообщение	Описание
007.01.1015	Системная ошибка в дочернем процессе	Ошибка при включении либо выключении WEB-интерфейса или SNMP-интерфейса администратора МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки.
007.01.1016	Ошибка запуска стартового сценария FNPSNMP	Ошибка при включении либо выключении SNMP-интерфейса администратора МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки.
007.01.1017	Стартовый сценарий FNPSNMP завершился неудачей	Ошибка при включении либо выключении SNMP-интерфейса администратора МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки.
007.01.101A	Недопустимый тип правила	Недопустимый тип правила в определении правила в текущей или дополнительной политике доступа. **Действия**: В случае ошибки в текущей или дополнительной политике доступа проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.01.101B	Недопустимый номер правила	Номер правила не удовлетворяет формату или допустимому диапазону значений.
007.01.101C	Недопустимое действие	Недопустимое действие для данного типа правил фильтрации.
007.01.101D	Недопустимый тип регистрации	Недопустимый тип регистрации в правиле фильтрации.
007.01.101E	Неверный формат глобального правила	В определении глобального общего правила или глобального АР-правила присутствуют недопустимые параметры.
007.01.101F	Недопустимый входной интерфейс	Недопустимый входной интерфейс в правиле фильтрации.
007.01.1020	Недопустимый выходной интерфейс	Недопустимый выходной интерфейс в правиле фильтрации.
007.01.1025	Недопустимое значение активности	Недопустимое значение активности правила фильтрации.
007.01.1026	Недопустимое регулярное выражение	Системная ошибка при компиляции регулярных выражений в библиотеке сервисных функций ПО МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.01.1027	Неверный формат комментария	Неверный формат комментария к объекту справочника или правилу.
007.01.1028	Недопустимый тип кадра Ethernet	Недопустимый тип кадра Ethernet в общем правиле.
007.01.1029	Недопустимые коды протоколов для указанного типа кадра	Недопустимые коды протоколов для указанного типа кадра в общем правиле.
007.01.102C	Слишком длинный список	Число элементов в списке в значении параметра объекта справочника или правила превышает максимально допустимое.
007.01.102D	Недопустимые значения протокола	Недопустимые значения протокола (в команде, текущей или дополнительной конфигурации, текущей или дополнительной политике доступа).
007.01.102E	Недопустимые значения порта	Недопустимые значения TCP-порта или UDP-порта (в команде, текущей или дополнительной конфигурации, текущей или дополнительной политике доступа).
007.01.1030	Недопустимые значения флагов TOS	Недопустимые значения флагов TOS в общем правиле.
007.01.1032	Недопустимая длина IP-пакета	Недопустимая длина IP-пакета в общем правиле.
007.01.1033	Недопустимое значение TTL	Недопустимое значение TTL в общем правиле.
007.01.1034	Недопустимое значение типа/кода ICMP	Недопустимое значение типа/кода ICMP в определении правила фильтрации или объекта справочника.
007.01.1036	Неверный формат IP-адреса	Неверный формат IP-адреса (в команде, конфигурации, политике доступа).
007.01.1037	Неверный формат IP-маски	Неверный формат IP-маски (в команде, конфигурации, политике доступа).
007.01.1038	Недопустимый интервал IP-адресов	Недопустимый интервал IP-адресов (в команде, конфигурации, политике доступа).
007.01.1039	Недопустимый прикладной протокол	Недопустимый прикладной протокол в AP-правиле.
007.01.103A	Недопустимая строка поиска	Недопустимая строка поиска в AP-правиле.
007.01.103B	Недопустимое значение зависимости от регистра	Недопустимое значение зависимости от регистра в AP-правиле.
007.01.103C	Недопустимое значение направления потока	Недопустимое значение направления потока в AP-правиле.
007.01.103E	Параметр определен дважды	Параметр команды дублируется.
007.01.103F	Недопустимое значение параметра <command> прикладного протокола	Недопустимое значение параметра <command> в AP-правиле.
007.01.1040	Недопустимое значение параметра <olv> прикладного протокола	Недопустимое значение параметра <olv> в AP-правиле.
007.01.1041	Недопустимое значение параметра <method> прикладного протокола	Недопустимое значение параметра <method> в AP-правиле.
007.01.1042	Недопустимое значение параметра <begin> прикладного протокола	Недопустимое значение параметра <begin> в AP-правиле.
007.01.1046	Недопустимое значение времени жизни	Недопустимое значение времени жизни в TMP-правиле.

Код	Сообщение	Описание
007.01.104C	Недопустимое значение идентификатора VLAN	Недопустимое значение идентификатора VLAN в определении правила или объекта справочника.
007.01.104E	Недопустимый интервал даты/времени	Недопустимый интервал даты/времени в объекте Интервал времени (time) справочника.
007.01.1051	Недопустимое значение параметра сигнализации	Недопустимое значение параметра сигнализации в правиле фильтрации.
007.01.1052	Обязательный параметр "action" не определен	Обязательный параметр "action" не определен в правиле фильтрации.
007.01.1055	Обязательный параметр "srcif" и один из следующих должны быть определены: "srcip4", "srcip6", "srcport", "dstip4", "dstip6" или "dstport"	В определении ТМР-правила отсутствует один из обязательных параметров.
007.01.1056	Недопустимое значение тайм-аута сессии	Недопустимое значение тайм-аута сессии в общем правиле.
007.01.1058	Недопустимое значение месяцев	Недопустимое значение месяцев в объекте Интервал времени (time) справочника.
007.01.1059	Недопустимое значение дней месяца	Недопустимое значение дней месяца в объекте Интервал времени (time) справочника
007.01.105A	Недопустимое значение дней недели	Недопустимое значение дней недели в объекте Интервал времени (time) справочника.
007.01.105C	Недопустимое значение параметра использования сессии	Недопустимое значение параметра создания сессии по данному общему правилу.
007.01.105D	Недопустимый параметр для данного прикладного протокола	Недопустимый параметр для данного прикладного протокола в АР-правиле.
007.01.105E	Недопустимое значение параметра	Недопустимое значение параметра в контексте некоторой команды.
007.01.1060	Изменение значения параметра "protocol" не допустимо	Попытка изменения значения параметра "protocol" АР-правила.
007.01.1061	Неподдерживаемая скорость передачи	Неподдерживаемая скорость передачи для сетевого интерфейса МЭ ССПТ-4А1.
007.01.1063	Ошибка чтения файла справочника	Системная ошибка чтения файла справочника текущей или дополнительной политики доступа. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1064	Объект не найден в файле справочника	Объект, на который ссылается определение правила или объекта справочника, не найден в файле справочника политики доступа.
007.01.1065	Неверный формат имени объекта справочника	Имя объекта справочника не соответствует формату.
007.01.1067	Обязательный параметр "name" не определен	Обязательный параметр "name" объекта справочника не определен.
007.01.1068	Обязательный параметр "months" или "mdays" или "wdays" или "dtime" не определен	Обязательный параметр "months" или "mdays" или "wdays" или "dtime" объекта Интервал времени (time) справочника не определен.
007.01.106A	Обязательный параметр "vid" не определен	Обязательный параметр "vid" объекта Группа VLAN (vlan-group) справочника не определен.
007.01.106B	Обязательный параметр "ip4" или "ip6" или "mac" не определен	Обязательный параметр "ip4" или "ip6" или "mac" объекта Узел сети (host) справочника не определен.

Код	Сообщение	Описание
007.01.106C	Обязательный параметр "ip4" или "ip6" не определен	Обязательный параметр "ip4" или "ip6" объекта Сеть (net) справочника не определен.
007.01.106D	Обязательный параметр "protocol" не определен	Обязательный параметр "protocol" объекта Сервис (service) справочника не определен.
007.01.106E	Обязательные параметры "service" и "host" или "net" или "net-group" не определены	Обязательные параметры "service" и "host" или "net" или "net-group" объекта Ресурс (resource) справочника не определены.
007.01.106F	Обязательный параметр "hostname" не определен	Обязательный параметр "hostname" объекта Группа доменных имен (domain-group) справочника не определен.
007.01.1070	Недопустимый параметр для данного протокола	Недопустимый параметр для данного протокола в объекте Сервис (service) справочника.
007.01.1072	Объект уже есть в списке	Имя объекта дублируется в списке.
007.01.1075	Данное имя уже используется в справочнике	Ошибка добавления объекта в справочник с именем уже существующего объекта.
007.01.1077	Недопустимый тип объекта справочника	Недопустимый тип объекта справочника.
007.01.1078	Неверный формат MAC-адреса	Неверный формат MAC-адреса.
007.01.107A	Недопустимая версия протокола IP	Недопустимая версия протокола IP в общем правиле.
007.01.107B	Недопустимое значение параметра Traffic class	Недопустимое значение параметра “Traffic class” (class) в общем правиле.
007.01.107C	Недопустимое значение параметра использования фрагментации	Недопустимое значение параметра использования фрагментации в общем правиле.
007.01.107D	Недопустимое значение параметра использования дополнительного заголовка IPv6	Недопустимое значение параметра использования дополнительного заголовка IPv6 в общем правиле.
007.01.107E	Ошибка чтения файла правил	Системная ошибка чтения файла правил текущей или дополнительной политики доступа. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.107F	Неверный формат строки определения	Несоответствие введенной команды общему формату.
007.01.1082	Оба обязательных параметра "host" и "net" не определены	Оба обязательных параметра "host" и "net" объекта Группа сетевых объектов (net-group) справочника не определены.
007.01.1083	Недопустимое значение параметра разрыва сессии	Недопустимое значение параметра разрыва сессии общего правила.
007.01.1084	Повтор номера правила	В политике доступа уже существует правило данного типа с данным номером.
007.01.1085	Повтор строки комментария	В файлах справочника и правил фильтрации политик доступа не допускается нескольких строк комментариев подряд.
007.01.1086	В конце файла отсутствует пустая строка	Файлы справочника и правил фильтрации должны заканчиваться пустой строкой.
007.01.1087	Отсутствует глобальное общее правило	В политике доступа отсутствует глобальное общее правило.
007.01.1088	Отсутствует глобальное AP-правило	В политике доступа отсутствует глобальное AP-правило.

Код	Сообщение	Описание
007.01.1089	Таблица общих правил переполнена	Число общих правил в политике доступа больше максимально допустимого значения.
007.01.108A	Таблица АР-правил переполнена	Число АР-правил в политике доступа больше максимально допустимого значения.
007.01.108B	Число объектов данного типа превышает максимальное	Число объектов справочника данного типа в политике доступа больше максимально допустимого значения.
007.01.10AA	Неверный формат комментария к дополнительной политике	Неверный формат комментария к дополнительной политике доступа.
007.01.1100	Ошибка соединения с сервером резервирования	Ошибка соединения с сервером резервирования. **Действия**: Проверить, запущен ли сервер резервирования. Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1101	Ошибка отправки запроса серверу резервирования	Ошибка отправки запроса серверу резервирования. **Действия**: Проверить, запущен ли сервер резервирования. Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1102	Ошибка получения ответа от сервера резервирования	Ошибка получения ответа от сервера резервирования. **Действия**: Проверить, запущен ли сервер резервирования. Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1103	Ошибка перезапуска сервера резервирования	Ошибка перезапуска сервера резервирования. **Действия**: Проверить, запущен ли сервер резервирования. Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1104	Ошибка синхронизации текущей политики сервером резервирования	Ошибка выполнения сервером резервирования запроса автоматической синхронизации текущей политики доступа. **Действия**: Проверить корректность настроек резервирования и состояний резервирования данного и смежного устройств МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1105	Ошибка получения состояния сервера резервирования	**Действия**: Проверить, запущен ли сервер резервирования. Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.1106	IP-маска недопустима	В данном контексте недопустимо использование IP-маски.
007.01.1107	IP-адреса узлов недопустимы	В данном контексте недопустимо использование IP-адресов узлов сети.

Код	Сообщение	Описание
007.01.1108	Диапазон IP-адресов недопустим	В данном контексте недопустимо использование диапазона IP-адресов.
007.01.1109	Недопустимый IP-адрес подсети	Недопустимый IP-адрес подсети, например вместо IP-адреса подсети указан IP-адрес узла сети.
007.01.110A	IP-маска должна быть указана	В данном контексте требуется указание IP-маски вместе с IP-адресом.
007.01.110B	Повтор значения в списке	В списке значений (например: IP-адресов, портов и т. д.) имеются одинаковые элементы.
007.01.1A00	Конфликт типа кадра и номеров протоколов	В определении общего правила выявлен конфликт типа кадра и номеров протоколов, инкапсулированных в кадр Ethernet.
007.01.1A01	Недопустимая комбинация типов использованных объектов	В определении общего правила выявлена недопустимая комбинация типов использованных объектов.
007.01.1A02	Списки объектов источника и приемника включают в себя один и тот же объект	В определении общего правила списки сетевых объектов источника и приемника включают в себя один и тот же объект.
007.01.1A03	Недопустимая комбинация использованных параметров правила и объектов	В определении общего правила выявлена недопустимая комбинация использованных параметров правила и объектов справочника.
007.01.1A04	Конфликт интерфейсов источника и приемника	В определении общего правила списки входных и выходных интерфейсов (для параметров правила или комбинаций используемых объектов) имеют общие интерфейсы.
007.01.1A05	Недопустимые значения параметра VLAN	В определении общего правила выявлен конфликт значений параметра VLAN общего правила и объектов, справочника, используемых в правиле. Либо в определении общего правила выявлен конфликт значений параметра VLAN объектов источника и приемника, используемых в правиле.
007.01.1A06	Порты источника и приемника - недопустимые параметры для данного протокола	В определении общего правила выявлен конфликт использования портов источника и/или приемника и значения параметра протокола, инкапсулированного в IP.
007.01.1A07	Коды/типы ICMP - недопустимые параметры для данного протокола	В определении общего правила выявлен конфликт использования типов и кодов ICMP и/или ICMP4 и значения параметра протокола, инкапсулированного в IP.
007.01.1A08	Недопустимая комбинация IP-адресов и версии протокола IP	В определении общего правила выявлен конфликт используемых IP-адресов источника и/или приемника и значения параметра версии протокола IP.
007.01.1A09	Недопустимая комбинация адресов источника и приемника	В определении общего правила выявлен неразрешимый конфликт по адресам источника и приемника (IPv4, IPv6 и MAC).
007.01.1A0A	AP-правило отсутствует в политике	В определении общего правила есть ссылки на AP-правила, отсутствующие в политике доступа.
007.01.1A0B	Правило с индексом для действия "goto" отсутствует в политике	В определении общего правила действие “goto” ссылается на другое общее правило, отсутствующее в политике доступа.
007.01.1A0C	Недопустимая комбинация версии протокола IP и кода протокола	В определении общего правила выявлена недопустимая комбинация версии протокола IP и кода протокола, инкапсулированного в IP.

Код	Сообщение	Описание
007.01.1A0D	Порты клиента и сервера - недопустимые параметры для данного протокола	В определении АР-правила выявлен конфликт использования портов клиента и/или сервера и значения параметра протокола, инкапсулированного в IP.
007.01.1A0E	IPv4 и IPv6 адреса вместе недопустимы для использования в ТМР-правиле	В определении ТМР-правила используются и IPv4-адреса и IPv6-адреса, что недопустимо.
007.01.1A0F	Недопустимая комбинация версии протокола IP и параметров заголовка IP	В определении общего правила выявлена недопустимая комбинация версии протокола IP и параметров заголовка IP (например: версия IP: 4 и при этом определен параметр “Класс трафика”, который относится к заголовку IPv6).
007.01.1B06	Некорректный интерфейс в записи ARP-таблицы NAT	В конфигурации МЭ ССПТ-4А1 запись ARP-таблицы ссылается на фильтрующий интерфейс, отсутствующий в данном экземпляре МЭ ССПТ-4А1.
007.01.1B08	Число записей не соответствует числу фильтрующих интерфейсов	В конфигурации МЭ ССПТ-4А1 число записей фильтрующих интерфейсов не соответствует числу фильтрующих интерфейсов данного экземпляра МЭ ССПТ-4А1.
007.01.1B09	Имя фильтрующего интерфейса не уникально	В конфигурации МЭ ССПТ-4А1 имеются фильтрующие интерфейсы с одинаковыми назначенными именами.
007.01.1B0A	Недопустимый зеркалируемый интерфейс	В конфигурации МЭ ССПТ-4А1 в качестве зеркалируемого интерфейса задан фильтрующий интерфейс, отсутствующий на данном экземпляре МЭ ССПТ-4А1.
007.01.1B0B	Недопустимый зеркалирующий интерфейс	В конфигурации МЭ ССПТ-4А1 в качестве зеркалирующего интерфейса задан фильтрующий интерфейс, отсутствующий на данном экземпляре МЭ ССПТ-4А1.
007.01.1B0C	Зеркалируемый и зеркалирующий интерфейсы должны быть различными	В конфигурации МЭ ССПТ-4А1 в качестве зеркалируемого и зеркалирующего интерфейсов задан один и тот же фильтрующий интерфейс.
007.01.1B0E	Несоответствие версий конфигурации и ПО устройства	В конфигурации МЭ ССПТ-4А1 версия не соответствует версии ПО данного экземпляра МЭ ССПТ-4А1.
007.01.1B0F	Недопустимый номер(а) интерфейса	В конфигурации МЭ ССПТ-4А1 в параметрах внутреннего или внешнего интерфейса NAT указан недопустимый номер фильтрующего интерфейса.
007.01.1B10	Интерфейс NAT отсутствует в контейнере NAT	В конфигурации МЭ ССПТ-4А1 в правиле трансляции, правиле переадресации или маршруте NAT имеется ссылка на интерфейс NAT, отсутствующий в контейнере NAT.
007.01.1B11	Имя контейнера NAT уже используется	В конфигурации МЭ ССПТ-4А1 несколько контейнеров NAT имеют одно и то же имя.
007.01.1B12	Имя интерфейса NAT уже используется	В конфигурации МЭ ССПТ-4А1 несколько внешних или внутренних интерфейсов NAT имеют одно и то же имя.
007.01.1B13	IP-адрес уже используется интерфейсом NAT	В конфигурации МЭ ССПТ-4А1 IP-адрес в списке IP-адресов внутреннего или внешнего интерфейса NAT не отвечает требованию уникальности IP-адресов для внутренного или внешнего интерфейса NAT соответственно.

Код	Сообщение	Описание
007.01.1B14	Внешний IP-адрес должен быть адресом внешнего интерфейса NAT	В конфигурации МЭ ССПТ-4А1 в правиле трансляции или правиле переадресации NAT внешний IP-адрес, не назначен ни на один из внешних интерфейсов NAT данного контейнера NAT.
007.01.1B15	Конфликт внешних и внутренних портов в правиле переадресации NAT	В конфигурации МЭ ССПТ-4А1 в правиле переадресации NAT число внутренних портов и число внешних портов отличаются.
007.01.1B16	Недопустимое значение номера правила трансляции NAT	В конфигурации МЭ ССПТ-4А1 правило трансляции имеет недопустимый номер.
007.01.1B17	Недопустимый IP-адрес назначения маршрута NAT	В конфигурации МЭ ССПТ-4А1 маршрут NAT имеет недопустимый IP-адрес назначения.
007.01.1B18	Недопустимый IP-адрес шлюза в маршруте NAT	В конфигурации МЭ ССПТ-4А1 маршрут NAT имеет недопустимый IP-адрес шлюза.
007.01.1B19	Интерфейс NAT делит фильтрующие интерфейсы с другим интерфейсом NAT	В конфигурации МЭ ССПТ-4А1 нарушены требования по совместному использованию фильтрующих интерфейсов для внутреннего или внешнего интерфейса NAT.
007.01.1B1A	Недопустимая скорость передачи для резервирования	В конфигурации МЭ ССПТ-4А1 скорость передачи фильтрующих интерфейсов в активном или заблокированном состоянии для резервирования является недопустимой (не поддерживается фильтрующими интерфейсами данного МЭ).
007.01.1B1B	Режим резервирования не соответствует аппаратной конфигурации	В конфигурации МЭ ССПТ-4А1 задан режим резервирования, который не может быть использован на данном экземпляре МЭ, т. к. списки допустимых скоростей передачи фильтрующих интерфейсов данного экземпляра МЭ ССПТ-4А1 не идентичны.
007.01.1B1C	Интерфейс не должен использоваться как зеркалирующий интерфейс и интерфейс NAT	В конфигурации МЭ ССПТ-4А1 один и тот же фильтрующий интерфейс используется в качестве зеркалирующего интерфейса и в составе интерфейса NAT.
007.01.1B1D	Внутренний IP-адрес не должен быть адресом внутреннего интерфейса NAT	В конфигурации МЭ ССПТ-4А1 в правиле переадресации NAT внутренний IP-адрес является IP-адресом внутреннего интерфейса NAT.
007.01.1B1E	MAC-адреса фильтрующих интерфейсов в контексте NAT повторяются	В конфигурации МЭ ССПТ-4А1 MAC-адреса фильтрующих интерфейсов в контексте функции NAT повторяются.
007.01.1B1F	Таблица правил трансляции NAT переполнена	В конфигурации МЭ ССПТ-4А1 число правил трансляции NAT превышает максимально допустимое.
007.01.1B20	Таблица правил переадресации NAT переполнена	В конфигурации МЭ ССПТ-4А1 число правил переадресации NAT превышает максимально допустимое.
007.01.1B21	Таблица маршрутов NAT переполнена	В конфигурации МЭ ССПТ-4А1 число маршрутов NAT превышает максимально допустимое.
007.01.1B22	Неверный формат имени устройства	В конфигурации МЭ ССПТ-4А1 имя устройства не имеет неверный формат.
007.01.1B23	Таблица PRI-правил переполнена	В политике доступа МЭ ССПТ-4А1 число правил приоритизации превышает максимально допустимое.
007.01.1B24	Недопустимый приоритет	Недопустимое значение приоритета в правиле приоритизации.

Код	Сообщение	Описание
007.01.1B25	Обязательный параметр "priority" и один из следующих должны быть определены: "srcif", "srcip4", "srcip6", "srcport", "dstip4", "dstip6" или "dstport"	В определении правила приоритизации отсутствуют обязательные параметры.
007.01.1B26	IPv4 и IPv6 адреса вместе недопустимы для использования в PRI-правиле	Недопустимая комбинация значений параметров в определении правила приоритизации.
007.01.1B27	Таблица маршрутов переполнена	В конфигурации МЭ ССПТ-4А1 число маршрутов превышает максимально допустимое.
007.01.1B28	Недопустимый IP-адрес назначения маршрута	В конфигурации МЭ ССПТ-4А1 маршрут имеет недопустимый IP-адрес назначения.
007.01.1B29	Недопустимый IP-адрес шлюза в маршруте	В конфигурации МЭ ССПТ-4А1 маршрут имеет недопустимый IP-адрес шлюза.
007.01.1B2A	Ошибка модификации маршрутной таблицы	Ошибка модификации маршрутной таблицы УОС МЭ ССПТ-4А1.
007.01.1B2B	Ошибка очистки маршрутной таблицы	Ошибка очистки маршрутной таблицы УОС МЭ ССПТ-4А1.
007.01.1B2C	Ошибка запуска стартового сценария FNPPROXY	Ошибка при включении либо выключении HTTP-посредника МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки
007.01.1B2D	Стартовый сценарий FNPPROXY завершился неудачей	Ошибка при включении HTTP-посредника МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки.
007.01.1B2E	HTTP-посредник включен, но IP-адрес не определен	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B2F	HTTP-посредник и зеркалирование не должны использовать общий интерфейс	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B30	HTTP-посредник и NAT не должны использовать общий интерфейс	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B31	HTTP-посредник и резервирование не должны использоваться совместно	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B32	Список доступа HTTP-посредника переполнен	В конфигурации МЭ ССПТ-4А1 число записей списка доступа HTTP-посредника превышает максимально допустимое.
007.01.1B33	IP-адреса HTTP-посредника и управляющего интерфейса должны быть из разных подсетей	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.

Код	Сообщение	Описание
007.01.1B34	Агрегирование портов управляющего интерфейса и зеркалирование не должны использовать общий интерфейс	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B35	Агрегирование портов управляющего интерфейса и NAT не должны использовать общий интерфейс	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B36	Агрегирование портов управляющего интерфейса и HTTP-посредник не должны использовать общий интерфейс	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B38	В устройстве недостаточно фильтрующих интерфейсов для использования данной функции	В конфигурации МЭ ССПТ-4А1 число фильтрующих интерфейсов недостаточно для использования включенной функции (HTTP-посредник или агрегирование портов).
007.01.1B39	MTU интерфейсов в составе агрегата не должны отличаться	В конфигурации МЭ ССПТ-4А1 включено агрегирование портов управляющего интерфейса и при этом MTU интерфейсов, входящих в состав агрегата, отличаются.
007.01.1B3A	HTTP-посредник и правило фильтрации используют общий интерфейс	Не допускается использование одного и того же фильтрующего интерфейса в качестве интерфейса HTTP-посредника и в правилах фильтрации.
007.01.1B3B	HTTP-посредник и объект справочника используют общий интерфейс	Не допускается использование одного и того же фильтрующего интерфейса в качестве интерфейса HTTP-посредника и в объектах справочника.
007.01.1B3C	Агрегирование портов управляющего интерфейса и правило фильтрации используют общий интерфейс	Не допускается использование одного и того же фильтрующего интерфейса в составе агрегата и в правилах фильтрации.
007.01.1B3D	Агрегирование портов управляющего интерфейса и объект справочника используют общий интерфейс	Не допускается использование одного и того же фильтрующего интерфейса в составе агрегата и в объектах справочника.
007.01.1B3E	Ошибка при сравнении по регулярному выражению	При выполнении проверки соответствия строки регулярному выражению произошла ошибка. Не удалось проверить строку на соответствие регулярному выражению.
007.01.1B3F	Недостаточный размер вектора выходных подстрок регулярного выражения	Неверный формат вспомогательного параметра, используемого при проверке строки по регулярному выражению.
007.01.1B40	Для использования NAT режим управления сессиями должен быть включен	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B41	Для использования NAT необходим контейнер с как минимум одним внутренним и одним внешним интерфейсом	В конфигурации МЭ ССПТ-4А1 указана недопустимая комбинация значений параметров.
007.01.1B42	Скорости передачи фильтрующих интерфейсов для активного и заблокированного состояний должны отличаться (резервирование)	В дополнительной конфигурации МЭ ССПТ-4А1 включена функция резервирования, и при этом скорости передачи фильтрующих интерфейсов для активного и заблокированного состояний совпадают.

Код	Сообщение	Описание
007.01.1B43	Ошибка установки исключительной блокировки на запись в файл контрольных сумм	При записи изменений в файл контрольных сумм командным интерпретатором произошла системная ошибка при попытке установки соответствующей блокировки.
007.01.1B44	Ошибка установки разделяемой блокировки на чтение из файла контрольных сумм	При чтении записей из файла контрольных сумм командным интерпретатором или сервером проверки контрольных сумм произошла системная ошибка при попытке установки соответствующей блокировки.
007.01.1B45	Ошибка снятия блокировки с файла контрольных сумм	При завершении операций с файлом контрольных сумм командным интерпретатором или сервером проверки контрольных сумм произошла системная ошибка при попытке снятия блокировки.

B.2.2. Предупреждающие сообщения

Коды всех предупреждающих сообщений библиотеки сервисных функций ПО МЭ ССПТ-4А1, их текстовая интерпретация и описание представлены в таблице B.2.

Таблица B.2: Предупреждающие сообщения библиотеки сервисных функций ПО МЭ ССПТ-4А1

Код	Сообщение	Описание
007.01.2000	Пакетный фильтр выключен	Запрос не может быть отправлен пакетному фильтру, т.к. он выключен. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.01.2001	WEB-интерфейс уже включен	Попытка включения WEB-интерфейса, в то время как он уже включен.
007.01.2002	WEB-интерфейс уже выключен	Попытка выключения WEB-интерфейса, в то время как он уже выключен.
007.01.2003	SNMP-интерфейс уже выключен	Попытка выключения SNMP-интерфейса, в то время как он уже выключен.
007.01.2004	SNMP-интерфейс уже включен	Попытка включения SNMP-интерфейса, в то время как он уже включен.
007.01.2005	HTTP-посредник уже выключен	Попытка выключения HTTP-посредника, в то время как он уже выключен.
007.01.2006	HTTP-посредник уже включен	Попытка включения HTTP-посредника, в то время как он уже включен.

B.3. Диагностические сообщения командного интерпретатора МЭ ССПТ-4А1

B.3.1. Сообщения об ошибках

Коды всех сообщений об ошибках командного интерпретатора МЭ ССПТ-4А1, их текстовая интерпретация и описание представлены в таблице B.3.

Таблица В.3: Сообщения об ошибках командного интерпретатора МЭ ССПТ-4А1

Код	*Сообщение*	*Описание*
007.02.1000	Ошибка распределения памяти	Системная ошибка, связанная с невозможностью динамически выделить запрошенный объем памяти. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие изготовитель.
007.02.1001	Ошибка инициализации настроек FNPSH	Ошибка инициализации структуры внутренних настроек командного интерфейса МЭ ССПТ-4А1, связанная с невозможностью динамически распределить память. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1002	Ошибка соединения с сервером авторизации	Недоступен сервер авторизации МЭ ССПТ-4А1. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1003	Ошибка отправки запроса входа администратора	Ошибка при отправке запроса входа администратора МЭ ССПТ-4А1. **Действия**: Повторно выполнить авторизацию администратора. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1004	Нет ответа от сервера авторизации	Истекло время ожидания ответа от сервера авторизации МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер авторизации. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1005	Вход администратора не выполнен	Запрос вход администратора отклонен. Неверные имя пользователя или пароль.
007.02.1006	ID сессии уже используется другим администратором	Идентификатор сессии работы администратора уже используется для другой сессии. **Действия**: Повторно выполнить авторизацию администратора. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1007	Слишком много активных администраторов	Достигнуто максимально допустимое количество активных сеансов работы администратора. **Действия**: Дождаться завершения хотя бы одного сеанса работы администратора и повторно выполнить авторизацию администратора.
007.02.1008	Сервер авторизации работает в однопользовательском режиме	Сервер авторизации МЭ ССПТ-4А1 перешел в однопользовательский режим работы по причине нарушения целостности компонентов операционной системы или программного обеспечения МЭ ССПТ-4А1. **Действия**: Выполнить авторизацию с *системной консоли* учетной записью *admin*. Проверить целостность программного обеспечения. В случае нарушения целостности **немедленно выключить** МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.02.1009	Системная ошибка на стороне сервера авторизации	Во время обработки запроса на стороне сервера авторизации МЭ ССПТ-4А1 произошла системная ошибка – ошибка операционной системы. **Действия**: Повторить запрос к серверу авторизации. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.100A	Ошибка отправки запроса выхода администратора	Ошибка при отправке запроса на завершение сессии работы администратора серверу авторизации МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер авторизации. Повторно выполнить запрос. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.100B	Учетная запись не найдена	Администратор или сетевой пользователь с указанным именем не найден среди учетных записей МЭ ССПТ-4А1 соответствующего типа.
007.02.100C	Ошибка разбора аргументов командной строки	Ошибочные аргументы строки запуска командного интерфейса МЭ ССПТ-4А1. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель
007.02.100D	Ошибка генерации ID сессии	Ошибка генерации уникального идентификатора сессии работы администратора. **Действия**: Повторить авторизацию администратора. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.100E	Неверный тип интерфейса управления	Ошибка определения или неизвестный тип интерфейса управления МЭ ССПТ-4А1. **Действия**: Использовать только средства управления, предоставляемые предприятием-изготовителем.
007.02.100F	Ошибка получения IP-адреса клиента	Невозможно определить IP-адрес управляющего компьютера, с которого выполняется авторизация администратора. **Действия**: Повторно выполнить авторизацию администратора с *системной консоли*, а затем опять с управляющего компьютера. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1010	Ошибка получения имени администратора	Ошибка получения имени администратора для администратора. **Действия**: Использовать только средства управления, предоставляемые предприятием-изготовителем. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1011	Ошибка чтения файла конфигурации	Системная ошибка чтения файла текущей конфигурации МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов операционной системы МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1012	Доступ запрещен в соответствии со списком доступа	Авторизация администратора осуществляется с управляющего компьютера, IP-адрес которого не удовлетворяет ни одной из записей списка доступа к управлению МЭ ССПТ-4А1.
007.02.1013	Неизвестная команда	Администратор ввел команду, которая не распознается командным интерфейсом МЭ ССПТ-4А1 и не входит в состав командного языка.

Код	Сообщение	Описание
007.02.1014	Ошибка получения пароля администратора	Ошибка получения пароля администратора для авторизации. **Действия**: Использовать только средства управления, предоставляемые предприятием-изготовителем. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1015	Некорректный параметр в командной строке	В команде используется параметр, не предусмотренный синтаксисом. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1016	Ошибка соединения с сервером регистрации	Недоступен сервер регистрации МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер регистрации. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1017	Язык не поддерживается программным обеспечением ССПТ-4А1	Попытка локализации сообщений командного интерфейса МЭ ССПТ-4А1 для неизвестного языка. Поддерживаемые языки – *английский*, *русский*. **Действия**: Работа командного интерфейса будет продолжена с выводом сообщений на английском языке.
007.02.1018	Пропущено имя пользователя FTP-сервера	В соответствии с синтаксисом команды необходимо указание имени пользователя FTP-сервера. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1019	Достигнуто неожидаемое окончание ввода	При чтении очередной лексемы командной строки обнаружено отсутствие данных. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.101A	Ошибка компиляции регулярного выражения	Системная ошибка при компиляции регулярных выражений в командном интерфейсе МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.101B	Неверный формат имени учетной записи	Имя администратора или сетевого пользователя МЭ ССПТ-4А1 не соответствует принятому формату.
007.02.101C	Учетная запись с данным именем уже существует	Учетная запись указанного администратора или сетевого пользователя МЭ ССПТ-4А1 уже существует в соответствующем файле паролей.
007.02.101D	Недопустимое значение параметра	Некорректное или недопустимое значение параметра команды. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.

Код	Сообщение	Описание
007.02.101E	Ошибка чтения файла паролей	Системная ошибка чтения: • файла паролей администраторов МЭ ССПТ-4А1; • файла паролей сетевых пользователей МЭ ССПТ-4А1; • файла паролей SNMP-интерфейса МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.101F	Неверный формат файла паролей	Нарушена внутренняя структура файла паролей администраторов или сетевых пользователей МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1021	Недопустимое значение привилегий	Привилегии администратора МЭ ССПТ-4А1 не соответствует принятому формату.
007.02.1022	Неверный аргумент	Некоторые аргументы выполнения функций командного интерфейса имеют недопустимые значения. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1023	Недостаточно привилегий для операции	Администратора не обладает привилегиями, требуемыми для выполнения команды.
007.02.1024	Ошибка регистрации события	Ошибка при отправке запроса серверу регистрации МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер регистрации. Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1025	Пропущен пароль	В соответствии с синтаксисом команды необходимо указание пароля, требуемого в данном контексте. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1026	Неверный формат пароля	Пароль не соответствует принятому формату для данного контекста. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1027	Ошибка записи файла паролей	Системная ошибка записи: • файла паролей администраторов МЭ ССПТ-4А1; • файла паролей сетевых пользователей МЭ ССПТ-4А1; • файла паролей SNMP-интерфейса МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.1028	Ошибка открытия временного файла	Системная ошибка открытия файла для хранения временных данных. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1029	Ожидается параметр	Отсутствуют необходимые параметры команды. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1030	Не найдено записей в файле паролей	Файл паролей администраторов либо файл паролей сетевых пользователей МЭ ССПТ-4А1 не содержит учетных записей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1031	Пропущен старый пароль	В соответствии с синтаксисом команды необходимо указание старого пароля для данной учетной записи. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1032	Недопустимый пароль учетной записи	Введен неверный пароль для данной учетной записи.
007.02.1033	Ошибка отправки запроса серверу авторизации	Ошибка при отправке запроса серверу авторизации МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер авторизации. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1034	Пропущено имя конфигурации	В соответствии с синтаксисом команды необходимо указание имени дополнительной конфигурации. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1035	Неверный формат имени дополнительной конфигурации	Имя дополнительной конфигурации не соответствует принятому формату.
007.02.1036	Ошибка чтения списка дополнительных конфигураций	Системная ошибка при получении списка имен файлов дополнительных конфигураций. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1037	Нет свободной позиции для дополнительной конфигурации	Достигнуто максимально допустимое количество сохраненных дополнительных конфигураций.
007.02.1039	Дополнительная конфигурация уже существует	Файл дополнительной конфигурации с указанным именем уже существует.
007.02.103A	Системная ошибка	Произошла ошибка операционной системы МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.103B	Ошибка открытия дополнительной конфигурации	Системная ошибка открытия файла дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.103E	Файл пуст	Файл системных сообщений не содержит записей (при просмотре журнала системных сообщений). Файл паролей SNMP-интерфейса не содержит записей (при попытке смены пароля пользователя SNMP-интерфейса). **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.103F	Ошибка чтения дополнительной конфигурации	Системная ошибка чтения файла дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1040	Недостаточно прав доступа к дополнительной конфигурации	Администратор не имеет прав записи в файл дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1041	Дополнительная конфигурация не найдена	Не существует дополнительной конфигурации с указанным именем
007.02.1042	Ошибка останова устройства	Системная ошибка при выполнении останова УОС МЭ ССПТ-4А1 и выключения МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов УОС МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1043	Ошибка перезагрузки устройства	Системная ошибка при выполнении перезагрузки операционной системы УОС МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов УОС МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1044	Неверный формат даты	Дата не соответствуют принятому формату.
007.02.1045	Неверный формат времени	Время не соответствуют принятому формату.
007.02.1047	Недопустимое значение даты/времени	Указано недопустимое значение даты/времени. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1048	Ошибка установки системного времени	Ошибка изменения системного времени. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.104D	Управляющий интерфейс выключен	Команда не может быть выполнена при выключенном управляющем Ethernet-интерфейсе МЭ ССПТ-4А1.
007.02.104E	NTP-сервер не определен	Перед выполнением команды необходимо установить IP-адрес NTP-сервера.
007.02.104F	Неверный формат IP-адреса	IP-адрес не соответствует принятому формату.

