Технология ДИОНИС

Двухсегментная архитектура

Руководство по настройке изделий и управлению их работой

RU.НКБГ.30009-03 91

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата
2049	11.10.2018	1729		

Содержание

1. Введение

Настоящий документ «Технология ДИОНИС. Двухсегментная архитектура. Руководство по настройке изделий и управлению их работой» RU.НКБГ.30009-03 91 (далее – РНУ) предназначено для обслуживающего персонала изделий защиты, исполненных в двухсегментной архитектуре технологии DioNIS®. РНУ содержит сведения о настройке программного обеспечения этих изделий и об управлении их функционированием. Версия 4.

1.1. Общие сведения

ООО «Фактор-ТС» является разработчиком непрерывно совершенствуемой технологии DioNIS®, применяемой в качестве базового компонента при создании широкого спектра телекоммуникационных IP-устройств, включая набор устройств защиты, сертифицированных для применения в составе защищенных сетей передачи данных (далее – ЗСПД) как при обмене конфиденциальной информацией, так и при обмене информацией, содержащей сведения, составляющие государственную тайну.

Под технологией DioNIS® понимается набор аппаратных и программных средств, с помощью которых обеспечивается оснащение специализированных вычислительных устройств, выполняющих в сетях передачи данных обработку потоков данных, оптимизированную в соответствии с потребностями Пользователя.

Изделие, оснащенное по технологии DioNIS®, является многофункциональным телекоммуникационным сервером с функциями защиты передаваемой через сети общего пользования информации, предназначенным для построения ЗСПД различного масштаба (организованных согласно системным требованиям `internet/intranet`-технологии). Применение технологии DioNIS® при этом позволяет обеспечить соответствие пакета сервисов, набора средств защиты и их уровня, предоставляемых изделием, оснащенным этой технологией, потребностям Пользователя.

Базовым компонентом технологии DioNIS® является универсальный программный комплекс, на основе которого выполняется генерация сетевой операционной системы, в результате чего формируется вариант кода *программы управления функционированием изделия* (далее – программа управления, программное обеспечение ДИОНИС или ПО ДИОНИС), оптимизированного с учетом потребностей Пользователя в функционале изделия.

С развитием технологии DioNIS® наряду с поколением изделий, разработанных ранее ООО «Фактор-ТС» на основе принципов *односегментной* архитектуры, появилось поколение изделий, функционирующих на основе принципов *двухсегментной* архитектуры. Это − изделия серии М-479Рх, условно называемые изделиями *нового поколения* или *новыми* изделиями.

В технических решениях, применяемых для изделий, исполненных в *односегментной* архитектуре технологии DioNIS®, все функции обработки потоков данных выполняются размещенным в моноблоке изделия набором специализированных контроллеров, использующих ресурсы *единственного* универсального вычислительного процессора (далее – УВП).

Рис. 1.1 Упрощенная схема информационного взаимодействия основных элементов изделия, исполненного в односегментной архитектуре технологии DioNIS®

Сокращения на рисунке:

УВП – универсальный вычислительный процессор;

МКЗ – модуль криптографической защиты;

КД – ключевые документы;

ЛВС – локальная вычислительная сеть.

В изделиях, исполненных в односегментной архитектуре технологии DioNIS®, через системные ресурсы УВП циркулируют все виды обрабатываемой изделием информации, включая информацию, подлежащую защите. Вычислительные мощности и ресурсы, сосредоточенные в рамках одного УВП и разделяемые встроенными в моноблок изделия специализированными контроллерами, ограничивают возможности повышения пропускной способности и надежности функционирования изделия в целом. Иллюстрирует сказанное приведенная на Рис. 1.1 схема обработки информационных потоков компонентами моноблока изделия, исполненного в односегментной архитектуре.

Управление работой таких изделий осуществляется с помощью загружаемой в УВП соответствующей программы управления функционированием изделия. Настройка режимов работы программы и управление работой этих изделий выполняются в соответствии со сведениями, изложенными в документе «ДИОНИС. Руководство по настройке программного обеспечения («сборка FW»)» НКБГ.465651.001Д10 и в руководстве по эксплуатации на конкретное изделие (далее – РЭ).

Настоящий документ предназначен для обслуживающего персонала, эксплуатирующего изделие, исполненное в двухсегментной архитектуре технологии DioNIS®, и представляет собой как руководство по настройке режимов работы программы управления функционированием, так и руководство по управлению работой изделия серии М-479Рх (далее – изделие).

Основные особенности *двухсегментной* архитектуры, реализуемой поколением изделий, использующих новые возможности технологии DioNIS®, изложены ниже.

1.2. Двухсегментная архитектура технологии DioNIS®

Необходимость совершенствования изделий потребовала дальнейшего развития технологии DioNIS® и привела к появлению поколения изделий, исполненных в *двухсегментной* архитектуре. Основные элементы этой архитектуры и характер их информационного взаимодействия приведены на схеме Рис. 1.2.

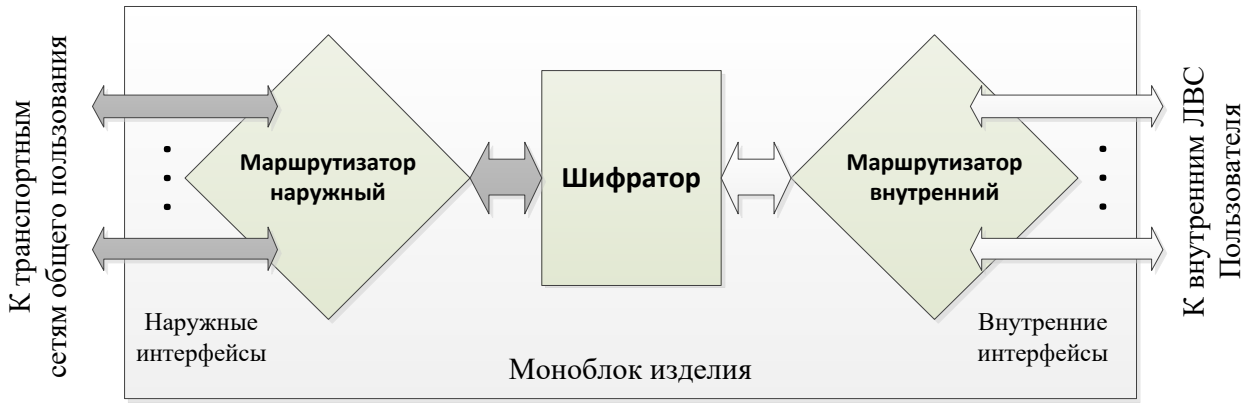


Рис. 1.2 Схема информационного взаимодействия основных элементов изделия, исполненного в двухсегментной архитектуре технологии DioNIS®

Основное содержание двухсегментной архитектуры технологии DioNIS® составляет реализация в моноблоке изделия схемы обработки IP-трафика в виде последовательной цепочки трех самостоятельных компонентов: двух конструктивно независимых IP-маршрутизаторов (наружного и внутреннего) и шифратора IP-потоков данных (см. Рис. 1.2). При этом информационное взаимодействие между маршрутизаторами осуществляется исключительно через шифратор.

Информация Пользователя, содержащая сведения, подлежащие защите, через внутренние сетевые интерфейсы моноблока поступает на внутренний маршрутизатор, выполненный как самостоятельный УВП; внутренний маршрутизатор передает исходящую открытую информацию Пользователя (на схеме – стрелки без заливки) шифратору.

Шифратор, выполненный в виде самостоятельного вычислительного устройства, получив открытую информацию Пользователя, осуществляет необходимые криптографические преобразования и передает зашифрованную информацию наружному маршрутизатору (на схеме Рис. 1.2 – стрелки с серой заливкой).

Наружный маршрутизатор выполнен также как самостоятельный УВП. Подлежащая передаче закрытая информация, полученная наружным маршрутизатором от шифратора, передается получателю через соответствующий внешний сетевой интерфейс моноблока.

Обработку закрытого IP-трафика, получаемого из сетей общего пользования, компоненты моноблока изделия осуществляют в обратном порядке, выполняя расшифрование входящего IP-трафика в шифраторе.

Конструктивно изделие, исполненное в двухсегментной архитектуре, представляет собой:

- моноблок, в корпус которого вмонтированы следующие основные элементы обработки IP-трафика:
  - два УВП – наружный и внутренний маршрутизаторы, конструктивно выполненные каждый в виде устройства на базе одного из сегментов двухсегментной объединительной платы или в виде отдельного устройства;
  - подключаемый между маршрутизаторами шифратор, выполненный в виде отдельного устройства;
- подключаемые к моноблоку необходимые внешние устройства.

На Рис. 1.3 приведена общая функциональная схема изделия, исполненного в двухсегментной архитектуре технологии DioNIS®. На рисунке группы устройств, входящие в состав моноблока, объединены в следующие функциональные блоки:

- блок обеспечения функционирования и управления изделием (далее – **БФУ**);
- блок наружной маршрутизации (далее – **БНМ**);
- блок внутренней маршрутизации (далее – **БВМ**);
- блок криптографической обработки – шифратор (далее – **БКО**).

БФУ содержит следующие компоненты, обеспечивающие работу изделия:

- блок электропитания внутренних устройств;
- технические средства локальной консоли управления изделием (далее – ЛКУ) – клавиатуру и видеомонитор (встроенные в моноблок изделия или выполненные в виде отдельного конструктива, подключаемого к моноблоку), а также устройство попеременного подключения технических средств ЛКУ к тому из УВП, который в настоящий момент требует управляющих действий обслуживающего персонала.

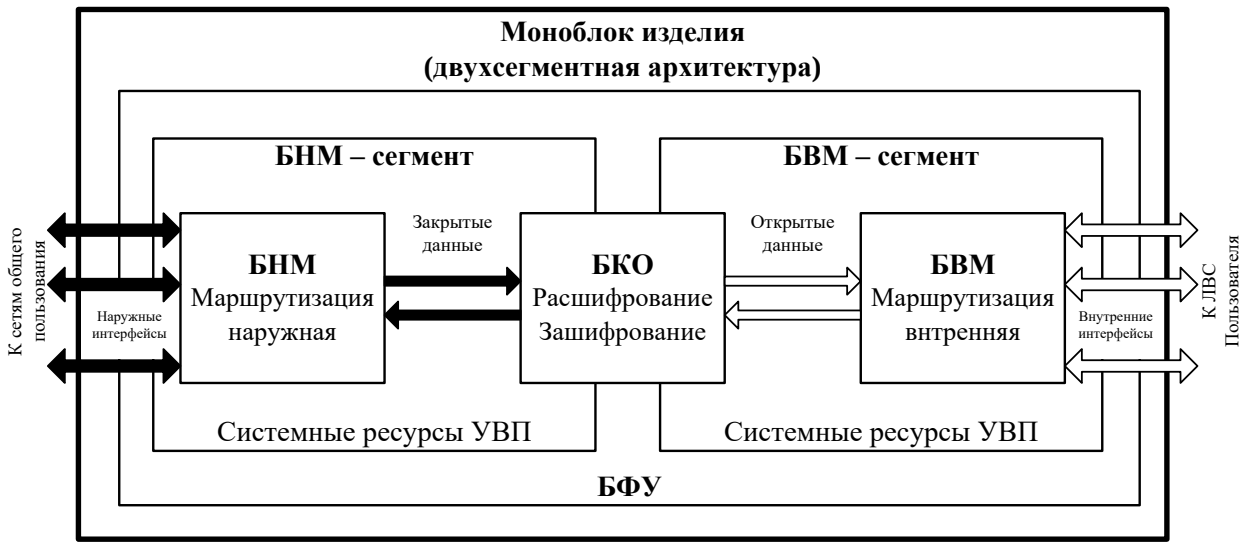


Рис. 1.3 Общая функциональная схема изделия, исполненного в двухсегментной архитектуре технологии DioNIS®

БНМ и БВМ обеспечивают обработку (маршрутизацию) трафиков подключенных к изделию сетей внешнего или внутреннего сегментов ЗСПД соответственно.

С помощью встроенных в моноблок сетевых интерфейсов изделие может быть подключено:

- по внутренним сетевым интерфейсам - к каналам связи, соединяющим изделие с сетями, в которых информация Пользователя, подлежащая защите, циркулирует в открытом виде;
- по наружным сетевым интерфейсам - к каналам связи, соединяющим изделие с сетями общего пользования, в которых циркулирует информация Пользователя, защищенная с помощью изделий, аттестованных для ее защиты.

Информационное взаимодействие между маршрутизаторами изделия – БНМ и БВМ – осуществляется исключительно через его шифратор – БКО, который обеспечивает криптографическую обработку *исходящего* (зашифрование) и *входящего* (расшифрование) трафиков изделия.

1.3. Управление изделиями

1.3.1. Архитектура системы управления

Для решения задач управления изделием, исполненным в двухсегментной архитектуре, в его состав включены функциональные элементы системы управления изделием, схема взаимодействия которых представлена на Рис. 1.4. Описание архитектурных элементов системы управления изделием приведено ниже.

Аппаратура локальной консоли управления (АЛКУ) – комплект аппаратуры, состоящий из:

- видеомонитора и клавиатуры (встроенных в моноблок изделия или внешних по отношению к нему);
- встроенного в моноблок переключателя, обеспечивающего возможность подключения технических средств ЛКУ к наружному или к внутреннему маршрутизатору (при этом информационное взаимодействие между маршрутизаторами через переключатель исключается).

Консоль управления наружная (КуН) и **Консоль управления внутренняя (КуВ)** – программные компоненты, обеспечивающие в соответствующем блоке маршрутизатора прием и интерпретацию потока данных канала управления от консоли управления локального изделия (или от консоли управления изделия, осуществляющего удаленное управление через сеть передачи данных) и передачу его соответствующему *агенту управления*. Индикация реакции агента управления на управляющие воздействия передается консолью управления на видеомонитор локального изделия (либо через сеть передачи данных на видеомонитор удаленного управляющего изделия).

Агент управления наружный (АуН) и **Агент управления внутренний (АуВ)** – программные компоненты, обеспечивающие собственно манипулирование параметрами управления (параметрами конфигуратора изделия, данными статистики и журналами изделия) соответственно в составе наружного или внутреннего маршрутизаторов.

Журналы и статистика наружного маршрутизатора (ЖсН) и **Журналы и статистика внутреннего маршрутизатора (ЖсВ)** – журналы, содержащие множество записей фиксации событий в работе соответственно наружного или внутреннего маршрутизаторов (хранятся журналы на энергонезависимом запоминающем устройстве БНМ или БВМ); множество значений текущих параметров статистики работы маршрутизатора (хранится статистика в оперативной памяти и, частично, на энергонезависимом запоминающем устройстве). Доступ к журналам и к параметрам статистики на чтение и на их запись имеет только агент управления соответствующего маршрутизатора.

Объединенная база параметров настройки (БпО) – множество значений параметров конфигуратора изделия, хранящееся в энергонезависимой памяти шифратора.

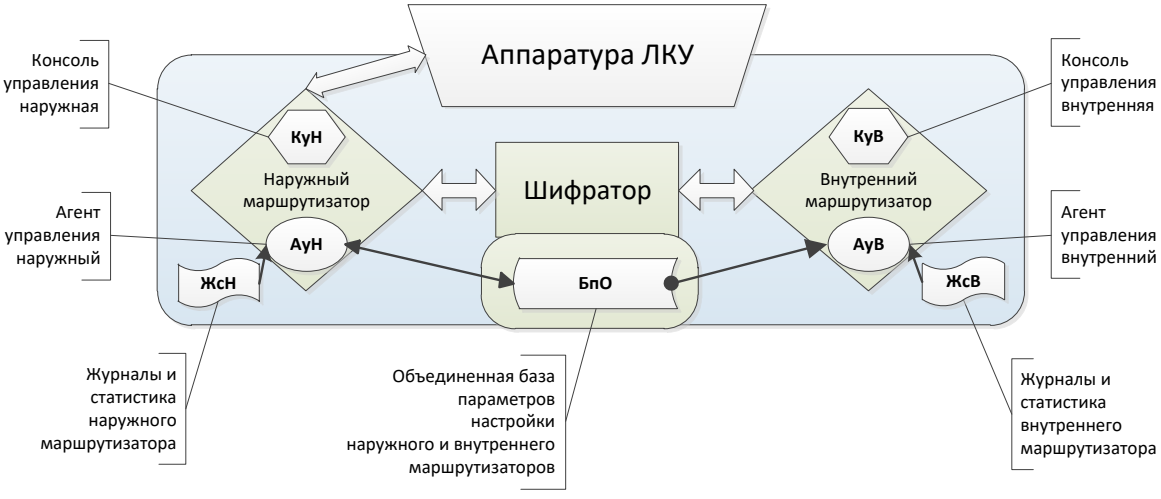


Рис. 1.4 Схема взаимодействия функциональных элементов системы управления изделием

Управление изделием подразумевает решение следующих трех задач:

1) **конфигурирование изделия** – изменение значений параметров *конфигуратора* (параметров настройки изделия) и выдача команд на ввод измененных параметров в действие;
2) **наблюдение за изделием** – получение оперативной информации о состоянии компонентов изделия путем считывания и интерпретации множества текущих значений параметров, получение статистики, а также применение функций, используемых при наладке работы изделия;
3) **работа с журналами изделия** – прием, накопление и анализ записей журналов фиксации событий в работе изделия, а также выдача команд на очистку локальной памяти журналов изделия.

Решение указанных задач выполняется в режиме *локального* или *удаленного* управления; особенности этих режимов рассмотрены ниже.

1.3.2. *Локальное управление*

Локальное управление изделием осуществляет обслуживающий персонал узла связи ЗСПД, на котором эксплуатируется изделие, с помощью встроенных в моноблок изделия или подключаемых к моноблоку дополнительных технических средств локальной консоли управления – клавиатуры и видеомонитора, а также с помощью переключателя, обеспечивающего попеременное подключение технических средств ЛКУ (встроенных или внешних) к требуемому блоку изделия – БВМ, БНМ или БКО.

Конфигурирование изделия – первая задача управления. Механизм конфигурирования изделия, реализованный в изделиях, исполненных в двухсегментной архитектуре, радикально отличается от механизма конфигурирования в изделиях, исполненных в односегментной архитектуре технологии DioNIS®. Вызвано это наличием в моноблоке изделия, исполненного в двухсегментной архитектуре, трех самостоятельных вычислительных устройств и, соответственно, трех независимо работающих программ управления функционированием этих устройств: программного обеспечения (ПО) управления блоком наружной маршрутизации, ПО управления блоком внутренней маршрутизации и ПО управления блоком криптографической обработки (шифратором). Каждая из программ управления имеет свой набор параметров, задающих режим ее работы, и настройка этих параметров для всех вычислительных устройств изделия (БВМ, БНМ и БКО) должна быть *синхронизирована*.

Выполнять настройку всего изделия, настраивая независимо друг от друга три вычислительных устройства, нецелесообразно – часть параметров, используемая БВМ, БНМ и БКО, имеет одни и те же значения (например, параметры настройки туннелей). При большом количестве параметров практически невозможно, записав их один раз, повторить вручную те же действия безошибочно.

Поэтому задача конфигурирования решается новыми изделиями следующим образом.

Все множество параметров, определяющих особенности режимов работы каждого из устройств моноблока изделия, – *конфигуратор изделия* – размещается в единой *объединенной Базе параметров* (**БпО –** на схеме Рис. 1.5), которая хранится в энергонезависимой памяти шифратора. Поэтому после выключения электропитания изделия его конфигуратор, записанный в **БпО**, сохраняется и определяет режим работы изделия при последующих запусках изделия. Наличие объединенной базы параметров **БпО** решает также задачу *синхронизации* значений параметров настройки БВМ, БНМ и БКО.

Доступ к объединенной базе **БпО** организован со стороны обоих маршрутизаторов. При этом наружному маршрутизатору разрешены *чтение и запись* информации в **БпО**, а внутреннему маршрутизатору – только ее *чтение*. Таким образом, изменение значений параметров объединенной базы **БпО** может быть выполнено только со стороны *наружного* маршрутизатора изделия.

Кроме объединенной базы **БпО** существуют две *оперативные* базы параметров (**БпН** и **БпВ** на Рис. 1.5):

- оперативная база параметров БНМ (**БпН**) – множество значений параметров конфигуратора, определяющих режим работы БНМ;
- оперативная база параметров БВМ (**БпВ**) – множество значений параметров конфигуратора, определяющих режим работы БВМ.

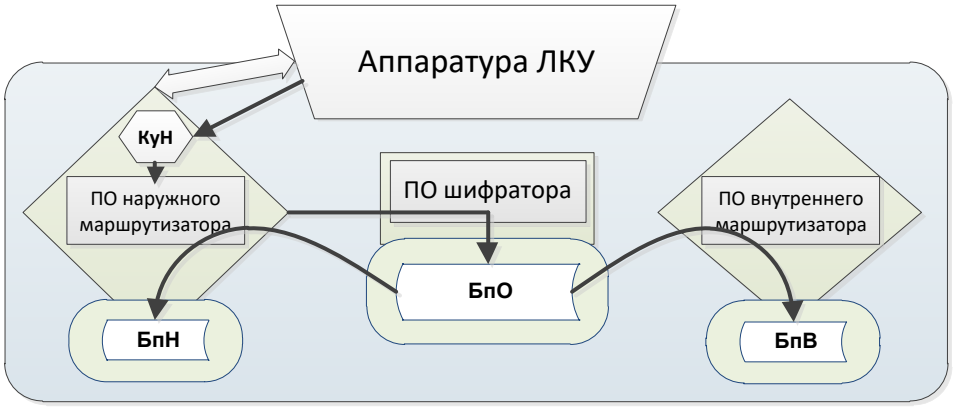


Рис. 1.5 Схема взаимосвязи баз параметров изделия и функциональных элементов системы управления

При выключении изделия и при каждом его перезапуске параметры из оперативных баз маршрутизаторов удаляются. При включении изделия (или при его перезапуске) соответствующие параметры конфигуратора считываются из объединенной базы **БпО** в соответствующие оперативные базы – в **БпН** и **БпВ**.

Чтобы выполнить настройку (конфигурирование) изделия, следует подключить технические средства ЛКУ к БНМ (см. раздел 1.3.4, с. 14), получить на экране видеомонитора ЛКУ меню первого уровня – Главное меню программы управления функционированием БНМ (см. Рис. 1.9, раздел 1.3.4, с. 14), перевести программу управления функционированием БНМ в режим *настройки*, выбрав альтернативу Главного меню **Настройка** (см. Рис. 1.10, раздел 1.3.4, с. 14), после чего задать требуемые значения параметров конфигуратора.

> *Примечание.* Альтернатива Главного меню **Настройка** доступна для управления лишь персоналу, имеющему привилегии *администратора* изделия (подробнее об обеспечиваемых изделием режимах разграничения и уровнях доступа персонала к управлению изделием см. раздел 1.3.4, с. 14 и раздел 8.4, с. 183).

Процесс конфигурирования при этом организован так, что одновременно настраиваются параметры обоих маршрутизаторов. В случаях, когда параметры должны иметь *одинаковые* значения для БНМ и БВМ (например, при настройке параметров туннелей), их настройка выполняется без предварительных запросов программы управления. Если возможны *различные* значения параметров БНМ и БВМ (например, при настройке параметров служб), то программа управления предварительно выдает запрос о том, параметр какого из маршрутизаторов – внутреннего или наружного – предстоит настроить.

> *Примечание.* Войти в меню **Настройка** можно и при подключении технических средств ЛКУ к БВМ, но, как отмечалось выше, БВМ имеет доступ к содержимому **БпО** только на чтение, поэтому запись новых значений параметров конфигуратора в **БпО** при обращении с БВМ невозможна. При входе в меню **Настройка** с использованием средств ЛКУ, подключенных к БВМ, программа управления выдает соответствующее предупреждение.

После того как будут настроены все параметры, обновленный конфигуратор следует записать в объединенную базу параметров – **БпО**. Но запись в **БпО** по умолчанию запрещена (это служит защитой от несанкционированной записи информации в **БпО**). Если значения каких-либо параметров были отредактированы (изменены), то по окончании процесса конфигурирования программа управления выдаст на видеомонитор ЛКУ запрос о необходимости или игнорировании записи выполненных обновлений конфигуратора в память **БпО**. Чтобы дать разрешение на запись, администратор должен перевести БКО в режим *разрешения записи* в **БпО**. Перевод БКО в этот режим осуществляется администратором вручную с использованием средств управления шифратором (о порядке управления работой шифратора см. РЭ на конкретное изделие).

После выполнения администратором действий, необходимых для сохранения обновленного конфигуратора, происходит следующее.

1. Отредактированные параметры конфигуратора из оперативной памяти наружного маршрутизатора перезаписываются в шифратор – в долговременную энергонезависимую память объединенной базы параметров **БпО** (в).
2. ПО наружного маршрутизатора загружает в свою оперативную базу (**БпН**) обновленные значения параметров из **БпО**.
3. На БВМ поступает сигнал об изменении настроек конфигуратора изделия. В ответ ПО внутреннего маршрутизатора считывает обновленные значения параметров настройки из объединенной базы **БпО** и загружает их в свою оперативную базу **БпВ**.
4. В зависимости от характера обновлений конфигуратора обоими маршрутизаторами изделия может быть выполнен перезапуск отдельных вычислительных процессов с учетом нового содержимого баз **БпН** и **БпВ** (рестарт сетевых интерфейсов, криптотуннелей и пр.)

> *Замечание.* Средства локальной консоли изделия можно подключить к БВМ, после чего на экране видеомонитора ЛКУ будет представлено Главное меню программы управления внутренним маршрутизатором. Это меню служит, главным образом, для контроля действующих значений параметров и сбора статистики о работе БВМ. Главное меню программы управления БВМ применяется также для получения сведений о криптотуннелях и загруженных в изделие ключах; эти сведения нельзя получить, подключив средства ЛКУ к БНМ.
>
> Есть несколько второстепенных параметров конфигуратора (параметры локальной консоли, удаленной консоли и параметры абонентов), которые можно изменить из БВМ, но в измененном виде они будут записаны только в оперативную базу параметров БВМ – **БпВ**. Никакого влияния на функционирование БНМ или БКО внесенные изменения оказывать не будут и будут потеряны после ближайшего перезапуска изделия.

Наблюдение за изделием и **работа с журналами** – вторая и третья задачи управления – решаются для каждого маршрутизатора с помощью соответствующего *Агента управления* (**АуН** или **АуВ**) и соответствующей *Консоли управления* (**КуН** или **КуВ**) после подключения средств ЛКУ к требуемому маршрутизатору (БВМ или БНМ).

1.3.3. **Удаленное управление**

Удаленное управление изделиями защиты осуществляет обслуживающий персонал специального узла связи, имеющего в составе ЗСПД статус *Центра удаленного администрирования* (далее – ЦУА). Администрацией ЗСПД может быть организовано несколько узлов связи, осуществляющих функции ЦУА (например, *основной* и *резервные* ЦУА).

Обслуживающий персонал ЦУА осуществляет удаленное управление изделиями с помощью оборудования специализированных телекоммуникационных *управляющих* средств, подключаемых по мере необходимости к *управляемым* изделиям через сети передачи данных по защищенным каналам связи. В качестве технических *средств удаленного управления* применяются изделия нового поколения, переведенные в режим ***Администратор сети*** (см. раздел 11, с. 204).

При этом система *удаленного* управления изделиями имеет ту же архитектуру и включает те же функциональные элементы управляющих и управляемых изделий, что и при организации *локального* управления изделиями.

Конфигурирование управляемых изделий − основная задача удаленного управления. Применение средств удаленного управления для изменения значений параметров конфигураторов управляемых изделий предполагает удаленное сетевое взаимодействие между *управляющим* и *управляемыми* изделиями в составе ЗСПД по защищенным каналам связи.

Основным вариантом удаленного конфигурирования является вариант, при котором персонал управляющего изделия удаленно (по защищенному каналу управления) получает на своем рабочем месте копию объединенной базы параметров **БпО** управляемого изделия, редактирует ее и передает обновленный конфигуратор на управляемое изделие для корректировки режима его работы. Если бы удаленное управление изделием выполнялось по той же схеме, что и локальное (см. раздел 1.3.2, с. 10), то потребовалось бы присутствие рядом с управляемым изделием его локального администратора, который должен был бы всякий раз при удаленном редактировании конфигуратора персоналом ЦУА вручную подтверждать на управляемом изделии разрешение на запись обновляемых параметров в **БпО** управляемого изделия.

Во избежание этого неудобства для организации удаленного конфигурирования изделия применяется алгоритм, отличающийся от алгоритма *локального* управления. Иллюстрирует работу алгоритма представленная ниже (Рис. 1.6) схема взаимодействия элементов системы управления при удаленном конфигурировании изделия.

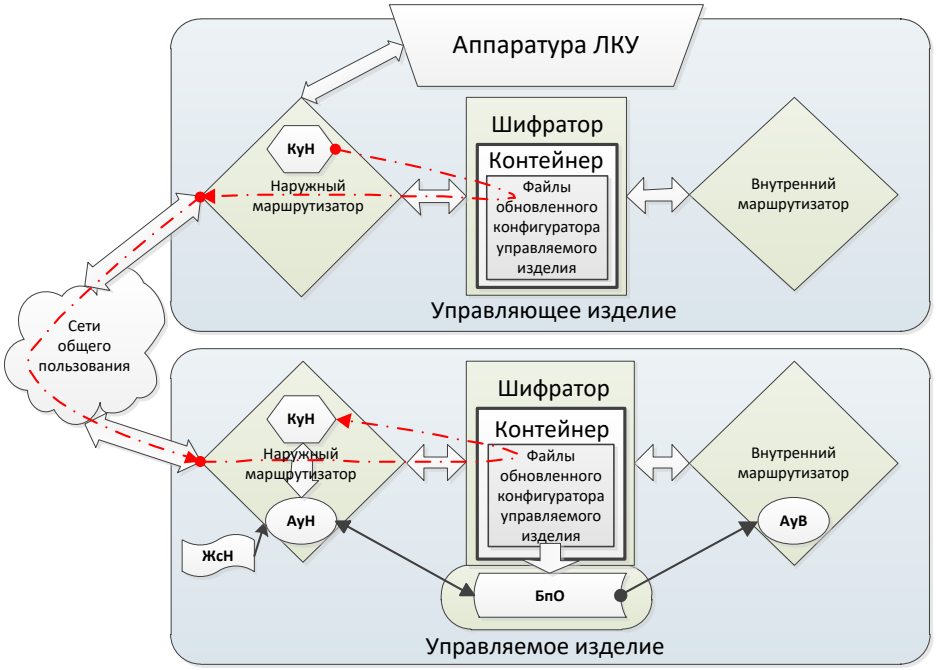


Рис. 1.6 Схема взаимодействия элементов системы управления при удаленном конфигурировании изделия

1. Персонал управляющего изделия, подключив средства ЛКУ к БНМ, устанавливает соединение с наружным агентом управления управляемого изделия и, используя сетевой протокол управления DCP (подробнее см. раздел 5.1, с. 152), считывает конфигуратор управляемого изделия из его **БпО**.
2. Персонал управляющего изделия в локальном режиме управления редактирует значения параметров, формируя требуемый конфигуратор управляемого изделия.
3. Чтобы исключить необходимость на управляемом изделии вручную подтверждать разрешение на запись обновленного конфигуратора в **БпО** (как это делается при локальном управлении), для передачи

конфигуратора на управляемое изделие шифратор управляющего изделия помещает обновленный конфигуратор управляемого изделия в *контейнер*, зашифровывает контейнер и передает его БНМ своего изделия для отправки на управляемое изделие.

4. БНМ управляемого изделия получает контейнер и отправляет его прямо шифратору (БНМ управляемого изделия при этом выполняет только роль маршрутизатора). Шифратор извлекает обновленный конфигуратор из контейнера и без подтверждения персоналом записывает конфигуратор в объединенную базу параметров **БпО**, после чего посылает на БНМ сигнал об изменении конфигуратора изделия.
5. Получив сигнал шифратора об изменении конфигуратора, БНМ считывает и загружает в свою оперативную базу **БпН** обновленные значения параметров, после чего посылает сигнал на БВМ об изменении содержимого **БпО**. В ответ БВМ также считывает новые значения параметров из объединенной базы **БпО** и загружает их в свою оперативную базу **БпВ**.
6. В зависимости от характера обновлений конфигуратора обоими маршрутизаторами управляемого изделия может быть выполнен перезапуск отдельных вычислительных процессов с учетом нового состояния **БпН** и **БпВ** (рестарт сетевых интерфейсов, открытие криптотуннелей и пр.).

При таком алгоритме удаленного управления подтверждения разрешения на запись в объединенную базу параметров **БпО** не требуется.

> *Примечание.* Удаленное конфигурирование управляемого изделия возможно во вспомогательном варианте, предусматривающем подключение БНМ управляющего изделия к БНМ управляемого изделия в режиме *удаленной консоли* (подробнее см. раздел 4.1.4, с. 134). При этом персонал ЦУА, используя консоль БНМ управляющего изделия, получает доступ к БНМ управляемого изделия, включая и управление настройкой его конфигуратора. Неудобством этого варианта конфигурирования является необходимость *синхронного* с действиями персонала ЦУА *ручного* подтверждения персоналом управляемых изделий разрешения на запись конфигуратора в **БпО** управляемого изделия.

Наблюдение за изделием – вторая задача управления. Для ее решения нельзя воспользоваться рассмотренным выше алгоритмом, т.к. наблюдение за работой управляемого изделия должно выполняться оперативно, в режиме реального времени.

Для решения задачи наблюдения следует использовать реализованную в изделиях возможность контроля функционирования управляемого изделия в режиме *удаленной консоли*. В этом режиме обслуживающий персонал управляющего изделия может подключиться по сети общего пользования к управляемому изделию и получить на своей наружной или внутренней консоли доступ к соответствующей консоли управляемого изделия – *удаленную консоль*.

Схема организации удаленного доступа к *наружной* консоли управляемого изделия представлена на Рис. 1.7.

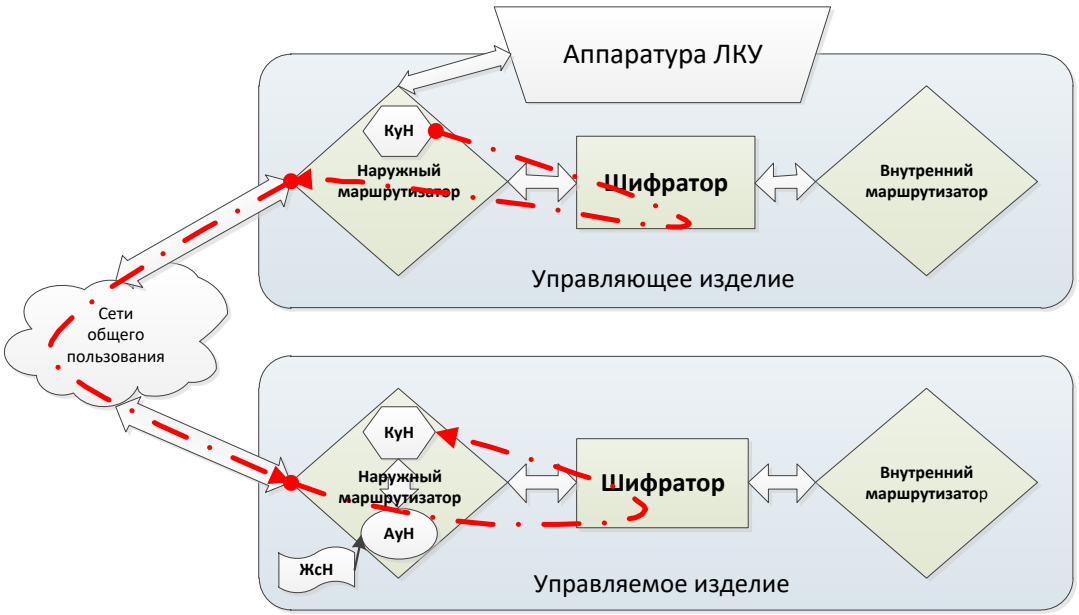


Рис. 1.7 Схема организации удаленного доступа к консоли БНМ управляемого изделия

На управляющем изделии средства ЛКУ подключаются персоналом ЦУА к БНМ и обеспечивается сессия доступа аппаратуры локальной консоли к наружной консоли управления. Через сеть устанавливается соединение с наружным агентом управления управляемого изделия (используется сетевой протокол управления DCP), и оперативный доступ к консоли наружного маршрутизатора управляемого изделия появляется на

управляющем изделии. При установлении соединения между наружными маршрутизаторами управляющего и управляемого изделий организуется криптографически защищенный канал управления.

В этом режиме можно проконтролировать работу и все настройки БНМ управляемого изделия, организовать трассировку его работы и оперативную наладку, проанализировать статистику функционирования БНМ, а также получить доступ к конфигурированию управляемого изделия.

Схема организации удаленного доступа к *внутренней* консоли управляемого изделия представлена на Рис. 1.8.

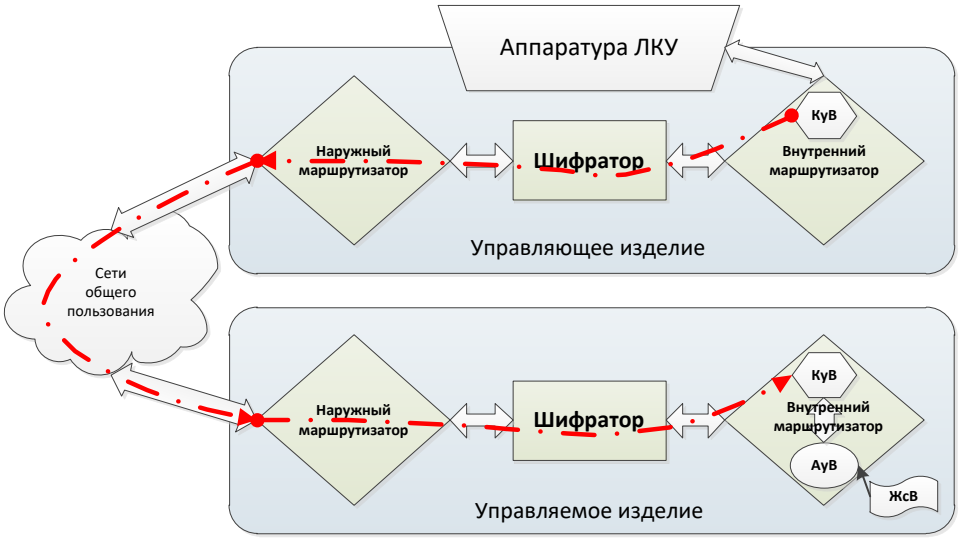


Рис. 1.8 Схема организации удаленного доступа к консоли БВМ управляемого изделия

На управляющем изделии средства ЛКУ подключаются персоналом ЦУА к БВМ и обеспечивается сессия доступа аппаратуры локальной консоли к консоли управления БВМ управляющего изделия. Для организации доступа используется штатная функция шифраторов управляющего и управляемого изделий – криптографический туннель, обеспечивающий защиту канала данных; специального защищенного канала управления в этом случае не требуется.

По штатному криптографическому туннелю устанавливается соединение через сеть с внутренним агентом управления управляемого изделия (используется сетевой протокол управления DCP), и персонал ЦУА получает на консоли БВМ управляющего изделия оперативный доступ к консоли БВМ управляемого изделия для контроля за настройками и работой БВМ управляемого изделия.

В этом режиме можно проконтролировать работу и все настройки БВМ, организовать трассировку его работы и оперативную наладку, проанализировать статистику функционирования БВМ управляемого изделия.

Работа с журналами – третья задача удаленного управления – решается также отдельно для каждого из маршрутизаторов изделия.

На управляющем изделии обеспечивается сессия доступа аппаратуры локальной консоли к наружной или к внутренней консоли управления; через сеть устанавливается соединение соответственно с наружным или с внутренним агентом управления управляемого изделия (**`АуН`** или **`АуВ`**) по той же схеме, что и при получении доступа к соответствующей консоли удаленного управляемого изделия (удаленной консоли). После установления соединения на управляющем изделии можно получить по сети журналы результатов работы БНМ или БВМ управляемого изделия.

1.3.4. *Общие вопросы управления работой изделия*

Управление работой изделия осуществляется с помощью программы управления функционированием изделия, состоящей из независимых компонентов, каждый из которых загружается в соответствующий блок изделия БКО, БВМ, БНМ. При запуске изделия после включения электропитания в блоки БВМ и БНМ загружается т.н. *общее* программное обеспечение – ОПО, управляющее функционированием обоих маршрутизаторов изделия. В блок БКО загружается *специальное* программное обеспечение – СПО, управляющее работой шифратора.

Порядок работы обслуживающего персонала в процессе диалога с СПО, функционирующим в составе БКО, рассмотрен в РЭ на конкретное изделие.

Порядок выполнения обслуживающим персоналом настройки ОПО и управления работой изделия в процессе диалога с соответствующим ОПО, функционирующим в составе БНМ или БВМ, приведен в настоящем РНУ. Диалог между обслуживающим персоналом и программой управления изделием осуществляется с применением технических средств ЛКУ и поддерживается с помощью иерархической системы меню, отображаемой на видеомониторе ЛКУ.

Персонал, допущенный к эксплуатации изделий, по уровню доступа к управлению изделиями подразделяется на *три* категории:

- *операторы*, выполняющие при эксплуатации изделий на узлах ЗСПД регламентные операции и контроль функционирования изделий в условиях неизменной среды окружения, не требующей перенастройки изделий;
- *администраторы узла*, обеспечивающие на штатных узлах ЗСПД по исходным данным Администрации ЗСПД настройку изделия при вводе его в эксплуатацию и перенастройку при дальнейшей его эксплуатации на объекте в условиях изменяющейся среды окружения;
- *администраторы сети*, использующие изделия (как правило, в составе выделенных узлов ЗСПД, осуществляющих функции Центров удаленного администрирования ЗСПД) как средства для удаленной (по защищенным каналам связи) настройки, контроля функционирования и управления работой других аналогичных изделий защиты в составе штатных узлов ЗСПД.

В соответствии с этим программа управления функционированием изделия поддерживает три приведенных ниже режима доступа обслуживающего персонала к управлению изделиями (процедура включения требуемого *режима доступа* к управлению изделием приведена в разделе 8.4, с. 183).

Режим **Оператор** − доступен сразу после включения электропитания и выполнения изделием необходимых подготовительных операций; в этом режиме обслуживающему персоналу доступен ограниченный набор функций изделия.

При условии ввода соответствующих паролей обслуживающий персонал изделия может перевести его в привилегированные режимы **Администратор узла** или **Администратор сети**.

Режим **Администратор узла** обеспечивает возможность применения полного набора функций для локального управления изделием.

> *Примечание.* Программа управления функционированием поддерживает работу с *несколькими* администраторами узла, каждый из которых может иметь индивидуальный настраиваемый набор прав доступа к функциям управления изделием (подробнее см. раздел 6.4, с. 171).

Режим **Администратор сети** предоставляет возможность применения полного набора функций удаленного управления аналогичными изделиями защиты в составе ЗСПД (подробнее см. раздел 11, с. 204).

Для управления блоками наружной и внутренней маршрутизации обслуживающий персонал изделий может использовать как *штатные* технические средства ЛКУ изделия, так и *дополнительные* технические средства ЛКУ)* – клавиатуру и видеомонитор.

Штатные технические средства ЛКУ встроены в моноблок изделия или выполнены в виде отдельного конструктива, подключенного к моноблоку изделия постоянно или подключаемого к нему только на время, необходимое для выполнения настройки, контроля функционирования или управления изделием.

Дополнительные технические средства ЛКУ – *стационарные* клавиатура и видеомонитор – могут быть подключены к моноблоку изделия в качестве внешних устройств. Использование дополнительных средств ЛКУ может быть продиктовано необходимостью длительной, регулярной работы персонала по настройке и управлению изделием (например, при пуско-наладочных работах, при использовании изделия в составе ЦУА ЗСПД в качестве средства удаленного управления).

Встроенный в моноблок переключатель технических средств локальной консоли управления обеспечивает возможность подключения средств ЛКУ – штатных или дополнительных – к блоку наружного или к блоку внутреннего маршрутизатора (при этом информационное взаимодействие блоков маршрутизации через переключатель исключается).

Для подключения технических средств ЛКУ к требуемому маршрутизатору следует:

а) при работе со *штатными* техническими средствами ЛКУ:
   - для подключения средств ЛКУ к БНМ – нажать одновременно клавишу-модификатор <F> и функциональную клавишу <F3>;
   - для подключения средств ЛКУ к БВМ – нажать одновременно клавишу-модификатор <F> и функциональную клавишу <F4>;

б) при работе с *дополнительными* техническими средствами ЛКУ:
   - для подключения средств ЛКУ к БНМ – нажать функциональную клавишу <F11>;
   - для подключения средств ЛКУ к БВМ – нажать функциональную клавишу <F12>.

---

* К дополнительным техническим средствам ЛКУ предъявляются специальные требования, укзанные в документах, регламентирующих порядок использования изделий (см. комплект эксплуатационной документации на изделие).

Изделием поддерживается три различных регистра раскладки клавиатуры (три набора раскладки символов по клавишам клавиатуры): набор латинских символов и два набора символов кириллицы – ЯВЕРТЫ или ЙЦУКЕН. При этом:

- нажатие клавиши <F9> включает латинский регистр; индикатор раскладки клавиатуры в левом верхнем углу экрана, выдаваемого на видеомонитор ЛКУ, принимает значение символа **L**;
- нажатие клавиши <F10> включает регистр кириллицы в раскладке ЯВЕРТЫ; индикатор принимает значение символа **R**;
- нажатие комбинации клавиш <Alt+F9> включает регистр кириллицы в раскладке ЙЦУКЕН; индикатор принимает значение символа **N**.

> *Примечание*. Клавиши для переключения между раскладками клавиатуры в регистре кириллицы (<F10> или <Alt+F9>) можно менять местами для удобства обслуживающего персонала (см. раздел 4.1.6, с. 137).

На этапе подготовки изделия к работе следует подключить к моноблоку изделия (при необходимости) средства ЛКУ и включить электропитание. По окончании процесса запуска на видеомонитор ЛКУ будет выдан экран Главного меню программы управления функционированием БНМ, аналогичное представленному на Рис. 1.9.

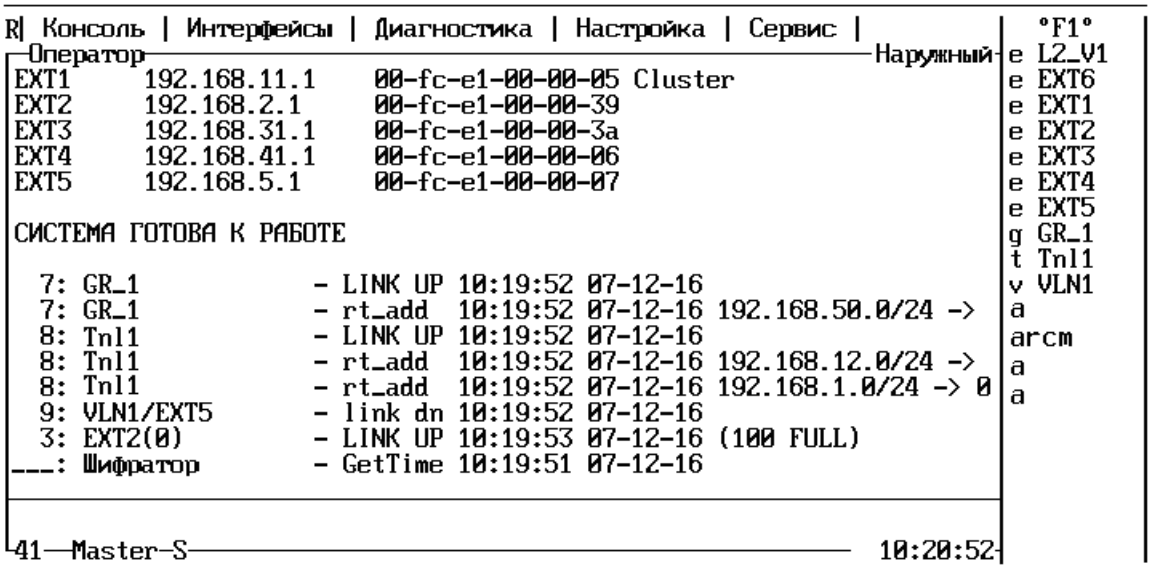


Рис. 1.9 Экран Главного меню программы управления функционированием БНМ

В верхнюю строку экрана в самую левую позицию выводится индикатор раскладки клавиатуры и затем – Главное меню (меню первого уровня) программы управления функционированием маршрутизатора (далее ГМ), включающее альтернативы: **Консоль**, **Интерфейсы**, **Диагностика**, **Настройка**, **Сервис**.

Средняя часть экрана обрамлена рамкой и отображает строки внесенных в основной журнал изделия записей последних сообщений программы управления о событиях, возникавших при работе изделия. Динамика и объем выдаваемой на экран информации зависит от интенсивности сетевой нагрузки на изделие, а также от установленной при настройке изделия степени детализации информации, необходимой для контроля и диагностики работы изделия.

> Полностью основной журнал изделия сохраняется в файле **LOG.EMA**, который всегда можно просмотреть с помощью альтернативы ГМ: **Консоль ⇨ Журналы**, описанной в разделе 8.2, с. 181.

В левом верхнем углу рамки указан текущий уровень доступа персонала к управлению изделием: **Оператор**, **Адм.узла** или **Адм.сети**. В правом верхнем углу рамки указан маршрутизатор, к которому в настоящий момент подключены технические средства ЛКУ (указатель **Внутренний** отображается на красном фоне, указатель **Наружный** – на зеленом).

Одна строка в нижней части экрана отведена для выдачи экстренных и аварийных сообщений программы управления, требующих оперативного вмешательства обслуживающего персонала; сообщения в эту область экрана выводятся *красным* цветом в мигающем режиме.

> Все сообщения из этой строки дублируются в системных журналах **LOG.EMA** и **LOG_SEND.EMA** (подробнее о журналах см. раздел ***Приложение Е***, с. 248).

На нижней границе рамки экрана могут быть размещены (в порядке следования слева направо):

- число – рабочая температура (в градусах Цельсия) центрального процессора соответствующего маршрутизатора (**41** – на Рис. 1.9);
- название статуса изделия (**Master** или **Slave**) и символ состояния (**S** – на Рис. 1.9), если изделие работает в составе кластера криптомаршрутизаторов (см. раздел 7, с. 174);
- время – текущее или прошедшее с момента включения изделия (в зависимости от настройки – см. раздел 4.1.6, с. 137).

В правой части экрана размещается *вертикальное* окно (окно *оперативного контроля* состояния интерфейсов), в котором отображается список сетевых интерфейсов соответствующего маршрутизатора. Окно служит для контроля текущего состояния отображаемых в нем интерфейсов и для оперативного получения дополнительной информации о них. Перейдя в это окно, обслуживающий персонал получает доступ к статистической информации о проделанной интерфейсом работе и к информации о параметрах настройки интерфейсов. Состав списка интерфейсов, отображаемых в этом окне, задается обслуживающим персоналом в зависимости от оперативных потребностей при управлении изделием в конкретный момент времени.

Переход в окно оперативного контроля состояния интерфейсов осуществляется нажатием клавиши <F1>. Нажатие клавиши <Esc> возвращает управление в ГМ.

> Подробнее об управлении составом списка интерфейсов, отображаемых на экране в вертикальном окне оперативного контроля, см. раздел 2.6, с. 52 настоящего РНУ.

Программы управления функционированием маршрутизаторов − БВМ и БНМ − одинаковы. Главные меню этих программ идентичны, структуры соответствующих меню и набор их альтернатив при управлении БВМ или БНМ в основном совпадают. Имеющиеся различия отмечены в тексте настоящего РНУ. Если значения параметров настройки могут быть различны для внутреннего и наружного маршрутизаторов, то перед тем как продолжить настройку программа управления предложит уточнить, параметр какого из маршрутизаторов – БВМ или БНМ – предстоит настроить.

Как было сказано выше, при управлении изделием используется иерархическая система меню. Выбор той или иной альтернативы меню первого (наивысшего) уровня иерархии приводит к появлению на экране меню более низкого уровня иерархии и т.д.

Диалог персонала с программой управления начинается с выбора той или иной альтернативы Главного меню (Рис. 1.9) и ведется по следующим правилам.

Для выбора требуемой альтернативы меню следует, пользуясь клавишами управляющих стрелок, переместить курсор на нужную альтернативу и нажать клавишу <Enter>. Кроме того, почти все альтернативы меню можно выбрать, нажав клавишу с символом, приписанным данной альтернативе: на экране этот символ выделен цветом (часто это первая буква названия альтернативы). Возврат в меню предыдущего (более высокого) уровня иерархии осуществляется нажатием клавиши <Esc>.

Меню последнего (самого нижнего) уровня в большинстве случаев содержит набор возможных значений того или иного параметра или функции изделия. Чтобы задать требуемое значение, достаточно выбрать соответствующую альтернативу. В других случаях значение параметра (функции) должно быть введено с клавиатуры. Нажатие клавиши <Esc> отменяет выбранное из меню или введенное с клавиатуры значение и возвращает процесс управления к меню предыдущего (более высокого) уровня иерархии.

Подсистема Настройка

Все вопросы настройки конфигуратора изделия для обеспечения оптимального применения и эффективного использования изделия на объектах эксплуатации решаются с использованием возможностей, предоставляемых подсистемой **Настройка** программы управления функционированием изделия. Описанию этих возможностей посвящена значительная часть разделов настоящего РНУ.

Доступ к работе с подсистемой **Настройка** предоставляется только привилегированным пользователям изделия – *администраторам изделия*. После перевода изделия в режим **Адм.узла** становится доступной альтернатива ГМ **Настройка** (см. Рис. 1.9, с. 16), при выборе которой на видеомонитор ЛКУ выдается аналогичный представленному на Рис. 1.10 экран Главного меню подсистемы **Настройка**.

Главное меню подсистемы **Настройка** содержит следующие альтернативы для настройки маршрутизатора: **Параметры**, **Интерфейсы**, **Службы**, **Защита**, **Абоненты**, **Разное**, **Выход**.

Экран, содержащий Главное меню подсистемы **Настройка** (Рис. 1.10), имеет ту же структуру, что и экран Главного меню программы управления функционированием маршрутизатора (Рис. 1.9).

Диалог персонала с программой управления при использовании Главного меню управления маршрутизатором и Главного меню подсистемы **Настройка** выполняется по одним и тем же приведенным выше правилам.

Главные меню подсистемы **Настройка** маршрутизаторов (БВМ и БНМ) идентичны, структуры соответствующих меню и набор их альтернатив, в основном, совпадают. Имеющиеся различия отмечены в тексте настоящего РНУ.

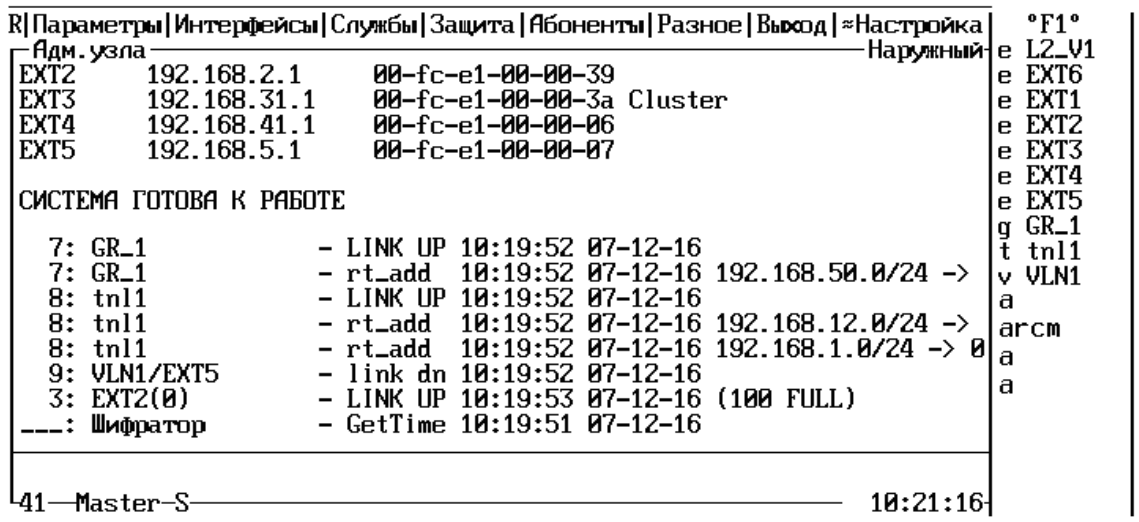


Рис. 1.10 Главное меню подсистемы **Настройка**

Примечание. Процедуру настройки значений параметров конфигуратора изделия следует выполнять только после подключения технических средств ЛКУ к БНМ изделия.

Подключив средства ЛКУ к БВМ изделия, можно изменить значения отдельных параметров в **БпВ**, но обновленные значения параметров будут утеряны после выключения электропитания изделия или перезагрузки ОПО внутреннего маршрутизатора.

2. Организация работы изделия с сетями передачи данных

2.1. Общие сведения об интерфейсах

Каждое из изделий нового поколения обеспечивает функционирование двух полнофункциональных IP-маршрутизаторов, обеспечивающих защищенный сетевой обмен IP-датаграммами между изделиями на *сетевом* уровне – L3-уровне – эталонной модели взаимодействия открытых систем (Open System Interconnection) – модели OSI. Один из маршрутизаторов функционирует в составе БНМ, взаимодействуя с транспортными сетями общего пользования, другой – в составе БВМ, взаимодействуя с защищаемыми внутренними сетями Пользователя.

Кроме того, в составе изделий этого исполнения могут быть созданы сетевые L2-интерфейсы, с помощью которых организуется функционирование прозрачных инкапсулирующих *криптомостов* (*encapsulating bridge*), обеспечивающих защищенный обмен между локальными и удаленными сегментами ЛВС Пользователя.

Таким образом, в отличие от изделий, исполненных в односегментной архитектуре технологии DioNIS®, функционал изделий нового поколения расширен и для организации защищенного сетевого обмена данными в составе ЗСПД изделия нового поколения по усмотрению Администрации ЗСПД могут быть применены как в качестве *криптомаршрутизаторов*, так и в качестве средства организации *криптомостов*. Можно обеспечить сочетание этих функций на разных сетевых интерфейсах изделия – обработка трафиков одними сетевыми интерфейсами изделия выполняется путем *маршрутизации* (на L3-уровне), а обработка трафиков другими сетевыми интерфейсами – путем организации `bridgee`-*соединений* (на L2-уровне).

Сетевое взаимодействие изделий осуществляется через *сетевые интерфейсы* – программно-аппаратные или программные (виртуальные) компоненты, предназначенные для передачи данных между изделиями по каналам связи через сети передачи данных.

Сетевые интерфейсы изделия являются одними из основных объектов настройки изделия. Поэтому важным этапом подготовки изделия к функционированию в составе ЗСПД является этап *создания*, *настройки* и *комплексной проверки* функционирования сетевых интерфейсов изделия.

Сетевые интерфейсы изделия подразделяются на *физические* и *виртуальные*.

Общее количество физических и виртуальных интерфейсов изделия не может превышать числа 2048.

Физический интерфейс является *программно-аппаратным* компонентом изделия, обеспечивающим физическое подключение изделия к той или иной сетевой среде передачи данных через порт сетевого Ethernet-адаптера, а также обеспечивающим управление обменом данными через эту среду.

В изделиях могут применяться *многопортовые* Ethernet-адаптеры, конструкция которых предусматривает наличие в адаптере более одного порта (подробнее см. раздел ***Приложение Ж***, с. 253). Сведения о конкретном оснащении изделия Ethernet-адаптерами содержатся в эксплуатационной документации (далее – ЭД) на конкретное изделие.

Программа управления изделиями поддерживает функционирование физических интерфейсов следующих двух типов (см. раздел 2.2, с. 21):

- физические интерфейсы типа **`Ethernet`**;
- физические интерфейсы типа **`L2-Eth`**.

> *Примечание.* Тип функционирования физического интерфейса (**`Ethernet`** или **`L2-Eth`**) определяется программой управления на основе параметров его конфигурирования и *не зависит* от конструктивных особенностей Ethernet-адаптера. Изделием может поддерживаться *любая* комбинация типов физических интерфейсов, ограничиваемая только общим числом портов Ethernet-адаптеров, которыми оснащено изделие.

Физический интерфейс типа **`Ethernet`** (или Ethernet-интерфейс) предназначен для обработки маршрутизаторами изделия трафика *IP-датаграмм* на L3-уровне. Программой управления поддерживается функционирование Ethernet-интерфейсов как в составе БВМ, так и в составе БНМ изделия.

Ethernet-интерфейсы выполняют следующие функции:

- физическое взаимодействие изделия с каналом связи, включая контроль формата принятых Ethernet-кадров и качества их передачи по каналу связи; прием на дальнейшую обработку Ethernet-кадров, транспортирующих *только* IP-датаграмму или ARP-запрос;
- упаковка исходящих IP-датаграмм в передаваемые по каналу связи Ethernet-кадры и извлечение IP-датаграмм из принимаемых по каналу связи Ethernet-кадров (отработка протокола инкапсуляции IP-датаграмм, выполняемая с учетом особенностей алгоритма преобразования, отмеченных в
- разделе ***Приложение В***, с. 230);

- передача всех принятых IP-датаграмм на обработку в IP-маршрутизатор, которому принадлежит Ethernet-интерфейс, и прием IP-датаграмм от IP-маршрутизатора для передачи их в канал связи.

Физический интерфейс типа **`L2-Eth`** (или L2–Eth-интерфейс) предназначен для обработки изделием трафика *Ethernet-кадров* на L2-уровне для обеспечения функционирования *криптомостов*, образуемых с применением изделий. Программой управления поддерживается функционирование L2–Eth-интерфейсов только в составе БВМ изделия.

L2–Eth-интерфейсы выполняют следующие функции:

- физическое взаимодействие изделия с каналом связи, включая контроль формата принятых Ethernet-кадров и качества их передачи по каналу связи; прием на дальнейшую обработку Ethernet-кадров, транспортирующих данные *любого* типа;
- прием из ЛВС Пользователя, к которой он подключен, *всех* полученных Ethernet-кадров и передача их (без какого-либо преобразования, минуя маршрутизацию в БВМ) на дальнейшую обработку в соответствующий *криптомост* через криптотуннель L2-уровня (подробнее см. раздел 2.4.5, с. 49);
- передача в ЛВС Пользователя (без какого-либо преобразования) всех Ethernet-кадров, принятых по соответствующему криптомосту через криптотуннель L2-уровня.

Физический интерфейс того или иного типа – **`Ethernet`** или **`L2-Eth`** – должен быть создан и настроен для каждого из тех портов сетевых Ethernet-адаптеров, которые будут использованы администратором для подключения изделия к каналам связи с требуемыми сетями (подробнее см. раздел 2.3, с. 25).

Виртуальный интерфейс является *программно* организованным (логическим) компонентом изделия, обеспечивающим тот или иной вид *дополнительной* обработки трафика, циркулирующего через базовые физические интерфейсы типа **`Ethernet`** или **`L2-Eth`**.

Виртуальные (или логические) интерфейсы не имеют собственной аппаратуры для взаимодействия с каналами связи, они используют аппаратуру одного из физических (реальных) интерфейсов изделия, подключаемых к каналам связи. Поэтому каждый виртуальный интерфейс изделия явно (при создании и настройке) или опосредованно (например, через взаимосвязь, фиксируемую организацией маршрутной таблицы маршрутизаторов) приписан к конкретному физическому – *базовому* − интерфейсу.

В соответствии с двумя типами физических интерфейсов, каждый из которых имеет свое назначение и логику работы, изделие поддерживает *две* группы виртуальных интерфейсов, каждая из которых предназначена для взаимодействия с физическим интерфейсом одного из двух типов.

К виртуальным интерфейсам, связанным с логикой обработки трафика физическими **`Ethernet`**-интерфейсами, относятся:

- VLAN-интерфейсы – поддерживаются изделием для организации обработки тегированного согласно стандарту IEEE 802.1Q трафика VLAN-сетей;
- TNL-интерфейсы – поддерживаются изделием для организации туннелированной (согласно спецификациям IPSec) криптообработки циркулирующего между удаленными изделиями на L3-уровне трафика IP-датаграмм с целью его криптографической защиты при передаче через сети общего пользования;
- GRE-интерфейсы – поддерживаются изделием для организации туннелированной согласно GRE-протоколу обработки трафика различных сетевых протоколов между удаленными изделиями.

К виртуальным интерфейсам, связанным с логикой обработки трафика физическими **`L2-Eth`**-интерфейсами, относятся:

- L2–VLAN-интерфейсы – поддерживаются изделием для организации обработки тегированного согласно стандарту IEEE 802.1Q трафика VLAN-сетей;
- L2–TNL-интерфейсы – поддерживаются изделием для организации туннелированной (согласно спецификациям IPSec) криптообработки циркулирующего на L2-уровне сетевого трафика Ethernet-кадров между удаленными изделиями с целью его криптографической защиты при передаче через сети общего пользования.

Ниже представлен полный набор поддерживаемых изделиями сетевых интерфейсов.

Уровень модели OSI	Класс интерфейса	Тип интерфейса	Реализация работы интерфейса	Примечание
L3	Физический	Ethernet	Программно-аппаратная	Монополизирует управление портом Ethernet-адаптера
	Виртуальный	TNL	Программная	
		VLAN		
		GRE		

L2	Физический	L2-Eth	Программно-аппаратная	Монополизирует управление портом Ethernet-адаптера
	Виртуальный	L2-TNL	Программная	
		L2-VLAN		

Внутренний (служебный) интерфейс. Кроме сетевых физических и виртуальных интерфейсов, каждым из IP-маршрутизаторов изделия поддерживается виртуальный *внутренний* (служебный) интерфейс, который обеспечивает обмен данными на L4-уровне модели OSI между программными приложениями (*службами* или *сервисами*) локального изделия и программными приложениями удаленных изделий.

Внутренние интерфейсы маршрутизаторов создаются при запуске изделия (или при перезапуске ОПО маршрутизатора) автоматически и не требуют настройки.

Входящий поток внутреннего интерфейса составляют отдельные данные, принимаемые по физическим интерфейсам из каналов связи и передаваемые для обработки IP-маршрутизатору.

Исходящий поток внутреннего интерфейса – это данные, передаваемые программными приложениями, службами и сервисами изделия IP-маршрутизатору или коммутатору для передачи этих данных в конечном итоге в каналы связи через соответствующие физические интерфейсы.

В рамках виртуального служебного интерфейса на каждом из блоков маршрутизации функционируют TCP-порты, предназначенные для обеспечения работы механизмов удаленного управления БНМ или БВМ с использованием протокола DCP. Эти порты служат для мониторинга состояния сеансов управления; кроме того, они обеспечивают функцию сброса соединений. Число TCP-портов в базовой конфигурации ОПО изделия на каждом из служебных интерфейсов равно *4*.

TCP-порты создаются при запуске изделия автоматически и не требуют действий администратора для их настройки.

2.2. Конфигурирование сетевых интерфейсов

Процесс создания и настройки сетевых интерфейсов рекомендуется выполнять в следующем порядке.

1. Создать и настроить связанный с конкретным *портом* сетевого Ethernet-адаптера изделия *физический* интерфейс требуемого типа (**`Ethernet`** или **`L2-Eth`**) как основу (базис) для организации обмена изделия с сетью на соответствующем (L2 или L3) уровне.
2. Проверить работоспособность физического интерфейса, для чего:
   - выполнить проверку функционирования интерфейса с помощью процедуры PING, запустив ее с помощью цепочки альтернатив ГМ: **Консоль ⇨ Тестирование ⇨ Ping** (раздел 8.1.1, с. 178);
   - выполнить (при необходимости) проверку настроек интерфейса или маршрутных таблиц, включив трассировку интерфейса с помощью следующей цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Трассировка** (см. раздел 4.1.3, с. 131);
   - получить (при необходимости) информацию о состоянии соединения, скорости обработки трафика, об ошибках на Ethernet-адаптере, а также получить дополнительную диагностическую информацию с помощью цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ Активные** (раздел 9.2.2, с. 189), или выбрав альтернативу ГМ: **Интерфейсы** (раздел 2.6, с. 52).
3. В дальнейшем к основной функции физического интерфейса могут быть добавлены дополнительные виды обработки проходящего через интерфейс трафика:
   - для Ethernet-интерфейсов эти виды обработки могут быть обеспечены:
     - VLAN-интерфейсами – для организации обработки тегированного трафика VLAN-сетей физическим Ethernet-интерфейсом изделия (подробнее см. раздел 2.4.1, с. 36);
     - TNL-интерфейсами – для организации туннелированной криптографической обработки трафика IP-датаграмм на сетевом (L3) уровне (подробнее см. разделы 3.1, с. 73 и 2.4.2, с. 39);
     - GRE-интерфейсами – для организации туннелированной согласно GRE-протоколу обработки трафика различных сетевых протоколов между удаленными изделиями (подробнее см. раздел 2.4.3, с. 43);
     - средствами статических криптотуннелей – для организации туннелированной криптографической обработки сетевого трафика на L3-уровне (подробнее см. раздел 3.1.1.2, с. 78);
     - средствами фильтрации трафика, проходящего через интерфейсы (подробнее см. раздел 3.2, с. 89);

- средствами NAT/PAT-обработки трафиков, проходящих через интерфейсы – для сокрытия структуры внутренних сетей Пользователя, а также в целях преодоления дефицита *реальных* глобальных IP-адресов (подробнее см. раздел 3.3, с. 111);
- прочими средствами изделия.

- для L2–Eth-интерфейсов эти виды обработки могут быть обеспечены:
  - L2–VLAN-интерфейсами – для организации обработки тегированного трафика VLAN-сетей физическим L2–Eth-интерфейсом изделия (подробнее см. раздел 2.4.4, с. 46);
  - L2–TNL-интерфейсами – для организации туннелированной криптообработки трафика Ethernet-кадров на канальном (L2) уровне (подробнее см. разделы 3.1, с. 73 и 2.4.5, с. 49).

4. Выполнить поэтапную настройку необходимых *дополнительных* средств обработки трафика с применением механизмов статических криптографических туннелей, средств виртуальных интерфейсов изделия различного типа (VLAN, TNL, GRE, L2–VLAN, L2–TNL), средств фильтрации, NAT-обработки трафика и пр., проверяя работоспособность настраиваемого тракта передачи данных в целом после очередного этапа настройки дополнительного средства обработки трафика (см. раздел 3, с. 71).

Создание и настройка сетевого интерфейса предполагает выполнение следующих действий:

- подключение средств ЛКУ к БНМ изделия и перевод наружного маршрутизатора в привилегированный режим **`Администратор узла`** (см. раздел 8.4, с. 183);
- перевод изделия из режима *управления* в режим *настройки*: выбор альтернативы ГМ **Настройка**;
- выбор цепочки альтернатив ГМ: **Настройка ⇨ Интерфейсы** (см. ниже комментарии к Рис. 2.1);
- выполнение собственно операций по созданию и настройке описателей сетевых интерфейсов изделия (см. разделы 2.3, с. 25; 2.4, с. 36 и 2.5, с. 50);
- перевод изделия из режима *настройки* в режим *управления*, сопровождаемый выдачей подтверждения разрешения на запись (и записью) обновленного конфигуратора изделия в объединенную базу параметров **`БпО`** изделия; команда подтверждения разрешения на запись выполняется с помощью средств управления работой БКО изделия (см. РЭ на конкретное изделие).

В ответ на выбор цепочки альтернатив ГМ: **Настройка ⇨ Интерфейсы** программа управления выдаст на видеомонитор ЛКУ экран создания и настройки сетевых интерфейсов изделия, аналогичный представленному на Рис. 2.1.

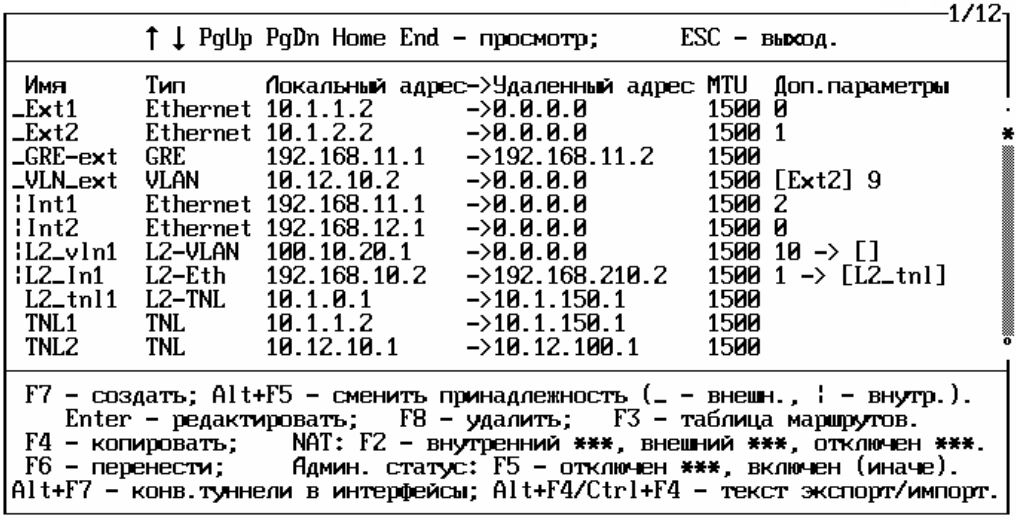


Рис. 2.1. Экран создания и настройки сетевых интерфейсов изделия

Примечание. В изделии используется один и тот же формат выдачи на экран информации, представляющей собой список описателей тех или иных объектов (интерфейсов, маршрутных записей, записей графика замены КД и пр.). При этом в верхней строке экрана содержится информация о средствах навигации по списку, представленному в средней части экрана. Средняя часть экрана содержит собственно список, каждый описатель объекта представлен в списке одной строкой. В нижней части экрана размещена справочная информация об управляющих действиях, которые может выполнить администратор с помощью данного экрана.

Средняя часть экрана на Рис. 2.1 содержит список всех ранее созданных описателей сетевых интерфейсов изделия.

Примечание. Конфигуратор поставляемых заказчику изделий (т.н. конфигуратор *заводских* настроек) включает описатели сетевых интерфейсов изделия типа **`Ethernet`** для каждого *порта* всех сетевых Ethernet-адаптеров, которыми оснащено изделие (подробнее см. раздел 4.1.8, с. 143).

Описание каждого интерфейса занимает в списке одну строку. В первой позиции строки размещается символ, определяющий принадлежность интерфейса блоку маршрутизации: символ <_> обозначает принадлежность интерфейса БНМ, символ <|> – принадлежность интерфейса БВМ, а символ <пробел> – принадлежность интерфейса (например, TNL-интерфейса) изделию в целом.

В правую часть верхней линии рамки экрана выдается номер строки описателя, на которую установлен курсор, а через косую черту от него – количество созданных описателей сетевых интерфейсов.

F7 – создать (Рис. 2.1). Клавиша <F7> служит для создания нового описателя интерфейса. После ее нажатия на экран выводится меню выбора типа и принадлежности создаваемого интерфейса (Рис. 2.2). Меню содержит альтернативы: **Ethernet**, **VLAN**, **GRE**, **TNL**, **L2–Eth**, **L2–TNL**, **L2–VLAN**, соответствующие всему набору типов поддерживаемых изделием физических и виртуальных сетевых интерфейсов. С вызова этого меню начинается создание и настройка любого сетевого интерфейса.

Для выбора *типа* создаваемого интерфейса следует перевести курсор на соответствующую строку и последовательно нажимать клавишу <Enter> для определения принадлежности создаваемого интерфейса. При этом в меню (Рис. 2.2) справа от выбранного типа интерфейса будут появляться слова: **наружный**, **внутренний** или **общий**, информирующие о принадлежности создаваемого интерфейса конкретному маршрутизатору или изделию в целом.

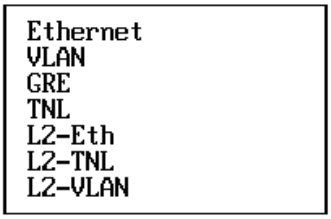


Рис. 2.2. Меню выбора типа и принадлежности создаваемого сетевого интерфейса

Выбрав тип и принадлежность создаваемого сетевого интерфейса, следует нажать клавишу <Esc> – в ответ на экран будет выдан соответствующий выбранному типу *бланк создания и настройки интерфейса*; форматы бланков различны для интерфейсов разного типа (см. разделы 2.3.1, с. 25; 2.3.2, с. 33; 2.4.1, с. 36 – 2.4.5, с. 49).

Примечания.

1. Если принадлежность создаваемого интерфейса не будет определена (в поле справа от выбранного типа интерфейса останется пробел), то после нажатия клавиши <Esc> процесс создания интерфейса будет прекращен, на видеомониторе ЛКУ снова появится экран со списком описателей ранее сконфигурированных интерфейсов (Рис. 2.1), позволяющий продолжить процесс создания и настройки интерфейсов.
2. Все создаваемые сетевые интерфейсы изделия должны иметь *уникальные* имена – уникальность имен контролирует программа управления.
3. По окончании процедуры создания и настройки (или редактирования) описателей сетевых интерфейсов (после того как в **БпО** изделия будет изменен хотя бы один из параметров сетевого интерфейса) программа управления автоматически выполнит рестарт работы всех интерфейсов изделия *обоих* маршрутизаторов, после чего обновленные параметры интерфейсов вступят в силу.

Alt+F5 – сменить принадлежность (Рис. 2.1). Нажатие комбинации клавиш <Alt+F5> позволяет изменить принадлежность того интерфейса, на строку описания которого установлен курсор. При изменении принадлежности изменяется символ в первой слева позиции строки описания интерфейса на Рис. 2.1: символ <_> – у интерфейсов БНМ, символ <|> – у интерфейсов БВМ, пробел – у TNL-интерфейсов и L2–TNL-интерфейсов.

Enter – редактировать (Рис. 2.1). Чтобы изменить параметры конфигурации ранее созданного описателя интерфейса, следует в списке (Рис. 2.1) перевести курсор на строку с описателем, подлежащим редактированию, и нажать клавишу <Enter>; в ответ на экран будет выдан *бланк создания и настройки интерфейса* с подлежащими редактированию ранее введенными параметрами.

F8 – удалить (Рис. 2.1). При нажатии клавиши <F8> после дополнительного запроса и подтверждения из списка будет удалена строка с описанием интерфейса, на которую был установлен курсор.

F3 – таблица маршрутов (Рис. 2.1). После нажатия клавиши <F3> на экран будет выдана *сводная* таблица маршрутов изделия. Эта таблица представляет собой совокупность маршрутных таблиц, настроенных при конфигурировании каждого из интерфейсов БНМ и БВМ (общая информация о маршрутизации в технологии DioNIS® приведена в разделе ***Приложение А***, с. 214).

F4 – копировать (Рис. 2.1). После нажатия клавиши <F4> будет создан интерфейс, параметры которого являются копией того интерфейса, на описании которого установлен курсор; функция облегчает труд

администратора при создании и настройке описателей новых интерфейсов, имеющих лишь небольшие отличия от уже созданных.

NAT: F2 (Рис. 2.1). Нажатие клавиши <F2> позволяет управлять статусом сетевого интерфейса с точки зрения NAT-обработки, выполняемой маршрутизатором: является ли интерфейс *внутренним* для NAT-обработчика этого маршрутизатора, является ли интерфейс для него *внешним* или NAT-обработку трафика, циркулирующего через данный интерфейс, маршрутизатор вообще не выполняет. Последовательное нажатие клавиши <F2> изменяет *статус* интерфейса и *цвет* соответствующей строки в списке интерфейсов (Рис. 2.1): *красный* цвет – интерфейс имеет статус внутреннего для NAT-обработчика, *зеленый* – статус внешнего для NAT-обработчика, *черный* – NAT-обработка на данном интерфейсе маршрутизатором не выполняется (подробнее вопросы трансляции адресов при NAT-обработке рассмотрены в разделе 3.3, с. 111).

F6 – перенести (Рис. 2.1). Нажатие клавиши <F6> позволяет изменить позицию интерфейса в списке описателей (позиция интерфейса в списке имеет значение, так как при запуске (перезапуске) изделия статические физические интерфейсы (каковыми являются Ethernet-интерфейсы и L2–Eth-интерфейсы) активизируются по очереди в соответствии с порядком следования интерфейса в списке описателей). После первого нажатия клавиши <F6> указанная курсором строка выделяется *белым* цветом. Далее можно переместить курсор на любую строку и повторно нажать клавишу <F6>. Отмеченный ранее описатель интерфейса будет перемещен под строку, на которой установлен курсор в момент повторного нажатия клавиши <F6>.

> *Замечание.* Между первым и вторым нажатием клавиши <F6> можно пользоваться только клавишами перемещения курсора. Нажатие любых других функциональных клавиш из набора операций, приведенных в нижней части экрана (Рис. 2.1), сбросит отметку подлежащей переносу строки.

Админ. статус: F5 (Рис. 2.1). Нажатие клавиши <F5> позволяет изменить административный статус интерфейса. Интерфейс можно отключить, не удаляя его из списка описателей. Последовательное нажатие клавиши <F5> изменяет статус интерфейса и цвет соответствующей строки в списке описателей интерфейсов: *серый* цвет – интерфейс отключен (заблокирован), *первоначальный* цвет – интерфейс включен (переведен в активное состояние).

Alt+F7 – конв.туннели в интерфейсы (Рис. 2.1). Использование комбинации клавиш <Alt+F7> позволяет выполнить конвертирование описателей *статических криптотуннелей* в описатели *TNL-интерфейсов* с аналогичными параметрами. В качестве исходных данных для конвертирования используется информация, сохраненная ранее в виде файла с системным именем **tnl_tcp.ema** в архиве конфигураций изделия или на съемном FLASH-диске (см. раздел 4.1.8, с. 143).

При нажатии комбинации клавиш <Alt+F7> выдается запрос:

```
Задайте имя файла (F1 - меню) :
```

Рис. 2.3 Запрос на ввод данных о файле

На запрос должно быть введено обязательное имя **tnl_tcp.ema** – системное имя файла, в котором хранится описание ранее настроенных статических криптотуннелей. Имя файла (с указанием пути его размещения на носителе) можно ввести с клавиатуры (после чего нажать клавишу <Enter>) или нажать клавишу <F1> и получить на экране окно, позволяющее просмотреть и найти папки и файлы на любом из доступных дисков.

Если предполагается конвертировать ранее созданные в изделии описатели *статических* криптотуннелей, то предварительно следует занести в архив текущий конфигуратор изделия (см. раздел 4.1.8, с. 143). Папка, содержащая архив конфигураций, имеет системное имя **D:\DIONISWT.CFG**, в ней следует найти папку с сохраненным конфигуратором изделия и в ней найти файл **tnl_tcp.ema**. Далее следует перевести курсор на имя найденного файла и нажать клавишу <Enter>.

Если указанный файл содержит корректное описание статических криптотуннелей, то конвертирование будет успешно выполнено и в дополнение к существующим описателям статических туннелей программа управления создаст описатели TNL-интерфейсов с параметрами, соответствующими описателям статических туннелей, после чего

поместит их в общий список описателей сетевых интерфейсов изделия.

Примечания.

1. Повторное применение операции приведет к повторному добавлению к общему списку описателей интерфейсов изделия конвертированных описателей TNL-интерфейсов.
2. Файл **tnl_tcp.ema** может находиться на съемном носителе, что позволяет перенести (импортировать) в конфигуратор изделия описания статических криптотуннелей, экспортированные на съемный носитель на другом аналогичном изделии. В дальнейшем они могут быть конвертированы в TNL-интерфейсы согласно процедурам, приведенным выше.

Alt+F4/Ctrl+F4 – текст экспорт/импорт (Рис. 2.1). Функция позволяет перенести сведения о параметрах настройки всех интерфейсов из конфигуратора изделия в текстовый файл или из текстового файла – в конфигуратор изделия. После нажатия комбинации клавиш <Alt+F4> (*экспорт* списка описаний интерфейсов на съемный носитель) или комбинации клавиш <Ctrl+F4> (*импорт* списка описаний интерфейсов со съемного носителя в конфигуратор изделия) на видеомонитор ЛКУ будет выдано окно с запросом на ввод *имени* этого текстового файла. Имя можно ввести с клавиатуры или нажать клавишу <F1> и получить на экране окно, позволяющее просмотреть и найти нужные папки и файлы на любом из доступных дисков. После того как будет указано местоположение и/или имя файла, список описаний всех интерфейсов выгрузится из конфигуратора изделия в текстовом формате в этот файл или загрузится из файла в конфигуратор. Текст описаний можно редактировать. Список описателей интерфейсов можно заимствовать с другого аналогичного изделия.

2.3. Создание и настройка физических сетевых интерфейсов

В процессе создания и настройки физических интерфейсов (Ethernet-интерфейсов или L2–Eth-интерфейсов) администратор изделия должен *соотнести* с каждым из создаваемых интерфейсов какой-либо из *портов* Ethernet-адаптера, через который будет организован канал связи БВМ или БНМ изделия с нужной сетью.

Это требование выполняется путем присвоения соответствующего значения параметру **Номер порта** (см. бланки настройки *дополнительных* параметров Ethernet-интерфейса – Рис. 2.9, с. 29 или L2–Eth-интерфейса – Рис. 2.16, с. 34). При этом с одним *портом* Ethernet-адаптера, как правило, может быть связан только *один* физический интерфейс (если речь не идет об использовании механизма *агрегирования* каналов связи – см. раздел 2.3.1, с. 25 и раздел ***Приложение Б***, с. 226).

В разделе ***Приложение Ж*** (с. 253) изложены сведения об особенностях конструкции применяемых в изделиях нового поколения Ethernet-адаптеров, полезные для правильного определения значений параметра **Номер порта** при настройке сетевых интерфейсов для Ethernet-адаптеров *различной конструкции*.

2.3.1. Ethernet-интерфейсы

На каждом обслуживаемом конкретным портом Ethernet-адаптера направлении обмена, где планируется применение изделия в качестве *криптомаршрутизатора* (для обеспечения защищенного обмена *IP-датаграммами* между ЛВС Пользователя на L3-уровне), должен быть создан и настроен сетевой физический интерфейс типа **Ethernet**.

С этой целью в меню на Рис. 2.2 (с. 23) следует выбрать альтернативу **Ethernet**, задать принадлежность создаваемого Ethernet-интерфейса наружному или внутреннему маршрутизатору и нажать клавишу <Esc>. В ответ на видеомонитор ЛКУ будет выдан бланк создания и настройки физического интерфейса типа **Ethernet**, представленный на Рис. 2.4.

Наружный

Имя интерфейса	Таблица маршрутов
Тип Ethernet	Режим активизации Статический
Локальный IP-адрес интерфейса 192.168.2.1	
Удаленный IP-адрес интерфейса 0.0.0.0	
Допустимое время неактивности интерфейса 0	
Максимальный размер IP-датаграмм (MTU) 1500	
Фильтр входящих	Фильтр исходящих
Специальные настройки	Дополнительные параметры

Рис. 2.4 Бланк создания и настройки физического интерфейса типа **Ethernet**

В левом верхнем углу рамки бланка указан маршрутизатор (**Наружный** или **Внутренний**), которому принадлежит создаваемый и настраиваемый интерфейс.

Ниже приведено описание порядка работы с полями бланка.

Имя интерфейса (Рис. 2.4) – имя сетевого физического Ethernet-интерфейса; значением параметра может быть до 7-ми любых символов, идентифицирующих интерфейс. Для ввода значения следует выбрать поле бланка − переместить на него курсор и нажать клавишу <Enter>. В появившееся окно ввода значения следует ввести имя интерфейса и нажать клавишу <Enter>. Все интерфейсы изделия должны иметь *уникальные* имена, уникальность имен интерфейсов контролирует программа управления.

Тип (Рис. 2.4) – параметр имеет значение `Ethernet`. Значение параметра задается автоматически при выборе типа настраиваемого интерфейса, изменить значение нельзя. В бланке приведено для информации.

Режим активизации (Рис. 2.4) – параметр имеет значение *Статический* (изменить значение нельзя). Интерфейсы, имеющие *статический* режим запуска, переводятся в рабочее состояние в момент запуска изделия (или перезапуска ОПО маршрутизатора) и сохраняют его до выключения изделия. Поэтому при изменении хотя бы одного параметра конфигуратора изделия, касающегося работы такого интерфейса, выполняется запись этого изменения в **БпО** изделия и перезапуск работы ОПО с обновленными параметрами (включая работу с сетевыми интерфейсами маршрутизаторов изделия), после чего изменения конфигуратора вступают в силу.

Локальный IP-адрес интерфейса (Рис. 2.4) – это IP-адрес интерфейса соответствующего маршрутизатора изделия в составе той сети, к которой изделие подключено с помощью *порта* Ethernet-адаптера. Этот адрес может совпадать, а может не совпадать с *собственным IP-адресом* соответствующего маршрутизатора изделия (см. разделы 4.1.2, с. 130 и 3.5, с. 127).

При выборе поля **Локальный IP-адрес интерфейса** на экран будет выдан запрос на ввод значения этого параметра (Рис. 2.5).

```
Локальный IP-адрес интерфейса (адрес/бит) :
```

Рис. 2.5 Запрос на ввод локального IP-адреса интерфейса и маски подсети, к которой он подключается

В ответе на запрос программа управления предлагает ввести значение параметра в формате **адрес/бит**. Поэтому, формируя ответ на запрос, администратору следует в предлагаемое поле ввода данных:

- ввести значение *локального IP-адреса интерфейса* в соответствующем формате;
- ввести символ </>;
- ввести целое десятичное число в диапазоне от ***0*** до ***32***, равное *длине маски* подсети, к которой будет подключен настраиваемый интерфейс;
- нажать клавишу <Enter>.

В результате к *маршрутной таблице* изделия *автоматически* будет добавлена новая маршрутная запись с характеристиками подсети, к которой будет подключен настраиваемый Ethernet-интерфейс.

Отметим, что эту маршрутную запись можно сформировать *вручную* (не вводя вслед за значением *локального IP-адреса интерфейса* символа </> и размера *длины маски подсети*) путем использования поля **Таблица маршрутов** (см. далее в подразделе) бланка создания и настройки физического интерфейса типа **Ethernet** (Рис. 2.4).

Примечание. Любой из маршрутизаторов изделия доступен (виден) по IP-сети, к которой подключен его физический интерфейс:

- по *собственному IP-адресу* того маршрутизатора, которому принадлежит физический интерфейс, подключенный к данной IP-сети (см. раздел 4.1.2, с. 130);
- по *локальному IP-адресу* его физического интерфейса, подключенного к данной IP-сети (см. разделы 2.3.1, с. 25 и 2.3.2, с. 33);
- по *локальному IP-адресу* его виртуального интерфейса, использующего физический интерфейс, подключенный к данной IP-сети.

Удаленный IP-адрес интерфейса (Рис. 2.4) – канал связи, организованный с помощью технологии Ethernet, является *многоточечным*, поэтому параметру присваивается значение ***0.0.0.0*** (подробнее см. раздел ***Приложение А***, с. 214).

Примечание. Значение параметра **Удаленный IP-адрес интерфейса**, отличное от значения ***0.0.0.0***, используется при настройке механизма PING-проб, когда необходимо обеспечить оперативный контроль доступности через данный Ethernet-интерфейс сетевого устройства с IP-адресом, указанным в поле **Удаленный IP-адрес интерфейса** бланка настройки (см. раздел 2.7.4, с. 60). Обычно – это IP-адрес ближайшего в сети шлюза.

Допустимое время неактивности интерфейса (Рис. 2.4) – параметр в данной версии ОПО не используется.

Максимальный размер IP-датаграмм (MTU) (Рис. 2.4) – параметр задает максимальный размер IP-датаграмм (Maximum-Transmission-Unit), обрабатываемых данным интерфейсом. Значением параметра может быть число в диапазоне от *28* до *2048* (*рекомендуемое* значение параметра – ***1500***, изменять его следует только в каких-то специальных случаях).

Фильтры входящих, **Фильтры исходящих** (Рис. 2.4) – параметры указывают имена соответствующих фильтров (поименованных списков правил фильтрации), которые будут использованы для фильтрации потоков соответственно входящих или исходящих IP-датаграмм через данный интерфейс.

Примечание. На начальном этапе настройки интерфейса эти параметры бланка рекомендуется не настраивать (оставить поля с именами фильтров пустыми). После того как будут созданы фильтры (подробнее см. раздел 3.2.1.2, с. 92), при необходимости фильтрации потока через данный интерфейс в соответствующее поле бланка следует занести имя фильтра, выбрав его из списка созданных ранее фильтров (подробнее о списке фильтров см. раздел 3.2.1.2, с. 92).

Таблица маршрутов (Рис. 2.4) – выбор поля параметра позволяет сформировать, отредактировать или удалить записи таблицы маршрутизации IP-датаграмм, отправляемых через данный Ethernet-интерфейс.

При выборе этого поля выдается экран настройки маршрутной таблицы, содержащий строки созданных ранее маршрутных записей, аналогичный представленному на Рис. 2.6 (о маршрутных таблицах см. раздел ***Приложение А***, с. 214).

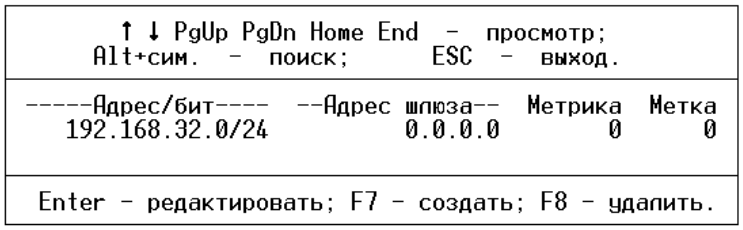


Рис. 2.6 Экран настройки маршрутной таблицы Ethernet-интерфейса

Таблицу маршрутов можно изменить: создать новые записи, отредактировать или удалить имеющиеся.

F7 – **создать** (Рис. 2.6). После нажатия клавиши <F7> на экран выводится бланк создания и настройки маршрутной записи интерфейса (см. Рис. 2.7), позволяющий создать маршрутную запись с параметрами, описание которых приведено ниже.

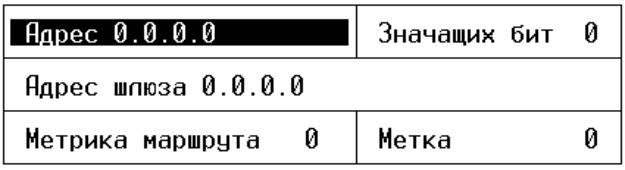


Рис. 2.7 Бланк создания и настройки маршрутной записи интерфейса

Адрес (Рис. 2.7) – определяет IP-адрес подсети, которая доступна через настраиваемый Ethernet-интерфейс.

Значащих бит (Рис. 2.7) – длина *маски* подсети (в битах), десятичное число в диапазоне от ***0*** до ***32*** – определяет, сколько бит IP-адреса используется для определения адреса той подсети, которая доступна через настраиваемый Ethernet-интерфейс.

Примечание. Значение маски *0* используется при составлении т. н. `default`-маршрута (подробнее см. ниже), а значение *32* – при формировании маршрута, обеспечивающего сетевой доступ к *конкретному* IP-устройству через данный интерфейс.

Адрес шлюза (Рис. 2.7) – определяет IP-адрес устройства, называемого *шлюзом*. Шлюзы – это IP-устройства, которые, находясь в подсети, к которой непосредственно подключается настраиваемый физический интерфейс изделия, обеспечивают доступ к устройствам, входящим в состав других IP-подсетей.

Если значение параметра **Адрес шлюза** равно значению по умолчанию – ***0.0.0.0***, то IP-устройства, маршрут доступа к которым определяется такой маршрутной записью, находятся в одной подсети с настраиваемым интерфейсом изделия, в использовании промежуточных шлюзов необходимости нет; в этом случае говорят о *прямой* адресации IP-ресурсов в подсети, а соответствующую маршрутную запись называют *прямым* маршрутом.

Если значение параметра **Адрес шлюза** *отлично* от значения ***0.0.0.0***, то маршрут доступа к подсети, в которой находятся требуемые IP-устройства, пролегает через шлюз, IP-адрес которого содержит маршрутная запись; в этом случае говорят о *косвенной* адресации IP-ресурсов в нужной подсети, а соответствующую маршрутную запись называют *косвенным* маршрутом. Подробнее о прямой и косвенной IP-адресации см. раздел ***Приложение А***, с. 214.

Метрика маршрута (Рис. 2.7) – целое десятичное число в диапазоне от *0* до *255*, задающее *приоритет* маршрута, определяемого данной маршрутной записью (при прочих равных условиях) в операциях маршрутизации (нулевое значение метрики означает *наивысший* приоритет маршрута).

Метка (Рис. 2.7) – целое десятичное число от *0* до *255*, при *равенстве* числовой *метки* маршрутной записи и *метки* конкретной PING-пробы обеспечивается функциональная взаимосвязь, в результате которой *статус* соответствующих маршрутных записей изделия зависит от результатов выполнения соответствующих PING-проб (подробнее см. раздел 2.7, с. 58).

Enter – **редактировать** (Рис. 2.6). После установки курсора на строку с описанием маршрутной записи и нажатия клавиши <Enter> на видеомонитор ЛКУ выводится такой же бланк, как при создании маршрутной записи (Рис. 2.7), но с присвоенными ранее значениями параметров. Администратору предоставляется возможность эти значения отредактировать.

F8 – **удалить** (Рис. 2.6). При нажатии клавиши <F8> после дополнительного запроса и подтверждения удаляется маршрутная запись, на строку с описанием которой был установлен курсор.

В *таблицу маршрутов* настраиваемого интерфейса должна быть внесена, как минимум, одна маршрутная запись – *прямой* маршрут к IP-устройствам, подключенным к локальной подсети, к которой непосредственно подключен данный физический Ethernet-интерфейс. Кроме прямого маршрута (прямых маршрутов) можно задать необходимое количество *косвенных* маршрутов, указывающих маршруты доступа к другим IP-сетям через *шлюзы*, расположенные в прямо адресуемой локальной сети (о *прямой* и *косвенной* адресациях см. раздел ***Приложение А***, с. 214).

Параметры *прямого* маршрута должны иметь следующие значения:

Адрес – адрес подсети, доступной непосредственно (по прямой адресации)

Значащих бит – размер значащей части адреса подсети (в соответствии с длиной маски подсети)

Адрес шлюза – *0.0.0.0*

Параметры *косвенного* маршрута должны иметь следующие значения:

Адрес – адрес подсети, доступной через шлюз

Значащих бит – размер значащей части адреса подсети (в соответствии с длиной маски подсети)

Адрес шлюза – IP-адрес шлюза, расположенного в прямо адресуемой локальной подсети, заданной прямым маршрутом

Вместо указания множества косвенных маршрутов можно использовать специальную маршрутную запись – маршрут по умолчанию (`default`-маршрут). Параметры такой записи имеют следующие значения:

Адрес – *0.0.0.0*

Значащих бит – *0*

Адрес шлюза – IP-адрес шлюза в составе прямо адресуемой локальной сети

Специальные настройки (Рис. 2.4). На начальном этапе создания сетевых интерфейсов (при наладке коммуникационных функций интерфейса) рекомендуется специальным параметрам задать значения так, как показано на бланке управления специальными настройками интерфейса, представленном на Рис. 2.8. Если справа от параметра стоит символ «*» (звездочка), то параметр принимает значение ***Да***, если символ «*» отсутствует, то параметр принимает значение ***Нет***.

Запретить обработку:	Включить:
пакетов DHCP-протокола *	фильтр "только туннели"
пакетов RIP-протокола *	статистику по IP-адресам
Multicast-датаграмм *	режим Proxy ARP
Cluster-пакетов *	LLDP-рассылку
транзитных датаграмм	LLDP-прием
	контроль в кластере

Рис. 2.8 Бланк управления специальными настройками интерфейса

Перед началом штатной эксплуатации сетевого интерфейса всем его специальным параметрам – ограничителям проходящего через интерфейс трафика – следует присвоить значения, требуемые конкретными условиями эксплуатации изделия (подробнее о специальных настройках интерфейсов изделия см. в разделе 2.5, с. 50).

Дополнительные параметры (Рис. 2.4). При выборе альтернативы появляется бланк настройки дополнительных параметров Ethernet-интерфейса. Его начальный вид (см. Рис. 2.9) и описание процедуры настройки параметров Ethernet-интерфейса с его помощью приведены ниже.

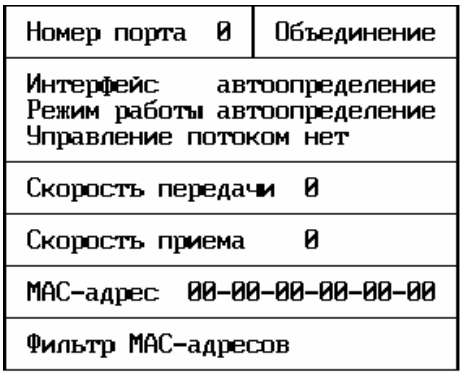


Рис. 2.9 Бланк настройки дополнительных параметров Ethernet-интерфейса

Номер порта (Рис. 2.9) – порядковый номер порта Ethernet-адаптера в соответствующем блоке маршрутизации изделия (БВМ или БНМ), выбранного для интерфейса. Этот параметр может принимать значения в диапазоне от ***0*** до ***255*** для каждого из маршрутизаторов. Должен быть указан *номер порта*, соответствующий приведенной в ЭД на конкретное изделие маркировке портов на моноблоке изделия (маркировке того физического *гнезда* Ethernet-адаптера, к которому подключается оптоволоконный или проводной сетевой кабель и для которого выполняется настройка поддерживаемого маршрутизатором Ethernet-интерфейса).

> *Примечание.* Изделия нового поколения, объединенные общим функциональным назначением, существенно отличаются друг от друга по конструкции, по климатико-механическим и специальным свойствам, по пропускной способности, энергопотреблению и пр. Конструкция и технические характеристики применяемых в составе этих изделий сетевых Ethernet-адаптеров также могут существенно отличаться, поэтому в целях исключения путаницы при определении значения параметра **Номер порта** в разделе ***Приложение Ж*** (с. 253) приведена дополнительная информация об особенностях конструкции применяемых в изделиях Ethernet-адаптеров и о маркировке их разъемов, используемых для подключения изделий к сетям с помощью сетевых кабелей.

Объединение (Рис. 2.9) – при выборе этого поля появляется экран настройки параметров механизма объединения (агрегирования) каналов связи интерфейсов изделия (подробнее о механизме агрегирования каналов см. раздел ***Приложение Б***, с. 226). Пример экрана настройки представлен на Рис. 2.10

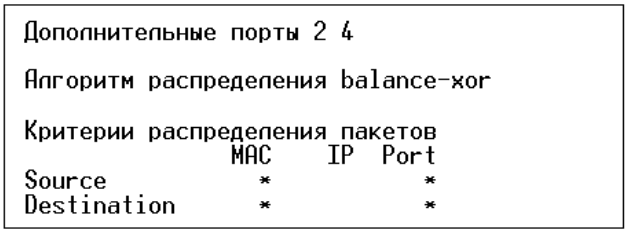


Рис. 2.10 Экран настройки параметров механизма объединения каналов связи интерфейсов

Дополнительные порты (Рис. 2.10) – при выборе этого поля появляется запрос на ввод номеров *дополнительных* портов (каналов связи) маршрутизатора изделия, объединяемых с *основным* портом, значение которого было указано при вводе значения параметра **Номер порта** бланка настройки дополнительных параметров Ethernet-интерфейса (Рис. 2.9). При вводе номеров дополнительных портов (каналов связи) следует через пробел указать номера портов, участвующих в объединении с основным.

> *Примечание.* При вводе дополнительных портов следует иметь в виду, что в случае, когда параметру **Алгоритм распределения** присвоено значение `active-backup` (см. ниже), *последовательность* ввода номеров дополнительных портов определяет очередность их использования в качестве замены вышедшему из строя основному порту.

Алгоритм распределения (Рис. 2.10) – параметр позволяет задать алгоритм распределения нагрузки на объединяемые интерфейсом порты (каналы связи). Параметр может принимать следующие значения: `round-robin`, `balance-xor` или `active-backup`.

Первые два алгоритма служат для повышения пропускной способности тракта передачи данных путем организации параллельной загрузки агрегированных каналов связи интерфейса.

- алгоритм *round-robin* обеспечивает равномерную циклическую загрузку всех имеющихся агрегированных каналов;
- алгоритм *balance-xor* при распределении пакетов между каналами учитывает параметры пакетов и загружает похожие пакеты (с одинаковыми параметрами, содержащимися в заголовке) в один и тот же канал.

Алгоритм *active-backup* используется с целью повышения надежности тракта передачи данных путем резервирования каналов связи.

> Подробное описание работы каждого из трех поддерживаемых изделием алгоритмов распределения трафика по агрегированным портам приведено в разделе ***Приложение Б*** (с. 226).

Для выбора типа алгоритма следует перевести курсор на это поле и нажимать последовательно клавишу <Enter>, при этом в правой части поля появляется очередной *тип алгоритма*. Получив нужный алгоритм, надо нажать клавишу <Esc>.

Критерии распределения пакетов (Рис. 2.10). В таблице под этим заголовком можно задать параметры пакетов, которые будут учитываться при расчете распределения пакетов между объединяемыми портами.

> *Примечание*. Задавать значения в этой таблице следует только в случае, если предыдущему параметру **Алгоритм распределения** установлено значение *balance-xor*.

Чтобы задать то или иное значение параметра, надо перевести курсор на ячейку таблицы и нажать клавишу <Enter> – в соответствующей ячейке появится «звездочка». Строками таблицы являются – **Source** (Отправитель) и **Destination** (Получатель); столбцами – **MAC**, **IP** и **Port**.

Таким образом, в качестве критериев, учитываемых при расчете распределения пакетов между портами, могут быть заданы 6 следующих параметров пакета: *MAC-адреса* отправителя и получателя пакетов (кадров), их *IP-адреса*, а также указанные в пакетах отправителя и получателя значения *портов* (*Port*) обработки передаваемых пакетами данных на 4-м уровне модели OSI.

Выбор значений для настройки двух следующих параметров Ethernet-интерфейса – **Интерфейс** и **Режим работы** (Рис. 2.9) – зависит от конкретных условий сетевой среды окружения, в которую на объекте эксплуатации должно быть встроено изделие.

> *Примечание* – В случае настройки интерфейсов изделия, обеспечивающих обработку трафика на скорости ***10*** *Гбит/с*, следует обоим параметрам – **Интерфейс** и **Режим работы** – присвоить значение **автоопределение**.

Интерфейс (Рис. 2.9) – значение параметра может принимать следующие значения: **автоопределение** / **витая пара** / **оптика** / **SFP** / **SFP100** / **SFP1000**.

Большое число возможных значений параметра обусловлено широким набором *модификаций* сетевых Ethernet-адаптеров, которыми может быть укомплектовано конкретное изделие; программа управления функционированием изделия учитывает все возможные модификации.

> *Примечание*. Сведения об особенностях сетевых Ethernet-адаптеров, которыми укомплектовано настраиваемое изделие, влияющих на выбор значения параметра **Интерфейс**, содержатся в ЭД на конкретное изделие.

Можно дать следующие общие рекомендации по выбору значения параметра **Интерфейс**:

автоопределение – специфику обработки трафика определит сама программа управления; в случае настройки интерфейса, обеспечивающего обработку трафика на скорости 10 Гбит/сек, следует устанавливать *только это* значение;

витая пара – обмен данными будет принудительно организован с помощью кабеля витой пары, подключенного к Ethernet-адаптеру через разъем RJ-45;

оптика – значение выбирается в случае, когда в Ethernet-адаптер изделия встроен трансивер, обеспечивающий обмен с помощью оптоволоконного кабеля в режиме 100FX на скорости 100 Мбит/сек;

SFP – значение выбирается в случае, когда обмен данными будет осуществляться с помощью оптоволоконного кабеля через

SFP-вставку в SFP-модуль адаптера без указания конкретной пропускной способности Ethernet-адаптера – ее значение определит сама программа управления;

SFP100 – значение выбирается в случае, когда обмен данными будет осуществляться с помощью оптоволоконного кабеля через SFP-вставку в SFP-модуль адаптера на скорости до 100 Мбит/сек;

SFP1000 – значение выбирается в случае, когда обмен данными будет осуществляться с помощью оптоволоконного кабеля через SFP-вставку в SFP-модуль адаптера на скорости 1 Гбит/сек.

Режим работы (Рис. 2.9) – параметр может принимать следующие значения: **автоопределение**/ **100Full** / **100Half** / **10Full** / **10Half** / **1000Full**.

Можно дать следующие общие рекомендации по выбору значения параметра **Режим работы**:

автоопределение – режим обмена данными (скорость, дуплексный / полудуплексный) определит сама программа управления; в случае настройки интерфейса, обеспечивающего обработку трафика на скорости 10 Гбит/сек, следует устанавливать *только это* значение;

100Full – будет принудительно установлен дуплексный режим обмена данными на скорости 100 Мбит/сек;

100Half – будет принудительно установлен полудуплексный режим обмена данными на скорости 100 Мбит/сек;

10Full – будет принудительно установлен дуплексный режим обмена данными на скорости 10 Мбит/сек;

10Half – будет принудительно установлен полудуплексный режим обмена данными на скорости 10 Мбит/сек;

1000Full – будет принудительно установлен дуплексный режим обмена данными на скорости 1 Гбит/сек.

Управление потоком (Рис. 2.9) – параметр может принимать значения: **нет** или **ДА**. Параметр обеспечивает включение (значение **ДА**) или выключение (значение **нет**) механизма *управления потоком* при выполнении интерфейсом обмена Ethernet-кадрами с устройствами сети. Подробнее о механизме управления потоком см. раздел ***Приложение В*** (с. 230).

Выбор конкретных значений для настройки двух следующих параметров Ethernet-интерфейса – **Скорость передачи** и **Скорость приема** – зависит от задачи, которую должен решить администратор изделия совместно с Администрацией ЗСПД, обеспечивая с помощью механизма *приоритизации* трафика приемлемый (в условиях ограниченной пропускной способности отдельных трактов передачи данных ЗСПД) режим обработки потоков данных различного характера, циркулирующих между приложениями Пользователя (подробнее о поддерживаемом изделием механизме приоритизации трафика и качестве обслуживания QoS см. раздел ***Приложение Г***, с. 238).

> *Примечание*. Алгоритм обработки трафика, *передаваемого* в сеть интерфейсами изделия, предусматривающими при их настройке возможность установки значений параметров **Скорость передачи** и **Скорость приема** (это интерфейсы типа **Ethernet**, **VLAN**, **TNL**, **L2-Eth**, **L2-TNL**, **L2-VLAN**), *отличается* от алгоритма обработки трафика, *принимаемого* этими интерфейсами. Для правильной настройки значений указанных параметров следует учитывать разницу в логике работы этих алгоритмов (подробнее см. раздел ***Приложение Г***, с. 238.

Скорость передачи (Рис. 2.9). При выборе поля на видеомонитор ЛКУ выводится аналогичный представленному на Рис. 2.11 бланк настройки режима работы механизма *приоритизации* трафика, обеспечиваемого интерфейсом.

Рис. 2.11 Бланк настройки режима работы механизма приоритизации, обеспечиваемого интерфейсом

В верхней строке экрана (Рис. 2.11) − параметр **Скорость передачи**, позволяющий установить максимальное значение скорости передачи в сеть исходящего через интерфейс трафика Ethernet-кадров; при выборе этой альтернативы на видеомонитор ЛКУ выдается запрос:

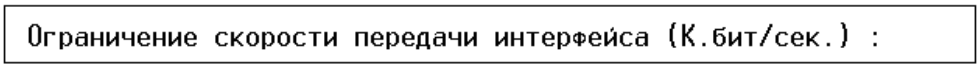


Рис. 2.12 Запрос на ограничение максимальной скорости передаваемых интерфейсом данных

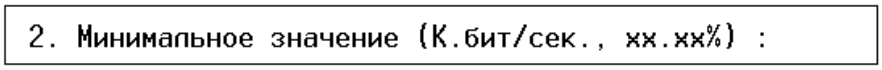
В качестве значения параметра задается *общая* пропускная способность канала передачи данных, обеспечиваемая настраиваемым интерфейсом (единица измерения – **Кбит/сек**). При выборе значения параметра **Скорость передачи** следует руководствоваться сведениями о поддерживаемом изделием механизме приоритизации трафика и качестве обслуживания QoS, изложенными в разделе ***Приложение Г***, с. 238.

Если установлено *нулевое* значение параметра, скорость трафика, передаваемого интерфейсом в сеть, не ограничивается, запуск механизма приоритизации передаваемого интерфейсом трафика не производится, исходящие пакеты отправляются интерфейсом в сеть в порядке их поступления.

Если установлено *отличное от нуля* значение параметра, запускается механизм обработки интерфейсом *исходящего* трафика с учетом *приоритета* передаваемых в сеть IP-датаграмм (с учетом значения подполя IPP поля ToS в заголовке IP-датаграммы) – механизм *приоритизации* передаваемого трафика.

Остальная часть экрана (Рис. 2.11) содержит таблицу: в первом столбце под заголовком **Прт** − семь возможных приоритетов передаваемых в сеть IP-датаграмм; во втором и третьем столбцах (под заголовками **Минимум** и **Максимум** могут быть заданы интервалы скоростей обработки интерфейсом *исходящего* трафика с учетом *приоритета* передаваемых в сеть IP-датаграмм.

Чтобы задать значение, надо перевести курсор на соответствующее место в таблице и нажать клавишу <Enter>. Появится запрос:



Требуемое значение можно задать в Кбит/сек или в процентах от значения параметра **Скорость передачи**

Скорость приема (Рис. 2.9). Параметр позволяет установить пороговое значение максимальной скорости *приема* из сети входящего через интерфейс трафика Ethernet-кадров (единица измерения – **Кбит/сек**). Если установлено *отличное от нуля* значение параметра, запускается механизм обработки интерфейсом *входящего* трафика с учетом *приоритета* принимаемых из сети IP-датаграмм – механизм *приоритизации* принимаемого трафика.

Если установлено *нулевое* значение параметра, скорость трафика, принимаемого интерфейсом из сети, не ограничивается, запуск механизма приоритизации входящего трафика не производится, входящие пакеты, принимаемые интерфейсом из сети, обрабатываются в порядке их поступления.

MAC-адрес (Рис. 2.9) – физический канальный адрес (на L2-уровне) порта (*гнезда*) Ethernet-адаптера, с помощью которого интерфейс изделия подключается к каналу связи и соответствующего ранее введенному при настройке интерфейса значению параметра **Номер порта** (Рис. 2.9).

При выборе поля **MAC-адрес** (Рис. 2.9) будет выдан запрос на ввод значения MAC-адреса, представленный на Рис. 2.13. Можно ввести любое значение параметра, соблюдая предложенный в запросе формат ввода.

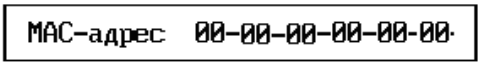


Рис. 2.13 Запрос на ввод MAC-адреса порта (гнезда) Ethernet-адаптера

Если указать (оставить) *нулевое* значение параметра, то программа управления считает заводской MAC-адрес порта (гнезда) Ethernet-адаптера, заданный при его изготовлении, и установит его в качестве значения параметра.

Если присвоить параметру *не нулевое* значение, то это значение и будет использовано в качестве значения MAC-адреса порта (гнезда) настраиваемого Ethernet-интерфейса.

Вместо ввода MAC-адреса можно нажать клавишу <F1>, после этого программой управления будет считан заводской адрес порта (гнезда) Ethernet-адаптера, и считанное значение MAC-адреса в предложенном формате будет выдано на видеомонитор ЛКУ в поле запроса (Рис. 2.14).

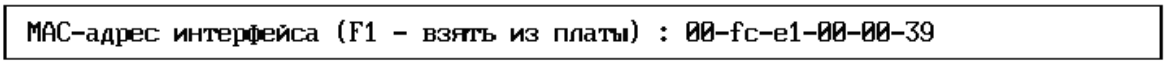


Рис. 2.14 Запрос на ввод MAC-адреса порта (гнезда) Ethernet-адаптера (после нажатия клавиши <F1>)

Введенное тем или иным способом в поле запроса значение MAC-адреса после нажатия клавиши <Enter> будет занесено в поле **MAC-адрес** бланка настройки дополнительных параметров Ethernet-интерфейса (Рис. 2.9).

> *Примечание.* При подготовке функционирования изделия в составе *кластера* следует соблюдать определенные требования по настройке MAC-адресов интерфейсов изделий, участвующих в работе кластера (подробнее см. раздел 7, с. 174).

Фильтр MAC-адресов (Рис. 2.9) – имя таблицы MAC-адресов, выбранное администратором для данного Ethernet-интерфейса из ранее созданного списка таблиц MAC-адресов. Таблица MAC-адресов содержит список MAC-адресов сетевых устройств, обмен с которыми через настраиваемый Ethernet-интерфейс будет *разрешен* (подробнее о фильтрации принимаемого из сети трафика по значению MAC-адреса его источника см. раздел 3.2.2, с. 109).

> *Примечание.* На начальном этапе настройки интерфейса параметр **Фильтр MAC-адресов** рекомендуется не настраивать (оставить поле пустым).

2.3.2. *L2–Eth-интерфейсы*

Если на *направлении* обмена, обслуживаемом конкретным портом (гнездом) Ethernet-адаптера, планируется применение изделия в качестве средства организации *криптомостов* с целью обеспечения обмена *Ethernet-кадрами* на L2-уровне по защищенным `bridge`-соединениям между локальным и удаленными сегментами защищаемых ЛВС Пользователя (подробнее см. раздел ***Приложение В***, с. 230), то для обеспечения работы по этому направлению должен быть создан и настроен связанный с этим портом (гнездом) Ethernet-адаптера сетевой физический интерфейс типа **L2-Eth**.

> *Примечание.* Логика работы интерфейсов типа **L2-Eth** ориентирована на обработку потока Ethernet-кадров на L2-уровне модели OSI и принадлежать они могут только БВМ изделия (подробнее см. раздел ***Приложение В***, с. 230).

Чтобы создать L2–Eth-интерфейс, следует в меню выбора типа и принадлежности создаваемого интерфейса (см. Рис. 2.2, с. 23) выбрать альтернативу **L2-Eth**, установить принадлежность создаваемого L2–Eth-интерфейса внутреннему маршрутизатору и нажать клавишу <Esc>. В ответ на видеомонитор ЛКУ будет выдан бланк создания и настройки физического интерфейса типа **L2-Eth**, аналогичный представленному на Рис. 2.15.

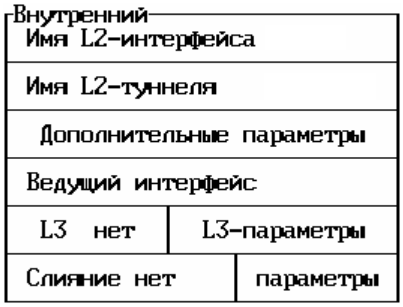


Рис. 2.15 Бланк создания и настройки физического интерфейса типа L2-Eth

В левом верхнем углу рамки бланка указан маршрутизатор изделия – **Внутренний**.

Имя L2-интерфейса (Рис. 2.15) – имя, идентифицирующее сетевой физический L2–Eth-интерфейс; заданное имя может содержать до 7-ми символов и должно быть уникальным.

Имя L2-туннеля (Рис. 2.15) – имя сетевого виртуального интерфейса типа **L2-TNL** – логического туннельного интерфейса L2-уровня (подробнее см. раздел ***Приложение В***, с. 230); значением параметра должно быть имя L2-TNL-интерфейса, задаваемое при его настройке (см. раздел 2.4.5, с. 49).

Дополнительные параметры (Рис. 2.15) – при выборе альтернативы появляется бланк настройки дополнительных параметров L2–Eth-интерфейса, аналогичный представленному на Рис. 2.16.

Номер порта 0	Объединение
Интерфейс автоопределение Режим работы автоопределение Управление потоком нет	
Скорость передачи 0	
Скорость приема 0	
MAC-адрес 00-00-00-00-00-00	
Фильтр MAC-адресов	

Рис. 2.16 Бланк настройки дополнительных параметров физического L2–Eth-интерфейса

Набор *дополнительных* параметров L2–Eth-интерфейса, представленный на Рис. 2.16, полностью соответствует набору дополнительных параметров Ethernet-интерфейса, представленному на Рис. 2.9.

Настройка дополнительных параметров L2–Eth-интерфейса: **Номер порта**, **Объединение**, **Интерфейс**, **Режим работы**, **Управление потоком**, **MAC-адрес** и **Фильтр MAC-адресов** (Рис. 2.16) − полностью совпадает с настройкой этих параметров Ethernet-интерфейса (Рис. 2.9), подробно описанной выше в разделе 2.3.1, с. 25.

Скорость передачи (Рис. 2.16) − обработка значения параметра L2–Eth-интерфейса настоящей версией ОПО изделия не поддерживается.

Скорость приема (Рис. 2.16) − параметр позволяет установить *пороговое* значение максимальной скорости приема из сети входящего через L2–Eth-интерфейс трафика Ethernet-кадров (единица измерения – **Кбит/сек**). При достижении скорости входящего трафика порогового значения программа управления прекращает обработку Ethernet-кадров, поступивших из сети в Ethernet-адаптер интерфейса.

Если при этом механизм управления потоком на L2–Eth-интерфейсе включен (параметру **Управление потоком** (см. Рис. 2.16) присвоено значение *ДА*), выполняется регулирование интенсивности потока Ethernet-кадров, генерируемого передающей стороной. Следствием снижения интенсивности принимаемого потока является отсутствие потерь входящих на L2–Eth-интерфейс Ethernet-кадров.

> Если механизм управления потоком на L2–Eth-интерфейсе выключен (параметру **Управление потоком** присвоено значение *нет*), достижение порогового значения скорости приема равносильно сбросу поступающих из сети Ethernet-кадров. Подробнее о механизме управления потоком см. раздел ***Приложение В*** (с. 230).

Ведущий интерфейс (Рис. 2.15) – параметр определяет имя *ведущего* интерфейса (из числа сетевых интерфейсов изделия, принадлежащих БВМ или БНМ) для настраиваемого L2–Eth-интерфейса (подробнее о *ведущем* интерфейсе при настройке L2-интерфейсов см. раздел ***Приложение В***, с. 230).

По состоянию сетевого интерфейса изделия, выбранного в качестве *ведущего*, программа управления будет судить о работоспособности физического L2–Eth-интерфейса в процессе его работы и автоматически реагировать на его состояние, аналогичное состоянию ведущего интерфейса.

> *Примечание.* По этой причине, например, целесообразно в качестве ведущих интерфейсов использовать L2–TNL-интерфейс с включенным механизмом контроля состояния туннеля – KEEPALIVE или Ethernet-интерфейс с включенным механизмом PING-проб для контроля состояния интерфейса.

L3 (Рис. 2.15) – параметру можно присвоить значения **Да** или **Нет**, установив курсор на поле бланка и последовательно нажимая клавишу <Enter>. Значение параметра указывает, будет ли при обработке трафика L2–Eth-интерфейсом задействован механизм информационного взаимодействия со *службами* (*сервисами*) БВМ изделия через обработку на L3-уровне (подробнее см. раздел ***Приложение В***, с. 230).

Значение параметра можно также трактовать как *выключатель*, с помощью которого работа механизма обмена IP-датаграммами между уровнями L2 и L3 при функционировании L2–Eth-интерфейса может быть активизирована или временно приостановлена.

> *Например*. Работающий механизм информационного взаимодействия между L2-уровнем и L3-уровнем можно выключить – параметру **L3** присвоить значение **Нет** и выполнить рестарт изделия, чтобы обновленные параметры L2–Eth-интерфейса вступили в силу. При этом не произойдет потери значений *параметров маршрутизации* (IP-адреса, таблица маршрутов,

фильтры и пр.), необходимых для обработки трафика на L3-уровне и заданных ранее при настройке параметра **L3-параметры**, описание которого приведено ниже (см. Рис. 2.17).

L3-параметры (Рис. 2.15) – при выборе этого поля в бланке создания и настройки физического интерфейса типа **L2-Eth** на видеомонитор ЛКУ выдается бланк настройки параметров маршрутизации L2–Eth-интерфейса, аналогичный представленному на Рис. 2.17. По завершении процесса настройки с помощью этого бланка L2-Eth-интерфейс приобретает все атрибуты маршрутизации, необходимые интерфейсу для обеспечения обработки *части* проходящего через него входящего трафика на L3-уровне (подробнее см. раздел ***Приложение В***, с. 230).

Локальный IP-адрес интерфейса 0.0.0.0	
Удаленный IP-адрес интерфейса 0.0.0.0	
Максимальный размер IP-датаграмм (MTU) 1500	
Фильтр входящих	Фильтр исходящих
Специальные настройки	Таблица маршрутов

Рис. 2.17 Бланк настройки параметров маршрутизации L2–Eth-интерфейса для обработки трафика на L3-уровне

Настройку параметров маршрутизации L2–Eth-интерфейса с помощью бланка настройки, представленного на Рис. 2.17, следует выполнять в соответствии с рекомендациями, приведенными при описании процедур настройки аналогичных параметров с помощью бланка создания и настройки физического интерфейса типа **Ethernet** (см. раздел 2.3.1, Рис. 2.4, с. 25).

Слияние (Рис. 2.15) – параметр позволяет выбрать вариант реализации L2–Eth-интерфейсом алгоритма *фрагментирования-слияния* Ethernet-кадров, поступающих из сети на порт Ethernet-адаптера интерфейса. Если установить курсор на поле бланка и последовательно нажимать клавишу <Enter>, параметру можно присвоить значения: **нет**, **ПРОГР.** или **АППАР.**, что означает соответственно: алгоритм фрагментирования-слияния Ethernet-кадров применен не будет; будет применен алгоритм, реализованный на *программном* уровне; будет применен алгоритм, реализованный на *аппаратном* уровне (подробнее см. раздел ***Приложение В***, с. 230).

Параметры (Рис. 2.15) – при выборе альтернативы появляется бланк настройки параметров работы реализуемого L2–Eth-интерфейсом алгоритма фрагментирования-слияния Ethernet-кадров, аналогичный представленному на Рис. 2.18. Набор доступных для настройки параметров бланка зависит от значения параметра **Слияние** (Рис. 2.15): при значении **ПРОГР.** доступны для настройки все параметры; при значении **АППАР.** доступен для настройки только параметр **Максимальный размер контейнера**.

Максимальный размер контейнера	1448
Подлежат слиянию кадры короче	512
Ограничение количества сливаемых кадров	3

Рис. 2.18 Бланк настройки параметров работы алгоритма фрагментирования-слияния Ethernet-кадров

Значения параметров бланка (Рис. 2.18) выбираются администратором изделия с учетом сведений о характеристиках обрабатываемого изделием трафика. Первоначально бланк содержит умалчиваемые значения параметров (показаны на Рис. 2.14).

Максимальный размер контейнера (Рис. 2.18). Параметр устанавливает максимальное значение размера *контейнера*, который будет использован программой управления для работы алгоритма фрагментирования-слияния Ethernet-кадров (единица измерения – **байт**).

Контейнер представляет собой блок оперативной памяти, который перед отправкой получателю через сети передачи данных заполняется *сегментами*. Каждый сегмент представляет собой снабженный управляющим заголовком исходный Ethernet-кадр или *целиком* (если длина кадра короче значения, указанного параметром **Подлежат слиянию кадры короче**), или *фрагмент* исходного Ethernet-кадра (если длина кадра превышает размер контейнера). Заголовки сегментов необходимы при распаковке контейнера у получателя для формирования исходных Ethernet-кадров.

Подлежат слиянию кадры короче (Рис. 2.18). Параметр устанавливает *пороговое* значение длины принятого Ethernet-кадра (единица измерения – **байт**). Если длина Ethernet-кадра не превышает порог, то кадр подвергается обработке алгоритмом фрагментирования-слияния Ethernet-кадров и упаковывается в контейнер. Если длина Ethernet-кадра превышает порог, то кадр обрабатывается интерфейсом в обычном порядке.

Ограничение количества сливаемых кадров (Рис. 2.18). Параметр устанавливает *пороговое* значение числа Ethernet-кадров при упаковке в контейнер.

2.4. Создание и настройка виртуальных сетевых интерфейсов

Выше отмечалось (см. раздел 2.1, с. 19), что изделиями нового поколения в целях организации *дополнительных* специальных видов обработки потоков данных, циркулирующих через *физические* интерфейсы изделия, поддерживается несколько видов сетевых *виртуальных* интерфейсов.

