ООО «АМИКОН»

УТВЕРЖДЕН

ПЕРС.26.20.40.140.004РЭ-ЛУ

Криптомаршрутизатор и межсетевой экран «ФПСУ-IP Amigo» версии 4

Руководство по эксплуатации

ПЕРС.26.20.40.140.004РЭ

Листов 527

2023

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением программных и программно-аппаратных комплексов «ФПСУ-IP» (версия ПО 4.0). В документе содержатся общие сведения о комплексе «ФПСУ-IP», приведен перечень необходимых организационно-технических мер и дано описание последовательности действий при настройке параметров функционирования комплекса в процессе эксплуатации и в аварийных ситуациях.

Одним из наиболее существенных факторов, обеспечивающих нормальную работу сети под защитой комплекса «ФПСУ-IP» и требуемый уровень безопасности, является отсутствие ошибок при конфигурировании комплекса. Поэтому конфигурирование комплекса «ФПСУ-IP» должно производиться квалифицированным специалистом, хорошо знакомым с топологией сети, имеющим опыт работы с различным сетевым оборудованием и его программным обеспечением, а также внимательно изучившим принципы, методику и конкретные процедуры конфигурирования, изложенные в соответствующих разделах данного документа. Рекомендуется обратить особое внимание на примеры конфигурирования комплекса «ФПСУ-IP» для различных сетевых топологий, представленные в разделе «Примеры настройки ФПСУ-IP».

По всем вопросам и предложениям, обращайтесь непосредственно в ООО «АМИКОН». Вам всегда будут представлены консультации по телефону или электронной почте.

Отзывы и предложения по документации просьба высылать на электронную почту.

Контакты:

Наш адрес: ООО «АМИКОН», Варшавское шоссе, д. 125 (секция 1, цокольный этаж), г. Москва, 117587.

Телефон и факс: +7-(495)797-64-12, +7-(495)797-64-13.

Адрес в Интернет: https://www.amicon.ru/

Электронная почта: info@amicon.ru

Веб-форум ООО «АМИКОН»: https://forum.amicon.ru

Мы работаем с 10:00 до 19:00 по московскому времени, кроме субботы и воскресенья.

Под явной компрометацией ключевой информации далее понимается хищение, утрата или временная потеря ключевого носителя, обнаружение следов взлома ключевого носителя.

В случае явной компрометации ключевой информации необходимо немедленно после выявления произвести действия, описанные в пункте далее, для каждого случая компрометации.

Под неявной компрометацией ключевой информации далее понимается подозрение на несанкционированное копирование информации с ключевого носителя, увольнение работников, имевших доступ к ключевым документам, выявление нарушений правил хранения ключевых носителей, нарушение пломбировки хранилищ ключевых носителей, любые случаи неработоспособности ключевых носителей.

Случаи неявной компрометации ключевой информации необходимо рассматривать в каждом случае отдельно и принимать решение о наличии или отсутствии компрометации исходя из результатов проведения разбирательства, проводимого в соответствии с требованиями политики безопасности, принятой в организации в области неявной компрометации ключевой информации.

Запрещается устанавливать ключевую информацию, скомпрометированную в процессе транспортировки.

При обнаружении попытки несанкционированного доступа к техническим средствам, на которых эксплуатируется ФПСУ-IP, необходимо переустановить операционную систему и ПО ФПСУ-IP, считать что скомпрометирована вся ключевая информация (и выполнить все следующие действия, описанные в пунктах компрометации каждого вида ключевых данных).

Компрометация ключа запуска:

Компрометация ключа запуска (ключевые данные в ТМ-идентификаторе) возможна при его хранении на отчуждаемых носителях. В этом случае необходимо средствами ФПСУ-IP немедленно исключить возможность работы ФПСУ-IP с данным ключом (см. пункт «Регистрация ТМ-идентификаторов»); при компрометации ключа запуска главного администратора необходимо переустановить ПО ФПСУ-IP.

Компрометация ключа запуска возможна при несанкционированном доступе к внутреннему накопителю при эксплуатации изделия с активированной подсистемой автозапуска, в этом случае при переустановке ПО ФПСУ-IP произойдет замена ключей запуска.

Компрометация парно-выборочных ключей:

Компрометация парно-выборочных ключей (ключевые данные полученные от ЦВК) возможна при хранении их на отчуждаемых носителях, если после установки их на внутренний носитель изделия, они были оставлены для аварийного восстановления (см. пункт «Восстановление работы ФПСУ-IP после сбоев». В этом случае, а также если стало известно о компрометации в ходе транспортировки, предусматривается следующий порядок действий:

1. Прекратить использование на ФПСУ-IP и взаимодействующих с ним ФПСУ-IP скомпрометированных ключей (см. пункт «Использование ключей»);

2. Установить новые или резервные (при условии их получения на не скомпрометированном носителе) парно-выборочные ключи и возобновить взаимодействие с ФПСУ-IP на новых ключах (см. пункт «Использование ключей»).

Компрометация парно-выборочных ключей возможна при несанкционированном доступе к внутреннему накопителю при эксплуатации ФПСУ-IP с активированной подсистемой автозапуска, в этом случае после переустановки ПО ФПСУ-IP следует установить новые или резервные парно-выборочные ключи и возобновить взаимодействие с ФПСУ-IP на новых ключах.

Компрометация общесистемного ключа:

Компрометация общесистемных ключей возможна при несанкционированном доступе к внутреннему накопителю при эксплуатации изделия с активированной подсистемой автозапуска, в этом случае, а также если стало известно о компрометации в ходе транспортировки, предусматривается следующий порядок действий:

1. Прекратить использование на ФПСУ-IP скомпрометированных ключей (см. пункт «Установка и удаление общесистемных ключей») и взаимодействующих с ними ФПСУ-IP/Клиентов на скомпрометированном ключе;

2. Установить новые общесистемные ключи (см. пункт «Установка и удаление общесистемных ключей») и заменить используемые ФПСУ-IP/Клиентами ключи клиентов, сформированные на основе скомпрометированного общесистемного.

Компрометация ключей для связи с АРМ УА:

Компрометация ключей для связи с АРМ УА (секретного ключа ФПСУ-IP и открытого ключа АРМ УА) возможна при несанкционированном доступе к внутреннему накопителю ФПСУ-IP при эксплуатации ФПСУ-IP с активированной подсистемой автозапуска, в этом случае, а также если стало известно о компрометации в ходе

Требования к программному обеспечению:

На технических средствах, оснащенных программным обеспечением из состава средств защиты семейства ФПСУ-IP, должны быть выполнены следующие требования:

- должны использоваться антивирусные средства в ОС Терминала и хостовой ОС (при эксплуатации ФПСУ-IP в гостевой ОС);
- должно использоваться только лицензионное ПО фирм-производителей. В случае необходимости использования иного программного обеспечения, его применение должно быть санкционировано администратором безопасности. В любом случае стороннее ПО не должно содержать средств разработки и отладки приложений, а также содержать в себе возможностей, позволяющих оказывать воздействие на функционирование ПО из состава средств защиты семейства ФПСУ-IP (требование для Терминала или хостовой ОС (при эксплуатации ФПСУ-IP в гостевой ОС));
- необходимо регулярно устанавливать пакеты обновления безопасности (Service Packs), обновлять антивирусные базы (требование для Терминала и хостовой ОС (при эксплуатации изделия ФПСУ-IP в гостевой ОС));
- при подключении к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов (например, JavaScript, VBScript, ActiveX) без проведения соответствующих проверок на предмет содержания в них вирусов (при эксплуатации ФПСУ-IP в гостевой ОС);
- должна быть установлена только одна операционная система, в том числе хостовая, правом установки и настройки которой должен обладать только администратор; при использовании виртуальных сред необходимо исключить одновременную работу в хостовой ОС нескольких пользователей, если в гостевых ОС запущены ФПСУ-IP;
- должна быть отключена возможность удаленного управления операционной системой, в том числе хостовой и гостевыми;
- необходимо предусмотреть меры, максимально ограничивающие доступ к ресурсам системы (системному реестру, файлам и каталогам, временным файлам, журналам системы, файлам подкачки, кэшируемой информации), неиспользуемые протоколы, сервисы и службы рекомендуется отключить (для Терминала и хостовой ОС (при эксплуатации ФПСУ-IP в гостевой ОС)).

Дополнительно на технических средствах, оснащенных Терминалом, функционирующих под управлением ОС Windows 10/Server 2016/Server 2019, или если хостовая ОС является одной из перечисленных ОС (при эксплуатации изделия ФПСУ-IP в гостевой ОС) необходимо реализовать следующие меры:

1. Проверить наличие и статус сервиса DiagTrack (Панель управления -> Система и

ознакомленным с изложенными в данном пункте правилами пользования изучившим эксплуатационную документацию на ФПСУ-IP;

2. Запретить разглашение содержимого ключевых носителей и передачу самих носителей лицам, к ним не допущенным, а также выводить ключевую информацию на дисплей и принтер;

3. Запретить использование ключевых носителей в режимах, не предусмотренных эксплуатационными документами на ФПСУ-IP, либо использовать ключевые носители на сторонних аппаратных средствах;

4. Запретить запись на ключевые носители посторонней информации;

5. Запретить оставлять без контроля вычислительные средства, на которых эксплуатируются средства защиты семейства ФПСУ-IP после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки (для Терминала и хостовой ОС (при эксплуатации ФПСУ-IP в гостевой ОС)).

6. При установке параметров, позволяющих создавать соединения отличные от криптографически защищенных (выбор режимов «запрещено» или «нежелательно» в настройках «Криптозащита», пункт «Описание параметров удаленных ФПСУ-IP», режим «Ретрансляция»), должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации или с объектов информатизации в защищаемой локальной вычислительной сети. Проверка достаточности принятых мер защиты проводится при аттестации объекта информатизации с установленным ФПСУ-IP по требованиям информационной безопасности.

Организационно-технические меры защиты от НСД:

1. В Терминале и хостовой ОС (при эксплуатации ФПСУ-IP в гостевой ОС) для класса КС1 перед началом работы ФПСУ-IP, пользователь должен осуществлять контроль целостности ПО программой контроля целостности, входящей в состав ФПСУ-IP. В состав модулей программного обеспечения, подлежащих проверке, должны быть включены исполняемые модули операционной системы, Терминала и гипервизора, а также его конфигурационные файлы. Перед первым запуском ПО Терминала необходимо сверить контрольные суммы, находящиеся в файле с эталонными контрольными суммами. Перед первым использованием гипервизора, необходимо рассчитать эталонные контрольные суммы на ПО гипервизора и настройки гипервизора (конфигурационные файлы) программой контроля целостности fpsuhash, входящей в состав средства защиты семейства ФПСУ-IP. Если в процессе работы программы будет обнаружено несовпадение контрольных

ключей.

Процедура аутентификации пользователя выполняется при включении ФПСУ-IP и каждый раз, когда при локальном администрировании ФПСУ-IP пользователь выполняет команду интерфейса, требующую идентификации и аутентификации пользователя. От пользователя требуется предъявить ТМ-идентификатор, на котором находятся являющиеся аутентификатором ключевые данные пользователя, одним из следующих способов (с учетом вида ТМ-идентификатора):

- iButton – прислонить к ТМ-считывателю ФПСУ-IP устройство iButton;
- TM-Key – подключить к USB порту ФПСУ-IP устройство TM-Key.

Подсистема аутентификации ФПСУ-IP считает с предъявленного ТМ-идентификатора аутентификационный ключ и, при успешной проверке, пользователь авторизуется на ФПСУ-IP с правами, закрепленными за предъявленным ключом.

При эксплуатации ФПСУ-IP с активированной подсистемой автозапуска, ряд требующих аутентификацию действий выполняется автоматически без предъявления ТМ-идентификатора, с использованием аутентификационного ключа, хранящего на внутреннем носителе ФПСУ-IP (подробнее о работе подсистемы автозапуска и разрешенных к автоматической аутентификации действиях см. пункты «Запуск ФПСУ-IP», «Окно состояния работы пользователей», «Окно состояния подсистемы «горячего» резервирования», «Меню управления ключами УА», «Включение автозапуска ФПСУ-IP», «Отключение автозапуска»).

2. Аутентификация пользователя ФПСУ-IP с использованием символьного пароля.

ФПСУ-IP должен быть настроен на использование аутентификации по символьному паролю условно-постоянного действия, при этом каждый раз при прохождении аутентификации пользователю должен помимо предъявления ТМ-идентификатора, ввести символьный пароль.

При работе ФПСУ-IP с активированной подсистемой автозапуска, ввод пароля происходит автоматически, с использованием пароля, хранящего на внутреннем носителе ФПСУ-IP (разрешены к автоматической аутентификации те же действия, что указаны в пункте 1.).

Если символьный пароль указан неверно, пользователю будет отказано в авторизации на ФПСУ-IP.

Удаленные администраторы не могут устанавливать или изменять символьный пароль.

3. Аутентификация средствами АПМДЗ.

Рисунок 1 - Настройки Proxy

3. 6. 2. TCP URG Pointer

Для противодействия данной атаке необходимо настроить правила фильтрации некорректных комбинаций флагов протокола TCP («Дополнительные параметры и защита от flood-атак»):

Рисунок 5 - Изменение общих свойств правила

3. 8. Гарантийные обязательства

Производитель (ООО «АМИКОН») гарантирует соответствие ФПСУ-IP требованиям технических условий при соблюдении потребителем условий и правил эксплуатации, транспортирования и хранения (см. пункт «Технические условия эксплуатации и хранения»).

Гарантийный срок эксплуатации ФПСУ-IP – 12 месяцев (возможен больший срок, если это определено договором на поставку или лицензионным соглашением) со дня передачи его потребителю (пользователю), включая срок хранения, с периодической перепроверкой ФПСУ-IP (визуальная оценка отсутствия механических повреждений, подсчет контрольных сумм файлов дистрибутива) один раз в год на объекте эксплуатации.

При обнаружении дефекта в ФПСУ-IP до истечения гарантийного срока эксплуатации при соблюдении пользователем условий и правил транспортирования, хранения и эксплуатации производитель обязуется произвести ремонт или замену на свое усмотрение.

Действие гарантийных обязательств на выполнение защитных функций ФПСУ-IP прекращается, если потребителем внесены изменения в ФПСУ-IP без согласования с производителем. Гарантийные обязательства не распространяются на копии ФПСУ-IP, изготовленные по инициативе потребителя.

Производитель принимает на себя обязательства по поиску ошибок реализации и уязвимостей в ФПСУ-IP на протяжении всего его жизненного цикла, а также обязательства по своевременному информированию потребителя о найденных ошибках и уязвимостях, методах безопасного применения ФПСУ-IP.

Гарантия не распространяется на изделия, вышедшие из строя:

- по вине его владельца вследствие нарушения условий эксплуатации и/или хранения;
- из-за неправильной эксплуатации или применения в целях, не предусмотренных функциональным назначением устройства;
- из-за несоблюдения указаний, приведенных в данном документе или возникшие в результате воздействия окружающей среды (дождь, снег, град, гроза и т. п.);
- наступления форс-мажорных обстоятельств (пожар, наводнение, землетрясение и др.);
- из-за небрежного обращения и дефектов, вызванных попаданием внутрь аппаратного обеспечения посторонних предметов, веществ, жидкостей, насекомых и т. д;
- при наличии механических внешних дефектов (явные механические повреждения, трещины, сколы на корпусе или внутри устройства, сломанные контакты разъемов);

пакетов, введите в строке терминала:

```
sudo apt update
```

Для установки пакетов библиотеки, введите в строке терминала:

```
sudo apt install qemu-kvm libvirt-clients libvirt-daemon-system bridge-utils virt-manager
```

qemu-kvm – эмулятор с открытым исходным кодом и пакет виртуализации, обеспечивающий аппаратную эмуляцию.

libvirt-daemon-system – файлы конфигурации для демона libvirt.

libvirt-clients – программное обеспечение позволяющее управлять виртуализацией.

bridge-utils – инструменты командной строки для настройки Ethernet мостов.

virtinst – инструменты командной строки для создания и модификации виртуальных машин.

virt-manager – графический интерфейс для управления виртуальными машинами через демон libvirt.

3. После установки пакетов необходимо настроить доступ к управлению виртуальной машиной. Добавить группу libvirtd и добавить пользователя в эту группу для управления виртуальными машинами. Данный пользователь получит доступ к расширенным сетевым опциям. Введите команды в терминале:

```
sudo groupadd libvirtd
sudo adduser $USER libvirtd
```

Если в качестве пользователя выбран текущий, потребуется выйти из системы и войти снова, чтобы применить новое членство в группе.

Проверить членство в группе можно командой:

```
groups <имя пользователя>
```

4. Включите поддержку встроенного ПО UEFI для виртуальной машины QEMU/KVM, установиив пакет ovmf:

```
sudo apt install ovmf
```

5. Для автоматизации процесса установки ОС используется утилита virt-install, могут быть использованы preseeds, kickstart и пр. Утилита virt-install является частью пакета virtinst. Данный пакет был установлен в пункте 2.

Запустите гостевую операционную систему ФПСУ-IP в виртуальной машине

Рисунок 20 - Оперативная память виртуальной машины

3. В настройках процессора количество ядер для виртуальной машины устанавливается исходя из лицензии ФПСУ-IP.
4. Для процессоров включите поддержку виртуализации – флаг «VirtualizeVT-x/EPT or AMD-V/RVI».

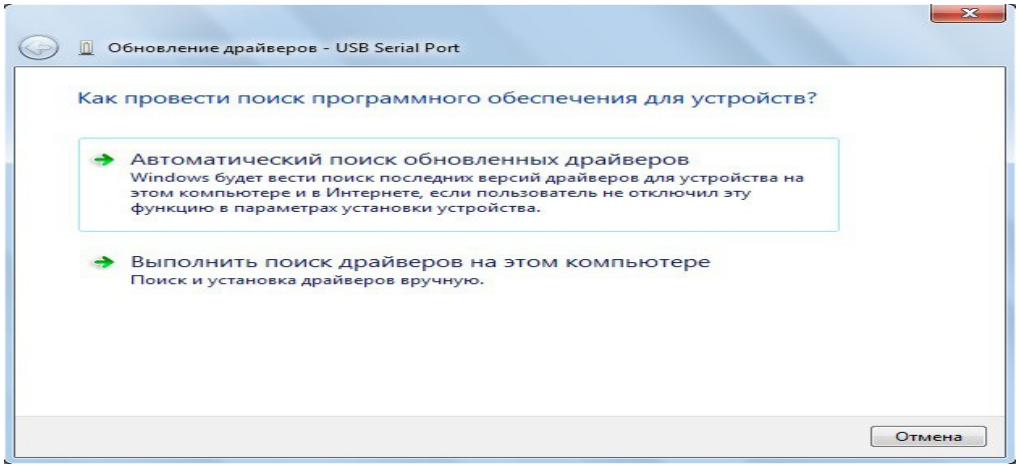

Рисунок 21 - Настройки процессора

5. Добавьте виртуальный жесткий диск объемом 1 GB, выберите контроллер

виртуального жесткого диска – «IDE». В ОС ФПСУ-IP поддерживается только данный контроллер.

6. Задайте минимум 2 сетевых адаптера, как показано на рисунке выше. Для корректной работы виртуальной машины рекомендуется заменить драйвера сетевых адаптеров. Для VMware EsXi в настройках сетевых адаптеров выберите драйвер «vmxnet3». Для VMware Workstation Pro/VMware Workstation после завершения процесса создания виртуальной машины внесите изменения в файл с расширением .vmx из каталога виртуальной машины, как указано в пункте 10.
7. Для подключения TM-Key, VPN-Key, USB-носителей добавьте устройство USB-контроллер, если не установлено по умолчанию.
8. Добавьте устройство дисплей, если не установлено по умолчанию.
9. Для VMware EsXi/VMware Workstation Pro выберите на вкладке «Options» пункт «Advanced». Установите тип встроенного ПО - «UEFI».

Рисунок 22 - Настройки интерфейса прошивки

Для VMware Workstation после завершения процесса создания виртуальной машины внесите изменения в файл с расширением .vmx из каталога виртуальной машины, как указано

в пункте 11.

Закройте окно настроек и завершите создание виртуальной машины.

10. Для VMware Workstation Pro/VMware Workstation измените в конфигурации виртуальной машины драйвер сетевых адаптеров. Откройте для редактирования файл с расширением .vmx из каталога виртуальной машины, для каждого адаптера в свойстве «virtualDev» задано значение по умолчанию «e1000», найдите строки с этим значением и замените его на «vmxnet3»:

```
ethernet0.virtualDev = "vmxnet3"
ethernet1.virtualDev = "vmxnet3"
```

Сохраните файл.

11. Для VMware Workstation измените в конфигурации виртуальной машины тип встроенного ПО «UEFI». Откройте для редактирования файл с расширением .vmx из каталога виртуальной машины, добавьте в середину файла (например после параметра mem.hotadd) строку:

```
firmware = "efi"
```

Сохраните файл.

Создание виртуальной машины закончено.

Описание процедуры установки ПО ФПСУ-IP находится в разделе «Установка ПО ФПСУ-IP с установочного носителя».

3. 10. Консольное подключение к ФПСУ-IP

Локальное управление ФПСУ-IP, обычно выполняемое с помощью подключаемых напрямую монитора и клавиатуры, может осуществляться от рабочей станции под управлением ОС Windows или Linux, с помощью консольного подключения через COM-порт. Консольное подключение должно выполняться программой PuTTy версии 0.70 сборки ООО «АМИКОН» (далее - Терминал).

Требуемое оборудование:

Для консольного подключения к ФПСУ-IP потребуется (опционально, если на рабочей станции нет COM-порта) кабель-переходник USB-COM, и следующее дополнительное оборудование, в зависимости от аппаратной платформы:

1. FPSUIP-STD, FPSUIP-EXT, FPSUIP-ORD, FPSUIP-ULT - консольный кабель для RJ45 интерфейса;
2. ФПСУ-IP на базе аппаратной платформы типоразмера 2U и 1U (FPSUIP-STD-2U,

Рисунок 32 - Выбор каталога с драйвером

После успешной установки драйвера консольный кабель должен обнаруживаться системой как «USB Serial Port» в группе устройств «Порты (COM и LPT)».

Рисунок 33 - Обновление драйвера консольного кабеля

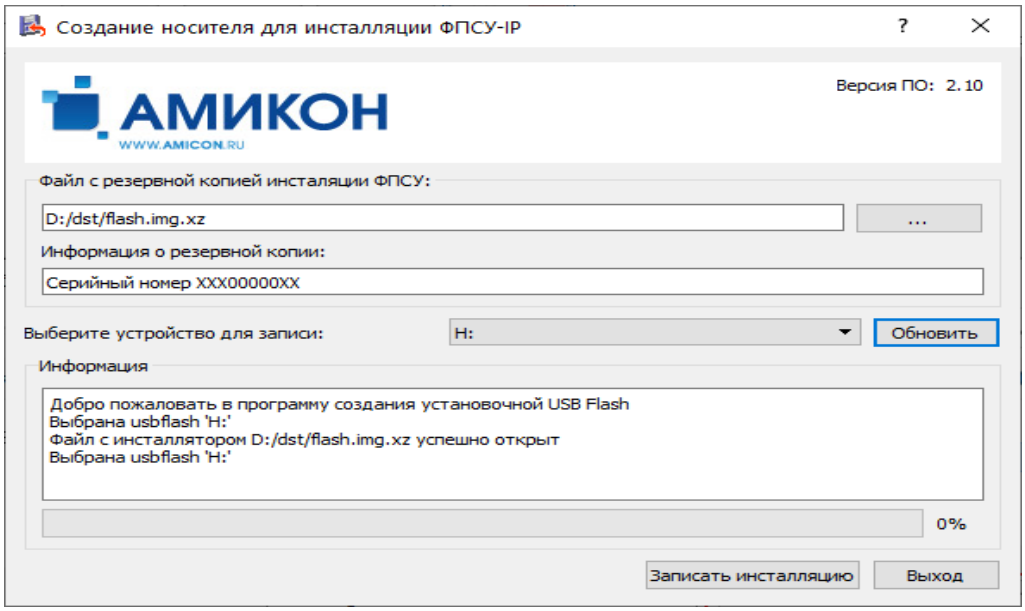

Рисунок 35 - Отображение консольного кабеля в диспетчере устройств

В диалоговом окне мастера установки выберите поиск драйверов на этом компьютере и укажите каталог с драйвером. Система установит драйвер и выдаст сообщение об успешном обновлении.

Рисунок 36 - Мастер установки драйвера

После успешной установки драйвера консольный кабель должен обнаруживаться системой как «USB-SERIAL CH340» в группе устройств «Порты (COM и LPT)».

Рисунок 41 - Выбор типа клавиатуры

Выберите кодировку UTF-8 (устанавливается в интерфейсе PuTTY: Window-Translation-Remote Character Set).

Рисунок 43 - Выбор количества строк

Нажмите «Open» для запуска соединения. Откроется консоль с интерфейсом управляемого ФПСУ-IP.

Рисунок 44 - Консольное подключение установлено

3. 11. Установка ПО ФПСУ-IP с дистрибутива

Программно-аппаратный комплекс ФПСУ IP поставляется предустановленным на аппаратную платформу. Описанные ниже процедуры установки программного обеспечения ФПСУ-IP используются в случае необходимости выполнения повторной установки программного обеспечения ФПСУ IP на аппаратную платформу.

Для установки программного обеспечения ФПСУ-IP с дистрибутива на аппаратную платформу администратору потребуются следующие компоненты, входящие в комплект поставки ФПСУ-IP:

- ПО записи дистрибутива ПАК «ФПСУ IP» на USB (утилита restore.exe);
- ПЭВМ под управлением операционной системы семейства Windows для запуска утилиты restore.exe, с возможность считать дистрибутивный носитель (CD-диск или USB-flash) и поддержкой USB 2.0 (консоль управления);
- Дистрибутивный носитель (CD-диск или USB-flash) с файлами:

Подтвердите продолжение установки выбором команды «Да»:

Рисунок 52 - Очистка ПЗУ ФПСУ-IP

4. После успешного завершения форматирования ПЗУ ФПСУ-IP, будет выдано служебное оповещение о завершении первого этапа установки программного обеспечения. Далее необходимо выполнить инструкции, перечисленные в оповещении:

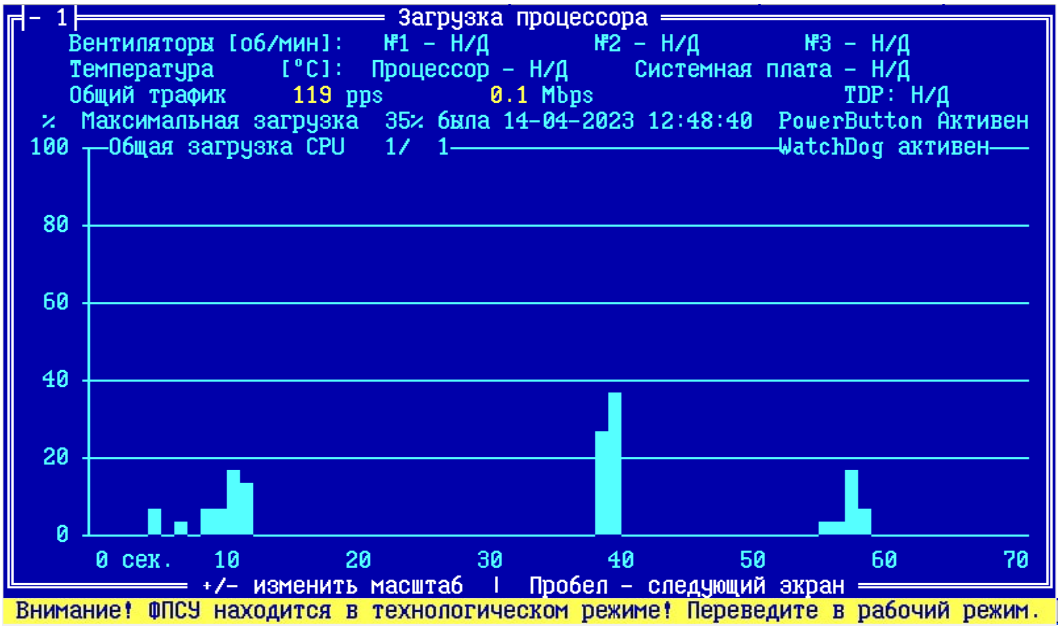

Рисунок 53 - Завершение первого этапа установки

5. После перезагрузки и запуска операционной системы ФПСУ-IP, начнется второй этап установки программного обеспечения. Для продолжения потребуется подтвердить полномочия Главного администратора (права роли *«Администратор»* класса *«Главный администратор»*, см. раздел «Общие сведения», таблица 1*)*, приложив ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-IP (или подключив USB ТМ-идентификатор к USB-порту ФПСУ-IP):

После завершения копирования системных файлов на ПЗУ комплекса, ***установка программного обеспечения комплекса завершается***. ФПСУ-IP будет перезагружен, и после перезагрузки начнет работать в технологическом режиме (см. пункт. «Технологический режим ФПСУ-IP»).

ВНИМАНИЕ! После перезагрузки ФПСУ-IP, до настройки сетевых адаптеров и до выполнения перехода из «Технологического режима» в «Рабочий», необходимо установить серийный номер для данного экземпляра ФПСУ-IP через подсистему установки обновлений!

Процедуру установки ПО ФПСУ-IP с USB-носителя на АП ФПСУ-IP или в виртуальную машину необходимо повторить для экземпляра ФПСУ-IP, который будет работать с основным в режиме «горячего резервирования». Порядок установки будет во всем совпадать с ранее описанным, кроме шага выбора «Режима функционирования устанавливаемого комплекса», где потребуется сделать выбор «Горячий резерв».

3. 11. 3. Установка ФПСУ-IP с готового образа диска на USB-носителе в QEMU/KVM

Установка ПО ФПСУ-IP с готового образа диска на USB-носителе в виртуальную среду заключается в подключении USB-носителя к виртуальной машине QEMU/KVM, последующего запуска виртуальной машины QEMU/KVM, и дальнейшего следования предложениям мастера установки.

Запустите виртуальную машину, нажав на зеленый треугольник (на рисунке QEMU/KVM 4.2.1 на Ubuntu 20.04.05 LTS).

4. Запуск и режим фильтрации ФПСУ-IP

После включения питания и проведения диагностических тестов BIOS, на экран будет выдан запрос на подтверждение права доступа пользователя к работе с ФПСУ-IP, сопровождаемый звуковым сигналом, замещающим экранную выдачу запроса в случае отсутствия монитора. Прижмите к контактному устройству зарегистрированный на ФПСУ-IP ТМ-идентификатор (или подключите USB ТМ-идентификатор к USB-порту ФПСУ-IP) с правами *«Оператор»* или выше. В случае успешной идентификации будет выдан звуковой сигнал, BIOS продолжит работу и ПО ФПСУ-IP будет загружено.

Если ФПСУ-IP уже сконфигурирован и параметры его работы установлены, система через несколько секунд автоматически осуществит перевод ФПСУ-IP в режим фильтрации пакетов.

В случае локального администрирования (наблюдения за процессами фильтрации пакетов сетевого уровня, установки или изменения правил фильтрации, регистрации удаленных администраторов, настройки параметров сетевых адаптеров и т.д.) к ФПСУ-IP должна быть подсоединена консоль, или монитор и клавиатура.

Если последовал отказ от запуска режима фильтрации (для изменения параметров конфигурации или настройки системы), будет осуществлен выход в главное меню ФПСУ-IP. Выход в главное меню будет осуществлен также и при выходе из режима отображения работы подсистемы фильтрации.

Главное меню имеет вид, представленный на рисунке ниже, и содержит команды для настройки системы, конфигурирования оборудования, установки режимов работы и настройки параметров фильтрации. Выбор каждой команды повлечет за собой запрос на идентификацию допущенного лица и проверку его прав доступа (с предъявлением ТМ-идентификатора) на запрашиваемые действия (права допущенных лиц различных классов, см. раздел «Общие сведения», таблица 1).

Рисунок 72 - Справочное меню

Меню «Справка» содержит следующие пункты:

- «Клавиши управления» - отображаются данные о функциональных клавишах и их назначении (см. пункт «Запуск ФПСУ-IP»);
- «Информация о версиях» - отображаются данные о версии и номере и дате сборке ПО ФПСУ-IP, модели материнской платы, аппаратной платформе, архитектуре ЦПУ;
- «Информация об установленных подсистемах» - отображаются данные об установленных подсистемах (горячий резерв, поддержка IP-клиентов и др.), серийном номере ФПСУ-IP, а также количестве лицензированных ядер процессора ФПСУ-IP;
- «Информация об аддонах» - отображаются данные об установленных дополнениях (dhcp, http-proxy); подробное описание настройки дополнений в конфигурации ФПСУ-IP приводится в пунктах «DHCP-Relay», «Http-proxy ФПСУ-IP»;
- «Информация о продукте» - отображаются данные о Разработчике.

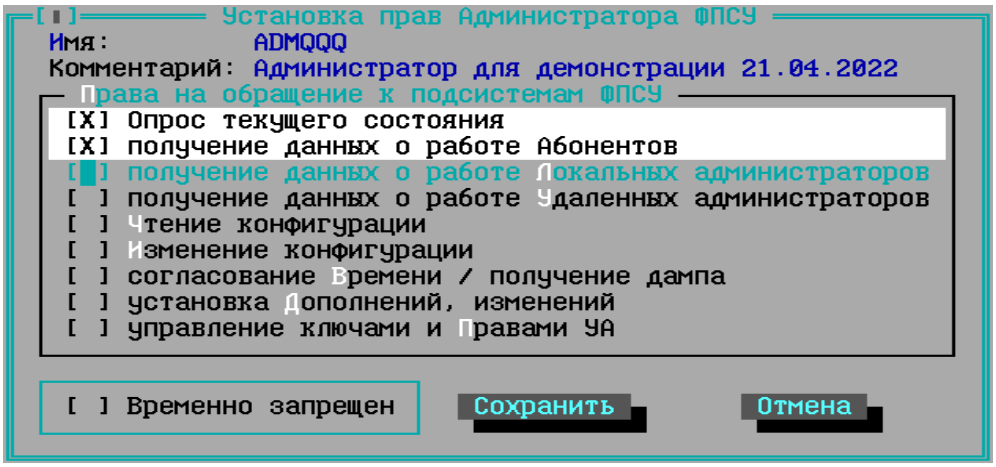

Рисунок 73 - Информация о версиях

аппаратуры пулов может быть несколько. ФПСУ-IP назначает пул каждому порту. Двум разным портам может быть назначен один и тот же общий пул, а могут быть назначены и разные пулы.

Когда ФПСУ-IP получает фрейм, для него выделяется часть памяти из пула, в зависимости от стадии обработки фрейм проходит несколько стадий: Буфер приёма, Буфер обработки и Буфер передачи, после отправки фрейма часть памяти освобождается и снова попадает в пул.

Для буферов выводится два значения. Первое значение буфера - сколько фреймов находится в очереди на данной стадии (0 - буфер пустой, нет фреймов в очереди), второе значение - размер буфера, максимально возможное количество фреймов, обрабатываемых на данной стадии.

В целях оптимизации скорости работы освобождённая часть память может быть кэширована и не попасть обратно в пул, такая часть памяти не отображается, поэтому количество свободных фреймов в пуле может быть меньше размера пула, даже если ФПСУ-IP простаивает.

Кроме состояния портов ФПСУ-IP, из данного окна доступен последовательный переход на два дополнительных экрана состояния, «Использование памяти» и «Мониторинг сетевых портов».

По нажатию клавиши *<Пробел>* осуществляется переход в окно «Использование памяти»:

Рисунок 80 - Использование памяти ФПСУ-IP

В окне выводится сведения о выделенной оперативной памяти для сетевых адаптеров и для служб межсетевого экрана ФПСУ-IP в мегабайтах.

По нажатию клавиши *<Пробел>* осуществляется переход в окно «Мониторинг сетевых портов»:

Рисунок 81 - Мониторинг сетевых портов ФПСУ-IP

Для каждого сетевого порта выводится номер сетевого адаптера адаптера, скорость соединения, в слоте указаны параметры PCI-порта (bus:device.function), состояние сетевого адаптера (рабочее - OK), IP-адрес порта и описатели VLAN.

По нажатию клавиши *<Пробел>* осуществляется переход в окно «Мониторинг SFP модулей»:

Рисунок 82 - SFP мониторинг ФПСУ-IP

При использовании модуля SFP мониторинг позволяет следить за состояние сетевого кабеля, отображает состояние и рабочие параметры модуля SFP в реальном времени. Если на ФПСУ-IP настроены протоколы SysLog и/или SNMP, в случае проблемы с SFP-модулем, ФПСУ-IP отправит сообщение о превышении порогового значения на сервер SysLog, параметры и состояние SFP-модуля регистрируются на сервере SNMP.

4. 6. Окно состояния ARP-кэша

Выход в описываемый режим осуществляется по нажатию клавиши *<F4>*, после чего на экран монитора будет выдана информация о состоянии работы ARP-протокола для обоих рабочих портов ФПСУ-IP. По умолчанию выводится информация по первым двум портам, зарезервированным в ОС ФПСУ-IP под номерами 1 и 2. Для переключения и отображения информации по другому порту следует воспользоваться комбинацией клавиш <Ctrl + > > и <Ctrl + < >.

В окне режима для каждого из портов представлен список записей, находящихся в ARP-кэше в текущий момент времени. Каждая запись имеет следующий вид:

Номер VLAN и символ «:» (если запись участвует в VLAN)	MAC-адрес (если найден)	IP-адрес, для которого ищется ARP-адрес	Время, оставшееся до вытеснения записи из списка	Состояние записи

Запись может находиться в следующих состояниях (последнее поле):
***F** (Find)* - начата процедура определения MAC-адреса IP-абонента;
***D** (Dyn)* - MAC-адрес для соответствующего IP-адреса определен и запись будет вытеснена по истечении указанного времени, указанный IP-адрес является IP адресом явно описанного в конфигурации ФПСУ-IP маршрутизатора или другого ФПСУ-IP;
***A** (Auto)* - MAC-адрес для соответствующего IP-адреса определен и запись будет вытеснена по истечении указанного времени;
***C** (Check)* — начата процедура проверки соответствия IP адреса и MAC адреса данной записи ввиду истечения времени состояний Dyn или Auto;
***B** (BadFind)* - процедура поиска закончилась отрицательно, запись будет вытеснена по истечении указанного времени;
***S** (Static)* - для IP адреса задан статический MAC адрес, указанный в строке.

Рисунок 83 - Состояние ARP-кэша

Цифры внизу («000005» и «000010» на рисунке) означают общее количество записей в

ARP-кэше для каждого порта.

Перемещение по списку записей осуществляется при помощи клавиш управления курсором < > и <v>, а между половинами окна - при помощи клавиш <*Tab*>, << > и <> >.

Нажатие клавиши <*Del*> вызывает процедуру обновления ARP-кэша на ФПСУ-IP.

4. 7. Окно состояния работы пользователей

Для просмотра состояния работы абонентов нажмите <F5>. В открывшемся окне отображается регистрационная информация, представленная записями следующего вида:

ФПСУ	IP-адрес абонента	IP-адрес абонента	ФПСУ	Количество байт для порта 1	Количество байт для порта 2	Err

В записи указываются IP-адреса абонентов, между которыми происходит обмен пакетами, признак работы через ФПСУ-IP (для левого адреса - с левой стороны, для правого адреса - с правой стороны), количество в байтах переданной и полученной информации для первого и второго порта и признак ошибки (если она имела место).

Записи добавляются в конец списка, по мере добавления новых записей некоторые записи будут вытесняться (передвижения по строкам осуществляется с помощью клавиш управления курсором < > и <v>).

В нижней части экрана для записи, на которую установлен курсор, отображаются дополнительные сведения. Они разбиты на две половины, относящиеся к каждому порту. Указывается количество пакетов, принятых на обработку с данного порта, количество отказов, согласованное использование сжатия и криптозащиты и время последнего обмена пакетами между данными абонентами.

Сбой LAN карты	- сбой LAN-адаптера. При повторении ошибки требуется локальное администрирование LAN-адаптеров;
Ошибка фрагментации	- длина полученного фрагмента фрагментированного пакета больше допустимой. Пакет будет сброшен;
Отмена фрагментации	- необходима фрагментация для дальнейшей передачи пакета, но стоит флаг запрета фрагментации;
Абонент через ФПСУ	- абонент в конфигурации портов ФПСУ-IP указан как работающий в режиме ретрансляция, но пакеты от него приходят из VPN-туннеля от другого ФПСУ-IP;
Запрет SourceRoute	- было сброшен пакет с опцией SourceRoute: в общих параметрах конфигурации ФПСУ-IP стоит запрет передачи пакетов с опцией SourceRoute;
Ошибочный фрагмент	- ошибка фрагментации удаленной станции;
Неверен список опций	- неверен список опций IP заголовка;
Нет ФПСУ-туннеля	- невозможно передать пакет в VPN-туннель, т.к. VPN-туннель между двумя ФПСУ не согласован;
Ошибочный ФПСУ-пакет	- ошибочный пакет от ФПСУ-IP, отправитель присылает пакет, обозначенный как пакет протокола взаимодействия между ФПСУ-IP, но структура пакета содержит ошибки.

Если на экране статистики переданных IP-пакетов нажать клавишу <*Tab*>, то выводится окно текущих соединений, которые находятся в таблице состояний межсетевого экрана ФПСУ-IP.

В строке соединения предоставляются следующие сведения о соединении:

- IP-адрес и порт (если применимо) источника соединения;
- IP-адрес и порт (если применимо) назначения соединения;
- протокол соединения;
- название правила межсетевого экрана, которое разрешает текущее соединение.

- *«Готов»* - туннель установлен и по нему происходит обмен служебной информацией.
- *«Нет связи»* - туннель между двумя ФПСУ-IP не может быть установлен: удаленный ФПСУ-IP выключен или на на нём не запущена подсистема фильтрации.
- *«Нет связи (не согласован ключ)»* - канал связи не может быть установлен по причине ошибки аутентификации, необходимо переустановить ключи (см. пункт «Параметры «Горячего резерва»»).
- *«Нет связи (ошибка установки)»* - канал связи не может быть установлен по причине ошибочных установок (например, различных MAC-адресов для соответствующих портов партнеров).

По каждому VPN-туннелю «горячего резерва» отображается статистическая информация по обработанным пакетам, пришедшим по этому туннелю:

- *«Передано»* - количество переданных пакетов от этого ФПСУ-IP в данный VPN-туннель «горячего резерва»;
- *«Принято»* - количество корректно принятых пакетов от удаленного ФПСУ-IP через данный VPN-туннель «горячего резерва»;
- *«Ошибочных»* - количество принятых пакетов от удаленного ФПСУ-IP через данный VPN-туннель «горячего резерва», которые были сброшены на этом ФПСУ-IP. Причиной сброса может быть несоответствие пакета протоколу или искажение содержимого пакета.

Если хотя бы один VPN-туннель находится в состоянии «*Готов»* – на экране отображается текущее время партнера ФПСУ-IP по резервированию.

Здесь же выводятся данные о состоянии местного и удаленного (если он на связи) ФПСУ-IP: аппаратный адрес портов резервирования, текущее состояние каждого ФПСУ-IP в процессе резервирования («в работе» или «в резерве»), а также оценка их работоспособности.

Локальная оценка состояния ФПСУ-IP «Работоспособность: ИСПРАВЕН» зависит от оценки системой состояния сетевых адаптеров рабочих портов и успешности их подключения к сети передачи данных. Если во время работы ФПСУ-IP обнаруживает сбой подключения сетевого адаптера рабочего порта к сети передачи данных (в строке состояния «Speed» сетевого адаптера появляется значение «No Link»), то состояние ФПСУ-IP устанавливается как «Работоспособность: ЧАСТИЧНАЯ» и ФПСУ-IP будет передавать управление партнеру по системе горячего резервирования.

Исключение: при включении питания и запуске ФПСУ-IP в режим фильтрации пакетов, система в течении одной минуты проверяет текущее состояние сетевых адаптеров

Рисунок 93 - Жидкокристаллический дисплей ФПСУ-IP

На экран выводится текстовая информация, две строки по двадцать символов в каждой. Дальше по тексту такая текстовая информация будет называться «информационным окном». Переключение между информационными окнами осуществляется механическими кнопками, маркированными символами «<», «>», «^» и «v».

Основное информационное окно

После запуска ФПСУ-IP в рабочий режим, на экран выводится основное информационное окно. В основном информационном окне отображаются:

- серийный номер ФПСУ-IP, например «*AMI00001CO*»;
- режим ФПСУ-IP в системе горячего резервирования, значение выбирается из списка *основной / резервный / единств.* (единственный);
- статус ФПСУ-IP: *в работе.* Постоянно указывается, когда ФПСУ-IP запущен в рабочий режим;
- текущее состояние ФПСУ-IP в системе горячего резервирования, значение выбирается из списка *активен / пассивен / блок.* (*блок* - блокирован ввиду ошибок системы горячего резервирования).

Схематичный пример основного информационного окна:

A	**M**	**I**	**0**	**0**	**0**	**0**	**1**	**C**	**O**			**O**	**C**	**H**	**O**	**B**	**H**	**O**	**Й**
/		**B**		**P**	**A**	**Б**	**O**	**T**	**E**			**A**	**K**	**T**	**И**	**B**	**E**	**H**	

Первый символ во 2-й строке (вращающаяся «/») предназначен для подтверждения

Рисунок 95 - Меню проверки целостности ПО

По внутренним данным без записи результатов - проверка целостности ПО ФПСУ-IP происходит по хранящимся на ПЗУ (SSD) контрольным эталонным суммам, с выводом результата проверки (успешно или обнаружена ошибка) на экран.

По внутренним данным с записью результатов - проверка целостности ПО ФПСУ-IP происходит по хранящимся на ПЗУ (SSD) контрольным эталонным суммам, с выводом результата проверки (успешно или обнаружена ошибка) на экран и в файл с расширением .LST на внешний носитель.