Код	Сообщение	Описание
007.02.1050	Недопустимый IP-адрес	Указано недопустимое значение IP-адреса. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1052	Ошибка записи файла конфигурации ССПТ-4А1	Системная ошибка записи файла текущей конфигурации МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1053	Недопустимое значение тайм-аута	Некорректное значение тайм-аута в контексте выполняемой команды. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1054	NTP-сервер не найден	Ошибка выполнения команды немедленной синхронизации даты и времени по NTP: NTP-сервер по IP-адресу, указанному в команде, не обнаружен.
007.02.1055	Тайм-аут опроса NTP-сервера	Ошибка выполнения команды немедленной синхронизации даты и времени по NTP: тайм-аут ожидания ответа от NTP-сервера.
007.02.1056	Список доступа заполнен	Список доступа к управлению МЭ ССПТ-4А1 содержит максимально допустимое количество записей.
007.02.1058	Недопустимая IP-маска	Некорректное значение маски IP-подсети.
007.02.1059	Неверный формат IP-адреса/маски	В данном контексте требуется указание и IP-адреса и маски IP-подсети.
007.02.105A	Недопустимый интервал IP-адресов	Некорректное значение диапазона IP-адресов.
007.02.105B	Недопустимый номер записи списка доступа	Номер элемента списка доступа к управлению МЭ ССПТ-4А1 не соответствует принятому формату.
007.02.105D	Неверный номер фильтрующего интерфейса	Недопустимый номер фильтрующего интерфейса МЭ ССПТ-4А1.
007.02.105E	Фильтрующий интерфейс с заданным именем не найден	Указанное в команде символическое имя не присвоено ни одному из фильтрующих интерфейсов МЭ ССПТ-4А1.
007.02.105F	Неверный формат номера или имени фильтрующего интерфейса	Номер или символическое имя фильтрующего интерфейса МЭ ССПТ-4А1 не соответствует принятому формату.
007.02.1060	Ошибка отправки запроса пакетному фильтру	Ошибка при отправке запроса пакетному фильтру МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли пакетный фильтр. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1061	Получен ошибочный ответ от пакетного фильтра	Ошибка выполнения запроса пакетным фильтром МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.1062	Пакетному фильтру отправлена неизвестная команда	Неизвестный код команды в структуре запроса, отправленном пакетному фильтру МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1064	Слишком мало фильтрующих интерфейсов для зеркалирования	Для использования функции зеркалирования трафика МЭ ССПТ-4А1 должен быть укомплектован тремя и более фильтрующими интерфейсами.
007.02.1065	Зеркалируемый и зеркалирующий интерфейсы должны быть различными	При использовании функции зеркалирования трафика в качестве зеркалируемого и слушающего интерфейсов должны использоваться различные фильтрующие интерфейсы МЭ ССПТ-4А1.
007.02.1066	Интерфейс не должен использоваться как зеркалирующий интерфейс и интерфейс NAT	Один и тот же фильтрующий интерфейс не должен использоваться как зеркалирующий интерфейс и как фильтрующий интерфейс в составе интерфейса NAT.
007.02.1068	Имя фильтрующего интерфейса уже используется	Указанное символическое имя уже присвоено другому фильтрующему интерфейсу МЭ ССПТ-4А1.
007.02.1069	Ошибка удаления дополнительной конфигурации	Администратор не имеет прав доступа для удаления файла дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.106A	Ошибка сохранения дополнительной конфигурации	Системная ошибка записи файла дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.106D	Недопустимые параметры NAT	Перед выполнением команды необходимо настроить параметры функции трансляции сетевых адресов (NAT).
007.02.106E	Неверный формат MAC-адреса	Значение MAC-адреса не соответствует принятому формату.
007.02.106F	Недопустимый MAC-адрес	Некорректное значение MAC-адреса.
007.02.1070	Неверный формат критерия отбора	Критерий отбора в команде не соответствует принятому формату.
007.02.1072	Не найдено подходящей записи в ARP-таблице	В ARP-таблице NAT не найдено записи данного типа (статическая или динамическая) с указанным MAC, IP-адресом или фильтрующим интерфейсом.
007.02.1073	IP-адрес уже существует в ARP-таблице	В ARP таблице NAT уже имеется запись с указанным IP-адресом.
007.02.1074	ARP-таблица заполнена	Достигнуто максимально допустимое количество записей в ARP-таблице NAT.
007.02.1075	Недопустимые значения порта	Недопустимое значение TCP-порта или UDP-порта для данного контекста. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1079	Неверное значение даты/времени	Указано недопустимое значение даты/времени. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.

Код	Сообщение	Описание
007.02.107A	Неверный формат даты/времени	Дата/время не соответствуют принятому формату.
007.02.107B	Недопустимый интервал даты/времени	Указано недопустимое значение интервала даты/времени. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.107C	Ошибка отправки запроса серверу регистрации	Ошибка при отправке запроса серверу регистрации МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер регистрации. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.107D	Недостаточно привилегий для запроса регистрации	У администратора недостаточно привилегий для выполнения запроса к серверу регистрации.
007.02.107E	Системная ошибка на стороне сервера регистрации	Во время обработки запроса на стороне сервера регистрации МЭ ССПТ-4А1 произошла системная ошибка – ошибка УОС МЭ ССПТ-4А1. **Действия**: Повторить запрос к серверу авторизации. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.107F	Серверу регистрации отправлена неизвестная команда	Неизвестный код команды в структуре запроса, отправленном серверу регистрации МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1080	Ошибка чтения файла системных сообщений	Системная ошибка чтения файла системных сообщений. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1081	Ошибка просмотра регистрационных записей	Системная ошибка во время обработки полученных регистрационных записей для просмотра. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1082	Некорректные значения параметров выгрузки на FTP-сервер	Перед выполнением команды необходимо настроить параметры выгрузки файлов регистрации на удаленный FTP сервер.
007.02.1083	Пропущен IP-адрес	В соответствии с синтаксисом команды необходимо указание IP-адреса. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1084	Неверный формат пути на FTP-сервере	Путь на FTP-сервере не соответствует принятому формату.
007.02.1085	Неверный формат имени пользователя FTP-сервера	Имя пользователя FTP-сервера не соответствует принятому формату.
007.02.108A	Общее правило уже существует	Общее правило фильтрации с указанным номером уже существует в текущей или дополнительной политике доступа.
007.02.108B	Общее правило не найдено	В текущей или дополнительной политике доступа не существует общего правила фильтрации с указанным номером.

Код	Сообщение	Описание
007.02.108D	АР-правило уже существует	АР-правило фильтрации с указанным номером уже существует в текущей или дополнительной политике доступа.
007.02.108E	АР-правило не найдено	В текущей или дополнительной политике доступа не существует АР-правила фильтрации с указанным номером.
007.02.108F	Пропущено определение правила фильтрации	В соответствии с синтаксисом команды необходимо указание определения правила фильтрации. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1093	Таблица общих правил переполнена	Достигнуто максимально допустимое количество общих правил фильтрации в текущей или дополнительной политике доступа.
007.02.1095	Таблица АР-правил переполнена	Достигнуто максимально допустимое количество АР-правил фильтрации в текущей или дополнительной политике доступа.
007.02.109A	Ошибка открытия файла правил дополнительной политики	Системная ошибка открытия файла правил дополнительной политики доступа. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.109D	Синтаксическая ошибка в определении правила	В определении правила фильтрации выявлена синтаксическая ошибка: • при добавлении или изменении правила фильтрации; • при загрузке дополнительной политики доступа с управляющего ПК; • во всех остальных случаях. **Действия**: • В случае ошибки при добавлении или изменении правила воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса. • В случае ошибки при загрузке дополнительной политики доступа с управляющего ПК исправить определение соответствующего правила в политике доступа на управляющем ПК и повторить попытку загрузки политики; • Во всех остальных случаях: проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.109E	Глобальное правило отсутствует в политике	В политике доступа отсутствует глобальное общее и/или глобальное АР-правило. **Действия**: • В случае ошибки при загрузке дополнительной политики доступа с управляющего ПК добавить в политику доступа на управляющем ПК отсутствующие глобальные правила и повторить попытку загрузки политики; • Во всех остальных случаях: проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10A8	Неверный формат номера правила фильтрации	Номер правила фильтрации не соответствует принятому формату.

Код	Сообщение	Описание
007.02.10A9	Недопустимое имя фильтрующего интерфейса	Указанное символическое имя не присвоено ни одному из фильтрующих интерфейсов МЭ ССПТ-4А1. В случае команды переименования фильтрующего интерфейса: указанное символическое имя уже присвоено одному из фильтрующих интерфейсов МЭ ССПТ-4А1.
007.02.10AB	Недопустимый тип правила фильтрации	В команде указан недопустимый тип правила фильтрации в критерии отбора. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.10AC	Недопустимый номер правила фильтрации	Указано недопустимое значение номера правила фильтрации. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.10AE	Глобальное правило не может быть удалено	Удаление глобальных правил фильтрации запрещено.
007.02.10AF	AP-правило используется в общих правилах фильтрации	Не допускается удаление и перемещение AP-правила фильтрации, на которое имеется ссылка из общих правил фильтрации политики доступа.
007.02.10B1	Ошибка запуска пакетного фильтра	Ошибка при запуске пакетного фильтра МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10B3	Нельзя копировать/переносить глобальное правило	Копирование или перенос глобальных правил фильтрации не допускается.
007.02.10B5	Ошибка инициализации соединения с пакетным фильтром	Ошибка инициализации соединения с пакетным фильтром при старте процесса командного интерпретатора МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10B6	Неверный формат номера	Некорректный ввод администратора при выборе нового часового пояса.
007.02.10B7	Не найдено подходящей сессии	В таблице сессий не найдено сессии, удовлетворяющей заданным критериям отбора.
007.02.10B8	Ошибка чтения файла контрольных сумм	Системная ошибка чтения файла контрольных сумм файлов УОС и программного обеспечения МЭ ССПТ-4А1. **Действия**: Немедленно выключить МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.02.10B9	Нарушен размер файла контрольных сумм	Файл контрольных сумм имеет неправильный размер. **Действия**: Немедленно выключить МЭ ССПТ-4А1 и обратиться на предприятие-изготовитель.
007.02.10BC	Ошибка инициализации контекста SSL	Ошибка инициализации контекста SSL. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.10BE	Не удалось изменить пароль пользователя SNMP-интерфейса	Ошибка смены пароля пользователя SNMP-интерфейса. **Действия**: Проверить правильность указания в команде текущего пароля. В случае повторения ошибки, сбросить пароль пользователя SNMP-интерфейса в начальное значение по команде “system default” или с помощью средства восстановления. обратиться на предприятие-изготовитель.
007.02.10BF	Ошибка изменения IP-адреса управляющего интерфейса	Системная ошибка УОС МЭ ССПТ-4А1 при попытке изменения IP-адреса управляющего интерфейса. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10C1	Недопустимое пороговое значение	Некорректное значение порога интенсивности трафика для функции обнаружения flood-атак.
007.02.10C2	Ошибка просмотра дополнительной конфигурации	Системная ошибка при обращении к файлу для просмотра дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10C5	Ошибка при использовании библиотеки ncurses	Ошибка при выполнении функции библиотеки управления терминалом в полноэкранном режиме просмотра данных командного интерфейса МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10C6	Сообщение слишком большое для вывода в данное окно	Размер данных для вывода превышает размеры окна. **Действия**: В случае использования неполноэкранного терминала увеличить его размер до максимально возможного. В случае повторения ошибки, после выполнения предыдущего шага, обратиться на предприятие-изготовитель.
007.02.10C7	Ошибка чтения временного файла	Системная ошибка чтения файла, содержащего временные данные. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10C9	Для установки режима передачи скорость передачи должна отличаться от "autoselect"	Режим передачи Ethernet-интерфейсов МЭ ССПТ-4А1 (управляющего или фильтрующих) может быть установлен только в том случае, если скорость передачи установлена в значение отличное от “autoselect”.
007.02.10CA	Ошибка получения ответа от сервера регистрации	Истекло время ожидания ответа от сервера регистрации МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер регистрации. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10CB	Пароли не совпадают	Повторный ввод пароля отличается от первоначального.

Код	Сообщение	Описание
007.02.10CC	Выгрузка по SYSLOG уже выключена	Повторное включение выгрузки системных сообщений на удаленный SYSLOG-сервер.
007.02.10CD	Выгрузка по SYSLOG уже включена	Повторное выключение выгрузки системных сообщений на удаленный SYSLOG-сервер.
007.02.10CE	Недопустимое значение тайм-аута	Некорректное значение тайм-аута в контексте введенной команды.
007.02.10D0	Данная запись уже существует в файле ключей аутентификации	Пара ключей аутентификации сетевых пользователей для указанного IP-адреса уже существует.
007.02.10D1	Нарушена структура файла ключей аутентификации	Нарушена внутренняя структура файла ключей аутентификации сетевых пользователей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1 и перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10D2	Ошибка чтения файла ключей аутентификации	Системная ошибка чтения файла ключей аутентификации сетевых пользователей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10D3	Ошибка генерации ключей	Ошибка генерации пары ключей аутентификации сетевых пользователей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Повторить выполнение команды. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10D4	Ошибка записи в файл ключей аутентификации	Системная ошибка записи файла ключей аутентификации сетевых пользователей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10D5	Запись в файле ключей аутентификации не найдена	Пара ключей аутентификации, соответствующая указанному IP-адресу, отсутствует.
007.02.10D6	Ошибка записи временного файла	Системная ошибка записи файла с временными данными. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10D9	Неверный формат комментария	Комментарий не соответствует принятому формату.
007.02.10DA	Некорректные параметры RADIUS-сервера	Некорректные значения параметров RADIUS-авторизации администраторов и сетевых пользователей МЭ ССПТ-4А1. **Действия**: Перед включением RADIUS-авторизации администраторов и сетевых пользователей МЭ ССПТ-4А1 необходимо задать IP-адрес и секретный ключ основного RADIUS-сервера.
007.02.10DB	Некорректное значение тайм-аута RADIUS	Значение тайм-аута ожидания ответа от RADIUS-сервера не соответствует принятому формату.
007.02.10DC	Некорректное значение числа обращений к RADIUS-серверу	Значение числа обращений к RADIUS-серверу не соответствует принятому формату.

Код	Сообщение	Описание
007.02.10DD	Неверная длина	Длина секретного ключа RADIUS-сервера превышает максимально допустимую.
007.02.10DE	Недопустимое значение идентификатора VLAN	Значение идентификатора VLAN не соответствует принятому формату.
007.02.10DF	Недопустимое значение времени жизни	Некорректное значение времени жизни для TMP-правила.
007.02.10EB	TMP-правило не найдено	В текущей политике доступа не существует TMP-правила фильтрации с указанным номером.
007.02.10EC	TMP-правило уже существует	TMP-правило фильтрации с указанным номером уже существует в текущей политике доступа.
007.02.10EF	Системная ошибка на стороне пакетного фильтра	Во время обработки запроса на стороне пакетного фильтра МЭ ССПТ-4А1 произошла системная ошибка – ошибка УОС МЭ ССПТ-4А1. **Действия**: Повторить запрос к пакетному фильтру. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10F5	Ошибка чтения файла сертификата УЦ (SSL)	Системная ошибка чтения файла сертификата Удостоверяющего Центра. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10F6	Ошибка чтения файла сертификата ССПТ-4А1 (SSL)	Системная ошибка чтения файла сертификата МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10F7	Ошибка чтения файла открытого ключа Diffie-Hellman ССПТ-4А1	Системная ошибка чтения файла открытого ключа Diffie-Hellman МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10F8	Ошибка чтения файла параметров Diffie-Hellman	Системная ошибка чтения файла параметров Diffie-Hellman МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10F9	Ошибка чтения системного файла паролей	Системная ошибка чтения системного файла паролей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10FA	Ошибка записи системного файла паролей	Системная ошибка записи системного файла паролей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.10FB	Ошибка блокировки системного файла паролей	Системная ошибка при операции блокировки системного файла паролей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10FC	Ошибка создания системной базы данных паролей	Системная ошибка обновления файлов учетных записей системных пользователей. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.10FD	Стартовый сценарий WEB-интерфейса завершился неудачей	Ошибка при включении WEB-интерфейса администратора МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки.
007.02.10FE	Стартовый сценарий SNMP-интерфейса завершился неудачей	Ошибка при включении SNMP-интерфейса администратора МЭ ССПТ-4А1. Действия: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно скопировав содержимое файла системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки.
007.02.10FF	Ошибка изменения часового пояса	Ошибка обращения или нарушена структура файла списка буквенных кодов ISO3166 для стран мира. Действия: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1100	Не найдено стран для континента/региона	В файлах описания часовых поясов обнаружен континент/регион, не содержащий стран. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1101	Ошибка получения системной информации	Ошибка при получении информации о состоянии программного обеспечения и УОС МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1102	Недопустимое имя системного пользователя	Системная авторизация с именем пользователя, отличным от *fnpsh*, не разрешается. **Действия**: Выполнить системную авторизацию для пользователя *fnpsh.*
007.02.1105	Недопустимые настройки резервирования	Некорректные значения параметров настройки сервера резервирования МЭ ССПТ-4А1.

Код	Сообщение	Описание
007.02.1106	Некорректный ответ от сервера резервирования	Нарушена структура ответа, полученного от сервера резервирования МЭ ССПТ-4А1, или неизвестный код ответа. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1107	Ошибка соединения с сервером резервирования	Недоступен сервер резервирования МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер резервирования. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1108	Ошибка отправки запроса серверу резервирования	Ошибка при отправке запроса серверу резервирования МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер резервирования. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1109	Ошибка получения ответа от сервера резервирования	Истекло время ожидания ответа от сервера резервирования МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер резервирования. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.110A	Системная ошибка на стороне сервера резервирования	Системная ошибка при обработке запроса сервером резервирования МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.110B	Недопустимый тип объекта справочника	Указанный в команде тип объекта справочника не существует.
007.02.110C	Неверный формат имени объекта справочника	Имя объекта справочника не соответствует принятому формату.
007.02.110E	Слишком много элементов в списке	Число элементов в списке значений параметра команды превышает максимально допустимое.
007.02.111A	Объект отсутствует в справочнике	Объект, с указанным именем, отсутствует в справочнике.
007.02.111E	Ошибка открытия файла справочника дополнительной политики	Системная ошибка открытия файла справочника дополнительной политики доступа. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1121	Ошибка обновления политики доступа в пакетном фильтре	Текущая политика доступа не была применена пакетным фильтром из-за ошибки. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1122	Комментарий уже существует	Строка комментария к группе правил фильтрации или объектов справочника политики доступа уже существует в данной позиции файла. **Действия**: Воспользоваться командой изменения комментария к группе правил фильтрации или объектов справочника.

Код	Сообщение	Описание
007.02.1123	Комментарий не найден	Строка комментария к группе правил фильтрации или объектов справочника отсутствует в данной позиции файла.
007.02.1124	Резервная копия политики отсутствует	Возврат к предыдущему состоянию текущей политики доступа не возможен, т. к. отсутствуют резервные копии политики доступа. **Действия**: Повторить команду после изменения в правилах фильтрации или объектах справочника (добавление, изменение, удаление и т. д. правила или объекта) текущей политики доступа. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1126	Неверный формат имени дополнительной политики	Имя дополнительной политики доступа не соответствует принятому формату.
007.02.1127	Ошибка перезаписи файлов политики доступа	Файлы политики доступа не были перезаписаны из-за системной ошибки УОС МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1129	Недостаточно прав доступа к дополнительной политике	Администратор не имеет прав записи в файл дополнительной политики доступа. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.112A	Дополнительная политика не найдена	Не существует дополнительной политики доступа с указанным именем.
007.02.112B	Ошибка удаления дополнительной политики	Администратор не имеет прав доступа для удаления файла дополнительной политики доступа. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.112C	Дополнительный политика уже существует	Дополнительная политика доступа с указанным именем уже существует и не может быть перезаписана при использовании WEB-интерфейса. **Действия**: Для того чтобы повторно сохранить дополнительную политику доступа через WEB-интерфейс, необходимо сначала удалить ее.
007.02.112D	Нет свободной позиции для дополнительной политики	Достигнуто максимально допустимое количество сохраненных дополнительных политик доступа.
007.02.112E	Ошибка чтения списка дополнительных политик	Системная ошибка при получении списка имен файлов дополнительных политик доступа. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.112F	Некорректное определение объекта справочника	В определении объекта справочника выявлена синтаксическая или семантическая ошибка: • при добавлении или изменении правила фильтрации; • при загрузке дополнительной политики доступа с управляющего ПК; • во всех остальных случаях. **Действия**: • В случае ошибки при добавлении или изменении объекта справочника воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса. • В случае ошибки при загрузке дополнительной политики доступа с управляющего ПК исправить определение соответствующего объекта справочника в политике доступа на управляющем ПК и повторить попытку загрузки политики; • Во всех остальных случаях: проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1132	Объект справочника используется в политике	Попытка удаления объекта справочника, используемого в правилах фильтрации политики доступа. Для удаления объекта необходимо, чтобы он не использовался в правилах фильтрации политики доступа.
007.02.1133	Комментарий не допустим после последнего правила некоторого типа	Не допускается добавление строки комментария к группе правил фильтрации в позицию файла, следующую за последним правилом некоторого типа.
007.02.1134	Комментарий не допустим после последнего объекта некоторого типа	Не допускается добавление строки комментария к группе объектов справочника в позицию файла, следующую за последним объектом некоторого типа.
007.02.1136	Совместное использование параметров недопустимо	В команде указаны параметры, совместное использование которых не допустимо. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса.
007.02.1137	Ошибка получения аппаратных параметров	Ошибка при получении информации об аппаратной конфигурации данного экземпляра МЭ ССПТ-4А1. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.1138	Некорректная конфигурация	В дополнительной конфигурации МЭ ССПТ-4А1 выявлены синтаксические или семантические ошибки: • при загрузке дополнительной конфигурации с управляющего ПК; • во всех остальных случаях. **Действия**: • В случае ошибки при загрузке дополнительной конфигурации с управляющего ПК исправить ошибки в файле дополнительной конфигурации и повторить попытку загрузки конфигурации; • Во всех остальных случаях: проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1139	Неподдерживаемая скорость передачи	В команде указана скорость передачи, которая не поддерживается данным сетевым интерфейсом МЭ ССПТ-4А1. **Действия**: Использовать при установке скорости передачи только те значения, которые выводятся по команде: • `inteface control media list` для управляющего интерфейса; • `inteface filter media list` для фильтрующих интерфейсов.
007.02.113A	Неподдерживаемый режим передачи для текущей скорости	В команде указан режим передачи, который не поддерживается текущим значением скорости передачи сетевого интерфейса МЭ ССПТ-4А1.
007.02.113B	Неподдерживаемое значение MTU	В команде указано значение MTU, которое не поддерживается данным сетевым интерфейсом МЭ ССПТ-4А1. **Действия**: Использовать при установке MTU только значения из допустимого диапазона для данного интерфейса, который можно узнать по команде: • `inteface control show` для управляющего интерфейса; • `inteface filter show` для фильтрующих интерфейсов.
007.02.113C	Семантически некорректное определение правила	В определении правила фильтрации выявлены семантические ошибки: • при добавлении или изменении правила фильтрации; • при загрузке дополнительной политики доступа с управляющего ПК; • во всех остальных случаях. **Действия**: • В случае ошибки при добавлении или изменении правила воспользоваться настоящим руководством для уточнения семантики правил и возможных конфликтов параметров правил. • В случае ошибки при загрузке дополнительной политики доступа с управляющего ПК исправить определение соответствующего правила в политике доступа на управляющем ПК и повторить попытку загрузки политики; • Во всех остальных случаях: проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.113D	Неверный формат имени устройства	Имя устройства не соответствует принятому формату.
007.02.113E	Нарушен формат файла правил дополнительной политики	Нарушен формат файла правил дополнительной политики доступа. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1140	Ошибка выключения управляющего интерфейса	Системная ошибка УОС МЭ ССПТ-4А1 при попытке выключения управляющего интерфейса. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1141	Ошибка включения управляющего интерфейса	Системная ошибка УОС МЭ ССПТ-4А1 при попытке включения управляющего интерфейса. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1143	Некорректные значения параметров выгрузки по SYSLOG	Перед включением выгрузки записей регистрации на SYSLOG-сервер необходимо задать IP-адрес SYSLOG-сервера.
007.02.1144	IP-адреса клиента и сервера должны быть одной версии протокола IP	При использовании критериев отбора IP-адреса клиента и IP-адреса сервера для удаления сессий из таблицы сессий необходимо чтобы оба адреса были IPv4-адресами, либо IPv6-адресами.
007.02.1145	Ошибка обновления записей ACL в ядре	Системная ошибка УОС МЭ ССПТ-4А1 при попытке обновить записи ACL. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1146	Ошибка установки имени устройства в качестве имени узла сети	Системная ошибка УОС МЭ ССПТ-4А1 при попытке установки имени устройства из конфигурации в качестве имени узла сети (доменное имя). **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1147	Ошибка установки файла часового пояса	Системная ошибка установки файла часового пояса. **Действия**: Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1148	Ошибка установки скорости передачи	Системная ошибка УОС МЭ ССПТ-4А1 при попытке установки скорости передачи сетевого интерфейса. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1149	Ошибка установки MTU	Системная ошибка УОС МЭ ССПТ-4А1 при попытке установки MTU сетевого интерфейса. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.114A	Пустые строки недопустимы в файле дополнительной политики	В файле дополнительной политики, загружаемой с управляющего ПК на МЭ ССПТ-4А1, выявлены пустые строки. **Действия:** Удалить пустые строки в файле дополнительной политики на управляющем ПК, и повторить загрузки политки.
007.02.114B	Имя контейнера NAT уже используется	Контейнер NAT с данным именем уже существует в текущей конфигурации.
007.02.114C	Контейнер NAT не найден	Контейнер NAT с данным именем отсутствует в текущей конфигурации.
007.02.114D	Имя интерфейса NAT уже используется	Интерфейс NAT с данным именем уже существует в контейнере NAT.
007.02.114E	Интерфейс NAT не найден	Интерфейс NAT с данным именем отсутствует в контейнере NAT.
007.02.114F	Фильтрующий интерфейс уже используется другим интерфейсом NAT	Фильтрующий интерфейс, добавляемый в интерфейс NAT, уже используется другим интерфейсом NAT. **Действия**: Воспользоваться настоящим руководством для уточнения требований к использованию фильтрующих интерфейсов в различных интерфейсах NAT.
007.02.1150	IP-адрес уже используется интерфейсом NAT	IP-адрес, назначаемый на интерфейс NAT, уже назначен на другой интерфейс NAT. **Действия**: Воспользоваться настоящим руководством для уточнения требований к использованию IP-адресов в различных интерфейсах NAT.
007.02.1151	Правило трансляции NAT уже существует	Правило трансляции NAT с данным номером уже существует в контейнере NAT.
007.02.1152	Таблица правил трансляции NAT переполнена	Достигнуто максимальное число правила трансляции NAT в контейнере NAT.
007.02.1153	Правило трансляции NAT не найдено	Правило трансляции NAT с данным номером отсутствует в контейнере NAT.
007.02.1154	Внешний IP-адрес должен быть адресом внешнего интерфейса NAT	В правилах трансляции и переадресации NAT в качестве внешних IP-адресов могут использоваться только IP-адреса назначенные на внешние интерфейсы NAT контейнера NAT.
007.02.1155	Правило переадресации NAT не найдено	Правило переадресации NAT с данным номером отсутствует в контейнере NAT.
007.02.1156	Конфликт внешних и внутренних портов в правиле переадресации NAT	В правиле переадресации NAT число внешних и внутренних портов должно совпадать.
007.02.1158	IP-адрес шлюза по умолчанию должен принадлежать одной из подсетей внешнего интерфейса NAT	IP-адрес шлюза по умолчанию в таблице маршрутов NAT должен принадлежать одной из подсетей внешнего интерфейса NAT данного контейнера NAT.
007.02.1159	Маршрут NAT не найден	Маршрут NAT с данным номером отсутствует в данном контейнере NAT.
007.02.115A	Интерфейс NAT используется в контейнере NAT	Интерфейс NAT не может быть удален, если он используется в контейнере NAT.
007.02.115B	IP-адрес назначения маршрута NAT уже используется интерфейсом NAT	В качестве IP-адрес назначения маршрута NAT нельзя использовать IP-адрес, назначенный на интерфейс NAT.

Код	Сообщение	Описание
007.02.115C	IP-адрес назначения маршрута NAT уже используется в другом маршруте NAT	В контейнере NAT не должно быть двух и более маршрутов с одним и тем же IP-адресом назначения.
007.02.115D	Не осталось свободных фильтрующих интерфейсов	Контейнер NAT не может быть добавлен, если все фильтрующие интерфейсы МЭ ССПТ-4А1 уже используются в интерфейсах NAT других контейнеров NAT.
007.02.115E	IP-адрес уже используется в качестве внутреннего адреса в правиле переадресации NAT	Интерфейсу NAT нельзя назначить IP-адрес, который уже используется в качестве внутреннего IP-адреса в правиле переадресации контейнера NAT.
007.02.115F	IP-адрес уже используется в качестве IP-адреса внутреннего интерфейса NAT	В правиле переадресации NAT нельзя в качестве внутреннего IP-адреса использовать IP-адрес, уже назначенный на внутренний интерфейс NAT контейнера.
007.02.1160	Несоответствие количества элементов в списках	В команде изменения MAC-адресов на фильтрующих интерфейсах в контексте NAT, число интерфейсов должно соответствовать числу MAC-адресов.
007.02.1161	Режим резервирования недоступен в случае разных поддерживаемых скоростей передачи на интерфейсах	Данный режим резервирования не может быть установлен на данном экземпляре МЭ ССПТ-4А1, т. к. фильтрующие интерфейсы имеют разные списки поддерживаемых скоростей передачи.
007.02.1162	Число объектов данного типа превышает максимальное	Число объектов справочника данного типа превышает максимально допустимое.
007.02.1163	Недопустимый режим командного интерпретатора для данной команды	Данная команда не может быть выполнена в данном режиме командного интерпретатора (режимы: интерактивный режим или режим сервера).
007.02.1164	Недопустимый тип интерфейса управления для данной команды	Данная команда не может быть выполнена через интерфейс управления данного типа (типы: командный интерфейс, WEB-инетрфейс, SNMP-инетрфейс и т.д.).
007.02.1165	Недопустимое действие	Действие — недопустимо для данного типа правила фильтрации.
007.02.1166	На данное правило есть ссылки из других правил с действием "goto"	Данное правило не может быть удалено или перемещено, т. к. на него есть ссылки из других правил с действием "goto".
007.02.1167	MAC-адреса фильтрующих интерфейсов в контексте NAT повторяются	MAC-адреса фильтрующих интерфейсов в контексте NAT не должны повторяться.
007.02.1168	Таблица правил переадресации NAT переполнена	Правило переадресации не может быть добавлено, т. к. таблица правил переадресации NAT переполнена.
007.02.1169	Таблица маршрутов NAT переполнена	Маршрут NAT не может быть добавлен, т. к. таблица правил переадресации NAT переполнена.
007.02.116A	IP-адрес шлюза должен принадлежать одной из подсетей интерфейса NAT	В маршруте NAT IP-адрес шлюза должен принадлежать одной из подсетей одного из имеющихся интерфейсов NAT.
007.02.116B	Ошибка инициализации генератора случайных чисел	Системная ошибка УОС МЭ при инициализации генератора случайных чисел. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.

Код	Сообщение	Описание
007.02.116C	Размер окна терминала должен быть не менее 80x16 символов	Для вывода данных, запрашиваемых по команде, размер окна терминала должен быть не менее 80x16 символов.
007.02.116D	IP-адреса интерфейса NAT используются в контейнере NAT	IP-адреса, назначенные на интерфейс NAT, не могут быть исключены, т. к. используются в контейнере NAT (в правилах трансляции, переадресации или маршрутах NAT).
007.02.116E	Команда отменена, так как привела бы к некорректной конфигурации	Выполнение данной команды привело бы к некорректному состоянию текущей конфигурации МЭ ССПТ-4А1, поэтому команда не была выполнена и текущая конфигурация не претерпела изменений. **Действия**: Обратиться на предприятие-изготовитель, по возможности предоставив информацию о команде.
007.02.116F	IP-адрес интерфейса NAT уже используется как IP-адрес назначения в маршруте NAT	IP-адрес, используемый в качестве IP-адерса назначения в маршруте NAT не может быть назначен на интерфейс NAT.
007.02.1170	Общее правило с действием "goto" может быть перемещено/скопировано в ограниченных пределах	Общее правило с действием "goto" может быть перемещено/скопировано только в позицию, находящуюся до правила, к которому должен осуществляться переход.
007.02.1171	Недопустимая скорость передачи для резервирования	Скорость передачи для интерфейсов в активном или заблокированном состоянии, указанная в команде установки параметров резервирования, не поддерживается фильтрующими интерфейсами данного экземпляра МЭ ССПТ-4А1.
007.02.1172	PRI-правило не найдено	В текущей или дополнительной политике доступа не существует правила приоритизации с указанным номером.
007.02.1173	PRI-правило уже существует	Правило приоритизации с указанным номером уже существует в текущей или дополнительной политике доступа.
007.02.1174	Таблица PRI-правил переполнена	Число правил приоритизации в политике доступа больше максимально допустимого значения.
007.02.1175	Ошибка записи файла DNS-серверов	Системная ошибка УОС МЭ при записи файла. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.1176	Маршрут не найден	Не найден маршрут с указанным номером.
007.02.1177	IP-адрес назначения маршрута уже используется интерфейсом	В качестве IP-адреса назначения маршрута не допускается указывать IP-адрес управляющего интерфейса и интерфейса HTTP-посредника.
007.02.1178	IP-адрес назначения маршрута уже используется в другом маршруте	IP-адрес узла или сети назначения должен быть уникален среди всех маршрутов.
007.02.1179	IP-адрес HTTP-посредника не определен	Перед включением HTTP-посредника необходимо установить его IP-адрес (IP-адрес по умолчанию 0.0.0.0 не допустим для использования).
007.02.117A	HTTP-посредник и зеркалирование не должны использовать общий интерфейс	Использование одного и того же фильтрующего интерфейса в качестве интерфейса HTTP-посредника и зеркалируемого либо зеркалирующего интерфейсов недопустимо.

Код	Сообщение	Описание
007.02.117B	HTTP-посредник и NAT не должны использовать общий интерфейс	Использование одного и того же фильтрующего интерфейса в качестве интерфейса HTTP-посредника и в составе интерфейса NAT недопустимо.
007.02.117C	HTTP-посредник и резервирование не должны использоваться совместно	Совместное использование указанных функций недопустимо.
007.02.117D	Ошибка записи файла конфигурации HTTP-посредника	Системная ошибка УОС МЭ при записи файла. **Действия:** Проверить целостность компонентов программного обеспечения МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие-изготовитель.
007.02.117E	PROXY-правило не найдено	В текущей или дополнительной политике доступа не существует правила PROXY-правил, с указанным номером.
007.02.117F	PROXY-правило уже существует	PROXY-правило с указанным номером уже существует в текущей или дополнительной политике доступа.
007.02.1180	Таблица PROXY-правил переполнена	Число PROXY-правил в политике доступа больше максимально допустимого значения.
007.02.1181	Список доступа HTTP-посредника переполнен	Список доступа к HTTP-посреднику содержит максимально допустимое количество записей.
007.02.1182	Запись списка доступа HTTP-посредника не найдена	В списке доступа к HTTP-посреднику отсутствует запись с указанным номером.
007.02.1183	Слишком мало фильтрующих интерфейсов для HTTP-посредника	Экземпляр устройства МЭ ССПТ-4А1 должен иметь как минимум три фильтрующих интерфейса для использования HTTP-посредника.
007.02.1184	IP-адреса HTTP-посредника и управляющего интерфейса должны быть из разных подсетей	Не допускается использование IP-адресов из одной подсети.
007.02.1185	Слишком мало фильтрующих интерфейсов для агрегирования портов управляющего интерфейса	Функция агрегирования портов управляющего интерфейса не может быть включена на данном устройстве МЭ ССПТ-4А1 из-за недостаточного числа фильтрующих интерфейсов.
007.02.1186	Агрегирование портов управляющего интерфейса и зеркалирование не должны использовать общий интерфейс	Один и тот же фильтрующий интерфейс не может одновременно использоваться в указанных функциональных возможностях.
007.02.1187	Агрегирование портов управляющего интерфейса и NAT не должны использовать общий интерфейс	Один и тот же фильтрующий интерфейс не может одновременно использоваться в указанных функциональных возможностях.
007.02.1188	Агрегирование портов управляющего интерфейса и HTTP-посредник не должны использовать общий интерфейс	Один и тот же фильтрующий интерфейс не может одновременно использоваться в указанных функциональных возможностях.
007.02.118A	MTU интерфейсов в составе агрегата не должны отличаться	Агрегирование портов управляющего интерфейса не может быть включено, если интерфейсы, входящие в состав агрегата, имеют разные значения MTU.
007.02.118B	Установка параметра недоступна при включенном агрегировании портов управляющего интерфейса	Установка параметра управляющего интерфейса не допустима, когда включено агрегирование портов управляющего интерфейса.

Код	Сообщение	Описание
007.02.118C	HTTP-посредник и текущая политика доступа не должны использовать общий интерфейс	Один и тот же фильтрующий интерфейс не может использоваться HTTP-посредником и в текущей политике доступа.
007.02.118D	Агрегирование портов управляющего интерфейса и текущая политика доступа не должны использовать общий интерфейс	Один и тот же фильтрующий интерфейс не может использоваться агрегатом и в текущей политике доступа.
007.02.118E	Дополнительная конфигурация не может быть применена, так как интерфейс HTTP-посредника и/или агрегирования портов используется в текущей политике	Дополнительная конфигурация не может быть применена, так как интерфейс HTTP-посредника и/или агрегирования портов (в применяемой конфигурации) уже используется в текущей политике доступа (в объектах справочника и/или правилах фильтрации).
007.02.118F	Ошибка при сравнении по регулярному выражению	При выполнении проверки соответствия строки регулярному выражению произошла ошибка. Не удалось проверить строку на соответствие регулярному выражению.
007.02.1190	Недостаточный размер вектора выходных подстрок регулярного выражения	Неверный формат вспомогательного параметра, используемого при проверке строки по регулярному выражению.
007.02.1191	Ошибка отправки запроса серверу проверки контрольных сумм	Запрос серверу проверки контрольных сумм не был отправлен из-за ошибки.
007.02.1192	Конфликт IP-адреса интерфейса и таблицы маршрутов	Попытка добавить статический маршрут, в котором указан IP-адрес шлюза, не принадлежащий ни сети управляющего интерфейса, ни сети интерфейса HTTP-посредника.

В.3.2. Предупреждающие сообщения

Коды всех предупреждающих сообщений, их текстовая интерпретация и описание представлены в таблице В.4.

Таблица В.4: Предупреждающие сообщения командного интерпретатора МЭ ССПТ-4А1

Код	Сообщение	Описание
007.02.2001	Администратор работает с ограниченными привилегиями	Для выполнения команды текущих привилегий администратора недостаточно.
007.02.2002	Вход администратора с ограниченными привилегиями	При авторизации администратор получил ограниченные привилегии — `read`, т. к. привилегии `full` или `admin` уже заняты другими активными администраторами.
007.02.2003	Пакетный фильтр выключен	Для выполнения команды требуется, чтобы пакетный фильтр МЭ ССПТ-4А1 был включен (запущен).
007.02.2004	Учетная запись с данным именем не может быть добавлена.	Попытка добавления нового администратора МЭ ССПТ-4А1 с именем `admin`. Новый администратор с именем `admin` не может быть добавлен.
007.02.2005	Администратор не может быть удален	Попытка удаления администратора МЭ ССПТ-4А1 с именем `admin`. Администратор `admin` не может быть удален.
007.02.200C	Должен быть настроен IP-адрес управляющего интерфейса	Перед выполнением команды необходимо назначить IP-адрес управляющему Ethernet-интерфейсу.

Код	Сообщение	Описание
007.02.200D	IP-адрес уже назначен управляющему интерфейсу	IP-адреса удаленного сервера (NTP-сервер, RADIUS-сервер, FTP-сервер или SYSLOG-сервер) и управляющего Ethernet-интерфейса МЭ ССПТ-4А1 должны быть различными.
007.02.200E	Список доступа пустой	Список доступа к управлению МЭ ССПТ-4А1 не содержит ни одной записи.
007.02.200F	Запись списка доступа пустая	Указан номер записи списка доступа к управлению МЭ ССПТ-4А1, которая не содержит данных.
007.02.2010	Выгрузка файлов регистрации по FTP остается включенной	В конфигурации МЭ ССПТ-4А1 выгрузка файлов регистрации на удаленный FTP-сервер остается включенной при выполнении одного из следующих действий: • удаление маршрута по умолчанию (команда `interface control set gateway=0.0.0.0`); • назначение IP-адреса управляющему интерфейсу (команда `interface control set address=<IP-адрес/маска>`); • выключение управляющего интерфейса (команда `interface control set state=disable`).
007.02.2011	Синхронизация по NTP остается включенной	В конфигурации МЭ ССПТ-4А1 синхронизация по NTP остается включенной при выполнении одного из следующих действий: • удаление маршрута по умолчанию (команда `interface control set gateway=0.0.0.0`); • назначение IP-адреса управляющему интерфейсу (команда `interface control set address=<IP-адрес/маска>`); • выключение управляющего интерфейса (команда `interface control set state=disable`).
007.02.2012	Тайм-аут ожидания ответа от пакетного фильтра	Истекло время ожидания ответа от пакетного фильтра МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли пакетный фильтр.
007.02.2013	Режим управления сессиями должен быть включен	Перед выполнением команды необходимо включить режим управления сессиями.
007.02.2016	Необходимо выключить NAT	Перед выполнением команды необходимо выключить функцию трансляции сетевых адресов (NAT).
007.02.2018	Отсутствуют данные для вывода	Данные, запрашиваемые по введенной команде, отсутствуют.
007.02.201B	Нет ответа от сервера регистрации	Истекло время ожидания ответа от сервера регистрации МЭ ССПТ-4А1. **Действия**: Проверить, запущен ли сервер регистрации.
007.02.201C	Нет заданных регистрационных записей	По заданным критериям отбора не найдено ни одной регистрационной записи.
007.02.201E	Нет заданных правил фильтрации	По заданным критериям отбора не найдено ни одного правила фильтрации.
007.02.201F	Пакетный фильтр уже работает	Попытка повторного запуска пакетного фильтра МЭ ССПТ-4А1.
007.02.2022	Дополнительные конфигурации отсутствуют	Для МЭ ССПТ-4А1 не сохранено ни одной дополнительной конфигурации.