Виртуальные (или логические) интерфейсы не имеют своей аппаратуры для взаимодействия с каналом связи и используют аппаратуру (порты Ethernet-адаптеров) одного из физических интерфейсов типа **Ethernet** или **L2-Eth**. Изделиями нового поколения поддерживаются *две* группы виртуальных интерфейсов в соответствии с двумя типами физических сетевых интерфейсов:

- виртуальные интерфейсы, связанные с физическими интерфейсами типа **Ethernet** как с базовыми; интерфейсы этой группы включают VLAN-интерфейсы (раздел 2.4.1, с. 36), TNL-интерфейсы (раздел 2.4.2, с. 39), GRE-интерфейсы (раздел 2.4.3, с. 43); интерфейсы этой группы выполняют необходимую дополнительную обработку *IP-датаграмм* на L3-уровне в случае применения изделия в качестве *криптомаршрутизатора*;
- виртуальные интерфейсы, связанные с физическими интерфейсами типа **L2-Eth** как с базовыми; эту группу составляют виртуальные интерфейсы типа **L2-VLAN** (раздел 2.4.4, с. 46) и типа **L2-TNL** (раздел 2.4.5, с. 49); интерфейсы этой группы выполняют необходимую дополнительную обработку *Ethernet-кадров* на L2-уровне в случае применения изделия в качестве средства организации *L2-криптомостов*.

Настоящий раздел РНУ посвящен вопросам создания и настройки сетевых виртуальных интерфейсов изделия, отнесенных к указанным группам.

2.4.1. VLAN-интерфейсы

В случае применения изделия в качестве криптомаршрутизатора полезным и эффективным может оказаться применение поддерживаемых изделием виртуальных VLAN-интерфейсов.

VLAN-интерфейсы логически связываются с *базовыми* физическими Ethernet-интерфейсами при создании и настройке VLAN-интерфейса через значение параметра **Базовый интерфейс** (см. Рис. 2.19, с. 38). Обеспечивая дополнительную обработку проходящего через Ethernet-интерфейс трафика, VLAN-интерфейсы позволяют эффективно управлять межсетевым трафиком в локальных сетях, в результате чего при реализации отдельных сетевых решений может быть достигнут заметный практический и экономический эффект.

> *Примечание.* Ниже приведены общие сведения о технологии VLAN-обмена и некоторые положения стандарта **IEEE802.1Q**, полезные при подготовке изделий к работе как с VLAN-интерфейсами (см. раздел 2.4.1.2, с. 38), обеспечивающими работу с VLAN-сетями при организации обмена на L3-уровне, так и с L2–VLAN-интерфейсами (см. раздел 2.4.4, с. 46), обеспечивающими работу с VLAN-сетями при организации обмена на L2-уровне.

2.4.1.1. Общие сведения

Практически все современные локальные вычислительные сети строятся с использованием технологии Ethernet, которая позволяет объединить множество рабочих станций абонентов, серверы приложений и оборудование построения глобальной сети (WAN) в единое коммуникационное пространство. Все участники Ethernet-сети сразу после подключения получают возможность непосредственного информационного обмена по схеме «каждый с каждым» (**unicast**-адресация), «каждый со всеми» (**broadcast**-адресация) или «каждый с группой» (**multicast**-адресация) – подробнее см. раздел 2.8, с. 60.

Если информационный обмен между некоторыми участниками сети нежелателен (запрещен), то для них приходится организовывать отдельную Ethernet-сеть (устанавливая дополнительное оборудование), управляя потоками данных между сетями с использованием межсетевых экранов, что приводит к существенным дополнительным затратам. Для решения указанной проблемы менее затратными средствами технологией Ethernet поддерживается возможность построения *виртуальных локальных сетей* – VLAN (Virtual Local Area Network), которую поддерживают практически все современные Ethernet-коммутаторы. В простейшем случае организация VLAN-сетей выполняется простым делением ресурсов коммутатора между сетями (закреплением части портов коммутатора за каждой из VLAN-сетей). Такой подход аналогичен применению нескольких независимых коммутаторов, установленных в один корпус, но позволяет гибко изменять количество выделяемых для каждой сети портов коммутатора в зависимости от текущих потребностей.

VLAN-сети информационно изолированы друг от друга. Если необходимо подключить VLAN-сети к маршрутизатору, то в каждой сети необходимо предусмотреть порт для этой цели, а в маршрутизаторе организовать отдельные Ethernet-интерфейсы для подключения каждой VLAN-сети. Такое решение крайне неудобно и затратно.

Решение проблемы объединения VLAN-сетей обеспечивается такой технологией работы, когда на Ethernet-коммутаторе выделяется один порт (его называют *транковым* (англ. `trunk` – магистраль) или *тегированным* (англ. `tag` – метка, признак) портом), принадлежащий одновременно нескольким VLAN-сетям. Исходящий трафик с этого порта должен передаваться с добавлением в заголовок каждого кадра специального

идентификатора – *тега*, по которому можно определить принадлежность кадров к конкретной VLAN-сети. Если к такому порту подключить маршрутизатор, интерфейс которого умеет реагировать на теги в кадрах, то маршрутизатор сможет получать информацию ото *всех* VLAN-сетей по *одному* интерфейсу и выполнять ее необходимую обработку. Справедливо и обратное, если маршрутизатору потребуется передать пакет в заданную VLAN-сеть, то он должен будет указать идентификатор требуемой сети – *тег* – в заголовке передаваемого кадра.

Технология построения виртуальных локальных сетей (VLAN) описана стандартом **IEEE802.1Q**, основное содержание которого изложено ниже.

В качестве идентификатора VLAN-сети – *тега* – используется VNID (Virtual Network Identificator – идентификатор виртуальной сети) – 12-битовое двоичное число (см. ниже формат кадра Ethernet_II_VLAN), которое может принимать значения от ***0*** до ***4095*** (первый и последний номера зарезервированы, их использовать нельзя). Соответственно, VLAN-сети с помеченным с помощью VNID трафиком называют *тегированными*. Чаще всего при настройке VLAN-сетей на Ethernet-коммутаторах задают несколько *нетегированных* портов для подключения абонентских станций и один или несколько *тегированных* (*транковых*) портов для подключения WAN-маршрутизаторов, серверов приложений или иных ресурсов, требующих одновременной работы с несколькими VLAN-сетями.

Для разделения информационных потоков в локальной сети по принадлежности к группам в стандартные заголовки Ethernet-кадров, циркулирующих в многоточечном канале связи локальной сети, добавляется информация, идентифицирующая группу, к которой принадлежит каждый кадр.

Рассмотрим формат кадров Ethernet_II (именно этот формат используется для передачи IP-датаграмм через локальную сеть):

Назначение поля	Длина (байт)
MAC-адрес получателя	6
MAC-адрес отправителя	6
Тип данных	2
Данные	46-1500

При использовании технологии VLAN к стандартному заголовку кадра Ethernet_II добавляются два дополнительных поля, и кадр приобретает следующий формат:

Назначение поля	Длина (байт)
MAC-адрес получателя	6
MAC-адрес отправителя	6
Тип данных (***0x8100***)	2
Идентификатор группы (VNID)	2
Исходный тип данных	2
Данные	46-1500

Формирование VLAN-модифицированных кадров формата Ethernet_II (будем называть их кадрами формата Ethernet_II_VLAN) производится по следующим правилам.

1. В поле **Тип данных** стандартного заголовка кадра формата Ethernet_II помещается шестнадцатеричное значение **8100**, которое означает, что в кадр упакованы VLAN-данные.
2. В добавочном поле **Идентификатор группы (VNID)** размещается идентификатор группы станций, относящихся к конкретной VLAN (значение **VNID** определяют 12 младших бит 2-байтового добавочного поля **Идентификатор группы**).
3. В добавочное поле **Исходный тип данных** переносится действительный тип следующих далее данных.
4. При дальнейшей обработке кадра формата Ethernet_II_VLAN два добавочных поля (общей длиной 4 байта) условно считаются принадлежащими полю данных.

Физическими интерфейсами изделий обеспечивается обработка Ethernet-кадров формата Ethernet_II_VLAN. При приеме таких кадров физические интерфейсы корректно извлекают содержащиеся в них данные, а при отправке данных – могут упаковать их в кадры формата Ethernet_II_VLAN.

Виртуальные интерфейсы изделия типа **VLAN** и **L2-VLAN** являются удобными для администратора изделия механизмами, обеспечивающими оперативное управление трафиками, проходящими через соответствующие базовые физические интерфейсы изделия.

Например, механизмы этих виртуальных интерфейсов позволяют дифференцировать в базовых физических интерфейсах условия фильтрации для трафиков, принадлежащих разным VLAN-сетям, путем *индивидуальной* настройки фильтров входящего и исходящего трафиков для каждого из виртуальных интерфейсов, обеспечивающих работу по VLAN-технологии (см. поля **Фильтр входящих** и **Фильтр исходящих** бланков создания и настройки интерфейсов типа **VLAN** и **L2-VLAN**).

2.4.1.2. Создание и настройка VLAN-интерфейса.

Чтобы создать VLAN-интерфейс, следует в меню выбора типа и принадлежности создаваемого интерфейса (Рис. 2.2, с. 23) выбрать альтернативу **VLAN**, установить принадлежность создаваемого VLAN-интерфейса наружному или внутреннему маршрутизатору и нажать клавишу <Esc>. На видеомонитор ЛКУ будет выдан бланк, представленный на Рис. 2.19.

Наружный

Имя интерфейса	Таблица маршрутов
VLAN-идентификатор 0	Базовый интерфейс
Локальный IP-адрес интерфейса 0.0.0.0	
Удаленный IP-адрес интерфейса 0.0.0.0	
Допустимое время неактивности интерфейса 0	
Максимальный размер IP-датаграмм (MTU) 1500	
Фильтр входящих	Фильтр исходящих
Специальные настройки	Дополнительные параметры

Рис. 2.19 Бланк создания и настройки VLAN-интерфейса

Этот бланк отличается от представленного на Рис. 2.4 бланка создания и настройки физического интерфейса типа **Ethernet** отсутствием полей **Тип** и **Режим активизации** и наличием двух дополнительных полей: **VLAN-идентификатор** и **Базовый интерфейс**. Остальные поля этих двух бланков совпадают.

Для VLAN-интерфейсов перечисленные ниже поля бланка настройки заполняются так же, как для физических Ethernet-интерфейсов (см. Рис. 2.4, раздел 2.3.1, с. 25):

- **Имя интерфейса**,
- **Таблица маршрутов**,
- **Локальный IP-адрес интерфейса**,
- **Удаленный IP-адрес интерфейса**,
- **Допустимое время неактивности интерфейса**,
- **Максимальный размер IP-датаграмм**,
- **Фильтры входящих**, **Фильтры исходящих**,
- **Специальные настройки**

Дополнительные параметры (Рис. 2.19) – при выборе этого поля бланка на видеомонитор ЛКУ выдается экран настройки, представленный на Рис. 2.20.

VLAN-интерфейсы имеют только два дополнительных параметра: **Скорость передачи** и **Скорость приема**. Настройка значений параметров должна выполняться с учетом рекомендаций, выданных в разделе 2.3.1 (с. 25) при настройке Ethernet-интерфейса (см. Рис. 2.9, с. 29). Это позволит обеспечить с помощью поддерживаемого изделием механизма *приоритизации трафика* приемлемого (в условиях ограниченной пропускной способности отдельных трактов передачи данных ЗСПД) режима обработки потоков данных различного характера (подробнее о механизме приоритизации трафика см. раздел ***Приложение Г*** (с. 238).

Скорость передачи 0
Скорость приема 0

Рис. 2.20 Экран настройки ограничения скорости обработки трафиков, проходящих через VLAN-интерфейс

> *Примечание.* Алгоритмы обработки трафика, *передаваемого* в сеть и *принимаемого* из сети интерфейсами изделия, при настройке которых предусмотрена возможность установки значений параметров **Скорость передачи** и **Скорость приема** (это интерфейсы типа **Ethernet**, **VLAN**, **TNL**), *различны* (подробнее об этих алгоритмах см. раздел ***Приложение Г***, с. 238). Для правильной настройки значений указанных параметров следует учитывать разницу в работе этих алгоритмов.

VLAN-идентификатор (Рис. 2.19) – целое десятичное число в диапазоне от *0* до *4095*, идентификатор VLAN-сети (VNID), значение которого задает администратор.

Базовый интерфейс (Рис. 2.19) – при выборе альтернативы на видеомонитор ЛКУ будет выдан список ранее сконфигурированных физических интерфейсов маршрутизатора, аналогичный представленному на Рис. 2.21.

В этом списке следует выбрать имя того интерфейса, к которому как к *базовому* будет привязан создаваемый VLAN-интерфейс, после чего имя выбранного интерфейса будет занесено в поле **Базовый интерфейс** бланка создания и настройки VLAN-интерфейса (Рис. 2.19).

Рис. 2.21 Список физических интерфейсов, созданных в маршрутизаторе

2.4.2. *TNL-интерфейсы*

Общие сведения. В рамках технологии DioNIS® администратору предоставлена возможность применения нескольких *видов* криптотуннелей, создаваемых с помощью разных инструментов (подробнее о видах криптотуннелей и способах их организации см. раздел 3.1, с. 73).

В изделиях нового поколения в качестве *основного* инструмента для передачи *IP-датаграмм* между БВМ и БНМ изделия через его шифратор применяются TNL-интерфейсы.

Наряду с TNL-интерфейсами новыми изделиями поддерживается применявшийся ранее механизм статических криптотуннелей, выполняющий аналогичную функцию. Применение механизма статических криптотуннелей обеспечивает совместимость работы изделий нового и старого поколений.

> *Примечание*. Применение TNL-интерфейсов для целей защиты IP-датаграмм, передаваемых на L3-уровне, имеет ряд преимуществ по сравнению с применением статических туннелей (подробнее см. раздел 3.1, с. 73). Но в ряде специальных случаев применение статических криптотуннелей может оказаться предпочтительнее, т.к. статические криптотуннели позволяют при настройке более *избирательно* очертить круг отбираемых в криптотуннель IP-датаграмм (хотя и требуют соответствующей квалификации администратора).

Создание и настройка TNL-интерфейса. Чтобы создать TNL-интерфейс, надо в меню выбора типа и принадлежности интерфейса (Рис. 2.2, с. 23) выбрать альтернативу **TNL**, установить параметру, определяющему принадлежность интерфейса, значение *общий* и нажать клавишу <Esc>. На видеомонитор ЛКУ будет выдан бланк, представленный на Рис. 2.22.

Этот бланк отличается от представленного на Рис. 2.4 (с. 25) бланка создания и настройки физического интерфейса типа **Ethernet**:

- отсутствием в левом верхнем углу рамки бланка указателя на маршрутизатор, которому принадлежит создаваемый и настраиваемый интерфейс, поскольку TNL-интерфейсы имеют *общую* принадлежность;
- наличием дополнительных полей **Идентификатор туннеля** и **Шифрование потока**;
- отсутствием полей **Тип**, **Режим активизации** и **Допустимое время неактивности интерфейса**.

Все остальные поля в двух бланках совпадают.

Имя интерфейса	Таблица маршрутов
Идентификатор туннеля 0	
Локальный IP-адрес интерфейса 0.0.0.0	
Удаленный IP-адрес интерфейса 0.0.0.0	
Шифрование потока (0)0.0->0 [vМПМ]	
Максимальный размер IP-датаграмм (MTU) 1500	
Фильтр входящих	Фильтр исходящих
Специальные настройки	Дополнительные параметры

Рис. 2.22 Бланк создания и настройки TNL-интерфейса

Для TNL-интерфейсов перечисленные ниже поля бланка настройки заполняются так же, как для физических Ethernet-интерфейсов (см. Рис. 2.4, раздел 2.3.1, с. 25):

- **Имя интерфейса**,
- **Таблица маршрутов**,

- **Фильтры входящих**, **Фильтры исходящих**,
- **Максимальный размер IP-датаграмм (TU)**,
- **Специальные настройки**.

Остальные поля бланка заполняются следующим образом.

Идентификатор туннеля (Рис. 2.22) – 5-значное десятичное число в диапазоне от ***0*** до ***32767***.

> *Примечание.* Значение идентификатора криптотуннеля в составе ЗСПД должно быть *уникальным* среди узлов, входящих в одну криптозону.

Параметр **Идентификатор туннеля** совместно с параметрами **Локальный IP-адрес интерфейса** и **Удаленный IP-адрес интерфейса** (см. ниже Рис. 2.24) однозначно определяет криптотуннель (со всеми его другими криптографическими характеристиками), организованный между изделиями (в составе узлов ЗСПД) с указанными IP-адресами.

Локальный IP-адрес интерфейса (Рис. 2.22) – задает IP-адрес того сетевого интерфейса БНМ изделия (поле **Source Address** в транспортном IP-заголовке – см. раздел 3.1, с. 73), который является локальным отправителем исходящего и получателем входящего туннелированного трафика для данного криптотуннеля.

При выборе поля **Локальный IP-адрес интерфейса** на видеомонитор ЛКУ будет выдан запрос (Рис. 2.23), аналогичный запросу, представленному на Рис. 2.5 (с. 26) при описании процедуры создания и настройки физического интерфейса типа Ethernet.

```
Локальный IP-адрес интерфейса (адрес/бит) :
```

Рис. 2.23 Запрос на ввод локального IP-адреса TNL-интерфейса и маски подсети, к которой он подключается

Отвечая на этот запрос, администратору следует руководствоваться выданными ранее рекомендациями (см. пояснения к Рис. 2.5, с. 26).

Удаленный IP-адрес интерфейса (Рис. 2.22) – задает IP-адрес того сетевого интерфейса БНМ (поле **Destination Address** в транспортном IP-заголовке – см. раздел 3.1, с. 73), который является удаленным получателем исходящего и отправителем входящего туннелированного трафика для данного криптотуннеля.

Шифрование потока (Рис. 2.22) – при выборе этого поля бланка создания и настройки TNL-интерфейса на видеомонитор будет выдано меню настройки криптопараметров TNL-интерфейса, представленное на Рис. 2.24.

```
Шифрование потока  ДА
Версия криптоалгоритма vМПМ
Номер серии ключей     0
Локальный криптономер  0
Удаленный криптономер  0
Номер ключевой зоны    0
```

Рис. 2.24 Меню настройки криптопараметров TNL-интерфейса

Шифрование потока (Рис. 2.24) – возможными значениями параметра могут быть значения: ***Да*** или ***Нет***, указывающие соответственно, будет ли зашифрован передаваемый изделием в сети общего пользования поток данных.

Применяя изделия для защиты информации Пользователя, содержащей сведения, составляющие государственную тайну, параметру **Шифрование потока** следует всегда присваивать значение ***Да***.

Программа управления функционированием изделия является универсальной и предназначена для широкого класса устройств, включая устройства защиты информации, не содержащей сведений, составляющих государственную тайну. При использовании устройств, предназначенных для этих целей, параметр **Шифрование потока** может иметь значение ***Нет***.

Версия криптоалгоритма (Рис. 2.24) – параметр управления криптографической совместимостью. Определяет вариант реализации версии криптографического алгоритма преобразования циркулирующего через настраиваемый TNL-интерфейс трафика IP-пакетов и может принимать одно из трех значений: ***vМПМ***, ***v07Ф*** или ***v07М***.

С помощью установки соответствующих значений параметра обеспечивается *синхронизация* на приемном и передающем концах криптотуннеля алгоритмов криптообработки циркулирующих по криптотуннелю зашифрованных IP-пакетов.

Выбор конкретного значения параметра выполняется с учетом того, с какими модификациями изделий на удаленных узлах ЗСПД предстоит осуществлять защищенный обмен по настраиваемому TNL-интерфейсу (критотуннелю):

- в случае обмена с изделием серии М-479Рх параметру следует присвоить значение ***vМПМ***;

- в случае обмена с изделием М-479К параметру следует присвоить значение ***v07Ф***;
- в случае обмена с изделием М-479Ж параметру следует присвоить значение ***v07М***.

Примечание. Изделия М-479Р2 могут осуществлять защищенный обмен только с изделиями серии М-479Рх, т.е. для них параметр **Версия криптоалгоритма** всегда имеет значение ***vМПМ***.

Номер серии ключей (Рис. 2.24) – целое десятичное число в диапазоне от ***1*** до ***999999***, равное номеру серии ключевого документа (далее – КД или ключ), используемой в криптографической сети в планируемый Администрацией ЗСПД период времени (подробнее см. раздел 3.4, с. 122, а также РЭ на конкретное изделие).

Локальный криптономер (Рис. 2.24) – целое десятичное число в диапазоне от ***1*** до ***9999***, соответствующее криптографическому номеру (*криптономеру*) настраиваемого изделия в криптографической сети.

Удаленный криптономер (Рис. 2.24) – целое десятичное число в диапазоне от ***1*** до ***9999***, соответствующее криптономеру в криптографической сети того изделия, с которым будет выполняться обмен информацией по настраиваемому криптотуннелю.

Номер ключевой зоны (Рис. 2.24) – целое десятичное число в диапазоне от ***1*** до ***999*** или ***0***.

Примечание. Каждый узел (изделие защиты) в криптографической сети должен иметь *уникальную* идентификацию. В ЗСПД, обеспечивающей защищенный обмен в пределах *нескольких* ключевых зон, уникальную идентификацию ключевого документа, используемого узлом для защищенного обмена, определяют *три* параметра создаваемого на требуемом направлении обмена криптографического туннеля: **Номер ключевой зоны**, **Номер серии ключей** и **Локальный криптономер**.

Если уникальность идентификации узла в криптосети значениями настроенных параметров криптотуннелей или значениями параметров введенных КД обеспечена не будет, криптотуннели на направлениях обмена с соответствующими удаленными узлами криптографической сети открыты не будут.

Если в криптографической сети предусматривается обмен в пределах *единственной* ключевой зоны, то для обеспечения уникальности идентификации КД достаточно двух параметров **Номер серии ключей** и **Локальный криптономер**. Поэтому в этом случае ввод реального значения параметра **Номер ключевой зоны** не обязателен и может быть сохранено его значение, предлагаемое по умолчанию, – значение ***0*** (Рис. 2.24).

Если в криптографической сети предусматривается обмен между узлами *нескольких* (двух и более) ключевых зон, при настройке криптотуннелей для обеспечения уникальности идентификации КД обязателен ввод *отличных от нуля* значений ключевых зон (значений параметра **Номер ключевой зоны**), в пределах которых может осуществляться защищенный обмен. В противном случае возможно совпадение пар значений параметров **Номер серии ключей** и **Локальный криптономер** для ключей, принадлежащих разным ключевым зонам, и уникальность идентификации узла обеспечена при этом не будет.

При значении параметра **Версия криптоалгоритма v07Ф** или **v07М** значение параметра **Номер ключевой зоны** можно оставить равным ***0***, так как данные версии алгоритма данный параметр не используют.

Дополнительные параметры (Рис. 2.22) – при выборе поля бланка на видеомонитор ЛКУ будет выдано представленное на Рис. 2.25 меню настройки дополнительных параметров TNL-интерфейса.

Описание	
Формат заголовка TNL	Метка туннеля 0
Контроль состояния Нет	
Скорость передачи 0	
Скорость приема 0	

Рис. 2.25 Меню настройки дополнительных параметров TNL-интерфейса

Описание (Рис. 2.25) – произвольный комментарий администратора изделия (длиной до 32-х символов).

Формат заголовка (Рис. 2.25) – параметр определяет тип транспортного протокола для передачи туннелированных датаграмм.

Параметр может принимать следующие значения:

TNL – в этом случае полю ***Protocol*** в IP-заголовках исходящих IP-пакетов TNL-интерфейса будет присвоено значение **4** (что означает инкапсуляцию IP in IP);

UDP – в этом случае полю ***Protocol*** в IP-заголовках исходящих IP-пакетов TNL-интерфейса будет присвоено значение **17**. Использование UDP-протокола позволяет обходить политику отдельных провайдеров, препятствующую передаче туннелированных (инкапсулированных) данных (когда полю ***Protocol*** в IP-заголовках исходящих IP-пакетов TNL-интерфейса присвоено значение **4**) через контролируемые ими сети передачи данных.

UDPnat – в этом случае полю ***Protocol*** в IP-заголовках исходящих IP-пакетов TNL-интерфейса будет присвоено значение **17**. Присвоение параметру **Формат заголовка** значения ***UDPnat*** обеспечивает возможность передачи туннелированных данных в режиме клиент-сервер из-под NAT-обработчика.

Если параметру **Формат заголовка** присваивается значение ***UDP*** или ***UDPnat***, то появляется меню управления значением портов UDP-датаграмм TNL-интерфейса (Рис. 2.26), с помощью которого можно настроить номера портов передачи и приема UDP-датаграмм, отличные от умалчиваемых (по умолчанию оба параметра имеют значение *500*).

Формат заголовка UDP
Порт отправителя 500
Порт получателя 500

Рис. 2.26 Меню управления значением портов

Метка туннеля (Рис. 2.25) – при выборе поля появляется запрос, в ответ на который может быть указано целое число в диапазоне от ***0*** до ***255***, обеспечивающее *привязку* настраиваемого туннеля к конкретной PING-пробе (подробнее о реализации PING-проб см. раздел 2.7, с. 58).

Контроль состояния (Рис. 2.25) – параметр позволяет установить контроль за состоянием криптотуннеля. При выборе поля появляется представленное на Рис. 2.27 меню настройки параметров работы механизма контроля состояния криптотуннеля (KEEPALIVE). Чтобы запустить механизм контроля, следует задать *ненулевые* значения параметров **Интервал отправки запросов** и **Максимальное время ожидания ответов** (единица измерения значений обоих параметров – секунда); если параметрам (или одному параметру **Интервал отправки запросов**) задать нулевые значения, то параметр **Контроль состояния** получит значение *Нет*, при этом контроль не выполняется.

Интервал отправки запросов	0
Максимальное время ожидания ответов	0

Рис. 2.27 Меню настройки параметров работы механизма контроля состояния криптотуннеля (KEEPALIVE)

Примечание. В списках интерфейсов БВМ, выводимых на видеомонитор ЛКУ в процессе оперативного контроля состояния интерфейсов (см. раздел 2.6, с. 52), имена TNL-интерфейсов, в которых установлен и в которых не установлен контроль за состоянием туннеля, отображаются разными цветами.

Выбор конкретных значений для настройки двух следующих параметров TNL-интерфейса – **Скорость передачи** и **Скорость приема** – должен выполняться с учетом ранее выданных в разделе 2.3.1, с. 25 рекомендаций по выбору значений этих параметров при настройке Ethernet-интерфейса.

Скорость передачи (Рис. 2.25) – указание отличного от нуля значения параметра (единица измерения – **Кбит/сек**) позволяет искусственно ограничить заданным значением максимальную скорость *передачи* датаграмм в локальную сеть. При этом запускается механизм приоритизации передаваемого интерфейсом трафика (обработки каждого IP-пакета в потоке с учетом его *приоритета*).

При нулевом значении параметра скорость передачи не ограничивается, механизм приоритизации не запускается и очереди, соответствующие 8-ми поддерживаемым изделием уровням приоритетов, не обслуживаются.

Скорость приема (Рис. 2.25) – указание отличного от нуля значения параметра позволяет искусственно ограничить заданным значением (единица измерения – **Кбит/сек**) максимальную скорость *приема* IP-датаграмм трафика, поступающего в интерфейс из локальной сети.

При нулевом значении параметра скорость трафика, принимаемого интерфейсом из сети, не ограничивается, запуск механизма приоритизации входящего трафика не производится, входящие пакеты, принимаемые интерфейсом из сети, обрабатываются в порядке их поступления.

2.4.3. ***GRE-интерфейсы***

Поддерживаемые изделием GRE-интерфейсы используются как инструмент построения виртуальных частных сетей (VPN), обеспечивающий передачу IP-датаграмм, принадлежащих *различным* протоколам обмена, упакованных в GRE-туннель, создаваемый между территориально удаленными локальными сетями.

Упаковка сетевых пакетов в GRE-туннель осуществляется согласно GRE-протоколу (*Generic Routing Encapsulation* – протоколу универсальной инкапсуляции маршрутов) в соответствии с RFC 2784, RFC 890. Это протокол туннелирования сетевых пакетов, используемый, например, при необходимости передачи пакетов одной сети через другую сеть.

Общие сведения. GRE-туннель представляет собой логическое соединение *точка-точка*, его можно считать разновидностью VPN-туннеля без шифрования. GRE-туннель предоставляет, в частности, возможность передачи сетевых пакетов, формируемых протоколами маршрутизации, генерирующими широковещательный трафик.

Для поддержания обмена с использованием GRE-туннеля, проброшенного через IP-сети общего пользования, в составе каждой локальной сети в качестве *пограничных* маршрутизаторов устанавливаются изделия, на которых создаются виртуальные GRE-интерфейсы, обеспечивающие необходимые преобразования сетевых пакетов – упаковку в GRE-туннель исходящих пакетов и извлечение из GRE-туннеля входящих пакетов, адресованных устройствам в составе локальной сети.

> *Примечание*. В настоящее время подавляющее большинство локальных сетей осуществляют межсетевой обмен на основе использования протоколов *стека TCP/IP*, трафик обмена между такими сетями представляет собой поток *IP-датаграмм*. Поэтому в дальнейшем мы будем говорить именно о них, не забывая при этом, что существуют сети, использующие другие (отличные от стека протоколов TCP/IP) сетевые протоколы, трафик обмена в таких сетях осуществляется с помощью *сетевых пакетов* соответствующего формата.

Все исходящие IP-датаграммы, которыми обмениваются соединенные GRE-туннелем изделия, снабжаются заголовком туннеля (GRE-заголовком) и новым транспортным IP-заголовком. Сформированные в результате *транспортные* IP-датаграммы отправляются в транспортную IP-сеть по GRE-туннелю, соединяющему пару пограничных изделий. На противоположной (приемной) стороне GRE-туннеля дополнительные заголовки отбрасываются, в результате чего полностью восстанавливаются исходные IP-датаграммы. В качестве транспортного протокола для передачи датаграмм используется протокол GRE (значение номера протокола в IP-заголовке – **47**), поэтому фильтры брандмауэров у провайдеров сетей общего пользования на маршрутах, используемых GRE-туннелем, должны быть прозрачны для транспортных IP-датаграмм с соответствующим номером протокола в заголовке.

Формат упаковки датаграмм в GRE-туннель:

Транспортный IP-заголовок
Заголовок туннеля (GRE - заголовок)
Туннелируемые данные

Транспортный IP-заголовок (длина 20 байт). IP-заголовок транспортной IP-датаграммы, передаваемой по GRE-туннелю, имеет стандартный для заголовка IP-датаграммы набор полей и имеет следующий формат (Рис. 2.28):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Version	**IHL**	**Type of Service**	**Total Length**
Identification		**Flags**	**Fragment Offset**
Time to Live	**Protocol**	**Header Checksum**	
Source Address			
Destination Address			

Рис. 2.28 Формат IP-заголовка транспортной IP-датаграммы, передаваемой по GRE-туннелю

Version – ***4***;

IHL – ***5***;

Type of Service – зависит от настройки GRE-интерфейса (**Доп.параметры ⇨ Поле TOS** – см. Рис. 2.31, с. 45);

Total Length – общая длина: длина туннелируемых данных + длина транспортного IP-заголовка (20 байт) + заголовок туннеля;

Identification – идентификатор пакетов, используемый для распознавания пакетов, образовавшихся при фрагментации;

Flags – зависит от настройки GRE-интерфейса (**Доп.параметры ⇨ Флаг DF** – см. Рис. 2.31, с. 45);
Fragment Offset – *0*;
Time to Live – заданное значение TTL транспортной IP-датаграммы;
Protocol – ***47***;
Header Checksum – рассчитывается;
Source Address – локальный IP-адрес туннеля;
Destination Address – удаленный IP-адрес туннеля.

Заголовок туннеля (GRE - заголовок) (длина от 4 до 16 байт) (Рис. 2.29):

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
C		**K**	**S**	**Reserved0**											**Ver**		**Protocol Type**														
Checksum (optional)																	**Reserved1 (optional)**														
Key (optional)																															
Sequence Number (optional)																															

Рис. 2.29 Заголовок GRE-туннеля (GRE - заголовок)

C – флаг использования поля **Checksum** (*0* – если значение параметра **Контрольная сумма** в бланке настройки дополнительных параметров (Рис. 2.31, с. 45) имеет значение *нет*, и *1* – если – *да*);
K – флаг использования поля **Key**;
S – флаг использования поля **Sequence Number** (*0* – если значение параметра **Нумерация пакетов** в бланке настройки дополнительных параметров (Рис. 2.31, с. 45) имеет значение *нет*, и *1* – если – *да*);
Reserved0 – поле не используется, должно быть значение ***0***;
Ver – версия протокола GRE (***0***);
Protocol Type – тип протокола (совпадает с полем **Type** заголовка Ethernet_II кадра);
Checksum – контрольная сумма (поле заполняется если поле **C** имеет значение *1*);
Reserved1 – поле не используется, должно быть значение ***0***;
Key – идентификационные данные пакета (в данной версии ПО поле не заполняется);
Sequence Number – порядковый номер датаграммы (заполняется если поле **S** имеет значение *1*).

Примечание. Производительность IP-маршрутизатора при использовании GRE-протокола может снизиться более чем вдвое за счет обработки маршрутизатором каждой IP-датаграммы дважды (повторная маршрутизация), а также за счет возможной фрагментации исходной IP-датаграммы (из-за увеличения общей длины туннелированной датаграммы, превышающей MTU физического интерфейса).

Создание и настройка GRE-интерфейса. С целью создания GRE-интерфейса следует в меню выбора типа и принадлежности создаваемого интерфейса (см. Рис. 2.2, с. 23) выбрать альтернативу **GRE**, установить принадлежность создаваемого GRE-интерфейса (**наружный** или **внутренний**), после чего нажать клавишу <Esc>. В ответ на видеомонитор ЛКУ будет выдан представленный на Рис. 2.30 бланк создания и настройки GRE-интерфейса.

Этот бланк отличается от похожего бланка создания и настройки TNL-интерфейса (Рис. 2.22, с. 39) отсутствием полей **Идентификатор туннеля** и **Шифрование потока**. Остальные поля бланков совпадают.

Имя интерфейса	Таблица маршрутов
Локальный IP-адрес интерфейса 0.0.0.0	
Удаленный IP-адрес интерфейса 0.0.0.0	
Максимальный размер IP-датаграмм (MTU) 1500	
Фильтр входящих	Фильтр исходящих
Специальные настройки	Дополнительные параметры

Рис. 2.30 Бланк создания и настройки GRE-интерфейса

Для GRE-интерфейсов перечисленные ниже поля бланка настройки заполняются так же, как аналогичные поля при создании и настройке физических Ethernet-интерфейсов (см. Рис. 2.4, раздел 2.3.1, с. 25):

- **Имя интерфейса**;
- **Таблица маршрутов**;
- **Максимальный размер IP-датаграмм (MTU)**;
- **Фильтры входящих**, **Фильтры исходящих**;
- **Специальные настройки**.

Остальные поля бланка создания и настройки GRE-интерфейса (Рис. 2.30) заполняются с учетом приведенных ниже сведений.

Локальный IP-адрес – задает IP-адрес того сетевого интерфейса (поле **Source Address** в транспортном IP- заголовке – см. раздел 3.1, с. 73), который является локальным отправителем исходящего и получателем входящего туннелированного трафика для данного GRE-интерфейса.

Удаленный IP-адрес – задает IP-адрес того сетевого интерфейса (поле **Destination Address** в транспортном IP- заголовке – см. раздел 3.1, с. 73), который является удаленным получателем исходящего и отправителем входящего туннелированного трафика для данного GRE-интерфейса.

Дополнительные параметры (Рис. 2.30) – при выборе поля на видеомонитор ЛКУ будет выдан представленный на Рис. 2.31 бланк настройки, с помощью которого следует настроить три группы значений дополнительных параметров GRE-туннеля.

```
Режимы формирования заголовков туннеля
 Нумерация пакетов нет
 Контрольная сумма нет
 Поле TOS копировать значение (HEX) 0
 Флаг DF  копировать

Восстановление последовательности пакетов
 Размер буфера                0
 Максимальная задержка пакетов 0

Контроль состояния туннеля
 Интервал отправки запросов          0
 Максимальное время ожидания ответов 0
```

Рис. 2.31 Бланк настройки дополнительных параметров GRE-туннеля

1. Группа параметров **Режимы формирования заголовков туннеля** (Рис. 2.31). Значения параметров этой группы влияют на подготовку к *передаче* в GRE-туннель IP-датаграммы, формируемой на основе исходной IP-датаграммы.

   Нумерация пакетов – параметр может принимать значения *Да* или *Нет*, которые определяют, будет ли производиться нумерация исходящих пакетов GRE-туннеля. Если параметру будет присвоено значение *Да*, то запускается механизм *нумерации*, вследствие чего: в GRE-заголовок (см. Рис. 2.29) устанавливается флаг **S**, а в поле **Sequence Number** записывается порядковый номер пакета (при этом длина заголовка исходящего пакета увеличивается на 4 байта).

   > *Примечание.* Порядок следования пакетов важен при работе некоторых приложений Пользователя (например, в IP-телефонии). В таких случаях на приемном конце GRE-туннеля должна быть восстановлена исходная последовательность пакетов. Этой цели служат параметры второй группы дополнительных параметров GRE-туннеля **Восстановление последовательности пакетов** (Рис. 2.31) – см. ниже.

   Контрольная сумма – параметр может принимать значения *Да* или *Нет*, которые определяют, будет ли производиться контрольное суммирование исходящих пакетов GRE-туннеля. Если параметру будет присвоено значение *Да*, то запускается механизм контрольного суммирования, вследствие чего: в GRE-заголовок (см. Рис. 2.29) устанавливается флаг **C**, включается механизм проверки контрольных сумм входящих пакетов GRE-туннеля, а также включается механизм расчета контрольных сумм исходящих пакетов GRE-туннеля и их записи в поле **Checksum** GRE-заголовка (при этом длина заголовка исходящего пакета увеличивается на 4 байта).

   Поле TOS – параметр может принимать значения: *копировать* или *установить*:

   - при значении параметра *копировать* в поле **Type of Service** транспортного IP-заголовка датаграммы (Рис. 2.28, с. 43) будет копироваться значение поля **ToS** из исходной IP-датаграммы;

- при значении параметра *установить* в поле **Type of Service** транспортного IP-заголовка датаграммы заносится то число (в шестнадцатеричном формате), которое указано в параметре **значение (HEX)** бланка (см. Рис. 2.31).

Флаг DF – параметр может принимать значения: *копировать*, *установить*, *сбросить*:

- при значении параметра *копировать* значение поля **Flags** транспортного заголовка формируемой для отправки в GRE-туннель IP-датаграммы будет скопировано из IP-заголовка исходной IP-датаграммы;
- при значении параметра *установить* полю **Flags** транспортного заголовка формируемой IP-датаграммы будет присвоено значение *1*;
- при значении параметра *сбросить* полю **Flags** будет присвоено значение *0*.

2. Группа параметров **Восстановление последовательности пакетов** (Рис. 2.31). Значения параметров этой группы влияют на организацию процесса *приема* IP-датаграмм из GRE-туннеля.

   Параметры этой группы позволяют включить механизм восстановления порядка следования принимаемых из GRE-туннеля входящих IP-датагармм – GRE-пакетов. Восстановление нарушенного порядка следования возможно при выполнении двух условий:

   - пакеты при отправке в GRE-туннель были пронумерованы;
   - значения обоих параметров этой группы – **Размер буфера** и **Максимальная задержка пакетов** – отличны от нуля.

   Процесс восстановления порядка следования принимаемых из GRE-туннеля IP-датаграмм иллюстрирует Рис. 2.32.

   Рис. 2.32 Иллюстрация работы механизма восстановления порядка следования принимаемых GRE-пакетов

   Пакеты 3 и 4, пришедшие раньше пакета 2, отправляются в буфер, задерживаются там до прихода пакета 2 и вставляются в поток поступивших пакетов после пакета 2.

   Размер буфера – параметр задает размер приемного буфера, определяемый числом GRE-пакетов, которое этот буфер сможет принять без переполнения. Параметр определяет глубину смешивания (в единицах пакетов), т.е. то отставание, при котором порядок следования входящих пакетов (принимаемых из GRE-туннеля) еще может быть восстановлен. Параметр подбирается эмпирическим путем. В приведенном примере (Рис. 2.32) значение параметра **Размер буфера** должно быть не меньше *2*.

   Максимальная задержка пакетов – параметр задает допустимое время (в миллисекундах) пребывания пакета в приемном буфере. По истечении указанного параметром времени даже в случае, когда запаздывающий пакет не появился, ожидающие его пакеты будут переданы на дальнейшую обработку из GRE-туннеля.

3. Настройка группы параметров **Контроль состояния туннеля** (Рис. 2.31). Параметры этой группы настраивают режим работы механизма автоматического самоконтроля состояния GRE-туннеля – KEEPALIVE.

   Интервал отправки запросов – параметр задает интервал (в секундах) отправки контрольных зондирующих пакетов в GRE-туннель.

   Максимальное время ожидания ответов – параметр задает допустимое время (в секундах) ожидания ответа. Это время должно превышать интервал отправки запросов (обычно в 2-3 раза).

   Отправка контрольного пакета и получение ответа за заданное параметрами время свидетельствует о том, что GRE-туннель активен, иначе – нет. При нулевом значении параметров контроль состояния туннеля не производится, и он считается всегда активным. «Туннель активен» – это означает, что в общей таблице маршрутов изделия присутствует маршрут этого GRE-туннеля.

   > *Замечание*. Имена интерфейсов в списке сетевых интерфейсов (см. Рис. 2.39, с. 52) и в окне оперативного контроля состояния интерфейсов (см. Рис. 2.47, с. 56) выводятся разными цветами (см. раздел 2.6, с. 52) в зависимости от того, установлен или не установлен режим автоматического самоконтроля состояния интерфейса.

2.4.4. *L2–VLAN-интерфейсы*

В случае применения изделия в качестве средства организации L2-криптомостов полезным и эффективным может оказаться применение поддерживаемых изделием виртуальных L2–VLAN-интерфейсов (подробнее см. раздел ***Приложение В***, с. 230).

2.4.4.1. Общие сведения

Как отмечалось выше (см. раздел 2.4, с. 36), L2–VLAN-интерфейсы относятся к разряду сетевых *виртуальных* интерфейсов, связанных с сетевыми физическими интерфейсами типа **L2-Eth** (см. раздел 2.3.2, с. 33) как с *базовыми*. Самостоятельное применение L2–VLAN-интерфейсов, как любых других виртуальных интерфейсов, невозможно, т.к. они не могут напрямую управлять работой Ethernet-адаптеров, осуществляющих непосредственное взаимодействие с каналами связи на физическом и канальном уровнях.

Из поступающего на вход физического L2–Eth-интерфейса потока *тегированных* Ethernet-кадров (подробнее см. раздел 2.4.1.1, с. 36) выбираются кадры с тегом L2–VLAN-интерфейса и передаются ему на вход. L2–VLAN-интерфейс без обработки передает выбранные Ethernet-кадры связанному с ним L2–TNL-интерфейсу.

По тракту обработки криптотуннеля, образованного с помощью L2–TNL-интерфейса (см. раздел 2.4.5, с. 49), Ethernet-кадры попадают на БНМ удаленного изделия, извлекаются из криптотуннеля и в исходном виде передаются на интерфейс, связанный с L2–TNL-интерфейсом на приемной стороне, по которому и будут доставлены получателю.

Поэтому L2–VLAN-интерфейсы являются одним из средств организации L2-криптомостов при необходимости применения изделия для обеспечения удаленного защищенного обмена на L2-уровне по *нескольким* направлениям между сегментами ЛВС Пользователя, использующими для разграничения трафика Ethernet-кадров технологию VLAN.

> *Примечание*. Необходимые сведения о работе технологии VLAN приведены в разделе 2.4.1, с. 36 настоящего РНУ.

L2–VLAN-интерфейс применяется для организации функционирования L2-криптомостов только в связке с базовым физическим L2–Eth-интерфейсом и с L2–TNL-интерфейсом, обеспечивающим криптозащиту передаваемого между сегментами VLAN-сети трафика Ethernet-кадров.

2.4.4.2. Создание и настройка L2–VLAN-интерфейса.

Для создания L2–VLAN-интерфейса следует в меню выбора типа и принадлежности создаваемого интерфейса (см. Рис. 2.2, с. 23) установить курсор на альтернативу **L2-VLAN**, параметру, определяющему принадлежность интерфейса, установить значение **внутренний** и нажать клавишу <Esc>. В ответ на экран видеомонитора ЛКУ будет выдан бланк, представленный на Рис. 2.33.

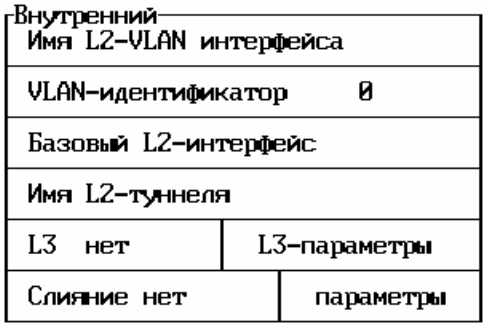


Рис. 2.33 Бланк создания и настройки L2–VLAN-интерфейса

Привязка L2–VLAN-интерфейса к другим интерфейсам технологической цепочки, реализующей выполнение функции L2-криптомоста, выполняется при настройке L2–VLAN-интерфейса установкой значений следующих параметров (Рис. 2.33):

- для связи с физическими L2–Eth-интерфейсами – через значение параметра **Базовый L2-интерфейс**;
- для связи с виртуальным L2–TNL-интерфейсами – через значение параметра **Имя L2-туннеля**.

Имя L2-VLAN интерфейса (Рис. 2.33) – имя сетевого L2–VLAN-интерфейса; значением параметра может быть до 7-ми любых символов, идентифицирующих интерфейс.

VLAN-идентификатор (Рис. 2.33) – целое десятичное число в диапазоне от ***0*** до ***4095***, идентификатор VLAN-сети (VNID), значение которого задает администратор (с помощью параметра **VLAN-идентификатор** L2–VLAN-интерфейсу присваивается уникальное значение *тега*).

> Тегированные Ethernet-кадры будут извлекаться из общего потока Ethernet-кадров, поступающих в базовый физический L2–Eth-интерфейс, и передаваться на обработку тому из группы L2–VLAN-интерфейсов, связанных с базовым интерфейсом, тег которого совпадает с тегом Ethernet-кадра.

Базовый L2-интерфейс (Рис. 2.33) – при выборе альтернативы на видеомонитор ЛКУ будет выдан список физических L2-интерфейсов внутреннего маршрутизатора, аналогичный представленному на Рис. 2.34.

Рис. 2.34 Список физических L2-интерфейсов внутреннего маршрутизатора

В этом списке следует установить курсор на описатель того интерфейса, к которому как к *базовому* будет привязан создаваемый L2-VLAN-интерфейс, и нажать клавишу <Enter>. Имя выбранного интерфейса будет занесено в поле **Базовый интерфейс** бланка создания и настройки L2-VLAN-интерфейса (Рис. 2.33).

Имя L2-туннеля (Рис. 2.33) – имя сетевого виртуального интерфейса типа **L2-TNL** – логического туннельного интерфейса L2-уровня (подробнее см. раздел ***Приложение В***, с. 230); значением параметра могут быть до 7-ми любых символов, идентифицирующих туннельный интерфейс L2-уровня. Имя должно быть уникальным.

L3 (Рис. 2.33) – параметру можно присвоить значения *Да* или *Нет* (установить курсор на поле **L3** и последовательно нажимать клавишу <Enter>). Значение параметра указывает, будет ли при обработке трафика L2–VLAN-интерфейсом задействован механизм информационного взаимодействия со *службами* (*сервисами*) изделия на L3-уровне. При значении параметра *Да* службы (сервисы) изделия выполняют обработку трафика IP-датаграмм, адресованных им устройствами в составе ЛВС Пользователя (аналогичный механизм для физического L2–Eth-интерфейса подробно рассмотрен в разделе ***Приложение В***, с. 230).

L3-параметры (Рис. 2.33) – при выборе этого поля на видеомонитор ЛКУ выдается бланк настройки параметров *маршрутизации* L2–VLAN-интерфейса, аналогичный представленному на Рис. 2.35.

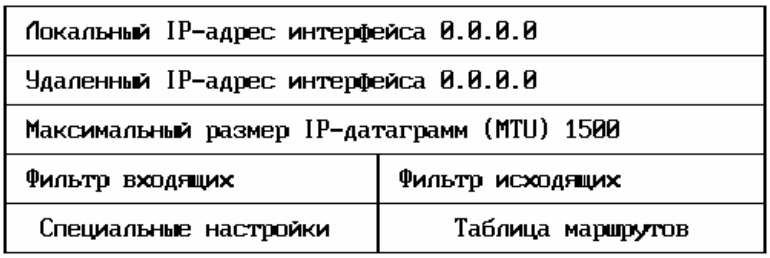


Рис. 2.35 Бланк настройки параметров маршрутизации L2–VLAN-интерфейса для обработки трафика на L3-уровне

Назначение параметров и процедуры настройки всех полей бланка, представленного на Рис. 2.35**,** рассматривались ранее при описании аналогичных полей бланка создания и настройки физического интерфейса типа **Ethernet**, представленного на Рис. 2.4, с. 25.

Настройку параметров маршрутизации L2–VLAN-интерфейса с помощью бланка настройки, представленного на Рис. 2.35, следует выполнять в соответствии с рекомендациями, приведенными при описании процедур настройки аналогичных параметров при создании и настройке физического интерфейса типа **Ethernet** (см. раздел 2.3.1, с. 25).

По завершении процесса настройки с помощью этого бланка L2–VLAN-интерфейс приобретает все атрибуты маршрутизации, необходимые интерфейсу для обеспечения обработки части проходящего через него *входящего* трафика на L3-уровне (аналогичный механизм для физического L2–Eth-интерфейса подробно рассмотрен в разделе ***Приложение В***, с. 230).

Слияние (Рис. 2.33) – параметр позволяет задать наличие/отсутствие реализации L2–VLAN-интерфейсом алгоритма *фрагментирования-слияния* Ethernet-кадров, поступающих из сети на порт Ethernet-адаптера того физического L2–Eth-интерфейса, который является базовым для настраиваемого L2–VLAN-интерфейса. Если установить курсор на альтернативу и последовательно нажимать клавишу <Enter>, будут последовательно выведены значения: **нет**, **ПРОГР.**, **АППАР.** L2–VLAN-интерфейс является виртуальным, поэтому при его работе возможна реализация алгоритма *фрагментирования-слияния* только на программном уровне, т.е. возможны только два значения параметра: **нет** − алгоритм фрагментирования-слияния применен не будет; **ПРОГР.–** будет применен алгоритм, реализованный на программном уровне.

Параметры (Рис. 2.33) – при выборе этого поля и при значении параметра **Слияние ПРОГР.** появляется бланк настройки параметров работы алгоритма *фрагментирования-слияния* Ethernet-кадров на программном уровне, аналогичный представленному на Рис. 2.36.

Максимальный размер контейнера	1448
Подлежат слиянию кадры короче	512
Ограничение количества сливаемых кадров	3

Рис. 2.36 Бланк настройки параметров работы алгоритма слияния Ethernet-кадров L2–VLAN-интерфейсом

Настройка параметров бланка, представленного на Рис. 2.36, выполняется согласно рекомендациям, приведенным при описании настройки аналогичных параметров L2–Eth-интерфейса (см. раздел 2.3.2, Рис. 2.18, с. 35).

2.4.5. ***L2–TNL-интерфейсы***

Общие сведения. В рамках технологии DioNIS® администратору предоставлена возможность применения нескольких *видов* криптотуннелей, создаваемых с помощью разных инструментов (подробнее о видах криптотуннелей и способах их организации см. раздел 3.1, с. 73).

L2–TNL-интерфейсы являются инструментом, применяемым в изделиях нового поколения в качестве инструмента для передачи *Ethernet-кадров* между БВМ и БНМ изделия через его шифратор.

Самостоятельное применение L2–TNL-интерфейсов, как любых других виртуальных интерфейсов, невозможно, т.к. они не могут напрямую управлять работой портов Ethernet-адаптеров, поэтому L2–TNL-интерфейсы применяются только в связке с *базовыми* физическими L2–Eth-интерфейсами. С помощью L2–TNL-интерфейсов осуществляется функционирование защищенного `bridge`-соединения для передачи между удаленными сегментами ЛВС Пользователя трафика Ethernet-кадров – *L2-криптомоста*. При этом защищенное взаимодействие удаленных сегментов ЛВС Пользователя на L2-уровне обеспечивается так, как если бы эти сегменты ЛВС были бы соединены простым Ethernet-кабелем.

При необходимости организации с помощью изделия нескольких *L2-криптомостов* по разным направлениям обмена L2–TNL-интерфейсы применяются в связке не только с физическими L2–Eth-интерфейсами, но и с виртуальными L2–VLAN-интерфейсами.

Возможны два варианта применения изделиями L2–TNL-интерфейса для организации защищенного обмена через сети общего пользования:

- для организации L2-криптомоста между сегментами ЛВС Пользователя на одном направлении обмена – в связке с базовыми физическими L2–Eth-интерфейсами;
- для организации необходимого количества L2-криптомостов между сегментами ЛВС Пользователя на нескольких направлениях обмена − в связке с базовыми физическими L2–Eth-интерфейсами и виртуальными L2–VLAN-интерфейсами.

> Подробнее об организации функционирования L2-криптомостов между сегментами ЛВС Пользователя на L2-уровне см. раздел ***Приложение В***, с. 230.

Создание и настройка L2–TNL-интерфейса. Чтобы создать L2–TNL-интерфейс, следует в меню выбора типа и принадлежности создаваемого интерфейса (Рис. 2.2, с. 23) выбрать альтернативу **L2–TNL**, установить параметру, определяющему принадлежность интерфейса, значение *общий* и нажать клавишу <Esc>. В ответ на видеомонитор ЛКУ будет выдан бланк, представленный на Рис. 2.37.

Имя интерфейса	Таблица маршрутов
Идентификатор туннеля 0	
Локальный IP-адрес интерфейса 0.0.0.0	
Удаленный IP-адрес интерфейса 0.0.0.0	
Шифрование потока (0)0.0->0 [vMПМ]	
Максимальный размер IP-датаграмм (MTU) 1500	
Фильтр входящих	Фильтр исходящих
Специальные настройки	Дополнительные параметры

Рис. 2.37 Бланк создания и настройки L2–TNL-интерфейса

Состав полей бланка создания и настройки L2–TNL-интерфейса полностью совпадает с форматом бланка создания и настройки TNL-интерфейса, представленного на Рис. 2.22.

Для L2–TNL-интерфейсов перечисленные ниже поля бланка неактивны и настройке не подлежат:

- **Таблица маршрутов**,
- **Максимальный размер IP-датаграмм (MTU)**,
- **Фильтр входящих**, **Фильтр исходящих**,
- **Специальные настройки**.

Остальные поля бланка L2–TNL-интерфейса заполняются так же, как аналогичные поля бланка TNL-интерфейса (см. раздел 2.4.2, с. 39).

Примечание. Обработка значений дополнительных параметров L2–TNL-интерфейса **Скорость передачи** и **Скорость приема** настоящей версией ОПО изделия не поддерживается.

2.5. Специальные настройки интерфейсов

Большинство сетевых интерфейсов изделия имеет набор параметров, устанавливающих ограничения обработки данных, проходящих через интерфейс. Все эти параметры-ограничители могут быть настроены при выборе альтернативы **Специальные настройки** в соответствующих бланках создания и настройки этих интерфейсов.

Как отмечалось выше (раздел 2.3.1, с. 25), на начальном этапе настройки сетевого интерфейса (независимо, физического или виртуального) всем параметрам, настраиваемым с помощью альтернатив **Специальные настройки** бланков создания и настройки интерфейсов, следует первоначально присвоить значения, приведенные на Рис. 2.38. Если справа от параметра стоит символ «*» (*звездочка*), то параметр имеет значение *ДА*, если символ «*» отсутствует, то параметр имеет значение *Нет*.

На Рис. 2.38 приведена копия бланка управления параметрами альтернативы **Специальные настройки**, представленного на Рис. 2.8 (с. 28) – формат этого бланка универсален при настройке сетевого интерфейса любого типа и вида.

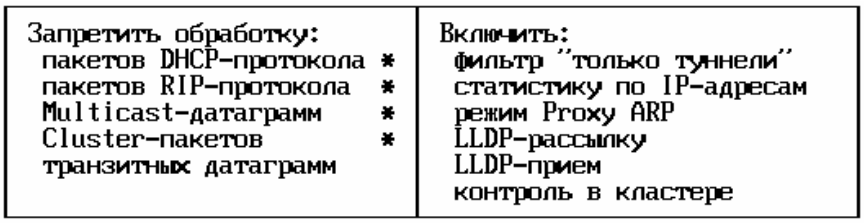


Рис. 2.38 Бланк управления специальными настройками интерфейса

После полной настройки и проверки функционирования сетевого интерфейса следует приступить к вводу ограничений проходящего через интерфейс трафика, требуемых при штатной эксплуатации изделия, с помощью бланка управления специальными настройками.

Бланк содержит две группы параметров – **Запретить обработку** и **Включить**.

1. Параметры группы **Запретить обработку:**.

пакетов DHCP-протокола (Рис. 2.38). Маршрутизаторы изделия обеспечивают обработку DHCP-запросов (см. раздел 5.5, с. 161), приходящих на любой сетевой интерфейс изделия. Если требуется отказаться от обслуживания приходящих из сети DHCP-запросов, то при настройке интерфейса, обеспечивающего связь с этой сетью, следует этому параметру присвоить значение *ДА*. Другими словами, если параметру присвоено значение *ДА*, то все DHCP-запросы, пришедшие по этому интерфейсу, будут изделием проигнорированы.

пакетов RIP-протокола (Рис. 2.38**).** Маршрутизаторы изделия обеспечивают необходимую обработку RIP-пакетов со сведениями об изменениях в маршрутных таблицах маршрутизаторов среды окружения изделия, приходящих из сопряженных сетей на любой интерфейс изделия (подробнее см. раздел 5.7, с. 165). Если требуется проигнорировать приходящие через настраиваемый интерфейс RIP-пакеты, следует присвоить этому параметру значение ***ДА***. Если необходимо в динамике корректировать маршрутную таблицу настраиваемого интерфейса изделия по информации RIP-пакетов, приходящих от маршрутизаторов сетей, доступных через настраиваемый интерфейс, следует присвоить этому параметру значение ***Нет***.

Multicast-датаграмм (Рис. 2.38). В составе изделия имеются средства обработки **MULTICAST**-датаграмм Ethernet-интерфейсами (подробнее о **MULTICAST**-адресации в IP-сетях см. раздел 2.8, с. 60). Настраивая параметр, можно включить или выключить эти средства обработки на данном интерфейсе. Установка значения ***ДА*** блокирует работу с **MULTICAST**-датаграммами, циркулирующими через настраиваемый интерфейс. Значение ***Нет*** обеспечивает штатную обработку интерфейсом циркулирующих через него **MULTICAST**-датаграмм.

Cluster-пакетов (Рис. 2.38). В изделии реализована возможность организации его функционирования в составе кластера (подробнее см. раздел 7, с. 174). Для обмена технологической

информацией между изделиями, функционирующими в составе кластера, используются специальные технологические *пакеты-извещения*. Эти пакеты могут быть отправлены по всем физическим интерфейсам (для организации передачи *пакетов-извещений* по интерфейсу следует присвоить параметру значение ***Нет***). Если параметру присвоить значение ***ДА***, то через интерфейс *пакеты-извещения* передаваться не будут.

транзитных датаграмм (Рис. 2.38). Если параметру присвоить значение ***ДА***, то все датаграммы, пришедшие на этот интерфейс, могут быть переданы только внутренним службам (сервисам) соответствующего маршрутизатора изделия. Датаграммы, которые должны быть переданы на другие интерфейсы, отбрасываются, т.е. *транзит* датаграмм, принятых по этому интерфейсу, не выполняется.

2. Параметры группы **Включить**.

фильтр "только туннели" (Рис. 2.38). Если параметру присвоено значение ***Нет***, то будут обрабатываться *все* датаграммы, проходящие через данный интерфейс. Если присвоить параметру значение ***ДА***, то будут обрабатываться *только туннелированные* датаграммы, проходящие через данный интерфейс, остальные будут отброшены. Это является одним из средств сокрытия узла со стороны других узлов сетей с целью обеспечения мер повышенной безопасности.

> *Внимание!* Возможность пропускать через интерфейс только туннелированные датаграммы нужна для организации функционирования виртуальных частных сетей (VPN). При этом, если параметру присвоено значение ***ДА***, то интерфейс может использоваться исключительно для передачи туннелированного трафика; если же интерфейс используется и для других целей (например, для передачи транзитного трафика или для передачи потока управления), то параметру следует установить значение ***Нет***.

статистику по IP-адресам (Рис. 2.38). Если параметру присвоено значение ***ДА***, сервисы изделия начинают анализировать объем проходящего через интерфейс IP-трафика (входящего и исходящего) с разбивкой датаграмм по IP-адресам. Статистика трафика по IP-адресам заносится в оперативную память, откуда она автоматически переносится в журнал (файл **LOG.EMA**) при завершении сеанса работы изделия или после выбора цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ IP-статистика** (см. раздел 9.2.6, с. 191).

режим PROXY ARP (Рис. 2.38). Протокол ARP (Address Resolution Protocol) обеспечивает автоматическое определение MAC-адреса доставки IP-датаграммы в среде локальной сети по IP-адресам назначения датаграмм. Условия и алгоритм обработки ARP-запросов для всех интерфейсов соответствующего маршрутизатора изделия задаются при выборе цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Параметры TCP/IP ⇨ Разрешена работа PROXY-ARP** (см. раздел 4.1.2, с. 130). Рассматриваемый параметр специальной настройки позволяет установить эти условия и алгоритм обработки ARP-запросов для отдельного интерфейса *индивидуально*.

LLDP-рассылку (Рис. 2.38). Протокол канального уровня LLDP (Link Layer Discovery Protocol) позволяет сетевому оборудованию оповещать локальную сеть о своем существовании и своих характеристиках, а также собирать такие же оповещения, поступающие от соседнего оборудования среды окружения. При значении параметра ***ДА*** включается автоматическая рассылка интерфейсом изделия *оповещений* согласно протоколу LLDP. Если параметр имеет значение ***Нет***, рассылка LLDP-оповещений интерфейсом изделия не выполняется.

LLDP-прием (Рис. 2.38**)**. При значении параметра ***ДА*** интерфейс изделия автоматически выполняет прием и соответствующую обработку LLDP-оповещений от соседних узлов. Если параметр имеет значение ***Нет***, прием и обработка LLDP-оповещений соседних узлов сети не выполняются.

> *Замечание*. В бланках настройки *туннельных* интерфейсов типа TNL и GRE два последних параметра – **Включить: LLDP-рассылку** и **Включить: LLDP-прием** – не активны.

контроль в кластере (Рис. 2.38). Если для интерфейса установлен такой контроль (параметр имеет значение ***ДА***), то при отключении (потере активности) такого интерфейса основное изделие в составе кластера (**MASTER**) будет считаться вышедшим из строя и обработку трафика продолжит резервное изделие в составе кластера (**SLAVE**).

Контролировать рекомендуется наименее надежные интерфейсы.

Примечания:

1. Контролировать можно несколько интерфейсов любого типа, но не следует включать функцию **контроль в кластере** *одновременно* в физическом интерфейсе (Ethernet) и связанном с ним (явно или опосредованно) туннельном интерфейсе (TNL, GRE).
2. Если предполагается задействовать функцию **Включить: контроль в кластере** в *туннельном* интерфейсе, то при настройке этого интерфейса должен быть установлен контроль за состоянием туннеля (параметр **Контроль состояния** (**туннеля**) из набора параметров, доступных при использовании бланков создания и настройки туннельных

интерфейсов всех видов через альтернативу **Дополнительные параметры** (подробнее см. разделы 2.4.2, с. 39, 2.4.3, с. 43 и 2.4.5, с. 49).

3.

2.6. Средства оперативного контроля состояния интерфейсов

В изделии реализованы средства, предоставляющие обслуживающему персоналу возможность оперативно вывести на видеомонитор ЛКУ диагностическую информацию, отображающую текущее состояние *активных* (находящихся в работе) сетевых интерфейсов маршрутизатора изделия, а также возможность оперативного выполнения отдельных операций с интерфейсами (сбор сведений о их текущем состоянии, сброс и пр.).

Список активных сетевых интерфейсов и TCP-портов изделия выводится на видеомонитор ЛКУ при выборе альтернативы ГМ **Интерфейсы**. Пример списка представлен на Рис. 2.39.

Примечание. В списке отсутствуют *заблокированные* интерфейсы – те интерфейсы, которые *временно* отключены администратором (подробнее см. раздел 2.2, с. 21, Рис. 2.1, с. 22, описание команды **Админ. статус: F5**).

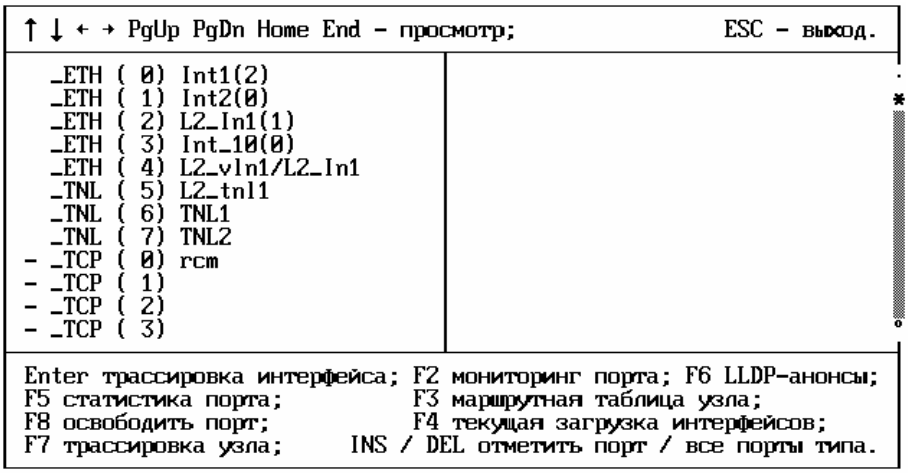


Рис. 2.39 Список активных сетевых интерфейсов и TCP-портов маршрутизатора

Каждая строка списка содержит описание активного сетевого интерфейса или TCP-порта. Сначала указывается *тип* интерфейса или порта, затем (в круглых скобках) – *порядковый номер* в списке (нумерация сверху вниз). После порядкового номера в строке указываются:

- для сетевых интерфейсов – *имя*; для физических интерфейсов (типа **Ethernet** или **L2-Eth**) в круглых скобках дополнительно приводится *номер порта*, указываемый при настройке физических интерфейсов изделия (см. раздел 2.3, с. 25).
- для TCP-портов – *имя абонента*, работающего через этот порт в данный момент.

Цвет, которым выводится строка с описанием интерфейса, характеризует тип интерфейса и его текущее состояние:

- *белый цвет* – Ethernet-интерфейс или L2-Eth-интерфейс находится в активном (работоспособном) состоянии;
- *серый цвет* – Ethernet-интерфейс или L2-Eth-интерфейс находится в неактивном состоянии (отсутствует несущая, интерфейс неработоспособен);
- *серый цвет* в *мигающем* режиме – TNL-интерфейс или L2–TNL-интерфейс в случае, когда реализованный с его помощью туннель находится в состоянии *не открыт* (см. раздел 3.1.3); адекватное состояние туннельных интерфейсов отображается только при просмотре списка с применением средств ЛКУ, подключенных к БВМ изделия;
- *зеленый цвет* – TNL-интерфейс или L2–TNL-интерфейс находится в активном состоянии;
- *желтый цвет* – TNL-интерфейс или L2–TNL-интерфейс находятся в неактивном состоянии, при этом контроль состояния туннельного интерфейса *включен*; адекватное состояние туннельных интерфейсов отображается только при просмотре списка с применением средств ЛКУ, подключенных к БВМ изделия;
- *желтый цвет* в *мигающем* режиме – TNL-интерфейс или L2–TNL-интерфейс находится в состоянии *не открыт*, контроль состояния интерфейса включён; состояние отображается только при просмотре из БВМ;
- *голубой цвет* – VLAN-интерфейс или L2-VLAN-интерфейс находится в *активном* состоянии;
- *синий цвет* – VLAN-интерфейс или L2-VLAN-интерфейс находится в *неактивном* состоянии;

- *малиновый цвет* – GRE-интерфейс:

  - при включённом контроле состояния туннеля – интерфейс находится в *активном* состоянии;

  - при выключенном контроле состояния туннеля, вне зависимости от состояния интерфейса;

- *оранжевый цвет* – GRE-интерфейс находится в неактивном состоянии при включённом контроле состояния GRE-интерфейса;

- *красный* – TCP-порт, через который осуществляется сеанс удаленного подключения к маршрутизатору изделия (удаленного управления).

Нижняя часть экрана (Рис. 2.39) содержит подсказки, информирующие о том, какие управляющие операции можно выполнить, используя экран со списком активных интерфейсов.

Enter – трассировка интерфейса (Рис. 2.39). Нажатие клавиши <Enter> позволяет изменить режим трассировки того интерфейса, на строку с именем которого установлен курсор в списке. В ответ на видеомонитор ЛКУ будет выдан представленный на Рис. 2.40 бланк оперативного управления режимом трассировки выбранного интерфейса, позволяющий задать объем и формат вывода информации о передаваемых интерфейсом IP-датаграммах и кадрах, а также уровень ее детализации. Кроме того, можно установить режим *трассировки фильтров*; при этом будут отслеживаться результаты работы фильтров при прохождении каждой датаграммы через данный интерфейс.

Установка знака «+» (*плюс*) справа от необходимой альтернативы включает требуемый вид трассировки; установка знака «-» (*минус*) процесс трассировки оперативно выключает. Для смены одного знака на другой надо перевести курсор на строку с нужным режимом трассировки и нажать клавишу <Enter>.

```
Режимы трассировки интерфейса
            Ext1

Анализ на уровне канала     -
Анализ IP и ARP             -
Анализ TCP, UDP и ICMP      -
Шестнадцатеричный DUMP      -
Трассировка фильтров        -
Расширенные сведения        -
```

Рис. 2.40 Бланк оперативного управления режимом трассировки интерфейса

Установленный режим трассировки интерфейса будет действовать только до перезапуска программы управления функционированием маршрутизатора или до изменения режима трассировки.

> *Примечание.* Подробнее о возможностях диагностирования качества функционирования изделия с помощью механизма трассировки см. раздел 4.1.3, с. 131.

F5 – **статистика порта** (Рис. 2.39). Программа управления изделием обеспечивает сбор статистики работы сетевого интерфейса маршрутизатора и позволяет просмотреть и обнулить результаты сбора статистики по команде обслуживающего персонала.

После нажатия клавиши <F5> на видеомонитор ЛКУ будет выдана статистическая информация (с момента запуска изделия или с момента сброса счетчиков сбора статистики) о работе того интерфейса, на строку описания которого в списке (Рис. 2.39) установлен курсор.

Характеристики интерфейсов и статистические данные выдаются на видеомонитор в форматах, зависящих от *типа* интерфейсов. На Рис. 2.41 представлены два примера выдачи сведений о характеристиках и статистике работы: для физического Ethernet-интерфейса и для виртуального TNL-интерфейса.

Пример сбора статистики для Ethernet-интерфейса:

```
                    Ext4
                Данные платы
Плата: номер  0 адрес fba01000/11 версия 32.50x1g1
Интерфейс: AUTO-TX AUTO (100 FULL)
MAC-адрес: 00-fc-e1-00-00-39      Температура 0
Флаги состояния: 8003 0001 LUp MMIO

              Статистика работы
Получено 313              Отправлено 45130
Ошибок приема 0           Ошибок передачи 145
   типа кадра 66
   MAC-адреса 0
         Мгновенная скорость (Кбит/с.)
Прием  0.0                Передача  0.0
-------------------------------------------------
Пробел - расширенные данные; 0 - сброс статистики;
       s - просмотреть параметры SFP-модуля.
```

Пример сбора статистики для TNL-интерфейса:

```
                    tnl1
Туннель [1 10.1.1.2->10.1.1.1] TNL

Криптография (1)1001.1->2 vMПМ

Номера: передачи 36332(с 0.488)
         приема 0(с 0.494)
Контроль

         Мгновенная скорость (Кбит/с.)
Прием  0.0                Передача  0.0
-------------------------------------------------
              0 сброс статистики.
```

Рис. 2.41 Примеры выдачи сведений о характеристиках и статистике работы интерфейсов

Примечание. Некоторые форматы выдачи позволяют получить дополнительную информацию об интерфейсе. В частности, для Ethernet-интерфейса можно просмотреть: расширенные данные об интерфейсе, нажав клавишу «*пробел*»; параметры SFP-модуля, если он имеется и задействован в изделии, нажав клавишу <S>.

F8 – **освободить порт** (Рис. 2.39). Нажатие клавиши <F8> является исполняемой командой, позволяющей (после предварительного запроса и подтверждения) принудительно освободить TCP-порт.

F7 – **трассировка узла** (Рис. 2.39). При нажатии клавиши <F7> на видеомонитор ЛКУ выдается бланк управления параметрами трассировки компонентов изделия (Рис. 4.4, с. 132). Возможности управления режимами трассировки, предоставляемые с его помощью, подробно рассмотрены в разделе 4.1.3, с. 131.

Примечание. Установленные с помощью альтернативы **F7** – **трассировка узла** режимы трассировки действуют только до перезапуска изделия или до явной отмены этих режимов.

F2 – **мониторинг порта** (Рис. 2.39). Нажатие клавиши <F2> приводит к появлению в нижней части экрана окна, в которое по мере выполнения обмена через выбранный в списке TCP-порт выдаются сведения об этом обмене.

Примечание. Мониторинг включается только для TCP-портов.

F6 – **LLDP-анонсы** (Рис. 2.39). При нажатии клавиши <F6> на видеомонитор ЛКУ выводится аналогичный представленному на Рис. 2.42 список LLDP-анонсов для интерфейса, если включены режимы автоматической рассылка и/или приема LLDP-анонсов (подробнее о LLDP-анонсах см. раздел 4.2.4, с. 150).

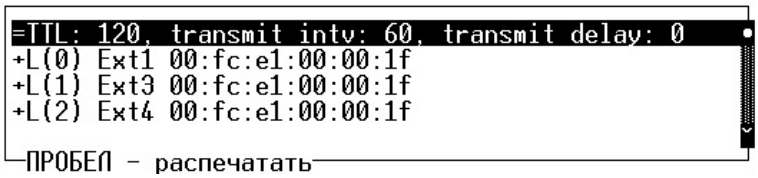


Рис. 2.42 Пример выдачи списка LLDP-анонсов для интерфейса

F3 – маршрутная таблица узла (Рис. 2.39). При нажатии клавиши <F3> на видеомонитор ЛКУ выводится аналогичный представленному на Рис. 2.43 экран с маршрутной таблицей маршрутизатора. Формируются описатели в составе маршрутной таблицы из трех источников: копируются из маршрутных таблиц интерфейсов (см. раздел 2.3.1, с. 25); автоматически добавляются протоколами динамической маршрутизации; при задании маски подсети локального IP-адреса в процессе настройки интерфейса (см. раздел 2.3.1, с. 25).

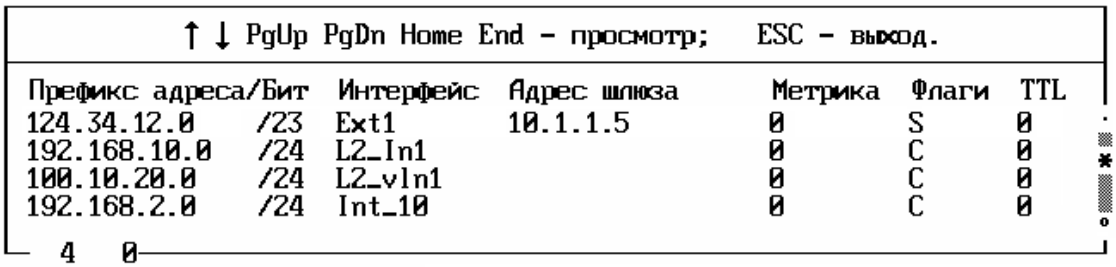


Рис. 2.43 Экран с маршрутной таблицей маршрутизатора

Для каждого маршрута его описатель указывает:

- **Префикс адреса** – IP-адрес;
- **Бит** – число значащих бит в адресе подсети – длина маски подсети;
- **Интерфейс** – имя интерфейса;
- **Адрес шлюза** – IP-адрес шлюза;
- **Метрика** – метрика маршрута;
- **Флаги** – тип маршрута: S – статический маршрут – прописанный в маршрутной таблице интерфейса с указанием адреса шлюза; C – connected-маршрут – маршрут непосредственного подключения к сети, созданный при задании маски подсети для локального IP-адреса в процессе заполнения бланка настройки интерфейса, или явно прописанный в маршрутной таблице интерфейса без указания адреса шлюза; R – маршрут, созданный протоколом динамической маршрутизации – RIP;
- **TTL** – время жизни маршрутной записи.

Примечание. В маршрутной таблице не будут отображены маршрутные записи, если:

- маршрут, контроль доступности которого с помощью соответствующей PING-пробы дает отрицательный результат (см. раздел 2.7, с. 58.);
- косвенный статический маршрут принадлежит интерфейсу, контроль активности которого с помощью соответствующей PING-пробы дает отрицательный результат (см. раздел 2.7.4, с. 60);
- маршрут принадлежит GRE, TNL или L2-TNL-интерфейсу, который на основании встроенного контроля признан системой неактивным (2.7.3, с. 60).

На нижней рамке маршрутной таблицы слева указаны два десятичных числа: первое указывает количество статических записей в маршрутной таблице; второе – количество **multicast**-адресов (см. раздел 2.8, с. 60).

F4 – текущая загрузка интерфейсов (Рис. 2.39). При нажатии клавиши <F4> на видеомонитор ЛКУ выводится аналогичная представленной на Рис. 2.44 таблица с данными для каждого сетевого активного интерфейса на текущий момент времени: мгновенная *скорость* при приеме и передаче через интерфейс, *трафик* за время от момента включения или от момента обнуления статистики и *число ошибок* за то же время. Значения этих параметров приведены в таблице построчно для каждого из *активных* интерфейсов, имена которых приведены в колонке **Имя**.

Имя	Скорость (Кбит/с)		Трафик (Мбайт)		Счетчики ошибок	
	Прием	Передача	Прием	Передача	Прием	Передача
Ext1	1.6	1.4	0.08	0.12	0	5
Ext3	1.0	1.0	0.03	0.03	0	39
Ext4	0.4	0.2	0.00	0.01	0	3
t2222	0.0	0.0	0.00	0.00	0	0
t1	0.0	0.0	0.00	0.00	0	0
GRE o	0.8	0.0	0.02	0.00	0	0

F8 – сбросить счетчики ошибок, F5 / F6 – показать статистику,
' ' – расширенная информация, 'c' – статистика шифратора.

Рис. 2.44 Таблица данных активных интерфейсов изделия

Используя подсказки в нижней части таблицы, можно уточнить статистические данные о работе каждого из интерфейсов, установив курсор на строку с именем конкретного интерфейса.

F8 – сбросить счетчики ошибок (Рис. 2.44). При нажатии клавиши <F8> выполняется сброс (установка в ноль) значений всех приведенных в таблице статистических параметров.

F5 – показать статистику (Рис. 2.44). При нажатии клавиши <F5> будет выдана та же информация о работе интерфейса, которая выводится при выполнении операции **F5 – статистика порта** (см. Рис. 2.41).

F6 – **показать статистику** (Рис. 2.44). При нажатии клавиши <F6> будет выдана статистическая информация, сгруппированная по *приоритетам* (QoS) в формате, представленном на Рис. 2.45.

Ext1

	Скорость	Окно
Передача	1028	10240
Прием	0	10240

#	Передано	Сброшено	Ждут	Ошибок
0	46	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0

0 – сброс статистики.

Рис. 2.45 Таблица статистики работы интерфейса, сгруппированная по приоритетам QoS

' ' – расширенная информация (Рис. 2.44). При нажатии клавиши <пробел> будет выдана расширенная информация о работе выбранного в таблице интерфейса.

«C» – статистика шифратора (Рис. 2.44). При нажатии клавиши <C> будет выдана в представленном на Рис. 2.46 виде статистическая информация о работе шифратора изделия.

Рис. 2.46 Статистическая информация о работе шифратора

INS/DEL – отметить порт/все порты типа (Рис. 2.39). Для удобства администратора реализована возможность отобрать имена отдельных (или всех) интерфейсов и портов, требующих особого внимания или более пристального (непрерывного) наблюдения. Отобранные интерфейсы будут автоматически отображаться в окне оперативного контроля состояния интерфейсов (см. далее в этом разделе Рис. 2.47, с. 56).

В общем списке активных интерфейсов (Рис. 2.39) во всех строках в первой позиции стоит *пробел* или знак «**-**» (*минус*). Все интерфейсы, перед именами которых *нет* знака минус, будут отображены в окне оперативного контроля (Рис. 2.47, с. 56).

Чтобы изменить символ перед именем, следует в списке интерфейсов перевести курсор на строку с этим именем и нажать клавишу <Ins> – слева от имени появится знак «–» (*минус*). Повторное нажатие клавиши <Ins> знак уберет.

Нажатие клавиши <Del> приведет к появлению знака минус слева от имен всех интерфейсов того типа, на котором установлен курсор. Повторное нажатие клавиши <Del> знак уберет.

Замечание. Порты TCP можно отобрать в окно оперативного контроля только всей группой одновременно (так как их функционирование связано с работой одного − служебного интерфейса – *внутреннего* интерфейса маршрутизатора).

Окно оперативного контроля состояния интерфейсов

Окно оперативного контроля состояния интерфейсов находится в правой части экрана Главного меню программы управления функционированием изделия (см. Рис. 1.9, с. 16). В это окно (Рис. 2.47) выводится вертикально расположенный список имен сетевых интерфейсов и TCP-портов, отобранных обслуживающим персоналом для оперативного контроля.

Примечание. Отбор интерфейсов, состояние которых отображается в окне оперативного контроля, выполняется с помощью клавиш <Ins> или <Del> (см. Рис. 2.39, с. 52).

Для оперативного контроля интерфейсов может быть отобрана произвольная группа интерфейсов, требующих повышенного внимания обслуживающего персонала в данный момент, например: все интерфейсы или единственный интерфейс; все физические интерфейсы или интерфейсы только одного типа (например, только TNL-интерфейсы); только TCP-порты (последние могут содержать полезную информацию, например, при работе в режиме удаленного управления или при анализе работы различных служб изделия); конкретный L2-интерфейс; группа VLAN-интерфейсов или GRE-интерфейсов и т.д.

Для перехода в окно оперативного контроля с целью управления отобранными интерфейсами следует, находясь в Главном меню программы управления или в Главном меню подсистемы настройки, нажать клавишу <F1>. Для выхода из окна служит клавиша <Esc>, при этом возврат будет осуществлен в ту точку диалога с программой управления изделием, из которой ранее был выполнен переход в окно оперативного контроля.

Рис. 2.47 Окно оперативного контроля состояния интерфейсов

Окно содержит список интерфейсов и портов, отобранных для вывода в это окно из общего списка интерфейсов маршрутизатора, представленного на Рис. 2.39, с. 52. Список в окне оперативного контроля аналогичен представленному на Рис. 2.47 (цвета строк в этом окне соответствуют цветам строк, отображающих состояния интерфейсов в общем списке активных интерфейсов и TCP-портов − Рис. 2.39, с. 52).

В каждой строке окна оперативного контроля символ слева от имени интерфейса соответствует одному из следующих типов интерфейсов:

e – Ethernet-интерфейс или L2-Eth-интерфейс;
t – TNL-интерфейс или L2-TNL-интерфейс;
g – GRE-интерфейс;
v – VLAN-интерфейс или L2-VLAN-интерфейс;
a – TCP-порт.

Находясь в окне оперативного контроля, можно нажать клавишу <F1> – в ответ на экран будет выведен список всех операций (команд), которые доступны для выполнения в этом окне (см. Рис. 2.48). Некоторые из этих операций совпадают с рассмотренными выше операциями, доступными через экран списка активных интерфейсов и TCP-портов (см. Рис. 2.39, с. 52).

```
⇧⇩ PgUp PgDn Home End - просмотр;
ESC          - выход.
Пробел       - отметить интерфейс.
Enter        - расширенные сведения;
Ctrl+Enter   - трассировка интерфейса;
F2       - фильтр сессий;
F3       - фильтр входящих;
F4       - фильтр исходящих;
F5       - общая информация и статистика;
F6       - статистика работы QoS;
F7       - текущая загрузка;
F8       - таблица маршрутов интерфейса.
```

Рис. 2.48 Операции окна оперативного контроля

Управляющие клавиши (**⇧ ⇩ PgUp PgDn Home End**) служат для передвижения по списку интерфейсов и TCP-портов, клавиша<**Esc**> – для выхода из окна и возврата в основную часть экрана.

Пробел – **отметить интерфейс** (Рис. 2.48). Нажатие клавиши <пробел> позволяет отметить тот интерфейс, на имени которого установлен курсор. Слева от имени появляется символ «*****» (*звездочка*). Повторное нажатие клавиши отметку снимает. Отмеченные таким способом интерфейсы будут выводиться на экран по команде **F7** – **текущая загрузка** (см. ниже).

Замечание. Отметить можно любое число сетевых интерфейсов маршрутизатора, TCP-порты отметить нельзя.

Enter – **расширенные сведения** (Рис. 2.48). При нажатии клавиши <Enter> на видеомонитор ЛКУ выводится сведения о конфигурационных параметрах интерфейса, статистические данные о скорости и объеме прошедшего через интерфейс трафика, об Ethernet-адаптере (для физических интерфейсов), о параметрах туннеля (для TNL-, GRE- или L2-TNL-интерфейсов) и некоторые другие сведения.

Замечание. Расширенные сведения можно получить только о сетевых интерфейсах (о TCP-портах – нельзя).

Ctrl+Enter – **трассировка интерфейса** (Рис. 2.48). Результат выполнения команды – появление на видеомониторе ЛКУ бланка управления режимом трассировки интерфейса (см. Рис. 2.40, с. 53) совпадает с результатом выполнения операции **Enter – трассировка**, выполняемой с помощью экрана списка всех сетевых интерфейсов и TCP-портов изделия, представленного на Рис. 2.39, с. 52).

Фильтры: F2-сессий, **F3-входящих**, **F4-исходящих** (Рис. 2.48). После нажатия одной из указанных клавиш (<F2>, <F3>, <F4>) на видеомонитор ЛКУ будет выдан соответствующий список правил фильтрации потока данных через интерфейс (если такой списки создан).

F5 – **общая информация и статистика** (Рис. 2.48). Результат совпадает с результатом операции **F5** – **статистика порта** (см. Рис. 2.41, с. 53).

F6 – **статистика работы QoS** (Рис. 2.48). Результат совпадает с результатом операции **F4** – **текущая загрузка интерфейсов ⇨ <F6>** (см. Рис. 2.45, с. 55).

F7 – **текущая загрузка** (Рис. 2.48). Результат совпадает с результатом операции **F4** – **текущая загрузка интерфейсов** (см. Рис. 2.44, с. 55).

F8 – **таблица маршрутов интерфейса** (Рис. 2.48). Результат совпадает с результатом операции **F3** – **маршрутная таблица узла** (см. Рис. 2.43, с. 54).

Приведем пример получения информации в окне оперативного контроля состояния интерфейсов.

```
──────────── Интерфейс Tnl1 ────────────┐
Имя: Tnl1 (Tnl1). Тип: TNL. MTU: 1500   ·
Локальный адрес: 10.1.1.2. Удаленный адрес: 10.1.1.1.  *

Интерфейс считается неактивным
Запрещена обработка пакетов DHCP-протокола
Запрещена обработка пакетов RIP-протокола
Запрещена обработка Multicast-датаграмм
Запрещена обработка Cluster-пакетов

Скорость приема: 0.0. Принято: 0.0 Мбайт.
Скорость передачи: 0.0. Передано: 0.0 Мбайт.

Туннель: [1 10.1.1.2->10.1.1.1] TNL
Описание:                                  °
└ ПРОБЕЛ - распечатать──────────────────────┘
```

Рис. 2.49 Пример экрана с оперативно полученными сведениями о настройках интерфейса с именем **Tnl1**

Пусть нас интересует информация о конкретном TNL-интерфейсе. Переходим из Главного меню программы управления изделием нажатием клавиши <F1> в окно оперативного контроля. Перемещаем курсор в списке имен и типов интерфейсов на строку с именем интерфейса, оперативное состояние которого мы хотим уточнить, и нажимаем клавишу <Enter>. В результате получим экран, аналогичный представленному на Рис. 2.49, содержащий интересующую нас информацию об интерфейсе с именем **Tnl1**.

Кроме того, если обслуживающему персоналу необходимо задокументировать эту оперативную информацию для последующего анализа, достаточно нажать клавишу <пробел>, после чего вся представленная на Рис. 2.49 информация об интерфейсе **Tnl1** будет записана в журнал регистрации событий изделия.

2.7. Механизм PING-проб и автоматизация управления сетевыми IP-ресурсами

Программа управления каждого из маршрутизаторов изделия поддерживает функционирование механизма PING-проб, который предполагает настройку (формирование заданий) и последующий запуск необходимого числа независимых процессов регулярной отправки зондирующих пакетов ICMP-протокола типа `Echo request` в адрес указанных при настройке PING-проб контролируемых IP-ресурсов сети с последующим анализом принятых от этих IP-ресурсов ответов в виде пакетов ICMP-протокола типа `Echo reply`.

Функционирование каждого из процессов PING-проб обеспечивается изделием в соответствии со стандартным для `internet/intranet`-технологии алгоритмом работы процедуры PING (подробное описание процедуры и ее параметров приведено в разделе 8.1.1, с. 178), но использование изделием результатов обработки ответов на PING-пробы отличается от принятого стандарта.

Возможности контроля и управления, предоставляемые применением механизма PING-проб, могут быть использованы в маршрутизаторах изделия для решения следующих задач управления ресурсами.

1. Контроль состояния доступности удаленных IP-ресурсов, взаимодействующих с маршрутизаторами изделий, и оценка характеристик быстродействия канала доступа к этим удаленным IP-ресурсам.
2. Управление текущим состоянием (*активизация* или *деактивизация*) записей маршрутных таблиц маршрутизаторов изделия в зависимости от результатов PING-проб.
3. Управление текущим состоянием функционирования (*активизация* или *деактивизация*) туннельных интерфейсов (GRE-туннелей, TNL-туннелей и L2-TNL-туннелей) в зависимости от результатов PING-проб (динамическое управление активностью поддерживаемых изделием туннелей).
4. Контроль работоспособности *физических* интерфейсов изделия типа **Ethernet** и **L2-Eth** и перевод их в зависимости от результатов PING-проб в состояние *активен* или *не активен* с *одновременной* (синхронной) активизацией или деактивизацией в маршрутных таблицах изделия маршрутных записей, соответствующих контролируемым интерфейсам.

Процесс PING-проб запускается сразу после завершения формирования задания на его выполнение. Если задание было сформировано в предыдущих сеансах работы изделия, то процесс PING-проб автоматически включается после запуска изделия.

Формирование задания на выполнение процесса PING-проб выполняется *двумя* описанными ниже способами в зависимости от решаемых задач.

1. Для решения перечисленных выше первых трех задач управления ресурсами процедура формирования задания на контроль описана в разделе 4.2.3, с. 148. В задании указывается IP-адрес удаленного узла, интервал времени между отправляемыми пакетами PING-проб и время ожидания ответа от удаленного узла. Кроме того, каждой PING-пробе присваивается *метка* – целое десятичное число в диапазоне от ***0*** до ***255***, необходимое для установления логической взаимосвязи между PING-пробой и соответствующим контролируемым ею ресурсом (для «*привязки*» маршрутной записи к конкретной PING-пробе).

   При решении первой и второй задач *такие же* значения меток присваиваются маршрутам при создании таблицы маршрутизации (см. раздел 2.3.1, с. 25). В результате организуется связь *маршрутов* конкретных интерфейсов с соответствующими PING-пробами.

   При решении третьей задачи *такие же* значения меток присваиваются туннелям (см. разделы 2.4.2, с. 39 (TNL-интерфейсы); 2.4.3, с. 43 (GRE-интерфейсы); 2.4.5, с. 49 (L2–TNL-интерфейсы); 3.1.1.2, с. 78 (статические криптотуннели). В результате организуется логическая взаимосвязь *туннелей* и соответствующих PING-проб.
2. Для решения четвертой задачи управления ресурсами формирование задания на запуск процесса PING-проб выполняется при настройке Ethernet-интерфейсов (см. раздел 2.3.1, с. 25) и L2-Eth-интерфейсов (см. раздел 2.3.2, с. 33). В этом случае в бланке настройки интерфейса параметру **Удаленный IP-адрес интерфейса** присваивается IP-адрес того устройства в локальной сети, которое будет использовано для тестирования интерфейса изделия (обычно – это ближайший шлюз). Параметрам Ping-пробы **Интервал отправки** и **Ожидание ответа** устанавливаются постоянные (неизменяемые) значения. Рекомендуемые значения соответственно 2 секунды и 5 секунд.

2.7.1. *Контроль доступности сетевых IP-устройств*

Информацию о доступности того или иного удаленного сетевого IP-устройства в составе ЗСПД обслуживающий персонал изделия может оперативно получать с помощью просмотра текущего состояния записей диагностической таблицы PING-проб маршрутизатора, аналогичной представленной на Рис. 2.50 (таблица выводится на видеомонитор ЛКУ при выборе цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие**

таблицы ⇨ PIng-пробы. Подробнее о параметрах и формате строк таблицы PING-проб см. раздел 9.3.8, с. 194.

В таблице отражается текущее состояние всех процессов PING-проб, организованных *обоими* (см. выше) способами формирования задания на выполнение процессов PING-проб.

Информация в записях таблицы PING-проб актуализируется непрерывно, и по показаниям счетчика (по разнице между числом посланных в сеть *проб* и *ответов* на них) можно определить, не выходил ли из строя удаленный сетевой IP-ресурс (например, за ночь). Если будет обнаружена разница (и параметр колонке под заголовком **%** получит значение, отличное от *100*), то персоналу следует просмотреть журнал изделия (файл **log.ema**), в котором фиксируются факты перехода удаленного IP-ресурса в недоступное для изделия состояние.

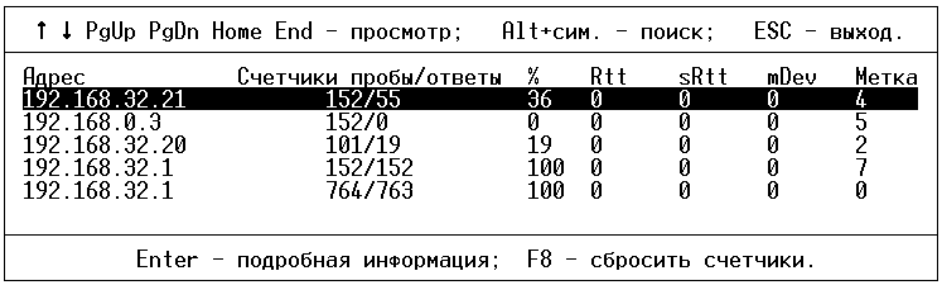


Рис. 2.50 Таблица текущего состояния записей PING-проб маршрутизатора изделия

Анализ фактов недоступности для изделия сетевых IP-устройств по результатам диагностики с помощью механизма PING-проб позволяет оценить стабильность работы оборудования сети, а также служит администратору сети исходной информацией для организации мероприятий по обеспечению работоспособности сети.

2.7.2. *Автоматизация управления маршрутизацией*

Автоматизация управления маршрутизацией обрабатываемого изделием трафика основана на применении механизма PING-проб, функционирование которого организовано следующим образом.

Изделие формирует ICMP-пакеты типа `Echo request` (зондирующие PING-запросы) и направляет их в адрес удаленного сетевого IP-устройства, состояние которого подлежит контролю. Пакеты-запросы регулярно формируются и посылаются через заданные при настройке PING-проб равные промежутки времени, определяемые значением параметра **Интервал отправки**.

Удаленное устройство, получив ICMP-пакет типа `Echo request`, обязано (согласно системным требованиям `internet/intranet`-технологии) послать в ответ ICMP-пакет типа `Echo reply` (PING-ответ). Если ответ приходит в течение заданного времени (регулируется значением параметра **Ожидание ответа** при настройке PING-пробы), то PING-проба оценивается программой управления изделием как *успешная*.

Каждой *PING-пробе* при ее настройке ставится в соответствие параметр – **Метка**. Такой же параметр присваивается каждой *маршрутной записи* сетевого интерфейса при его настройке. При совпадении значений параметров **Метка** у маршрутной записи и у PING-пробы говорят о *привязке* маршрутной записи к данной PING-пробе.

По окончании настройки PING-проб и *привязанных* к ним маршрутных записей автоматически запускаются процессы контроля доступности удаленных IP-устройств. В процессе контроля маршрутные записи, привязанные к успешным PING-пробам, остаются в маршрутной таблице маршрутизатора *актуальными*.

Если на отправленный в сеть зондирующий PING-запрос в указанное при настройке PING-пробы время ответ не приходит, PING-проба считается *неудачной*. Все маршрутные записи, привязанные к неудачной PING-пробе, будут помечены как *неактуальные* и при обработке трафика учитываться не будут. В составе маршрутной таблицы маршрутизатора неактуальные записи сохраняются. Посылка PING-проб в адрес удаленного IP-устройства при этом продолжается, и, если удаленное устройство в итоге ответит, маршрутные записи будут возвращены в маршрутную таблицу как актуальные.

Используя эти возможности механизма PING-проб, администратор изделия при создании и сопровождении таблицы маршрутизации может организовать маршруты через альтернативные (по отношению к основным) тракты передачи данных к одному и тому же удаленному IP-ресурсу, настраивая *резервные* маршруты и используя при этом для автоматического выбора оптимального из возможных на текущий момент маршрутов механизм PING-проб, оперирующий значениями *метрик* маршрутов и *меток* PING-проб.

> *Примечание.* В процессе настройки интерфейсов изделия выполняется формирование маршрутных записей маршрутизатора изделия (БВМ или БНМ). С помощью значения параметра **Метрика маршрута** задается приоритет, определяемый маршрутной записью; приоритет маршрутной записи учитывается маршрутизатором при поиске предпочтительного направления дальнейшего продвижения маршрутизируемого трафика (при совпадении в маршрутах IP-адресов подсетей получателей трафика).

Резервные маршруты при этом следует связать с разными PING-пробами, присвоив им разные *метки*. В результате рассмотренный механизм PING-проб при правильно организованной таблице маршрутизации и отлаженном наборе записей PING-проб обеспечит автоматический переход на передачу трафика по резервным направлениям в случае отказа основных направлений передачи.

Таким образом, таблицы маршрутизации маршрутизаторов изделия остаются *статическими* (сопровождаемыми администратором *вручную*), но с помощью организованного администратором набора записей PING-проб в работу изделия вносится элемент *динамической* настройки функционирования алгоритма маршрутизации в зависимости от реального состояния окружающей изделие среды передачи данных. Если программа управления изделием получает (путем контроля за состоянием удаленных сетевых IP-ресурсов с помощью механизма PING-проб) информацию о том, что основное направление передачи данных стало неработоспособным, то для дальнейшей передачи трафика автоматически будут использованы альтернативные (резервные) направления (согласно приоритетам имеющихся альтернативных маршрутов); когда основное направление передачи данных будет восстановлено, функционирование изделия вернется к исходному варианту и передача данных возобновится по основному тракту.

2.7.3. Автоматизация управления активностью туннелей

Процесс динамического управления активностью туннелей изделия реализуется на тех же принципах работы средств контроля, что и процесс автоматизации управления маршрутизацией: изделие формирует PING-запросы, через заданные промежутки времени направляемые в адреса удаленных устройств, указанные при настройке PING-проб.

Пока на регулярно выдаваемые механизмом PING-проб запросы приходит ответ в течение заданного времени ожидания (успешная PING-проба), *туннели*, имеющие соответствующие метки (привязанные к успешной PING-пробе), остаются активными.

Если результат PING-пробы окажется неудачным, все туннели, имеющие соответствующие метки, привязанные к неуспешной PING-пробе, станут неактивными.

Посылка PING-проб в этом случае регулярно продолжается, и, если удаленное устройство в итоге ответит, туннели станут снова активными.

2.7.4. Автоматизация контроля работоспособности физических интерфейсов

Важной характеристикой каждого физического интерфейса маршрутизатора (БНМ или БВМ) является наличие или отсутствие *несущей* в физическом канале связи с коммуникационным оборудованием сети. Но наличие несущей является лишь необходимым, но не достаточным условием для оценки работоспособности сетевого интерфейса.

Единственным способом убедиться в том, что физический интерфейс изделия (Ethernet-интерфейс или L2-Eth-интерфейс при условии, что на нем разрешен L3-уровень) работоспособен, является посылка PING-проб в адрес ближайшего стационарного узла в сети (часто это ближайший *шлюз*).

Процесс PING-проб запускается, как только в бланк создания и настройки физического интерфейса (см. Рис. 2.4, с. 25 или Рис. 2.17, с. 35) в поле **`Удаленный IP-адрес интерфейса`** будет занесено значение IP-адреса, отличное от значения ***`0.0.0.0`*** (IP-адрес устройства в сети, которое с высокой вероятностью находится в работе, обычно – IP-адрес ближайшего к изделию шлюза) и будет выполнена запись параметров обновленного конфигуратора в **БпО**.

По результатам тестирования (анализа результатов PING-проб) программа управления принимает решение, находится интерфейс в рабочем состоянии или нет.

Если в заданное время ожидания результатов PING-пробы не придет хотя бы один PING-ответ, интерфейс деактивизируется, программа управления считает его неактивным и выполняет следующие действия:

- из маршрутной таблицы интерфейса удаляются все *косвенные* маршруты этого интерфейса (о косвенных маршрутах см. раздел 2.3.1, с. 25 и раздел ***Приложение А***, с. 214);
- в списке интерфейсов (портов) цвет строки, отображающей интерфейс, изменяется на *серый* (см. раздел 2.6, с. 52);
- заносит соответствующую запись в журнал.

Регулярная посылка зондирующих пакетов PING-проб продолжается по-прежнему, и, если удаленное устройство в итоге ответит, обмен данными будет восстановлен в первоначальном варианте.

2.8. Поддержка MULTICAST-адресации

При использовании `internet/intranet`-технологий возможно применение следующих трех известных способов IP-адресации.

Примечание. Каждый IP-адрес пакета, подлежащего доставке, состоит из двух частей: *номера сети* и *номера узла* в этой сети. В зависимости от количества бит, используемых для

представления номера сети и номера узла в этой сети, различают 5 классов сетей – A, B, C, D, E (подробнее об адресации в IP-сетях см. раздел ***Приложение А***, с. 214).

1. **`UNICAST-адресация`**. В этом случае отправитель указывает *точный IP-адрес* абонента-получателя, и датаграмма доставляется *единственному* адресату.
2. **`BROADCAST-адресация`**. В этом случае отправитель формирует IP-адрес пакета в специальной *широковещательной* форме, которая означает, что датаграмма предназначена *всем абонентам* сети, адрес которой указан в адресе отправляемого IP-пакета.

   Для формирования `broadcast`-посылки вся пользовательская часть IP-адреса (часть, отведенная под *адрес узла*) заполняется двоичными единицами. Например, IP-адреса `broadcast`-пакетов, отправляемых в сети классов A, B и C будут выглядеть следующим образом:

   `<адрес сети>.255.255.255` – в `broadcast`-посылке для сети класса A;

   `<адрес сети>.255.255` – в `broadcast`-посылке для сети класса B;

   `<адрес сети>.255` – в `broadcast`-посылке для сети класса C.
3. **`MULTICAST-адресация`**. Позволяет адресовать датаграммы некоторой группе абонентов (MULTICAST-группе). Абоненты этой группы могут находиться как в одной, так и в разных IP-сетях. Если какая-либо станция, входящая в MULTICAST-группу, намерена послать информацию членам группы, она должна задать в качестве IP-адреса получателя датаграммы *групповой* адрес.

Для целей MULTICAST-адресации IP-адреса отправляемых пакетов формируются по правилам адресации в сетях класса D, т. е. старшие биты IP-адресов имеют значение **`1110`** (младший бит старшей тетрады IP-адреса равен ***0***, все остальные биты старшей тетрады равны ***1***).

Поэтому диапазон IP-адресов для адресации устройств, работающих в составе сетей класса D, выглядит следующим образом: **`224.0.0.0 - 239.255.255.255`**.

При этом в диапазоне адресов сетей класса D:

- адрес **`224.0.0.0`** – не используется;
- адрес **`224.0.0.1`** – присвоен всем хостам и маршрутизаторам подсети;
- адрес **`224.0.0.2`** – присвоен всем маршрутизаторам подсети.

Часть оставшихся адресов диапазона отдана в распоряжение организации IANA (Internet Assigned Numbers Authority). IANA присваивает имеющиеся в ее распоряжении адреса конкретным группам. Получить список этих групп (и присвоенных им адресов) можно по следующему адресу в Internet-сети:

`URL = http://www.iana.org/assignments/multicast-addresses`

Все остальные адреса из диапазона адресов класса D может брать любая станция и использовать их для организации локальных MULTICAST-групп. Локальные группы не требуют регистрации и не видны устройствам сети, не входящим в эти группы.

2.8.1. *Реализация MULTICAST-адресации*

Реализуется MULTICAST-адресация следующим образом.

Каждая рабочая станция (хост) выбирает групповой адрес и, выходя на связь, объявляет в своей локальной сети, что она намерена работать в составе MULTICAST-группы с этим адресом. Группа может быть новой или уже существующей. Ближайший к станции маршрутизатор получает эту информацию и сообщает всем о появлении хоста (станции) в группе.

Схема взаимодействия устройств в сети при организации работы с `MULTICAST`-адресацией приведена на Рис. 2.51.

Для обмена информацией о принадлежности к MULTICAST-группе между маршрутизатором и рабочими станциями используется специальный протокол IGMP (Internet Group Management Protocol).

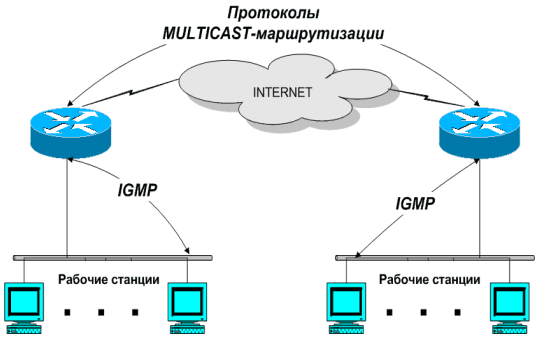


Рис. 2.51 Схема организации MULTICAST-адресации

Информация между маршрутизаторами передается с помощью специальных *протоколов MULTICAST-маршрутизации*. С помощью IGMP-протокола хост может объявить о выходе из группы, т. е. членство в группе *динамическое*. Каждый хост должен регулярно (и достаточно часто) подтверждать свое участие в группе.

Каждый маршрутизатор, начиная работу, не знает ни об одной группе. Информацию о группах он получает от соседних маршрутизаторов в соответствии с протоколами MULTICAST-маршрутизации и от своих рабочих станций, периодически посылая соответствующие запросы.

2.8.2. *Настройка изделия для работы с MULTICAST-группами*

При организации MULTICAST-адресации блоки маршрутизации (каждый в своем сегменте):

- принимают от рабочих станций своего сегмента по протоколу IGMP запросы на участие в MULTICAST-группах и ведут у себя список этих групп;
- обеспечивают маршрутизацию MULTICAST-датаграмм: прием исходящих MULTICAST-датаграмм от рабочих станций своего сегмента, входящих в MULTICAST-группы, и передачу их другим известным маршрутизатору абонентам MULTICAST-групп.

Обработка IGMP-протокола и работа с MULTICAST-группами выполняется изделием только в том случае, если специальными настройками интерфейса разрешена обработка MULTICAST-датаграмм этими интерфейсами (подробнее о специальных настройках см. раздел 2.5, с. 50).

Настройка блока маршрутизации для обеспечения обработки проходящего через интерфейс трафика, включающего пакеты с адресацией MULTICAST-группам, выполняется при конфигурировании интерфейсов изделия (см. раздел 2.3.1, с. 25).

В бланке создания и настройки интерфейса при выборе альтернативы **Специальные настройки** на видеомонитор ЛКУ будет выдан представленный на Рис. 2.52 бланк управления специальными настройками интерфейса – копия аналогичного бланка, представленного на Рис. 2.8 (с. 28).

В этом бланке следует параметру **Запретить обработку: Multicast-датаграмм** присвоить значение *Нет*, убрав в бланке символ «*» (звездочка) справа от названия параметра.

Значения всех остальных параметров бланка должны быть заданы по общим правилам конфигурирования интерфейсов.

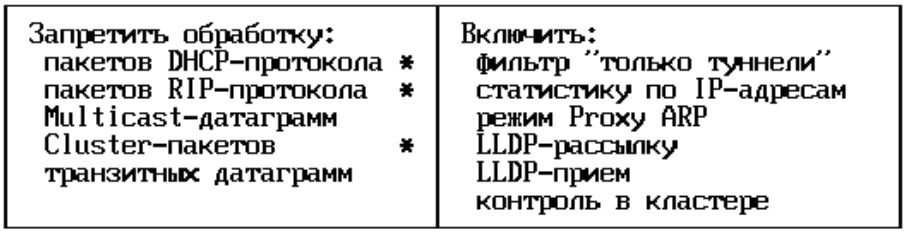


Рис. 2.52 Бланк управления специальными настройками интерфейса

Если в составе блока маршрутизации определен хотя бы один физический интерфейс с разрешенной обработкой MULTICAST-датаграмм (MULTICAST-интерфейс), работа блока маршрутизации с MULTICAST-датаграммами происходит следующим образом.

1. Для MULTICAST-интерфейса обрабатываются пакеты IGMP-протокола и формируются списки MULTICAST-групп.
2. С момента регистрации каждой MULTICAST-группы интерфейс начинает принимать датаграммы с соответствующими MULTICAST-адресами.
3. Все полученные MULTICAST-датаграммы автоматически передаются во все другие MULTICAST-интерфейсы, для которых есть регистрация тех же MULTICAST-групп.
4. Передача MULTICAST-датаграмм во внешние интерфейсы (не MULTICAST-интерфейсы) изделия возможна в том случае, если выполнено в составе изделия определены туннели, содержащие правила отбора, для которых в качестве адресов получателя заданы MULTICAST-адреса

В процессе работы блока маршрутизации для каждого интерфейса можно оперативно получить информацию о состоянии его IGMP-таблицы. Для этого необходимо выбрать цепочку альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ Активные** (см. раздел 9.2.2, с. 189), после чего в появившемся списке *активных* интерфейсов изделия (см. Рис. 9.5, с. 189) установить курсор на описание интересующего интерфейса и нажать комбинацию клавиш <Alt+F5>.

Примечание. Подробное описание протокола IGMP приведено в документе RFC 2236.

2.9. Примеры настройки изделий

Рассмотрим примеры настройки изделий, обеспечивающих защищенный обмен данными между двумя удаленными сегментами ЛВС Пользователя.

На Рис. 2.53 приведен пример простой монтажной схемы организации защищенной связи между двумя удаленными сегментами ЛВС Пользователя.

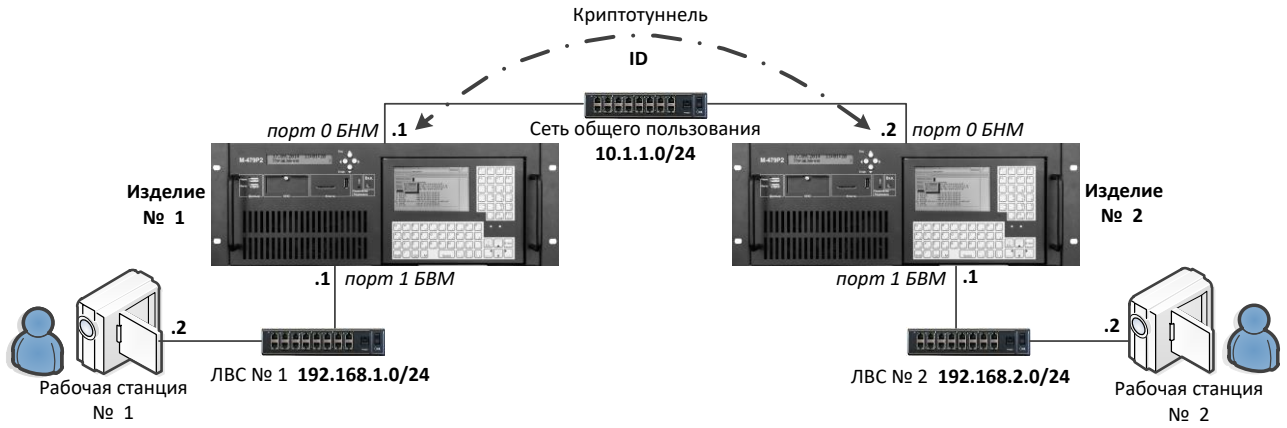


Рис. 2.53 Монтажная схема организации защищенного обмена между двумя сегментами ЛВС Пользователя

Согласно схеме защиту передаваемого между сегментами ЛВС трафика осуществляют два изделия Изделие № 1 и Изделие № 2.

Тракт передачи данных между изделиями через сеть общего пользования (адрес подсети: **`10.1.1.0/24`**) имитируют Ethernet-кабели, подключаемые через коммутатор к разъемам Ethernet-адаптеров БНМ соответствующего изделия. Порты БНМ изделий, к которым подключены кабели, промаркированы как порты с номером **`0`** на обоих изделиях.

Адрес наружного интерфейса Изделия № 1 в сети общего пользования: **`10.1.1.1`**.

Адрес наружного интерфейса Изделия № 2 в сети общего пользования: **`10.1.1.2`**.

Между наружными интерфейсами изделий организован криптотуннель с идентификатором **`ID`**.

В Изделия № 1 и № 2 загружены соответствующие ключевые документы с номером серии ***`1001`***.

К каждому из БВМ изделий № 1 и № 2 подключены соответственно ЛВС № 1 и № 2, в составе которых имеются рабочие станции (далее – РС) № 1 и № 2. Для подключения ЛВС на каждом из БВМ изделий использованы порты Ethernet-адаптеров с номером **`1`**.

К Изделию № 1 подключена ЛВС № 1, адрес которой: **`192.168.1.0/24`**. Адрес внутреннего интерфейса Изделия № 1 (порт **`1`**) в ЛВС: **`192.168.1.1`**, адрес рабочей станции: **`192.168.1.2`**.

К Изделию № 2 подключена ЛВС № 2, адрес которой: **`192.168.2.0/24`**. Адрес внутреннего интерфейса Изделия № 2 (порт **`1`**) в ЛВС: **`192.168.2.1`**, адрес рабочей станции: **`192.168.2.2`**.

С помощью представленного на монтажной схеме оборудования между рабочими станциями сегментов ЛВС Пользователя может быть организован режим обмена как *IP-датаграммами* на *L3-уровне*, так и *Ethernet-кадрами* на *L2-уровне*.

Для организации того или иного режима обмена должны быть выполнены соответствующие настройки Изделий № 1 и № 2; примеры настроек приведены в последующих разделах (2.9.1 и 2.9.2).

В разделе 2.9.1 приведен пример настройки изделий для организации обмена IP-датаграммами на L3-уровне.

В разделе 2.9.2 приведен пример настройки изделий для организации обмена Ethernet-кадрами на L2-уровне.

2.9.1. Настройка изделий для обмена IP-датаграммами на L3-уровне

На Рис. 2.54 представлена логическая схема организации связи между Изделиями № 1 и № 2, поясняющая особенности настройки изделий для обеспечения обмена IP-датаграммами на L3-уровне. Изделия смонтированы согласно монтажной схеме, представленной на Рис. 2.53.

Для организации защищенного обмена согласно схеме, приведенной на Рис. 2.54, на каждом из Изделий № 1 и № 2 следует выполнить:

- общие настройки обоих маршрутизаторов;
- на каждом из изделий создать и настроить необходимые для обмена IP-датаграммами на L3-уровне следующие сетевые интерфейсы и криптотуннели:
  - в составе Изделия № 1:
    - принадлежащий БВМ физический сетевой интерфейс типа **`Ethernet`** с именем **`IntETH1`**;
    - принадлежащий БНМ физический сетевой интерфейс типа **`Ethernet`** с именем **`ExtETH1`**;
    - общий туннельный интерфейс типа **`TNL`** с именем **`TNL1`**;
  - в составе Изделия № 2:

- принадлежащий БВМ физический сетевой интерфейс типа **Ethernet** с именем **IntETH2**;
- принадлежащий БНМ физический сетевой интерфейс типа **Ethernet** с именем **ExtETH2**;
- общий туннельный интерфейс типа **TNL** с именем **TNL2**.

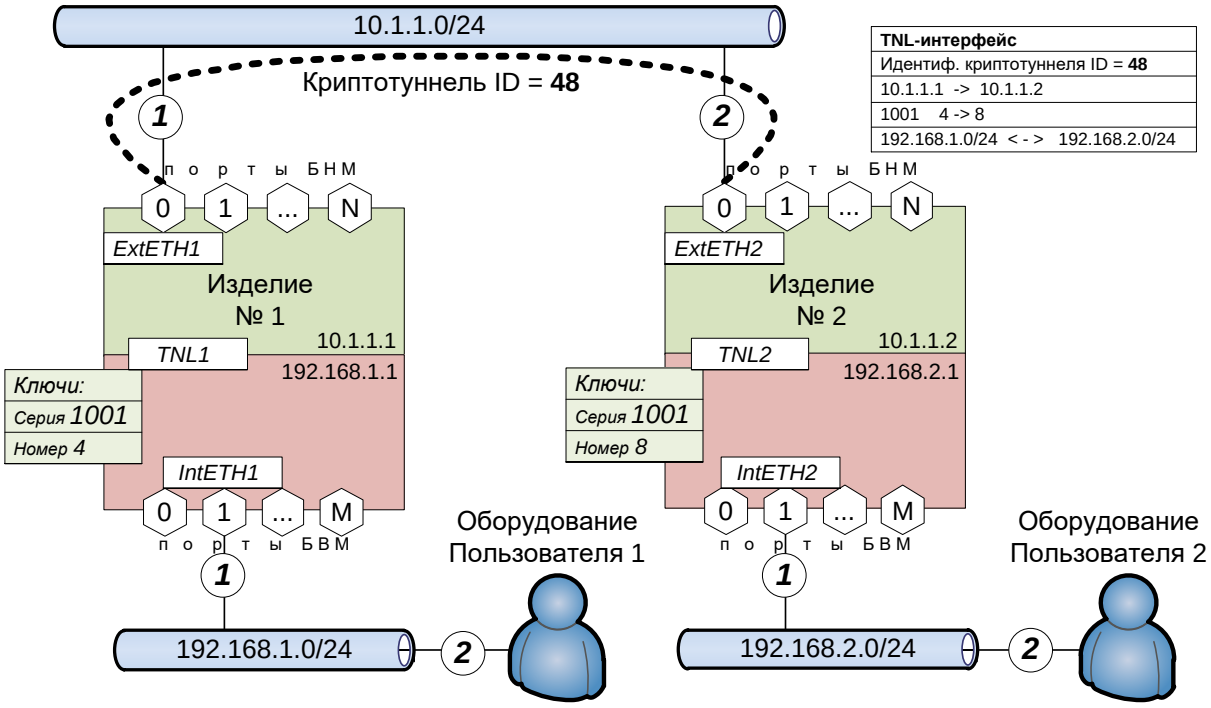


Рис. 2.54 Логическая схема организации связи между изделиями при обмене IP-датаграммами на L3-уровне

Ниже приведены значения основных параметров, которые следует присвоить при создании и настройке перечисленных элементов.

Изделие № 1

1. Общие параметры маршрутизаторов

Параметры TCP/IP (см. раздел 4.1.2, с. 130)

Собственный IP-адрес: наружный – ***10.1.1.1***;

внутренний – ***192.168.1.1***.

Время жизни IP-датаграмм (TTL) – ***32***.

Максимальный размер TCP-пакета (MSS) – ***512***.

Размер TCP-окна (Window) – ***8192***.

2. Сетевой физический интерфейс ExtETH1 (см. раздел 2.3.1, с. 25)

Тип – ***Ethernet***.

Принадлежность маршрутизатору – ***наружный***.

Имя интерфейса – ***ExtETH1***.

Локальный IP-адрес – ***10.1.1.1/24***.

Удаленный IP-адрес – ***0.0.0.0***.

Максимальный размер IP-датаграмм (MTU) – ***1600***.

Таблица маршрутов – ***не настраивать***.

Дополнительные параметры. Номер порта – ***0***.

Интерфейс – ***автоопределение***.

Режим работы – ***автоопределение***.

Специальные настройки. Запретить обработку: – ***пакетов DHCP-протокола***;

– ***пакетов RIP-протокола***;

– ***Multicast-датаграмм***;

– ***Cluster-пакетов***.

3. Сетевой физический интерфейс IntETH1 (см. раздел 2.3.1, с. 25)

Тип – ***Ethernet***.

Принадлежность маршрутизатору – ***внутренний***.

Имя интерфейса – ***IntETH1***.

Локальный IP-адрес – ***192.168.1.1/24***.

Удаленный IP-адрес – ***0.0.0.0***.

Максимальный размер IP-датаграмм (MTU) – ***1500***.

Дополнительные параметры. Номер порта – ***1***.

Интерфейс – ***автоопределение***.

Режим работы – ***автоопределение***.

Специальные настройки. Запретить обработку: – ***пакетов DHCP-протокола***;

– ***пакетов RIP-протокола***;

– ***Multicast-датаграмм***;

– ***Cluster-пакетов***.

4. Туннельный интерфейс TNL1 (см. разделы 2.4.2, с. 39 и 2.3.1, с. 25)

Тип – ***TNL***.

Принадлежность маршрутизатору – ***общий***.

Имя интерфейса – ***TNL1***.

Идентификатор туннеля – ***48***.

Локальный IP-адрес – ***10.1.1.1***.

Удаленный IP-адрес – ***10.1.1.2***.

Таблица маршрутов. Адрес – ***192.168.2.0***.

Значащих бит – ***24***.

Адрес шлюза – ***0.0.0.0***.

Метрика маршрута –***0***.

Метка –***0***.

Шифрование потока. Шифрование потока – ***ДА***.

Версия криптоалгоритма – ***vМПМ***.

Номер серии ключей –***1001***.

Локальный криптономер –***4***.

Удаленный криптономер –***8***.

Номер ключевой зоны –***0***.

Максимальный размер IP-датаграмм (MTU) – ***1500***.

Дополнительные параметры. Описание – произвольный текст.

Формат заголовка – ***TNL***.

Метка туннеля – ***0***.

Контроль состояния – ***Нет***.

Скорость передачи – ***0***.

Скорость приема – ***0***.

Специальные настройки. Запретить обработку: – ***пакетов DHCP-протокола***;

– ***пакетов RIP-протокола***;

– ***Multicast-датаграмм***;

– ***Cluster-пакетов***.

Примечание. Отметим, что при настройке физических интерфейсов параметру **Максимальный размер IP-датаграмм (MTU)** внутреннего физического интерфейса **IntETH2** присвоено значение ***1500***, а тому же параметру наружного интерфейса **ExtETH2** присвоено значение ***1600***.

Разница в значениях максимальной длины Ethernet-кадров, отправляемых соответствующими Ethernet-адаптерами в каналы связи, учитывает, что на наружном интерфейсе **ExtETH2** длина

любого принятого из внутренней сети и подлежащего передаче в сеть общего пользования Ethernet-кадра увеличивается на длину IP-заголовка транспортной IP-датаграммы, добавляемого к длине исходной IP-датаграммы. Заголовок транспортной IP-датаграммы включает: транспортный IP-заголовок длиной 20 байт, заголовок туннеля длиной 16 байт или более и, возможно, UDP-заголовок длиной 8 байт (подробнее см. раздел 3.1, Рис. 3.3, с. 74). Эта добавка к первоначальной длине принятого внутренним интерфейсом **IntETH2** Ethernet-кадра может вызвать необходимость включения при работе наружного интерфейса **ExtETH2** механизма фрагментации – передачи исходящего Ethernet-кадра интерфейсом **ExtETH2** в виде *двух* Ethernet-кадров, каждый из которых не превышает размер **MTU** для наружного интерфейса. Во избежание этих накладных расходов значение параметра **MTU** наружного интерфейса **ExtETH2** увеличено до ***1600***.

Отметим также, что прежде чем устанавливать значение MTU, равное ***1600***, следует убедиться, что тракт во внешней сети пропускает Ethernet-кадры такой длины. Выполнить эту проверку можно путем выдачи на оконечное устройство проверяемого тракта команды PING с соответствующей длиной передаваемых этой командой данных.

Изделие № 2.

1. Общие параметры маршрутизаторов

Параметры TCP/IP (см. раздел 4.1.2, с. 130)

Собственный IP-адрес: наружный – ***10.1.1.2***;

внутренний – ***192.168.2.1***.

Время жизни IP-датаграмм (TTL) – ***32***.

Максимальный размер TCP-пакета (MSS) – ***512***.

Размер TCP-окна (Window) – ***8192***.

2. Сетевой физический интерфейс ExtETH2 (см. раздел 2.3.1, с. 25)

Тип – ***Ethernet***.

Принадлежность маршрутизатору – ***наружный***.

Имя интерфейса – ***ExtETH2***.

Локальный IP-адрес – ***10.1.1.2/24***.

Удаленный IP-адрес – ***0.0.0.0***.

Максимальный размер IP-датаграмм (MTU) – ***1600***.

Дополнительные параметры. Номер порта – ***0***.

Интерфейс – ***автоопределение***.

Режим работы – ***автоопределение***.

Специальные настройки. Запретить обработку: – ***пакетов DHCP-протокола***;

– ***пакетов RIP-протокола***;

– ***Multicast-датаграмм***;

– ***Cluster-пакетов***.

3. Сетевой физический интерфейс IntETH2 (см. раздел 2.3.1, с. 25)

Тип – ***Ethernet***.

Принадлежность маршрутизатору – ***внутренний***.

Имя интерфейса – ***IntETH2***.

Локальный IP-адрес – ***192.168.2.1/24***.

Удаленный IP-адрес – ***0.0.0.0***.

Максимальный размер IP-датаграмм (MTU) – ***1500***.

Дополнительные параметры. Номер порта – ***1***.

Интерфейс – ***автоопределение***.

Режим работы – ***автоопределение***.

Специальные настройки. Запретить обработку: – ***пакетов DHCP-протокола***;

– ***пакетов RIP-протокола***;

– ***Multicast-датаграмм***;

– ***Cluster-пакетов***.

4. Туннельный интерфейс TNL2 (см. разделы 2.4.2, с. 39 и 2.3.1, с. 25)

Тип – ***TNL***.

Принадлежность маршрутизатору – ***общий***.

Имя интерфейса – ***TNL2***.

Идентификатор туннеля – ***48***.

Локальный IP-адрес – ***10.1.1.2***.

Удаленный IP-адрес – ***10.1.1.1***.

Таблица маршрутов. Адрес – ***192.168.1.0***.

Значащих бит – ***24***.

Адрес шлюза – ***0.0.0.0***.

Метрика маршрута –***0***.

Метка –***0***.

Шифрование потока. Шифрование потока – ***ДА***.

Версия криптоалгоритма – ***vМПМ***.

Номер серии ключей –***1001***.

Локальный криптономер –***8***.

Удаленный криптономер –***4***.

Номер ключевой зоны –***0***.

Максимальный размер IP-датаграмм (MTU) – ***1500***.

Дополнительные параметры. Описание – произвольный текст.

Формат заголовка – ***TNL***.

Метка туннеля – ***0***.

Контроль состояния – ***Нет***.

Скорость передачи – ***0***.

Скорость приема – ***0***.

Специальные настройки. Запретить обработку: – ***пакетов DHCP-протокола***;

– ***пакетов RIP-протокола***;

– ***Multicast-датаграмм***;

– ***Cluster-пакетов***.