По списку с внешнего носителя - проверка целостности ПО ФПСУ-IP происходит по специальному файлу-заданию с контрольными суммами, считываемого с внешнего носителя, с выводом результата проверки (успешно или обнаружена ошибка) на экран и в файл с расширением .LST на внешний носитель. Файл-задание FPSUHASH.HSH поставляется по отдельному запросу.

После активизации команды меню «Проверка целостности»> «По списку с внешнего носителя» на экране появится сообщение с приглашением вставить носитель с проверочными модулями в считывающее устройство ФПСУ-IP.

После отработки программы результаты проверки будут выданы на экран монитора и в файл FPSUHASH.LST на тот же носитель, с которого был считан файл-задание. Файл FPSUHASH.LST может быть прочитан и обработан на другом компьютере средствами текстового редактора, поддерживающим кодировку OEM/DOS.

ВНИМАНИЕ! Если в результате выполнения проверки появляется сообщение о нарушении целостности контролируемых файлов, или контрольные суммы не совпадают с эталонными, дальнейшая эксплуатация ФПСУ-IP не допускается. Следует проанализировать причину изменения контролируемых файлов. После следует восстановить измененные файлы путем установки обновления или повторной установки программного обеспечения ФПСУ-IP.

Рисунок 97 - Выполняется самотестирование ФПСУ

В случае успешной проверки, будет выдано оповещение:

Рисунок 98 - Сообщение об успешно пройденном самотестировании

В случаях, когда самотестирование ФПСУ-IP завершилось с ошибкой, требуется переустановить ФПСУ-IP с дистрибутива.

Результат прохождения самотестирования записывается в статистику ФПСУ-IP.

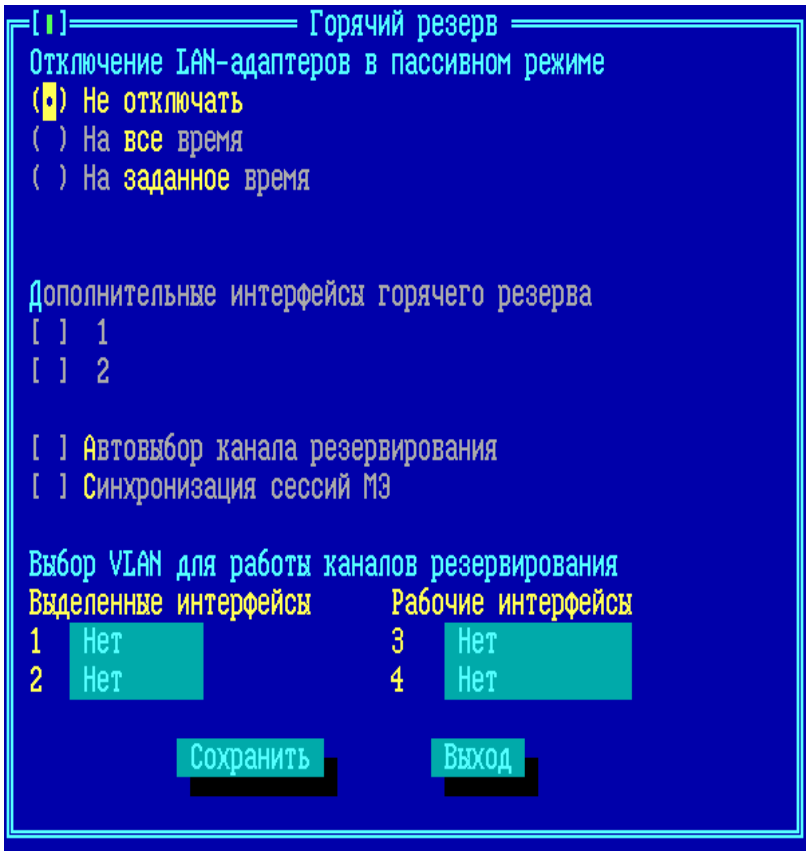

Рисунок 102 - Вход в общие настройки из основного меню конфигурации ФПСУ-IP

Окно установки содержит следующие настраиваемые общие параметры:

Переход на резервный. Если при работе ФПСУ-IP получает сигнал от сетевой аппаратуры об отсутствии физического соединения на каком-либо из рабочих портов, ФПСУ-IP может передать управление партнеру по системе горячего резервирования. В диалоговом поле строки укажите время, по истечении которого будет задействован резервный ФПСУ-IP (в диапазоне от 5 до 255 секунд), или оставьте поле пустым, если такая операция не требуется.

Включить сторожевой таймер (watchdog). Этот флаг позволяет активировать автоматическую перезагрузку ФПСУ-IP при аппаратном или программном «зависании» комплекса. При включении таймера активизируется аппаратный таймер, если материнская плата им оборудована, и его программный аналог, который реализован в операционной системе и не зависит от материнской платы. В случае задействования обоих датчиков, порядок их срабатывания следующий: через 30 секунд после зависания ФПСУ-IP должен сработать программный датчик, перегрузив ФПСУ-IP, если программный датчик не сработал в течение 5 минут, сработает аппаратный watchdog.

Запрет работы при сбоях жесткого диска. Если во время работы подсистемы фильтрации возникают сбои или неполадки ПЗУ, ФПСУ-IP продолжает функционировать до принудительного выхода из подсистемы фильтрации без записи регистрационных данных в хранилище статистической информации. Если политика безопасности исключает подобный аварийный режим без записи статистики, и ФПСУ-IP при сбоях ПЗУ должен прекращать свою работу – задействуйте этот флаг.

ВНИМАНИЕ! При работе ФПСУ-IP в режиме резервирования возможны ситуации, при которых запрет будет игнорироваться. При сбоях ПЗУ на активном ФПСУ-IP, управление передается резервному, который будет продолжать работу даже в случае возникновения собственных аппаратных неполадок.

Сокрытие работы ФПСУ. В зависимости от требуемой степени защиты администратор может включить флаг конфигурации, указывающий ФПСУ-IP, что он должен работать в режиме сокрытия своих защитных (фильтрующих) функций. При включенном флаге ICMP-сообщения о недоступности абонента по причине административного запрета для пакета, не прошедшего фильтрацию, генерироваться не будут, а если ошибка произошла по другой причине, в посылаемом ICMP-сообщении в качестве адреса отправителя сообщения будет проставлен не адрес ФПСУ-IP, а адрес того абонента, кому был направлен пакет, вызвавший ошибку.

Не выдавать ICMP-сообщения об ошибках. Если флаг установлен, ФПСУ-IP никогда не будет генерировать ICMP-сообщения, кроме сообщений о необходимости изменения MTU.

Рисунок 107 - Совместимость СКЗИ

Настройка криптопротоколов ФПСУ-ФПСУ - опции, устанавливающие работу ФПСУ-IP с ФПСУ-IP в режиме шифрования по заданному алгоритму, в отдельном окне «Виды шифров».

- ***Кузнечик-MGM*** - опция, разрешающая шифрование данных блочным шифром «Кузнечик» в режиме MGM (Multilinear Galois Mode), активируется лицензией. Если лицензия отсутствует, данная опция недоступна (отмечена белым фоном);
- ***Магма-MGM*** - опция, разрешающая шифрование данных блочным шифром «Магма» в режиме MGM, активируется лицензией. Если опция «Приоритет Кузнечик» не установлена, то работа ФПСУ-IP будет происходить по алгоритму шифрования «Магма MGM», в случае если партнер поддерживает этот алгоритм. Если лицензия отсутствует, данная опция недоступна (отмечена белым фоном);
- ***Магма*** - опция, разрешающая работу по алгоритму шифрования «Магма». Если опция «Приоритет ГОСТ» не установлена, то работа ФПСУ-IP будет происходить по алгоритму шифрования «Магма», в случае если партнер поддерживает этот алгоритм.
- ***ГОСТ 28147-89*** - опция, разрешающая работу по алгоритму шифрования ГОСТ 28147-89.
- ***Приоритет ГОСТ*** - при включении опции передаваемые данные между ФПСУ-IP будут шифроваться по алгоритму ГОСТ 28147-89, в случае если этот алгоритм не запрещен у партнера. Если не выбран ни один алгоритм, данная опция недоступна (отмечена белым фоном).
- ***Приоритет Кузнечик*** - при включении опции передаваемые данные между ФПСУ-IP будут шифроваться по алгоритму «Кузнечик MGM», в случае если партнер поддерживает этот алгоритм. Если лицензия на алгоритм шифрования «Кузнечик

<*Enter*> или <*Пробел*> на экран будет выдано окно выбора сетевых адаптеров. Выделите курсором строку с типом сетевого адаптера «Виртуальный Link Aggregation», назначаемого для агрегированного сетевого адаптера ФПСУ-IP и нажмите <*Enter*>.

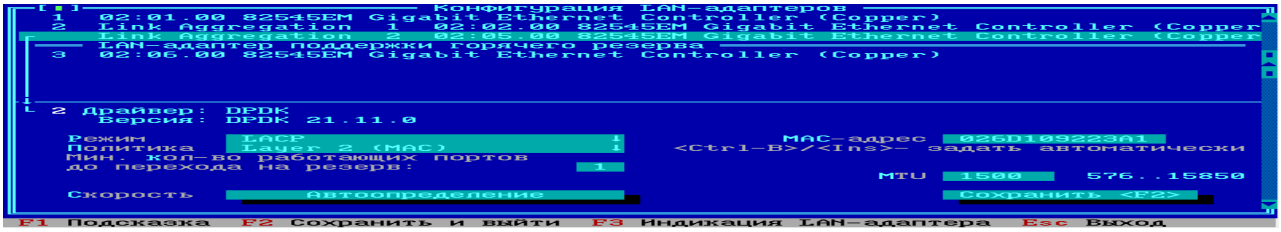

Рисунок 118 - Выбор сетевого адаптера для порта

Агрегированный сетевой адаптер отобразится в списке сетевых адаптеров с не заданными LAN-адаптерами.

Рисунок 119 - Агрегированный сетевой адаптер

Агрегированный сетевой адаптер может быть задан только для рабочих сетевых адаптеров, не используется для сетевых адаптеров «горячего» резерва. Агрегированный сетевой адаптер конфигурируется минимум двумя LAN-адаптерами.

Для добавления LAN-адаптера установите курсор на строку «Link Aggregation» и нажмите клавишу <*Ins*>.

Рисунок 120 - Добавление LAN-адаптера

На экран будет выдано окно диалога, нажмите кнопку «Да». Откроется список доступных сетевых адаптеров, выберите сетевой адаптер по нажатию клавиши <*Enter*> или <*Пробел*>, затем выберите драйвер для сетевого адаптера из списка доступных. Выделите строку с драйвером и нажмите клавишу <*Enter*> или <*Пробел*>. Аналогично задайте второй LAN-адаптер.

Для задания параметров выделите строку сетевого адаптера. По нажатию клавиши <*Tab*>, курсор переместится на параметры LAN-адаптер. В поле параметра, заданного списком значений, отображается символ «v», по нажатию клавиши <*Пробел*> открывается выпадающий список. Перемещение по списку осуществляется клавишами <v> и < >, для выбора значения из списка выделите строку значения и нажмите клавишу <*Enter*>.

дополнительного адреса, для доступа к резервному ФПСУ-IP системы горячего резервирования.

После активации опции «Интерфейс для удаленного управления ФПСУ» для второго сетевого адаптера поддержки горячего резерва, и добавления IP-адреса порту ФПСУ-IP в VLAN №4093 (и, опционально, в VLAN №4094), к запущенному в рабочий режим ФПСУ-IP будет разрешено подключение зарегистрированных на нём удаленных администраторов через этот сетевой адаптер (№4 на рисунке).

Можно проверить использование сетевого адаптера для доступа удаленных администраторов, переключившись на экран мониторинга системы горячего резервирования (см. пункт «Окно состояния подсистемы «горячего» резервирования»). На включение режима доступа удаленных администраторов указывает маркер «А» около строки второго адаптера системы горячего резервирования:

Рисунок 123 - Адаптер готов принимать соединения с удаленными администраторами

Рисунок 131 - Выбор файла обновления

4. Требуется подтвердить запуск процесса обновления, выбрав команду «Используем его», либо вернуться к выбору другого файла обновления.

Рисунок 132 - Подтверждение обновления

Начнется процесс установки обновления, необходимо подтверждать этапы установки.

ФПСУ-IP» выдает на внешний носитель файл с ключом аутентификации удаленного администратора;

5. файл с ключом аутентификации удаленного администратора отправляется локальному администратору ФПСУ-IP (передача файла с аутентификатором по незащищенной сети передачи данных запрещается);
6. локальный администратор ФПСУ-IP регистрирует удаленного администратора и предоставляет ему права на доступ к подсистемам ФПСУ-IP.

При выполнении команды меню настройки системы «*Регистрация удаленных администраторов»*, на экране появится окно, которое содержит те параметры ФПСУ-IP (серийный номер, комментарий к нему и дату создания ключей аутентификации ФПСУ-IP), с которыми его зарегистрирует удаленный администратор, а также список уже зарегистрированных удаленных администраторов ФПСУ-IP (по умолчанию, пустой, с текстом «Администраторы отсутствуют»).

Рисунок 142 - Список удаленных администраторов

Количество удаленных администраторов, зарегистрированных на ФПСУ-IP, не может превышать тридцати двух.

Выход из подсистемы регистрации удаленных администраторов осуществляется

получения протокола работы абонентов всегда включены) и разрешить/временно запретить работу удаленного администратора.

Рисунок 146 - Назначение прав удаленному администратору

Для того, чтобы удаленный администратор смог переключать находящиеся в горячем резерве ФПСУ-IP, ему следует выдать право на «получение данных о работе Удаленных администраторов».

Право на согласование времени разрешает ФПСУ-IP синхронизировать время со временем рабочей станции выбранного удаленного администратора. Право на согласование времени может быть выдано только одному удаленному администратору.

ВНИМАНИЕ! НЕ СЛЕДУЕТ одновременно задействовать NTP-клиента ФПСУ-IP (см. пункт «NTP-клиент ФПСУ-IP») и синхронизацию времени ФПСУ-IP с удаленным администратором!

Отметив соответствующие выдаваемым правам флаги клавишей <*Пробел*>, сохраните установки при помощи команды «*Сохранить*», при этом подсистема вернется в окно списка зарегистрированных удаленных администраторов.

7. 6. 2. Ключи аутентификации ФПСУ-IP

Ключи аутентификации ФПСУ-IP требуются для регистрации ФПСУ-IP удаленным администратором в программе «Удаленный администратор ФПСУ-IP».

Проверка линий связи выполняется для каждого порта ФПСУ-IP независимо. Если хотя бы для одного порта ФПСУ-IP проверка не пройдена, комплекс переходит в режим «частично неработоспособен» и передает управление партнеру по системе горячего резервирования.

При включении проверки линий связи для портов ФПСУ-IP, активный комплекс горячего резерва отправляет эхо-запросы на список указанных администратором IP-адресов. Если хотя бы один IP-адрес списка проверяемого порта ответил на эхо-запрос, проверка считается пройденной. Если ни одного эхо-ответа нет, проверка считается не пройденной, управление передается партнеру по горячему резерву (пассивному на момент опроса комплексу ФПСУ-IP). После передачи управления, ставший пассивным комплекс ФПСУ-IP ставит временный запрет на приём активной роли. При первой передаче управления по причине неуспешной проверки линии связи, запрет будет действовать столько минут, сколько указано в параметре «Время перепроверки линий связи», умноженное на первоначальный коэффициент 5 (т.е. если в параметре указано 2 минуты, запрет будет действовать 10 минут). На это же время состояние ФПСУ-IP в системе горячего резервирования устанавливается как «*Работоспособность: частичная»* с дополнительной строкой сообщения «*нет канала связи»*. Если передача управления по причине неуспешной проверки линии связи происходит не в первый раз, длительность запрета и состояния частичной работоспособности умножаться на первоначальный коэффициент 5 не будет.

Комплекс горячего резерва, который становится активным по причине отсутствии ответа от контролируемых IP-адресов, начинает сам проверять доступность IP-адресов того же списка. В случае отсутствия ответов, повторные проверки доступности IP-адресов проводятся через количество минут, указанное в параметре «Время перепроверки связи».

7. 7. 4. 1. Интерфейс настройки проверки линий связи

Интерфейс настройки проверки линий связи доступен из окна настройки общих параметров конфигурации ФПСУ-IP, по команде «Контроль сети»:

Рисунок 162 - Общие параметры ФПСУ-IP

При выполнении команды «Контроль сети» окна общих параметров ФПСУ-IP, откроется окно установки параметров проверки линий связи для портов ФПСУ-IP.

В окне будет отображен список параметров контроля сети и список абонентов, описанных как «хост» для выбранного порта (см. пункт «Описание абонента «Хост»). Если на выбранном порту ФПСУ-IP нет абонентов, описанных как «хост» (конфигурация определена, например, только записями типа «подсеть» и «любой»), то список будет пустой.

Переключение между списками разных портов выполняется перемещением курсора на кнопку «*Порт*» и нажатием клавиши <*Пробел*>.

По умолчанию, проверки не производятся, о чём дополнительно указывает метка «Проверка отключена».

период времени после успешного получения эхо-ответа хотя бы от одного из контролируемых IP-адресов.

Попыток повтора – количество повторных попыток отправки эхо-запросов, которые будет выполнять активный ФПСУ-IP, в случае если ни от одного из IP-адресов контролируемого списка не пришел ответ. Только после исчерпания попыток повтора активный ФПСУ-IP передаст управление партнеру по горячему резерву. Количество попыток повтора устанавливается в пределах от 3-х до 8-ми.

С интервалом – интервал времени, через который, после неудачной проверки, проводится новая **попытка повтора** активным комплексом ФПСУ-IP получить эхо-ответ от указанных администратором IP-адресов. Может быть установлен в пределах от 3-х до 32-х секунд.

Для внесения выполненных настроек в конфигурацию ФПСУ-IP следует выполнить команду «Сохранить» или нажать клавишу <F2>. Выход без внесения настроек в конфигурацию осуществляется по клавише <Esc> или команде «Выход».

7. 7. 4. 2. Пример работы системы проверки связи

Например, если настройки выполнены так, как указано на рисунке ниже (обратите внимание, данные настройки не являются рекомендуемыми!), то комплекс ФПСУ-IP с двумя рабочими портами, работающий в режиме «горячего» резервирования, будет проводить отдельную проверку для каждого рабочего порта следующим образом:

Рисунок 168 - Подтверждение отключения подсистемы автозапуска

Отключение системы автозапуска (выбор опции «Да») сопровождается перезагрузкой ФПСУ-IP, во время которой удаляется ключ автозапуска.

Для отмены отключения системы автозапуска, выберите опцию «Нет».

7. 8. 2. Переинициализация ПДСЧ

Команда «Переинициализация ПДСЧ» подменю «Настройки СКЗИ» предназначена для повторной инициализации программного датчика случайных чисел (ПДСЧ) ФПСУ-IP. Частота повторной инициализации программного датчика случайных чисел ФПСУ-IP регулируется правилами пользования СКЗИ.

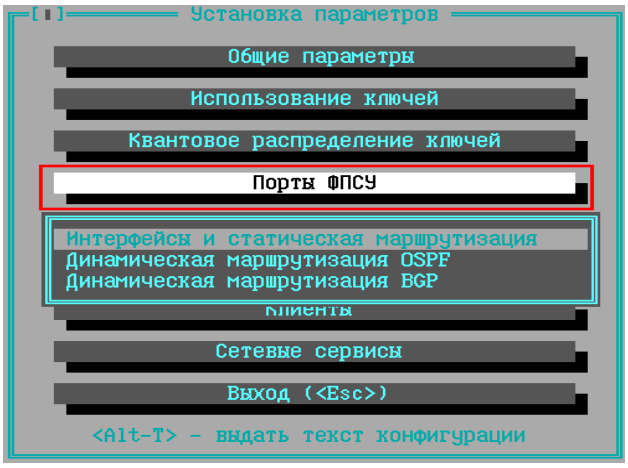

Рисунок 169 - Команда повторной инициализации ДСЧ

При выборе команды «Переинициализация ПДСЧ» запустится интерфейс программно-клавиатурного датчика случайных чисел. От администратора требуется ввести указываемые программой цифры:

Рисунок 170 - Программно-клавиатурный датчик случайных чисел

Переинициализация ПДСЧ завершится успешно, как только будет осуществлён корректный ввод достаточного числа символов. В любой момент до успешного завершения процесс можно отменить, вернувшись по клавише <*Esc*> обратно в подменю «Настройки СКЗИ».

7. 8. 3. Установка времени действия ключей

Команда «Установка времени действия ключей» меню «Настройки СКЗИ» предназначена для доступа в интерфейс настройки времени действия ключа хранения ФПСУ-IP (на нём зашифрована файловая система ФПСУ-IP) и ключа горячего резерва ФПСУ-IP.

Рисунок 176 - Установка параметров порта

Передвижение по одиночным полям окна осуществляется клавишами <v>, < >, <*Enter*> (движение вперед), а если поле содержит список параметров, выйти из него можно по нажатию клавиш << > или <> >.

Окно содержит следующие параметры порта ФПСУ-IP:

Порт — номер порта (1 или 2), соответствующий номеру LAN-адаптера (присвоенному LAN-адаптеру при конфигурировании), который осуществляет взаимодействие с сетью передачи данных со стороны описываемого порта.

Имя — имя порта, текстовое описание.

Адрес — IP-адрес порта, для которого осуществляются установки. При нажатии клавиши <*Пробел*> при установленном на поле «Адрес» курсоре, осуществляется переход к окну настройки VLAN, в которых участвует данный порт. По умолчанию, указанный в поле «Адрес» IP-адрес порта ФПСУ-IP в VLAN не участвует. Описание настроек VLAN порта см. пункт «Описание VLAN порта ФПСУ-IP».

принадлежит фрейм, допустимые значения идентификатора от 2 до 4094;

- ***Адрес —*** IP-адрес порта ФПСУ-IP в описываемом VLAN;
- ***Имя —*** имя порта, текстовое описание.
- ***Маска*** — маска IP-адреса порта ФПСУ-IP в описываемом VLAN;
- ***Запрет ARP*** — флаг, при включении которого ФПСУ не отсылает «Gratuitous ARP» и не отвечает на ARP в адрес этого порта.

Рисунок 179 - Настройка VLAN на порту ФПСУ-IP

Для выхода в список VLAN порта с сохранением настроек нового VLAN, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

В окне списка настроенных VLAN можно внести изменения в отмеченных курсором VLAN, нажав клавишу <*Пробел*>.

Для удаления отмеченного курсором описателя VLAN нажмите клавишу <*Del*>.

Эти сообщения будут учитываться ФПСУ-IP следующим образом:

- если в поле «Маршрутизаторы» при описании параметров работы конфигурируемого порта с удаленным ФПСУ-IP ни один маршрутизатор не отмечен (символом «> »), сообщение переадресации принимается ФПСУ-IP только в том случае, если оно получено от любого прописанного на принимающем порту маршрутизатора и переадресовывает IP-пакеты на любой другой прописанный на этом порту маршрутизатор.
- если в поле «Маршрутизаторы» есть отмеченные маршрутизаторы, то сообщение переадресации может быть принято только от одного из них и только в том случае, если в качестве нового маршрутизатора указывается также один из таких маршрутизаторов (в этом случае в конфигурации ФПСУ-IP должно быть указано как минимум два маршрутизатора).

В остальных случаях при передаче IP-пакетов удаленному ФПСУ-IP сообщения переадресации в адрес конфигурируемого ФПСУ-IP будут сброшены.

Остальные параметры для установления туннеля между ФПСУ-IP описываются в пунктах «Дополнительные параметры соединения ФПСУ-ФПСУ» и «Потоки данных в туннеле между ФПСУ-IP».

Когда все требуемые параметры в окне «ФПСУ» определены, следует активизировать команду «*Сохранить*» или нажать клавишу <*F2*>, после чего осуществится выход в окно установки параметров порта, в котором имя описанного ФПСУ-IP появится в списке, а внизу окна будут отображаться основные параметры его работы.

Если какой-либо ФПСУ-IP больше не существует или не участвует в работе, и его описатель не нужен, отметьте его и нажмите <*Del*> для удаления. В этом случае для всех абонентов, работающих через ФПСУ-IP с удаленным описателем, доступ будет автоматически запрещен.

8. 3. 1. Дополнительные параметры соединения ФПСУ-ФПСУ

Помимо основных, обязательных для установления туннеля между ФПСУ-IP параметров, существует ряд дополнительных:

Установленный режим на данном ФПСУ-IP	Установленный режим на удаленном ФПСУ-IP			
	запрещено	***нежелательно***	***желательно***	***обязательно***
запрещено	не используется	не используется	не используется	соединение не состоится
нежелательно	не используется	не используется	используется	используется
желательно	не используется	используется	используется	используется
обязательно	соединение не состоится	используется	используется	используется

Виды шифров – опции, устанавливающие работу ФПСУ-IP с ФПСУ-IP в режиме шифрования по заданному алгоритму, в отдельном окне «Виды шифров». Подробное описание приведено в пункте «Общие параметры конфигурации ФПСУ-IP» (опции «Настройка криптопротоколов ФПСУ-ФПСУ»). Значение по умолчанию может быть выбрано по нажатию соответствующей кнопки.

Протокол ФПСУ-ФПСУ: *IP или UDP* – флаг, меняющий основной протокол взаимодействия между двумя ФПСУ-IP с протокола по умолчанию, сетевой IP№53, на альтернативный транспортный UDP: 30004.

TOS в туннеле - выбор типа обслуживания пользовательских пакетов в отдельном окне «TOS в пакетах туннеля ФПСУ».

Абн (абоненты) - настройки типа обслуживания для пользовательского трафика (весь трафик кроме служебных соединений между ФПСУ-IP);

Служ (службы) - настройки типа обслуживания для служебного трафика (служебные соединения между ФПСУ-IP).

В пакетах абонентов - настройки для пользовательского трафика:

- *Не изменять* - не изменять тип обслуживания в пакете;
- *Во все пакеты* - изменить тип обслуживания для всех пакетов на заданное значение;
- *В пакеты с ненулевым TOS* - изменить тип обслуживания на заданный для пакетов с установленным типом обслуживания;
- *TOS* - значение в байтах.

В служебных пакетах ФПСУ *TOS* - значение в байтах.

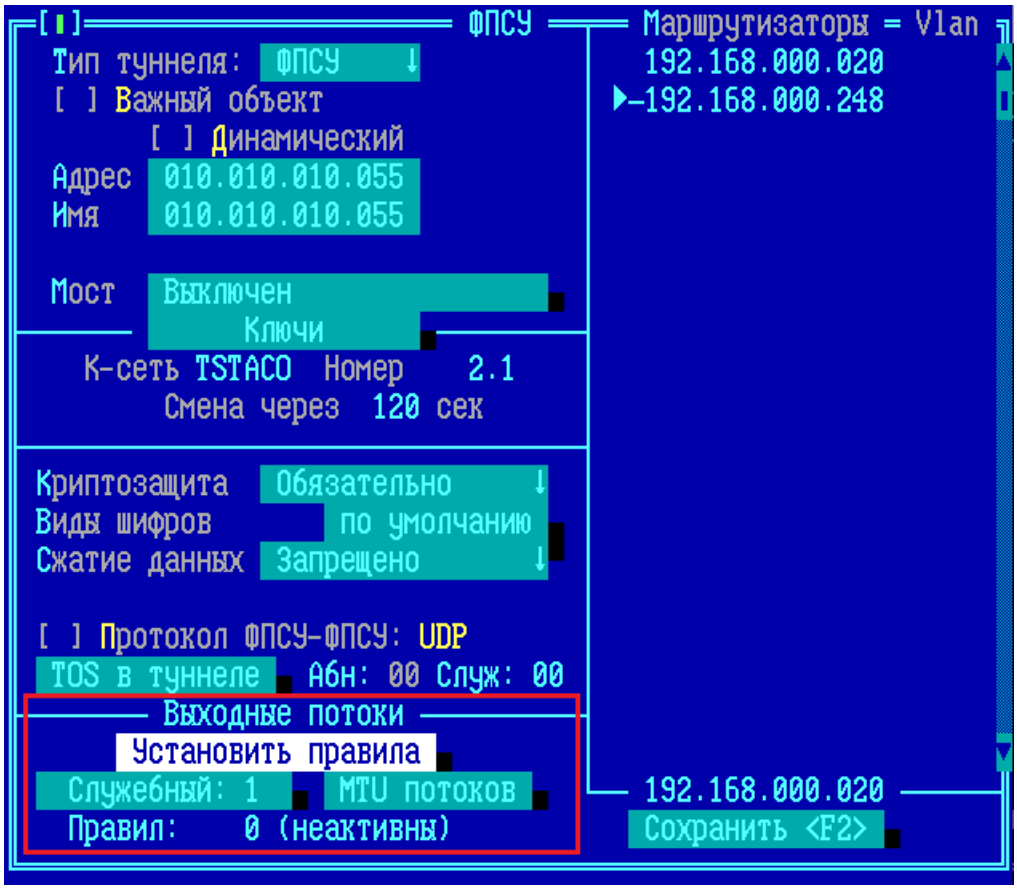

Рисунок 187 - Настройка типа обслуживания в туннеле

8. 3. 2. Потоки данных в туннеле между ФПСУ-IP

Дополнительно устанавливаются параметры для потоков данных в туннеле между ФПСУ-IP:

Выходные потоки - правила разделения поступающих в VPN-туннель между ФПСУ-IP данных на несколько (от 1 до 128) различных потоков. Установка и активизация этих правил требуются в том случае, если на пути следования данных по VPN-туннелю находится пограничный маршрутизатор, реализующий функцию «shaping» (ограничение полосы пропускания по различным критериям), и/или конфигурированный на использование различных маршрутов для доставки данных в одно и то же место назначения.

Подробная информация о принципе работы выходных потоков содержится в разделе «Общие правила разделения потоков». Описание индивидуальных правил для каждого VPN-туннеля производится аналогично общим.

Кнопка «*Служебный*» в области «Выходные потоки» позволяет установить номер

Рисунок 194 - Установка флага «Правила активны»

Для выхода из окна «Установка индивидуальных правил» в окно параметров туннеля между ФПСУ-IP с сохранением выполненных настроек, нажмите клавишу <*Esc*>.

Кнопка «*MTU потоков»* в поле «Выходные потоки» предназначена для установки максимального размера передаваемых IP-пакетов (в байтах), которые будут передаваться по потокам с соответствующими номерами.

Требуется обратить особое внимание при добавлении абонентов и маршрутизаторов в конфигурацию ФПСУ-IP, имеющему мостовой туннель. При задействованном механизме ARP-proxy в локальной сети может произойти обновление ARP-таблиц рабочих станций, и абоненты начнут обращаться в MAC-адрес ФПСУ-IP, что приведет к обычной фильтрации этих пакетов по правилам межсетевого экрана, с возможно блокировкой их передачи.

В конфигурации ФПСУ-IP версии ниже 4 только один туннель может быть настроен на работу в режиме моста.

В конфигурации ФПСУ-IP версии 4 на работу в режиме моста может быть настроено больше одного туннеля.

Режим моста предполагается задействовать в ситуациях, когда требуется объединить распределенную локальную сеть, создав защищенный механизм передачи данных без изменения сетевой конфигурации и добавления новых маршрутов.

Рисунок 197 - Режим моста в туннеле ФПСУ-ФПСУ

В приведенной на рисунке схеме требуется передавать пакеты внутри локальной сети, разделенной географически. Для того, чтобы организовать такую «прозрачную» защищенную передачу данных, достаточно на внешних портах ФПСУ 1 и ФПСУ 2 создать описатель партнера по шифрованию и включить режим моста для туннеля ФПСУ 1 - ФПСУ 2.

При этом на внутренних портах ФПСУ 1 и ФПСУ 2 не должно быть описано абонентов (хостов, подсетей, записи «любой хост») - пакеты от явно указанных на портах ФПСУ-IP абонентов не передаются в туннель типа «мост».

ВНИМАНИЕ! Исключение**.** Если используется удаленное администрирование ФПСУ-IP, задействованными в режиме моста, то рабочее место с АРМ УА необходимо указать в конфигурации ФПСУ-IP в качестве абонента! Например, на схеме выше, если АРМ УА находится в защищаемой с помощью ФПСУ 1 подсети слева, то его IP-адрес должен быть указан в качестве абонента на внешнем порту ФПСУ 2 и на внутреннем порту ФПСУ 1.

определенный» адрес. Сначала проверяется, не входит ли искомый адрес в список адресов индивидуальных хостов, если такой адрес в таблице обнаружен - поиск прекращается и для абонента производится фильтрация по правилам, установленным для данного конкретного адреса.

Если адрес не найден в записях индивидуальных адресов, ищется, не входит ли он в один из описанных диапазонов адресов подсетей, если да, то для него производится фильтрация по правилам, установленным для данной подсети. Если адрес абонента не найден в двух упомянутых категориях, он считается неописанным и пропускается по правилам, установленным администратором для категории «Любой Хост».

Всего в списке абонентов каждого порта может содержаться не более 65535 записей (любого типа).

Внесение в список порта нового описателя абонента осуществляется по нажатию клавиши <*Ins*>, редактирование установленных параметров для уже описанного абонента - по нажатию клавиши <*Пробел*>.

Выделенный курсором описатель может быть использован в качестве основы для создания нового описателя при помощи комбинации клавиш <*Ctrl+Ins*> или <*Ctrl+B*>.

Во всех случаях откроется окно «*Абонент»*, содержащее несколько полей, позволяющих определить тип адресной записи, ввести численные значения адресов, определить режим работы для описываемого адреса и определить другие необходимые параметры. Все установки осуществляются посредством выбора соответствующей строки и нажатия клавиши <*Пробел*>.

В первом поле открывшегося окна «*Абонент»* установите тип адреса абонента.

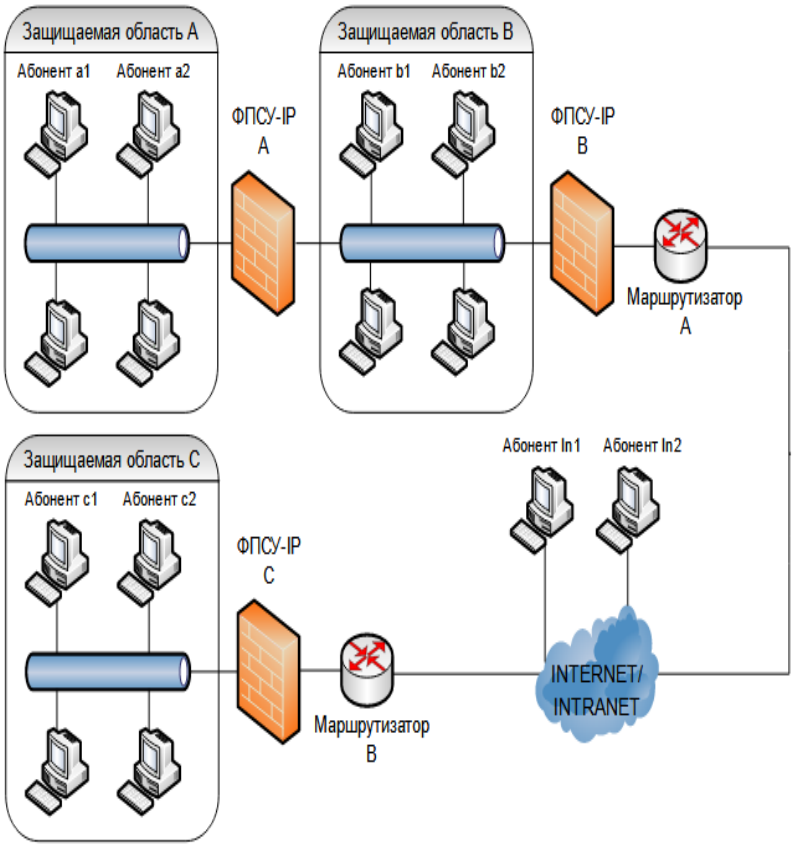

Рисунок 202 - Окно «Абонент»

Тип - индивидуальный (адрес хоста), групповой (IP-адрес подсети) или специальный адрес «Любой Хост». Остальные поля окна будут различными в зависимости от указанного типа адреса, о чем подробнее рассказывается в последующих пунктах, «Описание абонента «Хост», «Описание абонента «Подсеть» и «Описание абонента «Любой Хост».

8. 4. 1. Описание абонента «Хост»

Записи типа «Хост» предназначены для явного указания на порту ФПСУ-IP IP-адресов абонентов, которые смогут передавать через ФПСУ-IP данные абонентам противоположного и/или данного порта в случае соблюдения совокупности правил фильтрации, определенной для них администратором.

Для описания **индивидуального хоста** укажите следующие параметры:

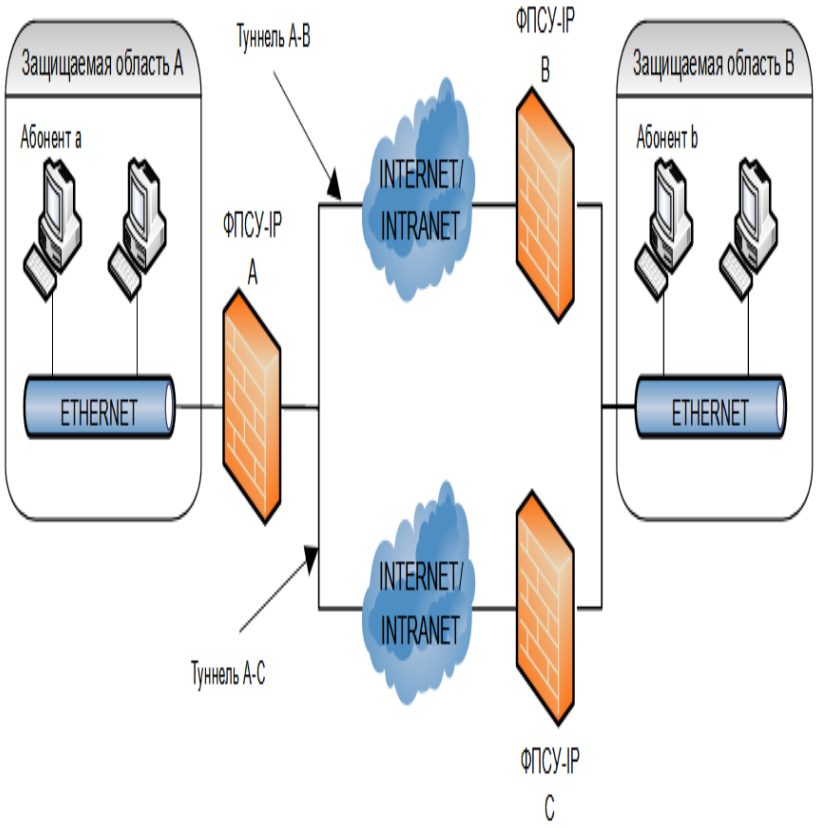

Рисунок 203 - Параметры абонента типа хост, режим «Ретрансляция»

Рисунок 204 - Параметры абонента типа хост, режим «Через ФПСУ»

Важный объект – флаг в положении «включено» запрещает удалять описание абонента из интерфейса портов ФПСУ-IP. Признак «Важный объект» добавлен как дополнительная защита от случайного удаления записи при редактировании конфигурации.

VLAN – номер виртуальной локальной сети, в которой участвует данный IP-адрес, если требуется. Только для абонентов в режиме «Ретрансляция».

Адрес – IP-адрес рабочей станции.

Имя – имя абонента, которое будет отображаться в списке.

MAC – Только для абонентов в режиме «Ретрансляция». Статически заданный аппаратный адрес для этого абонента. Если параметр задан, ФПСУ-IP будет отправлять пакеты в адрес этого абонента именно на указанный аппаратный адрес, вне зависимости от приходящих на ФПСУ-IP ARP-пакетов от IP-адреса абонента.

Проверять MAC – Только для абонентов типа «Хост», работающих в режиме «Ретрансляция». Требует заполненного поля «MAC». При включенной опции, ФПСУ-IP проверяет полученные от IP-адреса абонента пакеты на соответствие указанному MAC-

Рисунок 205 - Режим работы партнеров абонента

- **«*Через ФПСУ*»** (обмен между абонентом и портом ФПСУ-IP будет производиться через туннель со смежным ФПСУ-IP. В режиме возможно включение механизмов шифрования и/или сжатия передаваемых данных).

Выберите этот режим, если описываемый абонент подключается к настраиваемому ФПСУ-IP через установленный VPN-туннель с другим ФПСУ-IP. Например, для ФПСУ-IP A это будут «Абонент In1 через ФПСУ-IP B» или «Абонент c1 через ФПСУ-IP B»; для ФПСУ-IP B это будут «Абонент c1 через ФПСУ-IP C» или «Абонент a2 через ФПСУ-IP A»; для ФПСУ-IP C это будут «Абонент a2 через ФПСУ-IP B» или «Абонент b2 через ФПСУ-IP B».

В случае указания режима работы «*Через ФПСУ*» в правой части окна будет отображен список линий смежных ФПСУ-IP (если список пуст, вернитесь к процедурам, описанным ранее). При помощи клавиши *<Пробел>* отметьте имя удаленного ФПСУ-IP, через который будет доступен абонент (слева от строки появится значок отметки). Для абонента требуется выбрать основную линию ФПСУ-IP, через туннель с которым будут

передаваться данные. Если абонент может передавать данные через внешнюю сеть по нескольким маршрутам, то в настройках ФПСУ-IP есть возможность указать резервный (запасной) ФПСУ-IP, через туннель с которым будут передаваться данные в случае невозможности организовать туннель с основным ФПСУ-IP. Выберите описатель ФПСУ-IP, который требуется назначить запасным, и нажмите <*Alt+R*>. Нажмите <*Alt+C*> чтобы поменять для данного абонента основной ФПСУ-IP и запасной.

Например, на рис. «Использование основной и резервной (запасной) линий ФПСУ-IP» данные от «Абонент a» до «Абонент b» могут идти двумя путями:

- Абонент a > ФПСУ-IP A > туннель A-B > ФПСУ-IP B > Абонент b;
- Абонент a > ФПСУ-IP A > туннель A-C > ФПСУ-IP C > Абонент b.

В таком случае, «Абонент b» может быть описан на ФПСУ-IP A как абонент, работающий в режиме «Через ФПСУ» с указанием основной линии, идущей через ФПСУ-IP B и резервной (запасной) линии, идущей через ФПСУ-IP C.

Если абонент подключается через цепочку туннелей к настраиваемому ФПСУ-IP (как, например «Абонент c1» на рис. «Режим работы партнеров абонента» при настройке взаимодействия через ФПСУ-IP A, подключается через два тоннеля — туннель ***ФПСУ-IP C-ФПСУ-IP B*** и туннель ***ФПСУ-IP B-ФПСУ-IP A***), то указывать следует ближайший ФПСУ-IP (в приведенном примере это ФПСУ-IP B).

Рисунок 206 - Использование основной и резервной (запасной) линий ФПСУ-IP

Для каждого описываемого абонента может быть установлено дополнительное правило фильтрации по режиму работы с другими зарегистрированными на настраиваемом ФПСУ-IP абонентами, которые называются ***партнерами*** описываемого абонента. Настраивается в поле «Режим партнера».

данной подсети, описав их отдельно (см. подраздел «Описание абонента «Хост»). Такая запись отдельного хоста будет иметь больший приоритет, чем описание всей подсети, включающей в себя IP-адрес хоста.

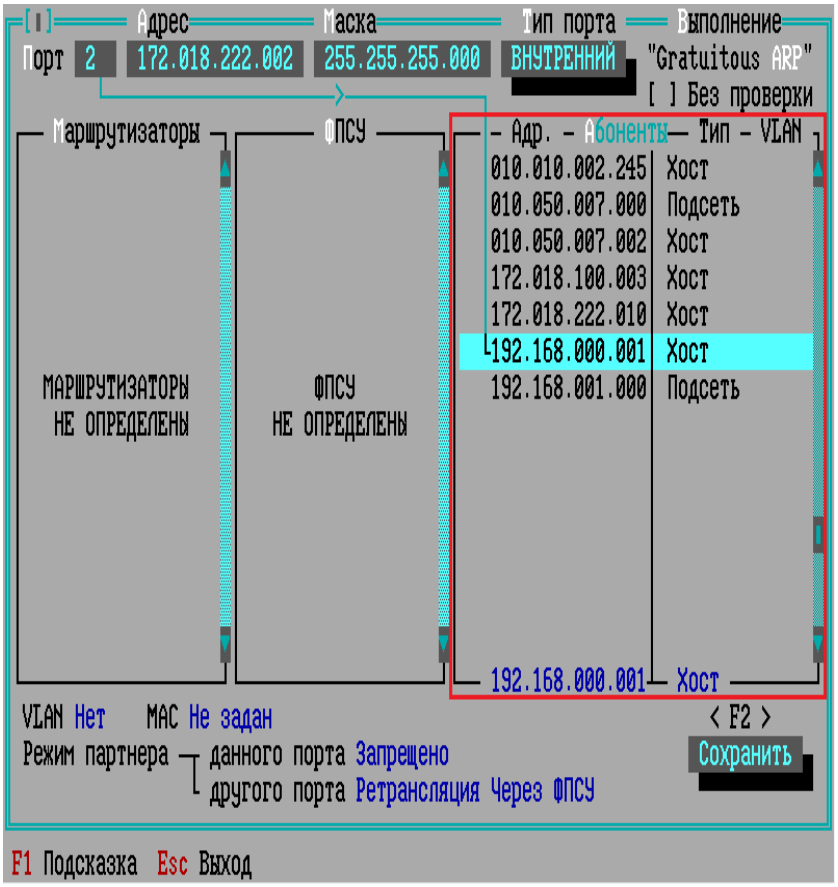

Рисунок 207 - Описание абонента ФПСУ-IP типа «Подсеть»

Для описания **подсети** заполните следующие поля:

Важный объект — флаг в положении «включено» запрещает удалять описание абонента из интерфейса портов ФПСУ-IP. Признак «Важный объект» добавлен как дополнительная защита от случайного удаления записи при редактировании конфигурации.

Поток — для описываемой подсети можно установить номер потока (от 1 до 128), в который будут направлены обмены подсети при передаче данных в туннеле между ФПСУ-IP.

Адрес подсети — IP-адрес подсети.

