Общество с ограниченной
ответственностью
«НПО «ФРАКТЕЛ»

Межсетевой экран ССПТ-2 версии 1.3

Руководство администратора

РКДЕ.5014107-05-0134 РА

Санкт-Петербург
2020

Версия документа: 1.3.1 (последнее обновление 09.07.2013) Версия программного обеспечения ССПТ-2: FNP2_RELEASE_1_3-p1.2

Санкт-Петербург. 194064. Российская Федерация
Телефон: +7 (812) 406-83-92
+7 (921) 781-62-00
E-mail: info@fractel.ru
www.fractel.ru

АННОТАЦИЯ

Настоящее руководство описывает общие принципы функционирования, порядок настройки и управления **межсетевым экраном ССПТ-2**, его конструктивные особенности и основные технические характеристики и предназначено для специалистов в области сетевой безопасности и администраторов сетей, использующих ССПТ-2 для решения вопросов, связанных с ограничением доступа к информационным и сетевым ресурсам в сетях Ethernet.

Для получения более подробной информации по работе и настройке подсистем ССПТ-2 следует обращаться к документу "*МЕЖСЕТЕВОЙ ЭКРАН ССПТ-2. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. Руководство администратора. РКДЕ.5014107-05-0134*". Указанный документ располагается на компакт-диске (CD-ROM), входящем в комплект поставки ССПТ-2 (`docs/fnp2_ag.pdf`, путь к файлу указан относительно корня файловой системы компакт-диска).

ССПТ-2 работает в режиме скрытной фильтрации и предназначен для защиты автоматизированных систем (АС), в которых обрабатывается информация различного уровня конфиденциальности.

ССПТ-2 может использоваться в локальных вычислительных сетях (ЛВС), построенных на базе технологии Ethernet с пропускной способностью 10/100/1000 Мбит/с.

Настоящий документ представляет собой краткое руководство администратора ССПТ-2:

- **Глава 1** – назначение, область применения и основные функциональные характеристики ССПТ-2;
- **Глава 2** – описание начала работы с ССПТ-2, подключение для управления и начальные настройки. Основы работы с командным интерфейсом и с WEB-интерфейсом администратора ССПТ-2;
- **Приложения**:
  - ✔ установка на управляющий компьютер программного обеспечения для управления ССПТ-2 через системную консоль и PPP соединение по последовательному порту RS-232;
  - ✔ командный язык ССПТ-2 – описание всех команд, синтаксис, условия применения и ограничения использования;
  - ✔ диагностические сообщения командного интерфейса ССПТ-2;
  - ✔ варианты исполнения ССПТ-2.

Настоящее руководство соответствует версии программного обеспечения ССПТ-2 FNP2_RELEASE_1_3-p1.2.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ

АС – автоматизированная система
ЛВС – локальная вычислительная сеть
ПО – программное обеспечение
ПФ – пакетный фильтр
УЦ – удостоверяющий центр
ЦП – центральный процессор

ARP – Address Resolution Protocol
BPF – Berkeley Packet Filter
BOFL – Breath OF Life
CPU – Central Processing Unit
ECN - Explicit Congestion Notification
FTP – File Transfer Protocol
HTTP – HyperText Transfer Protocol
ICMP – Internet Control Message Protocol
IP – Internet Protocol
IPX – Internetwork Packet eXchange
LAN – Local Area Network
MAC – Media Access Control
NAT – Network Address Translation
NTP – Network Time Protocol
OUI – Organizational Unique Identifier
POP3 – Post Office Protocol 3
PPP – Point-to-Point Protocol
RADIUS – Remote Authentication Dial In User Service
RARP – Reverse Address Resolution Protocol
SAP – Service Accesss Point
SMTP – Simple Mail Transfer Protocol
TCP – Transmission Control Protocol
TLS – Transport Layer Secure
TOS – Type Of Service
TTL – Time To Live
UDP – User Datagaram Protocol
URL – Universal Resource Locator
VLAN – Virtual Local Area Network

1. Общие положения

1.1. Назначение и область применения

Межсетевой экран ССПТ-2 работает в режиме скрытной фильтрации и предназначен для защиты автоматизированных систем (АС), в которых обрабатывается информация различных уровней конфиденциальности.

ССПТ-2 применяется для разделения сегментов локальной вычислительной сети (ЛВС) с целью обеспечения защиты информации от несанкционированного доступа посредством:

- пакетной фильтрации на основе анализа параметров заголовков пакетов на различных уровнях сетевого взаимодействия – от канального до транспортного уровней включительно;
- управления транспортными соединениями между узлами ЛВС на основе анализа параметров виртуальных соединений и/или запросов на их установление;
- контроля данных прикладного уровня на основе заданных критериев и с учетом направления передачи потока пакетов.

ССПТ-2 может использоваться в ЛВС, построенных на базе технологии Ethernet с пропускной способностью 10/100/1000 Мбит/с.

1.2. Основные функциональные характеристики

Межсетевой экран ССПТ-2 обладает следующими основными функциональными характеристиками:

- многоуровневая, многопротокольная скрытная пакетная фильтрация по совокупности критериев;
- управление сессиями – контроль транспортных соединений на основе проверки соответствия каждого обрабатываемого пакета контексту сессии;
- трансляция сетевых адресов (режим NAT) с целью сокрытия внутренней сети с выделением "*демилитаризованной зоны*";
- возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети – *аутентификация сетевых пользователей* (может быть активизирована только при включенном режиме NAT);
- блокировка сетевых flood-атак на основе выявления и последующей фильтрации аномальной активности сетевых потоков данных;
- выгрузка файлов регистрации событий и пакетов с использованием протоколов FTP и SYSLOG;
- защита канала управления на основе алгоритмов шифрования ГОСТ 28147-89 и ГОСТ Р 34.10-2001;
- контроль доступа к интерфейсам управления ССПТ-2 на основе списка доверенных IP-адресов;
- синхронизация системного времени операционной системы ССПТ-2 по протоколу NTP;
- "зеркалирование" трафика на заданный фильтрующий интерфейс для последующих анализа и проверки с использованием специальных средств контроля;
- горячее резервирование для создания систем фильтрации высокой готовности и отказоустойчивости.

1.3. Технология скрытной фильтрации

Эффективность применения ССПТ-2 достигается за счет использования технологии скрытной фильтрации (режим "stealth") – инновационного решения, защищенного Патентом РФ № 2214623, позволяющего скрывать для средств удаленного сетевого мониторинга место расположения

ССПТ-2, 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 ССПТ-2:

- 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;
- позволяет выявлять аномальные или неавторизованные воздействия (*intrusion detecting*) и для защиты от них формировать динамические правила фильтрации.

1.4. Режимы функционирования и характеристики

1.4.1. Пакетная фильтрация и управление сессиями

ССПТ-2 предоставляет широкие возможности по реализации режима скрытного контроля на основе фильтрации сетевого трафика. Правила фильтрации создаются независимо для различных уровней модели межсетевого взаимодействия OSI/ISO. Параметрами правил фильтрации являются поля заголовков пакетов. Действия, реализуемые над пакетом после применения к нему правила фильтрации, могут быть следующие:

1) **“отбросить”** пакет (“**drop**”) – пакет не будет передан ни на один из фильтрующих интерфейсов ССПТ-2;
2) “**пропустить**” пакет (“**accept**”) – пакет будет передан на следующий уровень фильтрации, если таковой имеется. В противном случае, пакет будет передан на фильтрующие интерфейсы ССПТ-2 в соответствии с маской выходных интерфейсов, определяемой совокупностью правил фильтрации всех уровней, которые были применены к данному пакету;
3) “**передать**” пакет (“**pass**”) – процедура фильтрации пакета будет завершена на данном уровне и пакет будет передан на фильтрующие интерфейсы ССПТ-2 в соответствии с маской выходных интерфейсов, определяемой совокупностью правил фильтрации всех уровней, которые были применены к данному пакету.

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

- для кадров **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;
- для протоколов **ARP/RARP**:
  - ✔ MAC-адреса отправителя/получателя;
  - ✔ IP-адреса отправителя/получателя;
  - ✔ тип сообщения (запрос/ответ);

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

- для протокола **IP версии 4**:
  - ✔ IP-адреса отправителя/получателя;
  - ✔ поле флагов TOS;
  - ✔ длина IP пакета;
  - ✔ фрагментация пакета (разрешена/запрещена, используется/не используется для данного пакета);
  - ✔ время жизни пакета (TTL);
  - ✔ протокол верхнего уровня;
- для протокола **IP версии 6** – в режиме “разрешить/запретить”;
- для протокола **IPX**:
  - ✔ адрес сети/узла отправителя;
  - ✔ сокет отправителя;
  - ✔ адрес сети/узла получателя;
  - ✔ сокет получателя;
  - ✔ тип пакета;
- для протокола **ICMP**:
  - ✔ тип ICMP сообщения;
  - ✔ код ICMP сообщения.

Транспортный уровень. Обеспечивается фильтрация следующих протоколов транспортного уровня, использующих на сетевом уровне протокол IP версии 4:

- для протокола **TCP**:
  - ✔ порт источника;
  - ✔ порт назначения;
  - ✔ флаги управления потоком (фильтрация по инициатору соединения);
- для протокола **UDP**:
  - ✔ порт источника;
  - ✔ порт назначения.

Прикладной уровень. Обеспечивается фильтрация следующих протоколов прикладного уровня:

- для протокола **HTTP** (доступ к WEB серверам):
  - ✔ фильтрация по адресам и фрагментам URL;
  - ✔ фильтрация по именам и фрагментам имен передаваемых файлов;
  - ✔ фильтрация по данным заголовка протокола HTTP;
- для протокола **SMTP** (электронная почта):
  - ✔ фильтрация по почтовым адресам отправителя/получателя;
  - ✔ фильтрация по данным заголовка протокола SMTP;
- для протокола **FTP** (обмен файлами):
  - ✔ 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 протоколов передачи **SQL** запросов (SQL*Net, MS-SQL, PostgreSQL, MySQL):
  - ✔ фильтрация по SQL запросам или их фрагментам.

Управление сессиями. Обеспечивается возможность управления сессиями для следующих протоколов:

- для протокола **TCP**:
  - ✔ контроль неизменности параметров (адреса, порты, интерфейсы) отправителя и получателя на протяжении всей сессии;
  - ✔ контроль корректности переходов между состояниями виртуального TCP соединения в соответствии с флагами управления;
  - ✔ контроль корректности номеров последовательностей;
- для протокола **UDP**:
  - ✔ контроль неизменности параметров (адреса, порты, интерфейсы) отправителя и получателя на протяжении всей сессии;
- для протокола **ICMP** (*только для режима утилиты ping*):
  - ✔ контроль неизменности параметров (адреса, идентификатор в заголовке ICMP) отправителя и получателя на протяжении всей сессии.

Режимы фильтрации и управления сессиями реализуются путем настройки правил фильтрации. В соответствии с моделью сетевого взаимодействия правила фильтрации имеют многоуровневую структуру, на которых выполняется пакетная фильтрация.

В системе правил фильтрации выделяются:

- **MAC-правила** – для канального уровня;
- **ARP-правила** – для уровня служебных протоколов ARP/RARP;
- **IP-правила** – для сетевого уровня, использующего протокол IP версии 4, включая транспортный уровень, использующий протоколы TCP или UDP, и уровень служебного протокола ICMP;
- **временные IP-правила** – динамически создаваемые IP-правила при работе пакетного фильтра. Могут быть использованы для отражения сетевых атак, временного блокирования абонентов защищаемых сегментов сети и т. п.;
- **IPX-правила** – для сетевого уровня, использующего протокол IPX;
- **AP-правила** – правила фильтрации прикладного уровня, всегда связаны с соответствующими IP-правилами;
- **интервалы времени** – вспомогательные структуры, позволяющие ограничивать время действия основных правил фильтрации (MAC, ARP, IP и IPX-правил);
- **VLAN-группы** – специальные структуры, используемые для управления процессом фильтрации с учетом идентификатора VLAN (IEEE 802.1p/Q).

1.4.2. Средства администрирования ССПТ-2

Администратору ССПТ-2 предоставляются различные средства администрирования:

- **интерфейс командной строки** как для локального (с системной консоли ССПТ-2), так и для удаленного сетевого администрирования;
- **WEB-интерфейс администратора** для удаленного сетевого администрирования;
- **монитор централизованного управления** для удаленного сетевого мониторинга и управления группой ССПТ-2.

Все средства администрирования предоставляют следующие возможности по настройке и управлению ССПТ-2:

- интерфейс командной строки ССПТ-2 предоставляет возможность как локального, так и удаленного администрирования ССПТ-2 в **интерактивном** режиме.
- WEB-интерфейс администратора предоставляет возможность удаленного администрирования ССПТ-2, используя стандартный WEB браузер, поддерживающий протокол HTTPS. HTTPS – протокол, предназначенный для организации безопасных транспортных TCP соединений в незащищенных компьютерных сетях при взаимодействии с WEB серверами. По сути протокол HTTPS является расширением протокола HTTP с использованием TLS.
- монитор централизованного управления обеспечивает возможность **одновременного управления** несколькими ССПТ-2 с отображением на мониторе управляющего компьютера следующей информации:
  - ✔ состояние всех контролируемых ССПТ-2;
  - ✔ статистика трафика по фильтрующим интерфейсам каждого из ССПТ-2;
  - ✔ отображение текущего набора правил фильтрации по каждому из ССПТ-2;

  Кроме того, монитор централизованного управления предоставляет возможность запуска средств администрирования любым из контролируемых ССПТ-2.

При этом в режимах удаленного сетевого управления, *за исключением WEB интерфейса администратора*, используется канал передачи данных, защищенный от несанкционированного доступа алгоритмами симметричного шифрования ГОСТ 28147-89 с использованием программной библиотеки “Агава-С” разработки ООО “Р-Альфа” (сертификат соответствия СФ/114-0805 от 01.09.2005).

WEB-интерфейс администратора использует канал передачи данных, защищенный от несанкционированного доступа алгоритмами симметричного шифрования с использованием программной библиотеки OpenSSL 0.9.8e (http://www.openssl.org).

1.4.3. Регистрация

Подсистема регистрации ССПТ-2 обеспечивает обработку запросов на регистрацию от других программных модулей ССПТ-2, хранение и выгрузку на удаленный FTP либо SYSLOG сервер регистрационной информации следующих категорий:

- события;
- трафик.

Регистрация событий. Событие отражает факт изменения состояния, конфигурационных параметров либо режима функционирования программного обеспечения ССПТ-2, произошедших в результате действий пользователей или в следствие возникновения сбоев или ошибок в работе ССПТ-2. ССПТ-2 обеспечивает регистрацию следующих событий:

- вход/выход администратора;
- загрузка и инициализация операционной системы ССПТ-2 и ее останов;
- действия администратора по изменению и загрузке правил фильтрации;
- действия администратора по изменению конфигурационных параметров ССПТ-2;
- действия администратора по управлению ССПТ-2 (запуск/останов пакетного фильтра, сброс файлов регистрации и т. д.);

При регистрации события всегда указывается:

- дата и время регистрируемого события с учетом часового пояса;
- код и описание события;
- идентификатор администратора ССПТ-2, действия которого привели к регистрации данного события;
- IP-адрес управляющего компьютера в случае удаленного сетевого администрирования.

Регистрация трафика. Трафик – это информация о зарегистрированных сетевых пакетах или взаимодействиях. Трафик подразделяется на следующие категории:

- **пакеты** – информация о пакетах, обработанных пакетным фильтром ССПТ-2 по правилам фильтрации. 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 ССПТ-2.

Подсистема регистрации трафика обеспечивает регистрацию пакетов с сохранением следующих основных параметров:

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

1.4.4. Идентификация, аутентификация и разграничение доступа

ССПТ-2 обеспечивает идентификацию и аутентификацию администратора ССПТ-2 при его локальных и удаленных запросах.

Каждый администратор имеет личный идентификатор, на основании которого определяются его права по управлению ССПТ-2. Права администратора определяются списком привилегий, хранящихся в его учетной записи.

При использовании средств удаленного администрирования в ССПТ-2 поддерживаются списки доступа на основе IP-адресов управляющих компьютеров.

1.4.5. Горячее резервирование

С целью повышения надежности функционирования два ССПТ-2 могут объединяться в вычислительный кластер, работающих по схемам “активный/резервный” или “активный/активный”, реализуя таким образом систему горячего резерва.

1.4.6. Контроль целостности

В ССПТ-2 обеспечивается контроль целостности основных компонентов операционной системы ССПТ-2, программных модулей ССПТ-2 и всех конфигурационных файлов. Контроль целостности осуществляется на основе периодической проверки контрольных сумм файлов, содержащих перечисленные выше компоненты.

Таким образом подсистема контроля целостности предотвращает попытки несанкционированного изменения программных модулей и конфигурационных файлов путем прямого редактирования, минуя использование штатных средств администрирования ССПТ-2.

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

- останов пакетного фильтра;
- регистрация события о нарушении контрольной суммы с указанием имени фала;
- перевод сервера авторизации в однопользовательский режим работы – доступ администратора к ССПТ-2 будет возможен только в режиме командного интерфейса, только с системной консоли и только для администратора с идентификатором “**admin**”.

2. Начало работы

2.1. Комплект поставки ССПТ-2

В комплект поставки ССПТ-2 входят:

- межсетевой экран ССПТ-2;
- шнур питания 220 В / 50 Гц;
- нуль-модемный кабель с 9-контактными гнездовыми разъемами. Используется для соединения ССПТ-2 с управляющим компьютером по последовательному порту RS-232;
- компакт-диск (CD-ROM), содержащий эксплуатационную документацию и дополнительное программное обеспечение, которое может быть установлено на управляющем компьютере администратора ССПТ-2.

2.2. Маркировка и назначение разъемов ССПТ-2

Разъемы ССПТ-2 имеют следующие маркировку и назначение:

- **VGA/USB (Console)** – разъем для подключения консольного терминала (*системная консоль*);
- **COM** – разъем последовательного порта RS-232, к которому подключается управляющий компьютер при помощи нуль-модемного кабеля (*имеется не во всех вариантах исполнения ССПТ-2*);
- **Eth 0**, **Eth 1**, **Eth 2, ..., Eth 5** – разъемы портов *фильтрующих интерфейсов* Ethernet, к которым подключаются защищаемые сегменты локальной сети. Количество фильтрующих интерфейсов зависит от варианта исполнения ССПТ-2. Используемый тип кабеля – “витая пара”, разъем – RJ-45;
- **Eth C** – разъем порта *управляющего интерфейса* Ethernet. Используемый тип кабеля – “витая пара”, разъем – RJ-45.

В качестве системной консоли ССПТ-2, в зависимости от варианта исполнения, может использоваться:

1) **VGA монитор / клавиатура** – к ССПТ-2 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 ССПТ-2 необходимо подключить управляющий компьютер к разъему **Console** (9-контактный штырьковый разъем RS-232), используя нуль-модемный кабель. Настройка подключения выполняется так, как описано в разделе 2.3, стр. 8 для случая подключения управляющего компьютера по последовательному порту RS-232 с использованием программы-эмулятора терминала.

Расположение разъемов ССПТ-2 зависит от варианта исполнения.

2.3. Подключение к ССПТ-2 для управления

Подключение к ССПТ-2 для первоначальной настройки и управления может быть выполнено одним из следующих способов:

- с системной консоли, используя командный интерфейс администратора. Системная консоль – это управляющий терминал операционной системы ССПТ-2. С системной консоли управление ССПТ-2 возможно только по командному интерфейсу администратора;
- с управляющего компьютера, подключаемого к ССПТ-2 по последовательному порту RS-232 (разъем **COM**). Могут быть использованы все средства администрирования ССПТ-2, перечисленные в разделе 1.4.2, стр. 4;

- с управляющего компьютера, подключаемого к управляющему сегменту Ethernet, к этому же сегменту должен быть подключен ССПТ-2 через управляющий Ethernet-интерфейс (разъем **EthC**). Могут быть использованы все средства администрирования ССПТ-2, перечисленные в разделе 1.4.2, стр. 4.

Последовательный порт RS-232. Для подключения к ССПТ-2 по последовательному порту необходим нуль-модемный кабель (входит в комплект поставки). Нуль-модемный кабель подключается к разъему **COM**. С другой стороны нуль-модемный кабель подключается к свободному порту RS-232 управляющего компьютера.

При использовании управляющего компьютера в качестве системной консоли ССПТ-2 нуль-модемный кабель подключается к разъему **Console**.

Связь с ССПТ-2 осуществляется несколькими способами:

- используя **программу-эмулятор удаленного терминала**. В этом случае управление ССПТ-2 возможно только по командному интерфейсу администратора. Рекомендуется использовать следующие программы эмуляторы удаленного терминала:
  - ✔ для управляющих компьютеров, работающих под управлением операционных систем MS Windows® 2000/XP – **IVT VT220 Freeware v.20.1a** (http://home.wxs.nl/~ruurdb/IVT.HTM). Пакет **IVT VT220 Freeware** имеется на компакт-диске, входящем в комплект поставки ССПТ-2;
  - ✔ для управляющих компьютеров, работающих под управлением операционных систем семейства UNIX (FreeBSD, различные версии на базе ядра Linux и т. д.) – **Minicom v.2.1** (http://alioth.debian.org/projects/minicom);

  Подробное описание использования программы-эмулятора терминала приводится в разделе 2.5.3, стр. 12.
- используя механизм **PPP соединения**. Могут быть использованы все средства администрирования ССПТ-2, перечисленные в разделе 1.4.2, стр. 4. Подробное руководство по настройке PPP соединения на управляющем компьютере приводится в приложении 3.2, стр. 40.

Использование PPP соединения возможно только для тех вариантов исполнения ССПТ-2, где имеется дополнительный последовательный порт RS-232 – разъем **COM**.

Управляющий Ethernet-интерфейс. Для подключения к ССПТ-2 по управляющему Ethernet-интерфейсу необходим кабель "*витая пара*" (категории 5):

- перекрестный (*cross-over*) кабель для непосредственного подключения управляющего компьютера;
- прямой кабель для подключения управляющего компьютера через концентратор (хаб или коммутатор).

По умолчанию управляющему Ethernet-интерфейсу назначен IP-адрес **10.234.28.71** с сетевой маской **255.255.0.0**.

В целях безопасности управляющий сегмент Ethernet рекомендуется изолировать от всей остальной сети.

Управляющему Ethernet-интерфейсу ССПТ-2 может быть назначен IP-адрес. Это можно выполнить, используя командный интерфейс администратора с подключением через системную консоль. Рекомендации по использованию управления ССПТ-2 по сети Ethernet и по выбору IP-адресов для управляющего Ethernet-интерфейса ССПТ-2 приводятся в приложении 3.3, стр. 51.

Доступ к командному интерфейсу с управляющего компьютера осуществляется с использованием утилиты терминального доступа по защищенному каналу `fnptel`, входящей в состав пакета сервисных утилит FNPUtils. Руководство по установке и использованию утилиты `fnptel` приводится в документе "***Межсетевой экран ССПТ-2. Утилиты. Руководство пользователя***".

Документ “***Межсетевой экран ССПТ-2. Утилиты. Руководство пользователя***” располагается на компакт-диске (CD-ROM), входящем в комплект поставки ССПТ-2 (`docs/fnputils_ag-1.4.0.pdf`, путь к файлу указан относительно корня файловой системы компакт-диска).

При организации удаленного доступа с использованием протокола PPP через последовательный порт RS-232 (разъем **COM**), доступ к командному интерфейсу ССПТ-2 с управляющего компьютера также осуществляется с использованием утилиты FNPtel.

2.4. Требования к управляющему компьютеру

Управляющий компьютер – это персональный компьютер общего назначения, который используется для управления и настройки параметров функционирования ССПТ-2. Управляющий компьютер должен работать под управлением одной из следующих операционных систем:

- Microsoft Windows® XP/Vista/7;
- FreeBSD версий не ниже 6.0-RELEASE;
- на базе ядра Linux версий не ниже 2.4.x.

Управляющий компьютер должен быть оснащен либо последовательным портом RS-232 для подключения к ССПТ-2 по нуль-модемному кабелю, либо адаптером Ethernet для подключения к сети управления.

Для организации удаленного доступа с использованием протокола PPP операционная система управляющего компьютера должна иметь поддержку протокола PPP.

Для администрирования ССПТ-2 с использованием WEB-интерфейса управления на управляющем компьютере должен быть установлен WEB браузер, отвечающий следующим требованиям:

- поддержка протокола **HTTPS** (Secure HTTP);
- поддержка закладок браузера **Cookie**.

Рекомендуется использование следующих WEB браузеров:

- **Mozilla Firefox** версии не ниже **9.0** (http://www.mozilla.org)
- **Opera** версии не ниже **10.0** (http://www.opera.com);
- **MS Internet Explorer** версии не ниже **7** (*только для операционных систем MS Windows® XP/Vista/7*, http://www.microsoft.com);

2.5. Первый запуск

2.5.1. Пользователи и пароли

Существует два уровня авторизации, которые последовательно должны пройти пользователи, чтобы получить доступ к управлению ССПТ-2:

- системная авторизация (*только для интерактивного режима командного интерфейса ССПТ-2*);
- авторизация ССПТ-2.

Системная авторизация выполняется средствами операционной системы ССПТ-2. Для системной авторизации используется следующие начальные параметры:

- имя пользователя – **`fnpsh`**. Это имя пользователя не может быть изменено;
- пароль пользователя – **`FilterD`**. Пароль системного пользователя `fnpsh` может быть изменен администратором ССПТ-2.

Авторизация ССПТ-2 выполняется после успешной системной авторизации. Первоначально существует один пользователь ССПТ-2, имеющий полный набор привилегий:

- имя пользователя – **admin**. Это имя пользователя также не может быть изменено;
- пароль пользователя – **FilterD**.

Пользователь admin не может быть удален, и для него не может быть изменен набор привилегий.

2.5.2. Использование системной консоли

Для первого подключения к ССПТ-2 следует использовать системную консоль. Чтобы получить доступ к управлению ССПТ-2 через системную консоль, необходимо:

- подключить системную консоль к разъемам ССПТ-2:
  - ✔ **VGA/USB** – при использовании VGA-монитора и PS/2 клавиатуры;
  - ✔ **Console** – при использовании управляющего компьютера, подключаемого по последовательному порту RS-232.
- включить питание на ССПТ-2;
- дождаться завершения загрузки операционной системы ССПТ-2. По окончании загрузки операционной системы на консоль будет выведена информация о состоянии ССПТ-2 и приглашение операционной системы на вход пользователя (рисунок 2.1).

```
Объем памяти                  ¦ 536870912 байт (512M)
Версия ПО ССПТ-2              ¦ FNP2_RELEASE_1_3-p1.2 (Jun 24 2013)
Всего интерфейсов             ¦ 4
    Фильтрующих интерфейсов   ¦ 3: eth0,eth1,eth2
    Управляющий интерфейс     ¦ включен, 10.234.28.71/255.255.0.0
Пакетная фильтрация           ¦ запущен
Контроль целостности          ¦ запущен
Авторизация                   ¦ запущен
Регистрация                   ¦ запущен
Резервирование                ¦ запущен
Удаленное администрирование   ¦ запущен
Удаленный терминальный доступ ¦ запущен
WEB интерфейс                 ¦ остановлен
SNMP интерфейс                ¦ остановлен

Starting sshd.
Starting cron.
Local package initialization:.
Starting background file system checks in 60 seconds.

Mon Jul  8 18:26:45 MSK 2013

FreeBSD/i386 (fnp2) (ttyv0)

login:
```

Рисунок 2.1: Вид экрана после загрузки операционной системы ССПТ-2

Для тех вариантов исполнений ССПТ-2, где в качестве системной консоли используется последовательный порт RS-232, для подключения следуют использовать нуль-модемный кабель, соединяющий ССПТ-2 и управляющий компьютер (раздел 2.5.3, стр. 12).

В вывод информации о состоянии ССПТ-2 включается (пример вывода – на рисунке 2.1):

- характеристики центрального процессора (ЦП) ССПТ-2 ("*Центральный процессор:*");
- объем установленной оперативной памяти ("*Оперативная память:*");
- Ethernet-интерфейсы:
  - ✔ общее количество Ethernet-интерфейсов в системе ("*Всего интерфейсов*");

- ✔ фильтрующие интерфейсы – общее количество и установленные символические имена каждого из интерфейсов; (“*Фильтрующих интерфейсов:*”)
- ✔ настройки управляющего Ethernet-интерфейса (“*Управляющий интерфейс:*”);

- версия ПО ССПТ-2 (“*Версия ПО ССПТ-2:*”);
- состояние процессов ССПТ-2. Для нормальной работы ССПТ-2 все процессы, **кроме процесса WEB-интерфейса**, должны находиться в состоянии “**`запущен`**”.

WEB-интерфейс может быть активирован только с системной консоли, используя командный интерфейс администратора – команда “`system web enable`”.

Далее для получения доступа к командному интерфейсу администратора ССПТ-2, необходимо пройти оба уровня авторизации, так как описано в разделе 2.5.1, стр 10. Пример авторизации пользователя в командном интерфейсе администратора ССПТ-2 с системной консоли приведен на рисунке 2.2. Ввод паролей на терминале не отображается.

```
FreeBSD/i386 (fnp2) (ttyv1)

login: fnpsh
Password:
Last login: Tue Nov 27 13:50:45 on ttyv1
Copyright (c) 1992-2009 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.


               Межсетевой экран ССПТ-2
           (c) ЗАО "НПО РТК", 2006-2013


Межсетевой экран ССПТ-2
  Командный интерфейс, версия 1.3
  (c) ЗАО "НПО РТК", 2000-2013. Все права защищены


Имя пользователя: admin
Пароль:

FNPSH-I-3001-Успешная авторизация пользователя
fnpsh>
```

Рисунок 2.2: Авторизация пользователя с системной консоли ССПТ-2

2.5.3. Использование последовательного порта RS-232

При первом подключении к ССПТ-2 также возможно использовать управляющий компьютер, соединенный с ССПТ-2 нуль-модемным кабелем по последовательному порту RS-232, в режиме эмуляции терминала. Рекомендуемые к использованию программы-эмуляторы терминала приведены в разделе 2.3, стр 8.

Последовательный порт RS-232 на управляющем компьютере должен иметь следующие настройки:

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

Настройка последовательного порта выполняется непосредственно в программах-эмуляторах терминала. Нуль-модемный кабель должен быть подключен к разъему **Console** или **COM** ССПТ-2 и к свободному порту RS-232 управляющего компьютера.

Пакет IVT VT220 Freeware (для операционных систем MS Windows® 2000/XP). Дистрибутив пакета **IVT VT220 Freeware 20.1a** имеется на компакт-диске, входящем в комплект поставки ССПТ-2. Краткое руководство по установке **IVT VT220 Freeware** приведено в приложении 3.1, стр. 36.

После запуска на управляющем компьютере программы **IVT VT220 Freeware**, необходимо в появившемся окне создания новой сессии "**Create session**" выполнить настройки последовательного порта так, как показано на рисунке 2.3.

В поле "**Portname**" окна создания новой сессии необходимо ввести имя последовательного порта управляющего компьютера, к которому подсоединен нуль-модемный кабель.

Для настройки последовательного порта нажать кнопку "`Setup`", затем в появившемся окне "**IVT Setup system**" (рисунок 2.4) нажать кнопку "`Serial settings`".

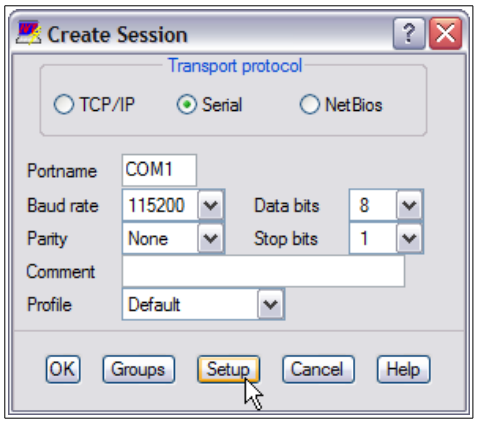

Рисунок 2.3: Настройки сессии в IVT VT220 Freware для подключения к ССПТ-2

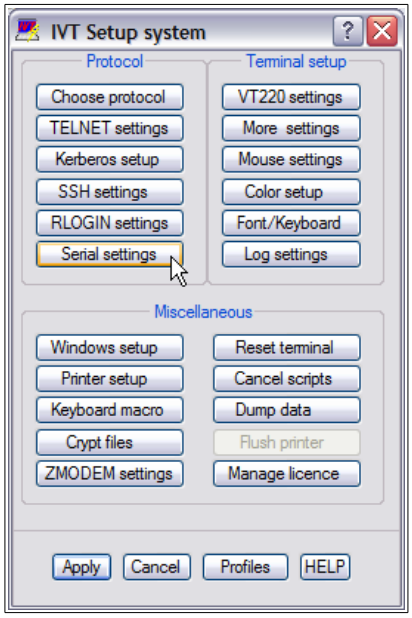

Рисунок 2.4: Окно "IVT Setup system"

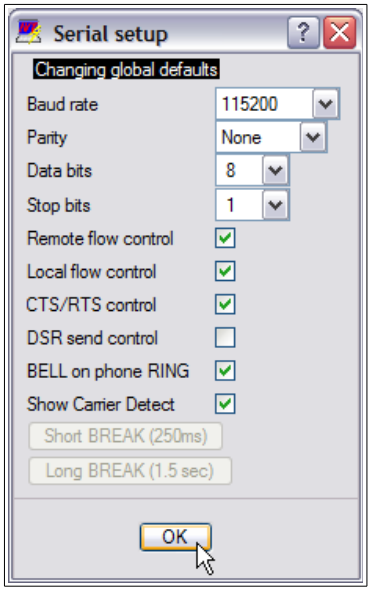

Рисунок 2.5: Окно "Serial setup"

В появившемся окне “**Serial setup**” установить параметры последовательного порта так, как это показано на рисунке 2.5, и нажать кнопку “ok”. Закрыть окно “**IVT Setup system**”, нажав кнопку “Apply” (рисунок 2.4).

Для подключения к ССПТ-2 в окне “**Create session**” нажать кнопку “ok”. Если настройки последовательного порта выполнены правильно и нуль-модемный кабель подключен как к последовательному порту управляющего компьютера, так и к разъему **Console** или **COM** ССПТ-2, в основном окне **IVT VT220 Freeware** появится приглашение операционной системы ССПТ-2 на вход пользователя (рисунок 2.6).

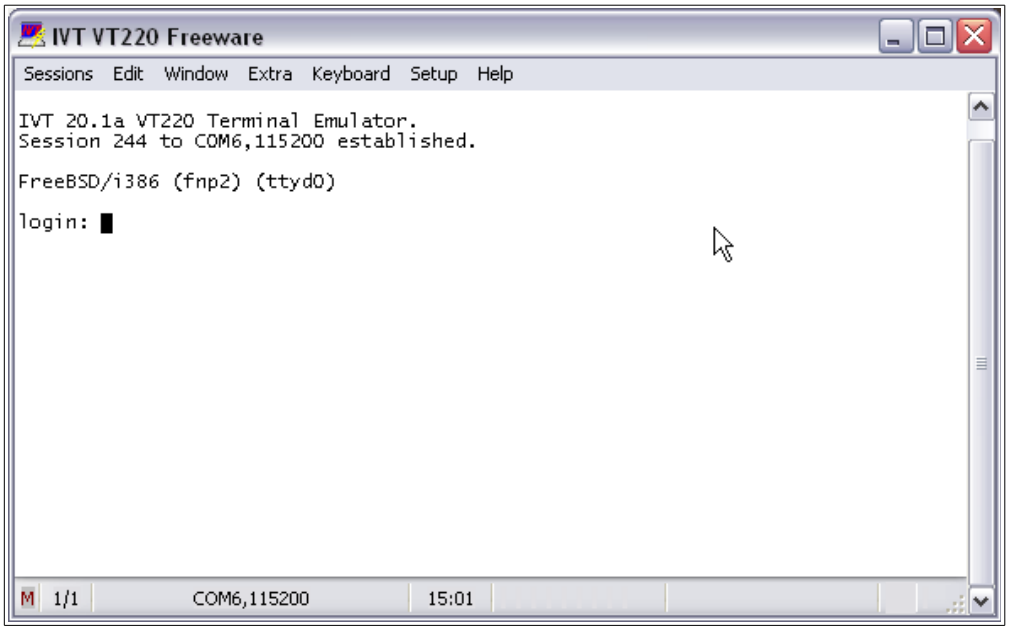

Рисунок 2.6: Вид основного окна IVT VT220 Freeware

Пакет Minicom (для операционных систем семейства UNIX). Для настройки последовательного порта, после запуска программы `minicom`, необходимо выполнить следующие действия:

- вызвать команду конфигурации, набрав на клавиатуре последовательность символов <Ctrl-A>, <O>;
- в появившемся меню конфигурации при помощи клавиш управления курсором <↑>, <↓> выбрать пункт меню "**Настройка последовательного порта**", затем нажать клавишу <Enter>;
- в параметрах настройки последовательного порта (рисунок 2.7) установить:

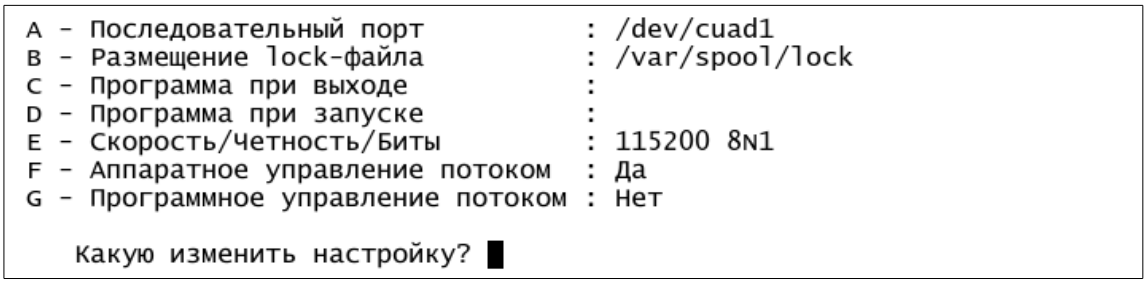

Рисунок 2.7: Параметры настройки последовательного порта в Minicom

- ✔ имя файла устройства последовательного порта управляющего компьютера, к которому подключен нуль-модемный кабель (команда <A> – **Последовательный порт**);
- ✔ параметры последовательного порта (команда <E> – **Скорость/Четность/Биты**). Для установки заданных параметров передачи последовательного порта, в форме "**Параметры связи**" (рисунок 2.8) последовательно ввести команды <I>, <Q>, затем нажать клавишу <Enter>;

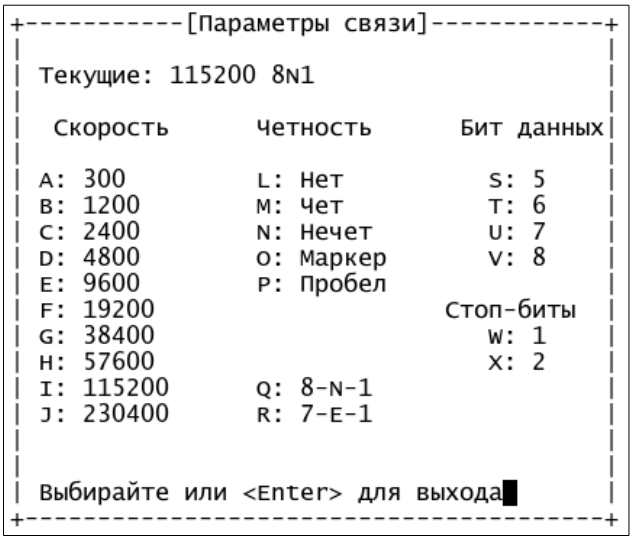

Рисунок 2.8: Форма параметров связи Minicom

- ✔ параметры управления потоком – при помощи команды <F> установить параметр "**Аппаратное управление потоком**" в значение "Да", при помощи команды <G> установить параметр "**Программное управление потоком**" в значение "Нет".

- нажать клавишу <Enter> для выхода из настроек последовательного порта;
- в меню конфигурации при помощи клавиш управления курсором <↑>, <↓> выбрать пункт меню "**Выход**", затем нажать клавишу <Enter>.

Пакет Minicom позволяет сохранять выбранные настройки как поименованную конфигурацию, которую затем можно будет указывать в качестве параметра командной строки minicom при последующих запусках.

Для этого после выполнения настройки последовательного порта, в меню конфигурации выбрать пункт “**Сохранить настройки как ...**”, ввести имя конфигурации (например, `fnp2`) и нажать клавишу `<Enter>`. В дальнейшем для соединения с ССПТ-2 по последовательному порту, на управляющем компьютере достаточно будет ввести команду:

```
% minicom fnp2
```

Если настройки последовательного порта выполнены правильно и нуль-модемный кабель подключен как к последовательному порту управляющего компьютера, так и к разъему **COM** ССПТ-2, программа `minicom` отобразит на экране терминала приглашение операционной системы ССПТ-2 на вход пользователя (рисунок 2.9).

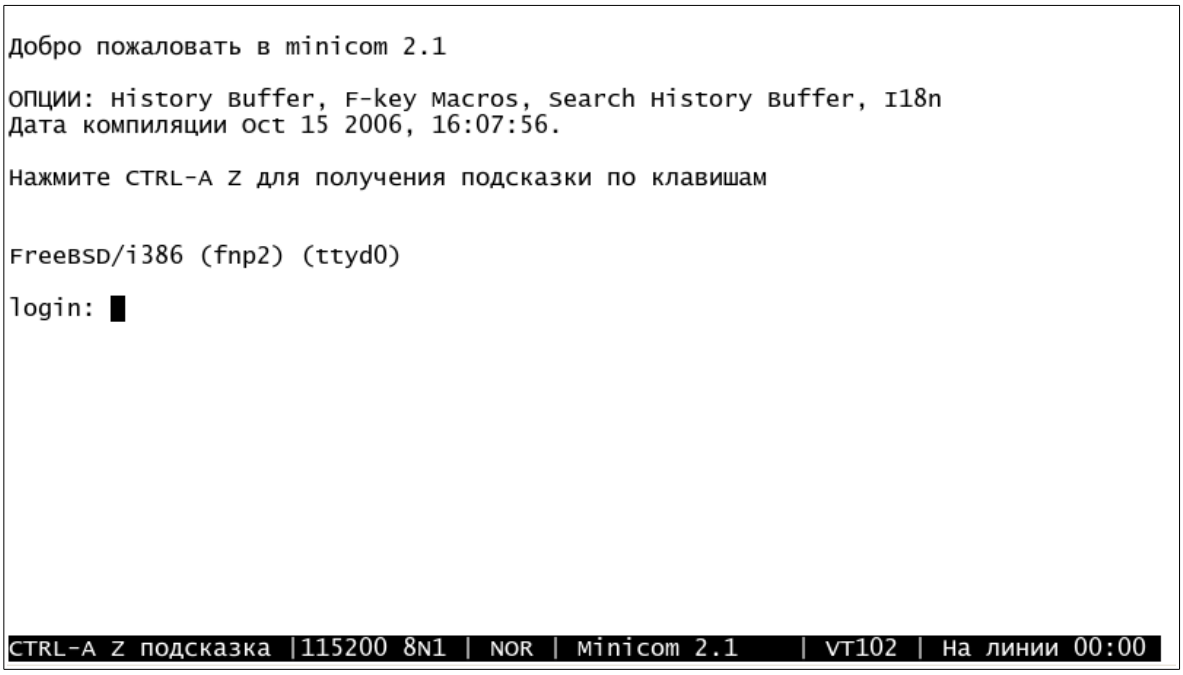

Рисунок 2.9: Вид терминального окна Minicom

Для получения доступа к командному интерфейсу администратора ССПТ-2, необходимо пройти оба уровня авторизации, так как описано в разделе 2.5.1, стр 10.

2.5.4. Использование PPP соединения по последовательному порту RS-232

Перед использованием PPP соединения, на управляющем компьютере необходимо выполнить соответствующие настройки. Руководство по настройке PPP соединения для операционных систем MS Windows® 2000/XP и FreeBSD/Linux приведено в приложении 3.2, стр. 40.

Между ССПТ-2 и управляющим компьютером устанавливается соединение “точка-точка” на базе протокола PPP, на сетевом и более высоких уровнях сетевого взаимодействия используется стек протоколов TCP/IP. Последовательным интерфейсам ССПТ-2 и управляющего компьютера в момент установления соединения автоматически назначаются IP-адреса **192.168.1.1** и **192.168.1.2** соответственно.

Операционные системы MS Windows® 2000/XP. Создать и настроить сетевое соединение, руководствуясь инструкцией, приведенной в приложении 3.2.1, стр. 41.

Открыть окно сетевого соединения **FNP-2** из раздела “Панель управления→Сетевые соединения”. В появившемся окне “**Подключение: FNP-2**”в поле ввода “**Пользователь:**” ввести “ppp”, в поле ввода “**Пароль:**” ввести “connect” и нажать кнопку “Вызов” (рисунок 2.10). PPP соединение с ССПТ-2 будет установлено.

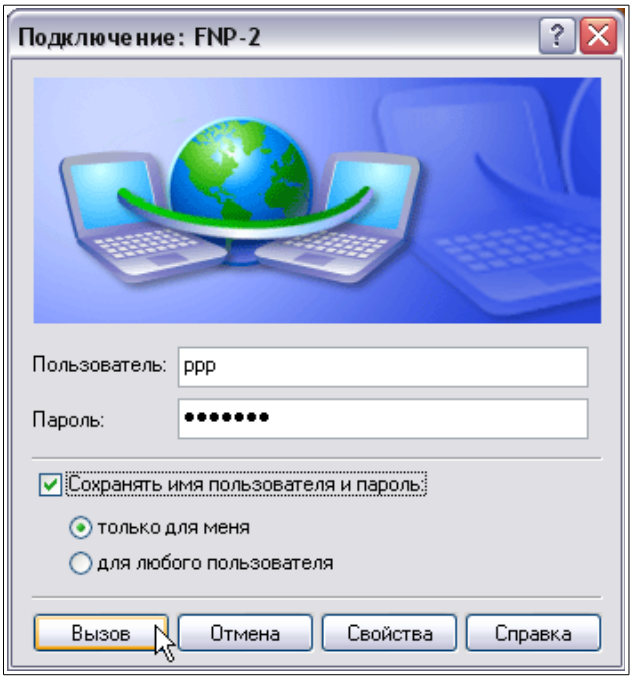

Рисунок 2.10: Подключение к ССПТ-2

Затем для получения доступа к командному интерфейсу ССПТ-2 необходимо использовать утилиту терминального доступа по защищенному каналу **FNPtel**, которая должна быть предварительно установлена на управляющем компьютере.

Далее для получения доступа к командному интерфейсу администратора ССПТ-2 необходимо пройти оба уровня авторизации так, как описано в разделе 2.5.1, стр 10.

Операционные системы FreeBSD/Linux. Настроить PPP соединение, руководствуясь инструкцией, приведенной в приложении 3.2.2, стр. 50.

Для того, чтобы установить PPP соединение с ССПТ-2, необходимо выполнить команду

```
$ /etc/ppp/fnp_ppp.sh start
```

Для того, чтобы разорвать PPP соединение с ССПТ-2, необходимо выполнить команду

```
$ /etc/ppp/fnp_ppp.sh stop
```

Затем для получения доступа к командному интерфейсу ССПТ-2 необходимо использовать утилиту терминального доступа по защищенному каналу **FNPtel** путем ввода следующей команды:

```
$ fnptel --host=192.168.1.1
```

Далее для получения доступа к командному интерфейсу администратора ССПТ-2, необходимо пройти оба уровня авторизации, так как описано в разделе 2.5.1, стр 10.

Доступ к WEB-интерфейсу ССПТ-2. После установления PPP соединения, WEB-интерфейс ССПТ-2, если он предварительно был активирован, доступен по адресу https://192.168.1.1.

2.5.5. Начальные настройки

После первого запуска ССПТ-2 и получения доступа к командному интерфейсу администратора, рекомендуется выполнить следующие действия:

- сменить пароль системного пользователя `fnpsh`;
- сменить пароль пользователя ССПТ-2 `admin`;
- если планируется администрирование ССПТ-2 по сети Ethernet – назначить IP-адрес управляющему Ethernet-интерфейсу и, при необходимости, настроить IP-адрес шлюза по умолчанию.

В ССПТ-2 существуют ограничения на формат пароля пользователя:

- длина пароля – от **6** до **128** символов;
- допустимые символы – только **печатаемые ASCII-символы**.

Смена пароля системного пользователя. Для смены пароля системного пользователя используется команда `system password` (приложение 3.4.157, стр. 168).

Сначала команда запросит ввод текущего пароля системного пользователя. Затем, если текущий пароль введен верно, команда запросит ввод нового пароля. Новый пароль необходимо вводить дважды, чтобы исключить опечатки при вводе пароля с клавиатуры. Ввод паролей на терминале не отображается:

```
fnpsh> system password
Старый пароль:
Новый пароль:
Новый пароль повторно:
FNPSH-I-309E-Пароль системного пользователя изменен
fnpsh>
```

Смена пароля пользователя ССПТ-2 `admin`. Для смены пароля пользователя ССПТ-2 используется команда `user password` (приложение 3.4.182, стр. 184).

Сначала команда запросит ввод текущего пароля пользователя `admin`. Затем, если текущий пароль введен верно, команда запросит ввод нового пароля. Новый пароль необходимо вводить дважды, чтобы исключить опечатки при вводе пароля с клавиатуры. Ввод паролей на терминале не отображается:

```
fnpsh> user password admin
Старый пароль:
Новый пароль:
Новый пароль повторно:
FNPSH-I-308D-Пароль пользователя изменен (admin)
fnpsh>
```

Настройка управляющего Ethernet-интерфейса. Для настройки управляющего Ethernet-интерфейса используются следующие команды:

- `interface control address` – назначение IP-адреса управляющему Ethernet-интерфейсу (приложение 3.4.22, стр. 70);
- `gateway set` – настройка IP-адреса шлюза по умолчанию (приложение 3.4.15, стр. 67).

IP-адрес управляющего Ethernet-интерфейса и маска IP-подсети передается команде `interface control address` в качестве параметра в формате `<IP_адрес/маска>`:

```
fnpsh> interface control address 10.98.7.1/255.255.255.0
FNPSH-I-3024-IP-адрес управляющего интерфейса изменен
fnpsh>
```

IP-адрес шлюза по умолчанию передается команде `gateway set` в качестве параметра:

```
fnpsh> gateway set 10.98.7.254
FNPSH-I-302B-Маршрут по умолчанию добавлен
fnpsh>
```

IP-адрес шлюза по умолчанию должен выбираться из той же самой IP-подсети, что и IP-адрес управляющего Ethernet-интерфейса.

Рекомендации по выбору IP-адресов для управляющего Ethernet-интерфейса ССПТ-2 приведены в приложении 3.3, стр. 51.

2.5.6. Использование управляющего Ethernet-интерфейса

После настройки управляющего Ethernet-интерфейса ССПТ-2 и подключения управляющего компьютера к сегменту управления, доступ к командному и WEB-интерфейсам управления ССПТ-2 осуществляется аналогично тому, как это делается при использовании PPP соединения. При этом вместо IP-адреса 192.168.1.1 указывается IP-адрес управляющего Ethernet-интерфейса ССПТ-2.

2.5.7. Дополнительные наборы правил

В ССПТ-2 существует два типа наборов правил:

1) **текущий набор правил** – правила фильтрации, VLAN-группы и интервалы времени, используемые пакетным фильтром при обработке пакетов, принимаемых фильтрующими интерфейсами ССПТ-2;
2) **дополнительные наборы правил** – хранятся в ССПТ-2 и могут быть использованы для резервного копирования текущего набора правил или хранения дополнительных конфигураций для пакетного фильтра. Каждому дополнительному набору правил присваивается символическое имя.

В ССПТ-2 существуют следующие ограничения при работе с дополнительными наборами правил:

- ССПТ-2 может хранить не более **16** дополнительных наборов правил;
- имя дополнительного набора правил должно отвечать следующим требованиям:
  - ✔ длина имени – от **1** до **128** символов;
  - ✔ допустимые символы в имени – **латинские буквы** (a-z, A-Z), **цифры** (0-9), и символы '_' (подчеркивание), '**-**' (дефис). Имя дополнительного набора должно начинаться с буквы либо с цифры.

Командный интерфейс ССПТ-2 предоставляет следующие команды для работы с наборами правил:

- `rule save` – сохранение текущего набора правил в дополнительном наборе с указанным именем (приложение 3.4.115, стр. 139);
- `rule load` – загрузка дополнительного набора правил в текущий набор (приложение 3.4.111, стр. 137);
- `rule remove` – удаление дополнительного набора правил (приложение 3.4.113, стр. 138);
- `rule show` – просмотр содержимого текущего или дополнительного набора правил (приложение 3.4.116, стр. 140);
- `rule list` – просмотр списка дополнительных наборов правил (приложение 3.4.110, стр. 137).

ССПТ-2 поставляется с двумя предустановленными дополнительными наборами правил:

1) `default_accept` – набор правил, разрешающий передачу всех пакетов через фильтрующие интерфейсы ССПТ-2;
2) `default_drop` – набор правил, запрещающий передачу всех пакетов через фильтрующие интерфейсы ССПТ-2.

Просмотреть список дополнительных наборов правил можно, используя команду `rule list`:

```
fnpsh> rule list
Список дополнительных наборов правил:
    Имя                 Время создания
    default_accept      10.02.2010 13:03:27 (GMT)
    default_drop        10.02.2010 13:03:27 (GMT)
Всего: 2        Свободно: 14
fnpsh>
```

Первоначально в качестве текущего набора в ССПТ-2 загружен набор правил `default_drop`. Для загрузки дополнительного набора `default_accept` следует использовать команду `rule load`:

```
fnpsh> rule load default_accept
Загрузить дополнительный набор правил (режим управления сессиями)? (Y/N)  [N]: Y
FNPSH-I-304A-Таблица сессий очищена
FNPSH-I-301E-Дополнительный набор правил загружен
fnpsh>
```

После выполнения приведенной выше команды все пакеты будут пропускаться через фильтрующие интерфейсы ССПТ-2.

2.6. Основы использования командного интерфейса ССПТ-2

2.6.1. Структура команды

Команда ССПТ-2 имеет следующий синтаксис:

```
ключевое_слово [...] [параметр [...]]
```

где:

- `ключевое_слово` – ключевое слово командного языка ССПТ-2. Ввод команды всегда начинается с одного или более ключевых слов;
- `параметр` – необязательный параметр команды. После последовательности ключевых слов в команде может быть указан один или более параметров. Формат параметра в значительной степени зависит от контекста его использования, т. е. от конкретной команды ССПТ-2.

В командной строке ключевые слова и параметры должны отделяться друг от друга произвольным количеством (одним или несколькими) *символов пропуска*. Последовательность символов, отделенная символами пропуска, называется *лексемой*.

В качестве символа пропуска может быть использован либо символ пробела, либо символ горизонтальной табуляции (клавиша <Tab> на клавиатуре).

Например, в команде

```
rule load default_accept
```

`rule load` являются ключевыми словами командного языка ССПТ-2, а `default_accept` – параметром команды, обозначающим имя дополнительного набора правил.

При вводе команд допускается использование ключевых слов как полностью, так и с сокращениями. Например:

```
rul lo default_accept
```

При описании синтаксиса каждой команды необязательные окончания ключевых слов заключаются в квадратные скобки. Например, `rul[e] lo[ad]`.

Синтаксис команд ССПТ-2, их описание и возможные особенности использования приводится в приложении 3.4, стр. 52.

2.6.2. Редактирование командной строки

В командном интерфейсе ССПТ-2 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 ССПТ-2 представлены в таблице 2.1.

Таблица 2.1: Редактирование в командной строке ССПТ-2

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
<→>, <Ctrl+F>	Перемещение курсора на одну позицию вправо
<Ctrl+A>	Перемещение курсора в начало командной строки
<Ctrl+E>	Перемещение курсора в конец 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
<Enter>	Передача набранной команды на выполнение

2.6.3. Буфер истории команд

После нажатия клавиши <Enter> набранная команда передается на выполнение командному интерпретатору ССПТ-2 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 2.1.

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

Командный интерфейс ССПТ-2 предоставляет следующие команды для управления буфером истории команд:

- `system fnpsh history clear` – очистка буфера истории команд (приложение 3.4.152, стр. 166);
- `system fnpsh history show` – просмотр содержимого буфера истории команд (приложение 3.4.153, стр. 167).

Например:

```
fnpsh> system fnpsh history show
Буфер истории команд:
   1 - system password
   2 - user password admin
   3 - interface control address 10.98.7.1/255.255.255.0
```

```
   4 - gateway set 10.98.7.254
   5 - rule list
   6 - rule load default_accept
fnpsh>

fnpsh> system fnpsh history clear
Очистить буфер истории команд? (Y/N)  [N]: Y
FNPSH-I-3022-Буфер истории команд очищен
fnpsh>
```

2.6.4. Получение контекстной справки

Командный интерфейс ССПТ-2 предоставляет возможность получения пользователем контекстной справки по введенной команде.

Для получения контекстной справки в качестве последней лексемы в командной строке необходимо ввести ключевое слово `help`, либо символ '?' (знак вопроса). Контекстную справку можно получить для любого уровня лексического разбора команды ССПТ-2. Например, для того чтобы получить справку по всем командам, предназначенных для работы с правилами фильтрации, следует ввести команду `rule help` (или `rule ?`):

```
fnpsh> rule help
  add:            добавление правила в текущий набор
  copy:           создание копии существующего правила в текущем наборе
  edit:           редактирование существующего правила в текущем наборе
  delete:         удаление правила из текущего набора
  default <cr>:   установка правил по умолчанию в текущем наборе
  list <cr>:      вывод списка дополнительных наборов правил
  load:           загрузка дополнительного набора правил в текущий набор
  move:           перемещение существующего правила в текущем наборе
  remove:         удаление дополнительного набора правил
  rollback <cr>: откат к предыдущему набору правил
  save:           сохранение текущего набора правил в дополнительном наборе
  show:           вывод текущего или дополнительного набора правил
  stats:          вывод статистики использования правил в текущем наборе
fnpsh>
```

А для того, чтобы получить справку по команде загрузки дополнительного набора правил `rule load`, следует ввести команду `rule load help` (или `rule load ?`):

```
fnpsh> rule load ?
  <имя_доп.набора> <cr>:  загрузить указанный дополнительный набор правил в
                          текущий набор
fnpsh>
```

Для получения краткой справки по всем категориям команд ССПТ-2 следует ввести команду `help` (или `?`):

```
fnpsh> help
  config:    управление конфигурациями устройства
  filter:    управление пакетным фильтром
  gateway:   настройка шлюза по умолчанию
  interface: настройка сетевых интерфейсов
  log:       управление подсистемой регистрации
  nat:       настройка механизма трансляции сетевых адресов (NAT)
  rule:      управление правилами фильтрации
  reserv:    управление подсистемой высокой готовности
  session:   управление механизмом контроля сессий
  system:    контроль параметров операционной системы
  user:      управление пользователями ССПТ-2
  exit <cr>: выход из командного интерфейса
  help <cr>: справка по командам

    Просмотр контекстной справки по командам:
  <команда> [<опции>] ? <cr>
    или
  <команда> [<опции>] help <cr>
    где <cr> - перевод строки
fnpsh>
```

2.6.5. Сеанс работы пользователя

Пройдя оба уровня авторизации (раздел 2.5.1, стр. 10), пользователь получает доступ к командному интерфейсу ССПТ-2. Появление на экране терминала подсказки командной строки "`fnpsh>` " означает, что командный интерфейс ССПТ-2 готов к работе и ожидает ввода команд. С этого момента начинается сеанс работы пользователя.

Сеанс работы пользователя завершается в одном из следующих случаев:

- пользователь выполнил команду `exit` (приложение 3.4.7, стр. 63):

```
fnpsh> exit
FNPSH-I-3003-Завершение работы пользователя (admin)
```

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

```
fnpsh>
FNPSH-I-3005-Таймаут неактивности
```

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

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

- минимальное значение – **10** секунд;
- максимальное значение – **3600** секунд (1 час).

Для изменения значения тайм-аута неактивности пользователя используется команда `system fnpsh timeout` (приложение 3.4.155, стр. 168). В качестве параметра указывается новое значение тайм-аута неактивности в секундах:

```
fnpsh> system fnpsh timeout 180
FNPSH-I-3088-Таймаут неактивности командного интерфейса изменен
fnpsh>
```

Для просмотра текущего значения тайм-аута неактивности пользователя используется команда `system show` (приложение 3.4.162, стр. 173) – строка "*Тайм-аут неактивности FNPSH*"):

```
fnpsh> system show
Модель ЦПУ                      | Intel(R) Core(TM) i7 CPU         870  @ 2.93GHz
Ядер ЦПУ                        | 1
Объем памяти                    | 536870912 байт (512M)
Версия ПО ССПТ-2                | FNP2_RELEASE_1_3-p1.2 (Jun 24 2013)
Всего интерфейсов               | 4
    Фильтрующих интерфейсов     | 3: eth0,eth1,eth2
    Управляющий интерфейс       | включен, 10.98.7.1/255.255.255.0
Пакетная фильтрация             | запущен
Контроль целостности            | запущен
Авторизация                     | запущен
Регистрация                     | запущен
Резервирование                  | запущен
Удаленное администрирование     | запущен
Удаленный терминальный доступ   | запущен
WEB интерфейс                   | запущен
SNMP интерфейс                  | запущен
Тайм-аут неактивности FNPSH     | 600 секунд
Просмотрщик по умолчанию FNPSH  | внутренний (internal)
fnpsh>
```

2.6.6. Настройка режима просмотра данных

Для удобства просмотра больших объемов данных, таких как наборы правил или параметры конфигурации, в командном интерфейсе ССПТ-2 предусмотрены следующие режимы просмотра данных:

- `internal` – полноэкранный режим просмотра данных. В этом режиме реализован как построчный так и постраничный просмотр данных в возможностью перемещения назад и вперед;

- more – упрощенный режим постраничного просмотра данных с возможностью перемещения назад и вперед;
- no – сплошной вывод данных на экран терминал без возможности построчного и постраничного просмотра. Возможно частичное исчезновение строк в верху терминала при выводе больших объемов данных, превышающих по количеству строк размер экрана терминала.

По умолчанию используется полноэкранный режим просмотра данных – internal.

Полноэкранный режим просмотра данных. В этом режиме пользователь имеет возможность просмотра данных, используя клавиши управления курсором и управляющие последовательности, перечисленные в таблице 2.2.

Таблица 2.2: 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 строк
<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
<Ctrl+W>	Режим просмотра без горизонтальной прокрутки. В этом режиме осуществляется автоматический перенос строк, длина которых превышает ширину окна вывода данных.
<H>	Вывод подсказки по клавишам управления просмотром данных
<F10>, <Q>	Завершение просмотра данных

Для иллюстрации работы полноэкранного режима на рисунке 2.11 представлен вывод параметров конфигурации ССПТ-2, выполненный по команде config show. Если терминал не поддерживает ANSI цвета, будет автоматически использоваться монхромный режим работы терминала.

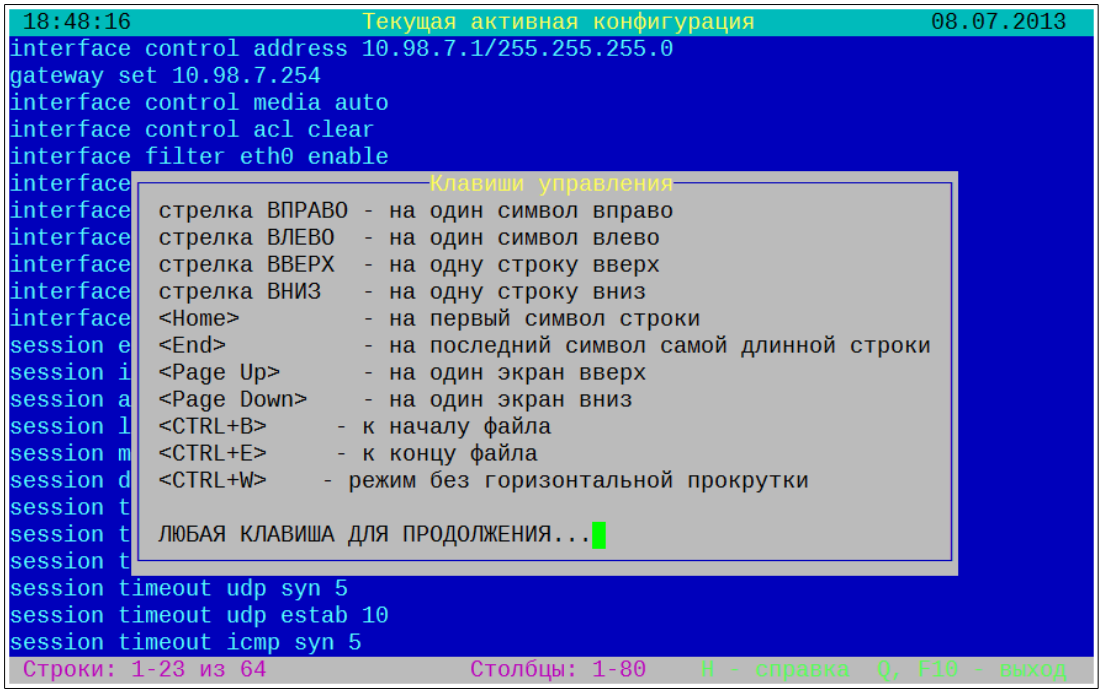

Рисунок 2.11: Полноэкранный режим просмотра данных

Режим постраничного просмотра данных. В этом режиме пользователь имеет возможность построчного и постраничного просмотра данных, используя клавиши управления курсором и управляющие последовательности, перечисленные в таблице 2.3.

Таблица 2.3: Управление в режиме постраничного просмотра данных

Управление	*Назначение*
<↑>	Перемещение на одну строку вверх
<↓>	Перемещение на одну строку вниз
<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 2.12 представлен вывод параметров конфигурации ССПТ-2, выполненный по команде `config show`. Используется только монохромный режим работы терминала. Просмотр автоматически завершается после вывода на экран терминала последней строки данных.

Режим сплошного вывода данных. В этом режиме пользователь 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.

```
Текущая активная конфигурация:

interface control address 10.98.7.1/255.255.255.0
gateway set 10.98.7.254
interface control media auto
interface control acl clear
interface filter eth0 enable
interface filter eth0 media auto
interface filter eth1 enable
interface filter eth1 media auto
interface filter eth2 enable
interface filter eth2 media auto
interface filter eth0 mirror disable
session enable
session ip enable
session ap disable
session log disable
session mac enable
session deeptcp enable
session timeout tcp syn 5
session timeout tcp estab 3600
session timeout tcp fin 180
session timeout udp syn 5
session timeout udp estab 10
<Enter> - Далее...       <Q> - Выход
```

Рисунок 2.12: Режим постраничного просмотра данных

Для установки режимов просмотра данных используется команда `system fnpsh viewer` (приложение 3.4.156, стр. 168):

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

Изменение режима просмотра данных действует только на время текущей сессии работы пользователя.

Следующий пример иллюстрирует установку режима постраничного просмотра данных:

```
fnpsh> system fnpsh viewer more
FNPSH-I-3087-Режим просмотра изменен
fnpsh>
```

Для просмотра установленного режима просмотра данных используется команда `system show` (строка "*Просмотрщик по умолчанию FNPSH*").

2.6.7. Диагностические сообщения командного интерфейса ССПТ-2

Выполнение любой команды в командном интерфейсе ССПТ-2 всегда завершается выводом диагностического сообщения на экран терминала. Диагностическое сообщение имеет следующий формат:

```
FNPSH-{I|W|E}-XXXX-<текст_сообщения>[ (<системная_ошибка>)]
```

где:

- `I|W|E` – один из трех возможных уровней диагностического сообщения:
  - ✔ `I` – информационное сообщение;
  - ✔ `W` – предупреждение;

✔ E – сообщение об ошибке.

- XXXX – шестнадцатеричный код диагностического сообщения;
- <текст_сообщения> – текстовая интерпретация кода диагностического сообщения;
- <системная_ошибка> – необязательное сообщение, включаемое в строку диагностического сообщения, если при выполнении команды произошла системная ошибка. Сообщения о системных ошибках являются стандартными для операционной системы ССПТ-2. Сообщение о системной ошибке всегда выводится на *английском языке*.

Например, диагностическое сообщение

```
FNPSH-I-3087-Режим просмотра изменен
```

является *информационным сообщением* с кодом 0x3087 (шестнадцатеричный).

Перечень всех диагностических сообщений командного интерфейса ССПТ-2 приводится в приложении 3.5, стр. 190.

2.7. Основы использования WEB-интерфейса ССПТ-2

WEB-интерфейс ССПТ-2 является универсальным графическим интерфейсом пользователя (GUI – Graphical User Interface), предназначенным для настройки и управления ССПТ-2.

WEB-интерфейс ССПТ-2 может использоваться при управлении ССПТ-2 по сети Ethernet или через установленное PPP соединение по последовательному порту RS-232.

Для работы с WEB-интерфейсом ССПТ-2 на управляющем компьютере не требуется установки специального программного обеспечения, за исключением стандартного WEB браузера. Перечень рекомендуемых к использованию WEB браузеров и требований, предъявляемых к ним, приводится в разделе 2.4, стр.10.

Все последующие иллюстрации работы WEB-интерфейса ССПТ-2 приводятся для WEB браузера **Mozilla Firefox 22.0**.

Для передачи данных между управляющим компьютером и ССПТ-2 используется защищенный канал управления на основе алгоритмов шифрования, реализованных в программной библиотеке OpenSSL (http://www.openssl.org).

2.7.1. Включение/отключение WEB-интерфейса

По умолчанию, после первого запуска ССПТ-2, WEB-интерфейс отключен и недоступен для использования. Для включения WEB-интерфейса ССПТ-2 необходимо использовать команду system web enable (приложение 3.4.176, стр.181).

Для отключения WEB-интерфейса ССПТ-2 необходимо использовать команду system web disable (приложение 3.4.175, стр.180).

Команды system web disable и system web enable могут быть выполнены только с системной консоли ССПТ-2 и только пользователем admin.

2.7.2. Сеанс работы пользователя

Из WEB браузера, запущенного на управляющем компьютере, необходимо послать запрос следующего вида:

```
https://<IP_адрес>,
```

где <IP_адрес> – IP-адрес управляющего интерфейса ССПТ-2, который может принимать одно из следующих значений:

- 192.168.1.1 – при управлении ССПТ-2 через установленное PPP соединение по последовательному порту RS-232;
- *IP-адрес управляющего Ethernet-интерфейса ССПТ-2* – при управлении по сети Ethernet.

Пример (соединение с ССПТ-2 по сети Ethernet по адресу 10.98.7.1):

```
https://10.87.7.1
```

Соединение по протоколу HTTPS обеспечивает защищенный канал управления для передачи данных между управляющим компьютером и ССПТ-2. Используемые алгоритмы шифрования и другая необходимая для этого информация содержится в *сертификате безопасности*, передаваемом от ССПТ-2 WEB браузеру управляющего компьютера. Сертификат безопасности подписывается *удостоверяющим центром* предприятия-изготовителя ССПТ-2. В этом случае WEB браузер управляющего компьютера может вывести диагностическое сообщение, суть которого заключается в том, что информация о данном удостоверяющем центре отсутствует в списке удостоверяющих центров, известных WEB браузеру (рисунок 2.13).