*2.9.2. **Настройка изделий для обмена Ethernet-кадрами на L2-уровне***

На Рис. 2.55 представлена логическая схема организации связи между Изделиями № 1 и № 2, поясняющая особенности настройки изделий для обеспечения обмена Ethernet-кадрами на L2-уровне. Изделия смонтированы согласно монтажной схеме, представленной на Рис. 2.53.

Чтобы схема (Рис. 2.55) заработала, на каждом из Изделий № 1 и № 2 следует выполнить:

- общие настройки обоих маршрутизаторов;
- на каждом из изделий создать и настроить необходимые для обмена Ethernet-кадрами на L2-уровне следующие сетевые интерфейсы и криптотуннели:
  - в составе Изделия № 1:
    - принадлежащий БВМ физический сетевой интерфейс типа **L2-Eth** с именем **L2_ETH1**;
    - принадлежащий БНМ физический сетевой интерфейс типа **Ethernet** с именем **ExtETH1**;
    - общий туннельный интерфейс типа **L2-TNL** с именем **L2_TNL1**;
  - в составе Изделия № 2:
    - принадлежащий БВМ физический сетевой интерфейс типа **L2-Eth** с именем **L2_ETH2**;
    - принадлежащий БНМ физический сетевой интерфейс типа **Ethernet** с именем **ExtETH2**;
    - общий туннельный интерфейс типа **L2-TNL** с именем **L2_TNL2**.

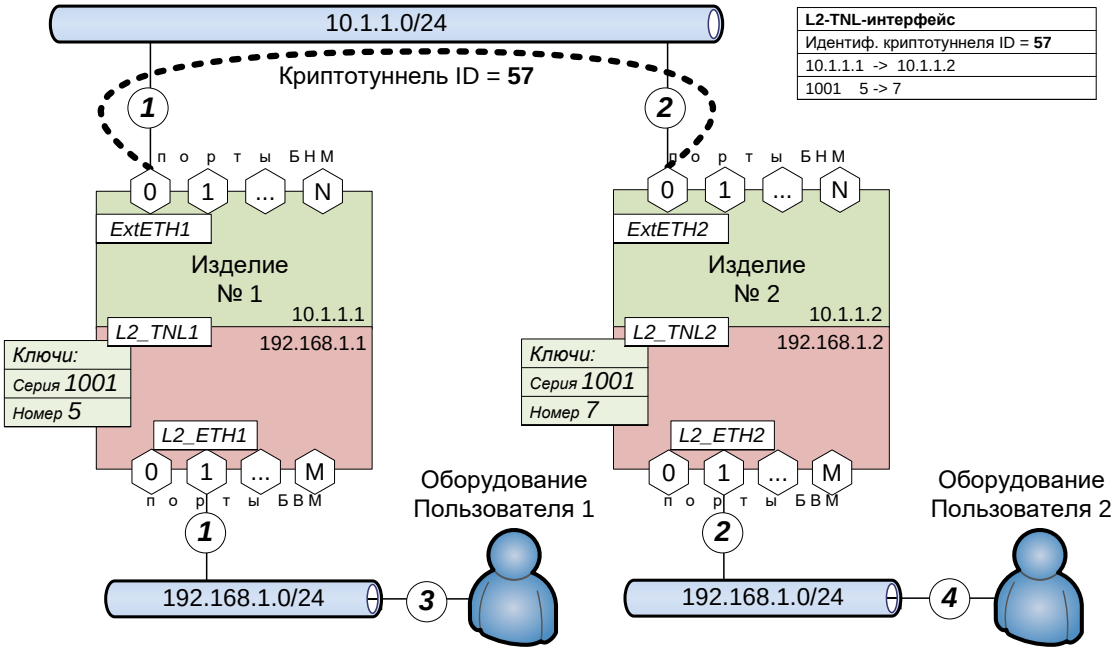


Рис. 2.55 Логическая схема организации связи между изделиями при обмене Ethernet-кадрами на L2-уровне

Ниже приведены значения основных параметров, которые следует присвоить при создании и настройке перечисленных элементов технологии обработки трафика Ethernet-кадров на L2-уровне.

Изделие № 1

1. Общие параметры маршрутизаторов

Параметры TCP/IP (см. раздел 4.1.2, с. 130)

Собственный IP-адрес: наружный – ***10.1.1.1***;

внутренний – ***192.168.1.1***.

Время жизни IP-датаграмм (TTL) – ***32***.

Максимальный размер TCP-пакета (MSS) – ***512***.

Размер TCP-окна (Window) – ***8192***.

2. Сетевой физический интерфейс ExtETH1 (см. раздел 2.3.1, с. 25)

Тип – ***Ethernet***.

Принадлежность маршрутизатору – ***наружный***.

Имя интерфейса – ***ExtETH1***.

Локальный IP-адрес – ***10.1.1.1/24***.

Удаленный IP-адрес – ***0.0.0.0***.

Максимальный размер IP-датаграмм (MTU) – ***1600***.

Дополнительные параметры. Номер порта – ***0***.

Интерфейс – ***автоопределение***.

Режим работы – ***автоопределение***.

Специальные настройки. Запретить обработку: – ***пакетов DHCP-протокола***;

– ***пакетов RIP-протокола***;

– ***Multicast-датаграмм***;

– ***Cluster-пакетов***.

3. Сетевой физический интерфейс L2_ETH1 (см. раздел 2.3.2, с. 33)

Тип – ***L2-Eth***.

Принадлежность маршрутизатору – ***внутренний***.

Имя L2-интерфейса – ***L2_ETH1***.

Имя L2-туннеля – ***L2_TNL1***.

Дополнительные параметры. Номер порта – ***1***.

Интерфейс – ***автоопределение***.

Режим работы – ***автоопределение***.

4. Туннельный интерфейс L2_TNL1 (см. разделы 2.4.5, с. 49)

Тип – ***L2-TNL***.

Принадлежность маршрутизатору – ***общий***.

Имя интерфейса – ***L2_TNL1***.

Идентификатор туннеля – ***57***.

Локальный IP-адрес – ***10.1.1.1***.

Удаленный IP-адрес – ***10.1.1.2*** (формат ввода: **адрес/бит**; маршрутная таблица при этом серая).

Шифрование потока. Шифрование потока – ***ДА***.

Версия криптоалгоритма – ***vМПМ***.

Номер серии ключей –***1001***.

Локальный криптономер –***5***.

Удаленный криптономер –***7***.

Номер ключевой зоны –***0***.

Дополнительные параметры. Описание – произвольный текст.

Формат заголовка – ***TNL***.

Метка туннеля – ***0***.

Контроль состояния – ***Нет***.

Скорость передачи – ***0***.

Скорость приема – ***0***.

Изделие № 2.

1. Общие параметры маршрутизаторов

Параметры TCP/IP (см. раздел 4.1.2, с. 130)

Собственный IP-адрес: наружный – ***10.1.1.2***;

внутренний – ***192.168.1.2***.

Время жизни IP-датаграмм (TTL) – ***32***.

Максимальный размер TCP-пакета (MSS) – ***512***.

Размер TCP-окна (Window) – ***8192***.

2. Сетевой физический интерфейс ExtETH2 (см. раздел 2.3.1, с. 25)

Тип – ***Ethernet***.

Принадлежность маршрутизатору – ***наружный***.

Имя интерфейса – ***ExtETH2***.

Локальный IP-адрес – ***10.1.1.2/24***.

Удаленный IP-адрес – ***0.0.0.0***.

Максимальный размер IP-датаграмм (MTU) – ***1600***.

Дополнительные параметры. Номер порта – ***0***.

Интерфейс – ***автоопределение***.

Режим работы – ***автоопределение***.

Специальные настройки. Запретить обработку: – ***пакетов DHCP-протокола***;

– ***пакетов RIP-протокола***;

– ***Multicast-датаграмм***;

– ***Cluster-пакетов***.

3. Сетевой физический интерфейс L2_ETH2 (см. раздел 2.3.2, с. 33)

Тип – ***L2-Eth***.

Принадлежность маршрутизатору – ***внутренний***.

Имя L2-интерфейса – ***L2_ETH2***.

Имя L2-туннеля – ***L2_TNL2***.

Дополнительные параметры. Номер порта – ***1***.

Интерфейс – ***автоопределение***.

Режим работы – ***автоопределение***.

4. Туннельный интерфейс L2_TNL2 (см. разделы 2.4.5, с. 49)

Тип – ***L2-TNL***.

Принадлежность маршрутизатору – ***общий***.

Имя интерфейса – ***L2_TNL2***.

Идентификатор туннеля – ***57***.

Локальный IP-адрес – ***10.1.1.2*** (формат ввода: **адрес/бит**; маршрутная таблица при этом серая).

Удаленный IP-адрес – ***10.1.1.1***.

Шифрование потока. Шифрование потока – ***ДА***.

Версия криптоалгоритма – ***vМПМ***.

Номер серии ключей –***1001***.

Локальный криптономер –***7***.

Удаленный криптономер –***5***.

Номер ключевой зоны –***0***.

Дополнительные параметры. Описание – произвольный текст.

Формат заголовка – ***TNL***.

Метка туннеля – ***0***.

Контроль состояния – ***Нет***.

Скорость передачи – ***0***.

Скорость приема – ***0***.

3. Средства защиты при обмене данными через сети

Общие сведения о средствах защиты. Архитектура защищенных сетей передачи данных, как правило, представляет собой совокупность множества территориально удаленных локальных сетей (*внутренних* сегментов ЗСПД), в которых циркулирует информация Пользователя. Доступ к этой информации регламентирует Пользователь ЗСПД.

Для обеспечения информационного обмена между локальными сетями Пользователя внутренние сегменты ЗСПД подключают к *внешним* сегментам ЗСПД – *сетям общего пользования* (сети операторов связи, сеть Интернет и пр.). Через каналы связи сетей общего пользования осуществляется транспортировка информации Пользователя между внутренними сегментами ЗСПД.

Создавая средства, обеспечивающие защиту информации при таком обмене, необходимо учитывать, что:

- информация Пользователя в сетях общего пользования может быть перехвачена;
- в сетях общего пользования могут находиться: источники нежелательного (паразитного) входящего трафика; источники, осуществляющие попытки несанкционированного доступа извне к информации во внутренних сегментах; источники трафика, представляющего собой атаку на внутренние сегменты ЗСПД, и пр.;
- во внутренних сетях Пользователя также могут находиться источники нежелательного исходящего трафика.

Рассматриваемые в настоящем Руководстве изделия обладают набором средств, обеспечивающих решение задачи *защиты* информации с учетом указанных выше аспектов. Краткие сведения об этих средствах приведены ниже.

С целью выполнения функций защиты передаваемой через сети общего пользования информации Пользователя изделие используется в качестве *пограничного* криптографического маршрутизатора – *криптомаршрутизатора* (устройства L3-уровня) или *пограничного* средства организации криптографических мостов – *криптомостов* (устройства L2-уровня), наведенных через внешние сегменты ЗСПД между ее внутренними сегментами, как представлено на схеме применения изделия в составе ЗСПД (см. Рис. 3.1).

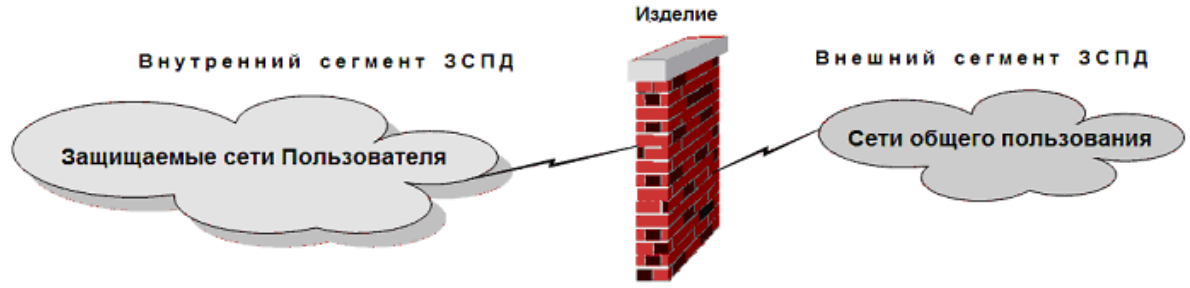


Рис. 3.1 Схема применения изделия в составе ЗСПД

С помощью сетевых интерфейсов БВМ изделие подключается к защищаемым локальным сетям Пользователя, а с помощью сетевых интерфейсов БНМ – к сетям общего пользования. Таким образом, БВМ и БНМ изделия обеспечивают маршрутизацию IP-потоков данных или обработку потоков Ethernet-кадров в подключенных к изделию сетях внутреннего и внешнего сегментов ЗСПД соответственно, а БКО изделия выполняет специальные преобразования исходящих и входящих IP-потоков данных или потоков Ethernet-кадров.

Ниже приведены краткие сведения о функциональном наборе *средств защиты*, предоставляемых изделием Администрации ЗСПД и администратору изделия.

1. **Криптографические туннели (криптотуннели).** Поддерживаемые изделием механизмы криптографического туннелирования в общем случае предусматривают при передаче данных *инкапсуляцию* (упаковку) отобранных в туннель исходных IP-датаграмм (L3-уровень) или исходных Ethernet-кадров (L2-уровень) после их соответствующей криптообработки во вновь формируемую т.н. *транспортную* IP-датаграмму, которая через сети общего пользования доставляется получателю, где из нее извлекается исходная IP-датаграмма или исходный Ethernet-кадр. Применяемый в изделии алгоритм криптообработки обеспечивает гарантированную стойкость, поэтому даже в случае перехвата передаваемых через сети общего пользования туннелированных транспортных IP-датаграмм не происходит утечки информации Пользователя. Криптотуннели являются единственным каналом *двунаправленного* обмена информацией между БВМ и БНМ изделия.

   Подробнее о работе криптотуннелей см. раздел 3.1, с. 73.

2. **Фильтрация IP-датаграмм**. Поддерживаемый изделием механизм фильтрации на *сетевом* уровне предусматривает наличие фильтров входящих и исходящих потоков IP-датаграмм на каждом из сетевых интерфейсов, физических или виртуальных, а также на внутреннем (служебном) интерфейсе обоих маршрутизаторов изделия – БВМ и БНМ. Анализ IP-датаграмм и принятие решения о дальнейшем

алгоритме их обработки принимается автоматически на основе правил фильтрации, формируемых администратором изделия при настройке. Механизм составления правил фильтрации обеспечивает необходимую глубину и гибкость, позволяющие изделию успешно отражать информационные атаки, бороться с нежелательными (паразитарными) входящим и исходящим трафиками, а также с попытками несанкционированного доступа извне к информации во внутренних сегментах ЗСПД – в ЛВС Пользователя.

Примечание. Отметим, что механизм фильтрации IP-датаграмм работает на *сетевом* уровне – L3-уровне модели OSI.

Подробнее о работе с фильтрами IP-датаграмм см. раздел 3.2.1, с. 90.

3. **Трансляция сетевых адресов (NAT/PAT-обработка)**. Поддерживаемый изделием механизм NAT/PAT-обработки предусматривает выполнение трансляции IP-адресов заголовков исходящих и входящих IP-датаграмм из одного множества IP-адресов в другое, определяемое при настройке изделия, поэтому использование механизма NAT-обработки обеспечивает полное сокрытие внутренней структуры (внутреннего адресного пространства) защищаемых сетей, усложняя неосведомленным пользователям реализацию несанкционированного доступа извне к информации, размещенной во внутренних сегментах ЗСПД. Кроме того, применение NAT-обработки позволяет назначать рабочим станциям защищаемых сетей Пользователя IP-адреса из фиктивных (т.н. приватных) областей адресов (например, `192.168.x.x`), помогая решать задачу оптимизации использования ограниченного адресного пространства сетей, организованных согласно системным требованиям `internet/intranet`-технологии.

Подробнее о работе с транслятором сетевых адресов см. раздел 3.3, с. 111.

4. **Групповая замена ключевых документов**. Известно, что стабильная и устойчивая работа ЗСПД нередко нарушается в периоды регламентной замены ключевых документов, когда обслуживающий персонал в сжатые сроки в масштабе всей ЗСПД вручную выполняет перевод работы изделий защиты с одной серии ключевых документов на другую. Изделием поддерживается механизм *групповой замены ключевых документов*, который позволяет обслуживающему персоналу изделий выполнить заранее вручную подготовительные операции к переводу работы изделия защиты с одной серии КД на другую и после этого в сжатый промежуток времени, установленный заранее администрацией ЗСПД, *автоматически* перевести обмен данными между криптоузлами в масштабе всей ЗСПД с предыдущей серии КД на новую.

Подробнее о работе механизма групповой замены ключевых документов см. раздел 3.4, с. 122.

5. **Фильтрация трафика с применением таблиц MAC-адресов**. Изделием поддерживается механизм фильтрации на *канальном* уровне физическими интерфейсами изделия (Ethernet-интерфейсами и L2–Eth-интерфейсами) *входящего* трафика Ethernet-кадров. Критерием приема на дальнейшую обработку изделием поступившего на его физический интерфейс Ethernet-кадра является наличие MAC-адреса отправителя кадра в связанной с данным интерфейсом таблице, предварительно настроенной администратором изделия. Принимаемые из сети Ethernet-кадры, MAC-адрес отправителя (источника генерации) которых отсутствует в соответствующей таблице MAC-адресов, изделием игнорируются, что повышает защитные свойства и устойчивость работы изделия на фоне сетевых атак.

Примечание. Отметим, что механизм фильтрации Ethernet-кадров с применением таблиц MAC-адресов работает на *канальном* уровне – L2-уровне модели OSI.

Подробнее о работе механизма фильтрации Ethernet-кадров с применением таблиц MAC-адресов см. раздел 3.2.2, с. 109.

6. **Регистрация событий**. Механизм регистрации событий, поддерживаемый изделием, позволяет протоколировать сведения о проходящем через изделие трафике, включая факты попыток несанкционированного доступа и нарушения штатного режима работы изделия. Анализ зарегистрированных событий позволяет обслуживающему персоналу принять дополнительные меры повышения эффективности работы средств защиты.

Подробнее о работе механизма регистрации событий см. раздел 8.2, с. 181.

Настройка и управление средствами защиты изделия осуществляется с помощью цепочки альтернатив ГМ: **Настройка ⇨ Защита**, после выбора которой на экран видеомонитора ЛКУ выводится меню, представленное на Рис. 3.2. Описание средств защиты, доступ к которым организован через это меню, приведено ниже.

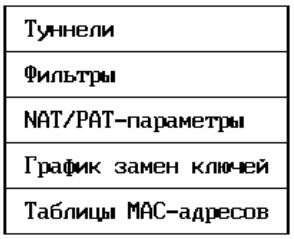


Рис. 3.2 Меню выбора средств защиты передаваемых по сетям данных

3.1. Криптографические туннели

Основным назначением изделия является защита информации Пользователя, передаваемой из одного защищаемого сегмента ЗСПД в другие защищаемые сегменты через сети общего пользования, в которых эта информация может быть перехвачена. Информация Пользователя передается через сети общего пользования в зашифрованном виде. Механизмом, реализующим функцию передачи информации Пользователя в зашифрованном виде по каналам связи между удаленными защищаемыми сегментами ЗСПД, является криптографический туннель – *криптотуннель*.

Изделия обеспечивают администратору возможность применения нескольких *видов* криптотуннелей.

Пусть имеются две локальные сети, обслуживающие территориально удаленные объекты одной организации, и ставится задача взаимного IP-доступа рабочих станций одной сети к информационным ресурсам другой через открытую IP-сеть общего пользования (например, сеть Internet).

Поставленная задача может быть решена путем установки в составе каждой защищаемой локальной сети изделий в качестве пограничных криптомаршрутизаторов или пограничных средств организации криптомостов (криптографических шлюзов) и организации с помощью криптошлюзов виртуальных криптографически защищенных каналов связи между локальными сетями через сети общего пользования – криптографических туннелей (криптотуннелей).

Принципы организации криптографически защищенных соединений, поддерживаемых изделием, соответствуют общим принципам, предложенным технологией IPSec (RFC 2401 и сопутствующие документы), но реализация этой технологии в изделии имеет свои особенности.

Криптографический туннель между изделиями может быть реализован путем создания на каждом из пары изделий, образующих криптотуннель, описателя криптотуннеля, использующего механизмы:

- *статического* криптотуннеля;
- туннельного *TNL-интерфейса*;
- туннельного *L2–TNL-интерфейса*.

Шифратором изделия обеспечивается одновременное функционирование до **256** криптотуннелей, образованных с помощью любого из механизмов их поддержки (статических криптотуннелей, TNL-интерфейсов или L2–TNL-интерфейсов).

> *Примечание.* При организации работы криптотуннелей с помощью механизмов TNL-интерфейсов или статических криптотуннелей обеспечивается защищенная передача трафика *IP-датаграмм* между изделиями на L3-уровне; при организации криптотуннелей с помощью механизма L2–TNL-интерфейсов обеспечивается защищенная передача трафика *Ethernet-кадров* между изделиями на L2-уровне.

При криптообработке изделием IP-датаграмм на L3-уровне (использование изделия в качестве криптомаршрутизатора) применение криптотуннелей, реализованных путем создания TNL-интерфейсов, дает следующие преимущества по сравнению с применением статических криптотуннелей:

- упрощается и *ускоряется* процесс отбора датаграмм в туннель при их отправке (отбор выполняется по одному параметру – IP-адресу назначения – в процессе обычной маршрутизации IP-датаграммы);
- TNL-интерфейсы, в отличие от статических криптотуннелей, обеспечивают поддержку механизма *приоритизации* трафика (QoS-приоритизацию);
- упрощается процесс конфигурирования криптотуннеля – он выполняется как стандартное конфигурирование сетевого интерфейса, не требуется составления правил отбора в криптотуннель, как этого требует организация статического криптотуннеля.

Тем не менее, в ряде случаев применение механизма статических криптотуннелей может оказаться *предпочтительнее*, т.к. статические криптотуннели позволяют при настройке более точно и избирательно очертить круг отбираемых в криптотуннель IP-датаграмм (хотя это и требует соответствующей квалификации администратора).

> *Примечание.* При функционировании изделия в качестве криптомаршрутизатора (при криптообработке изделием IP-датаграмм на L3-уровне) обеспечивается нормальное функционирование криптотуннеля между изделиями и в том случае, когда на одном из изделий криптотуннель образован как *статический*, а на другом – как *TNL-интерфейс* (при условии совпадения в описателях этих криптотуннелей соответствующих криптопараметров).

В изделии реализована возможность конвертирования описателя статического туннеля в описатель TNL-интерфейса (см. Рис. 2.1, с. 22, функция **Alt+F7 – конв. туннели в интерфейсы**).

Процедуры создания и настройки *TNL-интерфейсов* описаны в разделе 2.4.2, с. 39, создания и настройки *статических* туннелей – в разделе 3.1.1.2, с. 78, создания и настройки *L2–TNL-интерфейсов* – в разделе 2.4.5, с. 49.

Все IP-датаграммы, которыми обмениваются информационно *сопряженные* криптотуннелем узлы ЗСПД, подвергаются различным видам обработки (компрессия, шифрование, имитозащита) и снабжаются новыми IP-заголовками. Сформированные таким образом транспортные IP-датаграммы отправляются в открытую IP-сеть общего пользования, соединяющую пару узлов криптосети. На противоположной (приемной) стороне туннеля дополнительные (транспортные) IP-заголовки полученной транспортной IP-датаграммы отбрасываются, а доставленные с их помощью туннелированные данные Пользователя подвергаются обратному преобразованию, в результате чего полностью восстанавливаются исходные IP-датаграммы.

В качестве транспортного протокола для передачи туннелированных IP-датаграмм используются протокол **TNL** (IP in IP – номер протокола **4**), протокол **UDP** (номер протокола **17**) или протокол **UDPnat** (номер протокола **17**). Протокол **UDP** следует использовать в тех случаях, когда провайдер не пропускает датаграммы с протоколом **TNL**. Протокол **UDPnat** следует использовать в случаях, когда используется механизм NAT-преобразований.

> *Примечание.* При использовании для туннелирования протокола UDP длина IP-заголовков транспортных датаграмм увеличивается на 8 байт по сравнению с их длиной при использовании протокола TNL.

Механизм работы криптотуннеля, обеспечивающего защищенное информационное сопряжение изделий на L3-уровне, иллюстрирует схема, представленная на Рис. 3.3.

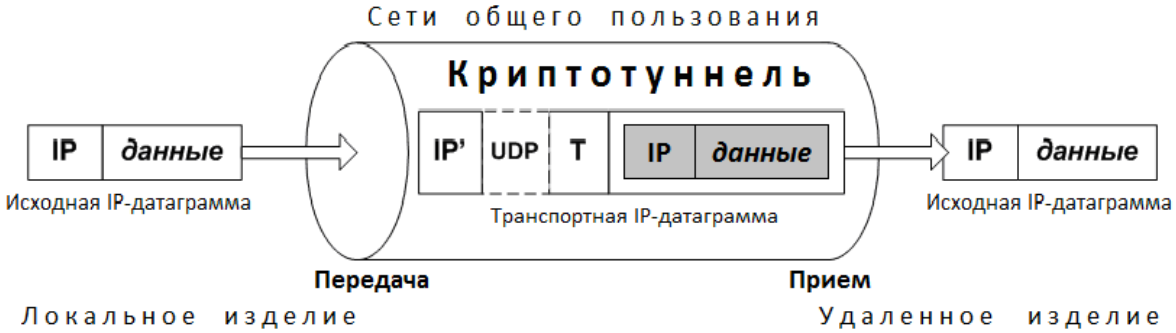


Рис. 3.3 Схема транспортировки IP-датаграммы в криптотуннеле через сети общего пользования

При попадании в криптотуннель исходная IP-датаграмма подвергается следующим преобразованиям.

1. Вся датаграмма (исходный IP-заголовок и данные) подвергается обработке: компрессия, зашифрование, имитозащита. К полученному блоку данных добавляется заголовок туннеля (**T** – на схеме), в который записывается информация о выполненных преобразованиях.
2. К сформированному на шаге 1 блоку данных добавляется новый IP-заголовок – транспортный (**IP'** – на схеме); если для туннелированных датаграмм используется протокол UDP, то кроме транспортного добавляется еще один заголовок (**UDP** – на рисунке). Полученная таким образом новая (транспортная) датаграмма отправляется передающим концом туннеля с локального изделия защиты в IP-сеть общего пользования.
3. Коммуникационное оборудование сетей общего пользования выполняет доставку транспортной IP-датаграммы к месту назначения – принимающему концу туннеля на удаленном изделии защиты, используя для этой цели только IP-адрес назначения из заголовка транспортной IP-датаграммы (**IP'**), который может не иметь ничего общего с IP-адресом назначения, указанным в заголовке исходной IP-датаграммы (**IP**).
4. По достижении транспортной IP-датаграммой противоположного (приемного) конца криптотуннеля на удаленном изделии защиты:
   - из транспортной IP-датаграммы извлекается исходная IP-датаграмма в зашифрованном виде;
   - восстанавливаются данные исходной IP-датаграммы путем обратного преобразования (расшифрование, декомпрессия, проверка имитозащиты) с использованием информации из заголовка криптотуннеля (**T**).
5. Восстановленная в исходном виде IP-датаграмма отправляется на дальнейшую доставку получателю обычным образом.

Одновременно с приведенным выше процессом передачи IP-датаграмм по криптотуннелю от локального изделия к удаленному по тому же криптотуннелю выполняется встречный процесс передачи IP-датаграмм от удаленного изделия к локальному.

> *Примечание.* Приведенная на Рис. 3.3 схема, иллюстрирующая процессы, происходящие при передаче исходной IP-датаграммы Пользователя через криптотуннель на L3-уровне, и приведенные выше описания этапов преобразования IP-датаграммы в криптотуннеле в принципе подходят и для иллюстрации процессов, происходящих при передаче через криптотуннель Ethernet-кадров на L2-уровне. Только из *локального* сегмента ЛВС Пользователя

на вход криптотуннеля вместо IP-датаграммы подается исходный Ethernet-кадр, который в итоге инкапсулируется криптотуннелем в транспортную IP-датаграмму. Она через IP-сеть общего пользования передается в виде транспортной IP-датаграммы точно такого же формата, как показано на Рис. 3.3, а на приемном конце криптотуннеля из нее извлекается транспортируемый ею исходный Ethernet-кадр, который затем передается в соответствующий *удаленный* сегмент ЛВС Пользователя.

Ниже приведена информация о форматах заголовков, добавляемых к туннелируемым датаграммам.

Формат упаковки передаваемых данных в криптотуннель – в общем случае имеет вид:

Транспортный IP-заголовок (20 байт) **UDP-заголовок (8 байт)** – необязательная часть транспортной IP-датаграммы **Заголовок туннеля (16 байт) и ключевая информация переменной длины** **Туннелируемые данные** – прошедшие криптообработку передаваемые данные

Транспортный IP-заголовок (20 байт) – в общем случае имеет вид:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Version	**IHL**	**Type of Service**	**Total Length**	
Identification			**Flags**	**Fragment Offset**
Time to Live		**Protocol**	**Header Checksum**	
Source Address				
Destination Address				

Version – ***4***;
IHL – ***5***;
Type of Service – совпадает со значением параметра исходного IP-заголовка;
Total Length – общая длина: длина туннелируемых данных + длина транспортного IP-заголовка (20 байт) + длина UDP-заголовка (если он есть − 8 байт) + заголовок туннеля (16 байт) + длина ключевой информации;
Identification – идентификатор пакетов, используемый для распознавания пакетов, образовавшихся при фрагментации;
Flags – ***0*** или ***DF***;
Fragment Offset – ***0***;
Time to Live – заданное значение TTL транспортной IP-датаграммы;
Protocol – ***4*** (TNL – IP in IP) или ***17*** (UDP или UDPnat);
Header Checksum – рассчитывается;
Source Address – локальный IP-адрес криптотуннеля;
Destination Address – удаленный IP-адрес криптотуннеля.

UDP-заголовок (8 байт) – в общем случае имеет вид:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Порт отправителя	Порт получателя
Длина данных и заголовка	Контрольная сумма

Заголовок туннеля – состоит из постоянной (16 байт) и переменной частей**:**

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

ID (идентификатор туннеля)		Sn (порядковый номер пакета - старшая часть)
Sn (порядковый номер пакета - младшая часть)		Имитовставка - старшая часть
Имитовставка - младшая часть		Длина данных и заголовка
Длина переменной части заголовка	Резерв	Флажки
Переменная часть заголовка *содержимое и длина переменной части заголовка зависит от вида применяемого криптоалгоритма*		

Ниже подробно рассмотрены особенности каждого вида криптотуннелей, поддерживаемых изделием.

3.1.1. *Криптотуннели для защиты обмена IP-датаграммами на L3-уровне*

Защита трафика *IP-датаграмм* с информацией Пользователя, передаваемого через сети общего пользования на L3-уровне, осуществляется изделиями с помощью статических криптотуннелей или TNL-интерфейсов.

3.1.1.1. Принципы работы криптотуннелей на L3-уровне

Общая схема функционирования криптотуннеля, устанавливаемого между локальным и удаленным изделиями и выполняющего криптозащиту трафика IP-датаграмм, передаваемых на L3-уровне через IP-сети общего пользования, представлена на Рис. 3.4. Функционирование криптотуннеля описано ниже.

Криптотуннель, устанавливаемый между изделиями для обеспечения защиты трафика IP-датаграмм на L3-уровне, вне зависимости от типа криптотуннеля (*статический* или *TNL-интерфейс*), можно представить (Рис. 3.4) в виде конструкции, состоящей из двух трубок (двух стволов). Один ствол туннеля выполняет обработку *исходящего* трафика, другой – обработку *входящего*.

Пакеты с информацией передаются между образующими криптотуннель изделиями по каждому из стволов криптотуннеля только в одном направлении: от изделия-отправителя к изделию-получателю.

Тракт обработки трафика защищаемых IP-датаграмм каждым из *однонаправленных* стволов криптотуннеля начинается в БВМ изделия-отправителя, проходит через шифратор и БНМ, продолжается далее через оборудование сетей общего пользования и оканчивается в БНМ изделия-получателя.

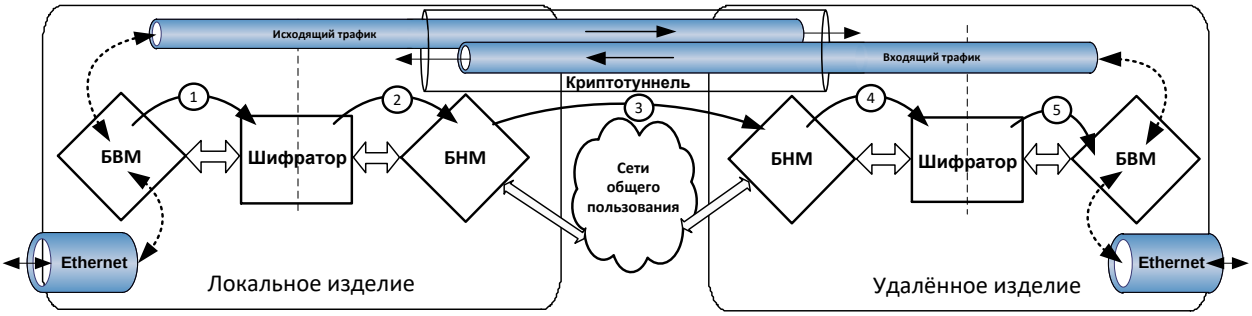


Рис. 3.4 Схема функционирования криптотуннеля при передаче IP-датаграмм на L3-уровне

Передача данных по криптотуннелю на L3-уровне. Каждый правильный Ethernet-кадр, принятый из ЛВС Пользователя Ethernet-интерфейсом БВМ локального изделия, подвергается анализу с целью определения типа данных, транспортируемых этим кадром. Если это не IP-датаграммы или ARP-запросы, дальнейшая обработка принятого Ethernet-кадра прекращается. Если Ethernet-кадром транспортировалась IP-датаграмма, она будет передана на дальнейшую обработку БВМ изделия.

На обработку в конкретный криптотуннель принятая IP-датаграмма будет передана только в том случае, когда она по своим параметрам соответствует *критериям отбора* в этот криптотуннель.

> *Внимание!* Проверка на возможность отправки IP-датаграммы через статические криптотуннели выполняется *раньше* процесса маршрутизации – проверки на возможность отправки IP-датаграммы через TNL-интерфейсы. Т.е. если установлено, что IP-датаграмма соответствует критериям отбора в статический туннель, то проверка возможности отправки IP-датаграммы через TNL-интерфейс не выполняется.

Если IP-датаграмма отобрана для отправки в криптотуннель (независимо от того, по каким критериям – через правила отбора – в статический криптотуннель или через маршрутную таблицу изделия – в TNL-интерфейс), БВМ составляет *задание* для шифратора на обработку *исходной* входящей IP-датаграммы, предусматривающее зашифрование с имитозащитой, и передает ее вместе с заданием шифратору (шаг 1 на схеме Рис. 3.4). Шифратор выполняет криптообработку согласно полученному заданию и результат своей работы передает далее в БНМ изделия (шаг 2 на схеме Рис. 3.4).

БНМ передающего изделия упаковывает (инкапсулирует) поступившие из шифратора данные в IP-датаграмму в транспортном формате (см. Рис. 3.3), добавляя к поступившим данным: заголовок туннеля, заголовок **`UDP`** (если должен использоваться протокол **`UDP`** или **`UDPnat`**) и транспортный IP-заголовок. Сформированная транспортная IP-датаграмма передается на дальнейшую маршрутизацию БНМ и через соответствующий наружный физический интерфейс изделия отправляется в сеть общего пользования (шаг 3 на Рис. 3.4).

Примечания.

1. Последовательность действий при обработке IP-датаграммы, подлежащей передаче по криптотуннелю на L3-уровне (после отбора IP-датаграммы в криптотуннель), не зависит от вида криптотуннеля – статический криптотуннель или TNL-интерфейс.
2. Структуры и форматы данных, которыми при обработке IP-датаграммы в криптотуннеле обмениваются БВМ, шифратор и БНМ передающего и принимающего изделий

унифицированы и не зависят от вида криптотуннеля – статический криптотуннель или TNL-интерфейс.

Прием данных по криптотуннелю на L3-уровне. Если на Ethernet-интерфейс БНМ удаленного (принимающего) изделия поступила *туннелированная* IP-датаграмма (т.е. поле **Protocol** IP-датаграммы имеет значение ***4*** или ***17***), то БНМ изделия начинает поиск криптотуннеля, соответствующего данным из заголовка туннеля принятой IP-датаграммы. Сначала выполняется поиск в списке статических туннелей, затем (если соответствующий статический туннель не будет найден) поиск продолжится среди туннельных интерфейсов (TNL-интерфейсов).

После того как криптотуннель будет найден, программа управления БНМ извлекает из транспортной IP-датаграммы исходную IP-датаграмму в зашифрованном виде и оформляет задание шифратору на ее обработку. Исходная IP-датаграмма в зашифрованном виде вместе с заданием отправляются в шифратор (шаг 4 на Рис. 3.4). Шифратор выполняет восстановление переданных через сеть исходных данных (расшифрование и проверку имитозащиты), после чего IP-датаграмма в исходном виде передается на маршрутизацию в БВМ (шаг 5 на Рис. 3.4) для доставки получателю во внутренних ЛВС Пользователя.

Если принадлежность принятой туннелированной IP-датаграммы к криптотуннелю не обнаружена, считается, что эта IP-датаграмма предназначена не для туннелей данного изделия и ее обработка продолжается на общих основаниях – IP-датаграмма отправляется на маршрутизацию в БНМ для обеспечения ее дальнейшего продвижения по сетям общего пользования (например, это может быть *транзитная* для данного изделия IP-датаграмма).

Ниже алгоритмы упаковки передаваемых данных в туннель и их распаковки рассмотрены более подробно.

Алгоритм отправки IP-датаграмм в криптотуннель. Для каждой IP-датаграммы, предназначенной к отправке в сети общего пользования, БВМ выполняет проверку, должна ли она быть упакована в криптотуннель.

1. Сначала просматривается список статических криптотуннелей (сверху вниз, начиная с первой строки) до первого совпадения параметров датаграммы и правил отбора в криптотуннель. Совпадение фиксируется в том случае, если выполнены следующие условия.
   - Значение параметра **Протокол** правила отбора в туннель совпадает со значением поля **Protocol** IP-датаграммы (если поле **Протокол** правила отбора в туннель имеет значение *ANY*, то условие считается выполненным при любом значении поля **Protocol** датаграммы).

     Замечание. Значениям *ICMP*, *TCP*, *UDP* и *TNL* элемента **Протокол** из правила отбора в туннель соответствуют значения ***1***, ***6***, ***17***, и ***4*** поля **Protocol** IP-датаграммы.
   - Значение параметра **Адрес отправителя** правила отбора в туннель совпадает со значением поля **Source Address** IP-датаграммы (проверка совпадения выполняется по числу старших бит, заданному в правиле отбора в туннель как число **Значащих бит** в адресе отправителя).
   - Значение параметра **Адрес получателя** правила отбора в туннель совпадает со значением поля **Destination Address** IP-датаграммы (проверка совпадения выполняется по числу старших бит, заданному в правиле отбора в туннель как число **Значащих бит** в адресе получателя).
   - При ненулевом значении **Начального номера порта** правила отбора в туннель значения поля **Destination Port** заголовков TCP- или UDP-датаграммы попадают в диапазон значений **Начальный номер порта – Конечный номер порта** правила отбора в туннель.

   Если зафиксировано совпадение и параметр **Режим** правила отбора в туннель имеет значение *разрешить*, датаграмма вместе с заданием на упаковку в туннель передается в шифратор.
2. Если не установлено соответствия IP-датаграммы критериям ее отбора в статические туннели, то программа управления БВМ начинает поиск подходящего туннельного интерфейса (TNL-интерфейса).
   - Из заголовка датаграммы извлекается IP-адрес назначения и по маршрутной таблице БВМ
   - изделия определяется имя интерфейса, которому IP-пакет передается на отправку.
   - Если искомым оказывается TNL-интерфейс, то датаграмма вместе с заданием на упаковку в туннель передается в шифратор.
3. Шифратор зашифровывает IP-датаграмму (исходные заголовок и данные) как единый блок данных и передает ее на обработку БНМ.
4. БНМ формирует транспортную IP-датаграмму (добавляет транспортный IP-заголовок, UDP-заголовок (если требуется), заголовок туннеля) и выполняет ее отправку через свой маршрутизатор.

   Если на БВМ изделия для IP-датаграммы не найдено соответствующего криптотуннеля (ни статического туннеля, ни TNL-интерфейса), то IP-датаграмма обрабатывается без упаковки в криптотуннель – она отправляется на маршрутизацию БВМ изделия как *транзитная* датаграмма.

Алгоритм приема IP-датаграмм из криптотуннеля. При поступлении из сети общего пользования на интерфейс БНМ изделия очередной датаграммы БНМ выполняет проверку, пришла IP-датаграмма по криптотуннелю или нет – проверяется значение поля **Protocol** транспортного заголовка IP-датаграммы. Если поле имеет значение ***4*** (IP in IP) или ***17*** (UDP или UDPnat), это значит, что IP-датаграмма потенциально может *туннелированной* – нуждаться в обработке каким-либо из криптотуннелей.

Если поле **Protocol** имеет любое *другое* значение, то IP-датаграмма считается нетуннелированной и сразу отправляется на обычную маршрутизацию БНМ.

1. Поиск криптотуннеля, по которому пришла туннелированная IP-датаграмма, начинается с просмотра списка статических криптотуннелей. Просмотр их списка выполняется сверху вниз, начиная с первой строки. Датаграмма считается принадлежащей статическому криптотуннелю, если выполняются следующие *условия*.
   - Значение поля **Source Address** транспортного IP-заголовка совпадает со значением параметра **Удаленный IP-адрес** туннеля.
   - Значение поля **Destination Address** Транспортного IP-заголовка совпадает со значением параметра **Локальный IP-адрес** туннеля.
   - Значение поля **Идентификатор туннеля** (**ID**) в заголовке туннеля IP-датаграммы совпадает со значением параметра туннеля **Идентификатор туннеля** в его описателе.
   - *Только для UDP-датаграмм*:
     - значение поля UDP-заголовка **Порт отправителя** совпадает со значением параметра **Порт получателя** туннеля;
     - значение поля UDP-заголовка **Порт получателя** совпадает со значением параметра **Порт отправителя** туннеля.

   Если будет найден статический криптотуннель, которому принадлежит IP-датаграмма, то она вместе с заданием на извлечение из туннеля передается в шифратор.
2. Если в списке статических криптотуннелей не найдено туннеля, соответствующего параметрам IP-датаграммы, начинается обработка списка TNL-интерфейсов. Обработка списка TNL-интерфейсов выполняется построчно сверху вниз, начиная с первой строки.
3. Датаграмма считается подлежащей обработке TNL-интерфейсов, если выполняются те же *условия*, что и при анализе соответствия параметров IP-датаграммы параметрам списка статических туннелей (см. выше).

   Если будет найден TNL-интерфейс, которому принадлежит IP-датаграмма, то она вместе с заданием на извлечение из криптотуннеля передается в шифратор.
4. В шифраторе выполняется извлечение IP-датаграммы из туннеля.
   - При извлечении из криптотуннеля: отбрасываются транспортный IP-заголовок, UDP-заголовок (если он имеется) и заголовок туннеля.
   - Выполняется расшифрование данных и IP-заголовка исходной IP-датаграммы в соответствии со сформированным БНМ заданием.
5. Далее IP-датаграмма передается шифратором в БВМ на маршрутизацию и доставку через соответствующий интерфейс БВМ в ЛВС Пользователя адресату.

> Если не найдено криптотуннеля (ни статического криптотуннеля, ни TNL-интерфейса), соответствующего параметрам туннелированной IP-датаграммы, то принятая БНМ IP-датаграмма отправляется на дальнейшую обработку – маршрутизацию БНМ изделия – *без распаковки*. В этом случае БНМ изделия используется в качестве обычного маршрутизатора – *транзитного* узла доставки туннелированных датаграмм, адресованных другим узлам ЗСПД.

3.1.1.2. Создание и настройка статических криптотуннелей

> *Внимание!* Механизм статических криптотуннелей поддерживается новыми изделиями в целях обеспечения совместимости при встречной работе изделий нового и старого поколений. Кроме того, применение статических туннелей в ряде случаев может оказаться предпочтительным, т.к. статические криптотуннели позволяют более *избирательно* очертить круг отбираемых в криптотуннель IP-датаграмм.

Обработка трафика статическими туннелями осуществляется с момента запуска изделия до его останова. Параметры настройки обоих окончаний криптотуннелей задаются администраторами соответствующих узлов и согласовываются для обоих концов туннеля с помощью любых доступных технологических средств коммуникации (телефон, e-mail, циркуляр Администрации ЗСПД и т. п.), т. е. без использования IP-сети и специальных алгоритмов.

Для создания статических туннелей (или редактирования описателей ранее созданных статических туннелей), а затем управления их работой следует выбрать цепочку альтернатив~~а~~ ГМ: **Настройка** ⇨ **Защита** ⇨ **Туннели**.

В ответ на видеомонитор ЛКУ будет выдано меню управления описателями статических криптотуннелей изделия, не содержащее описателей или содержащее список созданных ранее описателей статических криптотуннелей, аналогичное представленному на Рис. 3.5.

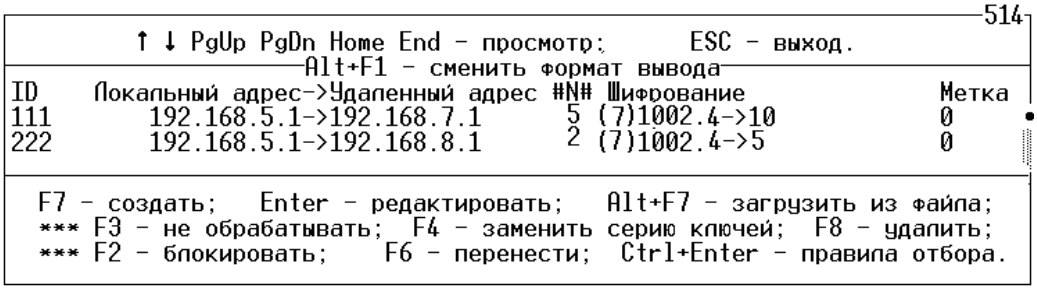


Рис. 3.5 Меню управления описателями статических криптотуннелей изделия

Описание каждого криптотуннеля в меню управления описателями (Рис. 3.5) занимает одну строку, в которую выводятся значения следующих параметров статического туннеля:

- в колонке **ID** – идентификатор криптотуннеля;
- в колонках **Локальный адрес** и **Удаленный адрес** – IP-адреса соответственно локального и удаленного концов туннеля;
- в колонке **#N#** – число правил отбора, сформированных при настройке параметра **Правила отбора** во время создания или редактирования описателя туннеля;
- в колонке **Шифрование** приведены криптопараметры в формате: число в скобках – номер ключевой зоны; затем – номер серии ключей; затем – локальный криптономер и (после стрелки вправо) удаленный криптономер;
- в колонке **Метка** – метка статического туннеля.

Сразу после создания туннель готов к работе, цвет соответствующей строки описателя – *черный* (туннель помечается как *рабочий*).

Статический туннель готов к работе сразу после создания, цвет соответствующей строки описателя – *черный* (туннель помечен как *рабочий*).

Если туннель помечен (см. ниже) как не *обрабатываемый* (выключенный), цвет строки – *зеленый*.

Если туннель *заблокирован* (см. ниже), цвет соответствующей строки – *красный*.

Формат вывода параметров туннеля может быть таким, как представлено на Рис. 3.5, а может быть изменен с помощью команды **Alt+F1 – сменить формат вывода** (команда приведена на линии рамки над списком туннелей). По этой команде вместо последних трех колонок на видеомонитор ЛКУ выводится комментарий, заданный в карточке туннеля в графе **Описание** (см. пояснения к Рис. 3.8, с. 80).

На рамке в правом верхнем углу (Рис. 3.5) выводится десятичное число, определяющее длину файла, содержащего описатели (в байтах), полезное для контроля при настройке изделия. Максимально возможная длина файла – ***256*** Кбайт.

Все операции по созданию, редактированию и управлению туннелями выполняются с помощью функциональных клавиш, назначение которых приведено в нижней части окна (Рис. 3.5). Далее приведены пояснения к выполнению этих операций.

F7 – **создать** (Рис. 3.5). Нажатие клавиши <F7> приводит к выводу на экран бланка создания и настройки статического криптотуннеля (Рис. 3.8, с. 80). Пояснения к работе с бланком приведены ниже в данном разделе.

Enter – **редактировать** (Рис. 3.5). Нажатие клавиши <Enter> приводит к выводу на экран бланка создания и настройки с параметрами того туннеля, на описателе которого установлен курсор (Рис. 3.8, с. 80), после чего предоставляется возможность изменить значения параметров созданного ранее туннеля. Пояснения к работе с бланком приведены ниже в данном разделе.

Alt+F7 – **загрузить из файла** (Рис. 3.5). Функция позволяет загрузить описание туннелей из файла. После нажатия комбинации клавиш <Alt+F7> выводится представленный на Рис. 3.6 запрос:

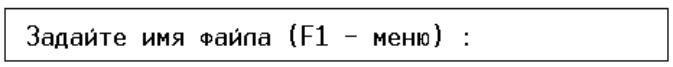


Рис. 3.6 Запрос на ввод имени файла с описателями статических туннелей

На запрос должно быть введено обязательное имя **tnl_tcp.ema** – системное имя файла, в котором хранится описание статических туннелей. Имя (с указанием пути) можно ввести с клавиатуры (после чего нажать клавишу <Enter>) или нажать клавишу <F1> и получить на экране окно, позволяющее просмотреть и найти папки и файлы на любом из доступных дисков.

Если предполагается использовать описание туннелей, имеющихся в архиве изделия, следует в папке **D:\DIONISWT.CFG** (папка содержит архив всех конфигураторов изделия – см. раздел 4.1.8, с. 143) найти нужный конфигуратор и выбрать в нем файл **tnl_tcp.ema** – перевести курсор на имя файла и нажать клавишу <Enter>. Перед тем как загрузить описание туннелей из файла, программа управления выдаст запрос: *добавить* описатели туннелей к списку или *заменить* имеющийся список туннелей целиком на другой.

> *Примечание.* Файл **tnl_tcp.ema** может находиться на съемном носителе, что позволяет перенести описание статических туннелей, сформированное на другом изделии.

F3 – **не обрабатывать** (Рис. 3.5). Нажатие клавиши <F3> помечает туннель, указанный курсором, как *не обрабатываемый* (выключенный). На экране цвет соответствующей строки при этом изменяется на *зеленый*. Повторное нажатие клавиши <F3> вернет туннель в рабочее состояние.

F2 – **блокировать** (Рис. 3.5). Нажатие клавиши <F2> блокирует туннель, указанный курсором. На экране цвет соответствующей строки при этом изменяется на *красный*. Через заблокированный туннель не будут передаваться датаграммы. Повторное нажатие клавиши <F2> туннель разблокирует.

F4 – **заменить серию ключей** (Рис. 3.5). Нажатие клавиши <F4> позволяет заменить серию ключей одновременно во всех описателях статических туннелей.

F6 – **перенести** (Рис. 3.5). Использование клавиши <F6> позволяет переместить строку описателя криптотуннеля в списке туннелей. Чтобы выполнить перемещение, следует установить курсор на строку, которую необходимо переместить, после чего нажать клавишу <F6> – при этом цвет строки изменится на *белый*. Далее следует переместить курсор в списке криптотуннелей (Рис. 3.5) на ту строку списка, после которой должна быть размещена обозначенная белым цветом строка описателя, и повторно нажать клавишу <F6>. В результате описатель криптотуннеля займет требуемое положение в списке.

> *Внимание!* Порядок следования описателей статических криптотуннелей в списке имеет значение, так как при отправке IP-датаграммы в сеть проверяется по списку описателей туннелей совпадение параметров IP-датаграммы с правилами отбора в туннель, при этом список описателей статических криптотуннелей (см. Рис. 3.5) просматривается *сверху вниз*.

Ctrl+Enter – **правила отбора** (Рис. 3.5). При нажатии комбинации клавиш <Ctrl+Enter> на видеомонитор ЛКУ выводится полный список правил отбора *всех* статических криптотуннелей изделия, аналогичный представленному на Рис. 3.7. Список можно визуально проконтролировать на видеомониторе ЛКУ, а также можно задокументировать текущее состояние списка правил отбора – занести в журнал (файл **LOG.EMA**), для чего следует нажать клавишу <пробел>.

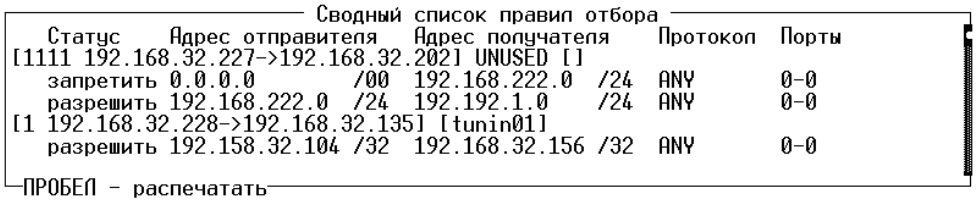


Рис. 3.7 Полный список правил отбора статических криптотуннелей

Создание и настройка статического криптотуннеля

Бланк создания и настройки статического криптотуннеля изделия представлен на Рис. 3.8. Пояснения, необходимые при работе с бланком, приведены ниже.

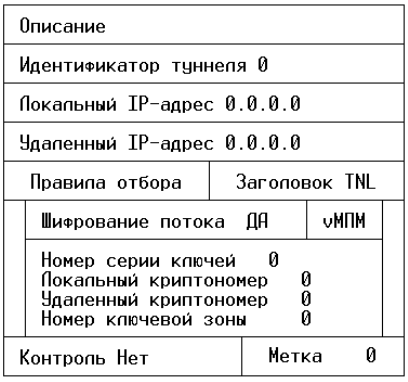


Рис. 3.8 Бланк создания и настройки статического криптотуннеля

Описание (Рис. 3.8) – параметр позволяет задать до 32-х символов произвольного текста. Его можно увидеть на экране, если изменить формат вывода списка туннелей (см. Рис. 3.5, с. 790), выдав команду **Alt+F1** – **сменить формат вывода**.

Идентификатор туннеля (Рис. 3.8) – параметр задает целое десятичное число в диапазоне от **0** до **32767** (до 5 цифр), идентифицирующее криптотуннель. Значение идентификатора должно совпадать на обоих концах туннеля – в списках статических криптотуннелей на обоих изделиях, между которыми организуется туннель.

> *Внимание!* Значение идентификатора криптотуннеля в составе ЗСПД должно быть *уникальным* среди узлов, входящих в одну и ту же ключевую зону.

Локальный IP-адрес (Рис. 3.8) – параметр задает IP-адрес локального конца криптотуннеля. Этот адрес будет подставлен в качестве адреса отправителя (**Source Address**) в IP-заголовок транспортной IP-датаграммы при упаковке датаграммы в туннель (см. раздел 3.1, с. 73).

Удаленный IP-адрес (Рис. 3.8) – параметр задает IP-адрес удаленного конца туннеля. Этот адрес будет подставлен в качестве адреса назначения (**Destination Address**) в IP-заголовок транспортной IP-датаграммы при упаковке датаграммы в туннель (см. раздел 3.1, с. 73).

Правила отбора (Рис. 3.8) –параметра обеспечивает вызов меню управления правилами отбора в статический туннель, аналогичного представленному на Рис. 3.9. Правила отбора регулируют выбор из потока всех входящих IP-датаграмм тех, которые должны быть направлены на дальнейшую обработку в конкретный криптотуннель, т.е. тех IP-датаграмм, параметры которых совпали с правилами отбора.

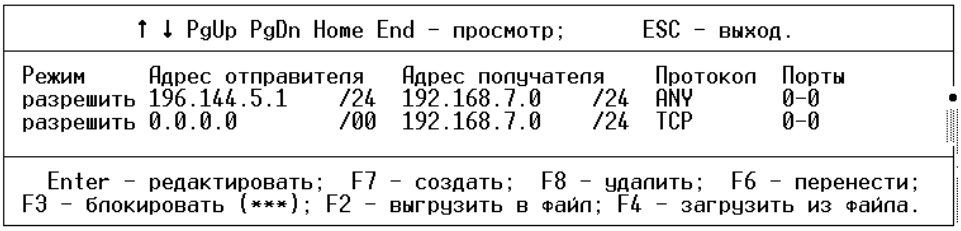


Рис. 3.9 Меню управления правилами отбора в статический криптотуннель

F7 – **создать** (Рис. 3.9). Нажатие клавиши <F7> приводит к выводу на видеомонитор бланка создания и настройки правила отбора в статический криптотуннель, представленному на Рис. 3.10 (с. 82). Пояснения к работе по настройке параметров этого бланка приведены ниже в данном разделе.

> *Примечание.* Описатель созданного правила будет помещен в общий список правил отбора (Рис. 3.9) первой строкой, если список был пуст, или строкой, следующей за строкой того описателя, на которую был установлен курсор непосредственно перед нажатием клавиши <F7>. Это следует иметь в виду, так как порядок следования описателей в списке правил влияет на результаты отбора IP-датаграмм в туннель.

Enter – **редактировать** (Рис. 3.9). Нажатие клавиши <Enter> приводит к выводу на видеомонитор ЛКУ бланка создания и настройки правила отбора, аналогичного представленному на Рис. 3.10 (с. 82); бланк содержит параметры того правила, на котором в меню управления правилами отбора (Рис. 3.9) был установлен курсор. Операция предоставляет возможность откорректировать параметры правила.

F8 – **удалить** (Рис. 3.9). Нажатие клавиши <F8> приводит к удалению строки с описателем правила отбора, на которую был установлен курсор.

F6 – **перенести** (Рис. 3.9). Использование клавиши <F6> позволяет переместить строку описателя в списке правил отбора. Чтобы выполнить перемещение, следует установить курсор на строку описателя правил, которую необходимо переместить, и нажать клавишу <F6> –цвет строки изменится на *белый*. Далее следует переместить курсор на ту строку списка описателей правил (Рис. 3.9), после которой должна быть размещена обозначенная белым цветом строка, и повторно нажать клавишу <F6>. В результате описатель правила отбора займет требуемое положение в списке.

> *Примечание.* Между первым и вторым нажатиями клавиши <F6> разрешается использовать только клавиши для перемещения курсора; нажатие любой другой клавиши приводит к сбросу первоначальной отметки описателя правила отбора.

F3 – **блокировать** (Рис. 3.9). Нажатие клавиши <F3> приводит к блокированию правила отбора, на строку с описателем которого был установлен курсор (программа управления игнорирует заблокированное правило). Цвет соответствующей строки изменится на *красный*. Повторное нажатие клавиши <F3> блокировку правила снимает. Указанная возможность удобна при комплексной настройке взаимодействия изделия и приложений Пользователя в составе ЗСПД.

F2 – **выгрузить в файл** (Рис. 3.9). Нажатие клавиши <F2> приводит к выдаче запроса на ввод имени файла (см. Рис. 2.3, с. 24), в который будет записан список правил отбора. Имя файла можно ввести с клавиатуры или можно нажать клавишу <F1> и получить на видеомониторе ЛКУ окно менеджера файлов, позволяющего просмотреть и найти нужные папки и файлы на любом из доступных дисков. Текст описаний правил отбора можно редактировать. Эта возможность позволяет оперативно заимствовать список правил отбора с другого аналогичного изделия.

F4 – **загрузить из файла** (Рис. 3.9). Нажатие клавиши <F4> приводит к выдаче запроса на ввод имени файла (см. Рис. 2.3, с. 24), из которого следует загрузить список правил отбора, сформированный ранее или заимствованный с аналогичного изделия.

На Рис. 3.10 представлен бланк создания и настройки правил отбора в статический криптотуннель.

Режим разрешить	Протокол ANY	
Фиксировать нет		
Диапазон номеров портов 0 - 0		
	Адрес	Зн. бит
Отправитель	0.0.0.0	0
Получатель	0.0.0.0	0

Рис. 3.10 Бланк создания и настройки правила отбора в статический криптотуннель

Режим (Рис. 3.10). Параметр может принимать значение *разрешить* или *запретить*. В первом случае входящая IP-датаграмма, соответствующая остальным параметрам правила, будет считаться отобранной в данный криптотуннель, во втором случае IP-датаграмма в туннель отобрана не будет и ее обработка будет продолжена на общих основаниях согласно алгоритму работы маршрутизатора.

Протокол (Рис. 3.10). Параметру может быть присвоено одно из следующих значений:

ANY, *ICMP*, *TCP*, *UDP*, *TNL*.

Фиксировать (Рис. 3.10). Параметр может принимать значения *да* или *нет*, определяя, будет ли выполняться протоколирование последовательности обработки IP-датаграмм, проходящих через статический криптотуннель, в журналах изделия

Диапазон номеров портов (Рис. 3.10). Параметр имеет смысл только для протоколов ***TCP*** и **UDP**. Он задает проверку значения порта назначения в IP-заголовках TCP- или UDP-датаграмм, транспортируемых подлежащими проверке IP-датаграммами. Порт назначения TCP- или UDP-пакета считается удовлетворяющим данному правилу отбора, если его значение укладывается в диапазон, заданный параметром **Диапазон номеров портов**.

Если обе цифры параметра **Диапазон номеров портов** имеют одинаковое *ненулевое* значение, то данному правилу отбора удовлетворяют TCP- или UDP-пакеты с единственным значением поля **порт назначения** заголовка пакета.

Если обе цифры параметра **Диапазон номеров портов** являются *нулями*, то проверка поля **порт назначения** заголовка IP-датаграммы не производится, т.е. любое значение порта назначения датаграммы считается удовлетворяющим данному правилу отбора.

Для параметров **Адрес: Отправитель** и **Адрес: Получатель** (Рис. 3.10) можно задать значения параметру **Зн. бит** – длину маски подсети, целое десятичное число в диапазоне от **0** до **32**. В этом случае в процессе отбора значения IP-адресов, заданные в бланке создания и настройки правил отбора, и значения IP-адресов датаграммы будут сравниваться только по заданному числу старших бит адресов.

Примечание. Количество сформированных правил отбора в каждый из статических криптотуннелей выводится в список описателей статических криптотуннелей изделия в колонке под заголовком **#N#** (см. Рис. 3.5, с. 79).

Заголовок (Рис. 3.8). При выборе альтернативы на видеомонитор ЛКУ будет выдан бланк настройки типа транспортного протокола для передачи туннелированных IP-датаграмм, представленный на Рис. 3.11.

Формат заголовка UDP
Порт отправителя 500
Порт получателя 500

Рис. 3.11 Бланк настройки типа транспортного протокола туннелированной IP-датаграммы

Формат заголовка (Рис. 3.11). Параметр может принимать одно из следующих значений:

TNL – полю ***Protocol*** в IP-заголовках исходящих туннелированных IP-датаграмм будет присвоено значение, равное *4* (что означает, что сформированная туннелированная IP-датаграмма представляет собой инкапсуляцию IP in IP);

UDP – полю ***Protocol*** в IP-заголовках исходящих туннелированных IP-датаграмм будет присвоено значение *17*. Политика отдельных провайдеров препятствует передаче

туннелированных данных (когда полю ***Protocol*** в IP-заголовках исходящих IP-датаграмм присвоено значение *4*) через контролируемые ими сети передачи данных. Присвоение значения ***UDP*** или ***UDPnat*** параметру **Формат заголовка** позволяет добиться передачи трафика через такие сети.

UDPnat – в этом случае полю ***Protocol*** в IP-заголовках исходящих туннелированных IP-датаграмм будет присвоено значение *17*. Присвоение параметру **Формат заголовка** (Рис. 3.11) значения ***UDPnat*** обеспечивает возможность передачи туннелированных данных в режиме клиент-сервер из-под NAT-обработчика.

Если параметр **Формат заголовка** имеет значение ***UDP*** или ***UDPnat***, то параметрам **Порт отправителя** и **Порт получателя** IP-датаграмм можно присвоить значения, отличные от умалчиваемых (по умолчанию оба параметра имеют значение *500*).

Шифрование потока (Рис. 3.8). Параметр для статических криптотуннелей всегда имеет значение ***ДА***, что означает безусловное выполнение *зашифрования* информации, передаваемой по статическому криптотуннелю.

Номер ключевой зоны (Рис. 3.8) – целое десятичное число в диапазоне от ***1*** до ***999*** или ***0*** (число **7** в скобках под заголовком **Шифрование** на Рис. 3.5)

Номер серии ключей (Рис. 3.8) – целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети (число **1002** под заголовком **Шифрование** на Рис. 3.5).

Локальный криптономер (Рис. 3.8) – целое десятичное число (до 5 цифр), соответствующее криптографическому номеру данного изделия в криптографической сети (число **4** под заголовком **Шифрование** на Рис. 3.5).

Удаленный криптономер (Рис. 3.8) – целое десятичное число (до 5 цифр), соответствующее криптографическому номеру в криптографической сети того удаленного изделия, с которым будет выполняться обмен информацией по данному криптотуннелю (число **10** под заголовком **Шифрование** на Рис. 3.5).

Примечание. При настройке значений параметров **Номер ключевой зоны**, **Номер серии ключей** и **Локальный криптономер** следует руководствоваться комментариями, приведенными в разделе 2.4.2, с. 39 при описании настройки аналогичных параметров меню настройки криптопараметров TNL-интерфейса (Рис. 2.24, с. 40).

vXXX (Рис. 3.8) – параметр управления криптографической совместимостью. Определяет вариант реализации в данном туннеле версии криптографического алгоритма обработки туннелируемых IP-пакетов; параметр необходим для настройки синхронной обработки IP-пакетов криптоалгоритмами одного и того же варианта реализации на приемном и передающем концах настраиваемого туннеля.

Параметр может принимать следующие значения:

vМПМ – версия криптографического алгоритма, реализованная в изделиях серии М-479Рх;

v07Ф – версия криптографического алгоритма, реализованная в изделиях М-479К;

v07М – версия криптографического алгоритма, реализованная в изделиях М-479Ж.

Внимание! При настройке криптотуннелей с применением изделия М-479Р2 параметру **vXXX** может быть присвоено *только* значение *vМПМ*.

Контроль (Рис. 3.8) – по умолчанию параметр имеет значение *Нет*, при этом режим самоконтроля криптотуннеля не запускается. При выборе параметра на видеомонитор ЛКУ выдается представленное на Рис. 3.12 меню настройки механизма самоконтроля состояния криптотуннеля, осуществляемого с помощью специального контрольного пакета (KEEPALIVE).

Интервал отправки запросов	0
Максимальное время ожидания ответов	0

Рис. 3.12 Меню настройки механизма самоконтроля состояния криптотуннеля (KEEPALIVE)

Интервал отправки запросов (Рис. 3.12) – выбор параметра позволяет установить значение величины интервала (единица измерения – секунда), через который будут регулярно (пока криптотуннель работоспособен) выдаваться на удаленный конец криптотуннеля зондирующий пакет специального формата (KEEPALIVE).

Максимальное время ожидания ответов (Рис. 3.12) – интервал времени (единица измерения – секунда), до истечения которого, начиная с момента отправки зондирующего пакета, криптотуннель считается работоспособным. Если по истечении этого интервала ответ на зондирующий пакет не получен, криптотуннель считается неработоспособным.

Метка (Рис. 3.8) – целое десятичное число в диапазоне от ***0*** до ***255***, служит для взаимной привязки данного криптотуннеля и конкретной PING-пробы (подробнее см. раздел 2.7.3, с. 60).

Пример конфигурирования статических криптотуннелей

В качестве примера конфигурирования статических криптотуннелей рассмотрим схему построения VPN некоторой организации, офисы которой расположены в трех территориально удаленных городах – например, в Москве, Краснодаре и Орле. Возможная схема организации связи в этом случае представлена на Рис. 3.13.

Каждый из офисов использует ЛВС, работающую в фиктивном адресном пространстве **`10.x.0.0/16`**. Для связи между локальными сетями офисов в качестве транспортной сети используется сеть Internet, в качестве устройств, обеспечивающих защиту передаваемой по каналам связи информации пользователей ЛВС, изделия серии М-479Px.

> *Примечание.* Изделия серии М-479Px могут обеспечивать защиту как на L3-уровне обмена данными (в качестве *криптомаршрутизатора*), так и на L2-уровне (в качестве средства организации *криптомоста*). Для организации функционирования криптотуннелей можно выбрать механизмы TNL-интерфейсов или статических туннелей (на L3-уровне обмена данными), а также механизм L2–TNL-интерфейсов (на L2-уровне обмена данными).
>
> Для решения предложенной в примере задачи используем изделия в качестве *криптомаршрутизаторов*, применяя для организации криптотуннелей механизм *статических криптотуннелей*.

IP-адреса внутренних и внешних сетевых интерфейсов изделий приведены на схеме.

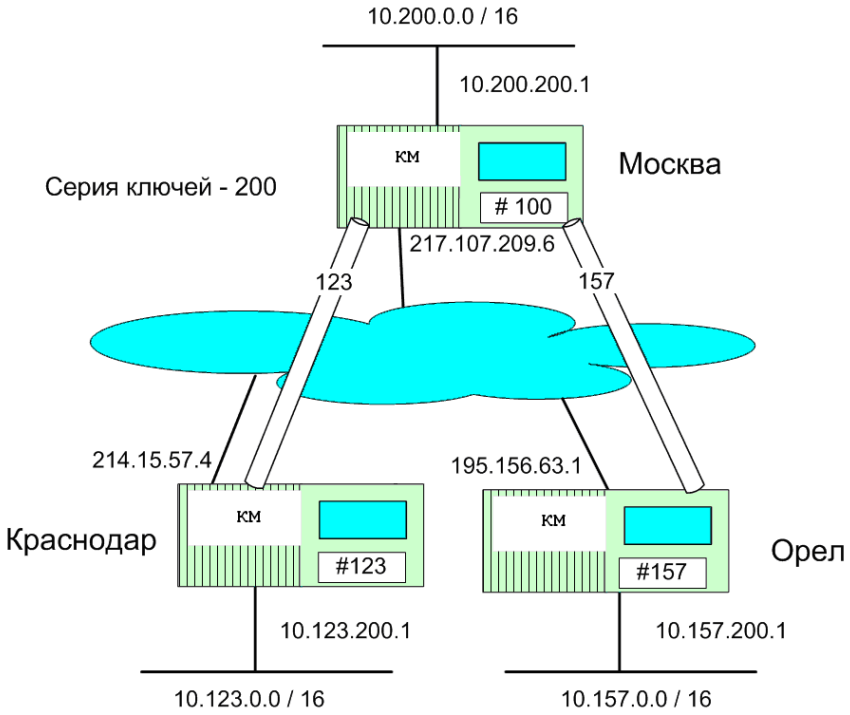


Рис. 3.13 Схема организации связи, иллюстрирующая применение статических криптотуннелей

Ставится задача организации VPN таким образом, чтобы пользователи (абоненты) локальной сети любого офиса могли обращаться к информационным ресурсам всех остальных офисов.

Сначала следует определить *топологию* сети, обеспечивающей работу офисов организации. Наиболее эффективной в этом случае является организация связи по схеме «каждый с каждым», но она требует организации большого количества криптотуннелей между ЛВС каждого из офисов, а именно (**`n-1`**), где **`n`** – число взаимодействующих офисов в сети VPN (в нашем примере необходима организация двух туннелей между ЛВС каждого из офисов).

Если информационный обмен сосредоточен в основном на направлениях `центральный офис – периферийный офис`, то VPN целесообразно строить по топологии «звезда». В этом случае в каждом периферийном офисе необходима организация только одного туннеля с центром, при этом потоки информации между ЛВС периферийных офисов (Краснодар, Орел) будут проходить *транзитом* через центральный офис (Москва), где будет выполняться процедура *переупаковки* данных из одного туннеля в другой.

После определения топологии сети необходимо спланировать криптографические параметры VPN, для чего следует получить ключевые документы с заданным номером серии ключей (серия **`200`** в нашем примере) и назначить криптографические номера для ЛВС каждого из офисов сети (в примере это: **`100`** – Москва, **`123`** – Краснодар, **`157`**– Орел).

После уточнения топологии сети, структуры криптопараметров узлов связи, типа и структуры криптотуннелей следует настроить статические криптотуннели на направлениях Москва-Краснодар и Москва-Орел, пользуясь значениями параметров криптотуннелей, приведенными ниже в таблицах.

Туннель между офисами	**Москва**	**Краснодар**
Идентификатор туннеля	***123***	***123***
Локальный IP-адрес	***217.107.209.6***	***214.15.57.4***
Удаленный IP-адрес	***214.15.57.4***	***217.107.209.6***
Шифрование потока	***ДА***	***ДА***
Номер серии ключей	***200***	***200***
Локальный криптономер	***100***	***123***
Удаленный криптономер	***123***	***100***

Правила отбора

Москва	**Краснодар**
разрешить 10.0.0.0/8 10.123.0.0/16 **ANY** 0-0	**запретить** 0.0.0.0/00 10.123.0.0/16 **ANY** 0-0 **разрешить** 10.123.0.0/16 10.0.0.0/8 **ANY** 0-0

Туннель между офисами	**Москва**	**Орел**
Идентификатор туннеля	***157***	***157***
Локальный IP-адрес	***217.107.209.6***	***195.156.63.1***
Удаленный IP-адрес	***195.156.63.1***	***217.107.209.6***
Шифрование потока	***ДА***	***ДА***
Номер серии ключей	***200***	***200***
Локальный криптономер	***100***	***157***
Удаленный криптономер	***157***	***100***

Правила отбора

Москва	**Орел**
разрешить 10.0.0.0/8 10.157.0.0/16 **ANY** 0-0	**запретить** 0.0.0.0/00 10.157.0.0/16 **ANY** 0-0 **разрешить** 10.157.0.0/16 10.0.0.0/8 **ANY** 0-0

Особое внимание при настройке статических криптотуннелей следует уделить *правилам отбора* в туннель. Ошибки в правилах отбора могут приводить к недоступности части офисов VPN, а также к появлению информационных циклов (петель), приводящих к резкому возрастанию трафика через внешнюю сеть.

В нашем примере московский узел должен разрешить упаковку в соответствующий туннель IP-датаграмм, предназначенных только для конкретной периферийной сети.

На периферийных концах туннелей должны быть заданы правила отбора для сетей всех остальных офисов (в Краснодаре – для Москвы и Орла). Однако такой подход резко увеличивает количество правил отбора в туннели периферийных узлов при увеличении количества взаимодействующих офисов. Поэтому в примере рассмотрен другой подход к формированию правил отбора в туннели на периферийных узлах.

Сначала запрещается отбор в туннель на Москву IP-датаграмм, адресованных станциям внутренней ЛВС офиса, а затем разрешается упаковка в туннель IP-датаграмм, адресованных всем остальным узлам VPN-сети. Другими словами, вместо перечисления IP-адресов всех соседних офисов дается общее разрешение на всю VPN, за вычетом адресатов собственной сети.

3.1.1.3. Создание и настройка TNL-интерфейсов

Процедуры создания и настройки TNL-интерфейсов, обеспечивающих защиту трафика IP-датаграмм, передаваемого через сети общего пользования на L3-уровне, приведены в разделе 2.4.2, с. 39.

3.1.1.4. Организация защиты трафика IP-датаграмм на L3-уровне

Для обеспечения функционирования технологии защиты обмена IP-датаграммами на L3-уровне изделие применяется как *криптомаршрутизатор*.

Для организации функционирования изделия в этом режиме необходимо:

- создать и настроить, руководствуясь схемой организации связи, необходимое число сетевых физических Ethernet-интерфейсов на БВМ и БНМ изделия (см. раздел 2.3.1, с. 25) – как основу для телекоммуникационного обмена изделия с удаленными сегментами ЛВС Пользователя и сетями общего пользования;
- создать и настроить необходимые криптотуннели, руководствуясь схемой организации связи и используя исходные данные Администрации ЗСПД о криптопараметрах сети, для чего:
  - выбрать предпочтительный способ организации криптотуннелей для защиты обмена IP-датаграммами на заданном *направлении* – с помощью статических криптотуннелей или с помощью TNL-интерфейсов;
  - создать и настроить статические криптотуннели (см. раздел 3.1.1.2, с. 78) на заданных направлениях обмена – при необходимости;
  - создать и настроить TNL-интерфейсы (раздел 2.4.2, с. 39) на заданных направлениях обмена – при необходимости;
- создать и настроить виртуальные VLAN-интерфейсы (см. раздел 2.4.1, с. 36) и GRE-интерфейсы (см. раздел 2.4.3, с. 43), обеспечивающие дополнительную необходимую обработку проходящего через базовый Ethernet-интерфейс трафика – при необходимости.

Приведенная последовательность действий по использованию предоставленного изделием инструментария обеспечивает решение задачи организации защиты трафика *IP-датаграмм*, передаваемого между субъектами обмена через сети общего пользования.

3.1.2. Криптотуннели для защиты обмена Ethernet-кадрами на L2-уровне

Защита трафика *Ethernet-кадров* с информацией Пользователя, передаваемого на L2-уровне через сети общего пользования, осуществляется изделиями с помощью L2–TNL-интерфейсов. Настоящий подраздел содержит сведения о принципах работы L2–TNL-интерфейсов и возможных вариантах их применения.

3.1.2.1. Принципы работы криптотуннелей на L2-уровне

Общая схема организации функционирования криптографического туннеля, устанавливаемого между локальным и удаленным изделиями и выполняющего криптозащиту передаваемого на L2-уровне через IP-сети общего пользования трафика Ethernet-кадров, представлена на Рис. 3.14.

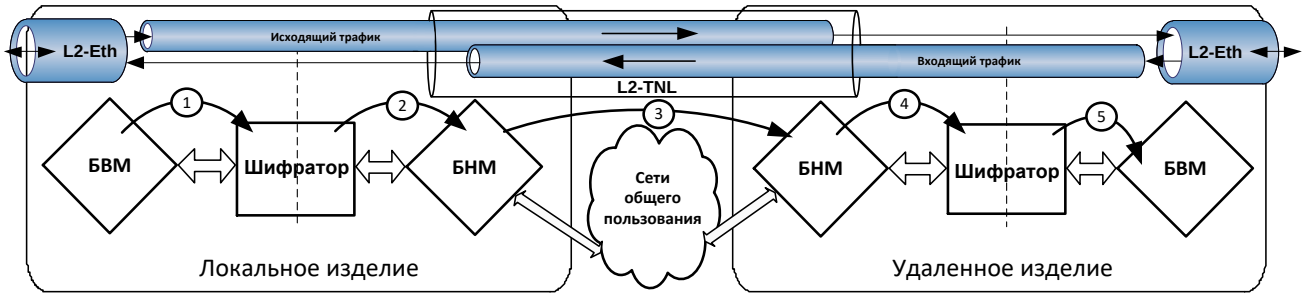


Рис. 3.14 Схема функционирования криптотуннеля при передаче Ethernet-кадров на L2-уровне

Такой криптотуннель можно представить в виде конструкции, состоящей из двух трубок (двух стволов), каждая из которых обрабатывает *исходящий* или *входящий* трафик изделия на данном направлении обмена (Рис. 3.14).

Пакеты с информацией передаются между образующими криптотуннель изделиями по каждому из стволов криптотуннеля только в одном направлении: от изделия-отправителя пакета к изделию-получателю.

Тракт обработки трафика защищаемых Ethernet-кадров каждым из *однонаправленных* стволов криптотуннеля начинается в БВМ изделия-отправителя, проходит через его шифратор и БНМ, продолжается далее через оборудование сетей общего пользования и оканчивается в БНМ изделия-получателя.

В своей основе тракт передачи Ethernet-кадров между изделиями защиты через сети общего пользования на L2-уровне представляет собой простую цепочку: L2–Eth-интерфейс БВМ изделия-отправителя – криптотуннель, образованный L2–TNL-интерфейсами изделия-отправителя и изделия-получателя – L2–Eth-интерфейс БВМ изделия-получателя.

> *Примечание.* Вопросы более сложной организации защищенного тракта передачи на L2-уровне и обработки потока Ethernet-кадров в нем с учетом применения L2–VLAN-интерфейсов и использования настроек L3-уровня в L2–Eth-интерфейсах рассмотрены в соответствующих разделах настоящего РНУ.

Передача данных по криптотуннелю на L2-уровне. Каждый правильный Ethernet-кадр, принятый из ЛВС Пользователя L2–Eth-интерфейсом БВМ локального изделия, направляется на L2–TNL-интерфейс, имя

которого было указано в качестве значения параметра **Имя L2-туннеля** при настройке L2–Eth-интерфейса (см. Рис. 2.15, с. 33). При этом не выполняется никаких процедур обработки − весь поток Ethernet-кадров направляется в L2–TNL-интерфейс (связанный с L2–Eth-интерфейсом) напрямую, минуя маршрутизацию в БВМ.

Далее выполняется обработка Ethernet-кадра L2–TNL-интерфейсом БВМ локального изделия, включающая составление *задания* для шифратора на обработку *исходного* входящего Ethernet-кадра (с учетом значений криптопараметров криптотуннеля, образованного с помощью соответствующего L2–TNL-интерфейса), предусматривающее зашифрование всего кадра с имитозащитой, а также передачу кадра вместе с заданием шифратору (шаг 1 на схеме Рис. 3.14, с. 86). Шифратор выполняет криптообработку исходного Ethernet-кадра согласно полученному заданию и результат своей работы передает далее в БНМ локального изделия (шаг 2 на схеме Рис. 3.14, с. 86).

Далее БНМ упаковывает (инкапсулирует) поступившие из шифратора данные в IP-датаграмму в транспортном формате (см. Рис. 3.3, с. 74), добавляя к поступившим данным заголовок туннеля, заголовок **UDP** (если необходимо) и транспортный IP-заголовок. Сформированная транспортная IP-датаграмма передается на маршрутизацию БНМ и через соответствующий наружный физический Ethernet-интерфейс отправляется в IP-сеть общего пользования (шаг 3 на схеме Рис. 3.14, с. 86).

Прием данных по криптотуннелю на L2-уровне. Если на интерфейс БНМ изделия поступила входящая *туннелированная* IP-датаграмма (т.е. поле **Protocol** IP-датаграммы имеет значения ***4*** или ***17***), то БНМ начинает поиск обрабатывающего IP-датаграмму криптотуннеля, соответствующего данным из заголовка криптотуннеля принятой IP-датаграммы (идентификатору криптотуннеля и IP-адресам).

После того как L2-криптотуннель найден, БНМ извлекает из транспортной IP-датаграммы исходный Ethernet-кадр в зашифрованном виде и оформляет задание шифратору на его обработку. Исходный Ethernet-кадр в зашифрованном виде вместе с заданием отправляются в шифратор (шаг 4 на схеме Рис. 3.14, с. 86). Шифратор выполняет восстановление переданных через сеть исходных данных (расшифрование и проверку имитозащиты), после чего извлеченный из L2–TNL-интерфейса Ethernet-кадр в исходном виде передается в БВМ (шаг 5 на схеме Рис. 3.14, с. 86), где он, минуя маршрутизатор, перенаправляется в связанный с L2–TNL-интерфейсом (через значение параметра **Имя L2-туннеля**) физический L2-Eth-интерфейс, непосредственно подключенный к удаленному сегменту ЛВС, в котором находится получатель исходного Ethernet-кадра.

Если принадлежность принятой туннелированной IP-датаграммы к криптотуннелю на удаленном изделии не обнаружена, считается, что эта IP-датаграмма предназначена не для криптотуннелей данного изделия, поэтому ее обработка продолжается на общих основаниях – IP-датаграмма отправляется на маршрутизацию в БНМ для дальнейшего продвижения по сетям общего пользования (это, например, может быть *транзитная* для данного изделия IP-датаграмма).

Подводя итог, можно выделить следующие фазы в работе каждого из стволов криптографического туннеля изделия для защищенной передачи Ethernet-кадров на L2-уровне:

- на локальном (передающем) изделии внутренняя часть L2-криптотуннеля (на БВМ), получив очередной *исходный* Ethernet-кадр от L2–Eth-интерфейса, выполняет для него формирование задания на обработку передаваемых данных, отправку их в шифратор (шаг 1 на схеме Рис. 3.14);
- на локальном (передающем) изделии внутренняя часть криптотуннеля средствами шифратора выполняет необходимые согласно заданию от БВМ преобразования передаваемых данных и отправку их в БНМ изделия (шаг 2 на схеме Рис. 3.14);
- на локальном (передающем) изделии наружная часть криптотуннеля (на БНМ) выполняет упаковку обработанных шифратором зашифрованных передаваемых данных в IP-датаграмму транспортного формата и выполняет ее отправку через маршрутизатор и соответствующий наружный интерфейс БНМ в сеть (шаг 3 на схеме Рис. 3.14);
- на удаленном (принимающем) изделии наружная часть криптотуннеля (на БНМ) распаковывает транспортную IP-датаграмму, выполняет на основе данных туннельного заголовка извлеченной зашифрованной IP-датаграммы подготовку задания шифратору на обратное преобразование принятых данных и отправку их в шифратор (шаг 4 на схеме Рис. 3.14); шифратор передает расшифрованный *исходный* Ethernet-кадр в БВМ (шаг 5 на схеме Рис. 3.14), где, учитывая, что данные (Ethernet-кадр) извлечены из криптотуннеля L2-уровня – L2–TNL-интерфейса, программой управления будет найден соответствующий L2-криптотуннелю физический L2–Eth-интерфейс, непосредственно подключенный к удаленному сегменту ЛВС Пользователя, в которой находится получатель, и исходный Ethernet-кадр будет перенаправлен найденному L2–Eth-интерфейсу, через который Ethernet-кадр попадет к получателю в удаленном сегменте ЛВС Пользователя.

3.1.2.2. Создание и настройка L2–TNL-интерфейсов

Процедуры создания и настройки L2–TNL-интерфейсов, обеспечивающих защиту передаваемого через сети общего пользования на L2-уровне трафика Ethernet-кадров приведены в разделе 2.4.5, с. 49.

3.1.2.3. Организация защиты трафика Ethernet-кадров на L2-уровне

Для обеспечения функционирования технологии защиты обмена Ethernet-кадрами на L2-уровне изделие применяется как средство организации *криптомостов*; формируются защищенные `bridge`-соединения, устанавливаемые через IP-сеть общего пользования между локальным и удаленными защищаемыми сегментами ЛВС Пользователя.

Для организации функционирования изделия в этом режиме необходимо:

- создать и настроить на БНМ локального и удаленных изделий, руководствуясь схемой организации связи, необходимое число сетевых физических Ethernet-интерфейсов (см. раздел 2.3.1, с. 25) – как основу для телекоммуникационного обмена изделий с сетями общего пользования и с удаленными сегментами ЛВС Пользователя;
- создать и настроить на БВМ локального и удаленных изделий, руководствуясь схемой организации связи, необходимое число сетевых физических L2–Eth-интерфейсов (см. раздел 2.3.2, с. 33) и виртуальных L2–VLAN-интерфейсов (см. раздел 2.4.4, с. 46) как основу для телекоммуникационного обмена изделий с соответствующими защищаемыми локальным и удаленными сегментами ЛВС Пользователя;
- создать и настроить на БВМ локального и удаленного изделий необходимые L2–TNL-интерфейсы (см. раздел 2.4.5, с. 49), обеспечивающие работу необходимых криптотуннелей, руководствуясь схемой организации связи и используя исходные данные Администрации ЗСПД о криптопараметрах сети.

Приведенная последовательность действий по применению предоставленного изделием инструментария обеспечивает решение задачи защиты трафика *Ethernet-кадров*, передаваемого через сети общего пользования на L2-уровне, с помощью организации функционирования L2-криптомостов между удаленными сегментами ЛВС Пользователя.

3.1.3. Оперативное управление криптотуннелями изделия

Администратор (оператор) изделия имеет возможность оперативно проконтролировать параметры *всех криптотуннелей* (всех типов), созданных в изделии к настоящему моменту времени. Для этого он должен выбрать цепочку альтернатив ГМ: **Диагностика ⇨ Туннели**.

В ответ будет выдан экран оперативного контроля параметров криптотуннелей, аналогичный представленному на Рис. 3.15, со списком описателей криптотуннелей, созданных в изделии на текущий момент. Описатели криптотуннелей отображаются на экране в том же формате, что и в списке описателей статических криптотуннелей изделия (см. раздел 3.1.1.2, с. 78).

В первой позиции строки описателя – символ, определяющий тип криптотуннеля:

- символ пробел у описателей статических криптотуннелей;
- символ «*» (*звездочка*) у описателей TNL- и L2–TNL-интерфейсов.

```
↑ ↓ PgUp PgDn Home End - просмотр; ESC - выход; F6 - график замен ключей.
                    Alt+F1 - сменить формат вывода
ID    Локальный адрес->Удаленный адрес #N# Шифрование              Метка
*55          10.1.0.1->10.1.150.1        0 (0)0.0->0               0
*77          10.1.1.2->10.1.150.1        0 (0)0.0->0               0
*33        10.12.10.1->10.12.100.1       0 (0)0.0->0               0
 22       10.10.10.22->10.10.10.52       1 (1)10001.3->6           0

 * - не отвечает;    Enter - просмотр; F5 - рестарт; * F2 - блокировка;
 * - не открыт; * - не исп.;  F4 - номер соединения; * F7 - трассировка;
 Ctrl+Enter - правила отбора. Alt+F4/Shift+F4 - вход./исход. соединения.
```

Рис. 3.15 Экран оперативного контроля параметров криптотуннелей изделия

Для визуализации состояния, в котором находится туннель, строка с его описателем выделяется цветом:

- черный цвет – туннель находится в рабочем состоянии;
- зеленый цвет – *статический* туннель настроен как не обрабатываемый (выключенный);
- красный – туннель заблокирован;
- голубой – в туннеле включена трассировка.

Следующие два состояния отображаются только при просмотре списка с применением средств ЛКУ, подключенных к БВМ изделия:

- *желтый цвет* – TNL- или L2–TNL-интерфейс открыт, но не активен; *включен* контроль состояния интерфейса;
- *желтый цвет* в *мигающем* режиме – TNL- или L2–TNL-интерфейс находится в состоянии не открыт, *включён* контроль состояния интерфейса.

Верхняя часть экрана содержит стандартную информацию о навигационных клавишах и справа от нее информацию об операции, выполняемой при нажатии клавиши <F6> (см. ниже).

В нижней части экрана приведены операции и клавиши (или их комбинации), с помощью которых эти операции выполняются. Пояснения по их назначению и применению даны ниже.

Enter – просмотр (Рис. 3.15). При нажатии клавиши <Enter> на видеомонитор ЛКУ выдается аналогичный представленному на Рис. 3.16 экран параметров настройки и текущих значений рабочих параметров того криптотуннеля, на строку с описателем которого был установлен курсор. Кроме значений параметров настройки (подробнее см. раздел 3.1, с. 73) можно проконтролировать текущие значения счетчиков пакетов и соединений для входящих и исходящих обрабатываемых криптотуннелем потоков данных.

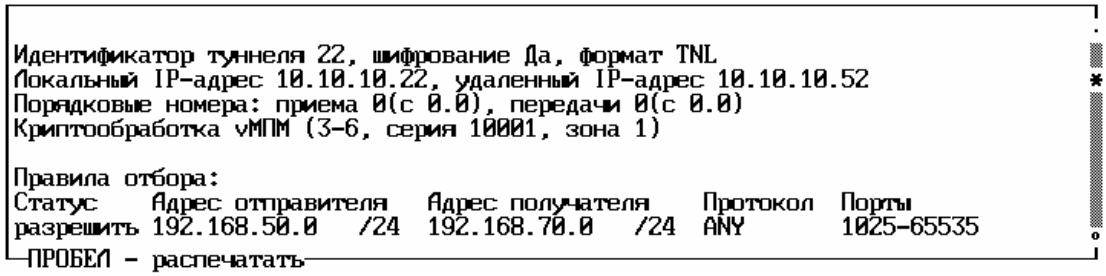


Рис. 3.16 Экран параметров настройки и текущих значений рабочих параметров криптотуннеля

F5 – рестарт (Рис. 3.15). При нажатии клавиши < F5> начинается процедура перезапуска туннеля.

F2 – блокировка (Рис. 3.15). Нажатие клавиши <F2> блокирует туннель – через заблокированный туннель не будут передаваться датаграммы. Цвет соответствующей строки в списке описателей изменится на красный.

F7 – трассировка (Рис. 3.15). При нажатии клавиши < F7> включается/отключается запись в системный журнал (файл **log.ema**) процесса обработки датаграммы данным туннелем. При включении трассировки цвет соответствующей строки в списке описателей меняется на голубой.

Ctrl+Enter – правила отбора (Рис. 3.15). При нажатии комбинации клавиш <Ctrl+Enter> на экран выводится полный список правил отбора всех туннелей. Список можно просмотреть, а также запротоколировать – занести в журнал (файл **LOG.EMA**), нажав клавишу <пробел>.

Следующие три команды доступны *только* при подключении блока ЛКУ к БВМ.

F4 – номер соединения (Рис. 3.15). При нажатии клавиши <F4> на БКО отправляется запрос значений номеров соединений (полученные значения будут выводиться на экран при просмотре состояния туннеля по команде <Enter>).

Alt+F4/Shift+F4 – вход./исход. соединения (Рис. 3.15). Команды позволяют при необходимости скорректировать порядковые номера входящего или исходящего соединения.

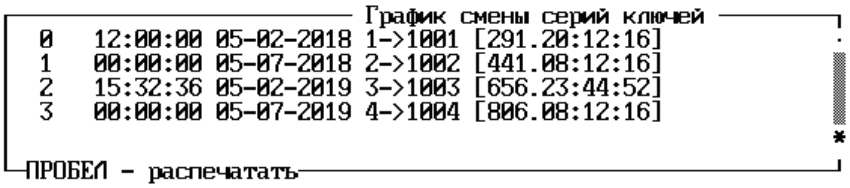


Рис. 3.17 Экран записей расписания графика замены ключевых документов изделия

F6 – график замен ключей (Рис. 3.15) – при нажатии клавиши <F6> на видеомонитор ЛКУ выводится расписание замены ключевых документов изделия, аналогичное представленному на Рис. 3.17 (подробнее о графике замены ключей при их групповой замене см. раздел 3.4, с. 122).

3.2. Фильтрация потоков данных

Одним из важнейших видов защиты, используемых при передаче данных Пользователя через сети общего пользования, является механизм *фильтрации* потоков данных, циркулирующих через сетевые интерфейсы и внутренние интерфейсы маршрутизаторов изделия. С помощью этого механизма выполняется управление исходящими и входящими потоками данных.

Логика обработки потоков данных, проходящих через *физические* интерфейсы двух типов различна (подробнее см. раздел 2.1, с. 19):

- обработка потоков данных физическим Ethernet-интерфейсом ориентирована на обработку *IP-датаграмм* на сетевом (L3) уровне;
- обработка потоков данных физическим L2–Eth-интерфейсом ориентирована на обработку *Ethernet-кадров* на канальном (L2) уровне.

И в соответствии с этим изделиями, исполненными в двухсегментной архитектуре технологии DioNIS®, поддерживаются *два вида фильтрации* потоков данных, проходящих через интерфейсы изделия:

- фильтрация на *сетевом* (L3) уровне – фильтрация потоков *IP-датаграмм*; фильтрация этого вида выполняется для потоков IP-датаграмм, циркулирующих через физические Ethernet-интерфейсы и через виртуальные интерфейсы (VLAN, TNL и GRE), для которых физический Ethernet-интерфейс является *базовым*, а также через внутренние (служебные) интерфейсы любого из маршрутизаторов изделия (вопросам организации работы механизма фильтрации потоков IP-датаграмм посвящен материал раздела 3.2.1, с. 90);
- фильтрация на *канальном* (L2) уровне – фильтрация потоков *Ethernet-кадров*; фильтрация этого вида выполняется для потоков Ethernet-кадров, циркулирующих через физические L2–Eth-интерфейсы (вопросы организации работы механизма фильтрации потоков Ethernet-кадров рассмотрены в разделе 3.2.2, с. 109).

3.2.1. *Фильтрация потоков IP-датаграмм*

Поддерживаемый изделием механизм фильтрации IP-датаграмм на сетевом (L3) уровне – механизм *IP-фильтрации* – предоставляет персоналу возможность организации обеспечения изделием процесса непрерывного анализа потоков IP-датаграмм, проходящих через сетевые и внутренние (служебные) интерфейсы любого из маршрутизаторов изделия (БВМ или БНМ) на соответствие набору настраиваемых персоналом параметров – *параметрам IP-фильтрации*. По результатам анализа на соответствие параметрам IP-фильтрации программой управления автоматически (в реальном масштабе времени) индивидуально для каждой проходящей через интерфейс IP-датаграммы принимается решение о продолжении или прекращении ее дальнейшей обработки.

3.2.1.1. Общие сведения о фильтрации потоков IP-датаграмм (L3-уровень)

При работе с изделием *фильтром* называется *поименованный список*, содержащий набор правил проверки IP-датаграмм – *правил IP-фильтрации*. Количество правил IP-фильтрации в каждом IP-фильтре, а также количество IP-фильтров в изделии не ограничено. Список IP-фильтров изделия является общим для наружного и внутреннего маршрутизаторов изделия. Текущее состояние всех IP-фильтров сохраняется в обобщенной базе параметров (**БпО.**

Работу механизма IP-фильтрации рассмотрим на примере схемы, приведенной на Рис. 3.18.

Рис. 3.18 Схема применения IP-фильтров на внутреннем и на сетевых интерфейсах маршрутизатора

Изделие взаимодействует с каналами связи через сетевые интерфейсы различного типа (подробнее см. раздел 2.1, с. 19). При этом через каждый интерфейс проходят два потока информации:

- входящий поток – поток данных, принимаемый сетевым интерфейсом из канала связи для дальнейшей обработки изделием;
- исходящий поток – поток данных, передаваемый изделием через сетевой интерфейс в канал связи.

Кроме того, для организации взаимодействия каждого из маршрутизаторов изделия с собственными обработчиками IP-пакетов, адресованных протоколам прикладного уровня, существует *внутренний* (служебный) интерфейс, через который также проходят два потока информации:

- входящий поток – поток IP-датаграмм, принимаемых от маршрутизатора обработчиками IP-датаграмм, адресованных протоколам прикладного уровня – службам маршрутизатора;
- исходящий поток – поток IP-датаграмм, передаваемых маршрутизатору от обработчиков IP-датаграмм.

Для полного контроля потоков IP-датаграмм, циркулирующих через каждый из интерфейсов маршрутизатора (включая внутренний интерфейс) может быть создано и настроено по два IP-фильтра для каждого из интерфейсов (сетевого или внутреннего):

- входной IP-фильтр – для IP-фильтрации входящего потока IP-датаграмм;
- выходной IP-фильтр – для IP-фильтрации исходящего потока IP-датаграмм.

Назначение конкретного списка правил IP-фильтрации в качестве входного или выходного IP-фильтра конкретного интерфейса выполняется простым указанием *имени* этого списка (заранее созданного – о порядке создания IP-фильтра см. раздел 3.2.1.2, с. 92) в качестве значения параметров **Фильтр входящих** или **Фильтр исходящих** соответствующего бланка создания и настройки интерфейсов (см. Рис. 2.4, с. 25; Рис. 2.19, с. 38; Рис. 2.22, с. 39; Рис. 2.30, с. 45).

Назначение IP-фильтров для внутренних (служебных) интерфейсов маршрутизаторов изделия выполняется путем применения специальных (*системных*) имен для обозначения соответствующего списка правил IP-фильтрации (в блоках наружной и внутренней маршрутизации используются IP-фильтры с разными системными именами):

- **int_in** – входной фильтр внутреннего интерфейса БВМ;
- **int_out** – выходной фильтр внутреннего интерфейса БВМ;
- **ext_in** – входной фильтр внутреннего интерфейса БНМ;
- **ext_out** – выходной фильтр внутреннего интерфейса БНМ.

В плане создания и настройки системные IP-фильтры ничем не отличаются от IP-фильтров общего назначения. Их особенностями являются только использование для обозначения специальных системных имен и место применения фильтра – внутренний (служебный) интерфейс маршрутизатора.

Программа управления изделием в процессе IP-фильтрации использует соответствующий IP-фильтр, состоящий из набора настраиваемых персоналом правил IP-фильтрации. Правила IP-фильтрации подразделяются на следующие виды:

- *простое* правило (см. раздел 3.2.1.3, с. 93);
- *расширенное* правило (см. раздел 3.2.1.6, с. 100);
- правило типа *элемент расписания* (см. раздел 3.2.1.6, с. 100).

В зависимости от набора правил IP-фильтрации, составляющих IP-фильтр, различают:

- *простой* IP-фильтр – в набор его правил входят только простые правила IP-фильтрации (см. раздел 3.2.1.3, с. 93);
- IP-фильтр *расширенного формата* – в набор его правил могут входить не только *простые* правила IP-фильтрации, но и *расширенные* правила и правила типа *элемент расписания* (см. раздел 3.2.1.6, с. 100).

  Системные IP-фильтры также могут быть простыми или фильтрами расширенного формата.

Смысловое содержание правил, составляющих IP-фильтр, зависит от места применения самого IP-фильтра. Рассмотрим это положение на примере схемы, представленной на Рис. 3.19.

Пусть изделие включается в ЗСПД по типовой схеме включения межсетевого экрана и имеет два интерфейса: один – во внешнюю сеть (**EXT** на схеме) и один – во внутреннюю сеть (**INT** на схеме). В такой схеме возможно одновременное использование до четырех фильтров одновременно. Присвоим IP-фильтрам следующие имена:

ФН_in – фильтр потока входящих IP-датаграмм интерфейса **EXT** блока наружной маршрутизации.

Фильтр **ФН_in** – *основной* фильтр, ограничивающий доступ абонентов сети общего пользования к ресурсам самого изделия и к защищаемой им сети Пользователя. Именно на этот фильтр приходится основная нагрузка по блокировке нежелательных воздействий на объекты внутренней сети со стороны источников нежелательного трафика, размещаемых во внешней сети общего пользования.

ФВ_in – фильтр потока входящих IP-датаграмм интерфейса **INT** блока внутренней маршрутизации.

ФВ_in – *основной* фильтр, ограничивающий доступ абонентов защищаемой (внутренней) сети Пользователя к открытым внешним ресурсам, размещаемым в сети общего пользования. Правилами этого IP-фильтра обеспечивается разграничение полномочий абонентов внутренней сети.

ФН_out – фильтр потока исходящих IP-датаграмм интерфейса **EXT** блока наружной маршрутизации.

ФН_out – вспомогательный фильтр. С его помощью можно уточнить действие фильтра **ФВ_in**, а также ограничить поток ответов от обработчиков прикладных протоколов изделия, направляемых во внешнюю сеть.

ФВ_out – фильтр потока исходящих IP-датаграмм интерфейса **INT** блока внутренней маршрутизации.

ФВ_out – вспомогательный фильтр. С его помощью можно ввести дополнительные ограничения на доступ к ресурсам защищаемой сети со стороны внешней сети, а также со стороны прикладных протоколов изделия.

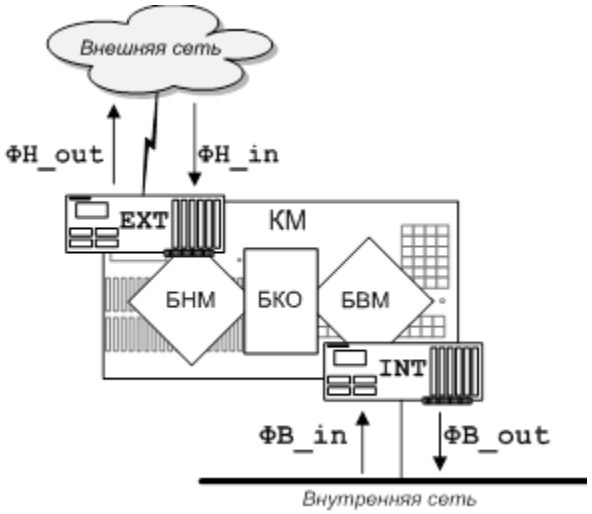


Рис. 3.19 Пример схемы применения IP-фильтров на сетевых интерфейсах изделия

3.2.1.2. Управление IP-фильтрами изделия

Управление IP-фильтрами изделия, независимо от того, являются ли они системными, простыми IP-фильтрами или IP-фильтрами расширенного формата, выполняется по единой технологии, описанной в данном подразделе.

Для создания и настройки IP-фильтра следует выбрать цепочку альтернатив ГМ: **Настройка ⇨ Защита ⇨ Фильтры**. В ответ будет выдан экран создания и настройки IP-фильтров, аналогичный представленному на Рис. 3.20.

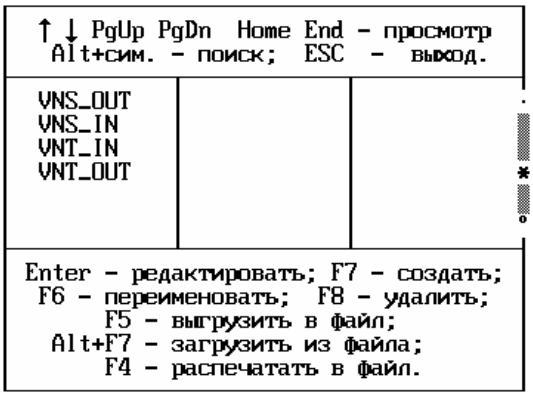


Рис. 3.20 Экран создания и настройки IP-фильтров изделия

Средняя часть экрана содержит список имен ранее созданных IP-фильтров (изначально список пустой).

В верхней части экрана − стандартная информация о средствах навигации по списку.

Нижняя часть экрана содержит сведения о клавишах и их комбинациях, с помощью которых администратор изделия выполняет создание и настройку IP-фильтров.

Создание нового IP-фильтра выполняется в два этапа: сначала надо задать его имя, а потом сформировать список правил, его составляющих.

F7 – **создать** (Рис. 3.20). Нажатие клавиши <F7> приводит к выводу на видеомонитор ЛКУ запроса, позволяющего ввести имя создаваемого IP-фильтра. Имя может быть произвольным, но обязательно уникальным (проверку уникальности выполняет программа управления).

После ввода имени IP-фильтра на видеомонитор ЛКУ выводится экран редактора IP-фильтра (Рис. 3.21, с. 93), позволяющий сформировать список правил IP-фильтрации (работа с редактором IP-фильтра описана ниже в разделе 3.2.1.3, с. 93).

Enter – **редактировать** (Рис. 3.20). Нажатие клавиши <Enter> вызывает редактор IP-фильтра (Рис. 3.21) и передает ему на обработку IP-фильтр, на имя которого в момент нажатия клавиши <Enter> указывает курсор.

F6 – **переименовать** (Рис. 3.20). Нажатие клавиши <F6> приводит к выводу на видеомонитор ЛКУ запроса на ввод имени IP-фильтра, в ответ на который следует ввести новое имя и нажать клавишу <Enter>.

В результате IP-фильтр, на имени которого в момент нажатия клавиши <F6> был установлен курсор, получит новое имя.

F8 – **удалить** (Рис. 3.20). При нажатии клавиши <F8> после дополнительного запроса и подтверждения будет удален тот IP-фильтр, на строку с именем которого был установлен курсор.

F5 – **выгрузить в файл** или **Alt+F7** – **загрузить из файла** (Рис. 3.20). Эти две операции служат для облегчения труда администратора изделия. Первая позволяет выгрузить указанный курсором IP-фильтр в файл, вторая позволяет создать новый IP-фильтр и загрузить в него содержимое IP-фильтра из файла. Имя файла и имя IP-фильтра для операции **Alt+F7** – **загрузить из файла** запрашиваются дополнительно. Информация, переносимая из конфигуратора в файл, хранится в нем в бинарном виде.

F4 – **распечатать в файл** (Рис. 3.20). При нажатии клавиши <F4> содержимое IP-фильтра, на имя которого указывает курсор, преобразуется в текстовый формат и записывается в файл. Имя файла при этом запрашивается дополнительно.

3.2.1.3. Создание и редактирование простых IP-фильтров

Большинство задач, решаемых изделием с помощью IP-фильтрации, решаются применением простых фильтров. Простые IP-фильтры включают только простые правила IP-фильтрации.

Создание и настройка простых правил IP-фильтрации. Перед тем как приступить к созданию правил IP-фильтрации, надо выполнить первый шаг создания IP-фильтра − задать имя фильтра (согласно порядку, приведенному в разделе 3.2.1.2, с. 92). После этого в списке имен IP-фильтров на экране создания и настройки IP-фильтров (Рис. 3.20, с. 92) появится заданное имя.

> *Примечание*. Экран создания и настройки IP-фильтров (Рис. 3.20, с. 92) можно вызвать на видеомонитор ЛКУ в любой момент, выбрав цепочку альтернатив ГМ: **Настройка ⇨ Защита ⇨ Фильтры**.

Для выполнения второго шага создания IP-фильтра (создание правил IP-фильтрации) надо в списке имен IP-фильтров (Рис. 3.20) перевести курсор на заданное имя и нажать клавишу <Enter>. После этого на видеомонитор ЛКУ будет выдан экран создания и настройки правил IP-фильтрации (редактор IP-фильтра), аналогичный представленному на Рис. 3.21.

На верхней рамке указаны: в центре – имя IP-фильтра (в нашем примере – **FLT2**); слева – номер строки в списке имен IP-фильтров на экране создания и настройки IP-фильтров (Рис. 3.20, с. 92), на которую был установлен курсор перед нажатием клавиши <Enter> (отсчет строк с именами фильтров начинается с *нуля*).

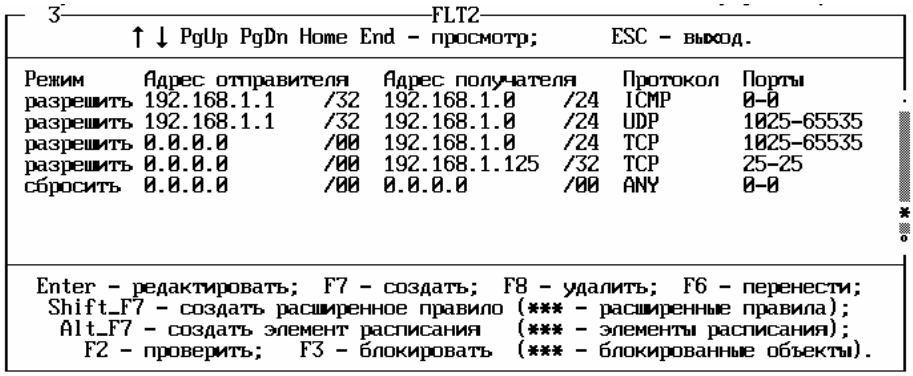


Рис. 3.21 Экран создания и настройки правил IP-фильтрации (редактор IP-фильтра)

В средней части экрана в удобной для просмотра форме отображаются строки описателей правил IP-фильтрации, содержащие значения параметров правил IP-фильтрации (изначально, если IP-фильтр только что создан, строки отсутствуют).

Строки описателей расширенных правил IP-фильтрации на экране (Рис. 3.21) выводятся *желтым* цветом; описатели правил IP-фильтрации типа элемент расписания – *зеленым*; описатели заблокированных правил IP-фильтрации – *красным*.

> *Примечание.* В настоящем разделе рассматривается создание (редактирование) только простых фильтров. Фильтры расширенного формата, содержащие расширенные правила и элементы расписания, рассмотрены ниже в разделе 3.2.1.6, с. 100.

Восклицательным знаком в первой позиции строки описателя отмечены те правила, для которых задано *фиксирование* в журнале IP-датаграмм, подпадающих под значения параметров этого правила (параметр правила **Фиксировать** имеет значение *ДА* – см. бланк создания и настройки простого правила IP-фильтрации, представленный на Рис. 3.22).

Нижняя часть экрана создания и настройки правил IP-фильтрации (Рис. 3.21) содержит сведения о клавишах, с помощью которых администратор изделия выполняет создание и настройку описателей правил IP-фильтрации.

F7 – **создать** (Рис. 3.21). При нажатии клавиши <F7> на видеомонитор ЛКУ выводится бланк создания и настройки простого правила IP-фильтрации (Рис. 3.22), позволяющий сформировать одно правило. Правило будет размещено в списке описателей правил после той строки, на которой был установлен курсор.

Режим разрешить	Протокол ANY	
Фиксировать нет	TCP-флаги нет	
Порты		
	Адрес	Зн. бит
Отправитель	0.0.0.0	0
Получатель	0.0.0.0	0

Рис. 3.22 Бланк создания и настройки простого правила IP-фильтрации

Каждое правило IP-фильтрации является описателем *одной* операции проверки IP-датаграмм и включает параметры, назначение которых приведены ниже. Чтобы задать значение того или иного параметра, надо переместить курсор в соответствующее поле бланка и последовательно нажимать клавишу <Enter>.

Режим (Рис. 3.22) – параметр задает вид действия, которое будет применено к фильтруемой IP-датаграмме в случае совпадения параметров IP-датаграммы со значениями соответствующих параметров правила IP-фильтрации.

Параметр **Режим** может принимать следующие значения:

- *Разрешить* – IP-датаграмма, соответствующая правилу, будет допущена IP-фильтром к дальнейшей обработке;
- *Запретить* – IP-датаграмма, соответствующая правилу, будет заблокирована IP-фильтром (при этом IP-датаграмма сбрасывается, а в адрес отправителя формируется соответствующее ICMP-сообщение);
- *Сбросить* – IP-датаграмма, соответствующая правилу, будет сброшена без отправки каких-либо сообщений в адрес отправителя;
- *Сессия* – проверяемая IP-датаграмма будет допущена к дальнейшей обработке с отслеживанием состояния соединения (подробнее см. раздел 3.2.1.8, с. 106).

  Примечание. Фильтры, в правилах фильтрации которых параметр **Режим** имеет одно из первых трех значений (*Разрешить*, *Запретить*, *Сбросить*), будем называть *обычными*; фильтры, в правилах фильтрации которых параметр **Режим** имеет значение *Сессия*, – *фильтрами сессий*.

Протокол (Рис. 3.22) – параметр задает проверку значения поля **Протокол** в заголовке IP-датаграммы. Параметр **Протокол** в правилах IP-фильтрации может принимать следующие значения:

- *ANY* – параметр **Протокол** в заголовке проверяемой IP-датаграммы может иметь любое значение;
- *ICMP* – параметр **Протокол** в заголовке проверяемой IP-датаграммы имеет значение **1** (ICMP);
- *TCP* – параметр **Протокол** в заголовке проверяемой IP-датаграммы имеет значение **6** (TCP);
- *UDP* – параметр **Протокол** в заголовке проверяемой IP-датаграммы имеет значение **17** (UDP – протокол может использоваться для передачи туннелированных датаграмм);
- *TNL* – параметр **Протокол** в заголовке проверяемой IP-датаграммы имеет значение **4** (IP in IP – протокол может использоваться для передачи туннелированных датаграмм).

Фиксировать (Рис. 3.22) – параметр определяет, будет ли записана в протокол (файл **LOG_TCP.EMA**) IP-датаграмма, параметры которой совпали с параметрами соответствующего правила IP-фильтрации (с указанием, прошла IP-датаграмма на дальнейшую обработку или заблокирована/сброшена). Возможны следующие значения параметра:

- *ДА* – IP-датаграмма будет записана в журнал;
- *НЕТ* – IP-датаграмма не будет записана в журнал.

TCP-флаги (Рис. 3.22) – параметр позволяет задать проверку поля **Флаги** TCP-пакета. Поле **TCP-флаги** в правилах IP-фильтрации может принимать следующие значения:

- *НЕТ* – проверка поля **Флаги** TCP-пакета не производится;
- *SYN* – в TCP-пакете установлен флаг **SYN** и сброшен флаг **ACK**;
- *ACK* – в TCP-пакете установлен флаг **ACK**, остальные флаги могут быть любыми.

  Поле **TCP-флаги** в правилах IP-фильтрации имеет смысл только для IP-пакетов протокола TCP.

Порты* (Рис. 3.22) – перевод курсора в поле бланка **Порты** и последовательное нажатие клавиши <Enter> выводит на экран меню, позволяющее задать пару чисел, которые будут интерпретированы программой управления как значения одного из следующих трех параметров:

- **Порт отправителя и получателя**;
- **Диапазон портов получателя**;
- **Диапазон портов отправителя**.

Выбрав требуемое значение, надо нажать клавишу <Esc> − пара цифр появится в поле бланка, например:

Порты 1025 -> 23

Порты (получатель) 22 - 23

При этом.

Значение параметра **Порт отправителя и получателя** позволяет указать необходимость проверки полей Порт отправителя и Порт получателя в заголовках TCP- или UDP-датаграмм, транспортируемых проверяемой IP-датаграммой. Параметры датаграммы считаются удовлетворяющими данному правилу IP-фильтрации, если соответствующие значения портов проверяемой датаграмм *совпадают* со значениями портов, заданными этим параметром правила.

Если одному или обоим значениям параметра присвоено нулевое значение, то проверка соответствующих полей фильтруемой IP-датаграммы не производится, т.е. любое значение портов проверяемой датаграммы считается удовлетворяющим данному правилу IP-фильтрации.

Значения **Диапазон портов отправителя** и **Диапазон портов получателя** позволяют указать необходимость проверки полей Порт отправления или Порт назначения в заголовках TCP- или UDP-датаграмм, транспортируемых проверяемой IP-датаграммой. Значение порта датаграммы считается удовлетворяющим данному правилу IP-фильтрации, если оно укладывается в диапазон, заданный соответствующим параметром правила.
Если параметр имеет *нулевое* значение, проверка соответствующего поля IP-датаграммы не производится, т.е. любое значение порта IP-датаграммы считается удовлетворяющим данному правилу IP-фильтрации.

Внимание! Простыми правилами IP-фильтрации можно задать только *один* диапазон значений портов. Если необходимо задать два диапазона, то можно воспользоваться *расширенными* правилами IP-фильтрации, описанными в разделе 3.2.1.6 (с. 100).

Отправитель Адрес и **Отправитель Зн. бит** (Рис. 3.22) – параметры задают значения для проверки поля Адрес отправителя из заголовка фильтруемой IP-датаграммы. Проверка выполняется следующим образом:

a) из заголовка IP-датаграммы извлекается значение поля Адрес отправителя;

b) в извлеченном значении адреса оставляются без изменения старшие биты в количестве, указанном полем **Отправитель Зн. бит**, остальные – обнуляются;

c) выполняется проверка совпадения полученного значения адреса со значением параметра правила IP-фильтрации **Отправитель Адрес**.

Если поля **Отправитель Адрес** и **Отправитель Зн. бит** правила IP-фильтрации имеют нулевые значения, то никакой проверки IP-датаграммы не производится, т. е. любое значение адреса отправителя IP-датаграммы считается удовлетворяющим данному правилу IP-фильтрации.

Получатель Адрес и **Получатель Зн. бит** (Рис. 3.22) – параметры задают значения для проверки поля Адрес получателя из заголовка фильтруемой IP-датаграммы. Проверка происходит следующим образом:

a) из заголовка IP-датаграммы извлекается значение поля Адрес получателя;

b) в извлеченном значении адреса оставляются без изменения старшие биты в количестве, указанном полем **Получатель Зн. бит**, остальные – обнуляются;

c) выполняется проверка совпадения полученного значения адреса со значением параметра правила IP-фильтрации **Получатель Адрес**.

---

* В настоящем разделе понятие «порт» подразумевает порт, указывающий соответствующее приложение Пользователя – подробнее см. раздел ***Приложение А*** (с. 214).

Если параметры **Получатель Адрес** и **Получатель Зн.бит** правила IP-фильтрации имеют нулевые значения, то никакой проверки IP-датаграммы не производится, т. е. любое значение адреса получателя IP-датаграммы считается удовлетворяющим данному правилу IP-фильтрации.

Enter – редактировать (Рис. 3.21). При нажатии клавиши <Enter> на видеомонитор ЛКУ выводится бланк создания и настройки правила IP-фильтрации с параметрами того правила, на описатель которого был установлен курсор (см. Рис. 3.22), позволяющий отредактировать параметры правила.

F6 – перенести (Рис. 3.21). После первого нажатия клавиши <F6> указанная курсором строка описателя правила IP-фильтрации выделяется *белым* цветом. Далее можно переместить курсор на любую строку описателей из списка правил и повторно нажать <F6>. Отмеченный ранее описатель правила будет перемещен непосредственно под строку, на которую был установлен курсор в момент повторного нажатия клавиши <F6>.

Замечание. Между первым и вторым нажатием клавиши <F6> можно пользоваться только клавишами перемещения курсора. Нажатие другой функциональной клавиши из списка операций внизу экрана сбросит отметку подлежащей переносу строки.

F2 – проверить (Рис. 3.21). При нажатии клавиши <F2> выполняется проверка того правила или той строки расписания (см. ниже раздел 3.2.1.6, с. 100), на которой установлен курсор. Для неправильно сформулированных условий (противоречащих одному или нескольким другим правилам IP-фильтра, пересекающимся с данным по *диапазону времени действия*) выводятся соответствующие сообщения.

F3 - блокировать элемент (Рис. 3.21). При нажатии клавиши <F3> без дополнительных запросов блокируется выполнение функции, представленной той строкой описателя в списке описателей правил IP-фильтрации, на которую установлен курсор. При этом на видеомониторе ЛКУ цвет соответствующей строки изменится на *красный*. Повторное нажатие клавиши <F3> блокировку снимает.

Замечание. Данная возможность является вспомогательной и служит в основном для целей отладки IP-фильтра. Операция блокирования правила равнозначна его удалению из списка, но позволяет впоследствии восстановить функциональность правила.

Две команды редактора фильтра **Shift_F7** – **создать расширенное правило** и **Alt_F7** – **создать элемент расписания** (Рис. 3.21) служат для создания и настройки элементов IP-фильтров расширенного формата. Порядок их применения рассмотрен ниже в разделе 3.2.1.6, с. 100.

3.2.1.4. Алгоритм работы простого IP-фильтра

При настройке изделия может быть сформировано большое количество IP-фильтров (поименованных наборов правил IP-фильтрации) с любыми (кроме системных IP-фильтров) именами.

Но сами по себе IP-фильтры являются просто хранилищами наполняющих их правил IP-фильтрации и могут не принимать никакого участия в работе изделия. IP-фильтры включаются в работу только в двух случаях.

1) Имя IP-фильтра указывается в качестве значения параметров **Фильтр входящих** или **Фильтр исходящих** хотя бы для одного из сетевых интерфейсов изделия.

   В этом случае указанный IP-фильтр будет активизирован в момент запуска интерфейса, с которым IP-фильтр связан, и начнет фильтровать соответствующий поток IP-датаграмм (входящий или исходящий).

2) IP-фильтру присваивается одно из *системных* имен.

   IP-фильтры с системными именами активизируются в момент запуска изделия и используются в соответствии с приписанным данному системному имени назначением (см. раздел 3.2.1.7, с. 104).

Принятая интерфейсом, связанным с *простыми* IP-фильтрами, входящая или исходящая IP-датаграмма обрабатывается в соответствии с приведенным ниже алгоритмом.

1. Полученная интерфейсом очередная IP-датаграмма соотносится программой управления с соответствующим IP-фильтром интерфейса – IP-фильтром входящих или исходящих потоков данных. Далее параметры IP-датаграммы последовательно сравниваются с параметрами каждого из правил IP-фильтрации соответствующего IP-фильтра, выбираемых из списка правил *сверху вниз* (см. Рис. 3.21), начиная с первого правила IP-фильтрации. Процесс проверки соответствия параметров IP-датаграммы параметрам очередного правила IP-фильтрации продолжается до первого совпадения.

   Решение о соответствии параметров IP-датаграммы параметрам правила IP-фильтрации принимается программой управления в том случае, когда выполняются следующие условия.

   a. Значение параметра **Протокол** правила IP-фильтрации совпадает со значением поля **Protocol** IP-датаграммы (если параметр **Протокол** IP-фильтра имеет значение *ANY*, то условие считается выполненным при любом значении поля **Protocol** IP-датаграммы).

b. Значение параметра **Отправитель Адрес** правила IP-фильтрации совпадает со значением поля **Source Address** IP-датаграммы (проверка совпадения выполняется по числу старших бит, заданному в описателе правила IP-фильтрации значением параметра **Отправитель Зн. бит**).

c. Значение параметра **Получатель Адрес** правила IP-фильтрации совпадает со значением поля **Destination Address** IP-датаграммы (проверка совпадения выполняется по числу старших бит, заданному в описателе правила IP-фильтрации значением параметра **Получатель Зн. бит**).

d. При ненулевых значениях соответствующие пары чисел параметра **Порт отправителя и получателя** правила IP-фильтрации попарно равны значениям соответствующих полей `Порт отправителя` и `Порт получателя` заголовка TCP- или UDP-датаграммы.

e. При ненулевых значениях соответствующей пары чисел параметра **Диапазон портов получателя** правила IP-фильтрации значение поля `Порт получателя` (**Destination Port**) заголовка TCP- или UDP-датаграммы попадает в диапазон значений правила.

f. При ненулевых значениях соответствующей пары чисел параметра **Диапазон портов отправителя** правила IP-фильтрации значение поля `Порт отправителя` (**Source Port**) заголовка TCP- или UDP-датаграммы попадает в диапазон значений правила.

2. Если зафиксировано совпадение и параметр **Режим** правила имеет значение *разрешить*, то результат проверки считается положительным и IP-датаграмма передается на дальнейшую обработку.

3. Если зафиксировано совпадение, но параметр **Режим** правила имеет значение *запретить*, то результат проверки считается отрицательным, датаграмма отбрасывается, а в адрес отправителя формируется ICMP-сообщение типа:
Destination Unreachable с кодом **Host Unreachable.**

4. Если зафиксировано совпадение, но параметр **Режим** правила имеет значение *сбросить*, результат проверки считается отрицательным, IP-датаграмма отбрасывается, никаких сообщений отправителю не посылается.

Внимание! Если проверяемая IP-датаграмма не подошла ни под одно из заданных правил IP-фильтрации, то вступает в действие правило *по умолчанию*, которое неявно присутствует в каждом IP-фильтре. Значения полей этого правила IP-фильтрации следующие:

Режим	Отправитель	Получатель	Протокол	Порты	Фиксировать
запретить	**0.0.0.0/00**	**0.0.0.0/00**	**ANY**	**0-0**	**ДА**

По этому правилу IP-фильтрации выполняются следующие действия:

- результат проверки IP-датаграммы считается отрицательным;
- IP-датаграмма отбрасывается;
- в адрес отправителя формируется соответствующее ICMP-сообщение;
- прохождение и результат проверки IP-датаграммы фиксируется в системном журнале изделия (см. раздел 3.2.1.9, с. 108).

Указанные действия *по умолчанию* можно легко изменить, если последним правилом IP-фильтра явно указать правило нужного содержания.

Фильтры со специальными (системными) именами работают по аналогичному алгоритму. Только в случае положительного или отрицательного результата проверки выполняется не продолжение обработки или отбрасывание датаграммы, а действие, предусмотренное назначением IP-фильтра.

Из рассмотрения алгоритма работы IP-фильтров следует несколько выводов:

1. Пустой IP-фильтр – не наполненный описателями правил IP-фильтрации – блокирует весь трафик.
2. Правила IP-фильтрации, определяющие более широкий диапазон влияния, следует размещать после правил с более узким диапазоном. Например, если необходимо запретить обращение ко всем компьютерам сети, кроме одного, по какому-либо порту и/или протоколу, то сначала следует разместить правило, разрешающее обращение по конкретному адресу, а потом – правило, запрещающее обращение ко всему диапазону адресов. Переместить правило в списке можно при помощи действий, описанных в разделе 3.2.1.3, с. 93.
3. Если необходимо проанализировать какой-либо вид IP-трафика в сети, следует сформировать соответствующее разрешающее правило IP-фильтрации со значением **ДА** параметра **Фиксировать** (с учетом предыдущего замечания). Соответствующую зафиксированную информацию можно будет найти в файле **LOG_TCP.EMA** и проанализировать.

3.2.1.5. Стратегии формирования IP-фильтров (на примере простых IP-фильтров)

Возможны две стратегии формирования содержательной части IP-фильтров: *запрещающая* и *разрешающая*. Согласно *запрещающей* стратегии сначала в списке описателей IP-фильтра правилами IP-фильтрации выдается *запрет* на пропуск через интерфейс некоторых отбираемых этими правилами IP-датаграмм, а затем для всех остальных IP-датаграмм последним в списке описателей правилом IP-фильтрации выдается *разрешение* на их пропуск через интерфейс. Другими словами, в «запрещающих» IP-фильтрах необходимо явно описать все требуемые запреты; все, что явно не запрещено, будет разрешено.