Маска подсети — можно ввести значение маски непосредственно, а можно выделить поле ввода и нажать <*Пробел*>, после чего в появившемся окне (см. рисунок ниже) ввести число значащих разрядов (от 1 до 30), в таком случае ФПСУ-IP рассчитает

значение маски автоматически.

Имя — имя подсети (произвольное), которое будет отображаться в списке абонентов порта.

Режим работы и ***режим партнера*** - описание этих параметров аналогично описанию их для индивидуальных хостов, в этом случае установленные параметры будут одинаковы для всех хостов подсети.

Маршрутизаторы или ***ФПСУ*** - соответствующие списки появляются в правой половине окна в зависимости от указанного режима работы всех абонентов описываемой подсети; требуется отметить соответственно маршрутизатор или ФПСУ-IP, через которые будет доступна подсеть. Выберите описатель маршрутизатора или ФПСУ-IP, через который будет доступна подсеть и нажмите клавишу <*Пробел*> (слева появится значок отметки).

Только Broadcast — флаг, указывающий ФПСУ-IP, что данная запись типа «подсеть» создана специально для определения правил работы с широковещательными передачами. Если флаг выключен - описываемая подсеть по установленным правилам будет обмениваться с партнерами как широковещательными IP-пакетами, так и IP-пакетами для отдельных хостов, входящих в данную подсеть.

Когда для всех рабочих станций подсети установлены одинаковые правила фильтрации, и эти правила фильтрации не отличаются от правил фильтрации широковещательных передач, вся подсеть может быть описана одной записью и флаг включать не нужно. В противном случае, если получение широковещательных пакетов желательно, но небезопасно для отдельных хостов подсети, следует создать специальную запись для передачи только широковещательных пакетов в описываемую подсеть (включив в ней флаг «*Только Broadcast*»), а для описания отдельных рабочих станций этой подсети создать отдельные записи (см. пункт «Описание абонента «Хост»).

Отвечать на Ping — указание ФПСУ-IP отвечать на ICMP (ECHO) пакеты, направленные от IP-адреса абонентов описываемой подсети в IP-адреса портов настраиваемого ФПСУ-IP. Отметка (разрешение отвечать на запросы) производится по нажатию клавиши <*Пробел*>. ФПСУ-IP отвечает только на те ICMP (ECHO) запросы, которые поступили на адреса его портов в одном IP пакете (т.е. не были фрагментированы в процессе доставки). Это означает, что размер пакета, на которые будет вырабатываться ответ, зависит от MTU маршрута: если пакет ICMP (ECHO) запроса передается по локальной сети, он не должен превышать 1464 байта, а если он передан через маршрутизатор - не должен превышать MTU за вычетом 40 байт.

Рисунок 208 - Абонент «Любой Хост», режим «Ретрансляция»

Если администратор разрешает абонентам защищаемой области обмениваться пакетами с абонентами общей сети, не описанными явно, он может включить запись «Любой Хост» в таблицу адресов абонентов со стороны того порта, который связан с пограничным маршрутизатором, отделяющим защищаемый фрагмент от общедоступной сети передачи данных. Для этого адреса можно также установить определенные совокупности правил фильтрации через включение его в правила трафика (см. пункт «Параметры доступа, правила трафика межсетевого экрана»), например, разрешить неописанным абонентам работать через ФПСУ-IP только по определенным протоколам и/или TCP/UDP-портам, или только в указанное время, или только с конкретными абонентами. Понятно, что для всех неописанных абонентов при этом устанавливаются одинаковые правила фильтрации.

Опция «*Отвечать на Ping*» абонентам записи «Любой Хост» не предоставляется.

ВНИМАНИЕ! На рабочих станциях защищаемого фрагмента, которым разрешается выход во внешнюю сеть, в качестве маршрутизатора по умолчанию должен быть указан пограничный маршрутизатор на выходе из защищаемой области.

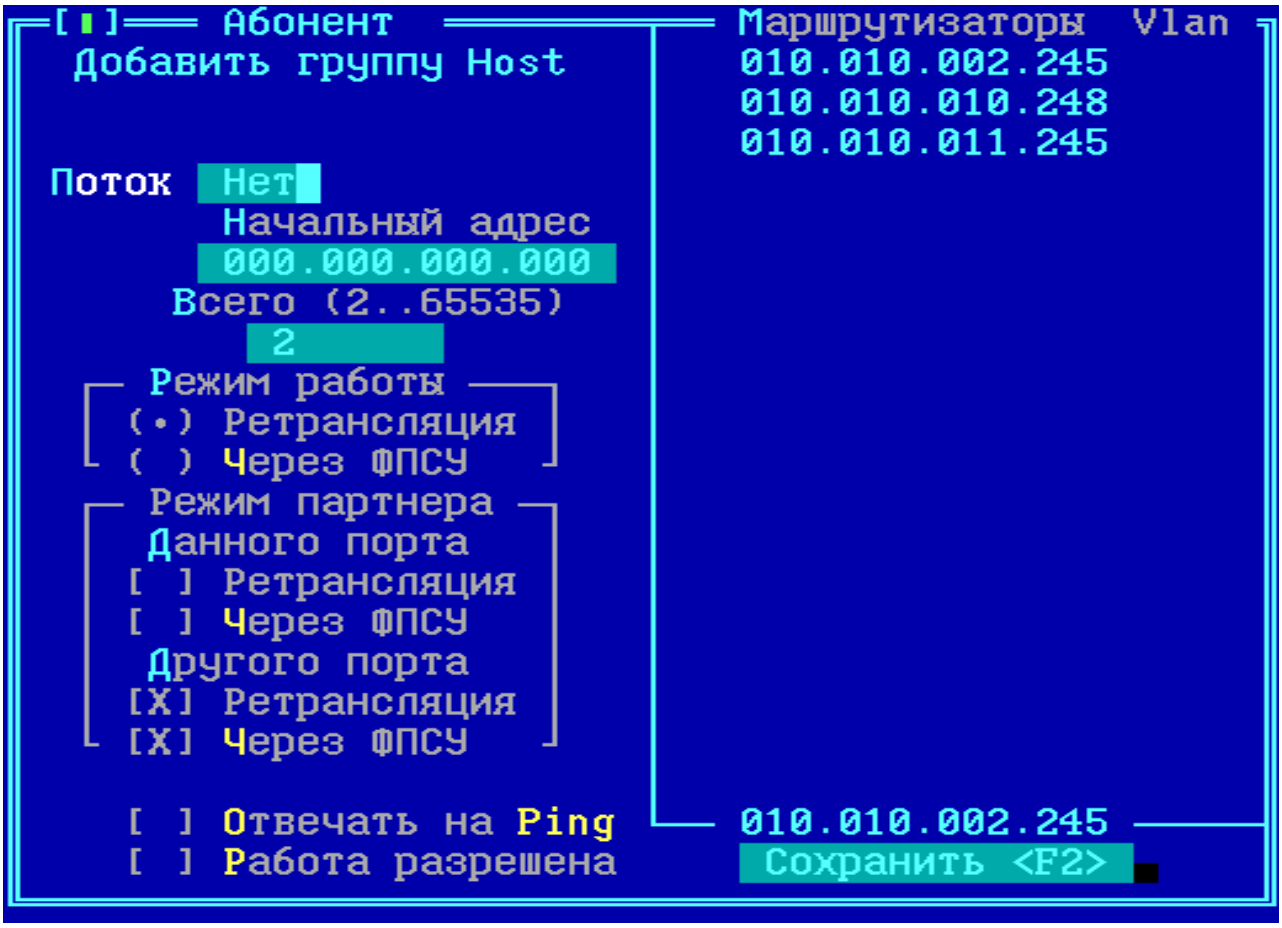

Рисунок 211 - Поиск абонента в списке

Поиск абонента в правилах межсетевого экрана ведётся по клавише *<F7>*, открывается окно со списком правил, в которых указан данный абонент в качестве источника или назначения.

Для поиска правила введите в поле ввода искомое правило или первые символы, по которым будет вестись поиск в списке правил, и нажмите сочетание клавиш <*Ctrl+F*>. При посимвольном поиске сочетание клавиш нажимается несколько раз.

Рисунок 212 - Поиск абонента в правилах МЭ

Добавление группы абонентов

Находясь курсором в списке абонентов окна параметров порта ФПСУ-IP (см. рис. «Абоненты порта ФПСУ»), при помощи комбинации клавиш <*Shift+Ins*> или <*Ctrl+N*> можно добавить группу хост-абонентов, IP-адреса которых начинаются с указанного. После нажатия любого из указанных сочетаний клавиш, появится окно добавления группы описателей типа «хост» с одинаковыми дополнительными параметрами.

Рисунок 214 - Групповое удаление абонентов

При нажатии кнопки *«Выполнить»*, все отмеченные описатели будут удалены. Для пометки знаком «v» описателя абонента следует установить на него курсор и нажать клавишу <*Пробел*>. Отметить можно сразу все доступные для удаления описатели абонентов, нажав клавишу <+>, <*Ctrl+Ins*> или <*Ctrl+B*>. Снять метки со всех описателей можно, нажав клавишу <–>, <*Ctrl+Del*> или <*Ctrl+D*>. При выполнении команды группового удаления происходит возврат в окно порта ФПСУ-IP.

- «Управление полосой пропускания» — переход в окно управления списком правил ограничения полосы пропускания для информационных обменов (traffic shaping), подробнее см. пункт «Управление полосой пропускания»;
- «Фильтрация трафика по содержимому» — переход в окно управления правилами пропускания http-трафика и сетевых протоколов приложений, подробнее см. пункт «Фильтрация трафика по содержимому (DPI)»;
- «Интервалы времени» — переход в окно управления списком разрешенных интервалов работы, подробнее см. пункт «Интервалы времени»;
- «Службы» — переход в окно управления списком шаблонов протоколов передачи данных, подробнее см. пункт «Службы»;
- «Группы IP-адресов» — переход в окно управления списком логических групп IP-адресов, к которым применяются правила дополнительной фильтрации, подробнее см. пункт «Группы IP-адресов»;
- «Параметры» — переход в окно управления списком дополнительных настроек, таких как параметры защиты от flood-атак и spoofing, подробнее см. пункт «Дополнительные параметры и защита от flood-атак».

Выход из подменю настроек правил дополнительной фильтрации в главное меню ФПСУ-IP осуществляется нажатием клавиши <*Esc*> или <*F2*>.

9. 1. Правила трафика

Переход в окно списка правил дополнительной фильтрации передаваемых данных осуществляется по нажатию кнопки «Правила трафика» меню Настройки «Параметров доступа»:

изменения без выхода из окна «Правила трафика».

Для создания нового правила трафика следует нажать клавишу <*Ins*> или кнопку «*Добавить*». Откроется окно добавления нового правила трафика (см. следующий пункт).

Для редактирования правила трафика следует выделить строку и нажать клавишу <*Enter*> или кнопку «*Правка*».

Для удаления правила трафика следует нажать клавишу <*Del*> или кнопку «*Удалить*».

Переход в таблице по строкам правил трафика осуществляется клавишами < > и <*v*>, по столбцам - клавишами << > и <> >, по экранам - клавишами <*PageUp*> и <*PageDown*>. Переход к первой строке производится по комбинации клавиш <*Ctrl+Home*>, переход к последней строке - <*Ctrl+End*>. Переход к первому столбцу производится по клавише <*Home*>, переход к последнему столбцу - <*End*>.

Ширина столбца изменяется по комбинации клавиш <*Ctrl* > > или <*Ctrl* < >.

Поиск правил трафика в таблице ведется с помощью комбинации клавиш <*Ctrl+F*>, продолжение поиска в таблице производится по клавише <*F3*>.

Строка правила трафика может быть дублирована по комбинации клавиш <*Ctrl+A*>. Новое правило будет вставлено в таблицу на позицию выше исходного правила, в комментарий будет добавлено «(copy)».

Вырезать строку правила можно комбинацией клавиш <*Ctrl+X*>. Для копирования строки правила нажмите комбинацию клавиш <*Ctrl+C*>. Вставить строку правила на позицию выше выбранной можно комбинацией клавиш <*Ctrl+V*>.

Перемещение правила трафика на одну позицию вверх или вниз осуществляется по комбинации клавиш <*Ctrl* > и <*Ctrl v*>.

Правило может быть создано, но не применено в межсетевом экране. Правило, применяемое в межсетевом экране, отмечается символом «v», требуется выделить строку правила и нажать клавишу <*Пробел*>.

9. 1. 1. Общие настройки правил трафика

В окне «Добавить правило» находятся четыре вкладки с настраиваемыми опциями.

Вкладка **Общие** (настройки) предназначена для выбора обязательного основного действия с передаваемым пакетом (сбросить или пропустить), и опциональных дополнительных действий. Символ «v» в конце настраиваемого поля обозначает наличие

В списке объектов вкладки **Источник** или **Назначение** могут быть внесены записи следующих типов (пояснение ведется для источника передаваемых пакетов, порядок действий для ведения списка назначения передаваемых пакетов аналогичен):

Адрес — для добавления в список обрабатываемых правилом источников отдельного IP-адреса, следует установить курсор на строке «Адрес», затем по нажатию клавиши <*Tab*> перейти на кнопку «*Добавить»* и нажать <*Enter*>. Указываемый в открывшемся окне IP-адрес должен быть предварительно описан в интерфейсе «Порты ФПСУ» как абонент любого типа, другой ФПСУ-IP, или маршрутизатор.

Рисунок 220 - Назначение источников для правила трафика

После выполнения команды *«Добавить»* следует указать Имя и IP-адрес добавляемого объекта, либо выбрать из списка маршрутизации:

которых внесены в соответствующие вкладки правила. Вкладка **Службы** позволяет ограничить действие правила не ко всем пакетам, а только тем, которые используют указанные в списке этой вкладки протоколы (службы). Шаблоны служб создаются администратором ФПСУ-IP в окне правил дополнительной фильтрации (см. пункт «Службы»).

Список примененных к правилу служб по умолчанию пуст:

Рисунок 226 - Пустой список служб у нового добавляемого правила

Введите в поле ввода искомую службу или первые символы, по которым будет вестись поиск в списке служб, и нажмите сочетание клавиш <*Ctrl+F*>. При посимвольном поиске сочетание клавиш нажимается несколько раз.

После подтверждения выбора службы клавишей <*Enter*>, в списке применяемых к правилу служб появится запись о добавленной службе:

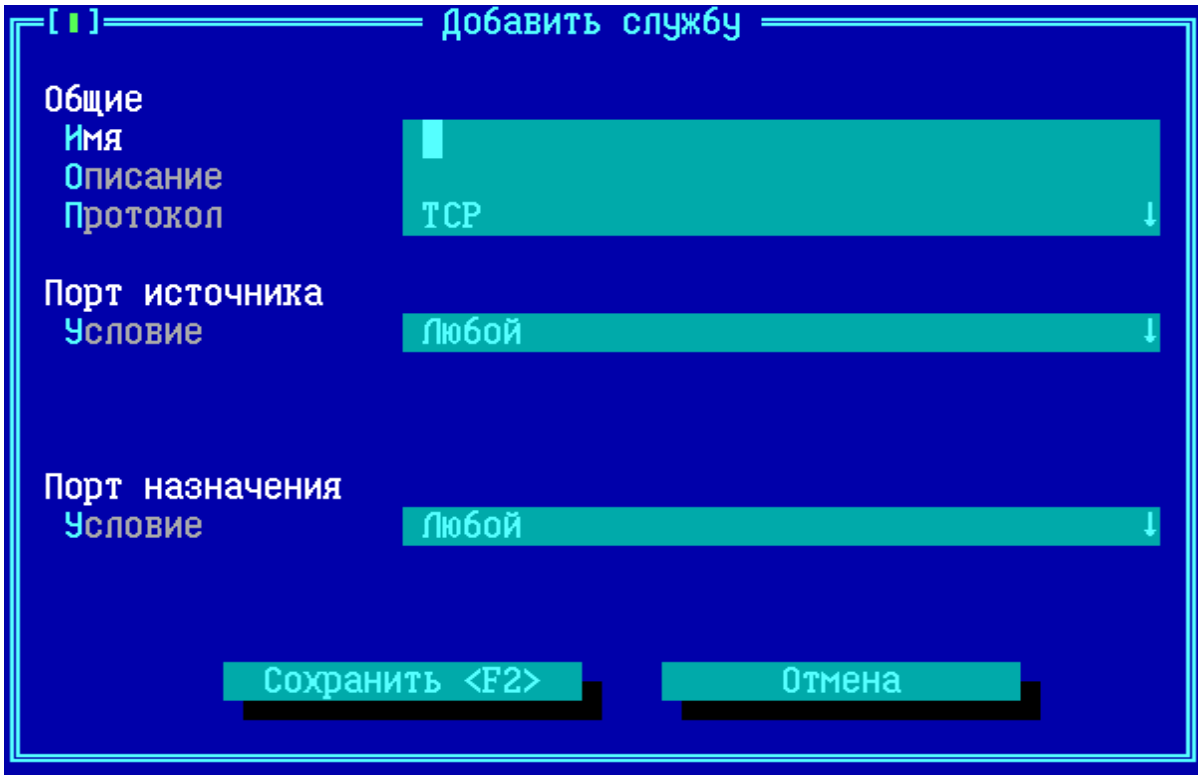

Рисунок 228 - Вкладка со списком служб правила трафика

Внести изменения в параметры выбранной курсором службы можно, нажав кнопку *«Изменить службу»* — при этом происходит переход в окно изменения настроек обрабатываемых протоколов (подробнее см. пункт «Службы»):

Рисунок 229 - Изменение службы из окна настроек правила доступа

9. 2. Службы

Действие создаваемого правила трафика (пункт «Правила трафика») можно ограничить, установив его применение не на все передаваемые данные, а только на пакеты определенного списка протоколов. Такое ограничение устанавливается с помощью специального контейнера: службы.

Переход в окно создания и управления списком доступных служб осуществляется по команде меню «Параметры доступа» > «Службы»:

Рисунок 230 - Команда «Службы» настроек правил доступа

В списке служб по умолчанию отображаются шаблоны популярных служб.

Рисунок 231 - Список служб

Рисунок 233 - Выбор сообщений ICMP в службе

Если правило трафика не должно применяться ко всем типам ICMP-сообщений, в службе при выборе протокола ICMP не следует включать флаг «[ ] Любой». Вместо этого можно отметить отдельные типы ICMP сообщений:

- *Ping* – тип ICMP сообщения «8» или «0», эхо-запрос доступности IP-адреса или ответ на эхо-запрос;
- *Redirect* – тип ICMP сообщения «8», эхо-запрос доступности IP-адреса;
- *Destination Unreachable* – тип ICMP сообщения «5», перенаправление маршрута передаваемого пакета;
- *Time Exceeded* – тип ICMP сообщения «11», истекло время жизни (TTL) IP-пакета;
- *Source Quench* – тип ICMP сообщения «4», сдерживание скорости передачи отправителя IP-пакетов;
- *Parameter Problem* – тип ICMP сообщения «12», сообщение о неверном параметре IP-пакета или отсутствии необходимой для дальнейшей передачи пакета опции.

9. 2. 2. Служба для запрета фрагментированных пакетов

При добавлении службы и выборе RAW в качестве параметра поля «*Протокол*», в изменившемся окне установки дополнительных параметров можно выбрать заранее созданный шаблон фильтра фрагментированных IP-пакетов.

Для этого следует перейти в поле «*Взять из шаблона*» и выбрать из выпадающего списка шаблон «*Фрагментированные IP пакеты*». Шаблон устанавливает настраиваемые ниже опции фильтра в следующие значения:

- флаг «Отрицание» – задействован;
- тип «Word»;
- смещение «6» (допустимое значение от 0 до 65535);
- маска «3fff»;
- начало «0»;
- конец «0».

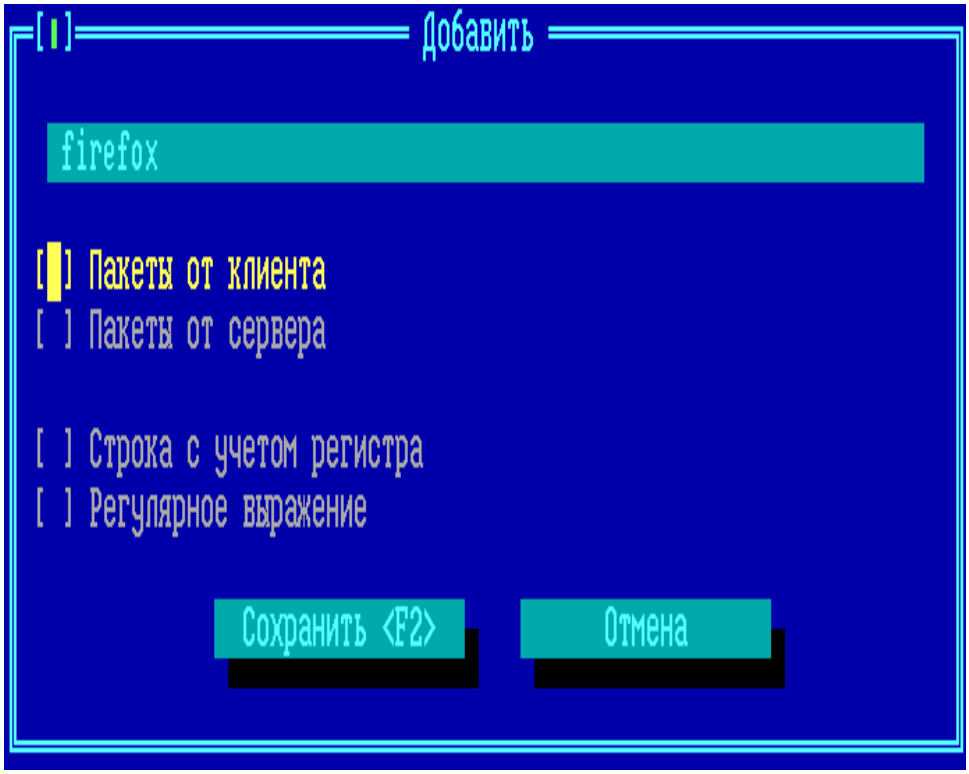

Рисунок 234 - Шаблон для фильтра фрагментированных IP-пакетов

После сохранения службы, её можно добавить к любому правилу **фильтрации трафика по содержимому** (см.«Фильтрация трафика по содержимому (DPI)») межсетевого экрана ФПСУ-IP.

При добавлении такой службы к правилу фильтрации трафика по содержимому межсетевого экрана ФПСУ-IP, у которого основным действием с пакетами является **Drop**, будут скинуты все пакеты, идущие от **источника**, в IP-заголовке которых установлен признак фрагментации передаваемых данных.

хотя бы одной из перечисленных символьных строк/регулярных выражений. Для удаления выбранной курсором записи нажмите клавишу <Del>.

Применение протокола REGEXP для частичной или полной блокировки приложений

Фильтр на основе протокола REGEXP может быть использован для частичной или полной блокировки прикладного программного обеспечения, которое использует в сетевых взаимодействиях характерный для него идентификатор на основе символьной строки.

Например:

Для блокировки сетевой работы браузера Mozilla Firefox следует создать следующие два активных правила фильтрации трафика по содержимому:

1) правило с основным действием Drop или Reject, протоколом HTTP и службой REGEXP со следующими параметрами:

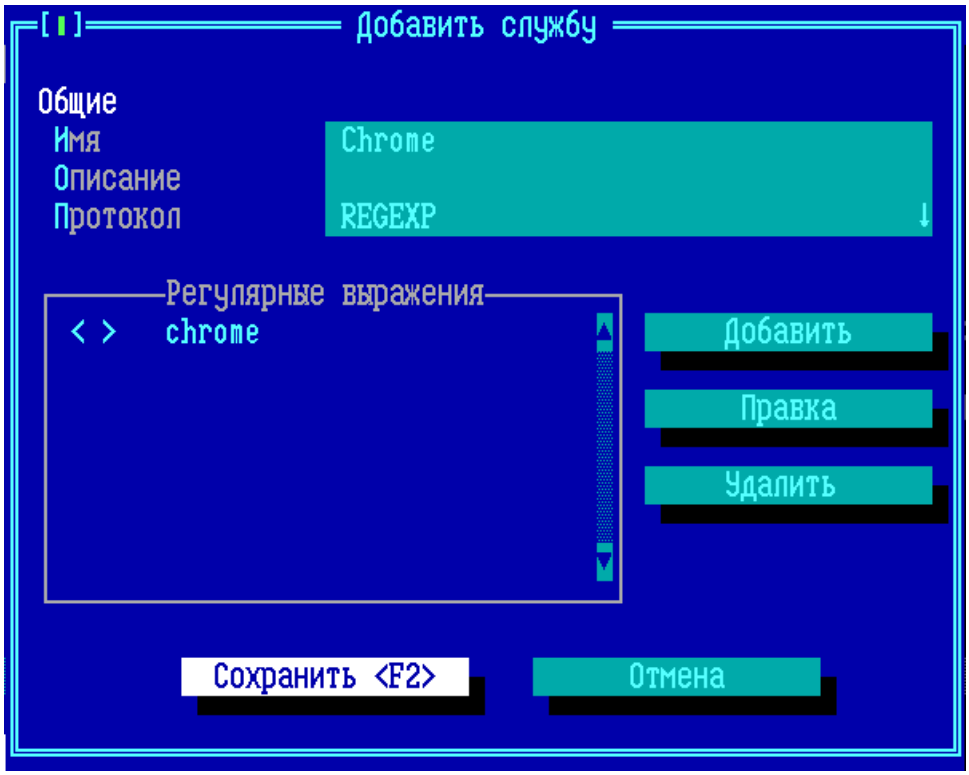

Рисунок 238 - Блокировка браузера Mozilla Firefox, правило 1

2) правило с основным действием Drop или Reject, протоколом FTP с дополнительным анализом по наличию FTP-запроса «OPTS»:

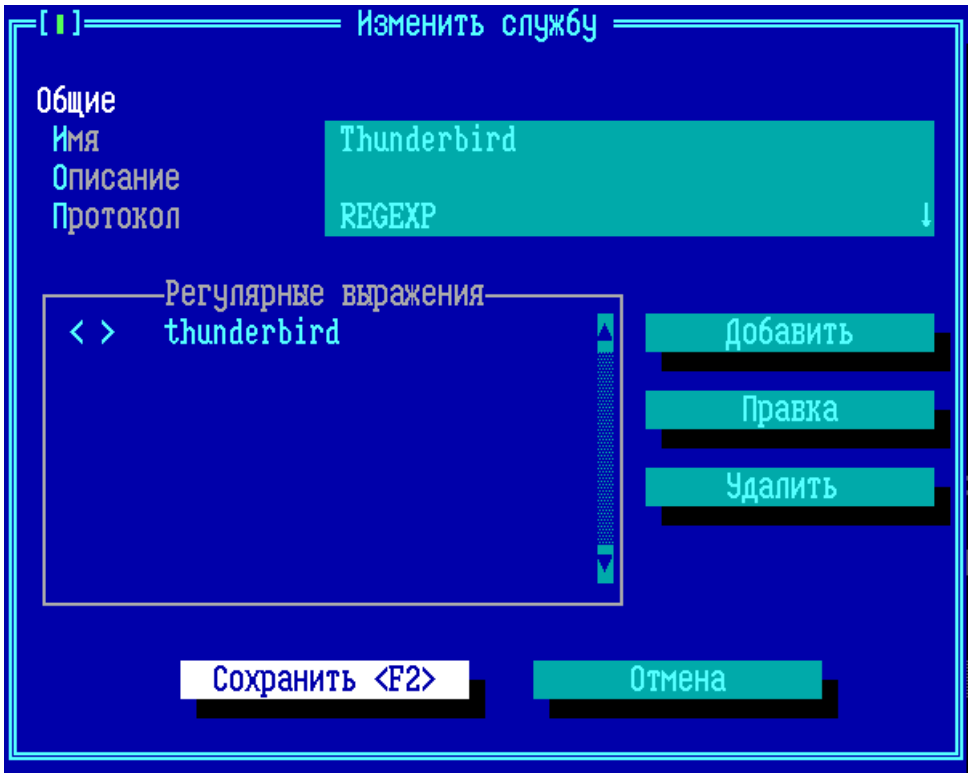

Рисунок 240 - Блокировка браузера Google Chrome, правило 1

2) правило с основным действием Drop или Reject, протоколом FTP с дополнительным анализом по наличию FTP-запроса «SIZE»:

Рисунок 242 - Блокировка работы почтового клиента Dreammail по протоколу SMTP

Для частичной блокировки сетевой работы почтового клиента Thunderbird, запрета работы по протоколу SMTP, следует создать активное правило трафика межсетевого экрана с запретительным основным действием (Drop или Reject) и службой REGEXP со следующими параметрами:

после чего для каждой записи списка указывает тип трафика и верхнюю границу скорости передачи данных этого типа трафика.

В окне «Управления полосой пропускания» отображен текущий список используемых на ФПСУ-IP правил ограничения скорости передачи данных. Правило по умолчанию одно — **Other —** не устанавливает никаких ограничений на скорость передачи трафика через ФПСУ-IP.

Управление полосой пропускания осуществляется только при активном межсетевом экране. Флаг «*Межсетевой экран активен»* указывает на работу дополнительных правил фильтрации и правил ограничений скорости передачи данных.

Рисунок 245 - Окно списка правил управления полосой пропускания

Для внесения изменений в конфигурацию без выхода из окна, нажмите кнопку «*Применить»*. Сохранение изменений с выходом в подменю «Настройки» осуществляется по нажатии клавиши <*F2*>.

Выход с отменой внесенных изменений осуществляется по нажатию клавиши <*Esc*>, кнопка «*Восстановить»* отменяет внесенные за последний сеанс администрирования изменения без выхода из окна «Управление полосой пропускания».

Передача (Kbit/sec) —установка разрешенной скорости передачи данных от источника к назначению, килобит в секунду (ВНИМАНИЕ! На ФПСУ-IP используется метрика 1 Kbit/sec = 1024 bit/sec). По умолчанию, не ограничено.

Время работы — выбор из ранее созданных интервалов времени (см. пункт «Интервалы времени»). Если выбран интервал времени работы, то подпадающие под действие правила трафика пакеты не будут пропускаться в запрещенное этим интервалом время.

Лог — если требуется вести журнал, содержащий разрешенные и запрещенные в рамках данного правила передачи данных, то следует выбрать из выпадающего списка опцию *Вести лог*.

Указанные выше настройки будут применяться только к передачам данных между сетевыми объектами, определяемыми во вкладках **Источник** и **Назначение**. Если во вкладке **Источник** и/или **Назначение** не указано сетевых объектов, ограничение скорости передачи данных будет применено ко всему исходящему или входящему трафику (подробнее про вкладки **Источник** и **Назначение** см. пункт «Вкладки «Источник» и «Назначение» правил трафика»).

На вкладке **Служба** устанавливаются ограничения в скорости передачи данных не для всего трафика между указанными сетевыми объектами, а только для подпадающего под дополнительные фильтры (подробнее про вкладку **Служба** см. пункт «Службы в правилах трафика»).

Перемещение между вкладками осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* > > и <*Ctrl* < > или клавиш <> > и << >.

Для того, чтобы все указанные в правиле службы после выхода с сохранением (<F2>) были задействованы, следует перед выходом установить флаг «*Активно*».

9. 4. Фильтрация трафика по содержимому (DPI)

В дополнение к фильтрации по правилам маршрутизации и правилам трафика межсетевого экрана, на ФПСУ-IP реализована фильтрация и принятие решения о блокировке пакета на основе передаваемого содержимого. Анализируются передаваемые данные различных протоколов, в том числе методы, контент и адрес http-запросов.

ВНИМАНИЕ! В случае использования версии ФПСУ-IP для виртуальной среды, виртуальной машине необходимо выделить минимум 2 гигабайта оперативной памяти для работы модуля фильтрации трафика по содержимому!

Переход в окно списка правил фильтрации трафика по содержимому передаваемых пакетов осуществляется выбором команды «Фильтрация трафика по содержимому» подменю «Настройки»:

Рисунок 247 - Меню настройки межсетевого экрана ФПСУ-IP

В открывшемся окне будет выведен список используемых на ФПСУ-IP правил фильтрации трафика по содержимому. Правило по умолчанию одно — **Other —** носит разрешительный характер, самый низкий приоритет, и не устанавливает никаких дополнительных ограничений к проходящим через ФПСУ-IP пакетам.

Время работы — выбор из ранее созданных интервалов времени (см. пункт «Интервалы времени»). Если выбран интервал времени работы, то пакеты, подпадающие под действие правила фильтрации трафика по содержимому, не будут пропускаться в запрещенное этим интервалом время.

Активно – флаг, задействующий данное правило при работе межсетевого экрана.

Перемещение между вкладками осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* > > и <*Ctrl* < > или клавиш <> > и << >.

Правило фильтрации трафика по содержимому применяется только к пакетам, IP-адрес источника или назначения указан во вкладке **Источник**. Исключение: если во вкладке **Источник** нет ни одной записи (список пуст), то правило фильтрации трафика по содержимому применяется ко всем пакетам.

Описание вкладки **Источник** и правил работы с ним см. пункт «Вкладки «Источник» и «Назначение» правил трафика». Отличие состоит в том, что добавить в список вкладки **Источник** можно только записи типа *Адрес*, *Сеть* и *Клиент*.

На вкладке **Служба** может быть дополнительно установлено, что правило фильтрации трафика по содержимому будет применено не ко всем пакетам указанных сетевых объектов, а только для подпадающих под дополнительные условия (подробнее см. пункт «Службы в правилах трафика»).

9. 4. 2. Исследуемый правилом фильтрации трафика по содержимому протокол

Правило фильтрации трафика по содержимому исследует передающиеся в IP-пакете данные на предмет используемого прикладного протокола, и – там, где это возможно – на предмет запрещенных для указанного протокола команд (например, команды STOR протокола FTP, обозначающую попытку загрузить файл на FTP-сервер).

Рисунок 255 - Доступные опции исследования протокола HTTP

При выборе опции «Метод» будет отрыто окно, где можно выбрать из выпадающего списка один или несколько фильтруемых правилом методов протокола HTTP:

Рисунок 260 - Служба для протокола RAW

2. Если требуется выполнить фильтрацию трафика по содержимому одновременно и по **Службам**, и по **Протоколу**, то потребуется создать два активных правила фильтрации трафика по содержимому.

В первом правиле требуется указать RAW-службу, по которой будет выполняться фильтрация. При этом во вкладке **Протоколы** требуется указать **другой протокол** (не тот, по которому требуется выполнить фильтрацию!). Например, если требуется исследование и фильтрация данных протокола SSH, то в первом правиле указывается любой другой из списка протоколов, например AFP.

Во втором правиле требуется во вкладке **Протоколы** указать протокол, по которому совместно со службой RAW будет выполняться фильтрация (SSH из примера выше). При этом вкладка **Службы** оставляется пустой, а во вкладке **Источник** требуется указать хотя бы один IP-адрес (рекомендуется брать из списка зарезервированных для специального использования IP-адресов, которые не должны назначаться сетевому оборудованию, например 198.051.100.1).

Приоритет этих двух правил относительно друг друга не важен.

сброшены. Для каждого состояния TCP-соединения используется одна запись в таблице контроля соединений межсетевого экрана ФПСУ-IP, но таймауты различаются.

Совместимость с FULL TRANSP. RiverBed – флаг, активирующий на ФПСУ-IP механизм совместимости с оптимизаторами трафика RiverBed, которые отклоняются от стандартных схем работы TCP-соединений (в том разрешение на пропуск ACK без данных).

Сброс TCP-пакетов с неверными флагами – флаг, указывающий межсетевому экрану ФПСУ-IP сбрасывать пакеты, в IP-заголовке которых обнаружены некорректные (не соответствующие рекомендуемым RFC) комбинации флагов протокола TCP.

Вкладка **Анти-флуд и СОВ** содержит параметры, по которым ФПСУ-IP определяет начало атаки в свои адреса или адреса защищаемых абонентов и управляет списком заблокированных IP-адресов.

Следует учитывать, что ФПСУ-IP **безусловно** переходит в режим защиты от flood-атаки, если оперативная память ФПСУ-IP загружается на 100%.

В режиме защиты от flood-атаки ФПСУ-IP использует тайминги удаления соединений, указанные во вкладке **Соединения**, а также заносит в стоп-лист IP-адреса абонентов, передающих больше пакетов в секунду, чем разрешено настройками.

10. Квантовое распределение ключей

В разделе содержатся сведения о настройке ФПСУ-IP 4-й версии для работы с устройствами квантового распределения ключей, описываются параметры настройки туннелей на квантовых и квантово-защищенных ключах.

В разделе приводятся сведения, необходимые администратору для подключения устройств системы выработки квантового распределения ключей (устройств СВКРК) к ФПСУ-IP. Указываются настройки, необходимые для построения VPN-туннелей с использованием квантовых и квантово-защищенных ключей.

Начиная с 4-й версии, ФПСУ-IP поддерживает работу с устройствами СВКРК. Для работы с СВКРК на ФПСУ-IP должны быть предварительно установлены дополнения «option_krk_pdu» и «ami-q_installer». Главное меню ФПСУ-IP, подготовленного для работы с устройствами СВКРК, содержит надписи «Криптомаршрутизатор "ФПСУ-IP Q"» и «модификация 4.0 Q».

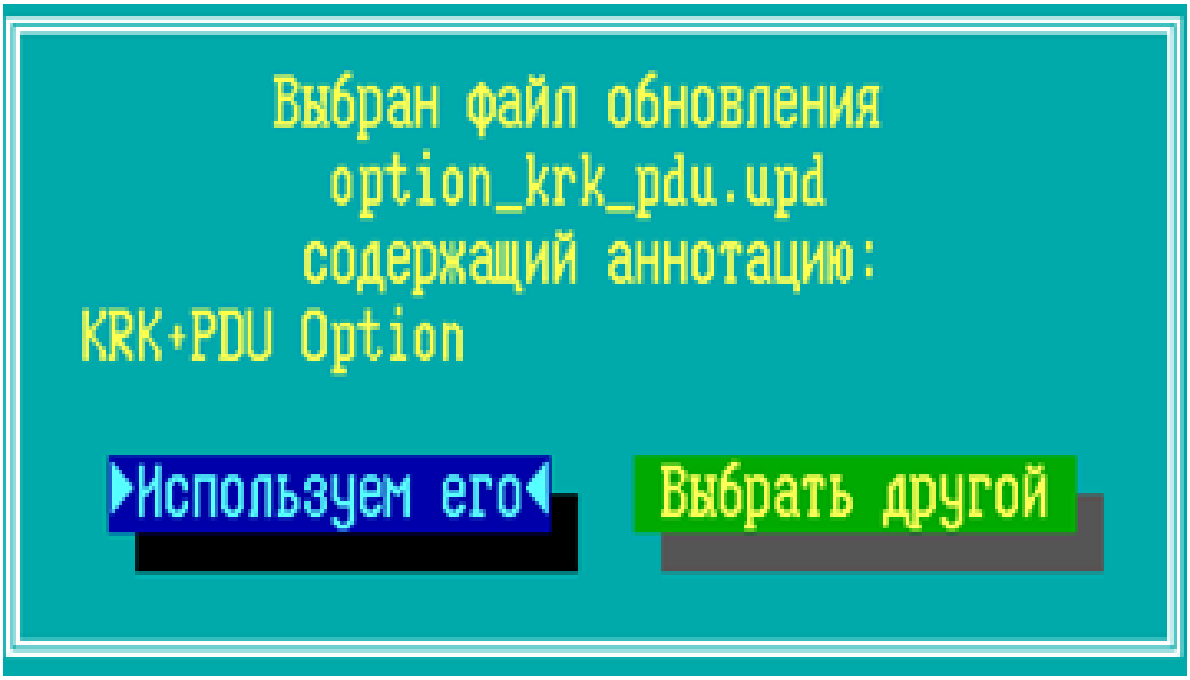

Рисунок 272 - Главное меню ФПСУ-IP с поддержкой СВКРК

Корректная работа дополнений поддерживается на всех аппаратных платформах ФПСУ-IP (см. примечание).

Примечание: аппаратная платформа FPSUIP-STD3 должна иметь не менее 4 Гб ОЗУ, аппаратная платформа FPSUIP-EXT3 должна иметь не менее 8 Гб ОЗУ.

Рисунок 275 - Выбор дополнения

3. В появившемся окне проверьте ещё раз параметры устанавливаемого дополнения и подтвердите продолжение установки командой «Используем его»:

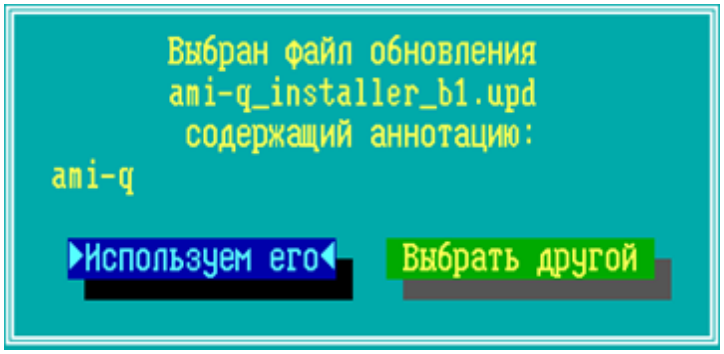

Рисунок 276 - Выбран файл с дополнением

4. Программа установки начнет копировать файлы дополнения на внутренний накопитель ФПСУ-IP. После успешного завершения копирования будет выдано оповещение о следующем шаге – процедуре установки дополнения. Подтвердите продолжение командой «Понятно»:

Рисунок 277 - Файлы дополнения скопированы

5. Запустится процедура обновления программного обеспечения. Критерием успешного выполнения будет служебное оповещение о необходимости перезагрузки операционной системы ФПСУ-IP. Подтвердите продолжение командой «Понятно»:

Рисунок 278 - Обновление установлено, требуется перезагрузка

6. После перезагрузки ФПСУ-IP проверьте результат установки дополнения, запустив ФПСУ-IP в режим фильтрации пакетов, нажав клавишу F1 и выбрав пункт «Информация об установленных подсистемах»:

10. 3. 2. Настройка СВКРК на сетевых адаптерах ФПСУ-IP

Порту ФПСУ-IP, к которому подключено локальное устройство СВКРК, должны быть назначены специальные MAC-адрес и IP-адрес. Это обязательное условие для корректного взаимодействия ФПСУ-IP с подключенным СВКРК.

MAC-адрес порта ФПСУ-IP должен соответствовать MAC-адресу соседнего СВКРК (того, с кем будет взаимодействовать локальный СВКРК).

Таблица соответствия MAC-адресов для настройки на ФПСУ-IP указана ниже:

Таблица. MAC-адреса СВКРК и ФПСУ-IP

Подключенный к ФПСУ-IP модуль	**Стандартный MAC-адрес СВКРК**	**MAC-адрес порта ФПСУ-IP**
СВКРК-А	FA:CE:AA:CC:EE:AA	FA:CE:B0:BB:0B:BB
СВКРК-Б	FA:CE:B0:BB:0B:BB	FA:CE:AA:CC:EE:AA

Например, если к порту ФПСУ-IP подключен СВКРК-Б со стандартными сетевыми параметрами, то MAC-адрес порта ФПСУ-IP должен быть установлен равным MAC-адресу соседнего СВКРК А:«**FA:CE:AA:CC:EE:AA**»:

увеличенным на единицу:«**192.168.000.221**»:

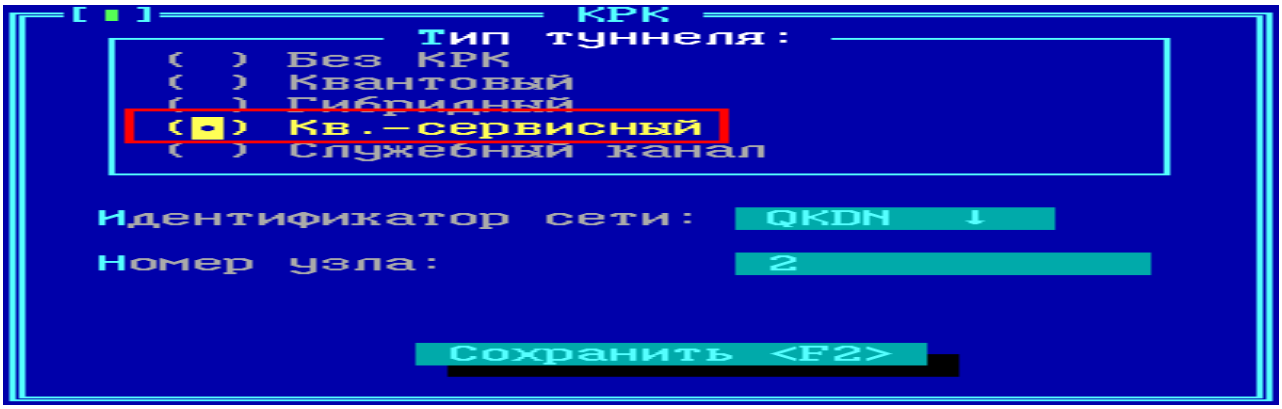

Рисунок 288 - IP-адрес порта ФПСУ-IP и КРК в списке абонентов

Следующим шагом потребуется внести IP-адрес подключенного к ФПСУ-IP СВКРК в список абонентов порта. Для этого следует внести в список абонентов запись типа «Хост» в режиме «Ретрансляция», с указанием сетевых параметров подключенного СВКРК (MAC-адрес и IP-адрес). Все остальные флаги записи должны быть установлены (все в поле «Режим партнера», «Отвечать на Ping»,«Работа разрешена»).

Например, если к порту ФПСУ-IP подключен СВКРК-Б со стандартными сетевыми параметрами, то запись абонента для СВКРК должна иметь следующие параметры:

Рисунок 289 - Запись абонента для подключенного СВКРК

- Тип записи: Хост;
- Адрес: 192.168.000.210;
- MAC: FACEAACCEEAA
- Флаги поле «Режим партнера», «Отвечать на Ping», «Работа разрешена» – установлены.

10. 4. Настройка квантовых туннелей

Для организации передачи данных пользователей по Квантовому туннелю, требуется выполнить на каждом ФПСУ-IP квантовой сети настройку параметров Квантового распределения ключей, указать параметры Квантовых и Служебных туннелей.