Если параметры сертификата безопасности, принятого WEB браузером, соответствуют тому, что приведено на рисунке 2.14, значит система шифрования управляющего канала не нарушена и подлинность ССПТ-2 установлена.

Для WEB-интерфейса ССПТ-2 не требуется выполнения системной авторизации так, как это нужно для работы в командном интерфейсе ССПТ-2 (раздел 2.5.1, стр. 10).

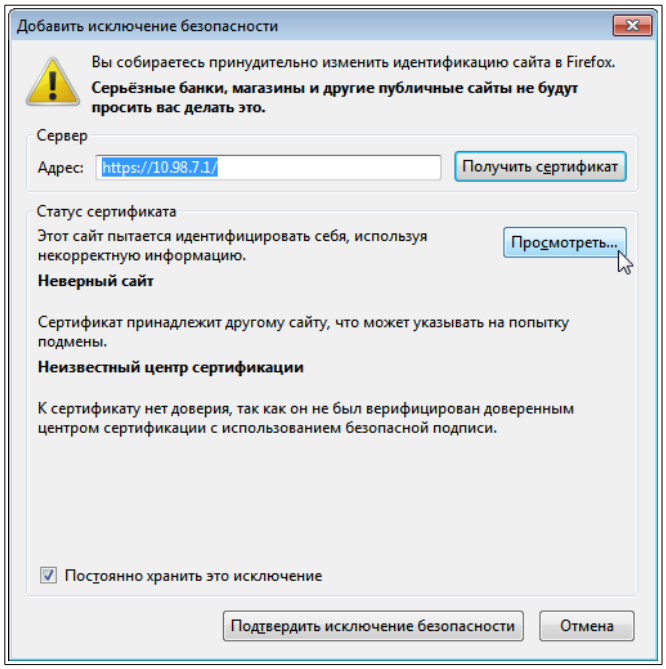

Рисунок 2.13: Неизвестный удостоверяющий центр

Для выполнения авторизации ССПТ-2 через WEB-интерфейс необходимо нажать кнопку “Вход”, выведенную в рабочей области окна WEB браузера (рисунок 2.15).

В появившемся окне авторизации пользователя (рисунок 2.16) необходимо ввести имя пользователя ССПТ-2 и пароль в полях ввода “Имя пользователя” и “Пароль” соответственно, затем нажать кнопку “Вход”. Для отказа от авторизации пользователя нажать кнопку “Отмена”.

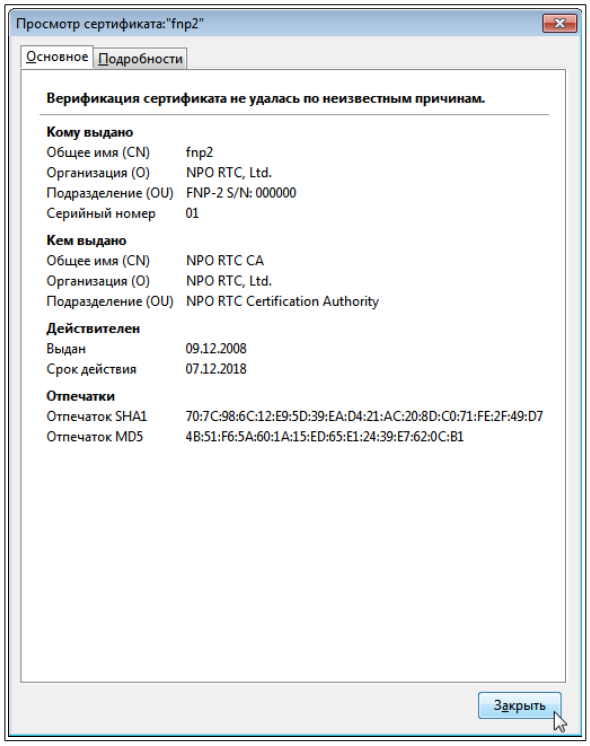

Рисунок 2.14: Просмотр сертификата ССПТ-2

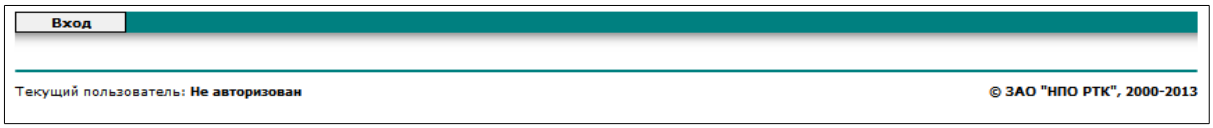

Рисунок 2.15: Страница для неавторизованного пользователя

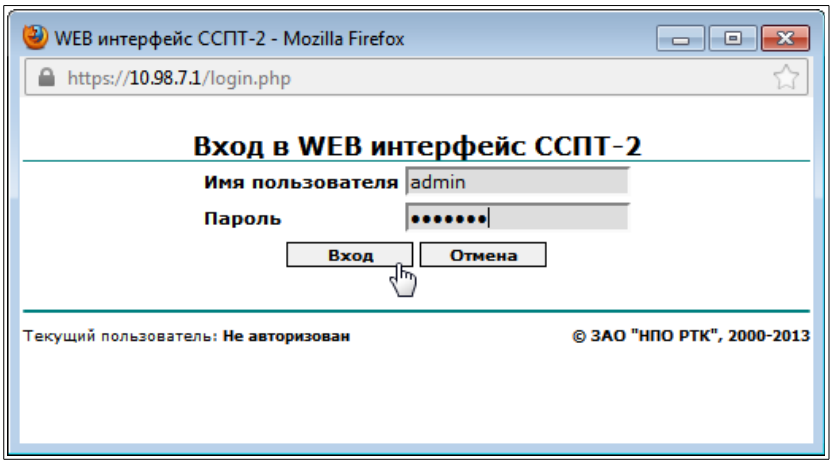

Рисунок 2.16: Окно авторизации пользователя

Если имя пользователя и пароль введены правильно, начнется сеанс работы пользователя и в рабочей области окна WEB браузера будет выведена страница WEB-интерфейса ССПТ-2 “Системная

информация” (рисунок 2.19, стр. 32).Сеанс работы пользователя завершается в одном из следующих случаев:

- пользователь нажал кнопку “Выход”, расположенную справа в строке основного меню WEB-интерфейса и в появившемся окне подтверждения завершения сеанса пользователя нажал кнопку “Выход”;
- превышен лимит времени неактивности пользователя – *тайм-аут неактивности*. Если пользователь не производит выполнение команд в течение этого времени, то сессия работы пользователя автоматически завершается. При попытке выполнения какого-либо действия по истечении тайм-аута неактивности WEB-интерфейс автоматически выведет страницу для неавторизованного пользователя (рисунок 2.15).

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

Изменить значение тайм-аута неактивности можно только из командного интерфейса ССПТ-2 (раздел 2.6.5, стр. 23).

2.7.3. Получение контекстной справки

Все страницы WEB-интерфейса ССПТ-2 снабжены кнопкой вызова контекстной справки. Нажатие на кнопку “Справка” приводит к выводу справки по текущей странице WEB-интерфейса в отдельном окне WEB браузера.

В качестве примера на рисунке 2.17 представлен вывод окна контекстной справки для страницы настройки системного времени ССПТ-2.

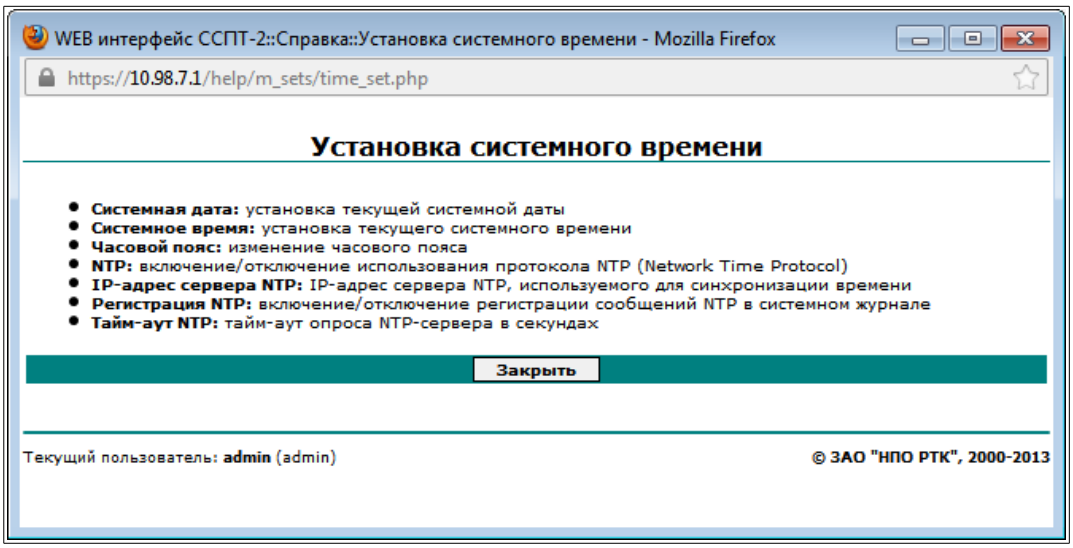

Рисунок 2.17: Контекстная справка WEB-интерфейса ССПТ-2

Для того, чтобы закрыть окно контекстной справки необходимо нажать кнопку “Закрыть”.

2.7.4. Структура WEB-интерфейса ССПТ-2

WEB-интерфейс ССПТ-2 состоит из нескольких разделов, состав которых определяется его *основным меню*. Основное меню WEB-интерфейса всегда выводится вверху рабочей области окна WEB браузера. Текущий раздел WEB-интерфейса отображается инверсным цветом. В качестве примера на рисунке 2.19 представлен вывод страницы “Системная информация” из раздела “Состояние”.

Каждый раздел WEB-интерфейса, за исключением раздела “Состояние”, содержит меню второго уровня, определяющее функциональность страниц данного раздела. Меню второго уровня располагается в верхней части рабочей области окна WEB браузера непосредственно под основным меню. Текущий пункт меню отображается на сером фоне.

WEB-интерфейс ССПТ-2 имеет следующие разделы:

- `Состояние` – содержит общую информацию о текущем состоянии ССПТ-2, статистику трафика по фильтрующим интерфейсам, а также кнопки управления пакетным фильтром и устройством в целом (рисунок 2.18):
  - ✔ `Система` – вывод страницы "`Системная информация`", содержащей информацию о характеристиках и состоянии программного и аппаратного обеспечения ССПТ-2;
  - ✔ `Фильтрация` – вывод страницы "`Фильтрация`", содержащей информацию о статистику трафика по фильтрующим интерфейсам ССПТ-2.

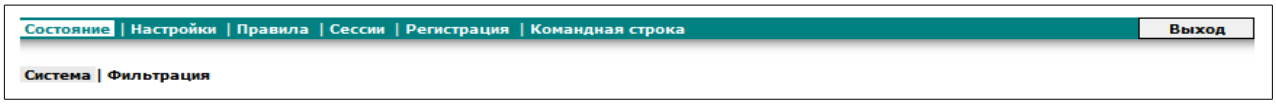

Рисунок 2.18: Меню раздела "Состояние"

Информация на страницах "Системная информация" и "Фильтрация" обновляется автоматически через каждые **10** секунд.

- `Настройки` – содержит страницы для настройки различных подсистем ССПТ-2 (рисунок 2.20):
  - ✔ `Система` – управление дополнительными конфигурациями и настройки системного времени ССПТ-2;
  - ✔ `Пользователи` – управление пользователями;
  - ✔ `Интерфейсы` – настройки управляющего Ethernet-интерфейса и фильтрующих интерфейсов ССПТ-2;
  - ✔ `NAT` – настройки подсистемы трансляции сетевых адресов NAT;
  - ✔ `Сетевые пользователи` – управление сетевыми пользователями;
  - ✔ `Ключи аутентификации` – управление ключами аутентификации сетевых пользователей;
  - ✔ `Горячий резерв` – настройки подсистемы высокой готовности;
  - ✔ `RADIUS` – настройки RADIUS авторизации пользователей ССПТ-2.

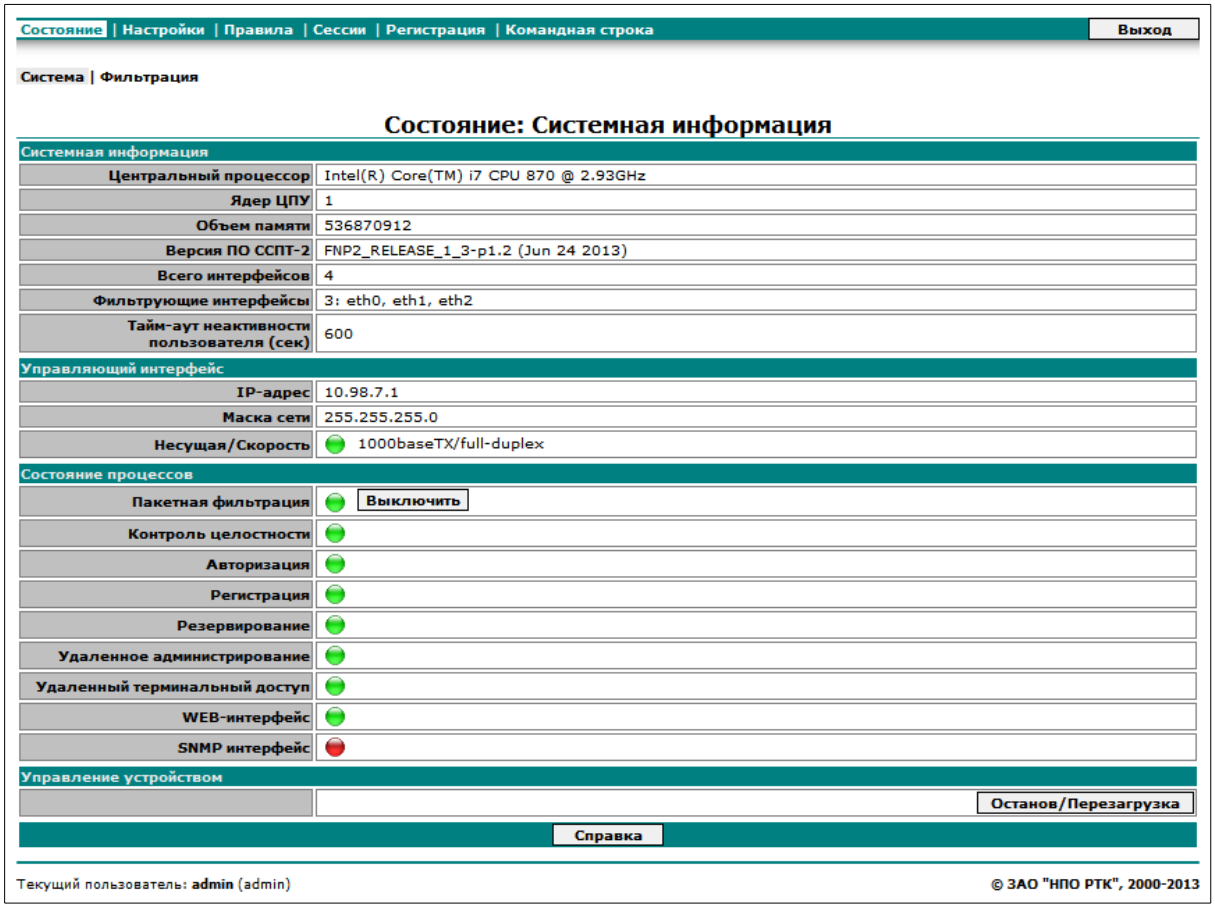

Рисунок 2.19: Страница "Системная информация" из раздела "Состояние"

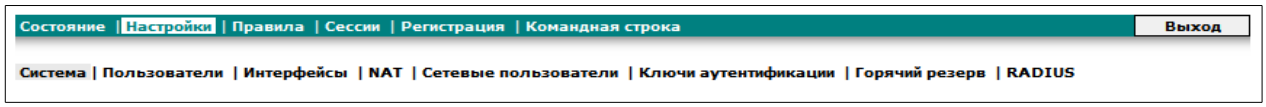

Рисунок 2.20: Меню раздела "Настройки"

- `Правила` – содержит страницы для настройки текущего набора правил и управления дополнительными наборами правил (рисунок 2.21):
  - ✔ `Основные` – настройки глобальных правил фильтрации текущего набора правил, управление дополнительными наборами правил;
  - ✔ `MAC` – управление MAC-правилами фильтрации текущего набора правил;
  - ✔ `ARP` – управление ARP-правилами фильтрации текущего набора правил;
  - ✔ `IPTMP` – управление временными IP-правилами фильтрации текущего набора правил;
  - ✔ `IP` – управление IP-правилами фильтрации текущего набора правил;
  - ✔ `IPX` – управление IPX-правилами фильтрации текущего набора правил;
  - ✔ `AP` – управление AP-правилами фильтрации (правила фильтрации прикладного уровня) текущего набора правил;
  - ✔ `Группы VLAN` – управление VLAN-группами текущего набора правил;
  - ✔ `Интервалы времени` – управление интервалами времени текущего набора правил;

- ✔ Статистика – вывод статистики использования правил фильтрации текущего набора правил в пакетном фильтре.

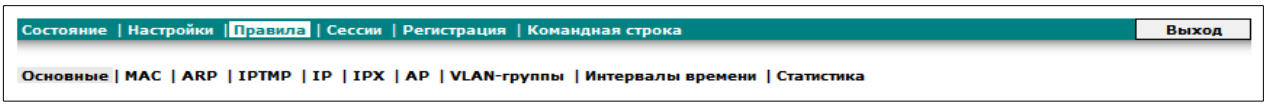

Рисунок 2.21: Меню раздела "Правила"

- Сессии – содержит страницы для настройки параметров подсистемы управления сессиями пакетного фильтра и вывода текущего состояния таблицы сессий (рисунок 2.22):
  - ✔ Настройки – настройки параметров подсистемы управления сессиями пакетного фильтра;
  - ✔ Таблица сессий – вывод текущего состояния таблицы сессий.

Информация на странице “Сессии: Таблица сессий” обновляется автоматически через каждые **10** секунд.

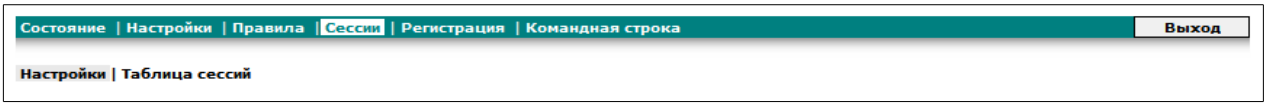

Рисунок 2.22: Меню раздела "Сессии"

- Регистрация – содержит страницы для настройки параметров подсистемы регистрации, вывода информации о зарегистрированных событиях, пакетах или сессиях, вывода зарегистрированных системных сообщений и для очистки файлов регистрации пакетов/сессий (рисунок 2.23):
  - ✔ Настройки – настройки параметров подсистемы регистрации;
  - ✔ События – вывод информации о зарегистрированных событиях с возможностью задания критериев отбора;
  - ✔ Пакеты – вывод информации о зарегистрированных пакетах с возможностью задания критериев отбора;
  - ✔ Сессии – вывод информации о зарегистрированных сессиях с возможностью задания критериев отбора;
  - ✔ Системные сообщения – вывод зарегистрированных системных сообщений;
  - ✔ Очистка файлов регистрации – удаление из файлов регистрации информации о зарегистрированных пакетах или сессиях.

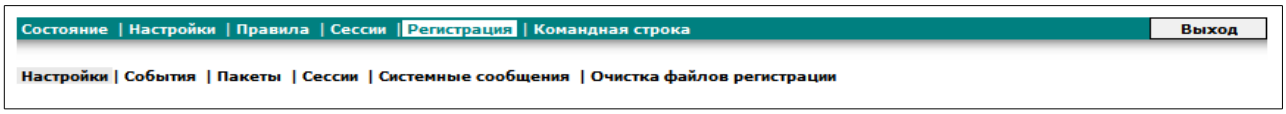

Рисунок 2.23: Меню раздела "Регистрация"

Информация о зарегистрированных событиях, пакетах и сессиях выводится в отдельном окне WEB браузера.

- Командная строка – страница для ввода команд командного интерфейса ССПТ-2. Является вспомогательным инструментом для проверки корректной передачи данных WEB-интерфейсу от командного сервера ССПТ-2 через защищенный канал управления (рисунок 2.24).

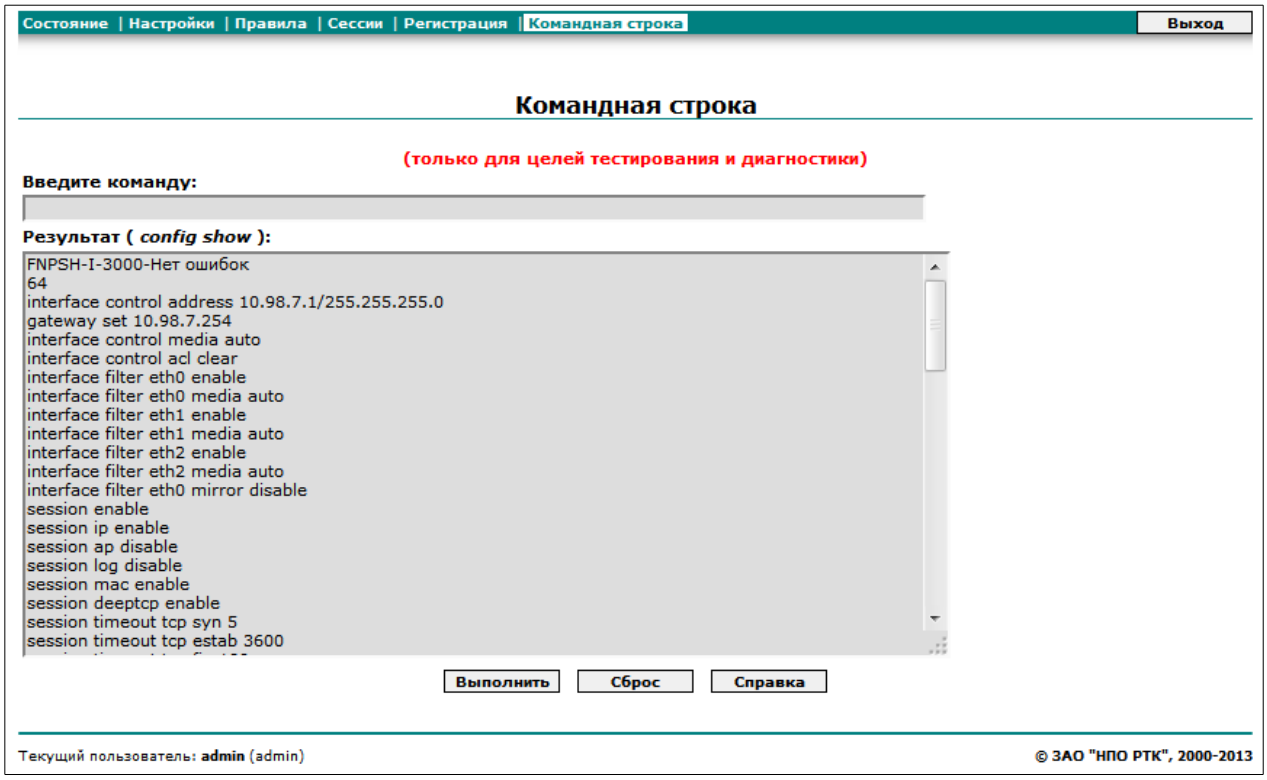

Рисунок 2.24: Раздел "Командная строка"

2.7.5. Вывод диагностических сообщений в WEB-интерфейсе ССПТ-2

Принцип работы WEB-интерфейса заключается в формировании команды или нескольких команд на основании действий, выполненных пользователем, и передачи этих команд на выполнение командному серверу ССПТ-2 по защищенному каналу управления.

Выполнение любой команды через WEB-интерфейс ССПТ-2 всегда завершается выводом диагностического сообщения в отдельном окне WEB браузера. Формат вывода диагностического сообщения совпадает с тем, что принято для командного интерфейса ССПТ-2 (приложение 3.5.1, стр. 190).

В WEB-интерфейсе диагностические сообщения разного уровня выводятся различными цветами:

- зеленый – для информационных сообщений;
- синий – для предупреждений;
- красный – для сообщений об ошибках.

На рисунке 2.25 приводится вывод *информационного сообщения* с кодом `0x3057` (шестнадцатеричный).

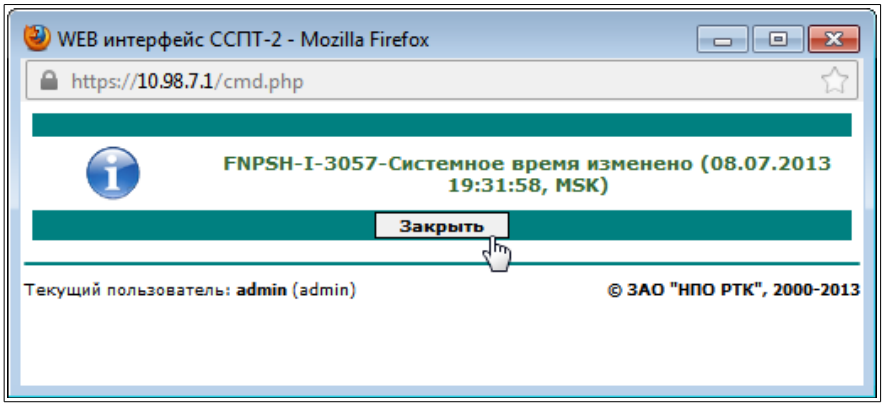

Рисунок 2.25: Вывод диагностического сообщения в WEB-интерфейсе ССПТ-2

Для того, чтобы закрыть окно диагностического сообщения необходимо нажать кнопку “Закрыть”.

Если действия пользователя в WEB-интерфейсе ССПТ-2 привели к формированию и передаче на выполнение сразу нескольких команд, то в окне диагностических сообщений будет также выведено несколько диагностических сообщений в порядке, соответствующем порядку выполнения сформированных команд.

Перечень всех диагностических сообщений командного интерфейса ССПТ-2 приводится в приложении 3.5, стр. 190.

3. Приложения

3.1. Установка IVT VT220 Freeware на управляющий компьютер

В данном разделе приводится краткое руководство по установке пакета **IVT VT220 Freeware**, который может быть использован для доступа к командному интерфейсу администратора ССПТ-2 по последовательному порту RS-232.

Пакет **IVT VT220 Freeware** предназначен для компьютеров, работающих по управлением операционных систем MS Windows® XP/Vista/7

Для установки **IVT VT220 Freeware** необходимо выполнить следующие действия:

- вставить компакт-диск ССПТ-2 в привод CD-ROM на управляющем компьютере;
- запустить программу установки IVT VT220 Freeware `setup.exe`, расположенную в каталоге `software/comms/ivt_vt220_freeware` на компакт-диске ССПТ-2;
- последовательно пройти все шаги по установке **IVT VT220 Freeware** так, как это показано на рисунках 3.1-3.6. Переход к очередному шагу установки осуществляется нажатием кнопки “`Next>`”(рисунки 3.1-3.5), завершение установки осуществляется нажатием кнопки “`Finish`” (рисунок 3.6);

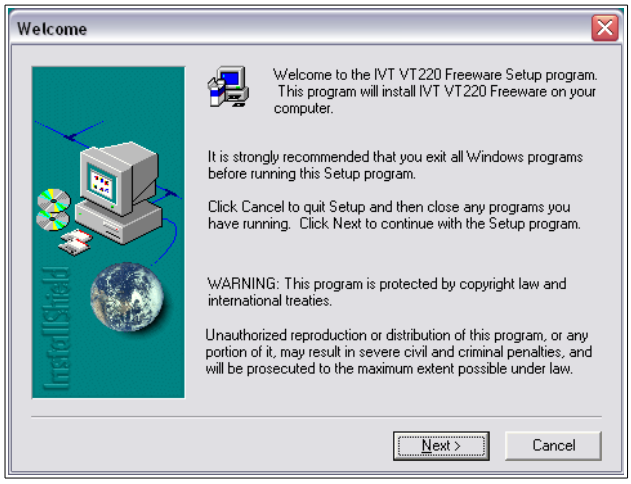

Рисунок 3.1: Установка IVT VT220 Freeware. Окно "Welcome"

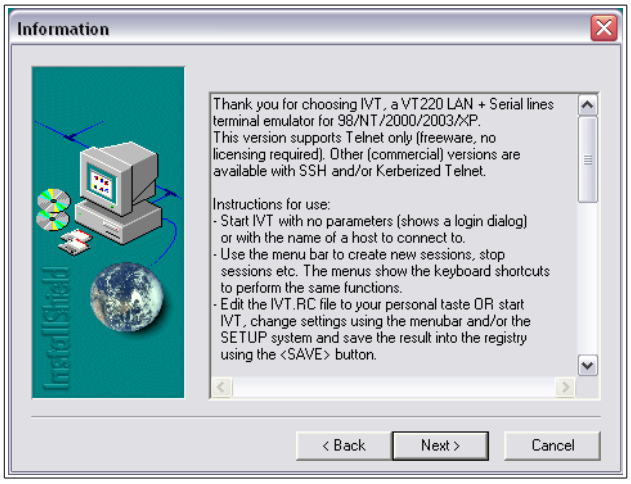

Рисунок 3.2: Установка IVT VT220 Freeware. Окно "Information"

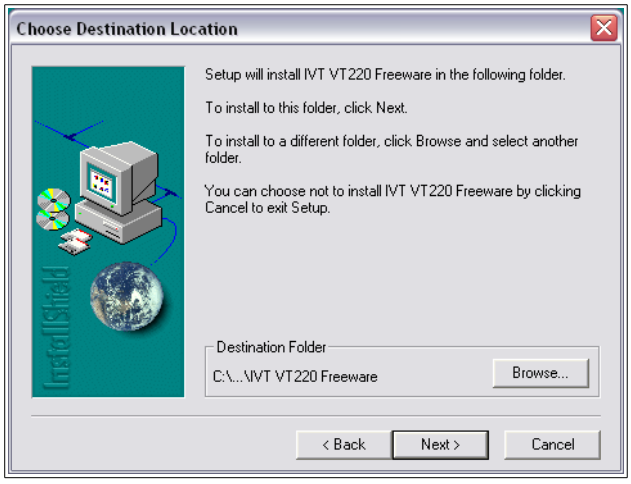

Рисунок 3.3: Установка IVT VT220 Freeware. Окно "Choose Destination Location"

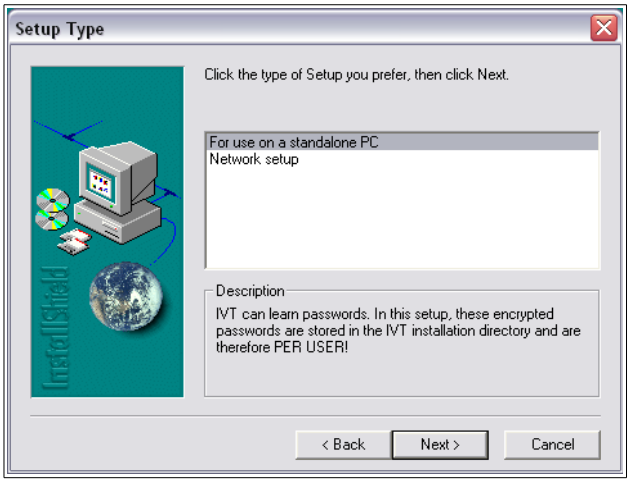

Рисунок 3.4: Установка IVT VT220 Freeware. Окно "Setup Type"

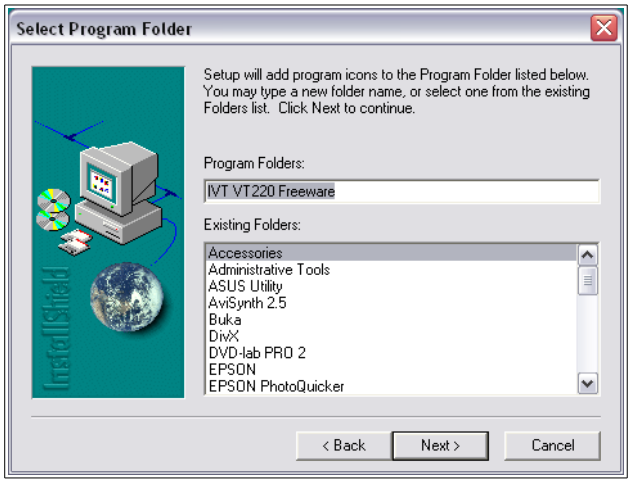

Рисунок 3.5: Установка IVT VT220 Freeware. Окно "Select Program Folder"

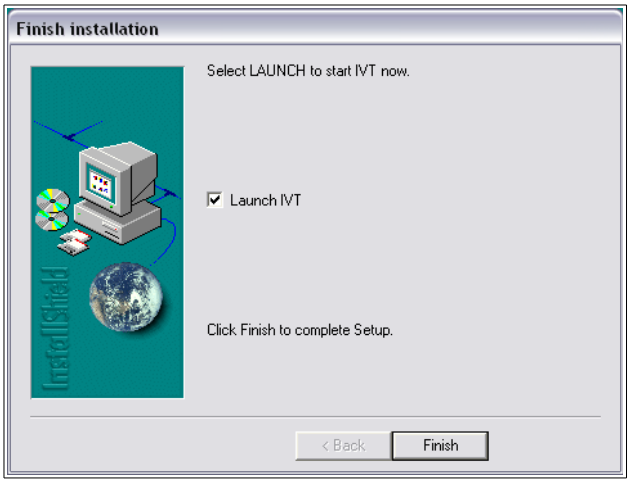

Рисунок 3.6: Установка IVT VT220 Freeware. Окно "Finish Installation"

- во время первого запуска **IVT VT220 Freeware** предлагает выполнить сценарий настройки некоторых параметров работы программы. Рекомендуется выполнить сценарий настройки, нажав клавишу <Enter> (рисунок 3.7). Сценарий настройки выполняется в **5 шагов**, диалог пользователя заключается в вводе номера пункта меню из предлагаемых сценарием настройки вариантов выбора:
  - ✔ **Шаг 1** – выбор языка пользовательского интерфейса. Выбрать использование английского языка – пункт меню **1** ("1) English"), затем нажать клавишу <Enter> (рисунок 3.8);
  - ✔ **Шаг 2** – выбор режима хранения паролей пользователей. Отказаться от хранения паролей пользователей – пункт меню **1** ("1) Never, ever, anywhere"), затем нажать клавишу <Enter> (рисунок 3.9);
  - ✔ **Шаг 3** – выбор режима эмуляции терминала VT220. Выбрать режим эмуляции для UNIX-систем – пункт меню **2** ("2) A slightly adjusted version with major benefits on most UNIX systems"), затем нажать клавишу <Enter> (рисунок 3.10);
  - ✔ **Шаг 4** – выбор режима регистрации сессий (функция AUTOLOG). Отключить использование функции AUTOLOG – пункт меню **1** ("1) Disabled entirely"), затем нажать клавишу <Enter> (рисунок 3.11);

✔ **Шаг 5** – сохранение конфигурации **IVT VT220 Freeware**. Сохранить выполненные настройки параметров – пункт меню **1** (“`1) Save this setup`”), затем нажать клавишу `<Enter>` (рисунок 3.12).

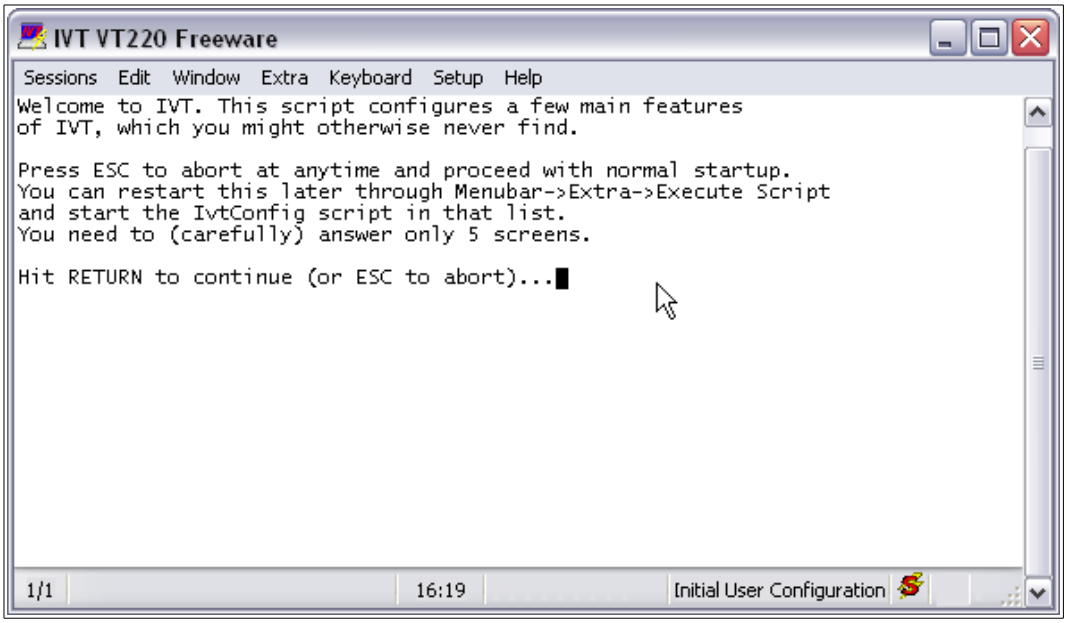

Рисунок 3.7: Сценарий настройки IVT VT220 Freeware

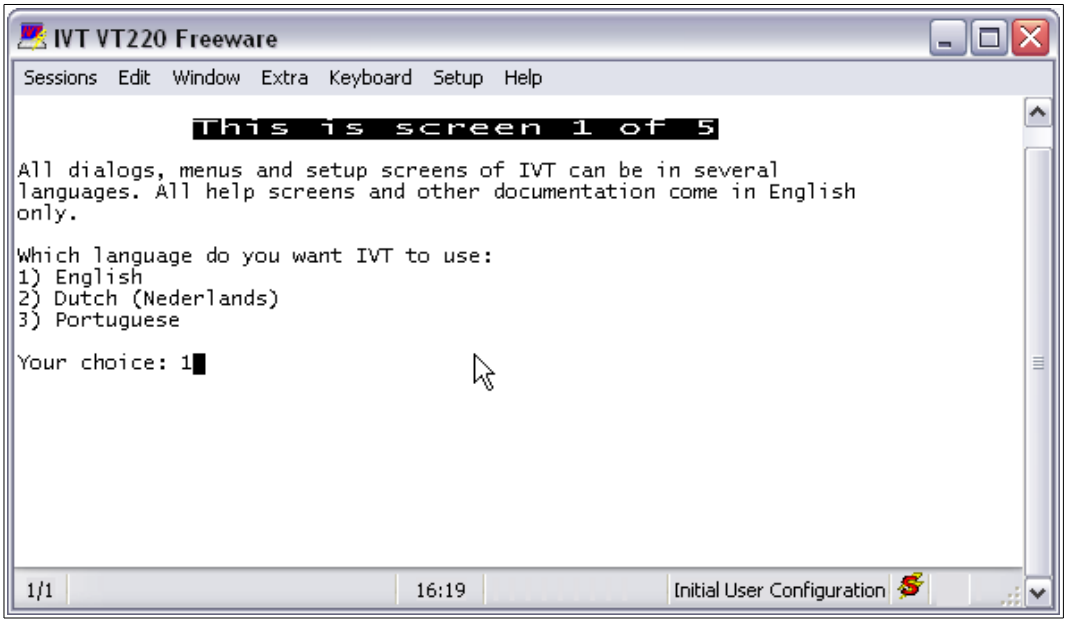

Рисунок 3.8: Шаг 1 – выбор языка пользовательского интерфейса

Рисунок 3.9: Шаг 2 – выбор режима хранения паролей пользователей

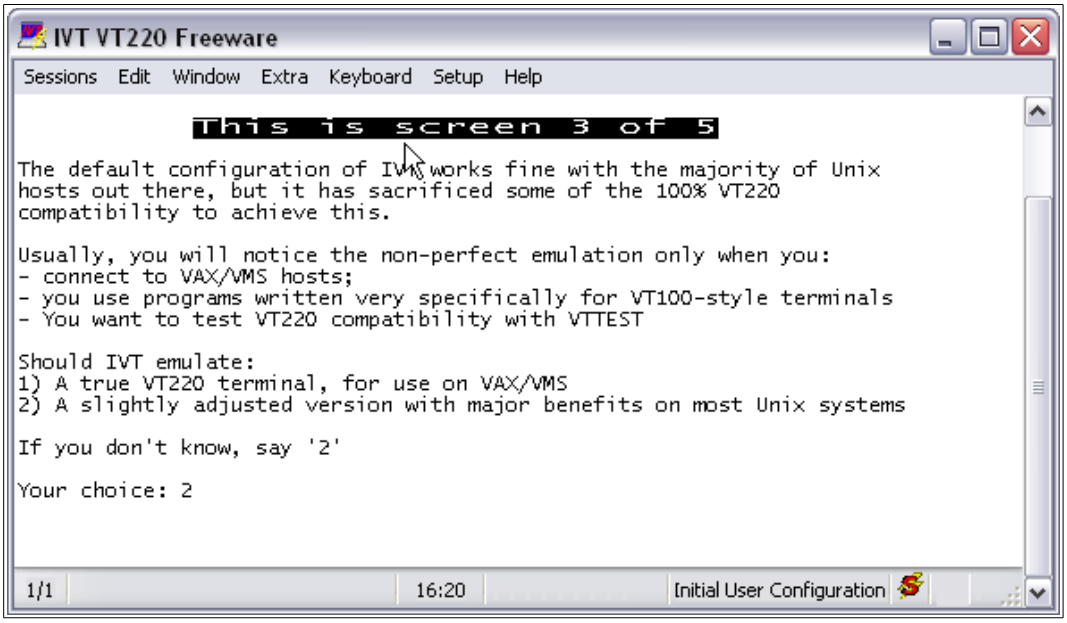

Рисунок 3.10: Шаг 3 – выбор режима эмуляции терминала VT220

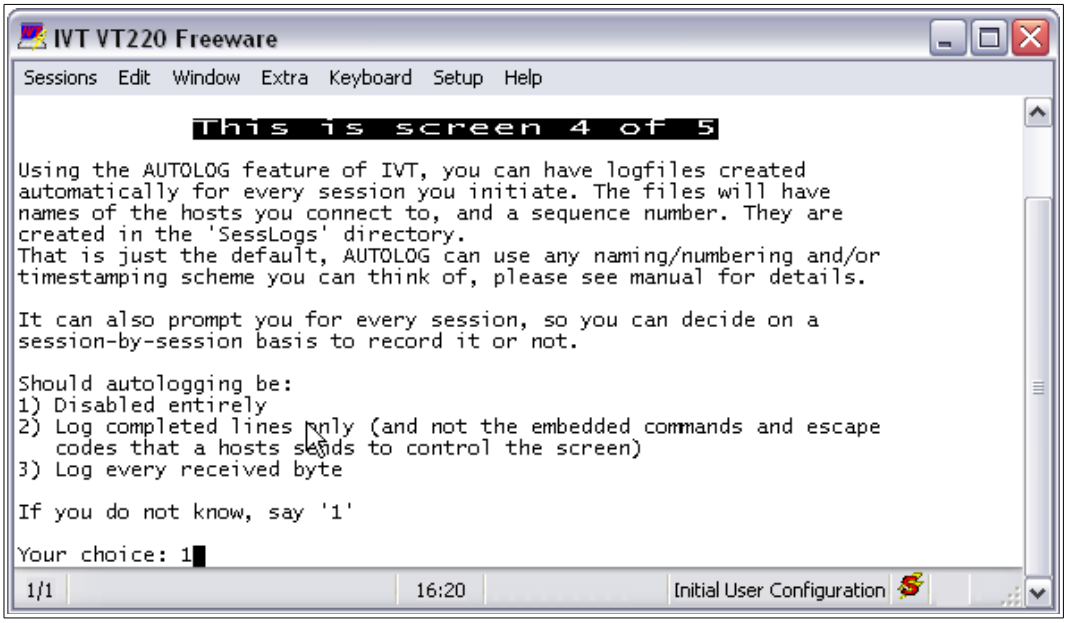

Рисунок 3.11: Шаг 4 – выбор режима регистрации сессий (функция AUTOLOG)

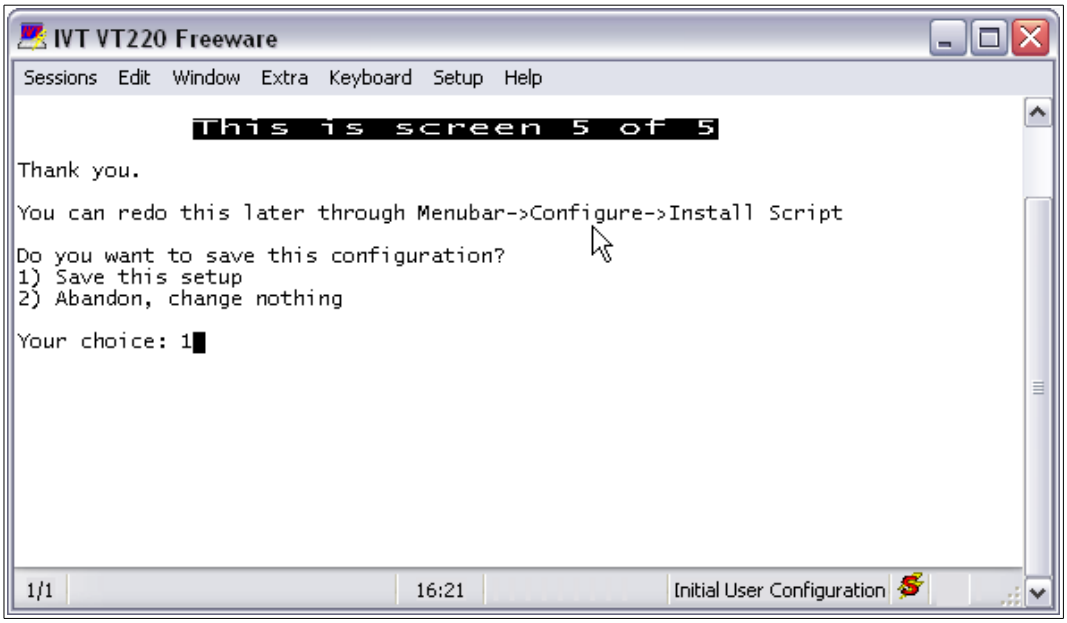

Рисунок 3.12: Шаг 5 – сохранение конфигурации IVT VT220 Freeware

3.2. Настройка PPP соединения на управляющем компьютере

PPP соединение может быть использовано для управления ССПТ-2 по последовательному порту RS-232, используя нуль-модемный кабель.

В данном разделе приводится руководство по настройке PPP соединения на управляющем компьютере, работающим под управлением операционных систем:

- MS Windows ® XP/Vista/7 (раздел 3.2.1, стр. 41). Руководство составлено на примере MS Windows ® XP;
- FreeBSD 5.x,6.x/Linux (раздел 3.2.2, стр. 50). Руководство составлено на примере операционной системы FreeBSD 6.2-RELEASE.

3.2.1. Настройка PPP соединения для операционных систем MS Windows® 2000/XP

Копирование сценария авторизации пользователя. Для работы PPP соединения необходим сценарий авторизации пользователя. Файл сценария с именем `fnp2_ppp_login.scp` располагается в каталоге `software\comms\ppp\fnp_null_modem` на компакт-диске ССПТ-2. Этот файл необходимо скопировать в каталог `%SystemRoot%\system32\ras`.

Установка драйвера модема "Null-modem PPP connection with FNP-2 Firewall". Для установки драйвера модема необходимо открыть раздел "`Панель управления→Телефон и модем`", после чего в появившемся окне выбрать закладку "`Модемы`" и нажать кнопку "`Добавить...`"(рисунок 3.13).

Запустится "**Мастер установки оборудования**". В появившемся окне необходимо выбрать пункт "`Не определять тип модема (выбор из списка)`" и нажать кнопку "`Далее >`" (рисунок 3.14).

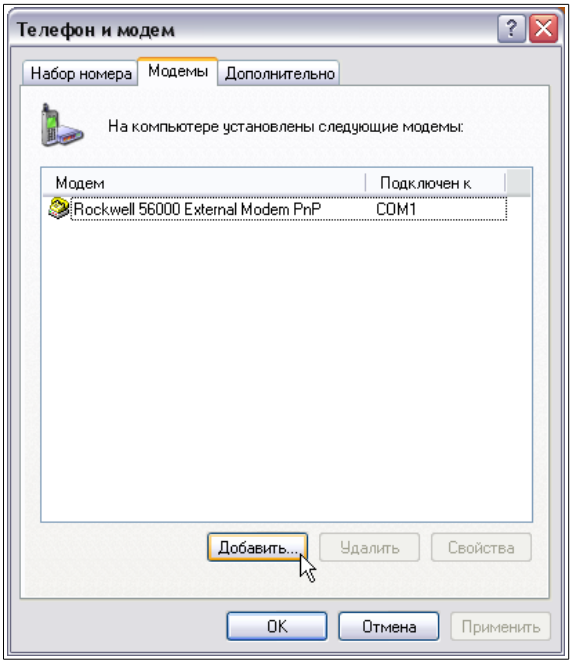

Рисунок 3.13: Телефон и модем

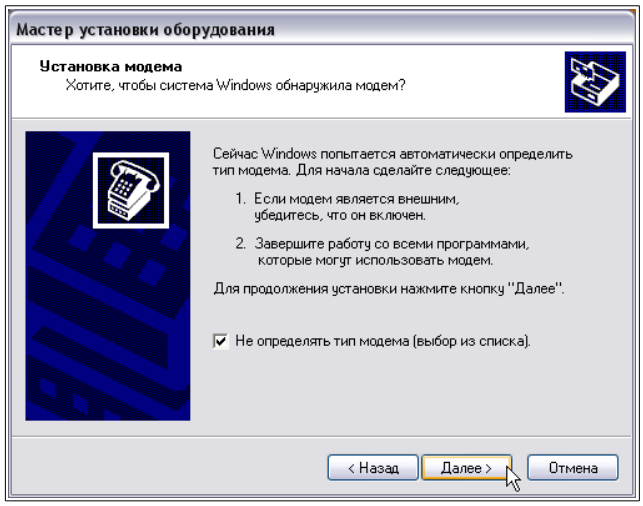

Рисунок 3.14: Мастер установки оборудования

В следующем окне осуществляется выбор изготовителя и модели модема. Файл драйвера модема "**Null-modem PPP connection with FNP-2 Firewall**" с именем `fnp2mdm.inf` располагается в каталоге `software\comms\ppp\fnp_null_modem` на компакт диске ССПТ-2. Для выбора файла драйвера модема нажать кнопку "`Установить с диска...`" (рисунок 3.15). В окне "**Установка с диска**" нажать кнопку "`Обзор...`"(рисунок 3.16) и выбрать файл драйвера модема с компакт-диска ССПТ-2 (рисунок 3.17).

После этого появится окно со списком доступных для установки устройств. В списке необходимо выделить строку "`Null-modem PPP connection with FNP-2 Firewall`" и нажать кнопку "`Далее >`" (рисунок 3.18).

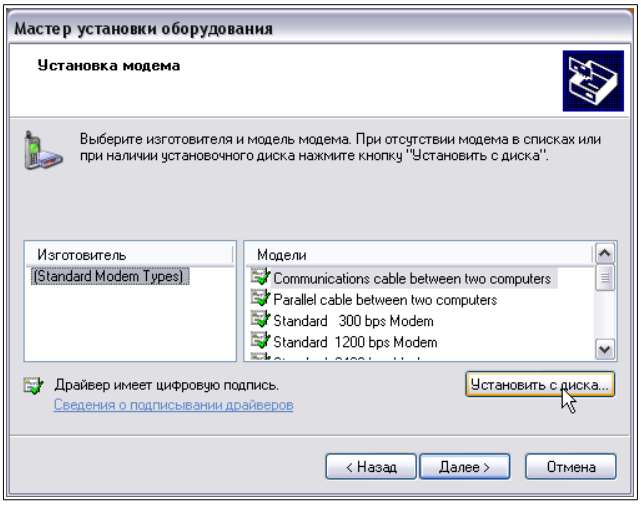

Рисунок 3.15: Выбор модема

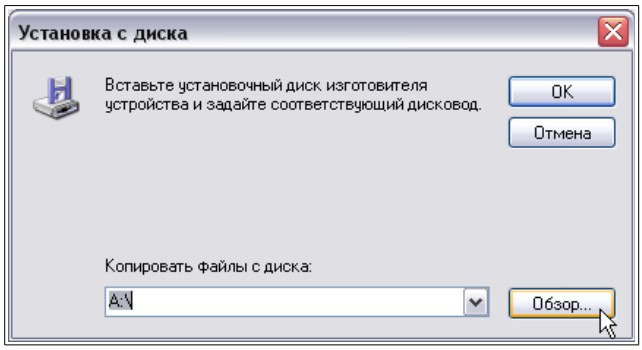

Рисунок 3.16: Установка с диска

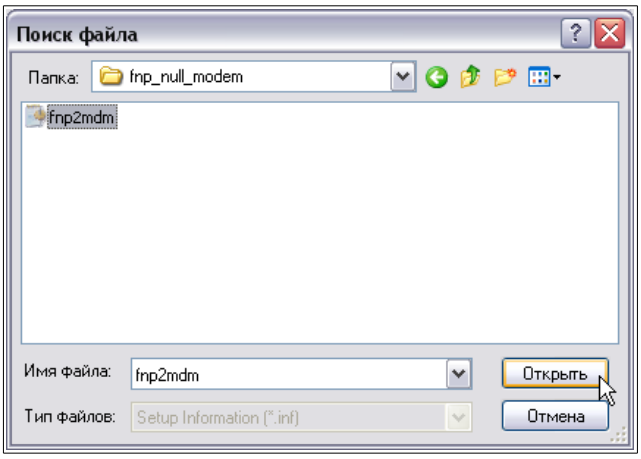

Рисунок 3.17: Выбор файла драйвера модема

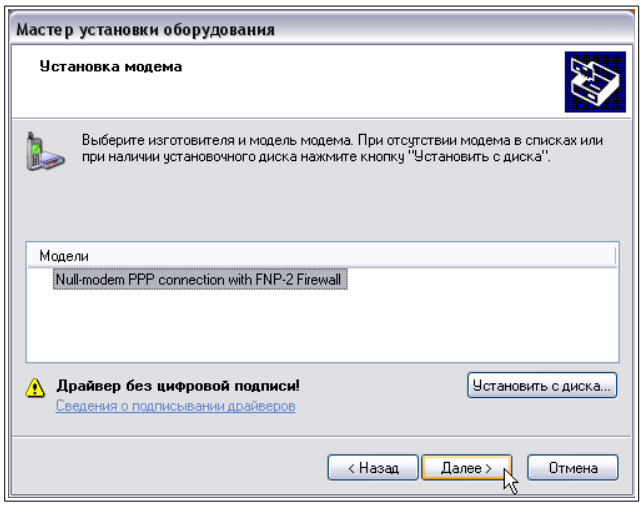

Рисунок 3.18: Выбор изготовителя и модели модема

В следующем окне необходимо выбрать последовательный порт управляющего компьютера, к которому будет подключаться нуль-модемный кабель, соединяющий управляющий компьютер с ССПТ-2. Для этого необходимо выделить переключатель “Выбранные порты” и нажать кнопку “Далее >” (рисунок 3.19).

Следующее окно будет содержать сообщение о том, что устанавливаемое программное обеспечение, в данном случае – драйвер модема “**Null-modem PPP connection with FNP-2 Firewall**”, не тестировалось на совместимость с операционной системой Windows XP. Необходимо продолжать установку модема, нажав кнопку “Все равно продолжить” (рисунок 3.20). В данном случае отсутствие подобного тестирования не скажется отрицательным образом на работоспособности системы в целом.

Далее будет выполнена установка драйвера модема “**Null-modem PPP connection with FNP-2 Firewall**”. В случае успешного окончания установки будет выведено окно с соответствующим сообщением. Для завершения работы “**Мастера установки оборудования**” необходимо нажать кнопку "Готово" (рисунок 3.21).

В окне “**Телефон и модем**”, закладка “**Модемы**” в списке установленных модемов появится строка “`Null-modem PPP connection with FNP-2 Firewall`”. Для проверки правильности настроек модема следует выполнить следующие действия:

- в списке установленных модемов окна “**Телефон и модем**” выделить строку “`Null-modem PPP connection with FNP-2 Firewall`” и нажать кнопку “`Свойства`” (рисунок 3.22);

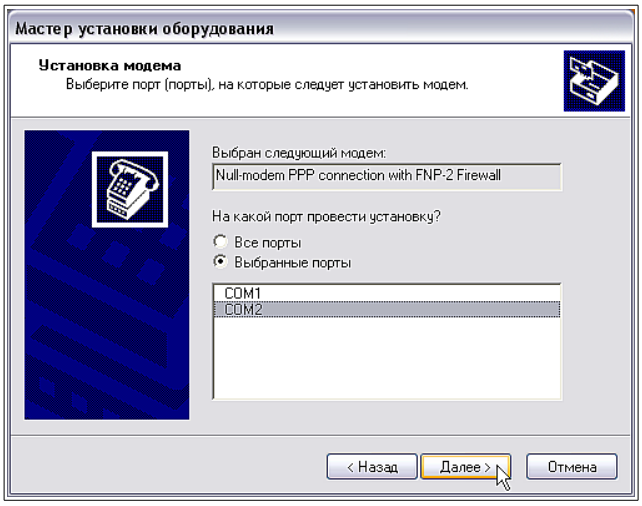

Рисунок 3.19: Выбор порта для модема

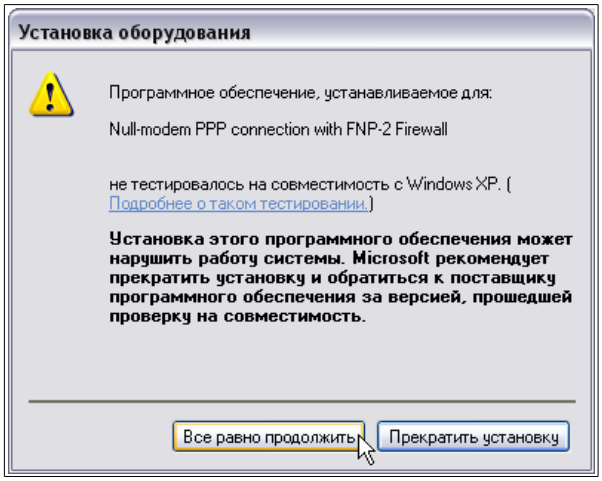

Рисунок 3.20: Тестирование на совместимость

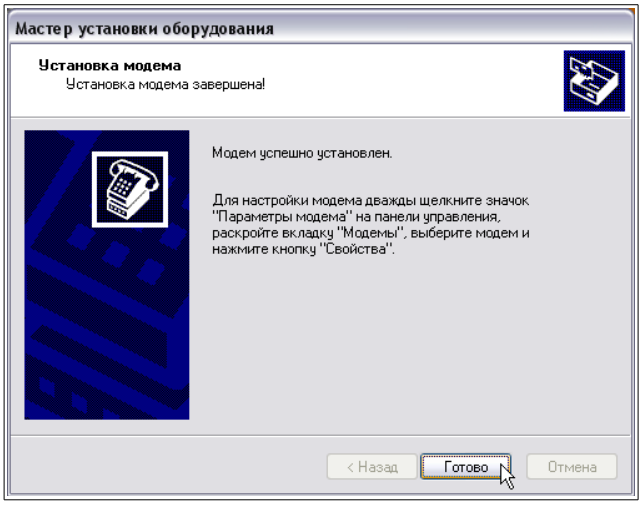

Рисунок 3.21: Завершение установки модема

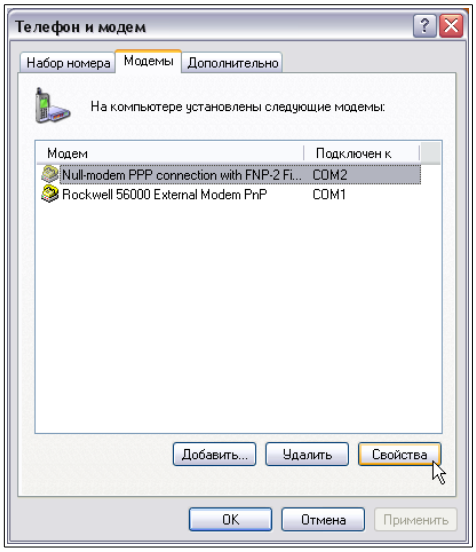

Рисунок 3.22: Проверка свойств модема

- убедиться, что установки полей закладки “**Модем**” соответствуют значениям, приведенным на рисунке 3.23;
- на закладке “**Дополнительные параметры связи**” нажать кнопку “`Изменить умолчания ...`” (рисунок 3.24) и убедиться, что установки полей закладки “**Общие**” соответствуют значениям, приведенным на рисунке 3.25, а установки полей закладки “**Дополнительные параметры связи**” соответствуют значениям, приведенным на рисунке 3.26;

Закрыть окно “**Телефон и модем**”, нажав кнопку “`Ok`”. Установка драйвера модема “**Null-modem PPP connection with FNP-2 Firewall**” завершена.

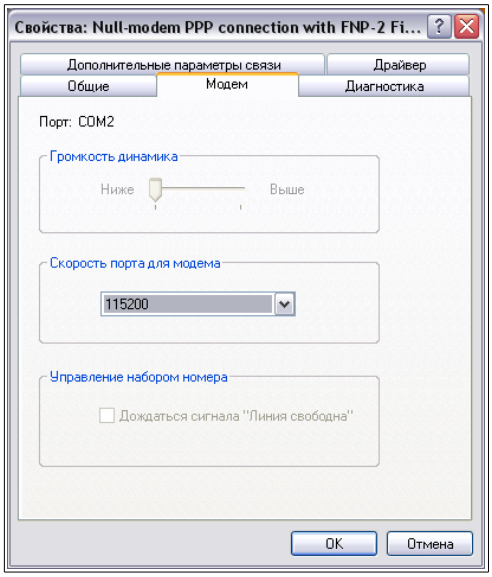

Рисунок 3.23: Свойства модема. Закладка “Модем”

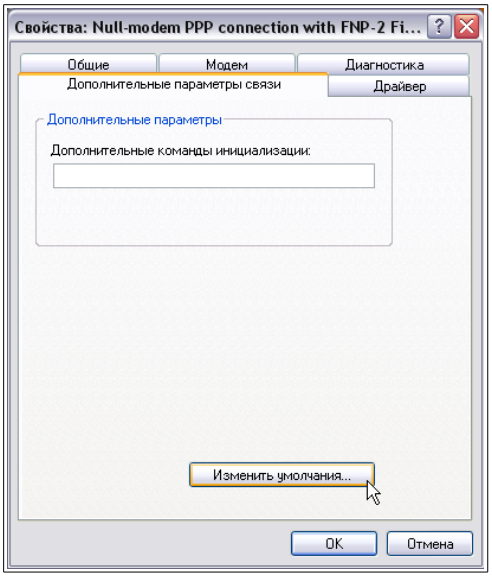

Рисунок 3.24: Свойства модема. Закладка “Дополнительные параметры связи”

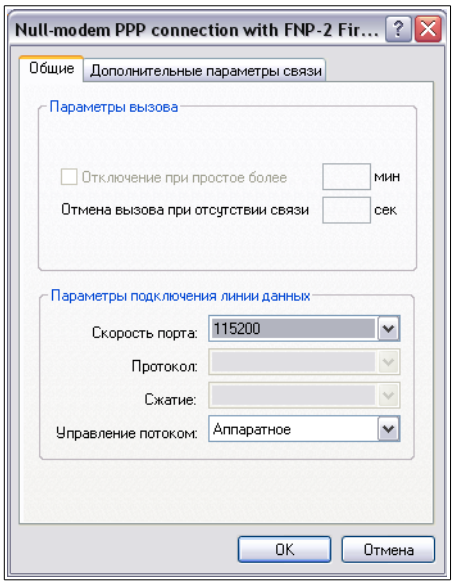

Рисунок 3.25: Свойства модема. Закладка “Дополнительные параметры связи → Общие”

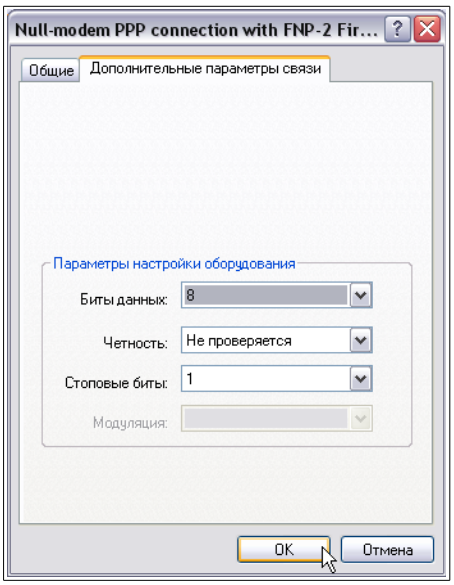

Рисунок 3.26: Свойства модема. Закладка “Дополнительные параметры связи→Дополнительные параметры связи”

Создание сетевого соединения. Для создания сетевого соединения необходимо открыть раздел “Панель управления → Сетевые подключения”, затем в появившемся окне щелкнуть на ссылке “Создание сетевого подключения” (рисунок 3.27).

Запустится “**Мастер новых подключений**”. В появившемся окне нажать кнопку “Далее >” (рисунок 3.28).

В следующем окне необходимо выбрать тип сеетвого соединения “Подключить к сети на рабочем месте” и нажать кнопку “Далее >” (рисунок 3.29).

В следующем окне необходимо выбрать способ подключения “Подключение удаленного доступа” и нажать кнопку “Далее >” (рисунок 3.30).

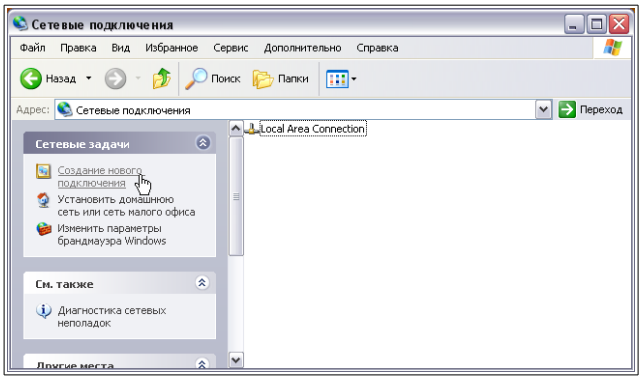

Рисунок 3.27: Создание сетевого соединения

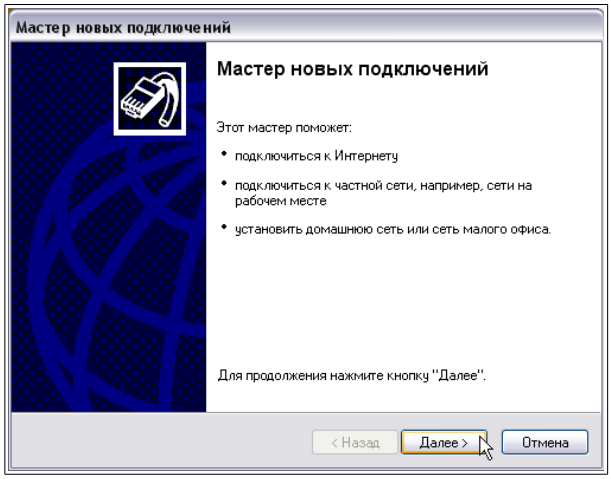

Рисунок 3.28: Мастер новых подключений

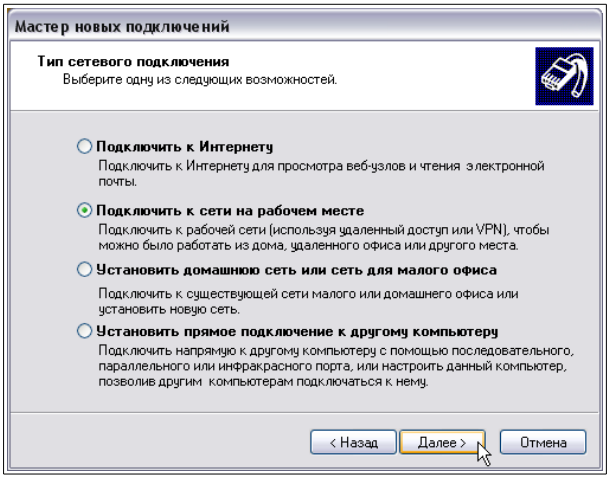

Рисунок 3.29: Тип сетевого подключения

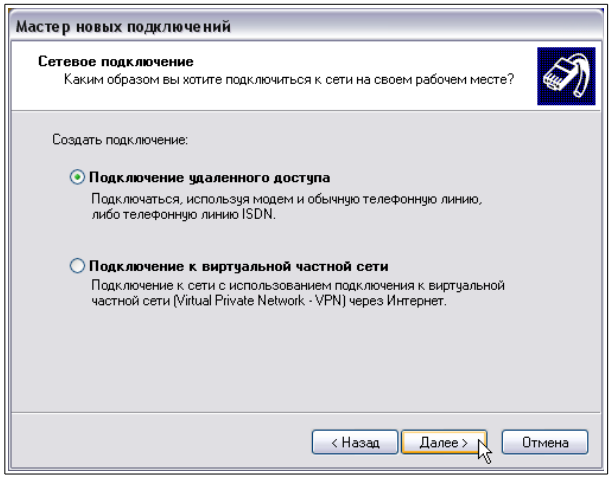

Рисунок 3.30: Сетевое подключение

Если в системе установлено несколько модемов, “**Мастер новых подключений**” предложит выбрать модем для создаваемого соединения. В списке выбора модема необходимо выделить модем “Null-modem PPP connection with FNP-2 Firewall” и нажать кнопку “Далее >” (рисунок 3.31).

В следующем окне необходимо ввести имя сетевого соединения и нажать кнопку “Далее >”. Оно может быть любым в рамках синтаксиса, определенного операционной системой. Например так, как показано на рисунке 3.32 – “FNP-2”.

В следующем окне необходимо ввести номер телефона. Для подключения к ССПТ-2 номер телефона не играет никакой роли, поэтому можно ввести любую последовательность цифр, и нажать кнопку “Далее >”. Пример ввода номера телефона – на рисунке 3.33.

“**Мастер новых подключений**” инициирует процесс создания нового сетевого соединения. При его успешном завершении будет выведено окно завершения работы “**Мастера новых подключений**” (рисунок 3.34). При желании, можно установить ярлык созданного соединения на рабочий стол, выделив свойство “Добавить ярлык подключения на рабочий стол”. Завешить работу “**Мастера новых подключений**”, нажав кнопку “Готово”.

В результате в списке сетевых соединений в окне “**Сетевые подключения**” появится новое сетевое соединение с именем **FNP-2**.