Согласно *разрешающей* стратегии правилами IP-фильтра задается *разрешение* на пропуск через интерфейс некоторых IP-датаграмм, а для всех остальных IP-датаграмм последним в списке описателей правилом IP-фильтрации выдается *запрет* на их пропуск через интерфейс. Другими словами, в «разрешающих» фильтрах необходимо явно описать все требуемые разрешения; все, что явно не разрешено, будет запрещено.

Безусловно, с точки зрения страховки от возможных ошибок, при формировании IP-фильтров лучше придерживаться разрешающей стратегии. Однако запрещающая стратегия может оказаться более удобной, особенно при формировании IP-фильтров разграничения доступа (например, при настройке IP-фильтра **ФВ_in** на Рис. 3.19, с. 92, ограничивающего доступ абонентов внутренней сети к открытым внешним ресурсам).

Пример применения простых IP-фильтров

Методику формирования IP-фильтров рассмотрим на примере стандартного включения изделия в состав ЗСПД по типовой схеме включения межсетевого экрана, приведенной ранее на Рис. 3.19, с. 92. На Рис. 3.23 приведена та же схема, уточненная конкретными значениями IP-адресов интерфейсов и рабочих станций внутренней сети.

Проведем формирование всех возможных в данной схеме IP-фильтров **ФН_in**, **ФВ_in**, **ФН_out**, **ФВ_out**, исходя из следующих соображений обеспечения безопасности защищаемой (внутренней) сети.

Наиболее опасными с точки зрения воздействия на защищаемую сеть являются протоколы UDP и ICMP. Лучше всего полностью блокировать прием и передачу IP-пакетов с данными этих протоколов через внешний интерфейс изделия. К сожалению, последствием такой блокировки будет отсутствие возможности выполнить процедуру PING через внешний интерфейс с целью проверки доступности узлов и маршрутизаторов во внешних сегментах ЗСПД (процедура PING использует ICMP- пакеты типа Echo-request и Echo-reply). Также последствием такой блокировки будет невозможность использования DNS-серверов во внешней сети для удовлетворения запросов станций внутренней сети на определение IP-адресов узлов по их доменным именам (DNS-служба использует протокол UDP с номером порта **53**).

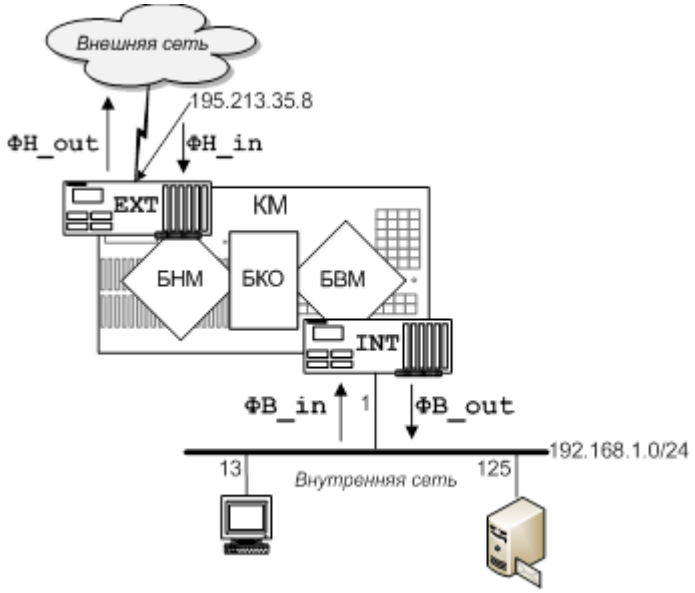


Рис. 3.23 Пример включения изделия в состав ЗСПД по типовой схеме организации межсетевого экрана

В качестве компромиссного разрешения указанных противоречий предлагается следующее.

1. Блокировать работу протокола ICMP для всех IP-адресов, кроме IP-адреса внешнего интерфейса изделия (**EXT** на Рис. 3.23). Это даст возможность выполнить процедуру PING с консоли БНМ изделия, а также обеспечит возможность проверки работоспособности внешнего интерфейса изделия устройствами внешней сети.
2. Блокировать работу протокола UDP для всех портов, за исключением номеров портов, указанных при настройке туннелей (см. раздел 3.1.1.2, с. 78) для входящих и исходящих UDP-датаграмм, а также порта **53** (DNS) для исходящих UDP-датаграмм и пользовательских портов (1025 – 65535) для входящих датаграмм

для IP-адреса внешнего интерфейса маршрутизатора изделия (**EXT** на Рис. 3.23). Разрешить работу DNS-сервера маршрутизатора изделия в режиме DNS-кэша. Это обеспечит ретрансляцию DNS-запросов станций внутренней сети к внешним DNS-серверам и обратно через маршрутизатор изделия.

Протокол TCP менее опасен для станций защищаемой сети, чем протоколы UDP и ICMP, но все-таки, чтобы устранить возможные проблемы, следует ограничить работу по протоколу TCP только необходимыми типами сервисов (номерами портов необходимых приложений). Для этого следует разрешить доступ в защищаемую сеть только для портов пользовательских приложений (с номерами из диапазона 1025 – 65535), а передачу во внешнюю сеть разрешить только для ограниченного перечня необходимых портов.

Назначим интерфейсу во внешнюю сеть (**EXT**) в качестве входного IP-фильтр с именем **ФН_in**, а в качестве выходного – IP-фильтр с именем **ФН_out**. Назначим интерфейсу во внутреннюю сеть (**INT**) в качестве входного IP-фильтр с именем **ФВ_in**, в качестве выходного – IP-фильтр с именем **ФВ_out**.

> *Внимание!* В процессе IP-фильтрации поток информации считается входящим или исходящим всегда *с точки зрения* изделия, т. е. входной IP-фильтр обрабатывает всегда поток, входящий в изделие, а выходной IP-фильтр – поток, исходящий из изделия.

Ниже приведены примеры организации на интерфейсах изделия IP-фильтров, реализующих описанный выше подход к повышению уровня обеспечения безопасного функционирования защищаемых изделием устройств во внутренней сети. Правила IP-фильтрации в фильтрах всех примерах реализуют разрешительную стратегию.

Фильтр ФН_in, контролирующий входящий в изделие поток IP-датаграмм из внешней сети.

ФН_in

	Режим	Адрес отправителя		Адрес получателя		Протокол	Порты
0	разрешить	0.0.0.0	/00	195.213.35.8	/32	ICMP	0-0
1	разрешить	0.0.0.0	/00	195.213.35.8	/32	UDP	1025-65535
2	сбросить	0.0.0.0	/00	195.213.35.8	/32	TCP	8080-8080
3	разрешить	0.0.0.0	/00	195.213.35.8	/32	TCP	0-0
4	разрешить	0.0.0.0	/00	0.0.0.0	/00	TCP	1025-65535
5	сбросить	0.0.0.0	/00	0.0.0.0	/00	ANY	0-0

Строка **0** – разрешает работу процедуры PING (протокол ICMP) между устройствами внешней сети и изделием (внешний интерфейс с адресом **195.213.35.8**).

Строка **1** – разрешает прием UDP-пакетов для пользовательских портов (ответы DNS-серверов внешней сети) только для маршрутизатора.

Строка **2** – сбрасывает TCP-пакеты, адресованные HTTP PROXY-серверу маршрутизатора (порт 8080). Это необходимо для устранения возможности транзитного использования PROXY-сервера маршрутизатора внешними абонентами

Строка **3** – разрешает прием любых TCP-пакетов приложениями изделия.

Строка **4** – разрешает не ограниченный адресами прием TCP-пакетов для пользовательских портов (ответы на запросы услуг внешних серверов из внутренней сети).

Строка **5** – сбрасывает все IP-датаграммы, для которых нет разрешения на пропуск через интерфейс предыдущими правилами.

Фильтр ФН_out, контролирующий исходящий поток IP-датаграмм от изделия во внешнюю сеть.

ФН_out

	Режим	Адрес отправителя		Адрес получателя		Протокол	Порты
0	разрешить	195.213.35.8	/32	0.0.0.0	/00	ICMP	0-0
1	разрешить	195.213.35.8	/32	0.0.0.0	/00	UDP	53-53
2	разрешить	0.0.0.0	/00	0.0.0.0	/00	TCP	0-0
3	сбросить	0.0.0.0	/00	0.0.0.0	/00	ANY	0-0

Строка **0** - разрешает работу процедуры PING (протокол ICMP) между изделием и устройствами внешней сети.

Строка **1** - разрешает отправку DNS-запросов (UDP порт 53) от изделия во внешнюю сеть.

Строка **2** - разрешает отправку любых TCP-пакетов во внешнюю сеть.

Строка **3** - сбрасывает все IP-датаграммы, для которых нет разрешения на пропуск через интерфейс предыдущими правилами.

Фильтр ФВ_in, контролирующий поток входящих в изделие IP-датаграмм из внутренней сети.

ФВ_in

	Режим	Адрес отправителя		Адрес получателя		Протокол	Порты
0	разрешить	192.168.1.0	/24	192.168.1.1	/32	ICMP	0-0
1	разрешить	192.168.1.0	/24	192.168.1.1	/32	UDP	53-53
2	разрешить	192.168.1.0	/24	0.0.0.0	/00	TCP	20-21
3	разрешить	192.168.1.0	/24	0.0.0.0	/00	TCP	80-80
4	разрешить	192.168.1.125	/32	0.0.0.0	/00	TCP	25-25
5	разрешить	192.168.1.125	/32	0.0.0.0	/00	TCP	110-110
6	разрешить	192.168.1.13	/32	0.0.0.0	/00	ANY	0-0
7	сбросить	0.0.0.0	/00	0.0.0.0	/00	ANY	0-0

Строка **0** – разрешает работу процедуры PING (протокол ICMP) между рабочими станциями внутренней сети и изделием.

Строка **1** – разрешает пропуск DNS-запросов (UDP порт 53) от станций внутренней сети к изделию.

Строка **2** – разрешает всем рабочим станциям внутренней сети работу с удаленными FTP-серверами (TCP-порты 20, 21).

Строка **3** – разрешает всем рабочим станциям внутренней сети работу с удаленными HTTP (WEB)-серверами (TCP-порт 80).

Строка **4** – разрешает почтовому серверу внутренней сети работу с удаленными SMTP-серверами (TCP- порт 25).

Строка **5** – разрешает почтовому серверу внутренней сети работу с удаленными POP3-серверами (TCP- порт 110).

Строка **6** – разрешает привилегированной рабочей станции внутренней сети полный доступ в удаленную сеть.

Строка **7** – сбрасывает все IP-датаграммы, для которых нет разрешения на пропуск через интерфейс предыдущими правилами.

Фильтр ФВ_out, контролирующий исходящий поток IP-датаграмм через внутренний интерфейс изделия во внутреннюю сеть.

ФВ_out

	Режим	Адрес отправителя		Адрес получателя		Протокол	Порты
0	разрешить	192.168.1.1	/32	192.168.1.0	/24	ICMP	0-0
1	разрешить	192.168.1.1	/32	192.168.1.0	/24	UDP	1025-65535
2	разрешить	0.0.0.0	/00	192.168.1.0	/24	TCP	1025-65535
3	разрешить	0.0.0.0	/00	192.168.1.125	/32	TCP	25-25
4	разрешить	0.0.0.0	/00	192.168.1.13	/32	ANY	0-0
5	сбросить	0.0.0.0	/00	0.0.0.0	/00	ANY	0-0

Строка **0** – разрешает работу процедуры PING (протокол ICMP) между рабочими станциями внутренней сети и изделием.

Строка **1** – разрешает прохождение ответов от DNS-сервера изделия к станциям внутренней сети.

Строка **2** – разрешает прохождение ответов от удаленных TCP-серверов к станциям внутренней сети.

Строка **3** – разрешает доступ к почтовому серверу внутренней сети всем SMTP-серверам (TCP порт 25) удаленной сети.

Строка **4** – разрешает доступ к привилегированной рабочей станции по любому протоколу

Строка **5** – сбрасывает все датаграммы, для которых нет разрешения на прохождение предыдущими правилами.

3.2.1.6. Фильтры расширенного формата

Большинство задач, решаемых изделием с использованием механизма IP-фильтрации, администратор изделия решает с применением простых IP-фильтров. Использование IP-фильтров расширенного формата позволяет решать более сложные и, как правило, реже встречающиеся задачи. Отметим, что создание IP-фильтров расширенного формата требует более высокой квалификации администратора изделия.

Фильтр расширенного формата, кроме рассмотренных выше простых правил IP-фильтрации, может содержать правила IP-фильтрации расширенного формата, а также правила IP-фильтрации типа элемент расписания.

В IP-фильтре расширенного формата несколько следующих подряд правил IP-фильтрации (простых или расширенного формата) образуют *блок правил*. Несколько следующих подряд правил IP-фильтрации типа элемент расписания образуют *блок расписания* (в частном случае любой из блоков может содержать

единственное правило IP-фильтрации). Элементы каждого блока расписания задают диапазон времени действия блока правил IP-фильтрации, следующего за блоком расписания.

В общем случае в состав IP-фильтра расширенного формата могут входить блоки правил IP-фильтрации, перемежающиеся блоками расписаний.

Создание и настройка расширенных правил IP-фильтрации. Расширенное правило IP-фильтрации выполняет все функции *простого* правила IP-фильтрации и, кроме того, в него добавлена возможность анализа до четырех полей, расположенных в любом месте IP-датаграммы. Анализируемое поле может иметь длину в один или два байта.

Чтобы создать и настроить описатель расширенного правила IP-фильтрации, следует выдать на видеомонитор ЛКУ (выбрав цепочку альтернатив ГМ: **Настройка ⇨ Защита ⇨ Фильтры**) список описателей созданных IP-фильтров (Рис. 3.20), перевести курсор на строку с нужным описателем IP-фильтра, нажать клавишу <Enter> и получить на видеомониторе ЛКУ экран редактора IP-фильтра (Рис. 3.21) со списком всех созданных ранее правил (элементов) IP-фильтрации.

Команда **`Shift_F7 – создать расширенное правило`** (Рис. 3.21) служит для создания описателя *расширенного* правила IP-фильтрации. По этой команде на видеомонитор ЛКУ будет выдан бланк создания и настройки расширенного правила IP-фильтрации (Рис. 3.24), позволяющий сформировать описатель одного расширенного правила IP-фильтрации (он будет размещен в списке описателей правил фильтрации IP-фильтра после той строки, на которую был установлен курсор перед выдачей команды).

Верхняя часть бланка создания и настройки расширенного правила IP-фильтрации и операции по настройке параметров этой части бланка аналогичны бланку для создания простого правила IP-фильтрации (Рис. 3.22, с. 94) и операциям по настройке его параметров.

Нижняя часть бланка предоставляет возможность задействовать до четырех наборов значений параметров (четырех шаблонов), каждый из которых характеризует поле фильтруемой IP-датаграммы, выбираемое для анализа, а также возможность задействовать три операции логической взаимосвязи результатов анализа полей IP-датаграммы (параметр **`Взаимосвязь`**).

Рис. 3.24 Бланк создания и настройки расширенного правила IP-фильтрации

Каждый шаблон для анализа полей позволяет задать значения следующих параметров.

`Смещение` (Рис. 3.24) – параметр указывает смещение анализируемого поля IP-датаграммы в *десятичной* системе счисления, измеряемое в байтах и отсчитываемое от начала заголовка IP-датаграммы или от начала поля данных IP-датаграммы (пропуская IP-заголовок).

Чтобы задать значение параметра, надо установить курсор на требуемое поле и нажать клавишу <Enter>. В появившееся окно ввести значение параметра (в *десятичной* системе счисления) и нажать клавишу <Enter>.

`Относительно` (Рис. 3.24) – параметр указывает точку отсчета смещения для анализируемого поля. Может принимать одно из следующих значений:

`0+` – смещение отсчитывается от начала заголовка IP-датаграммы;

`IP+` – смещение отсчитывается от начала поля данных IP-датаграммы.

Выбор нужного значения параметра осуществляется установкой курсора на требуемое поле с последующим нажатием клавиши <Enter> до появления требуемого значения.

`Значение` (Рис. 3.24) – параметр указывает эталонное значение анализируемого поля в *шестнадцатеричной* системе счисления.

Чтобы задать значение параметра, надо установить курсор на требуемое поле и нажать клавишу <Enter>. В появившееся окно ввести значение параметра (в *шестнадцатеричной* системе счисления) и нажать клавишу <Enter>.

Операция (Рис. 3.24) – параметр задает операцию сравнения анализируемого поля с эталонным значением. Возможные значения операции: **==** (равно), **!=** (не равно), **>** (больше), **>=** (больше или равно), **<** (меньше), **<=** (меньше или равно). Кроме того, параметр может принимать значение **??**; оно означает, что сравнение не выполняется.

Выбор нужного значения параметра осуществляется установкой курсора на требуемое поле с последующим нажатием клавиши <Enter> до появления требуемого значения.

Взаимосвязь – параметр предоставляет возможность указать значение максимум трех логических операций, выполняемых над результатами операций сравнения эталонных значений и содержимого полей, выбираемых из фильтруемой IP-датаграммы. Параметр может принимать одно из значений: **AND** (операция **логического И**) или **OR** (операция **логического ИЛИ**).

Выбор нужного значения параметра осуществляется установкой курсора на требуемое поле с последующим нажатием клавиши <Enter> до появления требуемого значения операции.

Создание и настройка правил IP-фильтрации типа элемент расписания. Чтобы создать элемент расписания, следует вывести на видеомонитор ЛКУ (выбрав цепочку альтернатив ГМ: **Настройка ⇨ Защита ⇨ Фильтры**) список созданных ранее IP-фильтров (см. Рис. 3.20, с. 92), перевести курсор на строку с нужным описателем IP-фильтра, нажать клавишу <Enter> и получить на видеомониторе ЛКУ экран редактора IP-фильтра (Рис. 3.21, с. 93) со списком всех созданных ранее правил (элементов) IP-фильтрации.

Команда **Alt_F7** – **создать элемент расписания** (Рис. 3.21) служит для создания правила IP-фильтрации типа *элемент расписания*. По этой команде на видеомонитор ЛКУ будет выдан бланк создания и настройки элемента расписания (см. Рис. 3.25), позволяющий сформировать строку описателя элемента расписания (она будет размещена в списке правил фильтрации IP-фильтра после той строки, на которую при выдаче команды был установлен курсор).

Каждый элемент расписания содержит параметр **Режим** (верхняя строка бланка) и собственно **Расписание** (нижняя часть бланка).

Режим (Рис. 3.25). Параметр может принимать одно из значений: *ДА* или *НЕТ*. Параметр определяет, как программой управления будут интерпретированы заданные в расписании интервалы времени: если параметру присвоено значение *ДА*, правила IP-фильтрации в указанные интервалы будут действовать (разрешающие интервалы), если значение *НЕТ* – правила IP-фильтрации будут заблокированы (запрещающие интервалы).

Расписание (Рис. 3.25). В расписании можно указать:

- *дни недели* (левая колонка бланка): знак **+** (плюс) справа от обозначения дня недели включает в расписание соответствующий день недели, знак **–** (минус) – день недели из расписания исключает;
- *диапазон дат* (шаблон в двух верхних строчках правой колонки бланка): интервал дат задается в формате **дд/мм/гггг** (если диапазон дат не задан, то он считается бесконечным);
- *временные интервалы* (две последние строчки правой колонки бланка): цифры в формате **чч.мм** позволяют задать два временных интервала.

Режим Да	
Пн +	15/02/2018
Вт –	16/03/2018
Ср –	
Чт –	10.00 - 11.00
Пт –	
Сб +	13.30 - 14.45
Вс –	

Рис. 3.25 Бланк создания и настройки элемента расписания

Применение бланка создания и настройки элемента расписания с набором введенных в бланк параметров позволяет создать одну строку описателя элемента расписания в списке правил IP-фильтрации IP-фильтра. В зависимости от решаемых изделием задач следует создать и настроить необходимое число таких строк описателей элементов расписания.

Одна строка описателя элемента расписания позволяет задать максимум два временных интервала в один или несколько дней недели в заданном диапазоне дат. Если необходимо задать больше двух временных интервалов или необходимо задать разные временные интервалы в разные дни недели или разные диапазоны дат, то следует сформировать подряд несколько строк расписания.

Программа управления не позволит создать (или отредактировать) строку описателя элемента расписания, которая в совокупности с другими строками данного блока приведет к тому, что блок расписания не будет содержать ни одного разрешающего интервала.

Работа программы управления с блоками расписаний

> *Примечание.* Напомним, что программа управления обрабатывает и интерпретирует список всех правил IP-фильтра (простых, расширенных, элементов расписания) всегда последовательно в направлении сверху вниз.

При описании алгоритма работы блока расписания будем говорить о *диапазоне времени действия блока правил IP-фильтрации*. Этот диапазон времени может иметь значения: *ВСЕГДА*, *НИКОГДА* или принимать значение диапазона времени, объединяющего все временные интервалы, заданные правилами одного блока расписания.

Перед началом применения IP-фильтра *диапазон времени* действия блока правил IP-фильтрации имеет значение *ВСЕГДА*. Следовательно, если в IP-фильтре первым находится блок описателей правил (или единственный описатель правила) IP-фильтрации, то все содержащиеся в нем описатели правил IP-фильтрации будут действовать *всегда*: во все дни недели, в любое время.

Перед началом работы с каждым блоком описателей элементов расписания *диапазон времени* действия блока правил IP-фильтрации имеет значение *НИКОГДА*. Содержащиеся в блоке описатели элементов расписания задают один или несколько не нулевых интервалов времени (хотя бы один интервал должен быть задан обязательно). Диапазон времени получит значение, соответствующее заданному расписанию.

Если в момент применения программой управления IP-фильтра дата, день недели или интервалы времени попадают в *диапазон времени* действия блока правил фильтрации, следующий за блоком описателей элементов расписания блок описателей правил IP-фильтрации будет применен программой управления, если не попадает – блок описателей правил IP-фильтрации программой управления пропускается.

Пример описателей элементов расписания:

```
ДА Пн Вт Ср Чт Пт Сб Вс 01/05/2016 - 31/12/2017 08.00-18.00, 20.00-23.00
НЕТ Пн Вт Ср Чт Пт Сб Вс 13.00-14.00
```

Первый элемент, приведенный в примере, устанавливает параметру **Режим** значение *ДА* по расписанию: с 8 часов до 18 часов и с 20 часов до 23 часов во все дни недели с 1 мая 2016 года по 31 декабря 2017 года. Второй элемент исключает из этого времени интервал с 13 часов до 14, в течение которого пропуск IP-датаграмм через интерфейс запрещен.

Алгоритм работы IP-фильтра расширенного формата

Алгоритм сравнения параметров фильтруемой IP-датаграммы с параметрами расширенных правил IP-фильтрации реализуется программой управления в два этапа.

На первом этапе обработки выполняется сравнение в объеме сегмента параметров простого правила IP-фильтрации (согласно алгоритму, рассмотренному в разделе 3.2.1.3, с. 93).

> *Напомним*, что параметры *простого* правила входят в состав параметров правила IP-фильтрации *расширенного формата*.

Только в случае положительного результата сравнения на первом этапе обработки IP-датаграммы выполняется второй этап – анализ полей IP-датаграммы на соответствие значениям дополнительных параметров правила расширенного формата.

Алгоритм работы программы управления при выполнении анализа фильтруемой IP-датаграммы включает следующие шаги.

1. При передаче IP-датаграммы для проверки IP-фильтру вычисляется текущий момент времени. Элементы фильтра просматриваются сверху вниз, начиная с первого. Вычисляется *диапазон времени действия блока правил фильтрации* и проверяется, попадает ли текущий момент в этот *диапазон*. Если не попадает, то следующий за блоком расписания блок правил IP-фильтрации пропускается и просматривается следующий блок расписания.

2. Если текущий момент попадет в *диапазон времени действия блока правил фильтрации*, то IP-датаграмма предъявляется по очереди правилам IP-фильтра из блока, следующего за блоком расписания. Процесс проверок на соответствие параметров IP-датаграммы очередному правилу IP-фильтрации продолжается до первого совпадения. Соответствие данных IP-датаграммы правилу IP-фильтрации фиксируется в случае, когда выполняются следующие условия.
   a. Проведено сравнение параметров IP-датаграммы со всеми параметрами простого правила – с частью правила IP-фильтрации расширенного формата (см. раздел 3.2.1.3, с. 93) и получен положительный результат. В этом случае анализ данных IP-датаграммы продолжается и начинается сравнение значений полей IP-датаграммы с не проверявшимися на первом этапе обработки параметрами, указанными в описателе правила IP-фильтрации расширенного формата.
   b. Вычисляется положение первого контролируемого поля (обозначим значение первого контролируемого поля – **B1**) и выполняется заданная операция сравнения (**B1opE1**, где **E1** – значение эталонного поля, **op** – операция сравнения). Эти действия повторяются для всех контролируемых полей IP-датаграммы.

c. Результаты сравнения по всем заданным полям объединяются в одно логическое значение с помощью заданных значений взаимосвязи:

(B1opE1)V1_2(B2opE2)V2_3(B3opE3)V3_4(B4opE4), здесь **Vn_m** – значения параметра **Взаимосвязь** для соответствующих пар результатов сравнения.

d. Если полученное логическое значение равно **1**, то фиксируется соответствие данных IP-датаграммы параметрам правила IP-фильтрации расширенного формата; если логическое значение равно **0**, то IP-датаграмма данному правилу не соответствует.

3. Если зафиксировано совпадение и параметр **Режим** правила имеет значение *разрешить*, то результат проверки считается положительным, и IP-датаграмма передается на дальнейшую обработку.

4. Если зафиксировано совпадение, но параметр **Режим** правила имеет значение *запретить*, то результат проверки считается отрицательным, IP-датаграмма отбрасывается, а в адрес отправителя формируется ICMP-сообщение типа: **Destination Unreachable** с кодом **Host Unreachable**.

5. Если зафиксировано совпадение, но параметр **Режим** правила имеет значение *сбросить*, результат проверки считается отрицательным, IP-датаграмма отбрасывается, никаких сообщений отправителю не посылается.

6. Если проверяемая IP-датаграмма не соответствует ни одному правилу IP-фильтрации, то результат проверки считается отрицательным, IP-датаграмма отбрасывается, а в адрес отправителя формируется соответствующее ICMP-сообщение.

Процесс создания IP-фильтра и внесения в него любых изменений находится под контролем программы управления.

1. Программа управления проверяет, чтобы *диапазон времени действия блока правил фильтрации*, задаваемый блоком расписания, содержал хотя бы один *разрешающий* интервал.

   Программа управления *не позволит* создать блок расписания, в котором не выполнено это условие.

2. Программа управления проверяет каждый элемент фильтра (каждое правило): не противоречит ли он остальным элементам, пересекающимся с данным по *диапазону времени действия*. Программа управления не запретит создать правило, противоречащее другим правилам, но выдаст предупреждение.

3. Программа управления позволяет создать произвольное число IP-фильтров, каждый IP-фильтр может содержать произвольное число правил IP-фильтрации, но суммарное число всех строк описателей во всех IP-фильтрах не может превышать значения 4000.

Процесс создания IP-фильтра и внесения в него изменений фиксируется на видеомониторе ЛКУ, а также в виде записи в системном журнале (файл **LOG.EMA**). Каждое действие персонала сопровождается выводом на видеомонитор ЛКУ и записью в файл журнала двух текстовых строк следующего формата:

```
Фильтр <имя_фильтра>. <выполненное действие> элемент <номер_строки_фильтра>
[строка таблицы фильтра после внесения изменений]
```

Значение элемента записи <выполненное действие> – это одно из следующих значений: **Удален**, **Добавлен**, **Изменен**, **Заблокирован**, **Разблокирован**.

Пример:

```
Фильтр ФИЛЬТР1. Изменен элемент 3
[разрешить 0.0.0.0    /00  192.169.1.0     /24   ANY  0-0]
```

Таким образом, все действия персонала по сопровождению IP-фильтров (создание, удаление, корректировка) протоколируются в журнале изделия и могут быть распечатаны и проанализированы позднее.

3.2.1.7. Системные IP-фильтры

Системные IP-фильтры имеют фиксированные *системные имена* (см. раздел 3.2.1.1, с. 90). Формируются системные IP-фильтры так же, как и все остальные. Системные IP-фильтры могут включать простые правила IP-фильтрации, правила IP-фильтрации расширенного формата и элементы расписания.

Функции системных фильтров

1. **Фильтры внутренних (служебных) интерфейсов**. Внутренний (служебный) интерфейс в составе каждого из маршрутизаторов изделия (БНМ и БВМ) является логическим (фиктивным) и, не требуя действий администратора по его созданию и настройке, создается и активизируется программой управления при запуске изделия. Привязка IP-фильтров к внутреннему интерфейсу маршрутизатора обеспечивается путем использования зарезервированных системных имен при создании фильтров: **int_in** и **int_out** – во внутреннем блоке маршрутизации и **ext_in** и **ext_out** – в наружном блоке маршрутизации.

Правила IP-фильтрации потоков IP-датаграмм, *исходящих* через внутренние (служебные) интерфейсы маршрутизаторов от прикладных сервисов (служб) изделия, должны описываться соответственно в IP-фильтрах с системными именами **int_out** (в составе БВМ) и **ext_out** (в составе БНМ). *Входящие* потоки внутренних интерфейсов для служб маршрутизаторов фильтруется с помощью IP-фильтров с системными именами **int_in** и **ext_in**. Алгоритм работы этих IP-фильтров аналогичен алгоритму работы рассмотренных ранее IP-фильтров сетевых интерфейсов изделия.

2. **Фильтр избирательной трассировки**. Для реализации режима *избирательной* трассировки IP-трафика, проходящего через интерфейсы изделия (см. раздел 4.1.3, с. 131) в составе каждого из маршрутизаторов изделия может быть создан IP-фильтр с системным именем **trace**. При наличии такого фильтра трассировка будет выполняться только для IP-датаграмм, разрешенных этим фильтром.

   Замечания.

   1. Системный фильтр **trace** самостоятельно не включает никаких режимов трассировки, он лишь *ограничивает* поток вывода трассировочной информации, заданной установленными режимами трассировки интерфейсов. Для включения режима трассировки конкретного интерфейса с использованием системного фильтра **trace** необходимо:
      - сформировать IP-фильтр с системным именем **trace**;
      - включить трассировку этого интерфейса.
   2. Фильтр **trace** действует как ограничитель трассировки всех интерфейсов изделия.
   3. Фильтр **trace** не может ограничить поток трассировочной информации маршрутизатора.

3. **Фильтры управления приоритетом**. Фильтры с системными именами **prt_0**, **prt_1**, **prt_2**,**...prt_7** используются для изменения (*классификации* и *маркирования*) значения *приоритета* (подполе **IP Precedence** поля **Type of Service** (ToS) в заголовке IP-датаграммы − подробнее см. раздел ***Приложение Г***, с. 238 к настоящему РНУ) всех обрабатываемых интерфейсами изделия IP-датаграмм. Каждая из обрабатываемых IP-датаграмм анализируется на соответствие разрешающим правилам системных IP-фильтров: **prt_0**, **prt_1**, **prt_2**,**...prt_7**. Если соответствие фиксируется, то значение поля приоритета в IP-заголовке датаграммы (биты IPP поля ToS) принудительно изменяется на значение номера соответствующего IP-фильтра в *бинарном* представлении. Если IP-датаграмма не подпадает под условия ни одного из системных **prt**-фильтров, ее поле приоритета остается без изменения.

   С помощь системных **prt**-фильтров можно промаркировать поток IP-датаграмм, реагируя на множество их параметров, включая:
   - адреса отправителя и получателя IP-датаграммы;
   - значение поля протокола в IP-заголовке;
   - порты отправителя и получателя IP-датаграммы;
   - длина IP-датаграммы.

4. **Фильтр выполнения DNS-запросов из локального DNS-кэша**. Фильтр с системным именем **dnslocal** используется DNS-сервером маршрутизатора изделия. Все DNS-запросы, для которых правилами **dnslocal**-фильтра задан режим **разрешить**, удовлетворяются *только* из локального DNS-кэша маршрутизатора изделия (подробнее см. раздел 5.4.2, с. 160).

5. **Фильтр разделения DNS-запросов на внутренние и внешние**. Фильтр с системным именем **dns_int** используется DNS-сервером маршрутизатора изделия и предназначен для разделения всех поступающих к DNS-серверу запросов на *внутренние* и *внешние*. Все DNS-запросы, для которых правилами фильтра **dns_int** задан режим **разрешить**, считаются внутренними. Для ответов на такие запросы используются только *внутренние* зоны DNS-сервера и локальный DNS-кэш. Все остальные DNS-запросы (не подпавшие под разрешающие правила фильтра с именем **dns_int** и фильтра с именем **dnslocal**) считаются *внешними*. Для ответов на такие запросы используются только *внешние* зоны DNS-сервера и локальный DNS-кэш.

6. **Фильтр разрешения пересылки зон DNS-сервера**. Фильтр с системным именем **dns_zone** используется DNS-сервером маршрутизатора изделия и предназначен для указания *внешних* DNS-серверов, которым разрешена *пересылка зон* по TCP-протоколу. Операция *пересылки зоны* используется для организации *вторичных* DNS-серверов. С помощью этой операции вторичный DNS-сервер в любой момент может запросить полное копирование информации о любой DNS-зоне, хранящейся на *первичном* DNS-сервере. Для устранения возможности несанкционированного доступа к информации DNS-зон все внешние DNS-серверы, которым дано право чтения информации зон, должны быть указаны в разрешающих правилах фильтра с именем **dns_zone**. Все запросы на пересылку информации зон DNS-сервера маршрутизатора изделия, не подпавшие под разрешающие правила фильтра **dns_zone**, будут отвергнуты.

7. **Фильтр трафика удаленного управления**. Для обеспечения удаленного управления изделием, исполненным в *односегментной* архитектуре технологии DioNIS®, с помощью изделий нового поколения следует на управляемом изделии выполнить соответствующие настройки фильтра с системным именем **dcp** (**dcp**-фильтра) и инициировать работу его DCP-службы. Указанные настройки следует выполнить в соответствии с требованиями эксплуатационной документации на конкретное изделие защиты.

3.2.1.8. Фильтры с отслеживанием состояния соединения

Модель информационного взаимодействия при использовании internet/intranet-технологии часто организована в архитектуре *клиент-сервер*. Прикладная работа клиентов строится на понятии *сессии*[*]. Инициируется сессия всегда клиентом, сервер отвечает на предложение клиента об установлении соединения. Разрыв соединения могут выполнить как клиент, так и сервер.

В соответствии с правилами IP-адресации (см. ***Приложение А***, с. 214) для идентификации в сетях передачи данных приложений клиента и сервера следует указывать их *полный* адрес, состоящий из *IP-адреса* вычислительной системы и *номера порта*, идентифицирующего компонент прикладного программного обеспечения на этой вычислительной системе.

Номер порта здесь – это двухбайтовое целое число в диапазоне от ***0*** до ***65535***. Для нумерации портов сервера (служб) используется диапазон ***0–1024***, при этом номера портов сервера постоянно закреплены за приложением сервера конкретного типа. Например: порт **23** – служба Telnet, порт **25** – служба SNTP и т.д.

Для нумерации портов клиентов выделен пользовательский диапазон ***1025–65535***. Конкретное значение используемого порта выбирается программным обеспечением автоматически по некоему алгоритму. Поэтому несколько последовательных соединений одного клиента с одним и тем же сервером могут иметь один и тот же порт сервера и разные порты клиента.

Как было сказано выше, IP-фильтры обеспечивают контроль проходящих через интерфейсы изделия потоков информации: отфильтровывают нежелательные IP-датаграммы и пропускают на дальнейшую обработку IP-датаграммы, прошедшие барьер IP-фильтрации.

Если организовывать контроль сессий клиент-сервер с помощью обычных IP-фильтров (фильтров, во всех правилах которых параметр **Режим** имеет одно из значений *Разрешить*, *Запретить* или *Сбросить*), то необходимо:

- открыть IP-адреса и порты требуемых серверов;
- открыть *все* пользовательские порты в направлении **сервер ⇨ клиент**.

В результате возникает возможность прохождения трафика, не порожденного «правильной» сессией, что создает уязвимость системы защиты.

Кроме того, процесс проверки проходящего IP-потока (анализ правил IP-фильтрации) занимает время, особенно при большом количестве правил IP-фильтрации, что влияет на быстродействие работы изделия в целом.

Для решения обеих проблем (увеличения уровня безопасности и ускорения обработки IP-датаграмм) реализован особый класс фильтров – фильтры с отслеживанием состояния соединений – *фильтры сессий*. Такой фильтр отслеживает состояние текущих соединений и *автоматически* открывает (а затем закрывает) доступ для разрешенных IP-датаграмм.

Фильтр сессий представляет собой динамически сопровождаемую *таблицу сессий*. Записи в таблицу добавляются в момент начала сессии, инициируемой пользователем, если выполнены следующие условия:

- в изделии создан обычный IP-фильтр (фильтр входящих или фильтр исходящих IP-датаграмм) и в нем существует правило, в котором параметр **Режим** имеет значение *Сессия*;
- параметры IP-датаграммы совпадают с параметрами правила IP-фильтрации.

Когда приходит первая IP-датаграмма, удовлетворяющая этому правилу, она передается на дальнейшую обработку и одновременно формируется разрешающая запись в таблице (фильтре) сессий.

Все последующие IP-датаграммы, относящиеся к этой сессии, будут пропускаться без повторной IP-фильтрации в обычном IP-фильтре.

---

[*] Сессия – это периодический интерактивный сеанс обмена информацией (сообщениями) между двумя коммуникационными устройствами (или между клиентом и сервером). Сессия устанавливается в определенный момент времени и разрывается спустя какое-то время. Сессия может включать обмен несколькими сообщениями в каждом направлении. Жизненный цикл сессии включает следующие фазы (состояния): *установление соединения*, *передача данных*, *завершение соединения*.

Работу фильтра сессий можно проиллюстрировать с помощью схемы, представленной на Рис. 3.26. На рисунке представлен интерфейс маршрутизатора изделия с двумя IP-фильтрами: фильтром входящих и фильтром исходящих IP-датаграмм.

Когда на интерфейс приходит исходящая IP-датаграмма, прежде всего проверяется таблица сессий. Если в таблице есть запись, обеспечивающая прохождение IP-датаграммы (IP-датаграмма принадлежит уже установленной сессии), то IP-датаграмма сразу же пропускается дальше. Если записи в таблице сессий нет, датаграмма идет в IP-фильтр исходящих IP-датаграмм интерфейса.

Изначально таблица сессий пуста, т.е. вначале ни на одну IP-датаграмму в таблице записей нет. Поступившая на интерфейс исходящая IP-датаграмма передается на проверку ее соответствия правилам IP-фильтра исходящих IP-датаграмм и обрабатывается там стандартным для IP-фильтрации образом. Если при этом в IP-фильтре исходящих находится подходящее разрешающее правило IP-фильтрации, то датаграмма пропускается дальше и, если поле **Режим** этого правила имеет значение *Сессия*, то в таблице сессий формируется разрешающая запись.

Когда на интерфейс приходит входящая IP-датаграмма, прежде всего проверяется таблица сессий. Если IP-датаграмма принадлежит уже установленной сессии, то она передается на дальнейшую обработку, минуя фильтр входящих IP-датаграмм.

Если в таблице сессий нет записи, обеспечивающей прохождение IP-датаграммы, то IP-датаграмма передается в обычный IP-фильтр входящих и проверяется там обычной линейной IP-фильтрацией.

Если в IP-фильтре входящих находится подходящее разрешающее правило IP-фильтрации, то IP-датаграмма пропускается в маршрутизатор и, если поле **Режим** этого правила имеет значение *Сессия*, то в таблице сессий формируется соответствующая разрешающая запись.

В дальнейшем фильтр сессий отслеживает, откуда пришла IP-датаграмма – оттуда же, откуда пришла датаграмма, создавшая запись в таблице сессий, или нет, и в зависимости от этого тот или другой адрес в записи считает адресом отправителя и адресом получателя; это же относится и к номерам портов отправителя и получателя.

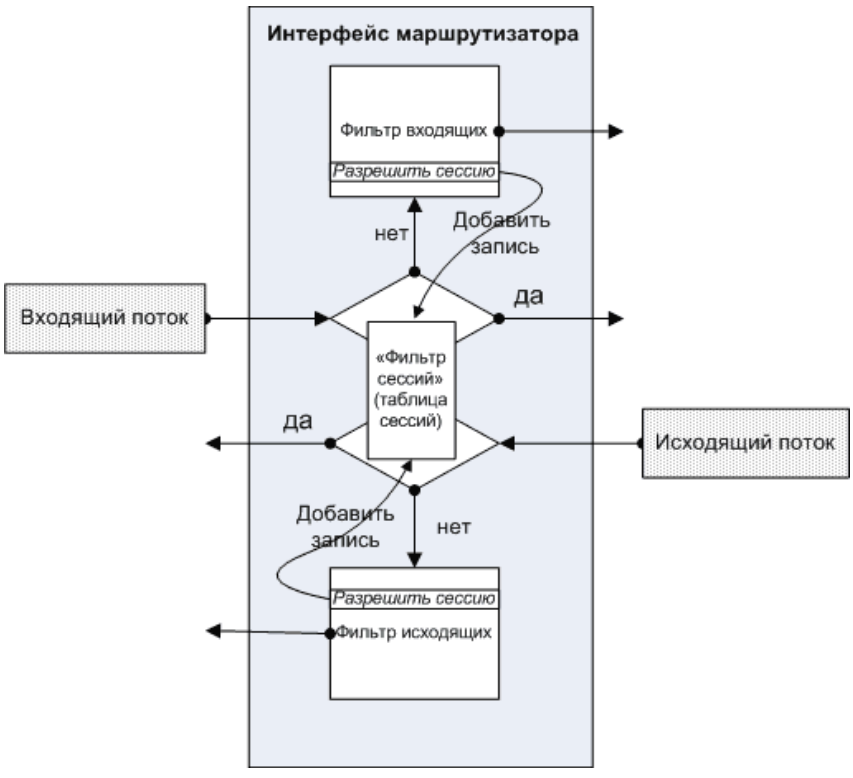


Рис. 3.26 Схема, иллюстрирующая алгоритм работы фильтра сессий

Записи в таблице сессий создаются *динамически* по мере необходимости и имеют ограниченное время жизни: записи исчезают из таблицы автоматически по окончании сессии или по истечении времени. Это повышает уровень безопасности.

Использование таблицы сессий особенно эффективно с точки зрения обеспечения безопасности при прохождении ответной IP-датаграммы от сервера к клиенту – нет необходимости открывать весь диапазон пользовательских портов.

Каждый интерфейс имеет собственную таблицу сессий.

Наличие рассмотренного механизма позволяет строить самые различные системы безопасности. Например, можно в IP-фильтре исходящих задать единственное правило – разрешить TCP-сессию всем внутренним абонентам, а в IP-фильтре входящих запретить все. Такие фильтры (содержащие по одному правилу) будут работать мгновенно. Фильтр входящих будет отсекать любые входящие IP-датаграммы, если для них нет записи в таблице сессий, а записи в таблицу сессий будут заноситься только тогда, когда будут исходящие запросы от внутренних абонентов. Таким образом, путем элементарного конфигурирования достигается очень серьезная защита: запрещено любое воздействие из внешней среды – заблокированы все внешние IP-датаграммы, кроме тех, которые идут в ответ в рамках сессий, установленных внутренними абонентами.

> *Внимание!* Для корректной работы фильтра сессий требуется, чтобы на интерфейсе были установлены два фильтра: IP-фильтр исходящих и IP-фильтр входящих IP-датаграмм. Это требование обусловлено особенностями реализации подсистемы IP-фильтрации в ПО изделия – в отсутствие фильтра исходящих или фильтра входящих IP-датаграмм соответствующий поток данных проходит через интерфейс без всяких проверок, т.е. этот поток не будет контролироваться таблицей сессий.

Фильтры сессий можно применять только к TCP, UDP и ICMP-пакетам. Т.е. в тех правилах обычного IP-фильтра (исходящих или входящих IP-датаграмм), в которых параметр **Режим** имеет значение *Сессия*, параметр **Протокол** может иметь только одно из трех значений *TCP*, *UDP* или *ICMP*.

В любом IP-фильтре (исходящих или входящих IP-датаграмм) может быть любое число правил IP-фильтрации, в которых параметр **Режим** имеет значение *Сессия*.

Понятие сессии в полной мере применимо только к TCP-протоколу: TCP-сессия имеет три состояния: состояние установления соединения, состояние передачи данных и состояние завершения соединения. Для других протоколов реально сессия не существует, но в таблице сессий выполняется ее имитация для того, чтобы можно было использовать фильтры сессий.

3.2.1.9. Фиксация последовательности обработки IP-датаграмм

Процесс последовательности обработки IP-датаграмм маршрутизатором может быть запротоколирован в системном журнале (в файле с именем **LOG_TCP.EMA**), если в правилах IP-фильтрации установлен режим *фиксации* IP-датаграмм. Режим фиксации IP-датаграмм устанавливается с помощью параметра IP-фильтра **Фиксировать**, которому следует присвоить значение *ДА* (см. выше – раздел 3.2.1.3, с. 93 и Рис. 3.22). Для всех IP-датаграмм, удовлетворяющих правилам таких IP-фильтров, будет выполняться запись в системный журнал соответствующего маршрутизатора.

> Формат заносимых в журнал записей рассмотрен в разделе ***Приложение Е*** (с. 248) при описании файла **LOG_TCP.EMA**. Оперативный просмотр файла **LOG_TCP.EMA** возможен с помощью цепочки альтернатив ГМ: **Консоль** ⇨ **Журналы** (см. раздел 8.2, с. 181).

Фиксация IP-датаграмм может быть затребована как в правилах IP-фильтрации, в которых параметр **Режим** имеет значение *запретить* или *сбросить*, так и в правилах, в которых параметр **Режим** имеет значение *разрешить*. В первом случае будут фиксироваться *все* нарушения правил IP-фильтрации. Во втором случае правилами IP-фильтрации можно задать режим отслеживания потоков данных, интересующих администрацию узла. Это позволяет, во-первых, вести статистику прохождения IP-датаграмм и, во-вторых, понимать, по какой причине (вследствие какого обстоятельства) IP-датаграмма не доставлена.

Для оперативного отслеживания появления в журнале записей фиксации IP-датаграмм программа управления ведет счетчик числа выполненных процедур фиксации. Значение счетчика выводится в левом нижнем углу меню функций **Диагностика** (см. раздел 9, Рис. 9.1, с. 187). При запуске изделия счетчик фиксации IP-датаграмм обнуляется. При выполнении очередной процедуры фиксации IP-датаграммы значение счетчика увеличивается на единицу. Наблюдая за счетчиком, персонал изделия может отследить появление в потоке IP-датаграмм и в журнале ожидаемой информации.

Фиксация IP-датаграмм требует значительных ресурсов изделия (времени процессора и дискового пространства) и существенно замедляет его работу, поэтому устанавливать режим фиксации IP-датаграмм следует только для тех правил IP-фильтрации, которые действительно представляют интерес.

> *Примечание.* Напомним, что правило *по умолчанию* в составе любого IP-фильтра (см. раздел 3.2.1.4, п. 4, с. 96) предполагает фиксацию в журнале всех IP-датаграмм, не подпавших под основные правила IP-фильтра. Часто в этом нет необходимости. В этом случае рекомендуется последним правилом IP-фильтра *явно* ставить правило следующего содержания:
>
> **Сбросить 0.0.0.0 /00 0.0.0.0 /00 ANY 0-0**
>
> и в нем параметру **Фиксировать** присвоить значение *НЕТ*.

3.2.1.10. Отладка IP-фильтров

Создание IP-фильтров требует определенного навыка и достаточных знаний о структуре Ethernet-кадров, формате IP-пакетов и организации обработки IP-потоков. В процессе работы с IP-фильтрами неизбежно возникают ошибки, которые иногда бывает трудно диагностировать визуальным контролем содержательной части IP-фильтров (набора правил IP-фильтрации и их последовательности в IP-фильтре).

В помощь администратору в изделии предусмотрена возможность трассировки потоков данных, проходящих через IP-фильтры (диагностика процесса работы IP-фильтров).

Включается трассировка процесса обработки проходящих через фильтры IP-датаграмм с помощью цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ Активные**. При выборе указанной цепочки альтернатив на видеомонитор ЛКУ выводится список всех *активных* в настоящее время сетевых интерфейсов. Для каждого из сетевых интерфейсов изделия с помощью клавиши <Enter> можно установить необходимые режимы трассировки и, в частности, можно задать трассировку IP-фильтров интерфейса (подробнее см. раздел 9.2.2, с. 189).

Если задана трассировка IP-фильтров активного интерфейса, то при поступлении IP-датаграммы на соответствующий IP-фильтр входящих или исходящих IP-потоков выполняется запись процесса обработки IP-датаграммы согласно правилам IP-фильтрации в системный журнал **LOG.EMA**.

Для просмотра журнала **LOG.EMA** следует воспользоваться цепочкой альтернатив ГМ: **Консоль ⇨ Журналы** (см. раздел 8.2, с. 181).

3.2.2. Фильтрация потоков Ethernet-кадров

С целью повышения устойчивости функционирования изделия на фоне сетевых атак со стороны сетей передачи данных, к которым изделие подключается с помощью внутренних и внешних *физических* сетевых интерфейсов, изделием поддерживается механизм фильтрации потоков Ethernet-кадров, *входящих* в каждый из физических интерфейсов изделия.

3.2.2.1. Общие сведения о фильтрации потоков Ethernet-кадров (L2- уровень)

Каждый Ethernet-кадр, принятый из сети физическим интерфейсом изделия (L2–Eth-интерфейсом или Ethernet-интерфейсом), может быть подвергнут путем настройки соответствующих параметров интерфейса *анализу*, автоматически выполняемому программой управления. Цель анализа − принять решение, продолжить дальнейшую обработку Ethernet-кадра изделием или немедленно прекратить ее.

> *Примечание.* Отметим, что фильтрация потоков Ethernet-кадров выполняется на L2-уровне – канальном уровне – модели OSI, что, помимо повышения устойчивости работы изделия в условиях сетевых атак, повышает и эффективность работы маршрутизаторов изделия, поскольку они не участвуют в процессе отбраковки нежелательных Ethernet-кадров.

Анализ выполняется путем сравнения MAC-адреса того устройства в сети, которое является источником поступившего на физический интерфейс изделия входящего Ethernet-кадра, со списком значений MAC-адресов, подготовленным заранее администратором изделия при настройке соответствующего сетевого интерфейса.

Для каждого из используемых физических сетевых интерфейсов изделия его администратором может быть подготовлен соответствующий список MAC-адресов доверенных устройств в сети, с которыми изделию предстоит обмениваться данными. Организационная сторона составления списков MAC-адресов настоящим РНУ не рассматривается.

Фильтрация поступившего из сети Ethernet-кадра на соответствие MAC-адреса его отправителя списку доверенных MAC-адресов выполняется только для *физических* интерфейсов маршрутизаторов изделия – L2–Eth-интерфейсов (БВМ) и Ethernet-интерфейсов (БВМ и БНМ).

3.2.2.2. Создание и настройка таблиц фильтрации потоков Ethernet-кадров по MAC-адресам

Организация процессов фильтрации на соответствие спискам MAC-адресов поступающих из сети на физические интерфейсы изделия *входящих* потоков Ethernet-кадров похожа на организацию процессов фильтрации *входящих* в интерфейс и *исходящих* из него IP-датаграмм (см. раздел 3.2.1.2, с. 92).

Для организации процесса фильтрации Ethernet-кадров по MAC-адресам следует:

- создать и настроить соответствующую таблицу, содержащую список MAC-адресов доверенных сетевых устройств;
- связать созданную ранее таблицу, содержащую список MAC-адресов, с соответствующим физическим L2–Eth-интерфейсом или Ethernet-интерфейсом.

С целью создания и настройки таблицы, содержащей список MAC-адресов, следует выбрать цепочку альтернатив ГМ: **Настройка ⇨ Защита ⇨ Таблица MAC-адресов**. В ответ на видеомонитор ЛКУ будет выдан аналогичный представленному на Рис. 3.27 экран создания и настройки таблиц MAC-адресов.

Средняя часть экрана содержит список *имен* ранее созданных таблиц MAC-адресов (изначально список пустой).

В нижней части экрана размещена справочная информация о клавишах и их комбинациях, с помощью которых администратор изделия может выполнить создание и настройку таблиц MAC-адресов.

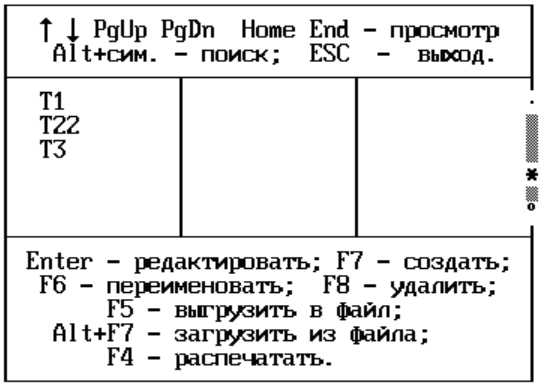


Рис. 3.27 Экран создания и настройки таблиц MAC-адресов

Для создания новой таблицы MAC-адресов следует сначала, используя экран создания и настройки таблиц MAC-адресов (Рис. 3.27), создать структуру описателя новой таблицы, присвоив ей *имя*, а затем, используя бланк создания и настройки записей таблицы MAC-адресов (Рис. 3.28), наполнить таблицу соответствующим списком MAC-адресов доверенных сетевых устройств.

F7 – **создать** (Рис. 3.27). Нажатие клавиши <F7> приводит к выводу на видеомонитор ЛКУ запроса, позволяющего ввести имя создаваемой таблицы MAC-адресов. Имя может быть произвольным, но уникальным (проверку уникальности выполняет программа управления). После ввода имени таблицы MAC-адресов на видеомонитор ЛКУ выводится бланк создания и настройки записей таблицы MAC-адресов (Рис. 3.28), позволяющий сформировать собственно список MAC-адресов соответствующей таблицы.

Enter – **редактировать** (Рис. 3.27). Нажатие клавиши <Enter> вызывает выдачу на видеомонитор ЛКУ бланка создания и настройки записей той таблицы MAC-адресов (Рис. 3.28), на строку с именем которой в момент нажатия клавиши <Enter> был установлен курсор.

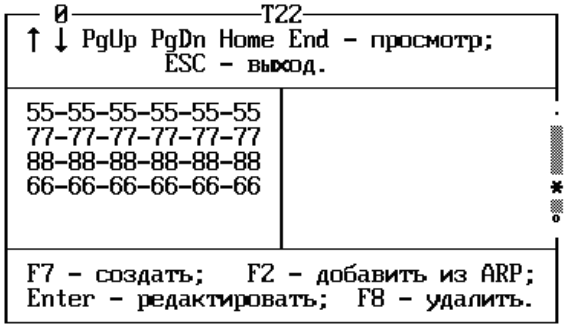


Рис. 3.28 Бланк создания и настройки записей таблицы MAC-адресов

Ниже приведены пояснения к операциям, которые можно выполнить с помощью этого бланка.

F7 – **создать** (Рис. 3.28). Нажатие клавиши <F7> приводит к выводу на видеомонитор ЛКУ запроса на ввод вручную MAC-адреса доверенного сетевого устройства. Запрос должен быть введен с учетом предлагаемого формата ввода значения MAC-адреса.

F2 – **добавить из ARP** (Рис. 3.28). Нажатие клавиши <F2> приводит к автоматическому пополнению списка ранее введенных в таблицу MAC-адресов MAC-адресами, содержащимися в ARP-таблице соответствующего маршрутизатора изделия.

> *Замечание.* Напомним, что работа каждого из маршрутизаторов изделия – БВМ или БНМ – организована со своей индивидуальной ARP-таблицей.
>
> Применение клавиши <F2> с целью пополнения таблицы MAC-адресов из ARP-таблицы маршрутизатора носит вспомогательный (сервисный) характер. Этот сервис призван облегчить труд администратора и снизить число ошибок при вводе конкретных MAC-адресов.
>
> Отметим однако, что при нажатии клавиши <F2> в настраиваемую таблицу фильтрации по MAC-адресам из ARP-таблицы БВМ будут внесены *все* MAC-адреса, с которыми маршрутизатор работает в текущий момент времени по *всем* его сетевым физическим интерфейсам. Поэтому для повышения эффективности работы настраиваемого сетевого интерфейса администратору следует удалить не относящиеся к его работе MAC-адреса устройств, с которыми БВМ работает по соседним сетевым физическим интерфейсам.

Enter – **редактировать** (Рис. 3.28). Нажатие клавиши <Enter> вызывает выдачу на видеомонитор ЛКУ запроса на ввод нового значения MAC-адреса. Введя в поле запроса (в соответствующем формате) новое значение MAC-адреса, следует нажать клавишу <Enter>, после чего будет обновлено значение того MAC-адреса, на строку с которым был установлен курсор перед первым нажатием клавиши <Enter>.

F8 – **удалить** (Рис. 3.28). При нажатии клавиши <F8> будет выдан дополнительный запрос и после его подтверждения будет удален тот MAC-адрес, на строке которым был установлен курсор.

F6 – **переименовать** (Рис. 3.27). Для выполнения функции переименования таблицы MAC-адресов следует предварительно в списке имен таблиц MAC-адресов установить курсор на имя той таблицы, которую следует переименовать. Последующее нажатие клавиши <F6> приводит к выводу на видеомонитор ЛКУ запроса на ввод нового имени таблицы, в ответ на который следует ввести новое имя и нажать клавишу <Enter>. В результате ранее созданный описатель таблицы MAC-адресов получит новое имя.

F8 – **удалить** (Рис. 3.27). При нажатии клавиши <F8> будет выдан запрос и после подтверждения будет удален описатель той таблицы, на строку с именем которой был установлен курсор.

F5 – **выгрузить в файл** и **Alt+F7** – **загрузить из файла** (Рис. 3.27). Эти две операции служат для облегчения труда администратора изделия. Первая позволяет выгрузить указанный курсором описатель таблицы MAC-адресов в файл, вторая позволяет создать новую таблицу MAC-адресов и загрузить в нее содержимое таблицы из файла. Имя файла и имя таблицы запрашиваются дополнительно. Информация о таблицах MAC-адресов, переносимая в файл, хранится в нем в бинарном виде.

F4 – **распечатать в файл** (Рис. 3.27). При нажатии клавиши <F4> содержимое таблицы MAC-адресов, на описатель которой указывает курсор, преобразуется в текстовый формат и записывается в файл. Имя файла при этом запрашивается дополнительно.

- связать созданную ранее таблицу, содержащую список MAC-адресов, с соответствующим физическим L2–Eth-интерфейсом или Ethernet-интерфейсом.

Выполнив первый этап организации процесса фильтрации входящих Ethernet-кадров на соответствие ограниченным спискам MAC-адресов – создание и наполнение соответствующей таблицы MAC-адресами доверенных сетевых устройств, следует выполнить второй этап – настройку конкретного сетевого интерфейса на использование при функционировании созданной таблицы MAC-адресов (см. раздел 2.3.1, Рис. 2.9, с. 29).

3.3. Трансляция сетевых адресов (NAT/PAT-обработка)

Технология трансляции сетевых адресов (технология NAT) предполагает продвижение пакета во *внешней* (глобальной) сети на основании IP-адресов (или IP-адресов и портов), отличающихся от тех, которые используются для маршрутизации пакета во *внутренней* (корпоративной) сети.

Одной из наиболее частых причин использования технологии NAT является дефицит *реальных* глобальных IP-адресов. В этом случае для адресации узлов во внутренних сетях используются специально зарезервированные с этой целью *частные* (приватные) IP-адреса (подробнее см. RFC 1597). Чтобы узлы с частными IP-адресами могли связываться между собой через внешние (глобальные) сети или с узлами глобальных сетей, следует применять технологию NAT.

Использование технологии NAT также полезно, когда из соображений безопасности желательно скрыть IP-адреса узлов своей *внутренней* IP-сети, чтобы не дать возможности наблюдателю, находящемуся во *внешней* (глобальной) сети, составить представление о структуре и масштабах корпоративной IP-сети, а также о структуре и интенсивности исходящего и входящего трафиков отдельных узлов внутренней IP-сети.

Механизм NAT-обработки встроен в полный алгоритм работы маршрутизаторов изделия (см. раздел 3.5, с. 127) и стереотипно реализуется любым из блоков маршрутизации изделия – БНМ или БВМ – при обработке трафиков IP-пакетов, циркулирующих через их сетевые интерфейсы.

Тактика применения механизма NAT-обработки зависит от тех задач, которые администрация ЗСПД предполагает решать, планируя цели применения конкретного изделия.

> *Примечание.* Необходимо отметить, что фигурирующие в NAT-обработке понятия *внутренних* и *внешних* сетевых интерфейсов маршрутизатора, реализующего NAT-обработку, не следует смешивать с понятиями принадлежащих БВМ *внутренних* сетевых интерфейсов и принадлежащих БНМ *внешних* сетевых интерфейсов изделия.

Содержание механизма трансляции сетевых адресов NAT (Network Address Translator) составляет автоматическая (после соответствующей настройки) подмена IP-адресов (NAT-обработка) или номеров портов (NAT/PAT-обработка) в заголовках IP-датаграмм, проходящих через NAT-обработчик соответствующего блока маршрутизации изделия. Алгоритм подмены IP-адресов (или IP-адресов и номеров портов) зависит от направления движения IP-датаграммы и от выбранного администратором для применения в ЗСПД варианта NAT- или NAT/PAT-обработки, обеспечиваемого изделием:

- для исходящих IP-датаграмм NAT-обработчик заменяет IP-адрес отправителя (поле **Source Address** IP-заголовка);

- для входящих IP-датаграмм NAT-обработчик заменяет IP-адрес получателя (поле **Destination Address** IP-заголовка);
- для исходящих IP-датаграмм NAT/PAT-обработчик заменяет номер порта отправителя (поля **Source Address** и поля **Source Port** IP-заголовка);
- для входящих IP-датаграмм NAT/PAT-обработчик заменяет номер порта получателя (поля **Destination Address** и поля **Destination Port** IP-заголовка).

При решении своей основной задачи – подмены оригинального IP-адреса источника датаграммы – NAT-обработчик помогает решать и задачу оптимизации использования адресного пространства сети Internet, а также служит средством сокрытия структуры внутренних IP-сетей Пользователя и средством их защиты от несанкционированного доступа со стороны сетей общего пользования. Последнее обстоятельство позволяет отнести NAT-обработку к средствам защиты информации.

3.3.1. *Основы NAT-обработки*

Введем несколько определений, необходимых для дальнейшего изложения. Воспользуемся схемой, представленной на Рис. 3.29 (схема иллюстрирует работу одного из блоков маршрутизации изделия).

Реальное адресное пространство – множество IP-адресов, доступных для распределения между участниками IP-сети. Любой реальный IP-адрес используется в сети Internet или будет использоваться в ближайшем будущем.

Фиктивное адресное пространство – множество IP-адресов, которые не могут быть использованы в качестве реальных IP-адресов. Рекомендацией RFC 1597 в качестве фиктивных определены следующие блоки IP-адресов:

1 сеть класса A	10.0.0.0 - 10.255.255.255
16 сетей класса B	172.16.0.0 - 172.31.255.255
255 сетей класса C	192.168.0.0 - 192.168.255.255

Внутренняя сеть – защищаемая от внешнего воздействия IP-сеть Пользователя. Как правило, в случае применения NAT в качестве средства защиты информации внутренняя IP-сеть использует фиктивное адресное пространство.

Внутренний интерфейс – интерфейс (интерфейсы) маршрутизатора изделия, обслуживающий подключение к внутренней, с точки зрения NAT-обработки, IP-сети.

Внешняя сеть – совокупность внешних, с точки зрения NAT-обработки, внутренних IP-сетей Пользователя, каналов связи, маршрутизаторов и хостов. Внешняя сеть работает, как правило, в реальном пространстве IP-адресов. Именно в ней находятся необходимые абонентам внутренней IP-сети информационные ресурсы, а также рабочие станции злоумышленников, пытающихся проникнуть в защищаемые внутренние IP-сети.

Внешний интерфейс – интерфейс (интерфейсы) маршрутизатора изделия, обслуживающий подключение к внешней, с точки зрения NAT-обработки, IP-сети.

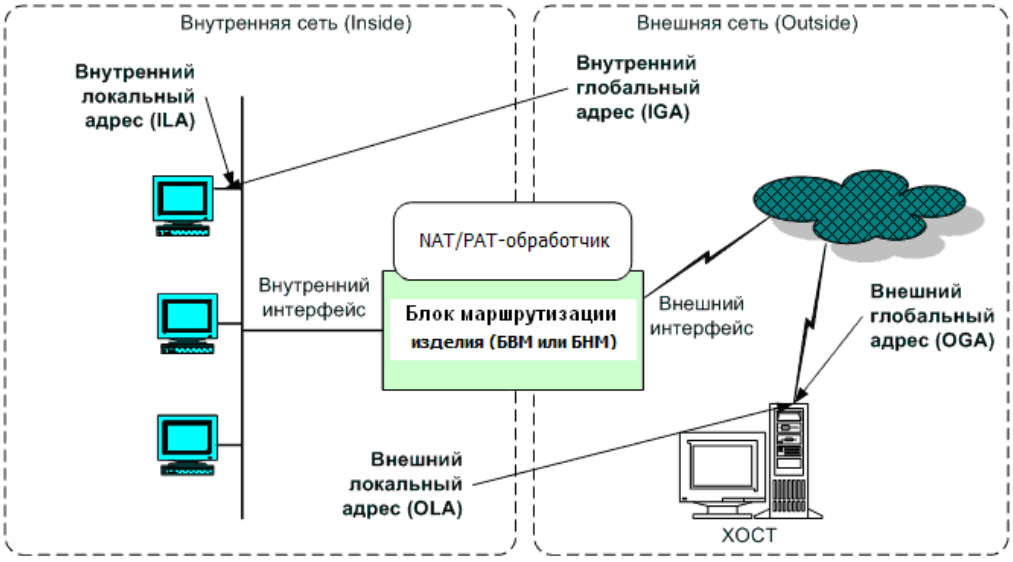


Рис. 3.29 Принципы работы механизма NAT/PAT-обработки, обеспечиваемой маршрутизатором

NAT-обработчик в маршрутизаторе отделяет внутреннюю (с точки зрения NAT/PAT-обработки) IP-сеть от внешней IP-сети. Внутренняя IP-сеть, как правило, работает в фиктивном адресном IP-пространстве.

В процессе своей работы NAT/PAT-обработчик транслирует значения IP-адресов (и, возможно, и значения портов) в заголовках IP-пакетов, обрабатываемых сетевыми интерфейсами маршрутизатора; при этом NAT-обработчик должен идентифицировать, какой интерфейс является внутренним, а какой – внешним.

В простейшем (базовом) варианте NAT-обработчик осуществляет трансляцию:

- IP-адресов интерфейсов внутренней IP-сети (фиктивных IP-адресов) в IP-адреса интерфейсов внешней IP-сети (реальные IP-адреса) – для исходящих IP-датаграмм;
- IP-адресов интерфейсов внешней IP-сети (реальных IP-адресов) в IP-адреса интерфейсов внутренней IP-сети (фиктивные IP-адреса) – для входящих IP-датаграмм.

С появлением NAT-обработчика у всех абонентов внутренней и внешней IP-сетей возникает по два IP-адреса: первый – IP-адрес абонента в своей IP-сети (внутренней или внешней); второй – IP-адрес абонента, видимый из другой IP-сети. Эти адреса могут совпадать, но могут быть и разными, поскольку NAT-обработчик изменяет IP-адреса в проходящих через него IP-датаграммах. Определим эти IP-адреса абонентов следующим образом.

> **Внутренний локальный адрес** (**ILA** – inside local address) – IP-адрес, присвоенный хосту или рабочей станции внутренней IP-сети Пользователя из фиктивного (не зарегистрированного) адресного IP-пространства.
>
> **Внутренний глобальный адрес** (**IGA** – inside global address) – реальный (зарегистрированный) IP-адрес, по которому может быть доступна станция или хост внутренней IP-сети из внешней IP-сети.
>
> **Внешний глобальный адрес** (**OGA** – outside global address) – реальный IP-адрес узла во внешней IP-сети, под которым владелец узла регистрирует его в сети Internet. Адрес выделяется из IP-пространства глобально маршрутизируемых IP-адресов или сетевых IP-адресов.
>
> **Внешний локальный адрес** (**OLA** – outside local address) – IP-адрес узла во внешней IP-сети; это IP-адрес узла назначения IP-датаграммы, по которому хост может быть вызван со станций внутренней IP-сети Пользователя; этот IP-адрес может совпадать с реальным IP-адресом узла, но может быть и фиктивным.

NAT-обработчик может использовать различные алгоритмы вычисления значений IP-адресов, подставляемых в поля заголовка IP-датаграммы вместо их исходных значений. Существует множество вариантов алгоритмов NAT-обработки.

Изделие обеспечивает поддержку двух вариантов алгоритмов NAT-обработки:

- NAT-обработка со статической таблицей;
- NAT-обработка с перегрузкой адреса.

Подробнее алгоритмы NAT-обработки рассмотрены в последующих подразделах настоящего РНУ. Здесь отметим только следующее: программа управления изделием, реализуя алгоритмы NAT-обработки, не выполняет преобразований **OLA ⇨ OGA** и **OGA ⇨ OLA** (**внешнего локального адреса** во **внешний глобальный адрес** и обратно). Это означает, что изделие обеспечивает доступ из внутренней (с точки зрения NAT/PAT-обработки) IP-сети только к узлам с реальными IP-адресами; NAT-обработчик при этом считает, что внешний локальный IP-адрес совпадает с внешним глобальным IP-адресом (**OLA = OGA**).

3.3.2. NAT-обработка со статической таблицей IP-адресов

Для *исходящих* IP-датаграмм IP-адрес отправителя IP-датаграммы подвергается преобразованию: **ILA ⇨ IGA** (**внутренний локальный адрес** преобразуется во **внутренний глобальный адрес**).

Для *входящих* IP-датаграмм IP-адрес получателя IP-датаграммы подвергается преобразованию **IGA ⇨ ILA** (**внутренний глобальный адрес** преобразуется во **внутренний локальный адрес**). NAT-обработка со статической таблицей обеспечивает взаимно-однозначное преобразование адресов, т. е. каждому **внутреннему локальному адресу** ставится в соответствие *один* **внутренний глобальный адрес**.

Алгоритм NAT-обработки со статической таблицей рассмотрим на примере схемы, представленной на Рис. 3.30 (схема иллюстрирует работу одного блока маршрутизации).

1. Рабочая станция с IP-адресом **192.168.1.2** должна установить соединение с хостом по IP-адресу **213.36.96.8**, для чего отправляет IP-датаграмму-запрос на установление соединения с ним.
2. При получении IP-датаграммы от рабочей станции соответствующий блок маршрутизации изделия извлекает из нее IP-адрес отправителя (**192.168.1.2**) и проверяет наличие в NAT-таблице записи с внутренним локальным IP-адресом, равным **192.168.1.2**. Если такой записи нет, то IP-датаграмма снимается с доставки.
3. Если запись найдена, то NAT-обработчик соответствующего блока маршрутизации заменяет в IP-адресе отправителя IP-датаграммы внутренний локальный IP-адрес соответствующим внутренним глобальным

IP-адресом и отправляет модифицированную IP-датаграмму во внешнюю сеть. В примере локальному IP-адресу **192.168.1.2** поставлен в соответствие внутренний глобальный IP-адрес **201.15.36.2**.

4. Получив IP-датаграмму, хост посылает ответ на нее по IP-адресу **201.15.36.2**.
5. При получении IP-датаграммы из внешней сети NAT-обработчик соответствующего блока маршрутизации извлекает из нее IP-адрес получателя (**201.15.36.2**) и проверяет наличие в NAT-таблице записи с внутренним глобальным IP-адресом, равным **201.15.36.2**. Если такой записи нет, то IP-датаграмма снимается с доставки.
6. Если запись найдена, то NAT-обработчик соответствующего блока маршрутизации заменяет в IP-адресе получателя IP-датаграммы внутренний глобальный IP-адрес соответствующим внутренним локальным IP-адресом и отправляет модифицированную IP-датаграмму во внутреннюю сеть. В примере глобальному IP-адресу **201.15.36.2** поставлен в соответствие внутренний локальный адрес **192.168.1.2**.
7. Рабочая станция с IP-адресом **192.168.1.2** получает ответ на свой запрос и продолжает дальнейшую работу.

Шаги 2 – 6 описанной процедуры выполняются для каждой IP-датаграммы.

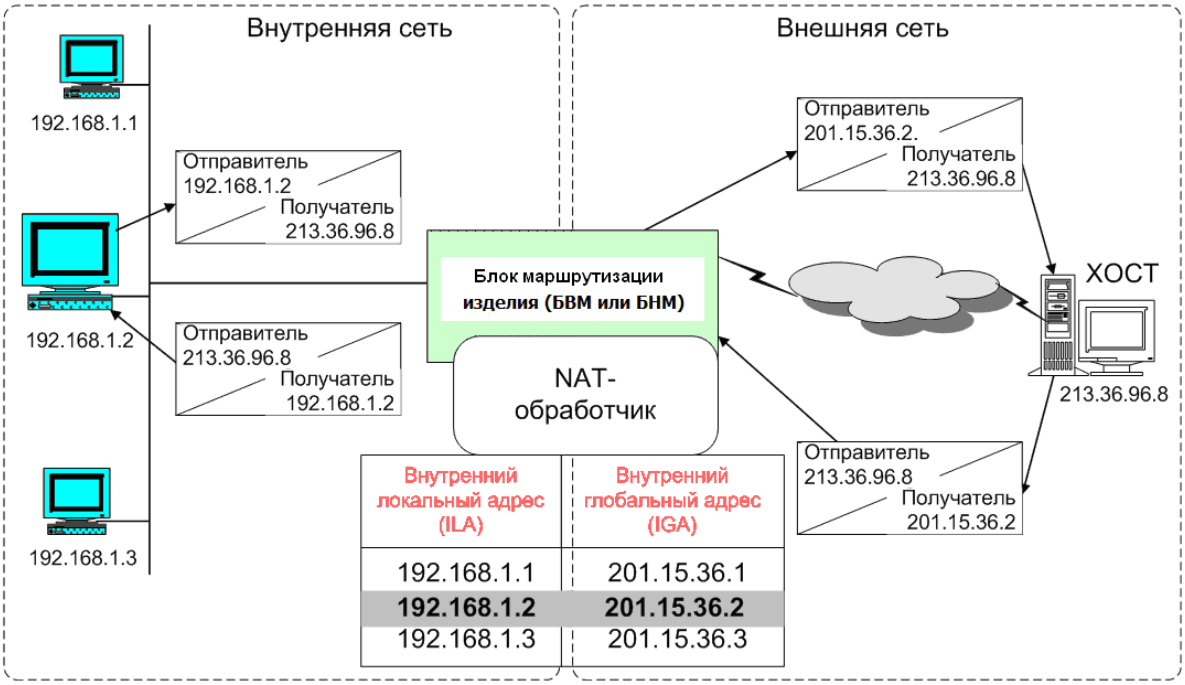


Рис. 3.30 Схема NAT-обработки со статической таблицей

При NAT-обработке со статической таблицей NAT-обработчик может дополнительно выполнять замену портов в заголовках IP-датаграмм (механизм PAT – Port Address Translator):

- для исходящих IP-датаграмм преобразуется порт отправителя IP-датаграммы (поле **Source Port** IP-заголовка);
- для входящих IP-датаграмм преобразуется порт получателя IP-датаграммы (поле **Destination Port** IP-заголовка).

Для того чтобы выполнялась трансляция портов (PAT-обработка), надо в записях статической таблицы в дополнение к IP-адресам ввести номера портов.

Преобразование портов выполняется по следующим правилам.

1. При получении IP-датаграммы от рабочей станции NAT-обработчик соответствующего блока маршрутизации извлекает из нее IP-адрес и номер порта отправителя и проверяет наличие в NAT-таблице записи с таким же значением номера порта и с внутренним локальным IP-адресом, совпадающим с IP-адресом отправителя.
2. Если запись найдена, то NAT-обработчик соответствующего блока маршрутизации заменяет значение порта отправителя в IP-датаграмме соответствующим значением из статической таблицы (если требуется, преобразует и IP-адрес в соответствии с записью таблицы) и отправляет модифицированную IP-датаграмму во внешнюю сеть.
3. При получении IP-датаграммы из внешней сети NAT-обработчик соответствующего блока маршрутизации извлекает из нее IP-адрес и номер порта получателя и проверяет наличие в NAT-таблице записи с таким же значением номера порта и с внутренним глобальным IP-адресом, совпадающим с IP-адресом получателя.

4. Если запись найдена, то NAT-обработчик соответствующего блока маршрутизации заменяет значение порта получателя в IP-датаграмме соответствующим значением из статической таблицы (если требуется, преобразует и IP-адрес в соответствии с записью таблицы) и отправляет модифицированную IP-датаграмму во внутреннюю сеть.

Отметим основные свойства NAT-обработки со статической таблицей.

1) Выполняется замена IP-адресов и/или портов в заголовках IP-датаграмм с использованием статической таблицы соответствия внутренних локальных (**внутренних**) адресов/портов внутренним глобальным (**внешним**) адресам/портам.

   Замечание. **Внутренними** и **внешними** обозначены соответственно внутренние локальные и внутренние глобальные IP-адреса и порты в статической таблице экрана настройки NAT-обработчика (см. Рис. 3.34, с. 118).

2) Статическая таблица устанавливает взаимно-однозначное соответствие **внутренних** и **внешних** IP-адресов всех входящих в таблицу станций внутренней сети. NAT-обработка со статической таблицей (без трансляции портов) никакой экономии адресного пространства IP-адресов не обеспечивает, так как *каждому* фиктивному IP-адресу необходимо поставить в соответствие реальный IP-адрес. Наличие PAT-обработки адресное пространство экономит. Кроме того, PAT-обработка обеспечивает маскировку стандартных сервисов, которые получают нестандартные номера портов.

3) Сформированная статическая таблица (в отличие от динамической, рассмотренной ниже) присутствует в соответствующих маршрутизаторах постоянно, следовательно, записи таблицы, устанавливающие правила преобразования **внутренних** адресов/портов во **внешние** и обратно, доступны NAT-обработчикам соответствующих маршрутизаторов постоянно. Это означает, что никаких защитных функций для указанных в таблице станций внутренней сети NAT-обработчик не выполняет, поскольку любая станция внешней сети может обратиться по реальному IP-адресу к станции внутренней сети и NAT-обработчик пропустит такое обращение.

4) Ко всем станциям, указанным в статической таблице, возможны обращения из внешней IP-сети, следовательно, эти станции можно использовать в качестве хостов для предоставления информационных услуг как абонентам внутренней IP-сети, так и абонентам внешней IP-сети. Причем, абоненты внутренней IP-сети должны вызывать эти хосты по их **внутренним** IP-адресам, а абоненты внешней сети – по **внешним** IP-адресам.

Учитывая рассмотренные свойства, можно сделать следующий вывод.

NAT-обработчик со статической таблицей нужно применять для расположенных во внутренней IP-сети информационных хостов, к которым необходим доступ из внешней IP-сети. NAT-обработчик не обеспечивает информационную безопасность этих хостов, поэтому для них обязательно надо предусмотреть использование других защитных функций изделия в первую очередь IP-фильтров (см. раздел 3.2, с. 89).

3.3.3. NAT-обработка с перегрузкой IP-адреса

Адрес перегрузки является внутренним глобальным IP-адресом (**IGA**), в который преобразуется множество внутренних локальных IP-адресов (**ILA**). Операция *перегрузки адреса* обеспечивает преобразование множества внутренних локальных IP-адресов в один внутренний глобальный IP-адрес и обратно.

Для *исходящих* IP-датаграмм IP-адрес отправителя датаграммы подвергается преобразованию **ILA ⇨ Адрес перегрузки** (внутренний локальный IP-адрес преобразуется в IP-адрес перегрузки). Для *входящих* IP-датаграмм IP-адрес получателя датаграммы подвергается преобразованию **Адрес перегрузки ⇨ ILA** (адрес перегрузки преобразуется во внутренний локальный IP-адрес).

Алгоритм перегрузки адреса NAT-обработчиком рассмотрим на примере схемы, представленной на Рис. 3.31.

1. Рабочая станция с адресом **192.168.1.2** должна установить соединение (например, по протоколу Telnet) с хостом по IP-адресу **213.36.96.8**, для чего отправляет IP-датаграмму-запрос на установление соединения с ним.

2. При получении IP-датаграммы от рабочей станции NAT-обработчик соответствующего маршрутизатора извлекает из нее IP-адрес отправителя (**192.168.1.2**), IP-адрес получателя (**213.36.96.8**), протокол (**TCP**), номер порта отправителя (**1726**) и номер порта получателя (**23**). Проверяется наличие в NAT-таблице записи, у которой протокол, внутренний локальный IP-адрес и номер порта, внешний глобальный IP-адрес и номер порта совпадают с данными IP-датаграммы. Если запись есть, то NAT-обработчик соответствующего маршрутизатора заменяет в IP-адресе отправителя IP-датаграммы внутренний локальный IP-адрес адресом перегрузки (**201.15.36.254**) и отправляет модифицированную IP-датаграмму во внешнюю сеть.

   Замечание. NAT-обработчик маршрутизатора, выполняя в исходящей IP-датаграмме замену внутреннего локального IP-адреса отправителя IP-адресом перегрузки, для устранения неоднозначности при работе разных станций внутренней сети с одним IP-адресом во внешней

сети автоматически меняет и номер порта отправителя. Вместо номера порта отправителя подставляет порядковый номер – число, начиная с **10001** до **20000**.

Наличие уникального номера порта решает проблемы с возможными конфликтами работы через NAT-обработчик с нескольких рабочих станций.

3. Если запись не найдена, то в рабочую NAT-таблицу помещается новая запись, у которой в столбец «Внутренний глобальный адрес и номер порта» заносится IP-адрес перегрузки (**201.15.36.254**) и номер порта отправителя (**1726**).
4. NAT-обработчик соответствующего маршрутизатора заменяет в IP-датаграмме IP-адрес отправителя со значения **192.168.1.2** на значение **201.15.36.254** и отправляет модифицированную IP-датаграмму во внешнюю сеть.
5. Получив IP-датаграмму, хост посылает ответ на нее по IP-адресу **201.15.36.254**.
6. При получении IP-датаграммы из внешней сети NAT-обработчик соответствующего маршрутизатора извлекает из нее IP-адрес отправителя (**213.36.96.8**), IP-адрес получателя (**201.15.36.254**), протокол (**TCP**) и номера портов отправителя (**23**) и получателя (**1726**). Проверяется наличие в NAT-таблице записи, у которой протокол, внешний глобальный IP-адрес с номером порта и внутренний глобальный IP-адрес с номером порта совпадают с данными IP-датаграммы. Если искомой записи нет, то IP-датаграмма без всяких преобразовании пропускается на дальнейшую обработку (на маршрутизацию).
7. Если запись найдена, то из нее извлекается внутренний локальный IP-адрес (**192.168.1.2**), NAT-обработчик соответствующего маршрутизатора заменяет в IP-датаграмме IP-адрес получателя со значения **201.15.36.254** на значение **192.168.1.2** и отправляет модифицированную IP-датаграмму во внутреннюю сеть.
8. Рабочая станция с IP-адресом **192.168.1.2** получает ответ на свой запрос и продолжает дальнейшую работу.

Шаги 2-6 описанной процедуры выполняются для каждой IP-датаграммы.

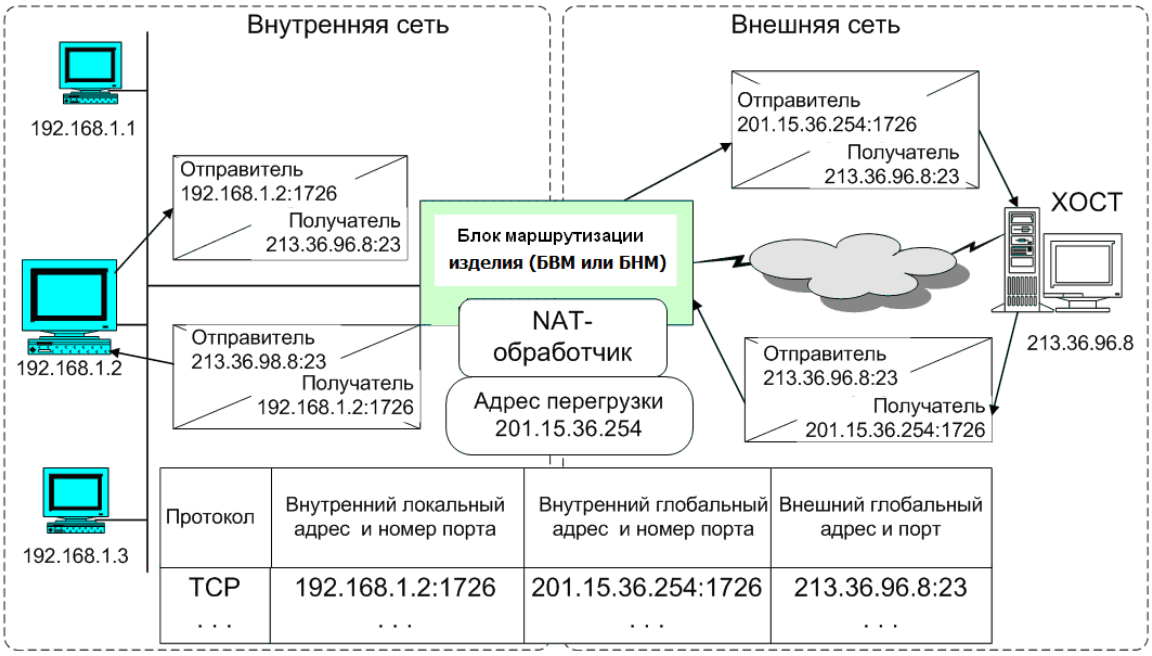


Рис. 3.31 Схема NAT-обработки с перегрузкой IP-адреса

Отметим основные свойства NAT-обработки с перегрузкой IP-адреса.

1. Выполняется динамическая замена IP-адресов отправителей (станций внутренней сети) на IP-адрес перегрузки и обратная замена IP-адреса перегрузки на IP-адреса получателей (станций внутренней сети). Все станции внутренней сети работают с внешней сетью, используя единственный реальный IP-адрес – IP-адрес перегрузки. В результате обеспечивается существенная экономия адресного IP-пространства сети Internet.
2. Реализуется защита доступа к станциям внутренней сети из внешней, поскольку записи в рабочей NAT-таблице создаются только по запросам из внутренней сети и немедленно удаляются по окончании сеанса связи станции внутренней сети с хостом внешней сети.

Замечание. Для защиты от злоумышленников доступ из внешней сети по фиктивным адресам внутренней сети должен быть блокирован с помощью IP-фильтров (см. раздел 3.2, с. 89).

Учитывая рассмотренные свойства, можно сделать следующий вывод: NAT-обработчик с перегрузкой IP-адреса следует применять для защиты рабочих станций внутренней сети от внешнего воздействия.

Для информационных хостов, расположенных во внутренней сети и требующих доступа из внешней сети, NAT-обработчик с перегрузкой IP-адреса не пригоден (он полностью блокирует доступ из внешней сети во внутреннюю). Для этих хостов необходимо использовать NAT-обработчик со статической таблицей.

3.3.4. *Полный алгоритм NAT-обработки*

При прохождении IP-датаграмм через NAT-обработчик соответствующего маршрутизатора NAT-обработке подвергаются только те из них, которые соответствуют записям NAT-таблиц, статической или динамической.

> *Примечание.* Напомним, что статическая таблица присутствует постоянно в неизменном виде. Записи в динамическую таблицу заносятся по инициативе абонентов, работающих по внутренним интерфейсам NAT-обработчика; эти записи автоматически удаляются из таблицы по окончании сессии работы абонента.

Если на интерфейс изделия приходит IP-датаграмма, то для нее ведется поиск соответствующей записи в статической и динамической NAT-таблицах. Если запись найдена (вне зависимости от того, в какой таблице), то делается NAT-преобразование и IP-датаграмма отправляется дальше.

Если записи нет и IP-датаграмма пришла из внутреннего интерфейса NAT-обработчика, то образуется новая запись в динамической таблице, IP-датаграмма преобразуется и отправляется дальше. Если IP-датаграмма пришла не из внутреннего интерфейса NAT-обработчика, то она без всяких преобразований пропускается на дальнейшую обработку (на маршрутизацию).

3.3.5. *Настройка NAT-обработчика*

Для того чтобы обеспечить выполнение рассмотренных выше операций, NAT/PAT-обработчик должен быть предварительно настроен.

Настройку NAT-обработчика будем рассматривать на примере схемы, представленной на Рис. 3.32.

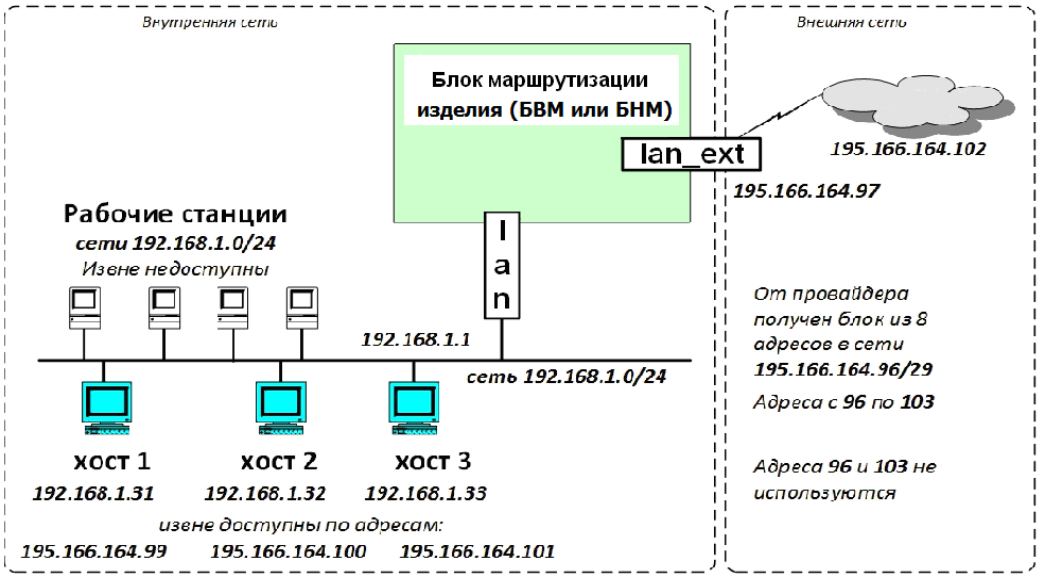


Рис. 3.32 Пример схемы, поясняющей процесс настройки NAT/PAT-обработчика

В процессе подготовки NAT/PAT-обработчика к функционированию следует выполнить следующие шаги по настройке изделия:

1. Указать предназначенный для обслуживания внутренней (в смысле NAT/PAT-обработки) IP-сети интерфейс как *внутренний*, а предназначенный для обслуживания внешней (в смысле NAT/PAT-обработки) IP-сети интерфейс указать как *внешний*.
2. Указать значение IP-адреса перегрузки.
3. Сформировать статическую NAT/PAT-таблицу.

Чтобы выполнить *первый шаг* настройки (отметить внутренние и внешние интерфейсы для NAT/PAT-обработки), следует выбрать цепочку альтернатив~~у~~ ГМ: **Настройка ⇨ Интерфейсы**.

В ответ на видеомонитор ЛКУ будет выдан экран создания и настройки сетевых интерфейсов изделия, аналогичный представленному на Рис. 3.33. На этом экране *внутренние* (в смысле NAT/PAT-обработки) интерфейсы отмечены *красным* цветом, внешние – *зеленым*. Интерфейсы, для которых NAT/PAT-обработка отключена, – *черным*. Чтобы изменить статус NAT/PAT-обработки для интерфейса, следует перевести курсор на строку описания соответствующего интерфейса и нажать клавишу <F2> необходимое число раз.

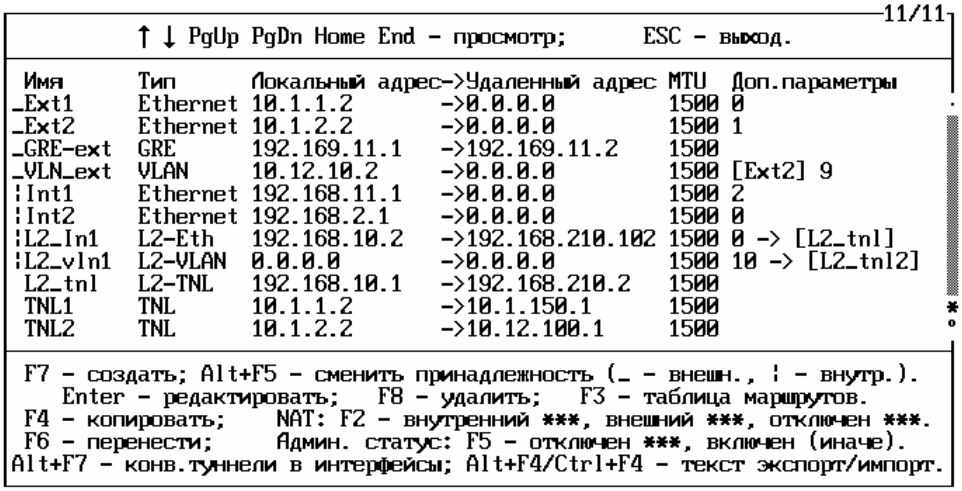


Рис. 3.33 Экран создания и настройки сетевых интерфейсов изделия

Для выполнения *второго* и *третьего* шагов процесса настройки (соответственно задать IP-адрес перегрузки и создать статическую NAT/PAT-таблицу) следует выбрать цепочку альтернатив ГМ: **Настройка ⇨ Защита ⇨ NAT/PAT-параметры**.

В ответ на видеомонитор ЛКУ будет выдан экран настройки NAT/PAT-обработчика соответствующего маршрутизатора изделия, аналогичный представленному на Рис. 3.34.

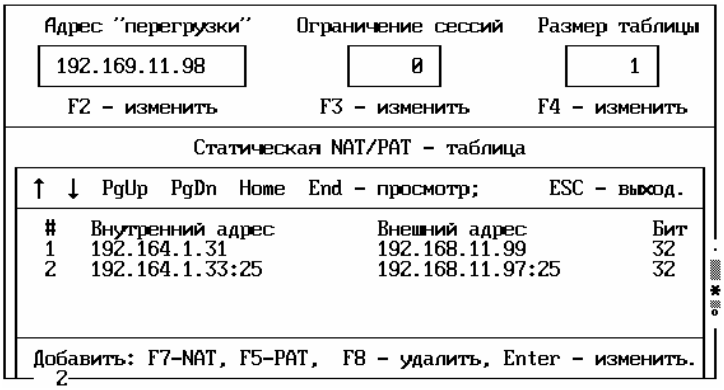


Рис. 3.34 Экран настройки основных параметров NAT/PAT-обработчика маршрутизатора изделия

Адрес "перегрузки" (Рис. 3.34). При нажатии клавиши <F2> на видеомонитор ЛКУ выдается представленное на Рис. 3.35 меню управления с тремя возможными значениями, позволяющее выбрать режимы работы программы управления с параметром **Адрес перегрузки**. Чтобы установить требуемый режим, надо установить курсор на соответствующую альтернативу и нажать клавишу <Enter>.

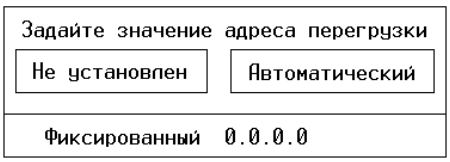


Рис. 3.35 Меню выбора режима работы программы управления с параметром **Адрес перегрузки**

Выбор того или иного режима работы с параметром **Адрес перегрузки** означает следующее:

Не установлен – NAT/PAT-обработчик не будет работать с адресом перегрузки.

Автоматический – в качестве адреса перегрузки будет использован локальный IP-адрес *внешнего* (в смысле NAT/PAT-обработки) интерфейса. Если внешних интерфейсов несколько, то NAT/PAT-обработчик будет подставлять в качестве адреса перегрузки локальный IP-адрес того интерфейса, по которому будет выполняться доставка конкретной IP-датаграммы во внешнюю сеть.

Фиксированный – адресом перегрузки будет заданное этим полем значение IP-адреса.

Ограничение сессий (Рис. 3.34). Параметр позволяет ограничить количество NAT-сессий (записей в динамической NAT-таблице), которые могут быть установлены с одной рабочей станции. Умалчиваемое значение параметра – *0*, при этом ограничений на количество NAT-сессий нет. Изменить значение порога ограничения можно с помощью клавиши <F3>: после нажатия клавиши программа управления выдаст запрос, в ответ на который следует ввести требуемое число и нажать клавишу <Enter>.

Размер таблицы (Рис. 3.34). Параметр задает размер оперативной памяти в блоках (страницах), выделяемой под NAT-таблицу. Один блок содержит 2048 записей. Умалчиваемое значение параметра – ***1***. Если требуется больший размер, следует нажать клавишу <F4>, в поле появившегося запроса ввести требуемое значение нового размера NAT-таблицы, после чего нажать клавишу <Enter>.

Статическая NAT/PAT-таблица (Рис. 3.34). Нижнее поле экрана настройки NAT/PAT-обработчика содержит строки с ранее созданными записями NAT/PAT-таблицы или это поле еще не заполнено. Для создания новой записи таблицы служат клавиши <F7> и <F5>.

Добавить:F7-NAT (Рис. 3.34). При нажатии клавиши <F7> будет предложено задать внутренний и внешний IP-адреса с указанием числа значащих в адресе бит (длины маски).

Добавить:F5-PAT (Рис. 3.34). При нажатии клавиши <F5> будет предложено задать внутренний и внешний IP-адреса с указанием числа бит и значений портов.

На Рис. 3.36 представлены примеры меню настроек записей NAT/PAT статической NAT/PAT-таблицы.

F7 - NAT

Внутренний адрес	192.164.1.31
Внешний адрес	192.168.11.99
Значащих бит	32

F5 - PAT

Внутренний адрес	192.164.1.33	порт 25
Внешний адрес	192.168.11.97	порт 25
Значащих бит	32	

Рис. 3.36 Примеры меню настроек записей NAT или PAT статической NAT/PAT-таблицы

Enter – изменить (Рис. 3.34). При нажатии клавиши <Enter> на видеомонитор ЛКУ выдается меню настройки той записи статической NAT/PAT-таблицы, на строку описателя которой был установлен курсор.

F8 – удалить (Рис. 3.34). Нажатие клавиши <F8> вызывает удаление той записи статической NAT/PAT-таблицы, на строку описателя которой был установлен курсор.

3.3.6. Пример использования NAT-обработчика

Рассмотрим, как с помощью NAT-обработки можно обеспечить обмен данными между одной локальной сетью (внутренней) и другой локальной сетью – внешней (см. схему на Рис. 3.32, с. 117).

Пусть внутренняя локальная сеть организации объединяет три узла и несколько рабочих станций.

Провайдером во внешней сети для организации выделена подсеть на восемь IP-адресов **195.166.164.96/29** (маска **255.255.255.248** – т.е. **29** значащих бит). В соответствии с правилами маршрутизации для нужд организации в этом случае могут быть использованы шесть IP-адресов: с IP-адреса **195.166.164.97** по IP-адрес **195.166.164.102** включительно.

Из этих шести выделенных для организации работы сети IP-адресов:

- два используются на линии с провайдером: интерфейс **lan_ext**, локальный IP-адрес интерфейса – **195.166.164.97**, IP-адрес шлюза провайдера – **195.166.164.102**;
- один IP-адрес резервируется под адрес перегрузки – **195.166.164.98**;
- три оставшихся IP-адреса из реального пространства IP-адресов (**195.166.164.99** – **195.166.164.101**) отданы трем узлам, находящимся в локальной сети.

В результате к узлам можно прислать вызов из внешней сети. Рабочие станции используют IP-адрес перегрузки. Они не могут быть вызваны из внешней сети, они могут только вызывать сами и получить ответ на вызов.

Все рабочие станции организации будут использовать внутренние (фиктивные) IP-адреса сети **192.168.1.0/24**.

Для реализации работы изделия согласно указанной схеме (см. Рис. 3.32, с. 117).необходимо выполнить следующие действия на соответствующем маршрутизаторе изделия.

1. Создать интерфейсы (выбором цепочки альтернатив ГМ: **Настройка ⇨ Интерфейсы ⇨ F7 - создать**). В полученном списке описателей интерфейсов (см. Рис. 3.33, с. 118 или Рис. 2.1, с. 22) отметить интерфейс **lan_ext** как «NAT-внешний» (*зеленый* цвет на экране), а интерфейс **lan** – как «NAT-внутренний» (*красный* цвет).

2. Заполнить таблицу NAT-параметров, выбрав цепочку альтернатив ГМ: **Настройка ⇨ Защита ⇨ NAT/PAT-параметры** (см. Рис. 3.34, с. 118).

3. Записать выполненные изменения параметров в **БпО** и перезапустить изделие.

После выполнения указанных действий NAT-обработчик соответствующего маршрутизатора обеспечит следующий режим работы.

Из внешней сети маршрутизатор будет доступен по IP-адресу **195.166.164.97**. Из внутренней сети маршрутизатор будет доступен по IP-адресу **192.168.1.1**.

Хосты внутренней сети с IP-адресами **192.168.1.31**, **192.168.1.32**, **192.168.1.33** будут доступны из внешней сети (и сами смогут выходить во внешнюю сеть) под IP-адресами **195.166.164.99**, **195.166.164.100**, **195.166.164.101** соответственно.

Остальные рабочие станции локальной сети **192.168.1.0/24** смогут выходить во внешнюю сеть, при этом для них NAT-обработчик соответствующего маршрутизатора будет подставлять в качестве адреса отправителя IP-адрес **195.166.164.98**. Послать вызов на эти станции из внешней сети нельзя.

Датаграммы из внешней сети, пришедшие на IP-адрес **195.166.164.97** и на порт **25** (SMTP), будут перенаправляться на сервер с IP-адресом **192.168.1.33** в соответствии с NAT/PAT-таблицей (см. Рис. 3.34, с. 118). Адрес **195.166.164.97** в нашем примере является адресом изделия, поэтому из всех IP-датаграмм, пришедших на этот IP-адрес, только IP-датаграммы, пришедшие на порт 25, будут для изделия транзитными и будут переданы на другой сервер, остальные будут обрабатываться самим изделием.

> *Замечание*. В рассмотренном примере (Рис. 3.32, с. 117) в качестве адреса перегрузки можно было использовать локальный IP-адрес внешнего интерфейса **195.166.164.97**. Значение адреса перегрузки, отличного от локального адреса внешнего интерфейса, необходимо только для целей трассировки, чтобы можно было отделить поток датаграмм для станций внутренней сети от потока датаграмм к собственным сервисам соответствующего маршрутизатора изделия.

3.3.7. *Оперативный контроль и управление состоянием NAT-обработчика*

В процессе работы обслуживающий персонал изделия может отслеживать текущее состояние NAT/PAT-обработчика любого из маршрутизаторов (БВМ или БНМ) и выполнять отдельные операции с целью анализа функционирования NAT/PAT-обработки. Для этих целей следует выбрать цепочку альтернатив ГМ: **Диагностика ⇨ NAT**. Полученное в ответ меню выбора режима визуального контроля NAT/PAT-обработки (Рис. 3.37) содержит две альтернативы – **Конфигурация** и **Рабочая таблица**.

Конфигурация
Рабочая таблица

Рис. 3.37 Меню выбора режима визуального контроля NAT/PAT-обработки

Конфигурация (Рис. 3.37). Выбор альтернативы позволяет просмотреть параметры настройки NAT/PAT-обработчика соответствующего маршрутизатора. Выбор альтернативы приводит к выводу на видеомонитор ЛКУ экрана настройки этого NAT-обработчика (см. Рис. 3.34, с. 118).

Рабочая таблица (Рис. 3.37). Альтернатива служит для просмотра текущего состояния динамической NAT/PAT-таблицы соответствующего маршрутизатора. Выбор альтернативы приводит к выводу на видеомонитор ЛКУ экрана текущего состояния динамической NAT/PAT-таблицы маршрутизатора, аналогичного представленному на Рис. 3.38.

Средняя часть экрана текущего состояния динамической NAT/PAT-таблицы маршрутизатора представляет собой динамически изменяемую таблицу, заполненную текущими записями. Параметры записей, регистрируемых в NAT/PAT-таблице, заносятся в колонки таблицы, описание которых приведено ниже:

T	–	*время жизни записи в секундах.* При создании записи в рабочей NAT-таблице поле **T** получает исходное значение, зависящее от протокола (услуги): **1800** – протокол **TCP**; **180** – протокол **UDP**; **60** – услуга **DNS** (**UDP** по порту **53**). Исходное значение уменьшается на единицу каждую секунду. При достижении нуля запись из таблицы удаляется. Пока запись существует, при каждом ее использовании в поле **T** восстанавливается исходное значение. При завершении TCP-соединений (после получения пакетов **FIN** или **RST**) поле **T** получает значение **30**.

Прот	–	*номер протокола:* **0** – поле не используется; **1** – **ICMP**; **4** – **TNL**; **6** – **TCP**; **17** – **UDP**.
Фл	–	*флаги состояния записи:* **00** – запись образуется в соответствии с алгоритмом перегрузки адреса; **80** – запись заменяет предыдущую для завершающегося TCP-соединения (получен пакет **FIN** или **RST**);
Внутренний локальный	–	*внутренний локальный адрес и номер порта*.
Внутренний глобальн.	–	*внутренний глобальный адрес и номер порта*.
Внешний глобальный	–	*внешний глобальный адрес и номер порта*.

```
Стр. 176. 130
↑ ↓ PgUp PgDn Home End - просмотр; ESC - выход; Tab ShiftTab - смена страницы.

T    Прот Фл Внутренний локальный  Внутренний глобальный Внешний глобальный
1544    6 00 192.168.32.65:1575    192.168.0.4:10013     84.0.226.178:11990
1545    6 00 192.168.32.73:1198    192.168.0.4:10021     88.212.196.66:80
1799    6 00 192.168.16.101:4380   192.168.0.4:10022     217.106.229.196:80
1545    6 00 192.168.16.101:4381   192.168.0.4:10023     217.106.229.196:80
1539    6 00 192.168.16.101:4378   192.168.0.4:10178     217.106.229.196:80
1539    6 00 192.168.16.101:4379   192.168.0.4:10179     217.106.229.196:80
1732    6 00 192.168.32.93:2745    192.168.0.4:10219     205.188.13.44:5190
1541    6 00 192.168.48.37:2845    192.168.0.4:10240     83.216.234.4:11475
1541    6 00 192.168.48.37:2857    192.168.0.4:10253     213.67.144.93:50334
1777    6 00 192.168.48.37:2858    192.168.0.4:10254     81.236.201.110:25452
1737    6 00 192.168.48.83:2327    192.168.0.4:10337     205.188.7.236:5190
1554    6 00 192.168.16.101:4382   192.168.0.4:10338     217.106.229.196:80
1562    6 00 192.168.32.94:2180    192.168.0.4:10434     64.12.30.72:5190

  Enter - параметры;  F8 - сбросить;  F3 - окно счетчиков;  F6 - распечатать.
Всего 355
```

Рис. 3.38 Экран текущего состояния динамической NAT/PAT-таблицы маршрутизатора

Enter – параметры (Рис. 3.38). При установке курсора на интересующую строку записи в общей NAT/PAT-таблице и нажатии клавиши <Enter> на экран выводится представленная ниже информация о параметрах этой записи – та же, что и в общей NAT/PAT-таблице, но в более развернутом формате (Рис. 3.39) и дополнительно – значение внешнего локального адреса (и номера порта).

```
Внутренние адреса:                    Внешние адреса:
локальный  192.168.32.65:1575         локальный  84.0.226.178:11990
глобальный 192.168.0.4:10013          глобальный 84.0.226.178:11990

Протокол    6          Время жизни 1355              Флаги 00
```

Рис. 3.39 Развернутый формат представления параметров записей NAT/PAT-таблицы

F8 – сбросить (Рис. 3.38). При установке курсора на интересующую строку записи в общей NAT/PAT-таблице и нажатии клавиши <F8> указанная курсором строка будет вычеркнута из NAT/PAT-таблицы до следующего события трансляции IP-адресов (портов).

```
Стр. ####   Стр. ####   Стр. ####   Стр. ####
   1  189
   2   36
   3   54
   4  156
   5   47
   6   35

Достигнутый максимум записей     645
Превышений размера страницы      0
Превышений ограничений абонентов 81
Ошибок 0          0
```

Рис. 3.40 Сведения о текущих технических характеристиках при работе с NAT/PAT-таблицей

F3 – окно счетчиков (Рис. 3.38). При нажатии клавиши <F3> на видеомонитор ЛКУ выводится (см. Рис. 3.40) список страниц (блоков памяти), выделенных под NAT-таблицу (см. раздел 3.3.5, с. 117), текущее количество записей трансляции на каждой странице и прочие технические характеристики, полезные для анализа работы изделия как обслуживающему персоналу изделия, так и его разработчику.

F6 – распечатать (Рис. 3.38). При нажатии клавиши <F6> выдаваемые на видеомонитор ЛКУ сведения о текущем состоянии NAT/PAT-таблицы будут перезаписаны в журнал изделия для последующего отложенного анализа работы изделия.

3.4. Групповая замена ключевых документов

Поддержка функционирования ЗСПД (всех ее звеньев, включая изделия защиты) в высокой степени готовности зависит от успешного решения Администрацией ЗСПД ряда задач.

Одной из этих задач является обеспечение *синхронной* в масштабе ЗСПД замены ключевых документов (КД), используемых работающими в сети криптотуннелями; замена выполняется периодически на всех изделиях защиты в регулируемые Администрацией ЗСПД сжатые сроки.

3.4.1. Общие сведения

Для обеспечения защиты трафика, передаваемого через сети общего пользования, следует на этапе подготовки изделий криптозащиты к совместной работе в составе ЗСПД создать и настроить на каждом из этих изделий те *виды* криптотуннелей и то их *количество*, которые обеспечат необходимую *функциональность ЗСПД в целом* – необходимую топологию сети, связь субъектов обмена в ней, защищенный обмен между ее различными криптозонами, реализацию функций удаленного управления изделиями защиты, повышенную надежность их работы, резервирование защищенных трактов передачи данных и пр.

Для обеспечения функционирования криптотуннелей необходимо на этапе подготовки конкретного изделия к работе выполнить *загрузку* в него ключевых документов, определенных Администрацией ЗСПД. Соответствующие ключевые документы должны быть загружены и во все *удаленные* изделия ЗСПД, с которыми *локальному* изделию предстоит обмениваться защищаемыми данными (по криптотуннелям). Это одно из основных требований, без выполнения которого нормальное функционирование ЗСПД невозможно.

Срок действия, в течение которого изделия защиты в составе ЗСПД могут использовать ключевые документы одной *серии* (с одним и тем же значением криптопараметра **номер серии ключей**), ограничен. Для обеспечения функционирования ЗСПД после срока, в течение которого разрешено использовать КД одной серии, необходимо до окончания срока действия КД выполнить процедуру перехода всех изделий ЗСПД на работу с ключевыми документами другой серии – только в этом случае будет обеспечена *информационно-криптографическая совместимость* при обмене по криптотуннелям между изделиями защиты в сети.

Замена КД на локальном и удаленном изделиях защиты должна быть выполнена одновременно (синхронно). В противном случае защищенный обмен по криптотуннелю, установленному между этими изделиями защиты, станет невозможным, и функционирование ЗСПД на данном направлении обмена нарушится. Для сохранения работоспособности ЗСПД в целом это требование должно быть соблюдено для всех существующих криптотуннелей (направлений защищенного обмена) сети. От степени синхронности выполнения требуемой процедуры перехода на работу с КД новой серии зависит период времени, в течение которого функционирование ЗСПД нарушается из-за отсутствия информационно-криптографической совместимости.

Очевидно, что время перехода ЗСПД на работу с КД новой серии следует сокращать. С этой целью в изделиях защиты нового поколения реализован механизм *автоматической замены ключевых документов* в соответствии с графиком их замены, определяемым Администрацией ЗСПД.

3.4.2. Принципы работы механизма замены ключевых документов по графику

Особенности работы ЗСПД при групповой замене КД. При настройке любого из возможных криптотуннелей должно быть указано значение криптопараметра **Номер серии ключей** (см. раздел 3.1.1.2, Рис. 3.8, с. 80 или раздел 2.4.2, Рис. 2.24, с. 40).

При эксплуатации ранее выпускавшихся изделий защиты при настройке криптотуннеля в качестве значения параметра **Номер серии ключей** должно быть указано *реальное* (действительное) значение *номера серии* КД, подлежащего загрузке в изделие. Как следствие, когда возникает необходимость перевода работы ЗСПД на использование КД с новым номером серии, приходится на всех изделиях защиты в настройках всех криптотуннелей изменить значение параметра **Номер серии ключей** с предыдущего на последующее, выполнив по возможности *синхронно* с этим соответствующую замену загруженных в изделие ключевых документов.

> *Примечание.* Процедура замены хранящихся в изделии КД (выполняемая согласно РЭ на конкретное изделие) предполагает удаление из изделия (во избежание недоразумений) отработавшего свой срок КД предыдущей серии и загрузку КД последующей серии для работы изделия в течение предстоящего периода действия нового КД. При этом в течение времени выполнения операций перезагрузки КД защищенный обмен по криптотуннелям на направлениях обмена, поддерживаемых данным изделием защиты, будет нарушен.

Изменение настроек криптотуннелей с заменой номера серии КД (в масштабе ЗСПД на тех узлах, которые затрагивает замена номера серии КД) персонал ЗСПД должен выполнить *вручную* и в *сжатые* строки, поэтому решение этой задачи выливается в проблему. С учетом того, что перевод ЗСПД на функционирование с КД новой серии осуществляется регулярно, становится ясно, что указанный метод замены КД трудоемок, вносит существенную напряженность в работу персонала ЗСПД в периоды переходов на работу с новыми КД и может вызывать временные нарушения в работе ЗСПД на отдельных направлениях обмена.

Неразрешимой проблемой становится выполнение перенастройки криптотуннелей на изделиях, функционирующих в составе *необслуживаемых* технических комплексов, когда доступ персонала к изделиям защиты невозможен физически – например, когда изделия функционируют в составе космической аппаратуры, автономных систем мониторинга морского или наземного базирования и т.д. При использовании применявшейся ранее технологии перехода ЗСПД на работу с КД новой серии по истечении допустимого срока действия КД, загруженного при запуске изделия, обмен с необслуживаемыми комплексами будет прекращен.

Поэтому (*в дополнение* к используемой ранее технологии перехода ЗСПД на работу с новыми КД) изделия защиты нового поколения поддерживают механизм *автоматической замены* ключевых документов и автоматического перехода ЗСПД на работу с КД новой серии в соответствии с графиком, заранее составляемым администратором изделия; исходные данные для составления графика администратор изделия получает от Администрации ЗСПД. При настройке криптотуннелей должны быть учтены дополнительные требования и, кроме того, предварительно должна быть выполнена загрузка в изделие ключевых документов всех серий, предусмотренных графиком их замены (пояснения см. ниже).

Основные принципы работы механизма автоматической замены КД. Ниже изложены *основные принципы*, положенные в основу работы механизма замены КД по графику.

1. В изделии обеспечивается загрузка и хранение ключевых документов одновременно *нескольких* серий (подробнее см. ЭД на конкретное изделие и документ «Правила пользования»).
2. При настройке всех криптотуннелей ЗСПД в качестве значения параметра **Номер серии ключей** используется не реальное значение номера серии КД, а условное числовое значение в *таблице-графике*, обозначающее идентификатор номера серии КД, отнесенный к работе данного криптотуннеля.
3. Таблица-график (пример на Рис. 3.41) содержит всю информацию, необходимую для работы механизма автоматической замены КД по графику. Записи таблицы определяют соответствие между идентификатором номера серии КД и реальным значением параметра **Номер серии ключей** для ключевого документа, который должен быть в определенный период времени использован для функционирования криптотуннеля. В составе таблицы-графика могут присутствовать записи двух видов:
   - *статические* – содержащие сведения о соответствии между идентификатором и реальным значением номера серии КД, но не содержащие сведений о дате и времени наступления события очередной замены КД; записи этого вида появляются в таблице-графике в случае, когда при создании записи (см. раздел 3.4.3, с. 125) поля параметров **Дата** и **Время** бланка создания и настройки записей графика замены ключей (см. Рис. 3.43, с. 126) остаются не заполненными;
   - *динамические* – содержащие сведения о соответствии между идентификатором и реальным значением номера серии КД, а также сведения о дате и времени наступления события очередной замены КД.
4. На этапе подготовки к работе в изделие загружаются КД нескольких серий. Ключи одной из серий планируется применить немедленно, а остальные − в перспективе согласно запланированному графику замены КД. По исходным данным Администрации ЗСПД выполняется настройка изделия, включающая:
   - настройку криптотуннелей изделия с использованием идентификаторов номеров серий КД, обеспечивающих работу криптотуннелей;
   - настройку таблицы-графика, включающей статические и/или динамические записи, содержащие информацию о соответствии идентификаторов реальным значениям параметра **Номер серии ключей** для каждого из криптотуннелей изделия.
5. На этапе штатной работы изделия программа управления автоматически обеспечивает работу механизма замены КД по графику, интерпретируя сведения, подготовленные администратором изделия в виде таблицы-графика.

   Примечание. Администратор изделия может использовать как существовавшую ранее и по-прежнему действующую технологию замены КД *вручную*, так и воспользоваться появившимися в новых изделиях средствами автоматической замены КД по графику.

Организация работы изделия в режиме автозамены КД. Рассмотрим подробнее те действия, которые должны выполнить администраторы (во взаимодействии с Администрацией ЗСПД) на этапе подготовки изделий защиты к функционированию в режиме автозамены КД в масштабе всей ЗСПД, а также остановимся на вопросах работы программ управления изделий.

На этапе подготовки администратор изделия должен, взаимодействуя с Администрацией ЗСПД, составить представление о всех *криптотуннелях*, с которыми придется работать изделию в течение всего предстоящего периода эксплуатации, а также о *реальных* номерах серий КД, с помощью которых в предстоящий период будет периодически (в режиме автозамены) обеспечиваться работа всех запланированных криптотуннелей.

Получив эту информацию, администратор может приступать к составлению списка *идентификаторов* номеров серий КД и таблиц-графиков соответствия каждого *идентификатора* номера серии (отнесенного к конкретному поддерживаемому изделием *криптотуннелю*) *реальному номеру* серии КД в конкретный *период* действия КД.

Криптотуннель	**Идентификатор номера серии КД**	**Номер серии КД**	**Начало периода действия КД (дата – время)**
TNL_1	1	287	–
	1	362	01.04.2017 – 00:00
	1	390	01.07.2017 – 00:00
	…	…	…
	1	400	01.04.2018 – 00:00
TNL_2	2	412	–
	2	812	01.04.2017 – 00:00
	2	890	01.07.2017 – 00:00
	…	…	…
	2	900	01.04.2018 – 00:00

Рис. 3.41 Пример таблицы-графика для настройки режима автозамены КД по графику

Рассмотрим простой *пример*. Пусть требуется подготовить к работе в предстоящий период изделие, которое должно поддерживать обмен по *двум* криптотуннелям – TNL_1 и TNL_2. Известны реальные номера серий КД и для каждого из криптотуннелей согласованная с Администрацией ЗСПД *очередность* использования КД для каждого периода работы изделия между моментами автозамены КД, известны также *моменты времени* (очередность *дат* и *времен*), в которые должна происходить автозамена очередных КД в ЗСПД. Пусть начало работы изделия запланировано на *январь* 2017 года.

Обладая этими данными, согласованными с Администрацией ЗСПД, администратор изделия может составить представленную на Рис. 3.41 таблицу, необходимую для выполнения настройки режима автозамены КД.

> При настройке криптотуннелей TNL_1 и TNL_2 в качестве значения параметра **Номер серии ключей** (см. раздел 3.1.1.2, Рис. 3.8, с. 80 или раздел 2.4.2, Рис. 2.24, с. 40) для TNL_1 должно быть указано значение идентификатора номера серии КД, равное *1*, а для TNL_2 указано значение идентификатора номера серии КД, равное *2*. Эти значения в настройках криптотуннелей TNL_1 и TNL_2 будут *неизменны* в течение всех периодов действия ключей всех сменяющих друг друга серий.
>
> КД может быть любым; период действия КД также может быть любым.

Итак, согласно исходным данным криптотуннель TNL_1 должен обеспечить работу для идентификатора номера серии КД, равного ***1***, а криптотуннель TNL_2 должен обеспечить работу для идентификатора номера серии КД, равного ***2***. Кроме того, согласно исходным данным, приведенным в таблице на Рис. 3.41 администратор перед началом работы изделия выполняет настройку изделия на работу в режиме автоматической замены КД по графику (процедура выполнения настройки приведена в разделе 3.4.3, с. 125). В результате этих действий в составе конфигуратора изделия формируется таблица-график соответствия всех *идентификаторов* реальным *номерам серии* ключевых документов.

После включения изделия в процессе инициализации его работы выполняется процедура *открытия криптотуннелей.* Этой процедурой в изделии управляет БВМ, которому доступен перечень *всех* криптотуннелей изделия – статических, TNL-интерфейсов и L2–TNL-интерфейсов. БВМ, открывая очередной криптотуннель, на основе информации из таблицы-графика устанавливает соответствие значения идентификатора номера серии (для TNL_1 в примере – это *1*) реальному значению номера серии (*287*) и выдает шифратору команду на открытие криптотуннеля на этом направлении с использованием номера серии КД *287*. Затем БВМ переходит к следующему в списке криптотуннелю – для криптотуннеля TNL_2 с идентификатором номера серии *2* шифратор получает команду на открытие на этом направлении криптотуннеля с номером серии КД *412*. И так БВМ обрабатывает весь список криптотуннелей, подлежащих открытию.

Проверка времени выполняется непрерывно (каждые 20 сек). Если подходящих промежутков несколько (промежутки пересекаются), берется первый в таблице. Действие строки заканчивается, когда вступает в действие другая строка. При этом выполняется перезагрузка всех туннелей.

Как было сказано выше, таблица-график может включать *статические* (не содержащие сведений о дате и времени замены КД) и *динамические* (содержащие сведения о дате и времени замены КД) записи. Если в таблице-графике присутствуют только статические записи, изделие будет работать без автозамены КД (весь период действия КД, пока администратор не выполнит перенастройку и перезагрузку КД *вручную*). В нашем примере ситуация была бы такой, если бы таблица-график, например, для криптотуннеля TNL_1 содержала бы единственную запись – верхнюю, с незаполненной колонкой **Начало периода действия КД**.

В нашем примере таблица-график (Рис. 3.41) содержит после статической записи несколько динамических, что означает следующее: с момента запуска изделия криптотуннель TNL_1 будет работать, используя номер серии *287*, но только до 24-х часов 31 марта 2017 года. В полночь будет выполнен переход работы криптотуннеля на КД с номером серии *362*, и так будет продолжаться до начала следующего периода действия КД. И т.д.

> *Примечание.* Отметим, что *маршрутизаторы* изделия в работе с криптотуннелями оперируют значениями идентификаторов номеров серий КД, а не значениями реальных номеров серий КД. Реальными номерами серий КД оперирует *шифратор* изделия.

Синхронизация процессов автозамены КД в масштабе ЗСПД. Весьма важным вопросом при выполнении автоматической (по графику) замены КД является вопрос *синхронизации* во времени всех процедур автозамены КД *в масштабе ЗСПД*. От степени синхронности выполнения этих процедур зависит величина *периода времени*, в течение которого защищенный обмен в ЗСПД может быть нарушен. Очевидно, величину этого периода следует сокращать. Очевидно также, что чем точнее и синхроннее идут внутренние часы каждого из изделий защиты в составе ЗСПД, тем *короче* будет время перехода изделий защиты на работу с КД новой серии.

Если в ЗСПД не допускается наличие перерывов в защищенной связи, то для обеспечения синхронной замены КД следует при настройке изделий защиты задействовать возможности, предоставляемые службой времени (SNTP-службой), поддерживаемой маршрутизаторами изделия (подробнее см. раздел 4.1.5, с. 135).

> *Внимание!* Уместно напомнить, что всякая ЗСПД логически может быть представлена в виде двух сегментов: *центрального* сегмента, представляющего собой транспортное ядро ЗСПД (состоит из инфраструктуры сетей общего пользования), и *периферийного* сегмента, представляющего собой сегмент защищенных сетей (состоит из ЛВС Пользователя). По условиям работы ЗСПД«Бастион3-Ф» в ее составе не может существовать ни одного устройства, с которого одновременно возможен информационный обмен как с устройствами в составе центрального, так и с устройствами в составе периферийного сегмента – в этом случае неминуемо возникает *канал утечки* защищаемой информации. Поэтому в составе ЗСПД приходится, соблюдая основополагающие принципы ее назначения, организовывать *два независимых контура* систем управления (в частности, системы удаленного управления изделиями защиты), систем единого сетевого времени (в частности, системы синхронизации работы SNTP-служб блоков внутренней и блоков наружной маршрутизации изделия) и пр.

При построении системы синхронизации единого времени в составе ЗСПД следует учесть необходимость рассмотрения организации *двух контуров* систем единого сетевого времени: системы синхронизации от SNTP-серверов, функционирующих в составе *центрального* сегмента ЗСПД (например, синхронизация показаний внутренних часов SNTP-служб блоков *наружной* маршрутизации изделий защиты) и системы синхронизации от SNTP-серверов, функционирующих в составе *периферийного* сегмента ЗСПД (например, синхронизация показаний внутренних часов SNTP-служб блоков *внутренней* маршрутизации изделий защиты).

В изделии служба синхронизации времени может быть организована и настроена в двух вариантах:

- время внутреннего маршрутизатора и шифратора изделия *зависит* от времени наружного маршрутизатора; при этом часы SNTP-службы БНМ настраиваются на корректировку от SNTP-серверов центрального сегмента ЗСПД (в качестве такого SNTP-сервера может выступать SNTP-служба какого-либо из БНМ изделия защиты), а шифратор и БВМ настраиваются по времени БНМ; понятно, что такая схема синхронизации уязвима со стороны сетей общего пользования и работа незащищенного SNTP-протокола может быть нарушена посылкой пакетов с ложными метками времени;
- время внутреннего маршрутизатора и шифратора изделия *не зависит* от времени наружного маршрутизатора (см. раздел 4.1.5, Рис. 4.6, с. 135, параметр **Время внутреннего маршрутизатора независимо**); при этом часы SNTP-службы БВМ изделия настраиваются на корректировку от SNTP-серверов периферийного сегмента ЗСПД (в качестве такого SNTP-сервера может выступать SNTP-служба какого-либо из БВМ изделия защиты); учитывая, что механизм автозамены КД работает, ориентируясь на часы БВМ, а все БВМ в ЗСПД связаны между собой, и часы их SNTP-служб могут быть синхронизированы между собой, а уязвимости SNTP-протокола практически ничто не угрожает, этот вариант организации в ЗСПД системы синхронизации времени с целью проведения автозамены КД по графику предпочтительнее.

3.4.3. Настройка режима замены ключевых документов по графику

Как следует из приведенных выше сведений, для обеспечения при функционирования изделия автоматической замены ключевых документов по графику следует выполнить следующие работы:

- подготовить исходные данные (во взаимодействии с Администрацией ЗСПД) для настройки таблицы-графика замены КД; процесс подготовки исходных данных рассмотрен на конкретном примере в разделе 3.4.2 (см. Рис. 3.41, с. 124);
- выполнить настройку работы изделия с соответствующими криптотуннелями согласно подготовленным исходным данным;
- выполнить настройку работы изделия в режиме автозамены КД согласно подготовленным исходным данным; процесс настройки приведен ниже в данном разделе РНУ;
- если принято решение о необходимости организации системы синхронизации единого времени в масштабе всей ЗСПД, выполнить настройку работы изделия в режиме синхронизации часов SNTP-служб маршрутизаторов изделия согласно установленному Администрацией ЗСПД варианту – с зависимостью или с независимостью часов SNTP-службы БВМ изделия от показаний часов SNTP-службы БНМ изделия (подробнее см. раздел 4.1.5, Рис. 4.6, с. 135, параметр **Время внутреннего маршрутизатора независимо**);
- выполнить запуск изделия и загрузить в него все ключевые документы, требуемые согласно графику замены.