Код	Сообщение	Описание
007.02.2024	RADIUS-авторизация остается включенной	В конфигурации МЭ ССПТ-4А1 RADIUS-авторизация остается включенной при выключение управляющего интерфейса (команда `interface control set state=disable`).
007.02.2026	Удаленная регистрация по SYSLOG остается включенной	В конфигурации МЭ ССПТ-4А1 выгрузка записей регистрации на удаленный SYSLOG-сервер остается включенной при выполнении одного из следующих действий: • удаление маршрута по умолчанию (команда `interface control set gateway=0.0.0.0`); • назначение IP-адреса управляющему интерфейсу (команда `interface control set address=<IP-адрес/маска>`); • выключение управляющего интерфейса (команда `interface control set state=disable`).
007.02.2027	Аутентификация сетевых пользователей уже включена	Попытка повторного включения функции аутентификации сетевых пользователей.
007.02.2028	Аутентификация сетевых пользователей уже выключена	Попытка повторного выключения функции аутентификации сетевых пользователей.
007.02.2029	RADIUS-авторизация уже включена	Попытка повторного включения использования удаленного RADIUS-сервера для авторизации администраторов и/или сетевых пользователей МЭ ССПТ-4А1.
007.02.202A	RADIUS-авторизация уже выключена	Попытка повторного выключения использования удаленного RADIUS-сервера для авторизации администраторов и/или сетевых пользователей МЭ ССПТ-4А1.
007.02.202C	WEB-интерфейс уже включен	Попытка повторного включения WEB-интерфейса МЭ ССПТ-4А1.
007.02.202D	WEB-интерфейс уже выключен	Попытка повторного выключения WEB-интерфейса МЭ ССПТ-4А1.
007.02.202E	SNMP-интерфейс уже включен	Попытка повторного включения SNMP-интерфейса МЭ ССПТ-4А1.
007.02.202F	SNMP-интерфейс уже выключен	Попытка повторного выключения SNMP-интерфейса МЭ ССПТ-4А1.
007.02.2030	Резервирование уже включено	Попытка повторного включения резервирования МЭ ССПТ-4А1.
007.02.2031	Резервирование уже выключено	Попытка повторного выключения резервирования МЭ ССПТ-4А1.
007.02.2032	Смежное устройство вне управляющей IP-сети	IP-адреса управляющих Ethernet-интерфейсов смежных МЭ ССПТ-4А1 в схеме резервирования должны быть в одной и той же IP-подсети.
007.02.2033	Необходимо выключить резервирование	Перед выполнением команды необходимо выключить резервирование МЭ ССПТ-4А1.
007.02.2034	IP-адрес смежного устройства должен отличаться от адреса управляющего интерфейса	IP-адреса управляющих Ethernet-интерфейсов смежных МЭ ССПТ-4А1 в схеме резервирования должны быть различными.
007.02.2035	Необходимо включить резервирование	Перед выполнением команды должно быть включено резервирование МЭ ССПТ-4А1.
007.02.2036	Ошибка выполнения запроса к серверу резервирования	Не удалось отправить запрос серверу резервирования МЭ ССПТ-4А1. **Действия**: Перезагрузить МЭ ССПТ-4А1 для того, чтобы проверить корректность запуска сервера резервирования.

Код	Сообщение	Описание
007.02.2037	Нет ответа от смежного устройства	Истекло время ожидания ответа от смежного устройства. **Действия**: проверить работоспособность смежного устройства (МЭ ССПТ-4А1) и наличие сетевого соединения между двумя устройствами.
007.02.2038	Некорректное состояние резервирования для синхронизации	Состояние резервирования данного устройства МЭ ССПТ-4А1 в схеме резервирования не допускает синхронизацию текущей политики (передачу смежному МЭ ССПТ-4А1 своей текущей политики доступа).
007.02.2039	Нет запрошенных объектов справочника	В политике доступа МЭ ССПТ-4А1 отсутствуют объекты справочника, соответствующие заданным критериям отбора.
007.02.203A	Нет дополнительных политик	Для МЭ ССПТ-4А1 не сохранено ни одной дополнительной политики доступа.
007.02.203C	Имя фильтрующего интерфейса не соответствует его номеру	В дополнительной конфигурации МЭ ССПТ-4А1: • при применении ранее сохраненной конфигурации на МЭ ССПТ-4А1; • при загрузке конфигурации на МЭ ССПТ-4А1 с управляющего ПК назначенное имя фильтрующего интерфейса не соответствует его номеру и было автоматически заменено на имя, соответствующее номеру.
007.02.203E	Значение MTU фильтрующего интерфейса некорректно	В дополнительной конфигурации МЭ ССПТ-4А1: • при применении ранее сохраненной конфигурации на МЭ ССПТ-4А1; • при загрузке конфигурации на МЭ ССПТ-4А1 с управляющего ПК значение MTU фильтрующего интерфейса не поддерживается соответствующим интерфейсом данного МЭ ССПТ-4А1 и было автоматически заменено на значение по умолчанию: `1500`.
007.02.203F	Значение MTU управляющего интерфейса некорректно	В дополнительной конфигурации МЭ ССПТ-4А1: • при применении ранее сохраненной конфигурации на МЭ ССПТ-4А1; • при загрузке конфигурации на МЭ ССПТ-4А1 с управляющего ПК значение MTU управляющего интерфейса не поддерживается управляющим интерфейсом данного МЭ ССПТ-4А1 и было автоматически заменено на значение по умолчанию: `1500`.
007.02.2040	NAT выключен	При выключенной функции NAT динамические ARP-записи не могут существовать, поэтому они не могут быть: • удалены; • просмотрены.
007.02.2041	Изменение параметров данного администратора недопустимо	Попытка изменения параметров учетной записи администратора МЭ ССПТ-4А1 с именем `admin`. Не допускается изменять параметры (привилегии, параметр блокировки) учетной записи администратора `admin`.
007.02.2043	Маршрут по умолчанию NAT уже есть в таблице маршрутизации контейнера NAT	Попытка повторного добавления маршрута по умолчанию NA в таблицу маршрутизации контейнера NAT.

Код	Сообщение	Описание
007.02.2044	Нарушен формат структуры ответа сервера регистрации	Недопустимый код ответа от сервера регистрации: нарушен формат структуры ответа. **Действия**: Повторить запрос к серверу регистрации. В случае повторения предупреждения перезагрузить МЭ ССПТ-4А1. В случае повторения предупреждения после перезагрузки МЭ ССПТ-4А1 обратиться обратиться на предприятие-изготовитель.
007.02.2045	Значения параметров сброшены	В объекте Сервис (service) справочника было изменено значение параметра протокола, инкапсулированного в IP, при этом в значения по умолчанию автоматически были установлены другие параметры (из числа: icmp4, icmp6, port) объекта Сервис (service), значения которых не соответствуют новому значению протокола).
007.02.2046	HTTP-посредник уже включен	Попытка повторного включения HTTP-посредника МЭ ССПТ-4А1.
007.02.2047	HTTP-посредник уже выключен	Попытка повторного выключения HTTP-посредника МЭ ССПТ-4А1.
007.02.2048	Сервис с указанным IP-адресом будет недоступен	В результате выполнения команды указанный сервис (NTP, RADIUS, FTP или SYSLOG) станет недоступен с управляющего интерфейса МЭ ССПТ-4А1.
007.02.2049	Агрегирование портов управляющего интерфейса уже включено	Попытка повторного включения агрегирования портов управляющего интерфейса.
007.02.204A	Агрегирование портов управляющего интерфейса уже выключено	Попытка повторного выключения агрегирования портов управляющего интерфейса.
007.02.204B	Необходимо выключить агрегирование портов управляющего интерфейса	До выполнения команды необходимо выключить агрегирование портов управляющего интерфейса.
007.02.204C	Фильтрующий интерфейс используется агрегированием портов управляющего интерфейса	Предупреждение, когда агрегирование портов управляющего интерфейса и резервирование начинают работать одновременно (соответствующий фильтрующий интерфейс не должен использоваться в схеме резервирования).
007.02.204D	Фильтрующий интерфейс используется HTTP-посредником	Предупреждение, когда HTTP-посредник и резервирование начинают работать одновременно (соответствующий фильтрующий интерфейс не должен использоваться в схеме резервирования).
007.02.204E	Отложенная перезагрузка уже инициирована	Отложенная загрузка уже была инициирована администратором ранее.
007.02.204F	Отложенная перезагрузка не была инициирована или была отменена ранее	Отложенная загрузка ранее не была инициирована администратором, поэтому отмена отложенной перезагрузки невозможна.
007.02.2050	Тайм-аут ожидания ответа от сервера проверки контрольных сумм	Сервер проверки контрольных сумм не ответил на запрос за приемлемое время.

В.3.3. Информационные сообщения

Коды всех информационных сообщений командного интерпретатора МЭ ССПТ-4А1, их текстовая интерпретация и описание представлены в таблице В.5.

Таблица В.5: Информационные сообщения командного интерпретатора МЭ ССПТ-4А1

Код	*Сообщение*	*Описание*
007.02.3000	Нет ошибок	Сообщение используется только для уведомления WEB-интерфейса и SNMP-инетрфейса МЭ ССПТ-4А1 об успешном завершении выполнения команды.
007.02.3001	Успешная авторизация администратора	Введены правильные имя администратора и пароль и начался сеанс работы администратора.
007.02.3002	Администратор все еще работает	Сообщение используется только для уведомления WEB-интерфейса МЭ ССПТ-4А1 о том, что администратор продолжает работу в рамках установленного сеанса работы.
007.02.3003	Завершение работы администратора	Администратор завершил сеанс работы.
007.02.3004	Тайм-аут неактивности	Сеанс работы администратора завершается автоматически по причине истечения времени тайм-аута неактивности.
007.02.3005	Выход администратора по тайм-ауту неактивности	Администратор завершил сеанс работы после истечения времени тайм-аута неактивности.
007.02.3006	Администратор добавлен	Добавлен новый администратора МЭ ССПТ-4А1.
007.02.3007	Администратор удален	Удален существующий администратор МЭ ССПТ-4А1.
007.02.3008	Администратор выключен	Существующий администратор МЭ ССПТ-4А1 заблокирован.
007.02.3009	Администратор включен	Существующий администратор МЭ ССПТ-4А1 разблокирован.
007.02.300A	Пароль администратора изменен	Изменен пароль администратора МЭ ССПТ-4А1.
007.02.300B	Дополнительная конфигурация сохранена	Текущая конфигурация МЭ ССПТ-4А1 сохранена в дополнительной конфигурации.
007.02.300C	Привилегии администратора изменены	Изменены привилегии администратора МЭ ССПТ-4А1.
007.02.300D	Устройство будет выключено через две минуты. Выход ...	Начался процесс останова УОС МЭ ССПТ-4А1 и выключения МЭ ССПТ-4А1.
007.02.300E	Устройство будет перезагружено через две минуты. Выход ...	Начался процесс перезагрузки УОС МЭ ССПТ-4А1.
007.02.300F	Системное время изменено	Изменено системное время УОС МЭ ССПТ-4А1.
007.02.3010	Часовой пояс изменен	Изменена системная дата УОС МЭ ССПТ-4А1.
007.02.3011	NTP включен	Включена синхронизация системного времени МЭ ССПТ-4А1 по протоколу NTP.
007.02.3012	NTP выключен	Синхронизация системного времени МЭ ССПТ-4А1 по протоколу NTP выключена.
007.02.3012	Параметры NTP удалены	Из текущей конфигурации удалены настройки синхронизации системного времени МЭ ССПТ-4А1 по протоколу NTP. Синхронизация системного времени выключена.
007.02.3012	Адрес NTP сервера изменен	Изменен IP-адрес NTP-сервера в текущей конфигурации МЭ ССПТ-4А1.
007.02.3012	Регистрация сообщений NTP включена	Включена регистрация системных сообщений о результатах выполнения синхронизации системного времени по протоколу NTP.
007.02.3012	Регистрация сообщений NTP выключена	Регистрация системных сообщений о результатах выполнения синхронизации системного времени по протоколу NTP выключена.

Код	Сообщение	Описание
007.02.3012	Тайм-аут NTP изменен	Изменено значение периода синхронизации системного времени по протоколу NTP – тайм-аут опроса NTP-сервера.
007.02.3012	Системное время изменено по NTP	Выполнена немедленная синхронизация системного времени МЭ ССПТ-4А1 по протоколу NTP в соответствии с настройками текущей конфигурации.
007.02.3012	Новая запись добавлена в список доступа	Добавлена новая запись в список доступа к управлению МЭ ССПТ-4А1.
007.02.3012	Список доступа очищен	Удалены все записи из списка доступа к управлению МЭ ССПТ-4А1. Доступ к управлению МЭ ССПТ-4А1 может быть получен с любого IP-адреса.
007.02.3012	Запись удалена из списка доступа	Удалена запись из списка доступа к управлению МЭ ССПТ-4А1.
007.02.3012	IP-адрес управляющего интерфейса изменен	Назначен новый IP-адрес управляющему Ethernet-интерфейсу МЭ ССПТ-4А1.
007.02.3012	Фильтрующий интерфейс выключен	Заблокирован фильтрующий интерфейс МЭ ССПТ-4А1. Прием и передача пакетов через этот интерфейс выполняться не будет. Выводится символическое имя фильтрующего интерфейса.
007.02.3012	Фильтрующий интерфейс включен	Разблокирован фильтрующий интерфейс МЭ ССПТ-4А1. Выводится символическое имя фильтрующего интерфейса.
007.02.3012	Зеркалирование интерфейсов выключено	Функция зеркалирования трафика выключена. Настройки удаляются из текущей конфигурации МЭ ССПТ-4А1.
007.02.3012	Зеркалирование интерфейсов включено	Включена функция зеркалирования трафика на фильтрующих интерфейсах МЭ ССПТ-4А1.
007.02.3012	Интерфейс переименован	Фильтрующему интерфейсу МЭ ССПТ-4А1 присвоено новое символическое имя.
007.02.3012	Дополнительная конфигурация удалена	Удалена дополнительная конфигурация МЭ ССПТ-4А1.
007.02.3024	Дополнительная конфигурация применена	Дополнительная конфигурация МЭ ССПТ-4А1 применена. Может потребоваться перезапуск пакетного фильтра.
007.02.3027	NAT включен	Включена функция трансляции сетевых адресов (NAT) пакетного фильтра в соответствии с имеющимися настройками текущей конфигурации МЭ ССПТ-4А1.
007.02.3028	NAT выключен	Функция трансляции сетевых адресов (NAT) пакетного фильтра выключена.
007.02.3029	Регистрация пакетов, удаленных NAT, включена	Начинается регистрация пакетов, отброшенных функцией трансляции сетевых адресов (NAT) пакетного фильтра МЭ ССПТ-4А1.
007.02.302A	Регистрация пакетов, удаленных NAT, выключена	Регистрация пакетов, отброшенных функцией трансляции сетевых адресов (NAT) пакетного фильтра МЭ ССПТ-4А1 прекращается.
007.02.3032	Запись удалена из ARP-таблицы	Удалена запись из ARP-таблицы функции трансляции сетевых адресов (NAT) пакетного фильтра МЭ ССПТ-4А1.
007.02.3033	Новая запись добавлена в ARP-таблицу	Добавлена новая запись в ARP-таблицу функции трансляции сетевых адресов (NAT) пакетного фильтра МЭ ССПТ-4А1.

Код	Сообщение	Описание
007.02.3034	ARP-таблица очищена	Из ARP-таблицы функции трансляции сетевых адресов (NAT) пакетного фильтра МЭ ССПТ-4А1 удалены все статические (команда `nat arp clear`) либо динамические записи (команда `nat arp clear type=dynamic`). Тип удаленных записей указывается после данного сообщения.
007.02.303C	Регистрация пакетов выключена	Регистрация пакетов на сервере регистрации МЭ ССПТ-4А1 выключена.
007.02.303D	Регистрация пакетов включена	Включена регистрация пакетов на сервере регистрации МЭ ССПТ-4А1.
007.02.303E	Регистрация пакетов очищена	Из файлов регистрации удалены все записи о зарегистрированных пакетах.
007.02.303F	Параметры выгрузки журналов регистрации по FTP сброшены	Из текущей конфигурации удалены настройки выгрузки файлов регистрации на удаленный FTP-сервер. Функция выгрузки файлов регистрации выключен.
007.02.3040	Выгрузка журналов регистрации по FTP включена	Включена функция выгрузки файлов регистрации на удаленный FTP-сервер в соответствии с имеющимися настройками текущей конфигурации.
007.02.3041	Выгрузка журналов регистрации по FTP выключена	Функция выгрузки файлов регистрации на удаленный FTP-сервер выключена.
007.02.3042	Параметры выгрузки журналов регистрации по FTP определены	В текущей конфигурации сохранены новые настройки выгрузки файлов регистрации на удаленный FTP-сервер.
007.02.3043	Регистрация сессий очищена	Из файлов регистрации удалены все записи о зарегистрированных сессиях.
007.02.3046	Общее правило добавлено	В текущую или дополнительную политику доступа добавлено новое общее правило фильтрации . Выводится номер добавленного правила.
007.02.3047	Общее правило изменено	Изменено существующее общее правило фильтрации текущей или дополнительной политики доступа. Выводится номер правила.
007.02.3048	AP-правило добавлено	В текущую или дополнительную политику доступа добавлено новое AP-правило фильтрации . Выводится номер добавленного правила.
007.02.3049	AP-правило изменено	Изменено существующее AP-правило фильтрации текущей или дополнительной политики доступа. Выводится номер правила.
007.02.304A	Таблица сессий очищена	Удалены все активные сессии из таблицы сессий пакетного фильтра МЭ ССПТ-4А1.
007.02.304E	Возврат к предыдущему состоянию текущей политики выполнен	Отменено последнее изменение в текущей политике доступа.
007.02.3050	Общее правило удалено	Удалено общее правило фильтрации из текущей или дополнительной политики доступа. Выводится номер удаленного правила.
007.02.3051	AP-правило удалено	Удалено AP-правило фильтрации из текущей или дополнительной политики доступа. Выводится номер удаленного правила.
007.02.3052	Регистрация IP-пакетов, отброшенных механизмом управления сессиями, включена	Начинается регистрация пакетов, отброшенных механизмом управления сессиями пакетного фильтра МЭ ССПТ-4А1.

Код	Сообщение	Описание
007.02.3053	Регистрация IP-пакетов, отброшенных механизмом управления сессиями, выключена	Регистрация пакетов, отброшенных механизмом управления сессиями пакетного фильтра МЭ ССПТ-4А1 прекращается.
007.02.3054	Пакетный фильтр запущен	Выполнен запуск пакетного фильтра МЭ ССПТ-4А1.
007.02.3055	Пакетный фильтр работает	Сообщение используется только для уведомления WEB-интерфейса и SNMP-интерфейса МЭ ССПТ-4А1 о том, что пакетный фильтр находится в активном состоянии.
007.02.3056	Пакетный фильтр остановлен	Выполнен останов пакетного фильтра МЭ ССПТ-4А1. Прекращается прием и передача пакетов через фильтрующие интерфейсы.
007.02.3059	Общее правило скопировано	В текущей либо дополнительной политике доступа создана копия (с другим номером) общего правило фильтрации.
007.02.305A	Общее правило перемещено	В текущей либо дополнительной политике доступа общее правило перемещено в позицию, соответствующую новому номеру правила.
007.02.305B	Прикладное правило скопировано	В текущей либо дополнительной политике доступа создана копия (с другим номером) АР-правила фильтрации.
007.02.305C	Прикладное правило перемещено	В текущей либо дополнительной политике доступа общее АР-правило перемещено в позицию, соответствующую новому номеру правила.
007.02.305D	Конфигурация по умолчанию применена	Всем параметрам текущей конфигурации МЭ ССПТ-4А1 присвоены значения по умолчанию.
007.02.305E	Выбранные сессии удалены	Из таблицы сессий пакетного фильтра МЭ ССПТ-4А1 удалены сессии, соответствующие заданным критериям отбора.
007.02.305F	Статистика правил очищена	Обнулена статистика использования правил фильтрации текущей политики доступа в пакетном фильтре МЭ ССПТ-4А1.
007.02.3060	Обнаружение flood-атак включено	Включена функция обнаружения flood-атак пакетного фильтра МЭ ССПТ-4А1.
007.02.3061	Обнаружение flood-атак выключено	Функция обнаружения flood-атак пакетного фильтра МЭ ССПТ-4А1 выключена.
007.02.3062	Регистрация обнаружения flood-атак включена	В TMP-правилах фильтрации, автоматически создаваемых пакетным фильтром МЭ ССПТ-4А1 для отражения flood-атак, будет включена регистрация пакетов. Параметр регистрации уже существующих TMP-правил не будет изменен.
007.02.3063	Регистрация обнаружения flood-атак выключена	В TMP-правилах фильтрации, автоматически создаваемых пакетным фильтром МЭ ССПТ-4А1 для отражения flood-атак, будет выключена регистрация пакетов. Параметр регистрации уже существующих TMP-правил не будет изменен.
007.02.3064	Пороговое значение изменено	Изменено пороговое значение интенсивности трафика для функции обнаружения flood-атак пакетного фильтра МЭ ССПТ-4А1.
007.02.3065	Пароль пользователя SNMP-интерфейса изменен	Изменен пароль пользователя `fnpsnmp` SNMP-интерфейса МЭ ССПТ-4А1.
007.02.3066	Действие отменено	Выполнение команды прервано администратором.

Код	Сообщение	Описание
007.02.3067	Режим передачи фильтрующего интерфейса изменен	Изменен режим передачи на фильтрующем интерфейсе МЭ ССПТ-4А1. Выводится символическое имя фильтрующего интерфейса.
007.02.3068	Скорость передачи фильтрующего интерфейса изменена	Изменена скорость передачи на фильтрующем интерфейсе МЭ ССПТ-4А1. Выводится символическое имя фильтрующего интерфейса.
007.02.3069	Управляющий интерфейс выключен	Выключен управляющий Ethernet-интерфейс МЭ ССПТ-4А1. Настройки IP-адреса управляющего Ethernet-интерфейса в текущей конфигурации остаются без изменения.
007.02.306A	Управляющий интерфейс включен	Включен управляющий Ethernet-интерфейс МЭ ССПТ-4А1 в соответствии с настройками IP-адреса в текущей конфигурации.
007.02.306B	Скорость передачи управляющего интерфейса изменена	Изменена скорость передачи на управляющем Ethernet-интерфейсе МЭ ССПТ-4А1.
007.02.306C	Режим передачи управляющего интерфейса изменен	Изменен режим передачи на управляющем Ethernet-интерфейсе МЭ ССПТ-4А1.
007.02.306D	Выгрузка записей регистрации на SYSLOG-сервер выключена	Функция выгрузки записей регистрации на удаленный SYSLOG сервер выключен.
007.02.306E	Выгрузка записей регистрации на SYSLOG-сервер включена	Функция выгрузки записей регистрации на удаленный SYSLOG сервер включен.
007.02.306F	Параметры выгрузки системных сообщений на SYSLOG-сервер изменены	Параметры выгрузки записей регистрации на удаленный SYSLOG-сервер изменены в текущей конфигурации МЭ ССПТ-4А1.
007.02.3071	Аутентификация сетевых пользователей включена	Включена функция аутентификации сетевых пользователей. Использование данной функции возможно только при включенной функции трансляции сетевых адресов (NAT).
007.02.3072	Аутентификация сетевых пользователей выключена	Выключена функция аутентификации сетевых пользователей.
007.02.3073	Новый сетевой пользователь добавлен	Добавлен новый сетевой пользователь.
007.02.3074	Сетевой пользователь удален	Удален существующий сетевой пользователь.
007.02.3075	Сетевой пользователь выключен	Существующий сетевой пользователь заблокирован.
007.02.3076	Сетевой пользователь включен	Существующий сетевой пользователь разблокирован.
007.02.3077	Пароль сетевого пользователя изменен	Изменен пароль существующего сетевого пользователя.
007.02.3078	Сетевой пользователь сброшен	Администратором МЭ ССПТ-4А1 завершен сеанс работы сетевого пользователя.
007.02.3079	Нет активных сетевых пользователей	Нет ни одного зарегистрированного сеанса работы сетевых пользователей.
007.02.307A	Тайм-аут неактивности сетевых пользователей изменен	Изменено максимально допустимое время неактивности сеанса работы сетевого пользователя.
007.02.307B	Параметры сетевого пользователя изменены	Изменены параметры существующего сетевого пользователя – ограничения доступа и/или комментарий.
007.02.307C	Новая запись добавлена в файл ключей аутентификации	Добавлена новая пара ключей аутентификации сетевых пользователей.
007.02.307D	Запись удалена из файла ключей аутентификации	Удалена существующая пара ключей аутентификации сетевых пользователей.

Код	Сообщение	Описание
007.02.307E	Запись изменена в файле ключей аутентификации	Сгенерированы новые значения для существующей пары ключей аутентификации сетевых пользователей.
007.02.307F	Конфигурация RADIUS-сервера изменена	Изменены параметры удаленного RADIUS-сервера, используемого для авторизации администраторов и/или сетевых пользователей МЭ ССПТ-4А1.
007.02.3080	RADIUS-авторизация включена	Включено использование удаленного RADIUS-сервера для авторизации администраторов и/или сетевых пользователей МЭ ССПТ-4А1.
007.02.3081	RADIUS-авторизация выключена	Использование удаленного RADIUS-сервера для авторизации администраторов и/или сетевых пользователей МЭ ССПТ-4А1 выключено.
007.02.3082	Таймаут ожидания ответа от RADIUS-сервера изменен	Изменено максимальное время ожидания ответа от удаленного RADIUS-сервера.
007.02.3083	Количество обращений к RADIUS-серверу изменено	Изменено максимальное количество попыток обращения к удаленному RADIUS-серверу при авторизации администраторов и/или сетевых пользователей МЭ ССПТ-4А1.
007.02.3084	Тип учетной записи для RADIUS-авторизации изменен	Изменен тип учетной записи (администраторы и/или сетевые пользователи МЭ ССПТ-4А1), для которого разрешена авторизация через удаленный RADIUS-сервер.
007.02.3085	Режим управления сессиями включен	Включен режим управления сессиями пакетного фильтра МЭ ССПТ-4А1.
007.02.3086	Режим управления сессиями выключен	Режим управления сессиями пакетного фильтра МЭ ССПТ-4А1 выключен.
007.02.3087	Использование АР-правил включено	При включенном режиме управления сессиями пакетного фильтра МЭ ССПТ-4А1 будут использоваться АР-правила фильтрации.
007.02.3088	Использование АР-правил выключено	При включенном режиме управления сессиями пакетного фильтра МЭ ССПТ-4А1 АР-правила фильтрации использоваться не будут.
007.02.3089	Тайм-аут неактивности TCP-сессии изменен	Изменено значение тайм-аута неактивности для сессий, базирующихся на протоколе TCP.
007.02.308A	Тайм-аут неактивности UDP-сессии изменен	Изменено значение тайм-аута неактивности для сессий, базирующихся на протоколе UDP.
007.02.308B	Тайм-аут неактивности ICMP-сессии изменен	Изменено значение тайм-аута неактивности для сессий, базирующихся на протоколе ICMP.
007.02.308C	Тайм-аут неактивности сессии остальных протоколов изменен	Изменено значение тайм-аута неактивности для сессий, базирующихся на протоколах, отличных от TCP, UDP и ICMP.
007.02.308D	Тайм-аут неактивности сессий установлен по умолчанию	Тайм-аутам неактивности сессий присвоены значения по умолчанию.
007.02.308E	Сигнализация обнаружения flood-атак включена	Начинается регистрация системных сообщений об обнаружении flood-атак пакетным фильтром МЭ ССПТ-4А1.
007.02.308F	Сигнализация обнаружения flood-атак выключена	Регистрация системных сообщений об обнаружении flood-атак пакетным фильтром МЭ ССПТ-4А1 прекращается.

Код	Сообщение	Описание
007.02.3090	Комментарий TMP-правила изменен	В TMP-правилах фильтрации, автоматически создаваемых пакетным фильтром МЭ ССПТ-4А1 для отражения flood-атак, будет установлен данный комментарий. Комментарий в уже существующих TMP-правилах не будет изменен.
007.02.3091	Время жизни TMP-правила изменено	В TMP-правилах фильтрации, автоматически создаваемых пакетным фильтром МЭ ССПТ-4А1 для отражения flood-атак, будет установлено данное время жизни правила. Время жизни в уже существующих TMP-правилах не будет изменено.
007.02.3092	Использование данных канального уровня включено	Включен контроль неизменности MAC-адресов отправителя и получателя в обрабатываемых пакетах при управлении сессиями.
007.02.3093	Использование данных канального уровня выключено	Выключен контроль неизменности MAC-адресов отправителя и получателя в обрабатываемых пакетах при управлении сессиями.
007.02.3094	Глубокий контроль TCP включен	Включена функция глубокого контроля TCP-сессий.
007.02.3095	Глубокий контроль TCP выключен	Выключена функция глубокого контроля TCP-сессий.
007.02.3096	TMP-правило добавлено	Добавлено новое TMP-правило фильтрации. Выводится номер добавленного TMP-правила. (Все TMP-правила удалаются при останове пакетного фильтра МЭ ССПТ-4А1).
007.02.30BC	TMP-правило удалено	Удалено TMP-правило фильтрации. Выводится номер удаленного TMP-правила.
007.02.30BD	Режим просмотра изменен	Изменен режим просмотра данных в командном интерфейсе МЭ ССПТ-4А1.
007.02.30BE	Тайм-аут неактивности командного интерфейса изменен	Изменено максимально допустимое время неактивности пользователя в командном интерфейсе, WEB-интерфейсе и SNMP-интерфейсе МЭ ССПТ-4А1.
007.02.30BF	Буфер истории команд очищен	Выполнена очистка буфера истории команд командного интерфейса МЭ ССПТ-4А1.
007.02.30C0	Буфер истории команд пустой	В буфере истории команд командного интерфейса МЭ ССПТ-4А1 нет ни одной сохраненной команды.
007.02.30C1	Пароль системного пользователя изменен	Изменен пароль системного пользователя `fnpsh`.
007.02.30C2	WEB-интерфейс включен	Разрешено использование WEB-интерфейса МЭ ССПТ-4А1.
007.02.30C3	WEB-интерфейс выключен	Использование WEB-интерфейса МЭ ССПТ-4А1 запрещено.
007.02.30C4	SNMP-интерфейс включен	Разрешено использование SNMP-интерфейса МЭ ССПТ-4А1.
007.02.30C5	SNMP-интерфейс выключен	Использование SNMP-интерфейса МЭ ССПТ-4А1 запрещено.
007.02.30C6	Режим резервирования изменен	Установлен новый режим резервирования для данного МЭ ССПТ-4А1 в схеме резервирования.
007.02.30C7	Резервирование включено	Резервирование включено для данного МЭ ССПТ-4А1. Устройство может быть включено в соответствующую схему резервирования.
007.02.30C8	Резервирование выключено	Резервирование выключено для данного МЭ ССПТ-4А1.

Код	Сообщение	Описание
007.02.30C9	IP-адрес смежного устройства изменен	В текущей конфигурации изменен IP-адрес смежного МЭ ССПТ-4А1 для резервирования.
007.02.30CA	Параметры резервирования установлены по умолчанию	Всем параметрам резервирования в текущей конфигурации МЭ ССПТ-4А1 присвоены значения по умолчанию.
007.02.30CE	Синхронизация политики включена	Автоматическая синхронизация текущей политики доступа включена в текущей конфигурации МЭ ССПТ-4А1. Для использования данной функции должно быть включено резервирование.
007.02.30CF	Синхронизация политики выключена	Автоматическая синхронизация текущей политики доступа выключена в текущей конфигурации МЭ ССПТ-4А1.
007.02.30D0	Синхронизация политики инициирована	Выполнена команда принудительной синхронизации текущей политики доступа, запрос передан серверу резервирования. Для использования данной функции должно быть включено резервирование.
007.02.30D2	Скорость фильтрующих интерфейсов при резервировании изменена	Изменена скорость передачи для активного или заблокированного состояния фильтрующих интерфейсов МЭ ССПТ-4А1 при резервировании.
007.02.30D3	Объект справочника добавлен	В политику доступа (текущую или дополнительную) добавлен объект справочника. Также выводится тип и имя объекта.
007.02.30D4	Объект справочника изменен	В политике доступа (текущей или дополнительной) изменены параметры объекта справочника. Также выводится тип и имя объекта.
007.02.30F2	Объект справочника скопирован	В политике доступа (текущей или дополнительной) скопирован объекта справочника. Также выводится имя исходного объекта и его копии.
007.02.30F3	Объект справочника перемещен	В политике доступа (текущей или дополнительной) объекта справочника перемещен в другую позицию. Также выводится имя объекта.
007.02.30F4	Объект справочника удален	Из политике доступа (текущей или дополнительной) удален объекта справочника. Также выводится имя удаленного объекта.
007.02.30F6	Строка комментария добавлена	Добавлена строка комментария к группе объектов справочника или правил политики доступа (текущей или дополнительной).
007.02.30F7	Строка комментария изменена	Изменена строка комментария к группе объектов справочника или правил политики доступа (текущей или дополнительной).
007.02.30F8	Строка комментария удалена	Удалена строка комментария к группе объектов справочника или правил политики доступа (текущей или дополнительной).
007.02.30FC	Дополнительная политика применена	Применена дополнительная политика доступа из числа ранее сохраненных политик доступа МЭ ССПТ-4А1.
007.02.30FD	Дополнительная политика сохранена	Текущая политика доступа МЭ ССПТ-4А1 сохранена в дополнительную политику доступа.
007.02.30FE	Дополнительная политика удалена	Удалена дополнительная политика доступа из числа ранее сохраненных политик доступа МЭ ССПТ-4А1.

Код	Сообщение	Описание
007.02.30FF	Политика установлена в состояние по умолчанию	Политика доступа установлена в состояние по умолчанию: • справочник объектов пуст; • в политике только два глобальных запрещающих правила (`rule:0` и `ap:0`).
007.02.3102	Комментарий к дополнительной конфигурации изменен	Изменен комментарий к ранее сохраненной дополнительной конфигурации МЭ ССПТ-4А1.
007.02.3103	Дополнительная конфигурация переименована	Изменено имя ранее сохраненной дополнительной конфигурации МЭ ССПТ-4А1.
007.02.3104	MTU управляющего интерфейса изменено	Изменено MTU управляющего интерфейса. Новое значение сохранено в текущей конфигурации МЭ ССПТ-4А1.
007.02.3105	MTU фильтрующего интерфейса изменено	Изменено MTU фильтрующего интерфейса. Новое значение сохранено в текущей конфигурации МЭ ССПТ-4А1.
007.02.3106	Имя устройства и/или комментарий к нему изменено	В текущей конфигурации МЭ ССПТ-4А1 изменено имя устройства и/или комментарий к нему.
007.02.3107	Комментарий к дополнительной политике изменен	Изменен комментарий к ранее сохраненной дополнительной политике досутпа МЭ ССПТ-4А1.
007.02.3108	Дополнительная политика переименована	Изменено имя ранее сохраненной дополнительной политики доступа МЭ ССПТ-4А1.
007.02.3109	Сеансы работы администраторов сброшены	Завершены сеансы работы всех администраторов МЭ ССПТ-4А1, кроме администратора, выполнившего данную команду.
007.02.310A	Файл паролей администраторов установлен в состояние по умолчанию	В результате выполнения команды `system default`: файл паролей администраторов МЭ ССПТ-4А1 установлен в состояние по умолчанию.
007.02.310B	Файл паролей сетевых пользователей установлен в состояние по умолчанию	В результате выполнения команды `system default`: файл паролей сетевых пользователей МЭ ССПТ-4А1 установлен в состояние по умолчанию.
007.02.310C	Файл паролей системных пользователей установлен в состояние по умолчанию	В результате выполнения команды `system default`: файл паролей системных пользователей МЭ ССПТ-4А1 установлен в состояние по умолчанию.
007.02.310D	Файл паролей SNMP-интерфейса установлен в состояние по умолчанию	В результате выполнения команды `system default`: файл паролей SNMP-интерфейс МЭ ССПТ-4А1 установлен в состояние по умолчанию.
007.02.310E	Файл ключей аутентификации установлен в состояние по умолчанию	В результате выполнения команды `system default`: файл ключей аутентификации сетевых пользователей МЭ ССПТ-4А1 установлен в состояние по умолчанию.
007.02.310F	Все дополнительные конфигурации и политики удалены	В результате выполнения команды `system default`: Все дополнительные конфигурации и политики удалены МЭ ССПТ-4А1 удалены.
007.02.3110	Настройки зеркалирования интерфейсов изменены	Изменены параметры зеркалирования фильтрующих интерфейсов МЭ ССПТ-4А1 в текущей конфигурации.
007.02.3111	Параметры выгрузки на SYSLOG-сервер сброшены	В текущей конфигурации параметры выгрузки на SYSLOG-сервер установлены в значения по умолчанию. Функция выгрузки записей регистрации на SYSLOG-сервер выключена.
007.02.3112	Пакетный фильтр перезапущен	Выполнен перезапуск пакетного фильтра МЭ ССПТ-4А1.

Код	Сообщение	Описание
007.02.3113	Контейнер NAT добавлен	В текущую конфигурацию МЭ ССПТ-4А1 добавлен пустой контейнер NAT.
007.02.3114	Контейнер NAT удален	Из текущей конфигурации МЭ ССПТ-4А1 удален контейнер NAT со всем содержимым.
007.02.3115	Интерфейс NAT добавлен	В заданный контейнер NAT текущей конфигурации МЭ ССПТ-4А1 добавлен новый интерфейс NAT,
007.02.3116	Интерфейс NAT изменен	В один из контейнеров NAT текущей конфигурации МЭ ССПТ-4А1 изменены параметры интерфейса NAT,
007.02.3117	Интерфейс NAT удален	Из заданного контейнера NAT текущей конфигурации МЭ ССПТ-4А1 удален интерфейс NAT.
007.02.3118	Правило трансляции NAT добавлено	В заданный контейнер NAT текущей конфигурации МЭ ССПТ-4А1 добавлено новое правило трансляции NAT.
007.02.3119	Правило трансляции NAT изменено	В заданном контейнере NAT текущей конфигурации МЭ ССПТ-4А1 изменено правило трансляции NAT.
007.02.311A	Правило трансляции NAT удалено	Из заданного контейнера NAT текущей конфигурации МЭ ССПТ-4А1 удалено правило трансляции NAT.
007.02.311B	Правило переадресации NAT добавлено	В заданный контейнер NAT текущей конфигурации МЭ ССПТ-4А1 добавлено новое правило переадресации NAT.
007.02.311C	Правило переадресации NAT изменено	В заданном контейнере NAT текущей конфигурации МЭ ССПТ-4А1 изменено правило трансляции NAT.
007.02.311D	Правило переадресации NAT удалено	Из заданного контейнера NAT текущей конфигурации МЭ ССПТ-4А1 удалено правило трансляции NAT.
007.02.311E	Маршрут NAT добавлен	В заданный контейнер NAT текущей конфигурации МЭ ССПТ-4А1 добавлен новый маршрут NAT.
007.02.311F	Маршрут NAT изменен	В заданном контейнере NAT текущей конфигурации МЭ ССПТ-4А1 изменен маршрут NAT.
007.02.3120	Маршрут NAT удален	Из заданного контейнера NAT текущей конфигурации МЭ ССПТ-4А1 удален маршрут NAT.
007.02.3121	MAC-адрес установлен на фильтрующий интерфейс в контексте NAT	В контексте функции NAT на один или более фильтрующих интерфейсов в текущей конфигурации МЭ ССПТ-4А1 были установлены новые MAC-адреса.
007.02.3122	Переадресация для контейнера NAT включена	Включена переадресация для заданного контейнера NAT текущей конфигурации МЭ ССПТ-4А1.
007.02.3123	Переадресация для контейнера NAT выключена	Выключена переадресация для заданного контейнера NAT текущей конфигурации МЭ ССПТ-4А1.
007.02.3124	Поддержка traceroute-сессий включена	В текущей конфигурации включена поддержка traceroute-сессий пакетным фильтром МЭ ССПТ-4А1.
007.02.3125	Поддержка traceroute-сессий выключена	В текущей конфигурации выключена поддержка traceroute-сессий пакетным фильтром МЭ ССПТ-4А1.
007.02.3126	PRI-правило добавлено	В текущую или дополнительную политику доступа добавлено новое правило приоритизации. Выводится номер добавленного правила.