10. 4. 1. Настройка квантового распределения ключей на ФПСУ-IP

Настройка квантового распределения ключей на ФПСУ-IP – это первоначальная настройка, которую необходимо выполнить до настройки квантовых туннелей.

Рисунок 291 - Настройки квантового распределения ключей

В верхней части окна «СКЗИ-Распределитель» требуется установить следующие параметры:

«Идентификатор сети» – название квантовой сети. Четыре латинских символа. Параметр по умолчанию выставлен в значение «QKDN», изменять не требуется. Необходимость изменения Имени сети устанавливается администратором безопасности квантовой сети.

«Номер узла» – уникальный в пределах указанной сети номер, присваиваемый данному ФПСУ-IP. Номер согласуется с администратором безопасности квантовой сети и не должен быть произвольным.

Область «Системы выработки квантово-распределенных ключей». Для каждого квантового туннеля, который будет строить данный ФПСУ-IP, заполняется строка со следующими параметрами квантового туннеля:

«Модуль СВКРК» – выбирается модуль СВКРК, подключенный к текущему ФПСУ-IP. По согласованию с администратором безопасности квантовой сети делается выбор из двух основных вариантов «Отправитель (А)» или «Получатель (Б)». Дополнительные варианты включают в себя «Стыковочный узел» «Звезда (А)» «Звезда (Б)».

«IP-адрес» – в этом поле указывается IP-адрес устройства СВКРК, подключенного к текущему ФПСУ-IP. Стандартные IP-адреса указаны в пункте «Стандартные сетевые параметры СВКРК». Указанный IP-адрес должен быть указан в списке абонентов у порта ФПСУ, к которому подключен СВКРК.

«Соседний узел» – номер узла соседнего ФПСУ-IP, с которым будет строиться квантовый туннель. Номер узла согласовывается с администратором безопасности квантовой сети.

Например, если ФПСУ-IP участвует в построении квантовых туннелей, к его порту подключен СВКРК-А, на СВКРК-А установлены стандартные сетевые параметры, администратор безопасности квантовой сети выдал данному ФПСУ-IP номер узла, равный «1», квантовый туннель будет строиться с ФПСУ-IP с номером узла равным «2», к которому подключен СВКРК-Б, то в окне «Квантовое распределение ключей» - «СКЗИ-Распределитель» следует указать следующее:

Рисунок 292 - Пример настройки квантового распределения ключей

- Идентификатор сети – «QKDN»;
- Номер узла – «1»;
- Соседний узел – «2»;
- Тип СВКРК – «(А) Отправитель»;
- IP-адрес – 192.168.000.210;
- остальные поля оставить в значениях по умолчанию.

Гибридный туннель описывается на порту, привязанному администратором ФПСУ-IP к интерфейсу, подключенному к сегменту управления сети передачи данных. Рекомендуется выполнять подключение ФПСУ-IP к сегменту управления посредством специально выделенного сетевого интерфейса ФПСУ-IP.

Гибридный туннель между двумя ФПСУ-IP описывается следующим образом (см. рисунок ниже):

Включенные флаги «Важный объект», «Динамический», «Протокол ФПСУ-ФПСУ:UDP», параметры «Мост», «TOS в туннеле», «Выходные потоки» не являются обязательными настройками для создания Гибридного туннеля и должны устанавливаться по согласованию с администратором безопасности квантовой сети.

Маршрутизаторы – если присутствует пограничный маршрутизатор, который будет передавать пакеты от настраиваемого ФПСУ-IP до соседнего ФПСУ-IP, то его требуется указать в этом поле;

Тип туннеля – ФПСУ;

Адрес – адрес соседнего ФПСУ-IP в VLAN, предназначенном для передачи трафика к серверам управления (на примере – 192.168.010.002 с указанием VLAN=10);

Имя – произвольное название, необязательный параметр. При выборе гибридного туннеля в окне КРК будет предложено имя QKD-%номер_соседнего_узла% (Hyb) (QKD-2 (Hyb) на примере);

MAC – не задается;

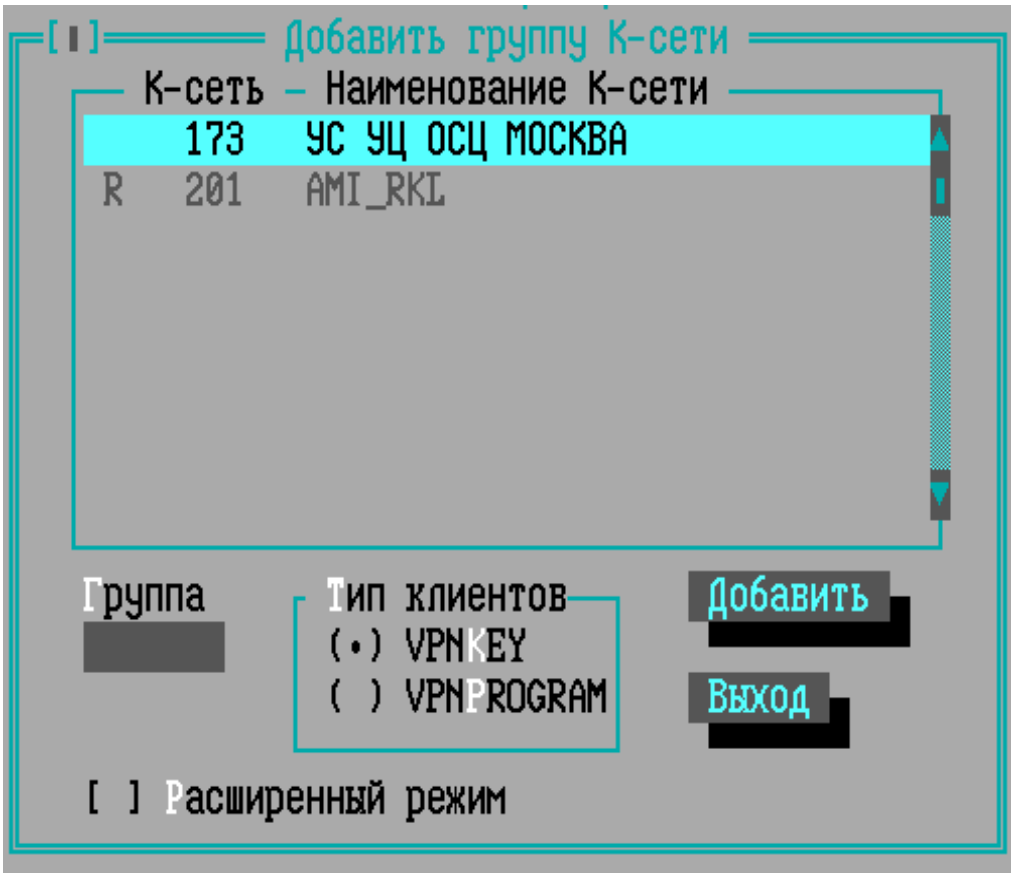

Рисунок 297 - Описание гибридного туннеля

Ключи – выбраны и установлены полученные от ЦВК парно-выборочные ключи, по согласованию с администратором безопасности квантовой сети;

Криптозащита – следует установить «Обязательно»;

Виды шифров – по согласованию с администратором безопасности квантовой сети, рекомендуется «по умолчанию»;

Сжатие данных – по согласованию с администратором безопасности квантовой сети, рекомендуется «Нежелательно»;

КРК – следует перейти в окно КРК и установить флаг «Гибридный», с указанием идентификатора сети и полученного от администратора безопасности квантовой сети номера узла, зарегистрированного за соседним ФПСУ-IP. Поле «Номер устройства» не заполняется (см. рисунок ниже):

11. Клиент для ФПСУ-IP

Под «клиентом» ФПСУ-IP в документе подразумевается ПАК «ФПСУ-IP/Клиент», предназначенный для защиты доступа отдельной рабочей станции к ресурсам сети передачи данных, защищенных ФПСУ-IP.

Взаимная аутентификация клиентов и ФПСУ-IP производится с использованием ключей, созданных при помощи специальной программы, СКЗИ «Центр генерации ключей клиентов» (далее ЦГКК).

В соответствии с иерархической структурой пользователей ПАК «ФПСУ-IP/Клиент», каждый клиент входит в логическую группу, а группы объединяются в системы (Криптосети Клиентов), принадлежащие, как правило, отдельным организациям. Таким образом, каждому клиенту ставится в соответствие совокупность системных идентификаторов - уникальных номеров (номер Криптосети, серия общесистемных ключей Криптосети, номер группы в Криптосети, номер клиента в группе, номер генерации для номера клиента).

ЦГКК вырабатывает общесистемный ключ Криптосети Клиентов, который может храниться в распределенном виде на нескольких электронных носителях Touch Memory (TM). Далее, ЦГКК на основе общесистемного ключа вырабатывает индивидуальные ключи клиентов, передаваемые на рабочие места «ФПСУ-IP/Клиент». Общесистемный ключ Криптосети Клиентов, хранящийся на TM-носителях, устанавливается на каждый ПАК ФПСУ-IP, который должен работать шлюзом для подключений клиентов.

На ФПСУ-IP/Клиент и ФПСУ-IP могут быть установлены две серии общесистемных ключей Криптосети Клиентов одновременно на период перехода с текущей серии на новую.

Администратор ФПСУ-IP регламентирует доступ клиентов к портам ФПСУ-IP и описывает правила их работы, а именно:

- явно указывает системные идентификаторы клиентов (номер криптосети, номер группы, номер пользователя), которые смогут работать через ФПСУ-IP;
- определяет совокупность рабочих станций, к которым клиенты могут получить доступ;
- указывает разрешенные IP-протоколы и время работы клиентов (календарный период, время суток по дням недели).

Нарушающие установленные ограничения запросы, так же, как и запросы от неизвестных клиентов, сбрасываются.

На время существования VPN-туннеля между ФПСУ-IP и клиентом, администратор ФПСУ-IP может передать обязательные настройки для рабочей станции клиента: во избежание динамического перехвата информации блокировать сторонние исходящие и

Криптосети Клиентов. Если ключи не используются в конфигурации ФПСУ-IP, их можно удалить с помощью клавиши <*Del*> или нажатием кнопки «*Удалить текущий <DEL>*».

Поле «КС№» – при выборе курсором Криптосети, внизу таблицы указывается класс защиты согласно требованиям ФСБ к шифровальным (криптографическим) средствам, КС1, КС2 или КС3.

Чтобы установить новые ключи, нажмите кнопку «*Установить <Ins>*», после чего на экран будут последовательно выдаваться приглашения на прижатие к контактному устройству всех ТМ-идентификаторов или на подключение к USB-порту USB TM-Key с первичными ключами, которые были выработаны ЦГКК.

Рисунок 303 - Ожидание ТМ-идентификатора

По мере предъявления ТМ-идентификаторов индикаторы готовности в нижней части экрана будут меняться с «–» на «+». Когда установка будет закончена и появится приглашение убрать ТМ-ключи. Нажмите клавишу «*Выход*», после чего название Криптосети Клиентов появится в списке установленных общесистемных ключей.

11. 2. Описание логической группы клиентов

Каждый Клиент обязан входить в логическую группу Клиентов. Если Групп Клиентов на ФПСУ-IP не указано, ФПСУ-IP не сможет принимать соединения Клиентов.

Создать запись логической группы клиентов можно только в том случае, если общесистемный ключ её Криптосети уже установлен на ФПСУ-IP (см. пункт «Установка и удаление общесистемных ключей»). Количество логических групп Криптосети на ФПСУ-IP не может превышать 128.

ВНИМАНИЕ! На аппаратных платформах с оперативной памятью меньше 8 ГБ введено ограничение на количество групп ФПСУ-IP/Клиентов – начиная с 3.30.b20 на таких платформах может работать не более 4 групп Криптосети Клиентов.

работы, причем для каждого клиента правила работы устанавливаются однозначно, то есть номера клиентов, входящих в одно описание, не могут повторяться в других описаниях.

Рисунок 307 - Пустой список описаний новой группы

Чтобы добавить в группу новое описание работы клиентов (с пустыми полями), нажмите <*Ins*> в окне списка описаний, а чтобы использовать имеющееся описание за основу – установите курсор на нужное описание и воспользуйтесь комбинацией клавиш <*Ctrl+Ins*>. В открывшемся окне введите имя для описателя диапазона номеров группы клиентов (произвольный текст-памятка для удобства администратора ФПСУ-IP) и нажмите кнопку *«Добавить»*.

Рисунок 308 - Наименование диапазона номеров

Появится окно указания параметров взаимодействия клиентов и ФПСУ-IP.

Рисунок 309 - Описание параметров работы диапазона Клиентов

Чтобы отредактировать/удалить существующее описание, воспользуйтесь соответствующими командами или клавишами <*Enter*>/<*Del*>.

ВНИМАНИЕ! Клиентам может быть предоставлен доступ со стороны каждого из портов ФПСУ-IP, поэтому некоторые параметры работы клиентов описываются отдельно для каждого порта.

Параметр	Описание параметра
	Данная опция важна для тех каналов, в которых происходят частые обрывы связи (например, PPP). В сочетании с опциями ПАК ФПСУ-IP/Клиент «Помнить введенный Pin-код пока VPN-Key не отсоединен» и «Автосоединение при подключении VPN-Key» (подробнее см. руководство пользователя ФПСУ-IP/Клиента) позволяет при таких разрывах автоматически восстанавливать туннель между Клиентом и ФПСУ-IP;
Описание активно	- указание ФПСУ-IP на активность описания. Если флаг не установлен в положение «X», работа клиентов данного диапазона будет блокирована. Флаг включается и выключается при помощи клавиши *<Пробел>*.

По нажатию кнопки «Локальные настройки» открывается окно с настройками ФПСУ-IP/Клиента, которые задаются на ФПСУ-IP и при соединении с ФПСУ-IP/Клиентом устанавливаются на клиенте, в этом случае настройки на клиенте недоступны для изменения.

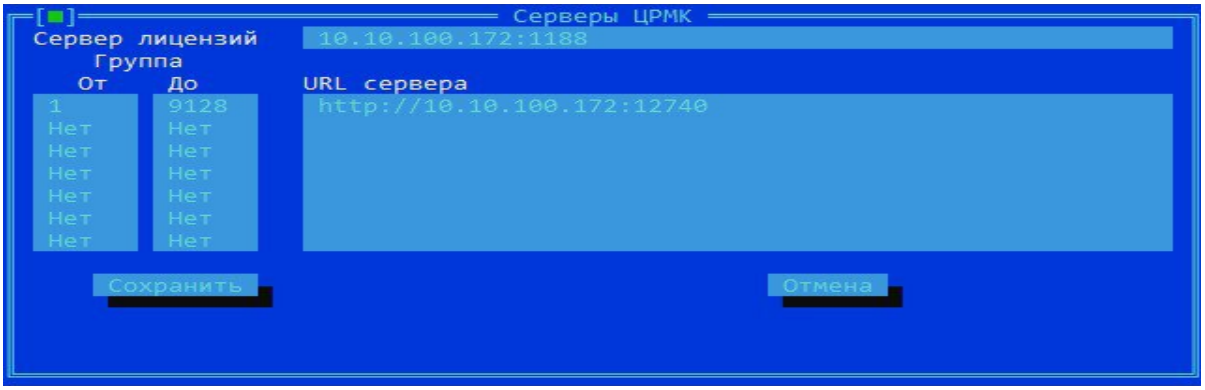

Рисунок 310 - Локальные настройки ФПСУ-IP/Клиента, устанавливаемые на ФПСУ-IP

Блокировать все пакеты, кроме IP-стека протоколов – установленный флаг означает, что при приеме и передаче все пакеты, не соответствующие формату пакетов стека TCP/IP, будут сброшены Клиентом.

Работа только через ФПСУ-IP, все остальные IP-пакеты блокируются – установленный флаг означает, что, при отсутствии соединения между ФПСУ-IP/Клиентом и ФПСУ-IP, рабочая станция или устройство с установленным программным обеспечением ФПСУ-IP/Клиент будет блокировать передачу в сеть всех IP пакетов, кроме служебных в адрес ФПСУ-IP. После установления соединения между ФПСУ-IP/Клиент и ФПСУ-IP блокировка передачи пакетов в сеть с помощью этой опции не осуществляется.

Рисунок 311 - Абоненты ФПСУ-IP, доступные ФПСУ-IP/Клиенту

Абонентами могут выступать описатели отдельного IP-адреса (столбец «Хост»), подсети (столбец «Подсеть»), диапазон последовательно идущих IP-адресов (столбец «Диапазон») и специальный абонент «DNS» (DNS-сервер).

Для добавления/удаления/редактирования описателя того или иного абонента для настраиваемой группы клиентов, перейдите в соответствующий столбец курсором и воспользуйтесь клавишами <*Ins*> (для добавления абонента), <*Del*> (для удаления), <*Enter*> или <*Пробел*> (для редактирования).

Настройки RKL – устанавливаемые для ФПСУ-IP/Клиентов настройки удаленной загрузки ключевых данных, передаются с ФПСУ-IP в момент соединения с ФПСУ-IP/Клиентом, позволяют удаленно обновлять ключевые данные ФПСУ-IP/Клиентам без участия администратора (см. пункт «Настройка диапазона клиентов на работу с RKL»).

Настройки Сервера лицензирования – устанавливаемые для ФПСУ-IP/Клиентов настройки удаленного автообновления программных лицензий, передаются с ФПСУ-IP в момент соединения с ФПСУ-IP/Клиентом, позволяют удаленно обновлять лицензии ФПСУ-IP/Клиентам без участия администратора до истечения срока действия лицензии, если

Рисунок 313 - Список зарегистрированных в группе Клиентов

Знак «v» около описания означает, что правила работы данного диапазона клиентов активны. Знак «–» означает, что правила работы данного диапазона клиентов установлены, но их работа временно блокирована. Описания содержат сведения о номерах клиентов, составляющих данный диапазон, о количестве клиентов в диапазоне и правилах NAT-трансляции.

Для сохранения списка описателей нажмите клавишу <*F2*> или кнопку «*Сохранить*», при этом система перейдет в режим отображения списка зарегистрированных на ФПСУ-IP клиентов логической группы.

Чтобы разрешить/запретить работу через ФПСУ-IP выбранному клиенту группы, воспользуйтесь клавишами <+>/<–>, а для диапазона номеров клиентов - клавишами <*Ins*> и <*Del*>.

Перемещение по списку осуществляется при помощи клавиш управления курсором, а перемещение по списку разрешенных (запрещенных) клиентов – при помощи клавиш <*Ctrl* v> (<*Alt* v>).

Pin-код - персональный идентификационный код текущей конфигурации ФПСУ-IP/Клиента, запрашивается при попытках доступа ФПСУ-IP/Клиента к ФПСУ-IP и при попытках редактирования текущего VPN-профиля. При использовании подсистемы RKL, Pin-код для VPN-профиля генерируется ФПСУ-IP и высылается ФПСУ-IP/Клиенту. Настройки pin-кода для профиля клиента устанавливаются на ФПСУ-IP – может быть задана ***Длина pin-кода***, по умолчанию 6 символов. В качестве pin-кода VPN-профиля ФПСУ-IP/Клиента может быть сгенерировано случайное число – флаг ***Случайный pin-код***. Также задаются способы рассылки pin-кода:

Отсылать pin-код вместе с профилем – флаг, при установлении которого профиль присылается ФПСУ-IP/Клиенту вместе с pin-кодом и при его сохранении дальнейшего ввода pin-кода для подтверждения операций не требуется. Дополнительно в настройках ФПСУ-IP/Клиента для профиля должен быть установлен флаг «Помнить введенный pin-код пока устройство не отсоединено» и задана «Пауза между попытками соединения».

Отсылать pin-код на ЦРМК-RKL – флаг, при включении отправляет pin-код на ЦРМК для хранения.

ВНИМАНИЕ. Настройки ***Случайный pin-код***, ***Отсылать pin-код вместе с профилем***, ***Отсылать pin-код на ЦРМК-RKL*** игнорируются, если диапазон номеров Клиентов из группы с установленным флагом «Расширенный режим» (группа отмечена буквой «**E**»), см. подробнее «Описание логической группы клиентов».

Автосоединение – при установлении флага будет производиться попытка соединения с ФПСУ-IP при подключении VPN-Key в USB-порт рабочей станции или устройства с установленным программным обеспечением ФПСУ-IP/Клиент, при выборе VPN-профиля, при старте ПО ФПСУ-IP/Клиент вручную, или после перезагрузки операционной системы (при наличии подключенного к устройству VPN-Key).

Автопривязка – установленный флаг позволяет привязать Клиента к рабочей станции или устройству с установленным программным обеспечением ФПСУ-IP/Клиент, чтобы пользователь данного VPN-Key (программно-аппаратного или программного) мог работать только на одном АРМ пользователя ФПСУ-IP/Клиент. Привязка клиента хранит данные о серийных номерах ОС (только для Windows), материнской платы и системного диска устройства с установленным программным обеспечением ФПСУ-IP/Клиент на устройстве. Каждый раз при подключении VPN-Key в USB-порт рабочей станции или устройства или выборе VPN-профиля эти данные сверяются, в случае подключения клиента с другого устройства работа данного клиента блокируется.

Автообновление ключа – флаг, позволяет планово (1 раз в год) удаленно обновлять общесистемные ключи на устройстве с установленным ПО ФПСУ-IP/Клиент. Для

Рисунок 323 - Настройки RADIUS

Основной/резервный адрес RADIUS сервера – в поле необходимо ввести IP-адрес сервера. RADIUS сервер разрешает или запрещает работу ФПСУ-IP/Клиента, в зависимости от полученных данных аутентификации, ФПСУ-IP получает аутентификационные данные и отправляет на RADIUS сервер.

DNS-имя – флаг, позволяющий вместо указания IP-адреса сохранить в настройках DNS-имя.

Порт основного/резервного сервера – в поле указывается номер порта сервера, установлено значение по умолчанию (порт 1812).

Пароль для аутентификации на сервере – ФПСУ-IP является RADIUS-клиентом и проходит аутентификацию на RADIUS-сервере с данным паролем. Требования к паролю определяются RADIUS-сервером.

В случае отсутствия ответа RADIUS сервера могут быть заданы ***Количество переповторов*** и ***Таймаут между переповторами***.

Доменный пароль – установить флаг, если требуется авторизация ФПСУ-IP/Клиента в домене.

OTP пароль – установить флаг, если используется двух-факторная авторизация ФПСУ-IP/Клиента с использованием временного OTP пароля.

Активно – флаг при включении задействует настройки RADIUS сервера на ФПСУ-IP.

Нажатие кнопки *«Сохранить»* или клавиши *<F2>* сохраняет настройки RADIUS и возвращает в окно описания абонентов для диапазона номеров.

11. 6. Настройка правил работы отдельного клиента

Период работы отдельного клиента может быть регламентирован при помощи индивидуальных настроек, вызываемых по нажатию клавиши *<F4>* в окне списка зарегистрированных в группе Клиентов, и содержит следующие настраиваемые параметры:

настройки блокировок недоступен.

протокола). Установки удаленного ФПСУ-IP по разделению потоков не влияют на выполнение описываемой функции конфигурируемым ФПСУ-IP.

Правила разделения потоков устанавливаются индивидуально для каждого VPN-туннеля, образуемого конфигурируемым ФПСУ-IP с соседними ФПСУ-IP, при описании параметров порта (см. пункт «Описание параметров удаленных ФПСУ-IP»). Однако с целью облегчения конфигурационных работ можно создать сначала «библиотеку» описателей правил, или общие правила-шаблоны, используемые потом в качестве заготовок при установке индивидуальных для каждого VPN-туннеля правил разделения потоков.

Общие правила разделения потоков могут быть описаны с использованием соответствующей команды меню конфигурации ФПСУ-IP. **ВНИМАНИЕ!** Операция по определению общих правил носит абстрактный характер, установленные здесь правила при работе комплекса не используются, а только служат «заготовками» при формировании параметров порта конфигурируемого ФПСУ-IP. Поэтому порядок следования общих правил в списке не имеет значения.

Рисунок 326 - Меню подсистемы конфигурирования ФПСУ-IP

По активизации команды «*Общие правила разделения потоков»* на экране появляется окно, содержащее список установленных общих правил или пустое, если правила еще не

Рисунок 329 - ФПСУ-IP в качестве сенсора IPFIX

Поддерживается протокол IPFIX (v. 10), основанный на протоколе Cisco NetFlow версии 9.

Доступ к окну настроек параметров учета трафика IPFIX на ФПСУ-IP предоставляется из меню «*Сетевые сервисы»* конфигурации ФПСУ-IP при выборе в подменю команды *«Учет трафика (IPFIX)»*.

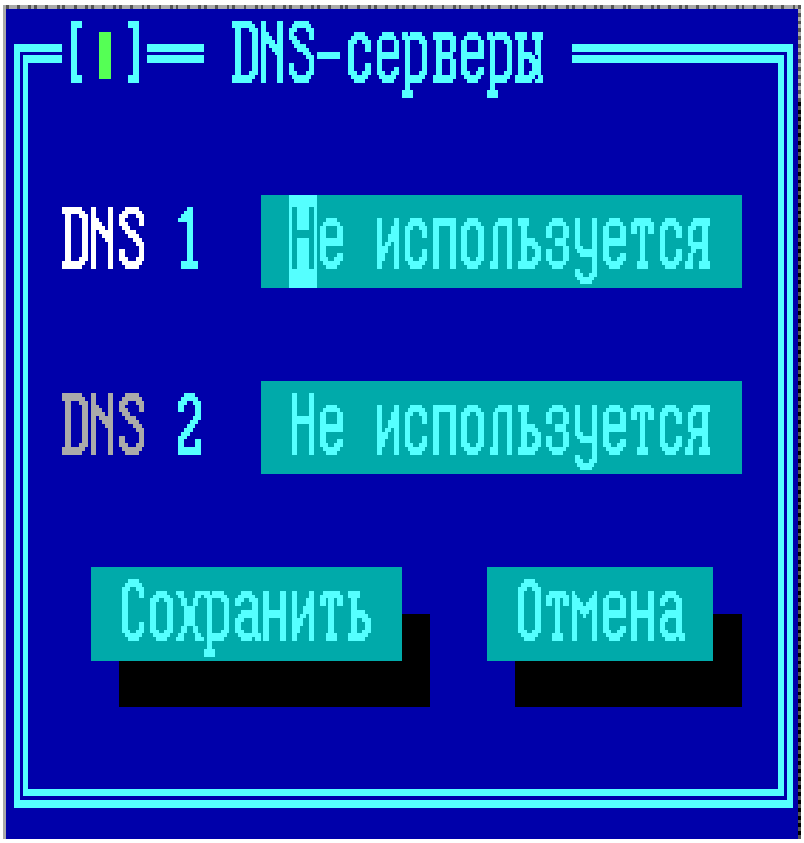

Рисунок 333 - Команда меню «Сетевые сервисы» > «SysLog/SNMP»

12. 3. 1. Настройка SysLog событий ФПСУ-IP

После выполнения команды «*SysLog/SNMP»* открывается интерфейс управления SysLog подсистемой на ФПСУ-IP. В левой части окна расположен список событий, при наступлении которых ФПСУ-IP следует выдать сообщение SysLog-серверу.

Рисунок 334 - Настройка параметров SysLog

Знак «+» с левой стороны от названия события означает, что оповещение о данном событии будет отправлено серверу SysLog. Включение или выключение отсылки оповещения о наступлении выбранного курсором строки события осуществляется клавишей <*Пробел*>. Серверу SysLog отправляются оповещения о следующих событиях:

Таблица 335. SysLog сообщения

Название события	Код события в тексте SysLog сообщения	Причина
Передача конфигурации АДМ	100001	Удаленный администратор ФПСУ-IP отправил запрос на получение конфигурации с ФПСУ-IP
Изменение конфигурации АДМ	100003	Удаленный администратор ФПСУ-IP передал на ФПСУ-IP и активизировал изменённую конфигурацию

Название события	Код события в тексте SysLog сообщения	Причина
Выключение ФПСУ	200004	Выход ФПСУ-IP из режима фильтрации пакетов
Перегруженность ФПСУ	200005	Загрузка ЦПУ ФПСУ-IP достигла порогового значения, указанного в параметре «Загрузка процессора, Предел»
MARK сообщения	200007	Служебное периодическое оповещение ФПСУ-IP о работоспособности комплекса
Соединение с клиентом	300001	Установлено защищенное соединение (туннель) с комплексом ФПСУ-IP/Клиент
Разъединение с клиентом	300002	Произошло разъединение защищенного соединения (туннеля) с комплексом ФПСУ-IP/Клиент
Переход Основной - Резервный	400001	Произошла передача управления партнёру по горячему резервированию
Нет связи Основной - Резервный	400002	Партнер по горячему резерву не ответил на запрос
Нет канала Основной - Резервный	400003	Отсутствует физический канал связи между партнерами по горячему резерву
Link UP порта	500001	Включение сетевого адаптера в сеть передачи данных
Link DOWN порта	500002	Прекращение работы сетевого адаптера с сетью передачи данных

указанного порта ФПСУ-IP.

Период MARK — временной диапазон, через который ФПСУ-IP отправляет на SysLog сервер периодическое служебное оповещение.

Сообщ/сек — максимальное количество SysLog-сообщений о событиях на настраиваемом ФПСУ-IP, отправляемое в секунду. Рекомендуется устанавливать значение не более 100.

Код UTF-8 — флаг, указывающий изменение кодировки отправляемых сообщений на UTF-8 (по умолчанию OEM/DOS 866). Включение или выключение осуществляется клавишей <*Пробел*>.

Загрузка процессора, Предел — отправка сообщения SysLog серверу о процентной загрузке центрального процессора ФПСУ-IP. Работает при включенном учёте события «*Перегруженность ФПСУ*». Если стоит значение «Нет», то сообщение будет отправляться вне зависимости от загрузки ЦПУ, если стоит числовое значение от 0 до 100, то сообщение будет отправляться только в случае загрузки ЦПУ, превышающей указанное предельное значение.

Загрузка процессора, Повтор — указание на периодичность отправки сообщений SysLog серверу о процентной загрузке центрального процессора ФПСУ-IP. Работает при включенном учёте события «*Перегруженность ФПСУ*» и/или «*Текущая загрузка ЦПУ*». Для события «*Перегруженность ФПСУ*». Если стоит значение «Нет», то сообщение будет отправлено однократно при наступлении события, если установить числовое значение — то, при продолжительном превышении предела загрузки ЦПУ, через каждый указанный промежуток времени сообщение будет отправляться повторно.

Перегрев процессора, Предел — отправка сообщения SysLog серверу о температуре центрального процессора ФПСУ-IP. Работает при включенном учёте события *«Перегрев»*. Если стоит значение «Нет», то сообщение будет отправляться вне зависимости от нагрева ЦПУ, если стоит числовое значение, то сообщение будет отправляться только в случае нагрева ЦПУ, превышающей указанное предельное значение в градусах Цельсия.

Перегрев процессора, Повтор — периодичность отправки сообщений SysLog серверу о температуре центрального процессора ФПСУ-IP. Работает при включенном учёте события *«Перегрев»* и/или «*Текущая Температура*». Для события *«Перегрев»* - если стоит значение «Нет», то сообщение будет отправлено однократно при наступлении события, если установить числовое значение — то, при продолжительном превышении предельной температуры ЦПУ, через каждый указанный промежуток времени сообщение будет отправляться повторно.

Повторы при потере связи, Связь горячего резерва **—** отправка сообщения SysLog серверу в случае отсутствия ответа от партнёра по горячему резерву. Работает при включенном учёте события «*Нет связи Основной - Резервный*». Если стоит значение «Нет», то сообщение будет отправлено однократно при наступлении события, если установить числовое значение — то, при продолжительном отсутствии связи с партнёром по горячему резерву, через каждый указанный промежуток времени сообщение будет отправляться повторно.

Повторы при потере связи, Связь с ФПСУ — отправка сообщения SysLog серверу в случае отсутствия ответа от удалённого ФПСУ-IP (см. пункт «Описание параметров удаленных ФПСУ-IP»). Работает при включенном учёте события «*Потеряна связь с ФПСУ*». Если стоит значение «Нет», то сообщение будет отправлено однократно при наступлении события, если установить числовое значение — то, при продолжительном отсутствии ответа от удаленного ФПСУ-IP, через каждый указанный промежуток времени сообщение будет отправляться повторно.

Параметры активны — флаг, при установлении которого включается обработка и отправка сообщений SysLog серверу, в поле под флагом основного и дополнительного SysLog сервера должен быть задан IP-адрес SysLog сервера. При выключенном флаге обработка и отправка сообщений SysLog серверу не происходит. Включение или выключение осуществляется клавишей <*Пробел*>.

Для сохранения изменений и выхода в меню общих настроек нажмите клавишу <*F2*> или кнопку «*Сохранить*». Для выхода в меню общих настроек без сохранения изменений нажмите <*Esc*>.

12. 3. 3. Формат отправляемых SysLog сообщений

По каждому из отслеживаемых событий, описанных в предыдущем пункте, ФПСУ-IP отправляет текстовое SysLog-сообщение, состоящее из нескольких информационных полей. Границы полей после поля «ФПСУ» обозначаются запятой «,».

Каждое сообщение начинается с обязательного для SysLog-сообщений от ФПСУ-IP заголовка, который состоит из следующих полей:

Таблица 338. Формат SysLog сообщения

Служебное число	Дата отправления сообщения с ФПСУ-IP	Серийный номер ФПСУ	ФПСУ	Код события	Имя события	Детали события	Номер ФПСУ в системе «горячего» резерва

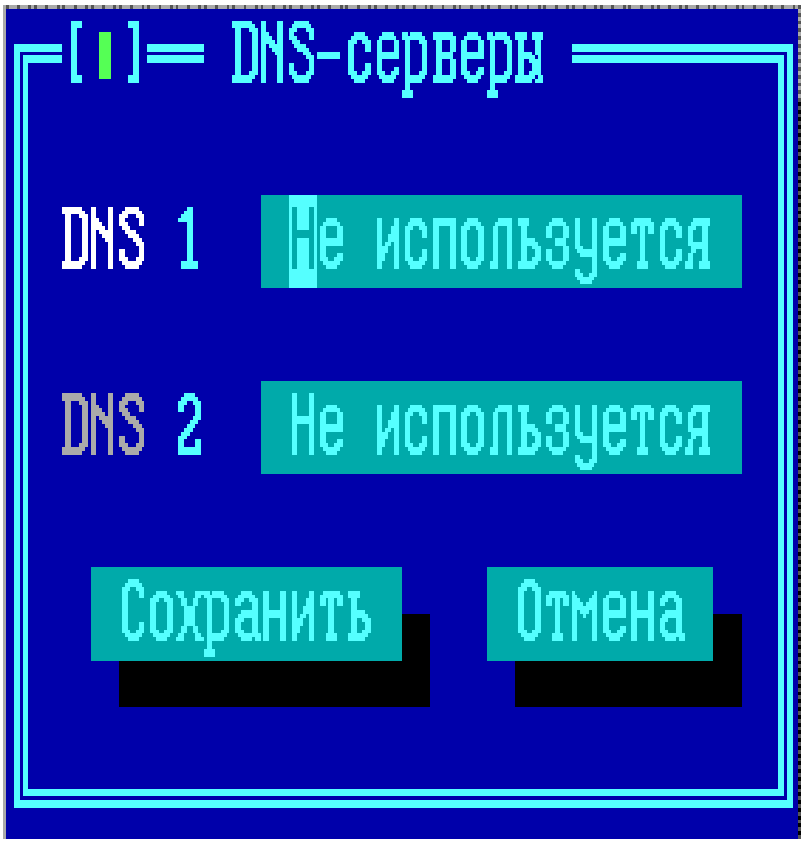

Рисунок 339 - Команда меню «Сетевые сервисы» > «SysLog/SNMP»

В правой нижней части окна настройки протокола SysLog и SNMP находится ряд параметров, относящихся к работе протокола SNMP на ФПСУ-IP. ФПСУ-IP может работать как в качестве SNMP-агента, отвечая на запросы, так и в качестве SNMP-trap, самостоятельно отправляя сообщения на указанный сервер.

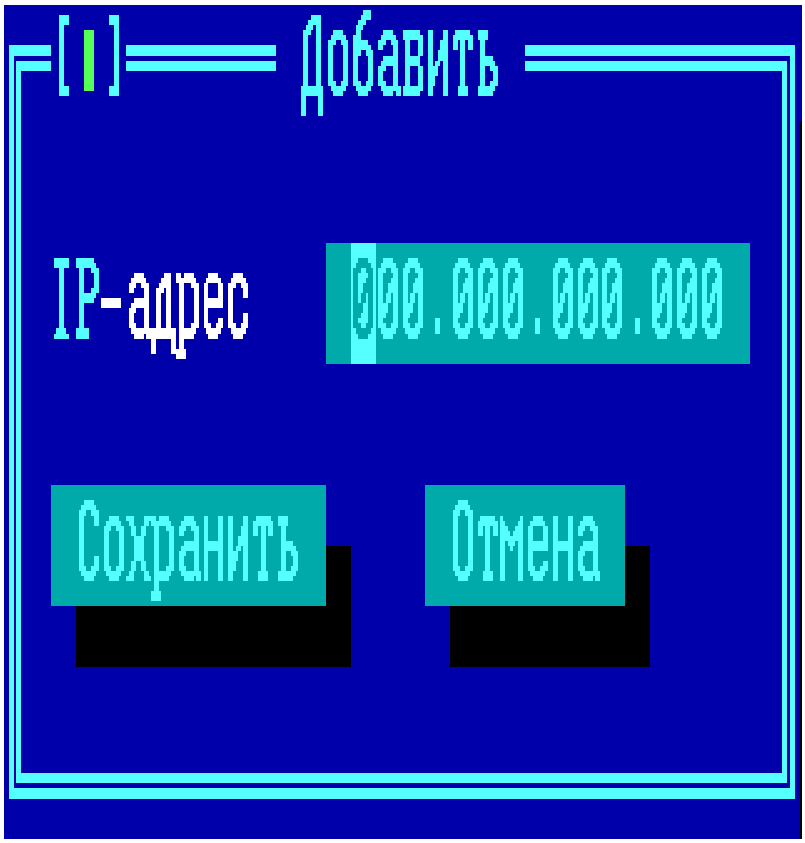

Рисунок 342 - Команда меню «Сетевые сервисы» > «DNS-серверы»

Откроется окно для задания основного и дополнительного DNS-сервера. IP-адреса DNS-серверов должны быть предварительно добавлены в конфигурации порта ФПСУ-IP как абоненты - записи типа «Хост» или «Подсеть», для которых установлен флаг *«Работа разрешена»* (см. пункт «Описание параметров абонентов»).

Рисунок 343 - Окно «DNS-серверы»

Приоритет DNS-серверов определяется очередностью указания. Если первый DNS-сервер не может ответить на запрос о разрешении имени хоста, запрос посылается на следующий DNS-сервер.

Для сохранения изменений и выхода в меню общих настроек нажмите клавишу <*F2*>

Рисунок 345 - Вкладка «DHCP»

Порт ФПСУ — IP-адрес интерфейса, который раздает адреса DHCP-клиентам.

Диапазон IP-адресов: *От, До* — диапазон допустимых IP-адресов подсети, которые могут арендовать абоненты ФПСУ-IP, DHCP-клиенты. ФПСУ-IP выдает DHCP-клиентам динамические IP-адреса из указанного здесь диапазона.

Маска — маска подсети IP-адресов, указанных в диапазоне для назначения DHCP-клиентам.

Шлюз — шлюз по умолчанию (маршрутизатор, соединяющий данную подсеть с другими подсетями), IP-адрес шлюза в подсети, который назначается DHCP-клиентам.

Суффикс — указывается, какой DNS-суффикс выдавать DHCP-клиентам. По умолчанию - пустой, DNS-суффикс DHCP-клиенту не выдается.

Аренда — продолжительность аренды выдаваемого DHCP-клиенту IP-адреса. Время указывается в секундах, по умолчанию составляет 3 часа (10800 секунд).

Только DNS-Relay — флаг, устанавливающий работу ФПСУ-IP в режиме ретрансляции DNS, клиенту не будут присылаться настройки внешних DNS-серверов. Если

флаг снят, DHCP-клиенту будут отправлены IP-адреса из полей *DNS 1 и DNS 2* в качестве основного и дополнительного DNS-сервера.

DNS 1, DNS 2 — IP-адреса DNS-серверов, которые отвечают на запросы о разрешении сетевых имен; после получения IP-адреса в аренду DHCP-клиент автоматически обновляет соответствующие DNS-записи. Серверы указываются в порядке предпочтения (DNS 1 - основной, DNS 2 - дополнительный).

Статические IP-адреса — список, содержащий зарезервированные IP-адреса для указанных MAC-адресов DHCP-клиентов. Абонент ФПСУ-IP запрашивает IP-адрес у DHCP-сервера, DHCP-сервер распознает MAC-адрес абонента и назначает ему соответствующий статический IP-адрес. Для DHCP-сервера может быть задан только список статических IP-адресов, в этом случае должен быть установлен флаг «Активно».

Для добавления статического IP-адреса в список нажмите кнопку *«Добавить»*, в открывшемся окне введите IP-адрес, MAC-адрес и сохраните по кнопке *«Сохранить»*.

Рисунок 346 - Добавление статического IP-адреса

Для изменения/удаления статического IP-адреса выделите его в списке клавишей <*Tab*> и нажмите кнопку *«Изменить»*/*«Удалить»*.

Активно — флаг при включении задействует настройки статических IP-адресов.

DHCP-сервер включен — флаг, включающий настройки DHCP-сервер на ФПСУ-IP.

DHCP-сервер и DNS-Relay включены — флаг, включающий работу протоколов.

ВНИМАНИЕ! Для работы DHCP-сервера с указанными настройками должны быть включены все три флага, «*Активно*», «*DHCP-сервер включен*!», «*DHCP-сервер и DNS-Relay включены*».

Вкладка **DNS-Relay** предназначена для настройки ретрансляции запросов DNS.

ФПСУ-IP поддерживает ретрансляцию запросов DNS. ФПСУ-IP получает DNS-запросы от абонентов, перенаправляет эти запросы на указанные в списке DNS-серверы и

Рисунок 349 - Команда меню «Сетевые сервисы» > «DHCP-Relay»

Список DHCP-серверов для ретрансляции по умолчанию пустой и в нём выведено служебное оповещение «Серверы не определены». Все IP-адреса, которые позднее будут использоваться в конфигурации порта ФПСУ-IP как DHCP-сервера для ретрансляции, должны быть предварительно добавлены в этот список.

Рисунок 350 - Список DHCP-серверов

Для добавления DHCP-сервера, нажмите клавишу <*Ins*> и введите его IP-адрес в появившемся окне.

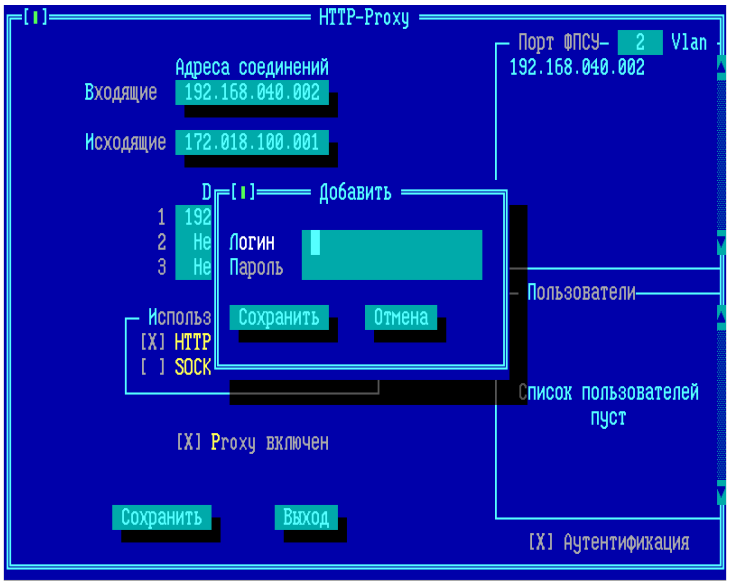

Рисунок 351 - Добавление DHCP-сервера

IP-адрес должен быть заранее описан в качестве абонента маршрутизации порта ФПСУ-IP, которому работа разрешена. То есть либо совпадать с адресом абонента типа хост, либо принадлежать подсети, описанной в качестве абонента (см. пункт «Описание параметров абонентов»).

Для удаления существующей записи IP-адреса из списка, установите курсор на строке и нажмите клавишу <*Del*>. Редактирование существующей записи выполняется по нажатию клавиши <*Enter*>.

ВНИМАНИЕ! Для включения сервиса DHCP-Relay требуется **включить** выключенный по умолчанию флаг *«DHCP разрешен»*.

После сохранения, IP-адрес можно использовать в конфигурации портов ФПСУ-IP в качестве получателя ретранслируемых DHCP-запросов (см. пункт «Настройка DHCP-Relay на портах ФПСУ»).

12. 7. 2. Настройка DHCP-Relay на портах ФПСУ

Для того, чтобы ФПСУ-IP ретранслировал DHCP-запросы, требуется для каждого порта (и каждого VLAN) ФПСУ-IP ***назначить*** основной и (опционально) запасной DHCP-сервер из **ранее заданного списка IP-адресов** (см. пункт «DHCP-сервер и DNS-Relay»). Таким образом, администратор определяет, куда ретранслировать пришедший DHCP-запрос, в зависимости от того, на какой порт (и в какой VLAN) он пришёл.

Рисунок 360 - Добавление учетной записи нового пользователя proxy ФПСУ-IP

Логин - имя для идентификации учетной записи нового пользователя прокси ФПСУ-IP;

Пароль - пароль для аутентификации учетной записи нового пользователя прокси ФПСУ-IP.

После указания логина и пароля к нему, нажмите кнопку «*Сохранить*». Новый пользователь прокси ФПСУ-IP будет добавлен в список:

Рисунок 361 - Новый пользователь proxy ФПСУ-IP добавлен

После сохранения указанных настроек, только пользователь, указавший логин учетной записи прокси User1 и корректный пароль к ней, сможет воспользоваться работой через прокси ФПСУ-IP. Успешные и не успешные попытки авторизации пользователей на прокси ФПСУ-IP записываются в статистику.