Для первоначального создания или для управления ранее созданной таблицей-графиком автозамены КД следует выбрать цепочку альтернатива ГМ: **Настройка** ⇨ **Защита** ⇨ **График замен ключей** (см. Рис. 3.2, с. 72).

В ответ на видеомонитор ЛКУ будет выдан аналогичный представленному на Рис. 3.42 экран расписания (графика) автозамены ключевых документов, содержащий записи графика автозамены ключевых документов (изначально график пустой). В средней части экрана (Рис. 3.42) представлены строки, содержащие записи расписания замены КД, имеющих идентификаторы номеров серий: ***1***, ***2***, ***3*** и ***4***, на КД, соответственно, с реальными номерами серий: ***1001***, ***1002***, ***1003*** и ***1004***.

Управление записями расписания выполняется с помощью функциональных клавиш, назначение которых приведено в нижней части экрана (Рис. 3.42).

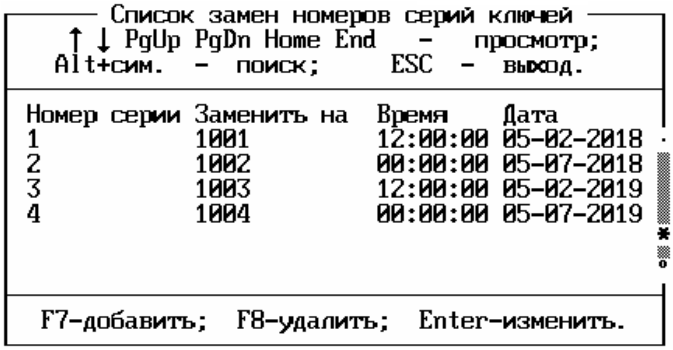


Рис. 3.42 Экран расписания автозамены ключевых документов

F7 – **добавить** (Рис. 3.42). Нажатие клавиши <F7> приводит к выводу на видеомонитор ЛКУ бланка создания и настройки записи графика автозамены ключевых документов, аналогичного представленному на Рис. 3.43. Для создания и настройки записи надо заполнить поля бланка.

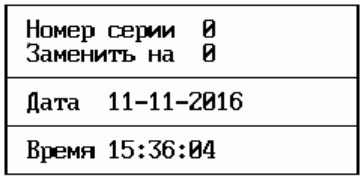
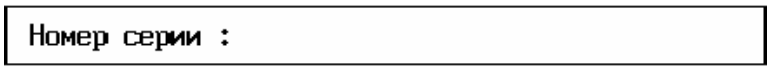


Рис. 3.43 Бланк создания и настройки записей графика автозамены ключевых документов

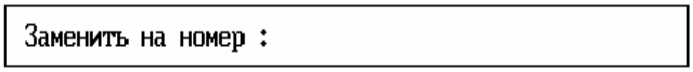
Номер серии (Рис. 3.43) − переместить курсор на строку бланка и нажать клавишу <Enter>. В ответ будет выдан запрос на ввод *заменяемого* номера серии КД:



В поле запроса надо ввести значение *номера серии* КД, заменяемой в перспективе согласно этой строке расписания, после чего нажать клавишу <Enter>. Как правило, это − *идентификатор* номера серии КД.

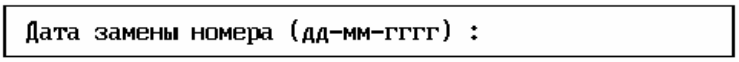
Примечание. В поле запроса может быть введено значение реального номера серии КД, если планируется, например, использовать ключи этой серии до первой замены.

Заменить на (Рис. 3.43) − переместить курсор на строку бланка и нажать клавишу <Enter>. В ответ будет выдан запрос на ввод *заменяющего* (реального) номера серии КД:



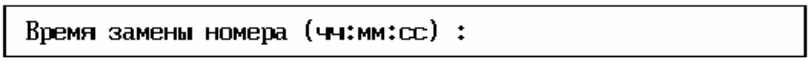
В поле запроса надо ввести реальный *номер серии* КД, заменяющей в перспективе предыдущую согласно этой строке расписания, после чего нажать клавишу <Enter>.

Дата (Рис. 3.43) − переместить курсор на строку бланка и нажать клавишу <Enter>. В ответ будет выдан запрос на ввод *даты* замены номера серии КД:



Следует ввести в поле запроса значение *даты* замены в перспективе согласно этой строке расписания номера серии КД в предложенном формате и нажать клавишу <Enter>.

Время (Рис. 3.43) − переместить курсор на строку бланка и нажать клавишу <Enter>. В ответ будет выдан запрос на ввод *времени* замены номера серии КД:



Следует ввести в поле запроса значение *времени* замены в перспективе согласно этой строке расписания номера серии КД в предложенном формате и нажать клавишу <Enter>.

> *Примечание.* При заполнении бланка поля **Дата** и **Время** могут остаться не заполненными (указаны *пустые* значения этих параметров). Это означает, что будут созданы *статические* записи расписания замены КД; при наличии в графике только статических записей автозамена КД изделием выполняться не будет (подробнее см. раздел 3.4.2 , с. 122).

После ввода значения времени замены номера создание (и настройка) строки расписания заканчивается и курсор перемещается в бланк создания и настройки записей графика автозамены ключевых документов (Рис. 3.43). Далее следует проверить правильность параметров настроенной строки расписания и нажать клавишу <Esc>, курсор переместится на экран расписания автозамены ключевых документов (Рис. 3.42).

F8 – **удалить** (Рис. 3.42). После нажатия клавиши <F8> будет удалена из списка та строку расписания, на которую был установлен курсор.

Enter – **изменить** (Рис. 3.42). Установив курсор в списке ранее созданных записей на строку расписания, параметры которой необходимо откорректировать, нажать клавишу <Enter>. На видеомонитор ЛКУ будет выдан бланк создания и настройки записей графика автозамены ключевых документов (Рис. 3.43), с помощью которого следует выполнить требуемую корректировку.

3.5. Алгоритм работы маршрутизаторов изделия

В состав каждого из маршрутизаторов изделия (БВМ или БНМ) включены обработчики всех средств защиты, поддерживаемых изделием. Максимальный уровень защиты информации Пользователя в аспектах обеспечения ее конфиденциальности, целостности и доступности достигается использованием *всех* возможных средств защиты: криптотуннелей (туннельных сетевых интерфейсов и/или статических туннелей), IP-фильтров и NAT-обработчиков. Для правильного конфигурирования средств защиты требуется понимание полного алгоритма работы маршрутизатора с учетом последовательности этапов обработки IP-датаграмм и обеспечения функционирования всех средств защиты. Обобщенное описание алгоритма работы маршрутизатора изделия приведено ниже.

После получения каждой IP-датаграммы через один из Ethernet-интерфейсов любого из маршрутизаторов ее дальнейшая обработка выполняется по приведенным ниже правилам. Обработка осуществляется в виде последовательности этапов, выполняемых один за другим тем или иным средством, обеспечиваемым изделием.

> *Замечание*. Если в процессе обработки датаграммы тот или иной этап алгоритма оказывается не востребованным администратором при настройке изделия (например, не будет выполняться п. 3 приведенной ниже последовательности этапов обработки, если на соответствующем маршрутизаторе не включен NAT-обработчик), то выполняется переход к следующему этапу обработки.

1. *Входной контроль датаграммы*: проверяются формат, длина и контрольная сумма поступившей через Ethernet-интерфейс датаграммы. При отрицательном результате проверки датаграмма снимается с дальнейшей обработки.

2. *Фильтрация* поступившей датаграммы по набору правил входного фильтра того сетевого интерфейса, по которому пришла датаграмма. Если результат проверки окажется отрицательным, датаграмма снимается с дальнейшей обработки.
3. *NAT-обработка* входящей датаграммы.
4. *Извлечение* поступившей датаграммы из GRE-туннеля.
5. *Извлечение* поступившей датаграммы из криптотуннеля (с помощью БКО).
6. Из датаграммы извлекается IP-адрес назначения. Используя значение параметра **Собственный IP-адрес** маршрутизатора (см. раздел 4.1.2, с. 130), значения параметров **Локальный IP-адрес** для всех сетевых (физических и виртуальных) интерфейсов маршрутизатора, а также содержание маршрутных записей сетевых (физических и виртуальных) интерфейсов маршрутизатора, сформированных с помощью значений параметра **Таблица маршрутизатора**, маршрутизатор проверяет, не предназначена ли IP-датаграмма собственно маршрутизатору, выполняющему обработку датаграммы (точнее, одному из его прикладных сервисов или служб).
7. Если датаграмма адресована прикладному сервису, то она отправляется по назначению, и на этом обработка датаграммы маршрутизатором заканчивается.

   Если датаграмма является *транзитной*, то обработка продолжается.
8. *Упаковка* датаграммы в криптотуннель, если такая обработка предусмотрена правилами отбора (для статического криптотуннеля).
9. *Маршрутизация.* Маршрутизатор, пользуясь своей маршрутной таблицей, определяет, по какому интерфейсу должна быть отправлена эта датаграмма. Если для ее отправки пригодны несколько интерфейсов, то из них выбирается оптимальный – интерфейс с меньшим значением параметра **Метрика**.

   Если маршрутной таблицей маршрутизатора датаграмма направляется в TNL-интерфейс, то выполняется упаковка датаграммы в криптотуннель (с помощью БКО).

   Если маршрутизатор не найдет подходящего интерфейса, то датаграмма будет снята с доставки и уничтожена. Отправителю будет послано соответствующее ICMP-сообщение.
10. *Фильтрация* отправляемой датаграммы по набору правил выходного фильтра интерфейса, выбранного для отправки. Если результат проверки окажется отрицательным, датаграмма снимается с доставки.
11. *NAT-обработка* исходящей датаграммы.
12. *Фрагментация* датаграммы в соответствии с параметром **MTU** (максимально возможный размер датаграммы) выбранного интерфейса.
13. *Отправка датаграммы*. Датаграмма передается выбранному интерфейсу. Интерфейс преобразует датаграмму в поток данных (инкапсуляция датаграммы) в соответствии со своим **типом** (протоколом инкапсуляции) и выполняет отправку.

4. Настройка отдельных параметров

В настоящем разделе рассмотрена настройка отдельных параметров конфигуратора изделия, влияющих на работу каждого из блоков маршрутизации изделия (БВМ или БНМ). Эти параметры не объединены общим смысловым значением, поэтому в настоящем руководстве их описание будет приведено в порядке, определяемом их следованием в двух меню:

- в представленном на Рис. 4.1 меню настройки параметров маршрутизатора изделия, выдаваемом на видеомонитор ЛКУ в ответ на выбор цепочки альтернатив ГМ: **Настройка ⇨ Параметры**;
- в представленном на Рис. 4.24, с. 146 меню настройки различных дополнительных параметров маршрутизатора изделия, выдаваемом на видеомонитор ЛКУ в ответ на выбор цепочки альтернатив ГМ: **Настройка ⇨ Разное**.

4.1. Настройка ⇨ Параметры

Основные константы
Параметры TCP/IP
Трассировка
Удаленная консоль
Служба времени
Параметры консоли
Параметры журналов
Архив конфигураций

Рис. 4.1 Меню настройки параметров маршрутизатора изделия

> *Примечание.* Цепочка альтернатив: **Настройка ⇨ Параметры ⇨ Архив конфигураций** доступна только при подключении блока ЛКУ к БНМ изделия.

Далее в настоящем разделе приведены пояснения, необходимые для правильной настройки этих параметров.

4.1.1. Настройка ⇨ Параметры ⇨ Основные константы

В ответ на выбор цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Основные константы** на видеомонитор ЛКУ выдается меню настройки основных параметров TCP/IP-компонента маршрутизатора изделия, аналогичное представленному на Рис. 4.2.

Количество TCB-блоков	: 24
Размер буфера каждого TCB-блока	: 16
Количество Proxy-буферов	: 132
Режим работы в кластере: Master	таймер 2
Размер таблиц фильтров сессий	: 512

Рис. 4.2 Меню настройки основных параметров маршрутизатора изделия

Количество TCB-блоков (Рис. 4.2). Параметр определяет количество обрабатываемых программой управления TCB-блоков. Каждый TCB-блок управляет одним TCP-соединением, устанавливаемым между сервисами изделия и абонентами.

Заданное количество TCB-блоков устанавливает разрешенное количество одновременно существующих TCP-соединений. Умалчиваемое значение параметра устанавливается равным **8+4*N**, где **N** – количество TCP-портов, имеющихся в конфигурации соответствующего маршрутизатора (в стандартной конфигурации четыре TCP-порта, количество TCB-блоков **8+4*4=24**). Администратор может изменить это значение, исходя из условий эксплуатации изделия. Максимально разрешенное количество блоков – ***450***.

Размер буфера каждого TCB-блока (Рис. 4.2). Параметр определяет объем буфера памяти (в килобайтах), резервируемого под TCB-блок для хранения данных. Значение должно быть не меньше удвоенного размера TCP-окна (см. ниже **Параметры TCP/IP ⇨ Размер TCP-окна (Window)**, с. 131). Лучше – больше, если позволяет память. Максимально возможное значение – 64 Кб.

Количество Proxy-буферов (Рис. 4.2). Параметр не используется.

Режим работы в кластере (Рис. 4.2). Параметр позволяет запустить изделие в режиме **Master** или в режиме **Slave** (о работе изделия в составе кластера см. раздел 7, с. 174).

Параметр **Режим работы в кластере** (Рис. 4.2) может принимать значения:

- *MASTER* **-** изделие будет запущено в режиме **Master**;
- *SLAVE* – изделие будет запущено в режиме **Slave**;
- *нет* – режим кластера не включен.

Параметр **Таймер** (Рис. 4.2). Чтобы задать значение интервала таймера при работе изделия в составе кластера, надо переместить курсор на альтернативу **таймер** и нажать клавишу <Enter>; на видеомонитор ЛКУ будет выдан запрос в формате:

```
Значение таймера кластерного режима (8..255 тик.) :
```

- для изделия в режиме **Master** параметр задает (в тиках; *тик* – около одной восемнадцатой секунды) периодичность, с которой изделие будет посылать технологический *пакет-извещение*, свидетельствующее о работоспособности изделия;
- для изделия в режиме **Slave** параметр задает (в тиках) максимальное время ожидания изделием очередного пакета-извещения от изделия, работающего в режиме **Master**; если изделие, работающее в режиме **Slave**, в течение этого времени не получит пакет-извещение, то оно перейдет из режима работы **Slave** в режим работы **Master**.

Значение параметра **Таймер** для изделия, работающего в режиме **Slave**, должно несколько превышать значение для изделия в режиме **Master**.

> *Примечание.* Конкретные значения параметра **Таймер** для изделий, работающих в режимах **Master** и **Slave**, зависят от условий применения кластера в составе ЗСПД. Рекомендуемые стартовые значения параметра **Таймер**: ***10*** – для изделия со статусом **Master**; ***12*** – для изделия со статусом **Slave**.

Размер таблиц фильтров сессий (Рис. 4.2). Параметр определяет максимально возможное количество записей в *фильтре сессий* одного интерфейса (фильтры с отслеживанием состояния соединений – фильтры сессий – рассмотрены в разделе 3.2.1.8, с. 106).

4.1.2. Настройка ⇨ Параметры ⇨ Параметры TCP/IP

В ответ на выбор цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Параметры TCP/IP** на видеомонитор ЛКУ выдается меню настройки TCP/IP-параметров маршрутизатора изделия, аналогичное представленному на Рис. 4.3.

Собственный IP-адрес наружн. : 192.168.32.228 внутр. : 192.168.222.1
Время жизни IP-датаграмм (TTL) : 32
Макс. размер TCP-пакета (MSS) : 512
Размер TCP-окна (Window) : 8192
Разрешена работа PROXY-ARP : Нет

Рис. 4.3 Меню настройки TCP/IP-параметров маршрутизатора изделия

Собственный IP-адрес (Рис. 4.3). Параметр задает значения собственных IP-адресов маршрутизаторов:

наружн.: собственный IP-адрес *наружного* маршрутизатора (БНМ);

внутр. : собственный IP-адрес *внутреннего* маршрутизатора (БВМ).

Время жизни IP-датаграмм (TTL) (Рис. 4.3). Параметр **TTL** (Time To Live) определяет максимальное количество узлов сети (маршрутизаторов), которое может быть пройдено IP-датаграммами на пути от точки отправления до адресата. Значением может быть целое число в диапазоне от ***0*** до ***255***. Умалчиваемое значение параметра – ***32***.

Начальное значение TTL устанавливается в точке отправки IP-датаграммы. Каждый узел, обрабатывающий данную датаграмму, уменьшает значение TTL на единицу. Если значение TTL станет равным нулю, то IP-датаграмма будет снята с доставки, а отправителю датаграммы будет отправлено ICMP-сообщение о снятии датаграммы с доставки (Time Exceeded).

Указанным способом ограничивается количество узлов сети, которое IP-датаграмма может пройти на пути к цели, что служит защитой от возможных маршрутных циклов.

Максимальный размер TCP-пакета (MSS) (Рис. 4.3). Параметр **MSS** (Maximum Segment Size) определяет максимальный размер данных, которые могут быть отправлены удаленным TCP-процессом в одном TCP-пакете. Значением параметра может быть целое число в диапазоне от ***0*** до ***2**16***. Умалчиваемое значение параметра – ***512***.

Рекомендуется устанавливать значение MSS в диапазоне от ***256*** до ***1460***.

Размер TCP-окна (Window) (Рис. 4.3). Параметр определяет размер данных (в байтах), которые могут быть отправлены по TCP-каналу без ожидания подтверждения. Значением может быть целое число в диапазоне от ***0*** до ***2**16***. Умалчиваемое значение параметра – ***8192***. Обычно размер TCP-окна устанавливается кратным MSS (**2*MSS**, **4*MSS** или более). Не рекомендуется устанавливать значение размера TCP-окна больше ***8192***.

Разрешена работа PROXY-ARP (Рис. 4.3). В рамках функционирования физических сетевых интерфейсов изделия, обеспечивающих соединение изделия с локальными сетями, реализована поддержка ARP-протокола. С помощью ARP-протокола обеспечивается автоматическое определение MAC-адреса доставки IP-датаграммы в среде локальной сети по IP-адресу назначения IP-датаграммы.

Поддержка ARP-протокола включает два компонента: *клиентский* и *серверный*. Клиентская часть обработчика ARP-протокола работает в тех случаях, когда для *исходящих* IP-датаграмм изделия следует найти соответствующий MAC-адрес в локальной сети. Серверная часть ARP-протокола работает в тех случаях, когда в изделие поступает *входящий* ARP-запрос от других маршрутизаторов локальной сети.

ARP-запрос содержит IP-адрес и имеет следующий смысл: «*Уважаемое устройство, не Ваш ли это IP-адрес? Если Ваш, то сообщите соответствующий ему MAC-адрес Вашего интерфейса*». Если изделие считает указанный в запросе IP-адрес своим, то оно посылает по обратному адресу ARP-запроса ответ, содержащий MAC-адрес того интерфейса, который принял ARP-запрос.

Набор IP-адресов, которые изделие считает своими, зависит от значения параметра **Разрешена работа PROXY-ARP** (Рис. 4.3).

Если параметру присвоено значение ***НЕТ***, изделие считает IP-адрес в ARP-запросе своим в следующих случаях.

1. IP-адрес в ARP-запросе совпадает с собственным IP-адресом соответствующего маршрутизатора изделия.
2. IP-адрес в ARP-запросе совпадает с локальным IP-адресом того интерфейса маршрутизатора, по которому получен ARP-запрос.
3. IP-адрес в ARP-запросе совпадает с IP-адресом перегрузки или с одним из *реальных* IP-адресов статической NAT-таблицы изделия.
4. Если в статической NAT-таблице в качестве *внутреннего* и *внешнего* адресов задан один и тот же IP-адрес и IP-адрес в ARP-запросе, пришедшем на внешний интерфейс NAT, совпадает с этим IP-адресом.

Если параметр **Разрешена работа PROXY-ARP** имеет значение ***ДА***, то к предыдущим четырем добавляется еще один случай:

5. IP-адрес в ARP-запросе совпадает с локальным или удаленным IP-адресом одного из активных интерфейсов.

4.1.3. Настройка ⇨ Параметры ⇨ Трассировка

При выборе цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Трассировка** на видеомонитор ЛКУ выдается представленный на Рис. 4.4 бланк управления параметрами трассировки компонентов изделия.

В состав изделия включены программные компоненты, которые обеспечивают возможность фиксации и интерпретации проходящей через изделие информации и вывод ее в удобочитаемой форме на видеомонитор ЛКУ с одновременным сохранением в журнале изделия **LOG.EMA** (см. раздел ***Приложение Е***, с. 248). Механизм, обеспечивающий документирование на машинных носителях и выдачу на видеомонитор ЛКУ диагностических данных, называется *трассировкой*.

Предусмотрена возможность трассировки функционирования следующих компонентов изделия.

1. Работа всех интерфейсов блоков маршрутизации изделия. Анализируются все датаграммы или кадры, принимаемые и отправляемые интерфейсами, и для каждой датаграммы (или кадра) формируется трассировочная информация, состоящая из:
   - текстового представления всех полей IP-заголовка датаграммы (или заголовка кадра);
   - текстового представления всех полей заголовков пакетов TCP, UDP и ICMP, транспортируемых IP-датаграммой;
   - шестнадцатеричного дампа всей IP-датаграммы (или кадра).
2. Работа ARP-протокола. Анализируются все ARP-пакеты (ARP-запросы и ARP-ответы). Для каждого ARP-пакета формируется трассировочная информация.

3. Работа маршрутизатора. Фиксируется каждая проходящая через маршрутизатор датаграмма и выводится информация о результате маршрутизации и о преобразованиях датаграммы (если они выполнялись – NAT, туннели).
4. Работа криптосистемы изделия.
5. Работа прикладных служб. Потоки информации, которой обменивается каждая служба с внешним миром, фиксируются в текстовом формате, соответствующем специфике конкретной службы.

В соответствии с перечисленными видами объектов трассировки бланк управления параметрами трассировки работы компонентов изделия разделен на несколько зон (см. Рис. 4.4).

Рис. 4.4 Бланк управления параметрами трассировки компонентов изделия

Параметры установки режима трассировки – зона **Интерфейсы** (Рис. 4.4):

Ethernet – трассировка Ethernet-интерфейсов;

Ethernet ext – трассировка Ethernet-интерфейсов (на L2-уровне);

Loopback&Bdcst – трассировка внутренних передач (отправка IP-датаграмм себе) и широковещательных (`broadcast`) пакетов;

HEX-дамп – если параметр задан (после параметра установлен знак «**+**» (*плюс*)), будет выводиться шестнадцатеричный дамп всей IP-датаграммы; если параметр не задан (после параметра установлен знак «–» (*минус*)), то будет выполняться только расшифровка заголовков в соответствии со значением параметра **Уровень**; параметр может быть задан только для наружного маршрутизатора.

Уровень – уровень анализа заголовков датаграмм – значения параметра от *0* до *7*:

- ***0*** – анализ заголовков датаграмм отсутствует;
- ***1*** – трассировка заголовков пакетов канального уровня;
- ***2*** – трассировка заголовков IP-пакетов и ARP-пакетов;
- ***4*** – трассировка TCP, UDP и ICMP- заголовков.

Примечание. Возможно указание *суммы* приведенных значений.

ARP – трассировка ARP-протокола.

Внимание! Все изменения в полях бланка (Рис. 4.4) вступают в силу только после автоперезапуска и записи обновленного конфигуратора в БпО.

Параметры установки режима трассировки – параметр **Маршрутизатор** (Рис. 4.4).

Маршрутизатор – значения параметра – десятичное число в диапазоне от *0* до *31*:

- ***0*** – анализ работы маршрутизатора отсутствует;
- ***1*** – выводятся только ошибки в маршрутизации датаграмм;
- ***2*** – выводятся сообщения, соответствующие нормальной работе маршрутизатора;
- ***4*** – трассировка всех обрабатываемых датаграмм, расшифровка IP-заголовков и вложенных TCP, UDP, ICMP-заголовков;
- ***8*** – к предыдущему добавляется представленный в шестнадцатеричном формате дамп обрабатываемых датаграмм (только для наружного маршрутизатора– БНМ);

  Примечание. Возможно указание *суммы* приведенных значений.
- ***16*** – выводится расширенная информация о причинах ошибок маршрутизации датаграмм.

Параметры установки режима трассировки – параметр **Криптография** (Рис. 4.4):

Криптография – значения параметра – десятичное число в диапазоне от ***0*** до ***255***:

- ***0*** – анализ работы криптосистемы отсутствует;
- ***1*** *- ERR* – выводятся сообщения о серьезных ошибках в работе шифратора (нехватка памяти, некорректная работа аппаратуры и т.п.);
- ***2*** *- REPORT* – выводится расшифровка сообщений, посланных шифратором блоку внутренней маршрутизации (шифратор посылает сообщения на БВМ, если возникают какие-то проблемы);
- ***4*** *- TNL* – трассировка упаковки и распаковки датаграмм в туннели;
- ***8*** *- TNLe* – более полная трассировка упаковки и распаковки датаграмм в туннели;
- ***16*** *- MGMT* – выводится дополнительная информация о причинах ошибок маршрутизации датаграмм.

Примечание. Возможно указание *суммы* приведенных значений.

Параметры установки режима трассировки – зона **Службы** (Рис. 4.4):

Примечание. Обозначения (аббревиатуры) приведенных в зоне **Службы** названий служб (сервисов), заканчивающиеся на букву ***D***, обозначают *серверные* компоненты соответствующих служб (сервисов) – например, **TelnetD**, **DHCPD**, **DNSD** и т. д.

Чтобы включить трассировку, следует перевести курсор на соответствующую строку бланка (Рис. 4.4) в зоне **Службы** и нажать клавишу <Enter>; в ответ символ «*минус*» после обозначения службы (сервиса) изменится на «*плюс*». Повторное нажатие клавиши <Enter> отменит трассировку (в бланк вернется знак «*минус*»).

Внимание! Трассировка существенно замедляет работу изделия. Поэтому включать трассировку следует только для целей наладки изделия, исключая ее использование в режиме штатной эксплуатации.

Включить трассировку компонентов изделия можно несколькими способами, описанными ниже.

1. С помощью описанного в настоящем разделе выбора цепочки альтернатив ГМ: **Настройка** ⇨ **Параметры** ⇨ **Трассировка**. Все установленные таким образом параметры трассировки заносятся в конфигурационный файл системы и действуют постоянно (даже после перезапуска изделия) вплоть до их явной отмены. Параметры действуют для обоих блоков маршрутизации, наружного и внутреннего.
2. С помощью выбора цепочки альтернатив ГМ: **Диагностика** ⇨ **Параметры** ⇨ **Трассировка** (см. раздел 9.1, с. 187). Это позволяет установить те же параметры, что и в предыдущем случае, но *без сохранения* настроек в конфигурационном файле. Это означает, что параметры трассировки, установленные таким способом, действуют только до перезапуска изделия (или до их явной отмены). Параметры трассировки устанавливаются для каждого маршрутизатора изделия независимо.

   Первым и вторым способом включается трассировка ARP-протокола, маршрутизатора, криптосистемы и служб. Что касается интерфейсов, то для них трассировка включается в момент активизации интерфейса при запуске изделия. При этом параметры трассировки формируется по следующим правилам.

   a). Программа управления считывает значения параметров режима трассировки для интерфейсов, установленного при выборе цепочек альтернатив **Настройка** ⇨ **Параметры** ⇨ **Трассировка** или **Диагностика** ⇨ **Параметры** ⇨ **Трассировка**.

   b). Если задана трассировка сетевых физических интерфейсов (в поле бланка на Рис. 4.4 справа от параметров **Ethernet** и/или **Ethernet ext** стоит символ «*плюс*»), то режим трассировки интерфейсов определяется полем **Уровень** бланка трассировки.
3. С помощью выбора цепочки альтернатив ГМ: **Диагностика** ⇨ **Интерфейсы** ⇨ **Активные** ⇨ **Трассировка** ⇨ **Ctrl+Enter** (см. раздел 9.2.2, с. 189) можно включить выборочную трассировку одного или нескольких *активных* интерфейсов и установить параметры трассировки. Такая настройка действует только до тех пор, пока интерфейс активен (или до явной отмены). Третий способ применяется, как правило, для оперативного включения трассировки интерфейса или оперативного внесения изменений в параметры трассировки.
4. Для включения выборочной трассировки активного интерфейса можно использовать средства оперативного контроля состояния интерфейсов (см. раздел 2.6, с. 52): команда **Enter – трассировка интерфейса** (Рис. 2.39, с. 52) и **Ctrl+Enter** – **трассировка интерфейса** (Рис. 2.48, с. 57).

   Примечание. В изделии реализован режим *избирательной* трассировки. Его организация обеспечивается с помощью *системного* фильтра с именем **trace** (см. раздел 3.2.1.7, с. 104). Если в составе маршрутизатора изделия описан фильтр с таким именем, то трассировка будет выполняться только для IP-датаграмм, разрешенных этим фильтром.

4.1.4. **Настройка ⇨ Параметры ⇨ Удаленная консоль**

Изделиями, исполненными в двухсегментной архитектуре технологии DioNIS®, поддерживается механизм удаленного управления. Одно изделие (*управляющее*) управляет другим (*управляемым*) по защищенным каналам связи.

Примечание. Об удаленном управлении см.также разделы 1.3.3, с. 12 и 11, с. 204.

Для решения целого ряда задач на управляемом изделии (наблюдение за работой внутреннего и наружного маршрутизатора, оперативная перенастройка маршрутизаторов, трассировка и др.) можно осуществить удаленное управление с управляющего изделия в режиме т.н. *удаленной консоли*. При этом в процессе установления соединения между управляющим и управляемыми изделиями выполняется процедура *аутентификации*, призванная повысить вероятность того, что управляющее изделие находится под управлением персонала ЗСПД, а не в руках злоумышленника.

Для выполнения процедуры аутентификации следует на управляемом изделии создать описание абонента, которому будет дано разрешение на удаленное управление, и указать, какие действия ему будут разрешены в процессе удаленного воздействия на управляемое изделие (см. раздел 6.4, с. 171).

Управляющее изделие подключается по каналу связи к управляемому от имени этого абонента и получает удаленно на консоли БВМ или БНМ копию соответствующей консоли управляемого изделия и, в зависимости от установленных полномочий, может наблюдать за информацией или выполнять контролирующие и управляющие действия, доступные с локальной консоли управляемого изделия.

Чтобы дать разрешение на удаленное управление, администратор *управляемого* изделия должен выбрать цепочку альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Удаленная консоль**. В ответ на видеомонитор ЛКУ будет выдан бланк настройки параметров для организации управления в режиме удаленной консоли, представленный на Рис. 4.5.

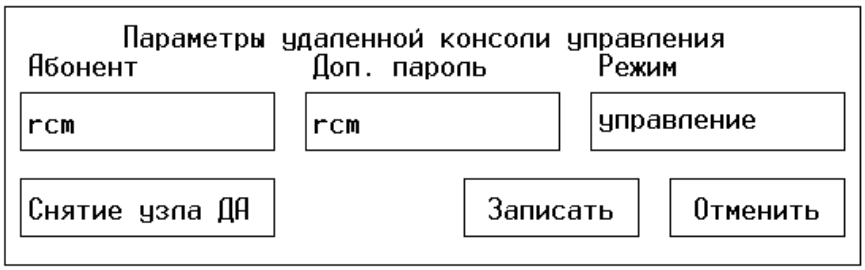


Рис. 4.5 Бланк настройки параметров для организации управления в режиме удаленной консоли

В поле под заголовком **Абонент** (Рис. 4.5) следует занести *имя абонента* – то имя, под которым управляющее изделие зарегистрировано как абонент управляемого изделия.

В поле под заголовком **Доп. пароль** (Рис. 4.5) следует занести произвольную комбинацию не более чем из 15 символов. Этот пароль служит для дополнительной защиты от несанкционированного доступа к удаленному управлению.

В поле под заголовком **Режим** (Рис. 4.5) – параметр, определяющий уровень полномочий, которыми будет обладать управляющее изделие в процессе удаленного управления. Возможные значения параметра: *Просмотр*, *Управление* или *Захват*.

> *Просмотр* – персонал управляющего изделия сможет только наблюдать на своей консоли – БВМ или БНМ – за работой соответствующего блока управляемого изделия – БВМ или БНМ.
>
> *Управление* – персонал управляющего изделия сможет управлять работой изделия наравне с локальным администратором; управляемое изделие будет одинаково исполнять команды, полученные как с локальной консоли, так и с удаленной.
>
> > Напомним, что для записи измененных параметров в БпО требуется вручную дать разрешение (см. раздел 1.3.3, с. 12).
>
> *Захват* – управляемое изделие исполняет только команды управляющего изделия, клавиатура управляемого изделия отключается.

Снятие узла (Рис. 4.5) – с помощью этого параметра локальный администратор может разрешить персоналу управляющего изделия в режиме удаленного управления свернуть работу узла. Возможные значения параметра: *Да*, *Нет*.

Заполнив графы бланка, следует активизировать альтернативу бланка **Записать** (Рис. 4.5).

4.1.5. ***Настройка ⇨ Параметры ⇨ Служба времени***

Выбор цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Служба времени** позволяет установить (откорректировать) для конкретного маршрутизатора изделия текущие *время* и *дату*, которыми в случае необходимости будут руководствоваться процессы, приложения, службы и сервисы настраиваемого маршрутизатора, а также позволяет согласовать работу своей службы времени (SNTP-службы) с SNTP-службами других маршрутизаторов – второго маршрутизатора собственного изделия и маршрутизаторов изделий, функционирующих в составе ЗСПД.

При выборе цепочки альтернатив на видеомонитор ЛКУ будет выдан бланк настройки режима работы SNTP-службы маршрутизатора изделия, аналогичный представленному на Рис. 4.6.

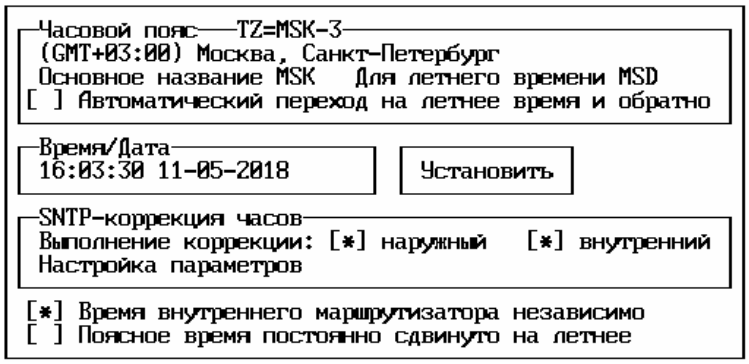


Рис. 4.6 Бланк настройки режима работы SNTP-службы маршрутизатора изделия

Параметры настройки SNTP-службы маршрутизатора объединены в бланке настройки (Рис. 4.6) в отдельные поля согласно своему функционалу; описание полей приведено ниже.

`Часовой пояс` (Рис. 4.6). Справа от заголовка в обрамляющую поле рамку выводится установленное ранее значение системной переменной **`TZ`** (`time zone` – часовой пояс).

Служба времени маршрутизатора изделия позволяет согласовать свою работу с работой SNTP-служб других изделий в составе ЗСПД, функционирующих как в одном часовом поясе с настраиваемым изделием, так и размещенных на объектах, находящихся в других часовых поясах.

С этой целью следует указать директивное значение *часового пояса* географической точки объекта, на котором готовится к эксплуатации настраиваемое изделие, для чего установить курсор на первую строку поля бланка под заголовком **`Часовой пояс`** и нажать клавишу <Enter>. На видеомонитор ЛКУ будет выведен список часовых поясов планеты; в этом списке надо установить курсор на строку, содержащую требуемый описатель часового пояса, и нажать клавишу <Enter>.

Список содержит 24 строки описателей часовых поясов, в каждом из которых приведено значение смещения времени в соответствующем часовом поясе (единица измерения смещения – один час) относительно времени *нулевого* часового пояса, средним меридианом которого является *нулевой Гринвичский* меридиан (его географическая долгота равна – 0 градусов 0 минут 0 секунд), давший название системе Мирового времени – **`GMT`** (Greenwich Mean Time). Каждый описатель часового пояса в списке включает мнемоническое имя (имена). В России пока не существует стандарта наименований часовых поясов, но для многих из них сложились устоявшиеся значения. Администратор изделия может указать собственное значение этого имени, выбрав альтернативу **`Основное название`**, для чего установить курсор на вторую строку поля бланка под заголовком **`Часовой пояс`**, нажать клавишу <Enter> и в поле появившегося запроса ввести имя часового пояса (**`MSK`** – для Москвы). Если для летнего времени есть другое имя, то его тоже следует указать (**`MSD`** – для Москвы).

`Автоматический переход на летнее время и обратно`. Если в позицию перед названием параметра между квадратными скобками поставить «*****» (символ *звездочка*), то программой управления будет автоматически выполняться переход на соответствующее время в нужный период.

`Время/Дата` (Рис. 4.6). Для установки текущих времени и даты службы времени маршрутизатора следует в поле бланка под заголовком **`Время/Дата`** перевести курсор на поле **`Установить`** и нажать клавишу <Enter>.

На видеомонитор ЛКУ будет выдан аналогичный представленному на Рис. 4.7 бланк установки текущего времени и даты. Для установки значения даты следует переместить курсор в поле бланка **`Дата`** и, последовательно выбирая курсором поля календаря, задать текущие значения *года*, *месяца* и *даты*.

После выбора даты и задания времени надо в поле бланка под заголовком **`Время`** (Рис. 4.7) переместить курсор на поле **`Установить`** и нажать клавишу <Enter>.

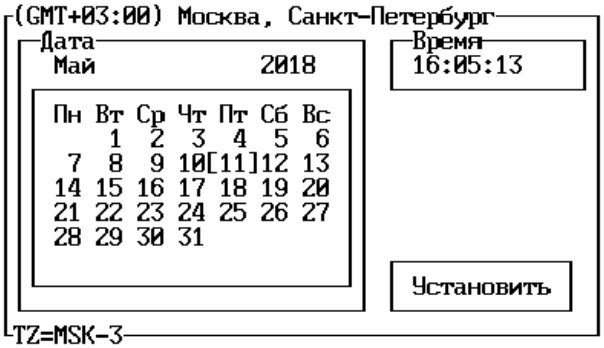


Рис. 4.7 Бланк установки текущего времени и даты маршрутизатора изделия

SNTP-коррекция часов (Рис. 4.6). Для повышения синхронности взаимодействия SNTP-служб маршрутизаторов изделий в составе ЗСПД работу внутренних часов SNTP-службы маршрутизатора необходимо корректировать, так как часы маршрутизатора изделия – это обычный аппаратный элемент, имеющий конечную точность (погрешность) хода. Необходимость коррекции должна быть определена при настройке отдельно для каждой из SNTP-служб соответствующего блока маршрутизации изделия.

Служба времени маршрутизатора изделия позволяет установить режим *автоматической* коррекции внутренних часов SNTP-службы маршрутизатора согласно SNTP-протоколу.

Примечание. Применение режима автоматической коррекции внутренних часов SNTP-службы маршрутизатора рекомендуется в случае использования механизма автозамены ключевых документов по графику (см. раздел 3.4, с. 122).

Для обеспечения режима коррекции следует, во-первых, включить механизм автоматической корректировки текущего времени SNTP-службы и, во-вторых, настроить параметры работы режима коррекции.

Выполнение коррекции: (Рис. 4.6). Для *включения* механизма автоматической корректировки следует в строке установить курсор на позицию в квадратных скобках – слева от параметра **наружный** и/или слева от параметра **внутренний**, после чего нажать клавишу <Enter>. При этом в указанную позицию будет занесена *звездочка* (символ «*****») и в SNTP-службе соответствующего блока маршрутизации будет установлен режим автоматической коррекции часов. Повторное нажатие клавиши < Enter > *звездочку* удалит – и режим коррекции соответствующей SNTP-службы будет отменен.

Настройка параметров (Рис. 4.6). Выбор альтернативы позволяет настроить параметры механизма коррекции текущего времени SNTP-служб, а также выполнить при необходимости корректировку текущего времени *вручную*. При выборе альтернативы на видеомонитор ЛКУ будет выдан представленный на Рис. 4.8 бланк настройки механизма корректировки текущего времени.

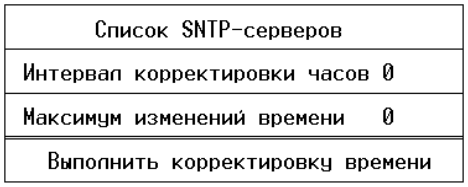


Рис. 4.8 Бланк настройки механизма корректировки текущего времени

Список SNTP-серверов (Рис. 4.8). Выбор альтернативы позволяет сформировать список IP-адресов тех SNTP-серверов, часы которых будут служить для настраиваемых SNTP-служб маршрутизаторов изделия эталоном. При выборе альтернативы на видеомонитор ЛКУ выдается экран управления списком IP-адресов SNTP-серверов, аналогичный представленному на Рис. 4.9. При этом предполагается, что в составе ЗСПД по указанным в списке IP-адресам функционируют сетевые устройства (в частности, аналогичные изделия защиты), обеспечивающие выполнение функций SNTP-серверов.

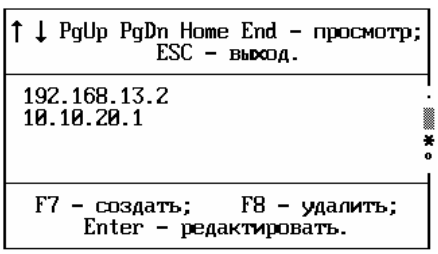


Рис. 4.9 Экран управления списком IP-адресов SNTP-серверов

F7 – **создать** (Рис. 4.9). При нажатии клавиши <F7> на видеомонитор ЛКУ выдается запрос на ввод IP-адреса SNTP-сервера, включаемого в список в качестве источника меток эталонного времени.

F8 – **удалить** (Рис. 4.9). При нажатии клавиши <F8> из списка IP-адресов SNTP-серверов удаляется строка, на которую предварительно был установлен курсор.

Enter – **редактировать** (Рис. 4.9). При нажатии клавиши <Enter> на видеомонитор ЛКУ для редактирования выдается строка с IP-адресом, на которую был установлен курсор.

Интервал корректировки часов (Рис. 4.8). Параметр позволяет определить, как часто SNTP-служба маршрутизатора изделия будет обращаться к SNTP-серверу, чтобы получить точное время по SNTP-протоколу. Значение параметра – число, указывающее интервал корректировки часов в *минутах*. Значение параметра по умолчанию - *0* (т.е. запросы на корректировку часов SNTP-службой не выдаются).

Максимум изменений времени (Рис. 4.8). Параметр позволяет определить, при какой максимальной разнице в показаниях корректируемых и эталонных часов разрешена коррекция часов по показаниям SNTP-сервера. Если разница во времени укладывается в заданное максимальное значение, то корректировка локальных часов выполняется; если не укладывается, то показания часов не изменяются и в системный журнал (файл **LOG.EMA**) заносится соответствующее сообщение. При правильно работающей системе и сравнительно небольшом *интервале корректировки часов* (порядка суток) уход часов SNTP-службы маршрутизатора изделия не превышает нескольких секунд. Значение параметра – число, указывающее максимальную величину разницы показаний часов в *секундах*. По умолчанию параметр принимает значение – ***0*** (величина разницы в показаниях локальных и эталонных часов не ограничена).

Выполнить корректировку времени (Рис. 4.8). При активизации альтернативы немедленно выполняется корректировка локальных часов SNTP-службы маршрутизатора. Коррекция выполняется по показаниям часов одного из SNTP-серверов, заданных параметром **Список SNTP-серверов**, при условии, что разница в показаниях часов не превышает значения, заданного параметром **Максимум изменения времени**, в противном случае команда выполняться не будет.

Если установлена автоматическая корректировка, то часы будут корректироваться при каждом запуске изделия, а также в процессе работы с интервалом, заданным параметром **Интервал корректировки часов** (Рис. 4.8).

Время внутреннего маршрутизатора независимо (Рис. 4.6). Этот параметр определяет алгоритм, согласно которому будет выполняться корректировка часов SNTP-службы *внутреннего* маршрутизатора изделия (БВМ). Если позиция между квадратными скобками слева от наименования параметра содержит символ «пробел», то показания часов SNTP-службы *наружного* маршрутизатора изделия передаются через шифратор на БВМ и определяют показания часов его SNTP-службы. Если по какой-либо причине требуется, чтобы время на БВМ устанавливалось автономно, то в позицию между квадратными скобками следует занести символ *звездочка* («*****»), для чего установить курсор между квадратными скобками и нажать клавишу <пробел>.

Поясное время постоянно сдвинуто на летнее (Рис. 4.6). Для того чтобы время оставалось постоянным, следует в позицию между квадратными скобками установить (см. выше) символ *звездочка* («*****»). Кроме того, необходимо отменить автоматический переход с одного времени на другое − для этого следует в поле бланка **Часовой пояс** (Рис. 4.6) в позиции между квадратными скобками слева от параметра **Автоматический переход на летнее время и обратно** убрать символ *звездочка* («*****»).

Примечание. Дополнительные сведения о работе SNTP-служб маршрутизаторов изделия приведены в разделе 0, с. 152.

*4.1.6. **Настройка ⇨ Параметры ⇨ Параметры консоли***

При выборе цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Параметры консоли** на видеомонитор ЛКУ выдается бланк настройки режима функционирования консоли управления изделием, аналогичный представленному на Рис. 4.10.

Имя узла noname	
Язык консоли Russian	Гашение экрана: Интервал 0 | Текст КМ-МПМ
Расписание перезагрузки	Восстановление нажатие клав.
Мониторинг закрытый	Раскладка клавиатуры ЯВЕРТЫ
Показ времени текущего	Стиль редактирования ДИОНИС

Рис. 4.10 Бланк настройки режима функционирования консоли управления изделием

Имя узла (Рис. 4.10). При выборе альтернативы на видеомонитор ЛКУ выдается запрос на ввод имени настраиваемого изделия. Под этим именем изделие фигурирует при удаленном управлении его работой согласно SNMP-протоколу.

Язык консоли (Рис. 4.10). Программа управления изделием поддерживает два варианта системы меню управления изделием на видеомониторе ЛКУ: вариант меню на *русском* языке (параметр имеет значение **Russian**) и вариант меню на *английском* языке (значение параметра − **English**). После запуска изделия консоль поддерживает систему меню на русском языке. Чтобы изменить значение параметра, надо установить курсор на альтернативу **Язык консоли** и нажать клавишу <Enter>. Повторное нажатие клавиши <Enter> вернет первоначальное значение параметра. Для ввода в действие изменений в параметре **Язык консоли** следует выполнить перезагрузку ОПО соответствующего маршрутизатора изделия.

> *Примечание.* Все программные компоненты изделия можно перезагрузить в любой момент, переключив средства блока ЛКУ на работу с БНМ и выбрав цепочку альтернатив ГМ: **Консоль ⇨ Выход ⇨ Завершить работу ⇨ Перезагрузить ПО** (см. раздел 8.3, с. 183).

Расписание перезагрузки (Рис. 4.10). Изделие может быть *автоматически* перезагружено в заданный администратором момент времени. Это может быть сделано, например, с целью фиксации суточной статистики или с целью архивирования данных. При выборе альтернативы на видеомонитор ЛКУ выдается таблица, представленная на Рис. 4.11; каждая ячейка таблицы соответствует одному часу одного дня недели.

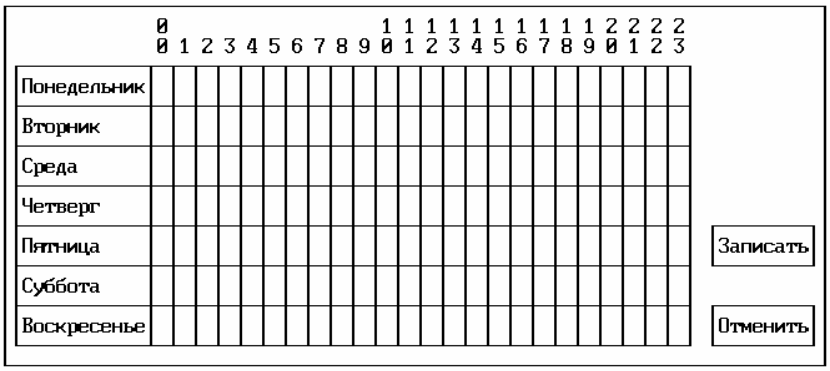


Рис. 4.11 Бланк настройки расписания автоматической перезагрузки изделия

В этой таблице следует перевести курсор на определенный час определенного дня недели и нажать клавишу <Enter> – в ответ ячейка для соответствующего часа в таблице будет отмечена символом «*****» (*звездочка*). Отметить таким образом можно любое число ячеек в таблице. В отмеченный час (часы) будет выполняться перезагрузка изделия.

Отметив все необходимые ячейки, следует переместить курсор на альтернативу бланка **Записать** и нажать клавишу <Enter>.

Если какие-либо отметки ячеек таблицы следует скорректировать, то необходимо установить курсор на отмеченную символом «*****» ячейку, после чего переместить курсор на альтернативу бланка **Отменить** и нажать клавишу <Enter> – ячейка вновь станет непомеченной.

При наступлении часа, заданного для перезагрузки, закрывается вход для новых абонентов, пользующихся услугами служб (сервисов) изделия. Если в наступивший час перезагрузки с изделием работают абоненты, то программа управления изделием ожидает 10 минут, после чего принудительно завершает сеансы работы всех абонентов и заканчивает работу изделия.

Мониторинг (Рис. 4.10). Параметр задает режим мониторинга, осуществляемого с использованием TCP-портов, и может принимать одно из следующих значений: *Открытый*, *Закрытый* или *Без пароля*. Выбор нужного режима мониторинга выполняется перемещением курсора на альтернативу **Мониторинг** (Рис. 4.10) с последующим нажатием клавиши <Enter> до той поры, пока не будет установлен нужный режим. Установленное значение параметра сохраняется после останова работы изделия. При повторном запуске изделия параметр сохраняет значение, которое было установлено последним.

Под мониторингом понимается просмотр информации, циркулирующей через TCP-порты. Если ведется открытый мониторинг (параметр имеет значение ***Открытый***), то на видеомонитор ЛКУ выдается все, что реально проходит через порт, включая имена, пароли, команды, послания и т. д. При закрытом мониторинге (параметр имеет значение ***Закрытый***) на видеомониторе ЛКУ отображается только факт прохождения информации через порт в виде двигающихся отрезков строк различного цвета, а содержательная часть проходящей информации не видна. При мониторинге со значением параметра ***Без пароля*** выполняется открытый мониторинг, за исключением моментов ввода пароля абонентом.

> *Примечание.* Чтобы включить процесс собственно мониторинга, следует выбрать альтернативу ГМ: **Интерфейсы**, в полученном списке интерфейсов (см. Рис. 2.39, с. 52) перевести курсор

на требуемый TCP-порт в списке интерфейсов и нажать клавишу <F2> для выполнения команды **мониторинг порта**.

Показ времени (Рис. 4.10). Параметр может принимать одно из трех значений: ***Текущего***, ***Работы***, ***НЕТ***. В первом случае (значение ***Текущего***) в правом нижнем углу видеомонитора ЛКУ (см. Рис. 1.9, с. 16) будет выводиться текущее время; во втором случае (значение ***Работы***) – время, прошедшее с момента запуска изделия; в третьем случае (значение ***НЕТ***) – время на экран Главного меню выводиться не будет.

Гашение экрана (Рис. 4.10). Под этим заголовком бланк содержит параметры: **Интервал**, **Текст** и **Восстановление**, характеризующих процессы, связанные с продлением срока службы видеомонитора ЛКУ.

Интервал (Рис. 4.10). Если параметру **Интервал** присвоено значение, отличное от нуля, то устанавливается режим, при котором экран видеомонитора ЛКУ в отсутствие ввода с клавиатуры гаснет через заданное значением параметра время (единица измерения – минута). При нулевом значении параметра экран видеомонитора ЛКУ не гаснет.

Восстановление (Рис. 4.10). Параметр может принимать одно из следующих значений: *Клав.+вывод*, *Нажатие клав.* и *Вывод на экран*. Выбранное значение определяет, при каких обстоятельствах экран видеомонитора ЛКУ будет выходить из погашенного состояния. При значении *Клав.+вывод* экран включится при выводе на экран информации программой управления и одновременном вводе информации с клавиатуры. При значении *Нажатие клав.* экран включится при вводе информации с клавиатуры. При значении *Вывод на экран* экран включится при выводе на него информации программой управления.

Текст (Рис. 4.10). Значением параметра может быть любой набор символов длиной до 20 символов. Указанный текст будет выводиться на погашенный экран видеомонитора ЛКУ.

Внимание! Если гашение экрана видеомонитора ЛКУ происходит в режиме Администратора (параметр **Режим** меню ГМ: **Консоль** имеет значения *Администратор узла* или *Администратор сети* – см. раздел 8.4, с. 183), то программа управления переключает процесс управления изделием на Главное меню (см. раздел 1.3.4, Рис. 1.9, с. 16) в режим **Оператор** (параметр **Режим** меню ГМ: **Консоль** имеет значение *Оператор*).

Раскладка клавиатуры (Рис. 4.10). Параметр может принимать одно из значений: *ЯВЕРТЫ* или *ЙЦУКЕН*.

После запуска изделия в зависимости от выбранного значения персоналу будет предложена та или иная раскладка клавиатуры (в регистре кириллицы). В дальнейшем для переключения на работу с необходимым вариантом раскладки клавиатуры персонал должен выполнять действия, приведенные в разделе 1.3.4, с. 14.

Программа управления изделием поддерживает *два* набора символов кириллицы: **ЯВЕРТЫ** или **ЙЦУКЕН**. Во время работы можно в любой момент переключить раскладку клавиатуры в регистре кириллицы нажатием клавиши <F10> или комбинации клавиш <Alt+F9>.

Если параметр **Раскладка клавиатуры** имеет значение *ЙЦУКЕН*, то нажатие «более удобной» клавиши <F10> будет включать кириллицу в конфигурации **ЙЦУКЕН**, а нажатие комбинации клавиш <Alt+F9> – кириллицу в конфигурации **ЯВЕРТЫ**.

Если параметр **Раскладка клавиатуры** имеет значение *ЯВЕРТЫ*, то нажатие клавиши <F10> будет включать кириллицу в конфигурации **ЯВЕРТЫ**, а нажатие комбинации клавиш<Alt+F9> – кириллицу в конфигурации **ЙЦУКЕН**.

Для установки значения параметра следует перевести курсор на параметр **Раскладка клавиатуры** и нажать клавишу <Enter>. В ответ на видеомонитор ЛКУ будет выдана таблица раскладки клавиатуры с альтернативами выбора варианта раскладки, аналогичная представленной на Рис. 4.12.

Следует переместить курсор на альтернативу с требуемым вариантом раскладки (**ЙЦУКЕН** или **ЯВЕРТЫ**) и нажать клавишу <Enter>.

Стиль редактирования (Рис. 4.10). Параметр может принимать одно из значений: ***ДИОНИС*** или ***Norton***. Он позволяет установить один из двух стилей редактирования при вводе текста с клавиатуры.

При вводе текста с клавиатуры в стиле ***ДИОНИС*** программа управления позволяет редактировать вводимый текст, используя:

- клавиши управляющих стрелок – для перемещения курсора по строке;
- клавишу <PgUp> – для вывода предыдущего значения;
- клавишу <Ins> – для вставки пробела;
- клавиши <Del>, <Bs> – для удаления символов;
- клавишу <Enter> – для фиксации значения.

При вводе текста с клавиатуры в стиле ***Norton*** имеются два отличия от работы в стиле ***ДИОНИС***:

- в окно редактирования выводится предыдущее значение параметра (функции) и курсор устанавливается в первую позицию строки; если первый вводимый с клавиатуры символ не является управляющим, то старое значение удаляется;
- клавиша <Ins> используется для переключения режима ввода символов: вставка/замена.

Рис. 4.12 Бланк выбора варианта раскладки клавиатуры в регистре кириллицы

4.1.7. *Настройка ⇨ Параметры ⇨ Параметры журналов*

При выборе цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Параметры журналов** на видеомонитор ЛКУ выдается представленное на Рис. 4.13 меню управления, позволяющее установить параметры режимов записи и просмотра файлов журналов маршрутизатора изделия (о журналах см. раздел ***Приложение Е***, с. 248).

> *Примечание.* Перевод консоли изделия в режим записи и просмотра журналов выполняется при выборе цепочки альтернатив ГМ: **Консоль ⇨ Журналы** (см. раздел 8.2, с. 181). Там же может быть временно изменено значение параметра **`Режим просмотра`**.

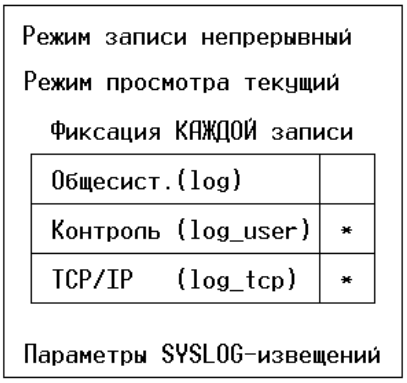


Рис. 4.13 Меню управления режимами записи и просмотра файлов журналов маршрутизатора изделия

Чтобы не допустить блокировки работы изделия из-за переполнения памяти, выделяемой под файлы журналов, существуют две возможности.

1. Своевременно переносить файлы журналов с носителей, встроенных в БВМ и БНМ, на другие (съемные) носители; при таком способе можно неограниченное время хранить неограниченное количество информации, сохраняемой в файлах журналов.
2. Ограничить размер памяти, выделяемой под файлы журналов, с потерей накопленной ранее в журналах информации.

Выбор варианта зависит от того, для чего предназначена информация, накапливаемая в файлах журналов: первый вариант необходим в случае, например, когда информация нужна для контроля (учета) работы изделия его администратором, и потеря информации является недопустимой; второй – в случае, когда информация нужна только администратору изделия для анализа текущего состояния изделия и для выполнения каких-либо настроек (другими словами, информация в журналах носит технологический характер). Какой способ записи информации в журналы будет реализован, определяется значением параметра **`Режим записи`** (Рис. 4.13).

`Режим записи` (Рис. 4.13). Выбор альтернативы приводит к выводу на видеомонитор ЛКУ меню управления режимами перезаписи журналов маршрутизатора изделия, представленного на Рис. 4.14.

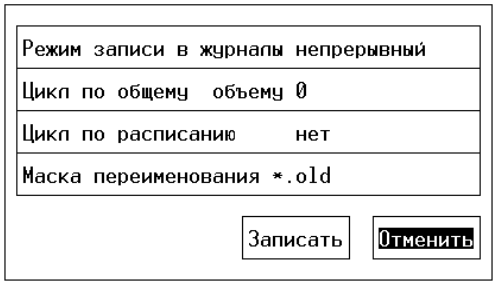


Рис. 4.14 Меню управления режимами перезаписи журналов маршрутизатора изделия

Режим записи в журналы (Рис. 4.14) – возможные значения параметра *непрерывный* или *ЦИКЛИЧЕСКИЙ*:

непрерывный – новая информация записывается в конец файла, объем файлов журналов при этом непрерывно увеличивается.

ЦИКЛИЧЕСКИЙ – новая информация записывается в журналы до тех пор, пока не будет выполнено одно из двух условий:

- суммарный объем всех журналов превысит значение, заданное параметром **Цикл по общему объему** (Рис. 4.14);
- настанет время зацикливания журналов, определенное параметром **Цикл по расписанию** (Рис. 4.14).

После выполнения любого из условий файлы журналов закрываются, переименовываются в соответствии со значением параметра **Маска переименования** (Рис. 4.14) и открываются снова.

Примечание. В ходе работы рекомендуется использовать непрерывный режим работы, при достижении файлами журналов объема в 200 МБ выполнить их экспорт на внешний носитель. При использовании циклического режима работы в обязательном порядке указывать маску имени и путь для сохранения переименованных файлов журналов на диске D:, например: d:\dioniswt.dat\logs*.old

Цикл по общему объему (Рис. 4.14). Параметр определяет максимальный суммарный объем файлов журналов маршрутизатора изделия (в Мегабайтах), возможные значения: ***0-2048***.

Цикл по расписанию (Рис. 4.14). При выборе параметра на видеомонитор ЛКУ будет выдан бланк настройки расписания выполнения регламентных работ на файлах журналов маршрутизатора изделия, аналогичный представленному на Рис. 4.11, с. 138. Используя предоставленные бланком возможности, следует с помощью управляющих стрелок перевести курсор на определенный час определенного дня недели и нажать клавишу <Enter> – этот час будет отмечен символом «*». Так отметить можно любое число ячеек бланка. В отмеченный час (часы) все файлы журналов соответствующего блока маршрутизации будут закрыты, переименованы и открыты вновь.

Маска переименования (Рис. 4.14). Параметр служит для определения имен *копий* файлов журналов маршрутизатора, создаваемых при сохранении содержимого ранее заполненных файлов журналов. Значением параметра должна быть *маска*, используемая при составлении имен копий файлов журналов, в которых будет храниться информация из ранее заполненных журналов.

При формировании маски имя файла журнала (основная часть имени без расширения) представляется символом «*****», который должен присутствовать обязательно. В маске можно использовать следующие макросы (имя макроса в маске должно быть заключено в фигурные скобки):

имя	значение	
ss	секунды (00 - 59)	Время начала зацикливания журналов
nn	минуты (00 - 59)	
hh	часы (00 - 23)	
dd	день (01 - 31)	Дата начала зацикливания журналов
mm	месяц (01 - 31)	
yy	год (00 - 99)	
yyyy	год (2000 -)	
alogs	Значение переменной окружения ALOGS	

Пример 1: маска **c:\logsarch\{yy}-{mm}-{dd}\{hh}_{nn}_{ss}*.ema**

При зацикливании системного журнала **LOG.EMA** будет создан файл

c:\logsarch\00-09-14\14_00_00\log.ema

Предварительно будет создана директория **c:\logsarch\00-09-14\14_00_00**.

Пример 2: маска **c:\logsarch*.old**

При наличии такой маски будет храниться одна – последняя – группа копий файлов журналов.

Режим просмотра (Рис. 4.13). Параметр определяет, какая часть информации из файла журнала будет выдаваться на видеомонитор ЛКУ, когда консоль будет переведена в режим просмотра файлов журналов.

Выбор альтернативы **Режим просмотра** приводит к выводу на экран представленного на Рис. 4.15 меню управления режимом просмотра файла журнала маршрутизатора изделия.

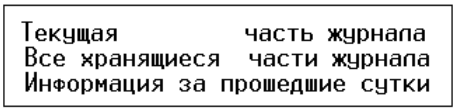


Рис. 4.15 Меню управления режимом просмотра журнала маршрутизатора изделия

С помощью этого меню (Рис. 4.15) можно присвоить одно из следующих значений параметру **Режим просмотра**: *текущий* (**Текущая часть журнала**), *архив* (**Все хранящиеся части журнала**), *за сутки* (**Информация за прошедшие сутки**). Для выбора режима просмотра следует установить курсор на строку меню, соответствующую требуемому значению, и нажать клавишу <Enter>.

Фиксация КАЖДОЙ записи (Рис. 4.13). Таблица под этим заголовком позволяет выбрать *класс* (*классы*) событий, информация о которых может представлять особый интерес: это *общесистемные* события (параметр **Общесист.(LOG)**), *контрольные* события (параметр **Контроль(LOG_USER)**) и события, связанные с работой *компонента TCP/IP* (параметр **Контроль(LOG_TCP)**). При наличии символа «*» (*звездочка*) в правой клеточке таблицы справа от выбранного класса устанавливается такой режим, при котором каждое событие соответствующего класса *немедленно* фиксируется в соответствующем файле журнала. Отсутствие *звездочки* этот режим отключает. При этом уменьшается нагрузка на УВП изделия, но возникает риск потери информации при зависании системы или в случае сбоя питания. При отключенном режиме фиксации каждой записи информация в файлы журналов будет заноситься, но только по мере заполнения соответствующего буфера.

Параметры SYSLOG-извещений (Рис. 4.13). При выборе этой альтернативы меню программа управления выдает на видеомонитор ЛКУ экран управления списком получателей SYSLOG-извещений (SYSLOG-серверов, ретрансляторов или коллекторов согласно RFC3164), аналогичный представленному на Рис. 4.16. Если настройка списка получателей SYSLOG-извещений ранее не выполнялась, то экран не содержит их описателей.

Под заголовками **Адрес** и **Порт** выведены, соответственно, *IP-адрес* и *порт* приложения-получателя того SYSLOG-сервера, по адресу (сокету) которого будут посылаться SYSLOG-извещения; под заголовком **Прт** – протокол передачи извещений; под заголовком **Очередь** – количество не отправленных SYSLOG-извещений.

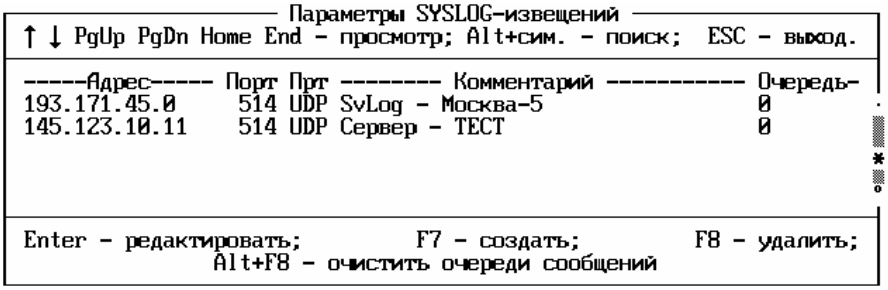


Рис. 4.16 Экран управления списком SYSLOG-серверов

Подсказки в нижней части экрана (Рис. 4.16) информируют о командах, позволяющих управлять списком описателей параметров SYSLOG-серверов и состоянием очередей с SYSLOG-извещениями.

Enter – редактировать (Рис. 4.16). При нажатии клавиши <Enter> на видеомонитор ЛКУ выводится бланк создания и настройки описателя получателя SYSLOG-извещений, аналогичный представленному на Рис. 4.17, позволяющий просмотреть и, при необходимости, изменить параметры указанного курсором описателя параметров SYSLOG-сервера. Кроме того, можно просмотреть и уточнить список *типов* SYSLOG-извещений, которые будут отправляться данному получателю – SYSLOG-серверу.

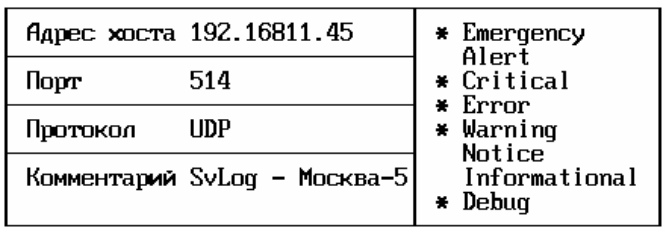


Рис. 4.17 Бланк создания и настройки описателя получателя SYSLOG-извещений

Полный список типов сообщений протокола SYSLOG (в соответствии с классификацией их уровней согласно RFC3164) приведен в правой части бланка. На указанный сервер будут отправлены сообщения тех типов, которые будут отмечены в списке слева от наименования типа символом «*» (*звездочка*).

Чтобы включить в состав отправляемых SYSLOG-извещений тот или иной тип, следует перевести курсор на строку с описанием этого типа и нажать клавишу <Enter> – в ответ появится отметка в виде символа «*». Повторное нажатие клавиши отметку уберет.

F7 – создать (Рис. 4.16). При нажатии клавиши <F7> на экран выводится бланк, аналогичный представленному на Рис. 4.17, позволяющий создать новый описатель получателя SYSLOG-извещений.

F8 – удалить (Рис. 4.16). При нажатии клавиши <F8> без дополнительных запросов из списка будет удален указанный курсором описатель получателя SYSLOG-извещений.

Alt+F8 – очистить очереди сообщений (Рис. 4.16). При нажатии клавиш <Alt+F8> будут удалены сформированные ранее SYSLOG-извещения, не отправленные на выбранный сервер на момент выдачи команды.

4.1.8. *Настройка ⇨ Параметры ⇨ Архив конфигураций*

Примечание. Работы по формированию (настройке) и сохранению *конфигуратора* изделия, его импортированию и экспортированию с применением съемных носителей и пр. выполняются с использованием средств блока ЛКУ, подключенных *только* к блоку наружной маршрутизации.

Общие сведения об архитектуре управления изделием, о роли *конфигуратора* изделия в процессах *локального* и *удаленного* управления изделиями приведены в разделе 1.3, с. 9 настоящего РНУ.

Напомним, что конфигурацией (конфигуратором) изделия мы называем всю совокупность параметров настройки компонентов изделия, хранящуюся в объединенной базе параметров (**БпО**) в энергонезависимой памяти шифратора и полностью определяющую режим функционирования изделия.

В целях выполнения операций сохранения различных модификаций конфигуратора изделия и сопровождения *архива* конфигураций изделия внутри самого изделия, для оперативного обмена конфигураторами между изделиями через съемные машинные носители, для удаленного управления изделиями с применением средств ЦУА и пр. применяется конфигуратор изделия в виде *набора двоичных файлов*. В технологии DioNIS® реализована возможность работы с этими файлами как с самостоятельным множеством параметров: конфигуратор целиком можно сохранить в архиве, можно перенести на внешний съемный носитель и, при необходимости, оперативно ввести в действие с этого носителя на другом (например, *резервном*) изделии.

Выпущенное предприятием-изготовителем изделие поставляется заказчику, как правило, с определенными параметрами настройки – с т.н. *заводским* конфигуратором. Конкретный набор значений параметров заводского конфигуратора зависит от назначения изделия. Кроме того, предприятие-изготовитель может выполнить настройку на определенные типовые схемы применения изделия и занести соответствующие схемам варианты конфигураторов в архив конфигураций. Наличие архива позволяет на местах эксплуатации изделий сэкономить время, воспользовавшись готовым набором конфигураторов различной модификации из архива.

При выборе цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Архив конфигураций** на видеомонитор ЛКУ выдается представленный на Рис. 4.18 экран управления архивом конфигураций изделия. Средняя часть экрана содержит список описателей ранее сохраненных в архиве конфигураций изделия. Каждая строка содержит сведения о конфигурации в колонках: **Имя**, **Дата**, **Время** и **Комментарий**.

Примечание. Под именем DEFAULT на Рис. 4.18 представлен описатель конфигуратора заводских настроек, включающий описатели сетевых интерфейсов изделия типа **Ethernet** для каждого *порта* всех сетевых Ethernet-адаптеров, которыми оснащено изделие. Используя этот описатель можно, при необходимости, восстановить первоначальные настройки изделия. Отметим, что описатель с системным именем DEFAULT из архива конфигураций удалить нельзя.

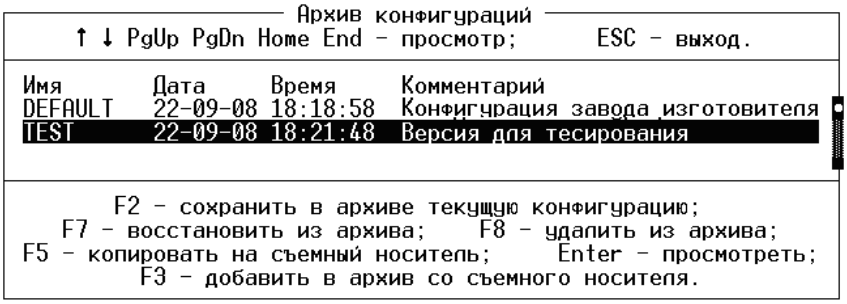


Рис. 4.18 Экран управления архивом конфигураций изделия

Нижняя часть экрана содержит команды сопровождения архива, которые может выполнить администратор.

F2 – сохранить в архиве текущую конфигурацию (Рис. 4.18). С помощью этой команды администратор может в любой момент занести текущую конфигурацию в архив. Архив, как правило, содержит заводскую конфигурацию, а также может содержать дополнительные, помещенные в архив администратором изделия.

При нажатии клавиши <F2> на экран выдается представленный на Рис. 4.19 бланк оформления записи в архив текущей конфигурации изделия.

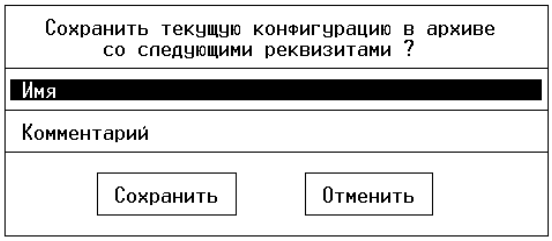


Рис. 4.19 Бланк оформления записи в архив текущей конфигурации изделия

Имя (Рис. 4.19). В графу бланка следует ввести произвольный набор до восьми алфавитно-цифровых символов, причем буквы допускаются только из *латинского* алфавита.

Комментарий (Рис. 4.19). В графу бланка можно ввести до 32 символов произвольного текста.

Присвоив конфигурации имя и снабдив ее комментарием, следует выдать команду на запись конфигурации в архив − переместить курсор в бланке на альтернативу **Сохранить** и нажать клавишу <Enter>. Текущая конфигурация изделия будет занесена в архив.

Примечания.

1. При записи конфигурации в архив создается папка с именем, совпадающим с заданным именем конфигурации (именно поэтому ввод значения параметра **Имя** (Рис. 4.19) выполняется в *латинском* регистре); сама папка размещается в папке **D:\DIONISWT.CFG**, содержащей архив всех конфигураций изделия.
2. Возможностью сохранения текущей конфигурации целесообразно пользоваться, например, в тех случаях, когда предполагается внесение значительных изменений и нет уверенности, что после модификации изделие сохранит свою работоспособность.

F3 – добавить в архив со съемного носителя (Рис. 4.18). Команда позволяет добавить конфигурацию изделия (не обязательно собственную) в архив, прочитав ее с внешнего съемного носителя. Перед выполнением команды съемный носитель следует установить в считывающее устройство.

После нажатия клавиши <F3> на видеомонитор ЛКУ выдается представленный на Рис. 4.20 бланк оформления записи конфигурации в архив со съемного носителя; в бланке следует указать имя конфигурации (до 8 символов) с комментарием (до 32 символов произвольного текста).

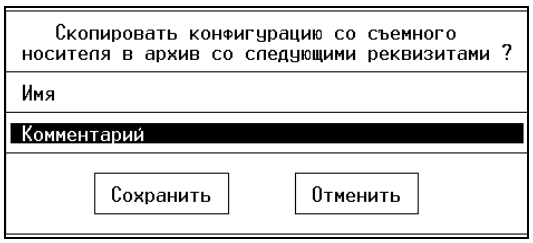


Рис. 4.20 Бланк оформления записи конфигурации в архив со съемного носителя

Присвоив конфигурации имя и снабдив ее комментарием, следует выдать команду на запись конфигурации в архив − переместить курсор в бланке на альтернативу **Сохранить** и нажать клавишу <Enter>. В ответ программа управления выдаст на видеомонитор ЛКУ экран выбора съемного носителя, аналогичный представленному на Рис. 4.21.

Рис. 4.21 Экран выбора съемного носителя

В верхней части экрана выводится и в круглых скобках количество подключенных съемных носителей (после выбора носителя − число элементов в его файловой структуре) и текущий путь для размещения конфигурации

В средней части экрана (Рис. 4.21) выводится номер (описатель) съемного носителя − FLASH-диска, подключенного к USB-порту. В общем случае описателей может быть несколько.

Администратор должен перевести курсор на описатель съемного носителя и нажать клавишу <Enter>. На видеомонитор ЛКУ будет выдан экран с файловой структурой съемного носителя. На этом экране надо выбрать директорию, откуда должна будет считываться конфигурация, и нажать клавишу <F2>, после чего следует проконтролировать завершение процедуры копирования конфигурации со съемного носителя в архив конфигураций.

F7 – восстановить из архива (Рис. 4.18). Любая из конфигураций, сохраненных в архиве, может быть восстановлена в качестве *текущей* конфигурации изделия. Для восстановления надо в списке описателей конфигураций (Рис. 4.18) переместить курсор на нужную и нажать клавишу <F7>. После чего будет выдан запрос, представленный на Рис. 4.22.

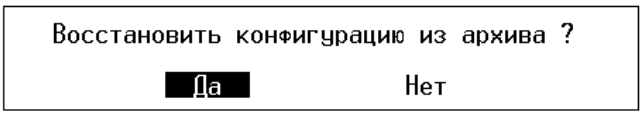
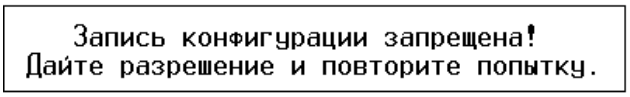


Рис. 4.22 Запрос на подтверждение замены текущей конфигурации изделия на конфигурацию из архива

После подтверждения (ответа *Да*) программа управления потребует выдать разрешение на запись конфигурации в память шифратора изделия, предупредив администратора следующим сообщением:



Разрешение должен дать администратор изделия соответствующей командой шифратора (процедура выдачи разрешения приведена в РЭ на конкретное изделие). После получения разрешения программа управления выполнит процедуру замены и выдаст сообщение, приведенное на Рис. 4.23. Чтобы новая конфигурация вступила в действие, следует выполнить предписанные сообщением действия и перезапустить изделие.

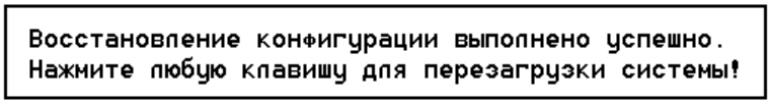


Рис. 4.23 Сообщение о замене текущей конфигурации

F8 – удалить из архива (Рис. 4.18). Для удаления конфигурации из архива следует в списке описателей конфигураций (Рис. 4.18) переместить курсор на нужную и нажать клавишу <F8>. После дополнительного запроса и подтверждения выбранный описатель из архива будет удален.

Некоторые из конфигураций удалять не разрешается. Запрет устанавливается на предприятии-изготовителе. В частности, как правило, нельзя удалить заводскую конфигурацию.

F5 – копировать на съемный носитель (Рис. 4.18). Команда предоставляет возможность копирования любой сохраненной в архиве конфигурации на съемный носитель.

Перед выдачей команды на копирование надо подключить съемный носитель к USB-устройству чтения-записи.

Чтобы получить копию, следует в списке описателей конфигураций (Рис. 4.18) переместить курсор на нужную и нажать клавишу <F5>.

Программа управления выдаст на видеомонитор ЛКУ экран выбора съемного носителя, аналогичный представленному на Рис. 4.21. На этом экране следует выбрать носитель и указать директорию, куда при копировании будет помещен конфигуратор изделия. При необходимости директорию можно создать с помощью клавиши **<F7> – создание директории**. Подготовив или выбрав необходимую директорию, следует нажать клавишу <F2> – в ответ программа управления скопирует конфигурацию как набор файлов и сделает соответствующую запись в системный журнал.

Съемный носитель с копией конфигурации можно установить на другом изделии и восстановить на нем конфигурацию в качестве текущей, полностью совпадающей с исходной.

Enter – просмотреть (Рис. 4.18). Предусмотрена возможность просмотра набора файлов, составляющих конфигурацию изделия. Для просмотра следует выбрать строку с описателем интересующего варианта конфигурации и нажать клавишу <Enter>.

4.2. Настройка ⇨ Разное

В ответ на выбор цепочки альтернатив ГМ: **Настройка ⇨ Разное** на видеомонитор ЛКУ выдается представленное на Рис. 4.24 меню настройки дополнительных параметров TCP/IP-компонента маршрутизатора изделия.

Рис. 4.24 Меню настройки дополнительных параметров TCP/IP-компонента маршрутизатора изделия

Далее в настоящем подразделе РНУ приведены пояснения, необходимые для правильной настройки этих параметров.

4.2.1. *Настройка ⇨ Разное ⇨ ARP-таблица*

Общие сведения об ARP-таблицах

Необходимость применения в `internet/intranet`-технологии ARP-протокола продиктована тем, что *сетевые* IP-адреса устройств в сети назначаются независимо от их *физических* MAC-адресов. Поэтому для доставки данных по сети необходимо определить *соответствие* между физическим адресом устройства (MAC-адресом) и его сетевым (логическим) адресом (IP-адресом). Процесс определения этого соответствия называется *разрешением* адресов и осуществляется с помощью ARP-протокола (Address Resolution Protocol).

ARP-протокол − специальный универсальный протокол определения соответствия физических и логических адресов − необходим в `internet/intranet`-технологии, так как прикладные программы, как правило, при отправке данных для адресации используют не MAC-адреса, а IP-адреса. Иногда приложения используют для адресации возможности DNS-серверов, с помощью которых структурированный текстовый адрес получателя в конечном итоге переводится в IP-адрес (подробнее о DNS-службе см. раздел ***Приложение Д***, с. 243). Схемы же физической адресации устройств весьма разнообразны.

Функционально ARP-протокол состоит из двух частей: одна часть протокола – клиентская – определяет физические адреса при отправке датаграммы, выдавая собственные ARP-запросы соответствующего интерфейса изделия, другая – серверная – отвечает на ARP-запросы других сетевых устройств, сообщая им свой IP-адрес. В `internet/intranet`-технологии предполагается, что любое сетевое устройство знает как свой *собственный IP-адрес*, так и свой физический *MAC-адрес*.

> *Примечание.* Подробнее об ARP-протоколе см. RFC 826 и раздел настоящего РНУ ***Приложение А***, с. 214.

Чтобы снизить количество посылаемых в сеть ARP-запросов, в устройстве, использующем ARP-протокол, должна быть организована работа со специальной *буферной* памятью, в которой хранятся записи о парах адресов – соответствующих друг другу IP-адреса и MAC-адреса одного сетевого устройства. Всякий раз, когда устройство получает ответ на свой ARP-запрос, программа управления сохраняет в этой памяти соответствующую пару адресов. Такая буферная память изделия называется *ARP-таблицей*. Если при подготовке данных к отправке в сеть MAC-адрес, соответствующий IP-адресу назначения, имеется в ARP-таблице, нет необходимости посылать ARP-запрос на определение MAC-адреса.

ARP-таблица используется при отправке интерфейсом изделия IP-датаграмм, адресованных станциям локальной сети, к которой этот интерфейс подключен. Для адресации передаваемых по сетям на канальном (L2) уровне Ethernet-кадров используется 48-битный *физический канальный* адрес – MAC-адрес. При подготовке принятых по `internet/intranet`-сети IP-датаграмм с *межсетевым* 32-битным IP-адресом к отправке в виде кадров в локальную Ethernet-сеть требуется *преобразование* 32-битного *IP-адреса* принятой IP-датаграммы в 48-битный *MAC-адрес* отправляемых в Ethernet-сеть кадров, которое и выполняется компонентами поддержки ARP-протокола для каждой проходящей через интерфейс IP-датаграммы с помощью ARP-таблицы соответствующего маршрутизатора изделия.

ARP-таблица может состоять из *двух* частей и включать как *динамические* (вносимые в таблицу программой управления автоматически), так и *статические* (вносимые в таблицу администратором изделия вручную) записи пар соответствующих адресов устройств. Динамические записи не только добавляются, но и удаляются автоматически, исчерпав свое «*время жизни*».

Настройка ARP-таблицы

При выборе цепочки альтернатив ГМ: **Настройка ⇨ Разное ⇨ ARP-таблица** на видеомонитор ЛКУ выдается меню управления списком *статических* записей ARP-таблицы маршрутизатора (Рис. 4.25).

Записи определяют соответствие *IP-адресов* хостов и абонентских станций *MAC-адресам* этих хостов и абонентских станций, находящихся в одной локальной Ethernet-сети с маршрутизатором изделия, подключенным к ней через соответствующий интерфейс.

Меню управления (Рис. 4.25) позволяет администратору изделия сформировать и при необходимости отредактировать статическую часть ARP-таблицы.

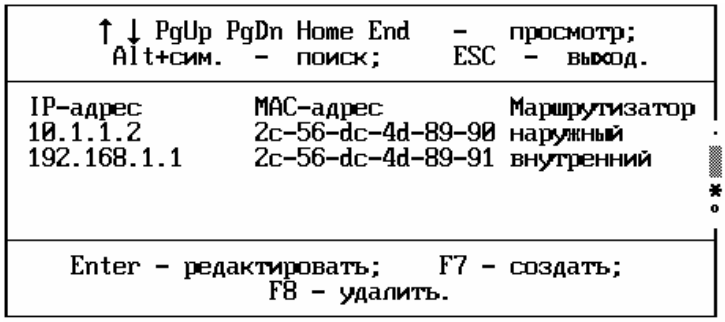


Рис. 4.25 Меню управления списком статических записей ARP-таблицы маршрутизатора

Описание адресов доступа (логического и физического) к каждому из IP-устройств сети в ARP-таблице занимает одну строку. В строке слева направо сначала записывается IP-адрес сетевого устройства, затем физический адрес (MAC-адрес) соответствующего *порта* Ethernet-адаптера, через который физический интерфейс изделия (типа **Ethernet** или **L2-Eth**) подключен к локальной сети, а затем – принадлежность к маршрутизатору изделия (внутреннему или наружному).

Описание возможных действий администратора с помощью меню управления списком статических записей ARP-таблицы маршрутизатора приведено ниже.

F7 – создать (Рис. 4.25). После нажатия клавиши <F7> на видеомонитор ЛКУ выводится представленный на Рис. 4.26 бланк создания и настройки статической записи ARP-таблицы маршрутизатора; бланк предоставляет возможность задать требуемые значения параметров записи ARP-таблицы (IP-адрес, MAC-адрес и маршрутизатор, которому принадлежит сетевой интерфейс).

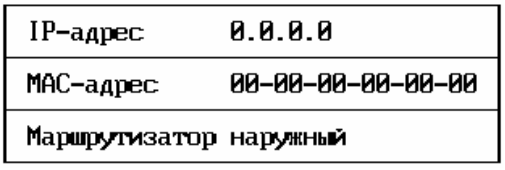


Рис. 4.26 Бланк создания и настройки статической записи ARP-таблицы маршрутизатора

Enter – редактировать (Рис. 4.25). После нажатия клавиши <Enter> на видеомонитор ЛКУ выводится тот же бланк, аналогичный представленному на Рис. 4.26, содержащий, возможно, ранее введенные администратором значения параметров статической записи ARP-таблицы, и предоставляется возможность эти значения скорректировать.

F8 – удалить (Рис. 4.25). После запроса на подтверждение удаления и положительного ответа строка, на которой установлен курсор, из ARP-таблицы удаляется.

Примечание. Наличие рационально заполненной ARP-таблицы позволяет избежать широковещательных ARP-запросов в Ethernet-сеть с целью определения MAC-адреса IP-устройства, соответствующего занесенному в таблицу IP-адресу.

Администраторам, не имеющим достаточного опыта, не рекомендуется создавать и редактировать записи ARP-таблицы.

4.2.2. *Настройка ⇨ Разное ⇨ Таблица адресов*

При выборе цепочки альтернатив ГМ: **Настройка ⇨ Разное ⇨ Таблица адресов** на видеомонитор ЛКУ выдается меню управления списком записей *таблицы доменных адресов* маршрутизатора, аналогичное представленному на Рис. 4.27. Меню позволяет создать и отредактировать эту таблицу.

Примечание. Таблица доменных адресов используется DNS-службой маршрутизатора изделия (см. раздел 5.4, с. 157) для хранения статических описателей соответствия IP-адресов доменным именам хостов.

Каждый элемент занимает в списке одну строку: под заголовком **Адрес** записывается IP-адрес узла и под заголовком **Имя домена** – мнемоническое имя узла. Подсказки в нижней части таблицы информируют об управляющих действиях, которые можно выполнить с помощью этого меню.

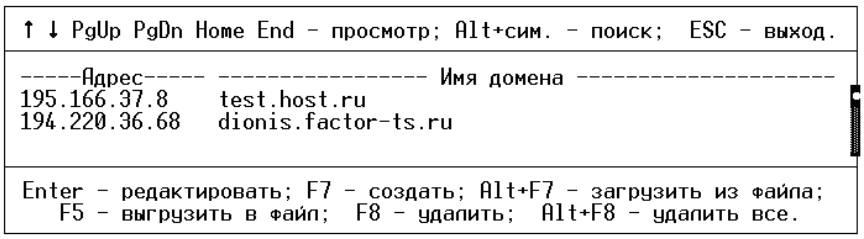


Рис. 4.27 Меню управления списком записей таблицы доменных адресов маршрутизатора

F7 – создать (Рис. 4.27). После нажатия клавиши <F7> на видеомонитор ЛКУ будет выдан представленный на Рис. 4.27 бланк ввода параметров записей таблицы доменных адресов, позволяющий ввести нужный IP-адрес и имя соответствующего IP-адресу домена.

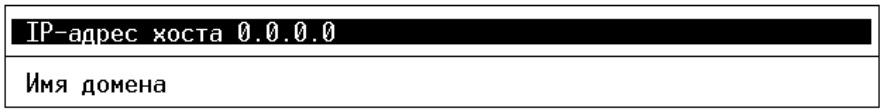


Рис. 4.28 Бланк ввода параметров записей таблицы доменных адресов

Закончив ввод данных, надо нажать клавишу <Esc> – заданные значения будут занесены в адресную таблицу.

Enter – редактировать (Рис. 4.27). При нажатии клавиши <Enter> будет выдано такое же меню, как и при создании элемента адресной таблицы (Рис. 4.28), но с ранее присвоенными значениями параметров; при этом предоставляется возможность эти значения изменить.

F8 - удалить (Рис. 4.27). После запроса на подтверждение удаления и положительного ответа строка с элементом, на которой установлен курсор, из таблицы удаляется.

Alt+F8 - удалить все (Рис. 4.27). После запроса на подтверждение удаления и положительного ответа удаляются все строки таблицы адресов.

F5 - выгрузить в файл (Рис. 4.27). Вся таблица адресов преобразуется в текстовый формат и записывается в файл. Предварительно программа управления запрашивает имя файла.

Alt+F7 - загрузить из файла (Рис. 4.27). Программа управления запрашивает имя файла и добавляет к существующей таблице строки из указанного текстового файла.

4.2.3. *Настройка ⇨ Разное ⇨ PIng-пробы*

При выборе цепочки альтернатив ГМ: **Настройка ⇨ Разное ⇨ PIng-пробы** на видеомонитор ЛКУ выдается представленный на Рис. 4.29 запрос о выборе маршрутизатора изделия – БНМ или БВМ, для которого предстоит создать (настроить) PING-пробу.

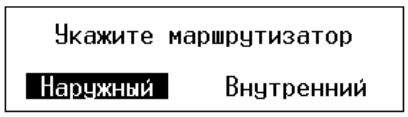


Рис. 4.29 Запрос на принадлежность процессов PING-проб соответствующему маршрутизатору

Примечание. Подробнее о механизме PING-проб, поддерживаемом изделием с целью автоматизации управления сетевыми ресурсами, см. раздел 2.7, с. 58.

После выбора маршрутизатора на видеомонитор ЛКУ выдается меню управления списком описателей процессов PING-проб для выбранного маршрутизатора, аналогичное представленному на Рис. 4.30.

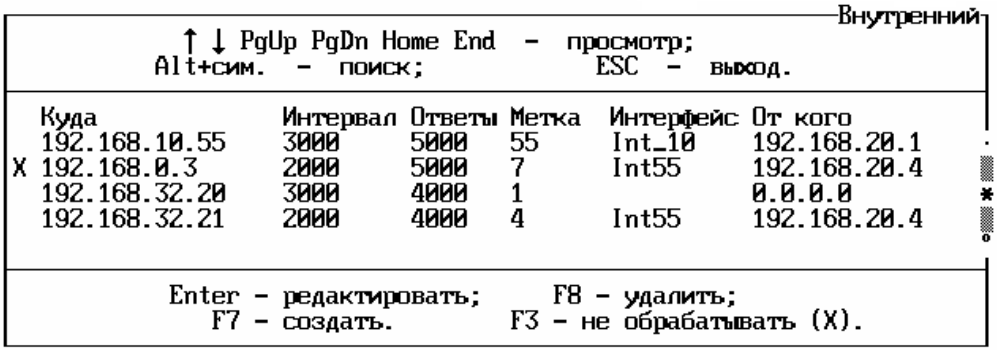


Рис. 4.30 Меню управления списком описателей процессов PING-проб

Ниже приведено описание возможностей управления описателями процессов PING-проб с использованием этого меню.

F7 – **создать** (Рис. 4.30). После нажатия клавиши <F7> на видеомонитор ЛКУ выдается представленный на Рис. 4.31 бланк ввода параметров описателя процесса PING-проб. В этом бланке для трех параметров **Интервал отправки**, **Ожидание ответа** и **Метка маршрута** выводятся значения, которые эти параметры имеют по умолчанию, соответственно: **2000**, **4000** и **1**. Значения могут быть скорректированы в процессе создания описателя PING-пробы.

Куда 0.0.0.0
Интервал отправки 2000
Ожидание ответа 4000
Метка маршрутов 1
Имя интерфейса
Шлюз 0.0.0.0
От кого 0.0.0.0

Рис. 4.31 Бланк ввода параметров описателя процесса PING-проб

Куда (Рис. 4.31) – IP-адрес удаленного сетевого устройства, тракт передачи данных с которым подлежит контролю с помощью PING-пробы.

Интервал отправки (Рис. 4.31) – интервал времени (в миллисекундах), через который осуществляется отправка ICMP-пакетов PING-пробы в адрес контролируемого узла сети.

Ожидание ответа (Рис. 4.31) – интервал времени (в миллисекундах), в течение которого изделие ожидает ответа от контролируемого узла (рекомендуется указывать значение интервала, как минимум, на 10% больше интервала отправки ICMP-пакетов PING-проб). Если ответ не придет в указанное этим параметром время, программа управления считает, что проверяемый узел не работает, и фиксирует состояние *отказа* PING-пробы, после чего увеличивает счетчик отказов.

Метка маршрутов (Рис. 4.31) – целое десятичное число в диапазоне от ***0*** до ***255***. Этот параметр необходим:

- для установления взаимосвязи (*привязки*) данной PING-пробы и конкретного проверяемого маршрута (значение метки содержится в записях соответствующей таблицы маршрутизации – см. раздел 2.3, с. 25);
- для установления взаимосвязи (*привязки*) данной PING-пробы и туннеля (туннелей) – см. раздел 3.1.1, с. 76.

Имя интерфейса (Рис. 4.31) – имя интерфейса, через который выполняется отправка PING-пробы; если **имя интерфейса** не указано, то PING-проба отправляется через маршрутную таблицу маршрутизатора (на общих основаниях).

Шлюз (Рис. 4.31) – IP-адрес того шлюза, через который должно быть доступно сетевое устройство, доступ к которому держим на контроле.

От кого (Рис. 4.31) – обычно указывается IP-адрес того интерфейса, через который отправляется PING-проба (задавать параметр не обязательно).

Enter – **редактировать** (Рис. 4.30). После нажатия клавиши <Enter> на экран выводится меню, аналогичное представленному на Рис. 4.31, содержащее ранее установленные значения параметров, и предоставляется возможность эти значения отредактировать.

F8 – **удалить** (Рис. 4.30). При нажатии клавиши <F8> без дополнительного запроса удаляется строка с описателем PING-пробы, на которой установлен курсор.

F3 – **не обрабатывать (X)** (Рис. 4.30). Нажатие клавиши <F3> позволяет временно отключить выполнение PING-пробы, на описатель которой установлен курсор, без удаления этого описателя из списка. При временном отключении PING-пробы в левой позиции строки с ее описателем появится символ «**X**» (на Рис. 4.30 временно отключена PING-проба по адресу **192.168.32.20**). При повторном нажатии клавиши <F3> PING-проба возобновляет контроль тракта, при этом символ «**X**» в левой позиции ее описателя исчезает.

4.2.4. *Настройка ⇨ Разное ⇨ Параметры LLDP*

При выборе цепочки альтернатив ГМ: **Настройка ⇨ Разное ⇨ Параметры LLDP** на видеомонитор ЛКУ выдается бланк настройки режима работы процессов передачи/приема анонсов при LLDP-взаимодействии, аналогичный представленному на Рис. 4.32.

Изделие может согласно протоколу LLDP выполнять автоматическую рассылку своего анонса (оповещать устройства в локальной сети о своем существовании и характеристиках) и прием анонсов соседних сетевых устройств (таких же оповещений, поступающих от соседнего сетевого оборудования). Механизм автоматической рассылки и приема анонсов включается при установке соответствующих значений параметрам **LLDP-рассылка** и **LLDP-прием** в бланке управления специальными настройками интерфейса (см. раздел 2.5, Рис. 2.38, с. 50).

Время жизни	120
Интервал рассылки	60
Задержка рассылки	0

Рис. 4.32 Бланк настройки режима работы процессов передачи/приема анонсов при LLDP-взаимодействии

С помощью бланка (Рис. 4.32) выполняется настройка параметров процессов передачи/приема анонсов при LLDP-взаимодействии.

Время жизни (Рис. 4.32) – параметр задает время (в секундах), в течение которого принятые анонсы хранятся изделием.

Интервал рассылки (Рис. 4.32) – период времени (в секундах) между отправками изделием анонсов.

Задержка рассылки (Рис. 4.32) – время (в секундах) между концом передачи изделием предыдущей рассылки анонса до начала следующей.

5. Настройка служб

В составе каждого из блоков маршрутизации (БНМ и БВМ) изделия реализован сервер приложений – *сервер обработки прикладных протоколов* – набор служб (прикладных сервисов), предоставляющих другим компонентам изделия, а также внешним абонентам различные информационные услуги.

Перечень всех служб (сервисов), поддерживаемых маршрутизаторами изделия, приведен в таблице:

Служба (сервис)	Назначение	Раздел РНУ
DCP	обеспечение удаленного (по защищенным каналам связи) управления работой изделий с помощью аналогичных изделий, работающих в режиме **Администратор сети**	5.1
SNTP	служба времени – обеспечение функционирования SNTP-службы	5.2
SNMP	обеспечение функционирования агента сбора статистики и удаленного управления работой изделия согласно протоколу SNMP	5.3
DNS	поиск в базе данных доменной системы имен для получения IP-адреса по имени хоста	5.4
DHCP	обеспечение автоматической настройки параметров взаимосвязи изделия с рабочими станциями абонентов и другими сетевыми устройствами	5.5
Telnet	обеспечение доступа абонентов IP-сети к сервисам изделия в терминальном режиме	5.6
RIP	обеспечение динамического сопровождения маршрутных таблиц изделия согласно протоколам динамической маршрутизации RIP v.1, RIP v.2, RIP-98	5.7

Все службы (сервисы) работают на уровне прикладных задач маршрутизатора изделия и обмениваются информацией с маршрутизаторами через внутренний (служебный) интерфейс соответствующего маршрутизатора (см. раздел 2.1, с. 19).

Доступ к службам маршрутизаторов изделия возможен по любому из следующих IP-адресов:

- собственный IP-адрес БНМ или БВМ изделия (раздел 4.1.2, с. 130),
- локальный IP-адрес любого из сетевых активных интерфейсов соответствующего маршрутизатора изделия (раздел 2.3, с. 25).

Работа служб изделия реализована по стандартной для Internet технологии *клиент-сервер*. Серверный компонент каждой службы (при наличии разрешения администратора на его запуск) активизируется при запуске изделия и ожидает запросов от клиентской части службы. Получив запрос, серверный компонент службы выполнит необходимые прикладные действия и сформирует ответ клиенту.

Часть служб (Telnet, SNMP, DHCP) имеет только серверные компоненты и обслуживает только внешних абонентов изделия. Остальные службы (DCP, SNTP, DNS, RIP) имеют и серверные, и клиентские компоненты. Эти службы могут сами обслуживать внешних абонентов, а также запрашивать у внешних информационных служб сервис, необходимый для внутренних компонентов и внешних абонентов.

Настройка и управление службами каждого из маршрутизаторов изделия осуществляется путем переключения средств ЛКУ к требуемому маршрутизатору изделия и выбора цепочки альтернатив ГМ: **Настройка ⇨ Службы**. На видеомонитор ЛКУ выводится представленное на Рис. 5.1 меню управления запуском служб маршрутизатора, содержащее перечень служб, поддерживаемых соответствующим маршрутизатором изделия. Настройка разрешений на запуск служб выполняется для каждого блока маршрутизации отдельно.

			Внутренний		
Служба	Порт	Пуск	Служба	Порт	Пуск
DCP	362	Да	Telnet	23	Да
SNTP	123	Нет	RIP	520	Нет
SNMP	161	Нет	OSPF	ip89	Нет
DNS	53	Нет	BGP	179	Нет
DHCP	67,68	Нет			Нет

Рис. 5.1 Меню управления запуском служб маршрутизатора

Примечание. Использование служб OSPF и BGP настоящей версией ОПО не поддерживается.

В представленном на Рис. 5.1 меню в колонках под заголовком **Служба** размещаются аббревиатуры названий служб; в колонках под заголовком **Порт** – номера (идентификаторы) портов (TCP или UDP), приписанных каждой службе стандартами Internet; в колонках под заголовком **Пуск** – параметр запуска: значение *Да* дает разрешение на запуск серверного компонента службы, при значении *Нет* разрешение отсутствует.

Чтобы та или иная служба могла работать, следует:

- дать разрешение на запуск ее серверного компонента;
- задать необходимые параметры службы (если требуется);
- завершить настройку службы, получив разрешение на запись измененного конфигуратора изделия в объединенную базу параметров **БпО**, используя средства БКО (см. ЭД на конкретное изделие).

Службы активизируются (или перестают быть активными) немедленно после выхода из режима настройки. В дальнейшем службы, которым при настройке разрешен запуск, активизируются автоматически при запуске изделия или при перезапуске работы ОПО соответствующего маршрутизатора.

Чтобы настроить параметры режима работы конкретной службы, следует в меню управления запуском служб маршрутизатора (Рис. 5.1) перевести курсор на ее название и нажать клавишу <Enter>.

В изделии предусмотрена возможность выполнения трассировки работы прикладных служб. Потоки информации, которой обменивается каждая служба с внешним миром, фиксируются в текстовом формате, соответствующем специфике конкретной службы, и выводятся на видеомонитор ЛКУ с одновременным сохранением в журнале **LOG.EMA**. Вопросы трассировки служб рассмотрены в разделе 4.1.3, с. 131.

За работой некоторых из служб (NAT, DHCP, DNS, RIP) можно наблюдать с помощью альтернативы ГМ: **Диагностика** (раздел 9, с. 187).

5.1. DCP

Для обеспечения функции удаленного управления изделиями в технологии DioNIS® разработан механизм технологического обмена данными по каналам связи, включающий:

- специальный протокол DioNIS Control Protocol (далее – DCP-протокол), предназначенный для обмена управляющей информацией между изделиями; DCP-протокол построен на основе стандартной клиент-серверной модели взаимодействия между объектами управления и менеджерами с использованием протокола TCP (порт ***362***); информационный обмен межу DCP-серверами и DCP-клиентами осуществляется пакетами, обе стороны жестко контролируют принимаемые пакеты на корректность формата, монотонное возрастание серийного номера пакета, совпадение имитовставки на данные пакета после его расшифрования; протокол UDP (порт ***362***) используется для
- программную поддержку функционирования DCP-сервера;
- программную поддержку функционирования DCP-клиента.

Порт ***362 UDP*** используется для пересылки служебных пакетов типа ***keepalive***.

Служба DCP обеспечивает серверную часть протокола DCP, предназначенного для удаленного управления изделиями − их конфигурирования, мониторинга, получения статистики, работы с журналами и пр. Клиентская часть протокола DCP реализуется программным компонентом **Администратор сети** (см. раздел 11, с. 204).

Служба DCP не требует настройки. При настройке маршрутизаторов (БВМ и БНМ) изделий, которым предстоит участие в процессе удаленного управления (как в качестве управляющих, так и в качестве управляемых изделий), должен быть предусмотрен запуск службы DCP – параметру запуска службы должно быть присвоено значение ***Да***.

5.2. SNTP

В телекоммуникационных сетях, организованных согласно системным требованиям `internet/intranet`-технологии, использование возможностей, предоставляемых SNTP-протоколом (Simple Network Time Protocol), позволяет организовать в масштабах всей IP-сети функционирование *службы времени* (SNTP-службы).

Служба времени обеспечивает поддержку показаний часов каждого из сетевых устройств соответствующими *эталону единого сетевого времени*, а при соблюдении дополнительных условий в сети – соответствие этого эталона (эталона единого сетевого времени) эталону *Мирового* времени (Greenwich Mean Time, **GMT**-времени).

При этом поддержка соответствия показаний часов сетевого устройства эталону обеспечивается путем *корректировки* текущего местного времени. Корректировка выполняется встроенным в устройство SNTP-клиентом на основе обмена с SNTP-серверами в составе сети, осуществляемого согласно SNTP-протоколу

> *Примечание.* SNTP-протокол является упрощенным вариантом стандартного полного протокола времени − NTP-протокола (Network Time Protocol).

В изделии реализованы оба компонента SNTP-протокола – SNTP-клиент и SNTP-сервер. Другими словами, изделия могут корректировать показания своих часов по показаниям часов других сетевых устройств и могут предоставлять показания своих часов всем заинтересованным сетевым устройствам в качестве эталонных.

Изделие поддерживает установку текущих значений даты и времени, настройку значения часового пояса географической точки, в которой эксплуатируется изделие, автоматический перевод часов на зимнее или летнее время и автоматическую корректировку часов изделия с помощью SNTP-протокола.

SNTP-клиент изделия выполняет следующие задачи:

- управляет часами данного локального узла (дата и время);
- корректирует локальные часы изделия по эталонным часам одного или нескольких доступных в сети серверов службы времени (SNTP-серверов);
- учитывает поясное время;
- выполняет автоматический переход на зимнее/летнее время (если задана соответствующая настройка);
- обеспечивает автоматическую корректировку часов (если задана соответствующая настройка).

В качестве SNTP-сервера служба времени маршрутизатора изделия предоставляет показания своих часов всем заинтересованным SNTP-клиентам.

Для того, чтобы изделие могло служить SNTP-сервером службы времени, необходимо:

- установить время на часах, установить часовой пояс, обеспечить (если требуется) автоматический переход на зимнее и летнее время (с помощью выбора цепочки альтернатив ГМ: **Настройка** ⇨ **Параметры** ⇨ **Служба времени**, подробнее см. раздел 4.1.5, с. 135);
- обеспечить контроль за правильностью хода часов вручную, либо задать их коррекцию от старших в иерархии всемирной службы времени SNTP-серверов (выбор SNTP-серверов соответствует замыслу, реализуемому в сети Администрацией ЗСПД);
- разрешить запуск SNTP-службы маршрутизатора изделия – установить значение *ДА* в графе справа от названия службы **SNTP** в списке служб (см. раздел 5, Рис. 5.1, с. 151).

Если в меню управления запуском служб маршрутизатора (Рис. 5.1, с. 151) выбрать альтернативу **SNTP**, на видеомонитор ЛКУ будет выдан бланк настройки механизма корректировки текущего времени (см. Рис. 5.2), позволяющий настроить параметры автоматической корректировки времени и выполнить при необходимости корректировку текущего времени вручную.

Список SNTP-серверов
Интервал корректировки часов 0
Максимум изменений времени 0
Выполнить корректировку времени

Рис. 5.2 Бланк настройки механизма корректировки текущего времени

Аналогичный бланк настройки выводится при выборе цепочки альтернатив ГМ: **Настройка** ⇨ **Параметры** ⇨ **Служба времени** ⇨ **Настройка параметров** – см. раздел 4.1.5, Рис. 4.8, с. 136; там же даны описание и пояснения, касающиеся настройки параметров этого бланка.

> *Обратите внимание!* Если параметру запуска службы SNTP (Рис. 5.1, с. 151) будет установлено значение ***НЕТ***, то маршрутизатор изделия не сможет служить SNTP-сервером, но сможет работать как SNTP-клиент службы времени.

5.3. SNMP

В изделиях реализована возможность удаленного наблюдения за работой изделия, а также возможность удаленного управления его работой с помощью протокола SNMP (Simple Network Management Protocol).

5.3.1. Общие сведения

SNMP представляет собой стандартный язык управления сетевыми устройствами. Он стал фактически общепринятым стандартом сетевых систем управления и поддерживается почти всеми производителями сетевого оборудования. Его понимают все сетевые устройства, и он используется всеми пакетами прикладных программ управления сетью для взаимодействия с конкретными сетевыми устройствами.

Основной концепцией протокола является то, что вся необходимая для управления устройством информация хранится на самом устройстве в Административной базе данных (MIB - Management Information Base).

Объектом управления являются переменные, характеризующие состояние управляемого устройства. База (MIB) содержит набор описаний всех переменных, которые подлежат управлению. Переменные могут отражать такие параметры как время функционирования устройства, состояние интерфейсов, количество пакетов, обработанных устройством, и т.п.

В процессе управления над каждой переменной можно выполнить две операции: *получить* ее текущее значение и *установить* новое. SNMP предоставляет набор команд для работы с переменными MIB. Для того чтобы

проконтролировать работу устройства сети, необходимо получить доступ к его MIB и проанализировать значения тех или иных переменных в ее составе.

Архитектура SNMP-модели управления сетевыми устройствами представлена на Рис. 5.3. Управляемое устройство (в нашем случае – изделие) имеет множество параметров управления. В составе управляемого изделия устанавливаются специальный модуль – SNMP-агент (агент управления) и база данных MIB.

Управляющая станция – сетевая рабочая станция, выполняющая задачу SNMP-управления сетью. На ней устанавливается программа SNMP-менеджер (пакет управления) и база данных MIB, совпадающая с базой, установленной на управляемом устройстве.

Если управляющая станция хочет выяснить состояние параметров управления на управляемом устройстве или изменить их значения, она посылает запрос. Этот запрос принимает SNMP-агент, сверяет данные запроса со своей базой и ставит в соответствие параметрам запроса реальные параметры управления.

SNMP-агент выполняет заданные в SNMP-запросе действия: считывает значение запрашиваемой переменной, формирует ответ и отправляет его согласно SNMP-протоколу; устанавливает значение переменной и выполняет в ответ на установку соответствующих переменных некоторые операции.

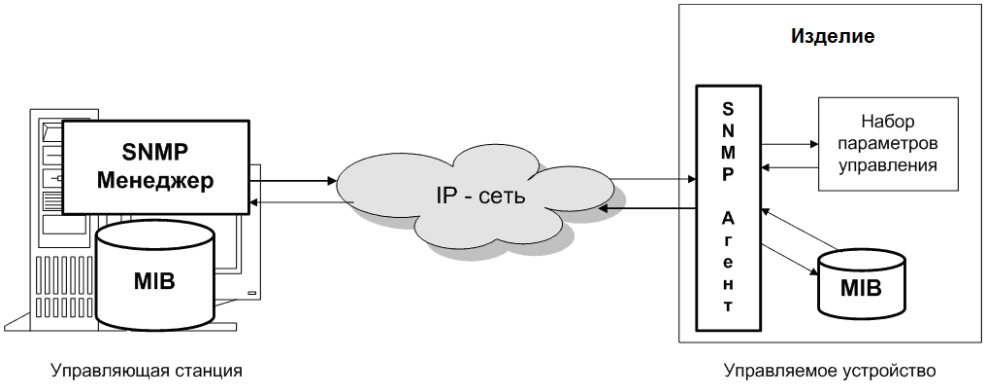


Рис. 5.3 Архитектура управления изделиями в сетях согласно SNMP-протоколу

Таким образом, SNMP-агент собирает информацию об управляемом устройстве (его параметрах управления), в котором он работает, и делает ее доступной для SNMP-менеджера с помощью протокола SNMP. Другими словами, SNMP-агент всегда является посредником между SNMP-менеджером и набором параметров управления.

При управлении по протоколу SNMP возможны *две* формы получения информации от управляемых устройств.

1. *Запрос-ответный.* Управляющие станции (SNMP-менеджеры) опрашивают по расписанию управляемые объекты и получают информацию. SNMP-агенты только отвечают на запросы.
2. *Событийный*. SNMP-агенты сами при возникновении «событий» в управляющей информации посылают уведомления своим управляющим станциям.

   «Событиями» стандартно считаются, например, такие действия: запуск и останов SNMP-агента, запуск и останов любого из IP-интерфейсов и т. д.

Выбор той или иной формы зависит от используемой программы SNMP-менеджер.

Если управляющая станция работает в сети с разнородными устройствами, то ее база MIB должна включать базы всех управляемых устройств, что может сделать ее очень громоздкой.

Разработана универсальная база MIB-II (спецификация базы - RFC 1213), которая содержит описание базового набора параметров управления. Поддержку базы MIB-II должны обеспечивать все SNMP-агенты.

Кроме базы MIB-II, стандартами RFC специфицирован целый ряд баз данных MIB, с помощью которых можно управлять на достаточно общем уровне большим количеством устройств.

И, наконец, каждый изготовитель сетевых устройств имеет право создать свои базы MIB и предоставить их управляющим станциям для включения в общую базу.

Подробнее о MIB

Как было сказано выше, элементом MIB является переменная. Каждая переменная имеет идентификатор **`OID`** (**`Object Identifier`**). Он является фактически ее именем. Для упрощения классификации в качестве **`OID`** используется последовательность целых десятичных чисел, разделенных точками. Для облегчения понимания (запоминания, чтения) численному представлению ставится в соответствие символьное. Например: **`1.3.6.1.2`** - переменная из базы MIB-II, соответствующее символьное представление: **`iso.org.dod.internet.mgmt`**.

Набор переменных, отвечающих за какую-то конкретную функцию управления, объединяется в базе в MIB - модули (MIB-modules).

Все переменные в базе можно изобразить в виде дерева с общим корнем, листьями которого являются отдельные элементы. Числа задают вершины графа управления соответствующего уровня.

В качестве примера на Рис. 5.4 представлен фрагмент структуры **OID**.

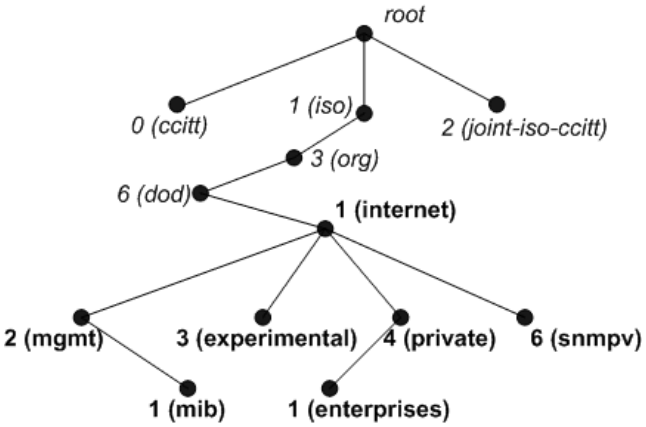


Рис. 5.4 Пример фрагмента структуры OID

Для каждой переменной, кроме имени, в базе содержится набор ее описаний. Например, формат представления переменной при передаче ее по каналу данных (численный, строковый, ...), диапазон значений, смысл переменной для управляемого устройства и т.п.

SNMP-Агент с помощью описанных в базе переменных получает доступ к реальным управляемым параметрам устройства.

Текущая реализации SNMP в изделии поддерживает базу MIB-II (RFC 1213) и некоторые ее стандартные расширения.

SNMP-агент изделия поддерживает форматы SNMP-сообщений версии ***v1*** (RFC 1157) и ***v2*** (RFC 1905). При этом в качестве транспортного протокола для SNMP-сообщений версии ***v2*** используется транспортный протокол, аналогичный протоколу версии ***v1*** – COMMUNITY-BASED (RFC 1901). Поэтому при настройке SNMP-агента изделия параметр **Версия** имеет значение – ***v2c***.

5.3.2. *Настройка SNMP-службы*

В модели SNMP-управления изделие является *управляемым* устройством и содержит SNMP-агента (программу SNMP-агент).

> *Примечание*. SNMP-агент общается с программой SNMP-менеджер по протоколу UDP с использованием портов ***161***, ***162***. В случае необходимости SNMP-наблюдения за изделием из внешней сети необходимо обеспечить прохождение указанных датаграмм (датаграмм UDP по портам ***161***, ***162***) через фильтры внешних сетевых интерфейсов.

Чтобы выполнить настройку SNMP-службы изделия, следует выбрать альтернативу **SNMP** в меню служб (см. Рис. 5.1, с. 151). В ответ на видеомонитор ЛКУ будет выдан бланк настройки SNMP-службы, аналогичный представленному на Рис. 5.5.

Максимальный размер SNMP-пакета 1500	
Данные администратора (sysContact)	
Данные местоположения (sysLocation)	
Доменное имя узла (sysName)	
Community-пароли доступа	Получатели уведомлений

Рис. 5.5 Бланк настройки SNMP-службы

Как отмечалось выше, возможны *две* формы получения информации от управляемых изделий по протоколу SNMP: *запрос-ответный* и *событийный*. Первые три параметра бланка настройки на Рис. 5.5 (**Максимальный размер SNMP-пакета**, **Данные администратора** и **Данные местоположения**) должны быть заданы в обоих случаях. Параметры поля **Community-пароли доступа** должны быть заданы для *запрос-ответной* формы получения информации, параметры поля **Получатели уведомлений** – для *событийный* формы получения информации от изделия.

Максимальный размер SNMP-пакета (Рис. 5.5). По умолчанию параметр имеет значения ***1500***. Изменять это значение следует *только* по требованию администратора управляющей станции (SNMP-менеджера).

Данные администратора и **Данные местоположения** (Рис. 5.5). В базе MIB-II есть две стандартные переменные с системными именами: **sysContact** и **sysLocation**. Они позволяют управляющей станции получить текстовую информацию об администраторе и местоположении управляемого изделия. Содержание этой информации определяется структурой управления сетью в целом.

При настройке SNMP-агента изделия в эти два поля бланка настройки (**Данные администратора** и **Данные местоположения**) следует занести ту текстовую информацию, которую закажет SNMP-менеджер (желательно без символов кириллицы). Как правило, это фамилия (имя) администратора и географическое местоположение изделия.

Доменное имя узла (Рис. 5.5). Параметр определяет имя изделия с точки зрения системы управления (обычно это имя узла).

Community-пароли доступа (Рис. 5.5). Выбор этого поля бланка приводит к выводу экрана управления списком, аналогичного представленному на Рис. 5.6; список содержит описатели тех управляющих SNMP-станций, которым разрешена *запрос-ответная* форма получения информации от изделия по SNMP-протоколу.

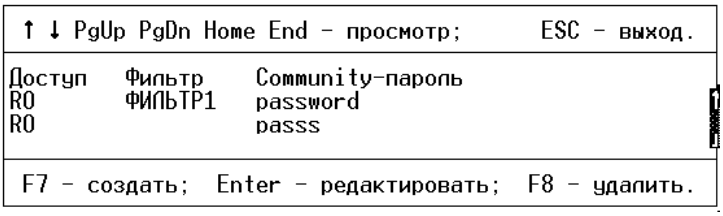


Рис. 5.6 Экран управления списком управляющих SNMP-станций (*запрос-ответная* форма)

Для редактирования (Рис. 5.6) ранее созданного описателя управляющей SNMP-станции (клавиша <Enter>) или для создания нового описателя (клавиша <F7>) служит бланк создания и настройки описателя управляющей SNMP-станции, аналогичный представленному на Рис. 5.7.

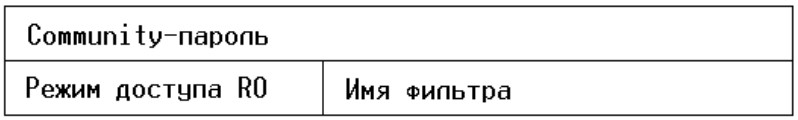


Рис. 5.7 Бланк создания и настройки описателя управляющей SNMP-станции (*запрос-ответная* форма)

Community-пароль (Рис. 5.7). Для целей аутентификации в транспортной части SNMP-протокола предусмотрено текстовое поле **Community**, содержащее *пароль*. Все SNMP-пакеты (циркулирующие в обоих направлениях) должны идти с указанием этого пароля: пакеты без пароля или с неправильным паролем будут отвергнуты.

Перед тем как начать управление, администраторы управляющей станции и изделия должны согласовать *пароль*. Пароль не должен содержать символов кириллицы. Значение согласованного с управляющей станцией пароля следует ввести в поле **Community-пароль**.

Специальное значение пароля. Можно создать пароль со специальным именем ***** (символ «звездочка»). При наличии такого пароля SNMP-агент будет принимать SNMP-запросы с любым паролем, выполнять предписанные действия и отправлять ответы с тем паролем, который был в запросе. Значения параметров **Режим доступа** и **Имя фильтра** задаются обычным образом.

Режим доступа (Рис. 5.7). Параметр позволяет установить разные режимы доступа к управляющей информации:

- *режим ограниченного доступа* (значение параметра – *RO*); в этом режиме SNMP-менеджер может только считывать информацию о параметрах управляемого устройства, т.е. может только наблюдать за работой устройства;
- *режим полного доступа* (значение параметра – *RW*); в этом режиме SNMP-менеджер может и считывать, и записывать информацию о параметрах управляемого устройства, т.е. может управлять работой устройства.

Имя фильтра (Рис. 5.7). Если выбрать это поле, на экран будет выдан список имеющихся IP-фильтров (см. раздел 3.2.1.2, Рис. 3.20, с. 92) и предоставлена возможность выбрать один из них. Выбранный фильтр программой управления будет соотнесен с паролем. В этом случае после проверки пароля будет выполняться проверка IP-датаграммы по правилам IP-фильтра. При помощи фильтра обеспечивается дополнительная (кроме пароля) защита – указывается та управляющая станция в сети, которой изделие разрешает собой управлять.

Замечание. Для одной управляющей станции разрешается использовать одновременно несколько паролей с разными режимами доступа и/или с разными фильтрами, устанавливая тем самым разные возможности доступа к управляющей информации.

Получатели уведомлений (Рис. 5.5). Выбор поля приводит к выводу экрана управления списком, аналогичного представленному на Рис. 5.8; список содержит описатели тех управляющих станций, которым SNMP-агент изделия будет посылать уведомления при возникновении *событий*, т. е. список тех SNMP-станций, которым разрешено управление изделием, если задана *событийная* форма получения информации от управляемых устройств.

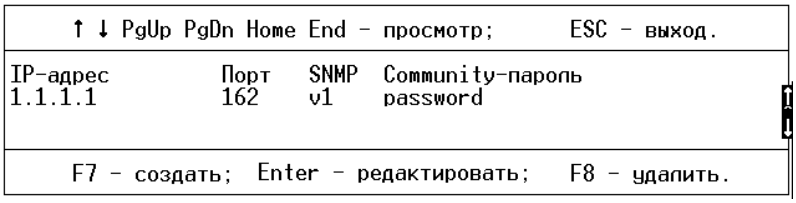


Рис. 5.8 Экран управления списком управляющих SNMP-станций (*событийная* форма)

Для редактирования ранее созданного элемента списка (клавиша <Enter>) или для создания нового элемента (клавиша <F7>) на видеомонитор ЛКУ выдается представленный на Рис. 5.9 бланк создания и настройки описателя управляющей SNMP-станции (*событийная* форма).

IP-адрес 1.1.1.1	Порт 162	Версия v1
Community-пароль password		

Рис. 5.9 Бланк создания и настройки описателя управляющей SNMP-станции (*событийная* форма)

IP-адрес (Рис. 5.5). IP-адрес управляющей станции.

Порт (Рис. 5.5). Номер порта на управляющей станции, по которому будут приходить уведомления от изделия. По стандарту SNMP для приема уведомлений используется порт *162*.

Версия (Рис. 5.5). Значением поля должна быть используемая версия - *v1* или *v2c*. Значение используемой версии задает менеджер.

Community-пароль (Рис. 5.5). В поле надо ввести пароль, согласованный с управляющей станцией.

5.4. DNS

DNS-служба обеспечивает обработку запросов на поиск в *доменной системе имен* сетей, функционирующих согласно системным требованиям internet/intranet-технологий, и возвращает результаты поиска. Запросы поступают от DNS-клиентов рабочих станций, а также от служб маршрутизаторов изделия.

> *Общие сведения* о доменной системе имен (Domain Name System, DNS) приведены в разделе ***Приложение Д***, с. 243.

5.4.1. ***Настройка DNS-службы***

В процессе настройки DNS-службы маршрутизатора изделия необходимо:

- установить основные параметры работы DNS-клиента;
- настроить DNS-сервер.

> *Примечание.* Из двух компонентов DNS-службы DNS-клиент настраивается всегда. Настройки DNS-сервера могут отсутствовать, в этом случае все поступающие запросы DNS-клиент транслирует указанным в его настройке *вышестоящим* в сети DNS-серверам.

Выбор альтернативы **DNS** в меню управления запуском служб маршрутизатора (Рис. 5.1, с. 151) приводит к выводу на видеомонитор ЛКУ меню настройки DNS-службы, аналогичного представленному на Рис. 5.10. В этом меню первая альтернатива касается управления списком DNS-серверов, следующие две альтернативы относятся к настройке DNS-клиента, а последние три – к настройке DNS-сервера.

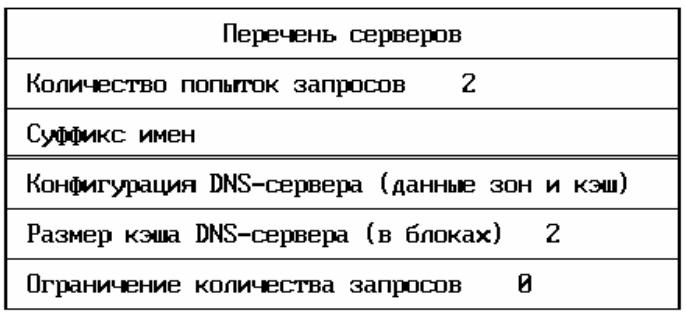


Рис. 5.10 Меню настройки DNS-службы

Управление списком DNS-серверов

Перечень серверов (Рис. 5.10). При выборе альтернативы на видеомонитор ЛКУ выдается экран управления списком DNS-серверов, аналогичный представленному на Рис. 5.11. С его помощью создается и настраивается список IP-адресов внешних DNS-серверов, доступных маршрутизатору изделия. Обычно список состоит из IP-адресов двух серверов: *основного* и *резервного* DNS-серверов `internet/intranet`-провайдера.

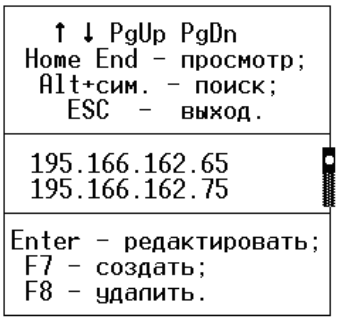


Рис. 5.11 Экран управления списком DNS-серверов для маршрутизатора изделия

Как следует из подсказок в нижней части экрана (Рис. 5.11), IP-адрес DNS-сервера можно отредактировать (переместив на строку с IP-адресом курсор и нажав клавишу <Enter>), а также можно включить в список IP-адрес нового DNS-сервера, нажав клавишу <F7>. В обоих случаях на видеомонитор ЛКУ будет выдан запрос:

Задайте IP-адрес DNS-сервера:

В ответ следует ввести новый IP-адрес DNS-сервера или отредактировать имеющийся в списке.

Нажатие клавиши <F8> (Рис. 5.11) позволяет удалить из списка IP-адрес, на строку с которым установлен курсор. Предварительно будет выдан запрос на подтверждение удаления.

Настройка DNS-клиента

Количество попыток запросов (Рис. 5.10). Параметр определяет, сколько попыток получить ответ от DNS-серверов может сделать DNS-клиент. Одной попыткой считается последовательный опрос всех DNS-серверов, доступных маршрутизатору изделия. В качестве значения параметра должно быть указано целое число в диапазоне от ***1*** до ***32***.

Суффикс имен (Рис. 5.10). Текстовый суффикс, который в DNS-запросах автоматически добавляется к простым именам (не имеющим точек в составе имени). Обычно в качестве суффикса используется имя домена сети, в состав которой входит маршрутизатор изделия.

Настройка DNS-сервера

DNS-сервер маршрутизатора изделия может обслуживать до восьми зон. Имена зон должны заканчиваться *точкой*. Имя зоны, используемой для накачки кэша, должно состоять из *одной точки* (в этой зоне могут быть любые записи, которые администратор сочтет нужным иметь в кэше при запуске DNS-сервера; ответы DNS-клиентам по этим записям не являются авторитетными).