Код	Сообщение	Описание
007.02.3127	PRI-правило изменено	Изменено существующее правило приоритизации текущей или дополнительной политики доступа. Выводится номер правила.
007.02.3128	PRI-правило удалено	Удалено правило приоритизации из текущей или дополнительной политики доступа. Выводится номер удаленного правила.
007.02.3129	PRI-правило скопировано	В текущей либо дополнительной политике доступа создана копия (с другим номером) правила приоритизации.
007.02.312A	PRI-правило перемещено	В текущей либо дополнительной политике доступа правило приоритизации перемещено в позицию, соответствующую новому номеру правила.
007.02.312B	Использование PRI-правил включено	Включено использование правил приоритизации пакетным фильтром.
007.02.312C	Использование PRI-правил выключено	Выключено использование правил приоритизации пакетным фильтром.
007.02.312D	Список DNS-серверов установлен	В УОС МЭ ССПТ-4А1 установлен список DNS-серверов.
007.02.312E	Список DNS-серверов очищен	В УОС МЭ ССПТ-4А1 очищен список DNS-серверов.
007.02.312F	Маршрут добавлен	В маршрутную таблицу УОС МЭ ССПТ-4А1 добавлен маршрут.
007.02.3130	Маршрут изменен	В маршрутной таблице УОС МЭ ССПТ-4А1 изменен маршрут.
007.02.3131	Маршрут удален	Из маршрутной таблицы УОС МЭ ССПТ-4А1 удален маршрут.
007.02.3132	HTTP-посредник включен	Использование HTTP-посредника включено.
007.02.3133	HTTP-посредник выключен	Использование HTTP-посредника выключено.
007.02.3134	Параметры HTTP-посредника установлены	Параметры HTTP-посредника успешно установлены.
007.02.3135	PROXY-правило добавлено	В текущую или дополнительную политику доступа добавлено новое PROXY-правило. Выводится номер добавленного правила.
007.02.3136	PROXY-правило изменено	Изменено существующее PROXY-правило текущей или дополнительной политики доступа. Выводится номер правила.
007.02.3137	PROXY-правило удалено	Удалено PROXY-правило из текущей или дополнительной политики доступа. Выводится номер удаленного правила.
007.02.3138	PROXY-правило скопировано	В текущей либо дополнительной политике доступа создана копия (с другим номером) PROXY-правила.
007.02.3139	PROXY-правило перемещено	В текущей либо дополнительной политике доступа PROXY-правило перемещено в позицию, соответствующую новому номеру правила.
007.02.313A	Новая запись добавлена в список доступа HTTP-посредника	Добавлена новая запись в список доступа к HTTP-посреднику МЭ ССПТ-4А1.
007.02.313B	Запись списка доступа HTTP-посредника изменена	Изменена запись списка доступа к HTTP-посреднику МЭ ССПТ-4А1.
007.02.313C	Запись удалена из списка доступа HTTP-посредника	Удалена запись из списка доступа к HTTP-посреднику МЭ ССПТ-4А1.

Код	Сообщение	Описание
007.02.313D	Агрегирование портов управляющего интерфейса включено	Включено агрегирование портов управляющего интерфейса.
007.02.313E	Агрегирование портов управляющего интерфейса выключено	Выключено агрегирование портов управляющего интерфейса.
007.02.313F	Протокол агрегирования портов изменен	Изменен протокол агрегирования портов управляющего интерфейса.
007.02.3140	Изменен интерфейс агрегета	Изменен фильтрующий интерфейс, который будет использован в составе агрегата при включении агрегирования портов управляющего интерфейса.
007.02.3141	Отложенная перезагрузка инициирована	Администратор инициировал отложенную перезагрузку устройства.
007.02.3142	Отложенная перезагрузка отменена	Администратор отменил отложенную перезагрузку устройства, инициированную ранее.

В.4. Диагностические сообщения командного сервера МЭ ССПТ-4А1

В.4.1. Сообщения об ошибках

Коды всех сообщений об ошибках командного сервера МЭ ССПТ-4А1, их текстовая интерпретация и описание представлены в таблице В.6.

Таблица В.6: Сообщения об ошибках командного сервера МЭ ССПТ-4А1

Код	Сообщение	Описание
007.03.0001	Нет свободных слотов для соединения	Все соединения заняты. **Действие**: совершить повторный запрос на соединение через несколько минут.
007.03.0002	Ошибка чтения SID	Ошибка чтения данных SID. **Действия**: Необходимо пройти авторизацию заново и повторно отправить команду.
007.03.0003	Ошибка чтения команды	Ошибка чтения данных команды. **Действия**: Необходимо пройти авторизацию заново и повторно отправить команду.
007.03.0004	Неверная длина SID	Идентификатор сессии слишком длинный. **Действия**: Выполнить повторную авторизацию администратора.
007.03.0005	Неверная длина команды	Превышена максимально допустимая длина команды. **Действия**: Проверить правильность вводимых данных.
007.03.0006	Необходимо вначале выполнить вход	SID в списке клиентов не найден. **Действия**: Выполнить авторизацию администратора.
007.03.0007	Список дочерних процессов заполнен	Все соединения заняты. **Действие**: Совершить повторный запрос на соединение через несколько минут.

Код	Сообщение	Описание
007.03.0008	Достигнуто максимальное число сетевых соединений	Новое сетевое соединение не может быть открыто, т. к. достигнуто максимальное число сетевых соединений. **Действие**: Совершить повторный запрос на соединение через несколько минут.
007.03.0009	Ошибка чтения имени администратора	Ошибка чтения имени администратора. **Действия**: Выполнить повторную авторизацию администратора.
007.03.000A	Ошибка чтения пароля администратора	Ошибка чтения пароля администратора. **Действия**: Выполнить повторную авторизацию администратора.
007.03.000B	Ошибка чтения IP-адреса клиента	Ошибка чтения IP-адреса клиента. **Действия**: Выполнить повторную авторизацию администратора.
007.03.000C	Ошибка чтения кода типа клиента	Ошибка при чтении типа клиента (сетевой или локальный). **Действия**: Выполните повторную авторизацию администратора.
007.03.000D	Неверный синтаксис клиентского запроса	Ошибка синтаксиса запроса. **Действия**: Выполните проверку вводимых данных.
007.03.000E	Ошибка создания пары сокетов	Системная ошибка создания пары сокетов. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие изготовитель.
007.03.000F	Ошибка создания дочернего процесса	Системная ошибка дочернего процесса. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие изготовитель.
007.03.0010	Ошибка установки переменной окружения	Системная ошибка установки переменной окружения. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие изготовитель.
007.03.0011	Ошибка загрузки командного интерпретатора	Системная ошибка загрузки командного интерпретатора. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие изготовитель.
007.03.0015	Ошибка получения ответа авторизации	Ошибка получения ответа авторизации. **Действия**: Выполните повторную авторизацию администратора.
007.03.0016	Тайм-аут получения ответа авторизации	Превышено время ожидания ответа авторизации. **Действия**: проверьте соединение и повторите попытку авторизации.
007.03.0017	Ошибка чтения ответа авторизации	Ошибка чтения ответа авторизации.
007.03.0018	Ошибка чтения диагностического сообщения	Ошибка чтения диагностического сообщения.
007.03.0019	Ошибка компиляции регулярного выражения	Системная ошибка компиляции регулярного выражения. **Действия**: Перезагрузить МЭ ССПТ-4А1. В случае повторения ошибки обратиться на предприятие изготовитель.
007.03.001D	Неверный формат диагностического сообщения	Неверный формат диагностического сообщения.

Приложение Г. Командный язык МЭ ССПТ-4А1

В данном приложении представлен полный перечень команд МЭ ССПТ-4А1, доступных для выполнения через командного интерфейс МЭ ССПТ-4А1. Команды имеющие общее первое ключевое слово объединены в одну группу. Команды каждой отдельной группы приводятся в отдельной таблице. Команда **`exit`** служит для завершения сеанса администратора. Поскольку она состоит из единственного ключевого слова, то не отнесена ни к одной из групп. Перечень основных групп команд и их краткое описание представлены в разделе 3.1.1, стр. 55.

Г.1. Группа команд “config”

Таблица Г.1: Группа команд "config"

Команда	***Описание***
`config apply name=<имя_конфигурации>`	Применить дополнительную конфигурацию
`config default`	Применить конфигурацию по умолчанию
`config device {name=<имя_устройства>| comment=<комментарий>}`	Установить имя устройства и комментарий к нему
`config list`	Вывести список дополнительных конфигураций
`config remove name=<имя_конфигурации>`	Удалить дополнительную конфигурацию
`config rename srcname=<старое_имя_конфигурации> {dstname=<новое_имя_конфигурации> | comment=<комментарий>}`	Переименовать дополнительную конфигурацию, изменить комментарий к ней
`config save name=<имя_конфигурации> [comment=<комментарий>]`	Сохранить текущую конфигурацию
`config show [name=<имя_конфигурации>] [viewer=<режим_просмотра>] [format=<формат>]`	Вывести текущую или дополнительную конфигурацию

Г.2. Группа команд “directory”

Таблица Г.2: Группа команд "directory"

Команда	***Описание***
`directory copy srcname=<имя_объекта> dstname=<имя_объекта> [(after=<имя_объекта | before=<имя_объекта)] [ policy=<имя_политики> ]`	Сделать копию объекта справочника
`directory move name=<имя_объекта> (after=<имя_объекта | before=<имя_объекта) [ policy=<имя_политики> ]`	Переместить строку определения объекта справочника
`directory show [policy=<имя_политики>] [viewer=<просмотрщик>] [format=<формат_вывода>] [type=<тип_объектов] [name=<имя_объекта>]`	Вывести объекты справочника
Группа команд “directory add”	

Команда	Описание
directory add comment [policy=<имя_политики>] (before=<имя_объекта>|after=<имя_объекта>) comment=<комментарий>	Добавить строку комментария
directory add <определение_объекта> [policy=<имя_политики>] [(before=<имя_объекта> | after=<имя_объекта>)]	Добавить объект справочника. Определение объекта содержит тип объекта и соответствующий типу объекта набор параметров (приложение Е, стр. 540).
Группа команд “directory delete”	
directory delete (type=<тип_объектов> | name=<имя_объекта>) [policy=<имя_политики>]	Удалить объект с данным именем либо объекты данного типа
directory delete all [policy=<имя_политики>]	Удалить все объекты справочника
directory delete comment [(after=<имя_объекта | before=<имя_объекта)] [policy=<имя_политики>]	Удалить строку комментария перед/после указанного объекта справочника либо все строки комментариев из справочника объектов
Группа команд “directory edit”	
directory edit comment [policy=<имя_политики>] (before=<имя_объекта>|after=<имя_объекта>) comment=<комментарий>	Изменить строку комментария
directory edit <тип_объекта> <параметры_объекта> [policy=<имя_политики>]	Изменить объект справочника. Допустимые параметры объекта определятся типом объекта (приложение Е, стр. 540).

Г.3. Группа команд “filter”

Таблица Г.3: Группа команд "filter"

Команда	Описание
filter restart	Перезапустить пакетный фильтр
filter start	Запустить пакетный фильтр
filter show	Вывести статистику работы пакетного фильтра
filter stop	Остановить пакетный фильтр

Г.4. Группа команд “interface”

Таблица Г.4: Группа команд "interface"

Команда	Описание
Группа команд “interface control”	
interface control ping host=<IP-адрес> [number=<число_запросов>]	Проверить доступность IP-адреса через управляющий интерфейс
interface control set {address=<IP-адрес>/<IP-маска> | media=<скорость> | duplex=<режим_передачи> | mtu=<MTU> | state=<состояние>}	Установить параметры управляющего интерфейса
interface control show	Вывести параметры управляющего интерфейса
interface control lagg {state=<состояние> | protocol=<протокол_агрегирования> | interface=<интерфейс>}	Установить параметры агрегирования портов управляющего интерфейса

Команда	*Описание*
Группа команд “interface control acl”	
`interface control acl add address=<IP-адреса>`	Добавить запись в список доступа
`interface control acl clear`	Очистить список доступа
`interface control acl delete number=<номер_записи>`	Удалить запись из списка доступа
`interface control acl show`	Вывести список доступа
Группа команд “interface control media”	
`interface control media list`	Вывести поддерживаемые скорости передачи
Группа команд “interface filter”	
`interface filter mirror {srcif=<интерфейс> | dstif=<интерфейс> | direction=<направление> | state=<состояние>}`	Установить параметры зеркалирования
`interface filter rename interface=<интерфейс> name=<имя_интерфейса>`	Переименовать фильтрующий интерфейс
`interface filter set [interface=<интерфейс> ] {media=<скорость> | duplex=<режим_передачи> | mtu=<MTU> | state=<состояние>}`	Установить параметры фильтрующих интерфейсов
`interface filter show [interface=<интерфейс>] [viewer=<режим_просмотра>]`	Вывести параметры фильтрующих интерфейсов
Группа команд “interface filter media”	
`interface filter media list [interface=<интерфейс>]`	Вывести поддерживаемые скорости передачи

Г.5. Группа команд “log”

Таблица Г.5: Группа команд "log"

Команда	*Описание*
`log show`	Вывести параметры подсистемы регистрации
Группа команд “log event”	
`log event show {type=<тип_события> code=<код_события> | time=<интервал_времени>} [order=<порядок_сортировки>] [viewer=<режим_просмотра>]`	Вывести события
Группа команд “log export”	
Группа команд “log export ftp”	
`log export ftp clear`	Сбросить параметры выгрузки файлов регистрации на FTP-сервер
`log export ftp set {state=<состояние> | server=<IP-адрес> | path=<путь_на_FTP-сервере> | user=<имя_пользователя> | port=<порт>}`	Установить параметры выгрузки файлов регистрации на FTP-сервер
Группа команд “log export syslog”	
`log export syslog clear`	Сбросить параметры выгрузки записей регистрации на SYSLOG-сервер
`log export syslog set {state=<состояние> | server=<IP-адрес> | port=<порт> | type=<типы_выгружаемых_записей>}`	Установить параметры выгрузки записей регистрации на SYSLOG-сервер
Группа команд “log packet”	

Команда	Описание
log packet clear	Очистить журнал регистрации пакетов
log packet disable	Выключить регистрацию пакетов
log packet enable	Включить регистрацию пакетов
log packet show {action=<действие_правила> | srcif=<входной_интерфейс> | dstif=<выходной_интерфейс> | rule=<правило> | frame=<тип_кадра> | protocol=<протоколы> | sid=<идентификатор_сессии> | srcmac=<MAC-адрес_источника> | dstmac=<MAC-адрес_приемника> | mac=<MAC> | srcip4=<IPv4-адрес_источника> | dstip4=<IPv4-адрес_приемника> | ip4=<IPv4-адрес> | srcip6=<IPv6-адрес_источника> | dstip6=<IPv6-адрес_приемника> | ip6=<IPv6-адрес> | srcport=<порт_источника> | dstport=<порт_приемника> | port=<порт> | code=<код_ошибки> | time=<интервал_времени>} [order=<порядок_сортировки>] [viewer=<режим_просмотра>]	Вывести журнал регистрации пакетов
Группа команд “log session”	
log session clear	Очистить журнал регистрации сессий
log session show {ifcl=<интерфейс_клиента> | ifsrv=<инетрфейсы_сервера> | ipcl4=<IPv4-адрес_клиента> | ipsrv4=<IPv4-адрес_сервера> | ip4=<IPv4-адрес> | ipcl6=<IPv6-адрес_клиента> | ipsrv6=<IPv6-адрес_сервера> | ip6=<IPv6-адрес> | portcl=<порт_клиента> | portsrv=<порт_сервера> | port=<порт> | tproto=<протокол_в_IP> | aproto=<прикладной_протокол> | sid=<идентификатор_сессии> | tstart=<время_открытия_сессии> | tend=<время_закрытия_сессии>} [order=<порядок_сортировки>] [viewer=<режим_просмотра>]	Вывести журнал регистрации сессий
Группа команд “log syslog”	
log syslog show [viewer=<режим_просмотра>]	Вывести журнал регистрации системных сообщений

Г.6. Группа команд “nat”

Таблица Г.6: Группа команд "nat"

Команда	Описание
nat disable	Выключить NAT
nat enable	Включить NAT
nat show	Вывести параметры NAT
Группа команд “nat arp”	
nat arp add interface=<интерфейс> ip=<IP-адрес> mac=<MAC-адрес>	Добавить запись в ARP-таблицу
nat arp clear [type=(dynamic|static)]	Очистить ARP-таблицу
nat arp delete type=<тип_записи> (interface=<интерфейс> | ip=<IP-адрес> | mac=<MAC-адрес>)	Удалить запись из ARP-таблицы

Команда	*Описание*
nat arp show {interface=<интерфейс> | mac=<MAC-адрес | ip=<IP-адрес> | type=<тип_записи>}	Вывести ARP-записи
Группа команд “nat authentication”	
nat authentication set {state=<состояние> | timeout=<таймаут>}	Установить параметры аутентификации сетевых пользователей
Группа команд “nat authentication key”	
nat authentication key add address=<IP-адрес>	Добавить запись в файл ключей аутентификации
nat authentication key delete address=<IP-адрес>	Удалить запись из файла ключей аутентификации
nat authentication key update address=<IP-адрес>	Обновить запись в файле ключей аутентификации
nat authentication key show [address=<IP-адрес>]	Вывести ключи аутентификации
Группа команд “nat authentication user”	
nat authentication user add name=<имя_пользователя> {mac=<MAC-адрес> | address=<IP-адрес> | interface=<интерфейс> | comment=<комментарий>}	Добавить сетевого пользователя
nat authentication user clear [name=<имя_пользователя>]	Завершить сеанс сетевого пользователя
nat authentication user delete name=<имя_пользователя>	Удалить сетевого пользователя
nat authentication user edit name=<имя_пользователя> { state=<состояние> | mac=<MAC-адрес> | address=<IP-адрес> | interface=<интерфейс> | comment=<комментарий> }	Изменить параметры сетевого пользователя
nat authentication user list	Вывести базу данных сетевых пользователей
nat authentication user password name=<имя_пользователя>	Сменить пароль сетевого пользователя
nat authentication user show	Вывести активных сетевых пользователей
Группа команд “nat case”	
nat case add name=<имя_контейнера_NAT>	Добавить пустой контейнер NAT
nat case delete name=<имя_контейнера_NAT>	Удалить контейнер NAT
nat case list	Вывести список контейнеров NAT
nat case show [name=<имя_контейнера_NAT>] [viewer=<режим_просмотра>]	Вывести контейнеры NAT с их содержимым
Группа команд “nat log”	
nat log disable	Выключить регистрацию пакетов, отброшенных NAT
nat log enable	Включить регистрацию пакетов, отброшенных NAT
Группа команд “nat mac”	
nat mac set interface=<интерфейсы> address=<MAC-адреса>	Установить MAC-адреса на интерфейсах
nat mac show	Вывести MAC-адреса на интерфейсах

Команда	*Описание*
Группа команд “nat private”	
nat private add case=<имя_контейнера_NAT> name=<имя_интерфейса_NAT> interface=<интерфейсы> address=<IP-адреса>	Добавить внутренний интерфейс NAT
nat private delete case=<имя_контейнера_NAT> name=<имя_интерфейса_NAT>	Удалить внутренний интерфейс NAT
nat private edit case=<имя_контейнера_NAT> name=<имя_интерфейса_NAT> {interface=<интерфейсы> | address=<IP-адреса> }	Изменить внутренний интерфейс NAT
nat private show case=<имя_контейнера_NAT> [name=<имя_интерфейса_NAT>]	Вывести внутренние интерфейсы NAT
Группа команд “nat public”	
nat public add case=<имя_контейнера_NAT> name=<имя_интерфейса_NAT> interface=<интерфейсы> address=<IP-адреса>	Добавить внешний интерфейс NAT
nat public delete case=<имя_контейнера_NAT> name=<имя_интерфейса_NAT>	Удалить внешний интерфейс NAT
nat public edit case=<имя_контейнера_NAT> name=<имя_интерфейса_NAT> {interface=<интерфейсы> | address=<IP-адреса> }	Изменить внешний интерфейс NAT
nat public show case=<имя_контейнера_NAT> [name=<имя_интерфейса_NAT>]	Вывести внешние интерфейсы NAT
Группа команд “nat redirect”	
nat redirect add case=<имя_контейнера_NAT> interface=<имя_внешнего_интерфейса_NAT> pub-address=<IP-адрес> prv-address=<IP-адрес> pub-port=<порты> [prv-port=<порты>] [src-address=<IP-адреса>] [protocol=<протокол>]	Добавить правило переадресации NAT
nat redirect delete case=<имя_контейнера_NAT> [number=<номер>]	Удалить правило переадресации NAT с данным номером. Удалить все правила переадресации.
nat redirect edit case=<имя_контейнера_NAT> number=<номер> {interface=<имя_внешнего_интерфейса_NAT> pub-address=<IP-адрес> | prv-address=<IP-адрес> | pub-port=<порты> | prv-port=<порты> | src-address=<IP-адреса> | protocol=<протокол>}	Изменить правило переадресации NAT
nat redirect show case=<имя_контейнера_NAT> [viewer=<режим_просмотра>]	Вывести правила переадресации NAT
nat redirect set case=<имя_контейнера_NAT> state=<состояние>	Включить/выключить переадресацию для определенного контейнера NAT
Группа команд “nat route”	
nat route add case=<имя_контейнера_NAT> dst-address=<IP-адрес>[/<маска>] gateway=<IP-адрес>	Добавить маршрут NAT
nat route delete case=<имя_контейнера_NAT> [number=<номер>]	Удалить маршрут NAT с данным номером. Удалить все маршруты NAT.
nat route edit case=<имя_контейнера_NAT> number=<номер> { dst-address=<IP-адрес>[/<маска>] | gateway=<IP-адрес>}	Изменить маршрут NAT

Команда	Описание
nat route show case=<имя_контейнера_NAT> [viewer=<режим_просмотра>]	Вывести маршруты NAT
Группа команд “nat translate”	
nat translate add case=<имя_контейнера_NAT> number=<номер> prv-address=<IP-адреса> pub-address=<IP-адреса> interface=<имя_внешнего_интерфейса NAT> [dst-address=<IP-адреса>] [protocol=<протокол>]	Добавить правило трансляции NAT
nat translate delete case=<имя_контейнера_NAT> [number=<номер>]	Удалить правило трансляции NAT с данным номером. Удалить все правила трансляции NAT.
nat translate edit case=<имя_контейнера_NAT> number=<номер> {prv-address=<IP-адреса> | pub-address=<IP-адреса> interface=<имя_внешнего_интерфейса> | dst-address=<IP-адреса> | protocol=<протокол>}	Изменить правило трансляции NAT
nat translate show case=<имя_контейнера_NAT> [viewer=<режим_просмотра>]	Вывести правила трансляции NAT

Г.7. Группа команд “policy”

Таблица Г.7: Группа команд "policy"

Команда	Описание
policy apply name=<имя_политики_доступа> [type=<тип_данных>]	Применить дополнительную политику
policy default [type=<тип_данных>]	Сбросить политику в состояние по умолчанию
policy list	Вывести список дополнительных политик
policy remove name=<имя_политики_доступа>	Удалить дополнительную конфигурацию
policy rename srcname=<старое_имя_политики_доступа> {dstname=<новое_имя_политики_доступа> | comment=<комментарий>}	Переименовать дополнительную политику, изменить комментарий к ней
policy rollback	Возврат к предыдущему состоянию текущей политики
policy save name=<имя_политики_доступа> [comment=<комментарий>]	Сохранить текущую политику как дополнительную

Г.8. Группа команд “reserv”

Таблица Г.8: Группа команд "reserv"

Команда	Описание
reserv default	Установить параметры резервирования в значения по умолчанию
reserv disable	Выключить резервирование
reserv enable	Включить резервирование
reserv set media-active=<скорость> media-blocked=<скорость> mode=<режим> neighbour=<IP-адрес> sync=<состояние>	Установить параметры резервирования
reserv show	Вывести параметры резервирования

Команда	Описание
reserv sync	Немедленная синхронизация текущей политики доступа

Г.9. Группа команд “rule”

Таблица Г.9: Группа команд "rule"

Команда	Описание
rule copy type=<тип_правила> srcnum=<номер_правила> dstnum=<новый_номер_правила> [policy=<имя_политики_доступа>]	Сделать копию правила
rule move type=<тип_правила> srcnum=<номер_правила> dstnum=<новый_номер_правила> [policy=<имя_политики_доступа>]	Переместить правило
rule show {type=<тип правила> | number=<номера_правил> | action=<действие_правила> | srcif=<интерфейсы_источника> | dstif=<интерфейсы_приемника> | active=<активность_правила> | object=<имя_объекта_справочника>} [viewer=<режим_просмотра>] [format=<формат_вывода>] [policy=<имя_политики_доступа>]	Вывести список правил
Группа команд “rule add”	
rule add <определение_правила> [policy=<имя_политики_доступа>]	Добавить правило. Определение правила содержит тип правила, номер правила и соответствующие типу правила параметры (приложение Д, стр. 514).
rule add comment (before=<тип_правила>:<номер_правила> | after=<тип_правила>:<номер_правила>) comment=<комментарий> [policy=<имя_политики_доступа>]	Добавить строку комментария
Группа команд “rule delete”	
rule delete <тип_правила>:<номер_правила> [policy=<имя_политики_доступа>]	Удалить правило
rule delete comment [(after=<тип_правила>:<номер_правила> | before=<тип_правила>:<номер_правила>)] [policy=<имя_политики_доступа>]	Удалить строку комментария после либо перед указанным правилом или удалить все строки комментариев
Группа команд “rule edit”	
rule edit <тип_правила>:<номер_правила> <параметры_правила> [policy=<имя_политики_доступа>]	Изменить правило. Допустимые параметры правила определяются типом правила (приложение Д, стр. 514).
rule edit (before=<тип_правила>:<номер_правила> | after=<тип_правила>:<номер_правила>) comment=<комментарий> [policy=<имя_политики_доступа>]	Изменить строку комментария
Группа команд “rule priority”	
rule priority disable	Выключить использование правил приоритизации

Команда	*Описание*
rule priority enable	Включить использование правил приоритизации
Группа команд “rule stats”	
rule stats clear	Очистить статистику правил текущей политики
rule stats clear rule	Очистить статистику общих правил
rule stats clear ap	Очистить статистику AP-правил
rule stats clear tmp	Очистить статистику TMP-правил
rule stats show {type=<тип_правила> | number=<номера_правил> | action=<действие_правила> | srcif=<интерфейсы_источника> | dstif=<интерфейсы_приемника>} [suffix=<использование_суффиксов>]	Вывести статистику правил текущей политики

Г.10. Группа команд “session”

Таблица Г.10: Группа команд "session"

Команда	*Описание*
session disable	Выключить управление сессиями
session enable	Включить управление сессиями
session show	Вывести параметры управления сессиями
Группа команд “session ap”	
session ap disable	Выключить использование прикладных правил
session ap enable	Включить использование прикладных правил
Группа команд “session deeptcp”	
session deeptcp disable	Выключить глубокий контроль TCP
session deeptcp enable	Включить глубокий контроль TCP
Группа команд “session flood”	
session flood disable	Выключить обнаружение flood-атак
session flood enable	Включить обнаружение flood-атак
session flood rule comment=<комментарий> lifetime=<время_жизни> log=<состояние>	Установить параметры TMP-правила, создаваемого для отражения flood-атак
Группа команд “session flood alarm”	
session flood alarm disable	Выключить сигнализацию обнаружения flood-атак
session flood alarm enable	Включить сигнализацию обнаружения flood-атак
Группа команд “session flood threshold”	
session flood threshold default	Установить пороговые значения для протоколов по умолчанию
session flood threshold {tcp=<значение> | udp=<значение> | icmp=<значение>}	Установить пороговые значения для протоколов
Группа команд “session invalid”	
Группа команд “session invalid log”	

Команда	*Описание*
`session invalid log disable`	Выключить регистрацию пакетов, отброшенных механизмом управления сессиями
`session invalid log enable`	Включить регистрацию пакетов, отброшенных механизмом управления сессиями
Группа команд “session mac”	
`session mac disable`	Выключить использования данных канального уровня в сессиях
`session mac enable`	Включить использования данных канального уровня в сессиях
Группа команд “session table”	
`session table clear [nolog]`	Очистить таблицу сессий (с регистрацией или без)
`session table delete {sid=<идентификатор_сессии> | ipcl=<IP-адрес_клиента> | ipsrv=<IP-адрес_сервера> | ip=<IP-адрес> | portcl=<порт_клиента> | portsrv=<порт_сервера> | port=<порт> | tproto=<протокол_в_IP> | aproto=<прикладной_протокол> | state=<состояние_сессии> | rule=<номер_правила>}`	Удалить одну или более сессий из таблицы сессий
`session table show {sid=<идентификатор_сессии> | vlan=<идентификатор_VLAN> | ifcl=<интерфейс_клиента> | ifsrv=<интерфейс_сервера> | ipcl4=<IPv4-адреса_клиента> | ipsrv4=<IPv4-адреса_сервера> | ip4=<IPv4-адреса> | ipcl6=<IPv6-адреса_клиента> | ipsrv6=<IPv6-адреса_сервера> | ip6=<IPv6-адреса> | portcl=<порт_клиента> | portsrv=<порт_сервера> | port=<порт> | tproto=<протокол_в_IP> | aproto=<прикладной_протокол> | state=<состояние_сессии> | rule=<номер_правила>} [sort=<критерий_сортировки>] [order=<порядок_сортировки>] [number=<число_сессий>]`	Вывести таблицу сессий целиком либо сессии, соответствующие заданным критериям выборки
Группа команд “session timeout”	
`session timeout default`	Установить тайм-ауты неактивности (состояний) сессий в значения по умолчанию
`session timeout protocol=<протокол> {syn=<значение> | established=<значение> | fin=<значение>}`	Установить тайм-ауты неактивности (состояний) сессий для указанного протокола
Группа команд “session trace”	
`session trace disable`	Выключить поддержку traceroute-сессий
`session trace enable`	Включить поддержку traceroute-сессий

Г.11. Группа команд “system”

Таблица Г.11: Группа команд "system"

Команда	***Описание***
system default	Сбросить настройки устройства
system halt	Выключить устройство
system icheck [viewer=<режим_просмотра>] [type=<тип_файлов>]	Выполнить проверку целостности по базовому списку файлов (по умолчанию) либо списку исполняемых файлов
system reboot [time=<интервал_до_перезагрузки> {policy=<имя_политики_доступа>| config=<имя_конфигурации>}]	Перезагрузить устройство немедленно или через заданный интервал времени с применением дополнительной политики и/или конфигурации
system show [type=(system|config)]	Вывести системную информацию по аппаратному и программному обеспечению либо основные параметры текущей конфигурации
system status	Вывести информацию по использованию аппаратного обеспечения (процессор, оперативная память, разделы носителя данных)
Группа команд “system dns”	
system dns clear	Очистить список DNS-серверов
system dns set address=(<IP-адрес>)[,...]	Установить список DNS-серверов
system dns show	Вывести список DNS-серверов
Группа команд “system fnpsh”	
system fnpsh password	Сменить пароль системного пользователя fnpsh
system fnpsh set {viewer=<режим_просмотра> | timeout=<значение>}	Установить тайм-аут неактивности администратора и/или просмотрщик по умолчанию
Группа команд “system fnpsh history”	
system fnpsh history clear	Очистить буфер истории команд данного администратора
system fnpsh history show	Вывести буфер истории команд данного администратора
Группа команд “system key”	
system key show	Вывести ключи и сертификаты данного устройства
Группа команд “system proxy”	
system proxy set {interface=<фильтрующий_интерфейс> | address=<IP-адрес>/<IP-маска> | port=<порт> | state=<состояние>}	Установить параметры HTTP-посредника. Включить либо выключить HTTP-посредник
system proxy show	Вывести параметры HTTP-посредника
Группа команд “system proxy acl”	
system proxy acl add address=(<IP-адрес>[/<IP-маска>])[,...]	Добавить запись в список доступа HTTP-посредника
system proxy acl edit number=<номер_записи> address=(<IP-адрес>[/<IP-маска>])[,...]	Изменить запись списка доступа HTTP-посредника

Команда	Описание
system proxy acl delete [number=<номер_записи>]	Удалить запись из списка доступа HTTP-посредника. Очистить список доступа HTTP-посредника
system proxy acl show [viewer=<режим_просмотра>]	Вывести список доступа HTTP-посредника
Группа команд “system route”	
system route add dst-address=(<IP-адрес>[/<IP-маска>]) gateway=<IP-адрес>	Добавить маршрут
system route edit number=<номер_маршрута> gateway=<IP-адрес>	Изменить маршрут
system route delete [number=<номер_маршрута>]	Удалить маршрут с указанным номером. Удалить все маршруты.
system route show [viewer=<режим_просмотра>]	Вывести маршруты
Группа команд “system snmp”	
system snmp disable	Выключить SNMP-интерфейс
system snmp enable	Включить SNMP-интерфейс
system snmp password	Сменить пароль пользователя SNMP-интерфейса
Группа команд “system time”	
system time set {time=<время> | date=<дата> | time=<время> date=<дата>}	Установить системные дату и время
system time show	Вывести системные дату и время и параметры их обновления через NTP-сервер
system time zone	Установить часовой пояс
Группа команд “system time ntp”	
system time ntp delete	Удалить параметры обновления системных даты и времени через NTP-сервер и выключить функцию обновления через NTP-сервер
system time ntp set {state=<состояние> | log=<регистрация> | server=<IP-адрес> | timeout=<значение>}	Установить параметры обновления системных даты и времени через NTP-сервер
system time ntp update [server=<IP-адрес>]	Опросить NTP-сервер немедленно
Группа команд “system web”	
system web disable	Выключить WEB-интерфейс
system web enable	Включить WEB-интерфейс

Г.12. Группа команд “user”

Таблица Г.12: Группа команд "user"

Команда	Описание
user add name=<имя_пользователя> [privilege=<привилегии>] [state=<состояние>]	Добавить администратора
user clear	Завершить сеансы работы администраторов
user delete name=<имя_администратора>	Удалить администратора

Команда	***Описание***
`user edit name=<имя_пользователя> {privilege=<привилегии> | state=<состояние>}`	Изменить администратора
`user list`	Вывести базу данных администраторов
`user password [name=<имя_администратора>]`	Изменить пароль администратора
`user show`	Вывести активных администраторов
Группа команд “user radius”	
`user radius set {master-server=<IP-адрес> | master-port=<порт> | master-key=<секретный_ключ> | slave-server=<IP-адрес> | slave-port=<порт> | slave-key=<секретный_ключ> | state=<состояние> | type=<тип_учетной_записи> | retry=<значение> | timeout=<значение>}`	Установить параметры идентификации и аутентификации через RADIUS-сервер
`user radius show`	Вывести параметры идентификации и аутентификации через RADIUS-сервер

Приложение Д. Определения правил фильтрации

Если комментарий к правилу фильтрации (параметр **comment)** содержит символы **“пробел”**, то в командном интерфейсе администратора МЭ ССПТ-4А1 такая строка комментария должна быть заключена в двойные кавычки, например: **comment=”запретить доступ”**

Если комментарий к правилу фильтрации (параметр comment) содержит символ **“двойная кавычка”**, то в командном интерфейсе администратора МЭ ССПТ-4А1 все символы **“двойная кавычка”** должны быть экранированы, например: **comment=”разрешить доступ к \”Name\””**

Д.1. Определение общего правила

```
rule:<номер> action=<действие> [frame=<фрейм>] [ethproto=<протоколы_ethernet>]
[srcif=<входной_интерфейс>] [srcmac=<MAC-адрес_источника>] [srcip4=<IPv4-
адрес_источника>] [srcip6=<IPv6-адрес_источника>] [srcport=<порт_источника>]
[srcobject=<сетевой_объект_источника>] [srcservice=<сервис_источника>]
[srcresource=<ресурс_источника>] [dstif=<выходной_интерфейс>] [dstmac=<MAC-
адрес_приемника>] [dstip4=<IPv4-адрес_приемника>] [dstip6=<IPv6-
адрес_приемника>] [dstport=<порт_приемника>]
[dstobject=<сетевой_объект_приемника>] [dstservice=<сервис_приемника]
[dstresource=<ресурс_приемника>] [ipproto=<протокол_в_IP>]
[version=<версия_IP>] [icmp4=<тип_код_ICMPv4>] [icmp6=<тип_код_ICMPv6>]
[ttl=<значение_ttl>] [length=<длина>] [tos=<значение_TOS>]
[class=<класс_трафика>] [fragment=<фрагментация>] [hopbyhop=<значение_опции>]
[destination=<значение_опции>] [routing=<значение_опции>]
[ah=<значение_опции>] [esp=<значение_опции>] [vlan=<идентификатор_vlan>]
[time=<интервал_времени>] [session=<создание_сессии>]
[timeout=<таймаут_сессии>] [sesbreak=<разрыв_сессии>]
[apr=<список_прикладных_правил>] [alarm=<сигнализация>] [active=<активность>]
[log=<регистрация>] [comment=<комментарий>]
```

Где:

- **<номер>** - номер общего правила. Допустимые значения: 1-65535 (Номер 0 используется для глобального общего правила);
- **action=<действие>** - действие правила. Ожидаются:
  - ✔ accept – передача пакета на прикладной уровень (в таблицу прикладных правил) либо на выходные интерфейсы (если АР-правил нет);
  - ✔ drop – удаление пакета;
  - ✔ deny – удаление пакета с отправкой клиенту пакета-уведомления (TCP-сегмента с флагом RST для TCP и ICMP-сообщения для остальных протоколов);
  - ✔ goto:<номер> – переход к правилу с номером <номер> в списке общих правил;
- **frame=<фрейм>** - тип Ethernet-фрейма. Возможно указание списком, например: `eth2,snap,raw`. Ожидаются:
  - ✔ any – любой фрейм Ethernet (по умолчанию);
  - ✔ eth2 - фрейм Ethernet-II;

✔ llc – фрейм IEEE-802.3 с заголовком IEEE-802.2/LLC (далее фрейм LLC);

✔ snap - фрейм IEEE-802.3 с заголовком IEEE-802.2/SNAP (далее фрейм SNAP);

✔ raw - фрейм IEEE-802.3;

- **ethproto=<протоколы>** - протокол, инкапсулированный в Ethernet-фрейм. В зависимости от типа Ethernet- фрейма ожидаются:

✔ any – любой инкапсулированный протокол (по умолчанию);

✔ (<num>[-<num>])[,...] - список номеров протоколов для фреймов Ethernet-II и llc:

◆ <num> - шестнадцатеричное число;

• Допустимые значения для фрейма Ethernet-II: 0x05ef-0xfffe;

• Допустимые значения для фрейма LLC: 0x00-0xff.