Удаление учетной записи пользователя осуществляется клавишей <*Del*> при установленном на удаляемой учетной записи пользователя курсоре.

Для выхода из окна и возвращение в меню конфигурации ФПСУ-IP с сохранением выполненных настроек, нажмите кнопку «*Сохранить*» или клавишу <*F2*>.

Для выхода из окна и возвращение в меню конфигурации ФПСУ-IP без внесения в конфигурацию сделанных изменений, нажмите кнопку «*Выход*» или клавишу <*Esc*>.

12. 9. Взаимодействие со средствами обнаружения вторжений

ФПСУ-IP поддерживает взаимодействие со сторонними средствами обнаружения вторжений (далее СОВ). На ФПСУ-IP реализован специальный SysLog сервер, принимающий сообщения по протоколу syslog, отправленные с одного IP-адреса СОВ,

регистрации осуществит поиск и выдаст результат на экран:

Рисунок 372 - Результат запроса статистики

Обратите внимание, что поиск будет выполняться лишь в том случае, если отмечен хотя бы один раздел запрашиваемых данных.

Данные выдаются в виде записей с указанием времени регистрации и типа события. Для текущей (отмеченной курсором) записи в нижней строке экрана указываются дополнительные сведения.

Выданные данные могут быть записаны на внешний носитель по нажатию комбинации клавиш <*Alt+W*>. Данные будут записаны на носитель в специальном формате и могут быть прочитаны средствами программно-аппаратного комплекса «Удаленный администратор ФПСУ-IP», который также поддерживает возможность конвертации записей статистики в текстовый формат для последующей обработки.

Для некоторых записей в нижней части окна отображается приглашение на получение дополнительной информации.

13. 2. Выдача системного журнала

Команда «Выдать системный журнал» окна просмотра статистики ФПСУ-IP («Статистика ФПСУ-IP») позволяет выдать на внешний носитель (USB-flash) файл с системным журналом статистики.

Рисунок 373 - Команда выдачи журнала изменений конфигурации межсетевого экрана

После выполнения команды система предложит подключить USB-носитель, на который будет выдан файл, к ФПСУ-IP:

Рисунок 374 - Предложение подключить USB-носитель

Подключите носитель к ФПСУ-IP и подтвердите выполнение команды, нажав клавишу <*Enter*>. Если USB-носитель будет обнаружен ФПСУ-IP, то откроется окно

диалога, в котором следует выбрать каталог на носителе.

Рисунок 375 - Выбор каталога для выгрузки файла

Подтвердите место выгрузки файла, выполнив команду *«Каталог выбран»*.

После выгрузки файла, ФПСУ-IP выдаст системное оповещение о завершении процедуры:

Рисунок 376 - Сообщение о завершении процедуры

13. 3. Выдача журнала изменений конфигурации межсетевого экрана

Команда «Выдать изменения КФГ» окна просмотра статистики ФПСУ-IP позволяет выдать на внешний USB-носитель файл с журналом изменений конфигурации ФПСУ-IP.

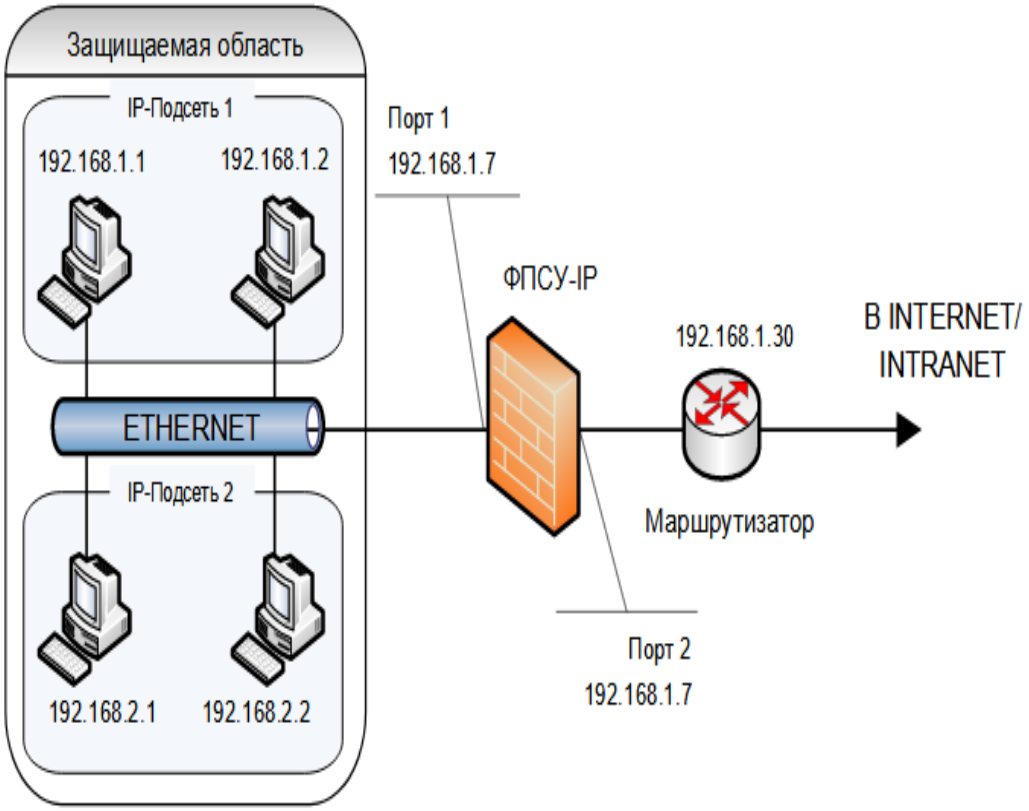

Рисунок 379 - Выбор каталога для выгрузки журнала

Подтвердите место выгрузки журнала, выполнив команду «Каталог выбран».

После выгрузки журнала, ФПСУ-IP выдаст системное оповещение о завершении процедуры:

Рисунок 380 - Сообщение о завершении процедуры

Полученный журнал можно открыть текстовым редактором на другом ПЭВМ для просмотра и анализа изменений.

14. Восстановление работы ФПСУ-IP после сбоев

Сбои оборудования не влияют на защитные функции ФПСУ-IP, но некоторые аппаратные неполадки могут нарушить его работоспособность, что приведет к изоляции защищенного им сегмента сети передачи данных.

При авариях таких аппаратных компонент ФПСУ-IP, как ЦПУ, материнская плата и др., неисправные устройства заменяются, после чего ФПСУ-IP запускается заново и продолжает свою работу.

Работоспособность сетевых адаптеров ФПСУ-IP автоматически контролируется им во время работы по специальным признакам аппаратного уровня, сигнализирующим о его неработоспособности. При выявлении описанных признаков, драйверы сетевых адаптеров и подсистемы фильтрации ФПСУ-IP полностью перезагружаются. Для реализации данного механизма восстановления при настройке комплекса в параметрах конфигурации должно быть установлено время, по истечении которого будет осуществлен аварийный перезапуск комплекса (см. раздел «Общие параметры конфигурации ФПСУ-IP»). Если работоспособность восстановить не удается, ФПСУ-IP переходит в режим звукового оповещения администратора для принятия мер по замене неисправного оборудования. Если замена оборудования повлечет за собой изменения в программных настройках LAN-адаптеров, такая операция доступна только локальному администратору с правами не ниже «*Инженер*».

При необходимости, ПЗУ ФПСУ-IP может быть переставлено на другой ФПСУ-IP (ПЗУ на ФПСУ-IP должен оставаться единственным).

Аварии ПЗУ (SSD) ФПСУ-IP, влекущие за собой необходимость его замены и повторной установки ПО ФПСУ-IP на новый, наиболее критичны в смысле времени восстановления работоспособности ФПСУ-IP и защищаемой им ЛВС, поскольку все рабочие установки ФПСУ-IP и записанные на носитель данные будут потеряны. Одна из опций конфигурации ФПСУ-IP позволяет настроить его на такой режим работы, что при возникновении фатальной ошибки в результате сбоя или отказа ПЗУ ФПСУ-IP продолжит функционировать без регистрации событий в хранилище ФПСУ-IP (если политика безопасности организации это позволяет). При этом подсистема мониторинга не прекращает своей работы, и контроль за процессом фильтрации может осуществлять удаленный администратор с помощью ПАК «Удаленный администратор ФПСУ-IP».

Для быстрого восстановления работы рекомендуется хранить текущую конфигурацию ФПСУ-IP на внешнем носителе. В таком случае при смене внутреннего накопителя и повторной инсталляции ПО ФПСУ-IP (или замене всего устройства ФПСУ-IP) администратор может восстановить конфигурацию ФПСУ-IP с внешнего носителя, после

15. 1. Базовая настройка ФПСУ-IP для ретрансляции пакетов локальной сети

Предположим, что IP-сеть организации до установки ФПСУ-IP представляла одну подсеть с IP-адресом 203.0.113.0 и маской 255.255.255.0 (24 разряда) и содержала маршрутизатор для выхода в другие IP-сети. IP-адреса 1 и 2 портов ФПСУ-IP совпадают, для ФПСУ-IP это допустимо, если в локальной сети доступно ограниченное количество свободных IP-адресов. После установки ФПСУ-IP топология сети приобрела вид, отображенный на схеме ниже.

С точки зрения конфигурирования ФПСУ-IP для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны порта 1 (защищаемая область) существует одна подсеть; маршрутизаторы и другие ФПСУ-IP, через которые абоненты будут доступны с порта 1, отсутствуют;
- со стороны порта 2 абоненты не определены, доступ к ним будет осуществляться через маршрутизатор (по IP-адресу связанного с ФПСУ-IP порта), а другие ФПСУ-IP отсутствуют;
- обмен абонентов защищаемой области с абонентами Internet/Intranet может производиться только в режиме ретрансляции. Сжатие и криптозащита трафика не применяется;
- работа с ключевыми данными при такой топологии не требуется.

Рисунок 384 - Применение ФПСУ-IP для защиты оконечной области

Конфигурация ФПСУ-IP должна содержать следующие установки:

15. 2. Защита локальной сети, состоящей из двух IP-подсетей

Представим теперь, что защищаемая область состоит из двух IP-подсетей, абоненты которых должны обмениваться пакетами не только с абонентами Internet/Intranet, но и друг с другом, причем эти обмены также должны фильтроваться установленным ФПСУ-IP. В таком случае пакеты от абонентов IP-подсети 1 будут передаваться на порт 1 комплекса ФПСУ-IP, с которого они будут передаваться обратно в защищаемую область и доставляться абонентам IP-подсети 2 (аналогично будут передаваться пакеты абонентов подсети 2, направленные абонентам подсети 1). IP-адреса 1 и 2 портов ФПСУ-IP совпадают, для ФПСУ-IP это допустимо, если в локальной сети доступно ограниченное количество свободных IP-адресов.

Такая организация защищаемой подсети приведет к следующей логике конфигурирования:

На порту 1 ФПСУ-IP должны быть описаны две различные IP-подсети и для каждой подсети (или ее отдельных абонентов) должна быть разрешена работа с партнером своего порта в режиме «ретрансляции». Кроме того, все хосты защищаемой области должны быть сконфигурированы таким образом, чтобы в качестве маршрутизатора по умолчанию у них был указан маршрутизатор с адресом 192.168.1.30 или IP-адрес 1-го порта ФПСУ-IP.

На работу подсети наложены следующие ограничения:

- хост с IP-адресом 192.168.1.1 является администратором маршрутизатора, обмен IP-пакетами с подсетью 2 ему запрещен; кроме того, он должен иметь круглосуточный доступ в сеть Internet/Intranet;
- остальные хосты подсети 1 и хосты подсети 2 имеют доступ друг к другу и не должны взаимодействовать с Internet/Intranet.

```
флаг "Работа разрешена" включен.
Хост; 203.0.113.5;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 203.0.113.6;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 203.0.113.8;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 203.0.113.9;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
```

Исходя из принципов конфигурирования ФПСУ-IP, со стороны одного из портов (в текущем примере - с порта 1) описана вся подсеть через хост вида «подсеть» с указанием адреса и маски сети (это сделано для простоты конфигурирования, чтобы не указывать индивидуальные адреса всех входящих в подсеть со стороны данного порта хостов), а со стороны противоположного порта - указаны индивидуальные адреса хостов, физически присутствующих с этой стороны, для регламентирования передачи индивидуальных пакетов и один повторный описатель типа «Подсеть» для регламентации широковещательных передач.

Для абонента 203.0.113.1 запрещение работы с абонентами области 2 осуществляется через выключение флага «Работа разрешена».

15. 4. Использование ФПСУ-IP для создания VPN-туннелей

Рассмотрим ситуацию, когда сеть организации представляет из себя отдельные локальные IP-подсети, разделенные территориально и связанные через участки WAN-сети

общего пользования. В таком случае, для обеспечения защищенного взаимодействия локальных подсетей, необходимо на выходе каждой из них установить ФПСУ-IP (со стороны внутреннего порта пограничного маршрутизатора) и организовать между ФПСУ-IP VPN-туннели через WAN-сеть общего доступа, по которым данные абонентов будут передаваться с использованием всех механизмов защиты, включая аутентификацию и, возможно, сжатие.

Предположим, что организация использует следующие IP-адреса:

- защищаемая область A - 192.168.1.0, маска 255.255.255.0 (24 бита);
- защищаемая область B - 192.168.2.0, маска 255.255.255.0 (24 бита);
- защищаемая область C - 192.168.3.0, маска 255.255.255.0 (24 бита);
- внутренний порт маршрутизатора A -192.168.1.1;
- внутренний порт маршрутизатора B -192.168.2.1;
- внутренний порт маршрутизатора C -192.168.3.1.

Для ФПСУ-IP в каждой подсети будут выделены адреса .50.

На работу сети наложены следующие ограничения:

- хосты из всех защищаемых областей должны иметь круглосуточный доступ друг к другу;
- управление пограничными маршрутизаторами (A, B, C) должно осуществляться только из защищаемой области C.

После установки ФПСУ-IP сеть организации имеет вид, представленный на рисунке ниже.

Рисунок 387 - Схема локальной сети с применением ФПСУ-IP

С точки зрения конфигурирования ФПСУ-IP A, B и C для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны внутреннего порта каждого ФПСУ-IP (например, порта 1) существует одна соответствующая IP-подсеть, а со стороны порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы и ФПСУ-IP отсутствуют;
- со стороны порта 2 существуют две IP-подсети, а со стороны порта 1 хостов, принадлежащих этим подсетям, нет; доступ к ним будет осуществляться через соответствующий удаленный ФПСУ-IP;
- обмен между защищаемыми областями должен производиться только внутри организованных ФПСУ-IP VPN-туннелей;
- на каждом ФПСУ-IP должны быть установлены ранее выработанные криптографические ключи парно-выборочной связи. Причем на ФПСУ-IP A указан используемый номер ключа 1, на ФПСУ-IP B - номер 2 и на ФПСУ-IP C - номер 3;
- со стороны внешнего порта ФПСУ-IP установлены пограничные маршрутизаторы, управление которыми должно осуществляться только из защищаемой области C, причем каналы управления маршрутизаторами за пределами их внешних портов должны быть защищены ФПСУ-IP.

В данном случае возможны два различных варианта конфигурации ФПСУ-IP,

подсеть с IP-адресом 192.168.1.0 и маской 255.255.255.0 (24 разряда), требуется передавать пакеты внутри локальной сети, разделенной географически. Для того, чтобы организовать такую «прозрачную» защищенную передачу данных, достаточно на внешних портах ФПСУ А и ФПСУ В создать описатель партнера по шифрованию и включить режим моста для туннеля ФПСУ А - ФПСУ В.

При этом на внутренних портах ФПСУ А и ФПСУ В не должно быть описано абонентов (хостов, подсетей, записи «любой хост») - пакеты от явно указанных на портах ФПСУ-IP абонентов не передаются в туннель типа «мост» (подробнее см. пункт «Режим «Мост» между ФПСУ-IP (L2-шифрование)»):

Рисунок 390 - L2-туннель типа "мост"

Используются следующие IP-адреса:

- защищаемая область А - 192.168.1.0, маска 255.255.255.0 (24 бита);
- внутренний порт ФПСУ А -192.168.1.50;
- внешний порт ФПСУ А -203.0.113.1;
- внутренний порт ФПСУ В -192.168.1.51;
- внешний порт ФПСУ В -203.0.113.2.

С точки зрения конфигурирования ФПСУ-IP А для работы в условиях такой топологии принципиальным является следующее:

- со стороны внутреннего порта ФПСУ-IP А (порта 1 со стороны области А) существует одна IP- подсеть,
- со стороны внешнего порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы отсутствуют; ФПСУ-IP В описан в режиме моста;
- на ФПСУ-IP А должны быть установлены, и указаны как используемые, ранее выработанные ЦВК криптографические ключи номер 1.

С точки зрения конфигурирования ФПСУ-IP В для работы в условиях такой топологии принципиальным является следующее:

- со стороны внутреннего порта ФПСУ-IP В (порта 1 со стороны области В)

Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.

Правила МЭ:
1 A_to_C
Общие
Действие : Accept
Время работы : Любое
Лог : Не вести лог
Активно : Да
Источник
Сеть : 192.168.001.000 192.168.000.000/24
Назначение
Сеть : 192.168.003.000 192.168.000.000/24
Служба : Любая
2 Block other traffic
Общие
Действие : Drop
Время работы : Любое
Лог : Не вести лог
Активно : Да
Источник : Любой
Назначение : Любой
Служба : Любая

Для ФПСУ-IP B:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 в настройках ФПСУ-IP B указаны как используемые.

Создано и активировано разрешающее правило трафика, в которое включены подсети 192.168.1.0 и 192.168.3.0. Подсети 192.168.2.0 со стороны порта 1 разрешено управление маршрутизатором 192.168.2.1.

Порт 1:
Номер 1,
Адрес 192.168.2.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.1.50, ключевые данные - 1.1; смена через 30 сек;

интернет.

Конфигурация ФПСУ должна содержать следующие установки:

Порт 1:

Номер 1,
Адрес 203.000.113.001,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы:203.000.113.002,
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.

Абоненты:
Хост; Адрес 203.000.113.002; Маска 255.255.255.000 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Хост; Адрес Произвольный (из незаданных)
режим работы ретрансляция;
Доступен через маршрутизатор 203.000.113.002
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2,
Адрес 192.168.000.254,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.000.000; Маска 255.255.255.000;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Абоненты:
Хост; Адрес 203.0.113.2; Маска 255.255.255.0 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
Client_local

Подсеть; Адрес 192.168.001.000; Маска 255.255.255.000 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" выключен.

Хост; Адрес Произвольный (из незаданных)
режим работы ретрансляция;
Доступен через маршрутизаторы 203.0.113.2
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Работа разрешена" включен.

Порт 2:
Номер 2,
Адрес 192.168.0.254,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.0.0; Маска 255.255.255.0;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
DNS

```
Client_local
Internet_All
```

ФПСУ-IP/Клиентами при работе с ФПСУ-IP используются два механизма NAT:

- для доступа во внутреннюю сеть, статический NAT (настраивается в описателях Клиентов);
- для работы с интернетом, используя ФПСУ-IP как посредника, динамический NAT (настраивается в правилах МЭ).

Описатель Клиентов:

К-сеть Crypt; **Группа** 1 Для программных устройств
Обслуживание Разрешено
Диапазон номеров 1 .. 25
Описание Активно
Контроль соединения 10 мин

Параметры для портов ФПСУ-IP

Порт 1		Порт 2
NAT при соединении		
192.168.003.001	Начальный адрес	192.168.003.001
255.255.255.000	Маска подсети	255.255.255.000

Правила межсетевого экрана для клиентов этого диапазона
Client_local

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее исходящие соединения с порта 2;
2. Правило, разрешающее исходящие соединения клиентов, программных (мобильных) клиентов и сервиса example.com в подсети 1 и 2 и порты ФПСУ-IP;
3. Правило, разрешающее исходящие соединения подсетей 1 и 2 с NAT в интернет
4. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

Правила МЭ:

1 DNS

```
      Общие
        Действие        : Accept
        Время работы    : Любое
```

- со стороны порта 1 описана подсеть с той же адресацией, что и на ФПСУ-IP A, обмен хостов данной подсети через комплекс производится в режиме ретрансляции;
- со стороны внешнего порта 2 определен ФПСУ-IP A, обмен данными с которым определяется правилом МЭ, в правиле задана переадресация порта;
- со стороны порта 2 описан абонент 11.11.11.11, обмен данными с которым определяется правилом МЭ, в правиле задана переадресация порта;

Хост 192.168.0.1 защищаемой области A отправляет эхо-запрос (ping) на внутренний IP-адрес ФПСУ-IP A. Правилом МЭ данный запрос разрешен. На ФПСУ-IP A с помощью NAT IP-адрес отправителя 192.168.0.1 подменяется на 11.11.11.11, с помощью MAP IP-адрес получателя 192.168.0.241 подменяется на внешний IP-адрес ФПСУ-IP B 1.1.1.2. Запрос отправляется на ФПСУ-IP B. Правилом МЭ данный запрос разрешен. На ФПСУ-IP B с помощью MAP IP-адрес получателя 1.1.1.2 подменяется на 192.168.0.1. Запрос отправляется хосту 192.168.0.1 защищаемой области B. Ответ хоста 192.168.0.1 защищаемой области B проходит обратное преобразование при прохождении ФПСУ-IP B и ФПСУ-IP A. На ФПСУ-IP реализовано отслеживание инициатора запроса - возвратный трафик разрешен.

Рисунок 394 - Схема подключения ФПСУ-IP/Клиентов

ФПСУ-IP A

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 указаны на ФПСУ A как используемые.

Порт 1:
Номер 1,
Адрес 192.168.000.241,
Маска 255.255.255.000 (24 разряда),
VLAN Нет;
ФПСУ не определены,
Маршрутизаторы:не определены,
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее исходящие соединения по протоколу ICMP хоста 192.168.0.1 на внутренний порт ФПСУ-IP A, IP-адрес источника и назначения преобразуются по заданным правилам NAT и MAP;
2. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

```
Правила МЭ:
1. ping over nat
      Общие
        Действие        : Accept
        Nat             : port2 iface2 vlan111 011.011.011.011
        Map             : 001.001.001.002 port -
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Адрес           :   192.168.000.001/32 192.168.000.001
      Назначение
        Интерфейс       :   port1 iface1 192.168.000.241
      Служба
        PING

2. Block other traffic
      Общие
        Действие        : Drop
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник        : Любой
      Назначение      : Любой
      Служба          : Любая

Службы
1. PING
        Описание        : Internet Control Message Protocol
        Протокол        : ICMP
      Тип сообщения ICMP: Любой
```

ФПСУ B

ФПСУ-IP будет менять порт назначения у всех пакетов, подпадающих под действие правила, на указанный администратором.

Рассмотрим пример использования ФПСУ-IP для переназначения порта у пакетов, отправленных в адрес внутреннего сервера. ФПСУ-IP получает пакет в адрес сервера 192.168.10.10 на порт 80 и изменяет порт получателя на 1080. Таким образом, входящие клиентские соединения можно перенаправлять на другой порт сервера.

Рисунок 395 - Схема перенаправления пакетов на другой порт сервера

В настройках конфигурации ФПСУ-IP порта 1 (IP- адрес 10.10.10.1) необходимо описать хост или подсеть, в которую входит хост 192.168.0.1, отправляющий запросы серверу, как абонента порта. В настройках конфигурации ФПСУ-IP порта 2 (IP- адрес 10.10.10.2) должен быть описан в качестве абонента сервер 192.168.10.10 или подсеть, в которой расположен сервер, принимающий запросы клиентов. Переназначение номеров портов входящих соединений клиентов задается правилом трафика межсетевого экрана, в котором указывается:

- в поле опции MAP, IP-адрес назначения и новый порт;
- IP-адрес отправителя в списке отправителей, пакеты которого требуется отслеживать и изменять порт назначения;
- только один IP-адрес сервера в списке назначений правила;
- служба, распространяющая действие правила только на пакеты TCP/UDP порта номер 80;
- правило разрешается (accept, активно).

Конфигурация ФПСУ-IP должна содержать следующие установки:

```
Порт 1      Адрес            Маска         VLAN
         010.010.010.001  255.255.255.000   Нет

АБОНЕНТЫ
 Адрес 192.168.000.001   Хост
 Имя   192.168.000.001
```

```
Режим работы     Ретрансляция
Режим партнера
 Данного порта   Ретрансляция  Через ФПСУ
 Другого порта   Ретрансляция  Через ФПСУ
Работа разрешена

Адрес 192.168.000.000   Маска 255.255.255.000
Имя   192.168.000.000
Режим работы     Ретрансляция
Режим партнера
 Данного порта   Ретрансляция  Через ФПСУ
 Другого порта   Ретрансляция  Через ФПСУ
Работа разрешена

Порт 2      Адрес            Маска         VLAN
       010.010.010.002  255.255.255.000   Нет
АБОНЕНТЫ
 Адрес 192.168.010.010   Хост
 Имя   192.168.010.010
 Режим работы     Ретрансляция
 Режим партнера
  Данного порта   Ретрансляция  Через ФПСУ
  Другого порта   Ретрансляция  Через ФПСУ
 Работа разрешена
 Правила межсетевого экрана для этого абонента
  map_port
```

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее любые входящие соединения по протоколу TCP/UDP с портом назначения 80, для указанных соединений порт назначения преобразуется по заданному правилу MAP на номер 1080. В правиле межсетевого экрана во вкладке «Назначение» должен быть указан один и только один адрес назначения, адрес сервера. Во вкладке «Источник» может быть явно указан хост или подсеть, отправляющие запросы. Если вкладка «Источник» пустая, ФПСУ-IP будет принимать и менять порт у любых входящих соединений с сервером и портом назначения 80. Во вкладке «Общие» в поле «MAP» указывается тот же IP-адрес сервера, что и во вкладке назначения, и новый порт 1080, на который должны перенаправляться запросы. Данное правило применяется на порту 2 ФПСУ-IP к абоненту сервер, указанному как хост;
2. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

```
Межсетевой экран активен: Да

Правила трафика

  1. map_port
Общие
      Действие        : Accept
      Map             : 192.168.010.010 1080
      Время работы    : Любое
      Лог             : Не вести лог
      Активно         : Да
    Источник        : Любой
    Назначение
      Адрес           :   192.168.010.010 192.168.010.010
    Служба
      TCP/UDP

  2. Block other traffic
    Общие
      Действие        : Drop
      Время работы    : Любое
      Лог             : Не вести лог
      Активно         : Да
    Источник        : Любой
    Назначение      : Любой
    Служба          : Любая

  Службы

1. TCP/UDP
    Общие
      Описание        :
      Протокол        : TCP/UDP
      Порт источника  : Любой
      Порт назначения : 80 (World Wide Web HTTP)
```

15. 11. Использование ФПСУ-IP для балансировки нагрузки на порты внутреннего сервера

Рассмотрим пример с балансировкой нагрузки на порты внутреннего сервера. Входящие клиентские соединения можно распределять по разным портам сервера.

ФПСУ-IP отслеживает входящие пакеты в адрес сервера 192.168.10.10 на порт 80 и в

зависимости от источника получения запроса изменяет порт получателя у входящего соединения. Хост 1 отправляет запросы серверу 192.168.10.10 на порт 80 по умолчанию, запросы данного хоста сервер получает на порт по умолчанию. Хосты 2 и 3 отправляют запросы серверу 192.168.10.10 на порт 80 по умолчанию, ФПСУ-IP по правилу МЭ с применением перенаправления порта MAP меняет порт назначения входящего соединения и сервер получает запросы данного хоста на другой указанный порт соответственно 1080 и 2080.

Рисунок 396 - Схема перенаправления пакетов на другой порт сервера

В настройках конфигурации ФПСУ-IP порта 1 (IP- адрес 10.10.10.1) необходимо описать хосты 192.168.0.1, 192.168.1.1, 192.168.2.1 или подсети, в которые они входят, как абоненты порта. В настройках конфигурации ФПСУ-IP порта 2 (IP- адрес 10.10.10.2) должен быть описан в качестве абонента сервер 192.168.10.10 или подсеть, в которой расположен сервер, принимающий запросы клиентов. Переназначение номеров портов входящих соединений клиентов задается правилами трафика межсетевого экрана, в которых указывается:

- в поле опции MAP, IP-адрес назначения и новый порт;
- IP-адрес отправителя в списке отправителей, пакеты которого требуется отслеживать и изменять порт назначения;
- только один IP-адрес сервера в списке назначений правила;
- служба, распространяющая действие правила только на пакеты TCP/UDP порта номер 80;
- правило разрешается (accept, активно).

Конфигурация ФПСУ-IP должна содержать следующие установки:

```
1. serv_host1
      Общие
        Действие        : Accept
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Адрес           :   192.168.000.001 192.168.000.001
      Назначение
        Адрес           :   192.168.010.010 192.168.010.010
      Служба
        TCP/UDP

2. map_port_1080
      Общие
        Действие        : Accept
        Мар             : 192.168.010.010 1080
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Адрес           :   192.168.001.001 192.168.001.001
      Назначение
        Адрес           :   192.168.010.010 192.168.010.010
      Служба
        TCP/UDP

3. map_port_2080
      Общие
        Действие        : Accept
        Мар             : 192.168.010.010 2080
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Адрес           :   192.168.002.001 192.168.002.001
      Назначение
        Адрес           :   192.168.010.010 192.168.010.010
      Служба
        TCP/UDP

4. Block other traffic
      Общие
        Действие        : Drop
```

Адрес 203.000.113.002,
Маска 255.255.255.000 (24 разряда),
ФПСУ
203.000.113.1, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы:203.000.113.012,
протоколы маршрутизации выключены;

Абоненты:
Адрес 192.168.000.000; Маска 255.255.255.000;
Доступен через маршрутизатор 203.000.113.012
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.

Порт 2:
Номер 2,
Адрес 192.168.001.254,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.001.000; Маска 255.255.255.000;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
Spoof

Правила МЭ:
1 Spoof
Общие
Действие : Accept
Время работы : Любое
Лог : Не вести лог
Spoof : Да
Активно : Да
Источник
Сеть : 192.168.000.000 192.168.000.000/24
Назначение
Сеть : 192.168.001.000 192.168.001.000/24

Отсутствие принимаемых пакетов на соответствующем порту ФПСУ-IP	Неправильно указанная (или определенная адаптером) скорость работы линии на сетевом адаптере	Установить в конфигурации соответствующего LAN-порта необходимую скорость работы линии
Появление на соответствующем порту ФПСУ-IP большого количества ошибочных пакетов (см. пункт «Окно состояния рабочих LAN портов») снижение скорости передачи или невозможность передачи данных через ФПСУ-IP.	Неправильное указание дуплексного режима работы линии (полный дуплекс или полудуплекс) или несовместимость режима одного из адаптеров комплекса с адаптерами смежного оборудования сети	Установить в конфигурации соответствующего LAN-порта или конфигурации смежного оборудования правильный дуплексный режим работы линии.

Диагностика	Пояснение	Причина возникновения
		Попытка межмаршрутизаторного обмена по неразрешенному протоколу маршрутизации для маршрутизатора-отправителя пакета. «Ping» - попытка ФПСУ-IP от прописанного абонента или маршрутизатора при выключенном флаге «Отвечать на Ping». «Ping» - попытка ФПСУ-IP длинным пакетом. Не «Ping» - попытка обращения прописанного абонента к удаленному ФПСУ-IP или абонент не является удаленным администратором или ФПСУ-IP.
Запрет по доступу	Запрет по режиму работы с партнером.	Запрет по режиму работы с партнером данного или противоположного порта.
Запрет SourceRoute	Запрет доступа по опции SourceRoute в IP-пакете.	В принятом IP-пакете присутствует одна из опций, требующая записывать маршрут прохождения пакета, а в конфигурации ФПСУ-IP установлен флаг «Пакеты с опцией SourceRoute» - «Не пропускать».
Абонент через ФПСУ	Абонент должен работать в режиме ретрансляции.	Принят пакет из VPN-туннеля от абонента, для которого на данном ФПСУ-IP установлен режим работы «Ретрансляция».
Абонент миновал ФПСУ	Абонент должен работать через ФПСУ.	Принят пакет не из VPN-туннеля от абонента, для которого на данном ФПСУ-IP установлен режим работы «Через ФПСУ».
ФПСУ не работает	Удаленный ФПСУ-IP не работает.	Не включен удаленный ФПСУ-IP или с ним нет связи. Не работает сетевой адаптер - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.

Диагностика	Пояснение	Причина возникновения
Нет ФПСУ-туннеля	Отсутствие взаимодействия между ФПСУ-IP.	VPN-туннель между двумя ФПСУ-IP не установлен к моменту попытки передачи через него пакетов от абонентов. Не включен удаленный ФПСУ-IP или с ним нет связи. Неустойчивая работа сбойного сетевого адаптера - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.
Ложный ФПСУ	Станция-отправитель использует ошибочный протокол установки соединения или поддержания VPN-туннеля	Попытка передачи пакетов в IP-адрес местного ФПСУ-IP от рабочей станции, зарегистрированной как удаленный ФПСУ-IP, но не являющейся таковой.
Ошибочный ФПСУ-пакет	Ошибочный пакет от ФПСУ-IP.	На местном или удаленном ФПСУ-IP указаны неверные значения номеров ключевых данных удаленных ФПСУ-IP. В процессе установки или поддержания VPN-туннеля произошел кратковременный сбой, что обычно очень редко проявляется в момент первичной установки VPN-туннеля. Попытка навязывания местному ФПСУ-IP VPN-данных или повторения ранее переданных удаленным ФПСУ-IP данных от «вредоносной» станции.
Ошибка клиент-пакет	Искажены или повреждены находящиеся в полученном от ФПСУ-IP/Клиента пакете данные.	Сообщение возникает на экране мониторинга подключенных ФПСУ-IP/Клиентов. Такие пакеты будут сброшены ФПСУ-IP.

Таблица 402. Ошибки, связанные с ключевыми данными

Служебное сообщение	Пояснение	Действия администратора
The TM does not contain the key	Ошибка возникает при попытке запуска ФПСУ-IP с помощью ТМ-идентификатора, на котором находится искаженный ключ запуска.	Если искажен ключ запуска Главного администратора - обратитесь к поставщику ФПСУ-IP для замены ТМ-идентификатора Главного администратора. Если искажен ключ запуска пользователя другого класса - повторно перезапишите ТМ-идентификатор пользователя средствами ФПСУ-IP (Настройка системы - Регистрация ТМ-идентификаторов)
Внимание! Повреждены критические компоненты комплекса. ВСЕ установленные ключевые данные и ТМ утрачены. Комплекс переведен в технологический режим. Возможно потребуется переустановка комплекса	ПО ФПСУ-IP обнаружило искажение ключа для хранения долговременных ключей. Требуется вмешательство администратора	Требуется выполнить повторный перевод ФПСУ-IP из технологического режима в рабочий режим, заново зарегистрировать все ТМ-идентификаторы пользователей и переустановить ключевые данные ЦВК и удаленных администраторов. В случае ошибки перевода ФПСУ-IP из технологического режима в рабочий режим, выполнить полную переустановку ПО ФПСУ-IP.
Внимание! Поврежден компонент комплекса. Необходима инициализация ДСЧ	ПО ФПСУ-IP обнаружило искажение ключа ПДСЧ. Требуется вмешательство администратора	Требуется выполнить повторный перевод ФПСУ-IP из технологического режима в рабочий режим.
Внимание! ФПСУ не работоспособен. Искажены данные конфигурации.	ПО ФПСУ-IP обнаружило искажение конфигурации ФПСУ-IP	Восстановить конфигурацию ФПСУ-IP любым из следующих способов: • локально с помощью резервной копии конфигурации;

Служебное сообщение	**Пояснение**	**Действия администратора**
Ожидание восстановления конфигурации с резервного комплекса или удаленного администратора		• подключить к ФПСУ-IP комплекс горячего резерва; • установить на ФПСУ-IP новую конфигурацию средствами удаленного администратора.
Ошибка инициализации! Служебный описатель искажен	Сообщение об ошибке выводится на экран просмотра состояний удаленных администраторов ФПСУ-IP. ПО ФПСУ-IP обнаружило искажение секретного ключа ФПСУ-IP подсистемы удаленного администрирования или открытых ключей удаленных администраторов. Удаленное управление ФПСУ-IP с такой ошибкой невозможно.	Заново зарегистрировать удаленных администраторов на ФПСУ-IP. Перерегистрировать ФПСУ-IP на всех удаленных администраторах.
Описатель удаленных администраторов испорчен или несовместимая версия!	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ-IP.	Заново зарегистрировать удаленных администраторов на ФПСУ-IP. Перерегистрировать ФПСУ-IP на всех удаленных администраторах.

Служебное сообщение	**Пояснение**	**Действия администратора**
	ПО ФПСУ-IP обнаружило искажение секретного ключа ФПСУ-IP подсистемы удаленного администрирования или открытых ключей удаленных администраторов Удаленное управление ФПСУ-IP с такой ошибкой невозможно.	
**Имя_файла_с_открытым_ключом_удаленного_администратора*----> Поврежден*	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ-IP при попытке зарегистрировать нового удаленного администратора. Причина - искажен или поврежден предъявленный на внешнем USB-носителе открытый ключ удаленного администратора	Заново получить от администратора АРМ УА открытый ключ удаленного администратора и повторить процедуру регистрации удаленного администратора на ФПСУ-IP
Состояние туннеля с другим ФПСУ-IP "WaitSynRR" с дополнительными сообщениями в журнале статистики	Хранящиеся на внутреннем накопителе ФПСУ-IP парно-выборочные ключи были искажены.	Заново установить на ФПСУ-IP полученные от администратора ЦВК парно-выборочные ключи.

Служебное сообщение	**Пояснение**	**Действия администратора**
"Аварийное состояние ключей/нештатные действия: Ошибка при зачитывании установленных ключей"	Требуется вмешательство администратора	
Данные искажены, пропускаю!	Сообщение об ошибке выводится на экране установки ключей меню конфигурации ФПСУ-IP. Возникает при искажении предъявленного на внешнем USB-носителе парно-выборочного ключа	Заново получить от администратора ЦВК парно-выборочный ключ взамен искаженного.
Испорчены служебные данные горячего резервирования	Сообщение об ошибке выводится на экране мониторинга состояния горячего резерва ФПСУ-IP (основной комплекс системы горячего резервирования). Ошибка возникает при искажении хранящегося на внутреннем накопителе ФПСУ-IP ключа горячего резерва	Считать на ТМ-идентификатор ключ горячего резерва с исправного комплекса (меню локального конфигурирования ФПСУ-IP «Настройка системы» - «Параметры горячего резерва»). Если ключ горячего резерва не считывается с исправного комплекса, создать новый ключ горячего резерва. Повторно зарегистрировать ключ горячего резерва на сообщившем об ошибке ФПСУ-IP.

Служебное сообщение	Пояснение	Действия администратора
ФАТАЛЬНАЯ ОШИБКА. Резервный комплекс не может функционировать, так как испорчены служебные данные горячего резервирования. Возможно потребуется переустановка комплекса	Сообщение об ошибке выводится при запуске ФПСУ-IP (резервный комплекс системы горячего резервирования). Ошибка возникает при искажении хранящегося на внутреннем накопителе ФПСУ-IP ключа горячего резерва	Считать на ТМ-идентификатор ключ горячего резерва с исправного комплекса (меню локального конфигурирования ФПСУ-IP «Настройка системы» - «Параметры горячего резерва»). Если ключ горячего резерва не считывается с исправного комплекса, создать новый ключ горячего резерва. Повторно зарегистрировать ключ горячего резерва на сообщившем об ошибке ФПСУ-IP.
Испорчен или не установлен ключ центра	Сообщение об ошибке выводится на экране мониторинга действий ФПСУ-IP\Клиентов. Искажен общесистемный ключ Криптосети Клиентов. ФПСУ-IP\Клиенты не могут соединиться с ФПСУ-IP	Заново установить на ФПСУ-IP общесистемный ключ Криптосети Клиентов вместо искаженного.
ТМ испорчена	Сообщение об ошибке выводится при попытке зарегистрировать общесистемный ключ Криптосети Клиентов на ФПСУ-IP. Находящийся на ТМ-идентификаторе общесистемный ключ Криптосети Клиентов искажен или испорчен.	Заново получить от администратора ЦГКК общесистемный ключ Криптосети Клиентов и повторить процедуру регистрации общесистемного ключа Криптосети Клиентов на ФПСУ-IP

Таблица 403. Ошибки при соединении ФПСУ-IP

Диагностика	Пояснение	Причина возникновения
Не совпадают RKL роли клиент/ФПСУ-IP	Оба участника ФПСУ-IP/Клиент и ФПСУ-IP при соединении должны поддерживать удаленную загрузку ключевых данных	На ФПСУ-IP с установленной подсистемой RKL (подсистемой удаленной загрузки ключевых данных) пытается соединиться ФПСУ-IP/Клиент, VPN-Key которого не поддерживает удаленную загрузку ключевых данных, или наоборот, к ФПСУ-IP без подсистемы RKL соединяется ФПСУ-IP/Клиент, VPN-Key которого поддерживает удаленную загрузку ключевых данных

17. 1. Выдача файла Kmsg

Команда «Выдать kmsg» окна просмотра статистики ФПСУ-IP («Статистика ФПСУ-IP») позволяет выдать на внешний носитель (USB-flash) файл для анализа сообщений ядра и использования памяти в случае падения ядра Linux.

Рисунок 406 - Выбор каталога для выгрузки файла

Подтвердите место выгрузки файла, выполнив команду «Каталог выбран».

После выгрузки файла, ФПСУ-IP выдаст системное оповещение о завершении процедуры:

Рисунок 407 - Сообщение о завершении процедуры

18. Удаление программного обеспечения ФПСУ-IP

18. 1. Удаление СКЗИ ФПСУ-IP

Локальному администратору ФПСУ-IP классов *«Администратор»* или *«Главный администратор»* доступна возможность форматирования внутреннего накопителя ФПСУ-IP с удалением операционной системы ФПСУ-IP и хранящихся файлов, в том числе ключевой информации СКЗИ, программных и служебных модулей СКЗИ, и программного обеспечения BIOS/UEFI.

Для запуска процедуры форматирования внутреннего накопителя:

1. Выполните команду «Настройка системы» главного меню:

Рисунок 408 - Главное меню ФПСУ-IP

2. Выполните команду «Настройки СКЗИ» меню настройки системы:

или кнопку «*Сохранить*». Для выхода в меню общих настроек без сохранения изменений нажмите <*Esc*> или кнопку «*Отмена*».

14. 6. DHCP-сервер и DNS-Relay

ФПСУ-IP поддерживает возможность автоматически выдавать IP-адрес и другие параметры конфигурации, необходимые для работы в сети, сетевыми устройствами по протоколу DHCP. Для включения протокола DHCP необходимо настроить DHCP-сервер на ФПСУ-IP.

Выберите в меню *«Сетевые сервисы»* конфигурации ФПСУ-IP команду «*DHCP-сервер и DNS-Relay»*:

Рисунок 403 - Команда меню «Сетевые сервисы» → «DHCP-сервер и DNS-Relay»

Вкладка **DHCP** предназначена для настройки параметров DHCP-сервера.

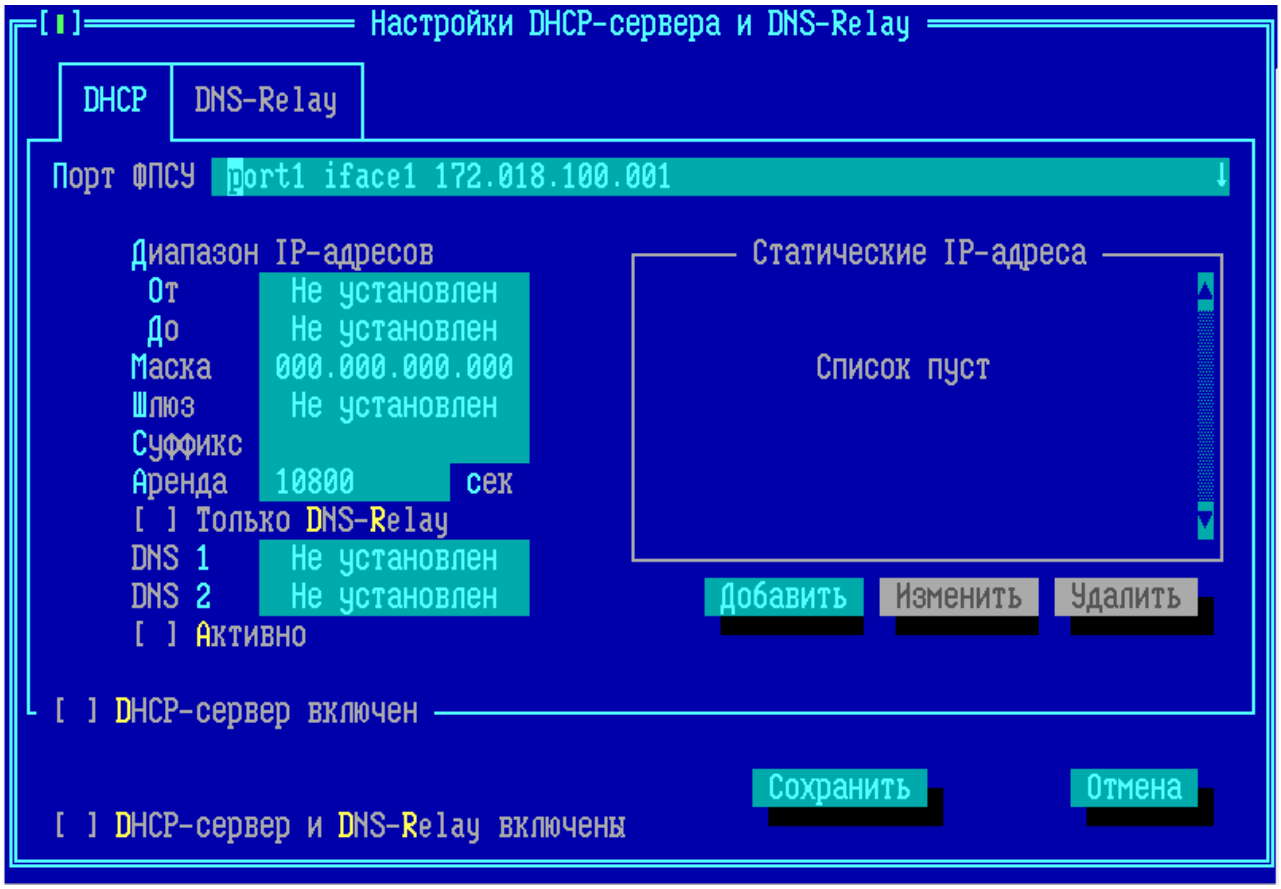

Рисунок 404 - Вкладка «DHCP»

Порт ФПСУ — IP-адрес интерфейса, который раздает адреса DHCP-клиентам.