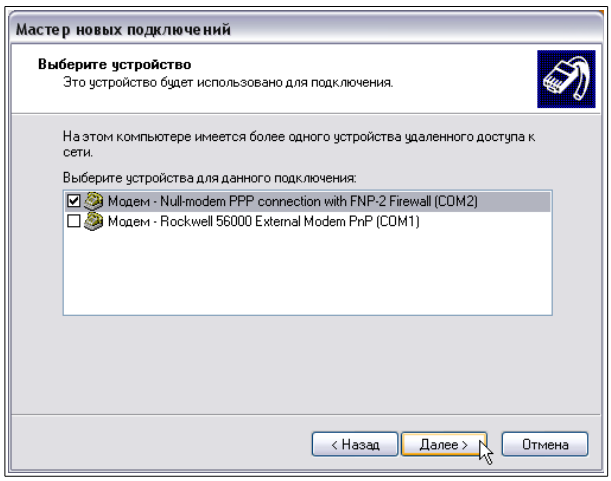

Рисунок 3.31: Выбор модема

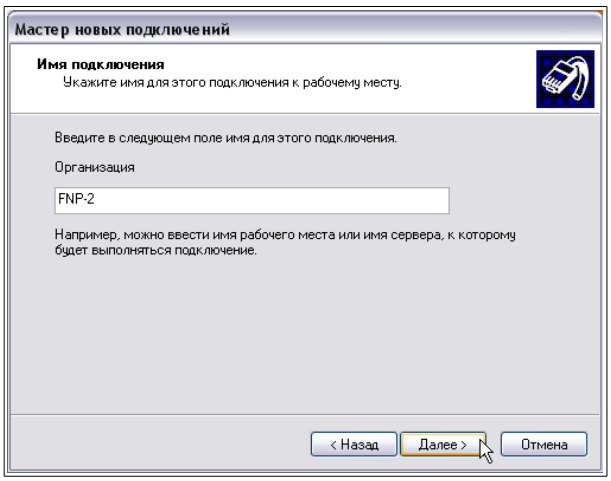

Рисунок 3.32: Имя подключения

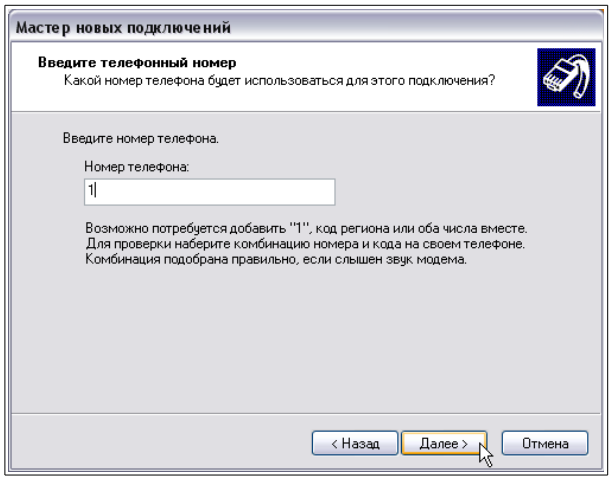

Рисунок 3.33: Номер телефона

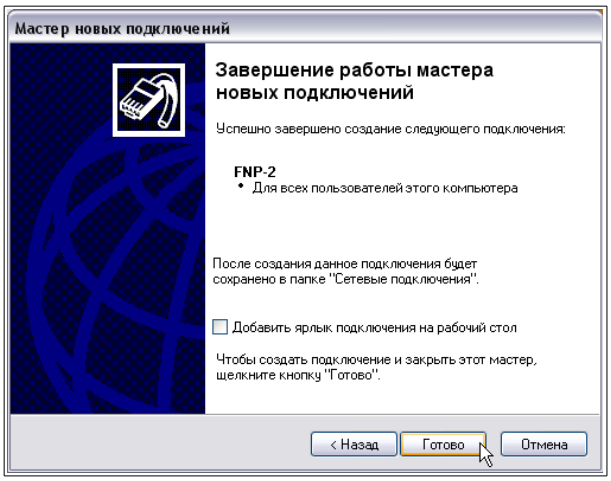

Рисунок 3.34: Завершение Мастера новых подключений

Настройка свойств сетевого соединения. Для настройки свойств сетевого соединения **FNP-2** необходимо двойным щелчком открыть окно соединения, и в появившемся окне “**Подключение к FNP-2**” нажать кнопку “Свойства” (рисунок 3.35). Появится окно свойств соединения “**FNP-2 Свойства**”.

Для настройки свойств сетевого соединения необходимо выполнить следующие действия:

- для настройки параметров модема в окне “**FNP-2 Свойства**” на закладке “**Общие**”нажать кнопку “Настроить...” (рисунок 3.36). Установить настройки модема в соответствии с рисунком 3.37 и нажать кнопку “Ok”;
- открыть закладку “**Параметры**” и установить параметры в соответствии с рисунком 3.38;
- открыть закладку “**Безопасность**” (рисунок 3.39). Установить группу свойств “**Параметры безопасности**” в состояние “Обычные (рекомендуемые параметры)”. В группе свойств “**Интерактивная регистрация и сценарий**” включить свойства “Вывести окно терминала” и

“Сценарий”, затем выбрать файл сценария авторизации пользователя `fnp2_ppp_login.scp`, нажав кнопку “`Обзор...`”;

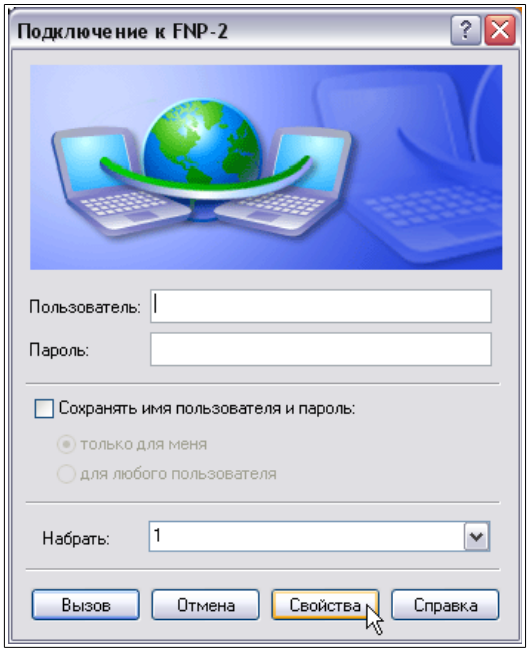

Рисунок 3.35: Окно соединения “Подключение к FNP-2”

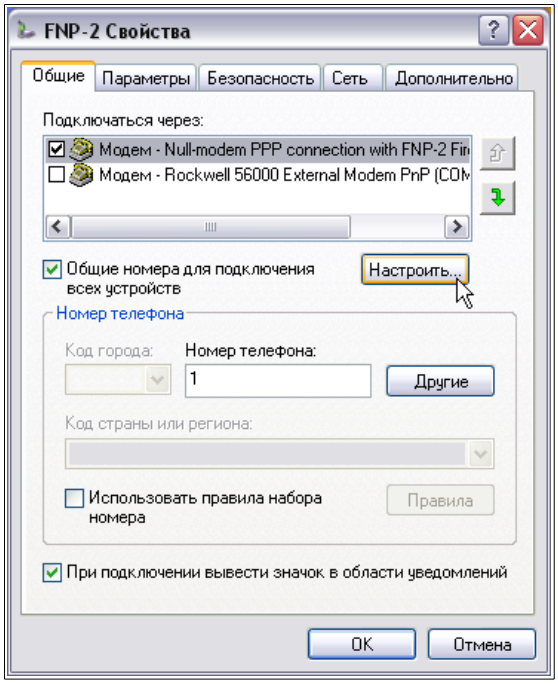

Рисунок 3.36: Свойства соединения. Закладка “Общие”

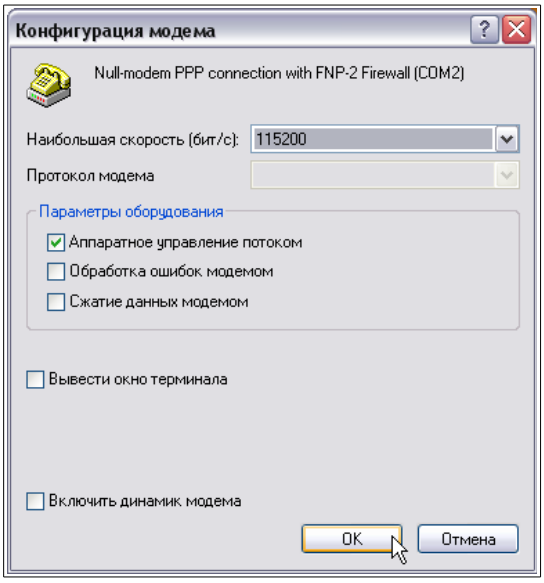

Рисунок 3.37: Конфигурация модема

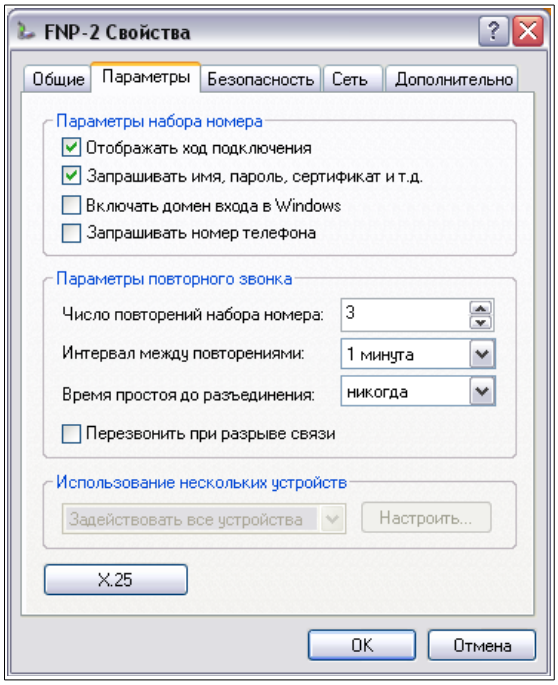

Рисунок 3.38: Свойства соединения. Закладка “Параметры”

- открыть закладку “**Сеть**” (рисунок 3.40). В списке “**Компоненты, используемые этим подключением:**” выбрать только “`Internet Protocol (TCP/IP)`” (компонент “`QoS Packet Scheduler`”, если он присутствует в этом списке, будет выбран всегда);
- в списке “**Тип подключаемого сервера удаленного доступа:**” выбрать пункт “`PPP: Windows 95/98/NT/2000, Internet`” и нажать кнопку “`Параметры`”. В появившемся окне “`Параметры PPP`” установить параметры в соответствии с рисунком 3.41, нажать кнопку “`Ok`”;

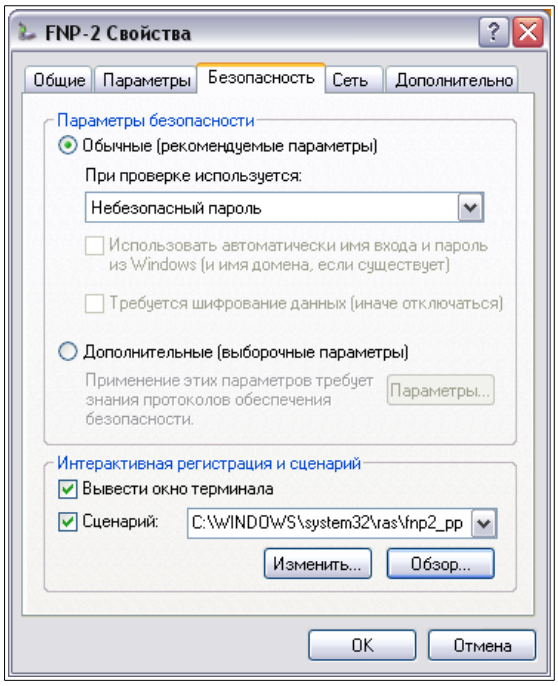

Рисунок 3.39: Свойства соединения. Закладка “Безопасность”

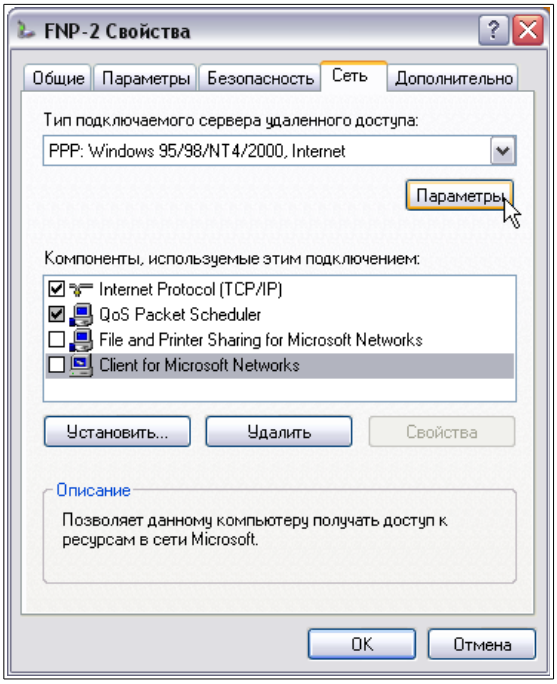

Рисунок 3.40: Свойства соединения. Закладка “Сеть”

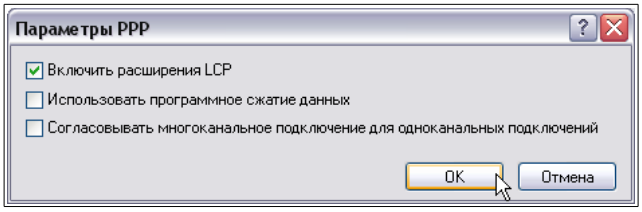

Рисунок 3.41: Окно “Параметры PPP”

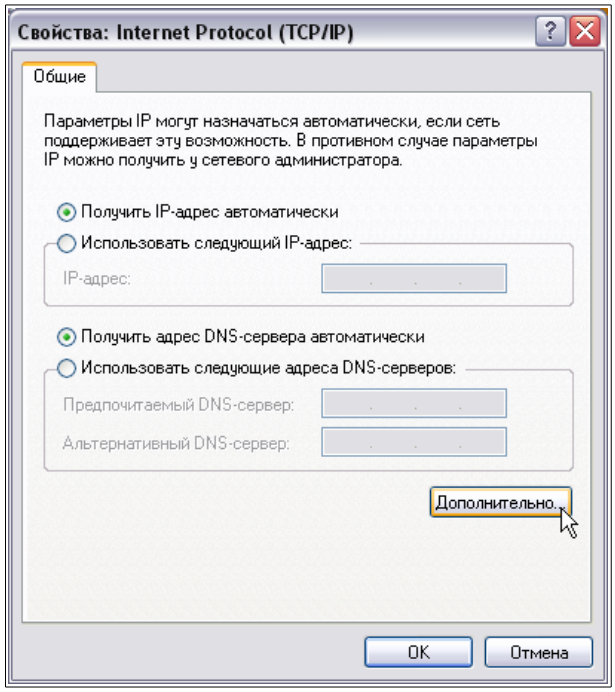

Рисунок 3.42:Свойства: Internet Protocol (TCP/IP)

- в списке “**Компоненты, используемые этим подключением:**” выбрать пункт “`Internet Protocol (TCP/IP)`” и нажать кнопку “`Свойства`”. В появившемся окне “**Свойства: Internet Protocol (TCP/IP)**” выбрать свойства “`Получить IP-адрес автоматически`” и “`Получить адрес DNS-сервера автоматически`” и нажать кнопку “`Дополнительно...`” (рисунок 3.42);
- в появившемся окне “**Дополнительные параметры TCP/IP**” на закладке “**Общие**” отключить свойство “`Использовать основной шлюз в удаленной сети`” и нажать кнопку “`Ok`” (рисунок 3.43).

Закрыть окно свойств сетевого соединения FNP-2, нажав кнопку “`Ok`”.

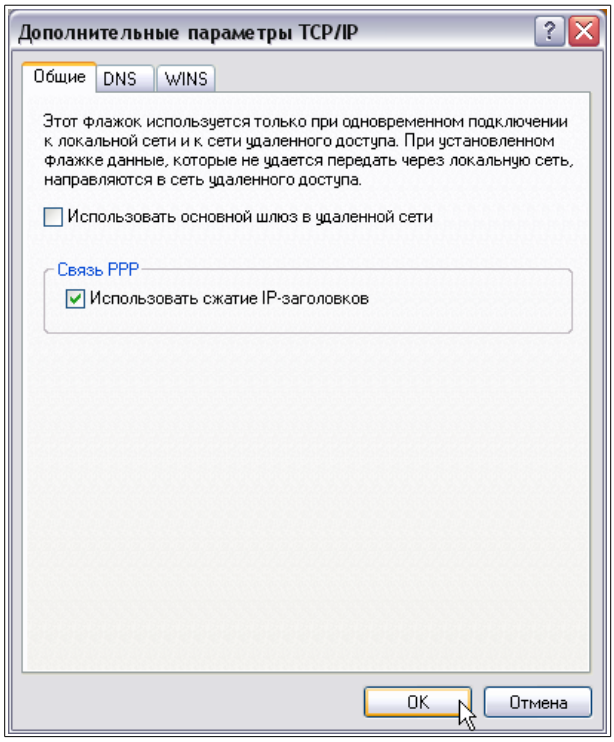

Рисунок 3.43: Дополнительные параметры TCP/IP

3.2.2. Настройка PPP соединения для операционных систем FreeBSD/Linux

Для управления ССПТ-2 по выделенному последовательному каналу, на управляющих компьютерах с установленными операционными системами FreeBSD/Linux необходимо использовать существующие в этих операционных системах механизмы реализации протокола PPP.

В данном руководстве предлагается использование утилиты **pppd** (PPP daemon), входящей в стандартную поставку указанных выше операционных систем и не требующей установки дополнительного программного обеспечения. Следует обратить внимание на то, что в ядро операционной системы необходимо включить поддержку протокола PPP. Вопросы настройки ядра операционной системы выходят за рамки настоящего руководства, поэтому администратору следует обратиться к соответствующей документации по операционной системе, которую он использует.

На компакт-диске ССПТ-2 в подкаталоге `software/comms/ppp/fnp_ppp_unix` имеется архивный файл `fnp_ppp_unix.tar.gz`, содержащий все необходимые файлы настроек для утилиты `pppd`. Необходимо скопировать его в файловую систему управляющего компьютера.

Дальнейшие действия по распаковке архива и настройке `pppd` необходимо выполнять, имея привилегии суперпользователя **`root`**.

Допустим, текущим каталогом является тот каталог, в который был скопирован файл `fnp_ppp_unix.tar.gz`. Тогда распаковку этого архива необходимо выполнить следующим образом:

```
# tar -xvzf fnp_ppp_unix.tar.gz -C /etc/ppp
```

В результате все содержимое архива будет распаковано в подкаталог `/etc/ppp` файловой системы управляющего компьютера.

В этом подкаталоге появятся следующие файлы (имена файлов указываются относительно подкаталога `/etc/ppp`):

- **`peers/fnp2`** – файл параметров `pppd` для соединения с ССПТ-2. Возможно, потребуется изменить первый параметр в первой строке этого файла, с тем, чтобы привести его в соответствие с

правилами именования файлов устройств в различных версиях операционных систем FreeBSD и Linux. Он обозначает имя файла устройства последовательного порта управляющего компьютера, к которому которому будет подключаться нуль-модемный кабель, соединяющий управляющий компьютер с ССПТ-2. Имя файла устройства указывается относительно каталога `/dev`;

- **`fnp2.chat`** – файл сценария для утилиты автоматизации диалога `chat`. Используется для автоматизированного ввода параметров авторизации для запуска сервера PPP на стороне ССПТ-2;
- **`fnp2_ppp.sh`** – shell-сценарий для установки и разрыва PPP-соединения с ССПТ-2;
- **`options`** – основной файл параметров `pppd` (не входит в архивный файл `fnp_ppp_unix.tar.gz`). Если этот файл уже существует и используется для выполнения других PPP соединений, его следует оставить без изменений, в противном случае этот файл должен содержать одну строку:

```
netmask 255.255.255.252
```

3.3. Управление ССПТ-2 по сети Ethernet

В ССПТ-2 имеется возможность организации **управления по сети Ethernet**. Для этого ССПТ-2 оснащается дополнительным интерфейсом Ethernet, разъем которого обозначен как **EthC.** Этот интерфейс используется **только для целей** управления, и не должен подключаться к защищаемым сегментам сети.

По умолчанию управляющему Ethernet-интерфейсу назначен IP-адрес **10.234.28.71** с сетевой маской **255.255.0.0**.

В целях безопасности сегмент сети управления должен быть **физически изолирован** от всей остальной сети, либо сеть управления должна быть организована как виртуальная сеть (VLAN), доступ к которой разрешается только ССПТ-2 и управляющему компьютеру.

Исходя из вышеизложенного, управляющим Ethernet-интерфейсам ССПТ-2, и только им, должны быть назначены **IP-адреса**, которые исходя из требований безопасности, рекомендуется выбирать из диапазонов “немаршрутизируемых” адресов IP сетей:

- **10.0.0.0** – **10.255.255.255** для сетей класса A;
- **172.16.0.0** – **172.31.255.255** для сетей класса B;
- **192.168.0.0** – **192.168.255.255** для сетей класса C.

Не рекомендуется назначать интерфейсам управления IP-адреса из сети **192.168.1.0/255.255.255.0**, поскольку эти адреса используются при подключении к ССПТ-2 по последовательному порту RS-232 с использованием PPP соединения.

Пример распределения IP-адресов в сети управления ССПТ-2 приведен на рисунке 3.44. В этом примере сетевой интерфейс управляющего компьютера, подключенный к сети управления, имеет IP-адрес **192.168.20.254** с маской IP-подсети **255.255.255.0**. Управляющие Ethernet-интерфейсы ССПТ-2, подключенные к сети управления имеют IP-адреса **192.168.20.1**, **192.168.20.2** и **192.168.20.3** с той же самой маской IP-подсети **255.255.255.0**.

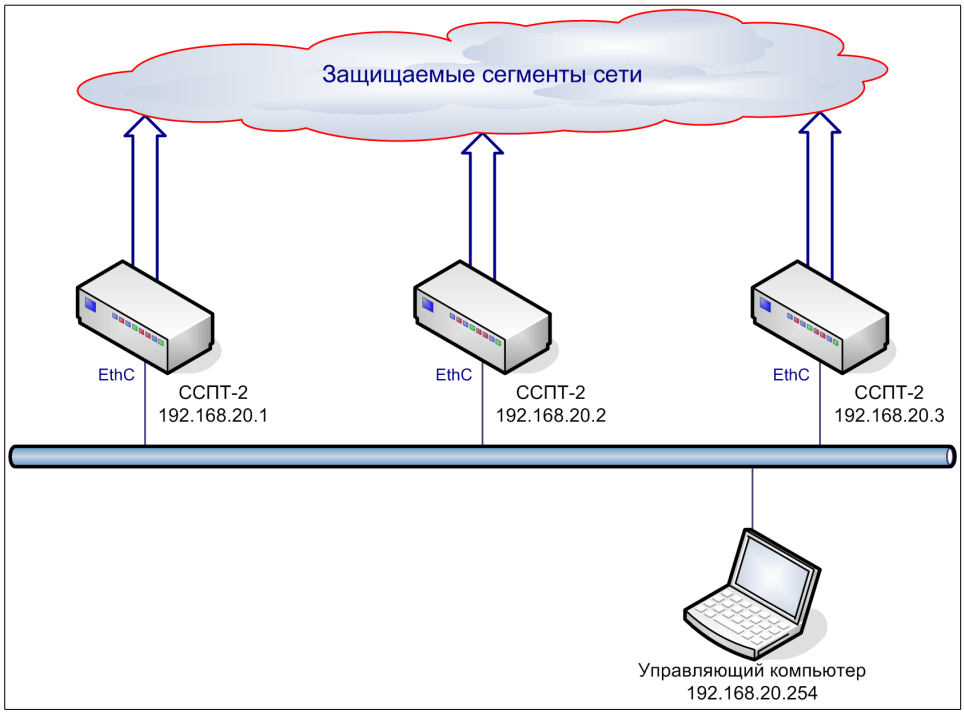

Рисунок 3.44: Управление по сети Ethernet

Таким образом, администратор имеет возможность управлять несколькими сетевыми процессорами ССПТ-2 с одного управляющего компьютера.

3.4. Командный язык ССПТ-2

В данном разделе приводится перечень всех команд командного интерфейса ССПТ-2. Таблица 3.1 содержит краткое описание команд – синтаксис, требуемые привилегии и назначение. Команды приводятся в алфавитном порядке.

В описании синтаксиса команд приводятся максимально допустимые сокращения ключевых слов командного языка ССПТ-2, обозначаемые парой квадратных скобок – `[]`. Например, описание `conf[ig] def[ault]` означает, что данная команда может быть введена одним из следующих способов:

```
fnpsh> conf def (максимально возможное сокращение)
fnpsh> confi defa
fnpsh> confi defau
```

и т. д.

Таблица 3.1: Список команд командного интерфейса ССПТ-2

Команда	*Требуемые привилегии*	*Описание*
conf[ig] def[ault]	cfg	Инициализация текущей конфигурации ССПТ-2 значениями по умолчанию
conf[ig] lis[t]	read	Просмотр списка дополнительных конфигураций
conf[ig] lo[ad] <имя_конфигурации>	cfg и pf	Загрузка дополнительной конфигурации
conf[ig] rem[ove] <имя_конфигурации>	cfg	Удаление дополнительной конфигурации
conf[ig] sav[e] <имя_конфигурации>	cfg	Сохранение текущей конфигурации в дополнительной
conf[ig] sh[ow] [<имя_конфигурации>] [viewer={intern[al]|mor[e]|no}]	read	Просмотр параметров текущей или дополнительной конфигурации

Команда	Требуемые привилегии	Описание
exit	read	Завершение сеанса работы пользователя
fil[ter] rest[art]	pf	Перезапуск пакетного фильтра
fil[ter] start	pf	Запуск пакетного фильтра
fil[ter] statu[s]	read	Вывод информации о состоянии пакетного фильтра
fil[ter] stop	pf	Останов пакетного фильтра
gate[way] del[ete]	cfg	Удаление маршрута по умолчанию
gate[way] dis[able]	cfg	Отключение маршрута по умолчанию
gate[way] en[able]	cfg	Включение маршрута по умолчанию
gate[way] set <IP_адрес>	cfg	Установка IP-адреса шлюза по умолчанию
gate[way] sh[ow]	read	Вывод настроек и состояния маршрута по умолчанию
help	read	Вывод краткой справки по всем категориям команд ССПТ-2
interf[ace] cont[rol] acl add <элемент_списка>	cfg	Добавление элемента в список доступа
interf[ace] cont[rol] acl cl[ear]	cfg	Очистка списка доступа
interf[ace] cont[rol] acl del[ete] <номер_элемента>	cfg	Удаление элемента из списка доступа
interf[ace] cont[rol] acl sh[ow]	read	Просмотр элементов списка доступа
interf[ace] cont[rol] addr[ess] <IP_адрес/маска>	cfg	Назначение IP-адреса управляющему интерфейсу
interf[ace] cont[rol] addr[ess] del[ete]	cfg	Удаление IP-адреса управляющего интерфейса
interf[ace] cont[rol] dis[able]	cfg	Отключение управляющего интерфейса
interf[ace] cont[rol] dup[lex] {half|ful[l]}	cfg	Установка режима передачи управляющего интерфейса
interf[ace] cont[rol] en[able]	cfg	Включение управляющего интерфейса
interf[ace] cont[rol] med[ia] {auto|10|100|1000}	cfg	Установка скорости передачи управляющего интерфейса
interf[ace] cont[rol] ping <IP_адрес>	read	Проверка доступности узлов в управляющей сети
interf[ace] cont[rol] sh[ow]	read	Просмотр настроек и состояния управляющего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} dis[able]	cfg	Отключение фильтрующего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} dup[lex] {half|ful[l]}	cfg	Установка режима передачи фильтрующего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} en[able]	cfg	Включение фильтрующего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} med[ia] {auto|10|100|1000}	cfg	Установка скорости передачи фильтрующего интерфейса
interf[ace] fil[ter] {<номер>|<имя>} mir[ror] <имя> {all|in|out}	cfg	Установка параметров зеркалирования фильтрующих интерфейсов
interf[ace] fil[ter] {<номер>|<имя>} mir[ror] dis[able]	cfg	Отключение зеркалирования фильтрующих интерфейсов
interf[ace] fil[ter] {<номер>|<имя>} ren[ame] <новое_имя>	cfg	Переименование фильтрующего интерфейса

Команда	Требуемые привилегии	Описание
interf[ace] fil[ter] {all|<номер>|<имя>} sh[ow]	read	Вывод информации о состоянии фильтрующего интерфейса
interf[ace] fil[ter] {all|<номер>|<имя>} stats	read	Вывод информации о статистике трафика на фильтрующем интерфейсе
log ev[ent] sh[ow] [<критерии_отбора>]	read	Просмотр зарегистрированных событий
log exp[ort] ftp cl[ear]	log или cfg	Удаление параметров выгрузки файлов регистрации по FTP
log exp[ort] ftp dis[able]	log или cfg	Отключение выгрузки файлов регистрации по FTP
log exp[ort] ftp en[able]	log или cfg	Включение выгрузки файлов регистрации по FTP
log exp[ort] ftp set <ftp_параметры>	log или cfg	Установка параметров выгрузки файлов регистрации по FTP
log exp[ort] sysl[og] dis[able]	log или cfg	Отключение выгрузки файлов регистрации по SYSLOG
log exp[ort] sysl[og] en[able]	log или cfg	Включение выгрузки файлов регистрации по SYSLOG
log exp[ort] sysl[og] serv[er] <IP_адрес>	log или cfg	Установка IP-адреса SYSLOG сервера
log pack[et] cl[ear]	log	Очистка регистрации пакетов
log pack[et] dis[able]	log или cfg	Отключение режима регистрации пакетов
log pack[et] en[able]	log или cfg	Включение режима регистрации пакетов
log pack[et] sh[ow] [<критерии_отбора>]	read	Просмотр зарегистрированных пакетов
log ses[sion] cl[ear]	log	Очистка регистрации сессий
log ses[sion] sh[ow] [<критерии_отбора>]	read	Просмотр зарегистрированных сессий
log sh[ow]	read	Просмотр параметров подсистемы регистрации
log sysl[og] sh[ow] [viewer={intern[al]|mor[e]|no}]	read	Просмотр системных сообщений
nat arp add {<номер>|<имя>} <IP_адрес> <MAC_адрес>	cfg или pf	Добавление записи в ARP таблицу
nat arp cl[ear]	cfg или pf	Очистка ARP таблицы
nat arp del[ete] {{<номер>|<имя>}|<IP_адрес>| <MAC_адрес>}	cfg или pf	Удаление записи из ARP таблицы
nat arp sh[ow] [<критерии_отбора>]	read	Просмотр записей ARP таблицы
nat aut[hentication] dis[able]	cfg или pf	Отключение режима аутентификации сетевых пользователей
nat aut[hentication] en[able]	cfg или pf	Включение режима аутентификации сетевых пользователей
nat aut[hentication] timeo[ut] <тайм_аут>	cfg или pf	Установка тайм-аута неактивности для сетевых пользователей
nat dis[able]	cfg или pf	Отключение режима NAT
nat en[able]	cfg или pf	Включение режима NAT
nat key add <IP_адрес>	user	Добавление новой пары ключей аутентификации сетевых пользователей
nat key del[ete] <IP_адрес>	user	Удаление существующей пары ключей аутентификации сетевых пользователей
nat key sh[ow] [<IP_адрес>]	read	Просмотр существующих пар ключей аутентификации сетевых пользователей
nat key upd[ate] <IP_адрес>	user	Изменение существующей пары ключей

Команда	Требуемые привилегии	Описание
		аутентификации сетевых пользователей
nat log dis[able]	cfg или pf	Отключение регистрации пакетов, удаляемых NAT
nat log en[able]	cfg или pf	Включение регистрации пакетов, удаляемых NAT
nat port <порт_мин>-<порт_макс>	cfg или pf	Установка диапазона портов NAT
nat priva[te] del[ete]	cfg или pf	Удаление параметров внутреннего интерфейса NAT
nat priva[te] ip <IP_адрес/маска>	cfg или pf	Установка IP-адреса внутреннего интерфейса NAT
nat priva[te] mac <MAC_адрес>	cfg или pf	Установка MAC-адреса внутреннего интерфейса NAT
nat pub[lic] del[ete]	cfg или pf	Удаление параметров внешнего интерфейса NAT
nat pub[lic] gate[way] <IP_адрес>	cfg или pf	Установка шлюза по умолчанию для внешнего интерфейса NAT
nat pub[lic] ip <IP_адрес/маска>	cfg или pf	Установка IP-адреса внешнего интерфейса NAT
nat pub[lic] mac <MAC_адрес>	cfg или pf	Установка MAC-адреса внешнего интерфейса NAT
nat red[irect] add <протокол> <внеш_порт> <IP_адрес> <внутр_порт>	cfg или pf	Добавление записи в таблицу переадресации NAT
nat red[irect] cl[ear]	cfg или pf	Очистка таблицы переадресации NAT
nat red[irect] del[ete] <внеш_порт>	cfg или pf	Удаление записи из таблицы переадресации NAT
nat red[irect] dmz dis[able]	cfg или pf	Отключение переадресации с интерфейсов DMZ
nat red[irect] dmz en[able]	cfg или pf	Включение переадресации с интерфейсов DMZ
nat red[irect] pub[lic] dis[able]	cfg или pf	Отключение переадресации с внешнего интерфейса
nat red[irect] pub[lic] en[able]	cfg или pf	Включение переадресации с внешнего интерфейса
nat red[irect] sh[ow]	read	Просмотр записей таблицы переадресации NAT
nat sh[ow]	read	Просмотр параметров NAT
nat us[er] add <имя> <MAC_адрес> <IP_адрес> <интерфейсы> <комментарий>	user	Добавление нового сетевого пользователя
nat us[er] cl[ear] [<имя>]	user	Сброс активного сетевого пользователя
nat us[er] del[ete] <имя>	user	Удаление сетевого пользователя
nat us[er] dis[able] <имя>	user	Отключение сетевого пользователя
nat us[er] en[able] <имя>	user	Включение сетевого пользователя
nat us[er] ed[it] <имя> <MAC_адрес> <IP_адрес> <интерфейсы> <комментарий>	user	Изменение параметров сетевого пользователя
nat us[er] lis[t]	read	Просмотр списка существующих сетевых пользователей
nat us[er] pass[word] <имя>	user	Изменение пароля сетевого пользователя
nat us[er] sh[ow]	read	Просмотр списка активных сетевых пользователей
rese[rv] conf[ig] sync[hronize]	cfg или ha	Немедленная синхронизация текущей конфигурации ССПТ-2 в режиме высокой

Команда	Требуемые привилегии	Описание
		готовности
rese[rv] def[ault]	cfg или ha	Установка параметров режима высокой готовности в значения по умолчанию
rese[rv] dis[able]	cfg или ha	Отключение режима высокой готовности
rese[rv] en[able]	cfg или ha	Включение режима высокой готовности
reserv interface {act[ive]|bl[ocked]} {media {10|100|1000}|duplex {half|full}}	cfg или ha	Настройка режимов работы фильтрующих интерфейсов для режима высокой готовности
rese[rv] mod[e] {bal[ance]|mas[ter]|sla[ve]|stp}	cfg или ha	Установка статуса ССПТ-2 для режима высокой готовности
rese[rv] ne[ighbour] <IP_адрес>	cfg или ha	Установка IP-адреса смежного ССПТ-2 для режима высокой готовности
rese[rv] rul[e] sync[hronize]	cfg или ha	Немедленная синхронизация правил фильтрации в режиме высокой готовности
rese[rv] sh[ow]	read	Просмотр параметров режима высокой готовности
rul[e] add <определение_правила>	rules	Добавление правила фильтрации в текущий набор
rul[e] copy <тип_правила> <старый_номер> <новый_номер>	rules	Копирование правила фильтрации в текущем наборе
rule def[ault]	rules	Установка текущего набора правил в состояние по умолчанию
rul[e] del[ete] <идентификатор_правила>	rules	Удаление правила фильтрации из текущего набора
rul[e] ed[it] <определение_правила>	rules	Изменение существующего правила фильтрации в текущем наборе
rul[e] lis[t]	read	Просмотр списка дополнительных наборов правил
rul[e] lo[ad] <имя_набора_правил>	rules	Загрузка дополнительного набора правил
rul[e] mov[e] <тип> <сущ_номер> <новый_номер>	rules	Перенос правила фильтрации в текущем наборе
rul[e] rem[ove] <имя_набора_правил>	rules	Удаление дополнительного набора правил
rul[e] roll[back]	rules	Возврат к предыдущему состоянию текущего набора правил
rul[e] sav[e] <имя_набора_правил>	rules	Сохранение текущего набора правил в дополнительном
rul[e] sh[ow] [<имя_набора_правил>]	read	Просмотр списка правил фильтрации текущего или дополнительного наборов правил
rul[e] stats cl[ear]	pf	Сброс статистики трафика по текущему набору правил
rul[e] stats sh[ow] [<критерии_отбора>]	read	Просмотр статистики трафика по текущему набору правил
ses[sion] ap dis[able]	cfg или pf	Отключение использования AP-правил фильтрации
ses[sion] ap en[able]	cfg или pf	Включение использования AP-правил фильтрации
ses[sion] deept[cp] dis[able]	cfg или pf	Отключение глубокого контроля TCP
ses[sion] deept[cp] en[able]	cfg или pf	Включение глубокого контроля TCP
ses[sion] dis[able]	cfg или pf	Отключение управления сессиями

Команда	Требуемые привилегии	Описание
ses[sion] en[able]	cfg или pf	Включение управления сессиями
ses[sion] fl[ood] ala[rm] dis[able]	cfg или pf	Отключение сигнализации обнаружения flood-атак
ses[sion] fl[ood] ala[rm] en[able]	cfg или pf	Включение сигнализации обнаружения flood-атак
ses[sion] fl[ood] dis[able]	cfg или pf	Отключение режима блокировки flood-атак
ses[sion] fl[ood] en[able]	cfg или pf	Включение режима блокировки flood-атак
ses[sion] fl[ood] rul[e] com[ments] <комметарий>	cfg или pf	Изменение комментария для временного IP-правила, блокирующего flood-атаку
ses[sion] fl[ood] rul[e] lif[etime] <время>	cfg или pf	Настройка времени жизни временного IP-правила, блокирующего flood-атаку
ses[sion] fl[ood] rul[e] log dis[able]	cfg или pf	Отключение регистрации пакетов во временном IP-правиле, блокирующем flood-атаку
ses[sion] fl[ood] rul[e] log en[able]	cfg или pf	Включение регистрации пакетов во временном IP-правиле, блокирующем flood-атаку
ses[sion] fl[ood] thr[eshold] def[ault]	cfg или pf	Установка порогов обнаружения flood-атак в значения по умолчанию
ses[sion] fl[ood] thr[eshold] icmp <порог>	cfg или pf	Установка порога обнаружения flood-атак для протокола ICMP
ses[sion] fl[ood] thr[eshold] tcp <порог>	cfg или pf	Установка порога обнаружения flood-атак для протокола TCP
ses[sion] fl[ood] thr[eshold] udp <порог>	cfg или pf	Установка порога обнаружения flood-атак для протокола UDP
ses[sion] ip dis[able]	cfg или pf	Отключение создания сессий по умолчанию для IP-правил фильтрации
ses[sion] ip en[able]	cfg или pf	Включение создания сессий по умолчанию для IP-правил фильтрации
ses[sion] log dis[able]	cfg или pf	Отключение регистрации пакетов, отброшенных сессиями
ses[sion] log en[able]	cfg или pf	Включение регистрации пакетов, отброшенных сессиями
ses[sion] mac dis[able]	cfg или pf	Отключение использования данных канального уровня в управлении сессиями
ses[sion] mac en[able]	cfg или pf	Включение использования данных канального уровня в управлении сессиями
ses[sion] sh[ow]	read	Просмотр параметров управления сессиями
ses[sion] tab[le] cl[ear]	pf	Очистка таблицы сессий
ses[sion] tab[le] del[ete] <номер_сессии>	pf	Удаление сессии из таблицы сессий
ses[sion] tab[le] sh[ow]	read	Просмотр таблицы сессий
ses[sion] tab[le] siz[e] <размер_таблицы>	cfg или pf	Изменение размера таблицы сессий
ses[sion] timeo[ut] def[ault]	cfg или pf	Установка тайм-аутов неактивности сессий в значения по умолчанию
ses[sion] timeo[ut] icmp {est[ablished]|syn} <тайм_аут>	cfg или pf	Установка тайм-аута неактивности для ICMP сессий
ses[sion] timeo[ut] tcp {est[ablished]|fin|syn}	cfg или pf	Установка тайм-аута неактивности для TCP сессий
ses[sion] timeo[ut] udp {est[ablished]|syn}	cfg или pf	Установка тайм-аута неактивности для UDP сессий
syst[em] fnpsh his[tory] cl[ear]	read	Очистка буфера истории команд

Команда	*Требуемые привилегии*	*Описание*
syst[em] fnpsh his[tory] sh[ow]	read	Просмотр содержимого буфера истории команд
syst[em] fnpsh pass[word]	user	Изменение пароля системного пользователя
syst[em] fnpsh timeo[ut] <тайм_аут>	cfg или sys	Установка тайм-аута неактивности для командного интерфейса ССПТ-2
syst[em] fnpsh v[iewer] {intern[al]|mor[e]|no}	read	Установка режима просмотра данных в командном интерфейсе ССПТ-2
syst[em] halt	sys	Выключение ССПТ-2
syst[em] ich[eck]	read	Проверка целостности программного обеспечения ССПТ-2
syst[em] key sh[ow]	read	Просмотр сертификатов и ключей ССПТ-2
syst[em] pass[word]	user	Изменение пароля системного пользователя
syst[em] reboot	sys	Перезагрузка ССПТ-2
syst[em] sh[ow]	read	Вывод информации о программном и аппаратном обеспечении ССПТ-2
syst[em] statu[s]	read	Вывод информации о состоянии ресурсов операционной системы ССПТ-2
syst[em] time ntp del[ete]	cfg	Удаление параметров синхронизации времени по NTP
syst[em] time ntp dis[able]	cfg	Отключение синхронизации времени по NTP
syst[em] time ntp en[able]	cfg	Включение синхронизации времени по NTP
syst[em] time ntp log dis[able]	cfg	Отключение регистрации NTP запросов
syst[em] time ntp log en[able]	cfg	Включение регистрации NTP запросов
syst[em] time ntp serv[er] <IP_адрес>	cfg	Установка IP-адреса NTP сервера
syst[em] time ntp timeo[ut] <тайм_аут>	cfg	Установка тайм-аута опроса NTP сервера
syst[em] time ntp upd[ate]	cfg	Немедленная синхронизация времени с NTP сервером
syst[em] time set {<ГГГГ/ММ/ДД [ЧЧ:ММ:СС]>|<ЧЧ:ММ:СС>}	sys	Установка системного времени
syst[em] time sh[ow]	read	Вывод системного времени и параметров синхронизации по NTP
syst[em] time zone [<файл_часового_пояса>]	sys	Установка часового пояса
syst[em] w[eb] dis[able]	sys (консоль)	Отключение WEB-интерфейса ССПТ-2
syst[em] w[eb] en[able]	sys (консоль)	Включение WEB-интерфейса ССПТ-2
us[er] add <имя_пользователя> <привилегии>	user	Добавление нового пользователя
us[er] del[ete] <имя_пользователя>	user	Удаление пользователя
us[er] dis[able] <имя_пользователя>	user	Отключение пользователя
us[er] en[able] <имя_пользователя>	user	Включение пользователя
us[er] lis[t]	read	Просмотр списка существующих пользователей
us[er] pass[word] <имя_пользователя>	user	Изменение пароля пользователя
us[er] privi[lege] <имя_пользователя> <привилегии>	user	Изменение привилегий пользователя
us[er] rad[ius] dis[able]	user	Отключение RADIUS авторизации
us[er] rad[ius] en[able]	user	Включение RADIUS авторизации
us[er] rad[ius] ret[ry] <число_попыток>	user	Установка максимального количества попыток обращения к RADIUS серверу
us[er] rad[ius] serv[er] <тип> <IP_адрес>	user	Настройка параметров RADIUS авторизации

Команда	Требуемые привилегии	Описание
<ключ> <порт>		
us[er] rad[ius] sh[ow]	read	Просмотр параметров RADIUS авторизации
us[er] rad[ius] timeout <тайм_аут>	user	Установка тайм-аута ожидания ответа от RADIUS сервера
us[er] sh[ow]	read	Просмотр списка активных пользователей

3.4.1. config default – инициализация текущей конфигурации ССПТ-2 значениями по умолчанию

`conf[ig] def[ault]`

Требуемые привилегии – **cfg**

Команда выполняет инициализацию текущей конфигурации ССПТ-2 значениями по умолчанию.

Не рекомендуется выполнять команду `config default` во время управления ССПТ-2 по сети Ethernet, поскольку отключение управляющего Ethernet-интерфейса ССПТ-2 приведет к потере соединения между управляющим компьютером и ССПТ-2.

Пример:

```
fnpsh> config default
Загрузить конфигурацию по умолчанию? (Y/N)  [N]: Y
FNPSH-I-3052-Конфигурация по умолчанию загружена
fnpsh>
```

Параметрам конфигурации ССПТ-2 значения по умолчанию присваиваются во время первого запуска. Значения по умолчанию параметров конфигурации соответствуют выводу команды `config show` (приложение 3.4.6, стр. 62), приведенному ниже:

```
fnpsh> config show
Текущая активная конфигурация:

interface control address 10.234.28.71/255.255.0.0
gateway delete
interface control media auto
interface control acl clear
interface filter eth0 enable
interface filter eth0 media auto
interface filter eth1 enable
interface filter eth1 media auto
interface filter eth2 enable
interface filter eth2 media auto
interface filter eth0 mirror disable
session enable
session ip enable
session ap disable
session log disable
session mac enable
session deeptcp enable
session timeout tcp syn 5
session timeout tcp estab 3600
session timeout tcp fin 180
session timeout udp syn 5
session timeout udp estab 10
session timeout icmp syn 5
session timeout icmp estab 20
session table size 8192
session flood disable
session flood alarm disable
session flood threshold tcp 1000
session flood threshold udp 500
session flood threshold icmp 300
session flood rule lifetime 60
session flood rule log disable
session flood rule comments "Blocked flood attack"
system time ntp log disable
```

```
system time ntp timeout 3600
system time ntp delete
system fnpsh timeout 600
system snmp disable
system web disable
log packet disable
log export ftp clear
log export ftp disable
log export syslog disable
nat disable
nat log disable
nat authentication disable
nat authentication timeout 600
nat port 45000-60000
nat public mac 02:01:01:01:01:01
nat public delete
nat private mac 02:01:01:01:01:02
nat private delete
nat arp clear
nat redirect public disable
nat redirect dmz disable
nat redirect clear
reserv disable
reserv interface active media 100
reserv interface active duplex full
reserv interface blocked media 10
reserv interface blocked duplex half
user radius timeout 5
user radius retry 3
user radius disable
```

3.4.2. config list – просмотр списка дополнительных конфигураций

`conf[ig] lis[t]`

Команда выводит на экран терминала список существующих дополнительных конфигураций. Для каждой дополнительной конфигурации выводится ее имя и время создания.

Пример:

```
fnpsh> config list
Дополнительные конфигурации:
    Имя          Время создания
    fnp2_ag      08.07.2013 20:41:01 (MSK)
Всего: 1         Свободно: 15
fnpsh>
```

3.4.3. config load – загрузка дополнительной конфигурации

`conf[ig] lo[ad] <имя_конфигурации>`

Требуемые привилегии – **cfg** и **pf**.

Параметры:

- `<имя_конфигурации>` – имя предварительно сохраненной дополнительной конфигурации.

Команда загружает конфигурационные параметры ССПТ-2, содержащиеся в дополнительной конфигурации с указанным именем, в текущую конфигурацию.

Предыдущие значения параметров текущей конфигурации будут потеряны.

Не следует загружать, используя WEB-интерфейс администратора, дополнительные конфигурации с отключенным параметром использования WEB-интерфейса. После загрузки такой дополнительной конфигурации, WEB-интерфейс администратора автоматически отключится и станет недоступен для использования.

При загрузке дополнительной конфигурации изменения некоторых конфигурационных параметров, касающихся работы пакетного фильтра ССПТ-2, не вступят в силу до тех пор, пока **пакетный фильтр не будет перезапущен**. К таким параметрам относятся:

- настройки подсистемы управления сессиями;

- настройки подсистемы трансляции сетевых адресов NAT;

Перезапуск пакетного фильтра можно выполнить отдельно, используя команду `filter restart`.

Пример:

```
fnpsh> config load fnp2_ag
Загрузить дополнительную конфигурацию? (Y/N)  [N]: Y
Перезапустить пакетный фильтр? (Y/N)  [N]: Y
FNPSH-I-3062-Пакетный фильтр перезапущен
FNPSH-I-3051-Дополнительная конфигурация загружена
fnpsh>
```

3.4.4. config remove – удаление дополнительной конфигурации

`conf[ig] rem[ove] <имя_конфигурации>`

Требуемые привилегии – **cfg**.

Параметры:

- `<имя_конфигурации>` – имя предварительно сохраненной дополнительной конфигурации.

Команда удаляет дополнительную конфигурацию с указанным именем.

Пример:

```
fnpsh> config remove fnp2_ag
Удалить дополнительную конфигурацию? (Y/N)  [N]: Y
FNPSH-I-3050-Дополнительная конфигурация удалена (fnp2_ag)
fnpsh>
```

3.4.5. config save – сохранение текущей конфигурации в дополнительной

`conf[ig] sav[e] <имя_конфигурации>`

Требуемые привилегии – **cfg**.

Параметры:

- `<имя_конфигурации>` – имя дополнительной конфигурации

Команда выполняет сохранение текущей конфигурации ССПТ-2 в дополнительной с указанным именем. Если дополнительная конфигурация с указанным именем уже существует, команда выполнена не будет.

Для перезаписи уже существующей дополнительной конфигурации ее необходимо предварительно удалить, используя команду `config remove` (приложение 3.4.4, стр. 61).

В дополнительной конфигурации не сохраняются настройки часового пояса.

В ССПТ-2 существуют следующие ограничения при работе с дополнительными конфигурациями:

- ССПТ-2 может хранить не более **16** дополнительных конфигураций;
- имя дополнительной конфигурации должно отвечать следующим требованиям:
  - ✔ длина имени – от **1** до **128** символов;
  - ✔ допустимые символы в имени – **латинские буквы** (a-z, A-Z), **цифры** (0-9), и символы '_' (подчеркивание), '**-**' (дефис). Имя дополнительного набора должно начинаться с буквы либо с цифры;
- имя дополнительной конфигурации является регистрово-зависимым.

Примеры:

```
fnpsh> config save fnp2_ag
FNPSH-I-304F-Дополнительная конфигурация сохранена
fnpsh>

fnpsh> config save fnp2_ag
FNPSH-E-10A5-Дополнительная конфигурация уже существует

fnpsh> config save fnp2_AG
FNPSH-I-304F-Дополнительная конфигурация сохранена
fnpsh>
```

3.4.6. config show – просмотр параметров текущей или дополнительной конфигурации

`config show [<имя_конфигурации>] [viewer={intern[al]|mor[e]|no}]`

Параметры:

- `<имя_конфигурации>` – имя дополнительной конфигурации;
- `viewer` — режим просмотра данных командного интерфейса ССПТ-2:
  - ✔ `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.

По умолчанию используется режим просмотра данных, установленный по команде `system fnpsh viewer` (раздел 3.4.156, стр. 168)

Просмотреть текущий установленный режим просмотра данных можно по команде `system show` (раздел 3.4.162, стр. 173).

Команда выводит на экран терминала параметры текущей или дополнительной конфигурации ССПТ-2. Имя дополнительной конфигурации указывается через параметр `<имя_конфигурации>`.

Если имя дополнительной конфигурации не указано, на экран терминала выводятся параметры текущей конфигурации ССПТ-2.

Параметры конфигурации выводятся в формате соответствующих команд командного интерфейса ССПТ-2.

Просмотр параметров конфигурации выполняется в соответствии с текущим режимом просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23).

Пример:

```
fnpsh>config show fnp2_ag viewer=no
Дополнительная конфигурация fnp2_ag:

interface control address 10.98.7.1/255.255.255.0
gateway set 10.98.7.254
interface control media auto
interface control acl clear
interface filter eth0 enable
interface filter eth0 media auto
interface filter eth1 enable
interface filter eth1 media auto
interface filter eth2 enable
interface filter eth2 media auto
interface filter eth0 mirror disable
session enable
session ip enable
session ap disable
session log disable
session mac enable
session deeptcp enable
session timeout tcp syn 5
session timeout tcp estab 3600
```

```
session timeout tcp fin 180
session timeout udp syn 5
session timeout udp estab 10
session timeout icmp syn 5
session timeout icmp estab 20
session table size 8192
session flood disable
session flood alarm disable
session flood threshold tcp 1000
session flood threshold udp 500
session flood threshold icmp 300
session flood rule lifetime 60
session flood rule log disable
session flood rule comments "Blocked flood attack"
system time ntp log disable
system time ntp timeout 3600
system time ntp delete
system fnpsh timeout 600
system snmp enable
system web enable
log packet disable
log export ftp clear
log export ftp disable
log export syslog disable
nat disable
nat log disable
nat authentication disable
nat authentication timeout 600
nat port 45000-60000
nat public mac 02:01:01:01:01:01
nat public delete
nat private mac 02:01:01:01:01:02
nat private delete
nat arp clear
nat redirect public disable
nat redirect dmz disable
nat redirect clear
reserv disable
reserv interface active media 100
reserv interface active duplex full
reserv interface blocked media 10
reserv interface blocked duplex half
user radius timeout 5
user radius retry 3
user radius disable
fnpsh>
```

3.4.7. exit – завершение сеанса работы пользователя

`exit`

Команда завершает сеанс работы пользователя с командным интерфейсом ССПТ-2.

Пример:

```
fnpsh> exit
FNPSH-I-3003-Завершение работы пользователя (admin)
```

3.4.8. filter restart – перезапуск пакетного фильтра

`fil[ter] rest[art]`

Требуемые привилегии – **pf**.

Команда выполняет перезапуск пакетного фильтра ССПТ-2.

При перезапуске пакетного фильтра обнуляется статистика трафика по правилам фильтрации текущего набора и очищается таблица сессий.

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

Пример:

```
fnpsh> filter restart
```

```
Перезапустить пакетный фильтр? (Y/N)  [N]: Y
FNPSH-I-3062-Пакетный фильтр перезапущен
fnpsh>
```

3.4.9. filter start – запуск пакетного фильтра

`fil[ter] start`

Требуемые привилегии – **pf**.

Команда выполняет запуск пакетного фильтра ССПТ-2.

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

Примеры:

```
fnpsh> filter start
FNPSH-I-3048-Пакетный фильтр запущен
fnpsh>

fnpsh> filter start
FNPSH-W-2007-Пакетный фильтр уже работает
fnpsh>
```

3.4.10. filter status – вывод информации о состоянии пакетного фильтра

`fil[ter] statu[s]`

Команда выводит на экран терминала информацию о состоянии пакетного фильтра и о статистике трафика по фильтрующим интерфейсам. Информация выводится только в том случае, если пакетный фильтр находится в активном состоянии (запущен). В противном случае командный интерфейс ССПТ-2 выведет на экран терминала предупреждающее сообщение:

```
fnpsh> filter status
FNPSH-W-2005-Пакетный фильтр не работает
```

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 подсистем управления сессиями или трансляции сетевых адресов.

Имеется возможность просмотра как суммарной статистики трафика, 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, ICMP, UDP, TCP, IPX.

В процессе выполнения команды информация о состоянии пакетного фильтра и статистике трафика обновляется периодически каждые **5** секунд.

Для просмотра статистики трафика используются клавиши и управляющие последовательности, перечисленные в таблице 3.2.

Таблица 3.2: 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 (IPX трафик)
<R>	Немедленное обновление информации о состоянии пакетного фильтра статистики трафика
<H>	Вывод подсказки по клавишам управления просмотром статистики (рисунок 3.45)
<F10>, <Q>	Завершение выполнения команды

Пример вывода информации о состоянии пакетного фильтра и статистике трафика приводится на рисунке 3.45.

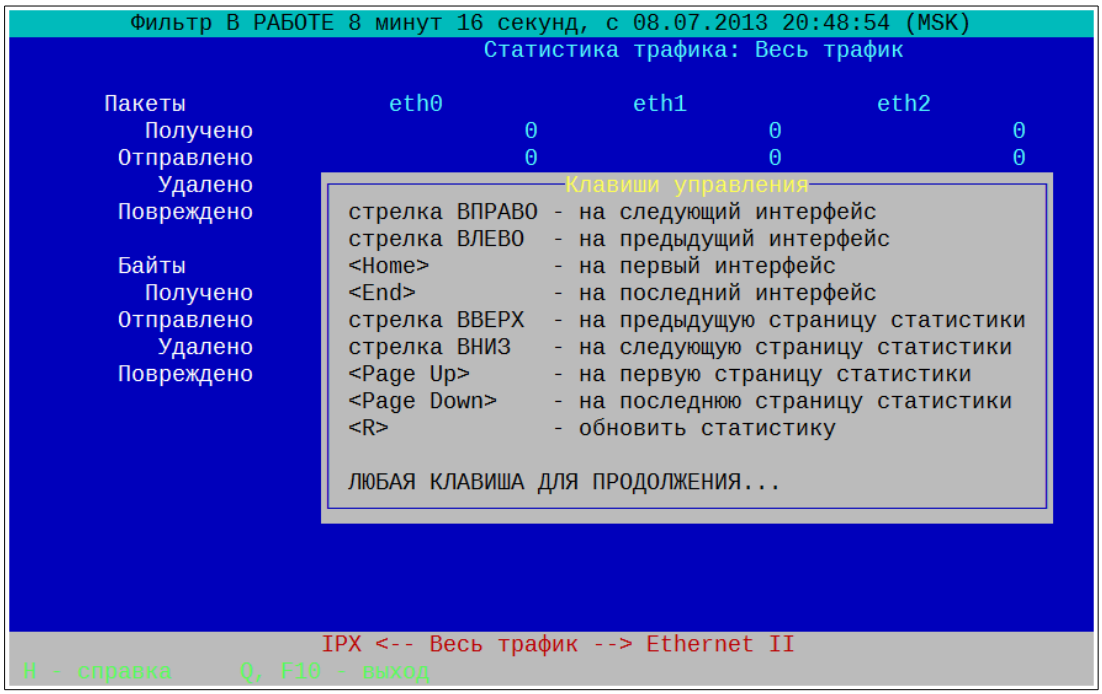

Рисунок 3.45: Состояние пакетного фильтра и статистика трафика

В нижних строках экрана терминала выводится подсказка:

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

3.4.11. filter stop – останов пакетного фильтра

```
fil[ter] stop
```

Требуемые привилегии – **pf**.

Команда выполняет останов пакетного фильтра ССПТ-2.

Останов пакетного фильтра влечет за собой прекращение передачи пакетов через фильтрующие интерфейсы ССПТ-2.

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

Примеры:

```
fnpsh> filter stop
Остановить пакетный фильтр? (Y/N)  [N]: Y
FNPSH-I-303A-Пакетный фильтр остановлен

fnpsh> filter stop
Остановить пакетный фильтр? (Y/N)  [N]: Y
FNPSH-W-2005-Пакетный фильтр не работает
fnpsh>
```

3.4.12. gateway delete – удаление маршрута по умолчанию

`gate[way] del[ete]`

Требуемые привилегии – **cfg**.

Команда удаляет запись о маршруте по умолчанию из маршрутной таблицы и удаляет информацию об IP-адресе шлюза по умолчанию из текущей конфигурации ССПТ-2.

После удаления маршрута по умолчанию доступ к управлению ССПТ-2 по сети Ethernet возможен только с компьютеров, у которых IP-адреса сетевых интерфейсов состоят в той же подсети, что и IP-адрес управляющего Ethernet-интерфейса ССПТ-2.

Пример:

```
fnpsh> gateway delete
Удалить маршрут по умолчанию? (Y/N)  [N]: Y
FNPSH-I-302C-Маршрут по умолчанию удален
fnpsh>
```

3.4.13. gateway disable – отключение маршрута по умолчанию

`gate[way] dis[able]`

Требуемые привилегии – **cfg**.

Команда удаляет запись о маршруте по умолчанию из маршрутной таблицы и изменяет информацию о состоянии маршрута по умолчанию в текущей конфигурации ССПТ-2.

Команда `gateway disable` не изменяет информацию об IP-адресе шлюза по умолчанию в текущей конфигурации ССПТ-2.

После отключения маршрута по умолчанию доступ к управлению ССПТ-2 по сети Ethernet возможен только с компьютеров, у которых IP-адреса сетевых интерфейсов состоят в той же подсети, что и IP-адрес управляющего Ethernet-интерфейса ССПТ-2.

Если на момент выполнения команды `gateway disable` маршрут по умолчанию уже был отключен, то его состояние останется без изменений.

Пример:

```
npsh> gateway disable
Выключить маршрут по умолчанию? (Y/N)  [N]: Y
FNPSH-I-3033-Маршрут по умолчанию отключен
fnpsh>
```

3.4.14. gateway enable – включение маршрута по умолчанию

`gate[way] en[able]`

Требуемые привилегии – **cfg**.

Команда добавляет маршрут по умолчанию в маршрутную таблицу в соответствии с информацией об IP-адресе шлюза, содержащейся в текущей конфигурации ССПТ-2.

IP-адрес шлюза по умолчанию должен быть предварительно установлен, используя команду `gateway set`.

Если на момент выполнения команды `gateway enable` маршрут по умолчанию уже был включен, то его состояние останется без изменений.

Пример:

```
fnpsh> gateway enable
FNPSH-I-3032-Маршрут по умолчанию включен
fnpsh>

fnpsh> gateway enable
FNPSH-E-1096-Маршрут по умолчанию уже существует (10.234.28.1)
fnpsh>
```

3.4.15. gateway set – установка IP-адреса шлюза по умолчанию

`gate[way] set <IP_адрес>`

Требуемые привилегии – **cfg**.

Параметры:

- `<IP_адрес>` – IP-адрес шлюза по умолчанию.

Команда устанавливает IP-адрес шлюза по умолчанию в текущей конфигурации ССПТ-2 и добавляет маршрут по умолчанию в маршрутную таблицу.

IP-адреса шлюза по умолчанию и управляющего Ethernet-интерфейса ССПТ-2 должны принадлежать одной и той же IP-подсети.

Если на момент выполнения команды `gateway set` IP-адрес шлюза по умолчанию уже был установлен, то его состояние останется без изменений.

Примеры:

```
fnpsh> gateway set 10.234.28.1
FNPSH-I-302B-Маршрут по умолчанию добавлен
fnpsh>

fnpsh> gateway set 10.234.28.1
FNPSH-E-1096-Маршрут по умолчанию уже существует (10.234.28.1)
fnpsh>
```

3.4.16. gateway show – вывод настроек и состояния маршрута по умолчанию

`gate[way] sh[ow]`

Команда выводит на экран терминала текущие настройки IP-адреса шлюза и состояние маршрута по умолчанию.

IP-адрес шлюза по умолчанию определяется по двум источникам:

- `Конфигурация` – настройка IP-адреса шлюза в текущей конфигурации ССПТ-2;
- `Определено` – IP-адрес шлюза по умолчанию, полученный из маршрутной таблицы.

Пример:

```
fnpsh> gateway show
Маршрут:                по умолчанию
        Состояние:      включено
        Конфигурация:   10.98.7.254
        Определено:     10.98.7.254
```

```
fnpsh>
```

3.4.17. help – вывод краткой справки по всем категориям команд ССПТ-2

`help`

Команда выводит на экран терминала перечень всех категорий команд ССПТ-2 и краткую справку по использованию системы контекстной помощи по командам командного интерфейса ССПТ-2.

Использование контекстной помощи в командном интерфейсе ССПТ-2 описывается в разделе 2.6.4, стр. 22.

Пример:

```
fnpsh> help
  config:    управление конфигурациями устройства
  filter:    управление пакетным фильтром
  gateway:   настройка шлюза по умолчанию
  interface: настройка сетевых интерфейсов
  log:       управление подсистемой регистрации
  nat:       настройка механизма трансляции сетевых адресов (NAT)
  rule:      управление правилами фильтрации
  reserv:    управление подсистемой высокой готовности
  session:   управление механизмом контроля сессий
  system:    контроль параметров операционной системы
  user:      управление пользователями ССПТ-2
  exit <cr>: выход из командного интерфейса
  help <cr>: справка по командам

    Просмотр контекстной справки по командам:
  <команда> [<опции>] ? <cr>
    или
  <команда> [<опции>] help <cr>
    где <cr> - перевод строки
fnpsh>
```

3.4.18. interface control acl add – добавление элемента в список доступа

`interf[ace] cont[rol] acl add <элемент_списка>`

Требуемые привилегии – **cfg**.

Параметры:

- `<элемент_списка>` – определение элемента, который будет добавлен в список доступа. Формат определения элемента списка доступа может быть одним из следующих:
  - ✔ `<IP_адрес>` – одиночный IP-адрес;
  - ✔ `<IP_адрес/маска>` – IP-подсеть;
  - ✔ `<IP_адрес_1>-<IP_адрес_2>` – диапазон IP-адресов от `<IP_адрес_1>` до `<IP_адрес_2>` включительно.

Команда добавляет новый элемент в список доступа текущей конфигурации ССПТ-2.

Список доступа используется для ограничения доступа к управлению ССПТ-2 по IP-адресам управляющих компьютеров.

Если список доступа пустой, доступ к управлению ССПТ-2 разрешается с любого IP-адреса.

Список доступа может содержать не более **16** элементов.

Если список доступа не пустой, доступ к управлению ССПТ-2 разрешается только с IP-адресов, удовлетворяющих какому-либо из элементов списка.

Примеры:

```
fnpsh> interface control acl add 10.98.7.254
FNPSH-I-302F-Новая запись добавлена в список доступа
```

```
fnpsh>

fnpsh> interface control acl add 10.98.7.0/255.255.255.0
FNPSH-I-302F-Новая запись добавлена в список доступа
fnpsh>

fnpsh> interface control acl add 10.98.1.1-10.98.1.4
FNPSH-I-302F-Новая запись добавлена в список доступа
fnpsh>
```

3.4.19. interface control acl clear – очистка списка доступа

`interf[ace] cont[rol] acl cl[ear]`

Требуемые привилегии – **cfg**.

Команда очищает список доступа текущей конфигурации ССПТ-2.

После выполнения команды `interface control acl clear` доступ к управлению ССПТ-2 будет разрешен с любого IP-адреса.

Пример:

```
fnpsh> interface control acl clear
Очистить список доступа? (Y/N)  [N]: Y
FNPSH-I-3031-Список доступа очищен
fnpsh>
```

3.4.20. interface control acl delete – удаление элемента из списка доступа

`interf[ace] cont[rol] acl del[ete] <номер_элемента>`

Требуемые привилегии – **cfg**.

Параметры:

- `<номер_элемента>` – номер удаляемого элемента списка доступа.

Команда удаляет существующий элемент из списка доступа.

Удаление элемента из списка доступа выполняется по его номеру. Просмотреть номера элементов списка доступа можно, выполнив команду `interface control acl show` (приложение 3.4.21, стр. 69).

Пример:

```
fnpsh> interface control acl show

Список доступа:
 1  10.98.7.254
 2  10.98.7.0/255.255.255.0
 3  10.98.1.1-10.98.1.4
Всего записей:  3   Свободных позиций: 13
fnpsh>

fnpsh>interface control acl delete 3
Удалить запись из списка доступа 3 - 10.98.1.1-10.98.1.4? (Y/N) [N]: y
FNPSH-I-3030-Запись удалена из списка доступа
fnpsh>
```

3.4.21. interface control acl show – просмотр элементов списка доступа

`interf[ace] cont[rol] acl sh[ow]`

Команда выводит на экран терминала содержимое элементов списка доступа. Для каждого существующего элемента выводятся его номер и определение.

Пример:

```
fnpsh> interface control acl show
Список доступа:
 1  10.98.7.254
 2  10.98.7.0/255.255.255.0
 3  10.98.1.1-10.98.1.4
Всего записей:  3   Свободных позиций: 13
fnpsh>
```

3.4.22. interface control address – назначение IP-адреса управляющему интерфейсу

`interf[ace] cont[rol] addr[ess] <IP_адрес/маска>`

Требуемые привилегии – **cfg**.

Параметры:

- `<IP_адрес/маска>` – IP-адрес и маска подсети, которые будут назначены управляющему Ethernet-интерфейсу ССПТ-2.

Команда назначает IP-адрес и маску подсети управляющему Ethernet-интерфейсу ССПТ-2 и сохраняет эти настройки в текущей конфигурации ССПТ-2.

По умолчанию управляющему Ethernet-интерфейсу назначен IP-адрес **10.234.28.71** с сетевой маской **255.255.0.0**.

Рекомендации по выбору IP-адресов для управляющего Ethernet-интерфейса ССПТ-2 приведены в приложении 3.3, стр. 51.

Если до выполнения команды `interface control address` управляющему Ethernet-интерфейсу ССПТ-2 уже был назначен IP-адрес, то он будет заменен новым значением.

При назначении IP-адреса управляющему Ethernet-интерфейсу стираются настройки шлюза по умолчанию из текущей конфигурации ССПТ-2 и удаляется маршрут по умолчанию из маршрутной таблицы.

Примеры:

```
fnpsh> interface control address 10.98.7.1/255.255.255.0
FNPSH-I-3024-IP-адрес управляющего интерфейса изменен
fnpsh> gateway set 10.98.7.254
FNPSH-I-302B-Маршрут по умолчанию добавлен
fnpsh> gateway show
Маршрут:                по умолчанию
        Состояние:      включено
        Конфигурация:   10.98.7.254
        Определено:     10.98.7.254
fnpsh>

fnpsh> interface control address 192.168.160.253/255.255.255.252
FNPSH-I-3024-IP-адрес управляющего интерфейса изменен
fnpsh> gateway show
Маршрут:                по умолчанию
        Состояние:      отключено
        Конфигурация:   отсутствует
        Определено:     отсутствует
fnpsh>
```

3.4.23. interface control address delete – удаление IP-адреса управляющего интерфейса

`interf[ace] cont[rol] addr[ess] del[ete]`

Требуемые привилегии – **cfg**.

Команда удаляет назначенный IP-адрес с управляющего Ethernet-интерфейса и стирает настройки IP-адреса в текущей конфигурации ССПТ-2.

После выполнения команды `interface control address delete` доступ к управлению ССПТ-2 по сети Ethernet станет невозможным.

При удалении IP-адреса управляющего Ethernet-интерфейса стираются настройки шлюза по умолчанию из текущей конфигурации ССПТ-2 и удаляется маршрут по умолчанию из маршрутной таблицы.

Пример:

```
fnpsh> interface control address delete
Удалить IP-адрес? (Y/N)  [N]: Y
FNPSH-I-3025-IP-адрес управляющего интерфейса удален
fnpsh> gateway show
Маршрут:                по умолчанию
        Состояние:      отключено
        Конфигурация:   отсутствует
        Определено:     отсутствует
fnpsh>
```

3.4.24. interface control disable – отключение управляющего интерфейса

`interf[ace] cont[rol] dis[able]`

Требуемые привилегии – **cfg**.