✔ <OUI>/(<num>[-<num>])[,...] - шестизначный шестнадцатеричный код производителя (<OUI>) и список номеров протоколов (<num>) для фрейма SNAP:

◆ Допустимые значения для <OUI>: 0x000000-0xffffff;

◆ Допустимые значения для <num>: 0x0001-0xfffe.

- **srcif=<входной интерфейс>** - входной интерфейс. Ожидаются:

✔ any - любой входной интерфейс (по умолчанию);

✔ (<имя_интерфейса> | <номер_интерфейса>)[,...] – список номеров и/или символических имен интерфейсов;

- **srcmac=<MAC-адрес_источника>** - MAC-адрес источника пакета. Ожидаются:

✔ any – любой MAC-адрес источника (по умолчанию);

✔ (<MAC-адрес>[/<MAC-маска>])[,...] - список MAC-адресов (например: 00e0fe7895cd/24,00:e0:fe:78:95:cd/ff:ff:ff:00:00:00,00-e0-fe-78-95-cd).

◆ <MAC-адрес>: без разделителей, например: aabbccddeeff;

◆ <MAC-адрес>: с разделителем ":", например: aa:bb:cc:dd:ee:ff;

◆ <MAC-адрес>: с разделителем "-", например: aa-bb-cc-dd-ee-ff;

◆ <MAC-маска>: без разделителей, например: ffffff000000;

◆ <MAC-маска>: с разделителем ":", например: ff:ff:ff:00:00:00;

◆ <MAC-маска>: с разделителем "-", например: ff-ff-ff-00-00-00;

◆ <MAC-маска>: в кратком формате (число бит): 24;

- **srcip4=<IPv4-адрес_источника>** - IP-адрес источника пакета. Ожидаются:

◆ any – любой IP-адрес источника (по умолчанию);

◆ (<IP-адрес>[-<IP-адрес>]|<IP-адрес>/маска)[,...] – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25)

• <маска>: краткий формат (CIDR), например: 24;

• <маска>: полный формат, например: 255.255.255.0.

- **srcip6=<IPv6_адрес_источника>** - IPv6-адрес источника пакета. Ожидаются:

✔ any – любой IPv6-адрес источника (по умолчанию);

✔ (<IPv6-адрес>[-<IPv6-адрес>] | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов (например: 2001:b08:3:123::67,2001:b08:3:123::100-2001:b08:3:123::1ff,2001:b08:3:123::/64)

- <длина_префикса>: число бит префикса (CIDR), например: 64;

- **srcport=<порт_источника>** - список TCP-портов или UDP-портов источника. Ожидаются:

✔ any – любой порт (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] - список номеров портов и/или **символьных псевдонимов портов** (например: 22-25,110,80,https,postgresql);

- **srcobject=<сетевой_объект_источника>** - список имен сетевых объектов источника из справочника. Ожидаются:

✔ none - параметр на задан (по умолчанию);

✔ (<имя_объекта>)[,...] - список имен объектов из справочника (в списке допускается указание имён объектов следующих типов: *узел сети, сеть, группа сетевых объектов*);

- **srcservice=<сервис_источника>** - список имен объектов типа *"service"* источника из справочника. Ожидаются:

✔ none - параметр не задан (по умолчанию);

✔ (<имя_объекта>)[,...] - список имен объектов типа *"service"* из справочника;

- **srcresource=<ресурс_источника>** - список имен объектов типа *"resource"* источника из справочника. Ожидаются:

✔ none - параметр на задан (по умолчанию);

✔ (<имя_объекта>)[,...] - список имен объектов типа *"resource"* из справочника;

- **dstif=<выходной_интерфейс>** - выходной интерфейс. Ожидаются:

✔ any - любой интерфейс назначения (по умолчанию). В случае значения *“any”* пакет передается на все интерфейсы кроме того, на который он был получен;

✔ (<имя_интерфейса> | <номер_интерфейса>)[,...] – список номеров и/или символических имен интерфейсов;

- **dstmac=<MAC-адрес_приемника>** - MAC-адрес приемника пакета. Ожидаются:

✔ any – любой MAC-адрес источника (по умолчанию);

✔ (<MAC-адрес>[/<MAC-маска>])[,...] - список MAC-адресов (например: 00e0fe7895cd/24,00:e0:fe:78:95:cd/ff:ff:ff:00:00:00,00-e0-fe-78-95-cd).

- <MAC-адрес>: без разделителей, например: aabbccddeeff;
- <MAC-адрес>: с разделителем ":", например: aa:bb:cc:dd:ee:ff;
- <MAC-адрес>: с разделителем "-", например: aa-bb-cc-dd-ee-ff;
- <MAC-маска>: без разделителей, например: ffffff000000;
- <MAC-маска>: с разделителем ":", например: ff:ff:ff:00:00:00;
- <MAC-маска>: с разделителем "-", например: ff-ff-ff-00-00-00;

- <MAC-маска>: в кратком формате (число бит): 24;

- **dstip4=<IPv4-адрес_приемника>** - список IP-адресов приемника пакета. Ожидаются:
  - ✔ any – любой IP-адрес приемника (по умолчанию);
  - ✔ (<IP-адрес>[-<IP-адрес>]|<IP-адрес>/маска)[,...] – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25)
    - <маска>: краткий формат (CIDR), например: 24;
    - <маска>: полный формат, например: 255.255.255.0.
- **dstip6=<IPv6-адрес_приемника>** - список IPv6-адресов приемника пакета. Ожидаются:
  - ✔ any – любой IPv6-адрес источника (по умолчанию);
  - ✔ (<IPv6-адрес>[-<IPv6-адрес>] | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов (например: 2001:b08:3:123::67,2001:b08:3:123::100-2001:b08:3:123::1ff,2001:b08:3:123::/64)
    - <длина_префикса>: число бит префикса (CIDR), например: 64;
- **dstport=<порт_приемника>** - список TCP-портов или UDP-портов приемника. Ожидаются:
  - ✔ any – любой порт (по умолчанию);
  - ✔ (<num>[-<num>] | <name>)[,...] - список номеров и/или **символьных псевдонимов портов** (например: 22-25,110,80,https,postgresql);
- **dstobject=<сетевой_объект_приемника>** - список имен сетевых объектов приемника из справочника. Ожидаются:
  - ✔ none - параметр на задан (по умолчанию);
  - ✔ (<имя_объекта>)[,...] - список имен объектов из справочника (в списке допускается указание имён объектов следующих типов: *узел сети, сеть, группа сетевых объектов*);
- **dstservice=<сервис_приемника>** - список имен объектов типа *"service"* приемника из справочника. Ожидаются:
  - ✔ none - параметр не задан (по умолчанию);
  - ✔ (<имя_объекта>)[,...] - список имен объектов типа *"service"* из справочника;
- **dstresource=<ресурс_приемника>** - список имен объектов типа *"resource"* приемника из справочника. Ожидаются:
  - ✔ none - параметр на задан (по умолчанию);
  - ✔ (<имя_объекта>)[,...] - список имен объектов типа *"resource"* из справочника;
- **ipproto=<протокол_в_IP>** - протокол, инкапсулированный в IP. Ожидаются:
  - ✔ any – любой протокол (по умолчанию);
  - ✔ (<num>[-<num>] | <name>)[,...] - список имен и/или номеров протоколов в десятичном виде (например, 1,icmp,10-13,tcp,udp).
- **version=<версия_IP>** - версия протокола IP. Ожидаются:
  - ✔ any – любая версия (по умолчанию);
  - ✔ 4 — IPv4;

✔ 6 — IPv6;

- **icmp4=<тип_код_ICMPv4>** - тип и код ICMPv4-сообщения. Ожидаются:

✔ any — любые тип и код ICMPv4-сообщения (по умолчанию);

✔ (<тип>[/(<код>[-<код>] | any)])[,...] - список типов и кодов ICMPv4-сообщения;

◆ <тип> - десятичное число от 0 до 255;

◆ <код> - десятичное число от 0 до 255;

◆ any - любой код ICMPv4-сообщения;

- **icmp6=<тип_код_ICMPv6>** - тип и код ICMPv6-сообщения. Ожидаются:

✔ any — любые тип и код ICMPv6-сообщения (по умолчанию);

✔ (<тип>[/(<код>[-<код>] | any)])[,...] - список типов и кодов ICMPv6-сообщения;

◆ <тип> - десятичное число от 0 до 255;

◆ <код> - десятичное число от 0 до 255;

◆ any - любой код ICMPv6-сообщения;

- **ttl=<значение_ttl>** - значение поля TTL заголовка IPv4 или заголовка HopLimit IPv6. Ожидаются:

✔ any - любое значение поля TTL (по умолчанию);

✔ <num>[-<num>] - значение или диапазон значений поля TTL или заголовка HopLimit.

◆ <num> - десятичное число, допустимые значения: 0-255;

- **length=<длина>** - длина IP-пакета. Ожидаются:

✔ any - любая длина (по умолчанию);

✔ <num>[-<num>] - значение или диапазон значений длины IP-пакета;

◆ <num> - десятичное число, допустимые значения: 20-65535;

- **tos=<значение_TOS>** - значение битов TOS заголовка IPv4. Ожидаются:

✔ any - любые биты TOS (по умолчанию);

✔ <смещение/значение> - значение битов в двоичной форме по указанному смещению (от младших к старшим битам), например: 3/110, 0/11010001;

- **class=<класс_трафика>** - значение битов поля "Traffic Class" заголовка IPv6-пакета. Ожидаются:

✔ any – любая двоичная последовательность (по умолчанию);

✔ <значение> - значение класса трафика: шестнадцатеричное число, допустимые значения: 0x00-0xff.

- **fragment=<фрагментация>** - использование фрагментации в пакете. Ожидаются:

✔ any - правило применяется как к фрагментированным, так и к нефрагментированным пакетам (по умолчанию);

✔ enable - правило применяется только к фрагментированным пакетам;

✔ disable - правило применяется только к нефрагментированным пакетам;

- **hopbyhop=<наличие_доп_заголовка>** - наличие/отсутствие дополнительного заголовка *Hop-by-Hop Options* в IPv6 -пакете. Ожидаются:
  - ✔ any - дополнительный заголовок может как присутствовать, так и отсутствовать (значение по умолчанию);
  - ✔ enable - дополнительный заголовок должен присутствовать в пакете;
  - ✔ disable - дополнительный заголовок должен отсутствовать в пакете;
- **destination=<наличие_доп_заголовка>** - наличие/отсутствие дополнительного заголовка *Destination Options* в IPv6 -пакете. Ожидаются:
  - ✔ any - дополнительный заголовок может как присутствовать, так и отсутствовать (значение по умолчанию);
  - ✔ enable - дополнительный заголовок должен присутствовать в пакете;
  - ✔ disable - дополнительный заголовок должен отсутствовать в пакете;
- **routing=<наличие_доп_заголовка>** - наличие/отсутствие дополнительного заголовка *Routing* в IPv6 -пакете. Ожидаются:
  - ✔ any - дополнительный заголовок может как присутствовать, так и отсутствовать (значение по умолчанию);
  - ✔ enable - дополнительный заголовок должен присутствовать в пакете;
  - ✔ disable - дополнительный заголовок должен отсутствовать в пакете;
- **ah=<наличие_доп_заголовка>** - наличие/отсутствие дополнительного заголовка *Authentication Header (AH)* в IPv6 -пакете. Ожидаются:
  - ✔ any - дополнительный заголовок может как присутствовать, так и отсутствовать (значение по умолчанию);
  - ✔ enable - дополнительный заголовок должен присутствовать в пакете;
  - ✔ disable - дополнительный заголовок должен отсутствовать в пакете;
- **esp=<наличие_доп_заголовка>** - наличие/отсутствие дополнительного заголовка *Encapsulating Security Payload (ESP)* в IPv6 -пакете. Ожидаются:
  - ✔ any - дополнительный заголовок может как присутствовать, так и отсутствовать (значение по умолчанию);
  - ✔ enable - дополнительный заголовок должен присутствовать в пакете;
  - ✔ disable - дополнительный заголовок должен отсутствовать в пакете;
- **vlan=<идентификатор_vlan>** - параметр использования VLAN. Ожидаются:
  - ✔ any – любой фрейм Ethernet (с тэгом IEEE 802.1q или без него - по умолчанию);
  - ✔ enable – только фреймы Ethernet с тегом IEEE 802.1q;
  - ✔ disable – только фреймы Ethernet без тега IEEE 802.1q;
  - ✔ (<num>[-<num>])[,...] - список идентификаторов и диапазонов идентификаторов VLAN; объекту будут сопоставлены фреймы Ethernet, содержащие идентификатор VLAN из

списка:

- ◆ <num> - десятичное число от 0 до 4095;

✔ <имя_группы_vlan> - имя группы VLAN из справочника. Правило будет действовать только для фреймов Ethernet, содержащих идентификаторы VLAN, указанные в группе.

- **time=<интервал_времени>** - интервал времени, в течение которого действует правило. Ожидается:

✔ none – правило действует всё время (по умолчанию);

✔ (<имя_объекта>)[,...] - список имён интервалов времени из справочника;

- **session=<создание_сессии>** - создание сессии на основе пакетов, обработанных данным правилом. Ожидаются:

✔ enable - создавать сессии по пакетам, обработанным данным правилом (по умолчанию);

✔ disable - не создавать сессии по пакетам, обработанным данным правилом;

- **timeout=<таймаут_сессии>** - таймаут неактивности для сессий, созданных по данному правилу (для состояния *ESTABLISHED*). Ожидаются:

✔ default - использовать значения по умолчанию для таймаутов сессий (по умолчанию);

✔ <num> - значение таймаута в секундах:

- ◆ Допустимые значения <num>: 0-2147483647;
- ◆ Значение 0 (ноль) означает бесконечный таймаут, т.е. такая сессия может быть удалена только после ее корректного завершения взаимодействующими сторонами;

- **sesbreak=<разрыв_сессии>** - корректность обработки TCP-сессии при сбросе инициирующего SYN-пакета (в случае, если действие правила - *drop*), а также при разрыве установившейся TCP-сессии. Ожидаются:

✔ silent - сессия разрывается без уведомления взаимодействующих сторон (по умолчанию);

✔ verbose - сессия разрывается с уведомлением взаимодействующих сторон TCP-сегментами с установленным флагом *RESET*;

- **apr=<список_прикладных_правил>** - список номеров прикладных правил, привязанных к данному общему правилу. Ожидаются:

✔ no - пакеты не будут обрабатываться на прикладном уровне (по умолчанию);

✔ yes - пакеты будут обрабатываться на прикладном уровне;

✔ (<номер> | <номер>-<номер>)[,...] - список номеров и/или диапазонов номеров прикладных правил; данные правила должны быть определены в таблице прикладных правил (например: 10,20,30-50,80);

- **alarm=<сигнализация>** - параметр сигнализации. Ожидаются следующие ключевые слова:

✔ enable – послать сообщение сигнализации о прохождении пакета;

✔ disable – не посылать сообщение сигнализации (по умолчанию);

- **active=<активность>** - активность правила. Ожидаются:
  - ✔ enable – правило активно (по умолчанию);
  - ✔ disable – правило неактивно;
- **log=<регистрация>** - параметр регистрации. Ожидаются:
  - ✔ enable – регистрировать пакеты, обработанные правилом, и сессии, созданные по правилу;
  - ✔ disable – не регистрировать пакеты и сессии (по умолчанию);
  - ✔ packet - регистрировать пакеты, обработанные правилом;
  - ✔ session - регистрировать сессии, созданные по правилу;
- **comment=<комментарий>** - строка комментария:
  - ✔ Длина: от 0 до 200 символов;
  - ✔ Допустимы любые печатаемые символы.

При редактировании **глобального общего правила (rule:0)** допустимыми являются параметры:
- action=<действие>;
- log=<регистрация>;
- session=<создание_сессии>;
- timeout=<таймаут_сессии>;
- sesbreak=<разрыв_сессии>;
- comment=<комментарий>.

Для глобального общего правила **(rule:0)** допустимы следующие значения параметра **action** (действие правила):
- accept;
- drop;
- deny

Для правила, предписывающего удаление пакета (**action=drop** или **action=deny**), значения выходных интерфейсов (параметр **dstif**) не учитывается.

Параметр **length** общего правила должен содержать суммарную длину пакета, включая длину IP-заголовка. Это относится как к IPv4-пакетам, так и к IPv6-пакетам. Минимальное значение параметра **length** – 20, т. к. длина заголовка IPv4-пакета – 20 Байт.

Если параметр **ipproto** имеет значение **any** (по умолчанию) и, при этом, в правиле заданы значениями отличными от **any** следующие параметры:
- **srcport** и/или **dstport**, то правило будет применено к TCP-сегментам и UDP-дейтаграммам с указанными портами;
- **icmp4**, то правило будет применено к ICMPv4-сообщениям с указанным типом и кодами;
- **icmp6**, то правило будет применено к ICMPv6-сообщениям с указанным типом и кодами.

То есть указание в правиле параметров, приведенных выше, при **ipproto** в значении **any**, ограничивает протоколы, инкапсулированные в IP, для которых будет применено данное правило протоколами, соответствующими указанным параметрам. Таким образом правило **не будет** применено к IP-пакетам с **любыми** протоколами, инкапсулированными в IP.

Д.1.1. Конфликты значений параметров общего правила

Конфликт - недопустимая комбинация значений параметров правила.

Если в определении общего правила выявлен хотя бы один конфликт: оно не будет добавлено или изменено по команде администратора. Дополнительная политика доступа,

включающее в себя такое правило будет признана некорректной и не будет доступна для применения.

На определение общего правила накладываются следующие ограничения по использованию параметров правила, связанные с использованием объектов в правиле.

Если объект используется в правиле в качестве источника или приемника, то ряд параметров правила источника (приемника), а также общих параметров правила запрещено устанавливать в значения отличные от значений по умолчанию. В таблице Д.1, стр. 522 для каждого типа объекта приводится перечень запрещенных к установке параметров правила.

Таблица Д.1: Конфликты совместного использования объектов справочника и параметров правила

Условный тип конфликта	***Тип объекта***	***Запрещенные к установке параметры правила***
1a	host	• **srcif** либо **dstif**; • **srcmac** либо **dstmac**; • **srcip4** либо **dstip4**; • **srcip6** либо **dstip6**
1b	net	• **srcif** либо **dstif**; • **srcip4** либо **dstip4**; • **srcip6** либо **dstip6**
1c	net-group	• **srcif** либо **dstif**; • **srcmac** либо **dstmac**; • **srcip4** либо **dstip4**; • **srcip6** либо **dstip6**
2	service	• **ipproto**; • **icmp4**; • **icmp6**; • **srcport** либо **dstport**
3	resource	• **srcif** либо **dstif**; • **srcmac** либо **dstmac**; • **srcip4** либо **dstip4**; • **srcip6** либо **dstip6;** • **ipproto**; • **icmp4**; • **icmp6**; • **srcport либо dstport**

Кроме того, в общем правиле запрещено использование определённых комбинаций объектов справочника. Имеются ограничения на совместное использование объектов **service** и **resource** (таблица Д.2, стр. 522).

Таблица Д.2: Конфликты совместного использования объектов service и resource

Номер комбинации	***Источник***	***Применик***
1	service	service
2	service	resource
3	resource	service
4	resource	resource

Если в правиле в качестве источника (приемника) указан объект **resource**, то запрещается указание в качестве источника (приемника) соответственно объектов следующих типов: **host**, **net**, **net-group**, **service**. Все остальные комбинации объектов разрешены к использованию в общих правилах.

Д.1.2. Конфликты по адресам IPv4, IPv6, MAC

Конфликт по адресам - это запрещенная комбинация значений адресных параметров для двух сторон взаимодействия.

Адресные параметры каждой стороны взаимодействия (источник либо приемник) могут быть заданы через сетевые объекты справочника (host, net, net-group) либо через адресные параметры правила (для источника: srcmac, srcip4, srcip6, для приемника: dstmac, dstip4, dstip6). Т. о. **конфликты по адресам** в общем правиле возможны, если параметр **version** (версия протокола IP) общего правила имеет значение отличное от *“any”* и в правиле используется одна из следующих комбинаций определения источника и приемника:

- источник: сетевой объект - приемник: адресные параметры правила;
- источник: адресные параметры правила - приемник: сетевой объект;
- источник: сетевой объект - приемник: сетевой объект.

При анализе конфликтов по адресам в общем правиле рассматривается каждая взаимодействующая пара приемника и источника. Например, если в правиле определено три объекта *host* в качестве источника (A,B,C) и два *host* в качестве приемника (D,E), то на конфликты будут проверено шесть пар: A и D, A и E, B и D, B и E, C и D, C и E. Если в качестве источника или приемника в правиле указан объект *net-group*, то в проверке на конфликты по адресам будут участвовать объекты *host* и/или *net*, входящие в его состав.

Объекты *host* и *net* для IPv4 и IPv6 адресов допускают значение *"none"* (отсутствие адреса соответствующей версии протокола IP).

В случае если для одной из сторон взаимодействия правила для IPv4 или IPv6 адресов указано значение "none" - то это конфликт по данному типу адресов: IPv4 или IPv6.

Если для взаимодействующей пары имеется конфликт как по IPv4-адресам, так и по IPv6-адресам, и при этом MAC-адрес источника и приемника имеет значение *"any"*, то это значит, что для данной взаимодействующей пары имеет место **неразрешимый конфликт по адресам**.

Общее правило, описывающее взаимодействующую пару источник-приемник, для которой имеется **неразрешимый конфликт по адресам**, является **некорректным**, поэтому администратору будет **отказано**:

- в добавлении такого правила;
- в применении изменений в правиле, в результате которых возникает неразрешимый конфликт по адресам;'
- в применении дополнительной политики доступа, в которой содержится общее правило с неразрешимым конфликтом по адресам.

Если хотя бы по одному типу адресов (IPv4, IPv6, MAC) для взаимодействующей пары отсутствует конфликт, то имеющиеся конфликты по адресам остальных типов из числа IPv4, IPv6, MAC будут **автоматически (без участия администратора) разрешены** в соответствии с алгоритмом, представленным ниже. В этом случае имеет место **разрешимый конфликт по адресам**.

Алгоритм разрешения конфликтов по адресам IPv4, IPv6, MAC:

4) Проверяется наличие конфликтов:
   ✔ по IPv4-адресам;
   ✔ по IPv6-адерсам;
5) Если два конфликта (по IPv4 и IPv6 адресам, то - переход к п.3). Если конфликт - только по IPv6, то - переход к п.4, если по IPv4 - к п.5.
6) Проверяется наличие конфликта по MAC. Конфликта нет - переход к п.6. Конфликт есть - конфликт по всем типам адресов: IPv4, IPv6 и MAC. Конец.
7) Конфликт по IPv6. В правиле, созданном по взаимодействующей паре, значение параметра *version* меняется с *"any"* на *"4"*, кроме того, значение параметра *srcip6* (*dstip6)* устанавливается в *"any"*, т. к. IPv6-адрес объекта источника (приемника) имеет значение "none".
8) Конфликт по IPv4: изменение значения параметра version с "any" на "6" в правиле, созданном по взаимодействующей паре. В правиле, созданном по взаимодействующей паре, значение параметра *version* меняется с *"any"* на *"6"*, кроме того, значение параметра *srcip4* (*dstip4)* устанавливается в *"any"*, т. к. IPv4-адрес объекта источника (приемника) имеет значение "none". Конец.
9) Конфликт по IPv4 и по IPv6. В правиле, созданном по взаимодействующей паре, значение параметра *srcip4* либо *dstip4* устанавливается в "any", также значение *srcip6* либо *dstip6* устанавливается в "any" (т. к. в объекте соответствующей стороны взаимодействия IPv4 и/или IPv6 адрес имеет значение *“none”*). В правиле, созданном по взаимодействующей паре, значения параметров *srcmac* и *dstmac* копируются из соответствующих параметров сторон взаимодействия (источник - приемник), так как конфликт по ним отсутствует. Конец.

Общее правило, имеющее **разрешимый конфликт по адресам**, является корректным, поэтому администратору будет **позволено**:

- добавление такого правила;
- применение изменений в правиле, в результате которых возникает разрешимый конфликт по адресам;'
- применение политики доступа, в которой содержится правило с разрешимым конфликтом по адресам.

Д.1.3. Конфликты по остальным параметрам общего правила

- **Конфликты по параметру VLAN** (между объектами, между параметров правила и объектами) возникает, если не соблюдаются следующие условия:
  - ✔ Если в правиле параметр *vlan* имеет значение отличное от *"any"*, то соответствующий параметр *vlan* всех используемых сетевых объектов *host* и *net* (как используемых непосредственно, так и через объекты *net-group* и *resource*) должен быть в значении *"any"* (любой);
  - ✔ Если в правиле сетевые объекты *host* и *net* используются только в качестве источников (параметр *srcobject* или *srcresource*), или только в качестве приемников (параметр *dstobject* или *dstresource*), то в сетевых объектах допускаются различные значения параметра *vlan;*
  - ✔ Если в правиле сетевые объекты *host* и *net* используются и в качестве источников (параметр *srcobject* или *srcresource*) и в качестве приемников (параметр *dstobject* или *dstresource*), и параметр *vlan* задан (не равен *"any"*) как для источника, так и для приемника, то для каждой пары объектов: источник-приемник значения параметра *vlan* должны быть идентичны. Если параметр *vlan* задан для объекта-источника и не задан (*"any"*) для объекта-приемника, либо наоборот, то такая комбинация является допустимой, и при, пакетной фильтрации, в правиле для данной пары объектов будет использовано значение параметра *vlan* из объекта, в котором оно задано.
- **Конфликт транспортного протокола и портов источника/приемника** возникает, если не соблюдается следующее условие:
  - ✔ Если в правиле значение параметра *ipproto* отлично от *"any"* и не включает в себя ни TCP, ни UDP, то параметры *srcport* и *dstport* должны быть в значении "any";
- **Конфликт транспортного протокола и параметра типов и кодов ICMP** возникает, если не соблюдаются следующие условия:
  - ✔ Если в правиле значение параметра *ipproto* отлично от *"any"* и не включает в себя ICMP, то параметр *icmp4* должен быть в значении *"any";*
  - ✔ Если в правиле значение параметра *ipproto* отлично от *"any"* и не включает в себя ICMP6, то параметр *icmp6* должен быть в значении *"any"*.

- **Конфликт версии протокола IP и версии протокола ICMP** возникает, если не соблюдаются следующие условия:
  - ✔ Если в правиле значение параметра *version* равно 4, то *ipproto* не должен включать в себя ICMPv6;
  - ✔ Если в правиле значение параметра *version* равно 4, то параметр *protocol* всех используемых в правиле объектов типа *service* не должен быть равен ICMP6;
  - ✔ Если в правиле значение параметра *version* равно 4, то параметр *icmp6* должен быть в значении "any";
  - ✔ Если в правиле значение параметра *version* равно 4, то параметр *icmp6* всех используемых в правиле объектов типа *service* должен быть в значении *"any";*
  - ✔ Если в правиле значение параметра *version* равно 6, то *ipproto* не должен включать в себя ICMP (ICMPv4);
  - ✔ Если в правиле значение параметра *version* равно 6, то параметр *protocol* всех используемых в правиле объектов типа *service* не должен быть равен ICMP (ICMP4);
  - ✔ Если в правиле значение параметра *version* равно 6, то параметр *icmp4* должен быть в значении *"any";*
  - ✔ Если в правиле значение параметра *version* равно 6, то параметр *icmp4* всех используемых в правиле объектов типа *service* должен быть в значении *"any"*.
- **Конфликт версии протокола IP и параметров IP** (установленные параметры правила не соответствуют версии протокола IP) возникает, если не соблюдаются следующие условия:
  - ✔ Если в правиле значение параметра *version* равно 4, то следующие параметры (IPv6) должны быть в значении *"any"*:
    - class;
    - hopbyhop;
    - destination;
    - routing;
    - ah;
    - esp.
  - ✔ Если в правиле значение параметра *version* равно 6, то параметр *tos* должны быть в значении *"any"*;
- **Конфликт типа кадра Ethernet и кодов протоколов, инкапсулированных в кадр Ethernet** возникает, если не соблюдается следующее условие:
  - ✔ Если в правиле параметр *frame* имеет значение отличное от *"eth2"*, *"llc"* или *"snap"*, то параметр *ethproto* должен быть в значении *"any"*.

Д.2. Определение AP-правила

```
ap:<номер> action=<действие> [protocol=<протокол_прикладного_уровня>]
[data=<текстовые_данные>] [olv=<двоичные_данные>] [case=<регистр>]
[direction=<направление>][ipproto=<протокол_в_IP>][ipcl4=<IPv4-адрес_клиента>]
[ipcl6=<IPv6-адрес_клиента>] [portcl=<порт_клиента>][ipsrv4=<IPv4-
адрес_сервера>] [ipsrv6=<IPv6-адрес_сервера>] [portsrv=<порт_сервера>]
[alarm=<сигнализация>] [active=<активность>] [log=<регистрация>]
[comment=<комментарий>]
```

Где:

- **<номер>** - номер прикладного правила. Допустимые значения: 1-65535 (Номер 0 используется для глобального AP-правила);
- **action=<действие>** - действие правила. Ожидаются:
  - ✔ accept – передача пакета на выходной интерфейс;
  - ✔ drop – удаление пакета;
- **protocol=<протокол_прикладного_уровня>** - идентификатор прикладного протокола. Ожидаются:
  - ✔ any – любой протокол (значение по умолчанию);
  - ✔ <name> – имя прикладного протокола;
  - ✔ <num> – номер прикладного протокола, соответствующий номеру TCP/UDP-порта для данного протокола;
- **data=<текстовые_данные>** - последовательность печатных символов. Ожидаются:
  - ✔ пустая строка (нет значения) – любая текстовая последовательность (по умолчанию);
  - ✔ <symbols>[,<symbols>] - список текстовых последовательностей (например: John_Smith,Oleg_Popov);
- **olv=<двоичные_данные>** - последовательность двоичных данных по указанному смещению. Ожидаются:
  - ✔ any – любая двоичная последовательность (по умолчанию);
  - ✔ <смещение>/<длина>/<значение>:
    - ◆ <значение> - двоичная последовательность в шестнадцатеричном виде
    - ◆ <длина> - длина двоичная последовательности в байтах;
    - ◆ <смещение>- смещение относительно начала прикладных данных в байтах (может принимать значение *any*, в этом случае указанные двоичные данные ищутся на всей длине прикладных данных пакета)

Например: 12/3/0xac16d3, т.е. будет произведен поиск двоичных данных 0xac16d3, длиной 3 байта по смещению 12 байт от начала прикладных данных пакета).

- **case=<регистр>** - регистр символов в текстовых данных (параметр *data)*. Ожидаются:
  - ✔ any – регистр не учитывается (по умолчанию);
  - ✔ upper – только символы в верхнем регистре;

✔ lower – только символы в нижнем регистре;

✔ sensitive – регистр учитывается (будет произведен поиска строки в том регистре, в котором строка указана в правиле);

- **direction=<направление>** - направление потока, в котором производится поиск. Ожидаются:

✔ any – правило применяется к обоим потокам – от клиента к серверу и от сервера к клиенту (по умолчанию);

✔ from-server: правило применяется только к потоку от сервера к клиенту;

✔ from-client: правило применяется только к потоку от клиента к серверу;

- **ipcl4=<IPv4-адрес_клиента>** - IP-адрес клиента. Ожидаются:

✔ any – любой IP-адрес клиента (по умолчанию);

✔ (<IP-адрес>[-<IP-адрес>] | <IP-адрес>/маска)[,...] – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);

- **ipcl6=<IPv6-адрес_клиента>** - IPv6-адрес клиента. Ожидаются:

✔ any – любой IPv6-адрес клиента (по умолчанию);

✔ (<IPv6-адрес>[-<IPv6-адрес>] | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов (например: 2001:b08:3:123::67,2001:b08:3:123::100-2001:b08:3:123::1ff,2001:b08:3:123::/64)

- **portcl=<порт_клиента>** - TCP-порт или UDP-порт клиента. Ожидаются:

✔ any – любой порт клиента (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] – список номеров портов и/или символьных псевдонимов портов клиента (например: 22-25,110,80,https,postgresql);

- **ipsrv4=<IPv4-адрес_сервера>** - IP-адрес сервера. Ожидаются:

✔ any – любой IP-адрес сервера (по умолчанию);

✔ (<IP-адрес>[-<IP-адрес>] | <IP-адрес>/маска)[,...] – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);

- **ipsrv6=<IPv6_адрес_назначения>** - список IPv6-адресов назначения пакета. Ожидаются:

✔ any – любой IPv6-адрес сервера (по умолчанию);

✔ (<IPv6-адрес>[-<IPv6-адрес>] | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов (например: 2001:b08:3:123::67,2001:b08:3:123::100-2001:b08:3:123::1ff,2001:b08:3:123::/64);

- **portsrv=<порт_сервера>** - TCP-порт или UDP-порт сервера. Ожидаются:

✔ any – любой порт сервера (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] - список номеров портов и/или символьных псевдонимов портов сервера (например: 22-25,110,80,https,postgresql);

- **ipproto=<протокол_в_IP>** - протокол, инкапсулированный в IP. Ожидаются:

✔ any – любой протокол (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] - список имен и/или номеров протоколов в десятичном виде (например: 1,icmp,10-13,tcp,udp).

- **alarm=<сигнализация>** - параметр сигнализации. Ожидаются:
  - ✔ enable – послать сообщение сигнализации о прохождении пакета;
  - ✔ disable – не посылать сообщение сигнализации (по умолчанию);
- **active=<активность>** - активность правила. Ожидаются следующие ключевые слова:
  - ✔ enable – правило активно (по умолчанию);
  - ✔ disable – правило неактивно;
- **log=<регистрация>** - параметр регистрации. Ожидаются следующие ключевые слова:
  - ✔ enable – регистрировать пакеты и сессии, обработанные по данному правилу;
  - ✔ disable – не регистрировать пакеты и сессии, обработанные по данному правилу (по умолчанию);
  - ✔ packet – регистрировать пакеты, обработанные по данному правилу;
  - ✔ session – регистрировать сессии, обработанные по данному правилу;
- **comment=<комментарий>** - строка комментария:
  - ✔ Длина: от 0 до 200 символов;
  - ✔ Допустимы любые печатаемые символы;
  - ✔ Комментарий, содержащий пробелы, должен заключаться в двойные кавычки.

При редактировании **глобального АР-правила (ар:0)** допустимыми являются параметры:
- action=<действие>;
- log=<регистрация>;
- comment=<комментарий>.

При редактировании АР-правила **н**е допускается изменения значения параметра **protocol**, поскольку от его значения зависит перечень допустимых дополнительных параметров, относящихся к определенному прикладному протоколу.

Если строка значения параметра:
- data;
- hostname (protocol=http или protocol=domain);
- file (protocol=http или protocol=ftp);
- user (protocol=ftp);
- password (protocol=ftp);
- query (protocol=sql)

содержит символы **“пробел”**, то в командном интерфейсе администратора МЭ ССПТ-4А1 такая строка должна быть заключена в двойные кавычки, например: **data=”abc def ghi”**

В значениях следующих параметров АР-правил:
- data;
- hostname (protocol=http или protocol=domain);
- file (protocol=http или protocol=ftp);
- user (protocol=ftp);
- password (protocol=ftp);
- from (protocol=smtp);
- to (protocol=smtp);
- query (protocol=sql)

допускается использование следующих **специальных символов**, обеспечивающих более гибкий поиск текстовых последовательностей:
- **'*'**: замещение 0 или более символов (любая комбинация символов, в т.ч. отсутствие символов)
- **'?'**: замещение ровно одного символа (один любой символ)
- **'+'**: замещение 1 или более символов
- **'^'**: начало прикладных данных;
- **'$'**: конец прикладных данных;
- **','**: разделитель для списка значений (прикладные данные должен удовлетворять хотя бы одному из значений в списке);
- **'\':** символ экранирования (указывает не рассматривать следующий за ним символ как специальный)**.**

В значениях следующих параметров АР-правил:
- data;
- hostname (protocol=http или protocol=domain);
- file (protocol=http или protocol=ftp);
- user (protocol=ftp);
- password (protocol=ftp);
- from (protocol=smtp);
- to (protocol=smtp);
- query (protocol=sql)

если необходимо **точное совпадение** значения параметра с соответствующей строкой в сообщении прикладного протокола, то необходимо искомую строку заключать между парой символов: **^** и **$**.
Например: *user=^tester$*, *from=^support@somedomain.org$* и т.п.

В противном случае будет проверяться вхождение указанной строки в соответствующую строку в сообщении прикладного протокола и, следовательно, могут быть удалены/пропущены лишние пакеты.

Параметр **case** (регистр символов в текстовых данных) применяется для следующих параметров АР-правила, относящихся к поиску текстовых строк в сообщениях прикладных протоколов:
- file (protocol=http и protocol=ftp);
- hostname (protocol=http или protocol=domain);
- from (protocol=smtp);
- to (protocol=smtp);
- user (protocol=ftp);
- password (protocol=ftp);
- query (protocol=sql);
- data (независимо от значения protocol);

Если параметр **ipproto** имеет значение **any** (по умолчанию) и, при этом, в правиле заданы значениями отличными от **any** параметры: **portcl** и/или **portsrv**, то правило будет применено только к TCP-сегментам и UDP-дейтаграммам и только с указанными портами.

То есть указание в правиле параметров, приведенных выше, при **ipproto** в значении **any**, ограничивает протоколы, инкапсулированные в IP, для которых будет применено данное правило протоколами TCP и UDP. Таким образом правило **не будет** применено к IP-пакетам с **любыми** протоколами, инкапсулированными в IP.

Д.2.1. Дополнительные параметры АР-правила для протокола HTTP (protocol=http)

```
[hostname=<имя_сервера>] [domain-group=<имя_группы>] [method=<http_метод>]
[file=<имя_файла>] [begin=<начало_поиска_двоичных_данных>]
```

Где:

- **hostname=<доменное_имя>** - доменные имена WEB-сайтов. Ожидаются:
  - ✔ пустая строка (нет значения) – любой WEB-сайт (по умолчанию);
  - ✔ <name>[,<name>] - список имён или фрагментов доменных имен WEB-сайтов (например: *fee.ru,*hotmail.com*)
- **domain-group=<имя_группы>** - имя группы доменных имен из справочника. Ожидаются:
  - ✔ none – нет значения (по умолчанию);
  - ✔ <name> - имя группы доменных имен из справочника;
- **method=<HTTP_метод>** - идентификаторы методов запроса к HTTP-серверу. Ожидаются:
  - ✔ (<HTTP_метод>)[,...] - список методов HTTP, где <HTTP-метод>:
    - any – любой метод запроса (по умолчанию);
    - get – метод GET;
    - put – метод PUT;
    - post – метод POST;
    - head – метод HEAD;
    - delete – метод DELETE;
    - options – метод OPTIONS;
    - patch – метод PATCH;
    - link – метод LINK;
    - unlink – метод UNLINK.
- **file=<имя_файла>** - имена файлов, запрашиваемых у WEB-сайта. Ожидаются:
  - ✔ пустая строка (нет значения) – любой файл (по умолчанию);
  - ✔ <name>[,<name>] - список имен или фрагментов имен файлов (например: *index.html,*.pdf,instuction.**);
- **begin=<начало_поиска_двоичных_данных>** - указывает точку отсчёта смещения для поиска последовательности двоичных данных (параметр *olv*). Ожидаются:
  - ✔ header – поиск будет производиться от начала заголовка HTTP-сообщения (по умолчанию);
  - ✔ body – поиск будет производиться от начала тела HTTP-сообщения (заголовок не учитывается).