Диапазон IP-адресов: *От, До* — диапазон допустимых IP-адресов подсети, которые могут арендовать абоненты ФПСУ-IP, DHCP-клиенты. ФПСУ-IP выдает DHCP-клиентам динамические IP-адреса из указанного здесь диапазона.

Маска — маска подсети IP-адресов, указанных в диапазоне для назначения DHCP-клиентам.

Шлюз — шлюз по умолчанию (маршрутизатор, соединяющий данную подсеть с другими подсетями), IP-адрес шлюза в подсети, который назначается DHCP-клиентам.

Суффикс — указывается, какой DNS-суффикс выдавать DHCP-клиентам. По умолчанию - пустой, DNS-суффикс DHCP-клиенту не выдается.

Аренда — продолжительность аренды выдаваемого DHCP-клиенту IP-адреса. Время указывается в секундах, по умолчанию составляет 3 часа (10800 секунд).

Только DNS-Relay — флаг, устанавливающий работу ФПСУ-IP в режиме ретрансляции DNS, клиенту не будут присылаться настройки внешних DNS-серверов. Если

флаг снят, DHCP-клиенту будут отправлены IP-адреса из полей *DNS 1 и DNS 2* в качестве основного и дополнительного DNS-сервера.

DNS 1, DNS 2 — IP-адреса DNS-серверов, которые отвечают на запросы о разрешении сетевых имен; после получения IP-адреса в аренду DHCP-клиент автоматически обновляет соответствующие DNS-записи. Серверы указываются в порядке предпочтения (DNS 1 - основной, DNS 2 - дополнительный).

Статические IP-адреса — список, содержащий зарезервированные IP-адреса для указанных MAC-адресов DHCP-клиентов. Абонент ФПСУ-IP запрашивает IP-адрес у DHCP-сервера, DHCP-сервер распознает MAC-адрес абонента и назначает ему соответствующий статический IP-адрес. Для DHCP-сервера может быть задан только список статических IP-адресов, в этом случае должен быть установлен флаг «Активно».

Для добавления статического IP-адреса в список нажмите кнопку *«Добавить»*, в открывшемся окне введите IP-адрес, MAC-адрес и сохраните по кнопке *«Сохранить»*.

Рисунок 405 - Добавление статического IP-адреса

Для изменения/удаления статического IP-адреса выделите его в списке клавишей <*Tab*> и нажмите кнопку *«Изменить»*/*«Удалить»*.

Активно — флаг при включении задействует настройки статических IP-адресов.

DHCP-сервер включен — флаг, включающий настройки DHCP-сервер на ФПСУ-IP.

DHCP-сервер и DNS-Relay включены — флаг, включающий работу протоколов.

ВНИМАНИЕ! Для работы DHCP-сервера с указанными настройками должны быть включены все три флага, «*Активно*», «*DHCP-сервер включен*!», «*DHCP-сервер и DNS-Relay включены*».

Вкладка **DNS-Relay** предназначена для настройки ретрансляции запросов DNS.

ФПСУ-IP поддерживает ретрансляцию запросов DNS. ФПСУ-IP получает DNS-запросы от абонентов, перенаправляет эти запросы на указанные в списке DNS-серверы и

пересылает обратно полученные ответы от DNS-серверов абонентам.

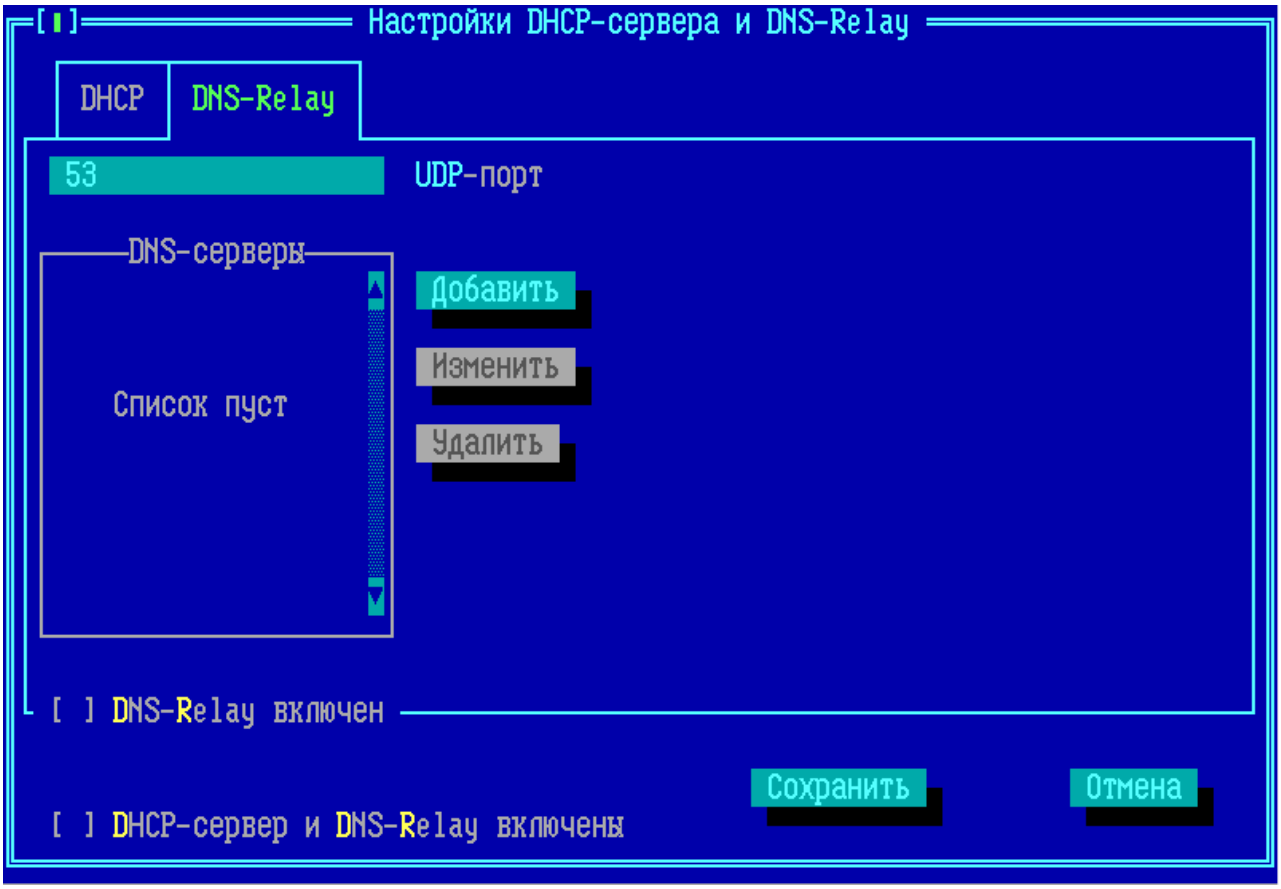

Рисунок 406 - Вкладка «DNS-Relay»

UDP-порт — не изменяемое информационное поле для справки; порт, используемый протоколом DNS, на который ФПСУ-IP получает запросы и отправляет на DNS-сервер.

DNS-серверы — ФПСУ-IP перенаправляет DNS-запросы абонентов на указанные DNS-серверы в списке.

Для добавления DNS-сервера в список нажмите кнопку *«Добавить»*, в открывшемся окне введите IP-адрес и сохраните по кнопке *«Сохранить»*.

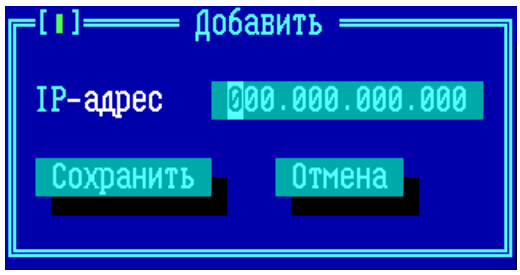

Рисунок 407 - Добавление DNS-сервера

Для изменения/удаления DNS-сервера выделите его в списке клавишей <*Tab*> и

нажмите кнопку *«Изменить»*/*«Удалить»*.

DNS-Relay включен — флаг, устанавливающий настройки ретрансляции DNS.

DHCP-сервер и DNS-Relay включены — флаг, включающий работу протоколов.

14. 7. DHCP-Relay

ФПСУ-IP может выступать в качестве сервера DHCP-Relay, пересылая DHCP-запросы абонентов на указанный в конфигурации адрес DHCP сервера.

Для включения службы в рабочий режим, требуется выполнить настройки:

- задать список доступных DHCP-серверов;
- для каждого порта ФПСУ-IP (см. пункт «Порты ФПСУ») и каждого VLAN портов ФПСУ-IP (см. пункт «Описание VLAN порта ФПСУ-IP») указать DHCP сервер, куда следует пересылать приходящие на порт и VLAN DHCP-запросы.

14. 7. 1. Создание списка DHCP-серверов

ФПСУ-IP может быть настроен в качестве агента ретрансляции DHCP-запросов. Для указания списка DHCP-серверов, которым ретранслируются DHCP-запросы, выберите в меню «Сетевые сервисы» конфигурации ФПСУ-IP команду *«DHCP-Relay»*:

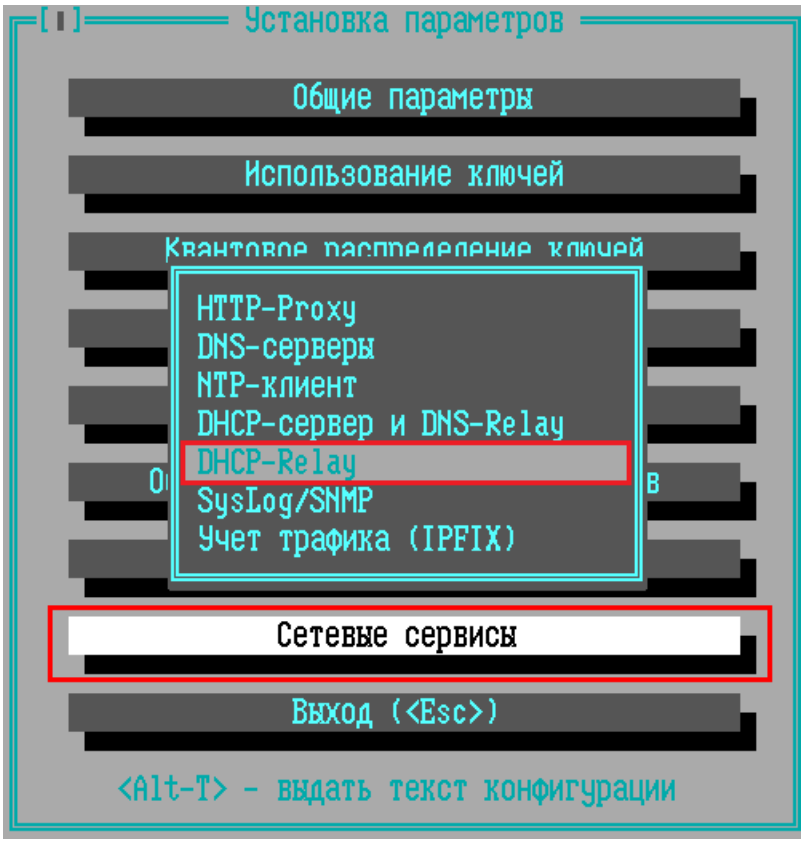

Рисунок 408 - Команда меню «Сетевые сервисы» → «DHCP-Relay»

Список DHCP-серверов для ретрансляции по умолчанию пустой и в нём выведено служебное оповещение «Серверы не определены». Все IP-адреса, которые позднее будут использоваться в конфигурации порта ФПСУ-IP как DHCP-сервера для ретрансляции, должны быть предварительно добавлены в этот список.

Рисунок 409 - Список DHCP-серверов

Для добавления DHCP-сервера, нажмите клавишу <*Ins*> и введите его IP-адрес в появившемся окне.

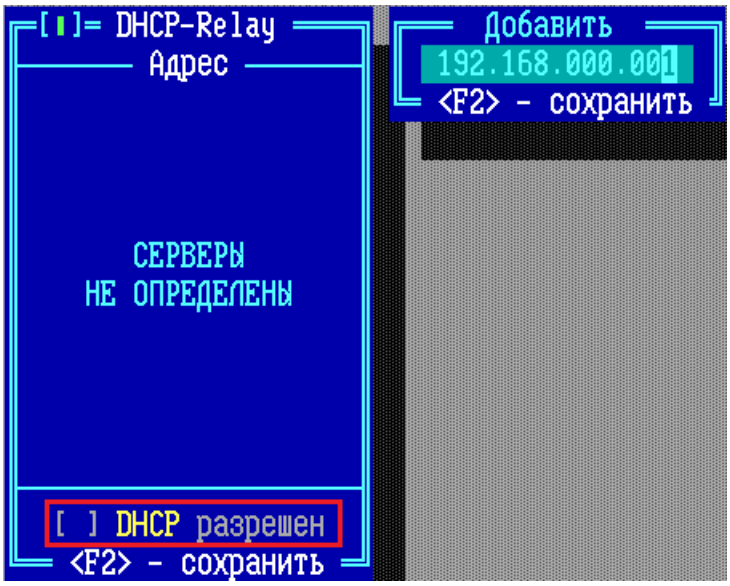

Рисунок 410 - Добавление DHCP-сервера

IP-адрес должен быть заранее описан в качестве абонента маршрутизации порта ФПСУ-IP, которому работа разрешена. То есть либо совпадать с адресом абонента типа хост, либо принадлежать подсети, описанной в качестве абонента (см. пункт «Описание параметров абонентов»).

Для удаления существующей записи IP-адреса из списка, установите курсор на строке и нажмите клавишу <*Del*>. Редактирование существующей записи выполняется по нажатию клавиши <*Enter*>.

ВНИМАНИЕ! Для включения сервиса DHCP-Relay требуется **включить** выключенный по умолчанию флаг *«DHCP разрешен»*.

После сохранения, IP-адрес можно использовать в конфигурации портов ФПСУ-IP в качестве получателя ретранслируемых DHCP-запросов (см. пункт «Настройка DHCP-Relay на портах ФПСУ»).

14. 7. 2. Настройка DHCP-Relay на портах ФПСУ

Для того, чтобы ФПСУ-IP ретранслировал DHCP-запросы, требуется для каждого порта (и каждого VLAN) ФПСУ-IP ***назначить*** основной и (опционально) запасной DHCP-сервер из **ранее заданного списка IP-адресов** (см. пункт «DHCP-сервер и DNS-Relay»). Таким образом, администратор определяет, куда ретранслировать пришедший DHCP-запрос, в зависимости от того, на какой порт (и в какой VLAN) он пришёл.

ВНИМАНИЕ! Назначить порту DHCP-сервер получится только в том случае, если IP-адреса портов 1 и 2 порта ФПСУ-IP **не совпадают** (то есть, если IP-адрес 2 порта установлен в «*192.168.000.**036**»*, то IP-адрес 1 порта должен быть установлен в другое значение, например «*192.168.000.**035**»* - см. рисунок ниже).

Вход в интерфейс назначения DHCP-серверов порту ФПСУ-IP происходит из окна описания порта. Для этого следует установить курсор на поле «*Адрес*» и нажать клавишу <*Пробел*>. Появляющийся по команде интерфейс настройки DHCP меняется, в зависимости от установленной на ФПСУ-IP подсистемы VLAN.

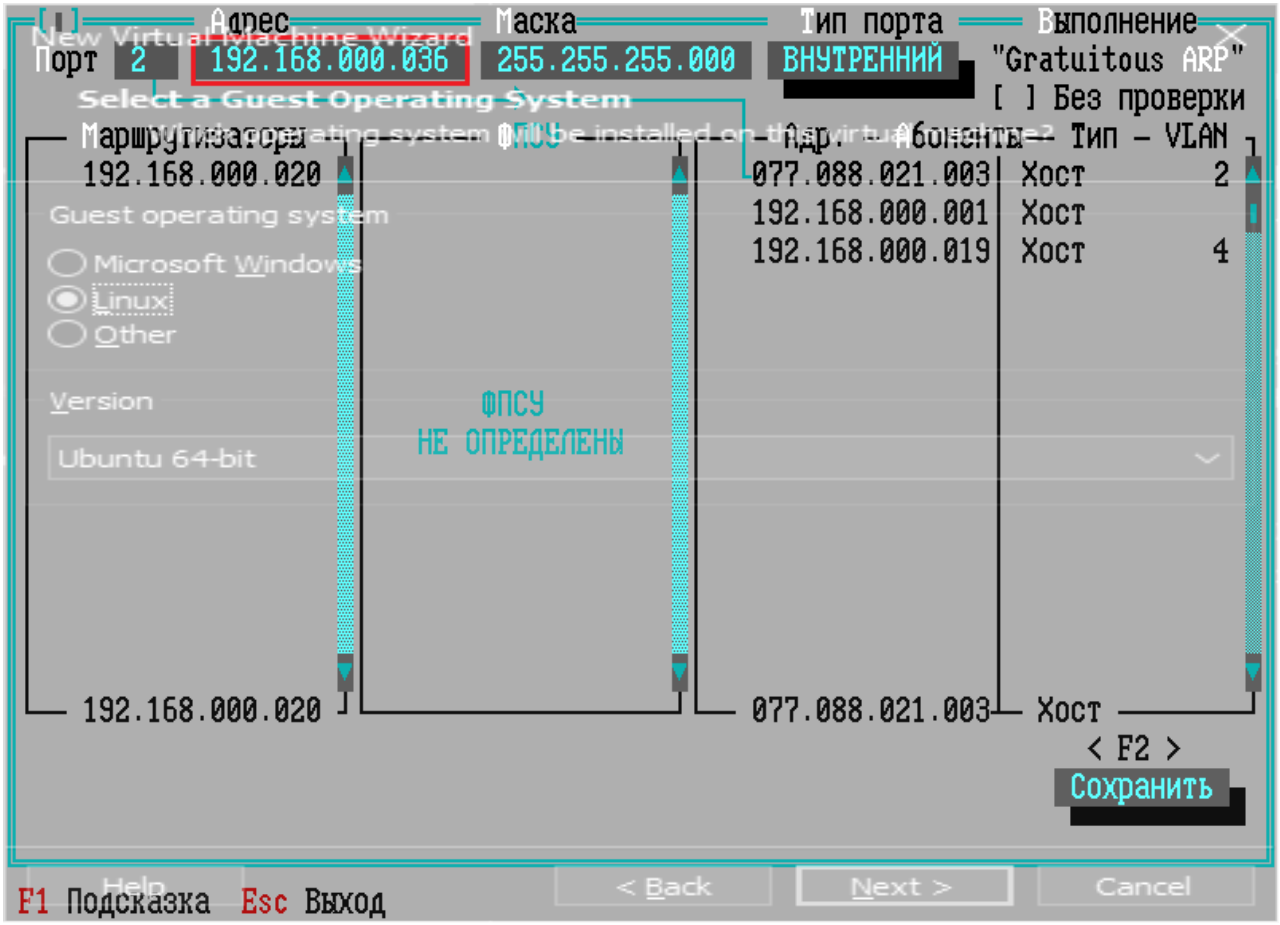

Рисунок 411 - Параметры порта ФПСУ-IP

Если на ФПСУ-IP **не установлена подсистема VLAN**, то в появившемся окне можно будет только выбрать основной и запасной DHCP-сервер для ретрансляции всех DHCP-запросов, поступающих на описываемый порт ФПСУ-IP.

Рисунок 412 - Настройка DHCP на порту без VLAN

Для указания адреса основного DHCP-сервера данного порта, выберите курсором строку и нажмите клавишу *<Пробел>*. Запись адреса основного DHCP-сервера будет выделена цветом и отмечена литерой «**О**».

После установления адреса основного DHCP-сервера, можно ещё один адрес, куда будет ретранслироваться полученный портом запрос. Для этого следует в окне DHCP-Relay выбрать курсором строку с IP-адресом и нажать сочетание клавиш *<Alt+R>*.

Нажатие кнопки «*Сохранить*» вносит выполненные изменения в конфигурацию ФПСУ-IP.

Такой же интерфейс и последовательность действий применяется, если на ФПСУ-IP **установлена подсистема VLAN, но не используется в конфигурации**. В этом случае при нажатии на клавишу *<Пробел>* в поле «Адрес» будет выдано служебное оповещение, предлагающее выбрать режим конфигурирования.

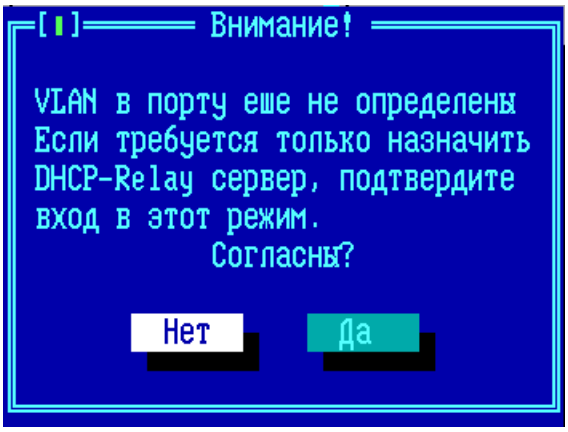

Рисунок 413 - Служебное оповещение

Если не требуется определять VLAN на портах ФПСУ-IP, нажмите кнопку «*Да*», после чего настройте работу DHCP, как описано выше, для ФПСУ-IP без подсистемы VLAN.

Если на ФПСУ-IP установлена подсистема VLAN, и порт комплекса участвует в нескольких VLAN, то определять DHCP-сервера потребуется для каждого VLAN.

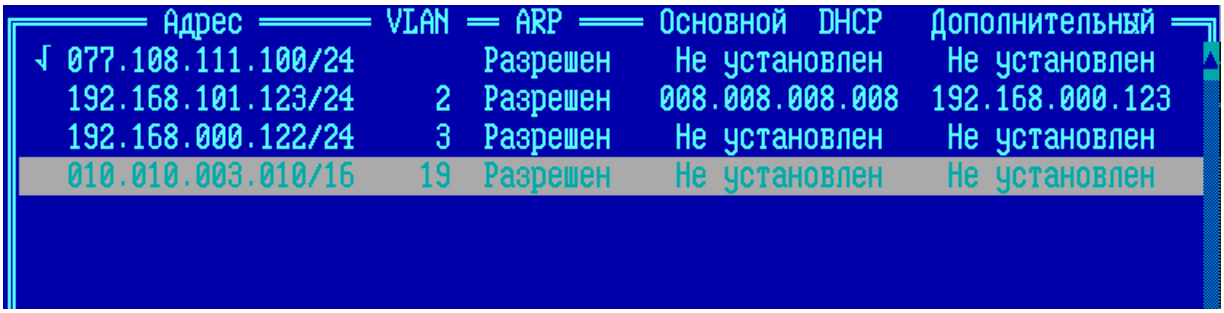

Рисунок 414 - Настройка DHCP на порту с определенными VLAN

DHCP-сервер для каждого VLAN устанавливается/изменяется отдельно, при выборе курсором строки VLAN и нажатии клавиши <*Пробел*>, открывается окно настройки DHCP.

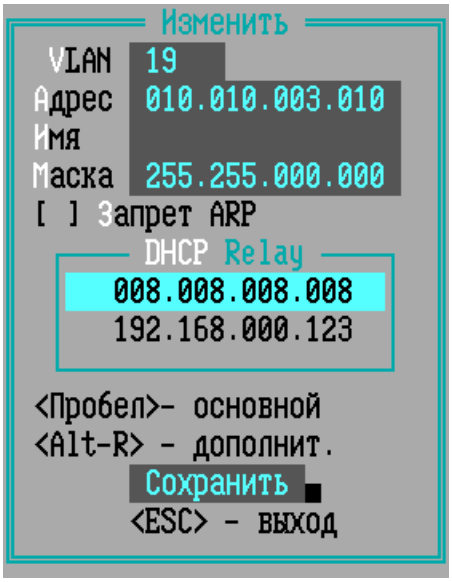

Рисунок 415 - Настройка DHCP-сервера для отдельного VLAN порта

Если в общий список доступных DHCP-серверов внесено больше одного IP-адреса, то для каждого VLAN порта ФПСУ-IP можно выбрать два – один основной DHCP-сервер, и один дополнительный.

По нажатию клавиши <*Пробел*> происходит выбор/отмена выбора основного DHCP-сервера. Сочетание клавиш <*Alt+R*> отмечает выбранный IP-адрес как дополнительный DHCP-сервер для редактируемого VLAN, это можно сделать только после выбора основного сервера. Также отменить выбор основного DHCP-сервера можно только тогда, когда не выбран или предварительно отменен выбор дополнительного сервера.

14. 8. Http-proxy ФПСУ-IP

На ФПСУ-IP может быть включен режим HTTP и SOCKS прокси (по умолчанию, прокси отключен). Для перехода в окно управления этими режимами, выполните команду

«*Сетевые сервисы*» → «*HTTP-Proxy*» меню конфигурации ФПСУ-IP:

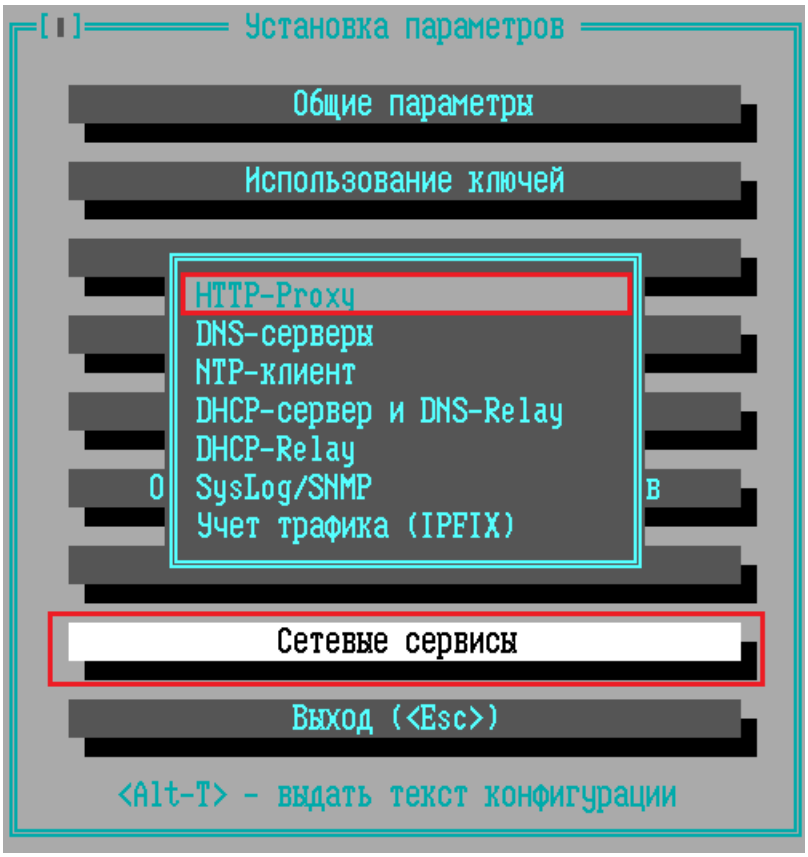

Рисунок 416 - Команда перехода в конфигурацию proxy на ФПСУ-IP

ВНИМАНИЕ! Подсистема http-прокси работает только для установленных на сетевых адаптерах драйверов типа **dpdk** (о выборе драйвера см. пункт «Конфигурация драйверов сетевых адаптеров»).

ВНИМАНИЕ! В случае использования версии ФПСУ-IP для виртуальной среды, виртуальной машине необходимо выделить минимум 2 гигабайта оперативной памяти для работы http-прокси!

Для запуска HTTP и/или SOCKS прокси на ФПСУ-IP, в открывшемся окне настройки следует установить следующие параметры:

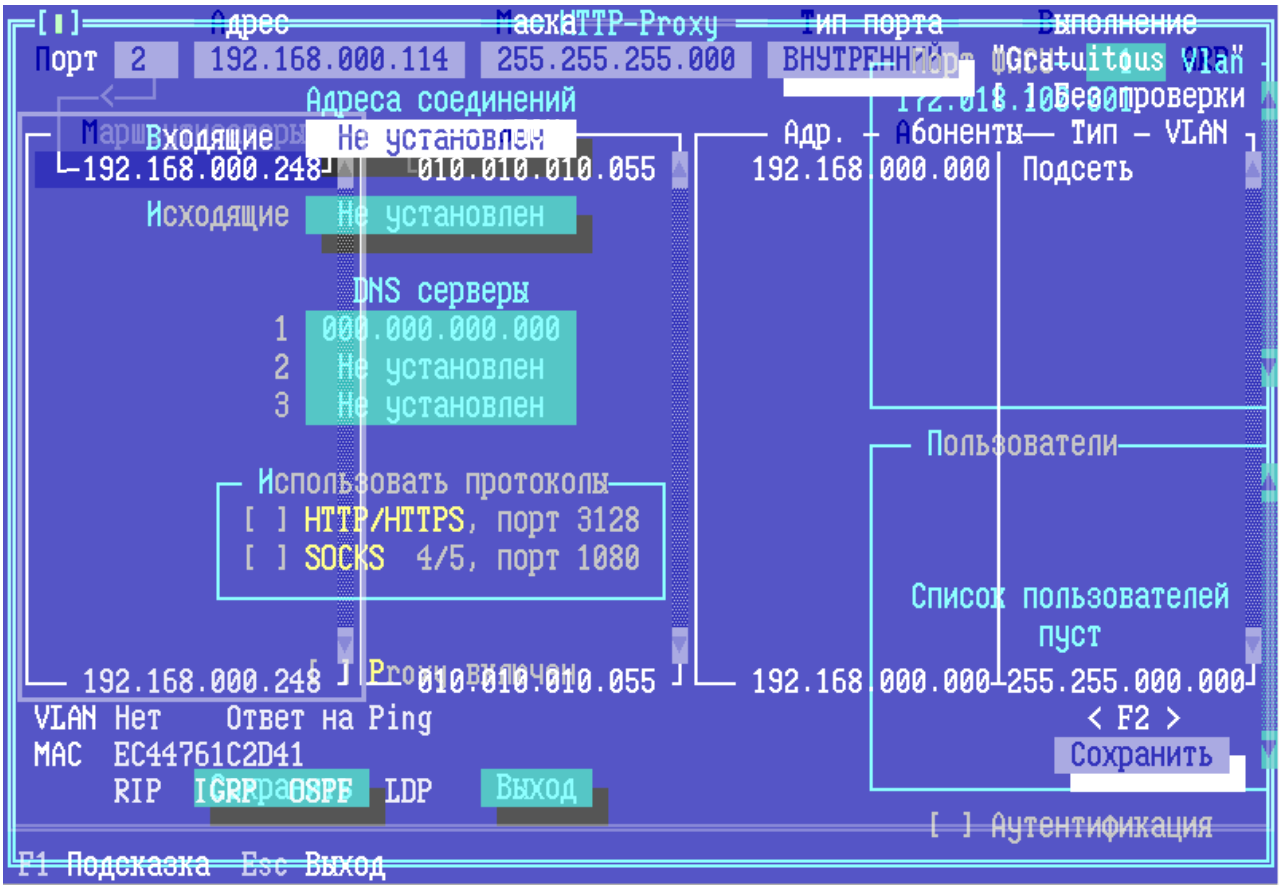

Рисунок 417 - Окно настроек HTTP-proxy

Адрес соединений, Входящие — здесь требуется указать IP-адрес логического порта ФПСУ-IP, на котором будет запущена служба прокси для входящих соединений. Адрес выбирается из списка портов в левой части окна. Этот IP-адрес входящих соединений пользователи должны будут указать в браузере или операционной системе как адрес прокси.

Адрес соединений, Исходящие — здесь требуется указать IP-адрес логического порта ФПСУ-IP, от которого будут переданы во внешнюю сеть пользовательские данные.

DNS серверы — для корректной работы http-прокси на ФПСУ-IP, в этом поле требуется указать IP-адрес хотя бы одного DNS-сервера, который будет разрешать имена пользовательских запросов.

Использовать протоколы — блок настроек, в котором администратор ФПСУ-IP должен выбрать запущенную службу прокси, *HTTP/HTTPS* и/или *SOCKS 4/5* версии. Для работы прокси требуется выбрать хотя бы один режим. Для каждого протокола указана справочная информация о номере порта, на котором прокси ФПСУ-IP будет принимать входящие соединения. Этот порт, вместе с IP-адресом входящих соединений, пользователи должны будут указать в браузере или операционной системе как порт прокси.

Proxy включен — флаг, запускающий прокси на ФПСУ-IP с указанными настройками. Если флаг снят, прокси не будет запущен.

Пользователи, Аутентификация — блок настроек, отвечающий за режим доступа пользователей к proxy по логину и паролю. По умолчанию выключен, и прокси ФПСУ-IP работает в анонимном режиме (подробнее см. пункт «Авторизация на http-proxy»).

Для выхода из окна и возвращение в меню конфигурации ФПСУ-IP с сохранением выполненных настроек, нажмите кнопку «*Сохранить*» или клавишу <*F2*>.

Для выхода из окна и возвращение в меню конфигурации ФПСУ-IP без внесения в конфигурацию сделанных изменений, нажмите кнопку «*Выход*» или клавишу <*Esc*>.

ВНИМАНИЕ! Если задействован межсетевой экран ФПСУ-IP (см. пункт «Параметры доступа, правила трафика межсетевого экрана»), прокси на ФПСУ-IP корректно работает только в случае добавления в межсетевой экран следующих дополнительных правил, разрешающих проход трафика:

1. Правило, разрешающее абоненту пакеты, источником которых устанавливаются пользователи, использующие ФПСУ-IP в качестве прокси. Назначением устанавливается интерфейс ФПСУ-IP, указанный в поле ***Адрес соединений, Входящие*** настроек прокси.
2. Правило, разрешающее передавать пакеты, источником которых является интерфейс ФПСУ-IP, указанный в поле ***Адрес соединений, Исходящие***. Назначением устанавливаются IP-адреса, с которыми будут работать пользователи прокси.
3. Правило, разрешающее ФПСУ-IP отправлять DNS-запросы на DNS-сервер. Источником пакетов является интерфейс ФПСУ-IP, указанный в поле ***Адрес соединений, Входящие***, а назначением – IP-адреса DNS-серверов, заданных для прокси ФПСУ-IP.

14. 8. 1. Авторизация на http-proxy

Блок настроек http- и socks-прокси ФПСУ-IP ***Пользователи и Аутентификация*** отвечает за режим доступа пользователей к proxy по логину и паролю. По умолчанию, аутентификация пользователей на прокси выключена и анонимный доступ к прокси разрешен:

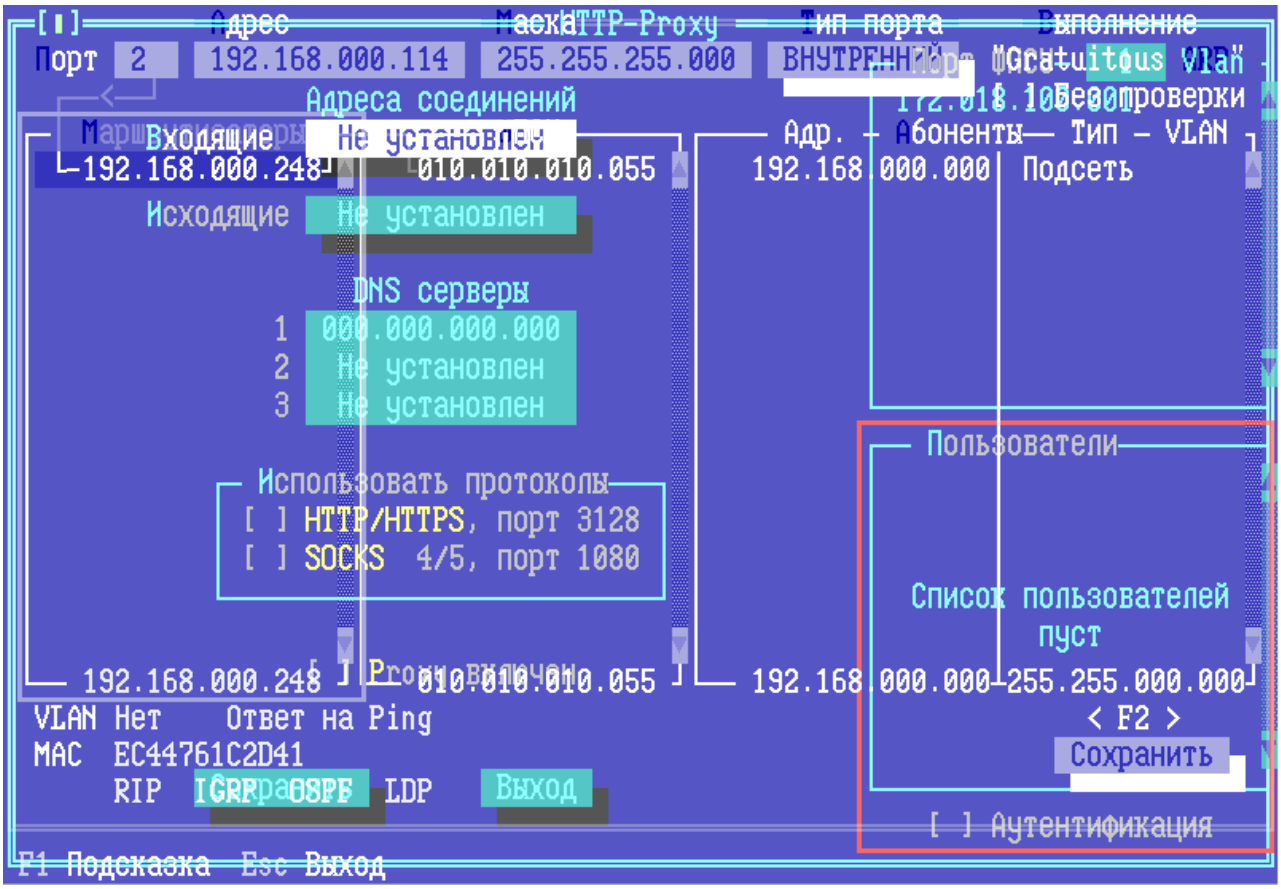

Рисунок 418 - Блок настройки пользователей proxy ФПСУ-IP

При включении опции ***Аутентификация*** анонимный доступ пользователей к прокси запрещается. Обращение пользователя к прокси ФПСУ-IP потребует авторизации - указания логина пользователя прокси и пароля. Включение опции ***Аутентификация*** выполняется клавишей <*Пробел*> при установленном на поле опции курсоре.

Список пользователей и паролей задается администратором ФПСУ-IP и отображается в списке блока ***Пользователи***.

Для добавления нового пользователя следует установить курсор на блоке ***Пользователи*** и нажать клавишу <*Ins*>. В появившемся окне потребуется указать следующую информация о новом пользователе:

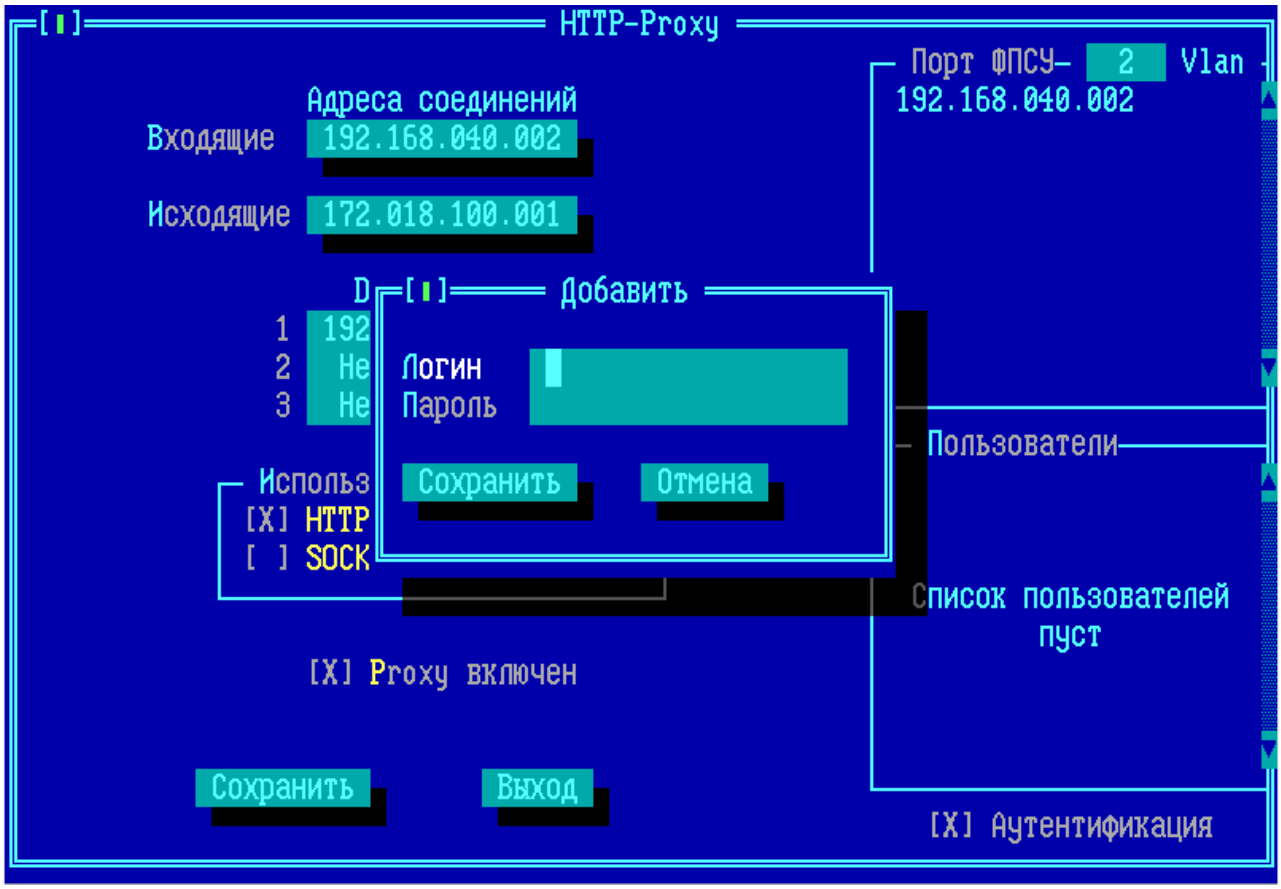

Рисунок 419 - Добавление учетной записи нового пользователя proxy ФПСУ-IP

Логин - имя для идентификации учетной записи нового пользователя прокси ФПСУ-IP;

Пароль - пароль для аутентификации учетной записи нового пользователя прокси ФПСУ-IP.

После указания логина и пароля к нему, нажмите кнопку «*Сохранить*». Новый пользователь прокси ФПСУ-IP будет добавлен в список:

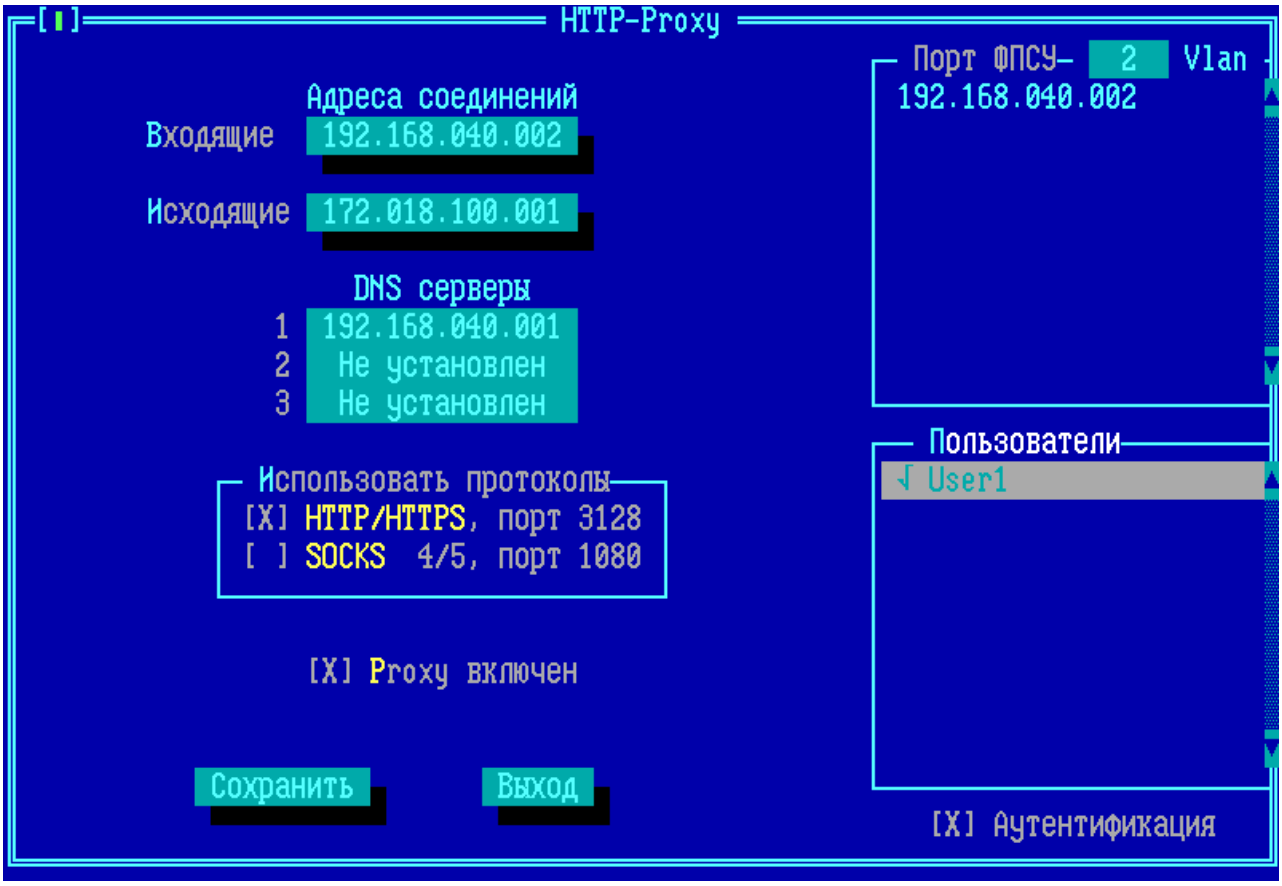

Рисунок 420 - Новый пользователь proxy ФПСУ-IP добавлен

После сохранения указанных настроек, только пользователь, указавший логин учетной записи прокси User1 и корректный пароль к ней, сможет воспользоваться работой через прокси ФПСУ-IP. Успешные и не успешные попытки авторизации пользователей на прокси ФПСУ-IP записываются в статистику.