Команда отключает управляющий Ethernet-интерфейс и изменяет соответствующие настройки в текущей конфигурации ССПТ-2. Установки IP-адреса управляющего интерфейса в текущей конфигурации остаются без изменения.

После выполнения команды `interface control disable` доступ к управлению ССПТ-2 по сети Ethernet станет невозможным.

Пример:

```
fnpsh> interface control disable
Выключить управляющий интерфейс? (Y/N)  [N]: Y
FNPSH-I-3053-Управляющий интерфейс отключен
fnpsh>
```

3.4.25. interface control duplex – установка режима передачи управляющего интерфейса

`interf[ace] cont[rol] dup[lex] {half|ful[l]}`

Требуемые привилегии – **cfg**.

Параметры:

- режим передачи управляющего Ethernet-интерфейса:
  - ✔ `half` – полудуплексный режим передачи;
  - ✔ `full` – полнодуплексный режим передачи.

Команда устанавливает режим передачи для управляющего Ethernet-интерфейса и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Установка режима передачи возможна только в том случае, когда скорость передачи управляющего Ethernet-интерфейса установлена в значение, отличное от `auto` (приложение 3.4.27, стр. 72).

Примеры:

```
fnpsh> interface control duplex full
FNPSH-E-10B2-Для установки режима передачи скорость передачи должна отличаться от
"autoselect"
fnpsh>
```

```
fnpsh> interface control media 100
Изменить скорость передачи управляющего интерфейса? (Y/N)  [N]: Y
FNPSH-I-3028-Скорость передачи управляющего интерфейса изменена
fnpsh> interface control duplex full
Изменить режим передачи управляющего интерфейса? (Y/N)  [N]: Y
FNPSH-I-3029-Режим передачи фильтрующего интерфейса изменен (full-duplex)
fnpsh>
```

3.4.26. interface control enable – включение управляющего интерфейса

`interf[ace] cont[rol] en[able]`

Требуемые привилегии – **cfg**.

Команда включает управляющий Ethernet-интерфейс и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Выполнение команды `interface control enable` возможно только в том случае, когда управляющему Ethernet-интерфейсу ССПТ-2 уже назначен IP-адрес (приложение 3.4.22, стр. 70).

Пример:

```
fnpsh> interface control enable
FNPSH-I-3054-Управляющий интерфейс включен
fnpsh>
```

3.4.27. interface control media – установка скорости передачи управляющего интерфейса

`interf[ace] cont[rol] med[ia] {auto|10|100|1000}`

Требуемые привилегии – **cfg**.

Параметры:

- скорость передачи управляющего Ethernet-интерфейса:
  - ✔ `auto` – режим автоматического выбора скорости и режима передачи;
  - ✔ `10` – скорость передачи 10 Мбит/с;
  - ✔ `100` – скорость передачи 100 Мбит/с;
  - ✔ `1000` – скорость передачи 1000 Мбит/с.

Команда устанавливает скорость передачи для управляющего Ethernet-интерфейса и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Скорость передачи 1000 Мбит/сек может быть установлена только для ССПТ-2, укомплектованных сетевыми интерфейсами, поддерживающими технологию *Gigabit Ethernet*.

Пример:

```
fnpsh> interface control media 100
Изменить скорость передачи управляющего интерфейса? (Y/N)  [N]: Y
FNPSH-I-3028-Скорость передачи управляющего интерфейса изменена
fnpsh>
```

3.4.28. interface control ping – проверка доступности узлов в управляющей сети

`interf[ace] cont[rol] ping <IP_адрес>`

Параметры:

- `<IP_адрес>` – IP-адрес узла, подключенного к управляющему сегменту Ethernet, доступность которого проверяется.

Команда позволяет проверить доступность узлов по их IP-адресам в управляющей сети Ethernet. Доступность проверяется на основе отправки эхо-запросов и ожидания эхо-ответов по протоколу ICMP по аналогии с утилитой `ping`.

Перед использованием команды `interface control ping` необходимо назначить IP-адрес управляющему Ethernet-интерфейсу и включить его.

Пример:

```
fnpsh> interface control ping 10.98.7.254
PING 10.98.7.254: 56 байт(а) данных
64 байт(а) от 10.98.7.254: icmp_seq=0 ttl=64 rtt=0,091 ms
64 байт(а) от 10.98.7.254: icmp_seq=1 ttl=64 rtt=0,246 ms
64 байт(а) от 10.98.7.254: icmp_seq=2 ttl=64 rtt=0,239 ms
64 байт(а) от 10.98.7.254: icmp_seq=3 ttl=64 rtt=0,250 ms
64 байт(а) от 10.98.7.254: icmp_seq=4 ttl=64 rtt=0,253 ms
Статистика ping 10.98.7.254:
5 пакетов передано, 5 пакетов получено, 0% пакетов потеряно
Задержка мин./сред./макс./отклонение = 0,091/0,216/0,253/0,063 мс
fnpsh>
```

3.4.29. interface control show – просмотр настроек и состояния управляющего интерфейса

`interf[ace] cont[rol] sh[ow]`

Команда выводит на экран терминала настройки и текущее состояние управляющего Ethernet-интерфейса ССПТ-2.

Настройки управляющего Ethernet-интерфейса определяются по двум источникам:

- `Настроено` – настройки управляющего Ethernet-интерфейса в текущей конфигурации ССПТ-2;
- `Определено` – текущие системные настройки и состояние управляющего Ethernet-интерфейса.

Пример:

```
npsh> interface control show
Интерфейс:              control
    Настроено :
        Состояние:      включено
        Адрес:          10.98.7.1
        Маска:          255.255.255.0
        Скорость:       autoselect
        Список доступа: любой
    Определено:
        Состояние:      включено
        Адрес:          10.98.7.1
        Маска:          255.255.255.0
        Скорость:       1000baseTX/full-duplex
        Несущая:        активна
fnpsh>
```

3.4.30. interface filter disable – отключение фильтрующего интерфейса

`interf[ace] fil[ter] {all|<номер>|<имя>} dis[able]`

Требуемые привилегии – **cfg**.

Параметры:

- фильтрующий интерфейс, который должен быть отключен:
  - ✔ `all` – все фильтрующие интерфейсы, имеющиеся в ССПТ-2;

- ✔ <номер> – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): 0 – **Eth0**, 1 – **Eth1** и т. д.;
- ✔ <имя> – символическое имя, присвоенное фильтрующему интерфейсу.

Команда выключает все или выбранный фильтрующие интерфейсы и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Примеры:

```
fnpsh> interface filter all disable
Выключить все фильтрующие интерфейсы? (Y/N)  [N]: Y
FNPSH-I-3026-Фильтрующий интерфейс отключен (eth0)
FNPSH-I-3026-Фильтрующий интерфейс отключен (eth1)
FNPSH-I-3026-Фильтрующий интерфейс отключен (eth2)
fnpsh>

fnpsh> interface filter 2 disable
Выключить фильтрующий интерфейс? (Y/N)  [N]: Y
FNPSH-I-3026-Фильтрующий интерфейс отключен (eth2)
fnpsh>

fnpsh> interface filter eth0 disable
Выключить фильтрующий интерфейс? (Y/N)  [N]: Y
FNPSH-I-3026-Фильтрующий интерфейс отключен (eth0)
fnpsh>
```

3.4.31. interface filter duplex – установка режима передачи фильтрующего интерфейса

`interf[ace] fil[ter] {all|<номер>|<имя>} dup[lex] {half|ful[l]}`

Требуемые привилегии – **cfg**.

Параметры:

- фильтрующий интерфейс, режим передачи которого должен быть установлен:
  - ✔ `all` – все фильтрующие интерфейсы, имеющиеся в ССПТ-2;
  - ✔ <номер> – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): 0 – **Eth0**, 1 – **Eth1** и т. д.;
  - ✔ <имя> – символическое имя, присвоенное фильтрующему интерфейсу;
- режим передачи фильтрующего интерфейса:
  - ✔ `half` – полудуплексный режим передачи;
  - ✔ `full` – полнодуплексный режим передачи.

Команда устанавливает режим передачи для всех или выбранного фильтрующих интерфейсов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Установка режима передачи возможна только в том случае, когда скорость передачи фильтрующего интерфейса установлена в значение, отличное от `auto` (приложение 3.4.33, стр. 75).

Примеры:

```
fnpsh> interface filter eth2 duplex full
Изменить режим передачи фильтрующего интерфейса? (Y/N)  [N]: Y
FNPSH-E-10B2-Для установки режима передачи скорость передачи должна отличаться от
"autoselect"
fnpsh>

fnpsh> interface filter eth2 media 100
Изменить скорость передачи фильтрующего интерфейса? (Y/N)  [N]: Y
FNPSH-I-302E-Скорость передачи фильтрующего интерфейса изменена (eth2)
```

```
fnpsh> interface filter 2 duplex full
Изменить режим передачи фильтрующего интерфейса? (Y/N)  [N]: Y
FNPSH-I-302D-Режим передачи фильтрующего интерфейса изменен (eth2)
fnpsh>
```

3.4.32. interface filter enable – включение фильтрующего интерфейса

`interf[ace] fil[ter] {all|<номер>|<имя>} en[able]`

Требуемые привилегии – **cfg**.

Параметры:

- фильтрующий интерфейс, который должен быть включен:
  - ✔ `all` – все фильтрующие интерфейсы, имеющиеся в ССПТ-2;
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу.

Команда включает все или выбранный фильтрующие интерфейсы и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Примеры:

```
fnpsh> interface filter all enable
FNPSH-I-3027-Фильтрующий интерфейс включен (eth0)
FNPSH-I-3027-Фильтрующий интерфейс включен (eth1)
FNPSH-I-3027-Фильтрующий интерфейс включен (eth2)
fnpsh>

fnpsh> interface filter 2 enable
FNPSH-I-3027-Фильтрующий интерфейс включен (eth2)
fnpsh>

fnpsh> interface filter eth0 enable
FNPSH-I-3027-Фильтрующий интерфейс включен (eth0)
fnpsh>
```

3.4.33. interface filter media – установка скорости передачи фильтрующего интерфейса

`interf[ace] fil[ter] {all|<номер>|<имя>} med[ia] {auto|10|100|1000}`

Требуемые привилегии – **cfg**.

Параметры:

- фильтрующий интерфейс, скорость передачи которого должна быть установлена:
  - ✔ `all` – все фильтрующие интерфейсы, имеющиеся в ССПТ-2;
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу;
- скорость передачи фильтрующего интерфейса:
  - ✔ `auto` – режим автоматического выбора скорости и режима передачи;
  - ✔ `10` – скорость передачи 10 Мбит/с;
  - ✔ `100` – скорость передачи 100 Мбит/с;
  - ✔ `1000` – скорость передачи 1000 Мбит/с.

Команда устанавливает скорость передачи для всех или выбранного фильтрующих интерфейсов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Скорость передачи 1000 Мбит/сек может быть установлена только для ССПТ-2, укомплектованных сетевыми интерфейсами, поддерживающими технологию *Gigabit Ethernet*.

Пример:

```
npsh> interface filter eth2 media 100
Изменить скорость передачи фильтрующего интерфейса? (Y/N)  [N]: Y
FNPSH-I-302E-Скорость передачи фильтрующего интерфейса изменена (eth2)
fnpsh>
```

3.4.34. interface filter mirror – установка параметров зеркалирования фильтрующих интерфейсов

```
interf[ace] fil[ter] {<номер>|<имя>} mir[ror] {<номер>|<имя>}
{all|in|out}
```

Требуемые привилегии – **cfg**.

Параметры:

- *зеркалируемый интерфейс* – фильтрующий интерфейс, являющийся источником пакетов для зеркалирования:
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу;
- *принимающий интерфейс* – фильтрующий интерфейс, на который будет передаваться трафик с зеркалируемого интерфейса:
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу;
- параметры зеркалирования:
  - ✔ `all` – на принимающий интерфейс с зеркалируемого будут передаваться копии входящих и исходящих пакетов;
  - ✔ `in` – на принимающий интерфейс с зеркалируемого будут передаваться копии только входящих пакетов;
  - ✔ `out` – на принимающий интерфейс с зеркалируемого будут передаваться копии только исходящих пакетов;

Команда выполняет установку параметров зеркалирования трафика фильтрующих интерфейсов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

При включенном режиме трансляции сетевых адресов (NAT) фильтрующие интерфейсы **Eth0** и **Eth1** не могут выступать в роли принимающего интерфейса.

Пример:

```
fnpsh> interface filter External mirror 2 all
FNPSH-I-3035-Зеркалирование интерфейсов включено
fnpsh>
```

3.4.35. interface filter mirror disable – отключение зеркалирования фильтрующих интерфейсов

```
interf[ace] fil[ter] {<номер>|<имя>} mir[ror] dis[able]
```

Требуемые привилегии – **cfg**.

Параметры:

- *зеркалируемый интерфейс* – фильтрующий интерфейс, для которого должен быть отключен режим зеркалирования трафика:
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу.

Команда выключает зеркалирование фильтрующих интерфейсов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

После выполнения команды `interface filter mirror disable` для повторного включения зеркалирования фильтрующих интерфейсов необходимо вновь использовать команду `interface filter mirror` (приложение 3.4.34, стр. 76) с указанием всех необходимых параметров зеркалирования.

Пример:

```
npsh> interface filter eth0 mirror disable
Выключить зеркалирование интерфейсов? (Y/N)  [N]: Y
FNPSH-I-3034-Зеркалирование интерфейсов отключено
fnpsh>
```

3.4.36. interface filter rename – переименование фильтрующего интерфейса

```
interf[ace] fil[ter] {<номер>|<имя>} ren[ame] <новое_имя>
```

Требуемые привилегии – **cfg**.

Параметры:

- номер или символическое имя фильтрующего интерфейса, для которого выполняется переименование:
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу;
- `<новое_имя>` – новое символическое имя, которое будет присвоено фильтрующему интерфейсу.

Команда присваивает фильтрующему интерфейсу новое символическое имя и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

В ССПТ-2 существуют следующие ограничения для символических имен фильтрующих интерфейсов:

- символическое имя должно отвечать следующим требованиям:
  - ✔ длина имени – от **1** до **16** символов;
  - ✔ допустимые символы в имени – любые **печатаемые символы**;
- символическое имя является регистрово-зависимым;
- одно и тоже символическое имя не может быть присвоено нескольким фильтрующим интерфейсам.

Первоначально фильтрующим интерфейсам ССПТ-2 присвоены символические имена `eth0` – для интерфейса **Eth0**, `eth1` – для интерфейса **Eth1**, и т. д.

Примеры:

```
fnpsh> interface filter eth0 rename External
FNPSH-I-302A-Интерфейс переименован
fnpsh> interface filter 1 rename Internal
FNPSH-I-302A-Интерфейс переименован
fnpsh> interface filter eth2 rename Mirror
FNPSH-I-302A-Интерфейс переименован
fnpsh>
```

3.4.37. interface filter show – вывод информации о состоянии фильтрующего интерфейса

`interf[ace] fil[ter] {all|<номер>|<имя>} sh[ow]`

Параметры:

- фильтрующий интерфейс для которого выводится информация о состоянии:
  - ✔ `all` – все фильтрующие интерфейсы, имеющиеся в ССПТ-2;
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу;

Команда выводит на экран терминала настройки и текущее состояние фильтрующего интерфейса ССПТ-2.

Настройки фильтрующего интерфейса определяются по двум источникам:

- `Настроено` – настройки фильтрующего интерфейса в текущей конфигурации ССПТ-2:
  - ✔ состояние интерфейса – включен/отключен;
  - ✔ скорость и режим передачи;
  - ✔ параметры зеркалирования;
- `Определено` – текущие системные настройки и состояние фильтрующего интерфейса:
  - ✔ состояние интерфейса – включен/отключен;
  - ✔ скорость и режим передачи;
  - ✔ наличие несущей.

Примеры:

```
fnpsh> interface filter all show
-----------------+-------------------------+-----------------------------------
                 |        Настроено        |            Определено
    Интерфейс    |-----+---------+---------+-----+--------------------+-------
                 |Сост.| Скорость|Зеркалиро.|Сост.|      Скорость      |Несущая
-----------------+-----+---------+---------+-----+--------------------+-------
0:External       | вкл.|  auto   | all to 2 | вкл.|1000baseTX full-dup.|  да
1:Internal       | вкл.|  auto   |  откл.   | вкл.|1000baseTX full-dup.|  да
2:Mirror         | вкл.|  auto   |all from 0| вкл.|                    |  нет
-----------------+-----+---------+---------+-----+--------------------+-------
fnpsh>

fnpsh> interface filter External show
-----------------+-------------------------+-----------------------------------
                 |        Настроено        |            Определено
    Интерфейс    |-----+---------+---------+-----+--------------------+-------
                 |Сост.| Скорость|Зеркалиро.|Сост.|      Скорость      |Несущая
-----------------+-----+---------+---------+-----+--------------------+-------
0:External       | вкл.|  auto   | all to 2 | вкл.|1000baseTX full-dup.|  да
```

```
-----------------+-----+--------+----------+-----+------------------+-------
fnpsh>

fnpsh> interface filter 2 show
-----------------+-------------------------+---------------------------------
                 |        Настроено        |            Определено
    Интерфейс    |-----+--------+----------+-----+------------------+-------
                 |Сост.| Скорость|Зеркалиро.|Сост.|      Скорость    |Несущая
-----------------+-----+--------+----------+-----+------------------+-------
2:Mirror         | вкл.|  auto   |all from 0| вкл.|                  |  нет
-----------------+-----+--------+----------+-----+------------------+-------
fnpsh>
```

3.4.38. interface filter stats – вывод информации о статистике трафика на фильтрующем интерфейсе

`interf[ace] fil[ter] {all|<номер>|<имя>} stats`

Параметры:

- фильтрующий интерфейс для которого выводится информация о статистике трафика:
  - ✔ `all` – все фильтрующие интерфейсы, имеющиеся в ССПТ-2;
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу;

Команда выводит статистику трафика с момента последнего запуска пакетного фильтра по всем или выбранному фильтрующим интерфейсам ССПТ-2. По каждому фильтрующему интерфейсу выводится информация о статистике трафика, аналогичная выводу команды `filter status` (приложение 3.4.10, стр. 64).

При выводе количества байт могут использоваться следующие сокращения:

- `K` – трафик в килобайтах;
- `M` – трафик в мегабайтах.

Пример:

```
fnpsh> interface filter External stats
Статистика с 20.05.2013, 14:10:03:
-----------------+--------------------+--------------------+--------------------
External         |   Принято(пак/байт)|  Передано(пак/байт)|   Удалено(пак/байт)
-----------------+--------------------+--------------------+--------------------
  Ethernet II    |       2178306/2987M|          1203513/90M|             108/119K
  IEEE 802.3/LLC |                0/0|                 0/0|                0/0
  IEEE 802.3/SNAP|                0/0|                 0/0|                0/0
  IEEE 802.3 raw |                0/0|                 0/0|                0/0
  Повреждено     |                0/0|                    |
Всего Ethernet   |       2178306/2987M|          1203513/90M|             108/119K
  ARP            |             795/14K|            1472/26K|                0/0
  RARP           |                0/0|                 0/0|                0/0
Всего ARP/RARP   |             795/14K|            1472/26K|                0/0
  TCP            |       2176946/2903M|          1192957/37M|             108/114K
  UDP            |            551/110K|           9008/915K|                0/0
  ICMP           |              14/464|              6/240|                0/0
  Прочие         |                0/-|               70/-|                0/-
Всего IP         |       2177511/2945M|          1202041/61M|             108/116K
Всего IPX        |                0/0|                 0/0|                0/0
Всего прочих     |                0/-|                 0/-|                0/-
-----------------+--------------------+--------------------+--------------------
fnpsh>
```

3.4.39. log event show – просмотр зарегистрированных событий

`log ev[ent] sh[ow] [<критерии_отбора>]`

Параметры:

- <критерии_отбора> – необязательный параметр, позволяющий выполнять просмотр только тех зарегистрированных событий, которые удовлетворяют введенным критериям.

Команда выполняет просмотр зарегистрированных событий ССПТ-2. Каждая строка вывода содержит информацию об одном зарегистрированном событии:

- порядковый номер события в списке событий, отобранных для просмотра;
- время регистрации события с точностью до секунды;
- описание события.

При отсутствии критериев отбора команда `log event show` выводит все зарегистрированные события.

ССПТ-2 одновременно может хранить до **6000** зарегистрированных событий.

Время регистрации события выводится в формате:

`ДД.ММ.ГГГГ ЧЧ:ММ:СС,`

где:

- `ДД.ММ.ГГГГ` – день (`ДД`), месяц (`ММ`) и год (`ГГГГ`);
- `ЧЧ:ММ:СС` – часы в 24-часовом формате (`ЧЧ`), минуты (`ММ`) и секунды (`СС`).

Описание события выводится в формате:

`{I|W|E}-XXXX-<текст_события> [<интерфейс>, <привилегии>] [(пользователь, IP_адрес)]`

где:

- `I|W|E` – категория события:
  - ✔ `I` – информационное событие;
  - ✔ `W` – предупреждение;
  - ✔ `E` – ошибка;
- `XXXX` – шестнадцатеричный код события. Каждое событие ССПТ-2 имеет свой уникальный числовой код. Перечень кодов всех событий приводится в приложении ;
- <текст_события> – текстовая интерпретация кода события;
- необязательные дополнения:
  - ✔ <интерфейс> – тип интерфейса администратора ССПТ-2 (раздел 1.4.2, стр. 4);
  - ✔ <привилегии> – текущие привилегии пользователя, действия которого привели к регистрации данного события;
  - ✔ <пользователь> – имя пользователя ССПТ-2, действия которого привели к регистрации данного события;
  - ✔ <IP_адрес> – IP-адрес управляющего компьютера в случае удаленного управления, `Console` – в случае управления с системной консоли ССПТ-2.

Для просмотра зарегистрированных событий используются клавиши и управляющие последовательности, перечисленные в таблице 3.3.

Таблица 3.3: Управление просмотром зарегистрированных событий

Управление	*Назначение*
<↑>	Переход к предыдущему по порядковому номеру событию
<↓>	Переход к следующему по порядковому номеру событию
<←>	Перемещение на одну позицию влево по строкам описания событий
<→>	Перемещение на одну позицию вправо по строкам описания событий

Управление	Назначение
<Home>	Перемещение к первой позиции строк описания событий
<End>	Перемещение к последней позиции самой длинной строки описания события, из тех что в данный момент видны на экране терминала
<Page Up>	Переход к предыдущей странице вывода строк описания событий
<Page Down>	Переход к следующей странице вывода строк описания событий
<Ctrl+B>	Переход к первому по порядковому номеру событию
<Ctrl+E>	Переход к последнему по порядковому номеру событию
<H>	Вывод подсказки по клавишам управления просмотром зарегистрированных событий (рисунок 3.46, стр. 82)
<Ctrl+W>	Режим просмотра без горизонтальной прокрутки. В этом режиме осуществляется автоматический перенос строк, длина которых превышает ширину окна вывода данных.
<F10>, <Q>	Завершение выполнения команды

Пример вывода информации о зарегистрированных событиях приводится на рисунке 3.46.

Критерии отбора событий. Параметр <критерии_отбора> представляет собой список именованных пар, разделенных пробелом, вида:

```
<имя_критерия>=<значение>[ ...]
```

Не допускается указывать в списке один и тот же критерий отбора более одного раза. В результате выполнения команды будут отобраны события, удовлетворяющие *всем критериям отбора, указанным в списке, в совокупности*.

В случае отсутствия зарегистрированных событий, удовлетворяющим критериям отбора, на экран терминала будет выведено предупреждение:

```
FNPSH-W-200C-Нет заданных регистрационных записей
```

В списке критериев отбора событий параметр <имя_критерия> может принимать одно из следующих значений:

- code – отбор по коду события;
- order – порядок сортировки отобранных событий при выводе;
- time – отбор по времени регистрации события;
- type – отбор по категории события;
- viewer – режим просмотра данных командного интерфейса ССПТ-2.

Отбор по коду события. Критерий code позволяет выбрать среди зарегистрированных событий события с указанным числовым кодом. Критерий отбора имеет следующий синтаксис:

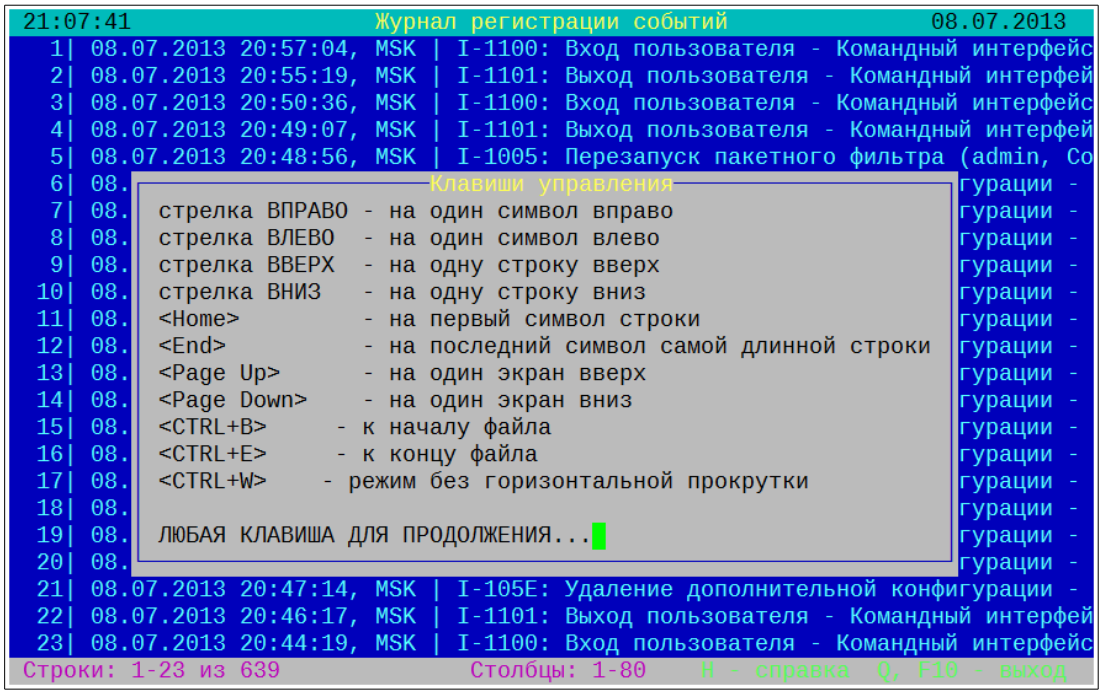

Рисунок 3.46: Просмотр зарегистрированных событий

`code=XXXX`

где

- `XXXX` – шестнадцатеричный код события.

Пример (показать все события с кодом `0x1100`):

```
fnpsh> log event show code=1100
```

Сортировка событий по времени регистрации. Критерий `order` позволяет отсортировать отобранные события по возрастанию или по убыванию времени их регистрации. Критерий имеет следующий синтаксис:

`order={asc|desc}`

где

- `asc` – сортировка по возрастанию времени регистрации события, наиболее ранние события выводятся в начале списка;
- `desc` – сортировка по убыванию времени регистрации события, наиболее поздние события выводятся в начале списка (*режим сортировки по умолчанию*).

При выводе, по умолчанию события сортируются по убыванию времени регистрации (`order=desc`).

Пример (вывод всех событий в порядке возрастания времени регистрации):

```
fnpsh> log event show order=asc
```

Отбор по времени регистрации события. Критерий `time` позволяет выбрать события, зарегистрированные в течение указанного времени. Критерий отбора имеет следующий синтаксис:

`time=<time_from>[-<time_to>]`

Возможно указание как точного времени регистрации, так и интервала времени. При указании точного времени регистрации будут отобраны события, время регистрации которых в точности совпадает с указанным временем в критерии отбора. При указании интервала времени будут

отобраны события, которые были зарегистрированы с момента времени <time_from> по момент времени <time_to> включительно.

Параметры <time_from> и <time_to> имеют следующий синтаксис:

```
{ГГГГ/ММ/ДД.ЧЧ:ММ[:СС]|ГГГГ/ММ/ДД|ЧЧ:ММ[:СС]}
```

где

- ГГГГ – четырехзначное значение года;
- ММ – месяц года (от 01 до 12);
- ДД – день месяца (от 01 до 31);
- ЧЧ – часы в 24-часовом формате (от 00 до 23);
- ММ – минуты (от 00 до 59);
- СС – секунды (от 00 до 59, по умолчанию – 00).

Для указания точного времени регистрации необходимо использовать только параметр <time_from>, при этом действуют следующие правила отбора зарегистрированных событий:

- если время указано в формате 'ГГГГ/ММ/ДД.ЧЧ:ММ[:СС]', то будут отобраны события, зарегистрированные в точности в указанное время;
- если время указано в формате 'ГГГГ/ММ/ДД', то будут отобраны события, зарегистрированные в течение указанных суток (от 00:00:00 до 23:59:59);
- если время указано в формате 'ЧЧ:ММ[:СС]', то будут отобраны события, зарегистрированные в указанное время в любой день.

Примеры:

- показать события, зарегистрированные с 12:00:00 30 марта 2013 года по 20:00:30 31 марта 2013 года

```
fnpsh> log event show time=2013/03/30.12:00-2013/03/31.20:00:30
```

- показать события, зарегистрированные с 09:00:00 до 23:00:00 в любой день

```
fnpsh> log event show time=09:00-23:00
```

- показать события, зарегистрированные в течение суток 4 марта 2013 года

```
fnpsh> log event show time=2013/03/04
```

- показать события, зарегистрированные в 10:39:25 в любой день

```
fnpsh> log event show time=10:39:25
```

- показать события, зарегистрированные 30 марта 2013 года в 12:09:45

```
fnpsh> log event show time=2013/03/30.12:09:45
```

Отбор по категории события. Критерий type позволяет выбрать среди зарегистрированных событий события указанных типов. Критерий отбора имеет следующий синтаксис:

```
type={message|warning|error}[, ...]
```

Значение критерия отбора type – список категорий событий, которые должны быть отобраны:

- message – информационное событие;
- warning – предупреждение;
- error – ошибка.

Пример (показать все информационные сообщения и ошибки):

```
fnpsh> log event show type=message,error
```

Режим просмотра данных командного интерфейса ССПТ-2. Критерий `viewer` позволяет изменить режим просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23) на время выполнения команды `log event show`. Критерий отбора имеет следующий синтаксис:

```
viewer={intern[al]|mor[e]|no}
```

где

- `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.

По умолчанию используется режим просмотра данных, установленный по команде `system fnpsh viewer` (раздел 3.4.156, стр. 168)

Просмотреть текущий установленный режим просмотра данных можно по команде `system show` (раздел 3.4.162, стр. 173).

Пример (показать все зарегистрированные события в режиме постраничного просмотра):

```
fnpsh> log event show viewer=more
```

В команде `log event show` можно указывать несколько *различных* критериев отбора, Например для вывода событий, зарегистрированных в течение суток 30 марта 2011 года и упорядоченных по возрастанию времени регистрации, следует выполнить команду

```
fnpsh> log event show time=2011/03/30 order=asc
```

3.4.40. log export ftp clear – удаление параметров выгрузки файлов регистрации по FTP

`log exp[ort] ftp cl[ear]`

Требуемые привилегии – **log** или **cfg**.

Команда удаляет настройки выгрузки файлов регистрации по FTP в текущей конфигурации ССПТ-2 и выключает выгрузку файлов регистрации по FTP.

Пример:

```
npsh> log export ftp clear
Удалить параметры выгрузки по FTP? (Y/N)  [N]: Y
FNPSH-I-3039-Параметры выгрузки журналов регистрации по FTP очищены
fnpsh>
```

3.4.41. log export ftp disable – отключение выгрузки файлов регистрации по FTP

`log exp[ort] ftp dis[able]`

Требуемые привилегии – **log** или **cfg**.

Команда выключает выгрузку файлов регистрации по FTP и изменяет соответствующие настройки в текущей конфигурации ССПТ-2. Установки параметров выгрузки, таких как IP-адрес FTP сервера, имя пользователя и пароль на FTP сервере и путь на FTP сервере, остаются без изменения.

Пример:

```
fnpsh> log export ftp disable
Отключить выгрузку журналов регистрации на FTP-сервер? (Y/N)  [N]: Y
FNPSH-I-3038-Выгрузка журналов регистрации по FTP отключена
fnpsh>
```

3.4.42. log export ftp enable – включение выгрузки файлов регистрации по FTP

```
log exp[ort] ftp en[able]
```

Требуемые привилегии – **log** или **cfg**.

Команда включает выгрузку файлов регистрации по FTP и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Включение выгрузки файлов регистрации по FTP возможно только в том случае, когда включен управляющий Ethernet-интерфейс.

Выполнение команды `log export ftp enable` возможно только в том случае, когда значения параметров выгрузки файлов регистрации по FTP уже установлены (приложение 3.4.43, стр. 85).

Пример:

```
fnpsh> log export ftp enable
FNPSH-I-3036-Выгрузка журналов регистрации по FTP включена
fnpsh>
```

3.4.43. log export ftp set – установка параметров выгрузки файлов регистрации по FTP

```
log exp[ort] ftp set <ftp_параметры>
```

Требуемые привилегии – **log** или **cfg**.

Параметры:

- `<ftp_параметры>` – параметры FTP-сервера для выгрузки файлов регистрации.

Команда устанавливает или изменяет параметры выгрузки в текущей конфигурации ССПТ-2.

Параметр `<ftp_параметры>` представляет собой список именованных пар, разделенных пробелом, вида:

```
<имя_параметра>=<значение>[ ...]
```

Не допускается указывать в списке один и тот же параметр более одного раза.

Команда позволяет установить любой из следующих параметров FTP-сервера независимо друг от друга:

- `serv[er]=<IP_адрес>` – установка IP-адреса FTP-сервера. Значение `<IP_адрес>` указывается в формате, принятом для IP-адресов – `XXX.XXX.XXX.XXX`, где `XXX` – целое число в диапазоне от `0` до `255`;
- `path=<ftp_путь>` – установка пути на FTP-сервере для хранения файлов регистрации;
- `us[er]=<ftp_вход> [pass[word]=<ftp_пароль>]` – установка имени и пароля пользователя FTP-сервера.

В целях безопасности не рекомендуется указывать пароль пользователя FTP сервера в командной строке. Если пароль не указан, командный интерфейс выведет на экран терминала запрос на ввод пароля пользователя FTP сервера, при этом ввод пароля на экране терминала отображаться не будет.

В ССПТ-2 существуют следующие ограничения для настроек параметров выгрузки файлов регистрации по FTP:

- путь к каталогу на FTP сервере должен отвечать следующим требованиям:
  - ✔ длина пути – не более **256** символов;
  - ✔ допустимые символы – **латинские буквы**, **цифры**, символы **косой черты** '/' и **точки** '.';
  - ✔ путь должен начинаться с символа **косой черты** '/' (абсолютный путь);
  - ✔ путь к каталогу на FTP сервере является **регистрово-зависимым**;
- имя пользователя FTP сервера должно отвечать следующим требованиям:
  - ✔ длина имени пользователя – от **2** до **128** символов;
  - ✔ допустимые символы:
    - первый символ – **строчные латинские символы** (a-z) **и цифры** (0-9);
    - последующие символы – **строчные латинские символы** (a-z), **цифры** (0-9) и символы '_' (подчеркивание), '.' (точка), '-' (дефис), '@';
- пароль пользователя FTP сервера должно отвечать следующим требованиям:
  - ✔ длина пароля – от **6** до **128** символов;
  - ✔ допустимые символы – только **печатаемые ASCII-символы**.

Примеры:

- установить все возможные параметры FTP-сервера:

```
fnpsh> log export ftp set server=10.234.28.1 path=/fnplog/10.234.28.75 user=fnplog
FTP пароль:
FTP пароль повторно:
FNPSH-I-3037-Параметры выгрузки журналов регистрации по FTP определены
fnpsh>
```

- установить/изменить только IP-адрес FTP-сервера:

```
fnpsh> log export ftp set server=10.234.28.2
FNPSH-I-3037-Параметры выгрузки журналов регистрации по FTP определены
fnpsh>
```

3.4.44. log export syslog disable – отключение выгрузки файлов регистрации по SYSLOG

```
log exp[ort] sysl[og] dis[able]
```

Требуемые привилегии – **log** или **cfg**.

Команда выключает выгрузку файлов регистрации по SYSLOG и изменяет соответствующие настройки в текущей конфигурации ССПТ-2. Установка IP-адреса SYSLOG сервера остается без изменения.

Если на момент выполнения команды `log export syslog disable` выгрузка файлов регистрации по SYSLOG уже была отключена, то настройки выгрузки останутся без изменения.

Примеры:

```
fnpsh> log export syslog disable
FNPSH-E-1109-Выгрузка по SYSLOG уже отключена
fnpsh>

fnpsh> log export syslog disable
Отключить выгрузку на SYSLOG сервер? (Y/N)  [N]: Y
FNPSH-I-30AE-Выгрузка системных сообщений на SYSLOG сервер отключена
fnpsh>
```

3.4.45. log export syslog enable – включение выгрузки файлов регистрации по SYSLOG

```
log exp[ort] sysl[og] en[able]
```

Требуемые привилегии – **log** или **cfg**.

Команда включает выгрузку файлов регистрации по SYSLOG и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Включение выгрузки файлов регистрации по SYSLOG возможно только в том случае, когда включен управляющий Ethernet-интерфейс.

Выполнение команды `log export syslog enable` возможно только в том случае, когда IP-адрес SYSLOG сервера уже установлен (приложение 3.4.46, стр. 87).

Пример:

```
fnpsh> log export syslog enable
FNPSH-I-30AF-Выгрузка системных сообщений на SYSLOG сервер включена
fnpsh>
```

3.4.46. log export syslog server – установка IP-адреса SYSLOG сервера

```
log exp[ort] sysl[og] serv[er] <IP_адрес>
```

Требуемые привилегии – **log** или **cfg**.

Параметры:

- `<IP_адрес>` – IP-адрес SYSLOG сервера.

Команда устанавливает IP-адрес SYSLOG сервера для выгрузки файлов регистрации и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> log export syslog server 10.234.28.1
FNPSH-I-30B0-Адрес SYSLOG сервера изменен
fnpsh>
```

3.4.47. log packet clear – очистка регистрации пакетов

```
log pack[et] cl[ear]
```

Требуемые привилегии – **log**.

Команда удаляет из файлов регистрации все записи о зарегистрированных пакетах.

Пример:

```
fnpsh> log packet clear
Очистить журнал регистрации пакетов? (Y/N)  [N]: Y
FNPSH-I-3066-Регистрация пакетов очищена
fnpsh>
```

3.4.48. log packet disable – отключение режима регистрации пакетов

```
log pack[et] dis[able]
```

Требуемые привилегии – **log** или **cfg**.

Команда выключает режим регистрации пакетов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

При отключенном режиме регистрации пакетов пакеты не будут регистрироваться даже, если в правилах фильтрации будет установлен флаг регистрации пакетов.

Пример:

```
fnpsh> log packet disable
FNPSH-I-3064-Регистрация пакетов отключена
fnpsh>
```

3.4.49. log packet enable – включение режима регистрации пакетов

`log pack[et] en[able]`

Требуемые привилегии – **log** или **cfg**.

Команда включает режим регистрации пакетов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> log packet enable
FNPSH-I-3063-Регистрация пакетов включена
fnpsh>
```

3.4.50. log packet show – просмотр зарегистрированных пакетов

`log packet show [<критерии_отбора>]`

Параметры:

- `<критерии_отбора>` – необязательный параметр, позволяющий выполнять просмотр только тех зарегистрированных пакетов, которые удовлетворяют введенным критериям.

Команда выполняет просмотр зарегистрированных пакетов. Вывод осуществляется в форме таблицы. Каждая строка таблицы содержит информацию об одном зарегистрированном пакете:

- время регистрации пакета с точностью до микросекунд. Выводится только время суток без указания даты;
- действие, которое было выполнено над пакетом;
- цепочка правил фильтрации, примененных к пакету;
- фильтрующие интерфейсы, через которые прошел пакет;
- тип протокола;
- адреса источника пакета;
- адреса приемника пакета.

При отсутствии критериев отбора команда `log packet show` выводит все зарегистрированные пакеты.

ССПТ-2 одновременно может хранить до **10000** зарегистрированных пакетов/сессий.

Время регистрации пакета выводится в формате:

`чч:мм:сс.дддддд`,

где:

- `чч:мм:сс` – часы в 24-часовом формате (`чч`), минуты (`мм`) и секунды (`сс`);
- `дддддд` – доли секунды с точностью до микросекунды.

Действие, выполненное над пакетом – `drop`, `accept` или `pass` (раздел 1.4.1, стр. 2).

Цепочка правил фильтрации отражает последовательность применения правил фильтрации различных уровней к данному пакету. В цепочке правил всегда будет присутствовать MAC-правило фильтрации. Каждое правило фильтрации в цепочке характеризуется его типом и номером. Например, цепочка правил

`mac:0,ip:10`

означает, что к пакету были последовательно применены глобальное MAC-правило (глобальные правила всегда имеют номер `0`) и IP-правило с номером `10`.

Путь прохождения пакета через фильтрующие интерфейсы ССПТ-2 характеризуется входным фильтрующим интерфейсом и, в общем случае, несколькими выходными фильтрующими интерфейсами. **Входной интерфейс** – это фильтрующий интерфейс ССПТ-2, на котором был принят данный пакет. **Выходные интерфейсы** – это фильтрующие интерфейсы, на которые был передан данный пакет после его обработки пакетным фильтром.

В выводе информации о зарегистрированном пакете список выходных интерфейсов будет отсутствовать для **удаленных** пакетов (действие `drop`).

В выводе информации о пакете для обозначения фильтрующих интерфейсов используются их символические имена.

Тип протокола характеризует протоколы сетевого и, возможно, транспортного уровня межсетевого взаимодействия, либо служебные протоколы, инкапсулированные в кадр Ethernet зарегистрированного пакета.

Адреса источника и приемника пакета соответствуют типу протокола зарегистрированного пакета.

Для просмотра зарегистрированных пакетов используются клавиши и управляющие последовательности, перечисленные в таблице 3.4.

Таблица 3.4: Управление просмотром зарегистрированных пакетов

Управление	***Назначение***
<↑>	Переход к предыдущему пакету
<↓>	Переход к следующему пакету
<←>	Перемещение влево на один столбец таблицы зарегистрированных пакетов
<→>	Перемещение вправо на один столбец таблицы зарегистрированных пакетов
<Home>	Перемещение к первому столбцу таблицы зарегистрированных пакетов
<End>	Перемещение к последнему столбцу таблицы зарегистрированных пакетов
<Page Up>	Переход к предыдущей странице вывода пакетов
<Page Down>	Переход к следующей странице вывода пакетов
<T>	Вывод текущего системного времени ССПТ-2
<Enter>	Вывод меню подробного просмотра пакета
<H>	Вывод подсказки по клавишам управления просмотром зарегистрированных событий (рисунок 3.47)
<F10>, <Q>	Завершение выполнения команды

Пример вывода информации о зарегистрированных пакетах приводится на рисунке 3.47.

Таблица зарегистрированных пакетов, пример вывода которой показан на рисунке 3.47, содержит только основные характеристики пакетов. По каждому из зарегистрированных пакетов имеется возможность просмотра всей имеющейся информации. Для этого необходимо выделить нужный пакет, используя клавиши управления <↑>, <↓>, <Page Up> и <Page Down>, а затем нажать клавишу <Enter> для вывода экран терминала меню подробного просмотра информации о пакете (рисунок 3.48).

Состав элементов меню подробного просмотра информации о пакете зависит от типа протокола в пакете. На рисунке 3.48 показан вывод меню подробного просмотра для TCP пакета.

Элементы меню “Общая информация” и “Ethernet” являются общими для всех зарегистрированных пакетов вне зависимости от их типа.

Для вывода подробной информации о пакете необходимо выбрать соответствующий пункт меню, используя клавиши управления <↑> и <↓>, а затем нажать клавишу <Enter>. Завершение просмотра и выход из меню осуществляется нажатиями клавиши <Q> или <F10>.

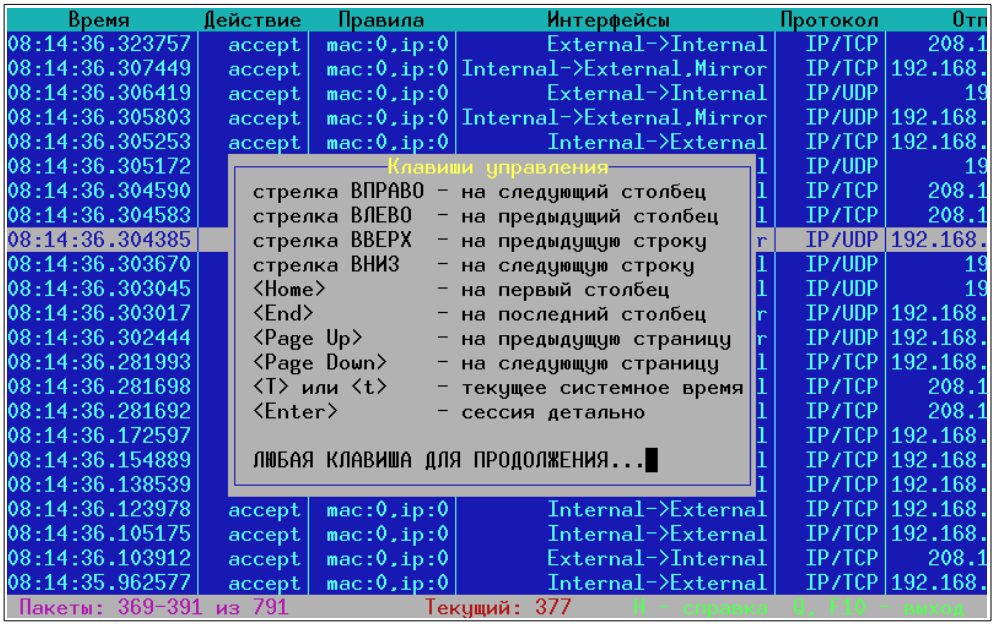

Рисунок 3.47: Просмотр зарегистрированных пакетов

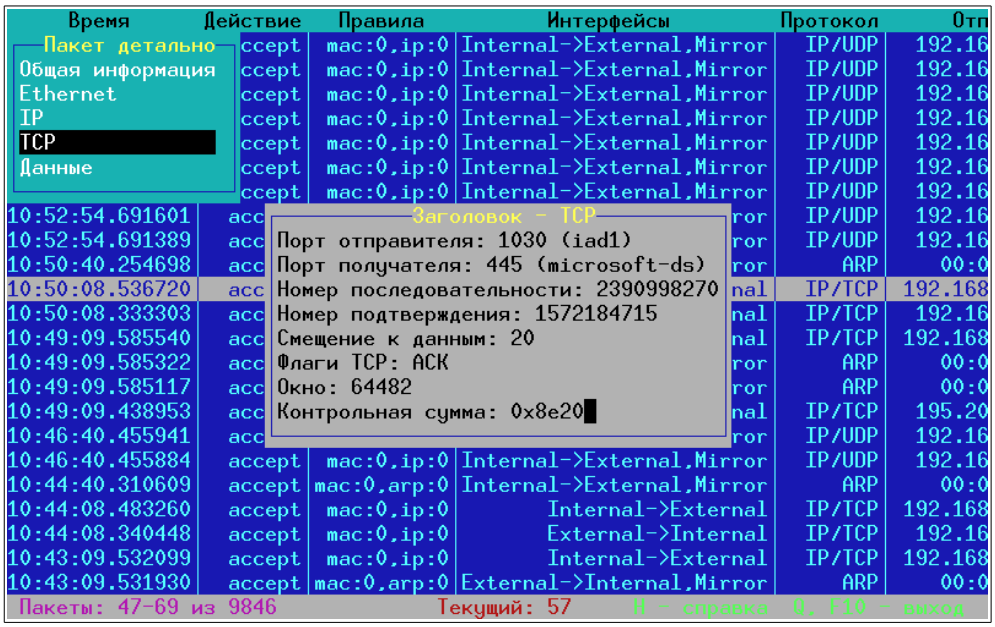

Рисунок 3.48: Подробный просмотр информации о пакете

Критерии отбора пакетов. Параметр <критерии_отбора> представляет собой список именованных пар, разделенных пробелом, вида:

<имя_критерия>=<значение>[...]

Не допускается указывать в списке один и тот же критерий отбора более одного раза. В результате выполнения команды будут отобраны пакеты, удовлетворяющие *всем критериям отбора, указанным в списке, в совокупности*.

В случае отсутствия зарегистрированных пакетов, удовлетворяющим критериям отбора, на экран терминала будет выведено предупреждение:

```
FNPSH-W-200C-Нет заданных регистрационных записей
```

В списке критериев отбора пакетов параметр `<имя_критерия>` может принимать одно из следующих значений:

- `action` – отбор по действию, выполненному над пакетом;
- `code` – отбор по коду события, связанного с пакетом;
- `dstip` – отбор по IP-адресам назначения пакета (*только для IP пакетов*);
- `dstport` – отбор по номерам прикладных портов назначения пакета (*только для UDP и TCP пакетов*);
- `frame` – отбор по типам кадров Ethernet;
- `in` – отбор по входным фильтрующим интерфейсам;
- `ip` – отбор по IP-адресам как источника, так и назначения пакета (*только для IP пакетов*);
- `mac` – отбор по MAC-адресам как источника, так и назначения пакета;
- `macdst` – отбор по MAC-адресам назначения пакета;
- `macsrc` – отбор по MAC-адресам источника пакета;
- `natsid` – отбор по номеру обратной сессии NAT, к которой принадлежал данный пакет;
- `order` – порядок сортировки отобранных пакетов при выводе;
- `out` – отбор по выходным фильтрующим интерфейсам;
- `port` – отбор по номерам прикладных портов как источника, так и назначения пакета (*только для UDP и TCP пакетов*);
- `proto` – отбор по типам протоколов, инкапсулированных в кадр Ethernet;
- `rule` – отбор по типу и номеру правила фильтрации, примененного к пакету;
- `sid` – отбор по номеру сессии, к которой принадлежал пакет;
- `srcip` – отбор по IP-адресам источника пакета (*только для IP пакетов*);
- `srcport` – отбор по номерам прикладных портов источника пакета (*только для UDP и TCP пакетов*);
- `time` – отбор по времени регистрации пакета;
- `viewer` – режим просмотра данных командного интерфейса ССПТ-2.

Отбор по действию, выполненному над пакетом. Критерий `action` позволяет выбрать пакеты, на которыми выполнено указанное действие. Критерий отбора имеет следующий синтаксис:

```
action={accept|drop|pass}[,...]
```

Значение критерия отбора `action` – список действий, выполненных над пакетами (раздел 1.4.1, стр. 2):

- `accept` – отбор пропущенных пакетов, прошедших обработку всех уровней правил фильтрации;
- `drop` – отбор удаленных пакетов;
- `pass` – отбор пропущенных пакетов, не прошедших обработку всех уровней правил фильтрации.

Одно и то же действие не может присутствовать в списке более одного раза.

Пример:

```
fnpsh> log packet show action=pass,drop
```

Отбор по коду события, связанного с пакетом. При обработке пакета могут возникать события, связанные с работой различных подсистем пакетного фильтра, таких как управление сессиями и NAT. Коды этих событий запоминаются при регистрации пакета.

Критерий `code` позволяет выбрать пакеты, при обработке которых произошло событие с указанным числовым кодом. Критерий отбора имеет следующий синтаксис:

```
code=XXXX
```

где

- `XXXX` – шестнадцатеричный код события.

Пример (выбрать пакеты, с которыми связано событие с кодом `0x3103`):

```
fnpsh> log packet show code=3103
```

Отбор по IP-адресам. Критерии `dstip`, `ip` и `srcip` позволяют выбирать IP пакеты с указанными IP-адресами назначения и источника пакета. Критерии отбора имеют следующий синтаксис:

```
{dstip|ip|srcip}={<IP_адрес>[/<маска>]}[,...]
```

где

- `dstip` – отбор IP пакетов по IP-адресам назначения;
- `ip` – отбор IP пакетов по IP-адресам как источника, так и назначения;
- `srcip` – отбор IP пакетов по IP-адресам источника.

Значение критерия отбора – список IP-подсетей и IP-адресов, разделенных запятой. Параметр `<IP_адрес>` указывается в формате, принятом для IP-адресов – `XXX.XXX.XXX.XXX`, где `XXX` – целое число в диапазоне от `0` до `255`.

Параметр `<маска>` указывается либо в формате IP-адреса, или в формате CIDR (количество единичных бит IP-адреса, отведенных под адресацию IP-подсети в целом) – целое число в диапазоне от `1` до `32`. Значение маски должно соответствовать правилам разбиения IP сетей на подсети.

Список IP-подсетей и IP-адресов может содержать не более **8** элементов.

Критерии отбора `dstip`, `ip`, `srcip` имеют смысл только для IP пакетов.

Примеры:

- выбрать IP пакеты с IP-адресами назначения `192.168.169.125` или `192.168.170.126`:

```
fnpsh> log packet show dstip=192.168.169.125,192.168.170.126
```

- выбрать IP пакеты с IP-адресами источника из подсети `192.168.169.0` с маской CIDR `25` (`255.255.255.128`):

```
fnpsh> log packet show srcip=192.168.169.0/25
```

- выбрать IP пакеты с IP-адресами назначения или источника из подсети `192.168.169.0/255.255.255.128` или `192.168.170.122`:

```
fnpsh> log packet show ip=192.168.169.0/255.255.255.128,192.168.170.122
```

Отбор по номерам прикладных портов. Критерии `dstport`, `port` и `srcport` позволяют выбирать TCP и UDP пакеты с указанными номерами прикладных портов источника и назначения. Критерии отбора имеют следующий синтаксис:

```
{dstport|port|srcport}={<номер_порта>|<порт_мин>-<порт_макс>}[,...]
```

где

- `dstport` – отбор TCP и UDP пакетов по номерам портов назначения;
- `port` – отбор TCP и UDP пакетов по номерам портов как источника, так и назначения;
- `srcport` – отбор TCP и UDP пакетов по номерам портов приемника.

Значение критерия отбора – список номеров прикладных портов. Элементом списка может быть:

- `<номер_порта>` – одиночное значение номера прикладного порта (целое десятичное число в диапазоне от `1` до `65535`);
- `<порт_мин>-<порт_макс>` – интервал прикладных портов от номера `<порт_мин>` до `<порт_макс>` включительно.

Список номеров прикладных портов может содержать не более **8** элементов.

Критерии отбора `dstport`, `port`, `srcport` имеют смысл только для IP пакетов с протоколами транспортного уровня TCP или UDP.

Примеры:

- выбрать TCP и UDP пакеты с номерами прикладных портов назначения из диапазона `137-139` и `445`:

```
fnpsh> log packet show dstport=137-139,445
```

- выбрать TCP и UDP пакеты с номерами прикладных портов источника и назначения `80` и `443`:

```
fnpsh> log packet show port=80,443
```

- выбрать TCP и UDP пакеты с номерами прикладных портов источника из диапазона `1024-65000`:

```
fnpsh> log packet show srcport=1024-65000
```

Отбор по типам кадров Ethernet. Критерий `frame` позволяет выбирать пакеты указанных типов кадров Ethernet. Критерий отбора имеет следующий синтаксис:

```
frame={eth2,llc,snap,raw}[,...]
```

Значение критерия отбора – список условных обозначений типов кадров Ethernet:

- `eth2` – кадр Ethernet II;
- `llc` – кадр IEEE 802.3-LLC;
- `snap` – кадр IEEE 802.3-SNAP;
- `raw` – кадр IEEE 802.3-raw.

Один и тот же тип кадра Ethernet не может присутствовать в списке более одного раза.

Пример (выбрать пакеты с типами кадров Ethernet IEEE 802.3-LLC и IEEE 802.3-raw):

```
fnpsh> log packet show frame=llc,raw
```

Отбор по фильтрующим интерфейсам. Критерии `in`, `out` позволяют выбирать пакеты, принятые или переданные через указанные фильтрующие интерфейсы ССПТ-2. Критерии отбора имеют следующий синтаксис:

```
{in|out}={<имя_интерфейса>|<номер_интерфейса>}[,...]
```

где

- `in` – отбор по входным интерфейсам;
- `out` – отбор по выходным интерфейсам.

Значение критерия отбора – список фильтрующих интерфейсов ССПТ-2:

- `<имя_интерфейса>` – символическое имя, присвоенное фильтрующему интерфейсу;
- `<номер_интерфейса>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.

Один и тот же фильтрующий интерфейс не может присутствовать в списке более одного раза.

Примеры:

- выбрать пакеты, принятые с фильтрующего интерфейса с символическим именем `External`:

```
fnpsh> log packet show in=External
```

- выбрать пакеты, переданные на фильтрующие интерфейсы с номером `1` (**Eth1**) и с символическим именем `Mirror`:

```
fnpsh> log packet show out=1,Mirror
```

Отбор по MAC-адресам. Критерии `mac`, `macdst`, `macsrc` позволяют выбирать пакеты с указанными MAC-адресами источника и назначения. Критерии отбора имеют следующий синтаксис:

```
{mac|macdst|macsrc}={<mac_адрес>[/<маска>}[,...]
```

где

- `mac` – отбор пакетов по MAC-адресам как источника, так и назначения;
- `macdst` – отбор пакетов по MAC-адресам назначения;
- `macsrc` – отбор пакетов по MAC-адресам источника.

Значение критерия отбора – список MAC-адресов и возможным указанием битовой маски MAC-адреса. Параметры `<mac_адрес>` и `<маска>` указываются в формате, принятом для MAC-адресов – `xx:xx:xx:xx:xx:xx`, где `xx` – шестнадцатеричное число в диапазоне от `00` до `ff`. Помимо этого, битовая маска MAC-адреса `<маска>` представляет собой непрерывную последовательность единиц, за которой может следовать только непрерывная последовательность нулей. Напрмер – `ff:ff:ff:00:00:00`.

Битовая маска MAC-адреса может быть использована для отбора пакетов на основе совпадения только той части MAC-адреса, которая соответствует единичным битам в маске.

Таким образом можно, например, выбрать пакеты, MAC адреса которых соответствуют Ethernet адаптерам какого-либо одного производителя.

Список MAC-адресов может содержать не более **8** элементов.

Примеры:

- выбрать пакеты с MAC-адресами источника и назначения, начинающихся с `00:11...`:

```
fnpsh> log packet show mac=00:11:00:00:00:00/ff:ff:00:00:00:00
```

- выбрать пакеты с MAC-адресами назначения `00:0e:35:4f:1e:0d` и `ff:ff:ff:ff:ff:ff` (широковещательные кадры Ethernet):

```
fnpsh> log packet show macdst=00:0e:35:4f:1e:0d,ff:ff:ff:ff:ff:ff
```

- выбрать пакеты с MAC-адресом источника `00:11:2f:70:b6:83`:

```
fnpsh> log packet show macsrc=00:11:2f:70:b6:83
```

Отбор по номеру обратной сессии NAT. Критерий natsid позволяют выбирать пакеты, входившие в контекст обратной сессии NAT с указанным номером, Критерий отбора имеет следующий синтаксис:

```
natsid=<номер_сессии>
```

где

- `<номер_сессии>` – номер обратной сессии NAT (целое десятичное число в диапазоне от `0` до `65535`).

Номер обратной сессии NAT зарегистрированного пакета можно увидеть при выполнении пункта “общая информация” меню подробного просмотра информации о пакете.

Пример (выбрать пакеты, входившие в контекст обратной сессии NAT с номером 1908):

```
fnpsh> log packet show natsid=1908
```

Сортировка пакетов по времени регистрации. Критерий `order` позволяет отсортировать отобранные пакеты по возрастанию или по убыванию времени их регистрации. Критерий имеет следующий синтаксис:

```
order={asc|desc}
```

где

- `asc` – сортировка по возрастанию времени регистрации пакета, наиболее ранние пакеты выводятся в начале списка;
- `desc` – сортировка по убыванию времени регистрации пакета, наиболее поздние пакеты выводятся в начале списка (*режим сортировки по умолчанию*).

При выводе, по умолчанию пакеты сортируются по убыванию времени регистрации (`order=desc`).

Пример (вывод всех пакетов в порядке возрастания времени регистрации):

```
fnpsh> log packet show order=asc
```

Отбор по типам протоколов, инкапсулированных в кадр Ethernet. Критерий `proto` позволяет выбирать пакеты, содержащие протоколы указанных типов. Критерий отбора имеет следующий синтаксис:

```
proto={arp|ip|icmp|udp|tcp|ipx|other}[,...]
```

Значение критерия отбора – список условных обозначений типов протоколов:

- `arp` – протоколы ARP/RARP;
- `ip` – протокол IP;
- `icmp` – протокол ICMP (*только для IP пакетов*);
- `udp` – протокол UDP (*только для IP пакетов*);
- `tcp` – протокол TCP (*только для IP пакетов*);
- `ipx` – протокол IPX;
- `other` – протокол, не подпадающий ни под один из перечисленных выше типов.

Список типов протоколов может содержать не более **8** элементов.

Один и тот же тип протокола не может присутствовать в списке более одного раза.

Пример (выбрать пакеты, содержащие протоколы ARP/RARP или TCP):

```
fnpsh> log packet show proto=arp,tcp
```

Отбор по типу и номеру правила фильтрации. Критерий rule позволяет выбрать пакеты, к которым было применено правило фильтрации указанного типа и номера. Критерий отбора имеет следующий синтаксис:

```
rule={mac|arp|ip|iptmp|ipx|ap}:<номер_правила>
```

Значение критерия отбора – тип и номер правила фильтрации, разделенные символом двоеточия:

- `mac` – MAC-правило фильтрации;
- `arp` – ARP-правило фильтрации;
- `ip` – IP-правило фильтрации;
- `iptmp` – временное IP-правило фильтрации;
- `ipx` – IPX-правило фильтрации;
- `ap` – AP-правило фильтрации (правило фильтрации прикладного уровня);
- `<номер_правила>` – номер правила фильтрации одного из перечисленных выше типов. Представляет собой целое десятичное число в диапазоне от `0` до `65535` для типов правил `mac`, `arp`, `ip`, `ipx`; целое десятичное число от `1` до `65535` для типов правил `iptmp` и `ap`.

Примеры:

- выбрать пакеты, к которым было применено IP-правило с номером `10`:

```
fnpsh> log packet show rule=ip:10
```

- выбрать пакеты, к которым было применено глобальное ARP-правило:

```
fnpsh> log packet show rule=arp:0
```

Отбор по номеру сессии. Критерий `sid` позволяет выбрать пакеты, входившие в контекст сессии с указанным номером. Критерий отбора имеет следующий синтаксис:

```
sid=<номер_сессии>
```

где

- `<номер_сессии>` – номер сессии (целое число в диапазоне от `0` до `65535`).

Номер сессии зарегистрированного пакета можно увидеть при выполнении пункта “общая информация” меню подробного просмотра информации о пакете.

Пример (выбрать пакеты, входившие в контекст сессии с номером `20194`):

```
fnpsh> log packet show sid=20194
```

Отбор по времени регистрации пакета. Критерий `time` позволяет выбрать пакеты, зарегистрированные в течение указанного времени. Критерий отбора имеет следующий синтаксис:

```
time=<time_from>[-<time_to>]
```

Возможно указание как точного времени регистрации, так и интервала времени. При указании точного времени регистрации будут отобраны пакеты, время регистрации которых в совпадает с точностью до секунды с указанным временем в критерии отбора. При указании интервала

времени будут отобраны пакеты, которые были зарегистрированы с момента времени <time_from> по момент времени <time_to> включительно.

Параметры <time_from> и <time_to> имеют следующий синтаксис:

```
{ГГГГ/ММ/ДД.ЧЧ:ММ[:СС]|ГГГГ/ММ/ДД|ЧЧ:ММ[:СС]}
```

где

- ГГГГ – четырехзначное значение года;
- ММ – месяц года (от 01 до 12);
- ДД – день месяца (от 01 до 31);
- ЧЧ – часы в 24-часовом формате (от 00 до 23);
- ММ – минуты (от 00 до 59);
- СС – секунды (от 00 до 59, по умолчанию – 00).

Для указания точного времени регистрации необходимо использовать только параметр <time_from>, при этом действуют следующие правила отбора зарегистрированных пакетов:

- если время указано в формате 'ГГГГ/ММ/ДД.ЧЧ:ММ[:СС]', то будут отобраны пакеты, зарегистрированные в точности в указанное время;
- если время указано в формате 'ГГГГ/ММ/ДД', то будут отобраны пакеты, зарегистрированные в течение указанных суток (от 00:00:00 до 23:59:59);
- если время указано в формате 'ЧЧ:ММ[:СС]', то будут отобраны пакеты, зарегистрированные в указанное время в любой день.

Примеры:

- показать пакеты, зарегистрированные с 12:00:00 30 марта 2013 года по 20:00:30 31 марта 2013 года

```
fnpsh> log packet show time=2013/03/30.12:00-2013/03/31.20:00:30
```

- показать пакеты, зарегистрированные с 09:00:00 до 23:00:00 в любой день

```
fnpsh> log packet show time=09:00-23:00
```

- показать пакеты, зарегистрированные в течение суток 4 марта 2013 года

```
fnpsh> log packet show time=2013/03/04
```

- показать пакеты, зарегистрированные в 10:39:25 в любой день

```
fnpsh> log packet show time=10:39:25
```

- показать пакеты, зарегистрированные 30 марта 2013 года в 12:09:45

```
fnpsh> log packet show time=2013/03/30.12:09:45
```

Режим просмотра данных командного интерфейса ССПТ-2. Критерий viewer позволяет изменить режим просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23) на время выполнения команды log packet show. Критерий отбора имеет следующий синтаксис:

```
viewer={intern[al]|mor[e]|no}
```

где

- 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.

По умолчанию используется режим просмотра данных, установленный по команде `system fnpsh viewer` (раздел 3.4.156, стр. 168)

Просмотреть текущий установленный режим просмотра данных можно по команде `system show` (раздел 3.4.162, стр. 173).

Пример (показать все зарегистрированные пакеты в режиме постраничного просмотра):

```
fnpsh> log packet show viewer=more
```

В команде `log packet show` можно указывать несколько *различных* критериев отбора, Например для вывода IP пакетов, зарегистрированных в течение суток 7 июня 2007 года и упорядоченных по возрастанию времени регистрации, следует выполнить команду

```
fnpsh> log packet show proto=ip time=2007/06/07 order=asc
```

3.4.51. log session clear – очистка регистрации сессий

`log ses[sion] cl[ear]`

Требуемые привилегии – **log**.

Команда удаляет из файлов регистрации все записи о зарегистрированных сессиях.

Пример:

```
fnpsh> log session clear
Очистить журнал регистрации сессий? (Y/N)  [N]: Y
FNPSH-I-30A9-Регистрация сессий очищена
fnpsh>
```

3.4.52. log session show – просмотр зарегистрированных сессий

`log ses[sion] sh[ow] [<критерии_отбора>]`

Параметры:

- `<критерии_отбора>` – необязательный параметр, позволяющий выполнять просмотр только тех зарегистрированных сессий, которые удовлетворяют введенным критериям.

Команда выполняет просмотр зарегистрированных сессий. Вывод осуществляется в форме таблицы. Каждая строка таблицы содержит информацию об одной зарегистрированной сессии:

- время регистрации сессии с точностью до микросекунд. Выводится только время суток без указания даты;

Время регистрации сессии совпадает с временем ее завершения.

- правила фильтрации, на основе которых создавалась сессия – IP-правило фильтрации присутствует всегда, возможно указание AP-правила фильтрации;
- атрибуты клиента – символическое имя фильтрующего интерфейса, IP-адрес клиента и номер прикладного порта (*для протоколов TCP и UDP*);
- атрибуты сервера – символическое имя фильтрующего интерфейса, IP-адрес сервера и номер прикладного порта (*для протоколов TCP и UDP*);
- типы протоколов транспортного и прикладного уровней;

При отсутствии критериев отбора команда `log session show` выводит все зарегистрированные сессии.

ССПТ-2 одновременно может хранить до **10000** зарегистрированных пакетов/сессий.

Время регистрации сессии выводится в формате:

ЧЧ:ММ:СС.ДДДДДД,

где:

- ЧЧ:ММ:СС – часы в 24-часовом формате (ЧЧ), минуты (ММ) и секунды (СС);
- ДДДДДД – доли секунды с точностью до микросекунды.

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

<имя_интерфейса>:<IP_адрес>[:<порт>]

где

- <имя_интерфейса> – символическое имя фильтрующего интерфейса ССПТ-2, на который принимаются пакеты, входящие в контекст сессии, от данной стороны сетевого взаимодействия – клиента или сервера;
- <IP_адрес> – IP-адрес стороны сетевого взаимодействия;
- <порт> – номер прикладного порта стороны сетевого взаимодействия (*только для сессий, базирующихся на транспортных протоколах TCP и UDP*).

Типы протоколов отражают имена протоколов транспортного и прикладного уровней, на которых базировалась данная сессия. Протоколы прикладного уровня указываются только для сессий, базирующихся на транспортных протоколах UDP и TCP.

Для просмотра зарегистрированных сессий используются клавиши и управляющие последовательности, перечисленные в таблице 3.5.

Таблица 3.5: Управление просмотром зарегистрированных сессий

Управление	***Назначение***
<↑>	Переход к предыдущей сессии
<↓>	Переход к следующей сессии
<←>	Перемещение влево на один столбец таблицы зарегистрированных сессий
<→>	Перемещение вправо на один столбец таблицы зарегистрированных сессий
<Home>	Перемещение к первому столбцу таблицы зарегистрированных сессий
<End>	Перемещение к последнему столбцу таблицы зарегистрированных сессий
<Page Up>	Переход к предыдущей странице вывода сессий
<Page Down>	Переход к следующей странице вывода сессий
<T>	Вывод текущего системного времени ССПТ-2
<Enter>	Подробный просмотр информации о зарегистрированной сессии
<H>	Вывод подсказки по клавишам управления просмотром зарегистрированных событий (рисунок 3.49)
<F10>, <Q>	Завершение выполнения команды

Пример вывода информации о зарегистрированных сессиях приводится на рисунке 3.49.

Таблица зарегистрированных сессий, пример вывода которой показан на рисунке 3.49, 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 (рисунок 3.50).

Завершение просмотра подробной информации о сессии осуществляется нажатием любой клавиши на клавиатуре.