Если в АР-правиле для протокола HTTP оба параметра: **hostname** и **domain-group** имеют значения отличные от значений по умолчанию, то при фильтрации будет использоваться список доменных имен, являющийся объединением значений этих параметров.

Логическая связь параметра **file** с параметром **method** АР-правила для протокола HTTP:

- Если параметр **method** в АР-правиле для HTTP не задан, а **file** задан, то на соответствие параметру **file** будут проверяться HTTP-запросы со всеми поддерживаемыми методами (см. описание параметра **method**).
- Если параметр **method** задан, то только HTTP-запросы с методами указанными в данном параметре.

Параметр **file** по умолчанию подразумевает указание пути к файлу (в HTTP-запросе, как правило, указывается путь к файлу с символами “/”). Если необходимо, чтобы АР-правило для HTTP срабатывало на конкретное имя файла, безотносительно пути к этому файлу, то следует указывать значение параметра **file** следующим образом:
`file=/filename$`, где:

- filename – пример имени файла;
- / – подразумевает последний символ “/” в пути к файлу, таким образом не допускаются символы до filename в имени файла;
- $ – задает, что поиск будет осуществляться в конце строки, т. е. после filename не допускается символов в имени файла.

Д.2.2. Дополнительные параметры АР-правила для протокола FTP (protocol=ftp)

```
[command=<команда>] [file=<имя_файла>] [user=<имя_пользователя>]
[password=<пароль>]
```

Где:

- **command=<команда>** - команда клиента протокола FTP. Ожидаются:
  - ✔ (<команда>)[,...] - список команд клиента протокола FTP, где <команда>:
    - any – любая команда (по умолчанию);
    - put - команда пересылки файла на FTP-сервер;
    - get - команда пересылки файла с FTP-сервера;
    - list - команда вывода содержимого каталога FTP-сервера;
- **file=<имя_файла>** - имена файлов, передаваемых между FTP-клиентом и FTP-сервером. Ожидаются:
  - ✔ пустая строка (нет значения) – любой файл (по умолчанию);
  - ✔ (<имя_файла>)[,...] - список имен или фрагментов имен файлов (например: document1.doc,*.zip,crack.*);
- **user=<имя_пользователя>** - имена пользователей, предъявляемые при доступе к FTP-серверу. Ожидаются:
  - ✔ пустая строка (нет значения) – любое имя пользователя (по умолчанию);
  - ✔ <имя_пользователя>[,...] - список имен или фрагментов имен пользователей (например andr,swb,anonymous,Alexander*);
- **password=<пароль>** - пароли пользователей, предъявляемые при доступе к FTP-серверу. Ожидаются:
  - ✔ пустая строка (нет значения) – любой пароль (по умолчанию);
  - ✔ (<пароль>)[,...] - список паролей или фрагментов паролей (например qwerty,*arm).

Д.2.3. Дополнительные параметры АР-правила для протокола SMTP (protocol=smtp)

```
[from=<отправитель>] [to=<получатель>]
```

Где:

- **from=<отправитель>** - почтовые адреса отправителей. Ожидаются:
  - ✔ пустая строка (нет значения) – любой e-mail адрес (по умолчанию);
  - ✔ (<email>)[,...] - список email-адресов или фрагментов адресов отправителей (например: abc@fee.ru,*@hotmail.com);
- **to=<получатель>** - почтовые адреса получателей. Ожидаются:
  - ✔ пустая строка (нет значения) – любой e-mail адрес (по умолчанию);
  - ✔ <email>[,...] - список email-адресов или фрагментов адресов получателей (например: abc@fee.ru,*@hotmail.com).

Д.2.4. Дополнительные параметры АР-правила для SQL-сервисов (protocol=sql)

```
[query=<sql_запрос>]
```

Где:

- **query=<sql_запрос>** – SQL-запрос или его фрагмент. Ожидаются:
  - ✔ пустая строка (нет значения) – любой запрос (по умолчанию);
  - ✔ (<запрос>)[,...] - список SQL-запросов и/или фрагментов SQL-запросов (например update_table_set_cl_id=*,select_*_from_table).

Если в АР-правиле для SQL-сервисов **(protocol=sql)** параметр **portsrv** (порты сервера) АР-правила не определен (имеет значение по умолчанию - "any"), то на соответствие такому АР-правилу проверяются пакеты следующих SQL-сервисов:

- Oracle SQL*NET (порт 66);
- SQL Services (порт 118);
- SQL Net (порт 150);
- SQL Service (порт 156);
- Microsoft-SQL-Server (порт 1433);
- Microsoft-SQL-Monitor (порт 1434);
- Watcom SQL (порт 1498);
- MySQL (порт 3306);
- PostgreSQL Database (порт 5432).

Для фильтрации пакетов конкретных SQL-сервисов в АР-правиле дополнительно необходимо определить параметр **portsrv** серверными портами данных SQL-сервисов, например: **portsrv=66,5432**

Д.2.5. Дополнительные параметры АР-правила для протокола DNS (protocol=dns либо protocol=domain)

```
[hostname=<доменное_имя>]
[domain-group=<имя_группы>]
```

Где:

- **hostname=<доменное_имя>** - запрашиваемое доменное имя. Ожидаются:
  - ✔ пустая строка (нет значения) – любое имя (по умолчанию);
  - ✔ (<доменное_имя>)[,...] - список доменных имён или фрагментов доменных имен (например: fee.ru,*hotmail.com);
- **domain-group=<имя_группы>** – имя группы доменных имен из справочника. Ожидаются:
  - ✔ none – нет значения (по умолчанию);
  - ✔ <name> - имя группы доменных имен из справочника;

Если в АР-правиле для протокола DNS оба параметра: **hostname** и **domain-group** имеют значения отличные от значений по умолчанию, то при фильтрации будет использоваться список доменных имен, являющийся объединением значений этих параметров.

Для фильтрации доменных имен в DNS-сообщениях (запросах и ответах) использование параметра **data** АР-правила не применимо, поскольку DNS-сообщения имеют двоичный, а не текстовый формат. Для решения данной задачи следует пользоваться параметром **hostname** и/или **domain-group**.

Д.3. Определение TMP-правила

```
tmp:<номер> srcif=<входной_интерфейс> ([srcip4=<IPv4-адрес_источника>]
[dstip4=<IPv4-адрес_приемника>] | [srcip6=<IPv6-адрес_источника>]
[dstip6=<IPv6-адрес_приемника>])[srcport=<порт_источника>]
[dstport=<порт_назначения>] [ipproto=<протокол_в_IP>] [log=<регистрация>]
[alarm=<сигнализация>] [time=<время_жизни>] [comment=<комментарий>]
```

Где:

- **<номер>** - номер TMP-правила. Допустимые значения: 1-65535;
- **srcif=<входной_интерфейс>** - входной интерфейс. Ожидаются:
  - ✔ (<имя_интерфейса> | <номер_интерфейса>)[,...] – список номеров и/или символических имен интерфейсов;
- **srcip4=<IPv4-адрес_источника>** - IP-адрес источника пакета. Ожидаются:
  - ✔ any – любой IP-адрес источника (по умолчанию);
  - ✔ (<IP-адрес>[-<IP-адрес>] | <IP-адрес>/маска)[,...] – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);
- **srcip6=<IPv6-адрес_источника>** - IPv6-адрес источника пакета. Ожидаются:
  - ✔ any – любой IPv6-адрес источника (по умолчанию);
  - ✔ (<IPv6-адрес>[-<IPv6-адрес>] | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов (например: 2001:b08:3:123::67,2001:b08:3:123::100-2001:b08:3:123::1ff,2001:b08:3:123::/64);
- **srcport=<порт_источника>** - TCP-порт или UDP-порт источника. Ожидаются:
  - ✔ any – любой порт источника (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] - список номеров и/или **символьных псевдонимов** портов источника (например, 22-25,110,80,https,postgresql);

- **dstip4=<IPv4-адрес_приемника>** - IP-адрес приемника пакета. Ожидаются:

✔ any – любой IP-адрес приемника (по умолчанию);

✔ (<IP-адрес>[-<IP-адрес>] | <IP-адрес>/маска)[,...] – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);

- **dstip6=<IPv6-адрес_приемника>** - список IPv6-адресов приемника пакета. Ожидаются:

✔ any – любой IPv6-адрес (по умолчанию);

✔ (<IPv6-адрес>[-<IPv6-адрес>] | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов (например: 2001:b08:3:123::67,2001:b08:3:123::100-2001:b08:3:123::1ff,2001:b08:3:123::/64);

- **dstport**=<порт_приемника> - TCP-порт или UDP-порт приемника. Ожидаются:

✔ any – любой порт приемника (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] - список номеров и/или **символьных псевдонимов** портов приемника (например, 22-25,110,80,https,postgresql);

- **ipproto**=<протокол_в_IP> - протокол, инкапсулированный в IP. Ожидаются:

✔ any – любой протокол (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] - список имен и/или номеров протоколов в десятичном виде (например, 1,icmp,10-13,tcp,udp);

- **log=<регистрация>** - параметр регистрации. Ожидаются:

✔ enable – регистрировать пакет, обработанный правилом;

✔ disable – не регистрировать пакет, обработанный правилом (по умолчанию);

- **alarm=<сигнализация>** - параметр сигнализации. Ожидаются:

✔ enable – послать сообщение сигнализации о прохождении пакета;

✔ disable – не посылать сообщение сигнализации (по умолчанию);

- **time=<время_жизни>** - время жизни правила в секундах:

✔ Допустимые значения: 60-31536000;

✔ Значение по умолчанию: 3600;

- **comment=<комментарий>** - строка комментария:

✔ Длина: от 0 до 200 символов;

✔ Допустимы любые печатаемые символы.

При добавлении TMP-правила параметр **srcif=<входной_инетрфейс>** должен иметь значение отличное от **“any”**, кроме того хотя бы один из следующих параметров должен также иметь значение отличное от **"any"**:

- srcip4;
- dstip4;
- srcip6;
- dstip6;
- srcport;
- dstport.

Если параметр **ipproto** имеет значение **any** (по умолчанию) и, при этом, в правиле заданы значениями отличными от **any** параметры: **srcport** и/или **dstport**, то правило будет применено только к TCP-сегментам и UDP-дейтаграммам и только с указанными портами.

То есть указание в правиле параметров, приведенных выше, при **ipproto** в значении **any**, ограничивает протоколы, инкапсулированные в IP, для которых будет применено данное правило протоколами TCP и UDP. Таким образом правило **не будет** применено к IP-пакетам с **любыми** протоколами, инкапсулированными в IP.

В отличие от **общего правила** и **AP-правила** в **TMP-правиле** не допускается одновременное использование IPv4-адресов и IPv6-адресов.
Т.е. в **TMP-правиле** не допускается, чтобы параметры **srcip4 (dstip4)** и **srcip6 (dstip6)** одновременно были в значениях отличных от **"any"**.

Д.4. Определение PRI-правила (правила приоритизации)

```
pri:<номер> priority=<приоритет> srcif=<входной_интерфейс> ([srcip4=<IPv4-
адрес_источника>] [dstip4=<IPv4-адрес_приемника>] | [srcip6=<IPv6-
адрес_источника>] [dstip6=<IPv6-адрес_приемника>])[srcport=<порт_источника>]
[dstport=<порт_назначения>] [ipproto=<протокол_в_IP>] [comment=<комментарий>]
```

Где:

- **<номер>** - номер PRI-правила. Допустимые значения: 1-65535;
- **srcif=<входной_интерфейс>** - входной интерфейс. Ожидаются:
  - ✔ (<имя_интерфейса> | <номер_интерфейса>)[,...] – список номеров и/или символических имен интерфейсов;
- **srcip4=<IPv4-адрес_источника>** - IP-адрес источника пакета. Ожидаются:
  - ✔ any – любой IP-адрес источника (по умолчанию);
  - ✔ (<IP-адрес>[-<IP-адрес>] | <IP-адрес>/маска)[,...] – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);
- **srcip6=<IPv6-адрес_источника>** - IPv6-адрес источника пакета. Ожидаются:
  - ✔ any – любой IPv6-адрес источника (по умолчанию);
  - ✔ (<IPv6-адрес>[-<IPv6-адрес>] | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов (например: 2001:b08:3:123::67,2001:b08:3:123::100-2001:b08:3:123::1ff,2001:b08:3:123::/64);
- **srcport=<порт_источника>** - TCP-порт или UDP-порт источника. Ожидаются:
  - ✔ any – любой порт источника (по умолчанию);
  - ✔ (<num>[-<num>] | <name>)[,...] - список номеров и/или **символьных псевдонимов** портов источника (например, 22-25,110,80,https,postgresql);
- **dstip4=<IPv4-адрес_приемника>** - IP-адрес приемника пакета. Ожидаются:
  - ✔ any – любой IP-адрес приемника (по умолчанию);
  - ✔ (<IP-адрес>[-<IP-адрес>] | <IP-адрес>/маска)[,...] – список IP-адресов (например: 192.168.10.1,192.168.10.10-192.168.10.20,192.168.10.32/255.255.255.224,192.168.10.128/25);
- **dstip6=<IPv6-адрес_приемника>** - список IPv6-адресов приемника пакета. Ожидаются:

✔ any – любой IPv6-адрес (по умолчанию);

✔ (<IPv6-адрес>[-<IPv6-адрес>] | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов (например: 2001:b08:3:123::67,2001:b08:3:123::100-2001:b08:3:123::1ff,2001:b08:3:123::/64);

- **dstport**=<порт_приемника> - TCP-порт или UDP-порт приемника. Ожидаются:

✔ any – любой порт приемника (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] - список номеров и/или **символьных псевдонимов** портов приемника (например, 22-25,110,80,https,postgresql);

- **ipproto**=<протокол_в_IP> - протокол, инкапсулированный в IP. Ожидаются:

✔ any – любой протокол (по умолчанию);

✔ (<num>[-<num>] | <name>)[,...] - список имен и/или номеров протоколов в десятичном виде (например, 1,icmp,10-13,tcp,udp);

- **comment=<комментарий>** - строка комментария:

✔ Длина: от 0 до 200 символов;

✔ Допустимы любые печатаемые символы.

При добавлении PRI-правила параметр **priority=<приоритет>** должен присутствовать в определении правила, кроме того, хотя бы один из следующих параметров должен иметь значение отличное от **"any"**:

- srcif;
- srcip4;
- dstip4;
- srcip6;
- dstip6;
- srcport;
- dstport.

Если параметр **ipproto** имеет значение **any** (по умолчанию) и, при этом, в правиле заданы значениями отличными от **any** параметры: **srcport** и/или **dstport**, то правило будет применено только к TCP-сегментам и UDP-дейтаграммам и только с указанными портами.

То есть указание в правиле параметров, приведенных выше, при **ipproto** в значении **any**, ограничивает протоколы, инкапсулированные в IP, для которых будет применено данное правило протоколами TCP и UDP. Таким образом правило **не будет** применено к IP-пакетам с **любыми** протоколами, инкапсулированными в IP.

В отличие от **общего правила** и **AP-правила** в **PRI-правиле** не допускается одновременное использование IPv4-адресов и IPv6-адресов.
Т.е. в **PRI-правиле** не допускается, чтобы параметры **srcip4 (dstip4)** и **srcip6 (dstip6)** одновременно были в значениях отличных от **"any"**.

Д.5. Определение PROXY-правила (правила HTTP-посредника)

```
proxy:<номер> action=<действие> [hostname=<доменные_имена>] [filter=<фильтр>]
[active=<активность>] [comment=<комментарий>]
```

Где:

- **<номер>** - номер PROXY-правила. Допустимые значения: 1-65535;
- **action=<действие>** - действие правила. Ожидаются:

- ✔ accept – прием HTTP-сообщений: разрешается доступ по HTTP/HTTPs к Web-страницам с указанными доменными именами;
- ✔ deny – отклонение HTTP-сообщений: запрещается доступ по HTTP/HTTPs к Web-страницам с указанными доменными именами;
- ✔ edit - изменение HTTP-сообщений в соответствии с указанными фильтром;

- **hostname=<доменные_имена>** - список доменных имен и/или фрагментов доменных имен. Ожидаются:
  - ✔ пустая строка — любое доменное имя (PROXY-правило применяется не зависимо от доменного имени Web-страницы (по умолчанию);
  - ✔ список доменных имен и/или фрагментов доменных имен, элементы которого должны удовлетворять:
    - domain1.domain2[…] - доменное имя (например: pogoda.yandex.ru, translate.google.com);
    - .domainN.domanN+1[...] - фрагмент доменного имени (его конечная часть), должен начинаться с точки (например: .yandex.ru, .google.com, .mail.ru);
- **filter=<фильтр>** - фильтр, применяемый к Web-страницам. Ожидаются:
  - ✔ javascript - фильтровать JavaScript: из Web-страниц удаляются сценарии JavaScript;
  - ✔ vbscript - фильтровать VBScript: из Web-страниц удаляются сценарии VBScript;
- **active=<активность>** - активность правила. Ожидаются:
  - ✔ enable – правило активно (по умолчанию);
  - ✔ disable – правило неактивно;
- **comment=<комментарий>** - строка комментария:
  - ✔ Длина: от 0 до 200 символов;
  - ✔ Допустимы любые печатаемые символы.

При добавлении PROXY-правила параметр **action=<действие>** должен присутствовать в определении правила.

В случае **action=edit** в определении PROXY-правила также должен присутствовать параметр **filter=<фильтр>**, поскольку данный параметр не имеет значения по умолчанию.

Для остальных параметров в случае их отсутствия принимаются значения по умолчанию.

Действие **edit** применяется только к Web-страницам, доступ к которым осуществляется по протоколу **HTTP**.
Для Web-страниц, доступ к которым осуществляется по протоколу **HTTPs** действие **edit** не выполняется: т.е. сценарии **JavaScript** и **VBScript** не удаляются из Web-страниц, доступ к которым осуществляется по протоколу **HTTPs**.

Д.6. Комментарий к группе правил

Комментарий к группе правил – строка комментария, располагающаяся в политике доступа перед либо после строки определения **общего правила** либо **АР-правила**.

Добавление комментария к группе правил доступно только для следующих типов правил:
- общее правило;
- АР-правило.

Работа с комментариями к группам правил (просмотр, добавление, изменение, удаление) возможна только при использовании **командного интерфейса МЭ ССПТ-4А1**.

Просмотр комментариев к группам правил также возможен при просмотре выгруженных файлов дополнительных политик доступа.

При просмотре правил политики доступа строка комментария к группе правил должна начинаться с символа "#".

Допустимые действия:

- добавление комментария:
  - ✔ перед любым общим или АР-правилом;
  - ✔ после любого общего или АР-правила, кроме последнего правила данного типа (с наибольшим номером);
- изменение комментария;
- удаление комментария.

Формат:

- Строка длиной до 200 символов.
- Допустимые символы:
  - ✔ латинские и кириллические буквы в верхнем и нижнем регистрах;
  - ✔ цифры;
  - ✔ символы пунктуации из ASCII-таблицы;
  - ✔ символы пробела и табуляции.

Приложение Е. Определения объектов справочника

Для всех типов объектов справочника имя **“none”** (параметр **name**) является запрещенным, поскольку“none” является ключевым словом, используемым в командном языке МЭ ССПТ-4А1, в качестве значений параметров, где также допускается указание имени объекта справочника.

Е.1. Определение объекта "Узел сети" (host)

```
host name=<имя> {ip4=<IPv4_адреса> |ip6=<IPv6_адреса> | mac=<MAC_адреса>}
[vlan=<использование_vlan>] [interface=<интерфейсы>] [comment=<комментарий>]
```

Где:

- **name=<имя>** - символьное имя объекта, уникальное в пределах справочника;
- **ip4=<IPv4-адреса>** - список IPv4-адресов узла сети. Ожидаются:
  - ✔ none - значение не установлено (по умолчанию);
  - ✔ (<IPv4-адрес>)[,...] - список IPv4-адресов узла сети;
- **ip6=<IPv6-адреса>** - список IPv6-адресов узла сети. Ожидаются:
  - ✔ none - значение не установлено (по умолчанию);
  - ✔ (<IPv6-адрес>)[,...] - список -адресов узла сети;
- **mac=<MAC-адреса>** - MAC-адреса узла сети. Ожидаются:
  - ✔ any - лобой MAC-адрес (по умолчанию);
  - ✔ (<MAC-адрес>)[,...] - MAC-адреса узла сети:
    - <MAC-адрес>: без разделителей, например: aabbccddeeff;
    - <MAC-адрес>: с разделителем ":", например: aa:bb:cc:dd:ee:ff;
    - <MAC-адрес>: с разделителем "-", например: aa-bb-cc-dd-ee-ff
- **vlan=<использование_VLAN>** - параметр использования VLAN. Ожидаются:
  - ✔ any – объекту могут быть сопоставлены любые фреймы Ethernet (с тэгом IEEE 802.1q или без него) (по умолчанию);
  - ✔ enable – объекту будут сопоставлены только фреймы Ethernet с тегом IEEE 802.1q;
  - ✔ disable – объекту будут сопоставлены только фреймы Ethernet без тега IEEE 802.1q;
  - ✔ (<num>[-<num>])[,...] - список идентификаторов и диапазонов идентификаторов VLAN; объекту будут сопоставлены фреймы Ethernet, содержащие идентификатор VLAN из списка:
    - <num> - десятичное число от 0 до 4095;
  - ✔ <имя_группы_VLAN> - имя группы VLAN из справочника; объекту будут сопоставлены фреймы Ethernet, содержащие идентификаторы VLAN, указанные в группе;

- **interface=<интерфейсы>** - параметр привязки к интерфейсу. Ожидаются:
  - any - любой интерфейс (по умолчанию);
  - (<имя_интерфейса>)[,...] – символические имена интерфейсов;
  - <номер_интерфейса>[,...] – номера интерфейсов (нумерация начинается с нуля);
- **comment=<комментарий>** - строка комментария:

✔ Длина: от 0 до 200 символов;

✔ Допустимы любые печатаемые символы.

> В определении объекта **"Узел сети" (host)** по крайней мере один из следующих параметров должен быть определён, т.е иметь значение, отличное от значения по умолчанию:
> - ip4;
> - ip6;
> - mac.

E.2. Определение объекта "Сеть" (net)

```
net name=<имя> {ip4=<IPv4_адреса> | ip6=<IPv6_адреса>}
[vlan=<использование_vlan>] [interface=<интерфейсы>] [comment=<комментарий>]
```

Где:

- **name=<имя>** - символьное имя объекта, уникальное в пределах справочника;
- **ip4=<IPv4-адреса>** - список IPv4-адресов. Ожидаются:

✔ none - значение не установлено (по умолчанию);

✔ (<IPv4-адрес>-<IPv4-адрес> | <IPv4-адрес_сети>/<маска>)[,...] - список IPv4-адресов:
  - <маска>: краткий формат (CIDR), например: 24;
  - <маска>: полный формат, например: 255.255.255.0;
- **ip6=<IPv6-адреса>** - список IPv6-адресов. Ожидаются:

✔ none - значение не установлено (по умолчанию);

✔ (<IPv6-адрес>-<IPv6-адрес> | <IPv6-адрес>/<длина_префикса>)[,...] – список IPv6-адресов;
  - <длина_префикса>: число бит префикса (CIDR), например: 64;
- **vlan=<использование_VLAN>** - параметр использования VLAN. Ожидаются:

✔ any – объекту могут быть сопоставлены любые фреймы Ethernet (с тэгом IEEE 802.1q или без него) (по умолчанию);

✔ enable – объекту будут сопоставлены только фреймы Ethernet с тегом IEEE 802.1q;

✔ disable – объекту будут сопоставлены только фреймы Ethernet без тега IEEE 802.1q;

✔ (<num>[-<num>])[,...] - список идентификаторов и диапазонов идентификаторов VLAN; объекту будут сопоставлены фреймы Ethernet, содержащие идентификатор VLAN из списка:
  - <num> - десятичное число от 0 до 4095;

✔ <имя_группы_VLAN> - имя группы VLAN из справочника; объекту будут сопоставлены фреймы Ethernet, содержащие идентификаторы VLAN, указанные в группе;

- **interface=<интерфейсы>** - параметр привязки к интерфейсу. Ожидаются:

✔ any – любой интерфейс (по умолчанию);

✔ (<имя_интерфейса>)[,...] – символические имена интерфейсов;

✔ (<номер_интерфейса>)[,...] – номера интерфейсов (нумерация начинается с нуля);

- **comment=<комментарий> - строка комментария:**

✔ Длина: от 0 до 200 символов;

✔ Допустимы любые печатаемые символы.

В определении объекта **"Сеть" (net)** по крайней мере один из следующих параметров должен быть определён, т.е иметь значение, отличное от значения по умолчанию:
- ip4;
- ip6.

E.3. Определение объекта "Группа сетевых объектов" (net-group)

```
net-group name=<имя> {host=<имена_объектов_host> | net=<имена_объектов_net>}
[comment=<комментарий>]
```

Где:

- **name=<имя>** - символьное имя объекта, уникальное в пределах справочника;
- **host=<имена_объектов_host>** - имена объектов *host* из справочника. Ожидаются:

✔ none — объекты *host* не входят в группу сетевых объектов (по умолчанию);

✔ (<имя_объекта>)[,...] - список имён объектов *host* из справочника;

- **net=<имена_объектов_net>** - имена объектов *net* из справочника. Ожидаются:

✔ none - сети не привязаны к ресурсу (по умолчанию);

✔ (<имя_объекта>)[,...] - список имён объектов *net* из справочника;

- **comment=<комментарий>** - строка комментария (опционально):

✔ Длина: от 0 до 200 символов;

✔ Допустимы любые печатаемые символы.

В определении объекта **"Группа сетевых объектов" (net-group)** по крайней мере один из следующих параметров должен быть определён, т.е иметь значение, отличное от значения по умолчанию:
- host;
- net.

E.4. Определение объекта "Сервис" (service)

```
service name=<имя> protocol=<протокол> [(port=<номера_портов> |
icmp4=<тип_код_ICMPv4> | icmp6=<тип_код_ICMPv6>)] [comment=<комментарий>]
```

Где:

- **name=<имя>** - символьное имя объекта, уникальное в пределах справочника;
- **protocol=<протокол>** - протокол, инкапсулированный в IP. Ожидаются:
  - ✔ <name> - имя протокола, инкапсулированного в IP (например: udp);
  - ✔ <num> - номер протокола: десятичное число от 1 до 255;
- **port=<номера_портов>** - список TCP-портов или UDP-портов. Ожидаются:
  - ✔ any – любой порт (по умолчанию);
  - ✔ (<num>[-<num>] | <name>)[,...] - список номеров и/или **символьных псевдонимов** портов (например: 22-25,110,80,https,postgresql):
    - <num> - десятичное число от 0 до 65535;
    - <name> - **символьный псевдоним порта** (имя прикладного сервиса): соответствует определенному номеру порта;
- **icmp4=<тип_код_ICMPv4>** - тип и код ICMPv4-сообщения. Ожидаются:
  - ✔ any - любые тип и код ICMP-сообщения (по умолчанию);
  - ✔ (<тип>[/(<код>[-<код>] | any)])[,...] - список типов и кодов ICMPv4-сообщения:
    - <тип> - десятичное число от 0 до 255;
    - <код> - десятичное число от 0 до 255;
    - any - любой код ICMP-сообщения;
- **icmp6=<тип_код_ICMPv6>** - тип и код ICMPv6-сообщения. Ожидаются:
  - ✔ any - любые тип и код ICMP-сообщения (по умолчанию);
  - ✔ (<тип>[/(<код>[-<код>] | any)])[,...] - список типов и кодов ICMPv6-сообщения;
    - <тип> - десятичное число от 0 до 255;
    - <код> - десятичное число от 0 до 255;
    - any - любой код ICMP-сообщения;
- **comment=<комментарий>** - строка комментария:
  - ✔ Длина: от 0 до 200 символов;
  - ✔ Допустимы любые печатаемые символы.

Требования к определению объекта **"Сервис" (service)**:
- Должен быть определён параметр **protocol**;
- Параметр **port** допустим только для протоколов TCP и UDP;
- Параметр **icmp4** - только для протокола ICMP;
- Параметр **icmp6** - только для протокола ICMPv6.

E.5. Определение объекта "Ресурс" (resource)

```
resource name=<имя> {host=<имена_объектов_host>| net=<имена_объектов_net> |
net-group=<имя_объекта_net-group>} service=<имя_объекта_service>
[comment=<комментарий>]
```

Где:

- **name=<имя>** - символьное имя объекта, уникальное в пределах справочника;
- **host=<имена_объектов_host>** - имена объектов *host* из справочника. Ожидаются:

  ✔ none — объекты *host* не привязаны к ресурсу (по умолчанию);

  ✔ (<имя_объекта>)[,...] - список имён объектов *host* из справочника;
- **net=<имена_объектов_net>** - имена объектов *net* из справочника. Ожидаются:

  ✔ none - сети не привязаны к ресурсу (по умолчанию);

  ✔ (<имя_объекта>)[,...] - список имён объектов *net* из справочника;
- **net-group=<имя_объекта_net-group>** - имя объекта *net-group* из справочника. Ожидаются:

  ✔ none - группа сетевых объектов не привязана к ресурсу (по умолчанию);

  ✔ <имя_объекта> - имя объекта *net-group* из справочника;
- **service=<имя_объекта_service>** - имя объекта *service* из справочника. Ожидаются:

  ✔ <имя_объекта> - имя объекта *service* из справочника;
- **comment=<комментарий>** - строка комментария:

  ✔ Длина: от 0 до 200 символов;

  ✔ Допустимы любые печатаемые символы.

В определении объекта **“Ресурс” (resource)** должны быть определены следующие параметры:
- по меньшей мере один из параметров: **host**, **net** или **net-group**;
- параметр service.

E.6. Определение объекта "Интервал времени" (time)

```
time name=<имя> {months=<месяцы> | mdays=<дни_месяца> | wdays=<дни_недели> |
dtime=<время>} [comment=<комментарии>]
```

Где:

- **name=<имя>** - символьное имя объекта, уникальное в пределах справочника;
- **months=<месяцы>** - список месяцев (опционально). Ожидаются следующие значения:

  ✔ any – любой месяц (по умолчанию);

  ✔ <месяцы> – одно или более разделенных запятыми имен месяцев из следующего списка:

  - jan,feb,mar,apr,may,jun,jul,aug,sep,oct,nov,dec;
- **mdays=<дни_месяца>** - список дней месяца. Ожидаются следующие значения:

  ✔ any – любой день месяца (по умолчанию);

  ✔ (<num>[-<num>])[,...]- список дней месяца, например: 5,9,12-20,29;
- **wdays=<дни_недели>** - список дней недели. Ожидаются следующие значения:

  ✔ any – любой день недели (по умолчанию);

  ✔ <дни_недели> - – один или более разделенных запятыми имен дней недели из следующего списка:

- mon,tue,wed,thu,fri,sat,sun;

- **dtime=<время>** - список интервалов времени суток. Ожидаются следующие значения:

✔ any – любое время;

✔ <ЧЧ:ММ:СС>--<ЧЧ:ММ:СС>[,<ЧЧ:ММ:СС>-<ЧЧ:ММ:СС>] - список интервалов времени суток, например: 00:00:00-09:30:00,12:30:00-17:30:59,23:00:00-23:59:59;

- **comment=<комментарий>** - строка комментария:

✔ Длина: от 0 до 200 символов;

✔ Допустимы любые печатаемые символы.

В определении объекта **“Интервал времени” (time)** по меньшей мере один из следующих параметров: должен иметь значение отличное от **any**:
- months;
- mdays;
- wdays;
- dtime.

Е.7. Определение объекта "Группа доменных имён" (domain-group)

```
domain-group name=<имя> hostname=<доменные_имена> [comment=<комментарии>]
```

Где:

- **name=<имя>** - символьное имя объекта, уникальное в пределах справочника;
- **hostname=<доменные_имена>** - список доменных имён (имён узлов сети). Ожидается:

✔ (<имя_домена>)[,...] - список доменных имён или их фрагментов;

- Длина списка имен: от 1 до 1024 символов;
- <имя_домена> - строка, допустимые символы: любые печатаемые символы;

- **comment=<комментарий>** - строка комментария:

✔ Длина: от 0 до 200 символов;

✔ Допустимы любые печатаемые символы.

В определении объекта **“Группа доменных имён” (domain-group)** должен быть определен параметр **hostname**.

Параметр **hostname** объекта **domain-group** допускает использование следующих специальных символов в элементе списка доменных имен, обеспечивающих более гибкий поиск:
- **'*'**: замещение 0 или более символов (любая комбинация символов, в т.ч. отсутствие символов)
- **'?'**: замещение ровно одного символа (один любой символ)
- **'+'**: замещение 1 или более символов
- **'\'**: символ экранирования (указывает не рассматривать следующий за ним символ как специальный).

E.8. Определение объекта "Группа VLAN" (vlan-group)

```
vlan-group name=<имя> vid=<идентификаторы> [comment=<комментарии>]
```

Где:

- **name=<имя>** - символьное имя объекта, уникальное в пределах справочника;
- **vid=<список_идентификаторов>** - список идентификаторов VLAN:
  - ✔ (<num>[-<num>])[,...] - список идентификаторов и диапазонов идентификаторов VLAN (например, 1,10-13):
    - ◆ <num> - десятичное число от 0 до 4095;
- **comment=<комментарий>** - строка комментария:
  - ✔ Длина: от 0 до 200 символов;
  - ✔ Допустимы любые печатаемые символы.

В определении объекта **“Группа VLAN” (vlan-group)** должен быть определен параметр **vid**.

Приложение Ж. Дерево MIB-переменных SNMP-интерфейса МЭ ССПТ-4А1

Дерево MIB-переменных SNMP-интерфейса МЭ ССПТ-4А1 состоит из следующих групп (узлов) объектов:

- `auth` – переменные для выполнения процедуры аутентификации администратора МЭ ССПТ-4А1 при работе через SNMP-интерфейс и завершения сеанса работы администратора МЭ ССПТ-4А1 через SNMP-интерфейс (раздел Ж.1, стр. 547);
- `filter` – статистика трафика, обработанного пакетным фильтром (раздел Ж.2, стр. 548);
- `rulesStats` – статистика использования правил фильтрации (раздел Ж.3, стр. 551);
- `system` – системная информация (раздел Ж.4, стр. 555): состояние программных подсистем, программная и аппаратная конфигурация, использование системных ресурсов МЭ ССПТ-4А1;
- `user` – информация об учётных записях администраторов и активных администраторах МЭ ССПТ-4А1 (раздел Ж.5, стр. 561).

До выполнения последовательности GET-запросов (и/или GETNEXT-запросов) к ячейкам таблицы (MIB-объект типа “таблица”) необходимо выполнить GET-запрос к соответствующему MIB-объекту типа “таблица”, иначе не будет выполнено заполнение/обновление строк и ячеек таблицы соответствующими данными.

Данное требование, как правило, автоматически выполняется при использовании программ MIB-браузеров, но его следует учитывать при использовании сценариев, запрашивающих по протоколу SNMP данные таблиц.

Ж.1. Группа auth

`auth (1.3.6.1.4.1.32907.102.1)`

Назначение группы. Аутентфикация администратора МЭ ССПТ-4А1 для работы через SNMP-интерфейс. Завершения сеанса работы администратора, ранее авторизованного через SNMP-интерфейс с данного узла.

Состав группы:

- `fnp4Uname` – указание имени администратора для процедуры аутентификации;
- `fnp4Passw` – указание пароля администратора. Установка данной переменной инициирует процедуру аутентификации;
- `fnp4Logout` – завершения сеанса администратора, ранее авторизованного через SNMP-интерфейс с данного узла сети.

`fnp4Uname (1.3.6.1.4.1.32907.102.1.1)`

Назначение. Указание имени администратора для процедуры аутентификации.

Права доступа. Чтение/запись.

Тип. Строка (DisplayString).

В ответ на запрос на чтение переменной **fnp4Uname** всегда возвращается пустая строка.

`fnp4Passw (1.3.6.1.4.1.32907.102.1.2)`

Назначение. Указание пароля администратора. Установка данной переменной инициирует процедуру аутентификации.

Права доступа. Чтение/запись.

Тип. Строка (DisplayString).

До установки переменной **fnp4Passw** должна быть установлена переменная **fnp4Uname**.
В ответ на запрос на чтение переменной **fnp4Passw** всегда возвращается пустая строка.

`fnp4Logout (1.3.6.1.4.1.32907.102.1.3)`

Назначение. Завершение сеанса администратора, ранее авторизованного через SNMP-интерфейс с данного узла сети.

Права доступа. Чтение/запись.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (null)`** - не используется;
- **`1 (logout)`** - завершения сеанса администратора.

Ж.2. Группа filter

`filter (1.3.6.1.4.1.32907.102.2)`

Назначение группы. Просмотр статистики пакетной фильтрации трафика.

Состав группы:

- `filterStartTime` – дата и время запуска пакетного фильтра;
- `filterWorkTime` – число секунд прошедшее с последнего запуска пакетного фильтра (время работы пакетного фильтра в секундах);
- `filterStatsTable` – таблица статистики фильтрации трафика.

`filterStartTime (1.3.6.1.4.1.32907.102.2.1)`

Назначение. Дата и время запуска пакетного фильтра.

Права доступа. Только чтение.

Тип. Дата и время (DateAndTime).

`filterWorkTime (1.3.6.1.4.1.32907.102.2.2)`

Назначение. Число секунд, прошедшее с последнего запуска пакетного фильтра (время работы пакетного фильтра в секундах).

Права доступа. Только чтение.

Тип. 32-битный счетчик (Counter32).

`filterStatsTable (1.3.6.1.4.1.32907.102.2.3)`

Назначение. Таблица статистики фильтрации трафика.

Тип. Таблица.

Состав полей таблицы:

- `fsIfNumber` – номер фильтрующего интерфейса;
- `fsType` – протокол, по трафику которого приводится статистика в данной записи таблицы;
- `fsUnits` – единицы измерения, в которых указаны значения статистики в данной записи;
- `fsReceived` – число единиц, принятых данным фильтрующим интерфейсом;
- `fsSent` – число единиц, отправленных данным фильтрующим интерфейсом;
- `fsDropped` – число единиц, отброшенных данным фильтрующим интерфейсом;
- fsBroken – число поврежденных единиц (имеющих нарушения формата).

`fsIfNumber (1.3.6.1.4.1.32907.102.2.3.1.1)`

Назначение. Номер фильтрующего интерфейса.

Права доступа. Только чтение.

Тип. Целочисленный (Integer32).

`fsType (1.3.6.1.4.1.32907.102.2.3.1.2)`

Назначение. Определяет протокол (тип пакетов), по которому приводится статистика в данной записи таблицы.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`1 (all)`** – общее число пакетов по всем учитываемым протоколам;

- **`2 (ethernet)`** – кадры Ethernet II;
- **`3 (llc)`** – кадры IEEE 802.3-LLC;
- **`4 (snap)`** – кадры IEEE 802.3-SNAP;
- **`5 (raw)`** – кадры IEEE 802.3-RAW;
- **`6 (arp)`** – ARP-пакеты;
- **`7 (rarp)`** – RARP-пакеты;
- **`8 (ip)`** – IPv4-пакеты;
- **`9 (ip6)`** – IPv6-пакеты;
- **`10 (icmp)`** – ICMP-пакеты;
- **`11 (icmp6)`** – ICMPv6-пакеты;
- **`12 (udp)`** – UDP-датаграммы;
- **`13 (tcp)`** – TCP-сегменты.

`fsUnits (1.3.6.1.4.1.102.2.3.1.3)`

Назначение. Определяет единицы измерения, в которых указаны значения статистики в данной записи.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`1 (packets)`** – единицы измерения для данной записи: протокольные единицы.
- **`2 (bytes)`** – единицы измерения для данной записи: количество байт в протокольных единицах.

Поля **fsIfNumber**, **fsType** и **fsUnits** таблицы **filterStatsTable**: — индексные

`fsReceived (1.3.6.1.4.1.32907.102.2.3.1.4)`

Назначение. Число единиц, принятых данным фильтрующим интерфейсом.