Удаление учетной записи пользователя осуществляется клавишей <*Del*> при установленном на удаляемой учетной записи пользователя курсоре.

Для выхода из окна и возвращение в меню конфигурации ФПСУ-IP с сохранением выполненных настроек, нажмите кнопку «*Сохранить*» или клавишу <*F2*>.

Для выхода из окна и возвращение в меню конфигурации ФПСУ-IP без внесения в конфигурацию сделанных изменений, нажмите кнопку «*Выход*» или клавишу <*Esc*>.

14. 9. Взаимодействие со средствами обнаружения вторжений

ФПСУ-IP поддерживает взаимодействие со сторонними средствами обнаружения вторжений (далее СОВ). На ФПСУ-IP реализован специальный SysLog сервер, принимающий сообщения по протоколу syslog, отправленные с одного IP-адреса СОВ,

указанного администратором ФПСУ-IP. Полученные с одобренного СОВ syslog-сообщения анализируются, и, если в них содержится текст заранее определенного администратором ФПСУ-IP шаблона, то указанный в syslog сообщении IP-адрес заносится в стоп-лист межсетевого экрана ФПСУ-IP на заданное администратором ФПСУ-IP время.

Интерфейс настройки взаимодействия с СОВ вызывается по нажатию кнопки *«Интеграция с внешней СОВ»* вкладки **Анти-флуд и СОВ** параметров трафика межсетевого экрана (см. пункт «Дополнительные параметры и защита от flood-атак»). Флаг *«Анти-флуд включен»* должен быть установлен для работы с СОВ.

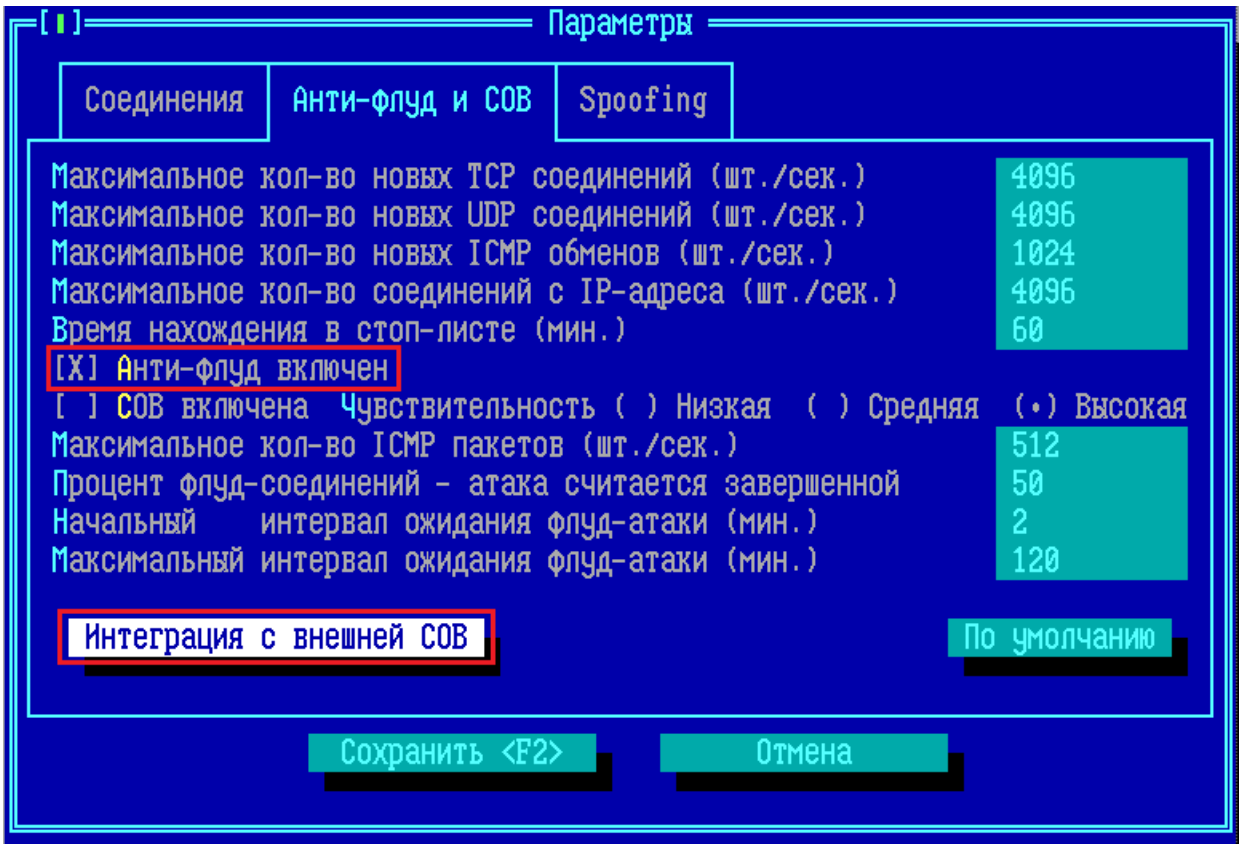

Рисунок 421 - Вызов интерфейса настройки взаимодействия с СОВ

В появившемся окне настройки взаимодействия с СОВ, администратор ФПСУ-IP может указать следующие параметры:

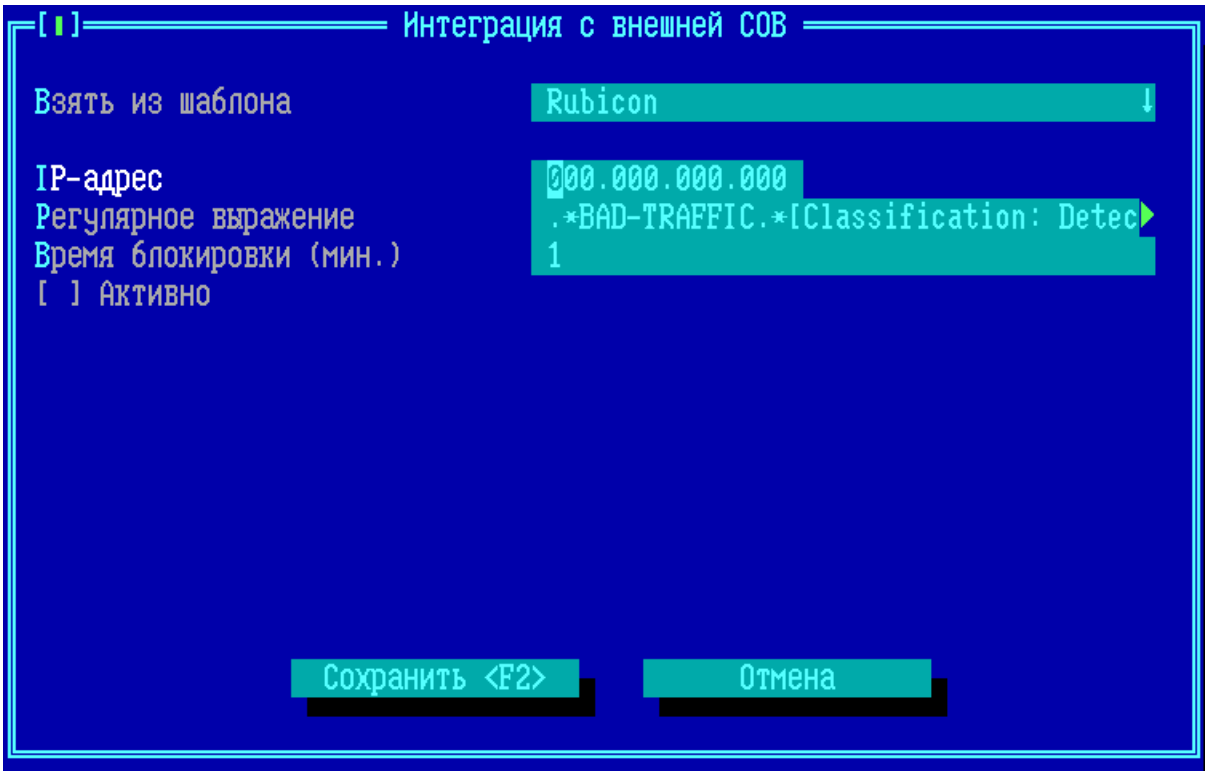

Рисунок 422 - Параметры взаимодействия с СОВ

Взять из шаблона – выбрать один из предложенных шаблонов взаимодействия с известными ФПСУ-IP средствами обнаружения вторжений. Поддерживается шаблон взаимодействия со средством защиты информации «Межсетевой экран и система обнаружения вторжений «Рубикон» версии 2.2.0.

Примечание. Шаблон рассчитан на сообщение об обнаружении подозрительного трафика по протоколу IP№53, для анализа других сообщений потребуется изменение шаблона.

IP-адрес – обязательная настройка; в этом поле указывается IP-адрес средства обнаружения вторжений, с которого ФПСУ-IP будет принимать и анализировать syslog-сообщения. Syslog-сообщения с других IP-адресов будут сброшены.

Регулярное выражение – обязательная настройка; несущий информацию о событии СОВ текст, поиск которого будет вестись в syslog-сообщении от СОВ. Если в syslog-сообщении будет найден текст из поля «Регулярное выражение», IP-адрес источника СОВ-события будет внесен в стоп-лист на указанное время блокировки.

Время блокировки (мин.) – таймер блокировки, в минутах; время, на которое будет помещен в стоп-лист IP-адрес, вызвавший событие СОВ. Устанавливается в пределах от 1 до 65535.

Активно – обязательная настройка; флаг, указывающий на включенный режим взаимодействия с СОВ. Если флаг снят, syslog-сообщения от СОВ не принимаются.

По окончании установки параметров, нажмите кнопку «*Сохранить <F2>*» для выхода из окна с сохранением выполненных настроек. Выход без сохранения осуществляется по клавише <*Esc*>.

Факты получения управляющих сообщений от СОВ могут быть отслежены в статистике по событию «Статистика IPS» (см. рисунок ниже).

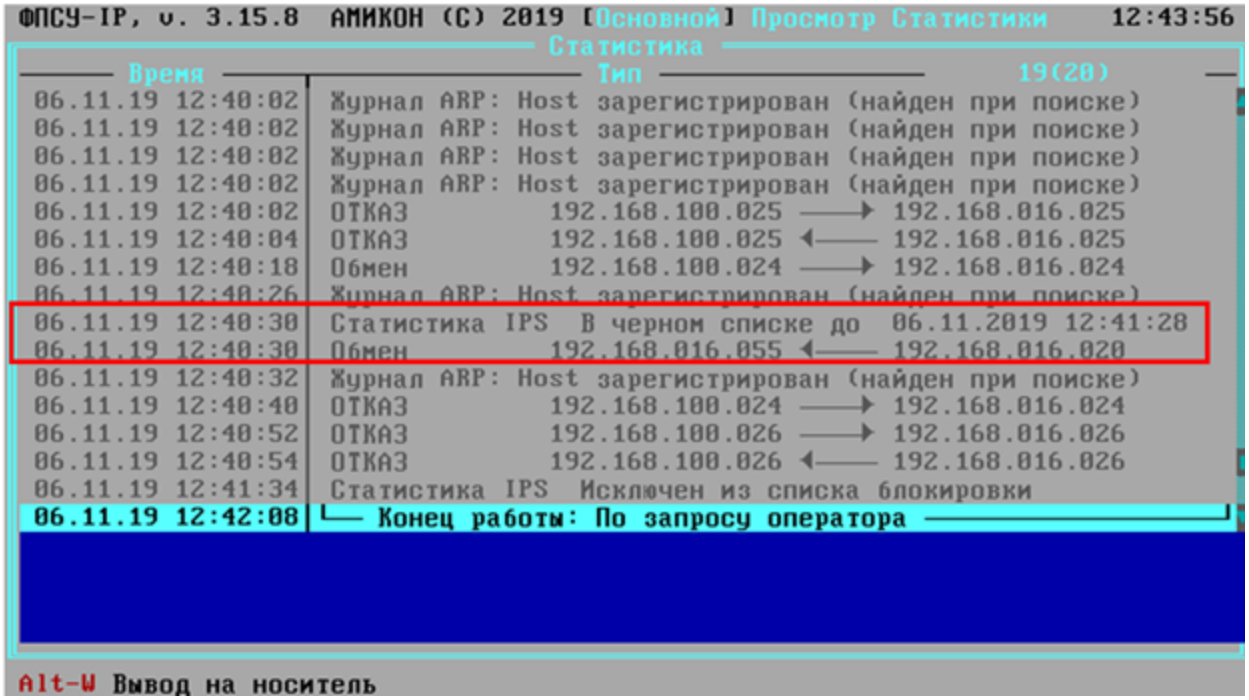

Рисунок 423 - Получено управляющее сообщение от СОВ

События блокировки передач абонентов по причине получения управляющего сообщения от СОВ (в случае совпадения полученного сообщения с заданным администратором ФПСУ-IP шаблоном) будут сопровождаться обменом от IP-адреса СОВ к IP-адресу порта ФПСУ-IP (на рисунке это обмен между от IP 192.168.016.020 к IP 192.168.016.055) записью «Статистика IPS» с комментарием «В черном списке до %ДД.ММ.ГГГГ% %чч.мм.сс%».

14. 10. NTP-клиент ФПСУ-IP

На ФПСУ-IP может быть установлен режим автоматической синхронизации текущего времени с одним из задаваемых тайм-серверов, работающих по протоколу NTP. NTP-клиент на ФПСУ-IP поддерживает синхронизацию с двумя NTP-серверами, которые указываются как «первичный» и «вторичный» в интерфейсе ФПСУ-IP. Синхронизация со вторичным

сервером включается при недоступности первичного.

ВНИМАНИЕ! НЕ СЛЕДУЕТ одновременно задействовать NTP-клиента и синхронизацию времени на ФПСУ-IP с удаленным администратором (см. пункт «Регистрация удаленного администратора на ФПСУ-IP»)!

Настройка синхронизации времени выполняется из пункта «*Сетевые сервисы*» → «*NTP-клиент*» конфигурации ФПСУ-IP:

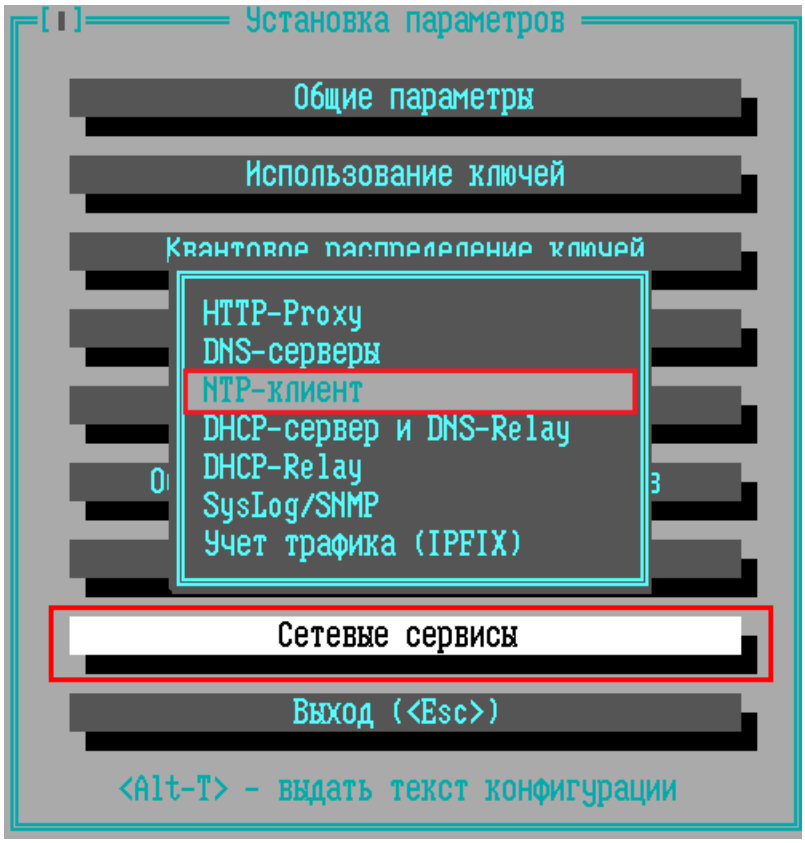

Рисунок 424 - Команда меню «Сетевые сервисы» → «NTP-клиент»

По умолчанию, параметры синхронизации времени не определены и NTP-клиент не задействован:

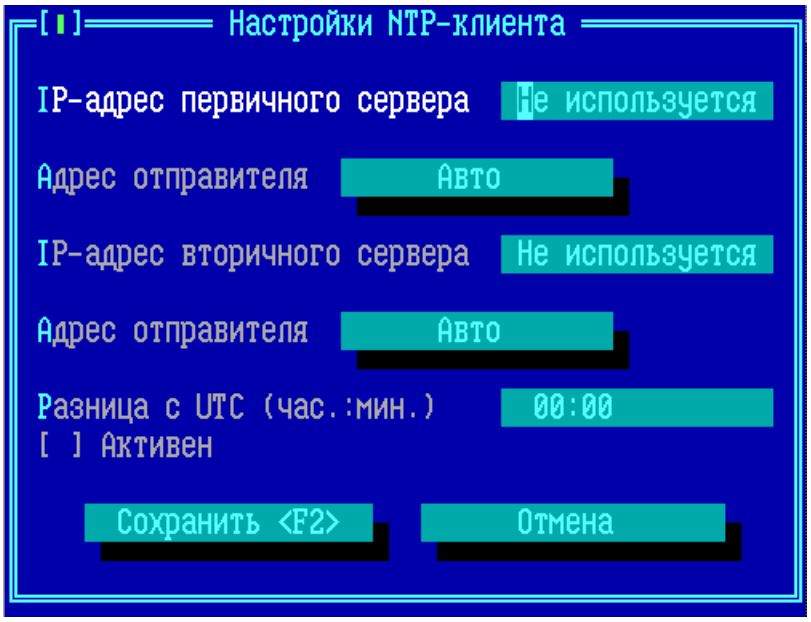

Рисунок 425 - Настройки NTP-клиента по умолчанию

Для включения NTP-клиента на ФПСУ-IP, следует выполнить следующие действия:

- указать адрес первичного NTP-сервера;
- задать для первичного NTP-сервера адрес отправителя - порт ФПСУ-IP или оставить автонастройку;
- указать адрес вторичного NTP-сервера, если требуется;
- задать для вторичного NTP-сервера адрес отправителя - порт ФПСУ-IP или оставить автонастройку;
- установить разницу временного пояса, в котором работает ФПСУ-IP, с UTC временем;
- задействовать флаг «*Активен*»;
- нажать кнопку «*Сохранить*».

Адрес отправителя - порт ФПСУ-IP, чей IP-адрес будет указан в качестве отправителя NTP-серверу. По умолчанию, режима «*Авто*», в качестве отправителя будет указан тот порт, на котором описан принадлежащий NTP-серверу IP-адрес. Администратор может безусловно указать, что сообщения следует отправлять от IP-адреса 1 или 2 порта ФПСУ-IP.

После нажатия кнопки «*Сохранить*» будет осуществлен выход в меню конфигурации ФПСУ-IP с сохранением выполненных настроек. Для выхода без сохранения нажмите клавишу <*Esc*> или кнопку «*Отмена*».

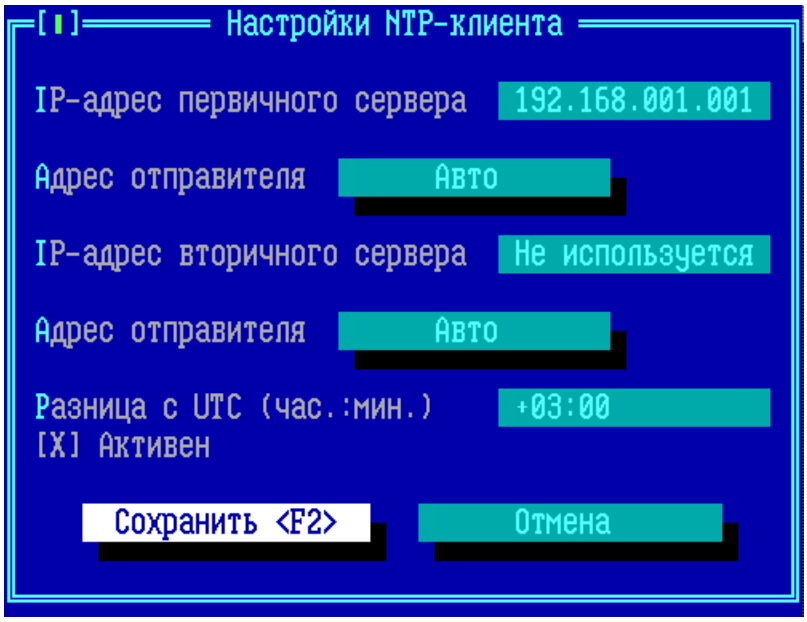

Рисунок 426 - Пример настроек NTP-клиента

IP-адрес вторичного NTP-сервера указывать не обязательно. После запуска ФПСУ-IP с задействованным NTP-клиентом, ФПСУ-IP каждую минуту опрашивает NTP-сервер и синхронизирует с ним время в случае расхождения.

14. 11. Особенности реализации ICMP протокола

При работе ФПСУ-IP с ICMP-сообщениями реализован ряд ограничений.

Полученный в адрес самого ФПСУ-IP ICMP-пакет, не содержащий ICMP-сообщения об ошибке, будет сброшен.

ФПСУ-IP отвечает на ICMP эхо-запросы в свои адреса, если запрос получен от:

- ФПСУ-IP/Клиента;
- другого ФПСУ-IP, с которым установлен туннель;
- абонента порта, которому явно выдано разрешение «отвечать на Ping».

ФПСУ-IP отправляет только следующие ICMP-сообщения об ошибках:

Таблица 427. Типы ICMP-ответов ФПСУ-IP

Тип	Статус	Код	Сообщение	Описание
3	Destination Unreachable	0	Destination network unreachable	– не найден MAC-адрес маршрутизатора; – абонент прописан через ФПСУ-IP, но туннель с этим ФПСУ-IP не установлен.

				Код устанавливается только для легальных пользователей.
		1	Destination host unreachable	– не найден MAC-адрес хоста-получателя. Код устанавливается только для легальных пользователей.
		2	Destination protocol unreachable	– обращение к ФПСУ-IP с неподдерживаемым протоколом. Код устанавливается только для легальных пользователей.
		4	Fragmentation required, and DF flag set	– пакет не может быть обработан, т.к. его размер превышает MTU следующего этапа маршрутизации или туннелирования и установлен флаг запрета фрагментации. Код устанавливается только для легальных пользователей.
		13	Communication administratively prohibited	– пакет не прошел фильтрацию на ФПСУ-IP; – не описан отправитель или получатель; – отправитель или получатель запрещен правилами межсетевого экрана; – отправителю запрещено отправлять эхо-запросы на ФПСУ-IP; – установлен запрет по работе с партнером; – при выставлении настройки «Сокрытие работы ФПСУ-IP» для ICMP-ответа с этим кодом в качестве адреса-ответчика устанавливается адрес получателя. Код устанавливается только для нелегальных пользователей.
11	Time Exceeded	0	TTL expired in transit	– истекло время жизни пакета.

Примечание. ICMP-ответ «Истекло время жизни пакета» не будет отправлен, если администратором включен режим сокрытия факта работы ФПСУ-IP (см. пункт «Общие параметры конфигурации ФПСУ-IP»).

14. 12. Поддержка Wake-on-Lan

На ФПСУ-IP поддерживается технология удаленного включения, Wake-on-LAN, позволяющая удаленно управлять включением рабочих станций. Удаленный администратор в программе «Удаленный администратор ФПСУ-IP» устанавливает параметры работы Wake-on-LAN на ФПСУ-IP. ФПСУ-IP от себя передаёт на указанные в параметрах рабочие станции так называемые magic packet. Подробно о включении данной функции на ФПСУ-IP изложено в руководстве «Удаленный администратор ФПСУ-IP».

14. 13. Служебные протоколы и порты на ФПСУ-IP

Таблица 428. Служебные протоколы и порты на ФПСУ-IP

Описание	Номер протокола или порта
Служебный протокол VPN-туннеля между ФПСУ-IP сетевого уровня, основной поток	IP №53
Служебный порт VPN-туннеля между ФПСУ-IP транспортного уровня, основной поток	UDP:30004
Служебный протокол удаленного администрирования сетевого уровня	IP №56
Служебный протокол удаленного администрирования транспортного уровня	UDP:30003
Служебный протокол отправляемых Syslog-сообщений	UDP:514
Служебный протокол для ответчика SNMP на ФПСУ-IP	UDP:161
Служебный протокол для SNMP trap на ФПСУ-IP	UDP:162
Служебный протокол NTP-клиента ФПСУ-IP	UDP:123

Описание	Номер протокола или порта
Служебные протоколы VPN-туннеля между ФПСУ-IP сетевого уровня, дополнительные потоки	IP №№110-226
Служебные порты VPN-туннеля между ФПСУ-IP транспортного уровня, дополнительные потоки	UDP:№№ 55 000 - 55 126
Служебные порты VPN-туннеля между ФПСУ-IP для динамических ФПСУ-IP	UDP:№№ 40 000 - 50 000
Служебные порты VPN-туннеля между ФПСУ-IP, для авторaспределения потоков	UDP:№№ 55 000 - 55 126

15. Статистика ФПСУ-IP

По умолчанию, ФПСУ-IP собирает всю статистику о всех происходящих на нём событиях и информационных обменах пользователей, и хранит её на ПЗУ. Статистика может быть отправлена удаленному администратору по запросу.

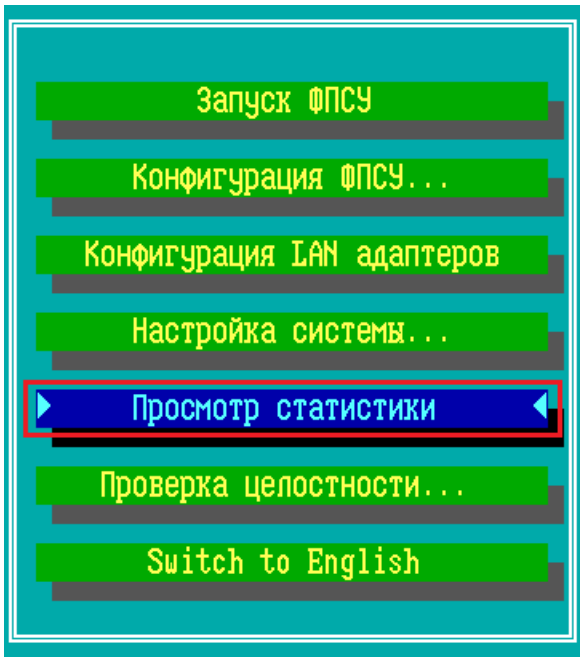

Рисунок 429 - Главное меню ФПСУ-IP

15. 1. Просмотр статистики

Команда «Просмотр статистики» главного меню ФПСУ-IP доступна администраторам класса «*Инженер*» и выше (см. раздел «Общие сведения», таблица 1).

При выборе команды, ФПСУ-IP осуществит выход в окно установки условий поиска накопленной регистрационной информации:

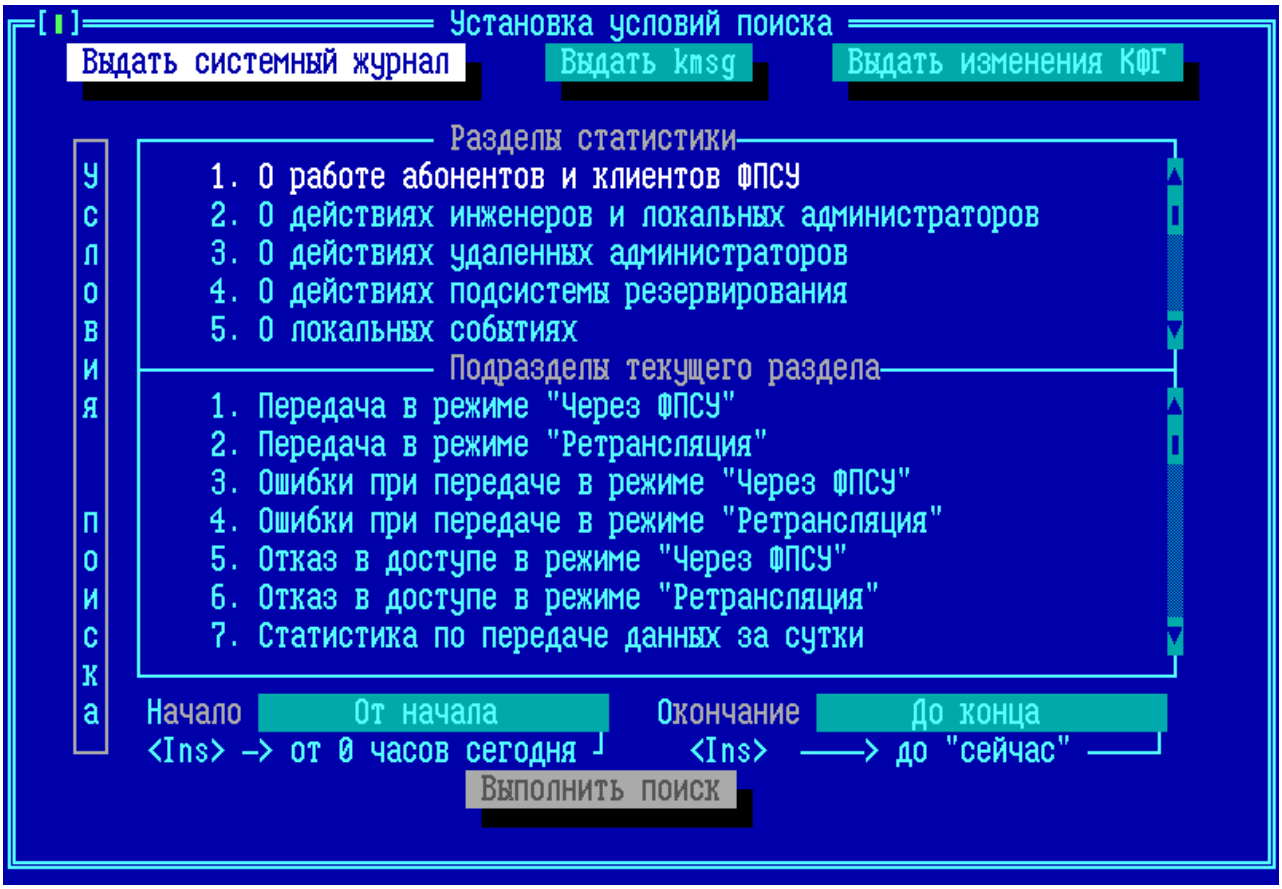

Рисунок 430 - Окно создания запроса на получение статистики

Для получения необходимых данных сначала отметьте нужный раздел, для чего выделите соответствующую строку и нажмите <*Пробел*>. При этом строка будет выделена слева знаком «√», а в окне подразделов отобразится относящийся к данному разделу список. Переход к подразделам осуществляется по нажатию <*Tab*> или <→>. Подразделы отмечаются так же, как и разделы. Возврат от подразделов к разделу осуществляется по нажатию клавиши <←>.

Далее укажите интервал времени, за который будет выбираться статистика. При входе в окно поля ввода времени будут содержать строки «*От начала*» и «*До конца*». Если необходимо задать другой интервал времени, можно вручную ввести необходимые значения в формате ДД.ММ.ГГГГ, где ДД - число, ММ - номер месяца, ГГГГ - год, и нажать <*Enter*>. Если формат введенных данных верен, установится новое значение, если нет - сохранится старая запись.

Переход между всеми полями осуществляется по нажатию <*Tab*>.

После задания всех требуемых установок для поиска следует при помощи клавиши <*Tab*> отметить команду «*Выполнить поиск*» и нажать клавишу <*Enter*>. Подсистема

регистрации осуществит поиск и выдаст результат на экран:

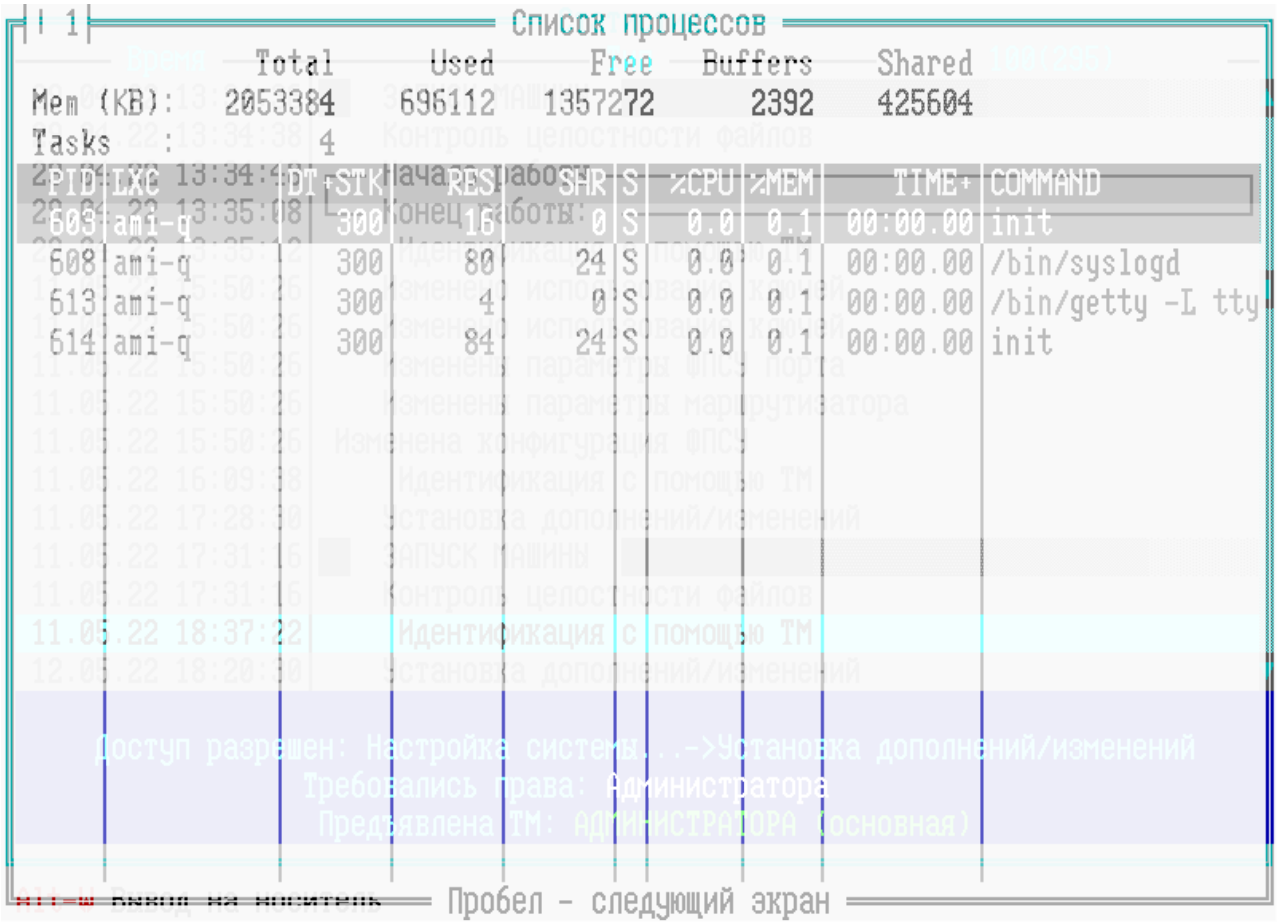

Рисунок 431 - Результат запроса статистики

Обратите внимание, что поиск будет выполняться лишь в том случае, если отмечен хотя бы один раздел запрашиваемых данных.

Данные выдаются в виде записей с указанием времени регистрации и типа события. Для текущей (отмеченной курсором) записи в нижней строке экрана указываются дополнительные сведения.

Выданные данные могут быть записаны на внешний носитель по нажатию комбинации клавиш <*Alt+W*>. Данные будут записаны на носитель в специальном формате и могут быть прочитаны средствами программно-аппаратного комплекса «Удаленный администратор ФПСУ-IP», который также поддерживает возможность конвертации записей статистики в текстовый формат для последующей обработки.

Для некоторых записей в нижней части окна отображается приглашение на получение дополнительной информации.

15. 2. Выдача системного журнала

Команда «Выдать системный журнал» окна просмотра статистики ФПСУ-IP («Статистика ФПСУ-IP») позволяет выдать на внешний носитель (USB-flash) файл с системным журналом статистики.

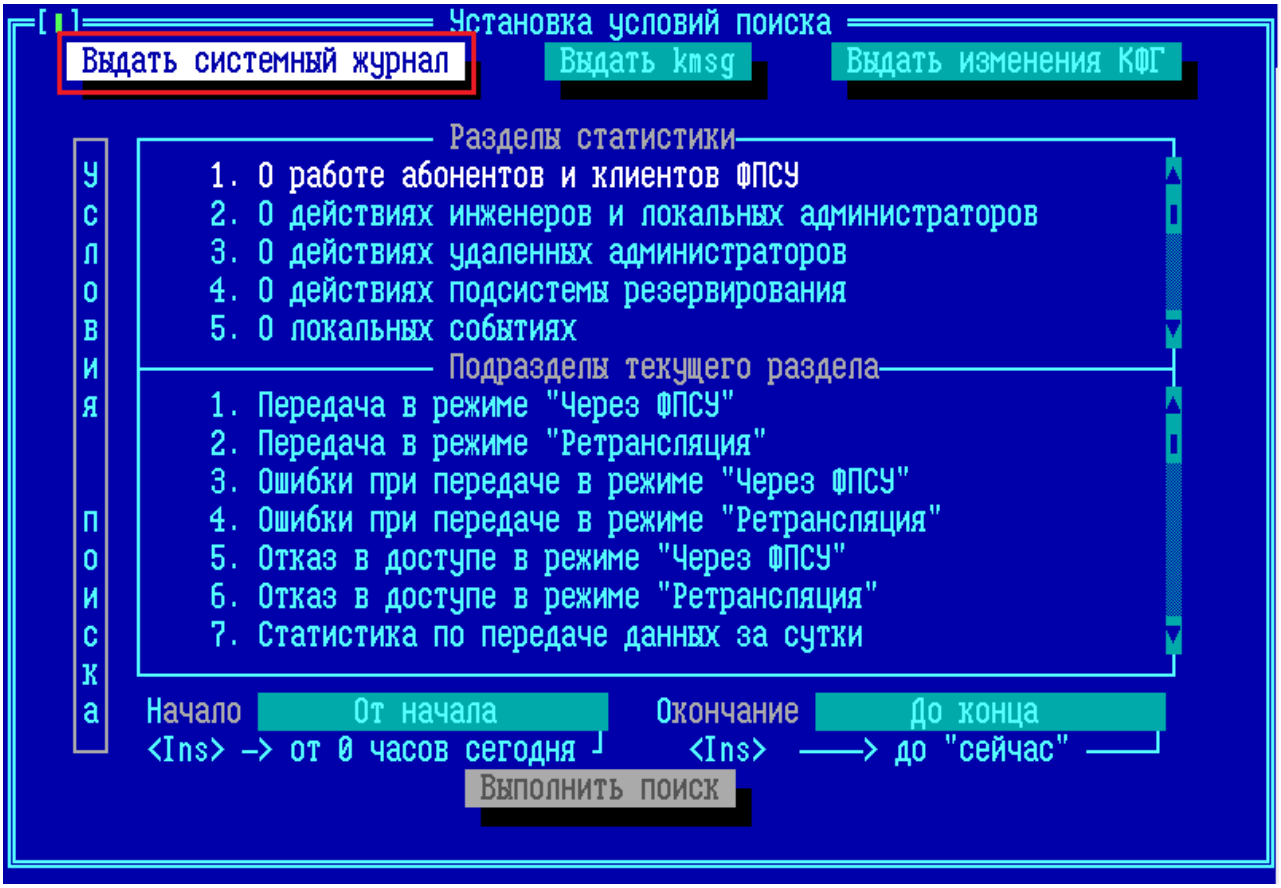

Рисунок 432 - Команда выдачи журнала изменений конфигурации межсетевого экрана

После выполнения команды система предложит подключить USB-носитель, на который будет выдан файл, к ФПСУ-IP:

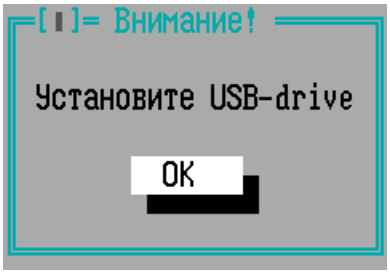

Рисунок 433 - Предложение подключить USB-носитель

Подключите носитель к ФПСУ-IP и подтвердите выполнение команды, нажав клавишу <*Enter*>. Если USB-носитель будет обнаружен ФПСУ-IP, то откроется окно

диалога, в котором следует выбрать каталог на носителе.

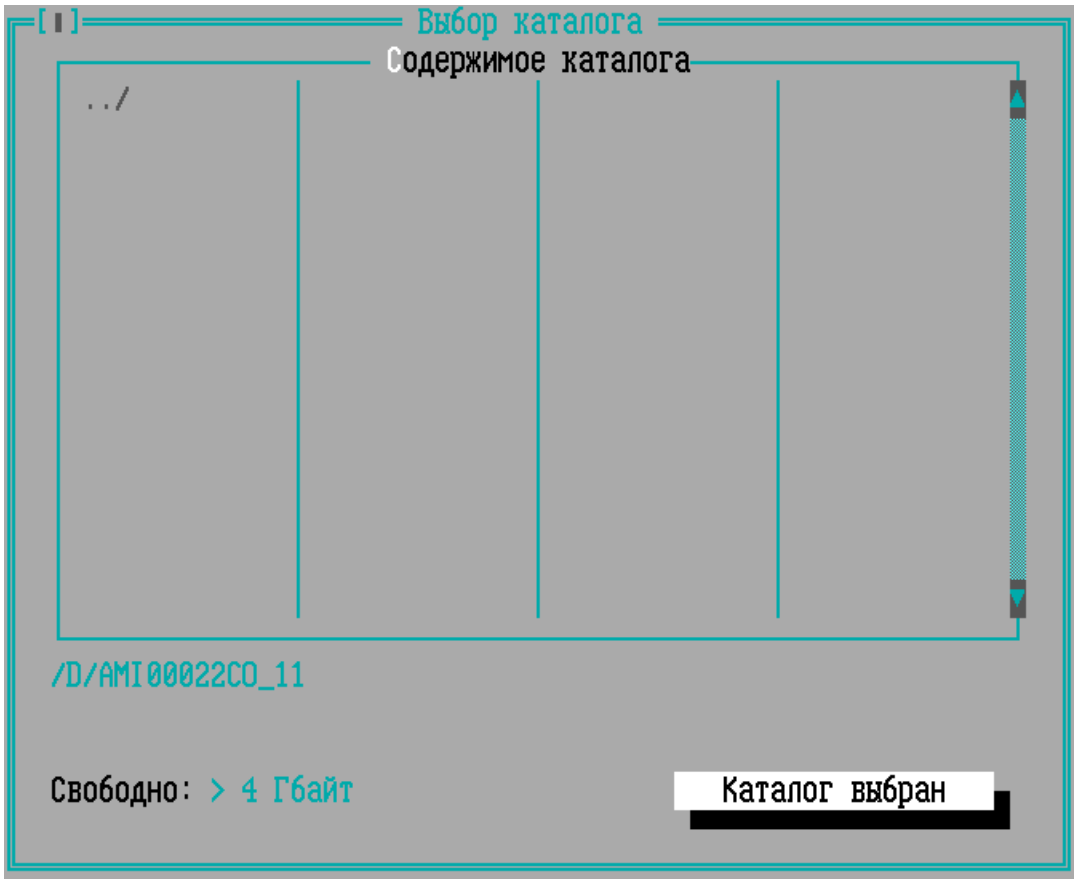

Рисунок 434 - Выбор каталога для выгрузки файла

Подтвердите место выгрузки файла, выполнив команду *«Каталог выбран»*.

После выгрузки файла, ФПСУ-IP выдаст системное оповещение о завершении процедуры:

Рисунок 435 - Сообщение о завершении процедуры

15. 3. Выдача журнала изменений конфигурации межсетевого экрана

Команда «Выдать изменения КФГ» окна просмотра статистики ФПСУ-IP позволяет выдать на внешний USB-носитель файл с журналом изменений конфигурации ФПСУ-IP.