Конфигурация DNS-сервера (данные зон и кэш) (Рис. 5.10). Выбор альтернативы выводит экран управления списком имен обслуживаемых DNS-сервером зон, аналогичный представленному на Рис. 5.12.

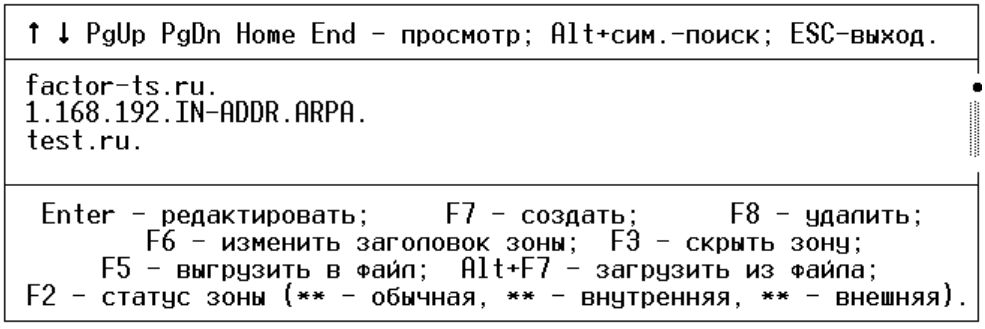


Рис. 5.12 Экран управления списком имен обслуживаемых DNS-сервером зон

Как следует из подсказок в нижней части экрана, администратору изделия предоставляются следующие возможности управления.

Enter - редактировать (Рис. 5.12). После того как курсор будет переведен на имя зоны и нажата клавиша <Enter>, на видеомонитор ЛКУ будет выдан экран управления списком **RR**-записей этой зоны, аналогичный представленному на Рис. 5.13.

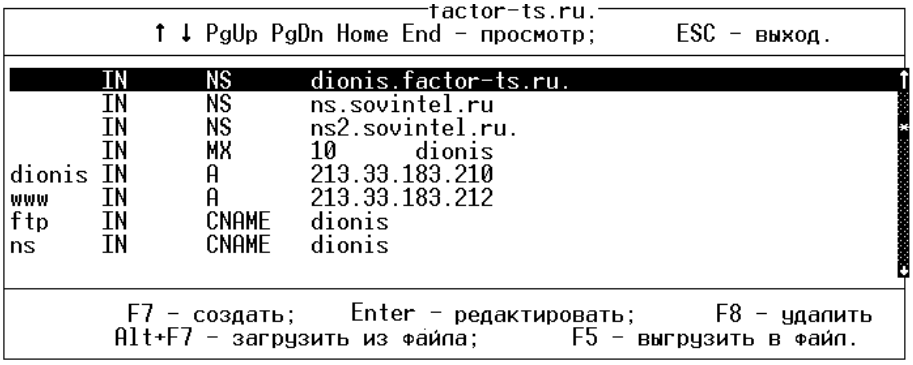


Рис. 5.13 Экран управления списком **RR**-записей редактируемой зоны

С помощью описанных далее возможностей, предоставляемых этим экраном управления, может быть сформирован полный списком **RR**-записей редактируемой зоны.

F7 – создать/Enter - редактировать (Рис. 5.13). При нажатии клавиш <F7> или <Enter> на видеомонитор ЛКУ будет выдан бланк, аналогичный представленному на Рис. 5.14. Бланк предоставляет возможность заполнить (изменить) поля **RR**-записи: **имя, время, тип, данные**.

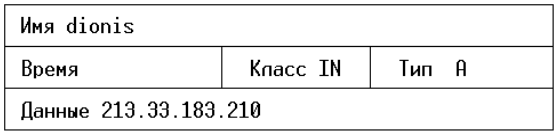


Рис. 5.14 Бланк создания (редактирования) **RR**-записи редактируемой зоны

Время (Рис. 5.14). Параметр задает время жизни **RR**-записи в секундах. Если поле не заполнено, то время жизни **RR**-записи не ограничено.

Параметры **RR**-записей **Имя** и **Данные** в зависимости от типа записи (от значения поля **Тип**) должны иметь следующие значения:

Тип	**Имя**	**Данные**
NS	*имя_зоны*	*имя_машины*
A	*имя_машины*	*IP-адрес*
PTR	*IP-адрес*	*имя_машины*
MX	*имя_домена*	*приоритет имя_машины*
CNAME	*алиас*	*имя_машины*

F8 - удалить (Рис. 5.13). После нажатия клавиши <F8> без дополнительного запроса программа управления удаляет описание **RR**-записи.

F5 - выгрузить в файл / **Alt+F7 - загрузить из файла** (Рис. 5.13). Содержимое описателей зон можно выгрузить в текстовый файл или загрузить из текстового файла. Предварительно программа управления запросит имя файла.

Формат **RR**-записей в текстовом файле соответствует формату системы **BIND**, за некоторыми исключениями, которые приведены в разделе ***Приложение Д***, с. 243.

F7 – создать (Рис. 5.12). При нажатии клавиши <F7> на видеомонитор ЛКУ будет выдан бланк управления заголовочными параметрами зоны (Рис. 5.15), предоставляя возможность создания нового описания зоны.

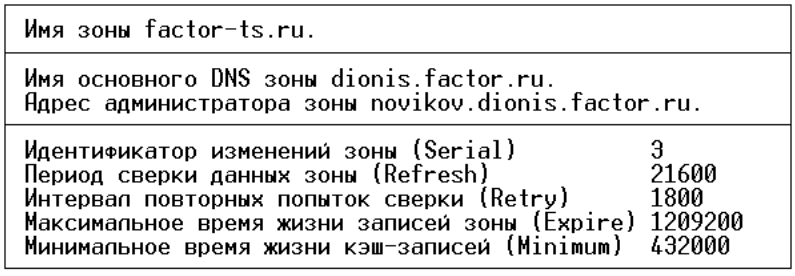


Рис. 5.15 Бланк управления заголовочными параметрами зоны

F8 – удалить (Рис. 5.12). При нажатии клавиши <F8> программа управления выдает запрос на подтверждение удаления и удаляет из списка имя зоны, на строку с которым был установлен курсор.

F6 – изменить заголовок зоны (Рис. 5.12). При нажатии клавиши <F6> на видеомонитор ЛКУ будет выдан бланк управления заголовочными параметрами зоны (поля записи типа **SOA**) – Рис. 5.15.

F3 – скрыть зону (Рис. 5.12). При нажатии клавиши <F3> та зона, на строку с именем которой был установлен курсор, станет скрытой: такая зона останется в списке, но не будет предъявляться ни на какие DNS-запросы. Цвет имени этой зоны на видеомониторе ЛКУ изменится на *серый*. При повторном нажатии клавиши <F3> зона перестанет быть скрытой (цвет описателя зоны изменится на первоначальный).

F2 - статус зоны (Рис. 5.12). После создания зона получает статус *обычная*, ее имя выводится на видеомонитор ЛКУ *черным* цветом. Если перевести курсор на строку с именем зоны и нажать клавишу <F2>, то зона получит статус *внутренняя*, цвет строки с именем этой зоны изменится на *красный*. При последующем нажатии клавиши <F2> статус зоны изменится на *внешняя*, цвет строки с именем – на зеленый.

> *Примечание.* Наличие зон с разным статусом позволяет использовать т.н. *разделенный DNS*. Все DNS-запросы с помощью системного фильтра **dns_int** делятся на *внутренние* (попадающие под разрешающие правила фильтра) и *внешние* (все остальные). Ответы на все внутренние DNS-запросы будут выданы из внутренних и из обычных зон, ответы на внешние DNS-запросы – из внешних и из обычных зон. Другими словами, внутренние запросы *не видят* внешних зон, а внешние – внутренних зон.

Размер кэша DNS-сервера (в блоках) (Рис. 5.10). Параметр позволяет задать число блоков кэша. Кэш DNS-сервера маршрутизатора изделия состоит из отдельных блоков, каждый по 64 Кб. Максимальное число блоков – ***16***, минимальное – ***1***. В одном блоке может храниться до 1024 записей.

Ограничение количества запросов (Рис. 5.10). С помощью параметра можно задать максимальное количество запросов к DNS-серверу маршрутизатора изделия, поступающих с одного IP-адреса. Точнее, можно ограничить размер очереди ожидания ответов на DNS-запросы, поступающие от устройства с одним IP-адресом. Эта возможность весьма полезна для защиты DNS-сервера маршрутизатора изделия от перегрузок, возникающих вследствие атаки изделия со стороны внешних злоумышленников, а также вследствие работы вирусов, проникающих на рабочие станции внутренней сети.

5.4.2. *Работа DNS-службы*

Как отмечалось выше, при старте маршрутизатора изделия автоматически запускается DNS-сервер**.** При запуске DNS-сервера выполняется инициализация *кэша*, в процессе которой в него помещаются записи всех сконфигурированных ранее зон.

Если запрос на DNS-сервер маршрутизатора поступает от служб маршрутизатора, то DNS-сервер сначала пытается найти ответ в таблице адресов (см. раздел 4.2.2, с. 147). Если ответ в таблице адресов не находится, то DNS-сервер продолжает поиск в своем локальном кэше. Если ответ и здесь не находится, то DNS-клиент маршрутизатора посылает DNS-запрос одному из доступных маршрутизатору DNS-серверов (пример списка серверов на Рис. 5.11, с. 158).

Если запрос на DNS-сервер поступает от DNS-клиентов рабочих станций, то DNS-сервер начинает поиск в своем локальном кэше. Если ответ на запрос не находится, то DNS-клиент маршрутизатора посылает DNS-запрос одному из доступных маршрутизатору DNS-серверов (см. Рис. 5.11, с. 158).

Все порожденные таким образом запросы заносятся в очередь DNS-запросов. При этом фиксируется, кто прислал первоначальный запрос, что содержится в запросе и кому послал запрос маршрутизатор. После того как ответ будет получен от другого DNS-сервера и передан DNS-клиенту, элемент из очереди удаляется. Поэтому на нормально работающем DNS-сервере, когда все запросы DNS-клиентов удовлетворяются в реальном времени, очередь DNS-запросов обычно пуста.

Полученные от других DNS-серверов ответы помещаются в кэш и хранятся в нем указанное в ответе время (время жизни записи в чужих кэшах) или до останова маршрутизатора.

Напомним, что в маршрутизаторе изделия могут применяться системные фильтры (см. раздел 3.2.1.7, с. 104). Для обеспечения работы DNS-сервера могут быть использованы следующие системные фильтры.

1. Фильтр с системным именем **dnslocal**. Все DNS-запросы, для которых правилами фильтра **dnslocal** задан режим **разрешить**, удовлетворяются только из локального DNS-кэша.

2. Фильтр с системным именем **dns_int** предназначен для разделения всех поступающих к DNS-серверу запросов на *внешние* и *внутренние*. Все DNS-запросы, для которых правилами фильтра **dns_int** задан режим **разрешить**, считаются внутренними. Для ответов на такие запросы используются *внутренние* и *обычные* зоны DNS-сервера. Все остальные DNS-запросы (не подпавшие под разрешающие правила фильтра с именем **dns_int**) считаются внешними. Для ответов на такие запросы используются *внешние* и *обычные* зоны DNS-сервера.

3. Фильтр с системным именем **dnszone** предназначен для указания внешних DNS-серверов, которым разрешена пересылка зон по TCP-протоколу. Операция *пересылки зоны* используется для организации вторичных DNS-серверов. С помощью этой операции вторичный DNS-сервер в определенные моменты времени может запросить полное копирование информации о любой DNS-зоне, хранящейся на первичном DNS-сервере. Для устранения возможности несанкционированного доступа к информации DNS-зон все внешние DNS-серверы, которым дано право чтения информации зон, должны быть указаны в разрешающих правилах фильтра **dnszone**. Все запросы на пересылку информации зон DNS-сервера маршрутизатора изделия, не подпавшие под разрешающие правила фильтра **dnszone**, будут отвергнуты.

5.5. DHCP

Служба DHCP обеспечивает автоматическую настройку параметров рабочих станций – абонентов услуг, предоставляемых службами и сервисами изделия, что упрощает администрирование больших локальных сетей, в которых применяются изделия.

5.5.1. Общие сведения

Любое устройство, подключаемое к TCP/IP-сети, должно иметь уникальный IP-адрес; кроме того, на каждом из устройств должен быть известен ряд параметров, необходимых для нормальной работы в сети. Корректное назначение IP-адреса и других параметров всем подключаемым к IP-сети устройствам обычно выполняется администратором сети. Если устройств много, задача становится весьма непростой даже на уровне одной организации, особенно в условиях неизбежно возникающих изменений в конфигурации сети и составе ее пользователей.

Рассмотрим, как выглядит задача администрирования локальной сети организации, состоящей из рабочих станций сотрудников, сервера и маршрутизатора, подключенного к магистральному каналу в Internet и выполняющего роль шлюза.

В процессе настройки магистрального канала администратор сети получает от Internet-провайдера пространство IP-адресов, предназначенных для абонентов его организации (пространство IP-адресов задается *адресом* сети и *маской* сети).

Из полученного адресного пространства администратор выделяет IP-адреса для маршрутизатора и сервера и выдает IP-адреса всем абонентам своей сети.

После этого администратор должен обойти машины всех сотрудников своей организации и установить на них следующие параметры:

- IP-адрес абонента;
- маска сети;
- адрес шлюза (адрес маршрутизатора);
- адрес DNS-сервера и т. п.

Проделав все это, администратор должен приготовиться к решению постоянно возникающих проблем: изменение количества рабочих станций и сетевых ресурсов, нехватка адресного пространства, появление в сети новых серверов и маршрутизаторов, изменение топологии сети, смена Интернет-провайдера с обязательной сменой пространства IP-адресов и т.п. Иными словами, администратор даже небольшой сети (20-30 рабочих станций) обречен на постоянный обход рабочих станций и *ручное* внесение изменений в их настроечные параметры.

Специально для облегчения труда сетевых администраторов и сосредоточения всех конфигурационных параметров сети в одном месте был разработан протокол DHCP.

> Протокол DHCP (Dynamic Host Configuration Protocol) предназначен для автоматического определения и передачи набора параметров, необходимых для настройки хостов и рабочих станций, подключаемых к TCP/IP сети. Официально протокол DHCP специфицирован в документах RFC 2131, RFC2132.

В соответствии с протоколом DHCP одна машина в сети назначается *сервером*, а все остальные становятся *клиентами* этого сервера. В процессе конфигурирования DHCP-серверу сообщаются подлежащие распределению среди абонентов сети IP-адреса и вся прочая информация. Машинам клиентов никакой информации, кроме указания *«Использовать DHCP»*, не сообщается.

Если на рабочих станциях используется ОС Windows, то достаточно в свойствах TCP/IP задать «**Получить IP-адрес автоматически**» и отказаться от конфигурирования шлюза и DNS.

Схему взаимодействия DHCP-клиента и DHCP-сервера в упрощенном виде можно представить так: абонент включает свою рабочую машину, программное обеспечение DHCP-клиента посылает широковещательный запрос с просьбой о выделении IP-адреса и других конфигурационных параметров. В ответ на такой запрос DHCP-сервер находит требуемые для рабочей станции параметры и посылает их запрашивающему абоненту.

Поддерживаемый маршрутизаторами изделия DHCP-сервер позволяет назначать IP-адреса (и параметры настройки) клиентским рабочим станциям двумя способами:

- *автоматическое назначение* – маршрутизатор изделия присваивает запрашивающему клиенту постоянный IP-адрес;
- *динамическое назначение* – маршрутизатор изделия выделяет IP-адрес на ограниченное время или до момента отказа клиента от IP-адреса (IP-адрес выделяется *в лизинг*).

Как правило, динамический метод назначения IP-адресов применяется для рабочих станций клиентов сети. Для серверов чаще используется автоматическое назначение постоянных IP-адресов.

Примечания.

1. Динамическое назначение параметров настройки рабочих станций не только избавляет администратора от утомительных обходов своих клиентов в случае изменений в сети, но и позволяет экономить пространство IP-адресов за счет того, что адреса выделяются только работающим станциям.
2. Необходимо следить, чтобы при наличии нескольких DHCP-серверов диапазоны используемых ими адресов не пересекались во избежание сетевых конфликтов.

5.5.2. *Настройка DHCP-службы*

Настройку DHCP-службы будем рассматривать на конкретном примере внутренней сети организации (см. Рис. 5.16).

Локальная сеть организации состоит из двух сегментов. Оба сегмента подключены к изделию. Изделие имеет магистральный канал в Internet и две сетевые карты (Ethernet-адаптера) для подключения к локальным сетям LAN1 и LAN2.

Первый сегмент сети. Имя интерфейса – **`LAN1`**. Работает в фиктивном адресном пространстве IP-адресов. Сегмент сети имеет IP-адрес **`192.168.4.0/24`** (маска **`255.255.255.0`**).

Второй сегмент сети. Имя интерфейса **`LAN2`**. Работает в реальном адресном пространстве IP-адресов. Сегмент сети имеет адрес **`194.220.36.64/28`** (маска **`255.255.255.240`**).

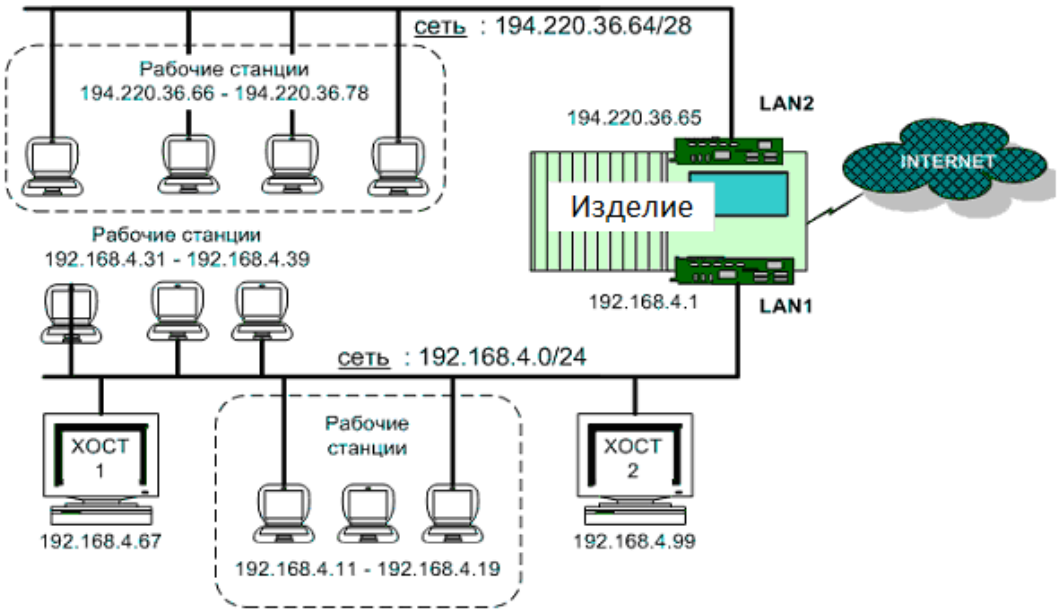


Рис. 5.16 Пример организации сети, использующей сервис DHCP-службы изделия

Чтобы выполнить настройку DHCP-службы изделия, следует выбрать альтернативу **`DHCP`** в меню служб (см. Рис. 5.1, с. 151). На видеомонитор ЛКУ будет выдан экран управления списком описателей подсетей и хостов DHCP-службы, аналогичный представленному на Рис. 5.17. Список состоит из элементов двух типов: *описатели подсетей* и *описатели хостов*.

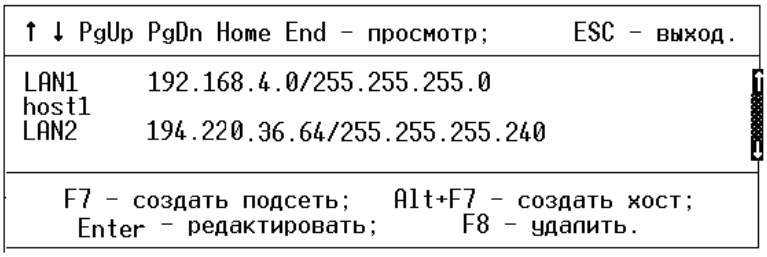


Рис. 5.17 Экран управления списком описателей подсетей и хостов DHCP-службы

С помощью описателей подсетей (первая и третья строки на Рис. 5.17) задаются диапазоны IP-адресов и другие параметры для *динамического* метода назначения конфигурационных параметров рабочих станций сети.

Описателями хостов (вторая строка на рисунке) задаются конкретные параметры для конкретных станций сети. Эти значения используются для *автоматического* метода назначения параметров.

F7 - создать подсеть / **Enter – редактировать** (Рис. 5.17). Если нажать клавишу <F7> или перевести курсор на строку с описателем подсети и нажать клавишу <Enter>, на видеомонитор ЛКУ будет выдан бланк описателя подсети (пустой или заполненный), аналогичный представленному на Рис. 5.18.

Интерфейс LAN1	Адрес сети 192.168.4.0	Маска сети 255.255.255.0

Перечень распределяемых IP-адресов

#	начальный	конечный	#	начальный	конечный
1	192.168.4.11	- 192.168.4.19	6	0.0.0.0	- 0.0.0.0
2	192.168.4.31	- 192.168.4.39	7	0.0.0.0	- 0.0.0.0
3	0.0.0.0	- 0.0.0.0	8	0.0.0.0	- 0.0.0.0
4	0.0.0.0	- 0.0.0.0	9	0.0.0.0	- 0.0.0.0
5	0.0.0.0	- 0.0.0.0	10	0.0.0.0	- 0.0.0.0

Шлюзы	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0
DNS-серверы	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0

Имя домена factor.ru	
Время доступа по умолчанию 259200	Время доступа максимальное 432000

Рис. 5.18 Бланк создания и настройки описателя подсети в структуре DHCP-службы

В этом бланке в поле **Интерфейс** должно быть имя того интерфейса, через который принимаются DHCP-запросы к данному элементу DHCP-таблицы.

Если с помощью DHCP распределяются IP-адреса и другая информация среди абонентов, подключенных к изделию через виртуальные локальные сети **VLAN**, то в графе **Интерфейс** должна быть указана следующая конструкция:

<имя_интерфейса>:<значение_VNID>, где:

имя_интерфейса – имя интерфейса, откуда принимаются DHCP-запросы;

значение_VNID – значение идентификатора виртуальной локальной сети.

Замечание. Длина имени интерфейса ограничена 7 символами. Если имя в графе **Интерфейс** включает двоеточие и значение **VNID**, то собственно имя интерфейса должно быть коротким (значение **VNID** может быть от одной до 4 цифр – на имя интерфейса остается от 5 до 2 символов).

Следующая группа параметров задает диапазон подлежащих распределению IP-адресов:

- **Адрес сети** – IP-адрес сети (подсети), откуда будут выделяться IP-адреса;
- **Маска сети** – маска сети (подсети);
- **Перечень распределяемых IP-адресов** – до 10 пар значений «**начальный-конечный**», задающих диапазоны подлежащих распределению IP-адресов из пространства, заданного параметрами **Адрес сети**, **Маска сети**.

Шлюзы – до четырех IP-адресов шлюзов, определенных для данной сети.

DNS-серверы – до четырех IP-адресов DNS-серверов, определенных для данной сети.

Имя домена – имя домена, к которому принадлежат рабочие станции данной сети.

Время доступа по умолчанию – время использования параметров DHCP-клиентом (в секундах), которое устанавливается в случае отсутствия в запросе явного требования времени.

Время доступа максимальное – максимальное время использования параметров DHCP-клиентом (в секундах).

Alt+F7 - создать хост / **Enter – редактировать** (Рис. 5.17). Если в окне на Рис. 5.17 нажать комбинацию клавиш <Alt+F7> или перевести курсор на описатель хоста и нажать клавишу <Enter>, на видеомонитор ЛКУ будет выдан бланк создания и настройки описателя хоста (пустой или заполненный), аналогичный представленному на Рис. 5.19.

В этом бланке:

Имя хоста – мнемоническое имя изделия;

Ethernet-адрес – уникальный MAC-адрес Ethernet-контроллера, используемого хостом;

IP-адрес – персональный IP-адрес изделия;

Маска сети – маска сети, к которой принадлежит адрес изделия.

Имя хоста host1				
Ethernet-адрес 35:00:3a:5b:45:66				
IP-адрес 192.168.4.68	Маска сети 255.255.255.0			
Шлюзы	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0
DNS-серверы	192.168.4.1	0.0.0.0	0.0.0.0	0.0.0.0
Имя домена				
Время доступа: по умолчанию 259200		максимальное 432000		

Рис. 5.19 Бланк создания и настройки описателя хоста в структуре DHCP-службы

Остальные параметры совпадают с аналогичными параметрами описателя подсети.

5.5.3. *Работа DHCP-службы*

В процессе работы сети DHCP-сервер ждет запроса от DHCP-клиента на выделение IP-адреса и, получив такой запрос, выполняет следующие действия.

1. Делает попытку найти параметры настройки устройства, с которого запросил обслуживание DHCP-клиент, в таблице лизинга.

   Таблица лизинга выполняет роль памяти, в которой DHCP-сервер хранит все параметры, выделенные по запросам DHCP-клиентов. Как только DHCP-сервер отдает IP-адрес (и другие параметры) в лизинг DHCP-клиенту, он сразу заносит соответствующую запись в таблицу лизинга.

2. Если данные будут найдены в таблице лизинга, то именно они и будут предложены DHCP-клиенту для дальнейшего использования. Это обеспечивает преемственность использования настроечных параметров при регулярной работе DHCP-клиента.

3. Если данных DHCP-клиента в таблице лизинга нет, DHCP-сервер делает попытку найти их среди описателей хостов в DHCP-таблице. В качестве ключа поиска используется MAC-адрес Ethernet-адаптера устройства DHCP-клиента. Если описатель будет найден, то находящиеся в нем данные будут переданы DHCP-клиенту для использования. Информация о выданных параметрах будет занесена в таблицу лизинга.

4. Если данных DHCP-клиента нет ни в таблице лизинга, ни в DHCP-таблице, то DHCP-сервер делает попытку выделить свободный IP-адрес из диапазона адресов, заданных описателями подсетей. По имени интерфейса, принявшего запрос, выбираются описатели подсетей, относящиеся к данному интерфейсу. Если в запросе DHCP-клиента был указан желаемый IP-адрес, то делается попытка выделить из диапазонов разрешенных адресов именно его. Если явного IP-адреса в запросе не было или он уже занят другим DHCP-клиентом, то выбирается первый свободный IP-адрес. Если IP-адрес будет выделен, то он и остальная информация из описателя подсети будут переданы DHCP-клиенту для использования. Информация о выданных параметрах будет занесена в таблицу лизинга.

5. Если DHCP-сервер не сможет найти свободный IP-адрес указанными выше способами, то DHCP-клиенту посылается отказ.

   Примечание. Программа управления изделием раз в минуту удаляет из таблицы устаревшие записи – записи, находящиеся в следующем состоянии:

   - предложен IP-адрес, но он не использован;
   - DHCP-клиент освободил полученный в лизинг IP-адрес, но срок лизинга не истек;
   - истек срок хранения записи, полученной в лизинг.

5.5.4. *Взаимосвязь DHCP- и DNS-служб*

В маршрутизаторах изделия выполняется привязка DHCP-таблицы лизинга к DNS-серверу. Все IP-адреса, выданные DHCP-сервером, регистрируются в DNS-кэше: имя компьютера расширяется именем домена, заданного в конфигурации DHCP, после чего имя заносится в DNS-кэш как запись типа A с указанием реального IP-адреса.

Все полученные от DHCP-сервера IP-адреса получают статус *внутренних*, т. е. выдаются только в ответ на *внутренние* запросы к DNS-серверу.

5.6. Telnet

Telnet-служба обеспечивает доступ абонентов IP-сети к службам и сервисам изделия в терминальном режиме. На рабочих местах абонентов должна использоваться какая-либо Telnet-программа. Telnet-доступ может использоваться только в целях удаленного управления изделиями согласно сведениям, изложенным в РЭ на конкретное изделие. При необходимости организации этого варианта удаленного управления изделиями следует в меню служб (см. Рис. 5.1, с. 151) маршрутизаторов изделий, участвующих в процессе удаленного управления, разрешить запуск службы **Telnet**. Настройка **Telnet**-службы сводится к регистрации абонентов, обслуживаемых изделием (см. раздел 6, с. 170).

5.7. RIP

Маршрутизаторами изделия поддерживается функционирование RIP-сервера – обработчика протокола динамической маршрутизации (Routing Information Protocol) – RIP-протокола. RIP-сервер получает из сети сведения о маршрутных таблицах соседних хостов и может периодически информировать своих соседей (всех или избранных) об изменениях в своей маршрутной таблице.

На основе информации о маршрутах, автоматически получаемой из сетей, RIP-сервер формирует динамическую часть таблицы маршрутизации соответствующего маршрутизатора изделия.

> *Замечание*. Правила формирования рабочей таблицы маршрутов (состоящей из статической и динамической части) подробно рассмотрены в разделе ***Приложение А***, с. 214.

Выбор протокола RIP и его версий для реализации в изделии обусловлен широкой распространенностью этого протокола, относительной простотой реализации и отсутствием необходимости в более сложных протоколах маршрутизации для решаемых изделиями задач.

Маршрутизаторами изделия поддерживается следующие протоколы динамической маршрутизации:

- **RIP версии 1** (RFC1058 1988 год);
- **RIP версии 2** (RFC1388 1993 год, RFC2453 1998 год).

Кроме того, маршрутизаторы изделия могут принимать и обрабатывать RIP-пакеты не стандартизированного, но широко применяемого на практике протокола **RIP 98**.

Обработчик протокола RIP (RIP-сервер в составе каждого из маршрутизаторов) имеет два возможных режима работы – *пассивный* и *активный*.

В *пассивном* режиме RIP-сервер только *слушает* окружающую изделие IP-среду, извлекает из нее все пакеты RIP-протокола и выполняет модификацию маршрутной таблицы собственного маршрутизатора. В пассивном режиме RIP-сервер не отвечает на запросы других RIP-серверов и не рассылает своих маршрутных таблиц.

В *активном* режиме RIP-сервер изделия не только *слушает*, но и сам рассылает сведения о своих маршрутных таблицах в соответствии с заданным администратором списком рассылки:

- периодически – в соответствии с заданным при настройке интервалом времени;
- немедленно – при получении запроса от другого RIP-сервера.

Режим работы RIP-сервера выбирается администратором изделия, исходя из решаемых данным узлом задач. Обычно пассивный режим работы выбирается для узлов, работающих в *подчиненном* по отношению к другим маршрутизаторам сети режиме. Активный режим работы RIP-сервера может потребоваться в тех случаях, когда изделием обеспечивается обмен данными на *магистральных* направлениях ЗСПД.

Модификации RIP-протокола. Одним из известных недостатков **RIP**-протокола является низкая скорость *сходимости*, т. е. достижения такого состояния, при котором все маршрутизаторы ЗСПД одинаково трактуют текущее состояние сетевой топологии. Поэтому при изменении топологии сети (обрыв каналов связи, добавление новых маршрутизаторов и т.д.) переход сети в новое равновесное состояние, в котором прекращаются изменения маршрутных таблиц узлов сети, выполняется достаточно медленно.

Следствием низкой скорости сходимости являются:

- увеличение объема трафика, которым обмениваются маршрутизаторы для достижения сходимости;
- образование *петель* маршрутизации;
- большое время, требуемое для реагирования на изменения в топологии сети.

Существует несколько технологий, с помощью которых протокол RIP может повысить показатели производительности в динамических средах и которые могут обеспечить повышение скорости сходимости. Это технологии ***Split Horizon***, ***Poisoned Reverse*** и ***Triggered Update***.

> *Примечание.* Здесь намеренно оставлены английские названия технологий, поскольку они используются при конфигурировании всех без исключения RIP-серверов, а их русский перевод плохо отражает суть технологий.

Split Horizon. По этой технологии в состав формируемых RIP-пакетов с информацией о рабочей маршрутной таблице изделия, подлежащих отправке через конкретный интерфейс изделия, не будут включаться

маршрутные записи, полученные ранее через этот же интерфейс. Другими словами, изделие не будет распространять информацию об определенном маршруте через интерфейс, который явился источником данной информации.

Для использования технологии ***Split Horizon*** в изделии необходимо присвоить параметру элементов списка рассылки (см. ниже раздел 5.7.1) **Стратегия "Split Horizon"** значение *Да*.

Poisoned Reverse. Технология является модификацией ***Split Horizon***. По технологии ***Poisoned Reverse*** нежелательные маршруты не исключаются из RIP-пакетов, а снабжаются указанием, что данный маршрут через изделие не доступен.

Для использования технологии ***Poisoned Reverse*** необходимо присвоить значения *Да* двум параметрам элементов списка рассылки (см. ниже раздел 5.7.1) **Стратегия "Split Horizon"** и **Стратегия "Poisoned Reverse"**.

> *Примечание.* Установка значения *Да только* параметру **Стратегия "Poisoned Reverse"** для включения технологии недостаточна.

Triggered Update. Эта технология предусматривает немедленное оповещение всех заданных в списке рассылки маршрутизаторов об изменениях в маршрутной таблице изделия. Технология ***Triggered Update*** в составе RIP-сервера изделия включена всегда.

5.7.1. *Настройка RIP-службы*

Конфигурирование сервера

Чтобы выполнить настройку RIP-службы изделия, надо в меню служб (Рис. 5.1, с. 151) выбрать альтернативу **RIP**. На видеомонитор ЛКУ будет выдан бланк настройки режима работы RIP-службы (Рис. 5.20).

Список рассылки маршрутных таблиц
Фильтр принимаемых маршрутных таблиц
Список аутентификации
Время жизни маршрутных записей 0
Прием default-маршрутов запрещен
Слияние маршрутных записей запрещено
Обрабатывать версии протокола выше 0
Прием RIP-98 запрещен

Рис. 5.20 Бланк настройки режима работы RIP-службы

Список рассылки маршрутных таблиц (Рис. 5.20). Альтернатива служит для формирования списка, в соответствии с которым будет выполняться рассылка данных из рабочей таблицы маршрутизации по указанным в списке адресам. RIP-сервер переводится в активный режим работы только при наличии в этом списке хотя бы одного элемента.

Выбор альтернативы приводит к выводу на видеомонитор ЛКУ экрана со списком рассылки сведений о маршрутах, аналогичного представленному на Рис. 5.21.

↑ ↓ PgUp PgDn Home End - просмотр; ESC - выход.

Адрес	Время	V	домен	метка	Адрес шлюза	Пароль
192.168.1.13	30	1	0	0	0.0.0.0	
192.168.250.0	100	2	0	0	0.0.0.0	password
192.168.1.15	30	2	0	0	0.0.0.0	
192.168.5.0	30	2	0	0	0.0.0.0	
192.168.1.0	50	2	0	0	0.0.0.0	pasp

F7 - создать; Enter - редактировать; F8 - удалить.

Рис. 5.21 Экран со списком рассылки сведений о маршрутах

F7 - создать (**Enter - редактировать**) (Рис. 5.21). После нажатия клавиши <F7> (или клавиши <Enter>) на видеомонитор ЛКУ выводится бланк создания и настройки элемента рассылки сведений о маршрутах, позволяющий сформировать (отредактировать) один элемент списка рассылки.

Бланк представлен на Рис. 5.22

Адрес 192.168.1.13		Широковещательная рассылка	Нет
Интервал рассылки 30		Вставка локального адреса	Нет
Версия протокола 1		Стратегия "Split Horizon"	Нет
Домен 0	Метка 0	Стратегия "Poisoned Reverse"	Нет
Адрес шлюза 0.0.0.0		Вставка данных аутентификации	Нет
Пароль			

Рис. 5.22 Бланк создания и настройки элемента рассылки сведений о маршрутах

Адрес (Рис. 5.22) – IP-адрес, подставляемый в поле **Destination address** IP-заголовка датаграммы при отправке RIP-пакета с таблицей маршрутов изделия. Адрес используется для маршрутизации, по нему определяется интерфейс изделия, в который будут отправляться IP-пакеты RIP-протокола с информацией о маршрутах.

Интервал рассылки (Рис. 5.22) – параметр задает периодичность рассылки (единица измерения – секунда) RIP-сервером своих маршрутных таблиц по указанному предыдущим параметром адресу. При нулевом значении параметра рассылка по указанному адресу не осуществляется.

Стандартом RIP-протокола для параметра **Интервал рассылки** предусмотрено значение *30* сек. Можно увеличить это значение с целью уменьшения нагрузки на сеть.

> Значение интервала рассылки должно быть согласовано с параметром **Время жизни маршрутных записей** других RIP-серверов данной сети. Обычно интервал рассылки равен одной трети значения **Время жизни маршрутных записей**. Список маршрутных записей и их параметров можно просмотреть с помощью команды ГМ: **Диагностика ⇨ Интерфейсы ⇨ Таблица маршрутов** (см. раздел 9.2.3, с. 190) и команды ГМ: **Интерфейсы ⇨ F3 – маршрутная таблица узла** (раздел 2.6, с. 52, параметр **TTL** в таблице на Рис. 2.43, с. 54).

Версия протокола (Рис. 5.22) – параметр задает версию RIP-протокола, используемого для рассылки маршрутных таблиц изделия. Возможные значения: ***1*** (**RIP версии 1**) или ***2*** (**RIP версии 2**).

Домен (Рис. 5.22) – целое число в диапазоне от ***0*** до ***65535***. Подставляется в поле **Routing Domain** пакетов протокола **RIP**. В большинстве случаев это поле должно иметь значение *0*. Отличное от нуля значение может потребоваться в тех случаях, когда на соседних маршрутизаторах работают одновременно несколько процессов маршрутизации, обслуживающих разные административные области сети. (Подробнее см. документацию по протоколу **RFC1388**).

Метка (Рис. 5.22) – целое число в диапазоне от ***0*** до ***65535***. Подставляется в поле **Route Tag** пакетов протокола **RIP версии 2**. В большинстве случаев это поле должно иметь значение *0*. Отличное от нуля значение может потребоваться для совместной работы изделия с маршрутизаторами, использующими другие протоколы динамической маршрутизации (**OSPF**, **IS-IS** и др.).

Адрес шлюза (Рис. 5.22) – IP-адрес шлюза, который подставляется в поле **Next Hop** пакетов протокола **RIP версии 2**. В большинстве случаев это поле должно иметь значение *0.0.0.0*. Отличное от нуля значение может использоваться в тех случаях, когда не все соседние с изделием маршрутизаторы используют протокол **RIP**. (Подробнее см. документацию по протоколу **RFC1388**).

Пароль (Рис. 5.22) – текстовая строка длиной до 16 символов, которая будет использоваться в качестве пароля в данных аутентификации пакетов протокола **RIP версии 2**. Вставка данных аутентификации производится только тогда, когда параметр **Вставка данных аутентификации** (Рис. 5.22) имеет значение *ДА*.

Широковещательная рассылка (Рис. 5.22) – параметр разрешает (значение *ДА*) или запрещает (значение *НЕТ*) отправку IP-датаграмм с RIP-пакетами в широковещательном (**broadcast**) режиме. Обычно RIP-информация отправляется в широковещательном режиме (всем станциям сети, подключенным к интерфейсу, назначенному для отправки RIP-пакета). Если администратор изделия запретит широковещательную рассылку, то поток RIP-информации будет отправляться только по адресу, заданному параметром **Адрес** (см. Рис. 5.22).

Вставка локального адреса (Рис. 5.22) – параметр разрешает (значение *ДА*) или запрещает (значение *НЕТ*) вставку маршрутной записи с локальным адресом интерфейса, через который будет выполнена отправка RIP-пакета. Обычно этот параметр имеет значение ***НЕТ***.

Стратегия "Split Horizon" (Рис. 5.22) – параметр разрешает (значение *ДА*) или запрещает (значение *НЕТ*) использование стратегии **Split Horizon** при формировании набора маршрутных записей для RIP-пакетов, отправляемых изделием.

Стратегия "Poisoned Reverse" (Рис. 5.22) – параметр разрешает (значение *ДА*) или запрещает (значение *НЕТ*) использование стратегии **Poisoned Reverse** при формировании набора маршрутных записей для RIP-пакетов, отправляемых изделием.

Вставка данных аутентификации (Рис. 5.22) – в зависимости от значения этого параметра выполняется (значение *ДА*) или не выполняется (значение *НЕТ*) вставка данных аутентификации, основанных на значении параметра **Пароль** (Рис. 5.22), в пакеты протокола **RIP версии 2**.

Фильтр принимаемых маршрутных таблиц (Рис. 5.20) – альтернатива служит для формирования списка фильтров, обеспечивающих запрет обработки некоторых из полученных криптомаршрутизатором RIP-данных. Выбор альтернативы приводит к выводу представленного на Рис. 5.23 бланка создания и настройки списка фильтруемых адресов подсетей.

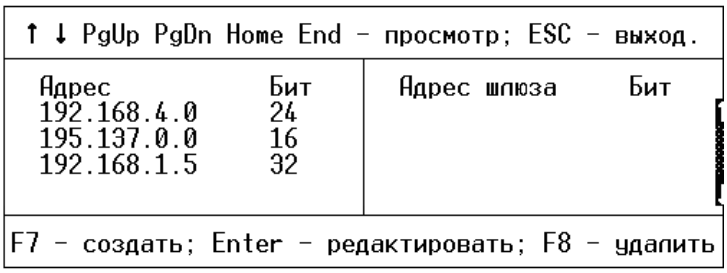


Рис. 5.23 Бланк создания и настройки списка фильтруемых адресов подсетей

Адрес (Рис. 5.23) – адрес IP-маршрутизатора, приславшего RIP-пакет.

Бит (Рис. 5.23) – целое десятичное число в диапазоне от ***0*** до ***32***, указывающее число старших бит IP-адреса (длину маски подсети).

Адреса IP-маршрутизаторов, присылающих RIP-пакеты, сравниваются с адресами в строках фильтра согласно указанной в соответствующей строке длине маски подсети (в битах). При совпадении пришедшие RIP-данные RIP-службой маршрутизатора не обрабатываются.

Адрес шлюза (Рис. 5.23) – IP-адрес шлюза.

Бит (Рис. 5.23) – целое десятичное число в диапазоне от ***0*** до ***32***, указывающее число старших бит IP-адреса (длину маски подсети).

После нажатия клавиши <F7> (<Enter>) на видеомонитор ЛКУ выдается бланк ввода параметров списка фильтруемых адресов подсетей, позволяющий сформировать (отредактировать) один элемент списка фильтруемых адресов подсетей – задать IP-адрес и число его значащих бит.

Нажатие клавиши <F8> без дополнительного запроса удаляет элемент списка, на котором установлен курсор.

Список аутентификации (Рис. 5.20) – альтернатива служит для формирования списка, содержащего данные аутентификации, необходимые для обмена RIP-информацией с соседними RIP-серверами. В **RIP-протоколе версии 2** предусмотрена возможность перед обработкой данных RIP-пакета проверить полномочия RIP-сервера, приславшего эти данные.

Замечание. RIP-сервер изделия, в свою очередь, может вставлять необходимые данные аутентификации в отправляемые пакеты. Для этого в **Списке рассылки** (см. Рис. 5.21, с. 166) необходимо задать **Пароль** и присвоить значение *ДА* параметру **Вставка данных аутентификации**.

Список аутентификации (Рис. 5.20) – выбор альтернативы приводит к выводу на видеомонитор ЛКУ экрана, аналогичного представленному на Рис. 5.24. Экран содержит список параметров аутентификации при обмене с RIP-серверами.

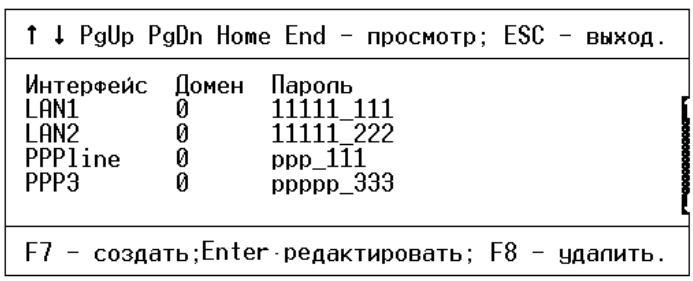


Рис. 5.24 Экран списка параметров аутентификации при обмене с RIP-серверами

Экран (Рис. 5.24) содержит список параметров аутентификации при обмене с RIP-серверами. Каждая строка (один элемент списка) имеет следующую структуру.

Под заголовком **Интерфейс** – *имя* интерфейса маршрутизатора изделия, через который принимается RIP-пакет.

Под заголовком **Домен** – значение параметра из элемента **Списка рассылки** (Рис. 5.21) для того IP-маршрутизатора, откуда пришел RIP-пакет.

Под заголовком **Пароль** – значение параметра из элемента **Списка рассылки** (Рис. 5.21) для того IP-маршрутизатора, откуда пришел RIP-пакет.

После нажатия клавиши <F7> (<Enter>) на видеомонитор ЛКУ выдается бланк ввода элементов списка с параметрами аутентификации, позволяющий сформировать (отредактировать) один элемент списка – задать имя интерфейса, значение домена и пароль.

Нажатие клавиши <F8> без дополнительного запроса удаляет элемент списка, на котором установлен курсор.

Алгоритм проверки полномочий RIP-сервера, приславшего RIP-пакет. При получении от соседних узлов пакета маршрутных данных по протоколу **RIP версии 2** на соответствующем маршрутизаторе выполняется процедура проверки возможности использования этих данных, для чего:

- среди записей списка аутентификации отбираются те, для которых значение поля **Интерфейс** совпадает с именем интерфейса, через который получен RIP-пакет;
- из отобранных записей оставляются только те, у которых значение поля **Домен** совпадает со значением поля **Routing Domain** RIP-пакета;
- проверяется совпадение присланного в RIP-пакете пароля со значением поля **Пароль** отобранных записей;
- при наличии хотя бы одного совпадения пароля данные RIP-пакета принимаются на дальнейшую обработку; в противном случае – пакет отбрасывается.

Время жизни маршрутных записей (Рис. 5.20) – параметр задает значение времени жизни (в секундах) записей, добавленных в рабочую таблицу маршрутизации с помощью RIP-сервера.

Каждая запись в рабочей таблице маршрутизации имеет счетчик времени, который устанавливается в начальное значение в момент добавления записи в таблицу. Каждую секунду значение этого счетчика уменьшается на единицу. При достижении нулевого значения счетчика запись из таблицы удаляется. Счетчик возвращается в начальное значение в момент каждого повторного получения RIP-сервером информации о данной маршрутной записи.

> *Замечание*. Нулевое значение параметра задает неограниченное время жизни записи в таблице маршрутизации. Устанавливать нулевое значение не рекомендуется.

Прием default-маршрутов (Рис. 5.20). Этот параметр может иметь значение *запрещен* или *разрешен*. В зависимости от значения этого параметра, соответственно, запрещается или разрешается прием и занесение в рабочую таблицу маршрутов вида *0.0.0.0/00*.

Слияние маршрутных записей (Рис. 5.20) – параметр может иметь значение *запрещено* или *разрешено*. При установке значения *разрешено* RIP-сервер может выполнять *слияние* – удаление маршрутных записей при получении нового маршрута для данного интерфейса, имеющего более широкую область действия, чем одна или несколько уже имеющихся в рабочей таблице маршрутизации записей.

Обрабатывать версии протокола выше (Рис. 5.20) – параметр может иметь значения ***0***, ***1*** или ***2***. RIP-сервер изделия отвергает все RIP-пакеты, имеющие номер версии RIP-протокола, меньшие или равные значению данного параметра.

Прием RIP-98 (Рис. 5.20) – параметр может иметь значение *разрешен* или *запрещен*. В зависимости от значения этого параметра RIP-сервер маршрутизатора изделия, соответственно, обрабатывает или отбрасывает пришедшие RIP-пакеты версии **RIP-98**.

> *Внимание!* Маршрутизаторы изделия принимают таблицы маршрутов по **unicast**-адресам и по **brodcast**-адресам. По **multicast**-адресам маршрутизаторы изделия таблицы маршрутов НЕ принимают (подробнее о способах адресации см. раздел 2.8, с. 60).

5.7.2. *Работа RIP-службы*

RIP-серверы изделия не требуют обязательной настройки, достаточно дать разрешение на его использование: присвоить значение *ДА* параметру **Пуск** в меню управления запуском служб маршрутизатора для службы **RIP** (см. Рис. 5.1, с. 151). Без настройки RIP-сервер будет работать в режиме *пассивного* прослушивания входящих по интерфейсам соответствующего маршрутизатора IP-датаграмм. Если среди них окажутся пакеты с RIP-информацией, то будет выполнена модификация рабочей таблицы маршрутизации соответствующего маршрутизатора.

Для задания параметров работы RIP-сервера, в том числе для перевода его в активный режим работы, необходимо выполнить его настройку (о настройке RIP-службы см. раздел 5.7.1, с. 166).

6. Настройка изделия для работы с абонентами

Для удобства работы с абонентами изделия введено понятие *групп* абонентов – каждый абонент размещается в конкретной группе. Сначала должна быть создана группа, а потом уже в составе этой группы следует создавать и настраивать учетные записи абонентов – их *паспорта*.

Программа управления изделием для обеспечения функций управления требует наличия специального абонента – *администратора узла*. Один администратор создается в процессе инициализации маршрутизатора изделия, он автоматически заносится во все группы абонентов, этого администратора нельзя удалить. Такой администратор имеет доступ *ко всем* функциям управления изделием.

Программа управления позволяет при необходимости создать несколько дополнительных учетных записей администраторов и дать каждому из них доступ только к определенному набору управляющих функций.

К администраторам, как и к рядовым абонентам, применимы все рассмотренные в настоящем разделе функции и операции управления и контроля, включая возможность корректировки параметров паспорта – изменения имени и пароля администратора.

Для регистрации абонентов в списках учета абонентов изделия и для настройки параметров их работы следует выбрать цепочку альтернатив ГМ: **Настройка ⇨ Абоненты**. При выборе этой цепочки альтернатив на видеомониторе ЛКУ появится аналогичный представленному на Рис. 6.1 экран управления списком групп абонентов с полным списком всех групп абонентов, которые может обслужить изделие в процессе своего функционирования. Имена групп в списке располагаются в алфавитном (точнее, в *лексикографическом*) порядке.

В группе с системным именем `administrators` должны быть зарегистрированы абоненты, обладающие правами администратора (дополнительные администраторы), а в группе с системным именем `system` – абоненты, имеющие право *удаленного* подключения к данному изделию. Чтобы последние могли осуществлять функции удаленного управления данным изделием, следует внести их данные в бланк настройки параметров для организации управления в режиме удаленной консоли (см. раздел 4.1.4, Рис. 4.5, с. 134).

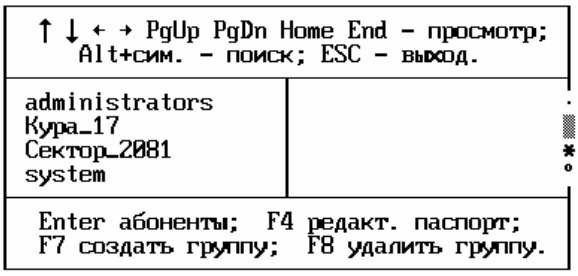


Рис. 6.1 Экран управления списком групп абонентов

В нижней части экрана управления списком групп абонентов размещены подсказки, информирующие о том, с помощью каких клавиш можно выполнить ту или иную операцию для управления группами абонентов. Все операции (кроме команды **F7 – создать группу**) выполняются для одной группы – той, на имени которой установлен курсор.

6.1. F7 - создать группу

<**F7**> **– создать группу** (Рис. 6.1). При нажатии клавиши <F7> на видеомонитор ЛКУ выводится меню, содержащее учетную запись − паспорт группы (Рис. 6.2), и предоставляется возможность заполнить графы паспорта.

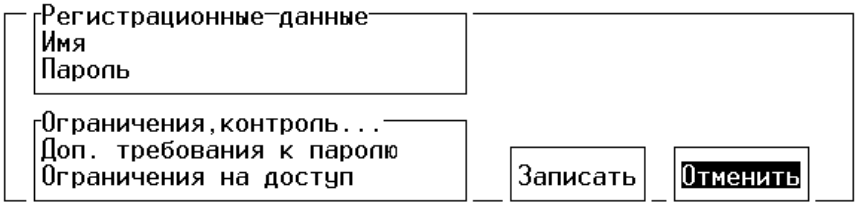


Рис. 6.2 Экран создания и настройки паспорта группы абонентов

Регистрационные данные.

> **Имя** (Рис. 6.2). Параметр идентифицирует группу, имя группы должно быть уникальным. Имя может содержать любые буквы, цифры и специальные символы, кроме символов: **@!%.,:*/=** и символа пробела. При идентификации имени группы прописные и строчные буквы в имени не различаются. Кроме того, идентичными являются символы латинского алфавита и кириллицы в кодировке КОИ-7. Для изделия имена: Катя, КАТЯ, katq, КатQ – являются одним и тем же именем.

Пароль (Рис. 6.2). Значением параметра может быть произвольный набор до 15 символов. Задавать пароль группы не обязательно.

> *Примечание!* Если для управления изделием требуется регистрация дополнительных администраторов, то необходимо создать группу с обязательным именем `administrators` и размещать абонентов-администраторов в ней.

Ограничения, контроль .... Из этой группы параметров настраивается только один:

Доп.требования к паролю (Рис. 6.2). Параметр служит для установки ограничений на доступ к службам и сервисам изделия для всех абонентов группы. Подробнее эти ограничения будут рассмотрены ниже (см. раздел 6.4.2, с. 172).

Присвоив значения параметрам паспорта, следует выбрать альтернативу **Записать** (Рис. 6.2). Если параметры паспорта заданы без ошибок, программа управления зарегистрирует новую группу абонентов изделия.

6.2. F4 - редактировать паспорт

F4 – редакт. паспорт (Рис. 6.1). При нажатии клавиши <F4> на видеомонитор ЛКУ будет выдан тот же экран создания и настройки паспорта группы, аналогичный представленному на Рис. 6.2, и предоставляется возможность отредактировать значения параметров.

Чтобы сделанные изменения были занесены в паспорт, следует выбрать альтернативу **Записать** (Рис. 6.2). Если при модификации паспорта была допущена какая-либо ошибка, программа управления сообщит о ней и не позволит произвести запись.

Если из экрана (Рис. 6.2) выйти через альтернативу **Отменить** или нажав клавишу <Esc>, паспорт группы абонентов останется неизмененным.

6.3. F8 - удалить группу

Удалить учетную запись группы абонентов (Рис. 6.1) можно только в том случае, когда в составе группы нет *ни одного* абонента (кроме первого администратора). Перед тем как произвести удаление, программа управления после нажатия клавиши <F8> выдаст контрольный запрос о необходимости удаления.

6.4. Работа с абонентами

Чтобы получить доступ к абонентам конкретной группы, следует в списке групп абонентов (Рис. 6.1) переместить курсор на строку с описателем этой группы и нажать клавишу <Enter>. На видеомонитор ЛКУ будет выдан один из двух вариантов экрана управления списком абонентов группы, аналогичных представленным на Рис. 6.3.

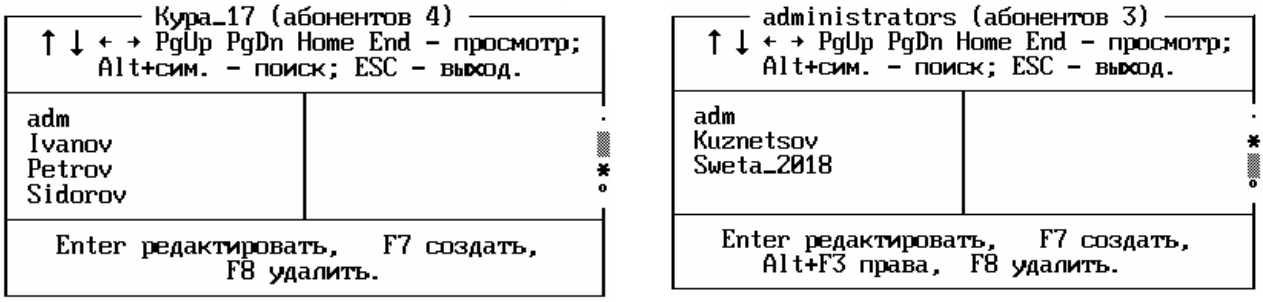


Рис. 6.3 Экраны управления списком абонентов группы

В верхней рамке экранов выводится: *имя группы*, а в круглых скобках справа от имени – количество абонентов, зарегистрированных в группе.

Как видно из подсказок в нижней части экранов, программа управления позволяет:

- **<F7> создать** – создать абонента (создать и настроить паспорт нового абонента);
- **<Enter> редактировать** – отредактировать паспорт абонента;
- **<F8> удалить** – удалить любого абонента (удалить паспорт), кроме *администратора*, паспорт которого создается программой управления;
- **<Alt+F3> права** – отрегулировать права доступа абонентам-администраторам (правый экран на Рис. 6.3).

По команде **<F7>** и по команде **<Enter>** на видеомонитор ЛКУ выводится экран настройки паспорта абонента (Рис. 6.4) и предоставляется возможность задать или отредактировать значения его параметров.

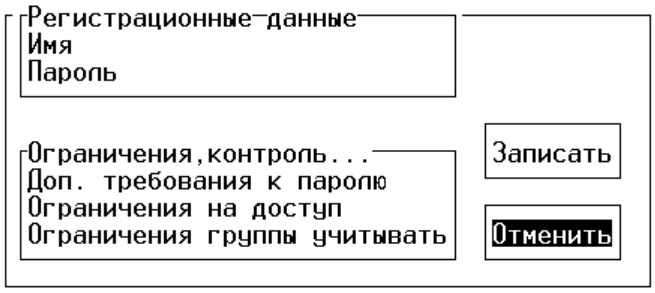


Рис. 6.4 Экран настройки паспорта абонента

6.4.1. *Регистрационные данные*

Имя (Рис. 6.4). Имя служит для идентификации пользователя – абонента изделия. Имя должно быть не короче трех символов и не длиннее пятнадцати. Имена *всех* абонентов изделия в пределах всех групп должны быть *уникальными*. Имя должно быть задано обязательно.

Имя может содержать любые буквы, цифры и специальные символы, кроме символов: **@!%.,:*/=** и символа пробел. Прописные и строчные буквы, а также символы латинского алфавита и кириллицы (в кодировке КОИ-7) для имени абонента *идентичны*. Для имени абонента не рекомендуется использовать символы русского алфавита (кириллицы).

Пароль (Рис. 6.4). Пароль на экран не выводится (вместо символов пароля на экране отображаются *звездочки*). Пароль должен быть задан обязательно.

6.4.2. *Ограничения, контроль ...*

Под этим заголовком доступна только альтернатива **Доп.требования к паролю**. Она позволяет задать необходимый уровень сложности пароля для абонента изделия.

Выбор альтернативы приводит к выводу экрана настройки ограничений на сложность пароля абонента изделия, представленного на Рис. 6.5.

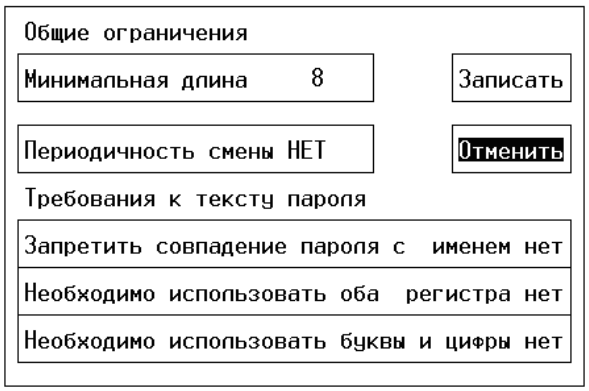


Рис. 6.5 Экран настройки ограничений на сложность пароля абонента изделия

Минимальная длина (Рис. 6.5). Параметр позволяет установить минимально допустимую длину пароля. Если параметру присвоено *нулевое* значение, то длина пароля может быть любой, начиная с одного символа.

Периодичность смены (Рис. 6.5). Параметр задает интервал времени, через который пароль должен быть обязательно заменен. Возможные значения: *день*, *неделя*, *месяц*, *квартал*, *год*, *НЕТ*. В последнем случае изменять пароль не требуется.

Запретить совпадение пароля с именем (Рис. 6.5). Если параметру присвоить значение *ДА*, то абоненту будет запрещено задавать пароль, совпадающий с именем.

Необходимо использовать оба регистра (Рис. 6.5). Если параметру присвоить значение *ДА*, то пароль абонента должен содержать как строчные, так и заглавные буквы (хотя бы по одной букве каждого регистра).

Необходимо использовать буквы и цифры. (Рис. 6.5). Если параметру присвоить значение *ДА*, то пароль абонента должен содержать и буквы, и цифры (хотя бы по одной).

Установку уровня сложности пароля можно выполнить индивидуально для каждого абонента или сразу для всех абонентов группы, воспользовавшись для этой цели альтернативами **Доп.требования к паролю** соответственно паспорта абонента (Рис. 6.4) или паспорта группы (Рис. 6.2). Если заданы и индивидуальные, и групповые ограничения, то для абонента действует сумма этих ограничений.

Если окажется, что пароль абонента не соответствует заданным ограничениям, то абонент к работе с изделием не допускается.

Установив значения параметров паспорта, следует выбрать альтернативу **Записать** (Рис. 6.4). Если параметры паспорта установлены без ошибок, программа управления зарегистрирует паспорт нового абонента.

После создания абонента-администратора будет выдано предупреждение «Нет заданных прав доступа».

6.4.3. ***Права доступа***

Чтобы закончить создание абонента-администратора, следует в списке абонентов (Рис. 6.3, правый экран) перевести курсор на его имя и нажать комбинацию клавиш <Alt+F3>. По этой команде на видеомонитор ЛКУ будет выдан представленный на Рис. 6.6 экран управления правами доступа абонента-администратора, содержащий практически все *функции* управления маршрутизатором изделия.

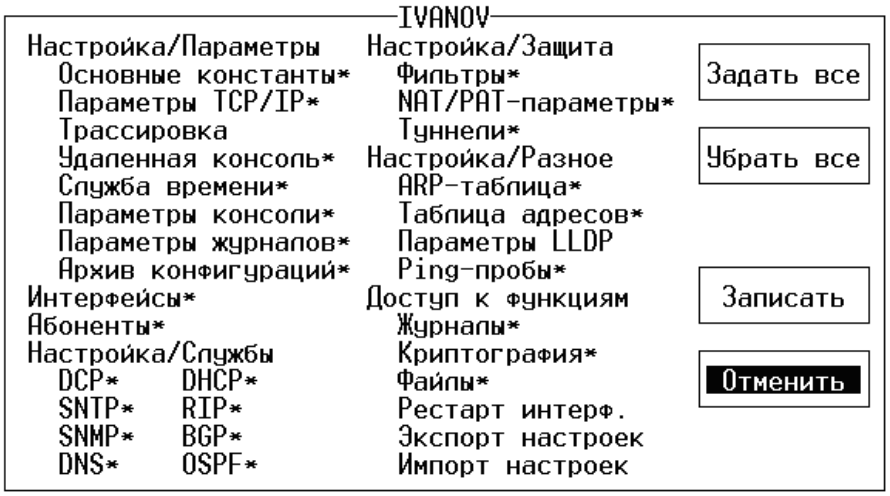


Рис. 6.6 Экран управления правами доступа абонента-администратора

Чтобы разрешить администратору доступ к выполнению той или иной функции управления, следует перевести курсор в экране на ее обозначение и нажать клавишу <Enter>. В ответ справа от обозначения функции появится отметка в виде символа «*» (звездочка). Установленные значения прав абонента-администратора вступают в силу после записи обновленного конфигуратора изделия в **БпО**.

7. Организация функционирования кластера изделий

7.1. Общие сведения

Изделие применяют в составе узлов ЗСПД с целью защиты информации, передаваемой между внутренними сегментами ЗСПД через сети общего пользования. При отказе функционирования отдельных блоков или устройств изделия обмен защищаемой информацией через данный узел ЗСПД может быть нарушен полностью или частично.

В случаях, когда к надежности работы узла ЗСПД предъявляются повышенные требования (когда даже кратковременное нарушение обработки проходящего через узел трафика недопустимо), следует организовать работу изделий на таком ответственном узле ЗСПД в виде *кластера* – системы двух взаимосвязанных изделий, осуществляющих *автоматическое резервирование* работы друг друга. Одно из изделий в конкретный момент времени выполняет в составе кластера функции *основного* изделия (изделие со статусом **MASTER**), а другое – функции *резервного* (изделие со статусом **SLAVE**). При этом осуществляется *постоянное* взаимное отслеживание состояния обоих изделий в составе кластера.

> *Примечание.* Отметим, что не все модификации изделий серии М-479Рх поддерживают функционирование в режиме кластера.

В штатном режиме работы кластера изделие **MASTER** выполняет всю обработку проходящего через узел ЗСПД трафика. В случае нарушения работы изделия **MASTER** обработку трафика *автоматически* продолжает изделие **SLAVE**, осуществляя тем самым т.н. *горячее* резервирование.

Когда работоспособность изделия, временно потерявшего статус **MASTER**, возобновится, оно снова возьмет управление на себя, вернув себе прежний статус (**MASTER**) в составе кластера.

Схема, поясняющая принципы организации кластера на основе изделий нового поколения, представлена на Рис. 7.1.

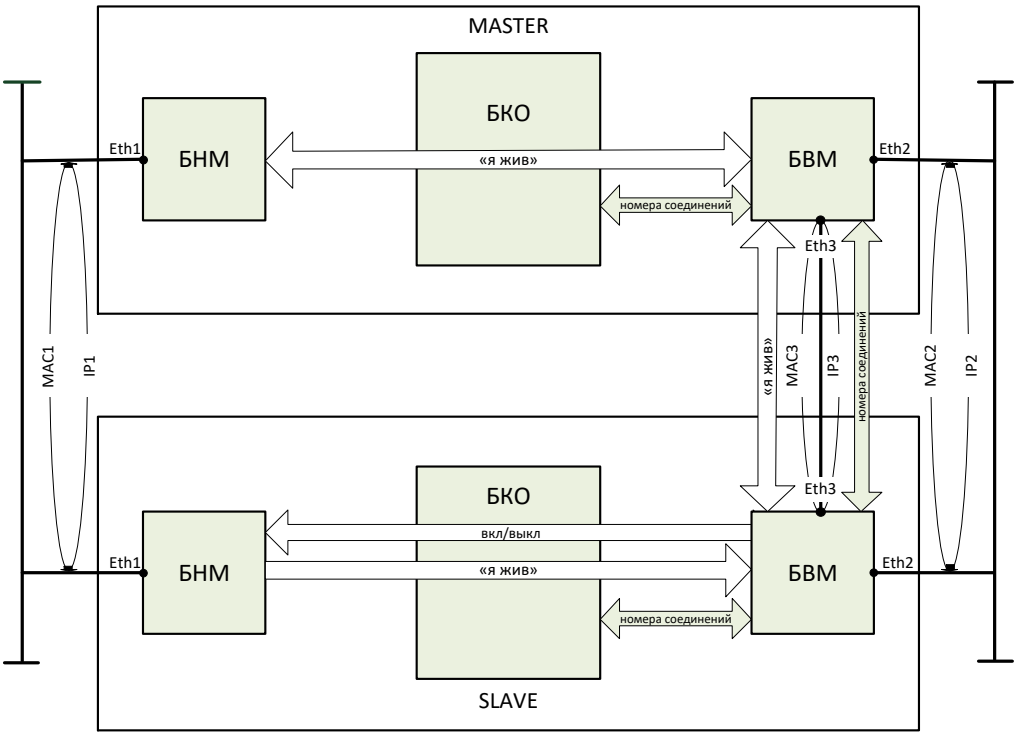


Рис. 7.1 Схема взаимодействия изделий нового поколения при функционировании в составе кластера

Основным принципом организации работы кластера является то, что каждая из локальных сетей, подключаемых на узле ЗСПД к кластеру (независимо от того, относится локальная сеть к внутреннему или к внешнему сегменту ЗСПД), должна быть физически *дважды* подключена к *соответствующим* сетевым интерфейсам каждого из изделий, образующих кластер.

При этом во время подготовки изделий к функционированию в составе кластера путем соответствующей настройки каждого из физических сетевых интерфейсов изделий должно быть обеспечено условие, когда в *каждой* из точек подключения изделий к сетям оба изделия кластера воспринимаются локальной сетью абсолютно *идентичными* с точки зрения адресации как на уровне L2, так и на уровне L3 модели OSI. Это достигается тем, что каждой паре соответствующих интерфейсов изделий в точках подключения изделий к

соответствующим локальным сетям при настройке присваиваются попарно *одинаковые* MAC-адреса и *одинаковые* IP-адреса, а также на обоих соответствующих сетевых интерфейсах изделий, составляющих кластер, выполняются идентичные настройки параметров функционирования.

Кроме того, оба изделия должны иметь *идентичные* конфигураторы параметров настройки, за исключением *статуса* изделий в составе кластера (**MASTER** или **SLAVE**).

Другими словами, входящие в кластер *два* изделия реагируют на потоки данных из локальных сетей и взаимодействуют с сетями так, как будто с локальными сетями работает *единственное* изделие (оба изделия кластера работают как одно).

При функционировании кластера **SLAVE**-устройство находится в режиме ожидания и только *слушает* соответствующие сети (через свои сетевые интерфейсы, подключенные к соответствующей сети), принимая к сведению всю информацию и никак на нее не реагируя. По внутренним сетевым интерфейсам, связывающим по *технологической* сети основное и резервное изделия кластера, изделие со статусом **MASTER** периодически посылает технологические сигналы (*пакеты-извещения*), смысл которых: «`я жив`». Изделие со статусом **SLAVE**, в свою очередь, тоже периодически посылает на изделие со статусом **MASTER** технологические пакеты «`я жив`».

Кроме сигнала «`я жив`» основное в кластере на текущий момент изделие передает на резервное актуальную информацию о параметрах (номерах) криптографических соединений для возможного последующего использования.

Если изделие со статусом **SLAVE** в какой-то момент не получит в заданное время пакет-извещение от изделия со статусом **MASTER**, то оно возьмет управление на себя и будет функционировать в качестве основного до тех пор, пока изделие, временно потерявшее статус **MASTER**, не вернется в рабочее состояние и не сообщит об этом изделию со статусом **SLAVE**.

Отметим еще раз, что оба изделия в составе кластера должны имеют *одинаковые собственные IP-адреса* блоков наружной и внутренней маршрутизации, а также *одинаковые* MAC-адреса и IP-адреса точек подключения – физических сетевых Ethernet-интерфейсов в каждой из подключенных к изделиям локальных сетей.

Когда кластер образован изделиями нового поколения, они соединяются между собой в кластер технологической сетью между блоками внутренней маршрутизации изделий (см. Рис. 7.1), т.е. *пакетами-извещениями* обмениваются между собой БВМ изделий. При этом *пакеты-извещения* содержат информацию о состоянии изделия-отправителя в целом – о состоянии всех трех его компонентов: БВМ, БНМ и БКО.

Получение необходимой информации о состоянии изделия организовано следующим образом.

В изделии со статусом **MASTER** регулярно генерируются *два* вида периодических посылок: от БНМ к БВМ и от БВМ к БНМ. Получение посылки является сигналом, что партнер (другой блок маршрутизации изделия) функционирует в штатном режиме – «жив». Посылки между блоками маршрутизации внутри изделия передаются через шифратор – БКО, поэтому БВМ, получив сигнал от БНМ, косвенно получает информацию о том, что шифратор также функционирует в штатном режиме («жив»).

БВМ изделия со статусом **MASTER** периодически опрашивает шифратор о значениях текущих номеров криптографических соединений. Полученную от шифратора информацию о текущих номерах соединений БВМ этого изделия объединяет с информацией о состоянии трех компонентов криптомаршрутизатора (БВМ, БНМ и БКО), упаковывает все в пакет-извещение и отправляет его на БВМ резервного изделия (на **SLAVE**).

В изделии со статусом **SLAVE** также регулярно генерируются посылки сигналов от БНМ к БВМ и от БВМ к БНМ. При этом посылка от БНМ к БВМ содержит сигнал «я жив», а посылка от БВМ к БНМ содержит сигнал *включения/выключения* изделия, т.е. сигнал о переводе резервного изделия из состояния **SLAVE** в состояние **MASTER** или обратно. При этом на изделии со статусом **SLAVE** непрерывно актуализируются значения *номеров соединений*, получаемых от изделия со статусом **MASTER**.

7.2. Настройка изделий для запуска кластера

Настройка изделий кластера состоит из нескольких шагов:

- настройка изделия, которое будет выполнять в кластере функции изделия со статусом **MASTER**;
- сохранение настроенного конфигуратора этого изделия в объединенной базе параметров **БпО**;
- копирование настроенного конфигуратора изделия со статусом **MASTER** на съемный машинный носитель и восстановление этого конфигуратора со съемного машинного носителя в качестве текущего конфигуратора на изделии, которое в кластере будет выполнять функции изделия со статусом **SLAVE**.

Подробнее процесс настройки изделий при подготовке их к функционированию в составе кластера рассмотрим на примере схемы взаимодействия, представленной на Рис. 7.1.

При настройке должны быть выполнены следующие действия.

1. В изделии со статусом **MASTER** присвоить значения параметрам **Собственный IP-адрес наружного маршрутизатора** и **Собственный IP-адрес внутреннего маршрутизатора** (раздел 4.1.2, с. 130).

2. В изделии **MASTER** сетевой физический Ethernet-интерфейс БВМ, который *технологически* связывает в кластере блоки внутренней маршрутизации изделий **MASTER** и **SLAVE**, создается и настраивается как стандартный физический Ethernet-интерфейс (см. раздел 2.3.1, с. 25).

   Имя интерфейса – например, ***Eth0*** (согласно обозначениям на схеме взаимодействия Рис. 7.1).

   Специальные настройки – на этом физическом интерфейсе следует установить двум параметрам значения, отличные от приведенных *по умолчанию*, а именно: снять *запрет* на обработку **Cluster-пакетов** (символ «*» справа от параметра должен отсутствовать) и *запретить* обработку **транзитных датаграмм** (символ «*» справа от параметра должен присутствовать). Значения параметров *по умолчанию* бланка управления специальными настройками интерфейса приведены на Рис. 2.8, с. 28 или Рис. 2.38, с. 50.

   Дополнительные параметры – в качестве значения параметра **MAC-адрес** интерфейса можно установить физический адрес Ethernet-адаптера или произвольное число (в нужном формате).

   > *Примечание.* Нулевое значение параметру **MAC-адрес** при настройке интерфейсов изделий, подготавливаемых к работе в составе кластера, устанавливать нельзя, т.к., напомним, при нулевом значении этого параметра считывается значение MAC-адреса из Ethernet-адаптера, заданное при его изготовлении, а при организации работы кластера оба изделия (**MASTER** и **SLAVE**) должны иметь *одинаковые* значения MAC-адресов точек подключения к соответствующей локальной сети (см. раздел 2.3, Рис. 2.9, с. 29 и раздел 2.3.2, Рис. 2.16, с. 34).

3. Прочие сетевые интерфейсы в изделии со статусом **MASTER**, которые связывают изделие **MASTER** с локальными сетями внутреннего и внешнего сегментов ЗСПД, создаются и настраиваются как стандартные физические Ethernet-интерфейсы (см. раздел 2.3.1, с. 25) или L2–Eth-интерфейсы (см. раздел 2.3.2, с. 33).

   Имена интерфейсов – например, ***Eth1*** и ***Eth2*** (согласно схеме взаимодействия Рис. 7.1).

   Специальные настройки – оставить стандартные (по умолчанию) значения всех параметров. Исключение составляет параметр **контроль в кластере** − с его помощью можно включить контроль активности интерфейса любого типа. Если параметру присвоить значение ***ДА*** (справа от параметра поставить символ «*»), то при отключении (потере активности) такого интерфейса основное изделие в составе кластера (**MASTER**) будет считаться вышедшим из строя и обработку трафика продолжит резервное изделие в составе кластера (**SLAVE**). (см. раздел 2.5, с. 50; Рис. 2.8, с. 28 или Рис. 2.38, с. 50).

   Контролировать рекомендуется наименее надежные интерфейсы.

   Дополнительные параметры – в качестве значений параметра **MAC-адрес** интерфейсов можно установить физические адреса соответствующих Ethernet-адаптеров или произвольные числа (в нужном формате). Нулевым значение параметра **MAC-адрес** оставлять нельзя (см. Примечание в п. 2), т.к. это приведет к неравенству MAC-адресов соответствующих пар сетевых интерфейсов основного и резервного изделий, что в работе кластера недопустимо.

4. Выполнить запись конфигуратора изделия со статусом **MASTER** в объединенную базу параметров **БпО** (подробнее см. раздел 1.3.2, с. 10 и РЭ на конкретное изделие).

5. Скопировать конфигуратор изделия со статусом **MASTER** на съемный носитель. Для выполнения этой процедуры служит цепочка альтернатив ГМ: **Сервис ⇨ Экспорт настроек** (см. раздел 10.7, с. 203).

6. Перенести конфигуратор изделия со съемного носителя на изделие со статусом **SLAVE**. Для выполнения этой процедуры служит цепочка альтернатив ГМ: **Сервис ⇨ Импорт настроек** (см. раздел 10.7, с. 203).

   > *Примечание.* Для переноса конфигуратора с изделия со статусом **MASTER** на изделие со статусом **SLAVE** можно применить другой способ переноса − через *архив конфигураций* (см. раздел 4.1.8, с. 143), используя другую последовательность действий: **Сохранить в архиве текущую конфигурацию ⇨ Копировать на съемный носитель ⇨ Восстановить из архива**.

7. Назначить изделие со статусом **MASTER** основным изделием кластера, а изделие со статусом **SLAVE** – резервным, установив на соответствующих изделиях необходимые значения статуса и таймера, используя цепочку альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Основные константы** (см. раздел 4.1.1, с. 129), например:

   Режим работы в кластере: *MASTER* **таймер** ***10*** (на основном изделии кластера)

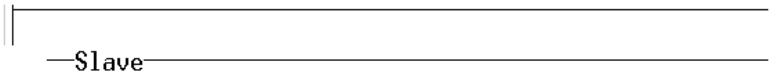
   Режим работы в кластере: *SLAVE* **таймер** ***12*** (на резервном изделии кластера).

8. Выполнить и проверить на функционирование все необходимые сетевые подключения к обоим изделиям.

9. Перезагрузить оба изделия в составе кластера.

После этого оба изделия кластера автоматически начинают работать в заданных режимах. В нижней части видеомонитора ЛКУ основного изделия появляется идентификатор режима работы **Master**:

В нижней части видеомонитора ЛКУ резервного изделия появляется идентификатор режима работы **Slave**:



Справа от идентификаторов режима работы могут следовать символы, обозначающие следующее:

На изделии со статусом **MASTER** – блок наружной маршрутизации БНМ:

- **I** – недоступен БВМ
- **C** – не активен один из интерфейсов, на котором установлен **Контроль в кластере**.

На изделии со статусом **MASTER** – блок внутренней маршрутизации БВМ:

- **S** – резервный узел недоступен
- **E** – недоступен БНМ
- **C** – не активен один из интерфейсов, на котором установлен **Контроль в кластере**

На изделии со статусом **SLAVE** – блок наружной маршрутизации БНМ:

- **A** – резервный узел активизирован
- **I** – недоступен БВМ
- **C** – не активен один из интерфейсов, на котором установлен **Контроль в кластере**

На изделии со статусом **SLAVE** – блок внутренней маршрутизации БВМ:

- **A** – резервный узел активизирован
- **E** – недоступен БНМ
- **C** – не активен один из интерфейсов, на котором установлен **Контроль в кластере**

> *Внимание!* В дальнейшем любые изменения настроек могут выполняться только на изделии со статусом **MASTER**. Отредактированный конфигуратор должен переноситься на изделие со статусом **SLAVE** так же, как при начальной настройке кластера, – с помощью съемного носителя.

8. Главное меню. Альтернатива *Консоль*

В ответ на выбор альтернативы ГМ: **Консоль** на ЛКУ выдается меню, представленное на Рис. 8.1.

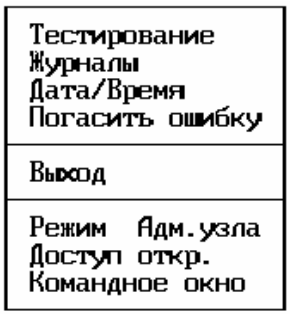


Рис. 8.1 Меню альтернативы ГМ: **Консоль**

Применение альтернатив меню **Консоль** (Рис. 8.1) обеспечивает выполнение набора разноплановых действий, пояснения к которым приведены ниже в данном разделе РНУ.

Примечания.

1. Альтернатива меню **Командное окно** настоящей версией ОПО не поддерживается.

2. Альтернативы меню **Журналы** и **Дата/Время** доступны для использования только в режиме администрирования.

8.1. Консоль ⇨ Тестирование

Выбор цепочки альтернатив ГМ: **Консоль ⇨ Тестирование** переводит изделие в режим выполнения диагностического тестирования, в котором возможно выполнение следующих стандартных процедур:

- **Ping** – процедура проверки наличия связи (получение отклика) с любым IP-ресурсом сети;
- **Trace Route** – процедура определения маршрута связи между изделием и любым IP- ресурсом сети;
- **Telnet** – процедура проверки возможности TCP-соединения с любым IP- ресурсом сети;
- **DNS-клиент** – процедура проверки работоспособности DNS-клиента маршрутизатора изделия путем отправки вводимых с клавиатуры DNS-запросов.

После того как оператор выберет одну из названных функций тестирования, программа управления выдаст запрос на ввод параметров, соответствующих выбранной процедуре, а затем на видеомониторе ЛКУ отобразит процесс выполнения тестовой процедуры.

Для каждой из процедур среди параметров должен быть один обязательный: ***address*** – IP-адрес (или мнемоническое имя) ресурса, для которого требуется выполнить процедуру.

> Мнемоническое имя ресурса должно быть занесено администратором в адресную таблицу хостов, известных изделию (см. раздел 4.2.2, с. 147). Если адреса в таблице не окажется, то перед выполнением тестовой процедуры маршрутизатор изделия автоматически выполнит DNS-запрос для определения IP-адреса по заданному мнемоническому имени.

Ниже приведено краткое описание каждой из процедур тестирования, набора требуемых параметров, а также интерпретация получаемых результатов.

8.1.1. Процедура PING

С целью диагностического тестирования персонал изделия может вручную запустить PING-процедуру для проверки наличия связи между изделием и каким-либо IP-ресурсом в сети, к которой подключено изделие.

Команда запуска процедуры **PING** имеет следующие параметры:

ping [-d length] [-t interval] [-i] [-f] address

address – IP-адрес ресурса в сети, наличие связи изделия с которым тестируется (обязательный параметр).

-d length – размер добавляемых в PING-пакеты данных. По умолчанию длина зондирующего пакета составляет 64 байта.

-t interval – интервал (в секундах) отправки PING-пакетов. По умолчанию – 1 секунда.

-i – режим инкремента IP-адреса. Если ***-i*** задан, то при отправке каждого последующего PING-пакета IP-адрес получателя будет увеличиваться на 1. Это средство дает возможность быстро проверять наличие работающих в сети узлов по целой серии IP-адресов (например, можно сразу проверить все адреса сети класса C).

-f – при наличии такого параметра в IP-заголовке каждого PING-пакета устанавливается флаг *запрета фрагментации* (DF).

Выполняется процедура **PING** следующим образом. Изделие формирует ICMP-пакеты типа «Echo request» (PING-запросы) и направляет их в адрес удаленного IP-устройства. Если указано в команде запуска, в ICMP-пакет добавляется поле данных заданной длины. Пакеты формируются непрерывно и посылаются через заданные параметром интервалы времени. Чтобы прервать формирование PING-запросов, оператору достаточно нажать клавишу <Esc>.

Удаленное устройство, получив ICMP-пакет, согласно системным требованиям internet/intranet-технологии обязано сформировать и послать ответ в виде ICMP-пакета типа «Echo reply» (PING-ответ).

После того как будет запущена PING-процедура, на видеомонитор ЛКУ будут выданы две строки следующего формата:

Pinging <address> (<address_IP>); **data** <length> **interval** <interval> **s**.
sent rcvd % rtt avg_rtt mdev

В первой строке повторяется значение параметров из команды запуска процедуры, при этом:

address – значение параметра из команды (IP-адрес или мнемоническое имя);

address_IP – IP-адрес, соответствующий значению параметра; если в команде задан IP-адрес, то два первых параметра в строке совпадают.

Вторая строка содержит заголовки граф будущей таблицы (в эти графы в дальнейшем будут заноситься данные из PING-ответа):

sent – порядковый номер запроса;

rcvd – порядковый номер ответа;

% – процент запросов, на которые пришли ответы;

rtt_(round-trip time) – время прохождения IP-датаграммы от отправителя (от интерфейса изделия) до получателя и обратно;

avg_rtt – среднее значение **rtt**;

mdev – отклонение **rtt** от **avg_rtt**.

Полученные PING-ответы преобразуются и выводятся на консоль в виде таблицы. Если таблица не заполняется данными, значит, удаленный ресурс *недоступен.*

Ниже на Рис. 8.2 приведен пример экрана с результатами выполнения процедуры PING.

```
ping 192.168.2.1
```

```
Pinging: 192.168.2.1 (192.168.2.1); data 64 interval 1 s.
      sent      rcvd    %       rtt   avg_rtt      mdev
         1         1  100         0         0         0
         2         2  100         0         0         0
         3         3  100         0         0         0
         4         4  100         0         0         0
Pinging: 192.168.2.1 (192.168.2.1); data 64 interval 1 s.
      sent      rcvd    %       rtt   avg_rtt      mdev
         5         5  100         0         0         0
         6         6  100         0         0         0
         7         7  100         0         0         0
         8         8  100         0         0         0
         9         9  100         0         0         0
```

Рис. 8.2 Пример экрана с результатами выполнения процедуры PING

Признаком того, что все PING-запросы дошли до удаленного ресурса и все PING-ответы получены, является совпадение данных в графах **sent** и **rcvd**.

8.1.2. Процедура Trace route

Команда запуска процедуры **Trace Route**:

Trace Route [-m maxttl] [-q nqueries] [-w waittime] address

address – IP-адрес ресурса в сети, состояние тракта передачи данных с которым тестируется (обязательный параметр).

-m maxttl – максимальное количество серий UDP-проб. По умолчанию 30.

-q nqueries – количество UDP-проб в серии. По умолчанию – 3.

-w waittime – интервал времени (в секундах) между отправками проб. По умолчанию – 5.

Выполняется процедура **Trace Route** следующим образом. Изделие отправляет UDP-датаграммы (UDP-пробы) в адрес сетевого ресурса с IP-адресом, указанным с помощью значения параметра <**address**>,

используя заведомо не обрабатываемый хостами номер порта (больше **30000**). Если UDP-датаграмма достигнет хоста назначения, то в адрес отправителя будет отправлено ICMP-сообщение «`port unreachable`», что будет означать нормальное завершение процедуры **Trace Route**. Если UDP-датаграмма будет снята с доставки промежуточным маршрутизатором из-за обнуления поля датаграммы `ttl`, то отправитель (изделие) получит ICMP-сообщение «`time exceeded`» (*время превышено*). Адрес маршрутизатора, снявшего датаграмму с доставки, будет указан в ICMP-сообщении в качестве адреса отправителя.

При выполнении процедуры **Trace Route** делается несколько серий проб с последовательно увеличивающимся значением **ttl** от 1 до значения параметра **maxttl**. В каждой серии отправляется по **nqueries** UDP-проб. Отправка каждой следующей UDP-пробы производится немедленно после получения ответа на предыдущую пробу. Если ответ на пробу не придет в течение **waittime** секунд после отправки, то фиксируется состояние «проба не дошла» и выполняется отправка следующей пробы.

По результатам отправки проб и получения ответов на них строится таблица трассировки. Каждая строка таблицы соответствует одной серии проб. Графы таблицы содержат следующую информацию:

1 графа – номер серии проб;

2 графа – адрес хоста, вернувшего пробу;

3 графа и последующие – время прохождения проб данной серии. Для каждой пробы в круглых скобках указывается время (в миллисекундах), прошедшее с момента отправки пробы до получения ответа на нее. Если ответ на пробу не приходит в течение времени **waittime**, то в строке ставится символ *****. В ответ на пробу может быть получено ICMP-сообщение об ошибке доставки пробы. Тогда в таблице ставится восклицательный знак и буква, идентифицирующая причину ошибки доставки (возможные коды окончания процедуры **Trace Route** приведены ниже). По окончании процедуры **Trace Route** выдается сообщение

`Traceroute done: <характеристика окончания>.`

Ниже приведены два примера выполнения процедуры **Trace Route**: представлена информация, выдаваемая на видеомонитор ЛКУ.

Пример 1. Успешное завершение **Trace Route**.

```
traceroute 198.105.232.1
Traceroute to (198.105.232.1), 30 hops max. 3 probes, 5 waittime
 1:    *  *  *
 2:    194.67.3.66       (0 ms)      (0 ms)       (0 ms)
 3:    194.67.1.33       (660 ms)    (650 ms)     (660 ms)
 4:    140.174.209.1     (660 ms)    (720 ms)     (710 ms)
 5:    140.174.122.17    (720 ms)    (660 ms)     (660 ms)
 6:    140.174.125.1     (660 ms)    (660 ms)     (660 ms)
 7:    204.70.32.49      (710 ms)    (660 ms)     (710 ms)
 8:    204.70.2.161      (660 ms)    (880 ms)     (770 ms)
 9:    204.70.1.49       (1040 ms)   *            (1040 ms)
 10:   204.70.2.146      (830 ms)    (930 ms)     (1150 ms)
 11:   204.70.52.6       (770 ms)    (880 ms)     (820 ms)
 12:   *  *  *
 13:   198.104.192.9     (830 ms)    (880 ms)     (880 ms)
 14:   131.107.249.1     (660 ms)    (660 ms)     (710 ms)
 15:   198.105.232.1     (660 ms)
Traceroute done: normal
```

Пример 2. Завершение **Trace Route** с ошибкой.

```
Trace route 198.105.200.1
Traceroute to (198.105.200.1), 30 hops max. 3 probes, 5 waittime
 12:   192.147.179.5     (720 ms)    (710 ms)     (660 ms)
 13:   660 ms !H
Traceroute done: !! (192.147.179.5) icmp_type=3 icmp_code=1
```

В таблице трассировки стоит восклицательный знак и символ `H`.

В сообщении об ошибочном завершении **TraceRoute** указывается адрес хоста, вернувшего ошибку (`192.147.179.5`), и значения полей `type` и `code` ICMP-сообщения.

В приведенном примере: хост `192.147.179.5` вернул ICMP-сообщение с `icmp_type=3` (Destination Unreachable Message) и `icmp_code=1` (Host unreachable).

Возможные коды окончания процедуры TraceRoute

icmp_code=	0	!N	Net unreachable
	1	!H	Host unreachable
	1	!P	Protocol unreachable
	4	!F	Fragmentation needed and DF set
	5	!S	Source route failed

8.1.3. ***Процедура Telnet***

Формат команды запуска процедуры **`Telnet`**:

`telnet [-8] [-v] [-e] [-u] address [port]`

`address` – обязательный параметр.

`-8` – включение прозрачного (8-битового) режима связи с удаленным хостом. Если прозрачный режим включен, то программа управления изделием будет «договариваться» с удаленным хостом на работу в 8-битовом режиме. Если удаленный хост откажется, то изделие переведет **`telnet`**-соединение в 7-битовый режим (в 7-битовом режиме у всех входящих символов старшие биты устанавливаются в нуль).

`-e` – отказ от предлагаемого удаленным хостом режима перехода на локальное эхо (будут отвергаться запросы WILL ECHO от удаленного хоста).

`-u` – включение принятого в UNIX-системах режима завершения строк. Если UNIX-режим включен, то перед отправкой строк в линию изделие заменит первый слева символ `\r` (`CR`) на символ `\n` (`LF`) и аннулирует оставшиеся справа символы строки. Если в команде задан параметр ***`-e`***, UNIX-режим не включится.

`-v` – включение индикации процесса установления и разрыва соединения.

`port` – номер порта (тип сервера), с которым должно быть установлено соединение. По умолчанию – 23 (**`telnet`**-сервер).

Пример 1. ***`telnet -8 -v 192.168.1.1`***

Команда на запуск **`telnet`**-соединения в прозрачном режиме (***`-8`***) с индикацией процесса установления и разрыва соединения (***`-v`***) с ресурсом, имеющим IP-адрес ***`192.168.1.1`***.

Пример 2. ***`telnet mail.test.ru 25`***

Команда на запуск **`telnet`**-соединения SMTP-сервером (порт 25) хоста ***`mail.test.ru`***.

Если необязательные параметры команды не заданы, то будет установлено 7-битовое **`telnet`**-соединение без индикации процесса установления и разрыва соединения. Будет устанавливаться режим обработки эха, предлагаемый удаленным хостом.

После установления **`telnet`**-соединения изделие предоставляет прозрачный канал доступа к услугам удаленного ресурса в режиме виртуального терминала. При этом вводимая с клавиатуры информация с помощью программа управления изделием преобразуется в **`telnet`**-формат и передается на удаленный ресурс. И наоборот, вся поступающая от ресурса информация преобразуется из **`telnet`**-формата и отображается в **`telnet`**-окне.

`Telnet`-соединение сохраняется либо до тех пор, пока оно не будет разорвано по инициативе удаленного ресурса, либо пока оператор не нажмет клавишу <Esc>.

8.1.4. ***Процедура DNS-клиент***

Формат команды запуска процедуры **`DNS-клиент`**:

`dnsquery address`

`address` – обязательный параметр.

Выполняется процедура следующим образом. По команде формируется DNS-запрос в формате, принятом в сетях, работающих согласно системным требованиям `internet/intranet`-технологии, для работы с DNS-серверами. Получив запрос, DNS-сервер отыскивает в своей базе данных всю информацию, касающуюся запрошенного адреса (адресную и вспомогательную), и отсылает ее маршрутизатору изделия, выдавшему запрос. Полученная информация в удобочитаемом виде выводится на видеомонитор ЛКУ.

8.2. Консоль ⇨ Журналы

При выборе цепочки альтернатив ГМ: **Консоль ⇨ Журналы** на видеомонитор ЛКУ выдается представленный на Рис. 8.3 экран управления работой с файлами журналов изделия (о журналах

см. раздел ***Приложение Е***, с. 248). С его помощью администратор изделия получает возможность просмотреть содержимое накопленных журналов для принятия оперативных решений о работоспособности изделия. Никаких средств модификации журналов в составе ПО изделия нет.

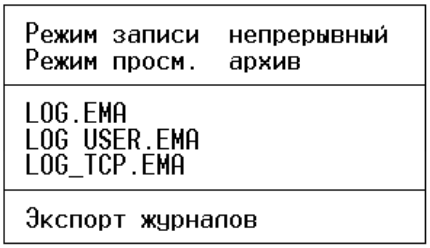


Рис. 8.3 Экран управления работой с файлами журналов изделия

В средней части экрана приведен список файлов журналов изделия. Чтобы просмотреть тот или иной **LOG**-файл, следует перевести курсор на строку с его именем и нажать клавишу <Enter>. На видеомонитор ЛКУ будет выдана первая страница журнала и предоставлены средства для просмотра остальной информации.

Режимы записи в журналы и просмотра журналов, а также возможные значения параметров подробно рассмотрены в разделе 4.1.7, с. 140. В процессе просмотра администратор может изменить значение параметра **Режим просм.** (Рис. 8.3). Это изменение сохранится до следующего изменения или до перезапуска изделия.

Экспорт журналов (Рис. 8.3). Альтернатива позволяет, не останавливая работу изделия, извлечь все системные журналы изделия (**LOG**-файлы), которые накоплены на данный момент, и переместить их на съемный носитель.

> *Примечание.* Экспорт журналов возможен только при значении параметра **Режим записи** – *непрерывный*.

Перед выбором альтернативы следует подключить съемный носитель к соответствующему разъему изделия (см. РЭ на конкретное изделие) и затем выбрать альтернативу **Экспорт журналов**. Программа управления выдаст на видеомонитор ЛКУ экран выбора съемного носителя, аналогичный представленному на Рис. 8.4.

Рис. 8.4 Экран выбора съемного носителя

В верхней части экрана выводится в круглых скобках количество подключенных съемных носителей (после выбора носителя − число элементов в его файловой структуре) и текущий путь для размещения экспортируемых журналов.

В средней части экрана выводится номер (описатель) съемного носителя − FLASH-диска, подключенного к USB-порту. В общем случае описателей может быть несколько.

Администратор должен перевести курсор на описатель съемного носителя и нажать клавишу <Enter>. На видеомонитор ЛКУ будет выдан экран с файловой структурой съемного носителя. На этом экране надо выбрать директорию, в которую будет выполнен экспорт журналов; при необходимости директорию можно создать – с помощью клавиши <F7>.

Выбрав (или создав) необходимую директорию, следует нажать клавишу <F2>. В ответ будет выполнен запуск процедуры экспорта журналов изделия. При этом выполняются следующие действия.

1. Текущие файлы журналов закрываются и переносятся в специально предусмотренную для этой цели директорию экспорта во внутренней памяти изделия. На время переноса файлов журналов работа программы управления по обслуживанию сетевых интерфейсов изделия приостанавливается.
2. Открываются новые файлы журналов и работа программы управления возобновляется.
3. Из директории экспорта все файлы с теми же именами будут переданы (скопированы) на съемный носитель в указанную директорию с одновременным расчетом контрольной суммы по алгоритму CRC-32. В этой же директории на съемном носителе формируются файлы с именами <имя_журнала>**.crc**, в каждый из которых записывается значение контрольной суммы соответствующего файла журнала.

4. В новом файле **LOG.EMA** фиксируются все контрольные суммы скопированных файлов с указанием имени журнала, даты и времени завершения копирования.
5. В случае успешного копирования всех журналов на съемный носитель старые файлы журналов удаляются из внутренней памяти изделия, а освободившееся пространство становится доступным для дальнейшей работы.

   Примечание. В процессе хранения файлов журналов на съемном носителе и работы с ними может возникнуть необходимость убедиться в их целостности. Вычислить контрольную сумму любого из файлов можно с помощью утилиты **CRC32.exe**. Утилита не входит в комплект поставки изделия, но она может быть предоставлена по запросу Заказчика.

В случае возникновения ошибок копирования старые файлы журналов (и скопированные, и не скопированные) остаются на внутреннем диске (в директории экспорта), и повторное выполнение команды **Консоль ⇨ Журналы ⇨ Экспорт** начинается с пункта 3 процедуры экспорта журналов: *все* файлы из директории экспорта будут скопированы на съемный носитель (скопированные ранее файлы из директории экспорта будут переданы повторно).

Процесс экспорта журналов отражается на экране и заносится в новый основной журнал (файл **LOG.EMA**). При этом фиксируется время начала копирования, директория экспорта, факты копирования вместе с указанием имени скопированного файла журнала, даты и времени завершения копирования, а также контрольная сумма.

8.3. Консоль ⇨ Выход

Выбор цепочки альтернатив ГМ: **Консоль ⇨ Выход** предназначен для корректной перезагрузки ОПО маршрутизаторов изделия. При выборе цепочки альтернатив на видеомонитор ЛКУ выдается экран управления перезагрузкой ОПО маршрутизатора изделия, представленный на Рис. 8.5.

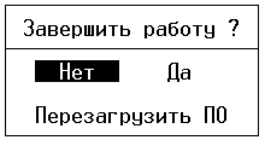


Рис. 8.5 Экран управления перезагрузкой ОПО маршрутизатора

В случае работы с БНМ (средства блока ЛКУ подключены к БНМ):

- при ответе **Да** – будет выполнена перезагрузка наружного маршрутизатора;
- при ответе **Перезагрузить ПО** – будет выполнена перезагрузка обоих маршрутизаторов.

  Примечание. По команде от БНМ сигнал на перезагрузку через шифратор передается на внутренний маршрутизатор. БВМ принимает сигнал и через шифратор посылает на БНМ свой сигнал о готовности к перезагрузке. После этого оба маршрутизатора будут перезагружены.

В случае работы с БВМ (средства блока ЛКУ подключены к БВМ):

- при ответе **Да** – будет выполнена перезагрузка внутреннего маршрутизатора,
- при ответе **Перезагрузить ПО** – никакие действия не выполняются.

8.4. Консоль ⇨ Режим

Альтернатива **Режим** позволяет установить уровень доступа обслуживающего персонала к управлению изделием. Выбор цепочки альтернатив ГМ: **Консоль ⇨ Режим** приводит к выводу на видеомонитор ЛКУ меню выбора уровня доступа к управлению изделием, представленного на Рис. 8.6.

Рис. 8.6 Меню выбора уровня доступа к управлению изделием

Выбор одного из двух первых значений меню позволяет задать уровень доступа при локальном управлении соответствующим блоком маршрутизации изделия (БВМ или БНМ):

- в режиме **Оператор** разрешается только просмотр (контроль) различной информации, доступа к функциям конфигурирования и управления нет;
- в режиме **Администратор узла** доступны функции контроля, конфигурирования и управления в полном объеме.

Примечание. Может быть создано несколько учетных записей администраторов, каждый из которых имеет доступ только к определенному набору функций управления изделием (см. раздел 6, с. 170).

Непосредственно после запуска изделие функционирует в режиме **Оператор**. Возможность переключения функционирования изделия в режим **Администратора узла** защищена процедурой ввода пароля. При наличии нескольких администраторов изделия каждый из них для допуска к работе должен ввести свой пароль.

Примечание. После гашения экрана и повторного его включения (см. раздел 4.1.6, с. 137) функционирование изделия автоматически переводится в режим **Оператор**.

Выбор альтернативы меню **Администратор сети** переводит изделие в режим, при котором он получает возможность удаленного управления другими аналогичными изделиями (работа в режиме **Администратор сети** подробно описана в разделе 11, с. 204). Возможность переключения функционирования изделия в режим **Администратора сети** защищена процедурой ввода пароля.

8.4.1. Пароль Администратора узла

В изделии предусмотрено два вида формирования пароля администратора и, соответственно, два способа ввода пароля в изделие по запросу программы управления:

- первый вид – это набор алфавитно-цифровых символов, удовлетворяющий требованиям, заданным при настройке параметров абонента-администратора (см. раздел 6.4.2, с. 172); администратор должен знать пароль и по запросу программы управления вводить его вручную с клавиатуры;
- второй вид – пароль по команде администратора узла генерирует программа управления и размещает его на съемном носителе; администратор должен хранить этот носитель в надежном месте и предъявлять его по запросу программы управления.

Вид формирования и режим ввода пароля администратора (с клавиатуры или со съемного носителя) устанавливается на предприятии-изготовителе и не может быть .

8.4.2. Замена заводского пароля администратора узла

В процессе подготовки изделия к работе на объекте эксплуатации администратор должен выполнить замену пароля предприятия-изготовителя на пароль, используемый службой эксплуатации изделия.

Изделие поставляется заказчику со сформированным на предприятии-изготовителе (заводским) алфавитно-цифровым паролем администратора узла вне зависимости от установленного режима ввода пароля. После запуска изделие начинает работу в режиме **Оператор**; для выполнения дальнейших действий по замене пароля изделие надо перевести в режим **Администратор узла** − выбрать цепочку альтернатив ГМ: **Консоль ⇨ Режим** и в полученном меню (Рис. 8.6) выбрать альтернативу **Администратор узла**. На видеомонитор ЛКУ будет выдан запрос, представленный на Рис. 8.7:

```
Пароль администратора (0 неверных вводов) :
```

Рис. 8.7 Запрос на ввод пароля администратора

В ответ следует ввести с клавиатуры блока ЛКУ, подключенного к наружному или внутреннему маршрутизатору, алфавитно-цифровой пароль администратора, сформированный предприятием-изготовителем (**adm**, если не оговорено иное).

Примечание. В изделии действуют два независимых пароля администратора: пароль для администрирования на БВМ и пароль для администрирования на БНМ. Процедуры ввода паролей выполняются независимо на двух блоках маршрутизации. Перевод изделия в режим администрирования может быть выполнен как при работе на БВМ, так и при работе на БНМ.

Если в изделии установлен режим ввода пароля с клавиатуры, то после ввода заводского пароля перевод изделия в режим **Администратор узла** режим заканчивается. Администратор узла должен заменить заводской пароль на свой (процедура смены пароля описана ниже − раздел 8.4.3, с. 185).

Если изделием поддерживается режим ввода пароля со съемного носителя, то следует:

- установить в устройство ввода/вывода маршрутизатора (наружного или внутреннего) съемный носитель, предназначенный для хранения генерируемого программой управления пароля администратора узла;
- выбрать цепочку альтернатив ГМ: **Консоль ⇨ Режим**;
- в появившемся меню выбора уровня доступа к управлению изделием (Рис. 8.6) выбрать альтернативу **Администратор узла**;

- получив запрос на ввод пароля (Рис. 8.7), ввести с клавиатуры блока ЛКУ, подключенного к необходимому блоку маршрутизации, алфавитно-цифровой пароль предприятия-изготовителя для администратора узла (**adm**, если не оговорено иное).

После ввода пароля программа управления выдаст представленный на Рис. 8.8 запрос на установку в USB-устройство ввода/вывода требуемого маршрутизатора изделия (наружного или внутреннего) съемного носителя, предназначенного для хранения пароля.

```
Будет выполнена генерация пароля администратора.
Выберите сменный носитель.
```

Рис. 8.8 Запрос на установку съемного носителя для формирования пароля администратора

После нажатия клавиши <Enter> программа управления выдаст на видеомонитор ЛКУ экран выбора съемного носителя со списком устройств ввода/вывода, аналогичный представленному на Рис. 4.21 (подробнее см. раздел 4.1.8, с.143).

Администратор должен перевести курсор на описатель требуемого съемного носителя, нажать клавишу <Enter> и затем сразу нажать клавишу <F2>. В ответ программа управления сгенерирует пароль **Администратора узла**, запишет его на носитель (пароль всегда записывается в корневую директорию носителя) и выдаст сообщение об успешном выполнении операции.

После извлечения носителя и нажатия клавиши <Enter> работа изделия будет переведена в режим **Администратор узла**.

> *Внимание!* Рекомендуется *изготовить* резервную копию файла с паролем **Администратора узла** (файл с именем **ADMPSWD.dat**) на другом носителе, обеспечив его надежное хранение.

В дальнейшем для перехода из режима **Оператор** в режим **Администратор узла** следует вставить в разъем устройства ввода/вывода съемный носитель с паролем, выбрать цепочку альтернатив ГМ: **Консоль ⇨ Режим** и в полученном меню (Рис. 8.6) выбрать альтернативу **Администратор узла**. Программа управления выдаст на видеомонитор ЛКУ экран выбора съемного носителя со списком устройств ввода/вывода. В этом списке следует переместить курсор на строку с описателем того устройства, к которому подключен носитель, содержащий пароль, нажать клавишу <Enter> и в появившемся окне нажать клавишу <F2> – программа управления считает пароль и переведет изделие в режим **Администратор узла**. После этого съемный носитель можно вынуть из разъема

8.4.3. *Смена паролей администратора узла и администратора сети*

Смена пароля администратора узла

При настройке изделия, как правило, устанавливается интервал времени, по истечении которого пароль должен быть заменен (см. раздел 6.4.2, с. 172). Кроме того, необходимость в замене пароля может возникнуть при нарушении его конфиденциальности или в соответствии с регламентом, принятым в эксплуатирующей ЗСПД организации.

> *Примечание.* Если в изделии установлен режим ввода пароля со съемного носителя, то перед началом выполнения операции смены пароля надо вставить в разъем устройства ввода/вывода соответствующего маршрутизатора съемный носитель, на котором хранится пароль.

Чтобы сменить пароль **Администратора узла**, следует выбрать цепочку альтернатив ГМ: **Настройка ⇨ Абоненты**, войти в любую из групп абонентов, перевести курсор на строку с именем администратора и нажать клавишу <F4> (см. раздел 6.2, с. 170). На видеомонитор ЛКУ будет выдан экран настройки параметров паспорта абонента (Рис. 6.4, с. 172), содержащий паспорт администратора, в котором следует выбрать альтернативу **Пароль**. На экран будет выведено окно, позволяющее ввести новое значение алфавитно-цифрового пароля. После ввода нового значения надо переместить курсор на альтернативу **Записать** и нажать клавишу <Enter>.

Если изделием поддерживается режим ввода пароля с клавиатуры, то на этом процедура смены пароля администратора заканчивается.

Если изделием поддерживается режим ввода пароля *со съемного носителя*, то после ввода нового (обязательно *нового*!) значения алфавитно-цифрового пароля и завершения работы с экраном настройки параметров паспорта абонента (Рис. 6.4) через альтернативу **Записать** программа управления выдаст представленное на Рис. 8.9 сообщение:

```
Будет выполнена генерация пароля администратора.
Выберите сменный носитель.
```

Рис. 8.9 Сообщение о необходимости подготовки сменного носителя для сгенерированного пароля

Администратор должен нажать клавишу <Enter>. После этого будет выполнена та же последовательность действий, что и при первоначальной генерации пароля.

Примечания.

1. При использовании пароля на съемном носителе администратор должен знать и помнить значение и алфавитно-цифрового пароля. Алфавитно-цифровой пароль понадобится, если выйдет из строя (будет поврежден или утерян) съемный носитель. При наличии разрешения на вскрытие корпуса моноблока изделия и известном алфавитно-цифровом пароле администратора узла можно выполнить процедуру генерации пароля администратора на новом носителе.
2. По отдельному заказу изделие может поставляться со съемным носителем, на котором уже сгенерирован пароль. По условиям безопасности эксплуатации этот пароль является технологическим и должен быть обязательно заменен при первом запуске изделия на объекте эксплуатации.

Смена пароля администратора сети

Изделие поставляется заказчику со сформированным на предприятии-изготовителе (заводским) паролем администратора сети. Пароль администратора сети может быть только алфавитно-цифровым.

Для смены пароля администратора сети надо перевести работу изделия в режим **Администратора сети**: выбрать цепочку альтернатив ГМ: **Консоль ⇨ Режим** и в полученном меню (Рис. 8.6) активизировать альтернативу **Администратор сети**.

На видеомонитор ЛКУ будет выведен запрос на ввод пароля, представленный на Рис. 8.10.

```
Введите пароль (F1 - сменить) :
```

Рис. 8.10 Запрос на ввод пароля администратора сети

В ответ следует ввести пароль администратора сети и нажать клавишу <F1>. Программа управления предложит ввести новый пароль и затем попросит повторить его еще раз (Рис. 8.11).

```
Задайте пароль для следующего входа : ******

Повторите пароль для следующего входа : ******
```

Рис. 8.11 Два запроса на ввод нового пароля администратора сети

8.5. Консоль ⇨ Доступ

Выбор цепочки альтернатив ГМ: **Консоль ⇨ Доступ** позволяет персоналу изделия открыть или при необходимости закрыть абонентам доступ к работе с изделием.

В штатном режиме работы изделия доступ *открыт*, т.е. разрешен вход абонентам для работы со службами и сервисами изделия. Если требуется, чтобы работа изделия с абонентами была принудительно прекращена (например, необходимо планово выключить изделие, или необходимо вывести сведения о статистике работы изделия в файл, или выполнить какие-то другие действия, требующие отсутствия работающих с изделием абонентов), то доступ следует закрыть. При этом будет запрещен вход в систему новым абонентам; все работающие абоненты смогут безо всяких помех закончить сеанс.

9. Главное меню. Альтернатива *Диагностика*

Сбор информации о работе отдельных компонентов изделия и диагностика состояния процессов, происходящих в изделии при обработке трафика, в значительной мере осуществляется персоналом изделия путем выбора альтернативы ГМ **Диагностика**. После активизации альтернативы на видеомонитор ЛКУ выводится представленное на Рис. 9.1, с. 187 меню, содержащее функции диагностики.

Это меню предоставляет возможность оперативного вывода на видеомонитор ЛКУ различной информации, отражающей текущее состояние изделия. Анализ такой информации позволяет персоналу изделия быстро находить решение проблем, возникающих в процессе эксплуатации изделия, обусловленных ошибками в настройке изделия или специфическими условиями работы телекоммуникационного окружения изделия.

Это меню предоставляет возможность оперативного вывода на видеомонитор ЛКУ различной информации, отражающей текущее состояние изделия. Анализ такой информации позволяет персоналу изделия быстро находить решение проблем, возникающих в процессе эксплуатации изделия, обусловленных ошибками в настройке изделия или специфическими условиями работы телекоммуникационного окружения изделия.

Большая часть средств, предоставляемых меню альтернативы ГМ **Диагностика**, рассчитана на пассивное наблюдение за состоянием процессов, происходящих в изделии, поэтому эти средства доступны не только Администратору узла, но и Оператору.

В левый нижний угол рамки меню выводится значение счетчика, фиксирующего прохождение IP-датаграмм через изделие, если в правилах IP-фильтрации установлен режим фиксации датаграмм (см. раздел 3.2.1.9, с. 108).

Рис. 9.1
Меню альтернативы ГМ **Диагностика**

9.1. Диагностика ⇨ Параметры

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Параметры** приводит к выдаче на видеомонитор ЛКУ меню альтернативы **Параметры** (см. Рис. 9.2).

Рис. 9.2 Меню управления сведениями о параметрах работы при диагностике

Выбор альтернатив: **Основные константы**, **Параметры TCP/IP** и **Трассировка** (Рис. 9.2) позволяет просмотреть текущие значения параметров настройки, заданные администратором (изменить указанные параметры средствами диагностики нельзя).

- **Основные константы** (подробнее см. раздел 4.1.1, с. 129);
- **Параметры TCP/IP** (подробнее см. раздел 4.1.2, с. 130);
- **Трассировка** – служит для оперативного управления текущими режимами трассировки происходящих в изделии процессов. Устанавливает режимы трассировки так же, как они устанавливаются при выборе цепочки альтернатив ГМ: **Настройка ⇨ Параметры ⇨ Трассировка** (подробнее см. раздел 4.1.3, с. 131), но без сохранения настроек в конфигураторе изделия. Другими словами, установленные с помощью рассматриваемой альтернативы режимы трассировки действуют только до перезапуска изделия или до их явной отмены.

9.2. Диагностика ⇨Интерфейсы

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы** приводит к выдаче на видеомонитор ЛКУ меню альтернативы **Интерфейсы** (см. Рис. 9.3).

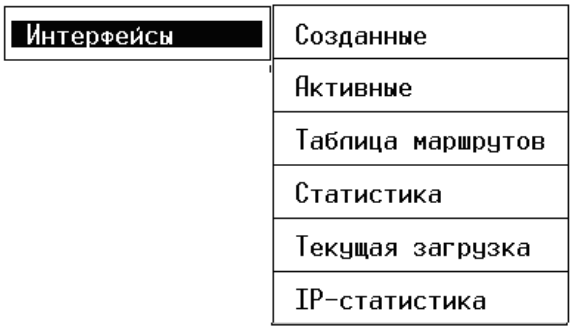


Рис. 9.3 Сведения об интерфейсах изделия при диагностике

Выбор альтернатив этого меню позволяет проконтролировать различные аспекты текущего состояния сетевых интерфейсов изделия.

9.2.1. *Созданные*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ Созданные** приводит к выдаче на видеомонитор ЛКУ экрана, аналогичного представленному на Рис. 9.4. Экран позволяет просматривать параметры всех сетевых интерфейсов, созданных на обоих маршрутизаторах изделия.

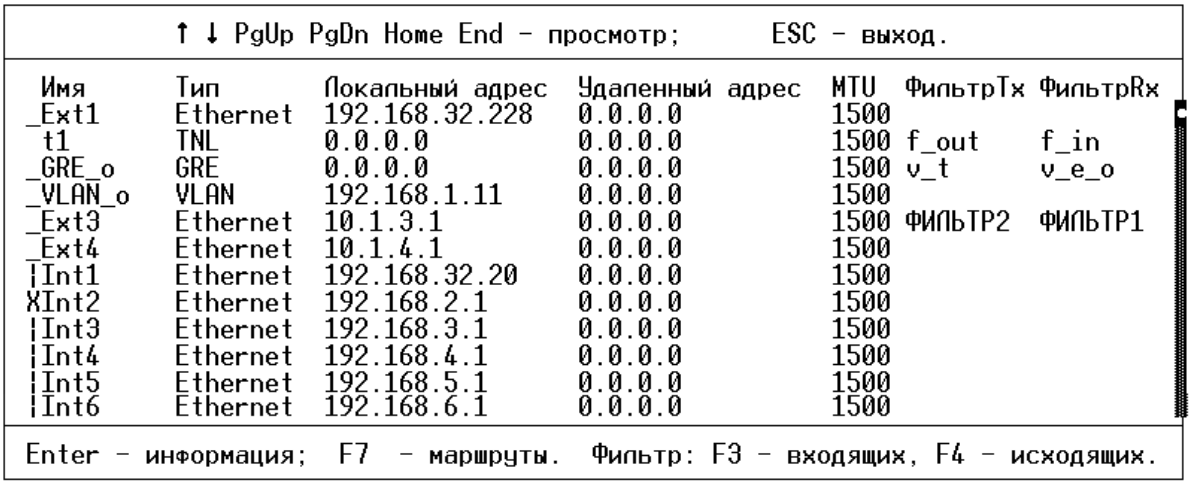


Рис. 9.4 Диагностика созданных сетевых интерфейсов изделия

Формат вывода описателей интерфейсов на экран (Рис. 9.4) практически совпадает форматом, подробно описанным при конфигурировании интерфейсов (см. раздел 2.2, с. 21). Отличия: здесь отсутствуют данные о *дополнительных* параметрах интерфейсов и в двух последних столбцах приведены имена фильтров, исходящих (**Tx**) и входящих (**Rx**).

В первой позиции строки описателя интерфейса размещается символ, определяющий принадлежность интерфейса блоку маршрутизации: символ <_> обозначает принадлежность интерфейса блоку наружного маршрутизатора – БНМ, символ <|> – принадлежность интерфейса блоку внутреннего маршрутизатора – БВМ, символ <пробел> – принадлежность интерфейса (например, TNL-интерфейса) изделию в целом; символ <X> означает, что интерфейс отключен (индикация статуса интерфейса с помощью цвета здесь не предусмотрена).

В нижней части экрана приведены сведения о возможных действиях персонала.

Enter – информация (Рис. 9.4). Для получения развернутой информации о параметрах интерфейса следует перевести курсор на строку с описателем этого интерфейса и нажать клавишу <Enter>.

F7 – маршруты (Рис. 9.4). Для просмотра таблицы маршрутов интерфейса следует перевести курсор на строку с описателем этого интерфейса и нажать клавишу <F7>.

Фильтр: F3–входящих, **F4–исходящих** (Рис. 9.4). Для просмотра заданной для интерфейса таблицы фильтрации входящего потока следует перевести курсор на строку с описателем этого интерфейса и нажать клавишу <F3>, для просмотра таблицы фильтрации *исходящего* потока – клавишу <F4>. В ответ выводится таблица в том же формате, что и при создании (редактировании) фильтров (см. раздел 3.2.1.2, с. 92).

*9.2.2. **Активные***

Для каждого интерфейса, работа которого проинициализирована программой управления, в оперативной памяти строится логическая структура данных, условно называемая *активный интерфейс*. Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ Активные** приводит к выводу на экран информации об этих структурах (Рис. 9.5); в список включаются данные об интерфейсах, принадлежащих соответствующему (наружному или внутреннему) маршрутизатору. Информация для диагностики активных сетевых интерфейсов изделия выводится в формате, аналогичном формату выдачи информации о сетевых интерфейсах (см. Рис. 9.4).

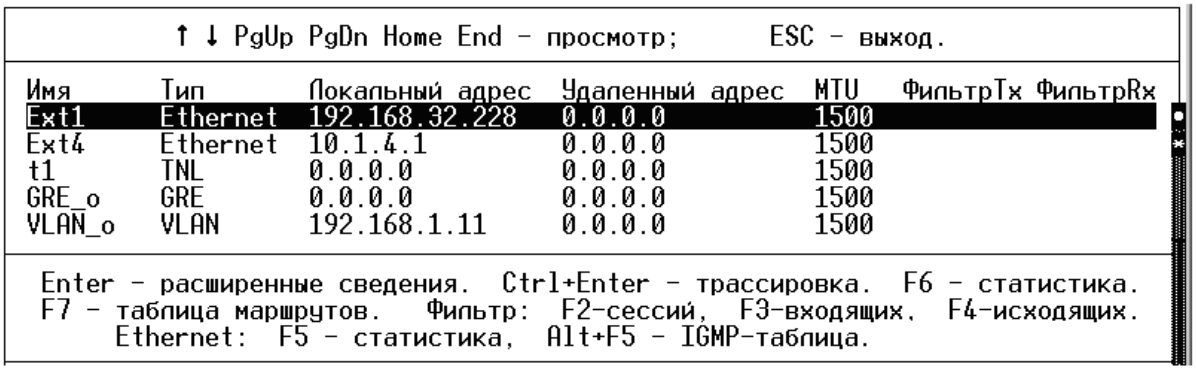


Рис. 9.5 Диагностика активных сетевых интерфейсов изделия

Персоналу изделия предоставлена возможность выбрать любой из интерфейсов (перевести курсор в списке интерфейсов на соответствующую строку) и выполнить для этого интерфейса любое из действий, сведения о которых приведены в нижней части экрана.

`Enter – расширенные сведения` (Рис. 9.5). После нажатия клавиши <Enter> на видеомонитор ЛКУ будут выданы в текстовом формате подробные сведения о параметрах работы интерфейса. Формат выдачи этих сведений различен для сетевых интерфейсов разных типов.

`Ctrl+Enter – трассировка` (Рис. 9.5). Нажатие клавиш <Ctrl+Enter> позволяет изменить режим трассировки того интерфейса, на описатель с именем которого установлен курсор.

Подробнее см. раздел 2.6, с. 52 (**`Enter – трассировка интерфейса`**).

`F6 – статистика` (Рис. 9.5). После нажатия клавиши <F6> на видеомонитор ЛКУ будет выдана аналогичная представленной на Рис. 9.6 информация об объеме трафика, прошедшего через интерфейс, о времени работы интерфейса (в секундах) с момента его активизации и о скорости прохождения информации, мгновенной – первая цифра, усредненной – цифра в скобках.

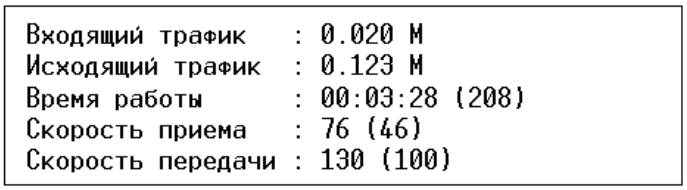


Рис. 9.6 Экран статистики работы сетевого интерфейса

`F7 – таблица маршрутов` (Рис. 9.5). Просмотр таблицы маршрутов интерфейса.

`Фильтры: F2-сессий, F3-входящих, F4-исходящих` (Рис. 9.5). После нажатия одной из клавиш (<F2>, <F3>, <F4>) на видеомонитор ЛКУ выводится соответствующая таблица фильтрации потока данных через интерфейс (если она есть). Выводится таблица в том же формате, что и при создании фильтров (см. раздел 3.2.1.2, с. 92).

Последние два действия могут быть выполнены только для физических интерфейсов типа **`Ethernet`**.

`F5 – статистика` (Рис. 9.5). После нажатия клавиши <F5> на видеомонитор ЛКУ будет выдана полная статистическая информация о работе интерфейса (от момента включения изделия или от момента последнего сброса статистики).

`Alt+F5 – IGMP-таблица` (Рис. 9.5). После нажатия комбинации клавиш <Alt+F5> на видеомонитор ЛКУ будет выдана IGMP-таблица данного интерфейса, аналогичная представленной на Рис. 9.7 (подробнее см. раздел 2.8, с. 60).

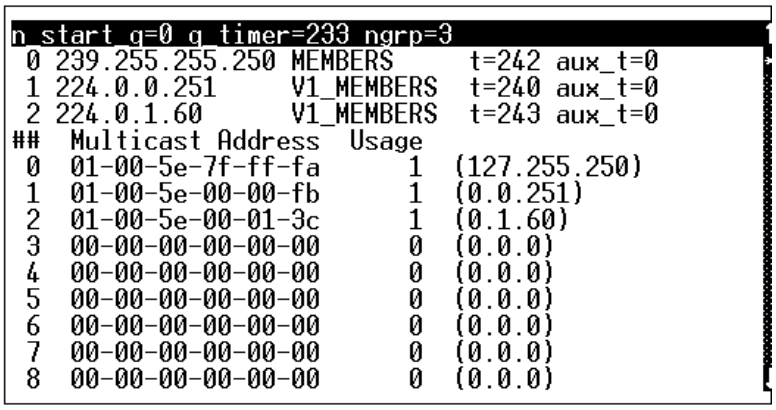


Рис. 9.7 IGMP-таблица интерфейса

9.2.3. *Таблица маршрутов*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ Таблица маршрутов** приводит к выводу на видеомонитор ЛКУ загруженной в настоящий момент в оперативную базу параметров маршрутизатора структуры данных *таблица маршрутов*. Подробнее см. раздел 2.6, с. 52 (**F3 – маршрутная таблица узла**, Рис. 2.43, с. 54).

9.2.4. *Статистика*

Статистические данные о работе сетевых интерфейсов изделия периодически (каждые 5 минут) заносятся в файл и в нем накапливается. Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ Статистика** приводит к выводу на видеомонитор ЛКУ аналогичного представленному на Рис. 9.8 экрана с данными статистики о работе сетевых интерфейсов маршрутизатора изделия.

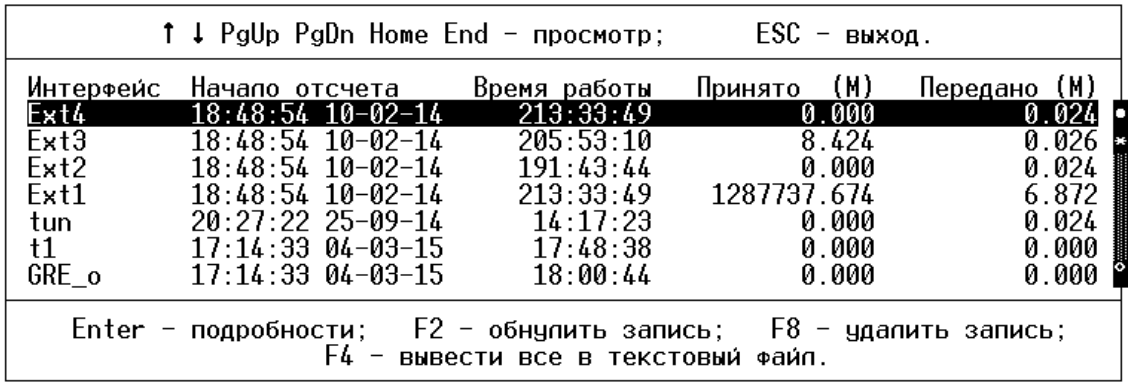


Рис. 9.8 Экран с данными статистики о работе сетевых интерфейсов маршрутизатора изделия

Каждая строка средней части экрана представляет данные статистики о работе конкретного сетевого интерфейса маршрутизатора. В колонке **Интерфейс** строка содержит *имя интерфейса*, в колонке **Начало отсчета** – данные о моменте, с которого ведется сбор статистики (*время*, *дата*). В колонке **Время работы** приводится время, в течение которого интерфейс находится в рабочем состоянии. В двух последних колонках **Принято** и **Передано** запись содержит объем соответственно принятой и переданной через интерфейс информации (в мегабайтах).

В нижней части экрана приведены сведения о возможных действиях персонала.

Enter – подробности (Рис. 9.8). Операция позволяет после нажатия клавиши <Enter> получить на видеомониторе ЛКУ дополнительные данные о статистике работы сетевого интерфейса, на строку описателя которого был установлен курсор.

F2 – обнулить запись (Рис. 9.8). Программа управления в ответ на нажатие клавиши <F2> выдаст запрос на подтверждение обнуления данных статистики для того интерфейса, на строку с описателем которого установлен курсор, и после положительного ответа запись будет закрыта. Отсчет статистики по данному интерфейсу начнется сначала.

F8 – удалить запись (Рис. 9.8). После дополнительного запроса и подтверждения запись, на строку с которой был установлен курсор, будет удалена из файла статистики.

F4 – вывести все в текстовый файл (Рис. 9.8). Операция служит для переноса всей статистики по всем интерфейсам в текстовый файл. Предварительно программа управления запросит имя файла.