Права доступа. Только чтение.

Тип. 64-битный счетчик (Counter64).

`fsSent (1.3.6.1.4.1.32907.102.2.3.1.5)`

Назначение. Число единиц, отправленных данным фильтрующим интерфейсом.

Права доступа. Только чтение.

Тип. 64-битный счетчик (Counter64).

`fsDropped (1.3.6.1.4.1.32907.102.2.3.1.6)`

Назначение. Число единиц, отброшенных данным фильтрующим интерфейсом.

Права доступа. Только чтение.

Тип. 64-битный счетчик (Counter64).

`fsBroken (1.3.6.1.4.1.32907.102.2.3.1.7)`

Назначение. Число поврежденных единиц (имеющих нарушения формата).

Права доступа. Только чтение.

Тип. 64-битный счетчик (Counter64).

Значения поля **fsBroken** таблицы **filterStatsTable** имеют смысл только в записях суммарной статистики по всем учитываемым протоколам.

Ж.3. Группа rulesStats

`rulesStats (1.3.6.1.4.1.32907.102.3)`

Назначение группы. Просмотр статистики использования правил фильтрации с возможностью выборки правил, по которым приводится статистика, по нескольким критериям.

Состав группы:

- `rulesStatsSelType` – критерий выборки правил по типу правил;
- `rulesStatsNum1` – критерий выборки правил по номеру либо по интервалу номеров (в последнем случае используется как левая граница интервала номеров);
- `rulesStatsNum2` – критерий выборки правил по интервалу номеров: правая граница интервала;
- `rulesStatsAction` – критерий выборки правил по значению поля действия правила;
- `rulesStatsIfsIn` – критерий выборки правил по значению поля входных интерфейсов;
- `rulesStatsIfsOut` – критерий выборки правил по значению поля выходных интерфейсов;
- `ruleStatsClear` – сброс (очистка) статистики использования правил фильтрации;
- `rulesStatsTable` – таблица статистики использования правил фильтрации.

Критерии выборки записей (**rulesStatsType**, **rulesStatsNum1**, **rulesStatsNum2**, **rulesStatsAction**, **rulesStatsIfsIn** и **rulesStatsIfsOut**) для вывода в таблице **rulesStatsTable** применяются только для одного запроса к данной таблице, после чего сбрасываются в значения по умолчанию.

Для выполнения повторного запроса к таблице с учетом критериев выборки их необходимо снова установить требуемыми значениями перед очередным запросом к таблице.

`rulesStatsSelType (1.3.6.1.4.1.32907.102.3.1)`

Назначение. Критерий выборки правил по типам правил.

Права доступа. Чтение/запись.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (any)`** – правила всех типов (по умолчанию).
- **`2 (rule)`** – общие правила;
- **`4 (ap)`** – AP-правила (прикладные);
- **`8 (tmp)`** – TMP-правила (временные).

`rulesStatsNum1 (1.3.6.1.4.1.32907.102.3.2)`

Назначение. Критерий выборки правил по номеру либо по интервалу номеров (в последнем случае используется как левая граница интервала номеров).

Права доступа. Чтение/запись.

Тип. Целочисленный (Integer32).

Формат значений:

- **`0`** – критерий не используется (по умолчанию);
- **`1..65535`** – номер правила либо левая граница интервала номеров правил для вывода в таблице статистики использования правил.

`rulesStatsNum2 (1.3.6.1.4.1.32907.102.3.3)`

Назначение. Критерий выборки правил по интервалу номеров: правая граница интервала.

Права доступа. Чтение/запись.

Тип. Целочисленный (Integer32).

Формат значений:

- **`0`** – критерий не используется (по-умолчанию);
- **`1..65535`** – правая граница (номер) интервала номеров правил для вывода в таблице статистики использования правил.

Для выборки записей таблицы **rulesStatsTable** по номеру правила должен быть установлен критерий **rulesStatsNum1**. Для выборки записей с определенным интервалом номеров должны быть установлены критерии **rulesStatsNum1** и **rulesStatsNum2**, задающие соответственно левую и правую границу интервала номеров правил.

`rulesStatsAction (1.3.6.1.4.1.32907.102.3.4)`

Назначение. Критерий выборки правил по значению поля действия правила.

Права доступа. Чтение/запись.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (any)`** – критерий не используется (любое действие – по умолчанию);
- **`1 (drop)`** – удаление пакета (действие “drop”);
- **`2 (accept)`** – передача пакета на следующий уровень обработки или на выходные интерфейсы (действие “accept”);
- **`4 (deny)`** – удаление пакета с отправкой источнику пакета-уведомления;
- **`8 (goto)`** – переход к некоторому правилу (действие “goto”);

`rulesStatsIfsIn (1.3.6.1.4.1.32907.102.3.5)`

Назначение. Критерий выборки правил по значению поля (правила) входных интерфейсов.

Права доступа. Чтение/запись.

Тип. Строка (DisplayString).

Формат значений:

- **`any`** – не использовать данный критерий (значение по умолчанию).
- **`<номер_интерфейса>[,<номер_интерфейса>]`** – номер или список номеров интерфейсов;
- **`<имя_интерфейса>[,<имя_интерфейса>]`** – имя или список имён интерфейсов.

`rulesStatsIfsOut (1.3.6.1.4.1.32907.102.3.6)`

Назначение. Критерий выборки правил по значению поля (правила) выходных интерфейсов.

Права доступа. Чтение/запись.

Тип. Строка (DisplayString).

Формат значений:

- **any** – не использовать данный критерий (значение по умолчанию).
- **<номер_интерфейса>[,<номер_интерфейса>]** – номер или список номеров интерфейсов;
- **<имя_интерфейса>[,<имя_интерфейса>]** – имя или список имён интерфейсов.

`rulesStatsClear (1.3.6.1.4.1.32907.102.3.7)`

Назначение. Сброс (очистка) статистики использования правил фильтрации.

Права доступа. Чтение/запись.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (null)`** - не используется;
- **`1 (clear)`** - сброс (очистка) статистики использования правил фильтрации.

`rulesStatsTable (1.3.6.1.4.1.32907.102.3.8)`

Назначение. таблица статистики использования правил фильтрации.

Тип. Таблица.

Состав полей таблицы:

- `rulesStatsIndex` – порядковый номер записи (индексное поле);
- `rulesStatsType` – тип правила;
- `rulesStatsRuleNum` – номер правила;
- `rulesStatsTime` – время последнего срабатывания данного правила;
- `rulesStatsPacketsLen` – число пакетов, к которым было применено данное правило;
- `rulesStatsBytesLen` – суммарное число байт всех пакетов, к которым было применено данное правило.

`rulesStatsIndex (1.3.6.1.4.1.32907.102.3.8.1.1)`

Назначение. Порядковый номер записи (индексное поле).

Права доступа. Только чтение.

Тип. Целочисленный (Integer32).

`rulesStatsType (1.3.6.1.4.1.32907.102.3.8.1.2)`

Назначение. Тип правила.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

`rulesStatsRuleNum (1.3.6.1.4.1.32907.102.3.8.1.3)`

Назначение. Номер правила.

Права доступа. Только чтение.

Тип. Целочисленный (Integer32).

`rulesStatsTime (1.3.6.1.4.1.32907.102.3.8.1.4)`

Назначение. Дата и время последнего срабатывания данного правила.

Права доступа. Только чтение.

Тип. Дата и время (DateAndTime).

`rulesStatsPacketsLen (1.3.6.1.4.1.32907.102.3.8.1.5)`

Назначение. Число пакетов, к которым было применено данное правило.

Права доступа. Только чтение.

Тип. 64-битный счетчик (Counter64).

`rulesStatsBytesLen (1.3.6.1.4.1.32907.102.3.8.1.6)`

Назначение. Суммарное число байт всех пакетов, к которым было применено данное правило.

Права доступа. Только чтение.

Тип. 64-битный счетчик (Counter64).

Ж.4. Группа system

`system (1.3.6.1.4.1.32907.102.4)`

Назначение группы. Системная информация МЭ ССПТ-4А1. Сведения об аппаратной конфигурации и версии ПО МЭ ССПТ-4А1. Сведения о состоянии программных подсистем МЭ ССПТ-4А1. Сведения об использовании системных ресурсов МЭ ССПТ-4А1.

Состав группы:

- `sysInfo` – сведения об аппаратной конфигурации и версии ПО МЭ ССПТ-4А1, сведения о состоянии программных подсистем МЭ ССПТ-4А1;
- `sysCpuStatus` — сведения о использовании ЦП (CPU);
- `sysRamStatus` - сведения об использовании ОЗУ (RAM);
- `sysPartitionTable` - таблица статистики свободного дискового пространства смонтированных разделов (файловых систем).

`sysInfo (1.3.6.1.4.1.32907.102.4.1)`

Назначение группы. Сведения об аппаратной конфигурации МЭ ССПТ-4А1 и версии ПО МЭ ССПТ-4А1. Сведения о состоянии программных подсистем МЭ ССПТ-4А1.

Состав группы:

- `sysCpuModel` – модель центрального процессора устройства;
- `sysCpuCoreNum` – количество ядер центрального процессора устройства;
- `sysRamSizeMb` – значение объёма оперативной памяти МЭ в мегабайтах;
- `sysInterfaceTotalNum` – общее число сетевых интерфейсов в устройстве;
- `sysInterfaceFilterNum` – число фильтрующих интерфейсов в устройстве;
- `sysSoftwareVersion` – версия ПО МЭ ССПТ-4А1;
- `sysFilteringStatus` – состояние пакетного фильтра;
- `sysIntegrityCheckStatus` – состояние подсистемы контроля целостности;
- `sysAuthStatus` – состояние подсистемы авторизации;
- `sysLoggingStatus` – состояние подсистемы регистрации;
- `sysHighAvailabilityStatus` – состояние подсистемы резервирования;

- `sysRemoteAdminStatus` – состояние командного сервера;
- `sysWebStatus` – состояние Web-интерфейса;
- `sysSnmpStatus` – состояние SNMP-интерфейса;
- `sysDateTime` – системные дата и время;

`sysCpuModel (1.3.6.1.4.1.32907.102.4.1.1)`

Назначение. Модель центрального процессора устройства.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysCpuCoreNum (1.3.6.1.4.1.32907.102.4.1.2)`

Назначение. Количество ядер центрального процессора устройства.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysRamSizeMb (1.3.6.1.4.1.32907.102.4.1.3)`

Назначение. Объем оперативной памяти устройства (в мегабайтах).

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysInterfaceTotalNum (1.3.6.1.4.1.32907.102.4.1.4)`

Назначение. Общее число сетевых интерфейсов в устройстве.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysInterfaceFilterNum (1.3.6.1.4.1.32907.102.4.1.5)`

Назначение. Число фильтрующих интерфейсов в устройстве.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysSoftwareVersion (1.3.6.1.4.1.32907.102.4.1.6)`

Назначение. Версия ПО МЭ ССПТ-4А1.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysFilteringStatus (1.3.6.1.4.1.32907.102.4.1.7)`

Назначение. Состояние пакетного фильтра.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (stopped)`** – процесс не запущен;
- **`1 (not-available)`** – процесс запущен, но не доступен;
- **`3 (available)`** – процесс запущен и доступен.

`sysIntegrityCheckStatus (1.3.6.1.4.1.32907.102.4.1.8)`

Назначение. Получение состояния подсистемы контроля целостности.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (stopped)`** – процесс не запущен;
- **`1 (not-available)`** – процесс запущен, но не доступен;
- **`3 (available)`** – процесс запущен и доступен.

`sysAuthStatus (1.3.6.1.4.1.32907.102.4.1.9)`

Назначение. Получение состояния подсистемы авторизации.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (stopped)`** – процесс не запущен;
- **`1 (not-available)`** – процесс запущен, но не доступен;
- **`3 (available)`** – процесс запущен и доступен.

`sysLoggingStatus (1.3.6.1.4.1.32907.102.4.1.10)`

Назначение. Получение состояния подсистемы регистрации.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (stopped)`** – процесс не запущен;
- **`1 (not-available)`** – процесс запущен, но не доступен;
- **`3 (available)`** – процесс запущен и доступен.

`sysHighAvailabilityStatus (1.3.6.1.4.1.32907.102.4.1.11)`

Назначение. Получение состояния подсистемы резервирования.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (stopped)`** – процесс не запущен;
- **`1 (not-available)`** – процесс запущен, но не доступен;
- **`3 (available)`** – процесс запущен и доступен.

`sysRemoteAdminStatus (1.3.6.1.4.1.32907.102.4.1.12)`

Назначение. Получение состояния командного сервера.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (stopped)`** – процесс не запущен;
- **`1 (not-available)`** – процесс запущен, но не доступен;
- **`3 (available)`** – процесс запущен и доступен.

`sysWebStatus (1.3.6.1.4.1.32907.102.4.1.13)`

Назначение. Получение состояния Web-интерфейса.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (stopped)`** – процесс не запущен;
- **`1 (not-available)`** – процесс запущен, но не доступен;
- **`3 (available)`** – процесс запущен и доступен.

`sysSnmpStatus (1.3.6.1.4.1.32907.102.4.1.14)`

Назначение. Получение состояния SNMP-интерфейса.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`0 (stopped)`** – процесс не запущен;

- **`1 (not-available)`** – процесс запущен, но не доступен;
- **`3 (available)`** – процесс запущен и доступен.

`sysDateTime (1.3.6.1.4.1.32907.102.4.1.15)`

Назначение. Получение системных даты и времени.

Права доступа. Только чтение.

Тип. Дата и время (DateAndTime).

Ж.4.1. Группа sysCpuStatus

`sysCpuStatus (1.3.6.1.4.1.32907.102.4.2)`

Назначение группы. Сведения об использовании ЦП (CPU) МЭ ССПТ-4А1.

Состав группы:

- `sysCpuUserLoad` – доля времени, проведённого ЦП в состоянии “user”;
- `sysCpuNice` – доля времени, проведённого ЦП в состоянии “nice”;
- `sysCpuSysLoad` – доля времени, проведённого ЦП в состоянии “system”;
- `sysCpuSysInterrupt` – доля времени, проведённого ЦП в состоянии “interrupt”;
- `sysCpuIdle` – доля времени, проведённого ЦП в состоянии “idle”.

`sysCpuUserLoad (1.3.6.1.4.1.32907.102.4.2.1)`

Назначение. Доля времени, проведённого ЦП в состоянии “user”.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysCpuNice (1.3.6.1.4.1.32907.102.4.2.2)`

Назначение. Доля времени, проведённого ЦП в состоянии «nice».

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysCpuSysLoad (1.3.6.1.4.1.32907.102.4.2.3)`

Назначение. Доля времени, проведённого ЦП в состоянии “system”.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysCpuSysInterrupt (1.3.6.1.4.1.32907.102.4.2.4)`

Назначение. Доля времени, проведённого ЦП в состоянии “interrupt”.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysCpuIdle (1.3.6.1.4.1.32907.102.4.2.5)`

Назначение. Доля времени, проведенного ЦП в состоянии “idle”.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

Ж.4.2. Группа sysRamStatus

`sysRamStatus (1.3.6.1.4.1.32907.102.4.3)`

Назначение группы. Сведения об использовании ОЗУ (RAM) МЭ ССПТ-4А1.

Состав группы:

- `sysRamActive` – объем активной памяти;
- `sysRamInactive` – объем неактивной памяти;
- `sysRamFree` – объем свободной памяти;
- `sysRamTotal` – полный объем памяти.

`sysRamActive (1.3.6.1.4.1.32907.102.4.3.1)`

Назначение. Объем активной памяти.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysRamInactive (1.3.6.1.4.1.32907.102.4.3.2)`

Назначение. Объем неактивной памяти.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysRamFree (1.3.6.1.4.1.32907.102.4.3.3)`

Назначение. Объем свободной памяти.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysRamTotal (1.3.6.1.4.1.32907.102.4.3.4)`

Назначение. Полный объем памяти.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysPartitionTable (1.3.6.1.4.1.32907.102.4.4)`

Назначение. Таблица статистики использования дискового пространства смонтированных разделов (файловых систем).

Тип. Таблица.

Состав полей таблицы:

- `sysPartitionNum` – порядковый номер раздела (файловой системы);
- `sysPartitionUsedSpace` – объем используемого дискового пространства;
- `sysPartitionFreeSpace` – объем свободного дискового пространства;
- `sysPartitionTotalSpace` – полный объем дискового пространства.

`sysPartitionNum (1.3.6.1.4.1.32907.102.4.4.1.1)`

Назначение. Порядковый номер раздела (файловой системы).

Права доступа. Только чтение.

Тип. Целочисленный (Integer32).

`sysPartitionUsedSpace (1.3.6.1.4.1.32907.102.4.4.1.2)`

Назначение. Объем используемого дискового пространства.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysPartitionFreeSpace (1.3.6.1.4.1.32907.102.4.4.1.3)`

Назначение. Объем свободного дискового пространства.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`sysPartitionTotalSpace (1.3.6.1.4.1.32907.102.4.4.1.4)`

Назначение. Полный объем дискового пространства.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

Ж.5. Группа user

`user (1.3.6.1.4.1.32907.102.5)`

Назначение группы. Просмотр учётных записей администраторов МЭ ССПТ-4А1. Просмотр списка активных администраторов МЭ ССПТ-4А1 (авторизованных в системе на данный момент времени).

Состав группы:

- `userTable` – таблица учётных записей администраторов МЭ ССПТ-4А1;
- `userActiveTable` – таблица активных администраторов МЭ ССПТ-4А1.

`userTable (1.3.6.1.4.1.32907.102.5.1)`

Назначение. Таблица учётных записей администраторов МЭ ССПТ-4А1.

Тип. Таблица.

Состав полей таблицы:

- `userIndexNum` – порядковый номер учётной записи администратора;
- `userName` – имя администратора;
- `userStatus` – состояние учётной записи администратора (включена/выключена);
- `userPrivilege` – привилегии администратора.

`userIndexNum (1.3.6.1.4.1.32907.102.5.1.1.1)`

Назначение. Порядковый номер учётной записи администратора (индексное поле).

Права доступа. Только чтение.

Тип. Целочисленный (Integer32).

`userName (1.3.6.1.4.1.32907.102.5.1.1.2)`

Назначение. Имя администратора.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`userStatus (1.3.6.1.4.1.32907.102.5.1.1.3)`

Назначение. Состояние учётной записи администратора (включена/выключена).

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`1 (enabled)`** – учётная запись включена;
- **`2 (disabled)`** – учётная запись выключена.

`userPrivilege (1.3.6.1.4.1.32907.102.5.1.1.4)`

Назначение. Привилегии администратора.

Права доступа. Только чтение.

Тип. Перечисление (Enumeration).

Допустимые значения:

- **`1 (read)`** – доступ только на чтение.
- **`2 (full)`** – полный доступ на чтение и запись кроме возможности управления учётными записями администраторов (обеспечивается возможность смены собственного пароля);
- **`3 (admin)`** – полный доступ, которым обладает только администратор admin.

`userActiveTable (1.3.6.1.4.1.32907.102.5.2)`

Назначение. Таблица активных администраторов МЭ ССПТ-4А1: информация об администраторах, авторизованных в системе на данный момент времени.

Тип. Таблица.

Состав полей таблицы:

- `userActiveNum` – порядковый номер администратора;
- `userActiveName` – имя администратора;
- `userActiveLoginTime` – дата и время авторизации администратора;
- `userActiveFrom` – тип интерфейса управления, используемого администратором, и IP-адрес узла, с которого администратор подключён к устройству;
- `userActivePrivileges` – привилегии администратора;
- `userActiveIdle` – время простоя администратора: число секунд, прошедшее с последней операции администратора в используемом им интерфейсе управления.

`userActiveNum (1.3.6.1.4.1.32907.102.5.2.1.1)`

Назначение. Порядковый номер администратора (индексное поле).

Права доступа. Только чтение.

Тип. Целочисленный (Integer32).

`userActiveName (1.3.6.1.4.1.32907.102.5.2.1.2)`

Назначение. Имя администратора.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`userActiveLoginTime (1.3.6.1.4.1.32907.102.5.2.1.3)`

Назначение. Дата и время авторизации администратора.

Права доступа. Только чтение.

Тип. Дата и время (DateAndTime).

`userActiveFrom (1.3.6.1.4.1.32907.102.5.2.1.4)`

Назначение. Тип интерфейса управления, используемого администратором, и IP-адрес узла сети, с которого администратор подключён к устройству.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`userActivePrivileges (1.3.6.1.4.1.32907.102.5.2.1.5)`

Назначение. Привилегии администратора.

Права доступа. Только чтение.

Тип. Строка (DisplayString).

`userActiveIdle (1.3.6.1.4.1.32907.102.5.2.1.6)`

Назначение. Время простоя администратора: число секунд, прошедшее с последней операции администратора в используемом им интерфейсе управления.

Права доступа. Только чтение.

Тип. Целочисленный (Integer32).

Приложение 3. Утилита аутентификации сетевого пользователя

Утилита аутентификации сетевого пользователя, входящая в состав программы «Утилиты МЭ серии ССПТ-4» (входит в комплект поставки) предназначена для формирования и отправки на МЭ ССПТ-4А1 запроса аутентификации сетевого пользователя. Утилита аутентификации сетевого пользователя должна запускаться на компьютере сетевого пользователя, расположенном в сегменте сети, подключенном к одному из фильтрующих интерфейсов МЭ ССПТ-4А1.

Поскольку фильтрующие интерфейсы МЭ ССПТ-4А1 функционируют в безадресном режиме, возможности реализации аутентификации входящих/исходящих запросов требует специальных методов обработки. Поэтому аутентификация сетевых пользователей возможна только при активном режиме NAT МЭ ССПТ-4А1. В этом режиме фильтрующим интерфейсам МЭ ССПТ-4А1 назначаются виртуальные IP-адреса, по которым и отправляется запрос аутентификации сетевого пользователя.

Запрос аутентификации сетевого пользователя представляет собой одиночный IP-пакет, посылаемый утилитой аутентификации сетевого пользователя от компьютера сетевого пользователя по виртуальному IP-адресу фильтрующего интерфейса, который защищает данный сегмент сети. Тело этого IP-пакета содержит имя и пароль сетевого пользователя, зашифрованные с использованием ключей аутентификации сетевого пользователя. Пара ключей аутентификации (открытый/закрытый) должна соответствовать IP-адресу компьютера сетевого пользователя, который является источником IP-пакета, содержащего запрос аутентификации.

Для нормальной работы утилиты аутентификации сетевого пользователя на компьютере сетевого пользователя необходимо иметь следующую ключевую информацию:

- файл параметров Diffie-Hellman экземпляра устройства МЭ ССПТ-4А1;
- файл открытого ключа Diffie-Hellman экземпляра устройства МЭ ССПТ-4А1;
- файл закрытого ключа Diffie-Hellman сетевого пользователя;
- файл открытого ключа Diffie-Hellman сетевого пользователя.

Эти файлы должны быть загружены администратором МЭ ССПТ-4А1 на управляющий компьютер при помощи WEB-интерфейса администратора МЭ ССПТ-4А1, а затем перенесены на компьютер сетевого пользователя.

Для файлов ключевой информации, используемых утилитой аутентификации сетевого пользователя, приняты имена по умолчанию, которые приведены в таблице 3.1, стр. 566. Если

имя файла отличается от имени, принятого по умолчанию, то необходимо указать его явно, используя соответствующие параметры командной строки запуска утилиты аутентификации сетевого пользователя.

Таблица 3.1: Стандартные имена файлов ключевой информации

Имя файла	*Назначение*
fnp_dhparam.pem	Файл параметров Diffie-Hellman экземпляра устройства МЭ ССПТ-4А1
fnp_dhpubkey.bn	Файл открытого ключа Diffie-Hellman экземпляра устройства МЭ ССПТ-4А1
fnpnl_dhkey.bn	Файл закрытого ключа Diffie-Hellman сетевого пользователя
fnpnl_dhpubkey.bn	Файл открытого ключа Diffie-Hellman сетевого пользователя

Файлы ключевой информации, используемые утилитой аутентификации сетевого пользователя, следует располагать в одном из следующих каталогов файловой системы компьютера сетевого пользователя:

- `etc/fnputils2` – основной подкаталог для хранения ключей и сертификатов относительно каталога инсталляции пакета утилиты аутентификации сетевого пользователя;
- `.fnputils2` – подкаталог в домашнем каталоге текущего пользователя, запускающего утилиту аутентификации сетевого пользователя.

Домашний каталог пользователя – это каталог в файловой системе компьютера, предназначенный для хранения файлов, принадлежащих данному пользователю.
Расположение домашнего каталога зависит от используемой операционной системы и ее настроек:
- для операционных систем семейства UNIX, домашние каталоги указываются в учетных записях пользователей и располагаются, как правило, в каталоге `/home` или `/usr/home`;
- для операционных систем Microsoft Windows®:
  - ✔ `C:\Documents and Settings` – для Microsoft Windows® XP;
  - ✔ `C:\Users` – для Microsoft Windows® Vista/7/8/10.

Для поиска файлов ключевой информации, утилитой аутентификации сетевого пользователя принят следующий порядок действий:

1) если имя файла указано явно через параметр командной строки запуска утилиты, то будет использован указанный файл. Если файла с указанным именем не существует или для чтения файла недостаточно прав доступа, то выполнение утилиты завершается. При этом причина ошибки отражается в диагностических сообщениях, выводимых на экран терминала;
2) если явное указание имени файла не используется, то выполняется поиск файла с именем, принятым по умолчанию, в пользовательском каталоге `.fnputils2`. Если файл существует, то он будет использован утилитой;
3) если файл в пользовательском каталоге `.fnputils2` не существует или для чтения файла недостаточно прав доступа, то выполняется поиск файла с именем, принятым по умолчанию, в каталоге `etc/fnputils2` относительно каталога инсталляции пакета утилиты аутентификации сетевого пользователя. Если файл существует, то он будет использован

утилитой. В противном случае, выполнение утилиты завершается. При этом причина ошибки отражается в диагностических сообщениях, выводимых на экран терминала.

3.1. Параметры командной строки

Утилита аутентификации сетевого пользователя представлена в двух вариантах сборки:

1) утилита `fnpnl2_ssl` – утилита аутентификации сетевого пользователя, использующая функции библиотеки FNPCrypt/OpenSSL, и предназначенная для взаимодействия с МЭ ССПТ-4А1;
2) утилита `fnpnl2_gost` – утилита аутентификации сетевого пользователя, использующая функции библиотеки FNPCrypt/Агава-С, и предназначенная для взаимодействия с МЭ ССПТ-2.

Ниже рассматривается использование утилиты аутентификации сетевого пользователя `fnpnl2_ssl` (далее – утилита `fnpnl2_ssl`).

Утилита `fnpnl2_ssl` представляет собой терминальное (консольное) приложение, все режимы работы которого задаются через параметры командной строки запуска.

Все сообщения утилиты `fnpnl2_ssl` могут выводиться на *английском* или *русском* языках в зависимости от настроек локализации в окружении процесса. По умолчанию язык вывода сообщений – *английский*.

Справку по использованию параметров командной строки утилиты `fnpnl2_ssl` можно получить, вызвав ее с параметром **`--help`** (или **`-h`**):

```
$ /usr/local/bin/fnpnl2_ssl --help
Межсетевой экран ССПТ-2/ССПТ-4
  Аутентификация сетевого пользователя (сборка OpenSSL), версия 2.0.0
  (c) ООО "НПО "ФРАКТЕЛ", 2018. Все права защищены

  Использование: fnpnl2_ssl [<список_параметров>]

  Допустимые параметры:
    --help, -h - вывод этого текста и завершение работы
    --debug, -d - вывод дополнительных отладочных сообщений
    --host=IP, -H IP - IP-адрес удаленного МЭ ССПТ-2/ССПТ-4
    --action=TYPE, -a TYPE - аутентификация/выход сетевого пользователя (по умолчанию
"login",
        корректными значениями являются "login", "logout")
    --user=UNAME, -U UNAME - имя сетевого пользователя
    --pwd=PWD, -P PWD - пароль сетевого пользователя
    --fnpdhp=FILE, -f FILE - имя файла параметров Diffie-Hellman
    --fnpdhk=FILE, -F FILE - имя файла открытого ключа Diffie-Hellman МЭ ССПТ
    --prvkey=FILE, -k FILE - имя файла закрытого ключа Diffie-Hellman пользователя
    --pubkey=FILE, -p FILE - имя файла открытого ключа Diffie-Hellman пользователя
    --lang=XX, -l XX - язык для вывода диагностических сообщений
                       (XX - двухсимвольный код языка)
    --version, -v - вывод информации о версии программы и завершение работы
```

Утилита `fnpnl2_ssl` принимает следующие параметры командной строки (перечень дается в алфавитном порядке):

- **`--action=TYPE`** (**`-a TYPE`**)

  задает тип запроса аутентификации сетевого пользователя через аргумент **`TYPE`**:

  ✔ `login` – запрос аутентификации сетевого пользователя (начало работы). Является *запросом по умолчанию*;

  ✔ `logout` – запрос на выход сетевого пользователя (завершение работы);

- **`--debug`** (**`-d`**)

  задает вывод дополнительных отладочных сообщений во время выполнения утилиты `fnpnl2_ssl`. Полезно использовать для уточнения причин возникающих ошибок;

- **`--fnpdhp=FILE`** (**`-f FILE`**)

  задает имя файла для чтения параметров Diffie-Hellman экземпляра устройства МЭ ССПТ-4А1 через аргумент **`FILE`** (по умолчанию – файл с именем `fnp_dhparam.pem` в одном из каталогов, перечисленных в разделе Приложение 3, стр. 565);

- **`--fnpdhk=FILE`** (**`-F FILE`**)

  задает имя файла для чтения открытого ключа Diffie-Hellman экземпляра устройства МЭ ССПТ-4А1 через аргумент **`FILE`** (по умолчанию – файл с именем `fnp_dhpubkey.bn` в одном из каталогов, перечисленных в разделе Приложение 3, стр. 565);

- **`--help`** (**`-h`**)

  выводит на терминал краткую справку об использовании утилиты `fnpnl2_ssl` как это показано выше;

- **`--host=IP`** (**`-H IP`**)

  задает IP-адрес или доменное имя удаленного МЭ ССПТ-4А1, на который будет отправлен запрос аутентификации сетевого пользователя, через аргумент **`IP`**;

- **`--lang=XX`** (**`-l XX`**)

  задается язык для вывода сообщений через аргумент **`XX`** (значение аргумента **`XX`** – двухсимвольный код языка);

> В утилите `fnpnl2_ssl` для вывода сообщений поддерживаются следующие двухсимвольные коды языков:
> - `ru` – русский язык;
> - `en` – английский язык.
>
> Язык по умолчанию выбирается на основании настроек локализации в окружении процесса.

- **`--prvkey=FILE`** (**`-k FILE`**)

  задает имя файла для чтения закрытого ключа Diffie-Hellman сетевого пользователя МЭ ССПТ-4А1 через аргумент **`FILE`** (по умолчанию – файл с именем `fnpnl_dhkey.bn` в одном из каталогов, перечисленных в разделе Приложение 3, стр. 565);

- **`--pubkey=FILE`** (**`-p FILE`**)

задает имя файла для чтения открытого ключа Diffie-Hellman сетевого пользователя МЭ ССПТ-4А1 через аргумент **FILE** (по умолчанию – файл с именем `fnpnl_dhpubkey.bn` в одном из каталогов, перечисленных в разделе Приложение 3, стр. 565);

- **`--pwd=PWD`** (**`-P PWD`**)

  задает пароль сетевого пользователя МЭ ССПТ-4А1 через аргумент **PWD** (по умолчанию – утилита `fnpnl2_ssl` запрашивает ввод пароля сетевого пользователя *с терминала в интерактивном режиме*);

> Строку, передаваемую в качестве значения аргумента **PWD**, следует заключать в кавычки ('″').
>
> Передавать пароль пользователя через параметры командной строки небезопасно.

- **`--user=UNAME`** (**`-U UNAME`**)

  задает имя сетевого пользователя МЭ ССПТ-4А1 через аргумент **UNAME** (по умолчанию – используется имя *текущего системного пользователя*, запустившего утилиту `fnpnl2_ssl`);

- **`--version`** (**`-v`**)

  вывод краткой информации об утилите `fnpnl2_ssl`, ее версии и завершение работы.

3.2. Переменные окружения

Перед запуском утилиты `fnpnl2_ssl` может быть определен ряд переменных окружения, которые модифицируют режимы работы утилиты. Явное указание параметров командной строки отменяет значения, содержащиеся в соответствующих переменных окружения.

Утилита `fnpnl2_ssl` проверяет наличие и обрабатывает значения следующих переменных окружения:

- `FNPUTILS_IP` – значение переменной окружения `FNPUTILS_IP` задает IP-адрес или доменное имя удаленного МЭ ССПТ-4А1, на который будет отправляться запрос аутентификации сетевого пользователя. Отменяется через использование параметра **`--host`** (**`-H`**).

3.3. Примеры использования

В данном разделе приводятся примеры использования параметров командной строки для запуска утилиты `fnpnl2_ssl`:

- отправка запроса аутентификации сетевого пользователя `nuser1` на удаленный МЭ ССПТ-4А1 по IP-адресу `10.2.253.246`:

```
/usr/local/bin/fnpnl2_ssl --host=10.2.253.246 --user=nuser1
```

- отправка запроса аутентификации сетевого пользователя на удаленный МЭ ССПТ-4А1 по IP-адресу `10.2.253.246`, используя файл открытого ключа Diffie-Hellman сетевого пользователя с именем `10.2.253.241-fnpnl_dhpubkey.bn` и файл закрытого ключа Diffie-Hellman сетевого пользователя с именем `10.2.253.241-fnpnl_dhkey.bn`, расположенные в текущем каталоге (*используется краткий формат параметров командной строки; для использования в операционных системах Microsoft Windows® XP/Vista/7/8/10*):

```
C:> “C:\Program Files\Fractel\FNPUtils\fnpnl2_ssl.exe” -H 10.2.253.246
    -p 10.2.253.241-fnpnl_dhpubkey.bn -k 10.2.253.241-fnpnl_dhkey.bn
```

3.4. Графическая оболочка утилиты аутентификации сетевого пользователя

Графическая оболочка обеспечивает тот же функционал, что и консольная утилита аутентификации сетевого пользователя, но предоставляет более дружественный интерфейс. Графическая оболочка и консольная утилита аутентификации сетевого пользователя входят в общий инсталляционный пакет, устанавливаемый на компьютере сетевого пользователя.

3.4.1. Главное окно графической оболочки

Основное меню графической оболочки состоит из двух пунктов – “`Файл`” и “`Справка`”. Подменю `Файл` в свою очередь содержит следующие пункты:

- `Очистить информационную область` – очищает информационную область от всех ранее выведенных диагностических сообщений;
- `Очистить поля ввода данных` – очищает все поля ввода данных, при этом список выбора конфигурации устанавливается в значение по умолчанию: не выбрана;
- `Выход` – закрывает главное окно графической оболочки и завершает выполнение программы.

Подменю “`Справка`” содержит единственный пункт “`О программе`”, при выборе которого выводится диалоговое окно с названием и версией программы.

На рисунке 3.1, стр. 571 приведено главное окно графической оболочки утилиты аутентификации сетевого пользователя.

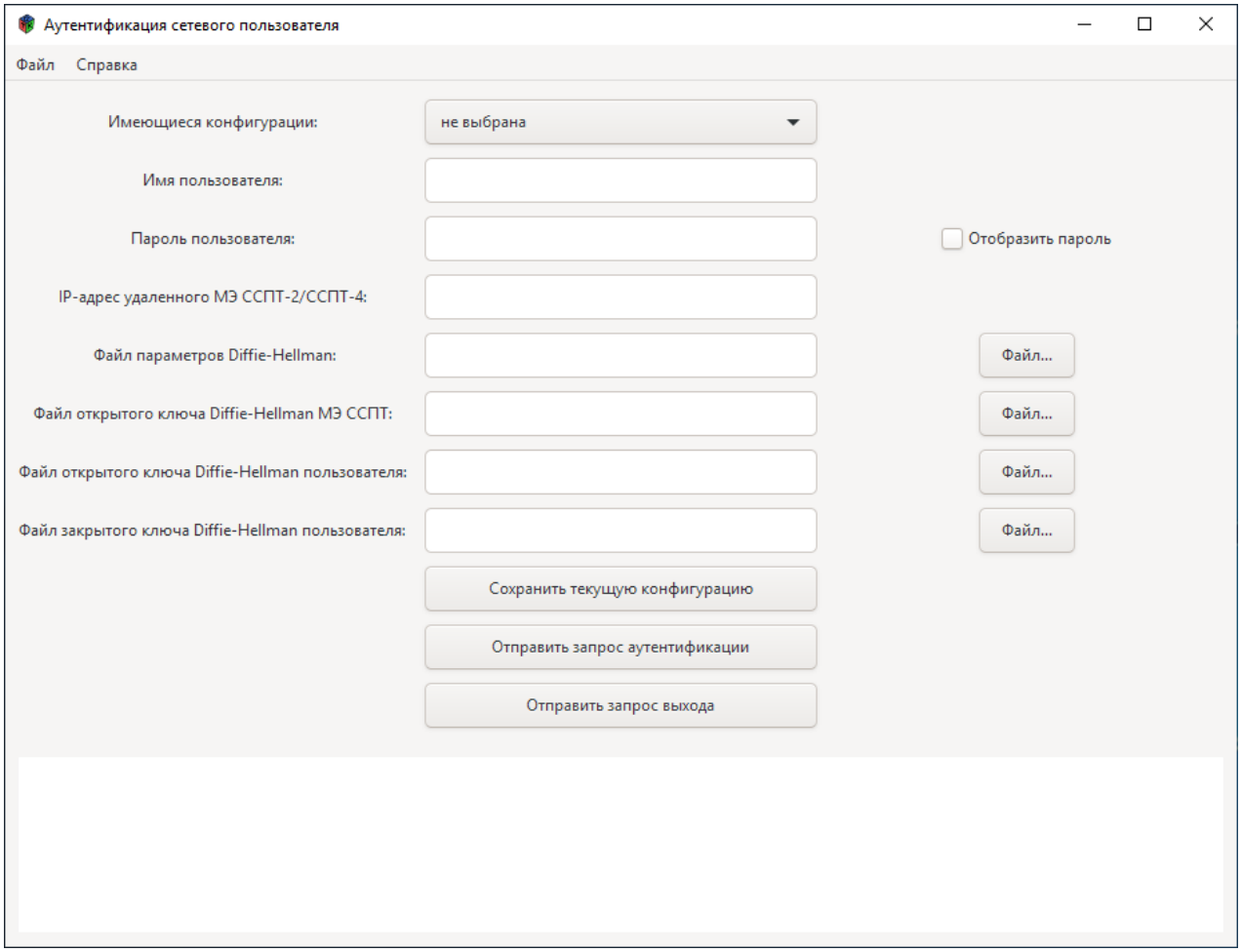


Рисунок 3.1: Главное окно графической оболочки

Главное окно содержит следующие элементы пользовательского интерфейса:

- `Имеющиеся конфигурации` – выпадающий список выбора ранее сохраненных конфигураций графической оболочки (значение, выводимое по умолчанию: не выбрана);
- `Имя пользователя` – поле ввода имени сетевого пользователя;
- `Пароль пользователя` – поле ввода пароля сетевого пользователя;
- `Отобразить пароль` – кнопка-флаг, используемая для отображения/сокрытия пароля, введенного в поле `Пароль пользователя`;
- `IP-адрес удаленного МЭ ССПТ-2/ССПТ-4` – поле ввода IP-адреса МЭ ССПТ-4А1;
- Поля ввода путей к файлам, необходимым для формирования защищенного запроса к МЭ ССПТ-4А1:
  - ✔ `Файл параметров Diffie-Hellman`;
  - ✔ `Файл открытого ключа Diffie-Hellman МЭ ССПТ`;
  - ✔ `Файл открытого ключа Diffie-Hellman пользователя`;
  - ✔ `Файл зарытого ключа Diffie-Hellman пользователя`;

- `Файл...` – кнопки выбора соответствующего файла (из числа перечисленных выше) на ПК сетевого пользователя, по нажатию на кнопку открывается диалоговое окно выбора файла;
- `Сохранить текущую конфигурацию` – кнопка сохранения набора введенных значений полей ввода в файле конфигурации графической оболочки под заданным именем для последующего автоматического заполнения полей ввода;
- `Отправить запрос аутентификации` – кнопка отправки запроса аутентификации удаленному МЭ ССПТ-4А1;
- `Отправить запрос выхода` – кнопка отправки запроса выхода (завершения сеанса работы сетевого пользователя) удаленному МЭ ССПТ-4А1;
- Информационная область – безымянное текстовое поле, расположенное внизу главного окна, предназначено для вывода диагностических сообщений.