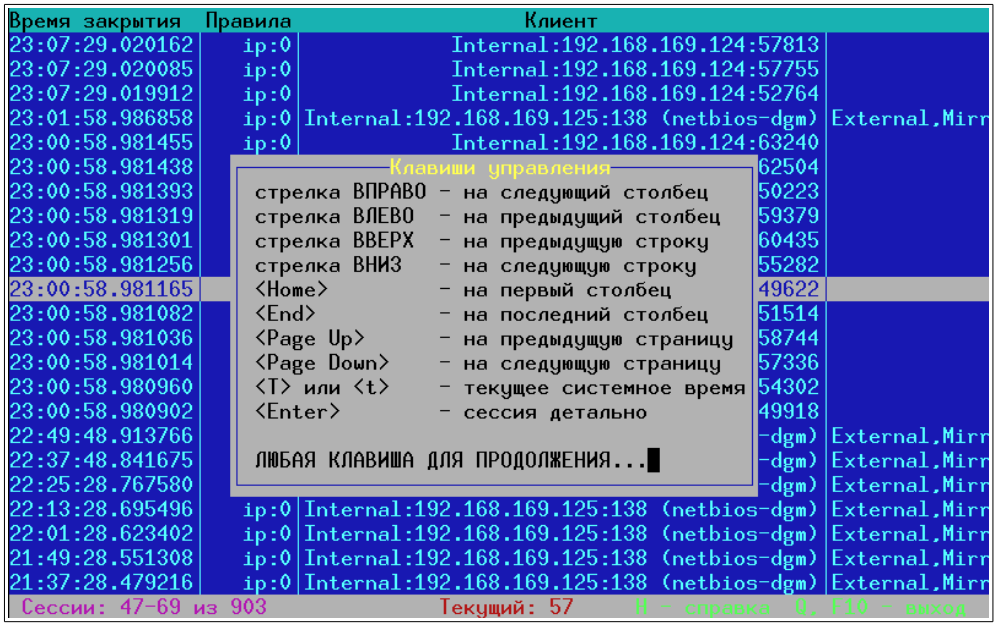

Рисунок 3.49: Просмотр зарегистрированных сессий

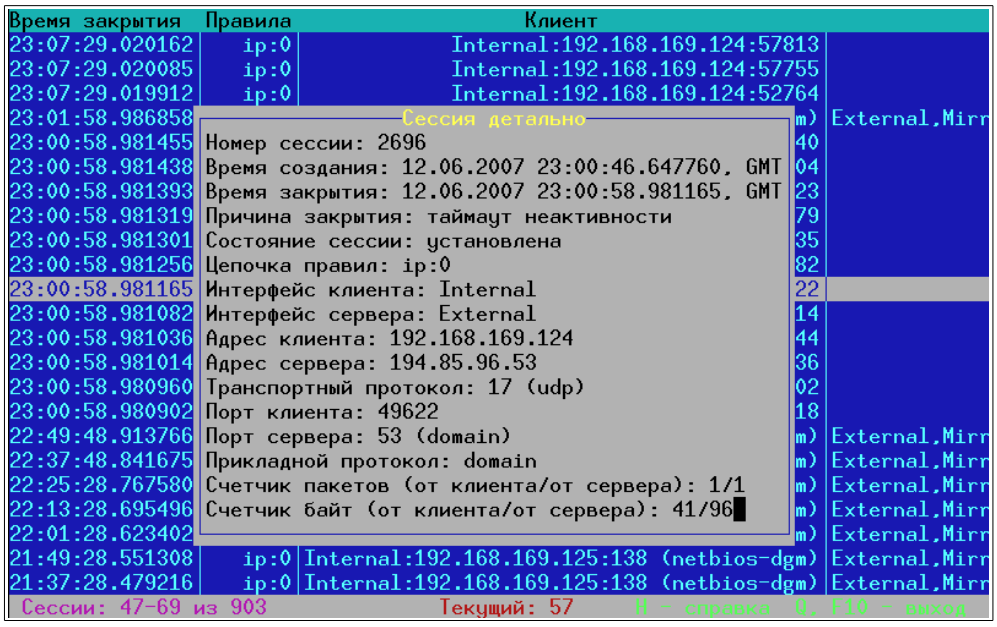

Рисунок 3.50: Подробный просмотр информации о сессии

Критерии отбора сессий. Параметр `<критерии_отбора>` представляет собой список именованных пар, разделенных пробелом, вида:

```
<имя_критерия>=<значение>[ ...]
```

Не допускается указывать в списке один и тот же критерий отбора более одного раза. В результате выполнения команды будут отобраны сессии, удовлетворяющие *всем критериям отбора, указанным в списке, в совокупности*.

В случае отсутствия зарегистрированных сессий, удовлетворяющим критериям отбора, на экран терминала будет выведено предупреждение:

```
FNPSH-W-200C-Нет заданных регистрационных записей
```

В списке критериев отбора сессий параметр <имя_критерия> может принимать одно из следующих значений:

- aproto – отбор по протоколу прикладного уровня;
- ifcl – отбор по фильтрующим интерфейсам клиента;
- ifsrv – отбор по фильтрующим интерфейсам сервера;
- ip – отбор по IP-адресам как клиента, так и сервера;
- ipcl – отбор по IP-адресам клиента;
- ipsrv – отбор по IP-адресам сервера;
- order – порядок сортировки отобранных сессий при выводе;
- port – отбор по номерам прикладных портов как клиента, так и сервера;
- portcl – отбор по номерам прикладных портов клиента;
- portsrv – отбор по номерам прикладных портов сервера;
- sid – отбор по номеру сессии;
- tend – отбор по времени завершения сессии (то же самое, что и время регистрации сессии);
- tproto – отбор по протоколу транспортного уровня;
- tstart – отбор по времени создания сессии;
- viewer – режим просмотра данных командного интерфейса ССПТ-2.

Отбор по протоколу прикладного уровня. Критерий aproto позволяет выбрать сессии, базирующиеся на транспортных протоколах TCP и UDP, с указанным номером или именем протокола прикладного уровня. Критерий отбора имеет следующий синтаксис:

```
aproto={<имя_протокола>|<номер_протокола>}
```

где

- <имя_протокола> – стандартное символическое имя протокола (например, ftp, smtp, http);
- <номер_протокола> – стандартный номер прикладного порта, соответствующий данному протоколу (например 21, 25, 80).

Критерий отбора aproto имеет смысл только для сессий, базирующихся на протоколах транспортного уровня TCP или UDP.

Примеры:

```
fnpsh> log session show aproto=smtp
```

```
fnpsh> log session show aproto=443
```

Отбор по фильтрующим интерфейсам. Критерии ifcl, ifsrv позволяют выбрать сессии с указанными фильтрующими интерфейсами клиента или сервера.

Интерфейс клиента – это фильтрующий интерфейс ССПТ-2, на который поступают пакеты в направлении от клиента к серверу в контексте данной сессии.

Интерфейс сервера – это фильтрующий интерфейс ССПТ-2, на который поступают пакеты в направлении от сервера к клиенту в контексте данной сессии.

Критерии отбора имеют следующий синтаксис:

```
{ifcl|ifsrv}={<имя_интерфейса>|<номер_интерфейса>}[,...]
```

где

- `ifcl` – отбор по интерфейсам клиента;
- `ifsrv` – отбор по интерфейсам сервера.

Значение критерия отбора – список фильтрующих интерфейсов ССПТ-2:

- `<имя_интерфейса>` – символическое имя, присвоенное фильтрующему интерфейсу;
- `<номер_интерфейса>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.

Один и тот же фильтрующий интерфейс не может присутствовать в списке более одного раза.

Примеры:

- выбрать сессии, у которых интерфейс клиента – фильтрующий интерфейс с символическим именем `Internal`:

```
fnpsh> log session show ifcl=Internal
```

- выбрать сессии, у которых интерфейс сервера – фильтрующий интерфейс `0` (**Eth0**) или фильтрующий интерфейс с символическим именем `Mirror`:

```
fnpsh> log session show ifsrv=0,Mirror
```

Отбор по IP-адресам. Критерии `ip`, `ipcl`, `ipsrv` позволяют выбрать сессии с указанными IP-адресами клиента и сервера. Критерии отбора имеют следующий синтаксис:

```
{ip|ipcl|ipsrv}={<IP_адрес>[/<маска>]}[,...]
```

где

- `ip` – отбор сессий по IP-адресам как клиента, так и сервера;
- `ipcl` – отбор сессий по IP-адресам клиента;
- `ipsrv` – отбор сессий по IP-адресам сервера.

Значение критерия отбора – список IP-подсетей и IP-адресов, разделенных запятой. Параметр `<IP_адрес>` указывается в формате, принятом для IP-адресов – `XXX.XXX.XXX.XXX`, где `XXX` – целое число в диапазоне от `0` до `255`.

Параметр `<маска>` указывается либо в формате IP-адреса, или в формате CIDR (количество единичных бит IP-адреса, отведенных под адресацию IP-подсети в целом) – целое число в диапазоне от `1` до `32`. Значение маски должно соответствовать правилам разбиения IP сетей на подсети.

Список IP-подсетей и IP-адресов может содержать не более **8** элементов.

Примеры:

- выбрать сессии с IP-адресами клиента или сервера `192.168.169.124`:

```
fnpsh> log session show ip=192.168.169.124
```

- выбрать сессии с IP-адресом клиента из подсети `192.168.170.0` с маской CIDR `25` (`255.255.255.128`) или `192.168.169.125`:

```
fnpsh> log session show ipcl=192.168.170.0/25,192.168.169.125
```

- выбрать сессии с IP-адресом сервера из подсети `192.168.169.0/255.255.255.128`:

```
fnpsh> log session show ipsrv=192.168.169.0/255.255.255.128
```

Сортировка сессий по времени регистрации. Критерий `order` позволяет отсортировать отобранные сессии по возрастанию или по убыванию времени их регистрации. Критерий имеет следующий синтаксис:

```
order={asc|desc}
```

где

- `asc` – сортировка по возрастанию времени регистрации сессии, наиболее ранние сессии выводятся в начале списка;
- `desc` – сортировка по убыванию времени регистрации сессии, наиболее поздние сессии выводятся в начале списка (*режим сортировки по умолчанию*).

При выводе, по умолчанию сессии сортируются по убыванию времени регистрации (`order=desc`).

Пример (вывод всех сессий в порядке возрастания времени регистрации):

```
fnpsh> log session show order=asc
```

Отбор по номерам прикладных портов. Критерии `port`, `portcl`, `portsrv` позволяют выбрать сессии, базирующиеся на транспортных протоколах TCP и UDP, с указанными значениями номеров прикладных портов клиента или сервера. Критерии имеют следующий синтаксис:

```
{port|portcl|portsrv}={<номер_порта>|<порт_мин>-<порт_макс>}[,...]
```

где

- `port` – отбор сессий по номерам прикладных портов как клиента, так и сервера;
- `portcl` – отбор сессий по номерам прикладных портов клиента;
- `portsrv` – отбор сессий по номерам прикладных портов сервера;

Значение критерия отбора – список номеров прикладных портов. Элементом списка может быть:

- `<номер_порта>` – одиночное значение номера прикладного порта (целое десятичное число в диапазоне от `1` до `65535`);
- `<порт_мин>-<порт_макс>` – интервал прикладных портов от номера `<порт_мин>` до `<порт_макс>` включительно.

Список номеров прикладных портов может содержать не более **8** элементов.

Критерии отбора `port`, `portcl`, `portsrv` имеют смысл только для сессий, базирующихся на протоколах транспортного уровня TCP или UDP.

Примеры:

- выбрать сессии с номерами прикладных портов клиента или сервера `80` и `443`:

```
fnpsh> log session show port=80,443
```

- выбрать сессии с номерами прикладных портов клиента из диапазона `1024-65000`:

```
fnpsh> log session show portcl=1024-65000
```

- выбрать сессии с номерами прикладных портов сервера из диапазона `137-139` и `445`:

```
fnpsh> log session show portsrv=137-139,445
```

Отбор по номеру сессии. Критерий `sid` позволяет выбрать сессии с указанным номером. Критерий отбора имеет следующий синтаксис:

```
sid=<номер_сессии>
```

где

- <номер_сессии> – номер сессии (целое число в диапазоне от 0 до 65535).

Пример (выбрать все сессии с номером 2):

```
fnpsh> log session show sid=2
```

Отбор по времени завершения сессии. Критерий tend позволяет выбрать сессии, завершенные в течение указанного времени. Критерий отбора имеет следующий синтаксис:

```
tend=<time_from>[-<time_to>]
```

Возможно указание как точного времени завершения сессии, так и интервала времени. При указании точного времени завершения будут отобраны сессии, время завершения которых в совпадает с точностью до секунды с указанным временем в критерии отбора. При указании интервала времени будут отобраны сессии, которые были завершены с момента времени <time_from> по момент времени <time_to> включительно.

Параметры <time_from> и <time_to> имеют следующий синтаксис:

```
{ГГГГ/ММ/ДД.ЧЧ:ММ[:СС]|ГГГГ/ММ/ДД|ЧЧ:ММ[:СС]}
```

где

- ГГГГ – четырехзначное значение года;
- ММ – месяц года (от 01 до 12);
- ДД – день месяца (от 01 до 31);
- ЧЧ – часы в 24-часовом формате (от 00 до 23);
- ММ – минуты (от 00 до 59);
- СС – секунды (от 00 до 59, по умолчанию – 00).

Для указания точного времени завершения сессии необходимо использовать только параметр <time_from>, при этом действуют следующие правила отбора зарегистрированных сессий:

- если время указано в формате 'ГГГГ/ММ/ДД.ЧЧ:ММ[:СС]', то будут отобраны сессии, завершившиеся в точности в указанное время;
- если время указано в формате 'ГГГГ/ММ/ДД', то будут отобраны сессии, завершившиеся в течение указанных суток (от 00:00:00 до 23:59:59);
- если время указано в формате 'ЧЧ:ММ[:СС]', то будут отобраны сессии, завершившиеся в указанное время в любой день.

Сессия регистрируется в момент ее завершения, поэтому время регистрации и время завершения сессии совпадают.

Примеры:

- выбрать сессии, завершенные с 12:00:00 30 марта 2013 года по 20:00:30 31 марта 2013 года

```
fnpsh> log session show tend=2013/03/30.12:00-2013/03/31.20:00:30
```

- показать сессии, завершенные с 09:00:00 до 23:00:00 в любой день

```
fnpsh> log session show tend=09:00-23:00
```

- выбрать сессии, завершенные в течение суток 4 марта 2013 года

```
fnpsh> log session show tend=2013/03/04
```

- выбрать сессии, завершенные в 10:39:25 в любой день

```
fnpsh> log session show tend=10:39:25
```

- выбрать сессии, завершенные 30 марта 2013 года в 12:09:45

```
fnpsh> log session show tend=2013/03/30.12:09:45
```

Отбор по протоколу транспортного уровня. Критерий `tproto` позволяет выбрать сессии с указанным номером или именем протокола транспортного уровня. Критерий отбора имеет следующий синтаксис:

```
tproto={<имя_протокола>|<номер_протокола>}
```

Значение критерия отбора – стандартное имя протокола или его номер. Поскольку сессии создаются только для протоколов транспортного уровня TCP, UDP и ICMP, значением критерия отбора tproto может быть:

- `<имя_протокола>` – `tcp`, `udp` или `icmp`;
- `<номер протокола>` – `6` (протокол TCP), `17` (протокол UDP) или `1` (протокол ICMP).

Примеры:

- выбрать сессии, базирующиеся на протоколе TCP:

```
fnpsh> log session show tproto=tcp
```

- выбрать сессии, базирующиеся на протоколе ICMP:

```
fnpsh> log session show tproto=1
```

Отбор по времени создания сессии. Критерий tstart позволяет выбрать сессии, созданные в течение указанного времени. Критерий отбора имеет следующий синтаксис:

```
tstart=<time_from>[-<time_to>]
```

Возможно указание как точного времени создания сессии, так и интервала времени. При указании точного времени создания будут отобраны сессии, время создания которых в совпадает с точностью до секунды с указанным временем в критерии отбора. При указании интервала времени будут отобраны сессии, которые были созданы с момента времени `<time_from>` по момент времени `<time_to>` включительно.

Параметры `<time_from>` и `<time_to>` имеют следующий синтаксис:

```
{ГГГГ/ММ/ДД.ЧЧ:ММ[:СС]|ГГГГ/ММ/ДД|ЧЧ:ММ[:СС]}
```

где

- `ГГГГ` – четырехзначное значение года;
- `ММ` – месяц года (от `01` до `12`);
- `ДД` – день месяца (от `01` до `31`);
- `ЧЧ` – часы в 24-часовом формате (от `00` до `23`);
- `ММ` – минуты (от `00` до `59`);
- `СС` – секунды (от `00` до `59`, по умолчанию – `00`).

Для указания точного времени создания сессии необходимо использовать только параметр `<time_from>`, при этом действуют следующие правила отбора зарегистрированных сессий:

- если время указано в формате '`ГГГГ/ММ/ДД.ЧЧ:ММ[:СС]`', то будут отобраны сессии, созданные в точности в указанное время;
- если время указано в формате '`ГГГГ/ММ/ДД`', то будут отобраны сессии, созданные в течение указанных суток (от `00:00:00` до `23:59:59`);
- если время указано в формате '`ЧЧ:ММ[:СС]`', то будут отобраны сессии, созданные в указанное время в любой день.

Примеры:

- выбрать сессии, созданные с 12:00:00 30 марта 2013 года по 20:00:30 31 марта 2013 года

```
fnpsh> log session show tstart=2013/03/30.12:00-2013/03/31.20:00:30
```

- показать сессии, созданные с 09:00:00 до 23:00:00 в любой день

```
fnpsh> log session show tstart=09:00-23:00
```

- выбрать сессии, созданные в течение суток 4 марта 2013 года

```
fnpsh> log session show tstart=2013/03/04
```

- выбрать сессии, созданные в 10:39:25 в любой день

```
fnpsh> log session show tstart=10:39:25
```

- выбрать сессии, созданные 30 марта 2013 года в 12:09:45

```
fnpsh> log session show tstart=2013/03/30.12:09:45
```

Режим просмотра данных командного интерфейса ССПТ-2. Критерий `viewer` позволяет изменить режим просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23) на время выполнения команды `log session show`. Критерий отбора имеет следующий синтаксис:

```
viewer={intern[al]|mor[e]|no}
```

где

- `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.

По умолчанию используется режим просмотра данных, установленный по команде `system fnpsh viewer` (раздел 3.4.156, стр. 168)

Просмотреть текущий установленный режим просмотра данных можно по команде `system show` (раздел 3.4.162, стр. 173).

Пример (показать все зарегистрированные сессии в режиме постраничного просмотра):

```
fnpsh> log session show viewer=more
```

В команде `log session show` можно указывать несколько *различных* критериев отбора, Например для вывода сессий, базирующихся на транспортном протоколе TCP, с IP-адресом сервера 192.168.169.126 и упорядоченных по возрастанию времени регистрации, следует выполнить команду:

```
fnpsh> log session show tproto=6 ipsrv=192.168.169.126 order=asc
```

3.4.53. log show – просмотр параметров подсистемы регистрации

```
log sh[ow]
```

Команда выводит на экран терминала параметры подсистемы регистрации, установленные в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> log show
Регистрация пакетов:                              включено
Регистрация ошибочных пакетов в сессиях:          отключено
Регистрация ошибочных пакетов в NAT:              отключено
Регистрация синхронизации по NTP:                 отключено
Выгрузка журналов регистрации по FTP:             отключено
    FTP-сервер:                                   10.234.28.1
    Путь на FTP-сервере:                          /fnplog/10.234.28.75
    Имя пользователя на FTP-сервере:              fnplog
Выгрузка системных сообщений по SYSLOG:           отключено
    SYSLOG-сервер:                                10.234.28.1
fnpsh>
```

3.4.54. log syslog show – просмотр системных сообщений

```
log sysl[og] sh[ow] [viewer={intern[al]|mor[e]|no}]
```

Параметры:

- `viewer` — режим просмотра данных командного интерфейса ССПТ-2:
  - ✔ `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.

По умолчанию используется режим просмотра данных, установленный по команде `system fnpsh viewer` (раздел 3.4.156, стр. 168)

Просмотреть текущий установленный режим просмотра данных можно по команде `system show` (раздел 3.4.162, стр. 173).

Команда выполняет просмотр сообщений, зарегистрированных локальным SYSLOG сервером ССПТ-2.

Системные сообщения – это текстовые строки, имеющие следующий формат:

```
<время_регистрации> fnp2 fnp[<PID>]: <имя_модуля>: <сообщение>
```

где

- `<время_регистрации>` – время регистрации системного сообщения SYSLOG сервером;
- `<PID>` – идентификатор процесса, отправивший данное сообщение SYSLOG серверу;
- `<имя_модуля>` – имя программного модуля ССПТ-2, отправившего данное сообщение;
- `<сообщение>` – текстовое сообщение.

Обновление списка системных сообщений выполняется операционной системой ССПТ-2 автоматически и не требует вмешательства администратора.

Системные сообщения всегда упорядочиваются в порядке возрастания времени их регистрации.

Для просмотра зарегистрированных событий используются клавиши и управляющие последовательности, перечисленные в таблице 3.6.

Таблица 3.6: Управление просмотром зарегистрированных системных сообщений

Управление	***Назначение***
<↑>	Переход к предыдущему системному сообщению
<↓>	Переход к следующему системному сообщению
<←>	Перемещение на одну позицию влево по строкам системных сообщений
<→>	Перемещение на одну позицию вправо по строкам системных сообщений
<Home>	Перемещение к первой позиции строк системных сообщений
<End>	Перемещение к последней позиции самой длинной строки системного сообщения, из тех что в данный момент видны на экране терминала
<Page Up>	Переход к предыдущей странице вывода строк системных сообщений
<Page Down>	Переход к следующей странице вывода строк системных сообщений
<Ctrl+B>	Переход к первому системному сообщению
<Ctrl+E>	Переход к последнему системному сообщению
<Ctrl+W>	Режим просмотра без горизонтальной прокрутки. В этом режиме осуществляется автоматический перенос строк, длина которых превышает ширину окна вывода данных.
<H>	Вывод подсказки по клавишам управления просмотром зарегистрированных системных сообщений (рисунок 3.51)

Управление	Назначение
<F10>, <Q>	Завершение выполнения команды

Пример вывода информации о зарегистрированных системных сообщениях приводится на рисунке 3.51.

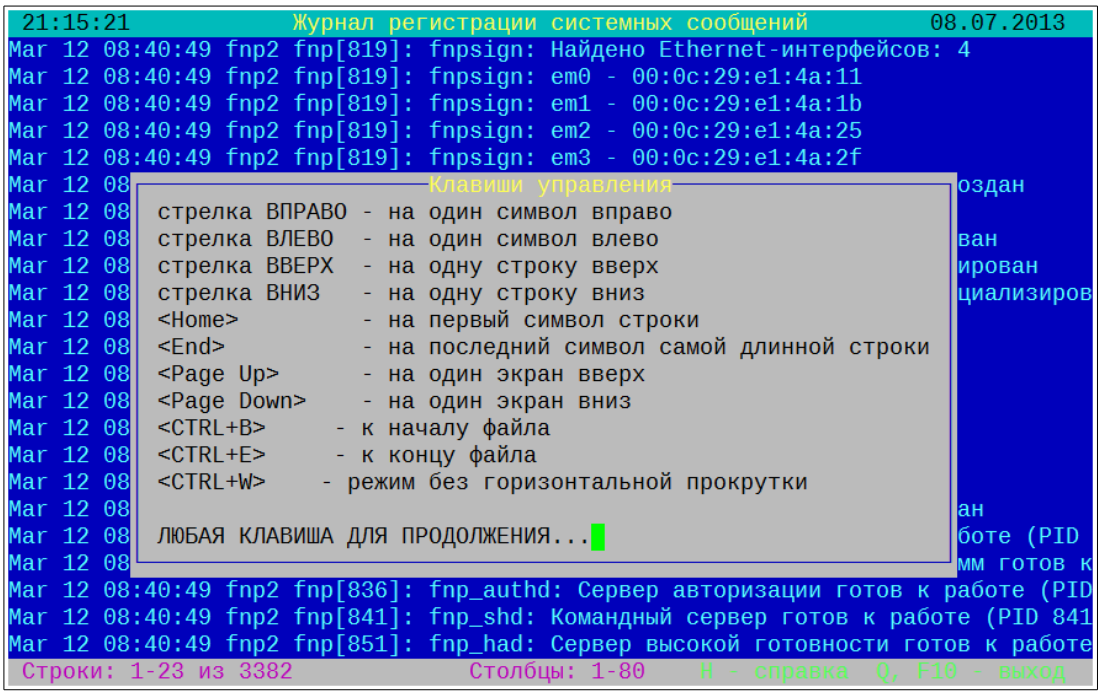

Рисунок 3.51: Просмотр системных сообщений

3.4.55. nat arp add – добавление записи в ARP таблицу

`nat arp add {<номер>|<имя>} <IP_адрес> <MAC_адрес>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- фильтрующий интерфейс, с которым будет связана добавляемая запись
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу;
- `<IP_адрес>` – IP-адрес узла, доступного через указанный фильтрующий интерфейс ССПТ-2;
- `<MAC_адрес>` – MAC-адрес сетевого адаптера узла, соответствующий указанному IP-адресу.

Команда добавляет новую запись в статическую ARP таблицу подсистемы трансляции сетевых адресов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Параметр `<IP_адрес>` указывается в формате, принятом для IP-адресов – `XXX.XXX.XXX.XXX`, где `XXX` – целое число в диапазоне от `0` до `255`.

Параметр `<MAC_адрес>` указывается в формате, принятом для MAC-адресов – `xx:xx:xx:xx:xx:xx`, где `xx` – шестнадцатеричное число в диапазоне от `00` до `ff`.

Статическая ARP таблица может содержать не более **256** записей.

Статическая ARP таблица не может содержать несколько записей с одинаковыми IP-адресами

Примеры:

```
fnpsh> nat arp add External 192.168.169.158 00:04:23:bd:0b:d1
FNPSH-I-3074-Новая запись добавлена в ARP таблицу
fnpsh>

fnpsh> nat arp add 0 192.168.169.158 00:04:23:bd:0b:d2
FNPSH-E-10DB-IP-адрес уже существует в ARP таблице (192.168.169.158)
fnpsh>
```

3.4.56. nat arp clear – очистка ARP таблицы

`nat arp cl[ear]`

Требуемые привилегии – **cfg** или **pf**.

Команда удаляет все записи из статической ARP таблицы подсистемы трансляции сетевых адресов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat arp clear
Очистить ARP-таблицу? (Y/N)  [N]: Y
FNPSH-I-3076-ARP таблица очищена
fnpsh>
```

3.4.57. nat arp delete – удаление записи из ARP таблицы

`nat arp del[ete] {{<номер>|<имя>}|<IP_адрес>|<MAC_адрес>}`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- фильтрующий интерфейс, с которым связана удаляемая запись
  - ✔ `<номер>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.;
  - ✔ `<имя>` – символическое имя, присвоенное фильтрующему интерфейсу;
- `<IP_адрес>` – IP-адрес, с которым связана удаляемая запись;
- `<MAC_адрес>` – MAC-адрес, с которым связана удаляемая запись.

Команда удаляет записи из статической ARP таблицы подсистемы трансляции сетевых адресов и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Режим удаления записей зависит от указанного параметра:

- если в качестве параметра указан фильтрующий интерфейс ССПТ-2, то из ARP таблицы будут удалены все записи, связанные с этим интерфейсом;
- если в качестве параметра указан IP-адрес, то из ARP таблицы будет удалена запись, связанная с этим IP-адресом;
- если в качестве параметра указан MAC-адрес, то из ARP таблицы будет удалена запись, связанная с этим MAC-адресом;

Примеры:

```
fnpsh> nat arp delete External
Удалить запись <External  192.168.169.158  00:04:23:bd:0b:d1>? (Y/N)  [N]: Y
FNPSH-I-3075-Запись удалена из ARP таблицы
Удалить запись <External  192.168.169.157  00:04:23:bd:0b:d2>? (Y/N)  [N]: Y
FNPSH-I-3075-Запись удалена из ARP таблицы
fnpsh>

fnpsh> nat arp delete 00:04:23:bd:0b:d1
Удалить запись <External  192.168.169.158  00:04:23:bd:0b:d1>? (Y/N)  [N]: Y
FNPSH-I-3075-Запись удалена из ARP таблицы
fnpsh>
```

```
fnpsh> nat arp delete 192.168.169.157
Удалить запись <External  192.168.169.157  00:04:23:bd:0b:d2>? (Y/N)  [N]: Y
FNPSH-I-3075-Запись удалена из ARP таблицы
fnpsh>
```

3.4.58. nat arp show – просмотр записей ARP-таблицы

```
nat arp sh[ow] [<критерии_отбора>]
```

Параметры:

- `<критерии_отбора>` – необязательный параметр, позволяющий выполнять просмотр только тех записей ARP-таблицы, которые удовлетворяют введенным критериям.

Команда выводит на экран терминала записи статической ARP-таблицы подсистемы трансляции сетевых адресов. Просмотр записей выполняется в соответствии с текущим режимом просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23).

Каждая запись ARP-таблицы состоит из следующих полей:

- символическое имя фильтрующего интерфейса ССПТ-2, с которым связана данная запись таблицы;
- IP-адрес узла сети, доступного через данный фильтрующий интерфейс;
- MAC-адрес сети, соответствующий данному IP-адресу.

Критерии отбора записей ARP-таблицы. Параметр `<критерии_отбора>` представляет собой список именованных пар, разделенных пробелом, вида:

```
<имя_критерия>=<значение>[ ...]
```

Не допускается указывать в списке один и тот же критерий отбора более одного раза. В результате выполнения команды будут отобраны записи ARP-таблицы, удовлетворяющие *всем критериям отбора, указанным в списке, в совокупности*.

При отсутствии критериев отбора команда `nat arp show` выводит все имеющиеся записи ARP-таблицы.

В списке критериев отбора записей ARP-таблицы параметр `<имя_критерия>` может принимать одно из следующих значений:

- `if` – отбор по фильтрующим интерфейсам;
- `ip` – отбор по IP-адресу;
- `mac` – отбор по MAC-адресу;
- `viewer` – режим просмотра данных командного интерфейса ССПТ-2.

Отбор по фильтрующим интерфейсам. Критерий `if` позволяет отобрать только те записи ARP-таблицы, которые привязаны к указанному фильтрующему интерфейсу. Критерий отбора имеют следующий синтаксис:

```
if={<имя_интерфейса>|<номер_интерфейса>}
```

где

- `<имя_интерфейса>` – символическое имя, присвоенное фильтрующему интерфейсу;
- `<номер_интерфейса>` – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): `0` – **Eth0**, `1` – **Eth1** и т. д.

Пример (просмотр записей ARP-таблицы, привязанных к фильтрующему интерфейсу с символическим именем `External`):

```
fnpsh> nat arp show if=External
```

Отбор по IP-адресу. Критерий `ip` позволяет отобрать только те записи ARP-таблицы, которые привязаны к указанному IP-адресу. Критерий отбора имеют следующий синтаксис:

```
ip=<IP_адрес>
```

Пример (просмотр записей ARP-таблицы, привязанных к IP-адресу `192.168.169.157`):

```
fnpsh> nat arp show ip=192.168.169.157
```

Отбор по MAC-адресу. Критерий `mac` позволяет отобрать только те записи ARP-таблицы, которые привязаны к указанному MAC-адресу. Критерий отбора имеют следующий синтаксис:

```
mac=<MAC_адрес>
```

Пример (просмотр записей ARP-таблицы, привязанных к MAC-адресу `00:04:23:bd:0b:d1`):

```
fnpsh> nat arp show mac=00:04:23:bd:0b:d1
```

Режим просмотра данных командного интерфейса ССПТ-2. Критерий `viewer` позволяет изменить режим просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23) на время выполнения команды `nat arp show`. Критерий отбора имеет следующий синтаксис:

```
viewer={intern[al]|mor[e]|no}
```

где

- `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.

По умолчанию используется режим просмотра данных, установленный по команде `system fnpsh viewer` (раздел 3.4.156, стр. 168)

Просмотреть текущий установленный режим просмотра данных можно по команде `system show` (раздел 3.4.162, стр. 173).

В команде `nat arp show` можно указывать несколько *различных* критериев отбора, Например для просмотра записей ARP-таблицы, привязанных к фильтрующему интерфейсу `External`, в режиме сплошного вывода данных следует выполнить команду:

```
fnpsh> nat arp show if=External viewer=no
Интерфейс          IP-адрес          MAC-адрес
External           192.168.169.158   00:04:23:bd:0b:d1
External           192.168.169.157   00:04:23:bd:0b:d2
fnpsh>
```

3.4.59. nat authentication disable – отключение режима аутентификации сетевых пользователей

```
nat aut[hentication] dis[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда отключает режим аутентификации сетевых пользователей и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Если на момент выполнения команды `nat authentication disable` режим аутентификации пользователей уже был отключен, то его состояние остается без изменений.

Пример:

```
fnpsh> nat authentication disable
Отключить аутентификацию пользователей? (Y/N)  [N]: Y
FNPSH-I-30BB-Аутентификация пользователей отключена
fnpsh>
```

```
fnpsh> nat authentication disable
FNPSH-W-2030-Аутентификация пользователей уже отключена
fnpsh>
```

3.4.60. nat authentication enable – включение режима аутентификации сетевых пользователей

`nat aut[hentication] en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда включает режим аутентификации сетевых пользователей и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Режим аутентификации сетевых пользователей активизируется только после включения режима трансляции сетевых адресов NAT – команда `nat enable` (приложение 3.4.63, стр. 113).

Если на момент выполнения команды `nat authentication enable` режим аутентификации пользователей уже был включен, то его состояние остается без изменений.

Пример:

```
fnpsh> nat authentication enable
FNPSH-I-30BA-Аутентификация пользователей включена
fnpsh>

fnpsh> nat authentication enable
FNPSH-W-202F-Аутентификация пользователей уже включена
fnpsh>
```

3.4.61. nat authentication timeout – установка тайм-аута неактивности для сетевых пользователей

`nat aut[hentication] timeo[ut] <тайм_аут>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<тайм_аут>` – новое значение тайм-аута неактивности для сетевых пользователей.

Команда устанавливает новое значение тайм-аута неактивности для сеансов работы сетевых пользователей и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию тайм-аут неактивности для сетевых пользователей составляет **600** секунд (10 минут).

Тайм-аут неактивности для сетевых пользователей может быть изменен в пределах от **10** до **864000** (10 суток) секунд.

Просмотреть текущее значение тайм-аута для сетевых пользователей можно, используя команду `nat show` (приложение 3.4.86, стр. 123).

Пример:

```
fnpsh> nat authentication timeout 3600
FNPSH-I-30C2-Тайм-аут неактивности сетевых пользователей изменен
fnpsh>
```

3.4.62. nat disable – отключение режима NAT

`nat dis[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда отключает режим трансляции сетевых адресов (NAT) пакетного фильтра и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh>
```

3.4.63. nat enable – включение режима NAT

`nat en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда включает режим трансляции сетевых адресов (NAT) пакетного фильтра и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Перед включением режима NAT необходимо выполнить следующие установки:

- установка IP-адреса внутреннего интерфейса NAT – команда `nat private ip` (приложение 3.4.72, стр. 117);
- установка IP-адреса внешнего интерфейса NAT – команда `nat public ip` (приложение 3.4.76, стр. 119);
- установка шлюза по умолчанию для внешнего интерфейса NAT – команда `nat public gateway` (приложение 3.4.75, стр. 118);
- добавление в статическую ARP таблицу записи об IP и MAC-адресах шлюза по умолчанию для внешнего интерфейса NAT – команда `nat arp add` (приложение 3.4.55, стр. 108).

Примеры:

```
fnpsh> nat enable
FNPSH-E-10D5-Недопустимые параметры NAT (адреса внутреннего и внешнего интерфейса, шлюз по
умолчанию)
fnpsh>

fnpsh> nat enable
FNPSH-I-3068-NAT включен
fnpsh>
```

3.4.64. nat key add – добавление новой пары ключей аутентификации сетевых пользователей

`nat key add <IP_адрес>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<IP_адрес>` – IP-адрес узла сети, который используется сетевым пользователем как IP-адрес отправителя запроса аутентификации и которому будет соответствовать создаваемая пара ключей.

Команда создает новую пару ключей, соответствующую указанному IP-адресу, и используемую при кодировании запроса аутентификации сетевого пользователя, отправляемого с указанного IP-адреса.

Созданная пара ключей должна быть передана на компьютер сетевого пользователя, которому назначен соответствующий IP-адрес.

Для выгрузки ключей аутентификации сетевых пользователей администратору необходимо воспользоваться утилитой `fnpld` из пакета служебных утилит ССПТ-2 *FNPUtils*.

Пример:

```
fnpsh> nat key add 172.20.0.35
```

```
FNPSH-I-30C4-Новая запись добавлена в файл ключей аутентификации (172.20.0.35)
fnpsh>
```

3.4.65. nat key delete – удаление существующей пары ключей аутентификации сетевых пользователей

`nat key del[ete] <IP_адрес>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<IP_адрес>` – IP-адрес узла сети, которому соответствует удаляемая пара ключей.

После удаления пары ключей работа сетевых пользователей с компьютера, которому назначен соответствующий IP-адрес, автоматически запрещается.

Пример:

```
fnpsh> nat key delete 172.20.0.35
Удалить запись? (Y/N)  [N]: Y
FNPSH-I-30C5-Запись удалена из файла ключей аутентификации (172.20.0.35)
fnpsh>
```

3.4.66. nat key show – просмотр существующих пар ключей аутентификации сетевых пользователей

`nat key sh[ow] [<IP_адрес>]`

Параметры:

- `<IP_адрес>` – IP-адрес узла сети, для которого необходимо просмотреть соответствующую ему пару ключей. Необязательный параметр, если он опущен, то выполняется просмотр всех существующих пар ключей аутентификации сетевых пользователей.

Команда выполняет просмотр всех пар ключей аутентификации сетевых пользователей, либо только пары ключей, соответствующей указанному в параметре команды IP-адресу.

Просмотр параметров конфигурации выполняется в соответствии с текущим режимом просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23).

Пример:

```
fnpsh> system fnpsh viewer no
FNPSH-I-3087-Режим просмотра изменен

fnpsh> nat key show
Файл ключей аутентификации:

Всего записей: 2

------------------------------------------------------------
IP-адрес: 192.168.169.123

Закрытый ключ: 3D8A6CB4EF0EFE8E51040B8B1E909944CC066AC42A7C545062DE3AAA22179908

Открытый ключ:
0112DBF220008543C798BBB782C5126790DA07CE678A52B9134E63BA9B4450273DB67AFB6D7ADCFDC590D4A7FA
067AA3421D713EC7F1F7E97188339AA80ED68F

------------------------------------------------------------
IP-адрес: 172.20.0.35

Закрытый ключ: 5F8DCAF42507DFC1756AA0C0F81EF503E11D17743324F52CB0EBEEB7D74C5593

Открытый ключ:
7EB9A0171882F89579146D57F6DE4DE7752651AF0C80E064B735225B0257A8C43B38A33794304343BD9DDFC346
6E8BEDAACC7E2E8EEE56F6B92B63798F20C4C9
fnpsh>
```

```
fnpsh> nat key show 172.20.0.35
Файл ключей аутентификации:

Всего записей: 1

------------------------------------------------------------
IP-адрес: 172.20.0.35

Закрытый ключ: 5F8DCAF42507DFC1756AA0C0F81EF503E11D17743324F52CB0EBEEB7D74C5593

Открытый ключ:
7EB9A0171882F89579146D57F6DE4DE7752651AF0C80E064B735225B0257A8C43B38A33794304343BD9DDFC346
6E8BEDAACC7E2E8EEE56F6B92B63798F20C4C9
fnpsh>
```

3.4.67. nat key update – изменение существующей пары ключей аутентификации сетевых пользователей

`nat key upd[ate] <IP_адрес>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<IP_адрес>` – IP-адрес узла сети, которому соответствует изменяемая пара ключей.

Команда обновляет пару ключей аутентификации сетевого пользователя, соответствующую указанному в параметре команды IP-адресу.

Измененная пара ключей должна быть передана на компьютер сетевого пользователя, которому назначен соответствующий IP-адрес.

Для выгрузки ключей аутентификации сетевых пользователей администратору необходимо воспользоваться утилитой `fnpld` входящей в состав пакета сервисных утилит FNPUtils. Руководство по установке и использованию утилиты `fnpld` приводится в документе "***Межсетевой экран ССПТ-2. Утилиты. Руководство пользователя***".

Документ "***Межсетевой экран ССПТ-2. Утилиты. Руководство пользователя***" располагается на компакт-диске (CD-ROM), входящем в комплект поставки ССПТ-2 (`docs/fnputils_ag-1.4.0.pdf`, путь к файлу указан относительно корня файловой системы компакт-диска).

Пример:

```
fnpsh> nat key update 172.20.0.35
Обновить запись? (Y/N)  [N]: Y
FNPSH-I-30C6-Запись изменена в файле ключей аутентификации (172.20.0.35)
fnpsh>
```

3.4.68. nat log disable – отключение регистрации пакетов, удаляемых NAT

`nat log dis[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда отключает регистрацию пакетов, отбрасываемых подсистемой трансляции сетевых адресов (NAT) и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat log disable
FNPSH-I-3071-Регистрация пакетов, удаленных NAT, отключена
fnpsh>
```

3.4.69. nat log enable – включение регистрации пакетов, удаляемых NAT

`nat log en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда включает регистрацию пакетов, удаляемых подсистемой трансляции сетевых адресов (NAT) и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

В режиме NAT пакеты могут удаляться из-за невозможности их передачи на выходные фильтрующие интерфейсы. Например, ARP пакеты не могут быть переданы из внутренней сети во внешнюю сеть и демилитаризованную зону.

Пример:

```
fnpsh> nat log enable
FNPSH-I-3070-Регистрация пакетов, удаленных NAT, включена
fnpsh>
```

3.4.70. nat port – установка диапазона портов NAT

`nat port <порт_мин>-<порт_макс>`

Требуемые привилегии – **cfg** или **pf**.

Параметры

- `<порт_мин>` – нижняя граница диапазона портов NAT;
- `<порт_макс>` – верхняя граница диапазона портов NAT.

Команда изменяет диапазон номеров портов, используемый для трансляции номера порта обрабатываемого пакета, передаваемого из внутренней сети во внешнюю сеть или демилитаризованную зону. Соответственно изменяются настройки текущей конфигурации ССПТ-2.

По умолчанию используется диапазон номеров портов 45000-60000.

Трансляция номеров портов выполняется только для TCP и UDP пакетов.

Диапазон номеров портов может устанавливаться в пределах от **30000** до **65535**. Минимально допустимая ширина диапазона портов (разность между верхней и нижней границами) составляет **10000**.

Перед изменением диапазона номеров портов режим NAT должен быть отключен – команда `nat disable` (приложение 3.4.62, стр. 112).

После изменения диапазона портов NAT необходимо перезапустить пакетный фильтр ССПТ-2 – команда `filter restart` (приложение 3.4.8, стр. 63).

Примеры:

```
fnpsh> nat port 30000-40000
FNPSH-W-2029-Необходимо отключить NAT
fnpsh>

fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh>nat port 30000-40000
Изменить диапазон портов NAT? (Y/N)  [N]: Y
FNPSH-I-306A-Диапазон портов NAT изменен. Необходимо перезапустить пакетный фильтр
fnpsh>
```

3.4.71. nat private delete – удаление параметров внутреннего интерфейса NAT

`nat priva[te] del[ete]`

Требуемые привилегии – **cfg** или **pf**.

Команда удаляет назначенный IP-адрес с внутреннего интерфейса NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Перед удалением параметров внутреннего интерфейса режим NAT должен быть отключен – команда `nat disable` (приложение 3.4.62, стр. 112).

Примеры:

```
fnpsh> nat private delete
FNPSH-W-2029-Необходимо отключить NAT
fnpsh>

fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh> nat private delete
Удалить IP-адрес внутреннего интерфейса? (Y/N)  [N]: Y
FNPSH-I-306F-IP-адрес внутреннего интерфейса NAT удален
fnpsh>
```

3.4.72. nat private ip – установка IP-адреса внутреннего интерфейса NAT

`nat priva[te] ip <IP_адрес/маска>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<IP_адрес/маска>` – IP-адрес и маска подсети, которые будут назначены внутреннему интерфейсу NAT.

Команда назначает IP-адрес и маску подсети внутреннему интерфейсу NAT и сохраняет эти настройки в текущей конфигурации ССПТ-2.

Установленный IP-адрес внутреннего интерфейса NAT должен выступать в качестве IP-адреса шлюза по умолчанию для узлов внутренней сети.

IP-адрес внутреннего интерфейса NAT является виртуальным адресом, используемым только пакетным фильтром ССПТ-2 для реализации режима NAT. Фильтрующие интерфейсы ССПТ-2 при этом продолжают функционировать в безадресном режиме.

Перед установкой IP-адреса внутреннего интерфейса режим NAT должен быть отключен – команда `nat disable` (приложение 3.4.62, стр. 112).

Примеры:

```
fnpsh> nat private ip 192.168.169.190/255.255.255.224
FNPSH-W-2029-Необходимо отключить NAT
fnpsh>

fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh> nat private ip 192.168.169.190/255.255.255.224
FNPSH-I-306E-IP-адрес внутреннего интерфейса NAT изменен
fnpsh>
```

3.4.73. nat private mac – установка MAC-адреса внутреннего интерфейса NAT

`nat priva[te] mac <MAC_адрес>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<MAC_адрес>` – MAC-адрес, который будет назначен внутреннему интерфейсу NAT.

Команда назначает MAC-адрес внутреннему интерфейсу NAT и сохраняет эти настройки в текущей конфигурации ССПТ-2.

По умолчанию внутреннему интерфейсу NAT назначен MAC-адрес `02:01:01:01:01:02`.

Перед установкой MAC-адреса внутреннего интерфейса режим NAT должен быть отключен – команда `nat disable` (приложение 3.4.62, стр. 112).

Параметр `<MAC_адрес>` указывается в формате, принятом для MAC-адресов – `xx:xx:xx:xx:xx:xx`, где `xx` – шестнадцатеричное число в диапазоне от `00` до `ff`.

Примеры:

```
fnpsh> nat private mac 03:12:01:03:03:03
FNPSH-W-2029-Необходимо отключить NAT
fnpsh>

fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh> nat private mac 03:12:01:03:03:03
FNPSH-I-3072-MAC-адрес внутреннего интерфейса NAT изменен
fnpsh>
```

3.4.74. nat public delete – удаление параметров внешнего интерфейса NAT

`nat pub[lic] del[ete]`

Требуемые привилегии – **cfg** или **pf**.

Команда удаляет назначенный IP-адрес с внешнего интерфейса NAT, IP-адрес шлюза по умолчанию для внешнего интерфейса NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Перед удалением параметров внешнего интерфейса режим NAT должен быть отключен – команда `nat disable` (приложение 3.4.62, стр. 112).

Примеры:

```
fnpsh> nat public delete
FNPSH-W-2029-Необходимо отключить NAT
fnpsh>

fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh> nat public delete
Удалить настройки внешнего интерфейса NAT? (Y/N)  [N]: Y
FNPSH-I-306C-IP-адреса внешнего интерфейса  NAT и шлюза удалены
fnpsh>
```

3.4.75. nat public gateway – установка шлюза по умолчанию для внешнего интерфейса NAT

`nat pub[lic] gate[way] <IP_адрес>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<IP_адрес>` – IP-адрес шлюза по умолчанию для внешнего интерфейса NAT.

Команда устанавливает IP-адрес шлюза по умолчанию для внешнего интерфейса NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Перед установкой IP-адреса шлюза по умолчанию для внешнего интерфейса режим NAT должен быть отключен – команда `nat disable` (приложение 3.4.62, стр. 112).

IP-адреса шлюза по умолчанию и внешнего интерфейса NAT должны находиться в одной IP-подсети.

Примеры:

```
fnpsh> nat public gateway 192.168.169.158
FNPSH-W-2029-Необходимо отключить NAT
fnpsh>

fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh> nat public gateway 192.168.169.158
FNPSH-I-306D-Адрес шлюза внешнего интерфейса NAT изменен
fnpsh>
```

3.4.76. nat public ip – установка IP-адреса внешнего интерфейса NAT

`nat pub[lic] ip <IP_адрес/маска>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<IP_адрес/маска>` – IP-адрес и маска подсети, которые будут назначены внешнему интерфейсу NAT.

Команда назначает IP-адрес и маску подсети внешнему интерфейсу NAT и сохраняет эти настройки в текущей конфигурации ССПТ-2.

IP-адрес внешнего интерфейса NAT является виртуальным адресом, используемым только пакетным фильтром ССПТ-2 для реализации режима NAT. Фильтрующие интерфейсы ССПТ-2 при этом продолжают функционировать в безадресном режиме.

Перед установкой IP-адреса внешнего интерфейса режим NAT должен быть отключен – команда `nat disable` (приложение 3.4.62, стр. 112).

Примеры:

```
fnpsh> nat public ip 192.168.169.129/255.255.255.224
FNPSH-W-2029-Необходимо отключить NAT
fnpsh>

fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh> nat public ip 192.168.169.129/255.255.255.224
FNPSH-I-306B-IP-адрес внешнего интерфейса NAT изменен
fnpsh>
```

3.4.77. nat public mac – установка MAC-адреса внешнего интерфейса NAT

`nat pub[lic] mac <MAC_адрес>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<MAC_адрес>` – MAC-адрес, который будет назначен внешнему интерфейсу NAT.

Команда назначает MAC-адрес внешнему интерфейсу NAT и сохраняет эти настройки в текущей конфигурации ССПТ-2.

По умолчанию внешнему интерфейсу NAT назначен MAC-адрес `02:01:01:01:01:01`.

Перед установкой MAC-адреса внешнего интерфейса режим NAT должен быть отключен – команда `nat disable` (приложение 3.4.62, стр. 112).

Параметр `<MAC_адрес>` указывается в формате, принятом для MAC-адресов – `xx:xx:xx:xx:xx:xx`, где `xx` – шестнадцатеричное число в диапазоне от `00` до `ff`.

Примеры:

```
fnpsh> nat public mac 03:12:01:02:02:02
FNPSH-W-2029-Необходимо отключить NAT
fnpsh>

fnpsh> nat disable
Отключить NAT? (Y/N)  [N]: Y
FNPSH-I-3069-NAT отключен
fnpsh>nat public mac 03:12:01:02:02:02
FNPSH-I-3072-MAC-адрес внешнего интерфейса NAT изменен
fnpsh>
```

3.4.78. nat redirect add – добавление записи в таблицу переадресации NAT

`nat red[irect] add <протокол> <внеш_порт> <IP_адрес> [<внутр_порт>]`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<протокол>` — протокол транспортного уровня. Допускаются следующие значения:
  - ✔ `tcp` — для указания протокола TCP;
  - ✔ `udp` — для указания протокола UDP;
- `<внеш_порт>` – номер прикладного порта, на который ожидаются запросы из внешней сети и демилитаризованной зоны (DMZ) для переадресации во внутреннюю сеть;
- `<IP_адрес>` – IP-адрес узла во внутренней сети, на который переадресуются запросы, поступающие из внешней сети и DMZ;
- `<внутр_порт>` – номер прикладного порта узла во внутренней сети с указанным IP-адресом, на который переадресуются запросы из внешней сети и DMZ.

Параметр `<внутр_порт>` необязательный. По умолчанию ему присваивается значение параметра `<внеш_порт>`.

Команда добавляет новую запись в таблицу переадресации NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

В режиме NAT все запросы, поступающие из внешней сети и DMZ на прикладной порт с номером `<внеш_порт>` (*внешний порт*), переадресуются во внутреннюю сеть на IP-адрес `<IP_адрес>` и номер прикладного порта `<внутр_порт>` (*внутренний порт*).

Для правильной работы функции переадресации запросов необходимо добавить записи в статическую ARP таблицу – команда `nat arp add` (приложение 3.4.55, стр. 108):

- для всех узлов внутренней сети на которые переадресуются запросы;
- для всех узлов внешней сети и DMZ, являющихся источниками запросов к прикладным сервисам, расположенным во внутренней сети.

Таблица переадресации NAT может содержать не более **16** записей.

Допустимые значения параметров `<внеш_порт>`, `<внутр_порт>` – целые числа в диапазоне от **1** до **65535**.

Переадресация запросов выполняется **только для протокола TCP**.

Примеры:

- переадресация TCP-запросов на порт с номером `6443` на IP-адрес `192.168.169.189`, порт `443`:

```
fnpsh> nat redirect add tcp 6443 192.168.169.189 443
FNPSH-I-3077-Новая запись добавлена в таблицу переадресации
fnpsh>
```

- переадресация TCP-запросов на порт с номером `80` на IP-адрес `192.168.169.189`, порт `80`:

```
fnpsh> nat redirect add tcp 80 192.168.169.189
FNPSH-I-3077-Новая запись добавлена в таблицу переадресации
fnpsh>
```

3.4.79. nat redirect clear – очистка таблицы переадресации NAT

`nat red[irect] cl[ear]`

Требуемые привилегии – **cfg** или **pf**.

Команда удаляет все записи из таблицы переадресации NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat redirect clear
Очистить таблицу переадресации (Y/N)  [N]: Y
FNPSH-I-3079-Таблица переадресации очищена
fnpsh>
```

3.4.80. nat redirect delete – удаление записи из таблицы переадресации

`nat red[irect] del[ete] <протокол> <внеш_порт>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<протокол>` — протокол транспортного уровня. Допускаются следующие значения:
  - ✔ `tcp` — для указания протокола TCP;
  - ✔ `udp` — для указания протокола UDP;
- `<внеш_порт>` – номер прикладного порта, на который ожидаются запросы из внешней сети и демилитаризованной зоны (DMZ) для переадресации во внутреннюю сеть;

Команда удаляет запись из таблицы переадресации NAT, содержащую указанное значение внешнего прикладного порта, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat redirect delete 6443
Удалить запись <6443  192.168.169.189  443>? (Y/N)  [N]: Y
FNPSH-I-3078-Запись удалена из таблицы переадресации
fnpsh>
```

3.4.81. nat redirect dmz disable – отключение переадресации с интерфейсов DMZ

```
nat red[irect] dmz dis[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда запрещает переадресацию запросов с фильтрующих интерфейсов DMZ во внутреннюю сеть NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat redirect dmz disable
FNPSH-I-307B-Переадресация из DMZ отключена
fnpsh>
```

3.4.82. nat redirect dmz enable – включение переадресации с интерфейсов DMZ

```
nat red[irect] dmz en[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда разрешает переадресацию запросов с фильтрующих интерфейсов DMZ во внутреннюю сеть NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat redirect dmz enable
FNPSH-I-307A-Переадресация из DMZ включена
fnpsh>
```

3.4.83. nat redirect public disable – отключение переадресации с внешнего интерфейса

```
nat red[irect] pub[lic] dis[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда запрещает переадресацию запросов с внешнего интерфейса во внутреннюю сеть NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat redirect public disable
FNPSH-I-307D-Переадресация с внешнего интерфейса отключена
fnpsh>
```

3.4.84. nat redirect public enable – включение переадресации с внешнего интерфейса

```
nat red[irect] pub[lic] en[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда разрешает переадресацию запросов с внешнего интерфейса во внутреннюю сеть NAT и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> nat redirect public enable
FNPSH-I-307C-Переадресация с внешнего интерфейса включена
fnpsh>
```

3.4.85. nat redirect show – просмотр записей таблицы переадресации NAT

```
nat red[irect] sh[ow]
```

Команда выводит на экран терминала содержимое таблицы переадресации NAT.

Вывод таблицы переадресации содержит три столбца:

- `Внешний порт` – номер прикладного порта, на который ожидаются запросы из внешней сети и демилитаризованной зоны (DMZ) для переадресации во внутреннюю сеть;
- `Внутренний IP-адрес` – IP-адрес узла во внутренней сети, на который переадресуются запросы, поступающие из внешней сети и DMZ;
- `Внутренний порт` – номер прикладного порта узла во внутренней сети с указанным IP-адресом, на который переадресуются запросы из внешней сети и DMZ.

Пример:

```
fnpsh> nat redirect show
Протокол   Внешний порт   Внутренний IP-адрес   Внутренний порт
     tcp             80       192.168.169.189                80
     tcp           6443       192.168.169.189               443
fnpsh>
```

3.4.86. nat show – просмотр параметров NAT

`nat sh[ow]`

Команда выводит на экран терминала настройки параметров текущей конфигурации ССПТ-2, используемые в пакетном фильтре для режима трансляции сетевых адресов.

Для обозначения фильтрующих интерфейсов используются их символические имена.

Пример:

```
fnpsh> nat show
Трансляция сетевых адресов (NAT):       включено
Регистрация отброшенных пакетов:        включено
Аутентификация пользователей:                   включено
Тайм-аут неактивности пользователей(сек):       600
Диапазон портов:                        30000-40000
Внешний интерфейс:                      External
    MAC-адрес:                          03:12:01:02:02:02
    IP-адрес:                           192.168.169.129
    Маска подсети:                      255.255.255.224
    IP-адрес шлюза по умолчанию:        192.168.169.158
    Переадресация:                      включено
Внутренний интерфейс:                   Internal
    MAC-адрес:                          03:12:01:03:03:03
    IP-адрес:                           192.168.169.190
    Маска подсети:                      255.255.255.224
Интерфейсы DMZ:                         Mirror
    Переадресация:                      включено
fnpsh>
```

3.4.87. nat user add – добавление нового сетевого пользователя

`nat us[er] add <имя> <MAC_адрес> <IP_адрес> <интерфейсы> <комментарий>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<имя>` – имя нового сетевого пользователя;
- `<MAC_адрес>` – ограничение доступа по MAC-адресу источника запроса аутентификации сетевого пользователя. Если указано ключевое слово `any`, то ограничение доступа по MAC-адресу отсутствует;
- `<IP_адрес>` – ограничение доступа по IP-адресу источника запроса аутентификации сетевого пользователя. Если указано ключевое слово `any`, то ограничение доступа по IP-адресу отсутствует;

- <интерфейсы> – ограничение доступа по фильтрующим интерфейсам ССПТ-2, на которых может быть получен запрос аутентификации сетевого пользователя. Если указано ключевое слово any, то ограничение доступа по фильтрующим интерфейсам отсутствует;
- <комментарий> – комментарий к сетевому пользователю.

Команда добавляет нового сетевого пользователя с указанными именем, ограничениями доступа и комментарием.

Добавлять нового сетевого пользователя имеет право только пользователь ССПТ-2 admin.

В ССПТ-2 существуют ограничения на формат имени сетевого пользователя:

- длина имени пользователя – от **2** до **128** символов;
- допустимые символы:
  - ✔ первый символ – **строчные латинские символы** (a-z) и **цифры** (0-9);
  - ✔ последующие символы – **строчные латинские символы** (a-z), **цифры** (0-9) и символы '_' (подчеркивание), '.' (точка), '-' (дефис), '@'.

В ССПТ-2 существуют ограничения на формат пароля сетевого пользователя:

- длина пароля – от **6** до **128** символов;
- допустимые символы – только **печатаемые ASCII-символы**;
- пароль пользователя является регистрово-зависимым;

В ССПТ-2 существуют ограничения на комментарий сетевого пользователя:

- длина комментария – не более **31** символа;
- допустимые символы – только **печатаемые ASCII-символы**;
- в команде строка комментария может быть окружена символами кавычек ("").

Ограничения доступа (MAC-адрес, IP-адрес, список фильтрующих интерфейсов):

- параметр <MAC_адрес> имеет один из следующих форматов:
  - ✔ XX:XX:XX:XX:XX:XX или XXXXXXXXXXXX, где X – шестнадцатеричная цифра. Например, 00:e0:75:90:da:e0 или 00e07590dae0;
- параметр <IP_адрес> имеет следующий формат:
  - ✔ XXX.XXX.XXX.XXX, где XXX – целое число в диапазоне от 0 до 255. Например, 172.20.0.35;
- параметр <интерфейсы> представляет собой список фильтрующих интерфейсов ССПТ-2 и имеет следующий формат:
  - ✔ {<имя_интерфейса>|<номер_интерфейса>}[,...], где <имя_интерфейса> - символическое имя, присвоенное фильтрующему интерфейсу; <номер_интерфейса> - порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): 0 – **Eth0**, 1 – **Eth1** и т. д.

Допускается указание пустого комментария к сетевому пользователю. Для этого необходимо в командной строке в позиции комментария ввести две кавычки подряд – "".

Команда запросит ввод пароля для нового сетевого пользователя. Пароль необходимо вводить дважды, чтобы исключить опечатки при вводе пароля с клавиатуры. Ввод паролей на терминале не отображается.

Примеры:

- добавление нового сетевого пользователя без ограничений доступа:

```
fnpsh> nat user add nuser1 any any any "Network user #1"
Новый пароль:
```

```
Новый пароль повторно:
Параметры сетевого пользователя:
  Имя пользователя: nuser1 (Network user #1)
  Ограничения доступа:
    MAC адрес: any
    IP адрес: any
    Фильтрующие интерфейсы: any
FNPSH-I-301D-Новый сетевой пользователь добавлен (nuser1)
fnpsh>
```

- добавление нового сетевого пользователя с ограничениями доступа по IP-адресу и фильтрующим интерфейсам и с пустым комментарием:

```
fnpsh> nat user add nuser2 any 172.20.0.35 Internal,2 ""
Новый пароль:
Новый пароль повторно:
Параметры сетевого пользователя:
  Имя пользователя: nuser2 ()
  Ограничения доступа:
    MAC адрес: any
    IP адрес: 172.20.0.35
    Фильтрующие интерфейсы: Internal,DMZ
FNPSH-I-301D-Новый сетевой пользователь добавлен (nuser2)
fnpsh>
```

- добавление нового сетевого пользователя с ограничением доступа по MAC-адресу:

```
fnpsh> nat user add nuser3 00:e0:75:90:da:e0 any any "Network user #3"
Новый пароль:
Новый пароль повторно:
  Имя пользователя: nuser3 (Network user #3)
  Ограничения доступа:
    MAC адрес:  00:e0:75:90:da:e0
    IP адрес: any
    Фильтрующие интерфейсы: any
FNPSH-I-301D-Новый сетевой пользователь добавлен (nuser3)
fnpsh>
```

3.4.88. nat user clear – сброс активного сетевого пользователя

`nat us[er] clear <имя>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<имя>` – имя активного сетевого пользователя.

Команда сбрасывает активного пользователя, имя которого указано в параметре команды.

Сбрасывать активных сетевых пользователей имеет право только пользователь ССПТ-2 `admin`.

Пример:

```
fnpsh> nat user clear nuser3
Сбросить сетевого пользователя? (Y/N)  [N]: Y
FNPSH-I-30BF-Сетевой пользователь сброшен (nuser3)
fnpsh>
```

3.4.89. nat user delete – удаление сетевого пользователя

`nat us[er] del[ete] <имя>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<имя>` – имя существующего сетевого пользователя.

Команда удаляет сетевого пользователя.

Удалять сетевых пользователей имеет право только пользователь ССПТ-2 admin.

Пример:

```
fnpsh> nat user delete nuser3
Удалить сетевого пользователя? (Y/N)  [N]: Y
FNPSH-I-30BC-Пользователь удален (nuser3)
fnpsh>
```

3.4.90. nat user disable – отключение сетевого пользователя

```
nat us[er] dis[able] <имя>
```

Требуемые привилегии – **user** (только пользователь admin).

Параметры:

- <имя> – имя существующего сетевого пользователя.

Команда отключает существующего сетевого пользователя без удаления его учетной записи, запрещая ему последующую работу при включенном режиме аутентификации сетевых пользователей.

Отключать сетевых пользователей имеет право только пользователь ССПТ-2 admin.

Пример:

```
fnpsh> nat user disable nuser2
Отключить пользователя? (Y/N)  [N]: Y
FNPSH-I-30BE-Сетевой пользователь отключен (nuser2)
fnpsh>
```

3.4.91. nat user enable – включение сетевого пользователя

```
nat us[er] en[able] <имя>
```

Требуемые привилегии – **user** (только пользователь admin).

Параметры:

- <имя> – имя существующего сетевого пользователя.

Команда включает существующего сетевого пользователя, разрешая ему последующую работу при включенном режиме аутентификации сетевых пользователей.

Включать сетевых пользователей имеет право только пользователь ССПТ-2 admin.

Пример:

```
fnpsh> nat user enable nuser2
FNPSH-I-30BD-Сетевой пользователь включен (nuser2)
fnpsh>
```

3.4.92. nat user edit – изменение параметров сетевого пользователя

```
nat us[er] ed[it] <имя> <MAC_адрес> <IP_адрес> <интерфейсы>
<комментарий>
```

Требуемые привилегии – **user** (только пользователь admin).

Параметры:

- <имя> – имя существующего сетевого пользователя;
- <MAC_адрес> – ограничение доступа по MAC-адресу источника запроса аутентификации сетевого пользователя. Если указано ключевое слово any, то ограничение доступа по MAC-адресу отсутствует;
- <IP_адрес> – ограничение доступа по IP-адресу источника запроса аутентификации сетевого пользователя. Если указано ключевое слово any, то ограничение доступа по IP-адресу отсутствует;
- <интерфейсы> – ограничение доступа по фильтрующим интерфейсам ССПТ-2, на которых может быть получен запрос аутентификации сетевого пользователя. Если указано ключевое слово any, то ограничение доступа по фильтрующим интерфейсам отсутствует;
- <комментарий> – комментарий к сетевому пользователю.

Команда изменяет ограничения доступа и комментарий для существующего сетевого пользователя с указанными именем.

Изменять параметры сетевого пользователя имеет право только пользователь ССПТ-2 admin.

В ССПТ-2 существуют ограничения на комментарий сетевого пользователя:

- длина комментария – не более **31** символа
- допустимые символы – только **печатаемые ASCII-символы**;
- в команде строка комментария может быть окружена символами кавычек ("").

Ограничения доступа (MAC-адрес, IP-адрес, список фильтрующих интерфейсов):

- параметр <MAC_адрес> имеет один из следующих форматов:
  - ✔ XX:XX:XX:XX:XX:XX или XXXXXXXXXXXX, где X – шестнадцатеричная цифра. Например, 00:e0:75:90:da:e0 или 00e07590dae0;
- параметр <IP_адрес> имеет следующий формат:
  - ✔ XXX.XXX.XXX.XXX, где XXX – целое число в диапазоне от 0 до 255. Например, 172.20.0.35;
- параметр <интерфейсы> представляет собой список фильтрующих интерфейсов ССПТ-2 и имеет следующий формат:
  - ✔ {<имя_интерфейса>|<номер_интерфейса>}[,...], где <имя_интерфейса> - символическое имя, присвоенное фильтрующему интерфейсу; <номер_интерфейса> - порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): 0 – **Eth0**, 1 – **Eth1** и т. д.

Допускается указание пустого комментария к сетевому пользователю. Для этого необходимо в командной строке в позиции комментария ввести две кавычки подряд – "".

Примеры:

```
fnpsh> nat user edit nuser2 any 172.20.0.36 DMZ "Network user #2"
Параметры сетевого пользователя:
  Имя пользователя: nuser2 (Network user #2)
  Ограничения доступа:
    MAC-адрес: any
    IP-адрес: 172.20.0.36
    Фильтрующие интерфейсы: DMZ

Изменить параметры сетевого пользователя? (Y/N)  [N]: y
FNPSH-I-30C3-Параметры сетевого пользователя изменены (nuser2)
fnpsh>
```

3.4.93. nat user list – просмотр списка существующих сетевых пользователей

```
nat us[er] lis[t]
```

Команда выводит на экран терминала общее количество существующих сетевых пользователей. Список сетевых пользователей выводится в виде таблицы, содержащей следующие поля:

- `Пользователь` – имя сетевого пользователя;
- `IP-адрес` – ограничение доступа по IP-адресу;
- `MAC-адрес` – ограничение доступа по MAC-адресу;
- `Интерфейс` – ограничение доступа по списку фильтрующих интерфейсов ССПТ-2;
- `Комментарий` – комментарий к сетевому пользователю.

Неактивные сетевые пользователи отмечаются в таблице символом дефиса ('-'), расположенным непосредственно перед именем пользователя.

Пример:

```
fnpsh> nat user list
Сетевых пользователей: 4 (Неактивные сетевые пользователи отмечены знаком '-')

 Пользователь IP-адрес      MAC-адрес    Интерфейс Комментарии
 hoha         любой         af04ff07b3ff любой     funny festival
 toto         88.87.86.123  45ff56aa230a любой
 nuser1       любой         любой        любой     Network user #1
 nuser2       172.20.0.36   любой        DMZ       Network user #2
fnpsh>
```

3.4.94. nat user password – изменение пароля сетевого пользователя

```
nat us[er] pass[word] <имя>
```

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<имя>` – имя существующего сетевого пользователя.

Команда изменяет пароль существующего сетевого пользователя.

Изменять пароль сетевого пользователя имеет право только пользователь ССПТ-2 `admin`.

В ССПТ-2 существуют ограничения на формат пароля сетевого пользователя:

- длина пароля – от **6** до **128** символов;
- допустимые символы – только **печатаемые ASCII-символы**;
- пароль пользователя является регистрово-зависимым.

Команда запросит ввод пароля для сетевого пользователя. Пароль необходимо вводить дважды, чтобы исключить опечатки при вводе пароля с клавиатуры. Ввод паролей на терминале не отображается.

Пример:

```
fnpsh> nat user password nuser1
Новый пароль:
Новый пароль повторно:
FNPSH-I-30C0-Пароль сетевого пользователя изменен (nuser1)
fnpsh>
```

3.4.95. nat user show – просмотр списка активных сетевых пользователей

```
nat us[er] sh[ow]
```

Команда выводит на экран терминала общее количество и список активных сеансов работы сетевых пользователей. Список активных сеансов работы сетевых пользователей выводится в виде таблицы, содержащей следующие поля:

- `Пользователь` – имя сетевого пользователя, которому принадлежит данный сеанс работы;
- `Начало работы` – время начала данного сеанса работы сетевого пользователя;
- `Откуда` – номер фильтрующего интерфейса ССПТ-2, MAC-адрес и IP-адрес источника запроса аутентификации данного сетевого пользователя;
- `Неактивность` – время, прошедшее с момента получения последнего пакета в рамках данного сеанса работы сетевого пользователя.

Пример:

```
fnpsh> nat user show
Активных сетевых пользователей: 1  Системное время: 29.05.2008 09:06:26 (MSD)

Пользователь  Начало работы        Откуда                              Неактивность
nuser2        29.05.2008 09:00:52  2,00:05:5d:e6:0a:c0,172.20.0.36     32c
```

3.4.96. reserv config synchronize – немедленная синхронизация текущей конфигурации ССПТ-2 в режиме высокой готовности

```
rese[rv] conf[ig] sync[hronize]
```

Требуемые привилегии – **cfg** или **ha**.

Команда выполняет синхронизацию текущей конфигурации ССПТ-2 – немедленную передачу параметров текущей конфигурации на смежный ССПТ-2.

На смежный ССПТ-2 будут переданы все параметры текущей конфигурации за исключением:

- настроек управляющего Ethernet-интерфейса;
- настроек фильтрующих интерфейсов;
- настроек подсистемы высокой готовности.

Пример:

```
fnpsh> reserv config synchronize
Синхронизировать конфигурацию? (Y/N)  [N]: y
FNPSH-I-30B1-Синхронизация конфигурации выполнена
fnpsh>
```

3.4.97. reserv default – установка параметров режима высокой готовности в значения по умолчанию

```
rese[rv] def[ault]
```

Требуемые привилегии – **cfg** или **ha**.

Команда устанавливает параметры текущей конфигурации ССПТ-2, используемые для режима высокой готовности, в значения по умолчанию.

Значения по умолчанию параметров режима высокой готовности соответствуют выводу команды `reserv show` (), приведенному ниже:

```
fnpsh> reserv show
Резервирование:                    отключено
Режим:                             не определено
Смежное устройство:
```