*9.2.5. **Текущая загрузка***

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Интерфейсы ⇨ Текущая загрузка** (см. Рис. 9.3, с. 188) приводит к выводу на видеомонитор ЛКУ таблицы с данными для каждого активного сетевого интерфейса, принадлежащего маршрутизатору (наружному или внутреннему), на текущий момент времени: мгновенная скорость при приеме и передаче через интерфейс, трафик за время от момента включения или от момента обнуления статистики и число ошибок за то же время.

Подробнее см. раздел 2.6, с. 52 (**F4 – текущая загрузка интерфейсов**, Рис. 2.39, с. 52).

*9.2.6. **IP-статистика***

В изделии реализована возможность подсчета объема IP-трафика, входящего и исходящего, через любой интерфейс, при этом фиксируется IP-адрес каждой IP-датаграммы. Статистика трафика по IP-адресам сначала накапливается в оперативной памяти, а затем переносится в журнал (файл **LOG.EMA**).

> Для того чтобы статистика трафика, проходящего через интерфейс (физический или виртуальный), начала накапливаться в оперативной памяти, следует в бланке создания и настройки интерфейса специальному параметру **Включить: статистику по IP-адресам** из группы параметров **Специальные настройки** присвоить значение *Да* (см. для примера раздел 2.3.1, бланк управления специальными настройками Ethernet-интерфейса Рис. 2.8, с. 28), после чего сохранить обновленный конфигуратор изделия.

Выбор альтернативы **IP-статистика** (см. Рис. 9.3) переносит накопленную информацию из оперативной памяти в журнал (при этом из оперативной памяти информация удаляется).

Если по завершении сеанса работы в оперативной памяти изделия останется статистическая информация по IP-адресам, то она будет автоматически перенесена в журнал (и удалена из оперативной памяти).

Пример записей, содержащих статистику трафика, проходящего через интерфейс, представлен на Рис. 9.9.

```
192.168.32.65   - IP-stat 20:19:00 17-07-15 S=0.002M R=0.000M
192.168.32.76   - IP-stat 20:19:00 17-07-15 S=0.000M R=0.000M
192.168.32.20   - IP-stat 20:19:00 17-07-15 S=0.000M R=0.000M
192.168.32.1    - IP-stat 20:19:00 17-07-15 S=0.000M R=0.000M
192.168.32.65   - IP-stat 20:19:08 17-07-15 S=0.002M R=0.000M
192.168.32.76   - IP-stat 20:19:08 17-07-15 S=0.000M R=0.002M
192.168.32.1    - IP-stat 20:19:08 17-07-15 S=0.000M R=0.000M
192.168.32.92   - IP-stat 20:19:08 17-07-15 S=0.000M R=0.000M
192.168.32.21   - IP-stat 20:19:08 17-07-15 S=0.000M R=0.000M
```

Рис. 9.9 Пример записей статистики о трафике, проходящем через интерфейс

В первой позиции записи выводится IP-адрес устройства – источника трафика, затем время снятия статистики и объем информации, переданной на этот адрес (**S**) или принятой с этого адреса (**R**).

9.3. Диагностика ⇨Рабочие таблицы

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы** приводит к выдаче на видеомонитор ЛКУ меню, представленного на Рис. 9.10.

Выбор альтернатив этого меню позволяет проконтролировать текущее состояние отдельных ресурсов изделия и происходящих в изделии процессов. Пояснения к применению альтернатив меню приведены ниже.

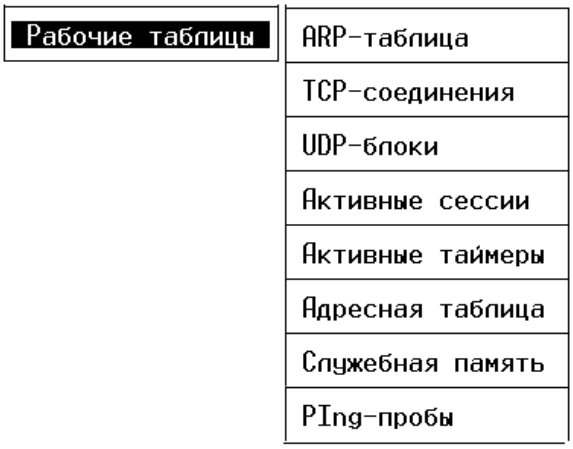


Рис. 9.10 Меню получения сведений из рабочих таблиц при диагностике

9.3.1. *ARP-таблица*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы ⇨ ARP-таблица** (Рис. 9.10) позволяет просмотреть текущее состояние ARP-таблицы маршрутизатора. Текущая ARP-таблица состоит из статических записей, включаемых в ARP-таблицу при настройке (см. раздел 4.2.1, с. 146), и динамических записей, наполняющих ARP-таблицу в процессе работы маршрутизатора изделия. Пример ARP-таблицы приведен на Рис. 9.11.

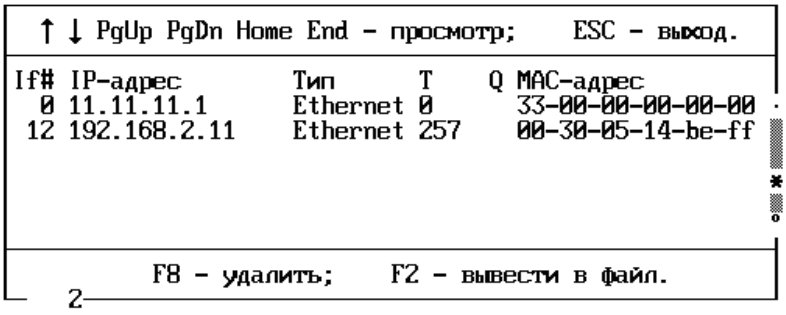


Рис. 9.11 Пример текущего состояния ARP-таблицы

Каждое сетевое устройство, с которым выполняет обмен маршрутизатор изделия, представлено в ARP-таблице одной строкой. В этой строке:

If#	– порядковый номер интерфейса в текущей ARP-таблице;
IP-адрес	– IP-адрес сетевого устройства;
Тип	– тип сети;
T	– время жизни ARP-записи (в секундах);
Q	– количество неудовлетворенных ARP-запросов;
MAC-адрес	– MAC-адрес сетевого устройства.

F8 – удалить (Рис. 9.11). При нажатии клавиши <F8> строка описателя записи ARP-таблицы, на которую был установлен курсор, будет удалена из ARP-таблицы.

F2 – вывести в файл (Рис. 9.11). Текущее содержимое ARP-таблицы маршрутизатора можно сохранить в файле на съемном носителе – FLASH-диске. FLASH-диск должен быть предварительно подключен к разъему USB-устройства ввода/вывода соответствующего маршрутизатора. Для организации собственно записи следует нажать клавишу <F2> и после завершения процедуры записи проконтролировать наличие файла с содержимым ARP-таблицы на FLASH-диске.

9.3.2. *TCP-соединения*

На каждое TCP-соединение строится структура данных **TCB** (TCP control block). Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы ⇨ TCP-соединения** (Рис. 9.10) позволяет просмотреть таблицу активных TCB (Рис. 9.12). На нижнюю рамку таблицы TCB выводятся две цифры, первая – число активных в настоящий момент TCB-блоков (***3***); вторая – полное число TCB-блоков (***16***).

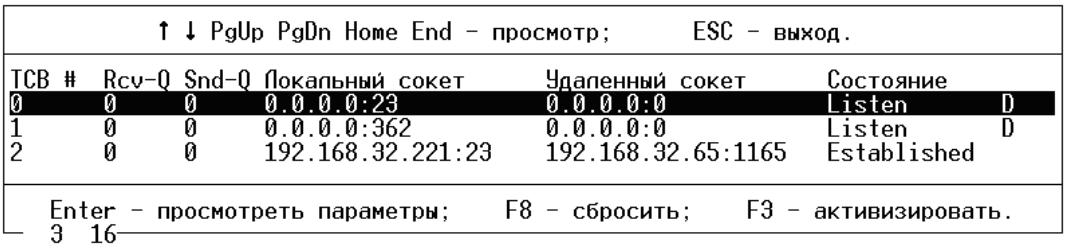


Рис. 9.12 Пример таблицы активных TCB

Каждое TCP-соединение представлено в таблице активных TCB одной строкой. В этой строке:

TCB	– номер TCB-блока;
Rcv-Q	– размер очереди приема;
Snd-Q	– размер очереди передачи;
Локальный сокет	– IP-адрес и порт локального конца TCP-соединения;
Удаленный сокет	– IP-адрес и порт удаленного конца TCP-соединения;
Состояние	– состояние TCP-соединения; наличие символа D означает принадлежность TCB серверному процессу, ожидающему клиентских подключений.

Персоналу предоставлена возможность просмотреть параметры каждого TCP-соединения (нажатие клавиши <Enter> приводит к выводу на видеомонитор ЛКУ подробной таблицы со значениями всех параметров соединения), *сбросить* любое активное TCP-соединение (клавиша <F8>), а также активизировать процесс передачи данных по какому-либо TCP-соединению (клавиша <F3>).

9.3.3. *UDP-блоки*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы ⇨ UDP-блоки** (Рис. 9.10) позволяет просмотреть статистику обработки UDP-пакетов. На видеомонитор ЛКУ выводится список активных UDP-блоков в виде справки, пример которой приведен на Рис. 9.13.

```
↑ ↓ PgUp PgDn Home End - просмотр;  ESC - выход.

Всего UDP: отправлено 2619          получено 25874
В том числе получено: широковещательных      23151
                      с ошибками             0
                      не обрабатываемых нами 22753

            Список активных UDP-блоков

        7fb91094     0 0.0.0.0:161
        7fb95fdc     0 0.0.0.0:67
        7fb95fbc     0 0.0.0.0:53
```

Рис. 9.13 Пример справки со списком активных UDP-блоков

9.3.4. *Активные сессии*

На каждый TCP-канал строится структура данных – ***сессия***. Когда активен канал, активна и сессия. Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы ⇨ Активные сессии** (Рис. 9.10) позволяет просмотреть список активных сессий работы с протоколами прикладного уровня компонента TCP/IP.

```
  ↑ ↓ PgUp PgDn Home End - просмотр;      ESC - выход.

  #  &TCB     Тип     Состояние    Время Удаленный сокет
> 0  c8024cf6 Telnet  Established  0     192.168.2.41:1028
> 1            0
< 2            0

                    F8 - закрыть сессию.
```

Рис. 9.14 Экран управления списком сессий

Сессия занимает в списке одну строку. В этой строке:

> или **<** – вид сессии: исходящая (>) или входящая (<);

– порядковый номер сессии;

&TCB – адрес TCB-блока;

Тип – тип сессии;

Состояние – состояние TCP-соединения;

Время – значение таймера неактивности сессии (в секундах);

Удаленный сокет – IP-адрес и порт клиента, использующего данную сессию.

Персоналу изделия предоставлена возможность принудительно закрыть любую активную сессию. Для этого следует перевести курсор на соответствующую строку в списке сессий (Рис. 9.14) и нажать клавишу <F8>.

9.3.5. *Активные таймеры*

На каждое ожидание какого-либо события строится структура данных – *таймер*. Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы ⇨ Активные таймеры** (Рис. 9.10) позволяет просмотреть на видеомониторе ЛКУ список этих структур, аналогичный представленному на Рис. 9.15.

```
  ↑ ↓ PgUp PgDn Home End - просмотр;      ESC - выход.

          Часы 4014e82a       Тики 12058

CT  Старт Время  Адрес     Функция      Файл         Строка
RN  00300 00242  6ECA:11D6 ifc_stat     tcptimer.c   (177)
```

Рис. 9.15 Экран списка активных таймеров

В первой строке экрана:

Часы – текущее значение системного времени в шестнадцатеричной форме;

Тики – время (в секундах) с момента запуска изделия.

Далее следует список таймеров. Таймер занимает в списке одну строку. В этой строке:

СТ – состояние таймера;
Старт – начальное значение таймера;
Время – остаток времени до конца истечения таймера;
Адрес – адрес функции обработки события;
Функция – имя функции обработки события;
Файл – имя программы, содержащей данную функцию;
Строка – номер строки в программе.

Информация, аналогичная представленной на Рис. 9.15, полезна для разработчиков изделия.

9.3.6. *Адресная таблица*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы ⇨ Адресная таблица** (Рис. 9.10) позволяет просмотреть адресную таблицу хостов в сети, известных изделию. При выборе цепочки альтернатив на видеомонитор ЛКУ выводится экран списка адресов хостов, аналогичный представленному на Рис. 9.16.

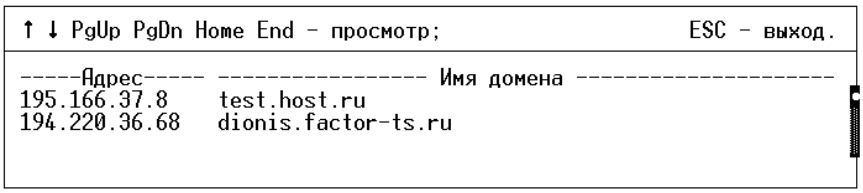


Рис. 9.16 Экран списка адресов хостов

Примечание. Адреса хостов выводятся на видеомонитор ЛКУ (Рис. 9.16) в таком же формате, как и при настройке (см. раздел 4.2.2, с. 147).

9.3.7. *Служебная память*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы ⇨ Служебная память** (Рис. 9.10) приводит к выводу на видеомонитор ЛКУ информации, предназначенной для разработчика изделия.

9.3.8. *PING-пробы*

При выборе цепочки альтернатив ГМ: **Диагностика ⇨ Рабочие таблицы ⇨ Plng-пробы** (Рис. 9.10) на видеомонитор ЛКУ будет выдана сводная диагностическая таблица PING-проб, аналогичная представленной на Рис. 9.17, в которой отражается текущее состояние всех PING-проб (подробнее о PING-пробах в изделии см. раздел 2.7, с. 58).

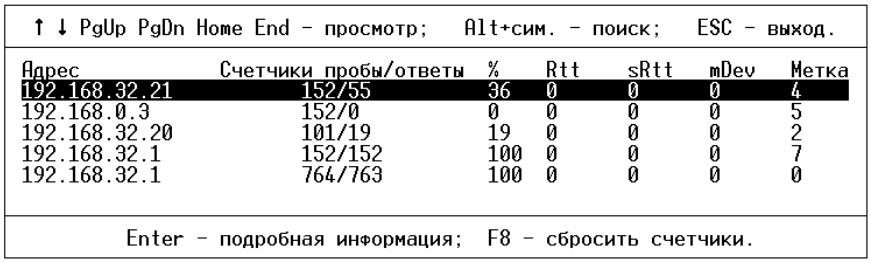


Рис. 9.17 Сводная диагностическая таблица PING-проб изделия

Каждая строка сводной диагностической таблицы PING-проб содержит следующие сведения:

Адрес – IP-адрес удаленного узла, с которым контролируется состояние тракта;
Счетчики проб/ответов – счетчики отправленных PING-запросов (**проба**) и полученных PING-ответов (**ответ**);
% – процент успешных ответов от общего числа переданных проб;
Rtt (round-trip time) – время прохождения датаграммы от отправителя к удаленному узлу и обратно;
sRtt – среднее значение **Rtt**;
mDev – отклонение **Rtt** от **sRtt**;
Метка – метка соответствующей PING-пробы.

Используя диагностическую таблицу PING-проб, можно выполнить следующие действия:

Enter - подробная информация (Рис. 9.17). Если перевести курсор на конкретную строку в таблице PING-проб и нажать клавишу <Enter>, то можно получить более подробную информацию об этой PING-пробе в текстовом формате.

F8 – сбросить счетчики (Рис. 9.17). Нажатие клавиши <F8> обнулит значения счетчиков проб и ответов в той PING-пробе, на строку которой установлен курсор.

Примечание. Значения счетчиков обнуляются также при оформлении задания на выполнение новых PING-проб.

9.4. Диагностика ⇨ Статистика

При выборе цепочки альтернатив ГМ: **Диагностика ⇨ Статистика** на видеомонитор ЛКУ выводится меню, представленное на Рис. 9.18.

Рис. 9.18 Подменю сбора статистики о работе протоколов стека TCP/IP

Меню (Рис. 9.18) позволяет с помощью своих альтернатив проконтролировать статистику обмена данными, обрабатываемыми соответствующими протоколами стека TCP/IP.

9.5. Диагностика ⇨ Туннели

Возможности диагностики созданных в изделии криптотуннелей с помощью выбора цепочки альтернатив ГМ: **Диагностика ⇨ Туннели** описаны в разделе 3.1.3, с. 88 (Рис. 3.15).

9.6. Диагностика ⇨ NAT

Описание диагностики функционирования **NAT**-обработчика приведено в разделе 3.3.7, с. 120.

9.7. Диагностика ⇨ DHCP

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ DHCP** приводит к выдаче на видеомонитор ЛКУ меню, представленного на Рис. 9.19.

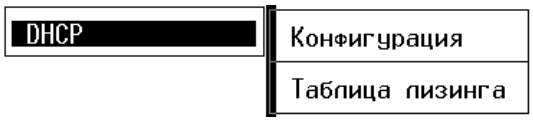


Рис. 9.19 Меню диагностики функционирования DHCP-службы маршрутизатора изделия

Меню позволяет с помощью альтернатив **Конфигурация** и **Таблица лизинга** проконтролировать статистику обмена данными, обрабатываемыми соответствующими протоколами стека TCP/IP.

9.7.1. Конфигурация

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ DHCP ⇨ Конфигурация** (см. Рис. 9.19) позволяет персоналу изделия в процессе работы проконтролировать конфигурацию DHCP-сервера (без права внесения изменений). Выбор цепочки альтернатив приводит к выводу на видеомонитор ЛКУ экрана списка элементов DHCP-таблицы, аналогичного представленному на Рис. 9.20.

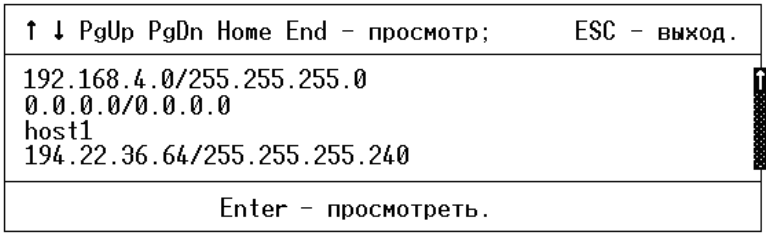


Рис. 9.20 Экран списка описателей подсетей и хостов DHCP-службы

Внешний вид экрана совпадает с экраном управления списком описателей подсетей и хостов DHCP-службы (см. раздел 5.5.2, Рис. 5.17, с. 162), но из всех функций управления персоналу изделия доступна только одна: **Enter – просмотреть** (Рис. 9.20).

9.7.2. Таблица лизинга

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ DHCP ⇨Таблица лизинга** (см. Рис. 9.19) позволяет персоналу изделия в процессе работы отслеживать текущее состояние *таблицы лизинга*.

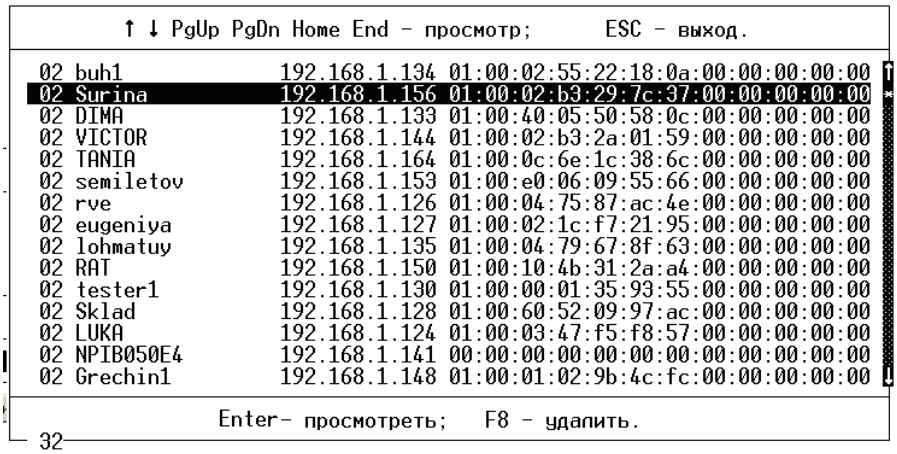


Рис. 9.21 Экран управления таблицей лизинга **DHCP**-службы маршрутизатора изделия

Выбор цепочки альтернатив приводит к выводу на видеомонитор ЛКУ экрана управления таблицей лизинга **DHCP**-службы маршрутизатора изделия, аналогичной представленной на Рис. 9.21.

Набор параметров, выданный одному клиенту DHCP-службы, занимает одну строку.

В этой строке:

- первая цифра – флаг состояния (**01** – **DHCP**-клиенту предложен набор параметров; **02** – **DHCP**-клиент принял предложенный набор; **04** – **DHCP**-клиент освободил набор параметров, но срок лизинга не истек);
- имя клиента;
- IP-адрес, выданный **DHCP**-клиенту;
- далее следует уникальный идентификатор DHCP-клиента; идентификатор занимает 12 байт и для сети Ethernet строится по следующему правилу: первый байт – тип сети (**01** – Ethernet), шесть байтов – адрес платы и пять нулевых байтов.

Цифра в левом нижнем углу экрана соответствует числу записей в таблице лизинга **DHCP**-службы.

Персонал изделия может удалить одну или несколько записей таблицы. Для этого следует перевести курсор на строку с записью таблицы и нажать клавишу <F8>.

При удалении записи из таблицы лизинга из памяти DHCP-сервера удаляются данные о параметрах, выданных DHCP-клиенту. При следующем обращении этого клиента DHCP-сервер будет искать для него новый IP-адрес и остальные параметры.

Персонал изделия имеет возможность просмотреть содержимое отдельных элементов таблицы лизинга. Для этой цели он должен перевести курсор на строку с этим элементом и нажать клавишу <Enter>.

9.8. Диагностика ⇨ DNS-служба

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ DNS-служба** приводит к выдаче на видеомонитор ЛКУ меню, представленного на Рис. 9.22.

Рис. 9.22 Меню диагностики функционирования DNS-службы маршрутизатора изделия

Меню (Рис. 9.22) позволяет с помощью альтернатив: **Конфигурация**, **Таблица запросов** и **Кэш** проконтролировать функционирование DNS-службы маршрутизатора изделия.

9.8.1. Конфигурация

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ DNS-служба ⇨ Конфигурация** (см. Рис. 9.22) позволяет персоналу изделия просмотреть основные параметры настройки DNS-службы и таблицу DNS-серверов, описанных в процессе настройки DNS-службы маршрутизатора изделия (см. раздел 5.4.1, с. 157). На видеомонитор ЛКУ выводится экран диагностических сведений, аналогичный представленному на Рис. 9.23.

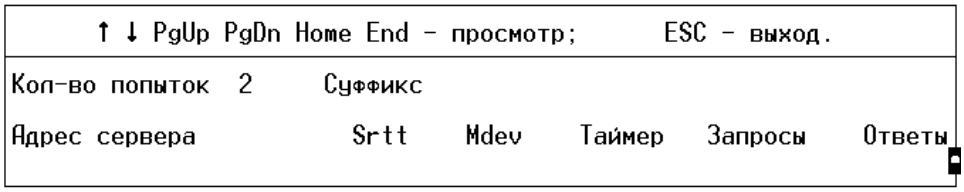


Рис. 9.23 Экран диагностических сведений о работе DNS-службы маршрутизатора изделия

Первая строка в средней части экрана содержит параметры:

Кол-во попыток – количество попыток получения ответа от DNS-сервиса;

Суффикс – текстовый суффикс, автоматически добавляемый в DNS-запросах к простым именам (не имеющим точек).

Далее следует список DNS-серверов. Описатель каждого сервера занимает одну строку в средней части экрана. Строка описателя DNS-сервера содержит значения следующих параметров:

Адрес сервера – IP-адрес сервера;

Srtt – среднее время ожидания ответа от DNS-серверов (в миллисекундах);

Mdev – оценка величины отклонения времени ожидания ответов от среднего значения;

Таймер – текущее значение таймера ожидания ответов (в миллисекундах);

Запросы – счетчик запросов к DNS-серверу;

Ответы – счетчик ответов, полученных от DNS-сервера.

9.8.2. *Таблица запросов*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ DNS-служба ⇨ Таблица запросов** (см. Рис. 9.22) позволяет просмотреть очередь DNS-запросов маршрутизатора изделия к другим DNS-серверам. На видеомонитор ЛКУ выводится экран управления, аналогичный представленному на Рис. 9.24.

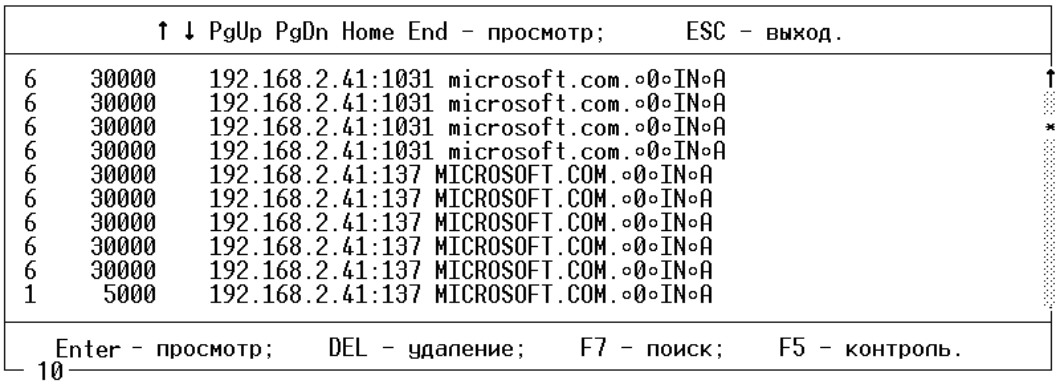


Рис. 9.24 Экран управления очередью DNS-запросов маршрутизатора

Каждая строка средней части экрана соответствует одному DNS-запросу.

Параметры строки DNS-запроса представлены на экране в следующем формате:

- *первое поле* – номер попытки получить ответ (*напомним*: максимальное число попыток получения ответа от DNS-серверов задается при настройке DNS-службы маршрутизатора);
- *второе поле* – время ожидания ответа на DNS-запрос;
- *третье поле* – адрес абонента, приславшего запрос на DNS-сервер маршрутизатора изделия (включая IP-адрес и номер порта);
- *четвертое поле* – текст DNS-запроса.

9.8.3. *Кэш*

При выборе цепочки альтернатив ГМ: **Диагностика ⇨ DNS-служба ⇨ Кэш** (см. Рис. 9.22) на видеомонитор ЛКУ будет выдано аналогичный представленному на Рис. 9.25 экран содержимого кэша DNS-службы маршрутизатора изделия.

Выбор этой цепочки альтернатив приводит к выводу на видеомонитор ЛКУ всех элементов кэша: записей зон и ответов других DNS-серверов на DNS-запросы нашего маршрутизатора изделия (сначала – записи зон, потом – ответы). В нижней рамке экрана приведены два числа: слева – число всех элементов в кэше, справа – число блоков, характеризующих объем кэша.

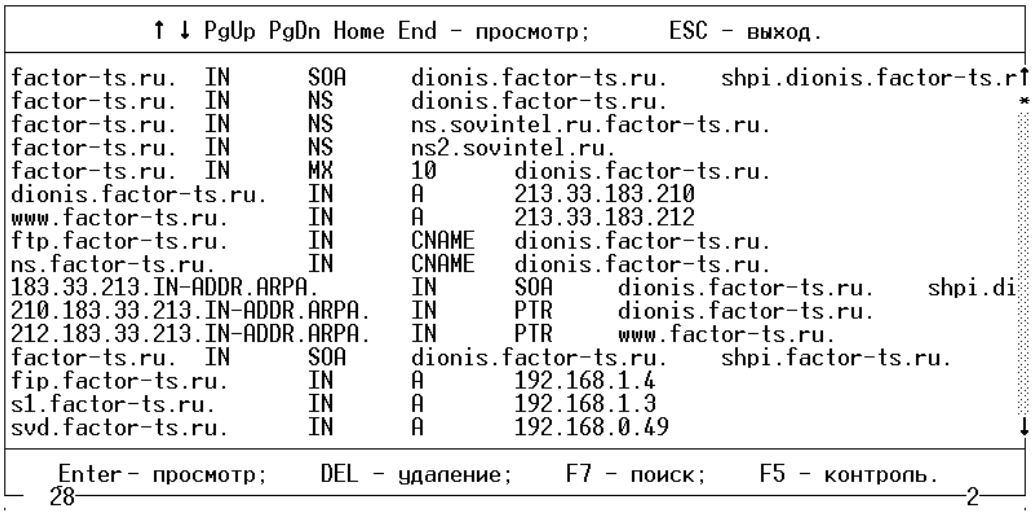


Рис. 9.25 Экран содержимого кэша DNS-службы маршрутизатора изделия

9.9. Диагностика ⇨ Маршрутизация

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Маршрутизация** приводит к выдаче на видеомонитор ЛКУ меню, представленного на Рис. 9.26.

Рис. 9.26 Меню диагностики маршрутов, обслуживаемых маршрутизатором изделия

> *Примечание.* Альтернативы меню **OSPF** и **BGP** действующей в настоящее время версией ОПО не поддерживаются.

Меню (Рис. 9.26) позволяет с помощью своих альтернатив: **RIP** и **Таблица маршрутов** проконтролировать состояние поддерживаемых маршрутизатором изделия направлений обмена данными.

9.9.1. *RIP*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Маршрутизация ⇨ RIP** (см. Рис. 9.26) позволяет персоналу изделия в сжатой форме просмотреть параметры конфигурации RIP-службы маршрутизатора изделия и статистику работы RIP-сервера. На видеомонитор ЛКУ будет выдан экран параметров конфигурации RIP-службы и статистики работы RIP-сервера маршрутизатора, аналогичный представленному на Рис. 9.27.

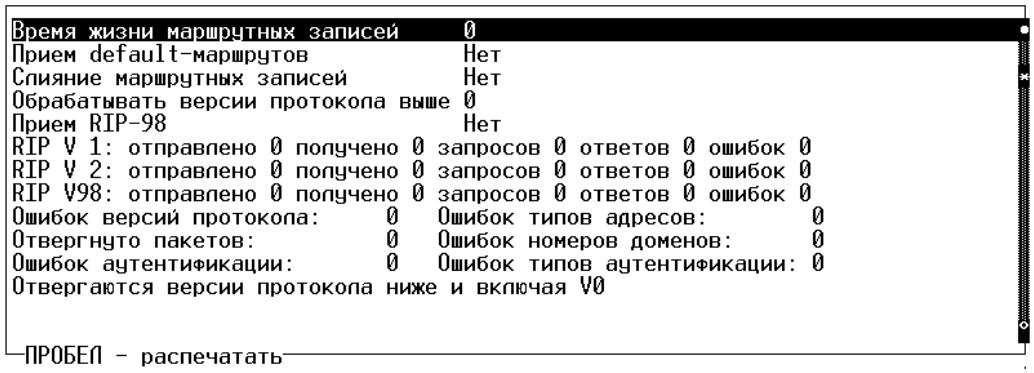


Рис. 9.27 Экран параметров конфигурации RIP-службы и статистики работы RIP-сервера маршрутизатора

9.9.2. *Таблица маршрутов*

Выбор цепочки альтернатив ГМ: **Диагностика ⇨ Маршрутизация ⇨ Таблица маршрутов** (см. Рис. 9.26) позволяет персоналу изделия просмотреть состояние загруженной в маршрутизатор изделия в текущий момент времени структуры данных, называемой *таблицей маршрутов*.

> Подробнее см. раздел 2.6, с. 52 (**F3 – маршрутная таблица узла** – Рис. 2.39, с. 52; Рис. 2.43, с. 54).

10. Главное меню. Альтернатива *Сервис*

Выбор альтернативы ГМ **Сервис** приводит в выводу на видеомонитор ЛКУ меню, представленного на Рис. 10.1.

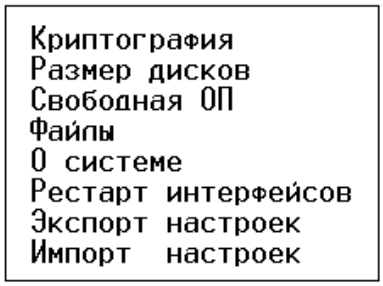


Рис. 10.1 Меню альтернативы ГМ: **Сервис**

Выбор альтернатив меню позволяет проконтролировать текущее состояние отдельных ресурсов изделия и происходящих в изделии процессов, перезапустить работу сетевых интерфейсов маршрутизатора изделия, выполнить сохранение на съемном носителе собственного конфигуратора изделия или заимствовать со съемного носителя ранее сформированный собственный конфигуратор изделия или конфигуратор другого аналогичного изделия. Пояснения к применению альтернатив подменю приведены ниже.

Примечания.

1. Альтернативы меню **Файлы**, **Экспорт настроек** и **Импорт настроек** доступны только в режиме администрирования.
2. Альтернатива меню **Импорт настроек** доступна только при подключении блока ЛКУ к наружному маршрутизатору изделия.

10.1. Сервис ⇨ Криптография

Выбор цепочки альтернатив ГМ: **Сервис ⇨ Криптография** (Рис. 10.1) приводит к выдаче на видеомонитор ЛКУ меню, представленного на Рис. 10.2.

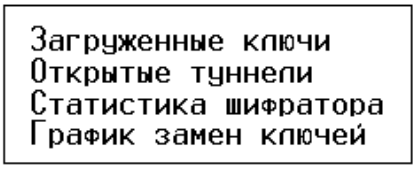


Рис. 10.2 Меню цепочки альтернатив ГМ: **Сервис ⇨ Криптография**

Выбор альтернатив этого меню позволяет проконтролировать текущее состояние отдельных ресурсов и механизмов изделия.

Примечание. Для внутреннего маршрутизатора доступны все альтернативы этого меню. Для наружного маршрутизатора доступна только одна альтернатива – **Статистика шифратора**.

Загруженные ключи (Рис. 10.2). При выборе альтернативы на видеомонитор ЛКУ выводится таблица с данными обо всех загруженных в изделие ключевых документах, представленная на Рис. 10.3.

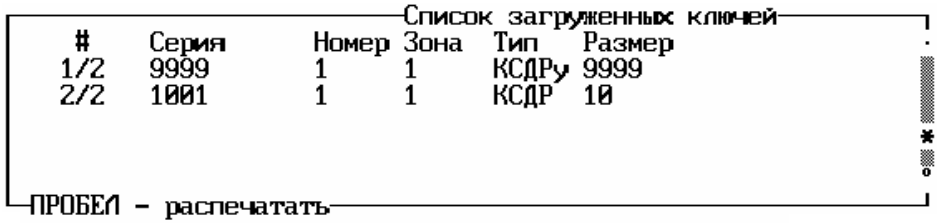


Рис. 10.3 Экран данных о списке загруженных в изделие ключевых документах

Примечание. Описание работы с ключевыми документами при эксплуатации изделия приведено в РЭ на конкретное изделие.

Открытые туннели (Рис. 10.2). При выборе альтернативы на видеомонитор ЛКУ выводится экран с данными обо всех открытых в изделии криптотуннелях, аналогичный представленному на Рис. 10.4.

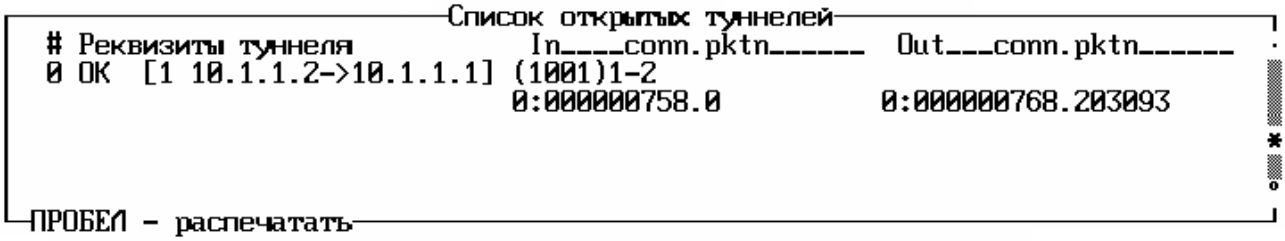


Рис. 10.4 Экран данных о списке открытых в изделии криптотуннелей

Статистика шифратора (Рис. 10.2). При выборе альтернативы на видеомонитор ЛКУ выводится экран данных статистики работы шифратора изделия, представленный на Рис. 10.5.

Рис. 10.5 Экран данных статистики работы шифратора изделия

Как видно из подсказок в нижней части экрана, после нажатия клавиши <c> будет выполнено обнуление всех счетчиков, а после нажатия клавиши <i> на экран будет выдана более подробная диагностическая информация о текущем состоянии шифратора (БКО) изделия (Рис. 10.6).

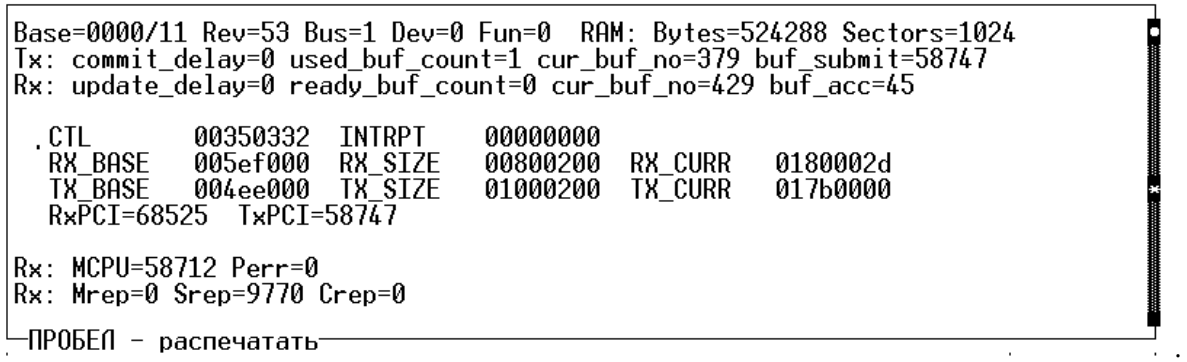


Рис. 10.6 Экран с уточненными данными о статистике работы шифратора изделия

График замен ключей (Рис. 10.2). При выборе альтернативы на видеомонитор ЛКУ выводится график автоматической замены серий ранее загруженных в изделие ключевых документов, аналогичный представленному на Рис. 10.7.

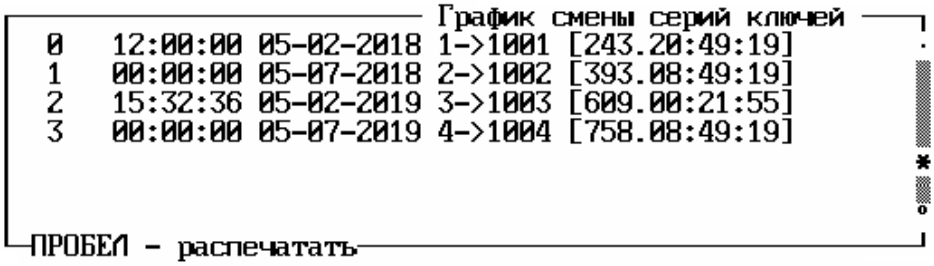


Рис. 10.7 Экран данных о графике замен ключей

Об использовании графика автоматической замены ранее загруженных в изделие ключевых документов см. раздел 3.4, с. 122.

10.2. Сервис ⇨ Размер дисков

Выбор цепочки альтернатив ГМ: **Сервис ⇨ Размер дисков** (Рис. 10.1) приводит к выдаче на видеомонитор ЛКУ представленного на Рис. 10.8 экрана с информацией об использовании дисков маршрутизатора.

Диск	Всего	Свободно
C	22614016	18378752
D	1982005248	1884389376

Диск	Всего	Свободно

```
Протокольные файлы : ALOGS c:\dioniswt\logs
Настройки          : AEMAS d:\dioniswt.cfg
Рабочие файлы      : AWORK d:\dioniswt.dat\workers
Ключевая информация:
```

Рис. 10.8 Экран с информацией об использовании дисков маршрутизатора

Экран с информацией (Рис. 10.8) содержит сведения о том, на каких логических дисках и в каких директориях размещаются различные данные: **Протокольные файлы** (журналы), **Настройки** (конфигуратор изделия), **Рабочие файлы** и **Ключевая информация**.

10.3. Сервис ⇨ Свободная ОП

Выбор цепочки альтернатив ГМ: **Сервис ⇨ Свободная ОП** (Рис. 10.1) приводит к выдаче на видеомонитор ЛКУ экрана управления данными об использовании оперативной памяти маршрутизатора, аналогичного представленному на Рис. 10.9. Эту цепочку альтернатив, как правило, используют по просьбе разработчика изделия с целью анализа возможных проблем в работе изделия.

свободная ОП	M байт	max	min
объем	188464	215302	188464
блоков	26	26	15
макс.блок	64002	64002	64002
отказов			

используемая ОП		max	min
объем	51944	51944	25214
блоков	72	72	29
макс.блок	17280	17280	8528

стек	6218	6474	4502
файлы	10	12	10

Трассировка ОП выключена | Dump

Рис. 10.9 Экран управления данными об использовании оперативной памяти маршрутизатора

С помощью экрана (Рис. 10.9) можно получить информацию о свободной и использованной оперативной памяти маршрутизатора изделия. Также при необходимости можно включить, выбрав альтернативу экрана **Трассировка ОП**, трассировку использования оперативной памяти; при этом будет выполняться запись в журнал **LOG.EMA** информации о каждом запросе на выделение или освобождение блоков памяти.
Кроме того, выбрав альтернативу экрана **Dump**, можно запротоколировать дамп оперативной памяти маршрутизатора.

Администратор изделия может контролировать информацию о текущем объеме свободной оперативной памяти (первое число под заголовком **свободная ОП**) – текущий объем не должен быть меньше значения ***80000*** и не должен уменьшаться с течением времени.

10.4. Сервис ⇨ Файлы

Выбор цепочки альтернатив ГМ: **Сервис ⇨ Файлы** (Рис. 10.1) приводит к выдаче на видеомонитор ЛКУ экрана управления файловой системой маршрутизатора, аналогичного представленному на Рис. 10.10. Средняя часть экрана содержит список директорий и файлов, используемых программой управления маршрутизатором изделия.

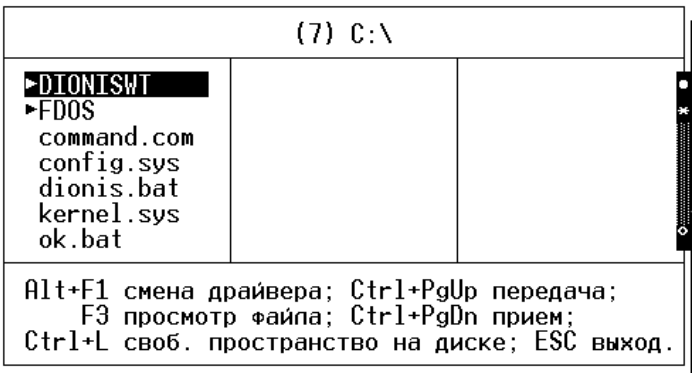


Рис. 10.10 Экран управления файловой системой маршрутизатора

В этом списке большими буквами (со стрелками перед ними) представлены директории, маленькими – файлы. Текущее значение имени директории отражается в верхней части экрана. Перемещение курсора по элементам экрана выполняется с помощью управляющих стрелок и клавиш <PgUp>, <PgDn>, <Home>, <End>; вход в директорию, на которой установлен курсор, – с помощью клавиши <Enter>; выход из директории – нажатием клавиши <Enter> в момент, когда курсор установлен на строке с двумя точками.

Нажатие комбинации клавиш <Alt+F1> обеспечивает переход на любой из доступный логических дисков.

Клавиша <F3> позволяет просмотреть файл на экране. При этом можно выполнить поиск заданного контекста и собрать фрагменты, содержащие заданный контекст, в отдельный файл.

Во время просмотра файла после нажатия клавиши <F3> можно нажать клавишу <F1>, в результате чего на видеомонитор ЛКУ будет выдан представленный на Рис. 10.11 экран с информацией о средствах автоматизации поиска в файле, упрощающих работу по анализу содержимого просматриваемого файла.

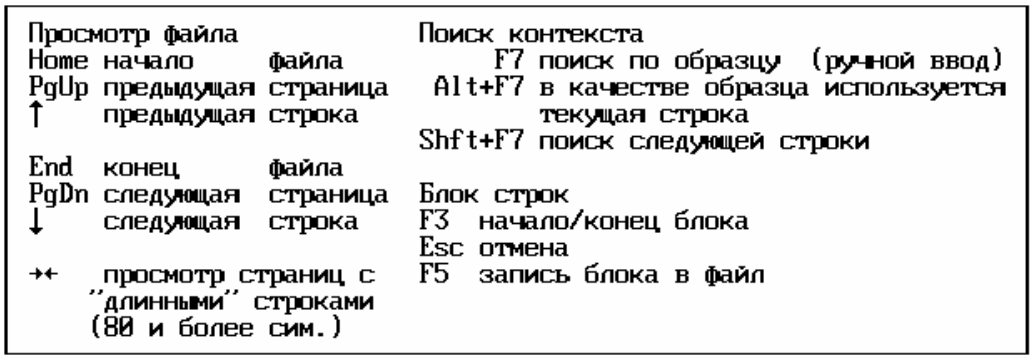


Рис. 10.11 Экран с информацией о средствах автоматизации поиска в файле

Нажатие комбинации клавиш <Ctrl+L> (Рис. 10.10) позволяет вывести на экран информацию о полном размере текущего диска и о размере свободного пространства на нем.

> *Примечание.* Операции <Ctrl+PgUp> и <Ctrl+PgDn> (Рис. 10.10) данной версией ОПО изделия не поддерживаются.

10.5. Сервис ⇨ О системе

Выбор цепочки альтернатив ГМ: **Сервис ⇨ О системе** (Рис. 10.1) приводит к выдаче на видеомонитор ЛКУ экрана с информацией о маршрутизаторе изделия, аналогичного представленному на Рис. 10.12.

В верхней строке – имя узла и его статус при работе в составе кластера. Во второй строке – данные установленного процессора.

Температуры – температура в градусах Цельсия: процессора, шифратора и физических интерфейсов.

Затем приведены данные о конфигураторе изделия, контрольная сумма варианта ОПО и шестнадцатеричный дамп загрузочного сектора.

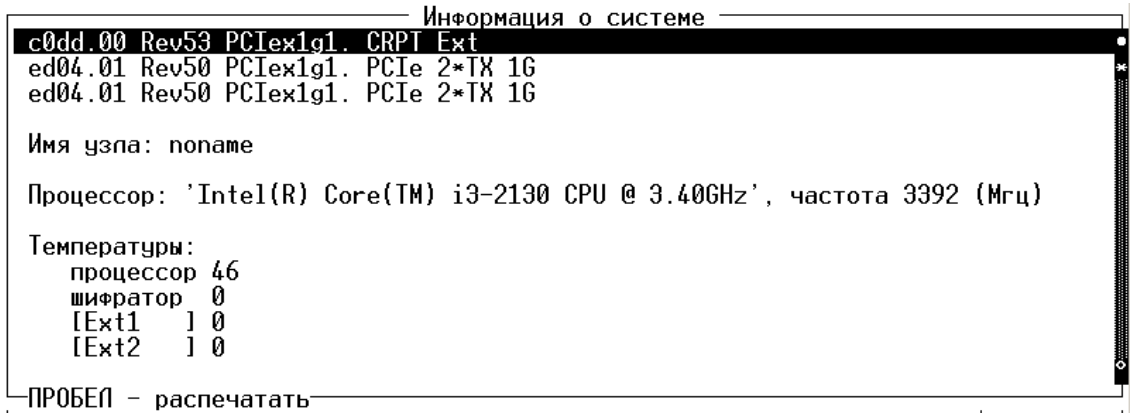


Рис. 10.12 Фрагмент экрана с информацией об изделии

10.6. Сервис ⇨ Рестарт интерфейсов

Выбор цепочки альтернатив ГМ: **Сервис ⇨ Рестарт интерфейсов** (Рис. 10.1) приводит к непосредственному исполнению команды на рестарт сетевых интерфейсов маршрутизатора изделия. При выборе цепочки альтернатив прекращается работа всех сетевых интерфейсов маршрутизатора, после чего выполняется их повторный запуск. Кроме того, все оборудование, подключенное к интерфейсам, получает сигнал о выполнении рестарта.

Команда может понадобиться, если после внесения изменений в настройки интерфейсов по каким-либо причинам не будет выполнен автоматический рестарт.

10.7. Сервис ⇨ Экспорт настроек / Импорт настроек

Выбор цепочки альтернатив ГМ: **Сервис ⇨ Экспорт настроек** (Рис. 10.1) позволяет скопировать все выполненные ранее настройки изделия – текущее состояние *конфигуратора изделия*, представляющего собой набор файлов – на съемный UCB FLASH-диск, предварительно подключенный к соответствующему разъему USB-устройства ввода/вывода – выполнить *экспорт* конфигуратора изделия.

Выбор цепочки альтернатив ГМ: **Сервис ⇨ Импорт настроек** (Рис. 10.1) позволяет перенести требуемый вариант настройки конфигуратора изделия со съемного UCB FLASH-диска, предварительно подключенного к соответствующему разъему USB-устройства ввода/вывода – выполнить *импорт* конфигуратора.

Перед выполнением обеих операций (экспорта и импорта конфигуратора) будет выдан стандартный запрос, аналогичный приведенному, например, на Рис. 4.21, с. 144, позволяющий указать файл (выбрать из уже существующих на USB-устройстве или создать новый).

Экспорт настроек можно выполнить из любого блока маршрутизации, наружного или внутреннего.

Импорт настроек можно выполнить только из блока наружной маршрутизации БНМ; при этом программа управления выдаст запрос на разрешение записи конфигуратора изделия в память шифратора – **БпО.** Разрешение на запись конфигуратора должен выдать администратор изделия соответствующей командой, выдаваемой с помощью средств управления БКО (подробнее см. РЭ на конкретное изделие).

> *Примечание.* Экспорт и импорт конфигуратора эффективен, например, при переносе конфигуратора с изделия со статусом **MASTER** на изделие со статусом **SLAVE** при работе изделий в составе кластера криптомаршрутизаторов (см. раздел 7, с. 174).

11. Работа изделия в режиме Администратор сети

Изделие может функционировать в качестве средства удаленного управления в составе Центра удаленного администрирования (ЦУА) ЗСПД, позволяющего управлять аналогичными криптомаршрутизаторами (изделиями, исполненными в *двухсегментной* архитектуре технологии DioNIS® – криптомаршрутизаторами серии М-479Рх) и частично криптомаршрутизаторами семейства М-479 (изделиями, исполненными в *односегментной* архитектуре технологии DioNIS®). Число управляемых изделий практически не ограничено).

При работе изделия в составе ЦУА в качестве технологического средства удаленного управления используется реализованный в составе изделия компонент **Администратор сети**.

> *Примечание.* Организация доступа управляющего изделия к управляемому для выполнения различных функций управления на каждом из его маршрутизаторов (БНМ и БВМ) подробно рассмотрена в разделе 1.3.3, с. 12. Отметим, что доступ для удаленного управления блоком наружной маршрутизации управляемого изделия обеспечивается только из БНМ управляющего изделия, а доступ для удаленного управления БВМ управляемого изделия обеспечивается только из БВМ управляющего изделия.

Криптомаршрутизаторы серии М-479Рх обеспечивают выполнение следующих функций удаленного управления.

1. Управляющее изделие с помощью специального транспортного протокола DCP может считать *конфигуратор* (все параметры настройки) любого управляемого криптомаршрутизатора и загрузить его в свою базу конфигураторов управляемых криптомаршрутизаторов ЗСПД, а также может извлечь из этой базы необходимый вариант конфигуратора и отправить его управляемому изделию для загрузки с целью его перенастройки. Редактирование базы конфигураторов на управляющем изделии выполняется в отсутствие связи с управляемыми изделиями.

   > *Примечание.* Функция доступна только из БНМ управляющего изделия.

2. На управляющем изделии можно получить копии журналов работы и сведения о статистике работы каждого из маршрутизаторов управляемого изделия.
3. Реализована функция управления блоком наружной или блоком внутренней маршрутизации управляемого изделия в режиме *удаленной консоли*.

Для обеспечения криптографической защиты канала управления на управляющем и на управляемом изделиях должны быть загружены два вида ключей: ключи *канала данных* и ключи *канала управления*.

> *Примечание.* Серия ключей, загружаемых в изделия как ключи канала управления, не может использоваться изделием с другими целями.

При удаленном управлении блоком наружной маршрутизации криптографическая защита канала управления реализуется на ключах управления. При управлении блоком внутренней маршрутизации канал управления криптографически защищен штатным криптотуннелем, работающем на ключе канала данных.

Ключевые документы доставляются на объекты эксплуатации изделий на отдельных ключевых носителях и применяются согласно требованиям документа «Правила пользования» и руководства по эксплуатации на конкретное изделие.

При подготовке к процессу удаленного управления на каждом управляющем изделии должен быть сформирован список описателей объектов управления и каждому управляемому изделию в составе ЗСПД должен быть поставлен в соответствие один из описателей.

В общем случае на управляющем изделии должно быть сформировано *два* списка описателей: один список должен быть сформирован на БВМ управляющего изделия для реализации управления всеми БВМ управляемых изделий, другой список − на БНМ управляющего изделия для реализации управления всеми БНМ управляемых изделий

> *Примечание*. Необходимость иметь два списка описателей вызвана следующим. Всякую ЗСПД можно рассматривать как два сегмента: *транспортный* (сегмент сети общего пользования, в которых информация Пользователя циркулирует в *защищенном* виде) и сегмент *Пользователя* (локальные сети Пользователя, в которых информация Пользователя циркулирует в *незащищенном* виде). Обмен потоками данных между этими двумя сегментами осуществляется *исключительно* через шифраторы изделий защиты. Получить доступ к информации, циркулирующей в этих двух сегментах, с одного и того же устройства ЗСПД невозможно, поэтому для реализации управления в масштабе *всей* ЗСПД необходимо рассматривать *два* самостоятельных *контура* процесса управления – *внутренний* и *внешний*.
>
> В масштабе ЗСПД фактически должно быть организовано функционирование *двух* систем управления: в одной из них объектами управления являются БВМ всех управляемых изделий (на БВМ управляющего изделия должен быть создан список всех БВМ управляемых изделий); в другой − объектами управления являются БНМ всех управляемых изделий (на БНМ управляющего изделия должен быть создан список всех БНМ управляемых изделий).

11.1. Начало работы

Чтобы получить возможность управлять удаленными изделиями в составе ЗСПД, следует средство удаленного управления в составе ЦУА – одно из изделий серии М-479Рх – перевести в режим **Администратор сети**. Для этого надо на каждом из маршрутизаторов изделия выбрать цепочку альтернатив ГМ: **Консоль ⇨ Режим** и в появившемся на видеомониторе ЛКУ меню (Рис. 8.6, с. 183) выбрать значение *Администратор сети* (подробнее см. раздел 8.4, с. 183). Возможность переключения в этот режим защищена своим паролем (не связанным с паролем для перевода в режим **Администратор узла**).

После ввода пароля администратора сети на видеомонитор ЛКУ будет выдан экран управления списком описателей управляемых изделий, аналогичный представленному на Рис. 11.1.

Средняя часть экрана содержит список всех ранее созданных описателей изделий защиты в составе ЗСПД, удаленное управление которыми осуществляется данным *управляющим* изделием.

Изначально список описателей пустой.

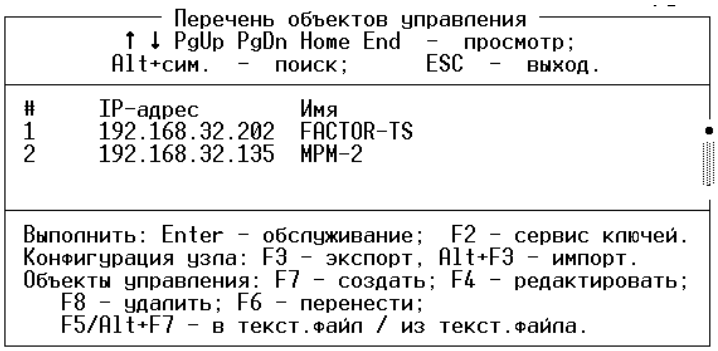


Рис. 11.1 Экран управления списком описателей управляемых изделий

Каждый описатель управляемого изделия занимает в списке одну строку и содержит идентификатор (номер) описателя (под заголовком **#**), IP-адрес управляемого изделия (под заголовком **IP-адрес**) и имя описателя (под заголовком **Имя**) – подробнее см. ниже (раздел 11.2, с. 206).

Enter – обслуживание (Рис. 11.1). Для выполнения операций удаленного управления тем или иным изделием следует в списке (Рис. 11.1) перевести курсор на строку с соответствующим описателем и нажать клавишу <Enter>. На видеомонитор ЛКУ будет выдан экран управления удаленным изделием, аналогичный представленному на Рис. 11.6. Описание выполняемых с помощью этого экрана операций управления приведено ниже – раздел 11.3, с. 207.

F2 – сервис ключей (Рис. 11.1). В списке описателей управляемых изделий перевести курсор на строку с описателем нужного изделия и нажать клавишу <F2>. На видеомонитор ЛКУ будет выдан экран управления загруженными ключами управляемого изделия, аналогичный представленному на Рис. 11.10, с. 210. Экран позволяет выполнить различные операции обслуживания ключевой информации, загруженной на управляемом изделии (подробнее см. ниже – раздел 11.4. с. 210).

F3 – экспорт (Рис. 11.1). Операция служит для копирования (*экспорта*) конфигуратора *управляемого* изделия на съемный носитель, подключенный к *управляющему* изделию. Предварительно следует подключить съемный носитель и затем в списке описателей управляемых изделий перевести курсор на строку с описателем нужного изделия и нажать клавишу <F3>. На видеомонитор ЛКУ будет выдан экран выбора устройств для подключения съемных носителей, аналогичный представленному на Рис. 4.21. С помощью этого экрана, управляя файловой структурой съемного носителя, следует выбрать директорию, в которую будет выполнено копирование, и нажать клавишу <F2> – в ответ будет выполнен запуск процедуры экспорта.

Alt+F3 – импорт (Рис. 11.1). Операция служит для копирования конфигуратора изделия со съемного носителя, предварительно подключенного к управляющему изделию, в хранилище конфигураторов на управляющем изделии. В списке описателей управляемых изделий следует переместить курсор на строку с нужным описателем и нажать комбинацию клавиш <Alt+F3>. На видеомонитор ЛКУ будет выдан экран выбора устройств для подключения съемных носителей, аналогичный представленному на Рис. 4.21. С помощью этого экрана, управляя файловой структурой съемного носителя, следует выбрать директорию, содержащую требуемый конфигуратор, и нажать клавишу <F2> – в ответ будет выполнен запуск процедуры импорта.

F7 – создать (Рис. 11.1). Для создания описателя нового объекта управления следует нажать клавишу <F7>, после чего на видеомонитор ЛКУ будет выдан бланк создания и настройки описателя объекта управления, представленный на Рис. 11.3 (подробнее см. раздел 11.2, с. 206).

F4 – редактировать (Рис. 11.1). Чтобы изменить (отредактировать) параметры имеющегося в списке объекта управления, надо переместить курсор на строку списка с соответствующим описателем и нажать клавишу <F4>.

На видеомонитор ЛКУ будет выдан бланк создания и настройки описателя объекта управления (Рис. 11.3), в котором следует отредактировать значения ранее внесенных параметров.

F8 – удалить (Рис. 11.1). После нажатия клавиши <F8> будет выдан дополнительный запрос, и при условии подтверждения будет удален описатель, на строку с которым в списке был установлен курсор.

F6 – перенести (Рис. 11.1). После первого нажатия клавиши <F6> указанная курсором строка в списке выделяется *белым* цветом. Далее можно переместить курсор на любую строку и повторно нажать клавишу <F6>. Отмеченный ранее описатель будет перемещен под строку, на которой был установлен курсор в момент повторного нажатия клавиши <F6>.

> *Замечание*. Между первым и вторым нажатиями клавиши <F6> можно пользоваться только клавишами перемещения курсора. Нажатие другой функциональной клавиши из списка операций в нижней части экрана (Рис. 11.1) сбросит отметку подлежащей переносу строки.

F5 – в текст.файл (Рис. 11.1). При нажатии клавиши <F5> весь список описателей (Рис. 11.1) может быть преобразован в текстовый формат и записан в файл на съемный носитель (FLASH-диск). Предварительно программа управления запрашивает имя файла.

Alt+F7 – из текст.файла (Рис. 11.1). Операция служит для корректировки списка управляемых изделий с помощью списка из файла. При нажатии клавиш <Alt+F7> программа управления запрашивает имя текстового файла со списком и выдает запрос, представленный на Рис. 11.2.

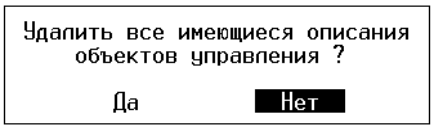


Рис. 11.2 Запрос на уточнение варианта корректировки списка управляемых изделий

При ответе на запрос **Да** новый набор описателей из файла *заменит* старый список описателей. При ответе **Нет** – новые описатели из файла будут *добавлены* к описателям управляемых изделий, имеющимися в списке.

11.2. Создание описателей объектов управления

> *Внимание!* Список описателей для управления блоками наружной маршрутизации *управляемых* изделий формируется на БНМ *управляющего* изделия ЦУА; список описателей для управления блоками внутренней маршрутизации *управляемых* изделий формируется на БВМ *управляющего* изделия ЦУА.

Для создания описателя объекта управления следует в списке (Рис. 11.1) нажать клавишу <F7>, получить бланк создания и настройки (Рис. 11.3) и настроить значения параметров объекта управления, используя этот бланк.

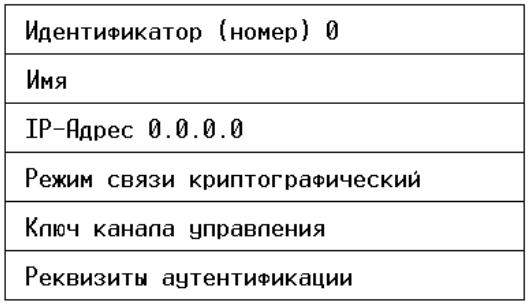


Рис. 11.3 Бланк создания и настройки описателя объекта управления

Идентификатор (Рис. 11.3). Значением параметра является целое число, под которым изделие заносится в базу управляемых изделий. В базе содержатся сведения обо всех изделиях, которыми предполагается управлять. Идентификатор должен быть уникальным, уникальность проверяет программа управления. Идентификатор в дальнейшем изменить нельзя.

Имя (Рис. 11.3). Значением параметра является произвольная алфавитно-цифровая строка длиной не более 32 символов.

IP-адрес (Рис. 11.3). Значением параметра должен быть IP-адрес сетевого интерфейса (или собственный IP-адрес) соответствующего блока маршрутизации управляемого узла.

Режим связи (Рис. 11.3). Параметр определяет способ защиты канала управления. Значение параметра может принимать значения:

- *криптографический* – для управления БНМ (канал управления шифруется на ключах управления);
- *только аутентификация* – для управления БВМ (канал управления защищен туннелем, требуется только аутентификация).

Ключ канала управления (Рис. 11.3). Альтернатива доступна только при подключении блока ЛКУ к БНМ управляющего изделия. При ее выборе на видеомонитор ЛКУ будет выдан представленный на Рис. 11.4 бланк настройки ключа канала управления.

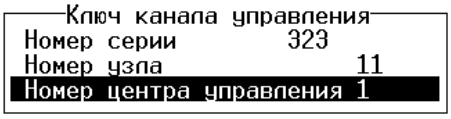


Рис. 11.4 Бланк настройки ключа канала управления

Номер серии (Рис. 11.4). Значением параметра является целое десятичное число, равное номеру серии ключей, используемой для шифрования потока управления.

Номер узла (Рис. 11.4). Значением параметра является целое число (до 5 цифр), равное криптографическому номеру ключа этой серии управляемого изделия.

Номер центра управления (Рис. 11.4). Значением параметра является целое число (до 5 цифр), равное криптографическому номеру ключа этой серии на управляющем изделии в составе ЦУА ЗСПД.

Реквизиты аутентификации (Рис. 11.3). Альтернатива доступна только при подключении блока ЛКУ к БВМ управляющего изделия. При ее выборе на видеомонитор ЛКУ будет выдан бланк настройки параметров аутентификации (Рис. 11.5), с помощью которого необходимо настроить следующие параметры:

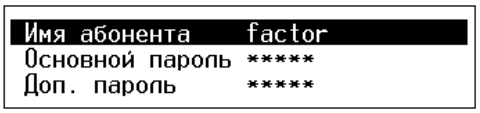


Рис. 11.5 Бланк настройки параметров аутентификации при управлении БВМ

Имя абонента (Рис. 11.5). Значением параметра является имя, под которым БВМ управляющего изделия ЦУА зарегистрирован как абонент на БВМ управляемого изделия.

Основной пароль (Рис. 11.5). Значением параметра является пароль этого абонента.

Доп. пароль (Рис. 11.5). Значением параметра является пароль, который используется для дополнительной защиты от несанкционированного доступа к удаленному управлению (см. раздел 4.1.4, с. 134).

Закончив заполнение бланков, следует нажать клавишу <Esc>. Программа управления вернет на видеомонитор ЛКУ экран управления списком описателей (Рис. 11.1), что позволит проконтролировать измененный список описателей объектов управления.

Внимание! После редактирования списка описателей рекомендуется сохранить обновленные данные на жестком диске маршрутизатора. Для сохранения надо выйти из режима **Администратор сети** и войти в этот режим снова, если требуется продолжить работу.

11.3. Управление удаленными изделиями защиты

Чтобы приступить к удаленному управлению каким-либо из изделий защиты, следует, используя экран управления (Рис. 11.1), перевести в списке курсор на строку с описателем нужного изделия и нажать клавишу <Enter>. На видеомонитор ЛКУ будет выдан экран управления удаленным изделием, аналогичный представленному на Рис. 11.6.

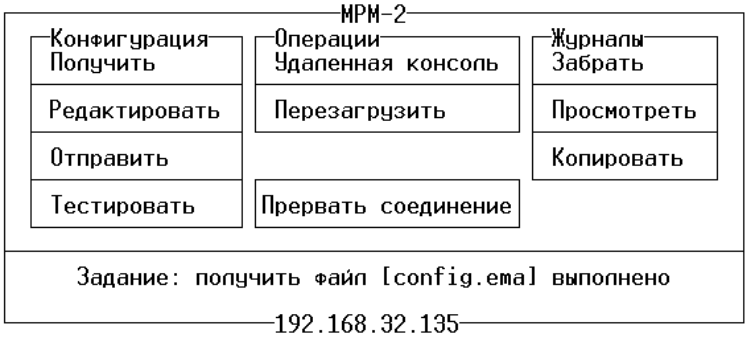


Рис. 11.6 Экран управления удаленным изделием

Верхняя линия рамки экрана содержит имя объекта управления из его описателя (см. Рис. 11.3), нижняя линия рамки содержит IP-адрес управляемого изделия. В нижней части экрана размещается окно для сообщений программы управления.

В средней части экрана приведены доступные для удаленного управления команды **Администратора сети**, объединенные в группы: **Конфигурация**, **Операции**, **Журналы**.

11.3.1. *Конфигурация*

Примечание. Команды группы **Конфигурация** доступны только при подключении блока ЛКУ к БНМ управляющего изделия.

Получение конфигурации. Для получения конфигуратора работающего управляемого изделия надо на экране управления удаленным изделием (Рис. 11.6) выбрать команду **Получить** − переместить на нее курсор и нажать клавишу <Enter>.

Выполнение команды начинается с установления соединения между управляющим и управляемым изделиями защиты. По завершении операции соединение разрывается, на экране (Рис. 11.6) в окне для сообщений программы управления появляется сообщение: «Задание: получить файл [config.ema] выполнено». Полученный с управляемого изделия конфигуратор сохраняется на жестком диске управляющего изделия.

Редактирование конфигурации. Для редактирования полученного от управляемого изделия конфигуратора надо на экране управления удаленным изделием (Рис. 11.6) выбрать команду **Редактировать** − переместить на нее курсор и нажать клавишу <Enter>.

Экран удаленного управления настройкой конфигуратора изделия (Рис. 11.7), выдаваемый на видеомонитор ЛКУ по этой команде, имеет тот же вид, что и экран главного меню программы управления при выполнении настройки *локально* управляемого изделия – в нем повторяются альтернативы главного меню подсистемы **Настройка** (см. Рис. 1.10, с. 18; раздел 1.3.4, с. 14).

Для удобства работы экран удаленного управления настройкой конфигуратора отличается наличием фона (подложки) и информационных строк (см. Рис. 11.7). Настройки, которые можно выполнить с использованием экрана (Рис. 11.7), идентичны настройкам, выполняемым при варианте локального управления изделием, описанном в настоящем РНУ.

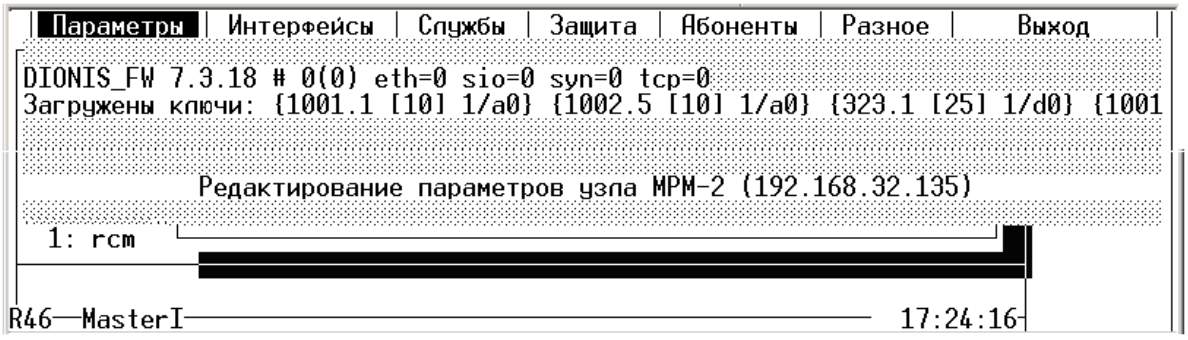


Рис. 11.7 Экран удаленного управления настройкой конфигуратора изделия

Перед началом процедуры редактирования конфигуратор удаленного изделия считывается в оперативную память и все вносимые в него изменения фиксируются только в оперативной памяти. Чтобы сохранить отредактированную администратором сети версию конфигуратора на жестком диске, надо, завершив редактирование, нажать клавишу <Esc>, после чего на видеомонитор ЛКУ будет выдан стандартный при корректировках конфигуратора запрос, представленный на Рис. 11.8.

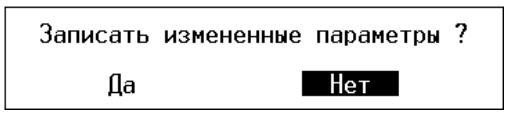


Рис. 11.8 Запрос на подтверждение сохранения внесенных в конфигуратор изменений

После подтверждения конфигуратор управляемого изделия будет сохранен на жестком диске управляющего изделия. Работа программы управления вернется на экран управления удаленным изделием (Рис. 11.6).

Отправка конфигурации. Для отправки конфигуратора на управляемое изделие служит команда **Отправить** (Рис. 11.6). По этой команде будет установлено соединение между управляющим и управляемым изделиями и конфигуратор будет передан на управляемое изделие. После выполнения операции соединение разрывается и на экране появляется сообщение: «Задание: отправить файл [config.ema]выполнено».

Большая часть внесенных в конфигуратор изменений начинает действовать немедленно, но некоторые изменения – только после перезапуска изделия. Поэтому после отправки и получения конфигуратора следует выдать команду **Перезагрузить** в окне управления (Рис. 11.6). Если команды на перезапуск управляемого изделия не будет, то параметры измененного конфигуратора в полном объеме войдут в действие после планового перезапуска управляемого изделия.

Тестирование. Измененный конфигуратор можно отправить на управляемое изделие в режиме *тестирования* с помощью команды **Тестировать** (Рис. 11.6). По этой команде полученный на управляемом изделии

конфигуратор вводится в действие временно – на 5 минут. Если в течение 5 минут на ЦУА не будет дана команда **Отправить**, то на управляемом изделии будет выполнена перезагрузка со старыми параметрами.

Этой возможностью следует пользоваться в тех случаях, когда есть сомнения в правильности вносимых изменений, особенно при редактировании маршрутных таблиц, так как ошибки в них могут привести к тому, что будет потеряна связь с удаленным изделием, т. е. внесенные в конфигуратор удаленного изделия ошибки нельзя будет исправить, используя канал связи с ЦУА.

> *Замечание*. Соединение между изделиями защиты во время получения или отправки конфигуратора можно прервать с помощью команды **Прервать соединение** экрана управления удаленным изделием (Рис. 11.6).

11.3.2. ***Работа в режиме удаленной консоли изделия***

Существует некоторый набор действий, которые нельзя выполнить простым *чтением-изменением-записью* конфигуратора управляемого изделия.

Например:

- нельзя отследить оперативную трассировочную информацию, проходящую через удаленное изделие;
- нельзя выполнить оперативную наладку и настройку;
- при неработоспособности сетевых интерфейсов найти причины можно только выполнением тестовых команд на самом изделии.

Если требуется выполнить какие-либо из перечисленных действий, надо войти на управляемое изделие в режиме *удаленной консоли*. Для этого, используя экран управления удаленным изделием (Рис. 11.6), следует выбрать команду **Удаленная консоль** группы команд **Операции**.

В ответ будет установлено соединение между управляющим и управляемым изделиями, а на видеомониторе ЛКУ управляющего изделия появится *удаленная консоль* управляемого изделия (на нижней рамке экрана при этом выводится *имя* управляемого изделия из описателя в списке объектов управления). В этом режиме управляемое изделие начинает воспринимать команды, выдаваемые Администратором сети с клавиатуры управляющего изделия. Реакция управляемого изделия на эти команды зависит от уровня полномочий, который был установлен для управляющего изделия при настройке работы управляемого изделия в режиме *удаленной консоли* – см. раздел 4.1.4, с. 134.

> *Примечание.* Чтобы закрыть сеанс работы в режиме удаленной консоли, следует разорвать соединение, нажав комбинацию клавиш <Alt=> на управляющем изделии.

11.3.3. ***Работа с журналами управляемого изделия***

При выполнении операции **Получение конфигурации** (раздел 11.3.1) журналы вместе с конфигуратором с управляемого изделия на управляющее не пересылаются.

Чтобы получить журналы управляемого изделия, следует, на экране управления (Рис. 11.6), выбрать команду **Забрать** в группе команд **Журналы**. Выполнение команды начинается с установления соединения между изделиями. Программа управления управляемого изделия, получив запрос, объединяет **LOG**-файлы изделия в один заархивированный файл (**LOGS.EMA**) и передает его на управляющее изделие.

После выполнения операции соединение разрывается и на экране управления (Рис. 11.6) появляется сообщение: «`Задание: принять файл [logs.ema] выполнено`».

Управляющее изделие, получив файл **LOGS.EMA**, разархивирует (распакует) его и добавит полученные фрагменты журналов к соответствующим файлам, полученным ранее.

После того как журналы будут успешно переданы, на управляемом узле они будут удалены.

На управляющем изделии полученные файлы журналов можно просмотреть, выбрав команду **Просмотреть** в группе команд **Журналы** (Рис. 11.6). На видеомонитор ЛКУ будет выдан представленный на Рис. 11.9 экран со списком всех полученных журналов.

Выбрав в списке строку с нужным файлом, следует нажать клавишу <Enter>. В ответ на видеомонитор ЛКУ управляющего изделия будет выдано содержимое журнала.

Полученные журналы можно переместить на съемный носитель (FLASH-диск). Для выполнения процедуры служит команда **Копировать** из группы команд **Журналы** (Рис. 11.6).

> *Замечание.* Рассмотренная здесь процедура копирования журналов во многом повторяет процедуру экспорта журналов на локально управляемом изделии, описанную в разделе 8.2, с. 181. Там же рассмотрена работа со съемными носителями, используемыми изделиями.

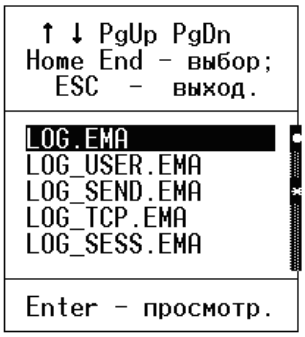


Рис. 11.9 Экран выбора файлов журнала для просмотра

Перед выбором команды **Копировать** надо подключить съемный носитель к разъему USB-устройства ввода/вывода, указать на носителе директорию, в которую будут скопированы журналы, и запустить процедуру копирования.

Все файлы журналов с теми же именами будут переданы (скопированы) на указанный съемный носитель в указанную директорию с одновременным расчетом контрольной суммы по алгоритму CRC-32.

11.4. Сервис ключей

Чтобы приступить к работе с ключами, следует в списке описателей (Рис. 11.1) перевести курсор на строку с описателем интересующего управляемого изделия и нажать клавишу <F2>. На видеомонитор ЛКУ будет выдан экран управления ключами управляемого изделия, аналогичный представленному на Рис. 11.10 и содержащий список ключей (сетевых наборов), которые загружены на управляемом изделии. Изначально список пустой.

На верхней рамке экрана (Рис. 11.10) выводится имя из строки описателя управляемого изделия (см. Рис. 11.1).

Список ключей занимает среднюю часть экрана: под заголовком **Серия.Номер** выводятся серия и криптографический номер ключа, загруженного на управляемом изделии; под заголовком **#** – размер криптографической матрицы (количество криптографических ключей в сетевом наборе); под заголовком **Тип** – наименование ключевого документа с символом **у** для ключей канала управления; под заголовком **Зона** – номер зоны.

На нижней рамке экрана – IP-адрес управляемого изделия.

Рис. 11.10 Экран управления загруженными ключами управляемого изделия

Администратор сети может выполнить следующие действия:

- получить список ключей с управляемого изделия;
- заблокировать один ключ из криптосистемы удаленного изделия;
- заблокировать серию ключей.

> *Внимание!* Ключи на управляемом изделии администратор сети может только заблокировать, удалить ключи удаленно нельзя.

F3 – получить информацию (Рис. 11.10). После нажатия клавиши <F3> выполняется соединение с управляемым изделием, список загруженных ключей пересылается на управляющее изделие и выводится на экран управления (Рис. 11.10). Затем соединение разрывается и на экране появляется сообщение:

«Задание: отправить файл [info.ema] выполнено».

F4 – удалить ключ (Рис. 11.10). Команда позволяет заблокировать один ключ из сетевого набора конкретной серии. Это – ключ того объекта в ЗСПД, с которым будет запрещена связь.

Чтобы выполнить команду, следует перевести курсор на соответствующую строку в списке и нажать клавишу <F4>. В ответ будет выдан запрос на ввод номера удаляемого ключа (Рис. 11.11):

```
Задайте номер удаляемого ключа серии (1)1001.1 :
```

Рис. 11.11 Запрос на ввод номера удаляемого ключа

Необходимо ввести номер ключа и нажать клавишу <Enter> – будет установлено соединение с управляемым изделием и указанный ключ будет заблокирован. Затем соединение разрывается и на экране появляется сообщение:

«Задание: команда 'Удалить ключ' [0000oh00100103_] выполнено».

F8 – удалить серию (Рис. 11.10). Команда позволяет заблокировать все ключи одной серии. После этого управляемому изделию будет запрещена связь со всеми изделиями конкретной криптографической сети.

Чтобы выполнить команду, следует в списке (Рис. 11.10) перевести курсор на строку с ключом этой серии и нажать клавишу <F8>. В ответ будет выдан представленный на Рис. 11.12 дополнительный запрос на подтверждение блокировки ключей указанной серии.

```
Заблокировать ключи на узле ?
          9999.1

     Да          Нет
```

Рис. 11.12 Запрос на подтверждение блокировки ключей указанной серии

После ответа **Да** будет установлено соединение с управляемым изделием и указанная серия ключей для использования изделием будет заблокирована. Затем соединение разрывается и появляется сообщение:

«Задание: команда 'Удалить серию ключей' [0005#-00100103_] выполнено».

11.5. Настройки на управляющем и управляемом изделиях

Чтобы изделие можно было передать на удаленное управление одному из ЦУА, должна быть обеспечена доступность управляемого изделия по телекоммуникационной сети для управляющего изделия, размещенного в составе ЦУА ЗСПД.

На управляемом изделии должен быть разрешен запуск службы DCP (чтобы разрешить запуск службы, следует в меню управления запуском служб маршрутизатора (Рис. 5.1, с. 151) в столбце **Пуск** службы DCP установить значение *Да* (см. раздел 5, с. 151).

Кроме того, на управляемом изделии при настройке режимов работы системных журналов следует отменить режим *зацикливания* журналов и отправку журналов, поскольку их хранение берет на себя управляющее изделие.

Настройки конфигураторов изделий, которые следует выполнить на управляемом и управляющем изделиях, рассмотрим на примере схемы, представленной на Рис. 11.13.

Рис. 11.13 Пример схемы организации связи при удаленном управлении изделиями

11.5.1. Настройки на управляющем и управляемом изделиях при управлении БНМ

С целью выполнения требований безопасности следует разрешить обмен информацией по TCP-порту 362 только с конкретного адреса – IP-адреса сетевого интерфейса БНМ управляющего изделия. Это обеспечивается созданием системных фильтров **ext_in** и **ext_out**, включающих приведенные ниже правила фильтрации и выполняющих фильтрацию на внутренних (служебных) интерфейсах БНМ управляющего и управляемого изделий.

На внутреннем интерфейсе блока наружной маршрутизации управляемого изделия:

фильтр ext_in

```
Разрешить 192.168.1.2/32 192.168.1.1/32 TNL 0 - 0
Разрешить 192.168.1.2/32 192.168.1.1/32 TCP 362 - 362
Сбросить 0.0.0.0/00 0.0.0.0/00 ANY  0 - 0
```

фильтр ext_out

```
Разрешить 192.168.1.1/32 192.168.1.2/32 TNL 0 - 0
Разрешить 192.168.1.1/32 192.168.1.2/32 TCP 1024 – 65535
Сбросить 0.0.0.0/00 0.0.0.0/00  ANY  0 - 0
```

На внутреннем интерфейсе блока наружной маршрутизации управляющего изделия:

фильтр ext_in

```
Разрешить 192.168.1.1/32 192.168.1.2/32 TNL 0 - 0
Разрешить 192.168.1.1/32 192.168.1.2/32 TCP 1024 – 65535
Сбросить 0.0.0.0/00 0.0.0.0/00  ANY  0 - 0
```

фильтр ext_out

```
Разрешить 192.168.1.2/32 192.168.1.1/32 TNL 0 - 0
Разрешить 192.168.1.2/32 192.168.1.1/32 TCP 362 – 362
Сбросить 0.0.0.0/00 0.0.0.0/00  ANY  0 - 0
```

11.5.2. ***Настройки на управляющем и управляемом изделиях при управлении БВМ***

Между управляющим и управляемым изделиями организован криптотуннель, по которому выполняется удаленное управление блоком внутренней маршрутизации. На каждом из изделий должна быть выполнена настройка криптотуннеля – статического туннеля (см. раздел 3.1.1.2, с. 78) или TNL-интерфейса (см. раздел 2.4.2, с. 39). В качестве локальных и удаленных IP-адресов криптотуннеля следует использовать адреса: **192.168.1.1** и **192.168.1.2**.

Чтобы обеспечить попадание управляющего потока в криптотуннель, следует задать следующие *правила отбора* при создании криптотуннеля:

На управляемом изделии:

Режим – **разрешить**
Протокол – **TCP**
Фиксировать – **нет**
TCP – флаги – **нет**
Диапазон номеров портов – **1024 – 65535**
Адрес отправителя – **10.0.0.1/32**
Адрес получателя - **10.10.10.1/32**

На управляющем изделии:

Режим – **разрешить**
Протокол – **TCP**
Фиксировать – **нет**
TCP – флаги – **нет**
Диапазон номеров портов – **362-362**
Адрес отправителя – **10.10.10.1/32**
Адрес получателя - **10.0.0.1/32**

Для выполнения требований безопасности надо разрешить обмен информацией по TCP-порту ***362*** только с конкретного адреса – IP-адреса сетевого интерфейса БВМ управляющего изделия. Это обеспечивается созданием системных фильтров **int_in** и **int_out**, выполняющих фильтрацию на внутренних интерфейсах БВМ управляющего и управляемого изделий и включающих приведенные ниже правила фильтрации.

На блоке внутренней маршрутизации управляемого изделия:

фильтр int_in

```
Разрешить 10.10.10.1/10.0.0.1/32 TCP 362 – 362
Сбросить 0.0.0.0/00 0.0.0.0/00  ANY  0 - 0
```

фильтр int_out

```
Разрешить 10.0.0.1/10.10.10.1/32 TCP 1024 – 65535
Сбросить 0.0.0.0/00 0.0.0.0/00  ANY  0 - 0
```

На блоке внутренней маршрутизации управляющего изделия:

фильтр int_in

```
Разрешить 10.0.0.1/10.10.10.1/32 TCP 1024 – 65535
Сбросить 0.0.0.0/00 0.0.0.0/00  ANY  0 - 0
```

фильтр int_out

```
Разрешить 10.10.10.1/10.0.0.1/32 TCP 362 – 362
Сбросить 0.0.0.0/00 0.0.0.0/00  ANY  0 - 0
```

Для выполнения процедуры аутентификации:

- на управляемом изделии следует создать учетную запись абонента (см. раздел 6, с. 170) и конфиденциально сообщить его регистрационные параметры (имя и пароль) персоналу ЦУА;
- этому абоненту надо дать постоянное разрешение на удаленное управление (раздел 4.1.4, с. 134) и конфиденциально сообщить установленный дополнительный пароль персоналу ЦУА.

Примечания.

1. В настоящем разделе рассмотрены вопросы удаленного управления в ситуации, когда в процессе участвуют только изделия, исполненные в двухсегментной архитектуре технологии DioNIS® (в том числе, изделия серии М-479Рх). Если требуется организовать удаленное управление ранее выпускавшимися изделиями семейства М-479 с применением в качестве управляющих изделий, исполненных в двухсегментной архитектуре технологии DioNIS®, то это возможно только с консоли внутреннего маршрутизатора управляющего изделия и только в режиме удаленной консоли.

2. Удаленное управление согласно протоколу DCP предусматривает использование ключей шифрования канала *управления*. Для изделий М-479К ключи шифрования канала управления не предусмотрены. Поэтому для защиты передаваемого трафика канала управления используются стандартные криптографические туннели. Чтобы разрешить циркуляцию между изделиями не зашифрованного трафика канала управления согласно протоколу DCP (т. е. разрешить управление изделием в режиме «Только аутентификация»), на *управляемом* изделии следует создать фильтр с системным именем **dcp**, содержащий правило фильтрации, аналогичное приведенному ниже:

```
разрешить 192.168.32.225/32 192.168.32.229/32 TCP 362 – 362
```

Приложение А. Основы IP-адресации и маршрутизации

Изложенный в настоящем Приложении материал содержит сведения об основах IP-адресации и маршрутизации, которыми следует руководствоваться при рассмотрении работы любого IP-маршрутизатора, работающего в сетях, функционирующих согласно системным требованиям `internet/intranet`-технологии, обмен данными в которых базируется на применении стека протоколов TCP/IP.

> *Примечание.* Настройка IP-маршрутизаторов изделий, исполненных в двухсегментной архитектуре технологии DioNIS®, имеет некоторые особенности при подготовке изделия к работе, поэтому материал настоящего Приложения может оказаться полезным и опытным сетевым администраторам.

Следует также учитывать ту особенность, что в составе изделия функционируют *два* самостоятельных маршрутизатора – БВМ и БНМ, каждый из которых, обладая собственным набором сетевых интерфейсов и внутренним интерфейсом, самостоятельно решает задачу маршрутизации поступающих на его интерфейсы IP-потоков данных.

Основной целью создания сетей передачи данных является организация взаимодействия между компонентами прикладного программного обеспечения (ПО) – приложениями Пользователя, функционирующими в составе территориально удаленных сетевых IP-устройств. Для упрощения разработки прикладного ПО все программные компоненты, отвечающие за взаимодействие с сетью передачи данных, выделили в отдельное множество – *сетевое ПО* и определили стандартный интерфейс взаимодействия между прикладным и сетевым программным обеспечением. Схема сетевого информационного взаимодействия между компонентами прикладного ПО, каждый из которых функционирует в составе удаленных друг от друга сетевых IP-устройств, с использованием сетевого ПО, каналов связи и собственно сети передачи данных изображена на Рис. А.1.

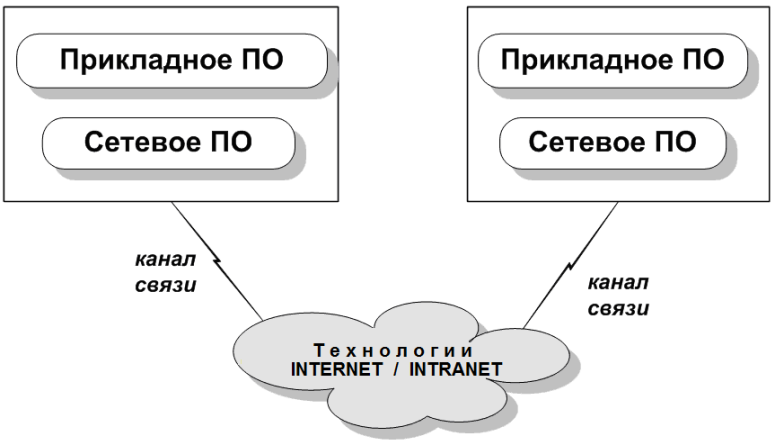


Рис. А.1 Схема организации сетевого обмена между компонентами прикладного ПО

Для сетей передачи данных, построенных на различных принципах, состав сетевого ПО существенно различен. Будем рассматривать сетевое ПО, используемое для взаимодействия прикладных задач – приложений Пользователя – через сети, функционирующие согласно системным требованиям `internet/intranet`-технологии, обмен данными в которых базируется на применении стека протоколов TCP/IP.

На приведенном ниже Рис. А.2 представлена структура такого сетевого ПО.

На нижнем уровне сетевого ПО находится компонент **`Интерфейс`**, который выполняет следующие функции:

1. Взаимодействует с аппаратурой канала связи, обеспечивая прием данных из канала и передачу данных в канал.
2. Выполняет упаковку подлежащих передаче в канал блоков данных в *транспортные* кадры, состоящие из собственно передаваемых данных и вспомогательной информации, необходимой аппаратуре канала связи для правильной доставки данных (физические адреса, контрольные суммы и пр.).
3. Некоторые типы интерфейсов для формирования заголовков транспортных кадров используют вспомогательный компонент ARP, подробное описание которого приведено ниже.
4. Выполняет прием от канала связи транспортных кадров, из которых извлекает данные, отправленные удаленной стороной.

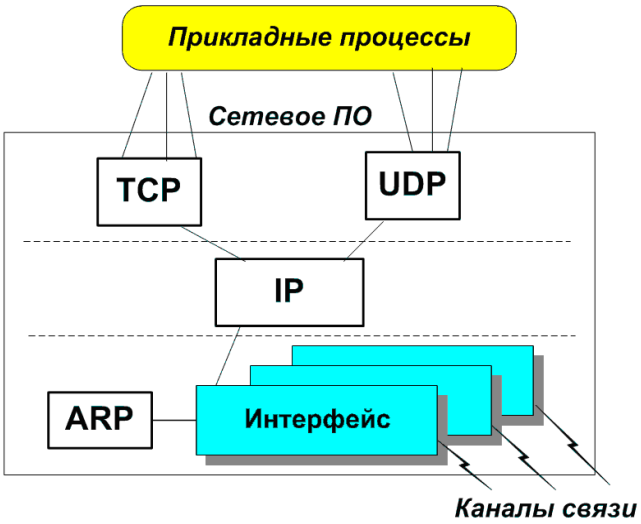


Рис. А.2 Структура сетевого ПО для обмена между приложениями согласно стеку протоколов TCP/IP

Интерфейсы используются следующим, более высоким уровнем сетевого ПО – уровнем **`IP`** (Internet Protocol). Компоненты программного обеспечения уровня IP выполняют следующие функции:

1. Получают от лежащих выше уровней сетевого ПО (**`TCP`**, **`UDP`** и др.) блоки данных, подлежащие доставке на удаленную вычислительную систему.
2. К каждому блоку данных добавляют IP-заголовок, в котором указывается адрес получателя блока данных, адрес его отправителя и некоторая вспомогательная информация. Блок данных, снабженный IP-заголовком, называется IP-пакетом или IP-датаграммой.
3. Выполняют процедуру маршрутизации, в результате которой по адресу назначения каждого IP-пакета определяется интерфейс (один из многих возможных), ответственный за дальнейшую доставку данных. При наличии подходящего интерфейса IP-пакет передается ему для передачи в канал связи.
4. Обрабатывают принятые всеми интерфейсами блоки данных, которые являются IP-пакетами, отправленными IP-уровнями сетевого ПО других вычислительных систем. Из каждого IP-пакета извлекаются данные и передаются лежащим выше уровням сетевого ПО (TCP, UDP и др.).

Самый верхний уровень сетевого ПО обеспечивает взаимодействие прикладного ПО с уровнем IP и, как следствие, с сетью передачи данных. В зависимости от потребностей прикладного ПО возможны два основных варианта взаимодействия компонентов.

1. Взаимодействие с помощью непрерывного дуплексного потока информации. При такой форме взаимодействия по команде прикладного ПО одной из сторон организуется *виртуальный* канал обмена прикладными данными, который может быть использован для непрерывной передачи любого объема информации между парой взаимодействующих приложений. Виртуальный канал обмена данными существует вплоть до его явной отмены по команде любой из взаимодействующих сторон. В составе сетевого ПО указанный тип передачи прикладных данных организуется с помощью компонента TCP (Transport Control Protocol). Компонент TCP выполняет следующие функции.

   На передающем изделии:

   - получает от прикладного ПО поток подлежащих передаче данных;
   - выполняет разбиение этого потока на фрагменты (пакеты);
   - снабжает каждый пакет TCP-заголовком и передает уровню IP для последующей доставки адресату;

   На принимающем изделии:

   - принимает от уровня IP все TCP-пакеты;
   - по информации из их заголовков восстанавливает исходный поток прикладных данных и передает его соответствующему прикладному ПО;
   - контролирует целостность принятого потока информации и, в случае потери сетью отдельных фрагментов этого потока, запрашивает повторную отправку утерянных данных передающей стороной.

2. Взаимодействие с помощью периодически отправляемых небольших порций информации – IP-датаграмм. Осуществляемая периодически нерегулярная передача IP-датаграмм не требует наличия постоянного виртуального канала обмена информацией, ее организация существенно проще, чем обеспечиваемая компонентом TCP процедура информационного обмена. Для поддержки датаграммой формы взаимодействия прикладного ПО в составе сетевого ПО имеется компонент UDP (User Datagram Protocol), выполняющий следующие функции.

На передающем изделии:

- получение от прикладного ПО блоков подлежащей передаче информации;
- снабжение каждого блока UDP-заголовком и передача UDP-датаграмм уровню IP для последующей доставки адресату;

На принимающем изделии:

- прием от уровня IP всех UDP-датаграмм;
- извлечение из них блоков прикладной информации и передача их для обработки соответствующему прикладному ПО – приложению.

Адресация в IP-сети

Одной из основных задач, возникающих при организации сети передачи данных, является задача выбора *системы адресации* объектов сети. Как следует из приведенной выше структуры сетевого ПО, в сети, функционирующей согласно системным требованиям `internet/intranet`-технологии, существуют два класса адресуемых объектов сети и, соответственно, два класса адресов.

1. **`Адреса точек доступа вычислительных систем к сети`**. Ближайшим к сети компонентом сетевого ПО являются *сетевые интерфейсы*, поэтому вся вычислительная система доступна (видна из сети) по ее *адресам сетевых интерфейсов*.
2. **`Идентификаторы компонентов прикладного ПО`**, работающих на каждой вычислительной системе. На одной вычислительной системе могут одновременно работать несколько прикладных задач, поэтому одного адреса интерфейса вычислительной системы недостаточно. Вместе с адресом интерфейса необходимо указывать *идентификатор* конкретной задачи.

Архитекторы `internet/intranet`-технологии решили проблему адресации объектов сети весьма просто. Все объекты сети нумеруются, и для указания требуемого объекта просто используется его порядковый номер. В сети, функционирующей согласно системным требованиям `internet/intranet`-технологии, предусмотрены *два типа адресов*.

1. *IP-адрес точки доступа* вычислительной системы к сети. Он задается 32-разрядным (4 байта) двоичным числом, означающим порядковый номер данного интерфейса данной вычислительной системы в сети. Естественно, организационными мерами должна быть обеспечена *уникальность* IP-адресов во всей сети. При указании IP-адресов обычно пользуются их точечно-десятичной (dotted-decimal) записью: 32-разрядное двоичное число в заголовке IP-пакета разделяется на 8-битные компоненты (*октеты*), каждый из которых представляется в документах десятичным числом в интервале от **`0`** до **`255`**. Десятичные представления компонентов IP-адреса отделяются друг от друга *точками*. Слева записывается наиболее значимый компонент 32-разрядного числа. Например, IP-адрес **`1100 0010 0100 0011 0000 0011 1000 1010`** должен записываться как **`194.67.3.138`**.
2. *Номер порта* (идентификатор компонента прикладного ПО). Он задается 16-разрядным (2 байта) двоичным числом, означающим порядковый номер компонента прикладного ПО на данной вычислительной системе. При указании номера порта используется его *десятичное* представление.

Таким образом, для указания требуемого компонента прикладного ПО в сети необходимо указать его полный адрес (**`socket`**), состоящий из *IP-адреса* сетевого интерфейса вычислительной системы и *номера порта*. При указании полных адресов два компонента, их составляющих, отделяют друг от друга *двоеточием*.

Например, полный адрес **`192.168.1.12:25`** обозначает прикладную задачу **`25`** на вычислительной системе с IP-адресом **`192.168.1.12`**.

Задача маршрутизации

Учитывая изложенное выше, можно сформулировать следующий алгоритм обмена данными в сети передачи данных, функционирующей согласно системным требованиям `internet/intranet`-технологии, следующим образом.

1. От каждого сетевого IP-устройства сеть получает поток IP-пакетов. В заголовке каждого из них указан *IP-адрес назначения* – IP-адрес сетевого IP-устройства (узла), которому должен быть доставлен данный IP-пакет.
2. Получив IP-пакет, каждый узел сети (IP-маршрутизатор) должен по IP-адресу назначения определить направление дальнейшей доставки пакета. Под направлением дальнейшей доставки понимается сетевой интерфейс, которому будет передан IP-пакет для передачи на следующий по маршруту доставки узел сети.
3. Если на текущий момент путь доставки IP-пакета адресату (сетевому IP-устройству назначения) существует, то, пройдя через несколько узлов IP-сети, каждый отправленный IP-пакет достигнет своего адресата.

Каждому маршрутизатору в составе сети приходится решать задачу *маршрутизации* – задачу выбора из набора собственных сетевых интерфейсов интерфейса дальнейшей доставки IP-пакета по содержащемуся в его заголовке IP-адресу назначения. Для успешного решения этой задачи каждый маршрутизатор сети должен обладать информацией о топологии всей сети, т.е. знать размещение всех подключенных к сети вычислительных систем. При выбранной системе 32-разрядной двоичной адресации в сети может быть до 4294967295 объектов, поэтому получение знаний о каждом из них в каждом узле сети нереально.

Для упрощения задачи маршрутизации архитекторами `internet/intranet`-технологии был использован следующий прием. Каждый IP-адрес разбили на две части: *номер сети* (**`netid`**) и *номер узла* в этой сети (**`hostid`**). Сначала, в *старших* битах 32-разрядного двоичного адреса, указывается номер сети, а затем, в *младших* битах адреса, – номер узла:

Номер сети	***Номер узла***

При этом для решения задачи маршрутизации – определения, через *какой* интерфейс данного маршрутизатора должен быть отправлен полученный IP-пакет, адресованный получателю с IP-адресом, указанным в его заголовке, – используется только часть IP-адреса, содержащая *номер сети*, что избавляет маршрутизаторы от необходимости получения информации обо *всех* подключенных к IP-сетям (например, к сети Интернет) сетевых устройствах (узлах).

Указанный подход требует от маршрутизаторов умения в каждом IP-адресе провести *границу* между номером сети и номером узла в этой сети.

Первоначально IP-адрес предполагали разбивать только *по границе октетов*, а информацию о точке разбиения хранить непосредственно в первом октете адреса. В результате появились 5 классов адресов: A, B, C, D, E. Адреса классов D и E используются только в специальных случаях. Адреса классов A, B, C присваиваются специальной службой Internet Network Information Center (InterNIC) по запросам крупных сетевых операторов (Service Providers). Последние, в свою очередь, производят регистрацию и подключение абонентов к сети Internet с одновременной обязательной выдачей IP-адресов из предоставленных им службой InterNIC зон адресов.

Определение принадлежности любого IP-адреса к одному из указанных классов выполняется простым анализом нескольких начальных бит адреса, как это показано на приведенном ниже рисунке.

Нетрудно подсчитать возможное количество сетей и возможное количество узлов в каждом классе адресов. Для справки эти данные приведены ниже.

Характеристики классов адресов

Класс	Диапазон значений первого октета	Возможное количество сетей	Возможное количество узлов в сети
A	1 - 126	126	16777214
B	128 - 191	16382	65534
C	192 – 223	2097150	254
D	224 – 239	-	268435454
E	240 - 247	-	134217726

Вместе с введением классификации были ведены *специальные* значения для IP-адресов. Основные из них указаны в приведенной ниже таблице.

Специальные IP-адреса

все нули		Данный узел
номер сети	**все нули**	Данная IP-сеть
все нули	**номер узла**	Узел в данной (локальной) IP-сети
все единицы		Все узлы в данной (локальной) IP-сети
номер сети	**все единицы**	Все узлы в указанной IP-сети
127	что-нибудь (часто **1**)	Петля

Напомним, что соглашениями Интернета в каждой подсети предусмотрены два *специальных* номера узла:

- *все нули* – используется для указания адреса сети без указания номера узла;
- *все единицы* – используется для указания сразу всех узлов данной сети (**broadcast**-адрес).

Наличие специальных номеров узлов уменьшает возможное количество узлов в сети каждого класса на два. Например, в сети класса С вместо ожидаемых 256 узлов может быть только 254 узла.

К сожалению, предложенный механизм разбиения IP-адресов на составляющие его номер сети и номер узла с использованием только классов адресов оказался не очень пригодным. Быстро пространство возможных номеров сетей в каждом классе адресов оказалось исчерпанным или близким к этому. Это привело к необходимости введения другого механизма разбиения IP-адресов на две части с точностью *до бита*. Иными словами, потребовалось проводить границу между номером сети и номером узла в любом месте IP-адреса. Для этой цели было введено понятие *маски сети*.

Маска сети – это 32-разрядное двоичное число, единичные разряды которого указывают на поле *номер сети* в IP-адресе, а нулевые – на поле *номер узла*. Нетрудно увидеть, что алгоритм *вычисления* номера сети по IP-адресу заключается в простом логическом умножении значения IP-адреса на значение маски сети.

Вычисление адреса сети

IP-адрес	&	Маска	=	Адрес сети

& – операция логического умножения

Маска сети, так же как и IP-адрес, записывается в точечно-десятичной (dotted-decimal) форме, как показано в примере:

0	8	16	24	31
1111 1111	1111 1111	1111 1111	1110 0000	
255.	255.	255.	224	

Классы каналов связи

Для организации связи между сетевыми устройствами в сети передачи данных используются *каналы связи*. Все многообразие применяемых при использовании internet/intranet-технологии каналов связи можно разделить на *два* следующих класса.

1. Двухточечные каналы связи.

На Рис. А.3 приведена условная схема *двухточечного* канала связи.

Рис. А.3 Схема двухточечного канала связи

Двухточечные каналы связи обладают следующими свойствами:

- соединяют только два сетевых устройства;
- поток данных от устройства **A** попадает только к устройству **B**;
- отсутствует проблема адресации на канальном уровне и, как следствие, отсутствует необходимость определения адреса канального уровня для устройства-получателя, которому направляется IP-пакет;
- для двухточечных каналов связи чаще всего используются следующие протоколы транспортировки IP-пакетов: **PPP**, **SLIP**, **CSLIP**.

Благодаря отсутствию проблемы адресации канального уровня двухточечные каналы весьма просты с точки зрения их использования интерфейсами. Все подлежащие транспортировке IP-пакеты просто упаковываются в транспортные кадры (фреймы) канала и извлекаются на противоположной стороне.

2. Многоточечные каналы связи.

Многоточечные каналы связи обладают следующими свойствами:

- соединяют два и более сетевых устройств;
- поток данных от устройства **A** может попасть к любому сетевому устройству, подключенному к каналу, следовательно, в заголовках кадров обязательно следует указывать адреса канального уровня для отправителя и получателя.

На Рис. А.4 приведена условная схема многоточечного канала связи.

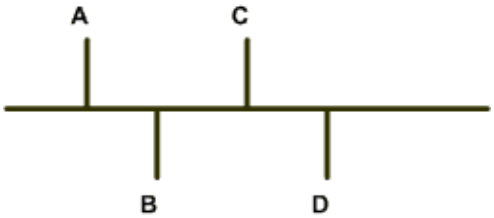


Рис. А.4 Схема многоточечного канала связи

Примером многоточечных каналов связи могут служить каналы локальных Ethernet-сетей, в которых для транспортировки IP-пакетов используются Ethernet-кадры в формате фрейма Ethernet_II.

Необходимость использования адресов канального уровня (L2-уровня модели OSI) при формировании транспортных кадров Ethernet-сети – Ethernet-кадров – требует применения специального протокола **ARP** (Address Resolution Protocol), который для каждого IP-адреса назначения в сети определяет транспортный адрес станции-получателя в данной локальной сети − т.н. MAC-адрес.

Для транспортировки по локальной сети все IP-пакеты должны быть упакованы в транспортные Ethernet-кадры в формате Ethernet_II, имеющие приведенный ниже следующий формат.

Формат кадров (фреймов) Ethernet_

6	6	2	46-1500
Dest	**Source**	**Type**	**Payload (Данные)**

Dest – MAC-адрес получателя

Source – MAC-адрес отправителя

Type – Тип данных показывает, пакет какого из сетевых протоколов находится в поле данных **Payload**

Payload – IP-пакет L3-уровня модели OSI размером от 46 до 1500 байт

Примечание. Отметим, что в составе приведенного выше формата Ethernet-кадра фрейма Ethernet_II не показаны обрамляющие его поля, обработкой которых на физическом (L1) уровне занимается Ethernet-адаптер – поле **Preamble** длиной 8 байт – последовательность бит, по сути не являющаяся частью заголовка Ethernet-кадра, а только определяющая его начало, а также поле **FCS** (**Frame Check Sequences**) длиной 4 байта, содержащее значение CRC (**Cyclic Redundancy Check**) – контрольной суммы, используемой для выявления ошибок передачи с помощью применения методов циклических кодов, оставляющих без изменения исходное содержимое передаваемых данных; вычисляется передающей стороной и помещается в поле **FCS**; принимающая сторона вычисляет данное значение самостоятельно и, сравнивая с полученным, принимает решение о качестве передачи Ethernet-кадра по сети.

MAC (**Media Access Control**) – шестибайтовый адрес *канального* уровня, присваиваемый изготовителем каждого Ethernet-адаптера, обеспечивающего физическое взаимодействие интерфейса изделия с локальной сетью. Специальное соглашение между изготовителями Ethernet-адаптеров гарантирует уникальность MAC-адресов в каждой из существующих локальных сетей.

Пример записи MAC-адреса в принятом специалистами формате: **00:01:39:00:2F:54**

Перед отправкой IP-пакета сетевой интерфейс должен определить значения для всех трех полей заголовка Ethernet-кадра в формате Ethernet_II. Значение поля **Source** интерфейс считывает непосредственно из своего Ethernet-адаптера. Поле **Type** должно иметь значение ***0x0800*** (в поле данных Ethernet-кадра находится IP-пакет). А вот значение поля **Dest** должно быть получено с помощью протокола ARP, схема работы которого приведена ниже на Рис. А.5.

Рис. А.5 Схема работы ARP-протокола

Между множествами IP-адресов и MAC-адресов нет никакой алгоритмической зависимости, поэтому единственным вариантом установления их взаимно однозначного соответствия является ARP-таблица, например, такая, как приведенная ниже.

IP-адрес	MAC-адрес
192.168.1.1	00:00:39:00:2F:C3
192.168.1.2	00:01:28:A7:5A:17
192.168.1.3	00:00:10:99:AC:54

На Рис. А.6 приведена блок-схема алгоритма работы ARP-протокола. Принцип работы протокола ARP основан на возможности отправки Ethernet-кадров сразу всем станциям локальной сети – т.н. *широковещательных* broadcast-кадров.

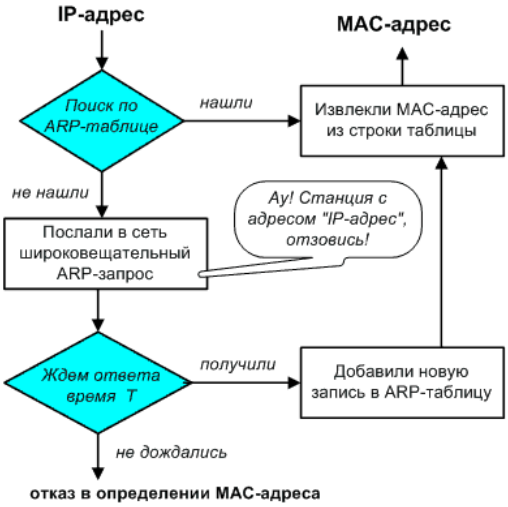


Рис. А.6 Блок-схема алгоритма работы ARP-протокола

После запуска любого физического интерфейса изделия, работающего с каналом локальной Ethernet-сети, ARP-таблица маршрутизатора изделия обычно пуста. Первый же IP-пакет, отправляемый сетевым интерфейсом, активизирует работу ARP-протокола. Широковещательный Ethernet-кадр, содержащий ARP-запрос, включающий IP-адрес получателя IP-пакета, отправляется всем рабочим станциям broadcast-домена сети.

> *Примечание.* Обычно L2-коммутатор со всеми подключёнными к нему сетевыми устройствами представляет собой *единый широковещательный домен* (broadcast-домен). Если одно из этих сетевых устройств посылает Ethernet-кадр в сеть на специальный широковещательный адрес (это MAC-адрес, все позиции которого имеют значение *единица*, т.е: **ff:ff:ff:ff:ff:ff**), коммутатор передает его во все свои порты (за исключением того порта, по которому Ethernet-кадр был коммутатором получен), и этот Ethernet-кадр получают все остальные сетевые устройства broadcast-домена.

Если одна из станций опознает указанный IP-адрес в качестве собственного, то она обязана прислать ARP-ответ, в котором будет указан ее MAC-адрес. На основе ответа станции будет сформирована строка в ARP-таблице, что обеспечит дальнейшую работу ARP-протокола для данного IP-адреса без выдачи повторных запросов в сеть.

Станции локальной сети в любой момент могут отключаться от сети, поэтому записи в ARP-таблице не могут храниться вечно. Их необходимо периодически удалять и заменять новыми. С этой целью каждой записи ARP-таблицы назначается *время жизни* (обычно от 5 до 15 минут), по истечении которого запись удаляется из таблицы.

Адресация в локальных сетях

В локальных сетях, как и во всех многоточечных каналах связи, возможны две формы адресации – *прямая* и *косвенная*.

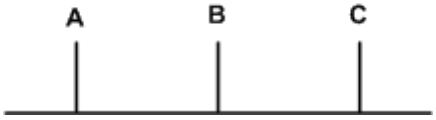
Прямая адресация. Используется для передачи IP-пакетов между станциями одного сегмента (broadcast-домена) локальной сети.

Рассмотрим механизм прямой адресации на следующем примере. Пусть станции **A**, **B** и **C** подключены к одному сегменту локальной сети, и станции **A** необходимо отправить IP-пакет станции **B**. IP-уровень сетевого ПО станции **A** формирует IP-пакет, указывая в его заголовке следующие IP-адреса: отправителя – **IP(A)** и получателя – **IP(B)**. Передавая этот IP-пакет интерфейсу, IP-уровень должен указать, что интерфейсу предписывается отправлять пакет с использованием *прямой* адресации. В этом случае интерфейс выполнит *упаковку* IP-пакета в транспортный кадр Ethernet_II и его отправку по следующему алгоритму.

1. MAC-адрес отправителя будет получен интерфейсом от его собственной платы локальной сети – **MAC(A)**.

2. Для получения MAC-адреса получателя интерфейс воспользуется ARP-протоколом, который по IP-адресу станции **B** определит ее MAC-адрес – **MAC(B)**.
3. Транспортный кадр будет отправлен в сеть непосредственно для станции **B**; интерфейс станции **B** его получит, извлечет IP-пакет и передаст на обработку.

Схему работы механизма прямой адресации поясняют приведенные ниже на Рис. А.7 рисунок и таблица. Отличительной чертой прямой адресации является формирование MAC-адреса получателя транспортного кадра *непосредственно* по IP-адресу станции назначения.



Адрес	Отправитель	Получатель
IP-заголовок	IP(A)	IP(B)
MAC-заголовок	MAC(A)	MAC(B)

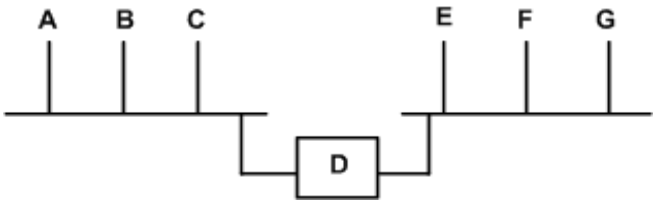
Рис. А.7 Схема работы механизма прямой адресации

Косвенная адресация. Должна использоваться в тех случаях, когда необходима передача IP-пакетов между станциями, расположенными в *разных* сегментах локальной сети, или в разных локальных сетях.

Рассмотрим механизм косвенной адресации на следующем примере. Пусть станции **A**, **B** и **C** подключены к одному сегменту локальной сети, а станции **E**, **F** и **G** – к другому. Взаимосвязь сегментов сети выполняет специальная станция **D**, называемая *шлюзом*. Пусть станции **A** необходимо отправить IP-пакет станции **E**. IP-уровень сетевого ПО станции **A** формирует IP-пакет, указывая в его заголовке следующие IP-адреса: отправителя – **IP(A)** и получателя – **IP(E)**. Поскольку станция **E** непосредственно со станции **A** недоступна, то применение прямой адресации в данном случае невозможно. Следовательно, передавая этот IP-пакет интерфейсу, IP-уровень должен указать, что интерфейс должен отправлять пакет с использованием *косвенной* адресации, причем, в качестве шлюза необходимо использовать станцию **D**. В этом случае интерфейс выполнит упаковку IP-пакета в транспортный кадр Ethernet_II и его отправку по следующему алгоритму.

1. MAC-адрес отправителя будет получен интерфейсом от его собственной платы локальной сети – **MAC(A)**.
2. Для получения MAC-адреса получателя интерфейс воспользуется ARP-протоколом, который по IP-адресу шлюза (станции **D**) определит его MAC-адрес – **MAC(D)**.
3. Транспортный кадр будет отправлен станцией **A** в свой сегмент сети для станции **D**, интерфейс которой его получит, извлечет IP-пакет и будет принимать решение по вопросу его дальнейшей обработки.
4. По IP-адресу назначения шлюз **D** определит, что IP-пакет на самом деле предназначен не для него, а для станции с адресом **IP(E)**. Поскольку станция **E** находится в одном сегменте сети со шлюзом **D**, то шлюз отправит этот транзитный IP-пакет станции **E** с использованием *прямой* адресации.

Схему работы механизма косвенной адресации поясняют приведенные ниже на Рис. А.8 рисунок и таблицы. Отличительной чертой косвенной адресации является то, что в исходной точке отправки формирование MAC-адреса получателя транспортного кадра выполняется не по IP-адресу станции назначения, а по IP-адресу *шлюза*.



Адрес	Отправитель	Получатель
IP-заголовок	IP(A)	IP(E)
MAC-заголовок	MAC(A)	MAC(D)

→

Отправитель	Получатель
IP(A)	IP(E)
MAC(D)	MAC(E)

Рис. А.8 Схема работы механизма косвенной адресации

Устройство таблицы маршрутизации

Как было сказано выше, каждому узлу сети приходится решать задачу *маршрутизации* – определения сетевого интерфейса дальнейшей доставки IP-пакета по содержащемуся в его заголовке IP-адресу назначения. Никакой функциональной связи между IP-адресами и интерфейсами конкретного маршрутизатора нет, поэтому единственной формой описания соответствия между множеством IP-адресов и множеством сетевых интерфейсов является таблица, называемая *таблицей маршрутизации*.

Устройство таблицы маршрутизации рассмотрим на примере приведенной ниже схемы на Рис. А.9. Пусть имеется некоторый маршрутизатор с двумя сетевыми интерфейсами: **`Lan1`** и **`Lan2`**. Интерфейс **`Lan1`** включен в сеть с адресом **`192.168.1.0`** и маской сети **`255.255.255.0`**. Интерфейс **`Lan2`** включен в сеть с адресом **`192.168.2.0`** и маской **`255.255.255.0`**. К этой же сети подключен внешний маршрутизатор, имеющий адрес **`192.168.2.254`** и обеспечивающий доступ по каналу связи в сеть Internet.

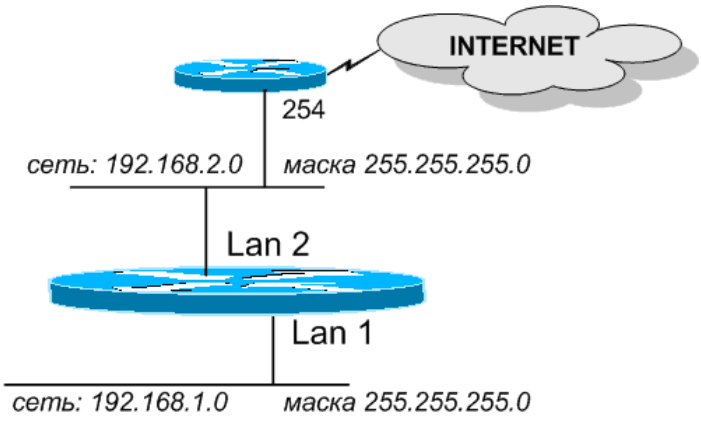


Рис. А.9 Пример схемы, поясняющей устройство традиционной рабочей таблицы маршрутизации

Для нормальной работы рассматриваемого маршрутизатора в него должна быть загружена следующая таблица маршрутизации.

Адрес	Маска	Шлюз	Интерфейс	Метрика
192.168.1.0	255.255.255.0	0.0.0.0	Lan1	0
192.168.2.0	255.255.255.0	0.0.0.0	Lan2	0
0.0.0.0	0.0.0.0	192.168.2.254	Lan2	0

Каждая строка таблицы содержит описание одного правила маршрутизации. Каждое правило состоит из следующих полей:

- **`Адрес/Маска`** – пара полей описывает множество IP-адресов, подпадающих под действие данного правила;
- **`Шлюз`** – указывает IP-адрес шлюза, используемый для указания режима *косвенной* маршрутизации (доставки) IP-пакетов, подпадающих под действие данного правила; если в качестве адреса шлюза задано значение **`0.0.0.0`**, то данное правило используется только для режима *прямой* маршрутизации;
- **`Интерфейс`** – указывает имя интерфейса, который будет выполнять отправку IP-пакетов, подпадающих под действие данного правила;
- **`Метрика`** – задает *приоритет* использования данной записи таблицы в операциях маршрутизации; значение метрики измеряется предполагаемым количеством транзитных узлов сети, которые должен пройти IP-пакет для достижения своей конечной цели; чем короче маршрут движения IP-пакета, тем лучше; следовательно, чем меньше значение поля **`Метрика`**, тем бо́льший приоритет имеет данная запись маршрутной таблицы.

Используется таблица маршрутизации следующим образом.

1. Из заголовка каждого IP-пакета извлекается IP-адрес назначения.
2. С помощью полей **`Адрес`** и **`Маска`** отыскивается строка таблицы маршрутизации, соответствующая IP-адресу назначения. Поиск строк производится по наиболее точному совпадению IP-адреса назначения. То есть сначала ищутся записи, совпадающие с IP-адресом назначения по всем 32 битам (по маске 255.255.255.255), затем – по 31 биту (по маске 255.255.255.254) и так далее.
3. Если найдено несколько подходящих записей маршрутной таблицы, то берется запись с наименьшим значением поля **`Метрика`**.

4. Из найденной записи извлекается имя интерфейса, которому IP-пакет передается на отправку. В зависимости от значения поля **шлюз** интерфейс выполняет отправку по алгоритму *прямой* или *косвенной* маршрутизации.
5. Если подходящей записи в маршрутной таблице нет, то IP-пакет снимается с дальнейшей доставки (сбрасывается).

В маршрутной таблице каждого маршрутизатора может присутствовать запись с *нулевым* значением полей **Адрес** и **Маска**. Такая запись имеет специальное название – *маршрут по умолчанию* (`default`-маршрут). В соответствии с `default`-маршрутом отправляются те IP-пакеты, для которых нет подходящей обычной маршрутной записи. При наличии `default`-маршрута ситуация, когда «`подходящей записи в маршрутной таблице нет`», исключается. В маршрутной таблице может быть несколько `default`-маршрутов, имеющих разные значения параметра **Маска**.

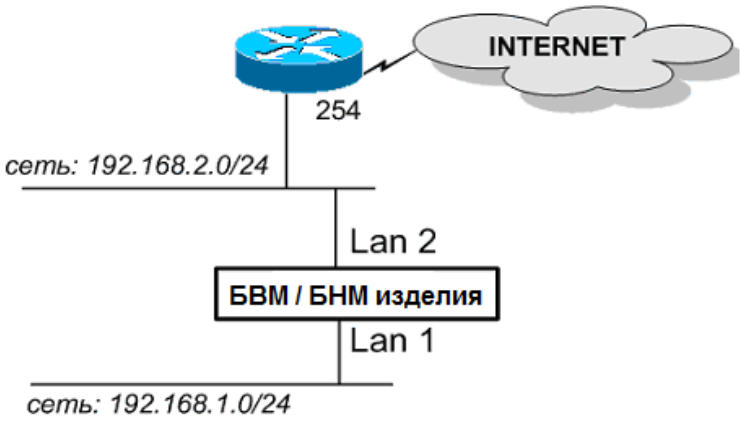
Таблица маршрутизации изделия

Представление информации в таблицах маршрутизации, используемых маршрутизаторами изделий защиты, несколько отличается от традиционного: вместо громоздкого в представлении понятия **Маска** используется аналогичное по смыслу, но компактное в представлении понятие **Количество значащих бит**, которое означает, какое количество *старших* бит IP-адреса используется для указания *номера сети*. При настройке изделий количество значащих бит записывается непосредственно в поле **Адрес** через косую черту вслед за IP-адресом. С учетом этого отличия приведенная выше таблица маршрутизации, не изменяя смыслового содержания, будет выглядеть следующим образом.

Адрес	Шлюз	Интерфейс	Метрика
192.168.1.0/24	0.0.0.0	Lan1	0
192.168.2.0/24	0.0.0.0	Lan2	0
0.0.0.0/00	192.168.2.254	Lan2	0

Рабочая таблица маршрутизации в изделии автоматически создается в момент запуска изделия при инициализации работы сетевых интерфейсов и формируется как простая совокупность (суперпозиция) маршрутных таблиц, заданных в конфигурации каждого из сетевых интерфейсов соответствующего блока маршрутизации. Это обстоятельство приводит к необходимости еще одной трансформации традиционной таблицы маршрутизации. В блоках маршрутизации вместо единой таблицы, содержащей столбец **Интерфейс**, пользуются отдельными для каждого интерфейса таблицами маршрутов.

Ниже на Рис. А.10 приведен рассмотренный ранее пример схемы (Рис. А.9), но применительно к БВМ или БНМ изделия.



Lan1

Адрес	Шлюз	Метрика
192.168.1.0/24	0.0.0.0	0

Lan2

Адрес	Шлюз	Метрика
192.168.2.0/24	0.0.0.0	0
0.0.0.0	192.168.2.254	0

Рис. А.10 Пример схемы, поясняющей устройство таблицы маршрутизации, применяемой в изделиях

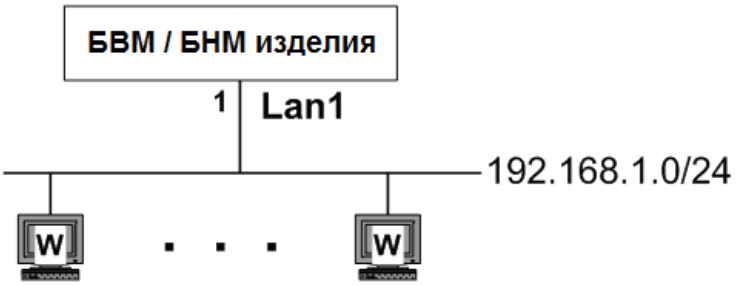
Приведенные в составе рисунка Рис. А.10 таблицы маршрутизации изделий защиты в смысловом содержании адекватны традиционным таблицам маршрутизации, приведенным под схемой на Рис. А.9, и отличаются только компактностью и удобством формы представления.

Примеры формирования маршрутных таблиц интерфейсов изделия

Ниже приведен ряд примеров формирования маршрутных таблиц интерфейсов блоков маршрутизации изделий для различных схем включения изделия в состав ЗСПД. При формировании маршрутных таблиц использованы следующие правила.

1. Для сетевых Ethernet-интерфейсов первым обязательно должен быть указан *прямой* маршрут, содержащий адрес локальной сети, к которой непосредственно подключен интерфейс. В качестве значения поля **Шлюз** такого маршрута должно быть задано значение **0.0.0.0**.
2. При указании *косвенных* маршрутов адреса шлюзов должны быть выбраны только из множества IP-адресов, имеющих прямую маршрутизацию через данный интерфейс.
3. Для двухточечных интерфейсов (PPP, SLIP, CSLIP) косвенная маршрутизация не используется, поэтому поле **Шлюз** для всех маршрутов таких интерфейсов должно иметь значение **0.0.0.0**.