Для отправки запроса удаленному МЭ ССПТ-4А1 должны быть заполнены все поля ввода главного окна графической оболочки, перечисленные выше.

На рисунке 3.2, стр. 573 приведен пример главного окна графической оболочки после ввода всех данных, необходимых для формирования и отправки запроса удаленному МЭ ССПТ-4А1.

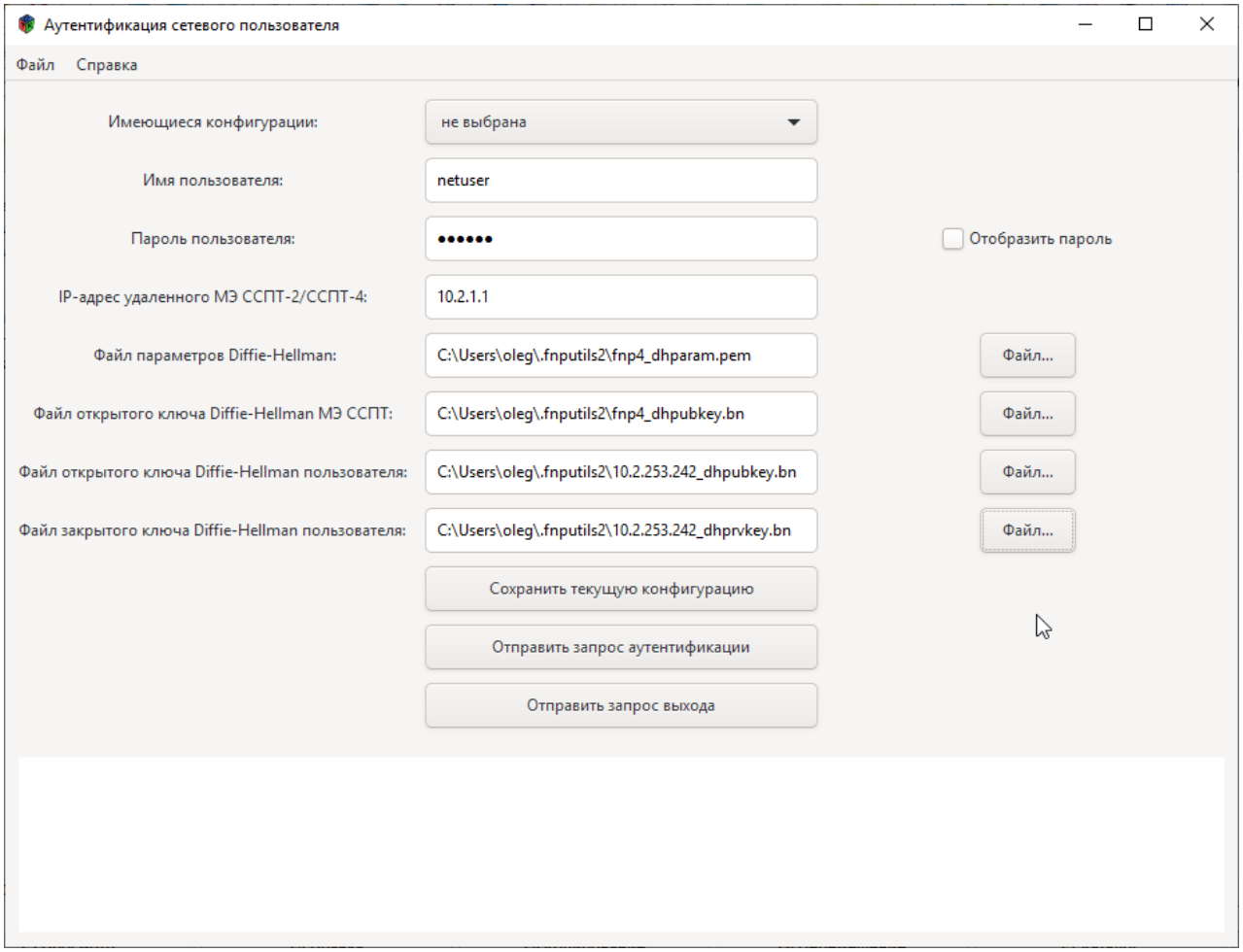


Рисунок 3.2: Главное окно графической оболочки: выполнен ввод данных

3.4.2. Отправка запросов удаленному МЭ ССПТ-4А1

Всего допускается два типа запросов к удаленному МЭ ССПТ-4А1:

- запрос аутентификации сетевого пользователя;
- запрос выхода (завершения сеанса работы) сетевого пользователя.

Для отправки запроса первого типа необходимо использовать кнопку **`Отправить запрос аутентификации`**, для отправки второго – кнопку **`Отправить запрос выхода`**.

Любая попытка отправки запроса удаленному МЭ ССПТ-4А1 сопровождается выводом диагностических сообщений от утилиты аутентификации сетевого пользователя в информационной области главного окна графической оболочки.

В случае успешной отправки запроса диагностические сообщения отображаются *зеленым цветом*. Если же запрос не был отправлен из-за какой-либо ошибки, то все диагностические сообщения, относящиеся к данной попытке запроса отображаются *красным цветом* и включают в себя сообщения о возникших ошибках.

Диагностика об успешной отправке запроса на указанный IP-адрес удаленного МЭ ССПТ-4А1 не подтверждает факт получения запроса удаленным МЭ ССПТ-4А1, а лишь свидетельствует о том что запрос был сформирован и отправлен по IP-адресу назначения.

При нажатии на кнопку отправки запроса выполняется контроль введенных данных, если выявлены какие-либо нарушения, то в информационную область выводятся соответствующие сообщения об ошибках.

Пример информационной области в результате успешной отправки *запроса аутентификации пользователя* приведен на рисунке 3.3, стр. 574. Если суммарное число строк диагностических сообщений превышает число строк информационной области, то в ней появляется вертикальная полоса прокрутки, которая позволяет просмотреть все выведенные сообщения. Пример информационной области в результате успешной отправки *запроса выхода пользователя* (для вывода всей диагностики по запросу использована полоса прокрутки)– на рисунке 3.4, стр. 574. Пример вывода диагностики в случае ошибки отправки запроса – на рисунке 3.5, стр. 574.

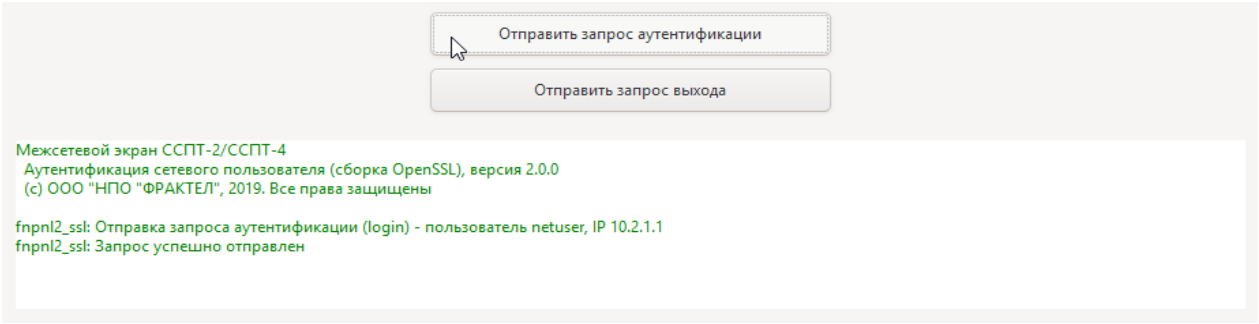


Рисунок 3.3: Запрос аутентификации: пример вывода

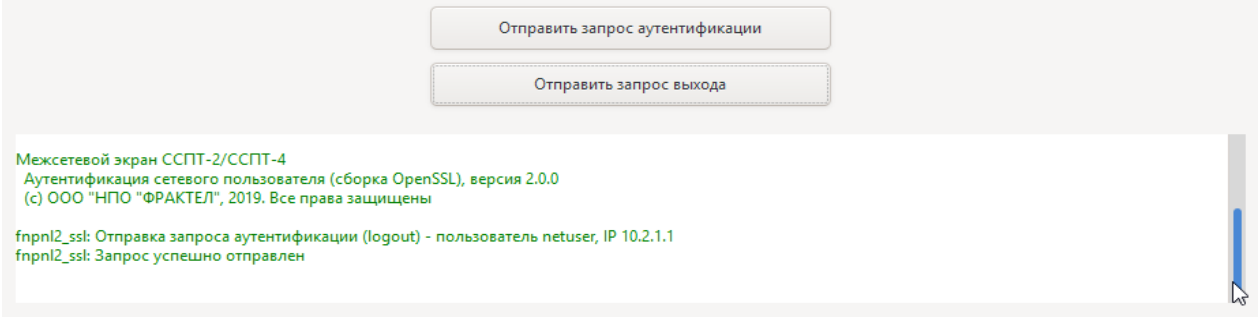


Рисунок 3.4: Запрос выхода пользователя: пример вывода при использовании прокрутки

Рисунок 3.5: Запрос аутентификации: пример вывода в случае ошибки

3.4.3. Использование конфигураций графической оболочки

Наборы значений полей ввода могут быть сохранены в виде именованных сущностей (*конфигураций графической оболочки*, далее – *конфигураций*) для последующего использования.

Конфигурация графической оболочки хранит значения всех полей ввода, кроме поля **“Пароль пользователя”**. Таким образом, для сохранения конфигурации заполнять поле **“Пароль пользователя”** не требуется. Если же оно заполнено, то его значение будет проигнорировано при сохранении конфигурации.

Графическая оболочка утилиты аутентификации позволяет хранить до **16** конфигураций.

Все конфигурации графической оболочки хранятся в конфигурационном файле **gfnpnl2_ssl.cfg**. Данный файл вместе с подкаталогом **.fnputils2** создается в домашнем каталоге пользователя ОС при первом запуске графической оболочки утилиты аутентификации.

Для сохранения текущего набора полей в конфигурацию необходимо нажать по кнопке **`Сохранить текущую конфигурацию`**. В результате будет выведено диалоговое окно, в котором должно быть указано имя сохраняемой конфигурации. По умолчанию в качестве имени конфигурации указывается имя пользователя, введенное в главном окне. Пример диалогового окна сохранения конфигурации приведен на рисунке 3.6, стр. 575.

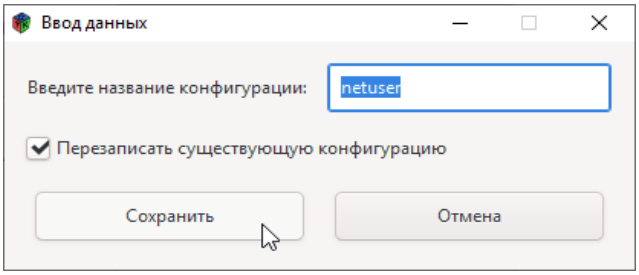


Рисунок 3.6: Пример диалогового окна сохранения конфигурации

Приведем пример сохранения еще одной конфигурации. Чтобы конфигурации отличались своим составом изменим значения полей “`Имя`” `пользователя` и “`IP-адрес удаленного ССПТ-2/ССПТ-4`”. Пример ввода новых значений данных полей приведен на рисунке 3.7, стр. 576. Пример диалогового окна сохранения конфигурации, соответствующего введенным данным приведен на рисунке 3.8, стр. 576.

Кнопка “Сохранить” диалогового окна сохранения конфигурации может быть заблокирована в следующих случаях:

- в конфигурационном файле графической оболочки уже сохранено **16** конфигураций и конфигурация с введенным именем отсутствует;
- посредством кнокпи-флага **запрещена** перезапись существующей конфигурации и конфигурация с введенным именем уже существует (по умолчанию перезапись **разрешена**).

Диалоговое окно сохранения конфигурации имеет кнопку-флаг **`Перезаписать существующую конфигурацию`**, которая служит для разрешения/запрета перезаписи

существующей конфигурации с именем равным введенному. Если выключить кнопку-флаг и ввести имя существующей конфигурации (**netuser**), то кнопка **Сохранить** будет заблокирована. При наведении курсора мышки на кнопку будет выведено всплывающее сообщение о причине блокировке кнопки. Пример блокировки кнопки **Сохранить** приведен на рисунке 3.9, стр. 576.

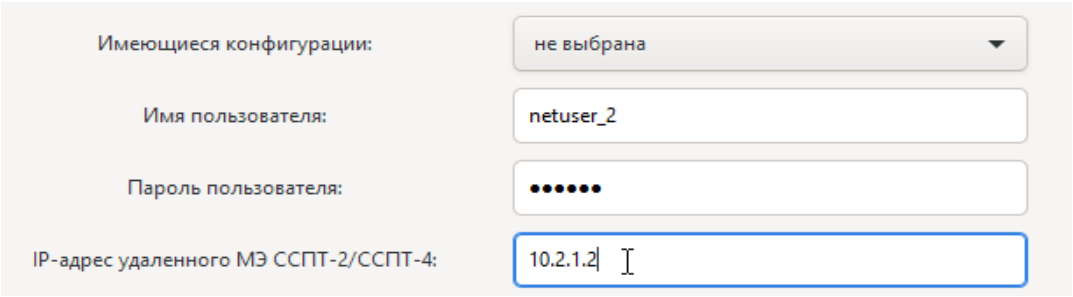


Рисунок 3.7: Изменение данных для сохранения во второй конфигурации

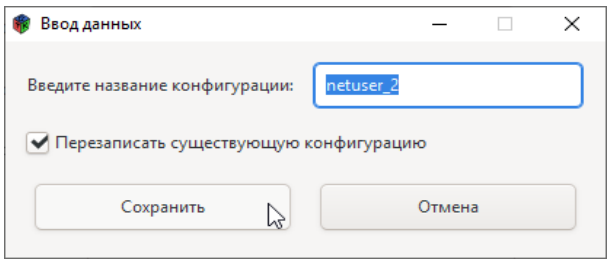


Рисунок 3.8: Диалоговое окно сохранения второй конфигурации

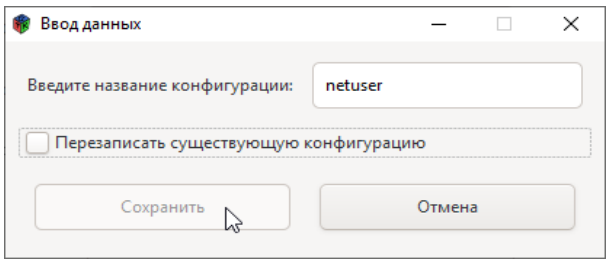


Рисунок 3.9: Пример блокировки кнопки "Сохранить"

Предположим, что вторая конфигурация была сохранена под именем `netuser_2`. Выбрать ранее сохраненную конфигурацию можно, воспользовавшись выпадающим списком “`Имеющиеся конфигурации`”. Пример выбора ранее сохраненной конфигурации `netuser_2` приведен на рисунке 3.10, стр 576. В результате выбора конфигурации поля ввода главного окна, за исключением поля `Пароль пользователя`, заполняются значениями из данной конфигурации, при этом справа от списка выбора конфигурации появляется кнопка **Удалить текущую конфигурацию**. Пример вывода данной кнопки приведен на рисунке 3.11, стр. 577.

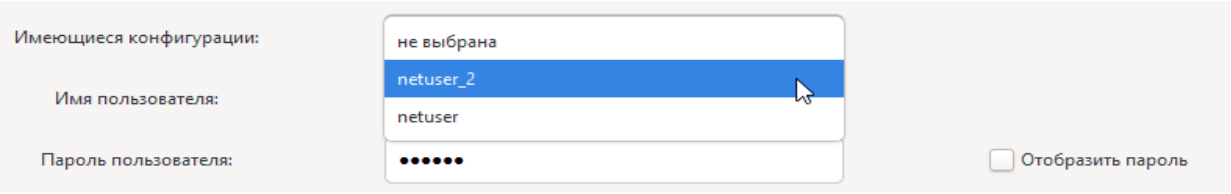


Рисунок 3.10: Выбор конфигурации из списка

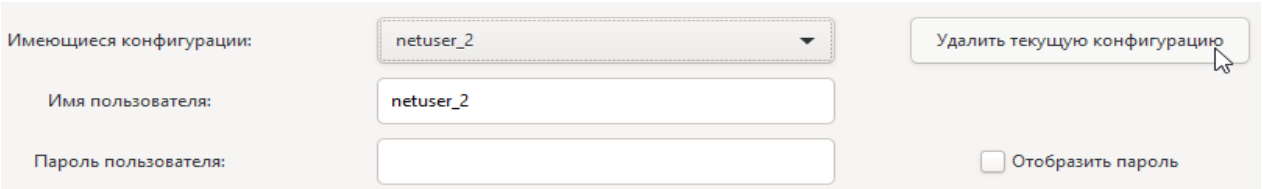


Рисунок 3.11: Кнопка удаления выбранной конфигурации

В результате удаления конфигурации в списке выводится значение по умолчанию: **не выбрана**, все поля ввода очищаются.

Приложение И. Протокол управления МЭ ССПТ-4А1 FNPCP

Протокол управления МЭ ССПТ-4А1 FNPCP (далее – протокол FNPCP, *FNPCP – FNP Control Protocol*) является протоколом прикладного уровня и предназначен для организации взаимодействия как локальных, так и удаленных клиентских приложений с командным сервером МЭ ССПТ-4А1.

Протокол FNPCP является текстовым протоколом, основанным на передаче текстовых строк предопределенного формата.

При взаимодействии клиентского приложения с командным сервером по протоколу FNPCP должна быть реализована следующая последовательность действий, которая может циклически повторяться:

1) передача запроса от клиентского приложения к командному серверу;
2) передача ответа на запрос от командного сервера к клиентскому приложению.

И.1. Формат запросов к командному серверу МЭ ССПТ-4А1

Существуют два типа сообщений (запросов), направляемых от клиентского приложения к командному серверу МЭ ССПТ-4А1:

1) **запрос на авторизацию**. Запрос на авторизацию посылается клиентским приложением для создания нового сеанса администратора МЭ ССПТ-4А1. Запрос на авторизацию состоит из трех текстовых строк, каждая из которых заканчивается символом перевода строки:

```
<идентификатор_администратора>\n
<пароль_администратора>\n
[<IP_адрес_клиента>]\n
```

   Параметр последней строки является необязательным. Последняя строка может быть оставлена пустой, но третий символ перевода строки должен присутствовать всегда. Если параметр <IP_адрес_клиента> отсутствует, то командный сервер будет пытаться определить его самостоятельно исходя из характеристик текущего сетевого либо локального соединения;

2) **запрос на выполнение команд МЭ ССПТ-4А1**. После успешного выполнения запроса на авторизацию клиентское приложение получает идентификатор сеанса администратора МЭ ССПТ-4А1, который оно использует при последующих передачах команд командного языка МЭ ССПТ-4А1 для их выполнения. Запрос на выполнение команд МЭ ССПТ-4А1 состоит из двух текстовых строк, каждая из которых заканчивается символом перевода строки:

```
<идентификатор_сеанса_администратора>\n
<команда_ССПТ-4А1>\n
```

Для корректного завершения сеанса администратора, клиентское приложение должно передать на выполнение команду **exit**.

И.2. Формат ответов от командного сервера МЭ ССПТ-4А1

После отправки запроса командному серверу клиентское приложение должно получить ответное сообщение, содержащее диагностику выполнения запроса и другую дополнительную информацию, содержание которой варьируется в зависимости от типа запроса и выполняемой команды МЭ ССПТ-4А1. В общем случае, ответ командного сервера также представляет собой набор текстовых строк:

```
<диагностика>\n
[<диагностика>\n]
[...]
[<дополнительная_информация>\n]
[...]
```

Строка диагностики имеет следующий формат:

```
<ПРЕФИКС_ПОДСИСТЕМЫ>-{E|W|I}-XXX.YY.ZZZZ-<текст_сообщения>[ (<системная_ошибка>)]
```

где:

- `<ПРЕФИКС_ПОДСИСТЕМЫ>` – идентификатор подсистемы, от которой получено сообщение:
  - ✔ `FNPAPI` – сообщения библиотеки сервисных функций ПО МЭ ССПТ-4А1;
  - ✔ `FNPSH` – сообщения командного интерпретатора МЭ ССПТ-4А1;
  - ✔ `FNPSHD` – сообщения командного сервера МЭ ССПТ-4А1
- {`E`|`W`|`I`} – класс (категория) сообщения:
  - ✔ `E` – сообщение об ошибке;
  - ✔ `W` – предупреждающее сообщение;
  - ✔ `I` - информационное сообщение;
- `XXX.YY.ZZZZ` – составной код сообщения (`XXX`, `YY`, `ZZZZ` - шестнадцатеричные числа):
  - ✔ `XXX` – код продукта. Для ПО МЭ ССПТ-4А1 код продукта – `007`;
  - ✔ `YY` – код подсистемы ПО МЭ ССПТ-4А1:
    - ◆ `01` – библиотека сервисных функций ПО МЭ ССПТ-4А1;
    - ◆ `02` – командный интерпретатор МЭ ССПТ-4А1;
    - ◆ `03` – командный сервер МЭ ССПТ-4А1;
  - ✔ `ZZZZ` – код диагностического сообщения данной подсистемы ПО МЭ ССПТ-4А1:
    - ◆ `1ZZZ` – диапазон кодов для сообщений об ошибках;
    - ◆ `2ZZZ` – диапазон кодов для предупреждающих сообщений;

- 3ZZZ – диапазон кодов для информационных сообщений;

- <текст_сообщения> – текстовая интерпретация кода диагностического сообщения. Текст сообщения выводится на русском языке в кодировке UTF-8;
- <системная_ошибка> – необязательное сообщение, включаемое в строку диагностического сообщения, если при выполнении команды произошла системная ошибка. Сообщения о системных ошибках являются стандартными для УОС МЭ ССПТ-4А1. Сообщение о системной ошибке всегда выводится на английском языке.

Например, диагностическое сообщение

```
FNPSH-I-007.02.30BD-Режим просмотра изменен
```

является информационным сообщением командного интерпретатора МЭ ССПТ-4А1 с кодом 0x30BD (шестнадцатеричный).

И.3. Ответ командного сервера МЭ ССПТ-4А1 на запрос авторизации

Формат ответа командного сервера МЭ ССПТ-4А1 на запрос авторизации варьируется в зависимости о результата самой процедуры авторизации администратора на МЭ ССПТ-4А1.

В случае успешной авторизации администратора ответ командного сервера выглядит следующим образом:

```
<диагностика>\n
<имя_администратора>\n
<идентификатор_сеанса_администратора>\n
<IP_адрес_клиента>\n
<PID_процесса>\n
<права_доступа>\n
```

где:

- <диагностика> – диагностическое сообщение командного интерпретатора МЭ , извещающее о результате процедуры авторизации администратора:
  - ✔ информационное сообщение с кодом 0x3000 – администратор авторизован, сеансу администратора назначены все права доступа, разрешенные в учетной записи администратора на МЭ ССПТ-4А1:

```
FNPSH-I-007.02.3000-Нет ошибок
```

  - ✔ предупреждение с кодом 0x2002 — пользователь авторизован, но сессии пользователя назначена только часть привилегий из списка разрешенных в учетной записи пользователя на МЭ ССПТ-4А1:

```
FNPSH-W-007.02.2002-Вход администратора с ограниченными привилегиями (read)
```

- <имя_администратора> – имя авторизованного администратора МЭ ССПТ-4А1. Длина имени администратора может быть от **2** до **128** символов, допустимые символы – строчные латинские буквы (a-z), цифры (0-9), символы подчеркивания ('_'), точки ('.'), коммерческого “at” ('@') и дефиса ('-');
- <идентификатор_сеанса_администратора> – строка идентификатора сеанса администратора МЭ ССПТ-4А1. После успешной авторизации администратора, сеансу этого администратора присваивается уникальный идентификатор, однозначно определяющий данный сеанс среди других сеансов администраторов на МЭ ССПТ-4А1. Длина идентификатора сеанса администратора составляет **128** байт;
- <IP_адрес_клиента> – IP-адрес, с которого клиентское приложение установило соединение с командным сервером МЭ ССПТ-4А1 и отправило запрос на авторизацию;
- <PID_процесса> – идентификатор процесса командного интерпретатора, запущенного на МЭ ССПТ-4А1 и выполняющего команды командного языка МЭ ССПТ-4А1, передаваемые в рамках данного сеанса администратора;
- <права_доступа> – список прав доступа, назначенных для данного сеанса администратора.

В случае неудачной авторизации администратора ответ командного сервера содержит только одну строку диагностического сообщения об ошибке, отражающую причину отказа.

И.4. Ответ командного сервера МЭ ССПТ-4А1 на запрос выполнения команд

Ответ командного сервера на запрос выполнения команд командного языка МЭ ССПТ-4А1 имеет следующий формат:

```
<диагностика>\n
[<диагностика>\n]
[...]
[<количество_строк>\n
<дополнительная_информация>\n
[<дополнительная_информация>\n]
[...]
```

Ответ может содержать одну строку или более одной строки:

- <диагностика> – диагностическое сообщение (информационное сообщение, предупреждение или ошибка), извещающее о результате выполнения команды. Диагностическое сообщение присутствует всегда. В зависимости от выполняемой команды, строк диагностических сообщений может быть несколько;
- <количество_строк> – указывает количество строк следующей ниже дополнительной информации, которые необходимо передать клиентскому приложению в результате выполнения команды;

- <дополнительная_информация> – строки дополнительной информации. Количество этих строк должно строго соответствовать значению параметра <количество_строк>, передаваемому в строке ответа, следующей после строк диагностических сообщений. Состав дополнительной информации существенно зависит от выполняемой команды.

Приложение К. Перечень диагностических сообщений ПО СОВа-4

К.1. Формат диагностических сообщений ПО СОВа-4

Формализованные диагностические сообщения ПО СОВа-4 имеют следующий формат:

```
FNPRUT-{E|W}-101.01.ZZZZ-<текст_сообщения>[ (<системная_ошибка>)]
```

где:

- `FNPRUT` – префикс (идентификатор) ПО СОВа-4;
- `{E|W}` – класс (категория) сообщения:
  - ✔ `E` – сообщение об ошибке;
  - ✔ `W` – предупреждающее сообщение;
- `101.01.ZZZZ` – составной код сообщения (`ZZZZ` - шестнадцатеричное число):
  - ✔ `101` – код продукта ПО СОВа-4;
  - ✔ `01` – код основной программы ПО СОВа-4 (код подсистемы);
  - ✔ `ZZZZ` – код диагностического сообщения данной подсистемы ПО СОВа-4:
    - ◆ `1ZZZ` – диапазон кодов для сообщений об ошибках;
    - ◆ `2ZZZ` – диапазон кодов для предупреждающих сообщений.
- `<текст_сообщения>` – текстовая интерпретация кода диагностического сообщения. Текст сообщения выводится на русском языке в кодировке UTF-8;
- `<системная_ошибка>` – необязательное сообщение, включаемое в строку диагностического сообщения, если при выполнении операции произошла системная ошибка. Сообщения о системных ошибках являются стандартными для УОС ПО СОВа-4.

Диагностические сообщения класса **предупреждающих сообщений** ПО СОВа-4 выводятся в том случае, если операция не может быть выполнена по каким-либо причинам, не относящимся к ошибкам выполнения (например: на FAT-разеделе USB-носителя СОВа-4 отсутствуют файлы обновлений и при этом в меню СОВа-4 был выбран пункт `Выбор файла обновления`).

Диагностические сообщения класса **сообщений об ошибках** ПО СОВа-4 выводятся в случае ошибок выполнения функций СОВа-4 (например: ошибка монтирования UFS-раздела носителя данных МЭ ССПТ-4А1).

Информационные сообщений ПО СОВа-4 не формализованы, т. е. не имеют уникальных кодов и выводятся в качестве подтверждения успешного выполнения функции ПО СОВа-4, выбранной администратором.

Формализованные диагностические сообщения ПО СОВа-4 приведены в разделе К.2, стр. 584.

Статус выполнения процедуры обновления ПО МЭ ССПТ-4А1 фиксируется в журнале обновлений ПО СОВа-4 (см. раздел 7, стр. 394). Все возможные статусы выполнения процедуры обновления, а также действий по подтверждению и отмене последнего выполненного обновления, приведены в разделе К.3, стр. 587.

К.2. Диагностические сообщения ПО СОВа-4

К.2.1. Сообщения об ошибках

Коды всех сообщений об ошибках ПО СОВа-4, их текстовая интерпретация и описание представлены в таблице К.1.

Таблица К.1: Сообщения об ошибках ПО СОВа-4

Код	*Сообщение*	*Описание*
101.01.1000	Ошибка распределения памяти	Системная ошибка, связанная с невозможностью динамически выделить запрошенный объем памяти.
101.01.1001	Недопустимый аргумент в вызове функции	В функцию передан аргумент с недопустимым значением.
101.01.1002	Ошибка компиляции регулярного выражения PCRE	Системная ошибка при компиляции регулярных выражений.
101.01.1003	Ошибка сравнения шаблона PCRE	Системная ошибка при сравнении строки с регулярным выражением (невозможно установить факт соответствия или несоответствия регулярному выражению).
101.01.1004	Размерность вектора обнаруженных подстрок недостаточна	Неверный формат вспомогательного параметра, используемого при проверке строки по регулярному выражению.
101.01.1005	Недопустимое терминальное устройство	Основная программа ПО СОВа-4 запущена на недопустимом терминальном устройстве.
101.01.1006	Ошибка переключения терминального устройства	Ошибка при попытке переключения терминального устройства.
101.01.1007	Ошибка вызова sysctl	Ошибка при вызове системной функции sysctl().
101.01.1008	Ошибка открытия устройства cpuctl	Ошибка при попытке открытия файла-устройства /dev/cpuctl<N>
101.01.1009	Ошибка получения CPUid	Ошика получения идентификатора ЦП МЭ ССПТ-4А1.
101.01.100A	Нарушен системный список интерфейсов	Нарушен формат списка структур УОС с данными о сетевых интерфейсах.
101.01.100B	Ошибка чтения файла ключа ПО СОВа	Ошибка чтения файла ключа привязки ПО СОВа-4 к экземпляру МЭ ССПТ-4А1

Код	Сообщение	Описание
101.01.100C	Системная ошибка	Системная ошибка УОС. Согласно формату диагностического сообщения: в скобках – сообщение о конкретной системной ошибке УОС.
101.01.100D	Ошибка библиотеки cdialog	Ошибка при вызове функции библиотеки cdialog
101.01.100E	Нарушен формат файла контрольных сумм	Формат файла контрольных сумм МЭ ССПТ-4А1 нарушен.
101.01.100F	Ошибка обновления файла контрольных сумм	Ошибка при попытке перезаписи файла контрольных сумм МЭ ССПТ-4А1 нарушен в ходе выполнения функции сброса одного из конфигурационных файлов МЭ ССПТ-4А1
101.01.1014	Ошибка чтения файла	Ошибка чтения какого-либо файла (например: журнала обновлений, dump-образа восстановления ПО и т. д.) в ходе работы ПО СОВа-4
101.01.1015	Ошибка записи файла	Ошибка записи какого-либо файла (например: журнала обновлений, dump-образа восстановления ПО и т. д.) в ходе работы ПО СОВа-4
101.01.1016	Ошибка установки атрибутов файла	Ошибка установки атрибутов какого-либо файла в ходе работы ПО СОВа-4
101.01.1017	Нарушен формат файла конфигурации	Нарушен формат основного файла конфигурации ПО СОВа-4
101.01.1018	Нарушен формат файла паролей	Нарушен формат файла учетных записей администраторов МЭ ССПТ-4А1
101.01.1019	Ошибка монтирования UFS-раздела	Ошибка в ходе монтирования UFS-раздела носителя данных МЭ ССПТ-4А1
101.01.101A	Ошибка размонтирования UFS-раздела	Ошибка в ходе размонтирования UFS-раздела носителя данных МЭ ССПТ-4А1
101.01.101B	Ошибка установки переменной окружения	Ошибка установки переменной окружения УОС
101.01.101C	Ошибка межпроцессного взаимодействия	Ошибка создания неименованного канала для взаимодействия основного процесса ПО СОВа-4 с дочерним утилитарным процессом.
101.01.101D	Ошибка создания дочернего процесса	Ошибка создания дочернего процесса основным процессом ПО СОВа-4
101.01.101E	Не достаточно прав доступа к файлу	У ПО СОВа-4 нет требуемых прав доступа к файлу.
101.01.102F	Ошибка записи файлов обновлений на устройство ССПТ	Ошибка записи файлов обновления ПО на носитель данных МЭ ССПТ-4А1
101.01.1030	Ошибка распаковки файлов обновления	Ошибка распаковки файлов обновления ПО МЭ ССПТ-4А1
101.01.1032	Ошибка удаления временных файлов	Временные файлы обновления не были удалены из-за ошибки выполнения команды удаления файлов УОС
101.01.1033	Ошибка проверки подписи обновления	Цифровая подпись файла обновления не верифицирована. Обновление не будет применено.
101.01.1034	Ошибка декодирования обновления	Ошибка преобразования файла обновления к формату для записи файлов обновления на носитель данных МЭ ССПТ-4А1
101.01.1035	Временный dump-образ носителя МЭ ССПТ отсутствует	Временный dump-образ носителя данных МЭ ССПТ-4А1 для отмены неподтвержденного уведомления отсутствует.
101.01.1036	Недопустимая версия обновления	Версия обновления должна быть больше текущей версии ПО МЭ ССПТ-4А1

Код	Сообщение	Описание
101.01.1037	Ошибка подтверждения обновления	Подтверждение последнего обновления не было выполнено из-за ошибки
101.01.103A	Ошибка создания резервных копий конфигурационных файлов МЭ ССПТ	Не удалось создать резервные копии конфигурационных файлов МЭ ССПТ-4А1 из-за ошибки.
101.01.103B	Ошибка форматирования носителя данных МЭ ССПТ	Форматирование раздела носителя данных МЭ ССПТ-4А1 не было выполнено из-за ошибки.
101.01.103C	Ошибка создания временного dump-образа носителя данных МЭ ССПТ	Временный dump-образ носителя данных МЭ ССПТ-4А1 (используемый для восстановления состояния МЭ до начала процедуры обновления) не был создан из-за ошибки.
101.01.103D	Недопустимое имя терминального устройства	Основная программа ПО СОВа-4 запущена на терминальном устройстве с недопустимым именем файла устройства.
101.01.103E	Недопустимый номер терминального устройства	Основная программа ПО СОВа-4 запущена на терминальном устройстве с недопустимым номером в имени файла устройства.

К.2.2. Предупреждающие сообщения

Коды всех предупреждающих сообщений ПО СОВа-4, их текстовая интерпретация и описание представлены в таблице К.2.

Таблица К.2: Предупреждающие сообщения ПО СОВа-4

Код	Сообщение	Описание
101.01.2000	ПО СОВа привязано к другому набору оборудования МЭ ССПТ	Данный экземпляр ПО СОВа-4 привязан к другому экземпляру МЭ ССПТ-4А1. Часть функций ПО СОВа-4 (восстановление и обновление ПО МЭ ССПТ-4А1, восстановление конфигурационных файлов) недоступны. Сообщение может быть выведено только при старте ПО СОВа-4
101.01.2003	Файлы обновлений отсутствуют	Файлы обновлений ПО МЭ ССПТ-4А1 отсутствуют на FAT-разделе USB-носителя СОВа-4.
101.01.2004	Отмена недоступна: обновления еще не выполнялись	Функция отмены последнего неподтвержденного обновления ПО МЭ ССПТ-4А1 недоступна, т. к. обновления еще не производились.
101.01.2005	Отмена недоступна: последнее обновление не было применено из-за ошибок	Отмена последнего неподтвержденного обновления ПО МЭ ССПТ-4А1 недоступна, так как оно не было применено из-за ошибок в ходе процедуры обновления ПО.
101.01.2006	Отмена недоступна: последнее обновление уже подтверждено	Обновление, подтвержденное администратором, не может быть отменено.
101.01.2007	Отмена недоступна: последнее обновление уже отменено	Отмена последнего обновления не доступна, так как уже была выполнена равнее администратором.
101.01.2008	Журнал обновлений пуст	Сообщение выводится при попытке просмотра журнала обновлений, когда в нем отсутствуют записи.
101.01.2009	Функция недоступна, так как ПО СОВа привязано к другому набору оборудования МЭ ССПТ	Данное сообщение выводится при выборе пунктов Восстановление и Обновление главного меню ПО СОВа-4 в случае несоответствия экземпляров ПО СОВа-4 и МЭ ССПТ-4А1 друг другу.

Код	Сообщение	Описание
101.01.200D	Проверка целостности не пройдена	При проверке целостности исполняемых файлов на носителе данных СОВа-4 возникла системная ошибка, либо целостность, как минимум, одного из файлов нарушена.
101.01.200E	Функция недоступна, так как последняя проверка целостности не была успешной	Данное сообщение выводится при выборе пунктов Восстановление и Обновление главного меню ПО СОВа-4 в случае, если последняя проверка целостности не была успешной.

К.3. Статусы выполнения процедуры обновления ПО МЭ ССПТ-4А1

Статус имевшей место процедуры обновления ПО МЭ ССПТ-4А1 фиксируется в журнале обновлений ПО СОВа-4. Статусы, относящиеся к ошибкам в ходе процедуры обновления, а также к ошибке подтверждения выполненного обновления имеют численные коды, которые фиксируются и отображаются в записях журнала обновлений. Статусы, свидетельствующие об успешном выполнении процедуры обновления ПО МЭ ССПТ-4А1, а также об успешных действиях по подтверждению или отмене выполненного обновления, отображаются в записях журнала обновлений в словесной форме. Полный перечень статусов процедуры обновления и связанных с ней действий (по подтверждению и отмене обновлений) представлен в таблице К.3.

Таблица К.3: Статусы выполнения процедуры обновления ПО МЭ ССПТ-4А1

Код/словесное обозначение	Описание
Выполнено	Обновление успешно выполнено, но еще не было подтверждено администратором. Возможна отмена данного обновления администратором.
Подтверждено	Успешно выполненное обновление было подтверждено администратором. Отмена обновления невозможна.
Отменено	Успешно выполненное обновление было отменено администратором. ПО МЭ ССПТ-4А1 возвращено к состоянию (версии) до выполнения данного обновления.
1	Ошибка декодирования файла обновления. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
2	Ошибка распаковки содержимого файла обновления. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
3	Нарушено содержимое файла обновления. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
4	Цифровая подпись не соответствует файлу обновления. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
5	Ошибка монтирования носителя МЭ ССПТ. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
6	Ошибка создания резервных копий конфигурационных файлов МЭ ССПТ. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
7	Ошибка формирования образа носителя данных. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
8	Ошибка форматирования носителя данных МЭ ССПТ. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.

Код/словесное обозначение	Описание
9	Ошибка копирования файлов на носитель МЭ ССПТ. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
10	Недопустимая версия обновления. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
11	Ошибка обновления контрольных сумм. Обновление не выполнено: ПО МЭ ССПТ-4А1 – в прежнем состоянии.
12	Ошибка подтверждения обновления. Успешно выполненное обновление не было подтверждено из-за системной ошибки

Лист регистрации изменений									
Изм	Номера листов (страниц)				Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					