```
    IP-адрес:                          не определено
    Режим:                             нет информации
Интерфейсы в активном состоянии:       100baseTX / full-duplex
Интерфейсы в заблокированном состоянии: 10baseT/UTP / half-duplex
fnpsh>
```

Пример:

```
fnpsh> reserv default
Установить параметры резервирования в значения по умолчанию? (Y/N)  [N]: Y
FNPSH-I-3082-Параметры резервирования установлены по умолчанию
fnpsh>
```

3.4.98. reserv disable – отключение режима высокой готовности

`rese[rv] dis[able]`

Требуемые привилегии – **cfg** или **ha**.

Команда отключает режим высокой готовности и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Если на момент выполнения команды `reserv disable` режим высокой готовности уже был отключен, то его состояние останется без изменений.

Примеры:

```
fnpsh> reserv disable
Отключить резервирование? (Y/N)  [N]: y
FNPSH-I-3080-Резервирование отключено
fnpsh>

fnpsh> reserv disable
FNPSH-W-2013-Режим резервирования уже остановлен
fnpsh>
```

3.4.99. reserv enable – включение режима высокой готовности

`rese[rv] en[able]`

Требуемые привилегии – **cfg** или **ha**.

Команда выключает режим высокой готовности и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Перед включением режима высокой готовности необходимо выполнить следующие установки:

- назначение IP-адреса управляющему интерфейсу ССПТ-2 – команда `interface control address` (приложение 3.4.22, стр. 70);
- установка IP-адреса смежного ССПТ-2 – команда `reserv neighbour` (приложение 3.4.102, стр.132);
- установка статуса ССПТ-2 для режима высокой готовности – команда `reserv mode` (приложение 3.4.101, стр. 131).

Если на момент выполнения команды `reserv enable` режим высокой готовности уже был включен, то его состояние останется без изменений.

Примеры:

```
fnpsh> reserv enable
FNPSH-E-10E6-Недопустимые настройки режима резервирования
fnpsh>

fnpsh> reserv enable
FNPSH-I-307F-Резервирование включено
fnpsh>
```

3.4.100. reserv interface – настройка режимов работы фильтрующих интерфейсов для режима высокой готовности

```
rese[rv] interf[ace] {act[ive]|bl[ocked]} {dup[lex] {half|full}|
med[ia] {10|100|1000}}
```

Требуемые привилегии – **cfg** или **ha**.

Параметры:

- один из возможных режимов работы ССПТ-2:
  - ✔ `active` – настройка режимов для активного состояния фильтрующих интерфейсов;
  - ✔ `blocked` – настройка режимов для заблокированного состояния фильтрующих интерфейсов;
- `duplex` – настройка режима передачи фильтрующих интерфейсов:
  - ✔ `half` – полудуплексный режим передачи;
  - ✔ `full` – полнодуплексный режим передачи;
- media – настройка скорости передачи фильтрующих интерфейсов:
  - ✔ `10` – скорость передачи 10 Мбит/с;
  - ✔ `100` – скорость передачи 100 Мбит/с;
  - ✔ `1000` – скорость передачи 1000 Мбит/с.

Команда настраивает скорость и режим передачи управляющего Ethernet-интерфейса для режима высокой готовности.

Скорость передачи 1000 Мбит/сек может быть установлена только для ССПТ-2, укомплектованных сетевыми интерфейсами, поддерживающими технологию *Gigabit Ethernet*.

По умолчанию настройки скорости и режима передачи фильтрующих интерфейсов имеют следующие значения:

- для активного состояния:
  - ✔ скорость передачи – **100 Мбит/с**;
  - ✔ режим передачи – **полнодуплексный**;
- для заблокированного состояния:
  - ✔ скорость передачи – **10 Мбит/с**;
  - ✔ режим передачи – **полудуплексный**.

Примеры:

```
fnpsh> reserv interface active media 1000
FNPSH-I-30AC-Скорость фильтрующих интерфейсов при резервировании изменена
fnpsh>

fnpsh> reserv interface active duplex full
FNPSH-I-30AD-Режим передачи фильтрующих интерфейсов при резервировании изменен
fnpsh>
```

3.4.101. reserv mode – установка статуса ССПТ-2 для режима высокой готовности

```
rese[rv] mod[e] {bal[ance]|mas[ter]|sla[ve]|stp}
```

Требуемые привилегии – **cfg** или **ha**.

Параметры:

- один из возможных статусов ССПТ-2 для режима высокой готовности:

- ✔ `balance` – режим балансировки нагрузки;
- ✔ `master` – режим ведущего (основного) устройства;
- ✔ `slave` – режим ведомого (резервного) устройства;
- ✔ `stp` – режим Spanning Tree.

Команда устанавливает статус ССПТ-2 для режима высокой готовности и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Примеры:

```
fnpsh> reserv mode balance
FNPSH-I-307E-Режим резервирования изменен
fnpsh>

fnpsh> reserv mode slave
FNPSH-I-307E-Режим резервирования изменен
fnpsh>
```

3.4.102. reserv neighbour – установка IP-адреса смежного ССПТ-2 для режима высокой готовности

`rese[rv] ne[ighbour] <IP_адрес>`

Требуемые привилегии – **cfg** или **ha**.

Параметры:

- `<IP_адрес>` – IP-адрес смежного ССПТ-2, доступного через управляющий Ethernet-интерфейс.

Команда устанавливает IP-адрес смежного ССПТ-2 для режима высокой готовности и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

IP-адреса управляющих интерфейсов смежных ССПТ-2 должны принадлежать одной и той же IP-подсети.

Примеры:

```
fnpsh> reserv neighbour 192.168.169.246
FNPSH-W-2015-Смежное устройство вне управляющей IP сети
fnpsh>

fnpsh> reserv neighbour 192.168.169.252
FNPSH-I-3081-IP-адрес смежного устройство изменен
fnpsh>
```

3.4.103. reserv rule synchronize – немедленная синхронизация текущего набора правил в режиме высокой готовности

`rese[rv] rul[e] sync[hronize]`

Требуемые привилегии – **cfg** или **ha**.

Команда выполняет синхронизацию текущего набора правил – немедленную передачу текущего набора правил на смежный ССПТ-2.

Пример:

```
fnpsh> reserv rule synchronize
Синхронизировать правила? (Y/N)  [N]: y
FNPSH-I-3086-Синхронизация правил выполнена
fnpsh>
```

3.4.104. reserv show – просмотр параметров режима высокой готовности

```
rese[rv] sh[ow]
```

Команда выводит на экран терминала настройки параметров текущей конфигурации ССПТ-2, используемые для режима высокой готовности.

Пример:

```
fnpsh> reserv show
Резервирование:                          отключено
Режим:                                   MASTER (активный)
Смежное устройство:
    IP-адрес:                            192.168.169.252
    Режим:                               нет информации
Интерфейсы для MASTER, BALANCE:          100baseTX / full-duplex
Интерфейсы для SLAVE, SOFTWARE FAILURE: 10baseT/UTP / half-duplex
fnpsh>
```

3.4.105. rule add – добавление правила фильтрации в текущий набор

```
rul[e] add <определение_правила>
```

Требуемые привилегии – **rules**.

Параметры:

- `<определение_правила>` – текстовое определение правила фильтрации, VLAN-группы или интервала времени. Синтаксис текстовых определений приводится в документе "*МЕЖСЕТЕВОЙ ЭКРАН ССПТ-2. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. Руководство администратора. 54323649.501410.00009-0134*".

Команда добавляет новое правило фильтрации, VLAN-группу или интервал времени в текущий набор в соответствии с указанным текстовым определением.

Изменения в текущем наборе вступают в силу сразу же после успешного выполнения команды `rule add`.

Не допускается существование на одном и том же уровне нескольких правил фильтрации, включая VLAN-группы и интервалы времени, с одинаковыми номерами.

Для восстановления предыдущего состояния текущего набора правил необходимо использовать команду `rule rollback` (приложение 3.4.114, стр. 139).

Примеры:

- добавление VLAN-группы с уже существующим номером:

```
fnpsh> rule add vlan:100:214:"214th VLAN"
FNPSH-E-1044-VLAN-группа уже существует
fnpsh>
```

- добавление VLAN-группы номер `200`:

```
fnpsh> rule add vlan:200:214:"214th VLAN"
FNPSH-I-3008-VLAN-группа добавлена (200)
fnpsh>
```

- добавление интервала времени номер `30`:

```
fnpsh> rule add time:30:jul:1-15:any:any:"First half of July"
FNPSH-I-300D-Интервал времени добавлен (30)
fnpsh>
```

- добавление IP-правила фильтрации номер `255`:

```
fnpsh> rule add ip:255 action=accept in=Internal out=External srcip=192.168.169.125
srcport=1024-65535 dstport=80 protocol=tcp log=yes comments="WEB services"
FNPSH-I-300B-IP-правило добавлено (255)
```

```
fnpsh>
```

3.4.106. rule copy – копирование правила фильтрации в текущем наборе

```
rul[e] copy <тип> <старый_номер> <новый_номер>
```

Требуемые привилегии – **rules**.

Параметры:

- `<тип>` – обозначение категории правила фильтрации или интервала времени (раздел 1.4.1, стр. 2):
  - ✔ `mac` – MAC-правило фильтрации;
  - ✔ `arp` – ARP-правило фильтрации;
  - ✔ `ip` – IP-правило фильтрации;
  - ✔ `ipx` – IPX-правило фильтрации;
  - ✔ `ap` – AP-правило фильтрации;
  - ✔ `time` – интервал времени;
- `<старый_номер>` – номер правила фильтрации указанной категории или интервала времени из текущего набора;
- `<новый_номер>` – новый номер, с которым будут скопированы в текущем наборе указанное правило фильтрации или интервал времени.

Команда копирует в текущем наборе правило фильтрации указанной категории или интервал времени с присвоением нового номера.

Не допускается копирование VLAN-групп в виду того, что один и тот же идентификатор VLAN может входить только в одну VLAN-группу.

Не допускается копирование глобальных правил фильтрации.

Изменения в текущем наборе вступают в силу сразу же после успешного выполнения команды `rule copy`.

Для восстановления предыдущего состояния текущего набора правил необходимо использовать команду `rule rollback` (приложение 3.4.114, стр. 139).

Примеры:

- копирование интервала времени `30` в интервал времени `500`:

```
fnpsh> rule copy time 30 500
FNPSH-I-3099-Интервал времени скопирован
```

- копирование MAC-правила фильтрации `100` в MAC-правило `1500`:

```
fnpsh> rule copy mac 100 1500
FNPSH-I-308F-MAC-правило скопировано
fnpsh>
```

- недопустимые операции:

```
fnpsh> rule copy vlan 100 1500
FNPSH-E-10F9-Невозможно копировать VLAN-группу
fnpsh>

fnpsh> rule copy ip 0 500
FNPSH-E-10F8-Невозможно копировать (переносить) глобальное правило
fnpsh>
```

3.4.107. rule default – установка текущего набора правил в состояние по умолчанию

```
rul[e] def[ault]
```

Требуемые привилегии – **rules**.

Команда устанавливает состояние по умолчанию для текущего набора правил ССПТ-2.

По умолчанию в текущий набор правил входят только глобальные правила фильтрации, запрещающие прохождение пакетов через фильтрующие интерфейсы ССПТ-2.

Изменения в текущем наборе вступают в силу сразу же после успешного выполнения команды `rule default`.

Текущий набор правил устанавливается в состояние по умолчанию во время первого запуска ССПТ-2.

Для восстановления предыдущего состояния текущего набора правил необходимо использовать команду `rule rollback` (приложение 3.4.114, стр. 139).

Пример:

```
fnpsh> rule default
Установить правила по умолчанию (удаление всех пакетов)? (Y/N)  [N]: Y
FNPSH-I-304A-Таблица сессий очищена
FNPSH-I-30A0-Установлены правила по умолчанию
fnpsh> rule show
Текущий активный набор правил:

mac:0:drop:nolog
arp:0:drop:nolog
ip:0:drop:nolog
ipx:0:drop:nolog
fnpsh>
```

3.4.108. rule delete – удаление правила фильтрации из текущего набора

```
rul[e] del[ete] <идентификатор_правила>
```

Требуемые привилегии – **rules**.

Параметры:

- `<идентификатор_правила>` – тип и номер удаляемого правила фильтрации, интервала времени или VLAN-группы. Параметр имеет следующий формат:

```
<тип>:<номер>
```

где

- ✔ `<тип>` – обозначение категории правила фильтрации VLAN-группы или интервала времени (раздел 1.4.1, стр. 2):
  - `mac` – MAC-правило фильтрации;
  - `arp` – ARP-правило фильтрации;
  - `ip` – IP-правило фильтрации;
  - `ipx` – IPX-правило фильтрации;
  - `ap` – AP-правило фильтрации;
  - `vlan` – VLAN-группа;
  - `time` – интервал времени;
- ✔ `<номер>` – номер удаляемого правила фильтрации, VLAN-группы или интервала времени.

Команда удаляет из текущего набора указанное правило фильтрации, VLAN-группу или интервал времени.

Не допускается удаление VLAN-группы или интервала времени, используемых в правилах фильтрации.

Удаление глобальных правил фильтрации запрещено.

Изменения в текущем наборе вступают в силу сразу же после успешного выполнения команды `rule delete`.

Для восстановления предыдущего состояния текущего набора правил необходимо использовать команду `rule rollback` (приложение 3.4.114, стр. 139).

Примеры:

- удаление интервала времени `500`:

```
fnpsh> rule delete time:500
Удалить интервал времени? (Y/N)  [N]: Y
FNPSH-I-301B-Интервал времени удален (500)
fnpsh>
```

- удаление MAC-правила `1500`:

```
fnpsh> rule delete mac:1500
Удалить MAC-правило? (Y/N)  [N]: Y
FNPSH-I-3017-MAC-правило удалено (1500)
fnpsh>
```

- недопустимые операции:

```
fnpsh> rule delete vlan:100
FNPSH-E-1067-VLAN-группа используется в правилах фильтрации (IP-правила)
fnpsh>

fnpsh> rule delete ip:0
FNPSH-E-106A-Глобальное правило не может быть удалено
fnpsh>
```

3.4.109. rule edit – изменение существующего правила фильтрации в текущем наборе

`rul[e] ed[it] <определение_правила>`

Требуемые привилегии – **rules**.

Параметры:

- `<определение_правила>` – текстовое определение правила фильтрации, VLAN-группы или интервала времени. Синтаксис текстовых определений приводится в документе "*МЕЖСЕТЕВОЙ ЭКРАН ССПТ-2. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ. Руководство администратора. РКДЕ.5014107-05-0134*".

Команда изменяет существующее правило фильтрации, VLAN-группу или интервал времени в текущем наборе в соответствии с указанным текстовым определением.

Изменения в текущем наборе вступают в силу сразу же после успешного выполнения команды `rule edit`.

Для восстановления предыдущего состояния текущего набора правил необходимо использовать команду `rule rollback` (приложение 3.4.114, стр. 139).

Примеры:

- изменение VLAN-группы `200`:

```
fnpsh> rule edit vlan:200:526-540:"Range of VLAN tags"
```

```
Изменить группу VLAN? (Y/N)  [N]: Y
FNPSH-I-300F-VLAN-группа изменена (200)
fnpsh>
```

- изменение IP-правила 255:

```
fnpsh> rule edit ip:255 dstport=80,443
Изменить IP-правило? (Y/N)  [N]: Y
FNPSH-I-3012-IP-правило изменено (255)
fnpsh>
```

3.4.110. rule list – просмотр списка дополнительных наборов правил

`rul[e] lis[t]`

Команда выводит на экран терминала список существующих дополнительных наборов правил. Для каждого дополнительного набора правил выводится его имя и время создания.

Пример:

```
fnpsh> rule list
Список дополнительных наборов правил:
    Имя                 Время создания
    default_accept      24.06.2013 14:30:12 (MSK)
    default_drop        24.06.2013 14:30:12 (MSK)
    fnp2_ag             08.07.2013 21:19:25 (MSK)
Всего: 3        Свободно: 13
fnpsh>
```

3.4.111. rule load – загрузка дополнительного набора правил

`rul[e] lo[ad]` <имя_набора_правил>

Требуемые привилегии – **rules**.

Параметры:

- <имя_набора_правил> – имя предварительно сохраненного дополнительного набора правил.

Команда загружает правила фильтрации, VLAN-группы и интервалы времени, содержащиеся в дополнительном наборе правил с указанным именем, в текущий набор правил.

Содержимое текущего набора правил будет заменено содержимым загружаемого дополнительного набора правил.

Для восстановления предыдущего состояния текущего набора правил необходимо использовать команду `rule rollback` (приложение 3.4.114, стр. 139).

Пример:

```
fnpsh> rule load fnp2_ag
Загрузить дополнительный набор правил (режим управления сессиями)? (Y/N)  [N]: Y
FNPSH-I-304A-Таблица сессий очищена
FNPSH-I-301E-Дополнительный набор правил загружен
fnpsh>
```

3.4.112. rule move – перенос правила фильтрации в текущем наборе

`rul[e] mov[e]` <тип> <старый_номер> <новый_номер>

Требуемые привилегии – **rules**.

Параметры:

- <тип> – обозначение категории правила фильтрации, VLAN-группы или интервала времени (раздел 1.4.1, стр. 2):
  - ✔ `mac` – MAC-правило фильтрации;

- ✔ `arp` – ARP-правило фильтрации;
- ✔ `ip` – IP-правило фильтрации;
- ✔ `ipx` – IPX-правило фильтрации;
- ✔ `ap` – AP-правило фильтрации;
- ✔ `vlan` – VLAN-группа;
- ✔ `time` – интервал времени;

- `<старый_номер>` – номер правила фильтрации указанной категории, VLAN-группы или интервала времени из текущего набора;
- `<новый_номер>` – новый номер, с которым будут перенесены в текущем наборе указанное правило фильтрации, VLAN-группа или интервал времени.

Команда переносит в текущем наборе правило фильтрации,VLAN-группу или интервал времени с новым номером.

Не допускается перенос VLAN-группы или интервала времени, используемых в правилах фильтрации.

Перенос глобальных правил фильтрации запрещен.

Изменения в текущем наборе вступают в силу сразу же после успешного выполнения команды `rule move`.

Для восстановления предыдущего состояния текущего набора правил необходимо использовать команду `rule rollback` (приложение 3.4.114, стр. 139).

Примеры:

- перенос интервала времени `30` в интервал времени `1300`:

```
fnpsh> rule move time 30 1300
FNPSH-I-309A-Интервал времени перемещен
fnpsh>
```

- перенос IP-правила `255` в IP-правило `10`:

```
fnpsh> rule move ip 255 10
FNPSH-I-3094-IP-правило перемещено
fnpsh>
```

- недопустимые операции:

```
fnpsh> rule move vlan 100 1000
FNPSH-E-1067-VLAN-группа используется в правилах фильтрации (IP-правила)
fnpsh>

fnpsh> rule move arp 0 780
FNPSH-E-10F8-Невозможно копировать (переносить) глобальное правило
fnpsh>
```

3.4.113. rule remove – удаление дополнительного набора правил

`rul[e] rem[ove] <имя_набора_правил>`

Требуемые привилегии – **rules**.

Параметры:

- `<имя_набора_правил>` – имя дополнительного набора правил.

Команда удаляет дополнительный набор правил с указанным именем.

Пример:

```
fnpsh> rule remove fnp2_ag
```

```
Удалить дополнительный набор правил? (Y/N)  [N]: y
FNPSH-I-3020-Дополнительный набор правил удален
fnpsh>
```

3.4.114. rule rollback – возврат к предыдущему состоянию текущего набора правил

`rul[e] roll[back]`

Команда отменяет последнее изменение в текущем наборе правил, возвращая его к предыдущему состоянию.

Последовательное выполнение команды `rule rollback` приводит к чередованию двух последних состояний текущего набора правил.

Пример:

```
fnpsh> rule rollback
Восстановить предыдущий набор правил (режим управления сессиями)? (Y/N)  [N]: Y
FNPSH-I-304A-Таблица сессий очищена
FNPSH-I-3021-Предыдущее состояние текущего набора правил восстановлено
fnpsh>
```

3.4.115. rule save – сохранение текущего набора правил в дополнительном

`rul[e] sav[e] <имя_набора_правил>`

Требуемые привилегии – **rules**.

Параметры:

- `<имя_набора_правил>` – имя дополнительного набора правил.

Команда выполняет сохранение текущего набора правил ССПТ-2 в дополнительный с указанным именем. Если дополнительный набор правил с указанным именем уже существует, команда выполнена не будет.

Для перезаписи уже существующего дополнительного набора правил его необходимо предварительно удалить, используя команду `rule remove` (приложение 3.4.113, стр. 138).

В ССПТ-2 существуют следующие ограничения при работе с дополнительными наборами правил:

- ССПТ-2 может хранить не более **16** дополнительных наборов правил;
- имя дополнительного набора правил должно отвечать следующим требованиям:
  - ✔ длина имени – от **1** до **128** символов;
  - ✔ допустимые символы в имени – **латинские буквы** (a-z, A-Z), **цифры** (0-9), и символы '_' (подчеркивание), '**-**' (дефис). Имя дополнительного набора должно начинаться с буквы либо с цифры;
- имя дополнительного набора правил является регистрово-зависимым.

Примеры:

```
fnpsh> rule save fnp2_ag
FNPSH-I-301F-Дополнительный набор правил сохранен
fnpsh>

fnpsh> rule save fnp2_ag
FNPSH-E-107D-Дополнительный набор правил уже существует
fnpsh> rule save fnp2_AG
FNPSH-I-301F-Дополнительный набор правил сохранен
fnpsh>
```

3.4.116. rule show – просмотр текущего или дополнительного наборов правил

```
rul[e] sh[ow] [<имя_набора правил>] [<критерии_отбора>]
```

Параметры:

- `<имя_набора_правил>` – имя дополнительного набора правил;
- `<критерии_отбора>` – необязательный параметр, позволяющий выполнять просмотр только тех правил фильтрации из набора, которые удовлетворяют введенным критериям.

Команда выводит на экран терминала содержимое текущего или дополнительного наборов правил. Имя дополнительного набора правил указывается через параметр `<имя_набора_правил>`.

Если имя дополнительного набора правил не указано, на экран терминала выводится содержимое текущего набора правил.

Просмотр набора правил выполняется в соответствии с текущим режимом просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23).

Критерии отбора правил фильтрации. Параметр `<критерии_отбора>` представляет собой список именованных пар, разделенных пробелом, вида:

```
<имя_критерия>=<значение>[ ...]
```

Не допускается указывать в списке один и тот же критерий отбора более одного раза. В результате выполнения команды будут отобраны правила фильтрации, VLAN-группы и интервалы времени, удовлетворяющие *всем критериям отбора, указанным в списке, в совокупности*.

При отсутствии критериев отбора команда `rule show` выводит все правила фильтрации, VLAN-группы и интервалы времени данного набора.

В списке критериев отбора правил фильтрации параметр `<имя_критерия>` может принимать одно из следующих значений:

- `action` – отбор по действию над пакетом;
- `active` – отбор по активности правил фильтрации;
- `in` – отбор по входным интерфейсам;
- `mode` – формат вывода правил фильтрации, VLAN-групп и интервалов времени;
- `out` – отбор по выходным интерфейсам;
- `rnum` – отбор по номерам правил фильтрации, VLAN-групп и интервалов времени;
- `type` – отбор по категории правил;
- `viewer` – режим просмотра данных командного интерфейса ССПТ-2.

Отбор по действию над пакетом. Критерий `action` позволяет выбрать правила фильтрации, имеющие указанное действие, выполняемое над обрабатываемым пакетом. Критерий отбора имеет следующий синтаксис:

```
action={accept,drop,pass}
```

Значение критерия – действие, выполняемое над пакетом в соответствии сданным правилом фильтрации (подробнее – раздел 1.4.1, стр. 2):

- `accept` – пропустить пакет;
- `drop` – удалить пакет;
- `pass` – передать пакет.

Действие критерия отбора `action` не распространяется на глобальные правила фильтрации, VLAN-группы и интервалы времени.

Пример:

```
fnpsh> rule show fnp2_ag action=drop
```

Отбор по активности правил фильтрации. Критерий `active` позволяет выбрать правила фильтрации с указанным значением флага активности. Критерий отбора имеет следующий синтаксис:

```
active={yes,no}
```

Значение критерия – состояние флага активности правила фильтрации:

- `yes` – вывод активных правил фильтрации;
- `no` – вывод неактивных правил фильтрации.

Действие критерия отбора `active` не распространяется на глобальные правила фильтрации, VLAN-группы и интервалы времени.

Пример:

```
fnpsh> rule show active=no
```

Отбор по входным интерфейсам. Критерий `in` позволяет выбрать правила фильтрации, использующие указанный список фильтрующих интерфейсов ССПТ-2 в качестве входных интерфейсов. Критерий отбора имеет следующий синтаксис:

```
in={<имя_интерфейса>}[,...]
```

Значение критерия отбора – список фильтрующих интерфейсов ССПТ-2:

- `<имя_интерфейса>` – символическое имя, присвоенное фильтрующему интерфейсу.

Один и тот же фильтрующий интерфейс не может присутствовать в списке более одного раза.

Действие критерия отбора `in` не распространяется на глобальные правила фильтрации, VLAN-группы и интервалы времени.

Пример:

```
fnpsh> rule show in=External,Mirror
```

Формат вывода правил. Критерий `mode` позволяет задать формат для вывода отобранных правил фильтрации, VLAN-групп и интервалов времени. Критерий отбора имеет следующий синтаксис:

```
mode={detail|line}
```

Значение критерия – условное обозначение формата вывода:

- `detail` – подробный формат вывода. Вывод каждого правила занимает несколько строк, каждая строка содержит наименование и значение одного параметра правила фильтрации, VLAN-группы или интервала времени. Например:

```
IP-правило 200 - "Laptop to WEB":
    Действие: accept (передача на выходные интерфейсы)
    Входные интерфейсы: Internal
    Выходные интерфейсы: External
    Инкапсулированные протоколы: tcp
    IP-адреса источника: 192.168.169.122
    Порты источника: 1024-65535
    Порты приемника: 80,8080
    Сессии: создаются по умолчанию; таймаут неактивности: по умолчанию
    Прикладные правила: 100
    VLAN-группа: 100 (идентификаторы 217)
    Регистрация пакетов: включено; сессий: включено
```

- `line` – текстовое определение правила в формате строки с разделителями (*используется по умолчанию*). Синтаксис текстовых определений приводится в приложении . Например:

```
ip:200:accept:logpkt,logses:1:0:0:tcp:192.168.169.122:1024-65535:any:80,8080:
any:any:any:any:any:any:active:"Laptop to WEB":100:defses:deftout:100:noalarm
```

Пример:

```
fnpsh> rule show fnp2_ag mode=detail
```

Отбор по выходным интерфейсам. Критерий `out` позволяет выбрать правила фильтрации, использующие указанный список фильтрующих интерфейсов ССПТ-2 в качестве выходных интерфейсов. Критерий отбора имеет следующий синтаксис:

```
out={<имя_интерфейса>}[,...]
```

Значение критерия отбора – список фильтрующих интерфейсов ССПТ-2:

- `<имя_интерфейса>` – символическое имя, присвоенное фильтрующему интерфейсу.

Один и тот же фильтрующий интерфейс не может присутствовать в списке более одного раза.

Действие критерия отбора `out` не распространяется на глобальные правила фильтрации, VLAN-группы и интервалы времени.

Пример:

```
fnpsh> rule show out=Internal
```

Отбор по номерам правил. Критерий `rnum` позволяет выбрать правила фильтрации, VLAN-группы и интервалы времени с указанными номерами. Критерий отбора имеет следующий синтаксис:

```
rnum={<номер>|<номер_мин>-<номер_макс>}
```

Значение критерия отбора – одиночный номер правила или интервал номеров:

- `<номер>` – одиночный номер правила фильтрации, VLAN-группы или интервала времени. Будут выбраны правила, номера которых совпадают с указанным значением;
- `<номер_мин>-<номер_макс>` – интервал номеров правил фильтрации, VLAN-групп или интервалов времени. Будут выбраны правила, значения номеров которых находятся в диапазоне от `<номер_мин>` до `<номер_макс>` включительно.

Действие критерия отбора `rnum` не распространяется на глобальные правила фильтрации.

Пример:

```
fnpsh> rule show rnum=200-350
```

Отбор по категории правил. Критерий `type` позволяет выбрать правила указанных категорий. Критерий отбора имеет следующий синтаксис:

```
type={mac|arp|ip|iptmp|ipx|ap|vlan|time}[,...]
```

Значение критерия отбора – список категорий правил:

- `mac` – MAC-правила фильтрации;
- `arp` – ARP-правила фильтрации;
- `ip` – IP-правила фильтрации;
- `iptmp` – временные IP-правила фильтрации (*только для текущего набора*);
- `ipx` – IPX-правила фильтрации;
- `ap` – AP-правила фильтрации;

- vlan – VLAN-группы;
- time – интервалы времени.

Одна и та же категория правил не может присутствовать в списке более одного раза.

Пример:

```
fnpsh> rule show fnp2_ag type=ip,time
```

Режим просмотра данных командного интерфейса ССПТ-2. Критерий viewer позволяет изменить режим просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23) на время выполнения команды rule show. Критерий отбора имеет следующий синтаксис:

```
viewer={intern[al]|mor[e]|no}
```

где

- 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.

По умолчанию используется режим просмотра данных, установленный по команде system fnpsh viewer (раздел 3.4.156, стр. 168)

Просмотреть текущий установленный режим просмотра данных можно по команде system show (раздел 3.4.162, стр. 173).

Пример:

```
fnpsh> rule show viewer=more
```

В команде rule show можно указывать несколько *различных* критериев отбора. Например для вывода IP-правил фильтрации и интервалов времени из текущего набора со значениями номеров от 200 до 350, используя режим сплошного вывода данных командного интерфейса ССПТ-2, следует выполнить команду

```
fnpsh> rule show type=ip,time rnum=200-350 viewer=no
```

3.4.117. rule stats clear – сброс статистики трафика по текущему набору правил

```
rul[e] stats cl[ear]
```

Требуемые привилегии – **pf**.

Команда выполняет сброс статистики трафика пакетного фильтра ССПТ-2 по правилам фильтрации текущего набора.

Статистика трафика по правилам фильтрации текущего набора сбрасывается также при останове и перезапуске пакетного фильтра ССПТ-2 – команды filter stop (приложение 3.4.11, стр. 65) и filter restart (приложение 3.4.8, стр. 63).

Пример:

```
fnpsh> rule stats clear
Очистить статистику использования правил? (Y/N)  [N]: Y
FNPSH-I-30AA-Статистика правил очищена
fnpsh>
```

3.4.118. rule stats show – просмотр статистики трафика по текущему набору правил

```
rul[e] stats sh[ow] [<критерии_отбора>]
```

Параметры:

- `<критерии_отбора>` – необязательный параметр, позволяющий выполнять просмотр статистики использования только тех правил фильтрации, которые удовлетворяют введенным критериям.

Команда выводит на экран терминала данные статистики использования правил фильтрации в пакетном фильтре ССПТ-2. Статистика выводится в виде таблицы, содержащей следующие поля:

- `Правила` – тип и номер правила фильтрации текущего набора в формате `<тип>:<номер>` (приложение 3.4.108, стр. 135);
- `Последнее изменение` – дата и время создания или последнего изменения данного правила фильтрации;
- `Пакеты` – количество пакетов, обработанных пакетным фильтром ССПТ-2 по данному правилу фильтрации;
- `Байты` – суммарная длина пакетов, обработанных пакетным фильтром ССПТ-2 по данному правилу фильтрации.

Просмотр статистики трафика по текущему набору правил выполняется в соответствии с текущим режимом просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23).

Критерии отбора правил фильтрации. Параметр `<критерии_отбора>` представляет собой список именованных пар, разделенных пробелом, вида:

```
<имя_критерия>=<значение>[ ...]
```

Не допускается указывать в списке один и тот же критерий отбора более одного раза. В результате выполнения команды будут отобраны правила фильтрации, удовлетворяющие *всем критериям отбора, указанным в списке, в совокупности*.

При отсутствии критериев отбора команда `rule stats show` выводит статистику использования всех правила фильтрации текущего набора.

В списке критериев отбора правил фильтрации параметр `<имя_критерия>` может принимать одно из следующих значений:

- `action` – отбор по действию над пакетом;
- `in` – отбор по входным интерфейсам;
- `out` – отбор по выходным интерфейсам;
- `rnum` – отбор по номерам правил фильтрации;
- `suffix` — использование десятичных суффиксов;
- `type` – отбор по категории правил;
- `viewer` – режим просмотра данных командного интерфейса ССПТ-2.

Отбор по действию над пакетом. Критерий `action` позволяет выбрать правила фильтрации, имеющие указанное действие, выполняемое над обрабатываемым пакетом. Критерий отбора имеет следующий синтаксис:

```
action={accept,drop,pass}
```

Значение критерия – действие, выполняемое над пакетом в соответствии сданным правилом фильтрации (подробнее – раздел 1.4.1, стр. 2):

- `accept` – пропустить пакет;

- drop – удалить пакет;
- pass – передать пакет.

Пример:

```
fnpsh> rule stats show action=drop
```

Отбор по входным интерфейсам. Критерий in позволяет выбрать правила фильтрации, использующие указанный список фильтрующих интерфейсов ССПТ-2 в качестве входных интерфейсов. Критерий отбора имеет следующий синтаксис:

```
in={<имя_интерфейса>|<номер_интерфейса>}[,...]
```

Значение критерия отбора – список фильтрующих интерфейсов ССПТ-2:

- <имя_интерфейса> – символическое имя, присвоенное фильтрующему интерфейсу;
- <номер_интерфейса> – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): 0 – **Eth0**, 1 – **Eth1** и т. д.

Один и тот же фильтрующий интерфейс не может присутствовать в списке более одного раза.

Пример:

```
fnpsh> rule stats show in=External,Mirror
```

Отбор по выходным интерфейсам. Критерий out позволяет выбрать правила фильтрации, использующие указанный список фильтрующих интерфейсов ССПТ-2 в качестве выходных интерфейсов. Критерий отбора имеет следующий синтаксис:

```
out={<имя_интерфейса>|<номер_интерфейса>}[,...]
```

Значение критерия отбора – список фильтрующих интерфейсов ССПТ-2:

- <имя_интерфейса> – символическое имя, присвоенное фильтрующему интерфейсу;
- <номер_интерфейса> – порядковый номер фильтрующего интерфейса. Номера фильтрующих интерфейсов ССПТ-2 определяются в соответствии с их маркировкой (раздел 2.2, стр. 8): 0 – **Eth0**, 1 – **Eth1** и т. д.

Один и тот же фильтрующий интерфейс не может присутствовать в списке более одного раза.

Пример:

```
fnpsh> rule stats show out=Internal
```

Отбор по номерам правил. Критерий rnum позволяет выбрать правила фильтрации с указанными номерами. Критерий отбора имеет следующий синтаксис:

```
rnum={<номер>|<номер_мин>-<номер_макс>}
```

Значение критерия отбора – одиночный номер правила или интервал номеров:

- <номер> – одиночный номер правила фильтрации. Будут выбраны правила, номера которых совпадают с указанным значением;
- <номер_мин>-<номер_макс> – интервал номеров правил фильтрации. Будут выбраны правила, значения номеров которых находятся в диапазоне от <номер_мин> до <номер_макс> включительно.

Пример:

```
fnpsh> rule stats show rnum=200-350
```

Использование десятичных суффиксов. Критерий `suffix` позволяет включить или отключить режим использования десятичных суффиксов используемых в выводе команды для округления значений количества пакетов и их суммарной длины, обработанных правилами фильтрации. Критерий отбора имеет следующий синтаксис:

```
suffix={yes|no}
```

где

- `yes` – включить использование десятичных суффиксов `K`, `M`, `G` (`K` – кило, `M` – мега, `G` – гига);
- `no` – отключить использование десятичных суффиксов.

По умолчанию режим использования десятичных суффиксов включен.

Пример:

```
fnpsh> rule stats show suffix=no
```

Отбор по категории правил. Критерий `type` позволяет выбрать правила указанных категорий. Критерий отбора имеет следующий синтаксис:

```
type={mac|arp|ip|iptmp|ipx|ap}[,...]
```

Значение критерия отбора – список категорий правил:

- `mac` – MAC-правила фильтрации;
- `arp` – ARP-правила фильтрации;
- `ip` – IP-правила фильтрации;
- `iptmp` – временные IP-правила фильтрации (*только для текущего набора*);
- `ipx` – IPX-правила фильтрации;
- `ap` – AP-правила фильтрации.

Одна и та же категория правил не может присутствовать в списке более одного раза.

Пример:

```
fnpsh> rule stats show type=mac,ip,ap
```

Режим просмотра данных командного интерфейса ССПТ-2. Критерий `viewer` позволяет изменить режим просмотра данных командного интерфейса ССПТ-2 (раздел 2.6.6, стр. 23) на время выполнения команды `rule stats show`. Критерий отбора имеет следующий синтаксис:

```
viewer={intern[al]|mor[e]|no}
```

где

- `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.

По умолчанию используется режим просмотра данных, установленный по команде `system fnpsh viewer` (раздел 3.4.156, стр. 168)

Просмотреть текущий установленный режим просмотра данных можно по команде `system show` (раздел 3.4.162, стр. 173).

Пример:

```
fnpsh> rule stats show viewer=more
```

В команде `rule stats show` можно указывать несколько *различных* критериев отбора. Например для вывода статистики использования MAC-правил и IP-правил фильтрации, используя режим сплошного вывода данных командного интерфейса ССПТ-2, следует выполнить команду

```
fnpsh> rule stats show type=mac,ip suffix=yes viewer=no
Правила     Последнее изменение   Пакеты     Байты
mac:0       10.05.2011, 10:05:52  8877K      8141M
mac:100     10.05.2011, 10:05:52  0          0
ip:0        10.05.2011, 10:05:52  4192K      3888M
ip:10       10.05.2011, 10:06:54  0          0
ip:100      10.05.2011, 10:05:52  0          0
ip:200      10.05.2011, 10:05:52  0          0
ip:250      07.05.2011, 12:22:11  4682K      4071M
ip:300      10.05.2011, 10:05:52  0          0
fnpsh>
```

3.4.119. session ap disable – отключение использования AP-правил фильтрации

`ses[sion] ap dis[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда отключает фильтрацию пакетов на прикладном уровне сетевого взаимодействия и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, использование AP-правил фильтрации отключено.

Пример:

```
fnpsh> session ap disable
Отключить использование AP-правил? (Y/N)  [N]: Y
FNPSH-I-3040-Использование AP-правил отключено
fnpsh>
```

3.4.120. session ap enable – включение использования AP-правил фильтрации

`ses[sion] ap en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда включает фильтрацию пакетов на прикладном уровне сетевого взаимодействия и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> session ap enable
FNPSH-I-303F-Использование AP-правил включено
fnpsh>
```

3.4.121. session deeptcp disable — отключение глубокого контроля TCP

`ses[sion] deept[cp] dis[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда отключает режим глубокого контроля для TCP-сессий и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Отключение глубокого контроля TCP означает, что:

- TCP-сессия создается по *любому TCP-пакету*, пропущенному по правилам фильтрации, без учета состояния флагов TCP;
- TCP-сессия переводится в состояние `ESTABLISH` (*сессия установлена*) по *любому TCP-пакету*, принятому ССПТ-2 со стороны сервера, без учета состояния флагов TCP и номера подтверждения;
- в TCP-пакетах, принадлежащих установленной TCP-сессии, не отслеживается наличие флагов `RST` и `FIN`, разрывающих соединение со стороны клиента или со стороны сервера;
- удаление установленной TCP-сессии осуществляется по тайм-ауту неактивности.

Пример:

```
fnpsh> session deeptcp disable
Отключить глубокий контроль TCP? (Y/N) [N]: y
FNPSH-I-30CB-Глубокий контроль TCP отключен
fnpsh>
```

3.4.122. session deeptcp enable — включение глубокого контроля TCP

`session deept[cp] en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда включает режим глубокого контроля для TCP-сессий и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, режим глубокого контроля для TCP-сессий включен.

Пример:

```
fnpsh> session deeptcp enable
FNPSH-I-30CA-Глубокий контроль TCP включен
fnpsh>
```

3.4.123. session disable – отключение управления сессиями

`ses[sion] dis[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда отключает подсистему управления сессиями пакетного фильтра и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Отключение управления сессиями влечет за собой:

- отключение фильтрации пакетов на прикладном уровне сетевого взаимодействия (использование AP-правил фильтрации);
- отключение режима обнаружения flood-атак.

Пример:

```
fnpsh> session disable
Отключить управление сессиями? (Y/N)  [N]: Y
FNPSH-I-303C-Режим управления сессиями отключен
fnpsh>
```

3.4.124. session enable – включение управления сессиями

`ses[sion] en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда выключает подсистему управления сессиями пакетного фильтра и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, управление сессиями включено.

Пример:

```
fnpsh> session enable
FNPSH-I-303B-Режим управления сессиями включен
fnpsh>
```

3.4.125. session flood alarm disable – отключение сигнализации обнаружения flood-атак

`ses[sion] fl[ood] ala[rm] dis[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда отключает сигнализацию обнаружения flood-атак и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, сигнализация обнаружения flood-атак отключена.

Пример:

```
fnpsh> session flood alarm disable
Отключить сигнализацию обнаружения flood-атак? (Y/N)  [N]: Y
FNPSH-I-30A2-Сигнализация обнаружения flood-атак отключена
fnpsh>
```

3.4.126. session flood alarm enable – включение сигнализации обнаружения flood-атак

`ses[sion] fl[ood] ala[rm] en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда выключает сигнализацию обнаружения flood-атак и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Сигнализация обнаружения flood-атаки заключается в формировании и регистрации системного сообщения. Например, при обнаружении flood-атаки по протоколу ICMP от источника с IP-адресом 192.168.169.125 будет сформировано системное сообщение

```
Aug  6 10:36:47 fnp2 fnp[12720]: fnp_filtd: Flood-атака обнаружена и
заблокирована - source 192.168.169.125 icmp
```

Просмотр системных сообщений выполняется по команде `log syslog show` (приложение 3.4.54, стр. 106).

Пример:

```
fnpsh> session flood alarm enable
FNPSH-I-30A1-Сигнализация обнаружения flood-атак включена
fnpsh>
```

3.4.127. session flood disable – отключение режима блокировки flood-атак

`ses[sion] fl[ood] dis[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда отключает режим блокировки flood-атак в пакетном фильтре и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, режим блокировки flood-атак в пакетном фильтре отключен.

Пример:

```
fnpsh> session flood disable
Отключить обнаружение flood-атак? (Y/N)  [N]: n
fnpsh>
```

3.4.128. session flood enable – включение режима блокировки flood-атак

`ses[sion] fl[ood] en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда включает режим блокировки flood-атак и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Каждая обнаруженная flood-атака блокируется путем создания временного IP-правила, запрещающее прохождение пакетов через фильтрующие интерфейсы ССПТ-2 от источника обнаруженной flood-атаки. Например, по временному IP-правилу

```
iptmp:1:nolog:1:60:icmp:192.168.169.125:any:any:any:"Blocked flood
attack":noalarm
```

блокируется flood-атака по протоколу ICMP от источника с IP-адресом 192.168.169.125.

Пример:

```
fnpsh> session flood enable
FNPSH-I-30A3-Обнаружение flood-атак включено
fnpsh>
```

3.4.129. session flood rule comments – изменение комментария для временного IP правила, блокирующего flood-атаку

`ses[sion] fl[ood] rul[e] com[ments] <комментарий>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<комментарий>` – новый комментарий для временных IP-правил, блокирующих flood-атаку.

Команда изменяет комментарий для временных IP-правил, создаваемых для блокировки flood-атак, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

В ССПТ-2 существуют следующие ограничения для комментариев к правилам фильтрации:

- длина комментария – от **0** до **31** символа (допускается отсутствие комментария);
- допустимые символы – все **печатаемые символы**, исключая **символ двоеточия** ':';
- комментарий, содержащий **символы пробела**, в командной строке должен заключаться в **двойные кавычки** '"'.

Примеры:

```
fnpsh> session flood rule comments Flood_detected_by_FNP-2
FNPSH-I-30A8-Комментарий временного IP-правила изменен
fnpsh>

fnpsh> session flood rule comments "Flood detected by FNP-2"
FNPSH-I-30A8-Комментарий временного IP-правила изменен
fnpsh>
```

3.4.130. session flood rule lifetime – настройка времени жизни временного IP-правила, блокирующего flood-атаку

```
ses[sion] fl[ood] rul[e] lif[etime] <время>
```

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<время>` – новое значение для времени жизни временного IP-правила, блокирующего flood-атаку.

Команда устанавливает новое значение времени жизни для временных IP-правил, создаваемых для блокировки flood-атак, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию время жизни временного IP-правила, блокирующего flood-атаку, составляет **60** секунд.

Время жизни временного IP-правила, блокирующего flood-атаку, может быть изменено в пределах от **10** до **3600** секунд включительно.

Пример:

```
fnpsh> session flood rule lifetime 180
FNPSH-I-30A9-Время жизни временного IP-правила изменено
fnpsh>
```

3.4.131. session flood rule log disable – отключение регистрации пакетов во временном IP-правиле, блокирующем flood-атаку

```
ses[sion] fl[ood] rul[e] log dis[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда отключает регистрацию пакетов во временных IP-правилах, создаваемых для блокировки flood-атак, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, регистрация пакетов во временных IP-правилах, блокирующих flood-атаки, отключена.

Пример:

```
fnpsh> session flood rule log disable
Отключить регистрацию временного IP-правила? (Y/N)  [N]: Y
FNPSH-I-30A7-Регистрация во временных IP-правилах отключена
fnpsh>
```

3.4.132. session flood rule log enable – включение регистрации пакетов во временном IP-правиле, блокирующем flood-атаку

```
ses[sion] fl[ood] rul[e] log en[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда включает регистрацию пакетов во временных IP-правилах, создаваемых для блокировки flood-атак, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Просмотр зарегистрированных пакетов выполняется по команде `log packet show` (приложение 3.4.50, стр. 88).

Пример:

```
fnpsh> session flood rule log enable
FNPSH-I-30A6-Регистрация во временных IP-правилах включена
fnpsh>
```

3.4.133. session flood threshold default – установка порогов обнаружения flood-атак в значения по умолчанию

`ses[sion] fl[ood] thr[eshold] def[ault]`

Требуемые привилегии – **cfg** или **pf**.

Команда устанавливает пороги обнаружения flood-атак в значения по умолчанию и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию пороги обнаружения flood-атак имеют следующие значения:

- для протокола ICMP – **300** пакетов в секунду;
- для протокола UDP – **500** пакетов в секунду;
- для протокола TCP – **1000** пакетов в секунду.

Пример:

```
fnpsh> session flood threshold default
Установить пороговые значения по умолчанию? (Y/N)  [N]: Y
FNPSH-I-30A5-Пороговое значение изменено
fnpsh>
```

3.4.134. session flood threshold icmp – установка порога обнаружения flood-атак для протокола ICMP

`ses[sion] fl[ood] thr[eshold] icmp <порог>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<порог>` – новое значение порога обнаружения flood-атак для протокола ICMP в пакетах в секунду.

Команда устанавливает новое значение порога обнаружения flood-атак для протокола ICMP и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию значение порога обнаружения flood-атак для протокола ICMP составляет **300** пакетов в секунду.

Значение порога обнаружения flood-атак для протокола ICMP может быть изменено в следующих пределах:

- минимальное значение – **10** пакетов в секунду;
- максимальное значение – в числовом выражении равняется **половине размера таблицы сессий**. Размер таблицы сессий можно узнать, используя команду `session show` (приложение 3.4.143, стр. 156).

Пример:

```
fnpsh> session flood threshold icmp 6000
FNPSH-E-1115-Недопустимое пороговое значение (ожидаются значения из диапазона 10-4096)
fnpsh>

fnpsh> session flood threshold icmp 100
FNPSH-I-30A5-Пороговое значение изменено
fnpsh>
```

3.4.135. session flood threshold tcp – установка порога обнаружения flood-атак для протокола TCP

```
ses[sion] fl[ood] thr[eshold] tcp <порог>
```

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<порог>` – новое значение порога обнаружения flood-атак для протокола TCP в пакетах в секунду.

Команда устанавливает новое значение порога обнаружения flood-атак для протокола TCP и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию значение порога обнаружения flood-атак для протокола TCP составляет **1000** пакетов в секунду.

Значение порога обнаружения flood-атак для протокола TCP может быть изменено в следующих пределах:

- минимальное значение – **10** пакетов в секунду;
- максимальное значение – в числовом выражении равняется **половине размера таблицы сессий**. Размер таблицы сессий можно узнать, используя команду `session show` (приложение 3.4.143, стр. 156).

Пример:

```
fnpsh> session flood threshold tcp 6000
FNPSH-E-1115-Недопустимое пороговое значение (ожидаются значения из диапазона 10-4096)
fnpsh>

fnpsh> session flood threshold tcp 800
FNPSH-I-30A5-Пороговое значение изменено
fnpsh>
```

3.4.136. session flood threshold udp – установка порога обнаружения flood-атак для протокола UDP

```
ses[sion] fl[ood] thr[eshold] udp <порог>
```

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- `<порог>` – новое значение порога обнаружения flood-атак для протокола UDP в пакетах в секунду.

Команда устанавливает новое значение порога обнаружения flood-атак для протокола UDP и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию значение порога обнаружения flood-атак для протокола UDP составляет **500** пакетов в секунду.

Значение порога обнаружения flood-атак для протокола UDP может быть изменено в следующих пределах:

- минимальное значение – **10** пакетов в секунду;
- максимальное значение – в числовом выражении равняется **половине размера таблицы сессий**. Размер таблицы сессий можно узнать, используя команду `session show` (приложение 3.4.143, стр. 156).

Пример:

```
fnpsh> session flood threshold udp 6000
FNPSH-E-1115-Недопустимое пороговое значение (ожидаются значения из диапазона 10-4096)
```

```
fnpsh>

fnpsh> session flood threshold udp 1000
FNPSH-I-30A5-Пороговое значение изменено
fnpsh>
```

3.4.137. session ip disable – отключение создания по умолчанию сессий для IP-правил фильтрации

`ses[sion] ip dis[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда отключает режим создания по умолчанию сессий для IP-правил фильтрации и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Отключение режима создания по умолчанию сессий для IP-правил фильтрации влечет за собой:

- отключение создания сессий для пакетов, обработанных по глобальному IP-правилу;
- отключение создания сессий для пакетов, обработанных по IP-правилам, в которых параметр `session` имеет значение `default` (или `defses`).

Сессии будут создаваться только для пакетов, обработанных по IP-правилам, в которых параметр `session` имеет значение `yes` (или `ses`).

Пример:

```
fnpsh> session ip disable
Отключить создание сессий по умолчанию для IP-правил? (Y/N)  [N]: Y
FNPSH-I-3042-Сессии не будут создаваться по умолчанию для IP-правил
fnpsh>
```

3.4.138. session ip enable – включение создания по умолчанию сессий для IP-правил фильтрации

`ses[sion] ip en[able]`

Требуемые привилегии – **cfg** или **pf**.

Команда включает режим создания по умолчанию сессий для IP-правил фильтрации и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, создание по умолчанию сессий для IP-правил фильтрации включено.

При включенном режиме создания по умолчанию сессий для IP-правил фильтрации сессии **будут создаваться**:

- для пакетов, обработанных по глобальному IP-правилу;
- для пакетов, обработанных по IP-правилам, в которых параметр `session` имеет значение `default` (или `defses`);
- для пакетов, обработанных по IP-правилам, в которых параметр `session` имеет значение `yes` (или `ses`).

Сессии **не будут создаваться** для пакетов, обработанных по IP-правилам, в которых параметр `session` имеет значение `no` (или `noses`).

Пример:

```
fnpsh> session ip enable
FNPSH-I-3041-Сессии будут создаваться по умолчанию для IP-правил
fnpsh>
```

3.4.139. session log disable – отключение регистрации пакетов, отброшенных сессиями

```
ses[sion] log dis[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда отключает регистрацию пакетов, отброшенных механизмом управления сессиями пакетного фильтра, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, регистрация пакетов, отброшенных механизмом управления сессиями, отключена.

Пример:

```
fnpsh> session log disable
FNPSH-I-303E-Регистрация IP пакетов, отброшенных механизмом управления сессиями, отключена
fnpsh>
```

3.4.140. session log enable – включение регистрации пакетов, отброшенных сессиями

```
ses[sion] log en[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда включает регистрацию пакетов, отброшенных механизмом управления сессиями пакетного фильтра, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Просмотр зарегистрированных пакетов выполняется по команде `log packet show` (приложение 3.4.50, стр. 88).

Причина удаления пакета механизмом управления сессии указывается в регистрационной записи об этом пакете.

Пример:

```
fnpsh> session log enable
FNPSH-I-303D-Регистрация IP пакетов, отброшенных механизмом управления сессиями, включена
fnpsh>
```

3.4.141. session mac disable – отключение использования данных канального уровня в управлении сессиями

```
ses[sion] mac dis[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда отключает контроль неизменности MAC-адресов отправителя и получателя в обрабатываемых пакетах при управлении сессиями.

По умолчанию использование данных канального уровня в управлении сессиями включено.

Пример:

```
fnpsh> session mac disable
Отключить использование данных канального уровня? (Y/N) [N]: Y
FNPSH-I-304E-Использование данных канального уровня отключено
fnpsh>
```

3.4.142. session mac enable – включение использования данных канального уровня в управлении сессиями

```
ses[sion] mac en[able]
```

Требуемые привилегии – **cfg** или **pf**.

Команда включает контроль неизменности MAC-адресов отправителя и получателя в обрабатываемых пакетах при управлении сессиями.

Пример:

```
fnpsh> session mac enable
FNPSH-I-304D-Использование данных канального уровня включено
fnpsh>
```

3.4.143. session show – просмотр параметров управления сессиями

```
ses[sion] sh[ow]
```

Команда выводит на экран терминала текущие параметры функционирования механизма управления сессиями пакетного фильтра ССПТ-2.

Пример:

```
fnpsh> session show
Управление сессиями:                              включено
Регистрация отброшенных пакетов:                  включено
Использование прикладных правил:                  включено
Создание сессий для IP-правил по умолчанию:       отключено
Использование данных канального уровня:           включено
Глубокий контроль TCP:                            включено
Размер таблицы сессий:                            8192
Таймауты неактивности сессий (сек):
    Состояние TCP SYN:                            5 (по умолчанию)
    Состояние TCP ESTABLISED:                     3600 (по умолчанию)
    Состояние TCP FIN:                            180 (по умолчанию)
    Состояние UDP SYN:                            5 (по умолчанию)
    Состояние TCP ESTABLISHED:                    10 (по умолчанию)
    Состояние ICMP SYN:                           5 (по умолчанию)
    Состояние ICMP ESTABLISHED:                   20 (по умолчанию)
Обнаружение flood-атак:                           включено
    Генерация сообщения alarm:                    включено
    Пороговое значение для TCP (пакеты/сек):      800
    Пороговое значение для UDP (пакеты/сек):      1000
    Пороговое значение для ICMP (пакеты/сек):     100
    Время жизни временного IP-правила (сек):      180
    Параметр регистрации временного IP-правила:   включено
    Комментарий для временного IP-правила:        "Flood detected by FNP-2"
fnpsh>
```

3.4.144. session table clear – очистка таблицы сессий

```
ses[sion] tab[le] cl[ear] [nolog]
```

Требуемые привилегии – **pf**.

Параметры:

- `nolog` – необязательный параметр, задающий режим очистки таблицы сессий без регистрации удаляемых сессий. Может применяться для ускорения выполнения команды.

Команда удаляет все записи из таблицы сессий пакетного фильтра ССПТ-2.

Очистка таблицы сессий означает удаление всех сессий, существовавших на момент выполнения команды `session table clear`.

После удаления сессий из таблицы все пакеты, входящие в контекст данных сессий и продолжающие поступать на фильтрующие интерфейсы ССПТ-2, будут **удаляться**.

По умолчанию очистка таблицы сессий выполняется с одновременной регистрацией каждой из удаляемых сессий. При большом количестве удаляемых сессий может приводить к временной потере производительности ССПТ-2.

Пример:

```
fnpsh> session table clear
Очистить таблицу сессий? (Y/N)  [N]: Y
FNPSH-I-304A-Таблица сессий очищена
fnpsh>
```

3.4.145. session table delete – удаление сессии из таблицы сессий

`ses[sion] tab[le] del[ete] <номер_сессии>`

Требуемые привилегии – **pf**.

Параметры:

- `<номер_сессии>` – номер удаляемой сессии в таблице сессий.

Команда удаляет запись о сессии с указанным номером из таблицы сессий пакетного фильтра ССПТ-2.

Номера сессий выводятся при просмотре таблицы сессий, используя команду `session table show` (приложение 3.4.146, стр. 157).

После удаления сессии из таблицы все пакеты, входящие в контекст данной сессии и продолжающие поступать на фильтрующие интерфейсы ССПТ-2, будут **удаляться**.

Пример:

```
fnpsh> session table delete 4062
Удалить сессию 4062? (Y/N)  [N]: Y
FNPSH-I-304B-Сессия удалена
fnpsh>
```

3.4.146. session table show – просмотр таблицы сессий

`ses[sion] tab[le] sh[ow] [<критерии_отбора>]`

Параметры:

- `<критерии_отбора>` – необязательный параметр, позволяющий выполнять просмотр только тех сессий, которые удовлетворяют введенным критериям.

Команда выполняет просмотр таблицы сессий пакетного фильтра ССПТ-2. Каждая строка вывода содержит информацию об одной сессии:

- номер сессии (столбец “Номер”);
- номер IP-правила, на основе которого создана сессия (столбец “Правило”);
- время создания сессии, время жизни сессии, время неактивности сессии (столбцы “Старт”, “Удаление” и “Таймаут” соответственно);
- идентификатор VLAN, к которой принадлежат пакеты данной сессии (значение `-1` означает, что VLAN не используется) (столбец “VLAN”);

- атрибуты клиента – номер фильтрующего интерфейса ССПТ-2, IP-адрес клиента и номер прикладного порта (*для протоколов TCP и UDP*) (столбец “Клиент”);
- атрибуты сервера – номер фильтрующего интерфейса ССПТ-2, IP-адрес сервера и номер прикладного порта (*для протоколов TCP и UDP*) (столбец “Сервер”);
- типы протоколов транспортного и прикладного уровней (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”).

При отсутствии критериев отбора команда `session table show` выводит все записи из таблицы сессий.

Время создания сессии выводится в формате:

`ЧЧ:ММ:СС`

где:

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

Время жизни 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 время жизни является отрицательным значением. Это означает, что сессия будет автоматически удалена пакетным фильтрам ССПТ-2 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 начала сетевого взаимодействия называется *клиентом*, другая сторона сетевого взаимодействия – *сервером*. Атрибуты клиента и сервера выводятся в формате:

`<интерфейс>:<IP_адрес>[:<порт>]`

где:

- `<интерфейс>` – номер фильтрующего интерфейса ССПТ-2, на который принимаются пакеты, входящие в контекст сессии, от данной стороны сетевого взаимодействия – клиента или сервера;
- `<IP_адрес>` – IP-адрес стороны сетевого взаимодействия;
- `<порт>` – номер прикладного порта стороны сетевого взаимодействия (*только для сессий, базирующихся на транспортных протоколах TCP и UDP*).

Используемые протоколы отражают имена протоколов транспортного и прикладного уровней, на которых базировалась данная сессия. Протоколы прикладного уровня указываются только для сессий, базирующихся на транспортных протоколах TCP и UDP.

По мере обработки пакетов каждая сессия может последовательно находиться в нескольких *состояниях*. Набор возможных состояний для сессий, базирующихся на разных типах протоколов (ICMP, UDP или TCP), различный. Набор состояний и их описание для протоколов ICMP, UDP и TCP приводится в таблицах 3.7, 3.8 и 3.9 соответственно.

Таблица 3.7: Состояния ICMP-сессии

Состояние	*Описание*
SYN	ICMP-сессия устанавливается – получен ICMP эхо-запрос (*echo request*) от клиента
ESTABLISH	ICMP-сессия установлена – получен ICMP эхо-ответ (*echo reply*) от сервера

Таблица 3.8: Состояния UDP-сессии

Состояние	*Описание*
SYN	UDP-сессия устанавливается – получен пакет от клиента
ESTABLISH	UDP-сессия установлена – получен пакет от сервера

Таблица 3.9: Состояния TCP-сессии

Состояние	*Описание*
При включенном режиме глубокого контроля TCP	
SYN	Виртуальное TCP-соединение устанавливается – получен SYN-пакет от клиента
SYNACK	Виртуальное TCP-соединение устанавливается – получен ответный SYN-пакет от сервера
ESTABLISH	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*)
CLOSED	Сессия закрыта
При отключенном режиме глубокого контроля TCP	
SYN	TCP-сессия устанавливается – получен пакет от клиента
ESTABLISH	TCP-сессия установлена – получен пакет от сервера

Количество пакетов/байтов, переданных в контексте сессии выводятся 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.

Для просмотра таблицы сессий используются клавиши и управляющие последовательности, перечисленные в таблице 3.10.

Таблица 3.10: 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

Управление	Назначение
<Page Down>	Переход к следующей странице вывода таблицы сессий
<R>	Обновление информации о таблице сессий
<1>	Скрыть/показать столбец “Правило” таблицы сессий
<2>	Последовательно скрыть/показать столбцы “Удаление”, “Старт” и “Таймаут” 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
<8>	Скрыть/показать столбец “Пакеты” таблицы сессий
<9>	Скрыть/показать столбец “Байты” таблицы сессий
<H>	Вывод подсказки по клавишам управления просмотром таблицы сессий (рисунок 3.53)
<F10>, <Q>	Завершение выполнения команды

Пример вывода таблицы сессий пакетного фильтра ССПТ-2 приводится на рисунке 3.52.

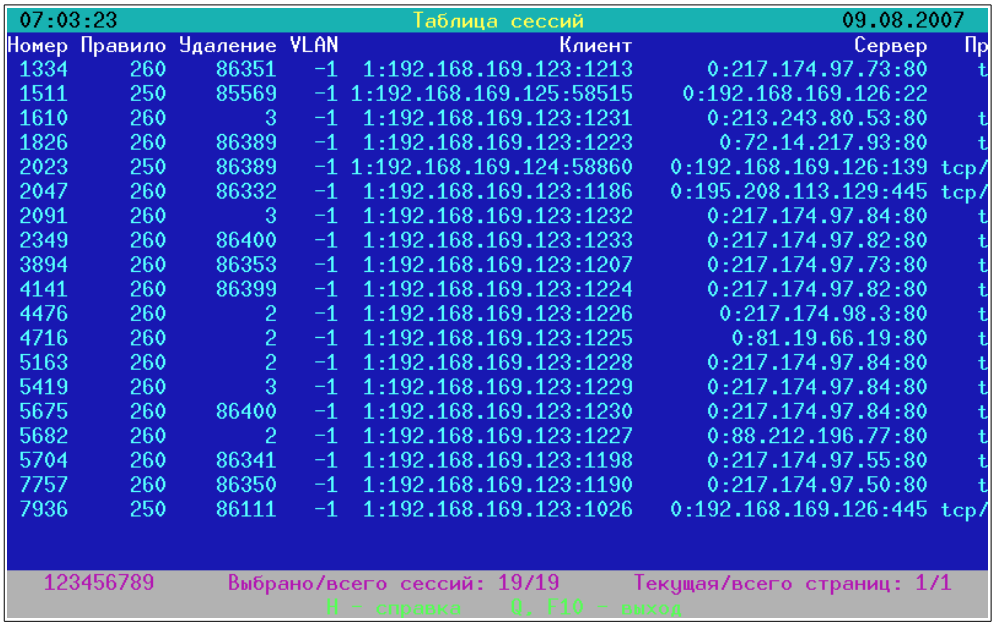

Рисунок 3.52: Просмотр таблицы сессий

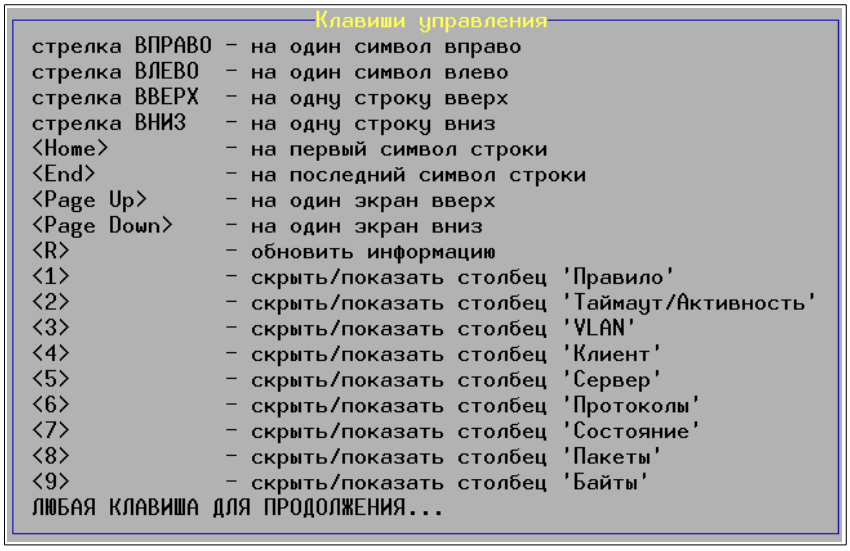

Рисунок 3.53: Управление просмотром таблицы сессий

Критерии отбора записей из таблицы сессий. Параметр `<критерии_отбора>` представляет собой список именованных пар, разделенных пробелом, вида:

```
<имя_критерия>=<значение>[ ...]
```

Не допускается указывать в списке один и тот же критерий отбора более одного раза. В результате выполнения команды будут отобраны записи из таблицы сессий, удовлетворяющие *всем критериям отбора, указанным в списке, в совокупности*.

В списке критериев отбора записей из таблицы сессий параметр `<имя_критерия>` может принимать одно из следующих значений:

- `aproto` – отбор по протоколу прикладного уровня;
- `ip` – отбор по IP-адресам как клиента, так и сервера;
- `ipcl` – отбор по IP-адресам клиента;
- `ipsrv` – отбор по IP-адресам сервера;
- `rule` – отбор по номеру IP-правила фильтрации;
- `state` – отбор по состоянию сессии;
- `tproto` – отбор по протоколу транспортного уровня;
- `vlan` – отбор по идентификатору VLAN.

Отбор по протоколу прикладного уровня. Критерий `aproto` позволяет выбрать записи о сессиях, базирующихся на транспортных протоколах TCP и UDP, с указанным номером или именем протокола прикладного уровня. Критерий отбора имеет следующий синтаксис:

```
aproto={<имя_протокола>|<номер_протокола>}
```

где

- `<имя_протокола>` – стандартное символическое имя протокола (например, `ftp`, `smtp`, `http`);
- `<номер_протокола>` – стандартный номер прикладного порта, соответствующий данному протоколу (например `21`, `25`, `80`).

Критерий отбора `aproto` имеет смысл только для сессий, базирующихся на протоколах транспортного уровня TCP или UDP.

Примеры:

```
fnpsh> session table show aproto=http
```

```
fnpsh> session table show aproto=445
```

Отбор по IP-адресам. Критерии `ip`, `ipcl`, `ipsrv` позволяют выбрать записи о сессиях с указанными IP-адресами клиента и сервера. Критерии отбора имеют следующий синтаксис:

```
{ip|ipcl|ipsrv}={<IP_адрес>[/<маска>]}[,...]
```

где

- `ip` – отбор сессий по IP-адресам как клиента, так и сервера;
- `ipcl` – отбор сессий по IP-адресам клиента;
- `ipsrv` – отбор сессий по IP-адресам сервера.

Значение критерия отбора – список IP-подсетей и IP-адресов, разделенных запятой. Параметр `<IP_адрес>` указывается в формате, принятом для IP-адресов – `XXX.XXX.XXX.XXX`, где `XXX` – целое число в диапазоне от `0` до `255`.

Параметр `<маска>` указывается либо в формате IP-адреса, или в формате CIDR (количество единичных бит IP-адреса, отведенных под адресацию IP-подсети в целом) – целое число в диапазоне от `1` до `32`. Значение маски должно соответствовать правилам разбиения IP сетей на подсети.

Список IP-подсетей и IP-адресов может содержать не более **8** элементов.

Примеры:

- выбрать записи о сессиях с IP-адресами клиента или сервера `192.168.169.124`:

```
fnpsh> session table show ip=192.168.169.124
```

- выбрать записи о сессиях с IP-адресом клиента из подсети `192.168.170.0` с маской CIDR `25` (`255.255.255.128`) или `192.168.169.123`:

```
fnpsh> session table show ipcl=192.168.170.0/25,192.168.169.123
```

- выбрать записи о сессиях с IP-адресом сервера из подсети `192.168.169.0/255.255.255.128`:

```
fnpsh> session table show ipsrv=192.168.169.0/255.255.255.128
```

Отбор по номеру IP-правила фильтрации. Критерий `rule` позволяет выбрать записи о сессиях, созданных на основе IP-правила фильтрации с указанным номером. Критерий отбора имеет следующий синтаксис:

```
rule=<номер_правила>,
```

где

- `<номер_правила>` – целое число в диапазоне от **0** до **65535** включительно.

Пример:

```
fnpsh> session table show rule=250
```

Отбор по состоянию сессии. Критерий `state` позволяет выбрать записи о сессиях с указанным состоянием. Критерий отбора имеет следующий синтаксис:

```
state={close|establish|fin|finack|finfin|finfinack|reset|syn|synack|timewait},
```

Значение критерия отбора – наименование состояния сессии в соответствии с таблицами 3.7, 3.8, 3.9.

Пример:

```
fnpsh> session table show state=timewait
```

Отбор по протоколу транспортного уровня. Критерий `tproto` позволяет выбрать записи о сессиях с указанным номером или именем протокола транспортного уровня. Критерий отбора имеет следующий синтаксис:

```
tproto={<имя_протокола>|<номер_протокола>}
```

Значение критерия отбора – стандартное имя протокола или его номер. Поскольку сессии создаются только для протоколов транспортного уровня TCP, UDP и ICMP, значением критерия отбора tproto может быть:

- `<имя_протокола>` – `tcp`, `udp` или `icmp`;
- `<номер протокола>` – `6` (протокол TCP), `17` (протокол UDP) или `1` (протокол ICMP).

Примеры:

- выбрать записи о сессиях, базирующихся на протоколе TCP:

```
fnpsh> session table show tproto=tcp
```

- выбрать записи о сессиях, базирующихся на протоколе ICMP:

```
fnpsh> session table show tproto=1
```

Отбор по идентификатору VLAN. Критерий `vlan` позволяет выбрать записи о сессиях, пакеты которых принадлежат VLAN с указанным идентификатором. Критерий отбора имеет следующий синтаксис:

```
vlan=<vlan_tag>,
```

где

- `<vlan_tag>` – целое число в диапазоне от `0` до `4095`, или `-1` для сессий, не использующих VLAN.

Примеры:

- выбрать записи о сессиях, пакеты которых не принадлежат ни к одной VLAN:

```
fnpsh> session table show vlan=-1
```

- выбрать записи о сессиях, пакеты которой принадлежат к VLAN с идентификатором `214`:

```
fnpsh> session table show vlan=214
```

3.4.147. session table size – изменение размера таблицы сессий

`ses[sion] tab[le] siz[e] <размер_таблицы>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

`<размер_таблицы>` – новый размер таблицы сессий пакетного фильтра ССПТ-2.

Команда изменяет размер таблицы сессий пакетного фильтра ССПТ-2 и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Размер таблицы сессий определяет максимальное количество записей о сессиях, которые могут быть в нее помещены.

По умолчанию размер таблицы сессий составляет **8192** записи.

Размер таблицы сессий может быть изменен в пределах от **1024** до **65536** записей включительно.

Пример:

```
fnpsh> session table size 16000
FNPSH-I-3049-Размер таблицы сессий изменен
fnpsh>
```

3.4.148. session timeout default – установка тайм-аута неактивности сессий в значения по умолчанию

`ses[sion] timeo[ut] def[ault]`

Требуемые привилегии – **cfg** или **pf**.

Команда устанавливает тайм-аут неактивности сессий в значения по умолчанию и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Тайм-аут неактивности сессии – это максимальное время существования сессии в секундах, в течение которого не было принято ни одного пакета, соответствующего контексту данной сессии. По истечении тайм-аута неактивности сессия автоматически удаляется пакетным фильтром ССПТ-2.

Тайм-аут неактивности сессий различается для разных протоколов и состояний. По умолчанию значение тайм-аута неактивности сессий составляет:

- для **ICMP**-сессий:
  - ✔ для состояния SYN – **5** секунд;
  - ✔ для состояния ESTABLISH – **20** секунд;
- для **UDP**-сессий:
  - ✔ для состояния SYN – **5** секунд;
  - ✔ для состояния ESTABLISH – **10** секунд;
- для **TCP**-сессий (*включенный режим глубокого контроля TCP*):
  - ✔ для состояния SYN – **5** секунд;
  - ✔ для состояния ESTABLISH – **3600** секунд (1 час);
  - ✔ для состояния FIN – **180** секунд;
- для **TCP**-сессий (*отключенный режим глубокого контроля TCP*):
  - ✔ для состояния SYN – **5** секунд;
  - ✔ для состояния ESTABLISH – **60** секунд.

Просмотреть текущие значения тайм-аута неактивности сессий можно, используя команду `session show` (приложение 3.4.143, стр. 156).

Пример:

```
npsh> session timeout default
Установить таймауты сессий в значения по умолчанию? (Y/N)  [N]: Y
FNPSH-I-304C-Таймаут неактивности сессий установлен по умолчанию
fnpsh>
```

3.4.149. session timeout icmp – установка тайм-аута неактивности для ICMP сессий

`ses[sion] timeo[ut] icmp {syn|est[ablished]} <тайм_аут>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- состояние сессии (таблица 3.7, стр. 159):
  - ✔ `syn` – состояние SYN;
  - ✔ `established` – состояние ESTABLISH;
- `<тайм_аут>` – новое значения тайм-аута неактивности для ICMP сессий.

Команда устанавливает новое значение тайм-аута неактивности для состояний SYN или ESTABLISH сессий, базирующихся на протоколе ICMP, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию значение тайм-аута неактивности ICMP сессий составляет:

- для состояния SYN – **5** секунд;
- для состояния ESTABLISH – **20** секунд;

Просмотреть текущие значения тайм-аута неактивности ICMP сессий можно, используя команду `session show` (приложение 3.4.143, стр. 156).

Тайм-аут неактивности для ICMP сессий может быть установлен в пределах от **1** до **2147483647** секунд включительно.

Пример:

```
fnpsh> session timeout icmp syn 60
FNPSH-I-3045-Таймаут неактивности ICMP сессии изменен
fnpsh> session timeout icmp established 3600
FNPSH-I-3045-Таймаут неактивности ICMP сессии изменен
fnpsh>
```

3.4.150. session timeout tcp – установка тайм-аута неактивности для TCP сессий

`ses[sion] timeo[ut] tcp {syn|est[ablished]|fin} <тайм_аут>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- состояние сессии (таблица 3.9, стр. 159):
  - ✔ `syn` – состояние SYN;
  - ✔ `established` – состояние ESTABLISH;
  - ✔ `fin` – состояние FIN.
- `<тайм_аут>` – новое значения тайм-аута неактивности для TCP сессий.

Команда устанавливает новое значение тайм-аута неактивности для состояний SYN, ESTABLISH или FIN сессий, базирующихся на протоколе TCP, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию значение тайм-аута неактивности TCP сессий составляет:

- для включенного режима глубокого контроля TCP:
  - ✔ для состояния SYN – **5** секунд;
  - ✔ для состояния ESTABLISH – **3600** секунд (1 час);
  - ✔ для состояния FIN – **180** секунд;
- для отключенного режима глубокого кнтроля TCP:
  - ✔ для состояния SYN – **5** секунд;
  - ✔ для состояния ESTABLISH – **60** секунд.

Просмотреть текущие значения тайм-аута неактивности TCP сессий можно, используя команду `session show` (приложение 3.4.143, стр. 156).

Тайм-аут неактивности для TCP сессий может быть установлен:

- для состояний SYN и FIN – в пределах от **1** до **2147483647** секунд включительно;
- для состояния ESTABLISHED – в пределах от **0** (*тайм-аут неактивности отсутствует*) до **2147483647** секунд включительно.

Тайм-аут неактивности для состояния FIN применяется только при включенном режиме глубокого контроля TCP.

Пример:

```
fnpsh> session timeout tcp syn 10
FNPSH-I-3043-Таймаут неактивности TCP сессии изменен
fnpsh> session timeout tcp established 172800
FNPSH-I-3043-Таймаут неактивности TCP сессии изменен
fnpsh> session timeout tcp fin 300
FNPSH-I-3043-Таймаут неактивности TCP сессии изменен
fnpsh>
```

3.4.151. session timeout udp – установка тайм-аута неактивности для UDP сессий

`ses[sion] timeo[ut] udp {syn|est[ablished]} <тайм_аут>`

Требуемые привилегии – **cfg** или **pf**.

Параметры:

- состояние сессии (таблица 3.8, стр. 159):
  - ✔ `syn` – состояние SYN;
  - ✔ `established` – состояние ESTABLISH;
- `<тайм_аут>` – новое значения тайм-аута неактивности для UDP сессий.

Команда устанавливает новое значение тайм-аута неактивности для состояний SYN или ESTABLISH сессий, базирующихся на протоколе UDP, и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию значение тайм-аута неактивности UDP сессий составляет:

- для состояния SYN – **5** секунд;
- для состояния ESTABLISH – 1**0** секунд;

Просмотреть текущие значения тайм-аута неактивности UDP сессий можно, используя команду `session show` (приложение 3.4.143, стр. 156).

Тайм-аут неактивности для UDP сессий может быть установлен в пределах от **1** до **2147483647** секунд включительно.

Пример:

```
fnpsh> session timeout udp syn 15
FNPSH-I-3044-Таймаут неактивности UDP сессии изменен
fnpsh> session timeout udp established 600
FNPSH-I-3044-Таймаут неактивности UDP сессии изменен
fnpsh>
```

3.4.152. system fnpsh history clear – очистка буфера истории команд

`syst[em] fnpsh his[tory] cl[ear]`

Команда очищает буфер истории команд для текущего сеанса работы пользователя в командном интерфейсе ССПТ-2.

Пример:

```
fnpsh> system fnpsh history clear
Очистить буфер истории команд? (Y/N)  [N]: Y
FNPSH-I-3022-Буфер истории команд очищен
fnpsh>
```

3.4.153. system fnpsh history show – просмотр содержимого буфера истории команд

`syst[em] fnpsh his[tory] sh[ow]`

Команда выводит на экран терминала содержимое буфера истории команд текущего сеанса работы пользователя в командном интерфейсе ССПТ-2.

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

Пример:

```
fnpsh> system fnpsh history show
Буфер истории команд:
   1 - system password
   2 - user password admin
   3 - interface control address 10.98.7.1/255.255.255.0
   4 - gateway set 10.98.7.254
   5 - rule list
   6 - rule load default_accept
fnpsh>
```

3.4.154. system fnpsh password – изменение пароля системного пользователя

`syst[em] fnpsh pass[word]`

Требуемые привилегии – **user** (только пользователь `admin`).

Команда изменяет пароль системного пользователя `fnpsh` для уровня системной авторизации, используемой для интерактивного режима командного интерфейса ССПТ-2 (раздел 2.5.1, стр. 10).

Изменить пароль системного пользователя имеет право только пользователь `admin`.

В ССПТ-2 существуют ограничения на формат пароля пользователя:

- длина пароля – от **6** до **128** символов;
- допустимые символы – только **печатаемые ASCII-символы**.

Эта команда является синонимом команды `system password` (приложение 3.4.160, стр. 172).

Сначала команда запросит ввод текущего пароля системного пользователя. Затем, если текущий пароль введен верно, команда запросит ввод нового пароля. Новый пароль необходимо вводить дважды, чтобы исключить опечатки при вводе пароля с клавиатуры. Ввод паролей на терминале не отображается.

Пример:

```
fnpsh> system fnpsh password
Старый пароль:
Новый пароль:
Новый пароль повторно:
FNPSH-I-309E-Пароль системного пользователя изменен
fnpsh>
```

3.4.155. system fnpsh timeout – установка тайм-аута неактивности для командного интерфейса ССПТ-2

```
syst[em] fnpsh timeo[ut] <тайм_аут>
```

Требуемые привилегии – **cfg** или **sys**.

Параметры:

- `<тайм-аут>` – новое значение тайм-аута неактивности для командного интерфейса ССПТ-2.

Команда устанавливает новое значение тайм-аута неактивности для сеансов работы пользователя в командном интерфейсе ССПТ-2 и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию тайм-аут неактивности для командного интерфейса ССПТ-2 составляет **600** секунд (10 минут).

Тайм-аут неактивности командного интерфейса ССПТ-2 может быть изменен в пределах от **10** до **3600** (1 час) секунд.

Просмотреть текущее значение тайм-аута неактивности можно, используя команду `system show` (приложение 3.4.162, стр. 173).

Пример:

```
fnpsh> system fnpsh timeout 180
FNPSH-I-3088-Таймаут неактивности командного интерфейса изменен
fnpsh>
```

3.4.156. system fnpsh viewer – установка режима просмотра данных в командном интерфейсе ССПТ-2

```
syst[em] fnpsh v[iewer] {intern[al]|mor[e]|no}
```

Параметры:

- режим 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.

Команда устанавливает режим просмотра данных для текущего сеанса работы пользователя в командном интерфейсе ССПТ-2.

Пример:

```
fnpsh> system fnpsh viewer more
FNPSH-I-3087-Режим просмотра изменен
fnpsh>
```

3.4.157. system halt – выключение ССПТ-2

```
syst[em] halt
```

Требуемые привилегии – **sys**.

Команда выполняет останов операционной системы и выключает питание ССПТ-2.

Не рекомендуется выключать ССПТ-2 без останова операционной системы, используя выключатель питания на корпусе ССПТ-2, поскольку это может привести к серьезным нарушениям целостности файловой системы ССПТ-2.

Пример:

```
npsh> system halt
Выключить устройство? (Y/N)  [N]: Y
FNPSH-I-3006-Устройство будет выключено через две минуты. Выход ...
```

3.4.158. system icheck – проверка целостности программного обеспечения ССПТ-2

`syst[em] ich[eck]`

Команда выполняет проверку целостности компонентов операционной системы и программного обеспечения ССПТ-2.

Перечень компонентов операционной системы и программного обеспечения ССПТ-2, целостность которых контролируется, приводится в таблице 3.11.

Таблица 3.11: Файлы, контролируемые подсистемой контроля целостности ССПТ-2

Имя файла	*Описание*
Неизменяемые файлы	
kernel	Файл ядра операционной системы
libc.so.7	Файл стандартной разделяемой библиотеки функций операционной системы
libkvm.so.4	Файл разделяемой библиотеки интерфейса доступа к памяти ядра операционной системы
libssl.so.5	Файл разделяемой библиотеки функций пакета OpenSSL
login	Утилита авторизации системного пользователя
ntpdate	Утилита синхронизации системного времени по протоколу NTP
telnetd	TELNET сервер
openssl	Файл интерфейса командной строки для использования криптографических функций пакета OpenSSL
fnpsh	Файл командного интерпретатора ССПТ-2
fnpinfo	Файл утилиты вывода системной информации
fnp_authd	Файл сервера авторизации ССПТ-2
fnp_cryd	Файл сервера терминального доступа ССПТ-2
fnp_csd	Файл сервера проверки контрольных сумм ССПТ-2
fnp_filtd	Файл пакетного фильтра ССПТ-2
fnp_had	Файл сервера высокой готовности ССПТ-2
fnp_logd	Файл сервера регистрации ССПТ-2
fnp_shd	Файл командного сервера ССПТ-2
libfnp.so.1	Файл разделяемой библиотеки сервисных функций ССПТ-2
libfnpcrypt.so.1	Файл разделяемой библиотеки криптографических функций FNPCrypt
Изменяемые файлы	
fnp2_gost.key	Файл закрытого ключа ССПТ-2 (ГОСТ)
fnp2_gost.sig	Файл сертификата ССПТ-2 (ГОСТ)
ca_gost.sig	Файл сертификата УЦ (ГОСТ)
fnp2_key.pem	Файл закрытого ключа ССПТ-2 (X.509, OpenSSL)
fnp2_cert.pem	Файл сертификата ССПТ-2 (X.509, OpenSSL)
ca_cert.pem	Файл сертификата УЦ (X.509, OpenSSL)
master.passwd	Файл учетных записей пользователей операционной системы

Имя файла	Описание
fnp.cf	Файл параметров конфигурации ССПТ-2
fnp_passwd	Файл учетных записей пользователей ССПТ-2
net_passwd	Файл учетных записей сетевых пользователей ССПТ-2
fnp_net.keys	Файл ключей аутентификации сетевых пользователей ССПТ-2
mac.cf	Файл MAC-правил текущего набора
arp.cf	Файл ARP-правил текущего набора
ip.cf	Файл IP-правил текущего набора
ipx.cf	Файл IPX-правил текущего набора
ap.cf	Файл AP-правил текущего набора
vlan.cf	Файл VLAN-групп текущего набора
time.cf	Файл интервалов времени текущего набора

Если нарушения контрольных сумм файлов не обнаружено, выводится информационной сообщение

`FNPSH-I-30AD-Проверка целостности выполнена,`

далее следует вывод на экран терминала списка имен файлов указанных компонентов и первые 6 символов контрольных сумм, соответствующих этим файлам.

В случае обнаружения нарушения контрольных сумм выводится сообщение об ошибке вида

`FNPSH-E-1106-Нарушена контрольная сумма файла. Пакетный фильтр остановлен (<имя_файла>),`

где

- `<имя_файла>` – имя файла в соответствии с таблицей 3.11, целостность которого была нарушена.

Во время работы ССПТ-2 автоматически выполняется периодическая проверка целостности программного обеспечения сервером проверки контрольных сумм ССПТ-2.

В случае нарушения контрольной суммы любого из проверяемых файлов ССПТ-2 переходит в **однопользовательский режим работы**. В этом режиме:

- пакетный фильтр ССПТ-2 остановлен;
- доступ к управлению ССПТ-2 возможен только с системной консоли и только для пользователя `admin`.

Примеры:

```
fnpsh> system icheck
FNPSH-I-30AE-Проверка целостности выполнена
kernel            095cb9...
libc.so.7         dfc575...
libkvm.so.4       802b7c...
libssl.so.5       87fb73...
login             b8bd77...
ntpdate           685b6d...
telnetd           3bacae...
openssl           ecbe3d...
libfnpcrypt.so.1  ccd528...
fnpsh             18b1fa...
fnpinfo           00739e...
fnp_authd         5bd494...
fnp_csd           00357a...
fnp_filtd         a0dd5a...
fnp_logd          5ae298...
fnp_shd           1d8575...
libfnp.so.1       3c1f7e...
fnp_had           01d172...
fnp_cryd          45a095...
fnp2_gost.key     d79b1a...
fnp2_gost.sig     fc1b1a...
```

```
ca_gost.sig       f12e67...
fnp2_key.pem      eb6f8a...
fnp2_cert.pem     e9a9c2...
ca_cert.pem       d394e0...
master.passwd     5d1d26...
fnp.cf            2cf560...
fnp_passwd        32ad52...
net_passwd        d41d8c...
fnp_net.keys      d41d8c...
mac.cf            5ab018...
arp.cf            ec90e1...
ip.cf             47c50b...
ipx.cf            1f6a64...
ap.cf             d41d8c...
vlan.cf           0829f7...
time.cf           c20019...
fnpsh>

fnpsh> system icheck
FNPSH-E-1106-Нарушена контрольная сумма файла. Пакетный фильтр остановлен (fnp_passwd)
fnpsh>
```

3.4.159. system key show — просмотр сертификатов и ключей ССПТ-2

```
syst[em] key sh[ow]
```

Команда выводит на экран терминала сертификаты и открытые ключи (в составе сертификатов) УЦ и ССПТ-2:

- сертификаты УЦ и ССПТ-2 для пакета OpenSSL, используемые для организации защищенного канала управления ССПТ-2 через WEB-интерфейс администратора;
- сертификаты УЦ и ССПТ-2 ГОСТ, используемые для организации защищенного канала управления ССПТ-2 через командный интерфейс ССПТ-2 в режиме удаленного терминального доступа.

Для просмотра зарегистрированных событий используются клавиши и управляющие последовательности, перечисленные в таблице 3.12.

Таблица 3.12: Управление просмотром сертификатов и ключей ССПТ-2

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 строк
<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
<Ctrl+W>	Режим просмотра без горизонтальной прокрутки. В этом режиме осуществляется автоматический перенос строк, длина которых превышает ширину окна вывода данных.
<H>	Вывод подсказки по клавишам управления просмотром данных
<F10>, <Q>	Завершение просмотра данных

Пример вывода информации о сертификатах и ключах ССПТ-2 приводится на рисунке 3.54.

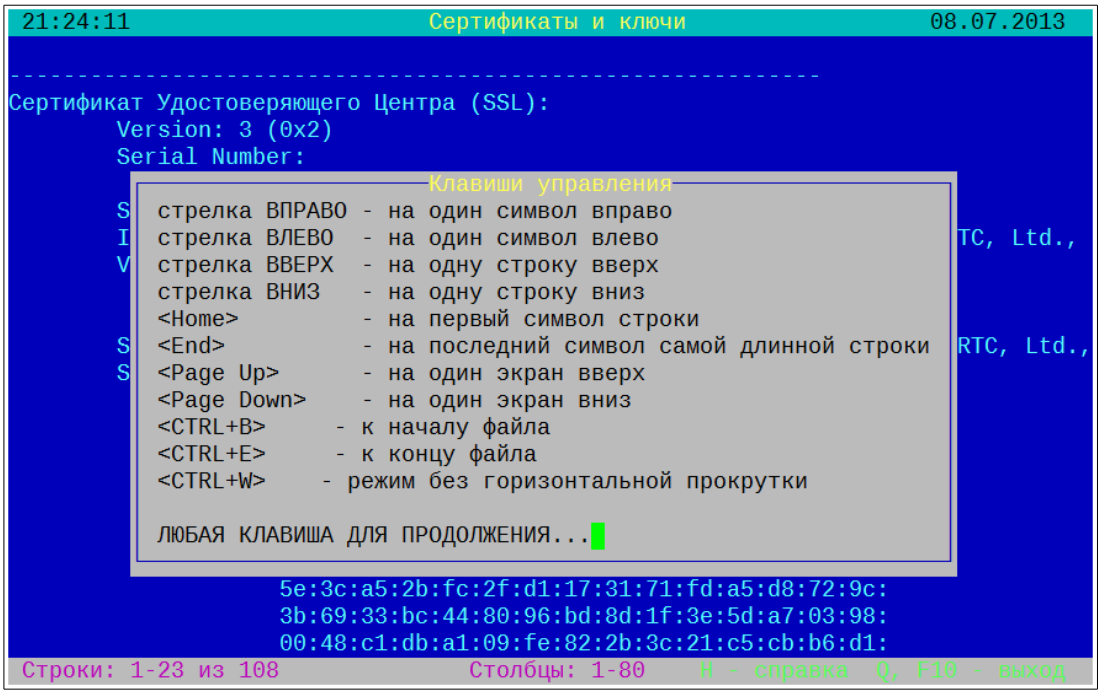

Рисунок 3.54: Просмотр сертификатов и ключей ССПТ-2

3.4.160. system password – изменение пароля системного пользователя

`syst[em] pass[word]`

Требуемые привилегии – **user** (только пользователь `admin`).

Команда изменяет пароль системного пользователя `fnpsh` для уровня системной авторизации, используемой для интерактивного режима командного интерфейса ССПТ-2 (раздел 2.5.1, стр. 10).

Изменить пароль системного пользователя имеет право только пользователь `admin`.

В ССПТ-2 существуют ограничения на формат пароля пользователя:

- длина пароля – от **6** до **128** символов;
- допустимые символы – только **печатаемые ASCII-символы**.

Эта команда является синонимом команды `system fnpsh password` (приложение 3.4.154, стр. 167).

Сначала команда запросит ввод текущего пароля системного пользователя. Затем, если текущий пароль введен верно, команда запросит ввод нового пароля. Новый пароль необходимо вводить дважды, чтобы исключить опечатки при вводе пароля с клавиатуры. Ввод паролей на терминале не отображается.

Пример:

```
fnpsh> system password
Старый пароль:
Новый пароль:
Новый пароль повторно:
FNPSH-I-309E-Пароль системного пользователя изменен
fnpsh>
```

3.4.161. system reboot – перезагрузка ССПТ-2

```
syst[em] reboot
```

Требуемые привилегии – **sys**.

Команда выполняет перезагрузку операционной системы ССПТ-2.

Не рекомендуется перезагружать ССПТ-2, используя кнопку аппаратного сброса (Reset), поскольку это может привести к серьезным нарушениям целостности файловой системы ССПТ-2.

Пример:

```
fnpsh> system reboot
Перегрузить устройство? (Y/N)  [N]: Y
FNPSH-I-3007-Устройство будет перезагружено через две минуты. Выход ...
```

3.4.162. system show – вывод информации о программном и аппаратном обеспечении ССПТ-2

```
syst[em] sh[ow]
```

Команда выводит на экран терминала информацию о характеристиках и состоянии программного и аппаратного обеспечения ССПТ-2.

Пояснения к строкам вывода команды `system show` приводятся в таблице 3.13.

Таблица 3.13: Информация о программном и аппаратном обеспечении ССПТ-2

Строка вывода	Описание
Модель ЦПУ	Характеристики центрального процессора – тип и тактовая частота, так как это распознается операционной системой ССПТ-2
Ядер ЦПУ	Количество вычислительных ядер центрального процессора, так как это определено операционной системой ССПТ-2
Объем памяти	Объем установленной оперативной памяти
Версия ПО ССПТ-2	Символическое имя и дата сборки используемой версии программного обеспечения ССПТ-2
Всего интерфейсов	Общее количество Ethernet-интерфейсов, установленных в системе
Фильтрующих интерфейсов	Общее количество фильтрующих интерфейсов ССПТ-2 и символические имена каждого из них
Управляющий интерфейс	Состояние и настройки IP-адреса управляющего Ethernet-интерфейса ССПТ-2
Пакетная фильтрация	Состояние пакетного фильтра ССПТ-2
Контроль целостности	Состояние сервера проверки контрольных сумм ССПТ-2
Авторизация	Состояние сервера авторизации ССПТ-2
Регистрация	Состояние сервера регистрации ССПТ-2
Резервирование	Состояние сервера высокой готовности ССПТ-2
Удаленное администрирование	Состояние командного сервера ССПТ-2
Удаленный терминальный доступ	Состояние сервера терминального доступа ССПТ-2
WEB интерфейс	Состояние WEB-интерфейса ССПТ-2
SNMP интерфейс	Состояние SNMP интерфейса ССПТ-2
Таймаут неактивности FNPSH	Тайм-аут неактивности для командного интерфейса ССПТ-2
Просмотрщик по умолчанию FNPSH	Режим просмотра данных для текущего сеанса пользователя в командном интерфейсе ССПТ-2

Пример:

```
fnpsh> system show
Модель ЦПУ                    | Intel(R) Core(TM) i7 CPU         870  @ 2.93GHz
```

```
Ядер ЦПУ                          | 1
Объем памяти                      | 536870912 байт (512М)
Версия ПО ССПТ-2                  | FNP2_RELEASE_1_3-p1.2 (Jun 24 2013)
Всего интерфейсов                 | 4
    Фильтрующих интерфейсов       | 3: eth0,eth1,eth2
    Управляющий интерфейс         | включен, 10.98.7.1/255.255.255.0
Пакетная фильтрация               | запущен
Контроль целостности              | запущен
Авторизация                       | запущен
Регистрация                       | запущен
Резервирование                    | запущен
Удаленное администрирование       | запущен
Удаленный терминальный доступ     | запущен
WEB интерфейс                     | запущен
SNMP интерфейс                    | остановлен
Тайм-аут неактивности FNPSH       | 600 секунд
Просмотрщик по умолчанию FNPSH    | внутренний (internal)
fnpsh>
```

3.4.163. system status – вывод информации о состоянии ресурсов операционной системы ССПТ-2

`syst[em] statu[s]`

Команда выводит на экран терминала информацию о состоянии и характеристиках ресурсов операционной системы ССПТ-2.

Пояснения к строкам вывода команды `system status` приводятся в таблице 3.14.

Таблица 3.14: Информация о состоянии ресурсов операционной системы ССПТ-2

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 flash-памяти:	Информация о разделах файловых систем – занятое пространство, свободное пространство, общий объем файловой системы: • `Раздел 0` – основной раздел на дисковом накопителе; • `Раздел 1` – специальная файловая система устройств (devfs – Device File System), используется только операционной системой ССПТ-2; • `Раздел 2` – файловая система в оперативной памяти (RAM-диск), используется для хранения временных файлов

Пример:

```
fnpsh> system status
Использование центрального процессора:
    Пользовательские процессы:  23,3%
    Приоритетные процессы:      0,0%
    Системные процессы:         71,4%
    Прерывания:                 5,3%
    Простой процессора:         0,0%
Использование оперативной памяти:
    Активная:                   14,0М
    Неактивная:                 3,0М
    Свободно:                   179,0М
    Всего:                      239М
Состояние flash-памяти:
  Раздел:               0
    Использовано:       54М (24%)
    Свободно:           175М (76%)
    Всего:              236М
  Раздел:               1
    Использовано:       1,0К (100%)
    Свободно:           0В (0%)
    Всего:              1,0К
  Раздел:               2
```

```
    Использовано:       4,0K (0%)
    Свободно:           26M (100%)
    Всего:              29M
fnpsh>
```

3.4.164. system time ntp delete – удаление параметров синхронизации времени по NTP

```
syst[em] time ntp del[ete]
```

Требуемые привилегии – **cfg**.

Команда выполняет удаление параметров синхронизации системного времени по протоколу NTP из текущей конфигурации ССПТ-2.

Предыдущие настройки параметров синхронизации системного времени по NTP, такие как IP-адрес NTP сервера и тайм-аут опроса NTP сервера, будут потеряны.

Синхронизация системного времени по NTP будет отключена.

Пример:

```
npsh> system time ntp delete
Удалить параметры NTP? (Y/N)  [N]: Y
FNPSH-I-305B-Параметры NTP удалены
fnpsh> system time show
Настройки системного времени:
    Дата:                       20.05.2011, пятница
    Время:                      12:19:22
    Часовой пояс:               GMT, GMT+0000
    NTP:                        отключено
    NTP сервер:                 отсутствует
    Регистрация сообщений NTP:  отключено
    Таймаут опроса NTP:         3600
fnpsh>
```

3.4.165. system time ntp disable – отключение синхронизации времени по NTP

```
syst[em] time ntp dis[able]
```

Требуемые привилегии – **cfg**.

Команда отключает синхронизацию системного времени по протоколу NTP и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, синхронизация системного времени по протоколу NTP отключена.

Пример:

```
fnpsh> system time ntp disable
Отключить NTP? (Y/N)  [N]: Y
FNPSH-I-305A-NTP отключен
fnpsh>
```

3.4.166. system time ntp enable – включение синхронизации времени по NTP

```
syst[em] time ntp en[able]
```

Требуемые привилегии – **cfg**.

Команда включает синхронизацию системного времени по протоколу NTP и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Для включения синхронизации системного времени по протоколу NTP необходимо предварительно установить IP-адрес NTP сервера, используя команду `system time ntp server` (приложение 3.4.169, стр. 176).

Примеры:

```
fnpsh> system time ntp enable
FNPSH-E-10BB-NTP сервер не определен
fnpsh>

fnpsh> system time ntp server 10.234.28.1
FNPSH-I-305C-Адрес NTP сервера изменен
fnpsh> system time ntp enable
FNPSH-I-3059-NTP включен
fnpsh>
```

3.4.167. system time ntp log disable – отключение регистрации NTP запросов

`syst[em] time ntp log dis[able]`

Требуемые привилегии – **cfg**.

Команда отключает регистрацию выполнения запросов синхронизации времени к NTP серверу и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, регистрация выполнения запросов синхронизации времени к NTP серверу отключена.

Пример:

```
fnpsh> system time ntp log disable
FNPSH-I-305F-Регистрация NTP сообщений отключена
fnpsh>
```

3.4.168. system time ntp log enable – включение регистрации NTP запросов

`syst[em] time ntp log en[able]`

Требуемые привилегии – **cfg**.

Команда включает регистрацию выполнения запросов синхронизации времени к NTP серверу и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Регистрация NTP запросов заключается в формировании и регистрации системного сообщения при каждом обращении к NTP серверу. Например:

```
Aug 16 07:47:36 fnp2 fnp[870]: fnp_csd: System time changed by NTP (server
192.168.169.254, offset -0.417829 sec)
```

Просмотр системных сообщений выполняется по команде `log syslog show` (приложение 3.4.54, стр. 106).

Пример:

```
fnpsh> system time ntp log enable
FNPSH-I-305E-Регистрация NTP сообщений включена
fnpsh>
```

3.4.169. system time ntp server – установка IP-адреса NTP сервера

`syst[em] time ntp serv[er] <IP_адрес>`

Требуемые привилегии – **cfg**.

Параметры:

- `<IP_адрес>` – IP-адрес NTP сервера.

Команда устанавливает IP-адрес NTP сервера в текущей конфигурации ССПТ-2.

Для успешного выполнения запросов NTP сервер должен быть доступен через управляющий Ethernet-интерфейс ССПТ-2.

Доступность NTP сервера по его IP-адресу можно проверить, используя команду `interface control ping` (приложение 3.4.28, стр. 72).

Пример:

```
fnpsh> system time ntp server 10.234.28.1
FNPSH-I-305C-Адрес NTP сервера изменен
fnpsh>
```

3.4.170. system time ntp timeout – установка тайм-аута опроса NTP сервера

`syst[em] time ntp timeo[ut] <тайм_аут>`

Требуемые привилегии – **cfg**.

Параметры:

- `<тайм_аут>` – новое значение тайм-аута опроса NTP сервера в секундах.

Команда изменяет значение тайм-аута опроса NTP сервера в текущей конфигурации ССПТ-2.

Тайм-аут опроса NTP сервера может быть изменен в пределах от **600** (10 минут) до **86400** (1 сутки) секунд включительно.

Пример:

```
fnpsh> system time ntp timeout 1800
FNPSH-I-3060-Таймаут NTP изменен
fnpsh>
```

3.4.171. system time ntp update – немедленная синхронизация времени с NTP сервером

`syst[em] time ntp upd[ate] [<IP_адрес>]`

Требуемые привилегии – **cfg**.

Параметры:

- `<IP_адрес>` – IP-адрес NTP сервера, которому будет отправлен запрос синхронизации системного времени.

Команда выполняет немедленную синхронизацию системного времени ССПТ-2 с NTP сервером.

IP-адрес NTP сервера может быть указан в командной строке как параметр `<IP_адрес>`. Если параметр отсутствует, будет использован IP-адрес NTP сервера, установленный в текущей конфигурации ССПТ-2 по команде `system time ntp server` (приложение 3.4.169, стр. 176).

Примеры:

```
fnpsh> system time ntp update
FNPSH-I-305D-Системное время изменено по NTP (поправка -0.005370 sec)
fnpsh>

fnpsh> system time ntp update 10.98.1.254
FNPSH-I-305D-Системное время изменено по NTP (поправка -0.009023 sec)
fnpsh>
```

3.4.172. system time set – установка системного времени

`syst[em] time set <время>`

Требуемые привилегии – **sys**.

Параметры:

- `<время>` – новое значение системного времени.

Команда устанавливает новое значение системного времени ССПТ-2 в соответствии с указанным параметром.

Параметр `<время>` имеет следующий синтаксис:

`{ГГГГ/ММ/ДД [ЧЧ:ММ:СС]|ЧЧ:ММ:СС},`

где

- `ГГГГ/ММ/ДД` – системная дата:
  - ✔ `ГГГГ` – четырехзначное значение года;
  - ✔ `ММ` – месяц года (от `01` до `12`);
  - ✔ `ДД` – день месяца от (`01` до `31`);
- `ЧЧ:ММ:СС` – системное время:
  - ✔ `ЧЧ` – часы в 24-х часовом формате (от `00` до `23`);
  - ✔ `ММ` – минуты (от `00` до `59`);
  - ✔ `СС` – секунды (от `00` до `59`).

При указании только системной даты системное время остается без изменения. И наоборот, при указании только системного времени не изменяется системная дата.

Просмотреть текущее значение системного времени можно, используя команду `system time show` (приложение 3.4.173, стр. 179).

Примеры:

- изменение только системной даты:

```
fnpsh> system time show
Настройки системного времени:
    Дата:                        20.05.2013, понедельник
    Время:                       12:21:32
    Часовой пояс:                GMT, GMT+0000
    NTP:                         включено
    NTP сервер:                  10.234.28.1
    Регистрация сообщений NTP:   включено
    Таймаут опроса NTP:          1800
fnpsh>system time set 2013/05/21
FNPSH-I-3057-Системное время изменено (21.05.2013 12:21:47, GMT)
fnpsh>
```

- изменение только системного времени:

```
fnpsh> system time set 12:22:00
FNPSH-I-3057-Системное время изменено (20.05.2011 12:22:00, GMT)
fnpsh>
```

- изменение системной даты и системного времени

```
fnpsh> system time set 2012/08/16 10:12:00
FNPSH-I-3057-Системное время изменено (16.08.2012 10:12:00, GMT)
fnpsh>
```

3.4.173. system time show – вывод системного времени и параметров синхронизации по NTP

```
syst[em] time sh[ow]
```

Команда выводит на экран терминала текущее значение системного времени ССПТ-2 с указанием часового пояса и значения параметров синхронизации системного времени по протоколу NTP.

Пояснения к строкам вывода команды `system time show` приводятся в таблице 3.15.

Таблица 3.15: Вывод системного времени ССПТ-2 и параметров синхронизации по NTP

Строка вывода	Описание
Дата:	Текущая системная дата с указанием дня недели
Время:	Текущее системное время
Часовой пояс:	Символическое обозначение часового пояса, сдвиг времени текущего часового пояса относительно Гринвича
NTP:	Флаг синхронизации системного времени по NTP
NTP сервер:	IP-адрес NTP сервера
Регистрация сообщений NTP:	Флаг регистрации запросов синхронизации времени к NTP серверу
Таймаут опроса NTP:	Значение тайм-аута опроса NTP сервера

Пример:

```
npsh> system time show
Настройки системного времени:
    Дата:                        20.05.2013, понедельник
    Время:                       12:21:32
    Часовой пояс:                GMT, GMT+0000
    NTP:                         включено
    NTP сервер:                  10.234.28.1
    Регистрация сообщений NTP:   включено
    Таймаут опроса NTP:          1800
fnpsh>
```

3.4.174. system time zone – установка часового пояса

```
syst[em] time zone
```

Требуемые привилегии – **sys**.

Команда запрашивает в интерактивном режиме и устанавливает новое значение часового пояса.

Выбор часового пояса осуществляется по запросу от командного интерфейса 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>`.

Уровни меню следующие:

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 только клавишу `<Enter>`.

Просмотреть текущие установки часового пояса можно, используя команду `system time show` (приложение 3.4.173, стр. 179).

Пример:

- установка Московского времени (часовой пояс `MSK` (зимнее время)/`MSD` (летнее время)):

```
fnpsh> 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
Выберите континент/регион (Отмена - <Enter>): 8
 [1] Aland Islands      [18] Guernsey          [35] Poland
 [2] Albania            [19] Hungary           [36] Portugal
 [3] Andorra            [20] Ireland           [37] Romania
 [4] Austria            [21] Isle of Man       [38] Russian Federatio
 [5] Belarus            [22] Italy             [39] San Marino
 [6] Belgium            [23] Jersey            [40] Serbia
 [7] Bosnia and Herzego [24] Latvia            [41] Slovakia
 [8] Bulgaria           [25] Liechtenstein     [42] Slovenia
 [9] Croatia            [26] Lithuania         [43] Spain
 [10] Czech Republic    [27] Luxembourg        [44] Sweden
 [11] Denmark           [28] Macedonia (The Fo [45] Switzerland
 [12] Estonia           [29] Malta             [46] Turkey
 [13] Finland           [30] Moldova           [47] Ukraine
 [14] France            [31] Monaco            [48] United Kingdom
 [15] Germany           [32] Montenegro        [49] Vatican City Stat
 [16] Gibraltar         [33] Netherlands
 [17] Greece            [34] Norway
Выберите страну/регион (Отмена - <Enter>): 38
 [1] Moscow-01 - Kaliningrad
 [2] Moscow+00 - west Russia
 [3] Moscow+00 - Caspian Sea
 [4] Moscow+01 - Samara, Udmurtia
 [5] Moscow+02 - Urals
 [6] Moscow+03 - west Siberia
 [7] Moscow+03 - Novosibirsk
 [8] Moscow+04 - Yenisei River
 [9] Moscow+05 - Lake Baikal
 [10] Moscow+06 - Lena River
 [11] Moscow+07 - Amur River
 [12] Moscow+07 - Sakhalin Island
 [13] Moscow+08 - Magadan
 [14] Moscow+09 - Kamchatka
 [15] Moscow+10 - Bering Sea
Выберите временную зону (Отмена - <Enter>): 2
FNPSH-I-3061-Часовой пояс изменен (MSK)
fnpsh>

npsh> system time show
Настройки системного времени:
    Дата:                       20.05.2013, понедельник
    Время:                      16:25:50
    Часовой пояс:               MSK, GMT+0400
    NTP:                        включено
    NTP сервер:                 10.234.28.1
    Регистрация сообщений NTP:  включено
    Таймаут опроса NTP:         1800
fnpsh>
```

3.4.175. system web disable – отключение WEB-интерфейса ССПТ-2

`syst[em] web dis[able]`

Требуемые привилегии – **sys** (консоль).

Команда отключает функционирование WEB-интерфейса администратора ССПТ-2.

По умолчанию, после первого запуска ССПТ-2, WEB-интерфейс администратора ССПТ-2 отключен.

Команда `system web disable` может быть выполнена только с системной консоли ССПТ-2 и только пользователем `admin`.

Примеры:

```
fnpsh> system web disable
FNPSH-E-111A-Выполнение данной команды разрешено только через системную консоль
fnpsh>

fnpsh> system web disable
FNPSH-I-30B8-WEB-интерфейс отключен
fnpsh>
```

3.4.176. system web enable – включение WEB-интерфейса ССПТ-2

`syst[em] web en[able]`

Требуемые привилегии – **sys** (консоль).

Команда включает функционирование WEB-интерфейса администратора ССПТ-2.

Команда `system web enable` может быть выполнена только с системной консоли ССПТ-2 и только пользователем `admin`.

Примеры:

```
fnpsh> system web enable
FNPSH-E-111A-Выполнение данной команды разрешено только через системную консоль
fnpsh>

fnpsh> system web enable
FNPSH-I-30B7-WEB-интерфейс включен
fnpsh>
```

3.4.177. user add – добавление нового пользователя

`us[er] add <имя_пользователя> <привилегии>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<имя_пользователя>` – имя нового пользователя;
- `<привилегии>` – набор привилегий, назначаемый новому пользователю.

Команда добавляет нового пользователя ССПТ-2 с указанным именем и с указанным набором привилегий.

Добавлять нового пользователя ССПТ-2 имеет право только пользователь `admin`.

В ССПТ-2 существуют ограничения на формат имени пользователя:

- длина имени пользователя – от **2** до **128** символов;
- допустимые символы:
  - ✔ первый символ – **строчные латинские символы** (a-z) и **цифры** (0-9);
  - ✔ последующие символы – **строчные латинские символы** (a-z), **цифры** (0-9) и символы '**_**' (подчеркивание), '**.**' (точка), '**-**' (дефис), '**@**'.

В ССПТ-2 существуют ограничения на формат пароля пользователя:

- длина пароля – от **6** до **128** символов;
- допустимые символы – только **печатаемые ASCII-символы**;
- пароль пользователя является регистрово-зависимым.

Каждому пользователю ССПТ-2 назначается список привилегий, определяющие права данного пользователя по управлению и настройке ССПТ-2. Привилегии дают право на работу с различными подсистемами ССПТ-2, каждая привилегия имеет символическое имя:

- `cfg` – настройка параметров конфигурации ССПТ-2;
- `ha` – работа с подсистемой высокой готовности;
- `log` – работа с подсистемой регистрации;
- `pf` – работа с пакетным фильтром;
- `rules` – работа с правилами фильтрации;
- `sys` – общее управление устройством и системные настройки;
- `user` – управление пользователями (*только для пользователя* `admin`).

Привилегией `user` обладает исключительно пользователь `admin`. Никакому другому пользователю ССПТ-2 эта привилегия назначена быть не может.

Списки привилегий могут задаваться двумя способами:

- используя символические имена привилегий;
- используя двоичную маску набора привилегий;

Использование символических имен. Формат списка привилегий, использующего символические имена следующий:

```
{cfg|ha|log|pf|rules|sys}[,...]
```

Список состоит из символических имен привилегий, разделенных запятой. Не допускается указывать в списке одну и ту же привилегию более одного раза. Например:

```
pf,log,sys
```

Пользователь получает тот набор прав, которые ему предоставляют в совокупности привилегии, указанные в списке.

Использование двоичной маски набора привилегий. Формат двоичной маски набора привилегий следующий:

```
{0|1}{0|1}{0|1}{0|1}{0|1}{0|1}{0|1}
```

При использовании двоичной маски наличие или отсутствие привилегии в наборе обозначается символами '`1`' или '`0`' соответственно. Длина двоичной маски всегда должна равняться общему количеству существующих привилегий – в ССПТ-2 имеется **7** различных привилегий. Каждая позиция в двоичной маске отвечает за одну привилегию. Если пронумеровать позиции справа налево от `1` до `7`, то используется следующее распределение привилегий по позициям двоичной маски:

```
7 – user|6 – ha|5 – sys|4 – pf|3 – rules|2 – cfg|1 – log
```

Для всех пользователей ССПТ-2, кроме `admin`, значение позиции двоичной маски, соответствующей привилегии `user`, всегда должно равняться `0`.

Например, двоичная маска

```
0011001
```

соответствует списку привилегий `sys,pf,log`.

Некоторые наборы привилегий имеют специальные символические имена

- `read` – означает отсутствие каких бы то ни было привилегий (режим "*только чтение*") – двоичная маска набора привилегий `0000000`;

- `full` – обозначает полный набор привилегий за исключением привилегии `user` – список привилегий `ha,sys,pf,rules,cfg,log`; двоичная маска `0111111`;
- `admin` – обозначает полный набор привилегий, включая привилегию `user` (*таким набором привилегий может обладать только пользователь* `admin`) – список привилегий `user,ha,sys,pf,rules,cfg,log`; двоичная маска `1111111`.

Команда запросит ввод пароля для нового пользователя. Пароль необходимо вводить дважды, чтобы исключить опечатки при вводе пароля с клавиатуры. Ввод паролей на терминале не отображается.

Примеры:

- использование символических имен привилегий:

```
fnpsh> user add fnp2_ag sys,pf,log
Новый пароль:
Новый пароль повторно:
FNPSH-I-3089-Пользователь добавлен (fnp2_ag)
```

- использование двоичной маски набора привилегий:

```
fnpsh> user add fnp2_ag 0011001
Новый пароль:
Новый пароль повторно:
FNPSH-I-3089-Пользователь добавлен (fnp2_ag)
```

3.4.178. user delete – удаление пользователя

`us[er] del[ete] <имя_пользователя>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<имя_пользователя>` – имя существующего пользователя ССПТ-2.

Команда удаляет пользователя ССПТ-2.

Удалять пользователей ССПТ-2 имеет право только пользователь `admin`.

Пользователь `admin` не может быть удален.

Примеры:

```
fnpsh> user delete fnp2_ag
FNPSH-E-101A-Недостаточно привилегий для операции
fnpsh>

fnpsh> user delete admin
FNPSH-W-2016-Пользователь не может быть удален
fnpsh>

fnpsh> user delete fnp2_ag
Удалить пользователя? (Y/N)  [N]: Y
FNPSH-I-308A-Пользователь удален (fnp2_ag)
fnpsh>
```

3.4.179. user disable – отключение пользователя

`us[er] dis[able] <имя_пользователя>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<имя_пользователя>` – имя существующего пользователя ССПТ-2.

Команда отключает существующего пользователя ССПТ-2 без удаления его учетной записи, запрещая ему последующую работу со средствами администрирования ССПТ-2.

Отключать пользователей ССПТ-2 имеет право только пользователь admin.

Пользователь admin не может быть отключен.

Пример:

```
fnpsh> user disable fnp2_ag
Отключить пользователя? (Y/N)  [N]: Y
FNPSH-I-308B-Пользователь отключен (fnp2_ag)
fnpsh>
```

3.4.180. user enable – включение пользователя

us[er] en[able] <имя_пользователя>

Требуемые привилегии – **user** (только пользователь admin).

Параметры:

- <имя_пользователя> – имя существующего пользователя ССПТ-2.

Команда включает существующего пользователя ССПТ-2, разрешая ему последующую работу со средствами администрирования ССПТ-2.

Включать пользователей ССПТ-2 имеет право только пользователь admin.

Пример:

```
fnpsh> user enable fnp2_ag
Активировать пользователя? (Y/N)  [N]: Y
FNPSH-I-308C-Пользователь включен (fnp2_ag)
fnpsh>
```

3.4.181. user list – просмотр списка существующих пользователей

us[er] lis[t]

Команда выводит на экран терминала общее количество и список существующих пользователей ССПТ-2. Список пользователей выводится в виде таблицы, содержащей следующие поля:

- Пользователь – имя пользователя;
- Привилегии – привилегии, назначенные данному пользователя. Выводятся в формате списка привилегий, использующего символические имена (приложение 3.4.177, стр.181);
- Статус – активность пользователя, управляемая командами user disable и user enable.

Пример:

```
fnpsh> user list
Всего пользователей: 2

Пользователь Привилегии Статус
admin        admin      включено
fnp2_ag      log,pf,sys включено
fnpsh>
```

3.4.182. user password – изменение пароля пользователя

us[er] pass[word] <имя_пользователя>

Требуемые привилегии – **user** (только пользователь admin) или тот же самый пользователь.

Параметры:

- <имя_пользователя> – имя существующего пользователя ССПТ-2.

Команда изменяет пароль пользователя ССПТ-2.

Изменять пароль всем пользователям ССПТ-2 имеет право только пользователь admin. Любой другой пользователь может изменить пароль **только самому себе**.

В ССПТ-2 существуют ограничения на формат пароля пользователя:

- длина пароля – от **6** до **128** символов;
- допустимые символы – только **печатаемые ASCII-символы**;
- пароль пользователя является регистрово-зависимым.

Команда запросит ввод старого пароля в том случае, когда пользователь изменяет пароль самому себе, включая также и пользователя admin. Затем, если старый пароль введен правильно, команда запросит ввод нового пароля. Новый пароль необходимо вводить дважды, чтобы исключить опечатки при вводе пароля с клавиатуры. Ввод паролей на терминале не отображается.

Ввод старого пароля не требуется, если пользователь admin изменяет пароль любому другому пользователю.

Пример:

```
fnpsh> user password fnp2_ag
Старый пароль:
Новый пароль:
Новый пароль повторно:
FNPSH-I-308D-Пароль пользователя изменен (fnp2_ag)
fnpsh>
```

3.4.183. user privilege – изменение привилегий пользователя

us[er] privi[lege] <имя_пользователя> <привилегии>

Требуемые привилегии – **user** (только пользователь admin).

Параметры:

- <имя_пользователя> – имя существующего пользователя ССПТ-2;
- <привилегии> – новый набор привилегий, который будет назначен указанному пользователю.

Команда назначает новый набор привилегий указанному пользователю ССПТ-2.

Изменять привилегии пользователей ССПТ-2 имеет право только пользователь admin.

Не допускается изменять привилегии пользователю admin.

Каждому пользователю ССПТ-2 назначается список привилегий, определяющие права данного пользователя по управлению и настройке ССПТ-2. Привилегии дают право на работу с различными подсистемами ССПТ-2, каждая привилегия имеет символическое имя:

- cfg – настройка параметров конфигурации ССПТ-2;
- ha – работа с подсистемой высокой готовности;
- log – работа с подсистемой регистрации;
- pf – работа с пакетным фильтром;
- rules – работа с правилами фильтрации;
- sys – общее управление устройством и системные настройки;
- user – управление пользователями (*только для пользователя* admin).

Привилегией `user` обладает исключительно пользователь `admin`. Никакому другому пользователю ССПТ-2 эта привилегия назначена быть не может.

Списки привилегий могут задаваться двумя способами:

- используя символические имена привилегий;
- используя двоичную маску набора привилегий;

Использование символических имен. Формат списка привилегий, использующего символические имена следующий:

```
{cfg|ha|log|pf|rules|sys}[,...]
```

Список состоит из символических имен привилегий, разделенных запятой. Не допускается указывать в списке одну и ту же привилегию более одного раза. Например:

```
cfg,rules,sys
```

Пользователь получает тот набор прав, которые ему предоставляют в совокупности привилегии, указанные в списке.

Использование двоичной маски набора привилегий. Формат двоичной маски набора привилегий следующий:

```
{0|1}{0|1}{0|1}{0|1}{0|1}{0|1}{0|1}
```

При использовании двоичной маски наличие или отсутствие привилегии в наборе обозначается символами '`1`' или '`0`' соответственно. Длина двоичной маски всегда должна равняться общему количеству существующих привилегий – в ССПТ-2 имеется **7** различных привилегий. Каждая позиция в двоичной маске отвечает за одну привилегию. Если пронумеровать позиции справа налево от `1` до `7`, то используется следующее распределение привилегий по позициям двоичной маски:

```
7 – user|6 – ha|5 – sys|4 – pf|3 – rules|2 – cfg|1 – log
```

Для всех пользователей ССПТ-2, кроме `admin`, значение позиции двоичной маски, соответствующей привилегии `user`, всегда должно равняться `0`.

Например, двоичная маска

```
0010110
```

соответствует списку привилегий `sys,rules,cfg`.

Некоторые наборы привилегий имеют специальные символические имена

- `read` – означает отсутствие каких бы то ни было привилегий (режим "*только чтение*") – двоичная маска набора привилегий `0000000`;
- `full` – обозначает полный набор привилегий за исключением привилегии `user` – список привилегий `ha,sys,pf,rules,cfg,log`; двоичная маска `0111111`;
- `admin` – обозначает полный набор привилегий, включая привилегию `user` (*таким набором привилегий может обладать только пользователь* `admin`) – список привилегий `user,ha,sys,pf,rules,cfg,log`; двоичная маска `1111111`.

Примеры:

- использование символических имен привилегий:

```
fnpsh> user privilege fnp2_ag sys,rules,cfg
Изменить привилегии пользователя? (Y/N)  [N]: Y
FNPSH-I-308E-Привилегии пользователя изменены (fnp2_ag)
fnpsh>
```

- использование двоичной маски набора привилегий:

```
fnpsh> user privilege fnp2_ag 0010110
Изменить привилегии пользователя? (Y/N)  [N]: Y
FNPSH-I-308E-Привилегии пользователя изменены (fnp2_ag)
fnpsh>
```

3.4.184. user radius disable – отключение RADIUS авторизации

`us[er] rad[ius] dis[able]`

Требуемые привилегии – **user** (только пользователь `admin`).

Команда отключает авторизацию пользователей ССПТ-2 на удаленном RADIUS сервере и изменяет соответствующие настройки в текущей конфигурации ССПТ-2. Авторизация пользователей будет выполняться в локальном режиме.

По умолчанию, после первого запуска ССПТ-2, авторизация пользователей на удаленном RADIUS сервере отключена.

Команда `user radius disable` может быть выполнена только с системной консоли ССПТ-2 и только пользователем `admin`.

Если на момент выполнения команды `user radius disable` RADIUS авторизация уже была отключена, то ее состояние останется без изменений.

Примеры:

```
fnpsh> user radius disable
FNPSH-E-111A-Выполнение данной команды разрешено только через системную консоль
fnpsh>

fnpsh> user radius disable
FNPSH-I-30B4-Использование RADIUS отключено
fnpsh>
```

3.4.185. user radius enable – включение RADIUS авторизации

`us[er] rad[ius] en[able]`

Требуемые привилегии – **user** (только пользователь `admin`).

Команда включает авторизацию пользователей ССПТ-2 на удаленном RADIUS сервере и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

Команда `user radius enable` может быть выполнена только с системной консоли ССПТ-2 и только пользователем `admin`.

Если на момент выполнения команды `user radius enable` RADIUS авторизация уже была отключена, то ее состояние останется без изменений.

Выполнение команды `user radius enable` возможно только при настроенных параметрах RADIUS сервера – команда `user radius server` ().

Примеры:

```
fnpsh> user radius enable
FNPSH-E-111A-Выполнение данной команды разрешено только через системную консоль
fnpsh>

fnpsh> user radius enable
FNPSH-I-30B3-Использование RADIUS включено
fnpsh>
```

3.4.186. user radius retry – установка максимального количества попыток обращения к RADIUS серверу

`us[er] rad[ius] ret[ry] <число_попыток>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<число_попыток>` – новое значение максимального количества попыток обращения к RADIUS серверу.

Команда устанавливает новое значение максимального количества попыток обращения к RADIUS серверу и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию установлено максимум **3** попытки обращения к RADIUS серверу.

Этот параметр учитывается только при неудачных обращениях к RADIUS серверу.

Изменять максимальное количество попыток обращения к RADIUS серверу имеет право только пользователь `admin`.

Максимальное количество попыток обращения к RADIUS серверу может быть установлено в пределах от **1** до **10** включительно.

Пример:

```
fnpsh> user radius retry 8
FNPSH-I-30B7-Количество обращений к RADIUS серверу изменено
fnpsh>
```

3.4.187. user radius server – настройка параметров RADIUS авторизации

`us[er] rad[ius] serv[er] <тип> <IP_адрес> <ключ> <порт>`

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<тип>` – тип RADIUS сервера. В параметрах RADIUS авторизации может быть задано два RADIUS сервера:
  - ✔ `master` – основной RADIUS сервер, его параметры должны быть заданы обязательно;
  - ✔ `slave` – дополнительный RADIUS сервер. Если его параметры заданы, то дополнительный RADIUS сервер будет использован в том случае, когда попытки соединения с основным RADIUS сервером завершились неудачно;
- `<IP_адрес>` – IP-адрес RADIUS сервера указанного типа;
- `<ключ>` – ключ для кодирования запросов авторизации пользователей, посылаемых на указанный RADIUS сервер;
- `<порт>` – номер прикладного порта указанного RADIUS сервера.

Команда устанавливает параметры RADIUS авторизации в текущей конфигурации ССПТ-2.

Общепринятым номером прикладного порта RADIUS сервера для авторизации пользователей является порт **1812**.

Ранее для этих целей использовался порт с номером **1645** (устаревшее значение).

Настраивать параметры RADIUS авторизации имеет право только пользователь `admin`.

В ССПТ-2 существуют ограничения на формат ключа RADIUS сервера:

- длина ключа – не более **128** символов;
- допустимые символы – только **печатаемые ASCII-символы**;
- ключ RADIUS сервера является регистрово-зависимым.

Примеры:

- настройка основного RADIUS сервера:

```
npsh> user radius server master 192.168.169.252 secret_master 1812
FNPSH-I-30B5-Конфигурация RADIUS сервера изменена
fnpsh>
```

- настройка дополнительного RADIUS сервера:

```
fnpsh> user radius server slave 192.168.169.252 secret_slave 1645
FNPSH-I-30B5-Конфигурация RADIUS сервера изменена
fnpsh>
```

3.4.188. user radius show – просмотр параметров RADIUS авторизации

```
us[er] rad[ius] sh[ow]
```

Команда выводит на экран терминала параметры RADIUS авторизации, установленные в текущей конфигурации ССПТ-2.

Пример:

```
fnpsh> user radius show
Использование RADIUS:           отключено
Таймаут ожидания:               10
Количество обращений к серверу: 8
Первичный (MASTER) сервер:      192.168.169.252
    Секретный ключ:             secret_master
    Порт:                       1812
Вторичный (SLAVE) сервер:       192.168.169.252
    Секретный ключ:             secret_slave
    Порт:                       1645
fnpsh>
```

3.4.189. user radius timeout – установка тайм-аута ожидания ответа от RADIUS сервера

```
us[er] rad[ius] timeo[ut] <тайм_аут>
```

Требуемые привилегии – **user** (только пользователь `admin`).

Параметры:

- `<тайм_аут>` – новое значение тайм-аута ожидания ответа от RADIUS сервера в секундах.

Команда устанавливает новое значение тайм-аута ожидания ответа от RADIUS сервера и изменяет соответствующие настройки в текущей конфигурации ССПТ-2.

По умолчанию тайм-аут ожидания ответа от RADIUS сервера составляет **5** секунд.

Установка тайм-аута ожидания ответа от RADIUS сервера в значение **0** означает получение ответа за время менее **1** секунды.

Изменять значение тайм-аута ожидания ответа от RADIUS сервера имеет право только пользователь `admin`.

Тайм-аут ожидания ответа от RADIUS сервера может быть установлен в пределах от **0** до **10** секунд включительно.

Пример:

```
fnpsh> user radius timeout 10
FNPSH-I-30B6-Таймаут ожидания ответа от RADIUS-сервера изменен
fnpsh>
```

3.4.190. user show – просмотр списка активных пользователей

```
us[er] sh[ow]
```

Команда выводит на экран терминала общее количество и список активных сеансов работы пользователей. Список активных сеансов работы пользователей выводится в виде таблицы, содержащей следующие поля:

- `Пользователь` – имя пользователя, которому принадлежит данный сеанс работы;
- `Начало работы` – время начала данного сеанса работы пользователя;
- `Откуда` – IP-адрес управляющего компьютера, с которого ведется данный сеанс работы пользователя. `Console` – в случае работы с системной консоли ССПТ-2;
- `Привилегии` – текущий набор привилегий, назначенный данному сеансу работы пользователя;
- `Неактивность` – время, прошедшее с момента ввода последней команды в рамках данного сеанса работы пользователя.

Пример:

```
fnpsh> user show
Активных пользователей: 2    Системное время: 06.09.2007 11:33:01 (GMT)

Пользователь Начало работы            Откуда          Привилегии     Неактивность
fnp2_ag      06.05.2013 11:31:38      10.98.1.1       cfg,rules,sys  1м 6с
admin        06.05.2013 11:32:31      Console         log,pf,user,ha 24с
fnpsh>
```

3.5. Диагностические сообщения командного интерфейса ССПТ-2

Приложение содержит следующие разделы:

- описание формата вывода диагностических сообщений командного интерфейса ССПТ-2 (приложение 3.5.1, стр. 190);
- описание всех диагностических сообщений командного интерфейса ССПТ-2:
  - ✔ информационные сообщения (приложение 3.5.2, стр. 191);
  - ✔ предупреждения (приложение 3.5.3, стр. 199);
  - ✔ сообщения об ошибках (приложение 3.5.4, стр. 203).

3.5.1. Формат вывода диагностических сообщений

Диагностическое сообщение имеет следующий формат вывода:

```
FNPSH-{I|W|E}-XXXX-<текст_сообщения>[ (<системная_ошибка>)]
```

где:

- `I|W|E` – один из трех возможных уровней диагностического сообщения:
  - ✔ `I` – информационное сообщение;
  - ✔ `W` – предупреждение;
  - ✔ `E` – сообщение об ошибке.
- `XXXX` – шестнадцатеричный код диагностического сообщения;
- `<текст_сообщения>` – текстовая интерпретация кода диагностического сообщения;
- `<системная_ошибка>` – необязательное сообщение, включаемое в строку диагностического сообщения, если при выполнении команды произошла системная ошибка. Сообщения о системных ошибках являются стандартными для операционной системы ССПТ-2. Сообщение о системной ошибке всегда выводится на *английском языке*.

Например, диагностическое сообщение