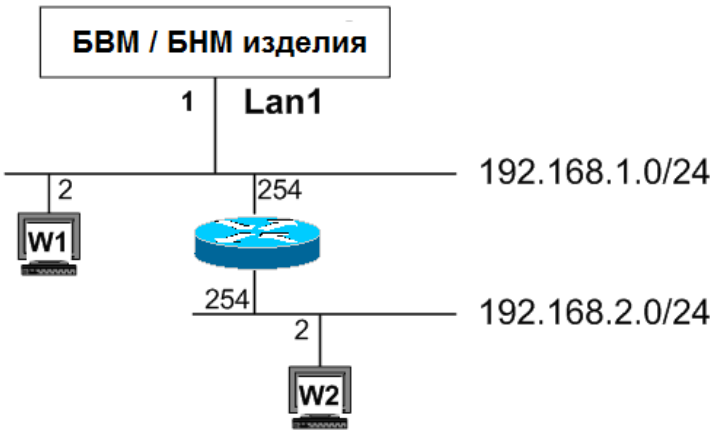
Прямая маршрутизация



	Адрес	Шлюз	Метрика
Lan1	192.168.1.0/24	0.0.0.0	0

Рис. А.11 Пример настройки схемы обмена с прямой маршрутизацией IP-датаграмм

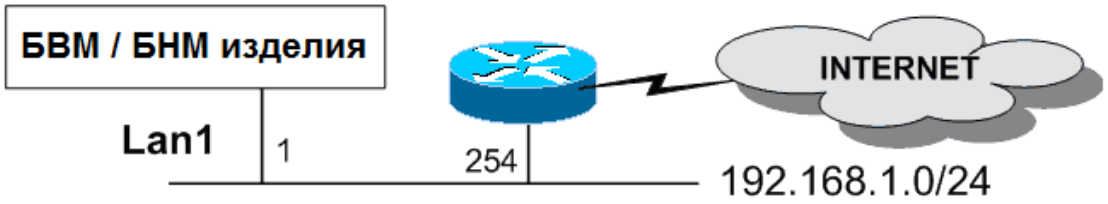
Косвенная маршрутизация



	Адрес	Шлюз	Метрика
Lan1	192.168.1.0/24	0.0.0.0	0
	192.168.2.0/24	192.168.1.254	0

Рис. А.12 Пример настройки схемы обмена с косвенной маршрутизацией IP-датаграмм

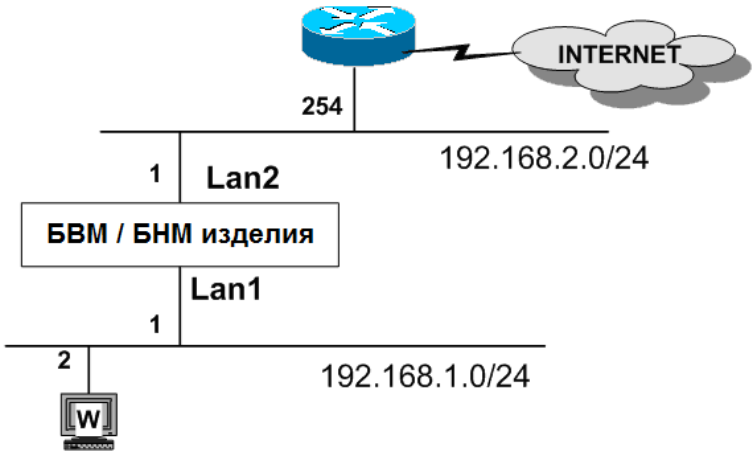
Работа с внешним маршрутизатором



	Адрес	Шлюз	Метрика
Lan1	192.168.1.0/24	0.0.0.0	0
	0.0.0.0	192.168.1.254	0

Рис. А.13 Пример настройки схемы обмена с внешним маршрутизатором

Работа с двумя сетями и внешним маршрутизатором



	Адрес	Шлюз	Метрика
Lan1	192.168.1.0/24	0.0.0.0	0

	Адрес	Шлюз	Метрика
Lan2	192.168.2.0/24	0.0.0.0	0
	0.0.0.0	192.168.2.254	0

Рис. А.14 Пример настройки схемы обмена с двумя сетями и внешним маршрутизатором

Приложение Б. Интерфейсы с агрегированием каналов связи

Агрегирование (объединение) каналов связи. Физическими интерфейсами изделий нового поколения поддерживается функция *агрегирования каналов связи* (`Link Aggregation`) – возможность организации обмена данными через сетевой интерфейс, связанный одновременно с несколькими Ethernet-адаптерами маршрутизатора. Делается это для того, чтобы организовать передачу *единого* потока данных не через один, а через *несколько* Ethernet-адаптеров с целью увеличения пропускной способности тракта передачи данных или для повышения надежности его работы.

В процессе настройки всех *физических* интерфейсов изделия – и Ethernet-интерфейсов (обработка потоков IP-датаграмм на L3-уровне), и L2–Eth-интерфейсов (обработка Ethernet-кадров на L2-уровне) – осуществляется привязка настраиваемого интерфейса, как минимум, к *одному* Ethernet-адаптеру маршрутизатора. Осуществляется эта привязка путем указания в настройках интерфейса значения параметра **`Номер порта`** (см. бланк настройки дополнительных параметров Ethernet-интерфейса – Рис. 2.9, с. 29 или бланк настройки дополнительных параметров физического L2–Eth-интерфейса – Рис. 2.16, с. 34, а также раздел ***Приложение Ж***, с. 253).

На Рис. Б.1 приведен пример схемы организации связи изделия с сетевым устройством по агрегированным каналам связи.

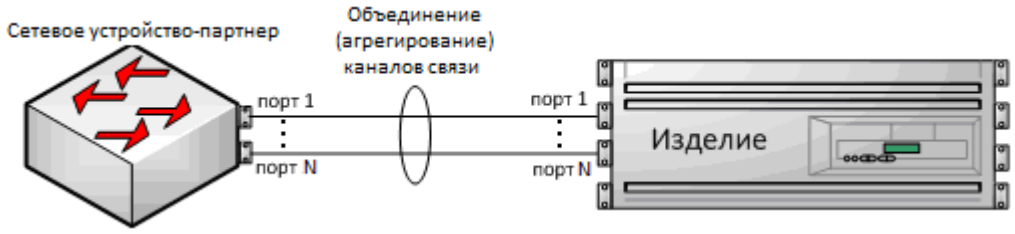


Рис. Б.1 Пример схемы организации связи изделия с сетевым устройством по агрегированным каналам связи

Процесс организации взаимодействия изделия с сетями передачи данных упрощенно можно представить в виде следующих технологических этапов:

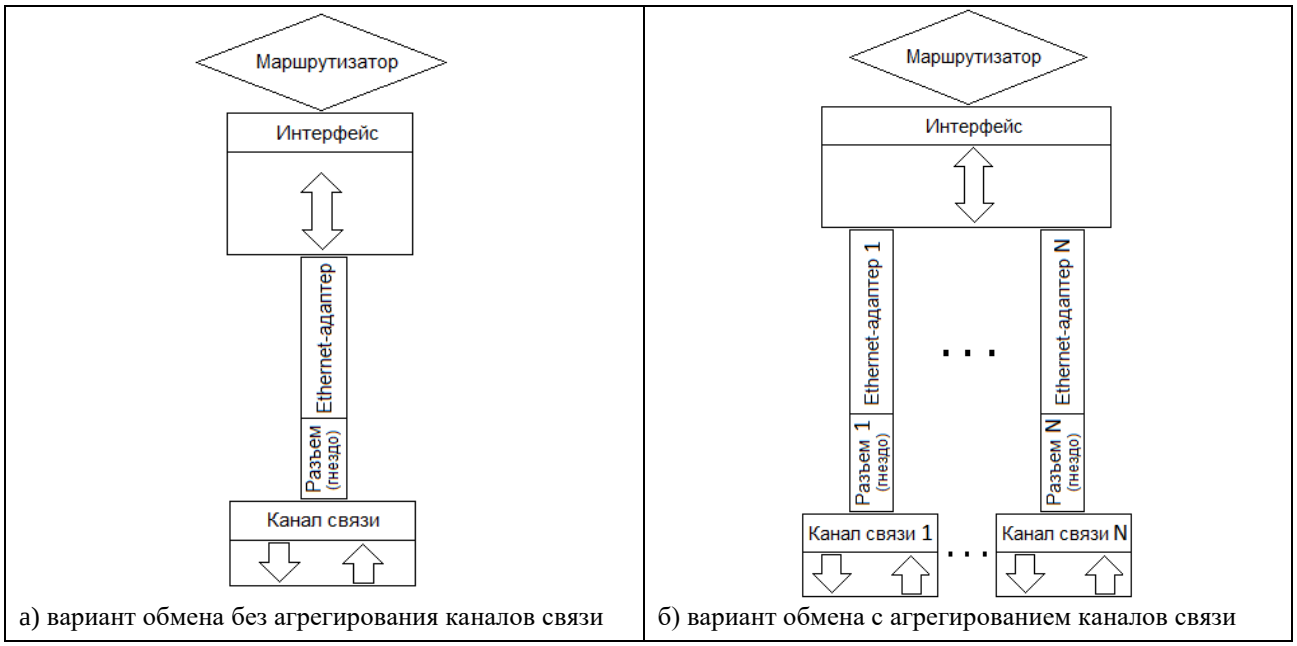
- на стадии подготовки изделия защиты к работе администратор изделия должен выполнить настройку работы тех *сетевых интерфейсов*, которые будут *задействованы* в предстоящей работе изделия (количество Ethernet-адаптеров в изделии может превышать потребности для реальной работы изделия на объекте эксплуатации; для экономии ресурсов и вычислительных мощностей изделия администратор может настраивать (задействовать) *не все* средства связи изделия);
- настройка сетевого интерфейса предполагает ввод администратором ряда значений параметров интерфейса, которые будут сохранены в составе конфигуратора изделия; одним из параметров настройки интерфейса является параметр **`Номер порта`**, определяющий конкретный Ethernet-адаптер (конкретные Ethernet-адаптеры), через который (которые) будет осуществляться весь обмен данными между изделием и каналом связи (каналами связи) по этому интерфейсу (подробнее о выборе значения параметра **`Номер порта`** см. раздел ***Приложение Ж***, с. 253);
- на стадии инициализации работы изделия программа управления его функционированием для каждого задействованного в предстоящей работе Ethernet-адаптера изделия создает *логическую* структуру – *интерфейс* – которая будет использована изделием в дальнейшей работе для обеспечения *логического* взаимодействия маршрутизатора изделия с конкретным каналом (каналами) связи; при этом собственно *физическое* взаимодействие интерфейса с каналом (каналами) связи (включая необходимый контроль формата принимаемых кадров, качества их передачи по каналу связи и пр.) осуществляется с помощью *единственного* порта Ethernet-адаптера – наиболее часто встречающийся типовой вариант функционирования сетевого интерфейса – или с помощью их *множества* – специальный вариант применения интерфейса, использующего преимущества механизма агрегирования каналов связи.

В результате выполненной работы будет установлен обмен данными между маршрутизатором и ближайшим сетевым устройством-партнером, иллюстрируемый рисунком Рис. Б.2. На нем приведены два возможных варианта организации обмена данными. Вариант *а)* иллюстрирует фрагмент тракта передачи данных, организованного с помощью единственного порта Ethernet-адаптера (без использования механизма агрегирования каналов связи). Вариант *б)* иллюстрирует фрагмент тракта передачи данных, организованного с помощью множества (более одного) портов Ethernet-адаптеров (с использованием механизма агрегирования каналов связи).

Таким образом, предварительно настроив интерфейс маршрутизатора изделия, обеспечивающий работу механизма агрегирования каналов связи, можно, соединив разъемы (гнезда) портов Ethernet-адаптеров, участвующих в работе этого интерфейса, параллельными кабелями (линиями связи) с соответствующими

разъемами (гнездами) сетевого устройства-партнера (см. Рис. Б.1 и Рис. Б.2), *зеркально* настроенного на работу по агрегированным каналам связи, получим между маршрутизатором изделия и сетевым устройством-партнером тракт для передачи *единого* потока данных повышенной пропускной способности, повышенной надежности или рассредоточенного (сбалансированного) по каналам связи, участвующим в агрегировании.

> *Примечание.* В качестве сетевого устройства-партнера может применяться ближайшее в сети аналогичное изделие защиты или ближайшее в сети сетевое устройство, работа которого может быть организована в режиме агрегирования каналов связи с применением алгоритмов агрегирования, аналогичных поддерживаемым изделием.



а) вариант обмена без агрегирования каналов связи

б) вариант обмена с агрегированием каналов связи

Рис. Б.2 Схема организации обмена данными между маршрутизатором изделия и сетевым устройством

Технологии передачи единого потока данных через интерфейсы изделия с использованием механизма агрегирования каналов связи могут применяться для достижения одного из следующих результатов:

- повышение пропускной способности тракта передачи данных (путем загрузки передаваемого через дополнительные каналы связи трафика);
- повышение надежности тракта передачи данных (путем резервирования технических средств передачи данных между передающей и принимающей сторонами – резервирования Ethernet-адаптеров, кабелей, разъемов и пр.);
- управление балансировкой трафика, передаваемого через конкретный канал связи, участвующий в агрегировании, в зависимости от характеристик передаваемых в трафике пакетов данных.

Понятно, что для получения эффекта повышения пропускной способности тракта передачи данных следует использовать алгоритмы *равномерной* загрузки всех имеющихся агрегированных каналов связи интерфейса.

Если целью применения интерфейса с агрегированием каналов связи является повышение надежности тракта передачи данных, следует применять другие алгоритмы, учитывающие следующее: первый в списке агрегированных каналов связи интерфейса объявляется *ведущим*, через него с момента начала работы интерфейса выполняется обмен трафиком до тех пор, пока на этом канале присутствует сигнал *несущей* частоты (сигнал LINK); как только работа ведущего канала связи нарушается, пропадает сигнал несущей (а это означает, что пропадание сигнала несущей – сигнала LINK – идентифицирует и сетевое устройство-партнер) и обмен трафиком переводится обеими сторонами на альтернативный канал связи.

Теория вопросов агрегирования каналов связи хорошо проработана, на практике широко применяются разнообразные методы оптимального с точки зрения различных критериев *статического* и *динамического* управления использованием интерфейсов с объединением (агрегированием) дополнительных каналов связи.

Из всего множества этих методов в изделиях нового поколения применяется несколько сравнительно простых методов, ограниченных следующими условиями:

- поддерживаются только методы *статического* управления использованием интерфейсов с агрегированием каналов связи;
- во всех применяемых методах используется только *статическое* управление использованием интерфейсов с агрегированием каналов связи

- объединяемые в интерфейсе каналы связи должны быть одинаковыми как по физической природе (среде передачи данных), так и по пропускной способности как у изделия, так и у сетевого устройства-партнера (коммутатора, маршрутизатора, аналогичного изделия защиты и пр.);
- на сетевом устройстве-партнере должны быть выполнены настройки, *зеркальные* по отношению к выполненным настройкам интерфейсов изделия с агрегированием каналов связи;
- используются *три* алгоритма управления работой интерфейсов с агрегированием каналов связи: **round-robin**, **balance-xor**, **active-backup**.

Настройка физического интерфейса на работу в режиме *объединения* (агрегирования) каналов связи выполняется при настройке значения параметра **Объединение** с помощью бланка настройки дополнительных параметров Ethernet-интерфейса (Рис. 2.9, с. 29) или бланка настройки дополнительных параметров физического L2–Eth-интерфейса (Рис. 2.16, с. 34).

Выбор алгоритма распределения для интерфейсов, работающих в режиме объединения (агрегирования) каналов связи, выполняется при настройке значения параметра **Алгоритм распределения** с помощью экрана настройки параметров механизма агрегирования каналов связи интерфейсов (см. Рис. 2.10, с. 29).

Приведенное ниже (в общих чертах) описание работы каждого из поддерживаемых изделием алгоритмов распределения трафика по агрегированным портам (каналам связи) сетевых интерфейсов изделия поможет администратору остановиться на наиболее подходящем алгоритме.

> *Примечание.* Отметим, что для принятия решения о выборе оптимального алгоритма, подходящего к конкретным условиям эксплуатации изделия, приведенного описания будет недостаточно, т.к. только администратор владеет информацией о *структуре* обрабатываемого изделием трафика, генерируемого приложениями. Различные приложения по-разному реагируют на результаты передачи трафика, получаемые с помощью разных алгоритмов распределения. Только обладая информацией о трафике, передаваемом между приложениями, администратор может отдать предпочтение тому или иному из приведенных алгоритмов.

Алгоритм ROUND-ROBIN. Алгоритм применяется в случае, когда интерфейс с агрегированием каналов связи применяется в целях повышения *пропускной способности* тракта передачи данных между изделием и сетевым устройством-партнером. Работа алгоритма направлена на обеспечение *равномерной* загрузки всех имеющихся агрегированных каналов связи интерфейса, с его помощью осуществляется *циклическая* (по кольцу) *последовательная* загрузка каждого из охваченных агрегированием каналов связи интерфейса очередной поступившей для обработки интерфейсом порции информации (Ethernet-кадра).

Допустим, что интерфейс объединяет (агрегирует) *два* порта (канала связи) маршрутизатора изделия – *основной* и *дополнительный*. *Основной* порт интерфейса указывается при настройке значения параметра **Номер порта** с помощью бланка настройки дополнительных параметров Ethernet-интерфейса – Рис. 2.9 (с. 29) или бланка настройки дополнительных параметров физического L2–Eth-интерфейса – Рис. 2.16 (с. 34). *Дополнительный* порт интерфейса указывается при настройке значения параметра **Дополнительные порты** (в нашем примере – *единственное* значение номера дополнительного порта маршрутизатора изделия) с помощью экрана настройки параметров механизма агрегирования каналов связи – Рис. 2.10, с. 29). В этом случае 1-ый поступивший на обработку интерфейсом кадр будет направлен в 1-ый порт интерфейса, 2-ой – во 2-ой порт, 3-ий – в 1-ый порт, 4-ый – во 2-ой порт, 5-ый – в 1-ый порт и т.д.

Если интерфейс будет объединять (агрегировать) *три* порта (канала связи) маршрутизатора изделия (один основной и два дополнительных), то в этом случае 1-ый поступивший кадр будет направлен в 1-ый порт интерфейса, 2-ой – во 2-ой порт, 3-ий – в 3-ий порт, 4-ый – в 1-ый порт, 5-ый – во 2-ой порт, 6-ой – в 3-ий порт, 7-ой – в 1-ый порт и т.д.

> **Примечание**. Отметим, что в последнем примере рассмотрен случай применения *трех* агрегированных портов интерфейса. Применение *нечетного* числа агрегированных портов (каналов связи) на практике встречается редко. Обычно при использовании алгоритма распределения **round-robin** практикуется применение 2-х, 4-х или 8-ми агрегированных портов.

Алгоритм **round-robin**, механически перенаправляя очередной кадр в очередной канал связи (по циклу), не учитывает характеристик поступающего на обработку трафика. При этом существует вероятность того, что пакеты, передаваемые между отправителем и получателем по параллельным каналам связи, в случае даже незначительных задержек в канале могут быть перемешаны на приемной стороне тракта. Для отдельных приложений это вполне допустимо (например, для видеоприложений). Для каких-то приложений это недопустимо (например, у приложений, использующих TCP-протокол, нарушение последовательности принимаемых IP-датаграмм приводит к *ретрансмиссии* – разрыву существующего TCP-соединения и его повторному установлению, что нарушает работу приложения в целом). Для преодоления этой ситуации более подходящим представляется алгоритм **balance-xor**, описание которого приведено ниже.

Алгоритм BALANCE-XOR. Алгоритм применяется также, как и предыдущий, для повышения *пропускной способности* тракта передачи данных между изделием и сетевым устройством-партнером.

Алгоритм обеспечивает балансировку нагрузки на агрегированные порты (каналы связи) интерфейса согласно значению *хэш-функции*, полученному в результате следующих вычислений: на первом этапе – получение результата операции XOR (сложение по модулю 2) над выбранными в соответствии с настроенными значениями параметра **Критерии распределения пакетов** (см. Рис. 2.10, с. 29) параметрами очередной порции информации, поступившей в интерфейс на обработку;

на втором этапе – получение *остатка* от деления результата вычислений на первом этапе на число агрегированных интерфейсом портов (каналов связи). Результат вычислений указывает номер порта, в который должна быть отправлена обработанная интерфейсом поступившая очередная порция информации.

Распределение пакетов между агрегированными портами (каналами связи) определяется в результате следующих вычислений:

- на первом этапе – получение результата операции XOR (сложение по модулю 2) над выбранными в соответствии с настроенными значениями параметра **Критерии распределения пакетов** (подробнее см. Рис. 2.10, с. 29) параметрами очередной порции информации, поступившей в интерфейс на обработку;
- на втором этапе – получение остатка от деления результата вычислений на первом этапе на число агрегированных интерфейсом портов (каналов связи). Результат вычислений указывает номер порта, в который должна быть отправлена обработанная интерфейсом поступившая очередная порция информации.

Алгоритм по-прежнему предназначен для параллельной загрузки разных агрегированных каналов связи интерфейса, но делать это алгоритм позволяет с учетом содержательной части пакета – его *параметров*, стремясь пакеты с похожей содержательной частью загружать в одно и то же гнездо интерфейса. Параметрами порции информации (IP-датаграммы, Ethernet-кадра) при этом являются значения, соответствующие значениям для очередной порции, выбираемым согласно выполненным ранее при настройке интерфейса установкам в ячейках таблицы **Критерии распределения пакетов**, выполненным с помощью представленного на Рис. 2.10 (с. 29) экрана настройки параметров механизма агрегирования каналов связи интерфейсов.

Строками таблицы **Критерии распределения пакетов** являются строки **Source** (Отправитель) и **Destination** (Получатель), а столбцами – столбцы **MAC**, **IP** и **Port** (номер сервиса на L4-уровне модели OSI). Таким образом, в качестве *критериев*, учитываемых при вычислении значения хэш-функции, могут быть заданы 6 следующих параметров: *MAC-адреса* отправителя и получателя пакетов (кадров), их *IP-адреса*, а также указанные в пакетах отправителя или получателя значения *портов* обработки передаваемых данных на L4-уровне.

При вычислении хэш-функции учитывается количество агрегированных интерфейсом каналов связи. Алгоритмом выполняется *свертка* по XOR значений тех параметров пакета, которые отмечены символом «*****» (*звездочка*) в таблице **Критерии распределения пакетов** (Рис. 2.10) и берется остаток от ее деления на количество гнезд, агрегированных в интерфейсе. Результат определяет номер агрегированного в интерфейсе канала, в который следует направить пакет.

Этот алгоритм обеспечивает неизменность очередности подачи пакетов с одними и теми же параметрами в один и тот же канал связи (что *исключает* перемешивание пакетов на приемной стороне тракта), но не гарантирует *равномерной* сбалансированной загрузки всех агрегированных каналов связи интерфейса.

Алгоритм ACTIVE-BACKUP. Алгоритм используется в случаях, когда механизм агрегирования каналов связи применяется с целью обеспечения *резервирования* каналов связи. Работает алгоритм следующим образом: первый в списке агрегированных каналов связи интерфейса объявляется *ведущим*, через него с момента начала работы интерфейса выполняется обмен трафиком до тех пор, пока на этом канале присутствует сигнал *несущей* частоты (сигнал LINK); как только работа ведущего канала связи нарушается, пропадает сигнал несущей (а это означает, что пропадание сигнала несущей – сигнала LINK – идентифицирует и сетевое устройство-партнер) и обмен трафиком переводится обеими сторонами на альтернативный канал связи. Если и по этому альтернативному каналу связи обмен нарушается, программы управления изделия и сетевого устройства-партнера пытаются восстановить обмен по каналу связи, следующему в списке агрегированных каналов связи вслед за отказавшим. Если обмен может быть восстановлен (появился сигнал LINK) по каналу связи, ранее вышедшему из строя, обмен данными переключается на выполнение по восстановившемуся каналу связи.

> *Примечание.* Отметим еще раз, что механизм агрегирования каналов связи применяется для всех типов физических интерфейсов изделия – и для Ethernet-интерфейсов, и для L2–Eth-интерфейсов.

Приложение В. Средства организации L2-криптомостов между сегментами защищаемых ЛВС

Общие сведения

На протяжении ряда лет изделиями ООО «Фактор-ТС» поддерживается технология защищенного сетевого обмена *IP-датаграммами* между изделиями на *сетевом* уровне – технология *криптомаршрутизатора*.

Новым поколением изделий поддерживается технология защищенного сетевого обмена *Ethernet-кадрами* на *канальном* уровне – технология организации *L2-криптомостов*, обеспечивающая функционирование локального и удаленного сегментов ЛВС Пользователя как *единого сегмента ЛВС*.

Появление в составе изделия средств поддержки технологии защищенного обмена на L2-уровне не случайно, оно продиктовано растущими потребностями Пользователя на отдельных направлениях развития технологий обработки информации и телекоммуникационных технологий.

Часто при решении прикладных задач, связанных с обменом информацией через сети передачи данных, целесообразно обеспечить удаленную связь между локальным и удаленным сегментами ЛВС без применения маршрутизаторов – сетевых устройств коммутации IP-датаграмм на L3-уровне. При этом *вся* информация, генерируемая в виде Ethernet-кадров любым из сегментов ЛВС (локальным или удаленным), свободно распространяется между обоими сегментами ЛВС.

В этом случае обмен между сегментами ЛВС выполняется Ethernet-кадрами, которые могут содержать *все* типы кадров. Ни один из принятых интерфейсом из сегмента ЛВС Ethernet-кадров в случае организации обмена данными на L2-уровне не отбраковывается (в отличие от организации обмена данными на L3-уровне), а направляется на дальнейшую обработку изделием, подробности которой приведены далее в настоящем Приложении.

> *Примечание.* Напомним, что для L3-интерфейсов трафик Ethernet-кадров при его подготовке к дальнейшей обработке маршрутизатором изделия на L3-уровне подвергается последовательности следующих операций:
>
> - у принятого от ЛВС Ethernet-кадра – фрейма формата Ethernet_II (подробнее см. раздел ***Приложение А***, с. 214) – отбрасываются выполнившие свою транспортную функцию заголовки и контрольные суммы из состава фрейма L2-уровня;
> - анализируется поле **Тип данных** Ethernet-кадра: если значение поля равно ***0x0806*** (Ethernet-кадр транспортирует ARP-пакет) или ***0x0800*** (Ethernet-кадр транспортирует IP-пакет), то выполняется дальнейшая обработка Ethernet-кадра; при прочих значениях поля **Тип данных** Ethernet-кадр считается ошибочным, он бракуется, и его обработка Ethernet-интерфейсом изделия прекращается;
> - из Ethernet-кадра извлекается транспортируемый им блок информации (IP-пакет или ARP-пакет) и отправляется на маршрутизацию в маршрутизатор изделия, которому принадлежит принявший кадр Ethernet-интерфейс;
> - после маршрутизации подлежащая передаче удаленному получателю IP-датаграмма подвергается необходимым преобразованиям, упаковывается в криптотуннель, инкапсулируется в транспортную IP-датаграмму и передается в соответствующий Ethernet-интерфейс изделия для отправки в сеть; исключение составляют только IP-датаграммы, направляемые маршрутизатором через собственный *внутренний* интерфейс соответствующим службам (сервисам) маршрутизатора.
>
> Такую типовую последовательность операций выполняют обычные IP-маршрутизаторы.
>
> Особенностью обработки трафика L3-интерфейсом является то, что из всего потока информации, поступившей из сети на Ethernet-интерфейс изделия, на дальнейшую обработку попадают только IP-пакеты или ARP-пакеты. Ethernet-кадры с типом транспортируемой информации, отличной от IP или ARP, изделием игнорируются.

Технология защищенного сетевого обмена *Ethernet-кадрами*, обеспечивающая функционирование локального и удаленного сегментов ЛВС Пользователя как единого сегмента ЛВС, востребована при решении множества современных прикладных задач.

Типовым примером применения этой технологии являются технические решения, обеспечивающие Пользователю подключение ЛВС удаленных офисов к центральному офису компании. При решении этой задачи связываться с организацией работы маршрутизаторов и пр. нецелесообразно. Пожалуй, самым существенным является то, что при использовании технологии обмена на L2-уровне (без маршрутизации, выполняемой на L3-уровне) обеспечивается передача по каналам связи *всего* возможного множества Ethernet-кадров, циркулирующих в ЛВС, независимо от транспортируемого ими типа данных.

Особую актуальность техническое решение по обеспечению защищенного обмена на L2-уровне приобретает в связи с бурно развивающимся в области информационных технологий направлением создания *Центров обработки данных* и организации сетевого взаимодействия между ними.

Средства организации L2-криптомостов и принципы их работы

Для организации беспрепятственного защищенного сетевого обмена Ethernet-кадрами на L2-уровне между локальным и удаленным сегментами ЛВС – организации L2-криптомоста – изделиями поддерживается функционирование следующих технологических средств сетевого обмена на L2-уровне:

- физический интерфейс типа L2–Eth (см. раздел 2.3.2, с. 33);
- виртуальный интерфейс типа L2–VLAN (см. раздел 2.4.4, с. 46);
- виртуальный интерфейс типа L2–TNL (см. раздел 2.4.5, с. 49).

С помощью этих средств изделия приобретают дополнительную возможность организации защищенного `bridge`-соединения, устанавливаемого через IP-сеть общего пользования, и обеспечения функционирования локального и удаленного сегментов ЛВС Пользователя как единого сегмента ЛВС.

Основной принцип работы L2-криптомоста. Для организации L2-криптомоста между локальным и удаленным сегментами ЛВС на каждом из БВМ локального и удаленного изделий, подключаемых к тем сегментам ЛВС, которые будут функционировать в составе *единого* сегмента ЛВС, должен быть создан и настроен физический интерфейс типа **`L2-Eth`**.

Работа L2–Eth-интерфейса осуществляется в специальном – *неразборчивом* (`promiscuous mode`) – режиме, часто используемом *снифферами*: при этом из ЛВС Пользователя принимаются абсолютно все пришедшие на связанный с L2–Eth-интерфейсом Ethernet-адаптер «правильные» – проверенные на корректность контрольных сумм – Ethernet-кадры, с помощью которых транспортируются данные *всех типов*, и по определенному алгоритму передаются на удаленную сторону через IP-сеть общего пользования.

Для обеспечения собственно передачи принятых из ЛВС Пользователя данных на удаленную сторону на локальном и удаленном изделиях должен быть создан и настроен виртуальный интерфейс типа **`L2-TNL`** (*общий* для БВМ и БНМ, жестко связанный при настройке с соответствующим базовым физическим L2–Eth-интерфейсом через значение его параметра **`Имя L2-туннеля`** (см. раздел 2.3.2, с. 33).

Основной принцип работы тракта взаимодействия на L2-уровне изделий, на которых созданы и настроены интерфейсы типа **`L2-Eth`** и **`L2-TNL`**, иллюстрирует схема функционирования средств организации L2-криптомоста между удаленными сегментами ЛВС, представленная на Рис. В.1.

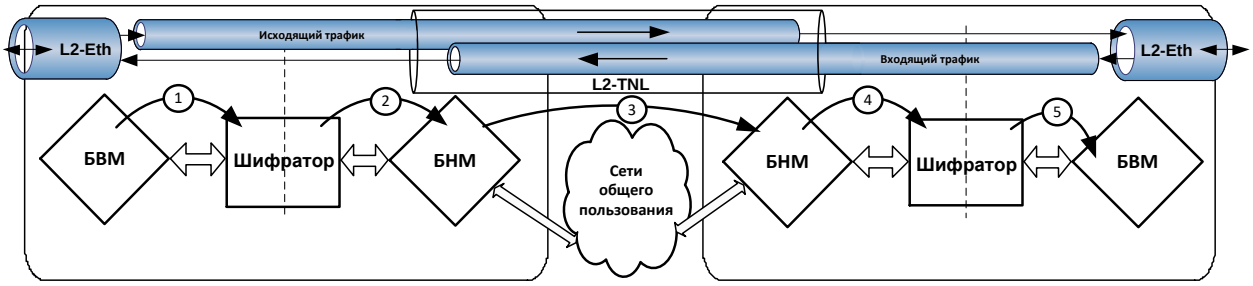


Рис. В.1 Схема функционирования средств организации L2-криптомоста между удаленными сегментами ЛВС

Все принимаемые из ЛВС Пользователя L2–Eth-интерфейсом *правильные* Ethernet-кадры без какой бы то ни было обработки перенаправляются в связанный с ним (через значение параметра **`Имя L2-туннеля`**) L2–TNL-интерфейс, который далее реализует функции криптотуннеля, работа которого по шагам подробно рассмотрена в разделе 3.1.2.1, с. 86. По криптотуннелю все поступившие в него Ethernet-кадры доставляются на удаленное изделие и далее в удаленный сегмент ЛВС Пользователя.

Попав в L2-криптотуннель, Ethernet-кадр подвергается обработке шифратором согласно параметрам L2-криптотуннеля и далее, попав в БНМ локального изделия, упаковывается (инкапсулируется) в транспортную IP-датаграмму согласно параметрам выбранного при маршрутизации блоком наружной маршрутизации Ethernet-интерфейса и с помощью этого интерфейса через IP-сети общего пользования попадает на удаленное изделие любым доступным на текущий момент времени маршрутом.

Поступив на Ethernet-интерфейс БНМ удаленного изделия в общем потоке туннелированных транспортных IP-датаграмм, инкапсулированный в IP-датаграмму зашифрованный Ethernet-кадр будет принят интерфейсом БНМ удаленного изделия. Далее он будет расшифрован и передан на БВМ удаленного изделия, где Ethernet-кадр подлежит извлечению из L2-криптотуннеля, перенаправлению в связанный с L2-криптотуннелем (через значение параметра **`Имя L2-туннеля`**) соответствующий L2–Eth-интерфейс БВМ удаленного изделия, который передаст исходный Ethernet-кадр локального сегмента ЛВС Пользователя в удаленный сегмент ЛВС Пользователя для доставки удаленной станции-получателю.

Так реализуется *основной* принцип организации работы защищенного тракта взаимодействия между локальным и удаленным изделиями при передаче потока Ethernet-кадров на L2-уровне – принцип организации *L2-криптомоста*.

Принцип работы L2-криптомостов с применением VLAN-технологии. Рассмотренная выше схема (Рис. В.1) иллюстрирует работу одного L2–TNL-интерфейса, демонстрируя возможность организации одного L2-криптомоста между локальным и удаленным сегментами ЛВС Пользователя. С помощью цепочки: L2–Eth-интерфейс (локальное изделие) – L2–TNL-интерфейс (криптотуннель через сети общего пользования) – L2–Eth-интерфейс (удаленное изделие) может быть организован только один защищенный тракт *точка-точка* – один L2-криптомост.

В случае необходимости *разделения* потока Ethernet-кадров, входящего на L2–Eth-интерфейс локального изделия, на *несколько* исходящих защищенных потоков инструментария, включающего интерфейсы только типа **L2-Eth** и **L2-TNL**, недостаточно, поскольку с L2–Eth-интерфейсом может быть связан только один L2–TNL-интерфейс, а это означает, что для L2–Eth-интерфейса может быть образован L2-криптомост только в *одном* направлении.

Для организации, скажем, еще одного L2-криптомоста потребовалось бы задействовать дополнительно L2–Eth-интерфейсы с портами их Ethernet-адаптеров изделий как на передающей, так и на приемной стороне, что возможно не всегда.

Решить задачу разделения поступающего на локальное изделие потока Ethernet-кадров на *несколько* исходящих защищенных потоков, адресуемых *по разным* направлениям, позволяет применение технологии VLAN, основные сведения о которой приведены в разделе 2.4.1.1, с. 36.

Воспользоваться возможностями этой технологии позволяет применение поддерживаемых изделием виртуальных интерфейсов типа **L2-VLAN**, общие сведения о которых, процедура создания и настройки которых приведены в разделе 2.4.4, с. 46.

В случае применения L2–VLAN-интерфейсов для организации функционирования L2-криптомостов технологическая цепочка обработки трафика Ethernet-кадров выглядит следующим образом: L2–Eth-интерфейс (локальное изделие) – L2–VLAN-интерфейс (локальное изделие) – L2–TNL-интерфейс (криптотуннель через сети общего пользования) – L2–Eth-интерфейс (удаленное изделие).

При настройке одним своим концом (входящим) L2–VLAN-интерфейс связывается с базовым физическим L2–Eth-интерфейсом, а другим (выходящим) – с L2–TNL-интерфейсом.

Назначение L2–VLAN-интерфейса в этой цепочке заключается в следующем. Если на вход L2–Eth-интерфейса изделия поступает поток т*егированных* Ethernet-кадров, то Ethernet-кадр с тегом соответствующего L2–VLAN-интерфейса будет извлечен из общего потока и передан на дальнейшую обработку этому L2–VLAN-интерфейсу. А тот, в свою очередь, передаст его без обработки на вход связанного с ним L2–TNL-интерфейса – в криптотуннель с заданным направлением. Таким образом, весь входящий поток тегированных Ethernet-кадров, поступивших на вход L2–Eth-интерфейса локального изделия, будет распределен и передан по разным криптотуннелям на разные удаленные изделия – веером по различным L2-криптомостам.

Логика работы L2–Eth-интерфейса локального изделия в этой технологической цепочке при *передаче* данных удаленному изделию сводится к следующему. Если на вход L2–Eth-интерфейса поступает поток т*егированных* Ethernet-кадров (поле **Тип данных** Ethernet-кадра имеет значение ***0x8100***), интерфейс определяет, связаны ли с ним при настройке интерфейсы типа **L2-VLAN**.

Если L2–VLAN-интерфейсы есть, то L2–Eth-интерфейс определяет, есть ли среди них L2–VLAN-интерфейс, значение параметра **VLAN-идентификатор** у которого (**VNID**) соответствует тегу очередного Ethernet-кадра:

- если L2–VLAN-интерфейс с таким тегом найден, то Ethernet-кадр будет передан ему на вход для дальнейшей передачи в связанный с ним L2–TNL-интерфейс, который отправит кадр по соответствующему криптотуннелю на удаленное изделие;
- если L2–VLAN-интерфейс с таким тегом не найден, то Ethernet-кадр будет передан в L2–TNL-интерфейс, связанный с базовым физическим L2–Eth-интерфейсом, для отправки кадра по соответствующему криптотуннелю на удаленное изделие.

Если L2–VLAN-интерфейсов нет, то Ethernet-кадр будет передан L2–Eth-интерфейсом в L2–TNL-интерфейс, связанный с базовым физическим L2–Eth-интерфейсом, для отправки кадра по соответствующему криптотуннелю на удаленное изделие.

При *приеме* удаленным изделием извлеченный из L2–TNL-интерфейса исходный Ethernet-кадр передается в связанный с L2–TNL-интерфейсом на удаленном изделии L2–Eth-интерфейс для доставки получателю в составе соответствующего удаленного сегмента ЛВС Пользователя.

Так реализуется принцип организации работы защищенных трактов взаимодействия между локальным и удаленными изделиями при передаче потока Ethernet-кадров на L2-уровне с применением VLAN-технологии – принцип организации *L2-криптомостов*.

Контроль работоспособности тракта передачи на L2–уровне. С помощью L2–Eth-интерфейса изделие подключается к какому-либо порту коммутатора внутренней ЛВС Пользователя. О работоспособности L2–Eth-интерфейса коммутатор судит по наличию сигнала т. н. *несущей* – наличию сигнала несущей частоты или, как принято говорить, наличию сигнала LINK в сетевом кабеле, соединяющем порт коммутатора и соответствующий порт Ethernet-адаптера БВМ изделия, который использует L2–Eth-интерфейс.

Если коммутатор, L2–Eth-интерфейс и соединяющий их кабель исправны, то сигнал несущей (сигнал LINK) всегда присутствует, и потому коммутатор считает, что тракт обмена данными через L2–Eth-интерфейс исправен, и будет отправлять в этот тракт адресуемый интерфейсу трафик.

Но тракт передачи данных от отправителя информации в локальном сегменте ЛВС Пользователя до ее получателя в удаленном сегменте ЛВС представляет собой, как правило, длинную многозвенную цепочку. Каждое из ее звеньев может выйти из строя, нарушив работу всего тракта. При этом коммутатор, определяя наличие сигнала LINK в сетевом кабеле, соединяющем его с L2–Eth-интерфейсом изделия, и потому считая, что тракт исправен, будет продолжать отправлять в него адресуемый интерфейсу трафик.

Для устранения этой нежелательной ситуации введено понятие *ведущего интерфейса*, указываемого при настройке L2–Eth-интерфейса (см. раздел 2.3.2, Рис. 2.15, с. 33, параметр **`Ведущий интерфейс`**).

В качестве *ведущего* администратор может указать любой сетевой интерфейс изделия. При пропадании сигнала LINK на ведущем интерфейсе программа управления принудительно погасит сигнал LINK на связанном с ним L2–Eth-интерфейсе. При пропадании сигнала LINK у L2–Eth-интерфейса коммутатор в локальном сегменте ЛВС Пользователя прекратит передачу трафика по вышедшему из строя тракту и продолжит обмен с изделием защиты по резервному тракту (при его наличии). При обнаружении восстановления сигнала LINK у ведущего интерфейса программой управления будет поднят сигнал LINK и у связанного с ведущим L2–Eth-интерфейса. Коммутатор, определив, что работоспособность L2–Eth-интерфейса восстановлена, вернется к работе с изделием по основному тракту.

Если в качестве ведущего интерфейса для L2–Eth-интерфейса указать соответствующий ему L2–TNL-интерфейс и на этом туннельном интерфейсе включить механизм автоматического контроля его готовности с помощью механизма KEEPALIVE (см. раздел 2.4.2, с. 39, Рис. 2.25), то в случае идентификации состояния неготовности L2–TNL-интерфейса программой управления автоматически будет установлен в состояние неготовности и L2–Eth-интерфейс – будет принудительно погашен сигнал LINK на его порту.

Целесообразно указывать работающий в режиме самоконтроля L2–TNL-интерфейс в качестве ведущего для связанного с ним L2–Eth-интерфейса, т.к. при этом с помощью отправляемых локальным изделием по L2-туннелю зондирующих запросов будет регулярно проверяться состояние готовности всего тракта передачи данных с удаленной стороной.

Особенно актуально применение описанного выше механизма контроля работоспособности тракта передачи данных в случаях, когда имеет место взаимодействие между сетевыми устройствами по *дублируемым* каналам связи.

Поддержка L2–Eth-интерфейсом частичного обмена IP-датаграммами на L3 уровне. Настраивая L2–Eth-интерфейс, можно его основные функции поддержки обмена *Ethernet-кадрами* на L2 уровне опционально дополнить функцией *частичной* поддержки обмена *IP-датаграммами* на L3 уровне.

Если, организовав с помощью L2-интерфейсов защищенный обмен данными на L2-уровне, ограничиться поддержкой L2–Eth-интерфейсом только его *основной* функции – обеспечения обмена *Ethernet-кадрами* на L2-уровне, то можно потерять возможность использования и применения некоторых полезных инструментов и функций, обеспечиваемых интерфейсами изделия на L3-уровне: например, для сетевых устройств локального сегмента ЛВС будет отсутствовать возможность контроля готовности L2–Eth-интерфейса с помощью процедуры PING, будет отсутствовать возможность использования сервисов, предоставляемых службами БВМ изделия – службами DNS, DHCP, SNTP, SNMP и пр., будет отсутствовать реакция изделия на запросы согласно ARP-протоколу и т.д.

При отсутствии поддержки L2–Eth-интерфейсом обработки *IP-датаграмм* на L3-уровне для обеспечения возможности использования указанных сервисов пришлось бы на этом же направлении обмена в сети создавать дополнительный Ethernet-интерфейс БВМ изделия, обеспечивающий обработку IP-датаграмм на L3-уровне, подключать к этому интерфейсу соответствующий дополнительный сетевой кабель, задействовав на коммутаторе в локальном сегменте ЛВС дополнительный порт (гнездо) для его подключения, использовать дополнительные ресурсы БВМ изделия на работу дополнительного интерфейса.
Но даже ценой перечисленных затрат цель при таком техническом решении достигнута не будет, т.к., например, при использовании процедуры PING со стороны коммутатора мы будем тестировать состояние совсем *другого* интерфейса изделия (другого порта Ethernet-адаптера), через другой сетевой кабель, через другой порт (гнездо) коммутатора, т.е. с помощью процедуры PING будем тестировать совсем другой комплект программно-аппаратных средств сети и изделия.

Поэтому кроме основной функции по обеспечению обмена Ethernet-кадрами на L2-уровне L2–Eth-интерфейсом дополнительно поддерживается функция *частичной* поддержки обмена IP-датаграммами на L3-уровне. Частичной поддержка обмена на L3-уровне является потому, что с ее помощью нельзя выполнить удаленную маршрутизацию (т.е. нельзя пришедшие на L2–Eth-интерфейс из локального сегмента ЛВС IP-датаграммы

передать на противоположную сторону). Другими словами, обработка пришедших на L2–Eth-интерфейс IP-датаграмм заканчивается их обработкой службами (DHCP, DNS, SNTP и пр.) или сервисами (PING, ARP и т.д.) БВМ изделия.

Особенности работы физических L2- и L3-интерфейсов изделия

Представленная на Рис. В.2 схема иллюстрирует особенности работы сетевых физических интерфейсов типа **`L2-Eth`** и **`Ethernet`**, знать которые полезно при планировании применения изделий в составе ЗСПД.

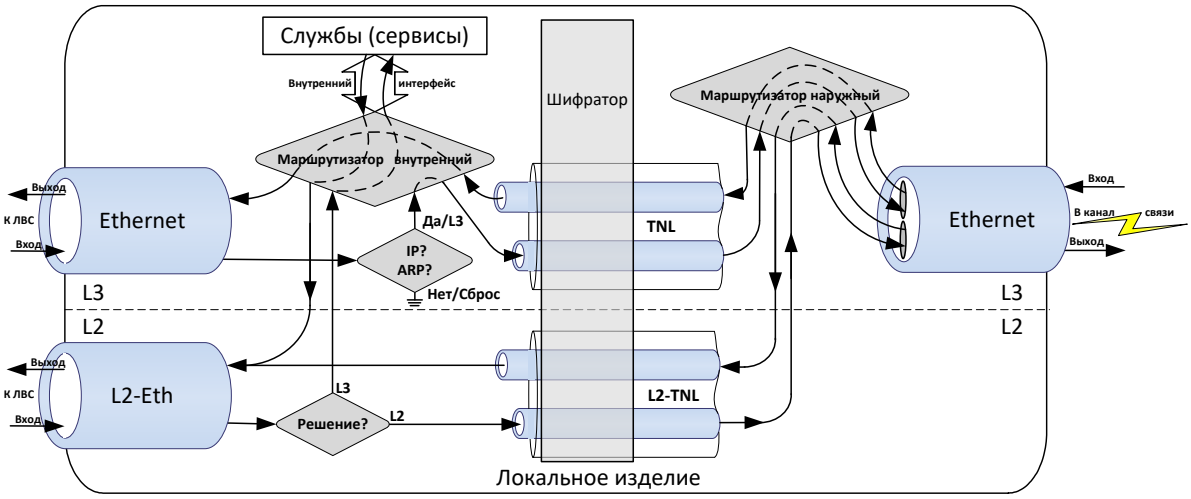


Рис. В.2 Схема обработки трафиков сетевыми физическими интерфейсами типа L2–Eth и Ethernet

L2–Eth-интерфейс. При настройке L2–Eth-интерфейса может быть включена функция *частичной* поддержки обмена IP-датаграммами на L3-уровне (см. раздел 2.3.2, с. 33), работу которой поясняет схема на Рис. В.2.

> *Примечание.* Напомним, что заголовок Ethernet-кадра содержит поле **`Тип данных`**, содержимое которого определяет *тип* транспортируемых этим Ethernet-кадром инкапсулируемых в кадр данных. Если поле **`Тип данных`** содержит значение ***`0x0806`***, то Ethernet-кадр транспортирует данные, обрабатываемые с помощью ARP-протокола. Если поле **`Тип данных`** содержит значение ***`0x0800`***, то Ethernet-кадр транспортирует данные, обрабатываемые с помощью IP-протокола – IP-датаграммы.

Принимаемый L2–Eth-интерфейсом из защищаемой ЛВС Пользователя входящий трафик Ethernet-кадров проверяется интерфейсом на корректность формата и отсутствие искажений при передаче по каналу ЛВС.

Далее программой управления работой L2–Eth-интерфейса принимается *решение* (см. Рис. В.2) о дальнейшем использовании принятого Ethernet-кадра:

1. Если **`MAC-адрес получателя`** (см. раздел 2.4.1, с. 36) у принятого Ethernet-кадра представляет собой специальный *широковещательный* адрес (MAC-адрес равен значению: **`ff:ff:ff:ff:ff:ff`**), то:
   - если Ethernet-кадр не транспортирует пакет, обрабатываемый с помощью ARP-протокола (поле Тип данных не содержит значение 0x0806), Ethernet-кадр направляется в связанный с L2–Eth-интерфейсом соответствующий L2–TNL-интерфейс и обработка кадра продолжается на L2-уровне;
   - если Ethernet-кадр транспортирует пакет, обрабатываемый с помощью ARP-протокола (поле Тип данных содержит значение 0x0806), то:
     - если **`MAC-адрес получателя`** принятого Ethernet-кадра не совпадает с MAC-адресом L2–Eth-интерфейса (т.е. имеет место случай транзита кадра), Ethernet-кадр направляется в связанный с L2–Eth-интерфейсом соответствующий L2–TNL-интерфейс и обработка кадра продолжается на L2-уровне;
     - если **`MAC-адрес получателя`** принятого Ethernet-кадра совпадает с MAC-адресом L2–Eth-интерфейса (т.е. имеет место случай, когда кадр уже *доставлен* по сети получателю), то транспортируемый Ethernet-кадром ARP-запрос извлекаются из него и направляются на обработку блоком внутренней маршрутизации (БВМ) изделия на L3-уровне; БВМ через *внутренний* интерфейс маршрутизатора отправляет ARP-запрос на обработку собственным сервисам; результаты обработки (например, пакеты **`Eho-replay`** в ответ на запросы **`Eho-request`**) маршрутизируются БВМ назад в тот L2–Eth-интерфейс, по которому пришел запрос на обслуживание.
2. Если MAC-адрес получателя принятого Ethernet-кадра не представляет собой unicast-адрес, то:

- если MAC-адрес получателя принятого Ethernet-кадра не совпадает с MAC-адресом L2–Eth-интерфейса (т.е. имеет место случай транзита кадра), Ethernet-кадр направляется в связанный с L2–Eth-интерфейсом соответствующий L2–TNL-интерфейс и обработка кадра продолжается на L2-уровне;
- если MAC-адрес получателя принятого Ethernet-кадра совпадает с MAC-адресом L2–Eth-интерфейса (т.е. кадр доставлен по сети получателю), содержимое Ethernet-кадра извлекаются из него и направляются на обработку блоком внутренней маршрутизации (БВМ) изделия на L3-уровне.

3. Если MAC-адрес получателя принятого Ethernet-кадра представляет собой unicast-адрес, то:
   - если MAC-адрес получателя принятого Ethernet-кадра не совпадает с MAC-адресом L2–Eth-интерфейса (т.е. имеет место случай транзита кадра), Ethernet-кадр направляется в связанный с L2–Eth-интерфейсом соответствующий L2–TNL-интерфейс и обработка кадра продолжается на L2-уровне;
   - если MAC-адрес получателя принятого Ethernet-кадра совпадает с MAC-адресом L2–Eth-интерфейса (т.е. кадр доставлен по сети получателю), содержимое Ethernet-кадра извлекаются из него и направляются на обработку блоком внутренней маршрутизации (БВМ) изделия на L3-уровне.

Попавшие из принятого L2–Eth-интерфейсом на обработку L3-уровнем извлеченные из Ethernet-кадров IP-датаграммы попадают в БВМ изделия, который через *внутренний* интерфейс маршрутизатора отправляет их на обработку собственным службам или сервисам. Результаты обработки (например, пакеты **`Eho-replay`** в ответ на запросы **`Eho-request`**) маршрутизируются БВМ назад в тот L2–Eth-интерфейс, по которому пришел запрос на обслуживание. L2–Eth-интерфейс инкапсулирует сформированные службами (сервисами) ответные IP-датаграммы в соответствующие Ethernet-кадры и передает в ЛВС Пользователя для рабочей станции-получателя, выдавшей запрос на обслуживание. Подчеркнем, что эта ветвь алгоритма обработки работает только в том случае, когда включена частичная поддержка L2–Eth-интерфейсом обмена IP-датаграммами на L3-уровне. Частичной поддержка обработки на L3-уровне L2–Eth-интерфейсом является потому, что IP-датаграммы, пришедшие на обработку из этого интерфейса, не могут быть переданы (промаршрутизированы) на удаленную сторону, поддержка L3-уровня ограничивается обработкой IP-датаграмм службами или сервисами БВМ изделия.

Таким образом, в силу того, что L2–Eth-интерфейс может поддерживать частичный обмен IP-датаграммами на L3-уровне, абонентам ЛВС Пользователя на L2-уровне становятся доступны возможности, предоставляемые службами и сервисами БВМ изделия.

Каждый из Ethernet-кадров, поступивший из ЛВС Пользователя на L2–Eth-интерфейс и направленный программой управления в связанный при настройке с данным L2–Eth-интерфейсом L2–TNL-интерфейс подвергается стандартным для криптотуннелей описанным ранее преобразованиям в шифраторе изделия. Далее он поступает на БНМ изделия, где маршрутизируется в нужный Ethernet-интерфейс, упаковывается в транспортную IP-датаграмму и отправляется адресату через сеть общего пользования.

> *Примечание.* Приведенный порядок обработки трафика L2–Eth-интерфейсом справедлив для одиночных Ethernet-кадров. При реализации алгоритма *аппаратного* фрагментирования-слияния Ethernet-кадров картина выглядит несколько иначе, но общий порядок обработки трафика сохраняется.

Ethernet-интерфейс. Ethernet-интерфейсы изделия обеспечивают полнофункциональную обработку *IP-датаграмм* на L3-уровне, порядок которой поясняет схема на Рис. В.2.

Принимаемый Ethernet-интерфейсом из защищаемой ЛВС Пользователя трафик Ethernet-кадров проверяется интерфейсом на корректность формата и отсутствие искажений при передаче по каналу ЛВС. У принятых интерфейсом прошедших контроль Ethernet-кадров отбрасываются выполнившие свою транспортную функцию заголовки и контрольные суммы из состава фрейма L2-уровня.

Далее анализируется поле **`Тип данных`** Ethernet-кадра: если значение поля равно ***`0x0806`*** (Ethernet-кадр транспортирует ARP-пакет) или ***`0x0800`*** (Ethernet-кадр транспортирует IP-пакет), то выполняется дальнейшая обработка Ethernet-кадра; при прочих значениях поля **`Тип данных`** Ethernet-кадр считается ошибочным, он бракуется и его обработка Ethernet-интерфейсом изделия прекращается.

Если Ethernet-кадр транспортирует IP-пакет или ARP-пакет, пакет извлекается из выполнившего транспортную функцию Ethernet-кадра и отправляется на маршрутизацию в маршрутизатор изделия, к которому относится принявший кадр Ethernet-интерфейс (на схеме Рис. В.2 – БВМ). ARP-пакет через внутренний интерфейс соответствующего маршрутизатора попадает на обработку соответствующим сервисом маршрутизатора.

После маршрутизации подлежащая передаче удаленному получателю IP-датаграмма, подвергаясь необходимым преобразованиям шифратором, упаковывается в криптотуннель, инкапсулируется в транспортную IP-датаграмму и передается в соответствующий Ethernet-интерфейс маршрутизатора изделия для отправки в сеть. Исключение составляют только IP-датаграммы, перенаправляемые маршрутизатором через собственный *внутренний* интерфейс соответствующим службам (сервисам) маршрутизатора.

Таким образом, особенностью обработки IP-датаграмм является то, что из всего потока информации, поступившей из сети на Ethernet-интерфейс изделия, на обработку маршрутизатором, выполняемую на L3-уровне, попадают только IP-пакеты или ARP-пакеты. Ethernet-кадры, поступившие на вход физического

Ethernet-интерфейса изделия, транспортирующие информацию, не являющуюся датаграммой, обрабатываемой протоколами IP или ARP, изделием игнорируются.

Фрагментирование-слияние Ethernet-кадров при обмене на L2-уровне. При обработке трафика, поступающего на вход сетевых физических интерфейсов изделия, работающих по технологии Ethernet, необходимо учитывать следующее:

- на обработку и коротких, и длинных Ethernet-кадров, поступающих из сети, изделием затрачивается примерно одинаковое время, поэтому при обработке трафика коротких Ethernet-кадров *эффективная* пропускная способность интерфейсов изделия заметно снижается;
- работающие по технологии Ethernet сетевых физические интерфейсы изделия не могут работать ни на прием, ни на передачу с Ethernet-кадрами, длина которых превышает 2 Кбайта.

При этом Пользователю необходимы характеристики изделия, обеспечивающие при обмене на L2-уровне высокую эффективную пропускную способность как при обработке длинных, так и при обработке коротких Ethernet-кадров. Кроме того, изделия должны обрабатывать *джамбо*-фреймы (jumbo frame) – Ethernet-кадры, длина которых существенно превышает определяемые ограничениями Ethernet-технологии пороговые 2 Кбайта.

Указанные требования обработки трафика Ethernet-кадров могут быть обеспечены изделием в двух вариантах – на *программном* и на *аппаратном* уровнях.

На программном уровне принятое из сети L2–Eth-интерфейсом множество коротких Ethernet-кадров, прежде чем быть переданными в тракт дальнейшей обработки изделием (зашифрование, маршрутизация, инкапсуляция и пр.), упаковываются в один, называемый *контейнером*. Далее контейнер обрабатывается локальным изделием как один Ethernet-кадр, через сети общего пользования передается на удаленное изделие, где проходит необходимую обработку, распаковывается, и из него извлекается множество исходных коротких Ethernet-кадров, которые передаются получателям в ЛВС Пользователя. В результате производительность тракта передачи данных возрастает в разы.

Отметим, что на программном уровне реализуется только одна из функций алгоритма – *слияние*.

Для реализации алгоритма фрагментирования-слияния Ethernet-кадров на *программном* уровне следует при настройке физического L2–Eth-интерфейса (см. раздел 2.3.2, с. 33, Рис. 2.15) параметру **Слияние** (см. Рис. 2.15, с. 33) присвоить значение **ПРОГР.**

На аппаратном уровне выполняются обе функции алгоритма фрагментирования-слияния Ethernet-кадров. Причем их реализация осуществляется до передачи адаптером полученного из сети обработанного трафика в шину УВП БВМ, что дополнительно сокращает время обработки очередной порции сетевого трафика как на локальном изделии, так и на удаленном.

Аппаратурой Ethernet-адаптера выполняется следующее:

- если на вход L2–Eth-интерфейса из сети поступают короткие Ethernet-кадры, они накапливаются и упаковываются в контейнер, который по заполнении передается адаптером в шину УВП БВМ;

  Примечание. Длина Ethernet-кадра, по сравнению с которой пришедший из сети кадр считается программой управления коротким, регулируется при настройке L2–Eth-интерфейса (см. раздел 2.3.2, с. 33, Рис. 2.15).

- если на вход L2–Eth-интерфейса из сети поступает Ethernet-кадр, длина которого превышает значение установленного для интерфейса **MTU** (Maximum-Transmission-Unit) – **jumbo**-фрейм – аппаратура Ethernet-адаптера нарезает этот гигантский кадр на фрагменты, помещаемые в контейнер, длина которого не превышает значения **MTU** интерфейса, после чего контейнеры передаются на шину УВП БВМ.

Пройдя необходимые стадии обработки на локальном изделии, контейнеры, наполненные короткими Ethernet-кадрами или фрагментами **jumbo**-фреймов передаются на удаленное изделие, где в результате необходимых обратных преобразований из контейнеров будут извлечены и направлены получателям исходные короткие Ethernet-кадры или фрагменты, из которых будет восстановлен исходный **jumbo**-фрейм.

Для реализации алгоритма фрагментирования-слияния Ethernet-кадров на *аппаратном* уровне следует при настройке физического L2–Eth-интерфейса (см. раздел 2.3.2, с. 33, Рис. 2.15) параметру **Слияние** (см. Рис. 2.15, с. 33) присвоить значение **АППАР.**

Примечание. Настройка режима работы алгоритма фрагментирования-слияния Ethernet-кадров – программного или аппаратного – на локальном и удаленном изделиях, обеспечивающих функционирование L2-криптомоста, должна быть выполнена синхронно.

Управление потоком Ethernet-кадров. Изделиями поддерживается работа механизма управления потоком Ethernet-кадров, поступающих на физические интерфейсы изделий. Работа механизма сводится к регулированию интенсивности генерации потока Ethernet-кадров передающей стороной в случае, когда принимающая сторона не справляется с обработкой поступающего из сети потока.

Используя параметр **Управление потоком** бланков настройки дополнительных параметров физических интерфейсов (см. раздел 2.3.1, Рис. 2.9, с. 29 или раздел 2.3.2, Рис. 2.16, с. 34), можно включить или выключить работу механизма управления потоком. Включенный механизм обеспечивает *двухстороннее* управление

потоком Ethernet-кадров: изделие сообщает в сеть как о своей перегруженности по *приему*, так и реагирует на сигналы о перегруженности из сети при *передаче* трафика.

Собственно функционирование механизма управления потоком реализуется аппаратными средствами Ethernet-адаптера соответствующего физического интерфейса изделия, программа управления лишь подает команды на включение или выключение работы этого механизма. При включенном механизме в случае, когда изделие, принимая трафик, не справляется с обработкой поступающего из сети потока, Ethernet-адаптером его физического интерфейса отправляется в сеть широковещательный Ethernet-кадр, содержащий сигнал о необходимости приостановки передачи трафика в свой адрес на определенное время. Этот сигнал принимается всеми устройствами сети, включая то устройство, которое корректирует (снижает) интенсивность передаваемого им трафика на указанный в сигнале период времени. Таким образом осуществляется регулирование интенсивности потока Ethernet-кадров между устройствами сети в условиях дефицита пропускной способности.

L3-уровень. Для организации работы механизма управления потоком при обмене на L3-уровне следует для Ethernet-интерфейса включить работу механизма, установив значение **ДА** для дополнительного параметра **Управление потоком** (см. раздел 2.3.1, Рис. 2.9, с. 29).

L2-уровень. Для организации работы механизма управления потоком при обмене на L2-уровне следует для L2–Eth-интерфейса включить работу механизма, установив значение **ДА** для дополнительного параметра **Управление потоком**. Также следует указать пороговое значение скорости принимаемого интерфейсом трафика для дополнительного параметра **Скорость приема** (см. раздел 2.3.2, Рис. 2.16, с. 34).

При этом механизм управления потоком при обмене на L2-уровне будет работать следующим образом. Если скорость принимаемого из сети потока превышает пороговое значение, программа управления прекращает обработку принимаемых Ethernet-адаптером кадров на определенное время. Если при этом включен механизм управления потоком, то происходит процесс регулирования интенсивности потока генерируемого передающей стороной трафика, в результате чего удается избежать потерь Ethernet-кадров при обмене.

Приложение Г. Обработка IP-датаграмм с учетом их приоритета

Общие сведения

Качество обслуживания в сетях (QoS). В настоящее время наряду с постоянным наращиванием скоростей передачи данных как у пользователей СПД вообще, так и у пользователей ЗСПД в частности наблюдается ускорение роста потребности в услугах *мультисервисных сетей* – универсальной многоцелевой среды *одновременной* передачи речи, изображения и данных с использованием IP-технологий, что подразумевает увеличение доли пульсирующего *интерактивного* (с обратной связью) трафика и трафика *реального времени*, порой крайне чувствительных к параметрам среды транспортировки. Поэтому задача обеспечения сквозного (на протяжении всего маршрута) *качества обслуживания* (**`Quality of Service`** или **`QoS`**) трафика в таких сетях становится все более актуальной.

Понятие качества обслуживания в IP-сетях (QoS) в целом – это комплекс самого разнообразного и широкого набора понятий, параметров, механизмов, технологий, алгоритмов и пр., многие из которых являются предметом отдельных математических дисциплин, таких как теория вероятностей, теория массового обслуживания, теория очередей.

Из широкого круга механизмов и алгоритмов, имеющих отношение к понятию QoS, изделиями, исполненными в двухсегментной архитектуре технологии DioNIS®, поддерживаются механизмы и алгоритмы, обеспечивающие обработку проходящего через изделие трафика IP-датаграмм с учетом их *приоритета* – приоритетную обработку.

Подходы к управлению перегрузками трафика в сетях. Перегрузка трафика в сетях передачи данных возникает в случае переполнения выходных буферов интерфейса сетевого устройства, передающего трафик. Основными причинами возникновения перегрузок является объединение (агрегирование) трафиков, когда общая скорость входящего в устройство трафика превышает скорость обработки исходящего, а также несогласованность скоростей на интерфейсах. Управление пропускной способностью устройства в случае возникновения перегрузок осуществляется с помощью *механизма очередей*, когда поступающие на обработку в устройство данные помещаются в очереди, которые упорядоченно обрабатываются по определенному алгоритму.

По существу, управление перегрузками трафика – это установление порядка, в котором данные выбираются из очереди интерфейса на основе *приоритета* данных. Если нет перегрузок, очереди не работают – в них просто нет необходимости.

Чтобы данные, передаваемые по сети, обрабатывались с учетом их приоритета сетевыми устройствами, встречающимися на протяжении их сквозного маршрута движения от отправителя к получателю, эти данные должны нести в себе сведения о своем приоритете. Далеко не все источники, генерирующие сетевой трафик, наделяют его сведениями о приоритете обработки.

Только после полной идентификации трафика – *классификации* и его *маркировки* – к нему можно применять QoS-правила (`policies`). Для применения любого из правил QoS следует, прежде всего, трафик, предъявляющий особые требования к своей обработке, *промаркировать* каким-либо способом, отнеся таким образом соответствующие передаваемые по сети данные (пакеты, фреймы) к какому-либо *классу*. Причем сделать это следует как можно ближе к источнику генерации трафика.

Инструмент классификации *помечает* IP-датаграмму или Ethernet-кадр (фрейм) определенным значением. Эти значения меток позволяют разграничить общий поток данных на разные типы трафика и применить затем к этим типам разные правила обработки в случае, если пропускная способность транзитного сетевого устройства недостаточна, возникает *перегрузка* и для сглаживания пульсирующей пиковой нагрузки необходимо пропустить трафик через систему буферирующих *очередей* этого устройства.

Механизмы *классификации* и *маркировки* потоков данных в IP-технологиях различными производителями сетевых устройств нередко выполняются по индивидуальным технологиям. Наиболее часто встречаются способы классификации и маркировки потоков данных, основанные на анализе следующих параметров, используемых устройствами на разных уровнях модели OSI:

- на L2-уровне – биты класса услуг стандарта IEEE 802.1Q [поле Class of Service (CoS)] заголовка Ethernet-кадра; значение экспериментальных бит MPLS;
- на L3-уровне – биты поля приоритета [поле IP Precedence (IPP)] в поле типа сервиса [поле Type of Service (ToS)] IP-заголовка датаграммы; кодовые точки механизма дифференцированных услуг [поле Differentiated Service Code Points (DSCP)] IP-заголовка датаграммы; IP-адреса отправителя и получателя IP-датаграмм;
- на L4-уровне – значения портов: TCP или UDP;
- на L7-уровне – значения подписей приложений.

На *канальном* (L2) уровне Ethernet-кадры могут помечаться с помощью бит в заголовке кадра с использованием согласно стандарту IEEE 802.1P бит приоритета (поле CoS) в заголовке IEEE 802.1Q (VLAN). Размер поля CoS – 3 бита, таким образом доступны для маркировки *восемь* классов сервиса (с 0 по 7) Ethernet-кадров.

На *сетевом* (L3) уровне в целях маркировки IP-датаграммы может быть использовано поле IP-заголовка Type of Service (ToS). Поле ToS в зависимости от решаемой задачи может быть интерпретировано в соответствии с классификатором поля IP Precedence (IPP) – поле имеет размерность 3 бита (принимает значения от ***0*** до ***7***).

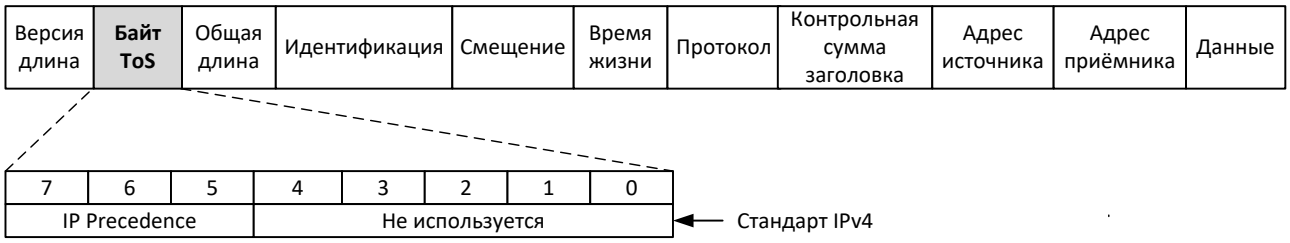


Рис. Г.1 Формат поля ToS в составе заголовка IP-датаграммы

Иллюстрирует сказанное приведенный на Рис. Г.1 формат размещаемого в заголовке IP-датаграммы поля ToS, используемого в целях маркировки IP-датаграммы согласно требуемому приоритету ее обработки.

В связи с тем, что в процессе продвижения данных от источника генерации трафика к его получателю среда передачи данных в сети на канальном (L2) уровне претерпевает частые изменения, метод маркировки IP-заголовков датаграмм на сетевом (L3) уровне представляется на текущий момент более практичным и универсальным.

Если упрощенно рассматривать жизненный цикл IP-датаграммы в сети с точки зрения процессов обеспечения качества обслуживания, то можно отметить следующие *этапы* этого цикла: генерация IP-датаграммы источником, ее классификация, маркировка в соответствии с классификацией, продвижение по маршруту к получателю *транзитом* через сетевые устройства с приоритетом согласно параметрам маркировки и, наконец, прибытие IP-датаграммы к адресату.

Процесс обработки промаркированного согласно приоритету потока транзитных данных сетевым устройством обобщенно выглядит следующим образом. Данные поступают на входной интерфейс устройства и обрабатываются в соответствии с назначением устройства (коммутируются, маршрутизируются или др.). По результатам обработки принимается решение, на какой выходной порт устройства и в каком виде передать данные для дальнейшей обработки – данные попадают в аппаратные очереди выходного порта (интерфейса). Аппаратные очереди представляют собой быструю память, хранящую данные перед тем, как они попадут непосредственно на выходной порт. Затем, согласно определенному алгоритму обработки, данные извлекаются из очередей и через выходной порт (интерфейс) устройства отправляются в сеть далее. Сказанное отчасти иллюстрирует приведенная на Рис. Г.2 схема обработки.

Механизмы приоритизации трафика, поддерживаемые изделием. Из всего многообразия понятий, составляющих понятие механизмов поддержки *качества обслуживания* в сетях (QoS), изделием поддерживается только механизм *приоритизации* – механизм приоритетной обработки IP-датаграмм на сетевом (L3) уровне согласно значениям 3-битного подполя *приоритета* (поле IP Precedence или IPP) в 8-битном поле *типа обслуживания* (поле Type of Service или ToS) заголовка IP-датаграммы (см. Рис. Г.1).

Поддерживаемые изделием механизмы приоритизации трафика включают два механизма:

- механизм *классификации* и *маркирования* IP-датаграмм, полученных изделием на обработку, путем корректировки подполя *приоритета* IPP поля ToS в зависимости от сочетания широкого набора критериев, учитываемых администратором изделия при настройке *системных* **`prt`**-фильтров (подробнее см. раздел 3.2.1.7, с. 104);
- механизм *приоритетной* обработки трафика IP-датаграмм путем организации на интерфейсах, при необходимости, *пула очередей*, пополняемого потоками *исходящих* IP-датаграмм согласно их приоритету (значению подполя IPP поля ToS) и обрабатываемого в соответствии с алгоритмом *строгой очередности приоритетов* (Strict Priority Queuing).

Порядок организации работы механизма *классификации* и *маркирования* IP-датаграмм, полученных изделием на обработку, подробно рассмотрен в разделе 3.2.1.7, с. 104. Отметим только общие (необязательные к исполнению) рекомендации по присвоению значений *приоритета* (подполе IPP поля ToS) отдельным типам IP-трафика, выработанные IT-сообществом:

- самые высокие по приоритету значения IPP, равные ***7*** и ***6***, резервируются для сетевого управляющего трафика (например, для протоколов маршрутизации);

-значение IPP, равное ***5***, рекомендовано для речевого трафика;

-значение IPP, равное ***4***, используется совместно трафиками видеоконференций и потокового видео;

-значение IPP, равное ***3***, предназначено для сигнализации вызовов;

-значения IPP, равные ***2*** и ***1***, могут использоваться для данных приложений;

-значение IPP, равное ***0***, представляет собой маркировку по умолчанию.

Далее коснемся работы механизма организации очередей и алгоритма их обработки.

При настройке большинства сетевых интерфейсов изделия (физических или виртуальных) администратору предоставляется возможность настройки значений их параметров **Скорость передачи** и **Скорость приема** (исключение составляют интерфейсы типа **GRE**, **L2–Eth**, **L2–VLAN** и **L2–TNL**). До той поры, пока значения этих параметров сохраняют *нулевое* значение, сетевые интерфейсы работают, не реагируя на значения поля приоритета в заголовках IP-датаграмм, выполняя обработку IP-датаграмм по мере их поступления.

Если же будут указаны *ненулевые* значения этих параметров, алгоритм работы интерфейсов перестраивается, начиная реагировать на значение поля приоритета IP-датаграмм. Причем алгоритмы обработки и реагирования на приоритеты IP-датаграмм, *принимаемых* и *передаваемых* интерфейсом, различны.

Приоритетная обработка передаваемого IP-трафика. Механизм приоритетной обработки для передаваемого интерфейсом изделия в сеть потока IP-датаграмм запускается на этапе инициализации работы интерфейса при условии, что администратор изделия указал при настройке этого интерфейса значение параметра **Скорость передачи**, *отличное* от нуля. Этот параметр может быть указан для следующих типов сетевых интерфейсов изделия – как физических, так и виртуальных: Ethernet-интерфейсов (см. бланки настройки: Рис. 2.9, с. 29), TNL-интерфейсов (см. Рис. 2.25, с. 41); VLAN-интерфейсов (см. Рис. 2.20, с. 38).

> **Примечание**. Значения параметров **Скорость передачи** и **Скорость приема** могут быть введены и при настройке дополнительных параметров интерфейсов L2-уровня – L2–Eth-интерфейсов и L2–TNL-интерфейсов, но обработка значений этих параметров и обеспечение работы механизма приоритизации для этих интерфейсов настоящей версией ОПО маршрутизаторов изделия не поддерживается.

Иллюстрирует работу механизма организации изделием приоритетной обработки IP-трафика при *передаче* схема, представленная на Рис. Г.2.

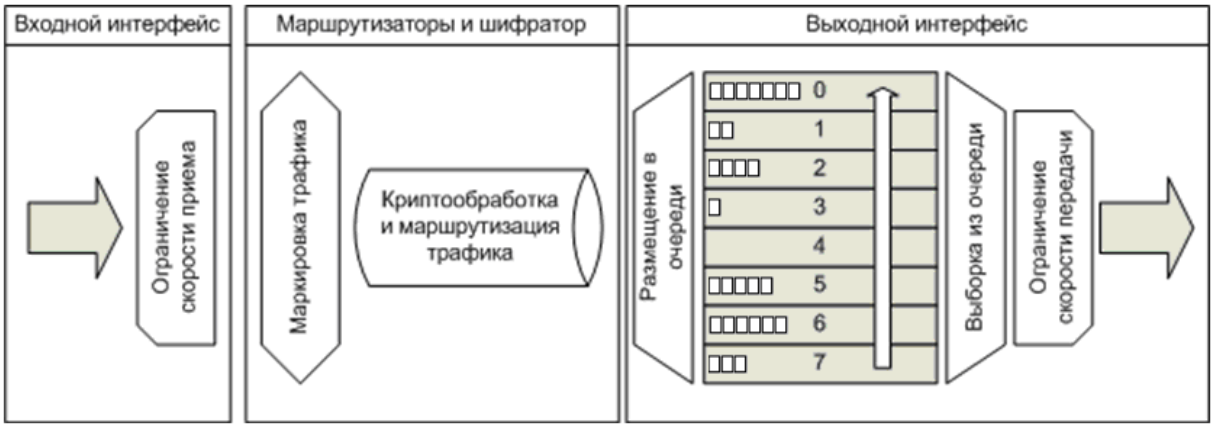


Рис. Г.2 Схема организации изделием приоритетной обработки IP-трафика при передаче

При включении на сетевом интерфейсе маршрутизатора механизма приоритетной обработки (параметр **Скорость передачи** в настройках интерфейса имеет значение, *отличное* от нуля) программа управления в оперативной памяти маршрутизатора образует для исходящих потоков IP-датаграмм этого интерфейса *пул* очередей – 8 выходных *логических* очередей, каждой из которых присваивается значение приоритета обработки от ***0*** (самый низкий приоритет) до **7** (самый высокий приоритет). Поступающие в этот интерфейс обработанные маршрутизатором *исходящие* IP-датаграммы попадают каждая в соответствующую из образованных очередей согласно своему приоритету – значению подполя IPP поля ToS в заголовке IP-датаграммы (на схеме Рис. Г.2 этот этап обработки представлен работой блока **Размещение в очереди**).

Попав в соответствующую очередь, IP-датаграммы будут извлекаться из нее для отправки в канал связи согласно применяемому в изделии алгоритму *строгой очередности приоритетов* (Strict Priority Queuing), работа которого сводится к следующему (на схеме Рис. Г.2 этот этап обработки представлен работой блока **Выборка из очереди**).

Программа управления начинает обработку с самой приоритетной очереди – той, которая имеет приоритет **7**. Поступившие в эту очередь IP-датаграммы будут выбираться для их передачи интерфейсом в сеть в том порядке, в каком они заполняли очередь – т.е. в соответствии с принципом: *первым пришел – первым вышел*. Если очередь с наивысшим приоритетом – приоритетом **7** – оказалась пуста, программа управления переходит к обработке очереди с приоритетом, на единицу меньшим – приоритетом **6**. Если очередь с приоритетом **6** оказалась пуста, программа управления переходит к обработке очереди с приоритетом **5** и т.д. Если при этом в очередях со старшими приоритетами (с приоритетом **7** или **6**) появятся IP-датаграммы, обработчик очередей приступит к обработке заполненной IP-датаграммами очереди с самым старшим приоритетом. Таким образом, до IP-датаграмм, попавших в очередь с приоритетом **0** (до IP-датаграмм без приоритета), дело дойдет лишь в том случае, когда все более приоритетные очереди будут пусты.

Приоритетная обработка принимаемого IP-трафика. Алгоритм обработки *принимаемого* из сети трафика с учетом приоритета поступающих IP-датаграмм отличается от алгоритма приоритетной обработки *передаваемого* интерфейсом в сеть исходящего трафика маршрутизатора следующим образом: при обработке принимаемого из сети входящего трафика механизмом приоритизации *не образуются* (как при передаче) *очереди* входящих IP-датаграмм, работа механизма сводится только к принятию решения о *прекращении* или о *продолжении* дальнейшей обработки интерфейсом поступившей из сети очередной порции информации.

Механизм приоритетной обработки для принимаемого из сети интерфейсом изделия потока IP-датаграмм запускается на этапе инициализации работы интерфейса только при условии, что администратор изделия указал при настройке этого интерфейса значение параметра **Скорость приема**, *отличное* от нуля.

При *нулевом* значении параметра **Скорость приема** скорость обработки интерфейсом поступающего из сети трафика искусственно не ограничивается; при этом механизм обработки интерфейсом входящего трафика с учетом приоритета входящих IP-датаграмм не запускается и *все* поступающие из сети порции информации обрабатываются интерфейсом в порядке их следования.

Если указано *отличное* от нуля – *пороговое* – значение параметра **Скорость приема**, включается механизм обработки интерфейсом *входящего* трафика с учетом *приоритета* входящих IP-датаграмм (значение подполя IPP поля ToS в заголовке IP-датаграммы).

При этом:

- если скорость потока входящего трафика IP-датаграмм на интерфейсе не превышает порогового значения параметра **Скорость приема**, то обработка трафика выполняется без учета анализа приоритета входящих IP-датаграмм;
- если скорость потока входящего трафика интерфейса превысила пороговое значение параметра **Скорость приема**, то включается механизм обработки интерфейсом входящего трафика IP-датаграмм с учетом приоритета (значения подполя IPP поля ToS в заголовке IP-датаграммы), работа которого заключается в следующем:
  - если значение подполя IPP поля ToS в заголовке IP-датаграммы *равно* нулю, ее дальнейшая обработка прекращается;
  - если значение подполя IPP поля ToS в заголовке IP-датаграммы *не равно* нулю, то осуществляется дальнейшая обработка IP-датаграммы в порядке ее следования маршрутизатором изделия, которому принадлежит сетевой интерфейс.

    Примечание. Отметим, что выбор значений параметров **Скорость передачи** и **Скорость приема** зависит от реальной пропускной способности трактов передачи данных, характера компонентов трафика, образующих общий соответственно *исходящий* или *входящий* поток интерфейса и подбор его величины зависит от множества факторов, которые администратору изделия следует учитывать в зависимости от приоритетов, устанавливаемых Администрацией ЗСПД для выполнения решаемых сетью задач по продвижению трафика, генерируемого различными приложениями Пользователя.

Приоритетная обработка IP-трафика на входе шифратора. Механизмы качества обслуживания, реализованные различными сетевыми устройствами, выполняют анализ требований, предъявляемых каждым из видов трафика, и, по возможности, предоставляют соответствующие результатам анализа значения параметров продвижения данного вида трафика по сети, касающиеся вопросов потери пакетов, их задержки, вариации задержки (джиттера) и т.д. Качество передачи информации напрямую зависит от этих параметров.

К защищенному трафику, циркулирующему в ЗСПД между изделиями защиты, предъявляются дополнительные специальные требования. Применение механизмов приоритетной обработки обеспечивает надлежащий уровень сервиса для различных типов сетевого трафика при наличии *ограниченного канального ресурса*.

Особенностью работы изделий защиты в этих условиях является то, что весь трафик, циркулирующий между внутренними и внешними сегментами ЗСПД продвигается *исключительно* через блок криптографической обработки (БКО) изделия, в котором исходящие во внешний сегмент сети потоки данных зашифровываются, а входящие – расшифровываются. Поэтому в изделиях защиты в случаях, когда основным ограничением продвижения трафика является пропускная способность канала связи, к которому подключено изделие,

недостаточно организовать работу механизмов приоритетной обработки трафика с помощью очередей (как часто делается в обычных маршрутизаторах) *только на выходе* изделия – на выходном интерфейсе БНМ изделия. В ряде случаев необходимо также (в силу ограничений, накладываемых особенностями работы криптоалгоритма, реализуемого БКО) организовывать обработку трафика с помощью механизма очередей также и на входе в БКО (в шифратор).

Выполнить это требование в изделии помогает применение сетевых виртуальных туннельных TNL-интерфейсов, обеспечивающих реализацию механизмов приоритетной обработки с помощью организации очередей разного приоритета и на входе в шифратор изделия, поскольку предоставляемый туннельными интерфейсами изделия механизм приоритетной обработки аналогичен рассмотренному выше механизму приоритетной обработки, предоставляемому физическими и рядом виртуальных интерфейсов изделия.

Приложение Д. Использование DNS-сервиса

Доменная система имен (**`Domain Name System`** или **`DNS`**) – это распределенная база данных, которая содержит информацию о компьютерах, включенных в сеть, организованную согласно `internet/intranet`-технологии.

DNS выполняет несколько задач, но основная – преобразование имени компьютеров в IP-адрес и наоборот. Пользователи сети в своей работе, как правило, применяют *имена* хостов, с которыми они обмениваются информацией. С другой стороны, программное обеспечение при обмене данными на сетевом уровне понимает только *IP-адреса*. Для разрешения этого противоречия и предназначена система DNS.

DNS, как и большинство информационных служб в сетях, организованных согласно `internet/intranet`-технологии, состоит из двух компонентов: множества связанных между собой *DNS-серверов* и неограниченного количества *DNS-клиентов*. DNS-клиенты посылают запросы к DNS-серверам и обрабатывают полученные от них ответы. DNS-серверы получают запросы от DNS-клиентов, производят поиск в своих базах данных и формируют ответы с результатами поиска. В случае необходимости DNS-серверы могут запрашивать у своих коллег недостающую информацию.

Изделие поддерживается функционирование обоих компонентов DNS: DNS-клиента и DNS-сервера. Порядок их настройки изложен в разделе 5.4, с. 157. Материал настоящего приложения может быть использован в качестве справочного руководства администратора DNS-сервера.

DNS-сервер изделия реализован в соответствии с рекомендацией **`RFC 1035`**.

Архитектура сервера и интерфейс взаимодействия с ним максимально приближены к известному DNS-серверу `The Berkeley Internet Name Domain` (BIND). Это сделано с целью упрощения процесса освоения администрирования DNS-сервера обслуживающим персоналом изделия.

В настоящее время издано большое количество различной документации по работе с DNS, включая официальные руководства и многочисленные пособия по сопровождению BIND. Учитывая это, предлагаемый ниже материал не содержит общих теоретических основ DNS, в нем приведены только некоторые основные понятия и описана конкретная реализация DNS-сервера, поддерживаемая изделием.
В конце настоящего Приложения рассмотрены особенности переноса конфигурационных файлов с сервера BIND на DNS-сервер изделия.

Понятие зоны

Пространство имен DNS имеет структуру дерева доменов с полномочиями, возрастающими по мере приближения к корню дерева. Это означает, что *родители* – домены старших уровней – имеют власть над *детьми*. Корень дерева имеет имя «**`.`**»; под ним находятся домены первого – *корневого* – уровня, каждый из которых управляет своим поддеревом. Домены второго и следующих уровней, в свою очередь, имеют управляемые ими поддеревья. Каждый домен – это отдельный фрагмент всемирного дерева, которым управляет один административный объект.

Каждый домен верхнего уровня может управлять всеми своими поддоменами самостоятельно, но может и делегировать свои полномочия по управлению администраторам младших поддоменов. Решение о делегировании полномочий управления принимается для каждого узла дерева имен самостоятельно. По этой причине при конфигурировании каждого DNS-сервера используется понятие *зоны*.

`Зона` – это множество имен данного домена за вычетом поддоменов, управление которыми передано своим администраторам. Иными словами, зона содержит все имена от конкретной точки дерева вниз, за исключением имен, делегированных в другие зоны.

Форматы записей файла зоны

Описание каждой зоны образует отдельный раздел базы данных DNS-сервера (*файл описания зоны* или просто *файл зоны*). Файл зоны состоит из записей описания ресурсов `Resource Record` (**`RR`**). Все **`RR`**-записи имеют следующий формат:

`[имя] [время] [класс] тип данные`

Первые три поля формата записи необязательны и могут отсутствовать.

`имя` – обозначает объект, к которому относится запись; значение поля зависит от типа записи (от значения поля **`тип`**); умалчиваемое значение – имя предыдущей **`RR`**-записи.

`время` – максимальное время хранения данной записи в кэшах прочих DNS-серверов (значение задается в секундах); умалчиваемое значение – **`не определено`**.

класс – тип сети; поле может иметь только одно значение **IN** (Internet), другие типы сетей изделие не обрабатывает; умалчиваемое значение – **IN**.

тип – тип записи; в базе данных **DNS**-сервера изделия могут быть записи следующих типов:

Тип	Функция
SOA	Задает основные параметры зоны
NS	Определяет серверы имен зоны
A	Задает преобразование имени в IP-адрес
PTR	Задает преобразование IP-адреса в имя
MX	Управляет маршрутизацией электронной почты
CNAME	Определяет дополнительные (алиасные) имена машины

данные – значение поля зависит от типа записи (от значения поля **тип**).

Правила подстановки имен в DNS-сервере изделия

Имена содержатся в двух полях **RR**-записи – в поле **имя** и в поле **данные**. При использовании записи для имен действует следующее правило. Если имя не заканчивается точкой, то оно считается *относительным.* К такому имени автоматически добавляется точка и «**имя_зоны**». Если имя заканчивается точкой, то оно считается полностью определенным и используется без всяких изменений.

Имя_зоны – это значение поля **имя** записи типа **SOA** (см. ниже). В изделии запись **SOA** содержится в заголовке раздела, поэтому ко всем относительным именам будет добавляться имя раздела (имя файла зоны).

Отсюда, в частности, следует, что имена всех зон должны иметь в конце точку!

Указанное правило подстановки имен позволяет сократить объем раздела базы (файла зоны) за счет того, что можно опустить текущее имя зоны для большинства записей. Но это же правило может создать проблемы, если недопустимо, чтобы происходила автоподстановка.

> *Наш практический совет*: если имя не находится в той зоне, для которой создается раздел базы данных **DNS**-сервера изделия, следует заканчивать такое имя точкой.

Примеры

В записях раздела **xyz.ru.** (обратите внимание на концевую точку в имени зоны) будут выполнены следующие преобразования имен:

user1 ⇨ user1.xyz.ru.

user1.host1 ⇨ user1.host1.xyz.ru.

В записях раздела **1.168.192.IN-ADDR.ARPA.** будет выполнено следующее преобразование имени:

11 ⇨ 11.1.168.192.IN-ADDR.ARPA.

Запись типа SOA

Записи **SOA** (начало полномочий Зоны, Start of a zone of Authority) отмечают начало зоны в области пространства имен DNS и сообщают основные характеристики этой зоны.

> ***Замечание***. Описания зон изделием хранятся в форме специализированной базы данных, поэтому запись **SOA** задается как заголовок раздела базы данных, описывающего зону. Внутри описания зоны **RR**-запись типа **SOA** задать невозможно.

Формат записи:

имя_зоны [время] IN SOA данные

Поле **данные** содержит **описание зоны**. В состав **описание зоны** входит следующая информация:

- имя основного DNS-сервера зоны;
- адрес электронной почты администратора зоны для возможности связи с ним; в почтовом адресе символ "@" должен быть заменен точкой;
- **Serial** – серийный номер (serial number) – номер версии *файла зоны* (целое положительное число); этот номер администратор зоны должен увеличивать каждый раз, когда в файл зоны вносятся изменения;
- **Refresh** – параметр показывает, как часто (в секундах) вторичные DNS-серверы должны проверять первичный (основной) DNS-сервер, чтобы узнать, не изменился ли серийный номер зоны (**Serial**) и

не нужно ли обновить зону; общепринятые значения для данного времени от ***3600*** до ***21600*** (от одного до шести часов);

- **Retry** – параметр показывает, как долго (в секундах) вторичный сервер должен ждать, прежде чем повторить неудавшуюся передачу данных зоны; обычно этот параметр имеет значение в интервале от ***1200*** до ***3600*** (от ***20*** до ***60*** минут);
- **Expire** – параметр указывает верхний предел времени (в секундах), в течение которого вторичный сервер может использовать данные без обновления; по истечении указанного времени данные теряют силу и должны быть удалены из кэша; обычно для этого параметра устанавливается значение в интервале от недели до месяца;
- **Minimum** – количество секунд, используемое в качестве умалчиваемого значения поля **время** в **RR**-записях (время жизни записи); это же значение является вынужденным минимумом для времени жизни, если оно задано явно в какой-либо **RR**–записи зоны.

Пример:

xyz.ru. IN SOA	**ns.xyz.ru.**	**root.mailer.xyz.ru.**	**140199001**	**10800**	**1800**	**3600000**	**259200**
	имя сервера	адрес ЭП адм.	Serial	Refresh	Retry	Expire	Minimum

Запись типа NS

С помощью записей **NS** (Сервер имен, Name Server) описываются DNS-серверы, которые авторитетны для данной зоны. Авторитетными называются те DNS-серверы, на которых размещаются и редактируются файлы зон и которые могут дать точный (авторитетный) ответ.

Замечание. Если **NS** -записи присутствуют в файле зоны, то они обычно идут первыми.

Формат записи:

имя_зоны [время] IN NS имя_машины

В записях типа **NS** значение первого поля (**имя_зоны**) совпадает с именем файла зоны, поэтому, если эти записи стоят первыми в файле зоны (т. е. сразу после записи типа **SOA**), то **имя_зоны** может быть опущено.

Примеры:

```
xyz.ru. 21600 IN NS ns1.xyz.ru.
              IN NS ns2.xyz.ru.
```

Запись типа A

Записи типа **A** (Адрес, Address) составляют основу файла зоны. С их помощью обеспечивается перевод имен машин в IP-адреса.

Формат записи:

имя_машины [время] IN A IP-адрес

Примеры:

```
user1          21600 IN A 192.168.1.11
user2.xyz.ru.        IN A 192.168.1.12
```

Запись типа CNAME

CNAME (Canonical Name) – каноническое имя. Каноническим называют основное имя машины. Записи типа **CNAME** позволяют задавать машинам дополнительные (алиасные) имена. Эта возможность часто используется для введения более коротких синонимов к основному имени машины, а также в случае изменения имени машины для сохранения доступа к ней по старому имени.

Формат записи:

алиас [время] IN CNAME имя_машины

Примеры:

```
anton 21600 IN CNAME user1.xyz.ru.
ivan        IN CNAME user2
```

Запись типа PTR

Записи типа **PTR** (указатель на доменное имя, Domain Name Pointer) выполняют обратное преобразование IP-адресов в имена машин.

Формат записи:

```
IP-адрес [время] IN PTR имя_машины
```

Примеры:

```
11 21600 IN PTR user1.xyz.ru.
12       IN PTR user2.xyz.ru.
```

> ***Внимание!*** С целью унификации процедур поиска записей **PTR** в базе данных DNS-сервера значение **IP-адрес** записывается не в обычной для IP-адресов нотации. Чтобы сохранить принципы формирования доменных имен, IP-адреса записывают, начиная с младшей части (в «перевернутом» формате). Кроме того, следом за «перевернутым» IP-адресом записывают имя специального домена «**.IN-ADDR.ARPA.**».
>
> Например, IP-адрес **192.168.1.11** должен быть записан как
> **11.1.168.192.IN-ADDR.ARPA.**
>
> Обычно при конфигурировании **DNS**-сервера изделия для каждой зоны формируют два раздела (два файла зоны). Первый – для прямого преобразования **имя ⇨ адрес**, второй – для обратного преобразования **адрес ⇨ имя**. Файл прямого преобразования имеет имя домена (например, **xyz.ru.**), а файл обратного преобразования должен иметь имя из домена **IN-ADDR.ARPA**. (например, **1.168.192.IN-ADDR.ARPA.**). Записи **PTR** помещаются именно в этот файл.
>
> Благодаря наличию *правила подстановки имен* в поле **имя** записи типа **PTR** в качестве **IP-адреса** достаточно поместить младшую часть IP-адреса машины. Система сама расширит запись адреса до полного формата за счет добавления имени файла зоны.

Запись типа MX

Записи типа **MX** (Почтовый коммутатор, Mail Exchange) используются системами электронной почты для более эффективной маршрутизации почты. С помощью записей **MX** назначаются узлы, ответственные за доставку почты в адрес абонентов конкретного домена.

Формат записи:

```
имя_домена [время] IN MX приоритет имя_машины
```

Примеры:

```
user1.xyz.ru. 21600 IN MX 10 mailer1.xyz.ru.
                    IN MX 20 mailer2.xyz.ru.
user2.xyz.ru.       IN MX 0 user2.xyz.ru.
```

Записи **MX** обеспечивают доставку почты в адрес домена **имя_домена** (**user1.xyz.ru.** – в первом примере) путем ее пересылки в адрес машины с именем **имя_машины**. Если для одного значения **имя_домена** имеется несколько **MX**-записей (как в нашем примере), то сначала делается попытка доставить почту в адрес машины с меньшим значением параметра **приоритет**. В случае проблем с доставкой почта автоматически доставляется в адрес другой машины.

Правильно сконфигурированная зона обязательно содержит **MX**-записи для всех машин, способных получать почту. Причем, если машина будет самостоятельно принимать свою почту, то в качестве **имени_домена** и **имени_машины** должно быть указано собственное имя машины так, как оно задано в записи типа **A** (см. третью строку примера).

> *Внимание!* Правила запрещают использование алиасных имен (определенных записями типа **CNAME**) в качестве **имени_машины** в поле **данные MX**-записей.

Отличия конфигурирования DNS-сервера изделия от конфигурирования BIND

1. **DNS**-сервер изделия может обслуживать до 8-ми зон.
2. Имена зон должны заканчиваться точкой. Имя зоны, используемой для накачки кэша, должно состоять из одной точки.

   Пример. Пусть стандартный файл **named.boot BIND** имеет вид:

   ```
   cache     .                    named.cache
   primary   factor.ru            named.hosts
   ```

```
primary   0.0.127.IN-ADDR.ARPA      named.local
primary   1.168.192.IN-ADDR.ARPA    named.rev
primary   factor.rospac.ru          factor.hosts
primary   36.220.194.IN-ADDR.ARPA   factor.rev
```

В **DNS**-сервере изделия для указания аналогичных **BIND** режимов работы следует создать 5 зон с именами:

```
.
factor.ru.
1.168.192.IN-ADDR.ARPA.
factor.rospac.ru.
36.220.194.IN-ADDR.ARPA.
```

Зону с именем **0.0.127.IN-ADDR.ARPA.** создавать не нужно.

3. При создании зоны в ее заголовке, кроме имени зоны, должны быть заданы все параметры записи **SOA** зоны. Внутри зоны записи типа **SOA** не допускаются.
4. При создании записей зон нужно руководствоваться стандартными правилами. Для загрузки записей зон можно использовать стандартные текстовые файлы системы **BIND** с учетом следующих ограничений:
   - каждая запись должна занимать одну строку; круглые скобки не обрабатываются;
   - запись типа **SOA** должна быть исключена или закомментирована;
   - команды `$origin` и `$include` не обрабатываются.
5. При загрузке записей зоны в кэш выполняются следующие соглашения.
   - Вместо отсутствующего имени записи подставляется имя предыдущей записи.
   - Вместо отсутствующего имени первой записи подставляется имя зоны.
   - К именам, не имеющим точки в конце, добавляется точка и имя зоны, которое обязательно должно заканчиваться точкой.
   - Если значения в поле **время** нет, подставляется время **Minimum** из заголовка зоны.
6. Если в процессе работы **DNS**-сервера изделия администратор зоны вносит какие-либо изменения в файл зоны, то программа управления сразу же выполняет перезагрузку кэша.
7. С целью обеспечения безопасности обслуживания программа управления изделием отказывает в исполнении запросов на пересылку зон, т. е. ни один внешний сервер не может извлечь целиком зону из **DNS**-сервера изделия.

Приложение Е. Системные журналы изделия

При работе изделия практически каждое выполненное действие (происходящее событие) фиксируется или может быть зафиксировано (в случае соответствующих настроек средств трассировки изделия) в одном из системных журналов изделия.

Системные журналы изделия представляют собой две группы файлов: группа файлов, в которых фиксируются события, происходящие в блоке внутренней маршрутизации (БВМ), и аналогичная группа файлов с такими же именами, в которых фиксируются события, происходящие в блоке наружной маршрутизации (БНМ).

Все системные журналы маршрутизаторов изделия представляют собой обычные текстовые файлы, имена которых сформированы по общему правилу: первые три символа *основной* части имени – **LOG**, *расширение* – **EMA** (системные журналы иначе называются **LOG** -файлами или файлами *протоколирования*).

1. Журнал LOG.EMA

Файл **LOG.EMA** – это основной системный журнал маршрутизатора изделия. Он служит для протоколирования общесистемной информации о работе маршрутизатора изделия. В файл **LOG.EMA** записывается вся информация, выдаваемая на видеомонитор ЛКУ соответствующего маршрутизатора – БВМ или БНМ.

Работа любого из маршрутизаторов изделия с журналами начинается с открытия файла **LOG.EMA**. На Рис. Е.1 приведен фрагмент записываемой в журнал информации о запуске маршрутизатора изделия.

```
Открыт протокольный файл "log.ema"

Процессор: 'Intel(R) Core(TM) i3-2130 CPU @ 3.40GHz', частота 3392 (Мгц)
Плата 'Бастион2-Ф': fe600000 Rev 53.53. Slave


Код завершения предыдущего сеанса работы: -1
(возможные причины - сбой питания или зависание системы)

FDI: 2, TIMEOUT 600 ----------- 15:05:43 17-08-15
FDI: DIGEST dioniswt.exe  OK
```

Рис. Е.1 Фрагмент записываемой в журнал информации о запуске маршрутизатора изделия

В протоколе после первой записи об открытии файла следуют записи с техническими характеристиками аппаратных компонентов маршрутизатора изделия и код завершения предыдущего сеанса его работы.

Затем следует информация о контроле целостности общего программного обеспечения маршрутизатора изделия:

TIMEOUT (интервал проверки в секундах), имя контролируемого файла (**dioniswt**) с результатом выполненного контроля (**OK**).

В файл **LOG.EMA** заносится запись «**СТОП**» в тех случаях, когда программа управления не допускает абонента к работе с маршрутизатором изделия. Запись содержит информацию о причине недопуска и имеет следующий формат:

```
N Who СТОП hh:mm:ss dd-mm-yy контроль=kod1 вход=kod2 <adress
```

где:

N – номер порта, через который абонент пытался начать работу с маршрутизатором изделия;

Who – имя абонента, который пытался начать работу с маршрутизатором изделия;

hh:mm:ss dd-mm-yy – время и дата записи в **LOG**-файл;

kod1,kod2,kod3 – коды завершения операции;

adress – адрес абонента, который пытался начать работу с маршрутизатором изделия.

Значения кодов завершения операции СТОП:

Kod1 (контроль)

- **1** Нет абонента с указанным именем
- **7** Абонент с таким именем уже есть
- **8** Неверно указан пароль

Kod2 (вход)

1 Произошло аварийное сворачивание работы ОПО

7 Неправильно указан язык

32 Неправильно указан дополнительный пароль

2. Журнал LOG_USER.EMA

В файле **LOG_USER.EMA** всегда фиксируется факт запуска и останова маршрутизатора изделия. В файл **LOG_USER.EMA** записывается информация о регистрации новых абонентов, об удалении или изменении полномочий ранее зарегистрированных абонентов, а также о начале или окончании работы абонента с маршрутизатором изделия.

Каждое фиксируемое событие представлено в файле **LOG_USER.EMA** отдельной записью; начинается запись всегда с первой позиции строки и имеет следующий формат:

```
PP_OO_exit: Who hh:mm:ss dd-mm-yy Add
```

PP – код процесса;

OO – код операции;

exit – код завершения операции;

Who – имя абонента, при работе которого производится запись в LOG-файл;

hh:mm:ss dd-mm-yy – время и дата записи в LOG -файл;

Add – дополнительная информация (может отсутствовать).

Процессы, фиксируемые в LOG-файле **LOG_USER.EMA**, имеют следующие коды:

PP (код)	**Процесс**
ss	работа изделия и работа абонентов
rc	удаленное управление
tm	служба времени

Операции каждого из процессов представлены в нижеследующих таблицах. Все таблицы имеют одну и ту же структуру, а именно:

OO (код)	**Операция**	**exit** (код завершения)	**Add** (дополнительная информация)

Первая графа (**OO**) – код операции.

Вторая графа (**Операция**) – название операции.

Третья графа (**exit**) – значение кода завершения операции (**OK** или **ERR**). Коды завершения предусмотрены не для всех операций; для некоторых из операций предусмотрен только один код (или при успешном завершении или при аварийном). Если код завершения не предусмотрен, то при записи операции в LOG-файл на месте кода (**exit**) ставятся два пробела.

Четвертая графа (**Add**) может содержать различную информацию.

После таблиц в качестве примера приведены фрагменты реального LOG-файла с нашими комментариями.

Процесс «Работа изделия и работа абонентов» (код **ss**)

OO	**Операция**	**exit**		**Add**
DO	запуск изделия			
DC	останов изделия	**OK**	**ER**	
UA	создание абонента или группы абонентов	**OK**		
UD	удаление абонента или группы абонентов	**OK**		
li	начало работы абонента с изделием	**OK**	**ER**	
br	прекращение сеанса из-за разрыва связи			
ab	абортирование абонента (по причине неактивности, при срочном останове системы и пр.)			
AP	неверно введен пароль администратора узла		**ER**	
	неверно введен пароль администратора группы		**ER**	**Gr:-**<имя_группы>
TA	изделие переведено в режим "**администратор узла**"	**OK**		
TO	изделие переведено в режим "**оператор**"	**OK**		
??	изделие переведено в режим "**администратор сети**"	**OK**		

Пример: фрагмент файла **LOG_USER.EMA**

```
Запуск КМ
ss_DO_ : DIONIS 16:56:02 28-09-15
Создание группы абонентов USERS
ss_UA_OK: -USERS 17:03:28 28-09-15 Gr:6 Id:6
Создание абонента uu1
ss_UA_OK: uu1 17:15:13 28-09-15 Gr:6 Id:12090
```

```
вход uu1 в КМ
ss_li_ : uu1 17:56:15 28-09-15
прекращение сеанса из-за разрыва связи
ss_br_ : uu1 18:07:22 28-09-15
Удаление абонента из системы
ss_UD_OK: uu1 18:58:15 28-09-15
Неверно введен пароль администратора узла
ss_AP_ER: admin 19:00:04 28-09-15
Узел переведен в режим "администратор узла"
ss_TA_OK: admin 19:03:15 28-09-15
узел переведен в режим "оператор" из режима "администратор узла"
ss_TO_OK: admin 19:10:04 28-09-15
Останов КМ
ss_DC_OK: DIONIS 19:50:31 28-09-15
```

Процесс «Удаленное управление» (код **rc**)

OO	Операция	exit		Add
au	автоматическое разрешение на удаленное управление	OK		Md:<режим_управл.>
er	отказано в разрешении на удаленное управление			Er:#

В графе **Add**:

<режим_управл.>: возможные значения: Look, Control и Grasp (уровень полномочий – **Захват**).

Er:# – символ **#** означает число;

возможные значения:

1 – не хватает ресурсов, чтобы разрешить удаленное управление;

5 – ошибочное имя или дополнительный пароль.

Процесс «Служба времени» (код **tm**)

OO	Операция	exit		Add
A+	включение автоматич. перехода на летнее/зимнее время	OK		
A-	отключение автоматич. перехода на летнее/зимнее время	OK		
S+	включение SNTP-протокола	OK		
S-	отключение SNTP-протокола	OK		
S?	проблемы при работе с SNTP-сервером		ER	Er:#
TS	автоматический переход на летнее время	OK		Ov:ДВ Nv:ДВ
			ER	Ov:ДВ Nv:ДВ Er:#
TW	автоматический переход на зимнее время	OK		Ov:ДВ Nv:ДВ
			ER	Ov:ДВ Nv:ДВ Er:#
S=	изменение системного времени SNTP-сервером	OK		Ov:ДВ Nv:ДВ
			ER	Ov:ДВ Nv:ДВ Er:#
ST	установка времени администратором	OK		Ov:ДВ Nv:ДВ
			ER	Ov:ДВ Nv:ДВ Er:#
SD	установка даты администратором	OK		Ov:ДВ Nv:ДВ
			ER	Ov:ДВ Nv:ДВ Er:#
TZ	установка переменной **TZ** администратором	OK		Ov:ДВ Nv:ДВ
			ER	Ov:ДВ Nv:ДВ Er:#

В графе **Add**:

ДВ – дата и время в стандартном формате (**hh:mm:ss dd-mm-yy**);

Ov – старые дата и время;

Nv – новые дата и время;

Er:# – символ **#** означает код; возможные значения:

101	–	не дождались ответа от сервера;
102	–	проблемы с чтением файла **sntp_tcp.ema**;
103	–	в конфигурации изделия не задано ни одного SNTP-сервера;
1	–	не хватает оперативной памяти;
2	–	ошибка при изменении значения переменной **TZ**;
22	–	ошибка при изменении даты/времени;
100	–	SNTP-сервер дал коррекцию времени вне заданного интервала.

3. Журнал LOG_TCP.EMA

В файле **LOG_TCP.EMA** дублируется информация файла **LOG.EMA**, относящаяся к работе подсистемы **Параметры [Компонент TCP/IP]**. Кроме того, в файл **LOG_TCP.EMA** заносятся записи, в которых фиксируется прохождение через маршрутизатор изделия тех IP-датаграмм, для которых в правилах IP-фильтрации установлен режим *фиксации* IP-датаграмм (см. раздел 3.2.1.9, с. 108).

Формат записей фиксации проходящих через маршрутизатор изделия датаграмм

На каждую датаграмму, подлежащую фиксации, в файле **LOG_TCP.EMA** формируется до 4 строк информации. В начале каждой строки ставится префикс **1f:**, **2f:**, **3f:** или **0f:**.

> Специальный формат префиксов позволяет быстро отобрать из всего многообразия записей файла **LOG_TCP.EMA** только записи фиксации датаграмм (по контексту "**f:** "). Кроме того, префикс определяет назначение (и формат) записи информации о фиксируемой датаграмме.

1f: – информация об элементе фильтра (о правиле), вызвавшем запись в LOG-файл;

2f: – расшифровка полей IP-заголовка датаграммы;

3f: – расшифровка заголовков протоколов, вложенных в IP;

0f: – строка-разделитель.

Записи с префиксами **1f:**, **2f:**, и **0f:** формируются для всех датаграмм. Запись с префиксом **3f:** формируется только для датаграмм, обеспечивающих транспортировку пакетов протоколов TCP, UDP и ICMP.

Первая строка (данные элемента фильтра):

```
1f: hh:mm:ss dd:mm:yy name fname[N]status prot flag L-M ADR_from/bit->ADR_to/bit LOG
```

hh:mm:ss dd-mm-yy – время и дата записи в **LOG**-файл;

name – имя интерфейса, через который передается датаграмма;

fname – имя фильтра;

N – порядковый номер сработавшего правила (элемента фильтра).

Далее следует в текстовом формате содержание сработавшего элемента фильтра:

status – значение параметра **Режим** (возможные значения: ***разрешить***, ***запретить***, ***сбросить***);

prot – значение параметра **Протокол** (возможные значения: ***ALL***, ***ICMP***, ***TCP***, ***UDP***);

flag – значение flagow TCP (возможные значения: **_** (пробел), ***SYN***, ***ACK***);

L-M – диапазон номеров портов;

ADR_from/bit – адрес отправителя и количество значащих бит в адресе отправителя;

ADR_to/bit – адрес получателя и количество значащих бит в адресе получателя;

LOG - признак записи в LOG-файл (параметр элемента фильтра **Фиксировать** имеет значение ***Да***).

Вторая строка (расшифровка полей IP-заголовка датаграммы):

```
2f: IP: ADR_from->ADR_to len XX ihl XX ttl XX prot XX tos XX id XX offs XX DF MF
```

ADR_from – адрес отправителя;
ADR_to – адрес получателя;
len XX– длина датаграммы в байтах (заголовок + данные);
ihl XX – длина IP-заголовка в байтах;
ttl XX – значение поля **TTL**;
prot XX – значение поля **Protocol**;
tos XX – значение поля **ToS**, если оно не равно нулю;
id XX offs XX – идентификатор датаграммы и смещение данных
(только для фрагментированных датаграмм: установлен флаг **MF** или **offset**!=0);
DF MF – флаги **DF** и **MF**, если они установлены.

Третья строка (расшифровка заголовков протоколов, вложенных в IP). Наличие третьей строки определяется значением поля **Protocol** в IP-заголовке датаграммы (значение **prot xx** во *второй строке*):

prot 6 – соответствует протоколу TCP;
prot 17 – соответствует протоколу UDP;
prot 1 – соответствует протоколу ICMP.

Заголовки остальных протоколов не расшифровываются, третья строка с префиксом **3f:** для них не формируется.

Расшифровка заголовка протокола TCP, вложенного в IP:

```
3f: TCP: Port_from->Port_to seq xXXXX [Ack xXXXX] flag Wnd XX [UP xXXXX] MSS XXXX
```

Port_from – порт отправителя;
Port_to – порт получателя;
seq xXXXX – значение поля Sequence Number;
Ack xXXXX – значение поля Acknowledgment Number (поле присутствует, если установлен флаг **ACK**);
Flag – установленный флаг (возможные значения: **FIN, SYN, RST, PSH, ACK, URG**);
Wnd XX – размер окна;
UP xXXXX – значение поля Urgent Pointer (поле присутствует, если установлен флаг **URG**);
MSS XXXX – значение опции Maximum Segment Size (если она присутствует в заголовке).

Расшифровка заголовка протокола UDP, вложенного в IP:

```
3f: UDP: Port_from->Port_to len XX
```

Port_from – порт отправителя;
Port_to – порт получателя;
len XX – длина UDP-пакета в байтах .

Расшифровка заголовка протокола ICMP, вложенного в IP:

```
3f: ICMP: type code XX
```

type – тип (для типов меньше 16 выводится словесная интерпретация типа);
code XX – значение кода для этого типа (типы и коды см. в стандарте RFC792).

Пример: фрагмент файла **LOG_TCP**

```
1f:  11:05:56  09-06-99  LAN_D_D  f1[1]  запретить  ALL  0-0  192.168.4.2/32-
>0.0.0.0/00 LOG
2f: IP: 192.168.4.2->192.168.4.1 len 96 ihl 20 ttl 15 prot 1
3f: ICMP: Echo Request code 0
0f:
1f:  14:29:01  09-06-99  LAN_D_D  f1[1]  запретить  ALL  0-0  192.168.4.2/32-
>0.0.0.0/00 LOG
2f: IP: 192.168.4.2->192.168.4.1 len 40 ihl 20 ttl 15 prot 6 tos 16
3f: TCP: 1024->23 Seq x3435001 RST Wnd 0
0f:
1f:  14:31:46  09-06-99  LAN_D_D  f1[1]  запретить  ALL  0-0  192.168.4.2/32-
>0.0.0.0/00 LOG
2f: IP: 192.168.4.2->192.168.4.1 len 53 ihl 20 ttl 15 prot 17
3f: UDP: 1028->53 len 33
0f:90
```

Приложение Ж. Ethernet-адаптеры изделий и настройка сетевых интерфейсов

В изделиях, исполненных в двухсегментной архитектуре технологии DioNIS®, применяется широкий набор сетевых Ethernet-адаптеров разнообразных конструкций.

Учитывая, что одним из важнейших аспектов подготовки изделия к штатной эксплуатации является процесс настройки сетевых интерфейсов маршрутизаторов (БВМ и БНМ) изделия, администратору изделия полезно ознакомиться с приведенными в настоящем Приложении сведениями об организации сетевого обмена и о применяемых в изделиях *типовых* конструкциях сетевых Ethernet-адаптеров, знание которых поможет избежать возможных затруднений при настройке физических сетевых интерфейсов изделия.

Напомним, что администратор изделия при создании и настройке физических интерфейсов изделия (Ethernet-интерфейса или L2–Eth-интерфейса) должен *соотнести* с каждым из создаваемых физических интерфейсов определенный *канал связи* маршрутизатора с сетью – *порт*, работа которого обеспечивается функционированием подключаемого к требуемой сети Ethernet-адаптеров соответствующего маршрутизатора изделия. Выполняется это требование при настройке физического интерфейса путем указания значения параметра **`Номер порта`** (см. бланк настройки дополнительных параметров Ethernet-интерфейса – Рис. 2.9, с. 29 или бланк настройки дополнительных параметров физического L2–Eth-интерфейса – Рис. 2.16, с. 34).

> *Примечание.* В случае, когда необходимо организовать функционирование создаваемого физического интерфейса в режиме *объединения* (агрегирования) каналов связи, следует *соотнести* с этим физическим интерфейсом не один порт (канал связи) маршрутизатора изделия, а их *группу* (подробнее см. раздел 2.3.1, Рис. 2.9, с. 29; раздел 2.3.2, Рис. 2.16, с. 34; раздел ***Приложение Б*** (с. 226) к настоящему РНУ).

Будем называть *гнездом* разъем Ethernet-адаптера, к которому может быть подключен сетевой кабель, соответствующий *виду* сетевой *среды передачи данных* подключаемой ЛВС – *проводной* или *оптической* – кабель витой пары или оптоволоконный кабель.

Маркировка номеров портов сетевых Ethernet-адаптеров изделия выполнена тем или иным способом на корпусах моноблоков изделий, сведения о маркировке приведены в ЭД на конкретное изделие. Тем не менее, представляется, что, учитывая широкое разнообразие применяемых в изделиях конструкций сетевых Ethernet-адаптеров, изложенные в настоящем Приложении сведения будут полезны при настройке физических сетевых интерфейсов.

При создании и настройке сетевого физического интерфейса в процессе подготовки каждого из маршрутизаторов изделия к сетевому обмену по конкретному *направлению* (каналу связи или их группировке) программа управления, используя ресурсы УВП соответствующего маршрутизатора, формирует логическую структуру – *физический интерфейс* (см. Рис. Ж.1 и Рис. Ж.2), использование которого программой далее в штатной работе обеспечивает управление обменом между сетевым и канальным уровнями на требуемом направлении. Для каждого из маршрутизаторов изделия на этапе подготовки к работе создается необходимое количество таких структур – физических интерфейсов.

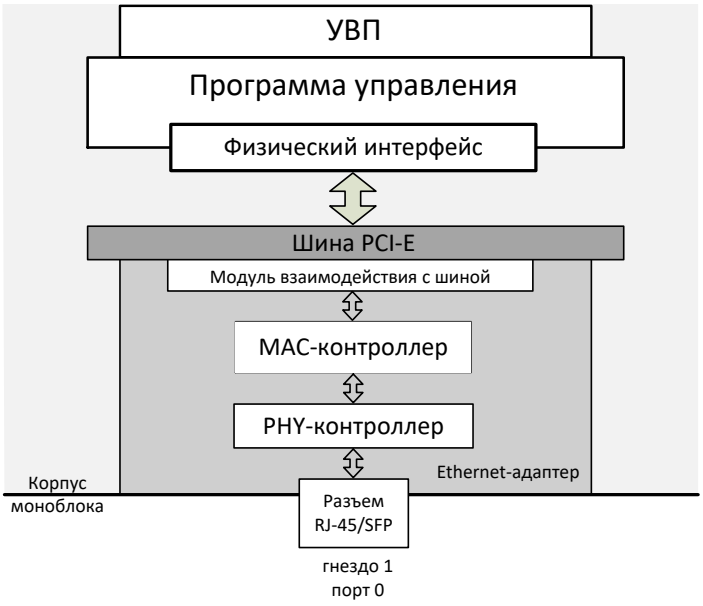


Рис. Ж.1 Схема организации обмена с применением однопортового Ethernet-адаптера изделия (классика)

В изделиях применяются как *однопортовые* (одноканальные), так и *многопортовые* (многоканальные) Ethernet-адаптеры разнообразных конструкций. В конструкции отдельных из них применяются *комбо-порты*; при этом обеспечивается возможность выбора варианта подключения изделия к сетям с различной средой передачи данных – с помощью оптоволоконного кабеля или с помощью кабеля витой пары. Поэтому выбор правильного значения параметра **`Номер порта`** может вызвать некоторые затруднения. Материал настоящего Приложения содержит сведения, которыми полезно руководствоваться при выборе значения параметра **`Номер порта`**.

На Рис. Ж.1 схематически представлена общая (упрощенная) архитектура простого *однопортового* (классического) Ethernet-адаптера и схема организации с его применением обмена между маршрутизатором изделия и сетью. С одной стороны Ethernet-адаптер стандартно подключается к шине PCI-E универсального вычислительного процессора маршрутизатора, что через *модуль взаимодействия с шиной* в составе адаптера обеспечивает его взаимодействие с ресурсами УВП соответствующего маршрутизатора изделия. С другой стороны через разъем, конструкция которого соответствует виду среды передачи данных, Ethernet-адаптер с помощью соответствующего кабеля подключается к сети с определенной средой передачи данных.

MAC-контроллер – обеспечивает на *канальном* (L2) уровне модели OSI реализацию выполнения собственно логики работы Ethernet-адаптера (включая управление MAC-адресом, обработку очередей потоков принимаемых и передаваемых Ethernet-кадров, предусматривающую контроль их формата, вычисление и проверку контрольных сумм и пр.), обеспечивая также информационное сопряжение как с ресурсами УВП маршрутизатора (через модуль взаимодействия с шиной PCI-E), так и с внешними физическими интерфейсами (через PHY-контроллер доступа к среде передачи данных).

PHY-контроллер – обеспечивает на *физическом* (L1) уровне модели OSI выполнение операций управления доступом к соответствующей среде передачи данных (оптоволоконной или проводной) и собственно стыковку с физической линией сети (с помощью сетевого кабеля через разъем соответствующей конструкции).

Представленный на Рис. Ж.1 Ethernet-адаптер обеспечивает работу с сетями по *единственному* каналу связи (*порту*), поэтому он укомплектован одной парой MAC-контроллера и PHY-контроллера. При этом PHY-контроллер обеспечивает взаимодействие только с одной из сетевых сред передачи данных, поэтому адаптер имеет *единственный* разъем (*гнездо*), обеспечивающий подключение к сетевой среде передачи данных определенного вида: разъем типа RJ-45 – для подключения к сети с помощью кабеля витой пары или SFP-разъем с оптоволоконной SFP-вставкой – для подключения к сети с помощью оптоволоконного кабеля. Конструкция такого Ethernet-адаптера обеспечивает функционирование *единственного* физического интерфейса маршрутизатора изделия.

На Рис. Ж.2 схематически представлена общая (упрощенная) архитектура *многопортового* (N-портового) Ethernet-адаптера с *комбо-портами*, каждый из которых обеспечивает доступ (по выбору) к одной из *двух* сред передачи данных: через разъем типа RJ-45 – для подключения к сети с помощью кабеля витой пары или через SFP-разъем с оптоволоконной SFP-вставкой – для подключения к сети с помощью оптоволоконного кабеля. Применение адаптера такой конструкции обеспечивает возможность выбора среды передачи данных сети, к которой должно быть выполнено подключение изделия.

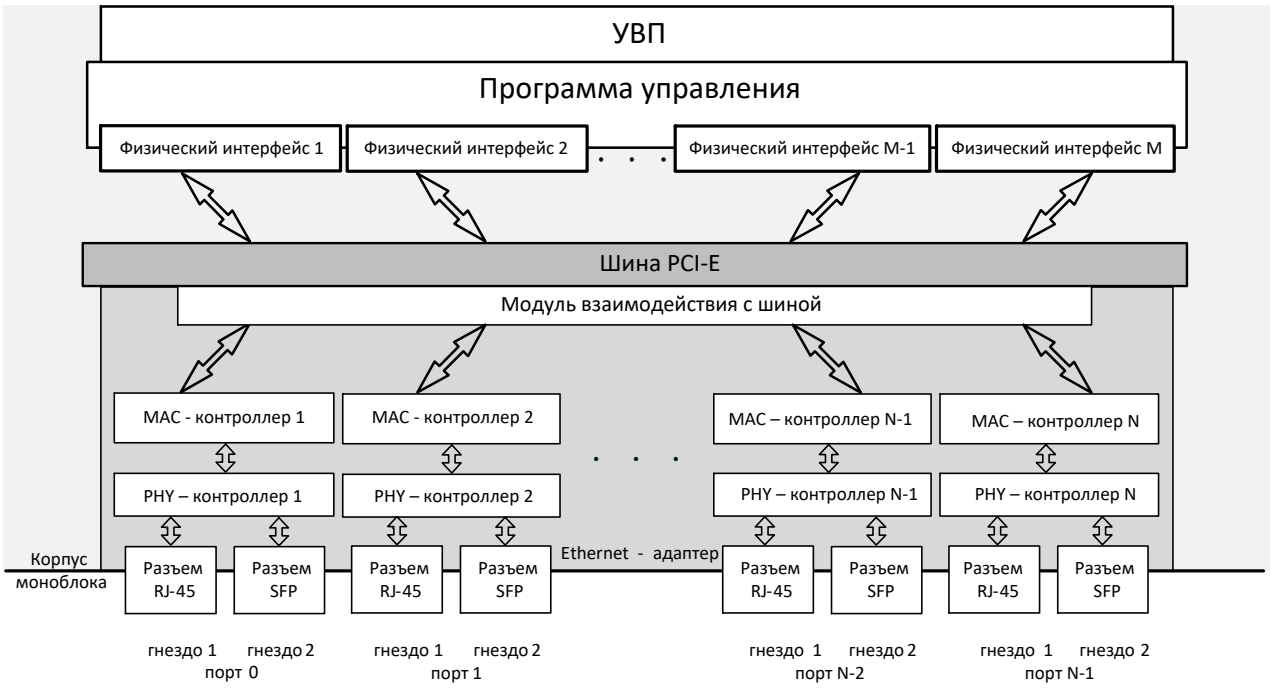


Рис. Ж.2 Схема организации обмена с применением N-портового Ethernet-адаптера изделия

Представленный на Рис. Ж.2 N-портовый Ethernet-адаптер обеспечивает работу с сетями по N (N>1) каналам связи (по N *портам*), поэтому в его составе имеется N пар MAC-контроллеров и PHY-контроллеров, а также 2N разъемов (*гнезд*) для подключения к одной и двух сетевых сред передачи данных по выбору. Модуль взаимодействия с шиной такого адаптера обеспечивает мультиплексный режим работы M интерфейсов маршрутизатора изделия по N каналам связи. Конструкция такого Ethernet-адаптера способна обеспечить функционирование количества физических интерфейсов (M) маршрутизатора изделия, равного количеству портов (N) Ethernet-адаптера.

> *Примечание.* Последнее утверждение верно в том случае, когда физическими интерфейсами, использующими порты Ethernet-адаптера такой конструкции, не применяется функция *объединения* (агрегирования) портов (подробнее см. раздел 2.3.1, Рис. 2.9, с. 29; раздел 2.3.2, Рис. 2.16, с. 34; раздел ***Приложение Б*** (с. 226) к настоящему РНУ).

Количество портов (N) в Ethernet-адаптерах, применяемых в изделиях нового поколения, может варьироваться в диапазоне от ***1*** до ***8***, а число разъемов (гнезд) в Ethernet-адаптерах – в диапазоне от ***1*** до ***16***. Тип конструкции Ethernet-адаптеров, их количество у каждого из маршрутизаторов изделия и у изделия в целом определяются назначением и конструкцией конкретного изделия, а значит количество и тип разъемов (гнезд) для подключения изделия к каналам связи и количество каналов связи (портов), по которым каждый из маршрутизаторов изделия может одновременно выполнять обмен данными, могут варьироваться в достаточно широких пределах.

Чтобы облегчить администратору выбор нужного значения параметра **Номер порта**, при изготовлении изделий выполняется *маркировка* портов изделия. Способ маркировки может варьироваться от изделия к изделию, сведения о маркировке приводятся в ЭД на конкретное изделие. Часто маркировка выполняется путем нанесения на корпус моноблока изделия (рядом с разъемом *порта* или рядом с разъемами *комбо-порта*) числа, равного значению параметра **Номер порта**, которое следует использовать при настройке соответствующего физического интерфейса маршрутизатора.

> *Внимание!* Нумерация портов изделия при маркировке выполняется для каждого маршрутизатора изделия *индивидуально*, начиная со значения ***0***. При вводе значения параметра **Номер порта** в процессе настройки физических интерфейсов используется тот же принцип нумерации портов, что и при их маркировке – нумерация портов сетевых Ethernet-адаптеров и у БВМ, и у БНМ изделия начинается со значения ***0***.

В настоящее время в изделиях применяются Ethernet-адаптеры, архитектурно-конструктивное решение которых можно отнести к одному из следующих типов:

- -однопортовый Ethernet-адаптер (классический);
- -двухпортовый Ethernet-адаптер;
- -однопортовый Ethernet-адаптер с комбо-портом;
- -двухпортовый Ethernet-адаптер с комбо-портами.

Приложение 3. Раскладки клавиатуры консоли управления

Изделием поддерживаются три набора раскладки символов по клавишам клавиатуры ЛКУ: набор символов в латинском регистре и два варианта наборов символов в регистре кириллицы – раскладка ЯВЕРТЫ или ЙЦУКЕН.

На Рис. 3.1 приведена раскладка ЙЦУКЕН регистра кириллицы для клавиатуры ЛКУ изделия.

Рис. 3.1 Раскладка ЙЦУКЕН при включении регистра кириллицы клавиатуры ЛКУ изделия

Раскладка ЙЦУКЕН на клавиатуре изделия действует после включения регистра кириллицы нажатием комбинации клавиш <Alt+F9>. При этом индикатор раскладки клавиатуры в левом верхнем углу экрана (см. Рис. 1.9, с. 16) принимает значение символа **N**.

На Рис. 3.2 приведена раскладка ЯВЕРТЫ регистра кириллицы для клавиатуры ЛКУ изделия.

Рис. 3.2 Раскладка ЯВЕРТЫ при включении регистра кириллицы клавиатуры ЛКУ изделия

Раскладка ЯВЕРТЫ на клавиатуре изделия действует после включения регистра кириллицы нажатием клавиши <F10>. При этом индикатор раскладки клавиатуры в левом верхнем углу экрана (см. Рис. 1.9 Экран Главного меню программы управления функционированием БНМ

, с. 16) принимает значение символа **R**.

> *Примечание*. Клавиши для переключения между раскладками клавиатуры в регистре кириллицы (<F10> или <Alt+F9>) можно настраивать, меняя их для удобства обслуживающего персонала местами (см. раздел 4.1.6, с. 137).

Нажатие клавиши <F9> включает латинский регистр клавиатуры изделия. Индикатор раскладки клавиатуры в левом верхнем углу экрана принимает при этом значение символа **L**.

Лист регистрации изменений

Номер изменения	Номера листов (страниц)				Всего листов (стр.) в документе	№ документа	Входящий № сопроводи-тельного документа	Подпись	Дата
	измененных	замененных	новых	аннулированных					
2		все			-	НКБГ.164-18	-		11.10.18
3		141, 152, 170			-	НКБГ.432-21	-		23.03.2021
4		141			-	НКБГ.448-21	-		24.05.2021

Итого в документе

пронумерованных листов 257.

кол-во