```
FNPSH-I-3087-Режим просмотра изменен
```

является *информационным сообщением* с кодом `0x3087` (шестнадцатеричный).

3.5.2. Информационные сообщения

Коды всех информационных сообщений, их текстовая интерпретация и описание представлены в таблице 3.16.

Таблица 3.16: Информационные сообщения командного интерфейса ССПТ-2

Код	Сообщение	Описание
3000	Нет ошибок	Сообщение используется только для уведомления WEB-интерфейса ССПТ-2 об успешном завершении выполнения команды
3001	Успешная авторизация пользователя	Введены правильные имя пользователя и пароль и начался сеанс работы пользователя
3002	Пользователь все еще работает	Сообщение используется только для уведомления WEB-интерфейса ССПТ-2 о том, что пользователь продолжает работу в рамках установленного сеанса работы
3003	Завершение работы пользователя	Пользователь завершил сеанс работы
3004	Выход пользователя по тайм-ауту неактивности	Пользователь завершил сеанс работы после истечения времени тайм-аута неактивности
3005	Таймаут неактивности	Сеанс работы пользователя завершается автоматически по причине истечения времени тайм-аута неактивности
3006	Устройство будет выключено через две минуты. Выход ...	Начался процесс останова операционной системы и выключения ССПТ-2
3007	Устройство будет перезагружено через две минуты. Выход ...	Начался процесс перезагрузки операционной системы ССПТ-2
3008	VLAN-группа добавлена	Добавлена новая VLAN-группа в текущий набор правил. Выводится номер добавленной VLAN-группы
3009	MAC-правило добавлено	Добавлено новое MAC-правило фильтрации в текущий набор правил. Выводится номер добавленного MAC-правила
300A	ARP-правило добавлено	Добавлено новое ARP-правило фильтрации в текущий набор правил. Выводится номер добавленного ARP-правила
300B	IP-правило добавлено	Добавлено новое IP-правило фильтрации в текущий набор правил. Выводится номер добавленного IP-правила
300C	IPX-правило добавлено	Добавлено новое IPX-правило фильтрации в текущий набор правил. Выводится номер добавленного IPX-правила
300D	Интервал времени добавлен	Добавлен новый интервал времени в текущий набор правил. Выводится номер добавленного интервала времени
300E	AP-правило добавлено	Добавлено новое AP-правило фильтрации в текущий набор правил. Выводится номер добавленного AP-правила
300F	VLAN-группа изменена	Изменена существующая VLAN-группа текущего набора правил. Выводится номер VLAN-группы
3010	MAC-правило изменено	Изменено существующее MAC-правило фильтрации текущего набора правил. Выводится номер MAC-правила
3011	ARP-правило изменено	Изменено существующее ARP-правило фильтрации текущего набора правил. Выводится номер ARP-правила
3012	IP-правило изменено	Изменено существующее IP-правило фильтрации текущего набора правил. Выводится номер IP-правила

Код	Сообщение	Описание
3013	IPX-правило изменено	Изменено существующее IPX-правило фильтрации текущего набора правил. Выводится номер IPX-правила
3014	Интервал времени изменен	Изменен существующий интервал времени текущего набора правил. Выводится номер интервала времени
3015	AP-правило изменено	Изменено существующее AP-правило фильтрации текущего набора правил. Выводится номер AP-правила
3016	VLAN-группа удалена	Удалена VLAN-группа из текущего набора правил. Выводится номер удаленной VLAN-группы
3017	MAC-правило удалено	Удалено MAC-правило фильтрации из текущего набора правил. Выводится номер удаленного MAC-правила
3018	ARP-правило удалено	Удалено ARP-правило фильтрации из текущего набора правил. Выводится номер удаленного ARP-правила
3019	IP-правило удалено	Удалено IP-правило фильтрации из текущего набора правил. Выводится номер удаленного IP-правила
301A	IPX-правило удалено	Удалено IPX-правило фильтрации из текущего набора правил. Выводится номер удаленного IPX-правила
301B	Интервал времени удален	Удален интервал времени из текущего набора правил. Выводится номер удаленного интервала времени
301C	AP-правило удалено	Удалено AP-правило фильтрации из текущего набора правил. Выводится номер удаленного AP-правила
301D	Сетевой пользователь добавлен	Добавлен новый сетевой пользователь
301E	Дополнительный набор правил загружен	Выполнена загрузка дополнительного набора правил в текущий
301F	Дополнительный набор правил сохранен	Выполнено сохранение текущего набора правил в дополнительный
3020	Дополнительный набор правил удален	Удален дополнительный набор правил. Удаленный набор правил не может быть восстановлен
3021	Предыдущее состояние текущего набора правил восстановлено	Отменено последнее изменение в текущем наборе правил
3022	Буфер истории команд очищен	Выполнена очистка буфера истории команд командного интерфейса ССПТ-2
3023	Буфер истории команд пустой	В буфере истории команд командного интерфейса ССПТ-2 нет ни одной сохраненной команды
3024	IP-адрес управляющего интерфейса изменен	Назначен новый IP-адрес управляющему Ethernet-интерфейсу ССПТ-2
3025	IP-адрес управляющего интерфейса удален	Удален IP-адрес с управляющего Ethernet-интерфейса ССПТ-2. Управление по сети Ethernet станет невозможным
3026	Фильтрующий интерфейс отключен	Заблокирован фильтрующий интерфейс ССПТ-2. Прием и передача пакетов через этот интерфейс выполняться не будет. Выводится символическое имя фильтрующего интерфейса
3027	Фильтрующий интерфейс включен	Разблокирован фильтрующий интерфейс ССПТ-2. Выводится символическое имя фильтрующего интерфейса
3028	Скорость передачи управляющего интерфейса изменена	Изменена скорость передачи на управляющем Ethernet-интерфейсе ССПТ-2
3029	Режим передачи управляющего интерфейса изменен	Изменен режим передачи на управляющем Ethernet-интерфейсе ССПТ-2
302A	Интерфейс переименован	Фильтрующему интерфейсу ССПТ-2 присвоено новое символическое имя

Код	Сообщение	Описание
302B	Маршрут по умолчанию добавлен	В маршрутную таблицу ССПТ-2 добавлен маршрут по умолчанию. Настройки запоминаются в текущей конфигурации
302C	Маршрут по умолчанию удален	Из маршрутной таблицы ССПТ-2 удален маршрут по умолчанию. Настройки удаляются из текущей конфигурации
302D	Режим передачи фильтрующего интерфейса изменен	Изменен режим передачи на фильтрующем интерфейсе ССПТ-2. Выводится символическое имя фильтрующего интерфейса
302E	Скорость передачи фильтрующего интерфейса изменена	Изменена скорость передачи на фильтрующем интерфейсе ССПТ-2. Выводится символическое имя фильтрующего интерфейса
302F	Новая запись добавлена в список доступа	Добавлена новая запись в список доступа к управлению ССПТ-2
3030	Запись удалена из списка доступа	Удалена запись из списка доступа к управлению ССПТ-2
3031	Список доступа очищен	Удалены все записи из списка доступа к управлению ССПТ-2. Доступ к управлению ССПТ-2 может быть получен с любого IP-адреса
3032	Маршрут по умолчанию включен	В маршрутную таблицу ССПТ-2 добавлен маршрут по умолчанию в соответствии с имеющимися настройками текущей конфигурации
3033	Маршрут по умолчанию отключен	Из маршрутной таблицы ССПТ-2 удален маршрут по умолчанию. Настройки IP-адреса шлюза по умолчанию в текущей конфигурации остаются без изменения
3034	Зеркалирование интерфейсов отключено	Режим зеркалирования трафика отключен. Настройки удаляются из текущей конфигурации
3035	Зеркалирование интерфейсов включено	Включен режим зеркалирования трафика на фильтрующих интерфейсах ССПТ-2
3036	Выгрузка журналов регистрации по FTP включена	Включен режим выгрузки файлов регистрации на удаленный FTP сервер в соответствии с имеющимися настройками текущей конфигурации
3037	Параметры выгрузки журналов регистрации по FTP определены	В текущей конфигурации сохранены новые настройки выгрузки файлов регистрации на удаленный FTP сервер
3038	Выгрузка журналов регистрации по FTP отключена	Режим выгрузки файлов регистрации на удаленный FTP сервер отключен.
3039	Параметры выгрузки журналов регистрации по FTP очищены	Из текущей конфигурации удалены настройки выгрузки файлов регистрации на удаленный FTP сервер. Режим выгрузки файлов регистрации отключен
303A	Пакетный фильтр остановлен	Выполнен останов пакетного фильтра ССПТ-2. Прекращается прием и передача пакетов через фильтрующие интерфейсы
303B	Режим управления сессиями включен	Включен режим управления сессиями пакетного фильтра ССПТ-2
303C	Режим управления сессиями отключен	Режим управления сессиями пакетного фильтра ССПТ-2 отключен
303D	Регистрация IP пакетов, отброшенных механизмом управления сессиямм, включена	Начинается регистрация пакетов, отброшенных механизмом управления сессиями пакетного фильтра ССПТ-2
303E	Регистрация IP пакетов, отброшенных механизмом управления сессиями, отключена	Регистрация пакетов, отброшенных механизмом управления сессиями пакетного фильтра ССПТ-2 прекращается
303F	Использование AP-правил включено	При включенном режиме управления сессиями пакетного фильтра ССПТ-2 будут использоваться AP-правила фильтрации

Код	Сообщение	Описание
3040	Использование АР-правил отключено	При включенном режиме управления сессиями пакетного фильтра ССПТ-2 АР-правила фильтрации использоваться не будут
3041	Сессии будут создаваться по умолчанию для IP-правил	Включается режим создания по умолчанию сессий для IP-правил фильтрации
3042	Сессии не будут создаваться по умолчанию для IP-правил	Режим создания по умолчанию сессий для IP-правил фильтрации выключается
3043	Таймаут неактивности TCP сессии изменен	Изменено значение тайм-аута неактивности для сессий, базирующихся на протоколе TCP
3044	Таймаут неактивности UDP сессии изменен	Изменено значение тайм-аута неактивности для сессий, базирующихся на протоколе UDP
3045	Таймаут неактивности ICMP сессии изменен	Изменено значение тайм-аута неактивности для сессий, базирующихся на протоколе ICMP
3046	Таймаут неактивности сессии для остальных протоколов изменен	Изменено значение тайм-аута неактивности для сессий, базирующихся на протоколах, отличных от TCP, UDP и ICMP
3047	Пакетный фильтр работает	Сообщение используется только для уведомления WEB-интерфейса ССПТ-2 о том, что пакетный фильтр находится в активном состоянии
3048	Пакетный фильтр запущен	Выполнен запуск пакетного фильтра ССПТ-2
3049	Размер таблицы сессий изменен. Необходимо перезапустить пакетный фильтр	Изменен размер таблицы сессий пакетного фильтра ССПТ-2. Для того, чтобы изменения вступили в силу необходимо перезапустить пакетный фильтр
304A	Таблица сессий очищена	Удалены все активные сессии из таблицы сессий пакетного фильтра ССПТ-2
304B	Сессия удалена	Выполнено удаление сессии с указанным номером из таблицы сессий пакетного фильтра ССПТ-2
304C	Таймаут неактивности сессий установлен по умолчанию	Тайм-аутам неактивности сессий присвоены значения по умолчанию
304D	Использование данных MAC-уровня в сессиях включено	В механизме управления сессиями для обрабатываемых пакетов включается контроль неизменности MAC-адресов источника и получателя
304E	Использование данных MAC-уровня в сессиях отключено	В механизме управления сессиями для обрабатываемых пакетов отключается контроль неизменности MAC-адресов источника и получателя
304F	Дополнительная конфигурация сохранена	Текущая конфигурация ССПТ-2 сохранена в дополнительной конфигурации
3050	Дополнительная конфигурация удалена	Удалена дополнительная конфигурация ССПТ-2
3051	Дополнительная конфигурация загружена	Дополнительная конфигурация ССПТ-2 загружена в текущую конфигурацию. Может потребоваться перезапуск пакетного фильтра
3052	Конфигурация по умолчанию загружена	Всем параметрам текущей конфигурации ССПТ-2 присвоены значения по умолчанию
3053	Управляющий интерфейс отключен	Отключен управляющий Ethernet-интерфейс ССПТ-2. Настройки IP-адреса управляющего Ethernet-интерфейса в текущей конфигурации остаются без изменения
3054	Управляющий интерфейс включен	Включен управляющий Ethernet-интерфейс ССПТ-2 в соответствии с настройками IP-адреса в текущей конфигурации
3055	Временное IP-правило добавлено	В текущий набор правил добавлено новое временное IP-правило фильтрации. Выводится номер добавленного временного IP-правила
3056	Временное IP-правило изменено	Изменено существующее временное IP-правило фильтрации текущего набора правил. Выводится номер временного IP-правила

Код	Сообщение	Описание
3057	Системное время изменено	Изменено системное время операционной системы ССПТ-2
3058	Системная дата изменена	Изменена системная дата операционной системы ССПТ-2
3059	NTP включен	Включена синхронизация системного времени ССПТ-2 по протоколу NTP
305A	NTP отключен	Синхронизация системного времени ССПТ-2 по протоколу NTP отключена
305B	Параметры NTP удалены	Из текущей конфигурации удалены настройки синхронизации системного времени ССПТ-2 по протоколу NTP. Синхронизация системного времени отключена
305C	Адрес NTP сервера изменен	Изменен IP-адрес NTP сервера в текущей конфигурации ССПТ-2
305D	Системное время изменено по NTP	Выполнена немедленная синхронизация системного времени ССПТ-2 по протоколу NTP в соответствии с настройками текущей конфигурации
305E	Регистрация NTP сообщений включена	Включена регистрация системных сообщений о результатах выполнения синхронизации системного времени по протоколу NTP
305F	Регистрация NTP сообщений отключена	Регистрация системных сообщений о результатах выполнения синхронизации системного времени по протоколу NTP отключена
3060	Таймаут NTP изменен	Изменено значение периода синхронизации системного времени по протоколу NTP – тайм-аут опроса NTP сервера
3061	Часовой пояс изменен	Изменены настройки часового пояса операционной системы ССПТ-2
3062	Пакетный фильтр перезапущен	Выполнен перезапуск пакетного фильтра ССПТ-2
3063	Регистрация пакетов включена	Включена регистрация пакетов на сервере регистрации ССПТ-2
3064	Регистрация пакетов отключена	Регистрация пакетов на сервере регистрации ССПТ-2 отключена
3065	Синхронизация правил отключена	Для подсистемы высокой готовности ССПТ-2 синхронизация текущего набора правил отключена
3066	Регистрация пакетов очищена	Из файлов регистрации удалены все записи о зарегистрированных пакетах
3067	Временное IP-правило удалено	Удалено временное IP-правило фильтрации из текущего набора правил. Выводится номер удаленного временного IP-правила
3068	NAT включен	Включен режим трансляции сетевых адресов пакетного фильтра в соответствии с имеющимися настройками текущей конфигурации ССПТ-2
3069	NAT отключен	Режим трансляции сетевых адресов пакетного фильтра отключен
306A	Диапазон портов NAT изменен. Необходимо перезапустить пакетный фильтр	Изменен диапазон прикладных портов, используемых для режима трансляции сетевых адресов пакетного фильтра. Для того, чтобы изменения вступили в силу необходимо перезапустить пакетный фильтр
306B	IP-адрес внешнего интерфейса NAT изменен	Изменен IP-адрес внешнего интерфейса режима трансляции сетевых адресов пакетного фильтра в текущей конфигурации ССПТ-2
306C	IP-адреса внешнего интерфейса NAT и шлюза удалены	Из текущей конфигурации ССПТ-2 удалены IP-адреса внешнего интерфейса и шлюза режима трансляции сетевых адресов пакетного фильтра
306D	Адрес шлюза внешнего интерфейса NAT изменен	Из текущей конфигурации ССПТ-2 удален IP-адрес шлюза внешнего интерфейса режима трансляции сетевых адресов пакетного фильтра

Код	Сообщение	Описание
306E	IP-адрес внутреннего интерфейса NAT изменен	Изменен IP-адрес внутреннего интерфейса режима трансляции сетевых адресов пакетного фильтра в текущей конфигурации ССПТ-2
306F	IP-адрес внутреннего интерфейса NAT удален	Из текущей конфигурации ССПТ-2 удален IP-адрес внутреннего интерфейса режима трансляции сетевых адресов пакетного фильтра
3070	Регистрация пакетов, удаленных NAT, включена	Начинается регистрация пакетов, отброшенных режимом трансляции сетевых адресов пакетного фильтра ССПТ-2
3071	Регистрация пакетов, удаленных NAT, отключена	Регистрация пакетов, отброшенных режимом трансляции сетевых адресов пакетного фильтра ССПТ-2 прекращается
3072	MAC-адрес внешнего интерфейса NAT изменен	Изменен MAC-адрес внешнего интерфейса режима трансляции сетевых адресов пакетного фильтра в текущей конфигурации ССПТ-2
3073	MAC-адрес внутреннего интерфейса NAT изменен	Изменен MAC-адрес внутреннего интерфейса режима трансляции сетевых адресов пакетного фильтра в текущей конфигурации ССПТ-2
3074	Новая запись добавлена в ARP таблицу	Добавлена новая запись в ARP таблицу режима трансляции сетевых адресов пакетного фильтра ССПТ-2
3075	Запись удалена из ARP таблицы	Удалена запись из ARP таблицы режима трансляции сетевых адресов пакетного фильтра ССПТ-2
3076	ARP таблица очищена	Из ARP таблицы режима трансляции сетевых адресов пакетного фильтра ССПТ-2 удалены все записи
3077	Новая запись добавлена в таблицу переадресации	Добавлена новая запись в таблицу переадресации режима трансляции сетевых адресов пакетного фильтра ССПТ-2
3078	Запись удалена из таблицы переадресации	Удалена запись из таблицы переадресации режима трансляции сетевых адресов пакетного фильтра ССПТ-2
3079	Таблица переадресации очищена	Из таблицы переадресации режима трансляции сетевых адресов пакетного фильтра ССПТ-2 удалены все записи
307A	Переадресация из DMZ включена	Включена переадресация запросов с интерфейсов DMZ в режиме трансляции сетевых адресов пакетного фильтра ССПТ-2
307B	Переадресация из DMZ отключена	Переадресация запросов с интерфейсов DMZ в режиме трансляции сетевых адресов пакетного фильтра ССПТ-2 отключена
307C	Переадресация с внешнего интерфейса включена	Включена переадресация запросов с внешнего интерфейса в режиме трансляции сетевых адресов пакетного фильтра ССПТ-2
307D	Переадресация с внешнего интерфейса отключена	Переадресация запросов с внешнего интерфейса в режиме трансляции сетевых адресов пакетного фильтра ССПТ-2 отключена
307E	Режим резервирования изменен	Установлен новый режим резервирования для подсистемы высокой готовности ССПТ-2
307F	Резервирование включено	Включена подсистема высокой готовности ССПТ-2
3080	Резервирование отключено	Подсистема высокой готовности ССПТ-2 отключена
3081	IP-адрес смежного устройство изменен	В текущей конфигурации изменен IP-адрес смежного ССПТ-2 для подсистемы высокой готовности
3082	Параметры резервирования установлены по умолчанию	Всем параметрам подсистемы высокой готовности в текущей конфигурации ССПТ-2 присвоены значения по умолчанию
3083	Синхронизация сессий включена	Для подсистемы высокой готовности ССПТ-2 включена синхронизация состояния таблицы сессий

Код	Сообщение	Описание
3084	Синхронизация сессий отключена	Для подсистемы высокой готовности ССПТ-2 синхронизация состояния таблицы сессий отключена
3086	Синхронизация правил инициирована	Выполняется немедленная синхронизация текущего набора правил для подсистемы высокой готовности ССПТ-2
3087	Режим просмотра изменен	Изменен режим просмотра данных в командном интерфейсе ССПТ-2
3088	Таймаут неактивности командного интерфейса изменен	Изменено максимально допустимое время неактивности пользователя в командном интерфейсе и в WEB-интерфейсе ССПТ-2
3089	Пользователь добавлен	Добавлен новый пользователь ССПТ-2
308A	Пользователь удален	Удален существующий пользователь ССПТ-2
308B	Пользователь отключен	Существующий пользователь ССПТ-2 заблокирован
308C	Пользователь включен	Существующий пользователь ССПТ-2 разблокирован
308D	Пароль пользователя изменен	Изменен пароль пользователя ССПТ-2
308E	Привилегии пользователя изменены	Изменен набор привилегий пользователя ССПТ-2
308F	MAC-правило скопировано	MAC-правило фильтрации скопировано в текущем наборе правил с другим номером
3090	MAC-правило перемещено	MAC-правило фильтрации перенесено в текущем наборе правил с другим номером
3091	ARP-правило скопировано	ARP-правило фильтрации скопировано в текущем наборе правил с другим номером
3092	ARP-правило перемещено	ARP-правило фильтрации перенесено в текущем наборе правил с другим номером
3093	IP-правило скопировано	IP-правило фильтрации скопировано в текущем наборе правил с другим номером
3094	IP-правило перемещено	IP-правило фильтрации перенесено в текущем наборе правил с другим номером
3095	IPX-правило скопировано	IPX-правило фильтрации скопировано в текущем наборе правил с другим номером
3096	IPX-правило перемещено	IPX-правило фильтрации перенесено в текущем наборе правил с другим номером
3097	Временное IP-правило скопировано	Временное IP-правило фильтрации скопировано в текущем наборе правил с другим номером
3098	Временное IP-правило перемещено	Временное IP-правило фильтрации перенесено в текущем наборе правил с другим номером
3099	Интервал времени скопирован	Интервал времени скопирован в текущем наборе правил с другим номером
309A	Интервал времени перемещен	Интервал времени перенесен в текущем наборе правил с другим номером
309B	AP-правило скопировано	AP-правило фильтрации скопировано в текущем наборе правил с другим номером
309C	AP-правило перемещено	AP-правило фильтрации перенесено в текущем наборе правил с другим номером
309D	VLAN-группа перемещена	VLAN-группа перенесена в текущем наборе правил с другим номером
309E	Пароль системного пользователя изменен	Изменен пароль системного пользователя `fnpsh`
309F	Действие отменено	Выполнение команды прервано пользователем
30A0	Установлены правила по умолчанию	Текущий набор правил приведен к начальному состоянию – только глобальные правила фильтрации, полностью запрещающие прохождение пакетов через ССПТ-2
30A1	Сигнализация обнаружения flood-атак включена	Начинается регистрация системных сообщений об обнаружении flood-атак пакетным фильтром ССПТ-2

Код	Сообщение	Описание
30A2	Сигнализация обнаружения flood-атак отключена	Регистрация системных сообщений об обнаружении flood-атак пакетным фильтром ССПТ-2 прекращается
30A3	Обнаружение flood-атак включено	Включен режим обнаружения flood-атак пакетного фильтра ССПТ-2
30A4	Обнаружение flood-атак отключено	Режим обнаружения flood-атак пакетного фильтра ССПТ-2 отключен
30A5	Пороговое значение изменено	Изменено пороговое значение интенсивности трафика для режима обнаружения flood-атак пакетного фильтра ССПТ-2
30A6	Регистрация во временных IP-правилах включена	По умолчанию во вновь создаваемых временных IP-правилах фильтрации текущего набора правил включается регистрация пакетов
30A7	Регистрация во временных IP-правилах отключена	По умолчанию во вновь создаваемых временных IP-правилах фильтрации текущего набора правил не включается регистрация пакетов
30A8	Комментарий временного IP-правила изменен	Изменен комментарий для временных IP-правил текущего набора правил
30A9	Время жизни временного IP-правила изменено	Изменено значение времени жизни по умолчанию для временного IP-правила
30AA	Регистрация сессий очищена	Из файлов регистрации удалены все записи о зарегистрированных сессиях
30AB	Статистика правил очищена	Обнулена статистика использования правил фильтрации текущего набора правил в пакетном фильтре
30AC	Скорость передачи для режима резервирования изменена	Изменена скорость передачи фильтрующих интерфейсов для подсистемы высокой готовности ССПТ-2
30AD	Режим передачи для режима резервирования изменен	Изменен режим передачи фильтрующих интерфейсов для подсистемы высокой готовности ССПТ-2
30AE	Проверка целостности выполнена	Выполнена проверка целостности компонентов операционной системы и программного обеспечения ССПТ-2. Нарушений не обнаружено
30AF	Выгрузка системных сообщений на SYSLOG сервер отключена	Режим выгрузки системных сообщений на удаленный SYSLOG сервер отключен
30B0	Выгрузка системных сообщений на SYSLOG сервер включена	Включен режим выгрузки системных сообщений на удаленный SYSLOG сервер
30B1	Адрес SYSLOG сервера изменен	В текущей конфигурации ССПТ-2 изменен IP-адрес удаленного SYSLOG сервера
30B2	Синхронизация конфигурации инициирована	Выполняется немедленная синхронизация текущей конфигурации для подсистемы высокой готовности ССПТ-2
30B3	Использование RADIUS включено	Включено использование удаленного RADIUS сервера для авторизации пользователей ССПТ-2
30B4	Использование RADIUS отключено	Использование удаленного RADIUS сервера для авторизации пользователей ССПТ-2 отключено
30B5	Конфигурация RADIUS сервера изменена	Изменены параметры удаленного RADIUS сервера, используемого для авторизации пользователей ССПТ-2
30B6	Таймаут ожидания ответа от RADIUS-сервера изменен	Изменено максимальное время ожидания ответа от удаленного RADIUS сервера
30B7	Количество обращений к RADIUS серверу изменено	Изменено максимальное количество попыток обращения к удаленному RADIUS серверу при авторизации пользователей ССПТ-2
30B8	WEB-интерфейс включен	Разрешено использование WEB-интерфейса ССПТ-2
30B9	WEB-интерфейс отключен	Использование WEB-интерфейса ССПТ-2 запрещено

Код	Сообщение	Описание
30BA	Аутентификация пользователей включена	Включен режим аутентификации сетевых пользователей. Активизация этого режима выполняется только при включении режима трансляции сетевых адресов (NAT)
30BB	Аутентификация пользователей отключена	Отключен режим аутентификации сетевых пользователей.
30BC	Пользователь удален	Удален существующий сетевой пользователь
30BD	Сетевой пользователь активирован	Существующий сетевой пользователь разблокирован
30BE	Сетевой пользователь отключен	Существующий сетевой пользователь заблокирован
30BF	Сетевой пользователь сброшен	Администратором ССПТ-2 завершен сеанс работы сетевого пользователя
30C0	Пароль сетевого пользователя изменен	Изменен пароль существующего сетевого пользователя
30C1	Нет активных пользователей	Нет ни одного зарегистрированного сеанса работы сетевых пользователей
30C2	Тайм-аут неактивности сетевых пользователей изменен	Изменено максимально допустимое время неактивности сеанса работы сетевого пользователя
30C3	Параметры сетевого пользователя изменены	Изменены параметры существующего сетевого пользователя – ограничения доступа и/или комментарий
30C4	Новая запись добавлена в файл ключей аутентификации	Добавлена новая пара ключей аутентификации сетевых пользователей
30C5	Запись удалена из файла ключей аутентификации	Удалена существующая пара ключей аутентификации сетевых пользователей
30C6	Запись изменена в файле ключей аутентификации	Сгенерированы новые значения для существующей пары ключей аутентификации сетевых пользователей
30C7	Пароль SNMP-пользователя изменен	Изменен пароль пользователя `fnpsnmp` для доступа к SNMP-агенту ССПТ-2
30C8	SNMP-интерфейс включен	Разрешено использование SNMP-интерфейса ССПТ-2
30C9	SNMP-интерфейс отключен	Использование SNMP-интерфейса ССПТ-2 запрещено
30CA	Глубокий контроль TCP включен	Включен режим глубокого контроля TCP-сессий
30CB	Глубокий контроль TCP отключен	Отключен режим глубокого контроля TCP-сессий

3.5.3. Предупреждения

Коды всех предупреждений, их текстовая интерпретация и описание представлены в таблице 3.17.

Таблица 3.17: Предупреждения командного интерфейса ССПТ-2

Код	Сообщение	Описание
2000	Вход пользователя с ограниченными привилегиями	Некоторые из привилегий, назначенных пользователю в соответствии с его учетной записью, уже заняты другими активными пользователями ССПТ-2
2001	Пользователь работает с ограниченными привилегиями	Для выполнения команды текущих привилегий пользователя недостаточно
2002	Команда не реализована	Введенная команда не поддерживается в текущей версии программного обеспечения ССПТ-2
2003	IP-адреса уже имеются в списке доступа	В списке доступа к управлению ССПТ-2 не может быть двух одинаковых записей
2004	Нет ранее сохраненных наборов правил	Невозможно вернуться к предыдущему состоянию текущего набора правил, поскольку резервные копии текущего набора правил отсутствуют

Код	Сообщение	Описание
2005	Пакетный фильтр не работает	Для выполнения команды требуется, чтобы пакетный фильтр ССПТ-2 был запущен
2006	Нет ответа от пакетного фильтра	Истекло время ожидания ответа от пакетного фильтра ССПТ-2. **Действия**: Проверить запущен ли пакетный фильтр
2007	Пакетный фильтр уже работает	Попытка повторного запуска пакетного фильтра ССПТ-2
2008	Пакетный фильтр не работает. Конфигурация сохраняется немедленно	Изменения в текущей конфигурации ССПТ-2 при остановленном пакетном фильтре записываются только в файл
2009	Конфигурация получена из файла	Текущая конфигурация ССПТ-2 прочитана из файла, а не получена от пакетного фильтра. Пакетный фильтр ССПТ-2 остановлен
200A	Сервер регистрации не работает	Не удалось отправить запрос серверу регистрации ССПТ-2. **Действия**: Перезагрузить ССПТ-2 для того, чтобы проверить корректность запуска сервера регистрации
200B	Нет ответа от сервера регистрации	Истекло время ожидания ответа от сервера регистрации ССПТ-2. **Действия**: Проверить запущен ли сервер регистрации
200C	Нет заданных регистрационных записей	По заданным критериям отбора не найдено ни одной регистрационной записи
200D	Нет заданных правил фильтрации	По заданным критериям отбора не найдено ни одного правила фильтрации, интервала времени или VLAN-группы
200E	IP-адреса шлюза и внешнего интерфейса должны быть различными	Для режима трансляции сетевых адресов IP-адреса внешнего интерфейса и шлюза не могут быть одинаковыми
200F	Режим управления сессиями должен быть включен	Перед выполнением команды необходимо включить управление сессиями
2010	Нет DMZ интерфейса в данной конфигурации	Для использования DMZ интерфейсов в режиме трансляции сетевых адресов необходим ССПТ-2, укомплектованный тремя и более фильтрующими интерфейсами
2011	Справка недоступна	Запрашиваемый раздел справки командного интерфейса ССПТ-2 отсутствует
2012	Режим резервирования уже включен	Попытка повторного включения подсистемы высокой готовностиССПТ-2
2013	Режим резервирования уже остановлен	Попытка повторного отключения подсистемы высокой готовностиССПТ-2
2014	Неподдерживаемый режим передачи	Попытка установить режим передачи, который не поддерживается данным сетевым Ethernet-интерфейсом
2015	Смежное устройство вне управляющей IP сети	IP-адреса управляющих Ethernet-интерфейсов смежных ССПТ-2 должны быть в одной и той же IP-подсети
2016	Пользователь не может быть удален	Попытка удаления пользователя ССПТ-2 с именем `admin`. Пользователь `admin` не может быть удален
2017	Пользователь не может быть добавлен	Попытка добавления нового пользователя ССПТ-2 с именем `admin`. Новый пользователь с именем `admin` не может быть добавлен
2018	Пользователь не может быть отключен	Попытка блокирования пользователя ССПТ-2 с именем `admin`. Пользователь `admin` не может быть заблокирован

Код	Сообщение	Описание
2019	Пользователь не может быть активирован	Попытка разблокирования пользователя ССПТ-2 с именем admin. Пользователь admin не может быть разблокирован
201A	Пароль пользователя не может быть изменен	Изменять пароль всем пользователям ССПТ-2 имеет право только пользователь admin. Любой другой пользователь может изменить пароль **только самому себе**.
201B	Привилегии пользователя не могут быть изменены	Попытка изменения набора привилегий пользователя ССПТ-2 с именем admin. Пользователю admin не может быть изменен набор привилегий
201C	Список доступа пустой	Список доступа к управлению ССПТ-2 не содержит ни одной записи
201D	Запись списка доступа пустая	Указан номер записи списка доступа к управлению ССПТ-2, которая не содержит данных
201E	Пустой набор	По заданным критериям отбора не найдено ни одной записи в ARP таблице режима трансляции сетевых адресов
201F	Резервирование включено. Сначала необходимо выключить	Перед выполнением команды необходимо выключить подсистему высокой готовности ССПТ-2
2020	Адрес смежного устройства должен отличаться от адреса управляющего интерфейса	IP-адреса управляющих Ethernet-интерфейсов смежных ССПТ-2 должны быть различными
2021	Должен быть настроен IP-адрес управляющего интерфейса	Перед выполнением команды необходимо назначить IP-адрес управляющему Ethernet-интерфейсу
2022	Адрес SYSLOG-сервера должен отличаться от адреса управляющего интерфейса	IP-адреса удаленного SYSLOG сервера и управляющего Ethernet-интерфейса ССПТ-2 должны быть различными
2023	IP-адреса SYSLOG сервера и управляющего интерфейса должны быть из одной подсети	IP-адреса удаленного SYSLOG сервера и управляющего Ethernet-интерфейса ССПТ-2 должны быть в одной и той же IP-подсети
2024	Должна быть отключена выгрузка на SYSLOG сервер	Перед выполнением команды необходимо выключить выгрузку системных сообщений на удаленный SYSLOG сервер
2025	Должно быть отключено использование RADIUS	Перед выполнением команды необходимо отключить использование удаленного RADIUS сервера для авторизации пользователей ССПТ-2
2026	Использование RADIUS уже включено	Попытка повторного включения использования удаленного RADIUS сервера для авторизации пользователей ССПТ-2
2027	Использование RADIUS уже отключено	Попытка повторного отключения использования удаленного RADIUS сервера для авторизации пользователей ССПТ-2
2028	MAC-адрес шлюза должен быть определен в ARP-таблице	Перед установкой IP-адреса шлюза внешнего интерфейса для режима трансляции сетевых адресов необходимо добавить запись в ARP таблицу, задающее соответствие MAC-адреса и IP-адреса шлюза
2029	Необходимо отключить NAT	Перед выполнением команды необходимо выключить режим трансляции сетевых адресов
202A	Нет дополнительных конфигураций	Для ССПТ-2 не сохранено ни одной дополнительной конфигурации
202B	Нет дополнительных наборов правил	Для ССПТ-2 не сохранено ни одного дополнительного набора правил
202C	WEB-интерфейс уже включен	Попытка повторного включения WEB-интерфейса ССПТ-2
202D	WEB-интерфейс уже отключен	Попытка повторного отключения WEB-интерфейса ССПТ-2
202E	Необходимо включить NAT	Перед выполнением команды необходимо включить режим трансляции сетевых адресов

Код	Сообщение	Описание
202F	Аутентификация пользователей уже включена	Попытка повторного включения режима аутентификации сетевых пользователей
2030	Аутентификация пользователей уже отключена	Попытка повторного отключения режима аутентификации сетевых пользователей
2031	Необходимо включить режим резервирования	Перед выполнением команды должна быть включена подсистема высокой готовности
2032	Ошибка выполнения запроса к серверу высокой готовности	Не удалось отправить запрос серверу высокой готовности ССПТ-2. **Действия**: Перезагрузить ССПТ-2 для того, чтобы проверить корректность запуска сервера высокой готовности
2033	Нет ответа от смежного устройства	Истекло время ожидания ответа от смежного устройства. **Действия**: проверить работоспособность смежного устройства (ССПТ-2) и наличие сетевого соединения между двумя устройствами
2034	Недопустимый режим резервирования для синхронизации	Запрашиваемый тип синхронизации не может быть выполнен при текущем режиме высокой готовности
2035	В ARP таблице MAC-адрес шлюза должен быть привязан к внешнему интерфейсу	При настройке режима трансляции сетевых адресов шлюз по умолчанию всегда должен находится в сегменте сети, подключенному к внешнему интерфейсу NAT ССПТ-2
2036	SNMP-интерфейс уже включен	Попытка повторного включения SNMP-интерфейса ССПТ-2
2037	SNMP-интерфейс уже отключен	Попытка повторного отключения SNMP-интерфейса ССПТ-2
2038	Синхронизация по NTP остается включенной	В конфигурации ССПТ-2 синхронизация системного времени по NTP остается включенной при выполнении одного из следующих действий: • удаление маршрута по умолчанию (команда `gateway delete` (п. 3.4.12, стр. 66)); • отключение маршрута по умолчанию (команда `gateway disable` (п. 3.4.13, стр. 66)); • назначение IP-адреса управляющему интерфейсу (команда `interface control address` (п. 3.4.22, стр. 70)); • удаление IP-адреса управляющего интерфейса (команда `interface control address delete` (п. 3.4.23, стр. 70)); • отключение управляющего интерфейса (команда `interface control disable` (п. 3.4.24, стр. 71))
2039	Выгрузка файлов регистрации по FTP остается включенной	В конфигурации ССПТ-2 выгрузка файлов регистрации на удаленный FTP-сервер остается включенной при выполнении одного из следующих действий: • удаление маршрута по умолчанию (команда `gateway delete` (п. 3.4.12, стр. 66)); • отключение маршрута по умолчанию (команда `gateway disable` (п. 3.4.13, стр. 66)); • назначение IP-адреса управляющему интерфейсу (команда `interface control address` (п. 3.4.22, стр. 70)); • удаление IP-адреса управляющего интерфейса (команда `interface control address delete` (п. 3.4.23, стр. 70)); • отключение управляющего интерфейса (команда `interface control disable` (п. 3.4.24, стр. 71))

Код	Сообщение	Описание
203A	Удаленная регистрация по SYSLOG остается включенной	В конфигурации ССПТ-2 регистрация событий на удаленном SYSLOG-сервере остается включенной при выполнении одного из следующих действий: • удаление маршрута по умолчанию (команда `gateway delete` (п. 3.4.12, стр. 66)); • отключение маршрута по умолчанию (команда `gateway disable` (п. 3.4.13, стр. 66)); • назначение IP-адреса управляющему интерфейсу (команда `interface control address` (п. 3.4.22, стр. 70)); • удаление IP-адреса управляющего интерфейса (команда `interface control address delete` (п. 3.4.23, стр. 70)); • отключение управляющего интерфейса (команда `interface control disable` (п. 3.4.24, стр. 71)); • установка IP-адреса SYSLOG-сервера (команда log export syslog server (п. 3.4.46, стр. 87))
203B	Маршрут по умолчанию остается отключенным	В конфигурации ССПТ-2 маршрут по умолчанию остается отключенным при выполнении одного из следующих действий: • включение выгрузки файлов регистрации по FTP (команда `log export ftp enable` (п. 3.4.42, стр. 85)); • установка параметров выгрузки файлов регистрации по FTP (команда `log export ftp set` (п. 3.4.43, стр. 85)); • включение выгрузки файлов регистрации по SYSLOG (команда `log export syslog enable` (п. 3.4.45, стр. 87)); • установка IP-адреса SYSLOG-сервера (команда `log export syslog server` (п. 3.4.46, стр. 87)); • включение синхронизации времени по NTP (команда `system time ntp enable` (п. 3.4.166, стр. 175)); • установка IP-адреса NTP-сервера (команда `system time ntp server` (п. 3.4.169, стр. 176)); • немедленная синхронизация времени по NTP (команда `system time ntp update` (п. 3.4.171, стр. 177)); • включение RADIUS-авторизации (команда `user radius enable` (п. 3.4.185, стр. 187)); • настройка параметров RADIUS-авторизации (команда `user radius server` (п. 3.4.187, стр. 188));

3.5.4. Сообщения об ошибках

Коды всех сообщений об ошибках, их текстовая интерпретация и описание представлены в таблице 3.18.

Таблица 3.18: Сообщения об ошибках командного интерфейса ССПТ-2

Код	Сообщение	Описание
1000	Ошибка распределения памяти	Системная ошибка, связанная с невозможностью динамически выделить запрошенный объем памяти. **Действия**: Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
1001	Ошибка инициализации настроек FNPSH	Ошибка инициализации структуры внутренних настроек командного интерфейса ССПТ-2 связанная с невозможностью динамически распределить память. **Действия**: Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1002	Язык не поддерживается программным обеспечением ССПТ	Попытка локализации сообщений командного интерфейса ССПТ-2 для неизвестного языка. Поддерживаемые языки – *английский*, *русский*. **Действия**: Работа командного интерфейса будет продолжена с выводом сообщений на английском языке
1003	Ошибка разбора аргументов командной строки	Ошибочные аргументы строки запуска командного интерфейса ССПТ-2. **Действия**: Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1004	Ошибка соединения с сервером регистрации	Недоступен сервер регистрации ССПТ-2 **Действия**: Проверить запущен ли сервер регистрации. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1005	Ошибка генерации ID сессии	Ошибка генерации уникального идентификатора сессии работы пользователя. **Действия**: Повторить авторизацию пользователя. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1006	Недопустимое системное имя пользователя	Системная авторизация с именем пользователя, отличным от `fnpsh`, не разрешается. **Действия**: Выполнить системную авторизацию для пользователя `fnpsh`
1007	Ошибка соединения с сервером авторизации	Недоступен сервер авторизации ССПТ-2 **Действия**: Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1008	Ошибка отправки запроса регистрации пользователя	Ошибка при отправке запроса регистрации пользователя серверу авторизации ССПТ-2. **Действия**: Повторно выполнить авторизацию пользователя. В случае повторения ошибки обратиться на предприятие-изготовитель
1009	Пользователь не зарегистрирован	Запрос на регистрацию пользователя отклонен. Неверные имя пользователя или пароль
100A	Нет ответа от сервера авторизации	Истекло время ожидания ответа от сервера авторизации ССПТ-2. **Действия**: Проверить запущен ли сервер авторизации. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
100B	ID сессии уже используется другим пользователем	Идентификатор сессии работы пользователя уже используется для другой сессии. **Действия**: Повторно выполнить авторизацию пользователя. В случае повторения ошибки обратиться на предприятие-изготовитель
100C	Слишком много активных пользователей	Достигнуто максимально допустимое количество активных сессий работы пользователя – **1024** сессии. **Действия**: Дождаться завершения хотя бы одной сессии работы пользователя и повторно выполнить авторизацию пользователя.

Код	Сообщение	Описание
100D	Сервер авторизации работает в однопользовательском режиме	Сервер авторизации ССПТ-2 перешел в однопользовательский режим работы по причине нарушения целостности компонентов операционной системы или программного обеспечения ССПТ-2. **Действия**: Выполнить авторизацию с *системной консоли* как пользователь `admin`. Проверить целостность программного обеспечения. В случае нарушения целостности **немедленно выключить** ССПТ-2 и обратиться на предприятие-изготовитель
100E	Системная ошибка на стороне сервера авторизации	Во время обработки запроса на стороне сервера авторизации ССПТ-2 произошла системная ошибка – ошибка операционной системы. **Действия**: Повторить запрос к серверу авторизации. В случае повторения ошибки обратиться на предприятие-изготовитель
100F	Ошибка отправки запроса выхода пользователя	Ошибка при отправке запроса на завершение сессии работы пользователя серверу авторизации ССПТ-2. **Действия**: Проверить запущен ли сервер авторизации. Повторно выполнить запрос. В случае повторения ошибки обратиться на предприятие-изготовитель
1010	Пользователь не найден	Пользователь с указанным именем не найден среди существующих пользователей ССПТ-2
1011	Ошибка получения IP-адреса клиента	Невозможно определить IP-адрес управляющего компьютера, с которого выполняется авторизация пользователя. **Действия**: Повторно выполнить авторизацию пользователя с *системной консоли*, а затем опять с управляющего компьютера. В случае повторения ошибки обратиться на предприятие-изготовитель
1012	Данная запись уже существует в файле ключей аутентификации	Пара ключей аутентификации сетевых пользователей для указанного IP-адреса уже существует
1013	Нарушена структура файла ключей аутентификации	Нарушена внутренняя структура файла ключей аутентификации сетевых пользователей. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2 и перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1014	Неверный тип интерфейса администратора	Ошибка определения или неизвестный тип интерфейса управления ССПТ-2. **Действия**: Использовать только средства управления, предоставляемые предприятием-изготовителем
1015	Ошибка получения имени пользователя	Ошибка получения имени пользователя для авторизации. **Действия**: Использовать только средства управления, предоставляемые предприятием-изготовителем. В случае повторения ошибки обратиться на предприятие-изготовитель
1016	Ошибка получения пароля пользователя	Ошибка получения пароля пользователя для авторизации. **Действия**: Использовать только средства управления, предоставляемые предприятием-изготовителем. В случае повторения ошибки обратиться на предприятие-изготовитель
1017	Ошибка компиляции регулярного выражения	Системная ошибка при компиляции регулярных выражений в командном интерфейсе ССПТ-2 **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1018	Неизвестная команда	Пользователь ввел команду, которая не распознается командным интерфейсом ССПТ-2 и не входит в состав командного языка.

Код	Сообщение	Описание
1019	Некорректный параметр в командной строке	В команде используется параметр, не предусмотренный синтаксисом. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
101A	Недостаточно привилегий для операции	Пользователь не обладает привилегией, требуемой для выполнения команды
101B	Неверный аргумент	Некоторые аргументы выполнения функций командного интерфейса имеют недопустимые значения **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
101C	Ошибка регистрации события	Ошибка при отправке запроса серверу регистрации ССПТ-2. **Действия**: Проверить запущен ли сервер регистрации. Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
101D	Ошибка останова устройства	Системная ошибка при выполнении останова операционной системы и отключения ССПТ-2. **Действия**: Проверить целостность компонентов операционной системы ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
101E	Ожидается параметр	Отсутствуют необходимые параметры команды. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
101F	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
1020	Ошибка перезагрузки устройства	Системная ошибка при выполнении перезагрузки операционной системы ССПТ-2. **Действия**: Проверить целостность компонентов операционной системы ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1021	Пропущен IP-адрес	В соответствии с синтаксисом команды необходимо указание IP-адреса. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1022	Пропущено имя фильтрующего интерфейса	В соответствии с синтаксисом команды необходимо указание символического имени фильтрующего интерфейса. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1023	Ошибка чтения файла конфигурации ССПТ	Системная ошибка чтения файла текущей конфигурации ССПТ-2. **Действия**: Проверить целостность компонентов операционной системы ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1024	Фильтрующий интерфейс с заданным именем не найден	Указанное в команде символическое имя не присвоено ни одному из фильтрующих интерфейсов ССПТ-2
1025	Неверный номер фильтрующего интерфейса	Недопустимый номер фильтрующего интерфейса ССПТ-2.

Код	Сообщение	Описание
1026	Неверный формат номера или имени фильтрующего интерфейса	Номер или символическое имя фильтрующего интерфейса ССПТ-2 не соответствует принятому формату
1027	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
1028	Неверный формат имени дополнительной конфигурации	Имя дополнительной конфигурации не соответствует принятому формату
1029	Пропущено имя пользователя	В соответствии с синтаксисом команды необходимо указание имени пользователя ССПТ-2. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
102A	Неверный формат имени пользователя	Имя пользователя ССПТ-2 не соответствует принятому формату
102B	Пропущен старый пароль	В соответствии с синтаксисом команды необходимо указание старого пароля пользователя ССПТ-2. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
102C	Пропущен пароль	В соответствии с синтаксисом команды необходимо указание пароля пользователя ССПТ-2. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
102D	Неверный формат пароля	Пароль пользователя ССПТ-2 не соответствует принятому формату
102E	Пароли не совпадают	Повторный ввод пароля пользователя отличается от первоначального
102F	Пропущен список привилегий пользователя	В соответствии с синтаксисом команды необходимо указание списка привилегий пользователя ССПТ-2. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1030	Неподдерживаемый параметр	Пользователь в командной строке ввел параметр, который не распознается командным интерфейсом ССПТ-2 и не входит в состав командного языка.
1031	Неверный формат критерия отбора	Критерий отбора не соответствует принятому формату
1032	Неверно дата/время	Указано недопустимое значение даты/времени. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1033	Неверный формат даты/времени	Дата/время не соответствуют принятому формату
1034	Недопустимый интервал даты/времени	Указано недопустимое значение интервала даты/времени. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1035	Неверный формат IP-адреса	IP-адрес не соответствует принятому формату
1036	Недопустимый IP-адрес	Указано недопустимое значение IP-адреса **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1037	Пропущен путь на FTP-сервере	В соответствии с синтаксисом команды необходимо указание пути на FTP сервере. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса

Код	Сообщение	Описание
1038	Неверный формат пути на FTP-сервере	Путь на FTP сервере не соответствует принятому формату
1039	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
103A	Неверный формат имени пользователя FTP-сервера	Имя пользователя FTP сервера не соответствует принятому формату
103B	Пропущен пароль пользователя FTP-сервера	В соответствии с синтаксисом команды необходимо указание пароля пользователя FTP сервера. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
103C	Недопустимый тип правила фильтрации	Указан недопустимый тип правила фильтрации в критерии отбора. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
103D	Недопустимый номер правила фильтрации	Указано недопустимое значение номера правила фильтрации, интервала времени или VLAN-группы. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
103E	Неверный формат номера правила фильтрации	Номер правила фильтрации, интервала времени или VLAN-группы не соответствует принятому формату
103F	Пропущено определение правила фильтрации	В соответствии с синтаксисом команды необходимо указание определения правила фильтрации, интервала времени или VLAN-группы **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1040	Недопустимый тип правила фильтрации	Указано правило фильтрации недопустимого типа. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1041	Ошибка чтения файла VLAN-групп	Системная ошибка чтения файла VLAN-групп текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1042	Идентификатор VLAN уже используется в другой VLAN-группе	Идентификатор VLAN не может входить в две и более VLAN-группы
1043	Таблица VLAN-групп переполнена	Достигнуто максимально допустимое количество VLAN-групп в текущем наборе правил
1044	VLAN-группа уже существует	VLAN-группа с указанным номером уже существует в текущем наборе правил
1045	VLAN-группа не найдена	В текущем наборе правил не существует VLAN-группы с указанным номером
1046	Ошибка записи файла VLAN-групп	Системная ошибка записи файла VLAN-групп текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1047	Внутренняя ошибка библиотеки ССПТ	Системная ошибка при выполнении функции библиотеки ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
1048	Синтаксическая ошибка в определении правила	Определение правила фильтрации, интервала времени или VLAN-группы не соответствует синтаксису
1049	Ошибка чтения файла MAC-правил	Системная ошибка чтения файла MAC-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
104A	Таблица MAC-правил переполнена	Достигнуто максимально допустимое количество MAC-правил фильтрации в текущем наборе правил
104B	MAC-правило уже существует	MAC-правило фильтрации с указанным номером уже существует в текущем наборе правил
104C	MAC-правило не найдено	В текущем наборе правил не существует MAC-правила фильтрации с указанным номером
104D	Ошибка записи файла MAC-правил	Системная ошибка записи файла MAC-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
104E	Ошибка чтения файла ARP-правил	Системная ошибка чтения файла ARP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
104F	Таблица ARP-правил переполнена	Достигнуто максимально допустимое количество ARP-правил фильтрации в текущем наборе правил
1050	ARP-правило уже существует	ARP-правило фильтрации с указанным номером уже существует в текущем наборе правил
1051	ARP-правило не найдено	В текущем наборе правил не существует ARP-правила фильтрации с указанным номером
1052	Ошибка записи файла ARP-правил	Системная ошибка записи файла ARP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1053	Ошибка чтения файла IP-правил	Системная ошибка чтения файла IP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1054	Таблица IP-правил переполнена	Достигнуто максимально допустимое количество IP-правил фильтрации в текущем наборе правил
1055	IP-правило уже существует	IP-правило фильтрации с указанным номером уже существует в текущем наборе правил
1056	IP-правило не найдено	В текущем наборе правил не существует IP-правила фильтрации с указанным номером
1057	Ошибка записи файла IP-правил	Системная ошибка записи файла IP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
1058	Ошибка чтения файла IPX-правил	Системная ошибка чтения файла IPX-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1059	Таблица IPX-правил переполнена	Достигнуто максимально допустимое количество IPX-правил фильтрации в текущем наборе правил
105A	IPX-правило уже существует	IPX-правило фильтрации с указанным номером уже существует в текущем наборе правил
105B	IPX-правило не найдено	В текущем наборе правил не существует IPX-правила фильтрации с указанным номером
105C	Ошибка записи файла IPX-правил	Системная ошибка записи файла IPX-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
105D	Ошибка чтения файла интервалов времени	Системная ошибка чтения файла интервалов времени текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
105E	Таблица интервалов времени переполнена	Достигнуто максимально допустимое количество интервалов времени в текущем наборе правил
105F	Интервал времени уже существует	Интервал времени с указанным номером уже существует в текущем наборе правил
1060	Интервал времени не найден	В текущем наборе правил не существует интервала времени с указанным номером
1061	Ошибка записи файла интервалов времени	Системная ошибка записи файла интервалов времени текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1062	Ошибка чтения файла AP-правил	Системная ошибка чтения файла AP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1063	Таблица AP-правил переполнена	Достигнуто максимально допустимое количество AP-правил фильтрации в текущем наборе правил
1064	AP-правило уже существует	AP-правило фильтрации с указанным номером уже существует в текущем наборе правил
1065	AP-правило не найдено	В текущем наборе правил не существует AP-правила фильтрации с указанным номером
1066	Ошибка записи файла AP-правил	Системная ошибка записи файла AP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1067	VLAN-группа используется в правилах фильтрации	Не допускается удаление из текущего набора правил VLAN-группы, на которую имеется ссылка из MAC, ARP, IP или IPX-правил фильтрации
1068	Интервал времени используется в правилах фильтрации	Не допускается удаление из текущего набора правил интервала времени, на который имеется ссылка из MAC, ARP, IP или IPX-правил фильтрации

Код	Сообщение	Описание
1069	AP-правило используется в IP-правилах фильтрации	Не допускается удаление из текущего набора правил AP-правила фильтрации, на которую имеется ссылка из IP-правил фильтрации
106A	Глобальное правило не может быть удалено	Удаление глобальных правил фильтрации запрещено
106B	Пропущено имя дополнительного набора правил	В соответствии с синтаксисом команды необходимо указание имени дополнительного набора правил. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
106C	Неверный формат имени дополнительного набора правил	Имя дополнительного набора правил не соответствует принятому формату
106D	Ошибка чтения списка дополнительных наборов правил	Системная ошибка при получении списка имен файлов дополнительных наборов правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
106E	Ошибка открытия дополнительного набора правил	Системная ошибка открытия файла дополнительного набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
106F	Глобальное MAC-правило отсутствует в наборе правил	Загружаемый набор правил обязательно должен содержать глобальное MAC-правило фильтрации. **Действия**: Откорректировать набор правил так, чтобы он содержал глобальное MAC-правило фильтрации
1070	Глобальное ARP-правило отсутствует в наборе правил	Загружаемый набор правил обязательно должен содержать глобальное ARP-правило фильтрации. **Действия**: Откорректировать набор правил так, чтобы он содержал глобальное ARP-правило фильтрации
1071	Глобальное IP-правило отсутствует в наборе правил	Загружаемый набор правил обязательно должен содержать глобальное IP-правило фильтрации. **Действия**: Откорректировать набор правил так, чтобы он содержал глобальное IP-правило фильтрации
1072	Глобальное IPX-правило отсутствует в наборе правил	Загружаемый набор правил обязательно должен содержать глобальное IPX-правило фильтрации. **Действия**: Откорректировать набор правил так, чтобы он содержал глобальное IPX-правило фильтрации
1073	MAC-правило ссылается на несуществующий интервал времени	MAC-правило фильтрации из загружаемого набора правил ссылается на интервал времени, отсутствующий в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив интервал времени или исправив MAC-правило
1074	ARP-правило ссылается на несуществующий интервал времени	ARP-правило фильтрации из загружаемого набора правил ссылается на интервал времени, отсутствующий в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив интервал времени или исправив ARP-правило
1075	IP-правило ссылается на несуществующий интервал времени	IP-правило фильтрации из загружаемого набора правил ссылается на интервал времени, отсутствующий в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив интервал времени или исправив IP-правило
1076	IPX-правило ссылается на несуществующий интервал времени	IPX-правило фильтрации из загружаемого набора правил ссылается на интервал времени, отсутствующий в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив интервал времени или исправив IPX-правило

Код	Сообщение	Описание
1077	MAC-правило ссылается на несуществующую VLAN-группу	MAC-правило фильтрации из загружаемого набора правил ссылается на VLAN-группу, отсутствующую в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив VLAN-группу или исправив MAC-правило
1078	ARP-правило ссылается на несуществующую VLAN-группу	ARP-правило фильтрации из загружаемого набора правил ссылается на VLAN-группу, отсутствующую в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив VLAN-группу или исправив ARP-правило
1079	IP-правило ссылается на несуществующую VLAN-группу	IP-правило фильтрации из загружаемого набора правил ссылается на VLAN-группу, отсутствующую в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив VLAN-группу или исправив IP-правило
107A	IPX-правило ссылается на несуществующую VLAN-группу	IPX-правило фильтрации из загружаемого набора правил ссылается на VLAN-группу, отсутствующую в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив VLAN-группу или исправив IPX-правило
107B	IP-правило ссылается на несуществующее AP-правило	IP-правило фильтрации из загружаемого набора правил ссылается на AP-правило фильтрации, отсутствующее в этом же наборе правил. **Действия**: Откорректировать набор правил, добавив AP-правило фильтрации или исправив IP-правило
107C	Ошибка чтения файла ключей аутентификации	Системная ошибка чтения файла ключей аутентификации сетевых пользователей. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
107D	Дополнительный набор правил уже существует	Дополнительный набор правил с указанным именем уже существует и не может быть перезаписан. **Действия**: Для того чтобы повторно сохранить дополнительный набор правил, его необходимо сначала удалить
107E	Нет свободной позиции для дополнительного набора правил	Достигнуто максимально допустимое количество сохраненных дополнительных наборов правил
107F	Ошибка сохранения дополнительного набора правил	Системная ошибка сохранения файла дополнительного набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1080	Недостаточно прав доступа к дополнительному набору правил	Пользователь не имеет прав записи в файл дополнительного набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1081	Дополнительный набор правил не найден	Не существует дополнительного набора правил с указанным именем
1082	Ошибка удаления дополнительного набора правил	Пользователь не имеет прав доступа для удаления файла дополнительного набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
1083	Ошибка восстановления VLAN-групп	Системная ошибка восстановления предыдущего состояния файла VLAN-групп текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1084	Ошибка восстановления MAC-правил	Системная ошибка восстановления предыдущего состояния файла MAC-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1085	Ошибка восстановления ARP-правил	Системная ошибка восстановления предыдущего состояния файла ARP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1086	Ошибка восстановления IP-правил	Системная ошибка восстановления предыдущего состояния файла IP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1087	Ошибка восстановления IPX-правил	Системная ошибка восстановления предыдущего состояния файла IPX-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1088	Ошибка восстановления интервалов времени	Системная ошибка восстановления предыдущего состояния файла интервалов времени текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1089	Ошибка восстановления AP-правил	Системная ошибка восстановления предыдущего состояния файла AP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
108A	Ошибка просмотра дополнительного набора правил	Системная ошибка при обращении к файлу для просмотра дополнительного набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
108B	Ошибка открытия временного файла	Системная ошибка открытия файла для хранения временных данных. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
108C	Ошибка при использовании библиотеки ncurses	Ошибка при выполнении функции библиотеки управления терминалом в полноэкранном режиме просмотра данных командного интерфейса ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
108D	Имя фильтрующего интерфейса уже используется	Указанное символическое имя уже присвоено другому фильтрующему интерфейсу ССПТ-2
108E	Ошибка записи файла конфигурации ССПТ	Системная ошибка записи файла текущей конфигурации ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
108F	Не поддерживается в этой редакции программного обеспечения	Команда не поддерживается в используемой версии программного обеспечения ССПТ-2
1090	Неверный формат IP-адреса/маски	IP-адрес или IP маска не соответствуют принятому формату
1091	Недопустимая IP маска	Некорректное значение маски IP-подсети
1092	Список доступа заполнен	Список доступа к управлению ССПТ-2 содержит максимально допустимое количество записей
1093	Пропущена запись списка доступа	В соответствии с синтаксисом команды необходимо указание записи списка доступа к управлению ССПТ-2. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1094	Доступ запрещен в соответствии со списком доступа	Авторизация пользователя осуществляется с управляющего компьютера, IP-адрес которого не удовлетворяет ни одной из записей списка доступа к управлению ССПТ-2
1095	Шлюз и IP-адрес из разных сетей	IP-адрес шлюза по умолчанию должен принадлежать той же самой IP-подсети, что и IP-адрес управляющего Ethernet-интерфейса ССПТ-2
1096	Маршрут по умолчанию уже существует	Попытка повторной настройки маршрута по умолчанию
1097	Маршрут по умолчанию уже был удален	Маршрут по умолчанию уже был удален из маршрутной таблицы ССПТ-2
1098	Невозможно использовать ключевое слово	Не допускается использование ключевого слова в контексте команды
1099	Слишком мало фильтрующих интерфейсов для зеркалирования	Для использования режима зеркалирования трафика ССПТ-2 должен быть укомплектован тремя и более фильтрующими интерфейсами
109A	Зеркалируемый и слушающий интерфейсы должны быть различными	В режиме зеркалирования трафика зеркалируемый и слушающий интерфейсы должны быть назначены на различные фильтрующие интерфейсы ССПТ-2
109B	Недопустимый зеркалируемый интерфейс	Номер указанного фильтрующего интерфейса ССПТ-2 не соответствует настройкам режима зеркалирования трафика
109C	Недопустимый интервал IP-адресов	Некорректное значение диапазона IP-адресов
109D	Ошибка отправки запроса пакетному фильтру	Ошибка при отправке запроса пакетному фильтру ССПТ-2. **Действия**: Проверить запущен ли пакетный фильтр. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
109E	Получен ошибочный ответ от пакетного фильтра	Нарушена структура ответа, полученного от пакетного фильтра ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
109F	Ошибка получения системной информации	Ошибка при получении информации о состоянии программного обеспечения и операционной системы ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10A0	Недопустимое значение тайм-аута	Некорректное значение тайм-аута
10A1	Ошибка запуска пакетного фильтра	Ошибка при запуске пакетного фильтра ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10A2	Недопустимый размер таблицы сессий	Некорректное значение размера таблицы сессий
10A3	Ошибка открытия дополнительной конфигурации	Системная ошибка открытия файла дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10A4	Ошибка сохранения дополнительной конфигурации	Системная ошибка записи файла дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10A5	Дополнительная конфигурация уже существует	Файл дополнительной конфигурации с указанным именем уже существует
10A6	Ошибка чтения списка дополнительных конфигураций	Системная ошибка при получении списка имен файлов дополнительных конфигураций. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10A7	Нет свободной позиции для дополнительной конфигурации	Достигнуто максимально допустимое количество сохраненных дополнительных конфигураций
10A8	Недостаточно прав доступа к дополнительной конфигурации	Пользователь не имеет прав записи в файл дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10A9	Дополнительная конфигурация не найдена	Не существует дополнительной конфигурации с указанным именем
10AA	Ошибка удаления дополнительной конфигурации	Пользователь не имеет прав доступа для удаления файла дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10AB	Неверный размер файла дополнительной конфигурации	Файл дополнительной конфигурации, загружаемый с управляющего компьютера на ССПТ-2, имеет неправильный размер

Код	Сообщение	Описание
10AC	Ошибка чтения дополнительной конфигурации	Системная ошибка чтения файла дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10AD	Ошибка просмотра дополнительной конфигурации	Системная ошибка при обращении к файлу для просмотра дополнительной конфигурации. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10AE	Ошибка генерации ключей	Внутренняя ошибка библиотеки криптографических функций FNPCrypt при генерации пары ключей аутентификации сетевых пользователей. Код ошибки библиотеки и строка описания ошибки выводится в диагностическом сообщении командного интерфейса ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Повторить выполнение команды. В случае повторения ошибки обратиться на предприятие-изготовитель
10AF	Ошибка инициализации генератора псевдослучайных чисел	Внутренняя ошибка библиотеки криптографических функций FNPCrypt при инициализации генератора псевдослучайных чисел. Код ошибки библиотеки и строка описания ошибки выводится в диагностическом сообщении командного интерфейса ССПТ-2. Действия: Проверить целостность компонентов программного обеспечения ССПТ-2. Повторить выполнение команды. В случае повторения ошибки обратиться на предприятие-изготовитель
10B0	Пакетному фильтру отправлена неизвестная команда	Неизвестный код команды в структуре запроса, отправленном пакетному фильтру ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10B2	Для установки режима передачи скорость передачи должна отличаться от "autoselect"	Режим передачи Ethernet-интерфейсов ССПТ-2 (управляющего или фильтрующих) может быть установлен только в том случае, если скорость передачи установлена в значение отличное от “`autoselect`”.
10B3	Пропущен MAC-адрес	В соответствии с синтаксисом команды необходимо указание MAC-адреса. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
10B4	Не указаны дата или время	В соответствии с синтаксисом команды необходимо указание даты или времени. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
10B5	Неверный формат времени	Время не соответствует принятому формату
10B6	Неверный формат даты	Дата не соответствует принятому формату
10B7	Ошибка установки системного времени	Ошибка изменения системного времени. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10B8	Недопустимая дата/время	Некорректное значение даты или времени
10B9	Управляющий интерфейс отключен	Команда не может быть выполнена при отключенном управляющем Ethernet-интерфейсе ССПТ-2

Код	Сообщение	Описание
10BA	IP-адреса NTP-сервера и управляющего интерфейса из разных сетей	При отключенном маршруте по умолчанию IP-адреса NTP-сервера и управляющего Ethernet-интерфейса ССПТ-2 должны принадлежать одной и той же IP-подсети
10BB	NTP-сервер не определен	Перед выполнением команды необходимо установить IP-адрес NTP-сервера
10BC	Ошибка получения системного времени	Ошибка получения системного времени от операционной системы ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10BD	Ошибка порождения процесса	Системная ошибка создания процесса. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10BE	Недопустимое значение тайм-аута	Некорректное значение тайм-аута синхронизации системного времени по протоколу NTP
10BF	Ошибка доступа к файлу часового пояса	Системная ошибка открытия или недостаточно прав доступа к файлу часового пояса. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10C0	Ошибка создания локального файла часового пояса	Системная ошибка создания файла текущего часового пояса. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10C1	Ошибка копирования файла часового пояса	Системная ошибка копирования данных в файл текущего часового пояса. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10C2	Ошибка создания символической ссылки на файл часового пояса	Системная ошибка создания символической ссылки на файл текущего часового пояса. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10C3	Ошибка изменения часового пояса	Ошибка обращения или нарушена структура файла списка буквенных кодов ISO3166 для стран мира. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10C4	Неверный формат номера	Некорректный ввод пользователя при выборе нового часового пояса
10C5	Не найдено стран для континента/региона	В файлах описания часовых поясов обнаружен континент/регион, не содержащий стран. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10C6	Некорректные параметры выгрузки на FTP-сервер	Перед выполнением команды необходимо настроить параметры выгрузки файлов регистрации на удаленный FTP сервер

Код	Сообщение	Описание
10C7	Ошибка отправки запроса серверу регистрации	Ошибка при отправке запроса серверу регистрации ССПТ-2. **Действия**: Проверить запущен ли сервер регистрации. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10C8	Недостаточно привилегий для запроса регистрации	У пользователя недостаточно привилегий для выполнения запроса к серверу регистрации
10C9	Системная ошибка на стороне сервера регистрации	Во время обработки запроса на стороне сервера регистрации ССПТ-2 произошла системная ошибка – ошибка операционной системы. **Действия**: Повторить запрос к серверу авторизации. В случае повторения ошибки обратиться на предприятие-изготовитель
10CA	Серверу регистрации отправлена неизвестная команда	Неизвестный код команды в структуре запроса, отправленном серверу регистрации ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10CB	Ошибка просмотра регистрационных записей	Системная ошибка во время обработки полученных регистрационных записей для просмотра. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10CC	Параметр уже существует	В списке критериев отбора указанный параметр встречается более одного раза
10CD	Не найдено подходящей сессии	В таблице сессий не найдено сессии с указанным номером
10CE	Ошибка чтения файла системных сообщений	Системная ошибка чтения файла системных сообщений. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10CF	Недопустимое имя фильтрующего интерфейса	Указанное символическое имя не присвоено ни одному из фильтрующих интерфейсов ССПТ-2
10D0	Системная ошибка на стороне пакетного фильтра	Во время обработки запроса на стороне пакетного фильтра ССПТ-2 произошла системная ошибка – ошибка операционной системы. **Действия**: Повторить запрос к серверу авторизации. В случае повторения ошибки обратиться на предприятие-изготовитель
10D1	Временное IP-правило не найдено	В текущем наборе правил не существует временного IP-правила фильтрации с указанным номером
10D2	Ошибка чтения временных IP-правил	Системная ошибка чтения файла временных IP-правил фильтрации текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10D3	Временное IP-правило уже существует	Временное IP-правило фильтрации с указанным номером уже существует в текущем наборе правил
10D4	Неверный идентификатор VLAN	Значение идентификатора VLAN не соответствует принятому формату
10D5	Недопустимые параметры NAT	Перед выполнением команды необходимо настроить параметры режима трансляции сетевых адресов

Код	Сообщение	Описание
10D6	Ошибка чтения файла сертификата УЦ (ГОСТ)	Системная ошибка чтения файла сертификата Удостоверяющего Центра. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10D7	Недопустимое значение порта	Некорректное значение номера прикладного порта
10D8	Недопустимый диапазон портов	Некорректное значение диапазона номеров прикладных портов
10D9	Неверный формат MAC-адреса	Значение MAC-адреса не соответствует принятому формату
10DA	Недопустимый MAC-адрес	Некорректное значение MAC-адреса
10DB	IP-адрес уже существует в ARP таблице	В ARP таблице режима трансляции сетевых адресов уже имеется запись с указанным IP-адресом
10DC	ARP таблица заполнена	Достигнуто максимально допустимое количество записей в ARP таблице режима трансляции сетевых адресов
10DD	Не найдено подходящей записи в ARP таблице	В ARP таблице режима трансляции сетевых адресов не найдено записи с указанным MAC или IP-адресом
10DE	Порт уже существует в таблице переадресации	В таблице переадресации режима трансляции сетевых адресов уже имеется запись с указанным номером прикладного порта
10DF	Таблица переадресации заполнена	Достигнуто максимально допустимое количество записей в таблице переадресации режима трансляции сетевых адресов
10E0	Не найдено подходящей записи в таблице переадресации	В таблице переадресации режима трансляции сетевых адресов не найдено записи с указанным номером прикладного порта
10E1	Системная ошибка	Произошла ошибка операционной системы ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10E2	Ошибка чтения файла справки ССПТ	Системная ошибка чтения файла контекстной справки командного интерфейса ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10E3	Нет контекстной справки для команды	Для команды не существует соответствующего раздела в файле контекстной справки командного интерфейса ССПТ-2
10E4	Нарушена структура файла справки ССПТ	Нарушена внутренняя структура файла контекстной справки командного интерфейса ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10E5	Недопустимый запрос к серверу высокой готовности	Неизвестный код команды в структуре запроса, отправленном серверу высокой готовности ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10E6	Недопустимые настройки режима резервирования	Некорректные значения параметров настройки режима высокой готовности ССПТ-2

Код	Сообщение	Описание
10E7	Некорректный ответ от сервера высокой готовности	Нарушена структура ответа, полученного от сервера высокой готовности ССПТ-2, или неизвестный код ответа. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10E8	Ошибка отправки запроса серверу высокой готовности	Ошибка при отправке запроса серверу высокой готовности ССПТ-2. **Действия**: Проверить запущен ли сервер высокой готовности. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10E9	Ошибка получения ответа от сервера высокой готовности	Истекло время ожидания ответа от сервера высокой готовности ССПТ-2. **Действия**: Проверить запущен ли сервер высокой готовности. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10EA	Ошибка соединения с сервером высокой готовности	Недоступен сервер высокой готовности ССПТ-2 **Действия**: Проверить запущен ли сервер высокой готовности. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10EB	Некорректный размер дополнительной конфигурации	Файл дополнительной конфигурации, загружаемой в текущую конфигурацию, имеет неправильный размер. **Действия**: Удалить дополнительную конфигурацию. Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10EC	Ошибка чтения временного файла	Системная ошибка файла, содержащего временные данные. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10ED	NTP сервер не найден	Недоступен NTP сервер для синхронизации системного времени
10EE	Таймаут опроса NTP сервера	Истекло время ожидания ответа от NTP сервера на запрос синхронизации системного времени
10EF	Ошибка отправки запроса серверу авторизации	Ошибка при отправке запроса серверу авторизации ССПТ-2. **Действия**: Проверить запущен ли сервер авторизации. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10F0	Ошибка чтения файла паролей	Системная ошибка чтения файла паролей пользователей ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10F1	Ошибка записи файла паролей	Системная ошибка записи файла паролей пользователей ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
10F2	Не найдено записей в файле паролей	Файл паролей не содержит учетных записей пользователей ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10F3	Неверный формат файла паролей	Нарушена внутренняя структура файла паролей пользователей ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10F4	Пользователь уже существует	Учетная запись указанного пользователя ССПТ-2 уже существует в файле паролей
10F5	Неверный формат списка привилегий	Список привилегий пользователя ССПТ-2 не соответствует принятому формату
10F6	Недопустимый пароль пользователя	Введен неверный пароль пользователя ССПТ-2
10F7	Недопустимый номер правила	Недопустимый номер правила фильтрации в операциях копирования или переноса правил. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
10F8	Невозможно копировать (переносить) глобальное правило	Копирование или перенос глобальных правил фильтрации не допускается
10F9	Невозможно копировать VLAN-группу	Копирование VLAN-групп не допускается
10FA	Ошибка чтения системного файла паролей	Системная ошибка чтения системного файла паролей. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10FB	Ошибка записи системного файла паролей	Системная ошибка записи системного файла паролей. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10FC	Ошибка блокировки системного файла паролей	Системная ошибка при операции блокировки системного файла паролей. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10FD	Ошибка создания системной базы данных паролей	Системная ошибка обновления файлов учетных записей системных пользователей. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10FE	Ошибка записи временного файла	Системная ошибка записи файла с временными данными. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
10FF	Ошибка чтения атрибутов удаленного пользователя	Ошибка получения атрибутов пользователя ССПТ-2 от терминального сервера при удаленном управлении. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
1100	Недопустимый номер записи списка доступа	Номер элемента списка доступа к управлению ССПТ-2 не соответствует принятому формату
1101	Слишком длинное правило	Строка определения правила фильтрации, VLAN-группы или интервала времени превышает максимально допустимую длину
1102	Недопустимое значение параметра	Некорректное или недопустимое значение параметра команды. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1103	Ошибка чтения файла контрольных сумм	Системная ошибка чтения файла контрольных сумм файлов операционной системы и программного обеспечения ССПТ-2. **Действия**: **Немедленно выключить** ССПТ-2 и обратиться на предприятие-изготовитель
1104	Нарушен размер файла контрольных сумм	Файл контрольных сумм имеет неправильный размер. **Действия**: **Немедленно выключить** ССПТ-2 и обратиться на предприятие-изготовитель
1105	Ошибка вычисления контрольной суммы	Ошибка вычисления контрольной суммы файла операционной системы или программного обеспечения ССПТ-2. **Действия**: Повторить выполнение команды. В случае повторения ошибки **немедленно выключить** ССПТ-2 и обратиться на предприятие-изготовитель
1106	Нарушена контрольная сумма файла. Пакетный фильтр остановлен	Контрольная сумма файла операционной системы или программного обеспечения ССПТ-2 не совпадает с данными файла контрольных сумм. Пакетный фильтр отключен, а сервер авторизации переведен в однопользовательский режим работы. **Действия**: Получить доступ к управлению ССПТ-2 с системной консоли как пользователь `admin`, **немедленно выключить** ССПТ-2 и обратиться на предприятие-изготовитель
1107	Файл пуст	Файл системных сообщений не содержит записей. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1108	Выгрузка по SYSLOG уже включена	Повторное включение выгрузки системных сообщений на удаленный SYSLOG сервер
1109	Выгрузка по SYSLOG уже отключена	Повторное отключение выгрузки системных сообщений на удаленный SYSLOG сервер
110A	Ошибка записи в файл ключей аутентификации	Системная ошибка записи файла ключей аутентификации сетевых пользователей. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
110B	Ошибка получения ответа от сервера регистрации	Истекло время ожидания ответа от сервера регистрации ССПТ-2. **Действия**: Проверить запущен ли сервер регистрации. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
110C	Сообщение слишком большое для вывода в данное окно	Размер данных для вывода превышает размеры окна. **Действия**: В случае повторения ошибки обратиться на предприятие-изготовитель
110D	Запись в файле ключей аутентификации не найдена	Пара ключей аутентификации, соответствующая указанному IP-адресу, отсутствует

Код	Сообщение	Описание
110E	Некорректные параметры RADIUS сервера	Некорректные значения параметров RADIUS авторизации пользователей ССПТ-2
110F	Некорректное значение таймаута RADIUS	Некорректное значение тайм-аута ожидания ответа от RADIUS сервера
1110	Некорректное значение числа обращений к RADIUS серверу	Некорректное значение максимального количества попыток обращения к RADIUS серверу
1111	Недопустимый слушающий интерфейс при включенном NAT	При включенном режиме трансляции сетевых адресов фильтрующие интерфейсы `Eth0` и `Eth1` не могут выступать в роли принимающего интерфейса
1112	Ошибка открытия сохраненного набора правил	Системная ошибка открытия файлов резервной копии текущего набора правил. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Повторить выполнение команды. В случае повторения ошибки обратиться на предприятие-изготовитель
1113	Получен некорректный символ	Встретился некорректный символ при загрузке с управляющего компьютера дополнительной конфигурации или дополнительного набора правил
1114	Получена некорректная конфигурация	Дополнительная конфигурация не соответствует комплектации ССПТ-2 по количеству фильтрующих интерфейсов
1115	Недопустимое пороговое значение	Некорректное значение порога интенсивности трафика для режима обнаружения flood-атак.
1116	Недопустимый формат комментария	Комментарий временного IP-правила не соответствует принятому формату.
1117	Недопустимое значение времени жизни	Некорректное значение времени жизни для временного IP-правила
1118	Недопустимые параметры зеркалирования	В дополнительной конфигурации установлены некорректные значения параметров зеркалирования трафика
1119	Неверная длина	Длина секретного ключа RADIUS сервера превышает максимально допустимую
111A	Выполнение данной команды разрешено только через системную консоль	Команда предназначена только для выполнения пользователем `admin` и только с системной консоли ССПТ-2
111B	Стартовый сценарий WEB-интерфейса завершился неудачей	Ошибка при включении WEB-интерфейса администратора ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно просмотрев файл системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки
111C	Ошибка чтения файла сертификата УЦ (SSL)	Системная ошибка чтения файла сертификата Удостоверяющего Центра (используется в OpenSSL). **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
111D	Ошибка чтения файла сертификата ССПТ-2 (SSL)	Системная ошибка чтения файла сертификата ССПТ-2 (используется в OpenSSL). **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
111E	Ошибка чтения файла сертификата ССПТ-2 (ГОСТ)	Системная ошибка чтения файла сертификата ССПТ-2 (используется в FNPCrypt). **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
111F	Пропущен комментарий	В соответствии с синтаксисом команды необходимо указание комментария. **Действия**: Воспользоваться контекстной справкой по команде или настоящим руководством для уточнения синтаксиса
1120	Системная ошибка на стороне сервера высокой готовности	Системная ошибка при обработке запроса сервером высокой готовности ССПТ-2 **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1121	Ошибка изменения пароля SNMP-пользователя	Системная ошибка при изменении пароля пользователя `fnpsnmp` для доступа к SNMP-агенту ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1122	Стартовый сценарий SNMP-интерфейса завершился неудачей	Ошибка при включении SNMP-интерфейса администратора ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно просмотрев файл системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки
1123	Неверный формат пароля SNMP-пользователя	Пароль пользователя `fnpsnmp` для доступа к SNMP-агенту ССПТ-2 не соответствует принятому формату
1124	Ошибка открытия файла конфигурации SNMP	Системная ошибка при открытии файла конфигурации SNMP-агента ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно просмотрев файл системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки
1125	Файл конфигурации SNMP поврежден	Нарушена внутренняя структура файла конфигурации SNMP-агента ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель, предварительно просмотрев файл системных сообщений (команда `log syslog show`) для уточнения причины возникновения ошибки
1126	Ошибка чтения файла конфигурации SNMP	Системная ошибка чтения файла конфигурации SNMP-агента ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель
1127	Ошибка записи файла конфигурации SNMP	Системная ошибка записи файла конфигурации SNMP-агента ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель

Код	Сообщение	Описание
1128	Ошибка генерации нового ключа SNMP-пользователя	Ошибка генерации ключа аутентификации пользователя `fnpsnmp` для доступа к SNMP-агенту ССПТ-2. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Повторить выполнение команды. В случае повторения ошибки обратиться на предприятие-изготовитель
1129	Ошибка отправки сигнала SNMP-агенту	Системная ошибка при отправке сигнала процессу SNMP-агента ССПТ-2, извещающего об изменении в конфигурации SNMP-интерфейса. **Действия**: Проверить целостность компонентов программного обеспечения ССПТ-2. Перезагрузить ССПТ-2. В случае повторения ошибки обратиться на предприятие-изготовитель