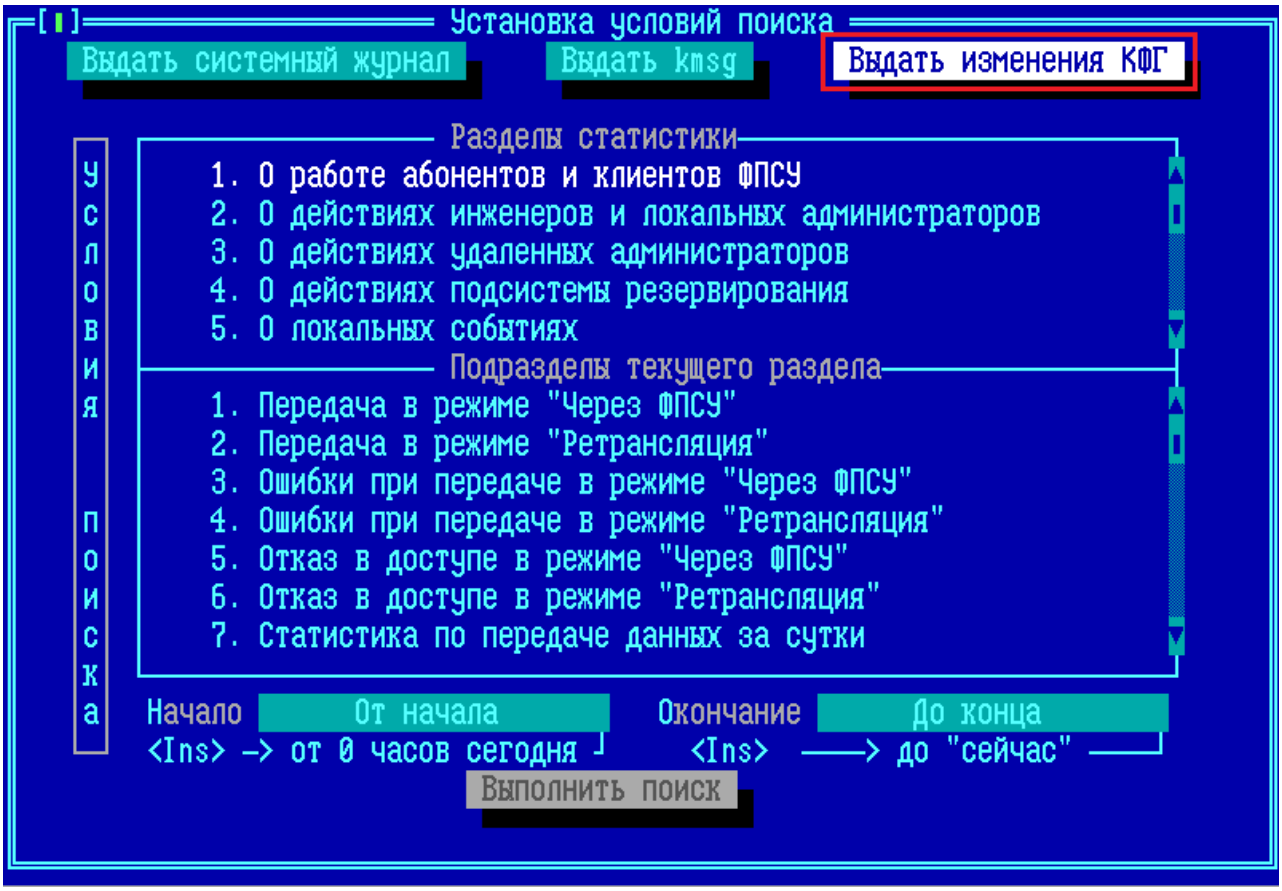

Рисунок 436 - Команда выдачи журнала изменений конфигурации межсетевого экрана

После выполнения команды система предложит подключить внешний носитель, на который будет выдан журнал, к ФПСУ-IP:

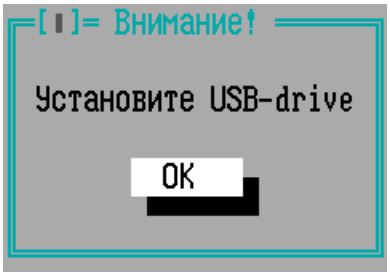

Рисунок 437 - Предложение подключить внешний носитель

Подключите носитель к ФПСУ-IP и подтвердите выполнение команды, нажав клавишу <*Enter*>. Если носитель будет обнаружен ФПСУ-IP, то откроется окно диалога, в котором следует выбрать каталог на носителе.

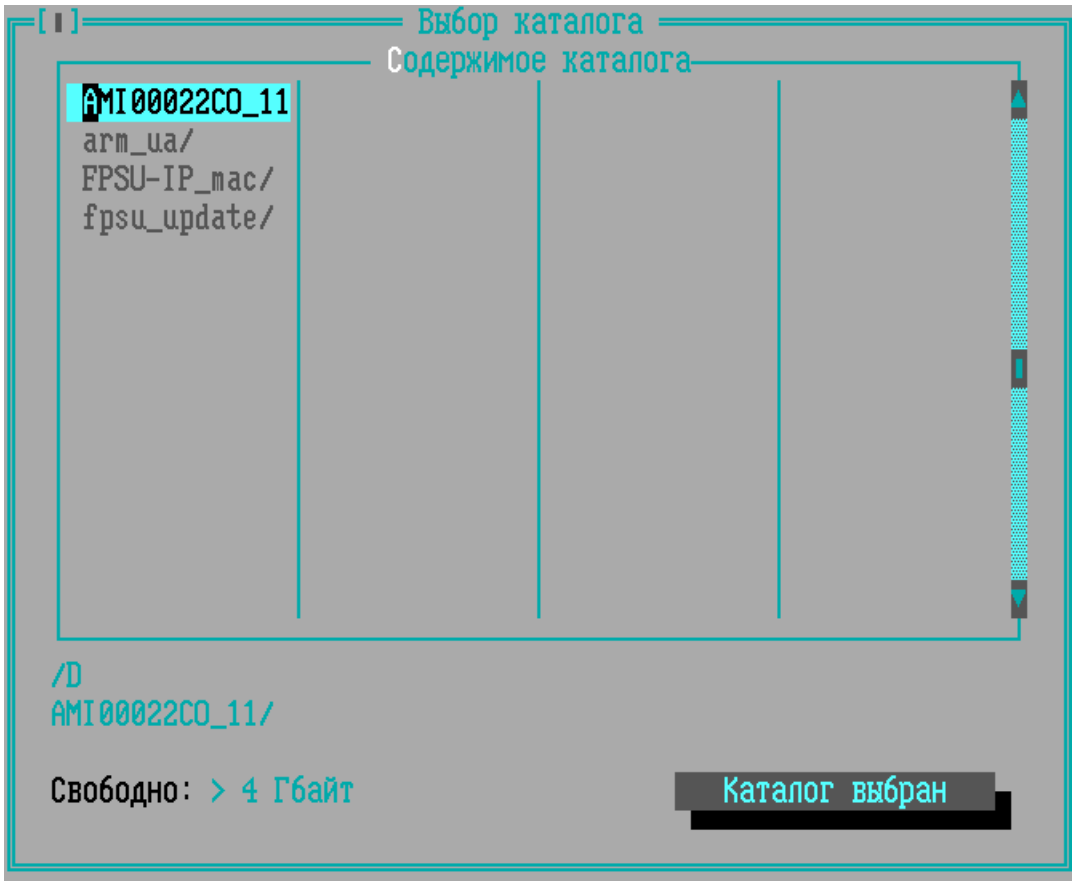

Рисунок 438 - Выбор каталога для выгрузки журнала

Подтвердите место выгрузки журнала, выполнив команду «Каталог выбран».

После выгрузки журнала, ФПСУ-IP выдаст системное оповещение о завершении процедуры:

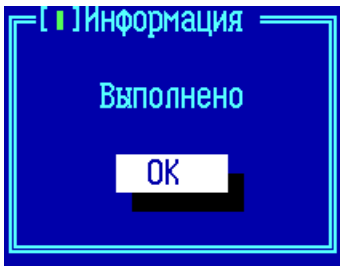

Рисунок 439 - Сообщение о завершении процедуры

Полученный журнал можно открыть текстовым редактором на другом ПЭВМ для просмотра и анализа изменений.

15. 4. Ограничение сбора статистики

Администратор может ввести ограничения на типы статистики, собираемой ФПСУ-IP. По умолчанию никаких ограничений не задано, собирается статистическая информация о всех происходящих на ФПСУ-IP событиях и всех передаваемых пакетах.

Отменить сбор статистики по ряду типов, таких как действия локальных администраторов, невозможно.

Переход в окно установки ограничений на сбор статистики осуществляется через окно общих параметров.

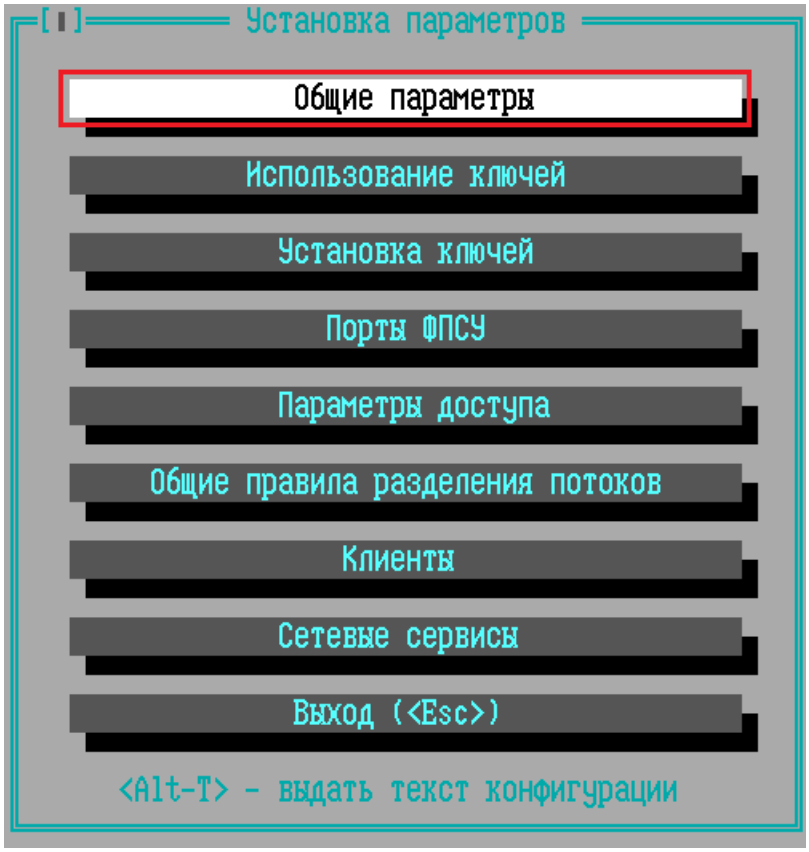

Рисунок 440 - Вход в общие настройки из основного меню конфигурации ФПСУ-IP

Выделите строку «Ограничения сбора статистики» курсором и нажмите клавишу <*Enter*> или <*Пробел*>.

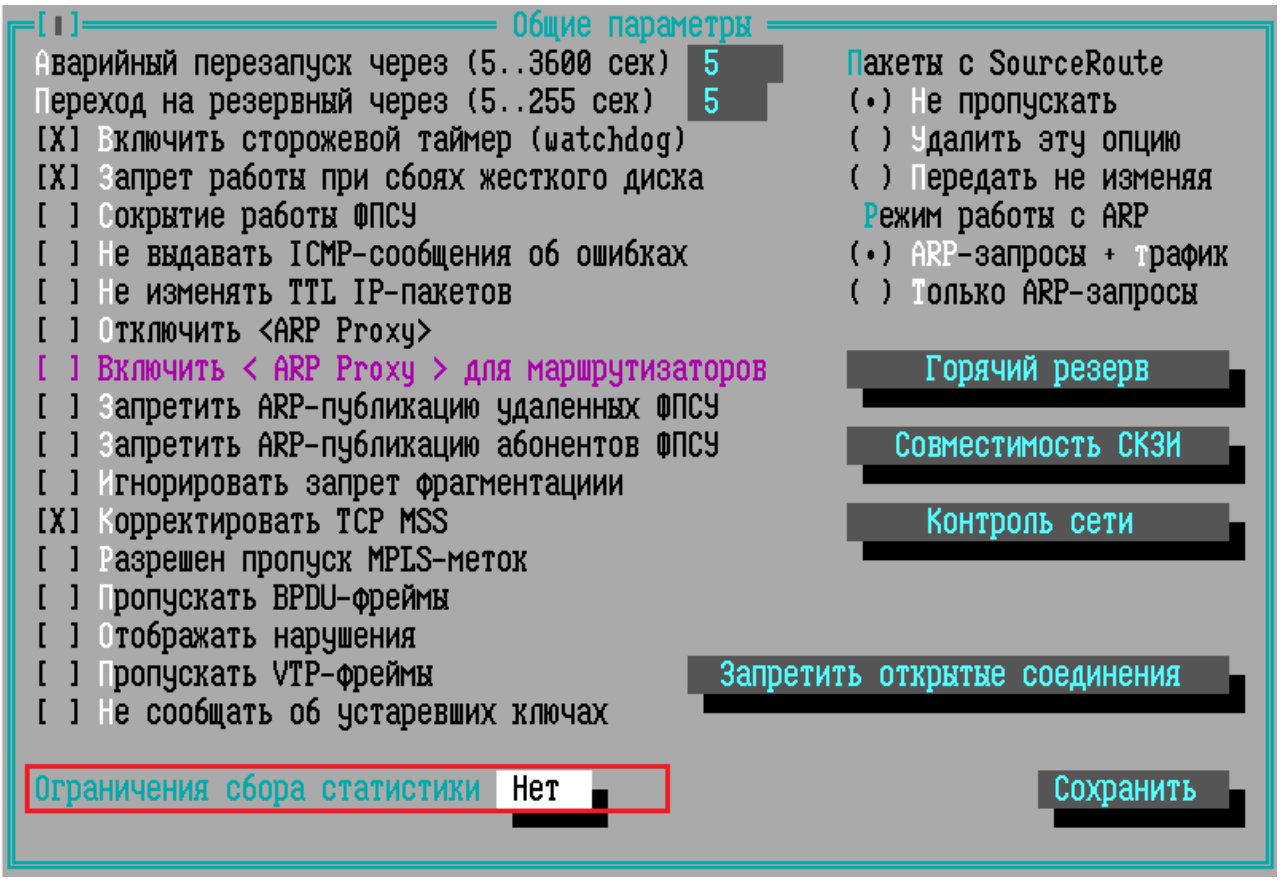

Рисунок 441 - Окно общих параметров ФПСУ-IP

В открывшемся окне при помощи клавиши *<Пробел>* отметьте те сведения, которые ФПСУ-IP не будет регистрировать во время своей работы.

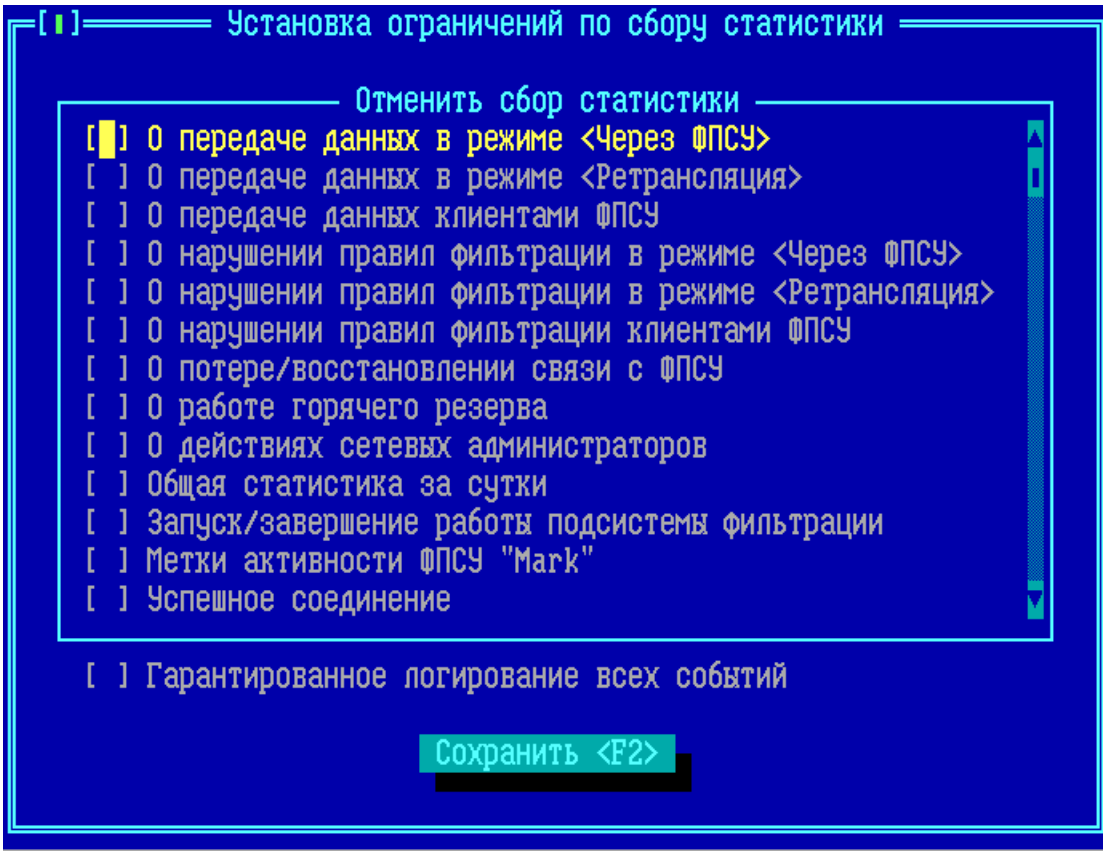

Рисунок 442 - Окно ограничения сбора статистики

Можно ограничить сбор статистики по следующим типам событий и передач данных:

О передаче данных в режиме <Через ФПСУ> – ФПСУ-IP не будет регистрировать происходящие через него информационные обмены, которые идут через VPN-туннель с другими ФПСУ-IP.

О передаче данных в режиме <Ретрансляция> – ФПСУ-IP не будет регистрировать происходящие через него информационные обмены абонентов, которые не передаются в VPN-туннель к другому ФПСУ-IP.

О передаче данных клиентами ФПСУ – ФПСУ-IP не будет регистрировать происходящие через него информационные обмены пользователей ФПСУ-IP/Клиентов.

О нарушении правил фильтрации в режиме <Через ФПСУ> – ФПСУ-IP не будет регистрировать попытки передать пакет в VPN-туннель к другому ФПСУ-IP, передача которого была не разрешена правилами доступа.

О нарушении правил фильтрации в режиме <Ретрансляция> – ФПСУ-IP не будет регистрировать попытки передать пакет в открытом виде, передача которого была не разрешена правилами доступа.

О нарушении правил фильтрации клиентами ФПСУ – ФПСУ-IP не будет регистрировать попытки передать не разрешенный правилами доступа пакет при обменах пользователей ФПСУ-IP/Клиентов.

О потере/восстановлении связи с ФПСУ – ФПСУ-IP не будет регистрировать события успешной и неуспешной установки VPN-туннеля с другим ФПСУ-IP.

О работе горячего резерва – ФПСУ-IP не будет регистрировать события передачи управления партнеру по системе «горячего резервирования».

О действиях сетевых администраторов – ФПСУ-IP не будет регистрировать действия пользователей программно-аппаратного комплекса «Удаленный администратор ФПСУ-IP».

Общая статистика за сутки – ФПСУ-IP не будет записывать ежедневную статистику в хранилище статистики.

Запуск/Завершение работы подсистемы фильтрации – ФПСУ-IP не будет регистрировать событие запуска и остановки штатного режима работы ФПСУ-IP.

Метки активности ФПСУ «Mark» – ФПСУ-IP не будет регистрировать факт отправления SysLog-серверу сообщения «Mark».

Успешное соединение – ФПСУ-IP не будет регистрировать успешное установление сессии при передаче пакетов.

Пакетный LOG – ФПСУ-IP не будет регистрировать для каждого обработанного межсетевым экраном пакета отдельную запись статистики (см. пункт «Параметры доступа, правила трафика межсетевого экрана»).

Статистика IPS – ФПСУ-IP не будет регистрировать события, связанные с системой защиты от flood-атак (см. пункт «Дополнительные параметры и защита от flood-атак»).

Журнал ARP – ФПСУ-IP не будет регистрировать факт обновления собственной ARP-таблицы.

Гарантированное логирование всех событий – флаг, при включении которого ФПСУ-IP будет гарантированно записывать необходимую статистику в хранилище, но при этом при увеличении количества пакетов скорость работы ФПСУ-IP может снижаться.

16. Восстановление работы ФПСУ-IP после сбоев

Сбои оборудования не влияют на защитные функции ФПСУ-IP, но некоторые аппаратные неполадки могут нарушить его работоспособность, что приведет к изоляции защищенного им сегмента сети передачи данных.

При авариях таких аппаратных компонент ФПСУ-IP, как ЦПУ, материнская плата и др., неисправные устройства заменяются, после чего ФПСУ-IP запускается заново и продолжает свою работу.

Работоспособность сетевых адаптеров ФПСУ-IP автоматически контролируется им во время работы по специальным признакам аппаратного уровня, сигнализирующим о его неработоспособности. При выявлении описанных признаков, драйверы сетевых адаптеров и подсистемы фильтрации ФПСУ-IP полностью перезагружаются. Для реализации данного механизма восстановления при настройке комплекса в параметрах конфигурации должно быть установлено время, по истечении которого будет осуществлен аварийный перезапуск комплекса (см. раздел «Общие параметры конфигурации ФПСУ-IP»). Если работоспособность восстановить не удается, ФПСУ-IP переходит в режим звукового оповещения администратора для принятия мер по замене неисправного оборудования. Если замена оборудования повлечет за собой изменения в программных настройках LAN-адаптеров, такая операция доступна только локальному администратору с правами не ниже «*Инженер*».

При необходимости, ПЗУ ФПСУ-IP может быть переставлено на другой ФПСУ-IP (ПЗУ на ФПСУ-IP должен оставаться единственным).

Аварии ПЗУ (SSD) ФПСУ-IP, влекущие за собой необходимость его замены и повторной установки ПО ФПСУ-IP на новый, наиболее критичны в смысле времени восстановления работоспособности ФПСУ-IP и защищаемой им ЛВС, поскольку все рабочие установки ФПСУ-IP и записанные на носитель данные будут потеряны. Одна из опций конфигурации ФПСУ-IP позволяет настроить его на такой режим работы, что при возникновении фатальной ошибки в результате сбоя или отказа ПЗУ ФПСУ-IP продолжит функционировать без регистрации событий в хранилище ФПСУ-IP (если политика безопасности организации это позволяет). При этом подсистема мониторинга не прекращает своей работы, и контроль за процессом фильтрации может осуществлять удаленный администратор с помощью ПАК «Удаленный администратор ФПСУ-IP».

Для быстрого восстановления работы рекомендуется хранить текущую конфигурацию ФПСУ-IP на внешнем носителе. В таком случае при смене внутреннего накопителя и повторной инсталляции ПО ФПСУ-IP (или замене всего устройства ФПСУ-IP) администратор может восстановить конфигурацию ФПСУ-IP с внешнего носителя, после

чего заново установить ключи парно-выборочной связи и общесистемные ключи клиентов, а также настроить сетевые адаптеры. Для осуществления указанных действий необходимы права классов *«Администратор»* или *«Главный администратор»* (см. раздел «Общие сведения», таблица 1).

Для возобновления работы ФПСУ-IP после сбоев электропитания без участия оператора ФПСУ-IP комплектуется **подсистемой автоматического старта**.

Во избежание нарушений межсетевого взаимодействия защищенных фрагментов локальных сетей, связанных с неполадками или отказами аппаратуры ФПСУ-IP, рекомендуется использовать комплект из двух ФПСУ-IP, работающих в режиме «горячего» резервирования. В такой паре один из ФПСУ-IP выполняет функциональные операции и считается активным, а второй находится в режиме ожидания. В случае аппаратных неполадок на активном ФПСУ-IP, резервный в течение короткого времени возобновляет фильтрацию и обмен данными между ЛВС в установленном режиме. Поскольку при обмене служебной информацией между партнерами по резервированию происходит синхронизация необходимых рабочих данных, работа ФПСУ-IP, на котором произошли аппаратные неполадки, также может быть достаточно быстро восстановлена (см. раздел «Принудительная синхронизация данных»).

17. Примеры настройки ФПСУ-IP

В данном пункте даются пояснения по конфигурированию ФПСУ-IP для некоторых стандартных сетевых топологий и удовлетворения определенных требований, налагаемых на работу подсетей. Эти примеры не являются реальными типичными схемами применения комплекса ФПСУ-IP и не дают исчерпывающего представления о его возможностях, а дают только общее представление о методологии конфигурирования для различных ситуаций.

Администратор должен четко представлять топологию используемых участков сети и маршруты следования передаваемых потоков информации. Приведенные примеры позволят администратору понять логику и принципы конфигурирования для отдельных частных случаев и обобщить их для построения единой конфигурации для конкретных условий.

Основные принципы конфигурирования маршрутизации на ФПСУ-IP:

- принцип белого листа (все, что явно не описано, считается запрещенным к передаче).
- описатели типа «Хост» используются для регламентации передачи индивидуальных пакетов (unicast);
- описатели типа «Подсеть» и «Любой Хост» используются для регламентации передачи как индивидуальных, так и широковещательных пакетов;
- индивидуальные IP-адреса абонентов (описатели типа «Хост») не могут быть дублированы. Однако IP-адреса, принадлежащие указанным в конфигурации маршрутизаторам, могут повторно указываться в разделе описания абонентов на соответствующем порту, а IP-адреса, принадлежащие указанным в конфигурации ФПСУ, могут повторно указываться в разделе описания маршрутизаторов;
- создание со стороны одного порта описателя хоста или подсети, принадлежащих или включающих в себя описатель (по IP-адресу и маске, для подсети), который уже определен на другом порту, разрешено. При этом ФПСУ-IP автоматически «вычеркнет» из более общего описателя на соответствующем порту более конкретный описатель и со стороны этого порта хосты, принадлежащие более конкретному описателю, будут считаться отсутствующими, т.е. не описанными в конфигурации порта;
- подсеть с одним и тем же IP-адресом и той же маской в общем случае (для передачи как индивидуальных, так и широковещательных пакетов) нельзя описать на двух портах одновременно. При попытке дублирования уже существующего на противоположном порту описателя типа «Подсеть» создаваемая запись типа «Подсеть» может быть использована только для передачи широковещательных пакетов (флаг «Только Broadcast» выключить нельзя).

17. 1. Базовая настройка ФПСУ-IP для ретрансляции пакетов локальной сети

Предположим, что IP-сеть организации до установки ФПСУ-IP представляла одну подсеть с IP-адресом 203.0.113.0 и маской 255.255.255.0 (24 разряда) и содержала маршрутизатор для выхода в другие IP-сети. IP-адреса 1 и 2 портов ФПСУ-IP совпадают, для ФПСУ-IP это допустимо, если в локальной сети доступно ограниченное количество свободных IP-адресов. После установки ФПСУ-IP топология сети приобрела вид, отображенный на схеме ниже.

С точки зрения конфигурирования ФПСУ-IP для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны порта 1 (защищаемая область) существует одна подсеть; маршрутизаторы и другие ФПСУ-IP, через которые абоненты будут доступны с порта 1, отсутствуют;
- со стороны порта 2 абоненты не определены, доступ к ним будет осуществляться через маршрутизатор (по IP-адресу связанного с ФПСУ-IP порта), а другие ФПСУ-IP отсутствуют;
- обмен абонентов защищаемой области с абонентами Internet/Intranet может производиться только в режиме ретрансляции. Сжатие и криптозащита трафика не применяется;
- работа с ключевыми данными при такой топологии не требуется.

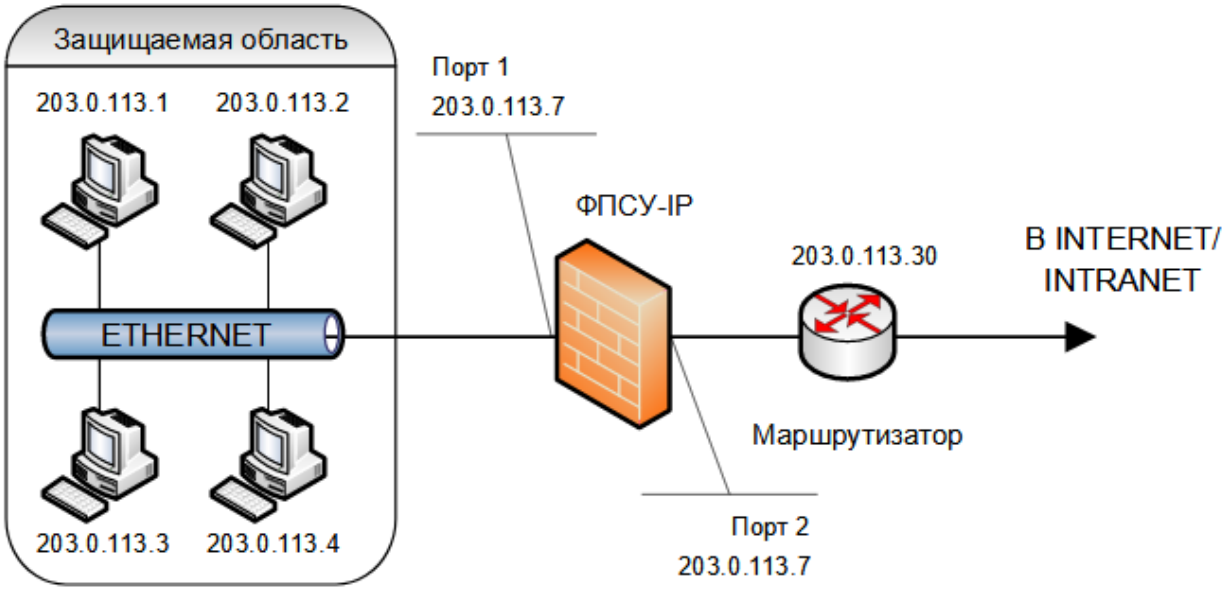

Рисунок 443 - Применение ФПСУ-IP для защиты оконечной области

Конфигурация ФПСУ-IP должна содержать следующие установки:

```
================================================================================
```

Порт 1:

Номер 1;
Адрес 203.0.113.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 203.0.113.0; Маска 255.255.255.0;
режим работы ретрансляция;
режим партнера этого порта — выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 203.0.113.1;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 203.0.113.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы 203.0.113.30;
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.
Абоненты: Любой хост
режим работы ретрансляция;
через маршрутизатор 203.0.113.30;
флаг "Работа разрешена" включен.

```
================================================================================
```

При необходимости администратор может регламентировать доступ к хостам своей подсети только по определенным протоколам и/или TCP/UDP-портам (через включение дополнительных правил межсетевого экрана, см. раздел «Параметры доступа, правила трафика межсетевого экрана», в данном примере их настройка не рассматривается).

Остальные параметры конфигурации (например, обработка IP-опций или сокрытие фильтрующих свойств комплекса) описываются на усмотрение администратора.

17. 2. Защита локальной сети, состоящей из двух IP-подсетей

Представим теперь, что защищаемая область состоит из двух IP-подсетей, абоненты которых должны обмениваться пакетами не только с абонентами Internet/Intranet, но и друг с другом, причем эти обмены также должны фильтроваться установленным ФПСУ-IP. В таком случае пакеты от абонентов IP-подсети 1 будут передаваться на порт 1 комплекса ФПСУ-IP, с которого они будут передаваться обратно в защищаемую область и доставляться абонентам IP-подсети 2 (аналогично будут передаваться пакеты абонентов подсети 2, направленные абонентам подсети 1). IP-адреса 1 и 2 портов ФПСУ-IP совпадают, для ФПСУ-IP это допустимо, если в локальной сети доступно ограниченное количество свободных IP-адресов.

Такая организация защищаемой подсети приведет к следующей логике конфигурирования:

На порту 1 ФПСУ-IP должны быть описаны две различные IP-подсети и для каждой подсети (или ее отдельных абонентов) должна быть разрешена работа с партнером своего порта в режиме «ретрансляции». Кроме того, все хосты защищаемой области должны быть сконфигурированы таким образом, чтобы в качестве маршрутизатора по умолчанию у них был указан маршрутизатор с адресом 192.168.1.30 или IP-адрес 1-го порта ФПСУ-IP.

На работу подсети наложены следующие ограничения:

- хост с IP-адресом 192.168.1.1 является администратором маршрутизатора, обмен IP-пакетами с подсетью 2 ему запрещен; кроме того, он должен иметь круглосуточный доступ в сеть Internet/Intranet;
- остальные хосты подсети 1 и хосты подсети 2 имеют доступ друг к другу и не должны взаимодействовать с Internet/Intranet.

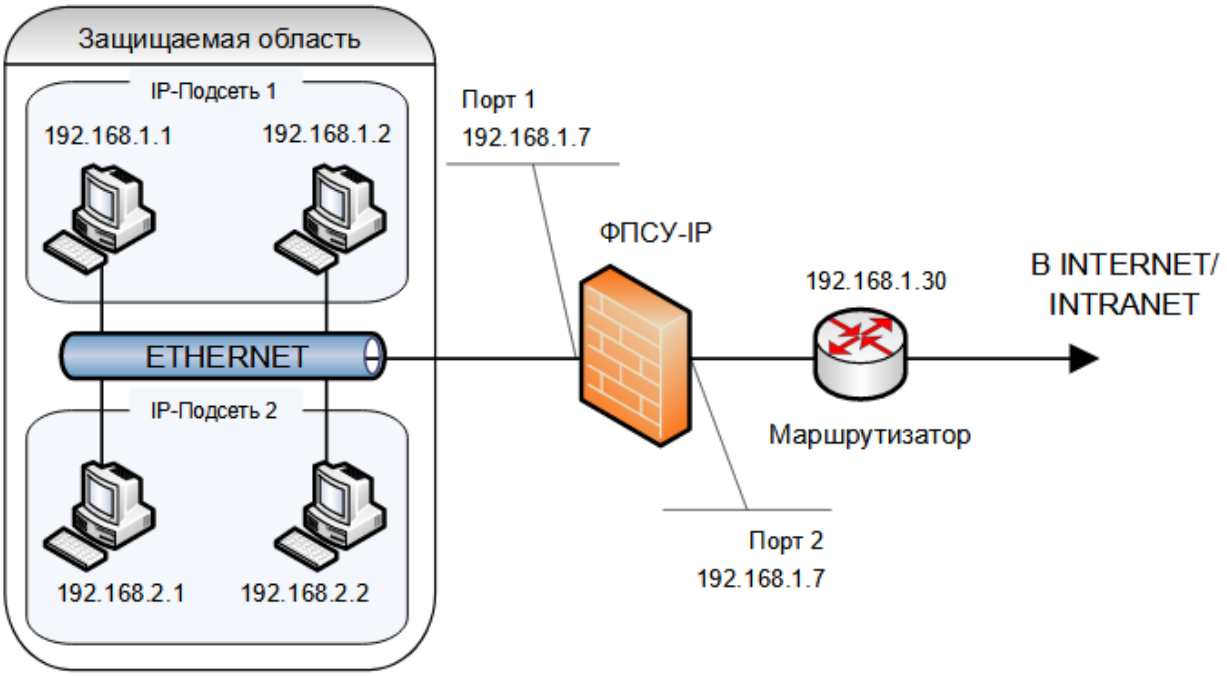

Рисунок 444 - Защита двух подсетей

С точки зрения конфигурирования ФПСУ-IP для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны внутреннего порта комплекса (порта 1) существуют две отдельные IP подсети, маршрутизаторы и ФПСУ-IP отсутствуют;
- со стороны порта 2 абоненты не определены, доступ к ним будет осуществляться через маршрутизатор (по IP-адресу связанного с ФПСУ-IP порта), а другие ФПСУ-IP отсутствуют;
- обмен администратора защищаемой области с абонентами общедоступной сети передачи данных может производиться только в режиме ретрансляции, сжатие и криптозащита не применяются;
- работа с ключевыми данными при такой топологии не требуется;
- абонентам подсетей 1 и 2 работа разрешается только с абонентами со стороны своего порта, причем администратор маршрутизатора не должен участвовать в таких обменах;
- абонент с IP-адресом 192.168.1.1 должен обмениваться пакетами с абонентами со стороны порта 2 и должен быть допущен к управлению маршрутизатором.

Конфигурация ФПСУ-IP должна содержать следующие установки:

==========

Порт 1:

Номер 1;
Адрес 192.168.1.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть; 192.168.1.0; 255.255.255.0 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта - включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть; 192.168.2.0; 255.255.255.0 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта - включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 192.168.1.1;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.1.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы
192.168.1.30;
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.
Абоненты:
Любой хост;
режим работы ретрансляция;
через маршрутизатор 192.168.1.30;
флаг "Работа разрешена" включен.

==========

Для выполнения дальнейших настроек рекомендуется ознакомиться с разделом «Параметры доступа, правила трафика межсетевого экрана».

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее взаимодействие абонента 192.168.1.1 (источник) с маршрутизатором 192.168.1.30 (назначение);
2. Правило, разрешающее взаимодействие абонента 192.168.1.1 (источник), и абонента Любой хост 2 порта ФПСУ-IP (назначение);
3. Правило, разрешающее взаимодействие абонентов всех абонентов подсетей 1 и 2 (источник), и абонентов подсетей 1 и 2 (назначение);
4. Правило, запрещающее взаимодействия абонента 192.168.1.1 (и в качестве источника, и в качестве назначения), с абонентами подсети 2 (источник и назначение). Причем это правило должно иметь приоритет выше, чем правило из пункта 3.

Дополнительно, администратор может регламентировать доступ по времени (через выбор из ранее созданных интервалов времени в выпадающем списке «Время работы» правила доступа, см. пункт «Интервалы времени»).

Остальные параметры конфигурации (например, обработка IP-опций или сокрытие фильтрующих свойств комплекса) описываются на усмотрение администратора.

В данном примере функциональное отделение абонента 192.168.1.1 от IP-подсети 2 (запрещение обменов) производится двумя независимыми друг от друга ограничениями:

1. По настройке абонента 192.168.1.1 в разделе конфигурации «Порты ФПСУ», по признаку «Режим партнера – Данного порта» (режим «Ретрансляция» выключен);
2. Правилом 4. межсетевого экрана из списка выше.

Несмотря на то, что хостам со стороны порта 1 (исключая администратора) запрещено выходить в общедоступную сеть передачи данных, режим работы с партнером другого порта (ретрансляция) для них включен. Это объясняется тем, что данный режим отключить нельзя, поскольку отключение обоих режимов работы с партнером другого порта (по недосмотру или ошибке администратора) может привести к тому, что обмен пакетами через ФПСУ-IP окажется невозможен и абоненты защищаемой области окажутся отрезанными от сети. Запрещение работы этим хостам будет обеспечиваться тем, что единственный абонент, описанный со стороны порта 2 через запись «Любой хост», включен только в одно правило доступа, разрешающее взаимодействие лишь с абонентом 192.168.1.1.

17. 3. Разделение подсети на два фрагмента ФПСУ-IP на уровне маршрутизации

Представим теперь, что до установки ФПСУ-IP существовала одна IP-подсеть с адресом 203.0.113.0 и маской 255.255.255.0, которую необходимо разделить физически на

два независимых фрагмента (например, по функциональному признаку) без переконфигурирования программного обеспечения хостов, причем требуется регламентировать обмены данными между хостами независимых фрагментов. Отметим, что в предыдущем примере (см. пункт «Защита локальной сети, состоящей из двух IP-подсетей») разделение абонентов на две подсети было логическим, то есть для его осуществления была необходима особая конфигурация TCP/IP-стека защищаемых хостов, при изменении которой выполнение наложенных в примере требований было бы невозможно. В данном примере рассматривается физическое разделение подсети, при котором абоненты отдельных фрагментов физически не могут обмениваться пакетами друг с другом в обход комплекса ФПСУ-IP.

IP-адреса 1 и 2 портов ФПСУ-IP совпадают, для ФПСУ-IP это допустимо, если в локальной сети доступно ограниченное количество свободных IP-адресов.

После установки ФПСУ-IP сеть имеет вид, изображенный на рисунке ниже.

Помимо физического разделения на работу двух подсетей накладываются следующие требования:

- хосты области 1, исключая хост 203.0.113.1, и все хосты области 2 должны иметь полный доступ друг к другу, в том числе должна обеспечиваться возможность поиска и подключения сетевых дисков;
- хост 203.0.113.1 не должен иметь доступа в область 2.

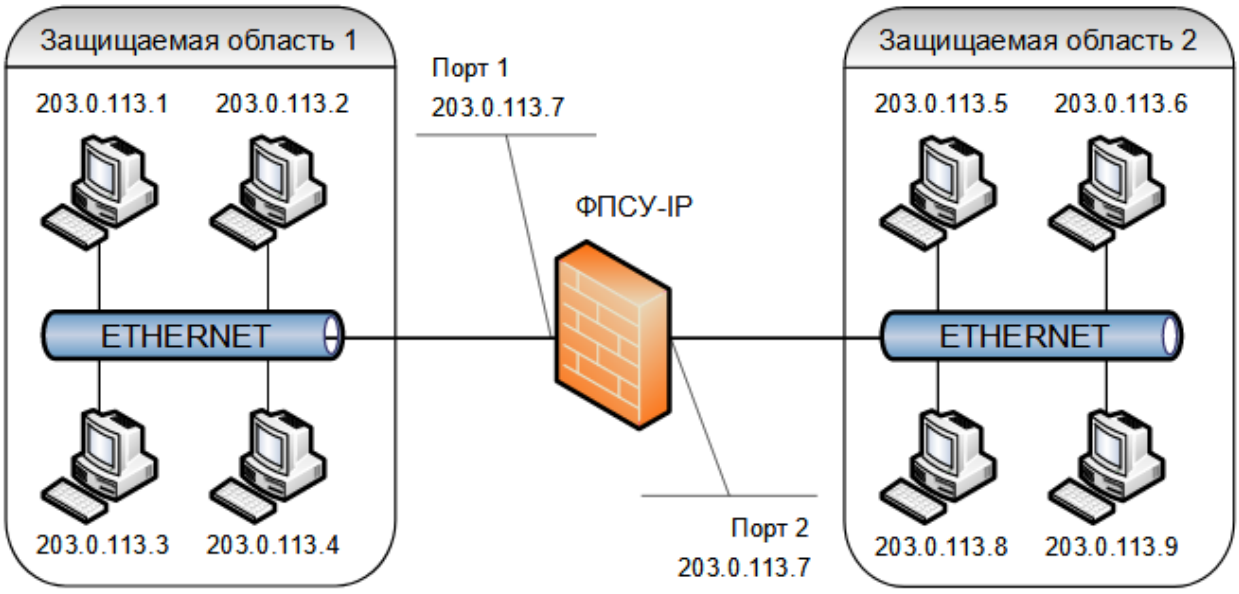

Рисунок 445 - Разбиение сети на фрагменты

С точки зрения конфигурирования ФПСУ-IP, для работы в условиях такой топологии

и удовлетворения наложенных требований принципиальным является следующее:

- со стороны портов 1 и 2 ФПСУ-IP существует одна и та же IP-подсеть, маршрутизаторы и другие ФПСУ-IP отсутствуют;
- обмен хостов через комплекс может производиться только в режиме ретрансляции, сжатие и криптозащита не применимы;
- работа с ключевыми данными при такой топологии не производится;
- абоненту с IP-адресом 203.0.113.1 должен быть запрещен обмен пакетами с абонентами со стороны порта 2;
- для обеспечения поиска и подключения сетевых дисков необходимо разрешить передачу через ФПСУ-IP широковещательных пакетов.

Конфигурация ФПСУ-IP должна содержать следующие установки:

Порт 1:

Номер 1;
Адрес 203.0.113.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть; 203.0.113.0; 255.255.255.0 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 203.0.113.1;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - выключен;
флаг "Работа разрешена" выключен.

Порт 2:

Номер 2;
Адрес 203.0.113.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть 203.0.113.0; 255.255.255.0 (24 разряда);
режим работы ретрансляция;
флаг "Только Broadcast" включен;

```
флаг "Работа разрешена" включен.
Хост; 203.0.113.5;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 203.0.113.6;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 203.0.113.8;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 203.0.113.9;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
```

Исходя из принципов конфигурирования ФПСУ-IP, со стороны одного из портов (в текущем примере - с порта 1) описана вся подсеть через хост вида «подсеть» с указанием адреса и маски сети (это сделано для простоты конфигурирования, чтобы не указывать индивидуальные адреса всех входящих в подсеть со стороны данного порта хостов), а со стороны противоположного порта - указаны индивидуальные адреса хостов, физически присутствующих с этой стороны, для регламентирования передачи индивидуальных пакетов и один повторный описатель типа «Подсеть» для регламентации широковещательных передач.

Для абонента 203.0.113.1 запрещение работы с абонентами области 2 осуществляется через выключение флага «Работа разрешена».

17. 4. Использование ФПСУ-IP для создания VPN-туннелей

Рассмотрим ситуацию, когда сеть организации представляет из себя отдельные локальные IP-подсети, разделенные территориально и связанные через участки WAN-сети

общего пользования. В таком случае, для обеспечения защищенного взаимодействия локальных подсетей, необходимо на выходе каждой из них установить ФПСУ-IP (со стороны внутреннего порта пограничного маршрутизатора) и организовать между ФПСУ-IP VPN-туннели через WAN-сеть общего доступа, по которым данные абонентов будут передаваться с использованием всех механизмов защиты, включая аутентификацию и, возможно, сжатие.

Предположим, что организация использует следующие IP-адреса:

- защищаемая область A - 192.168.1.0, маска 255.255.255.0 (24 бита);
- защищаемая область B - 192.168.2.0, маска 255.255.255.0 (24 бита);
- защищаемая область C - 192.168.3.0, маска 255.255.255.0 (24 бита);
- внутренний порт маршрутизатора A -192.168.1.1;
- внутренний порт маршрутизатора B -192.168.2.1;
- внутренний порт маршрутизатора C -192.168.3.1.

Для ФПСУ-IP в каждой подсети будут выделены адреса .50.

На работу сети наложены следующие ограничения:

- хосты из всех защищаемых областей должны иметь круглосуточный доступ друг к другу;
- управление пограничными маршрутизаторами (A, B, C) должно осуществляться только из защищаемой области C.

После установки ФПСУ-IP сеть организации имеет вид, представленный на рисунке ниже.

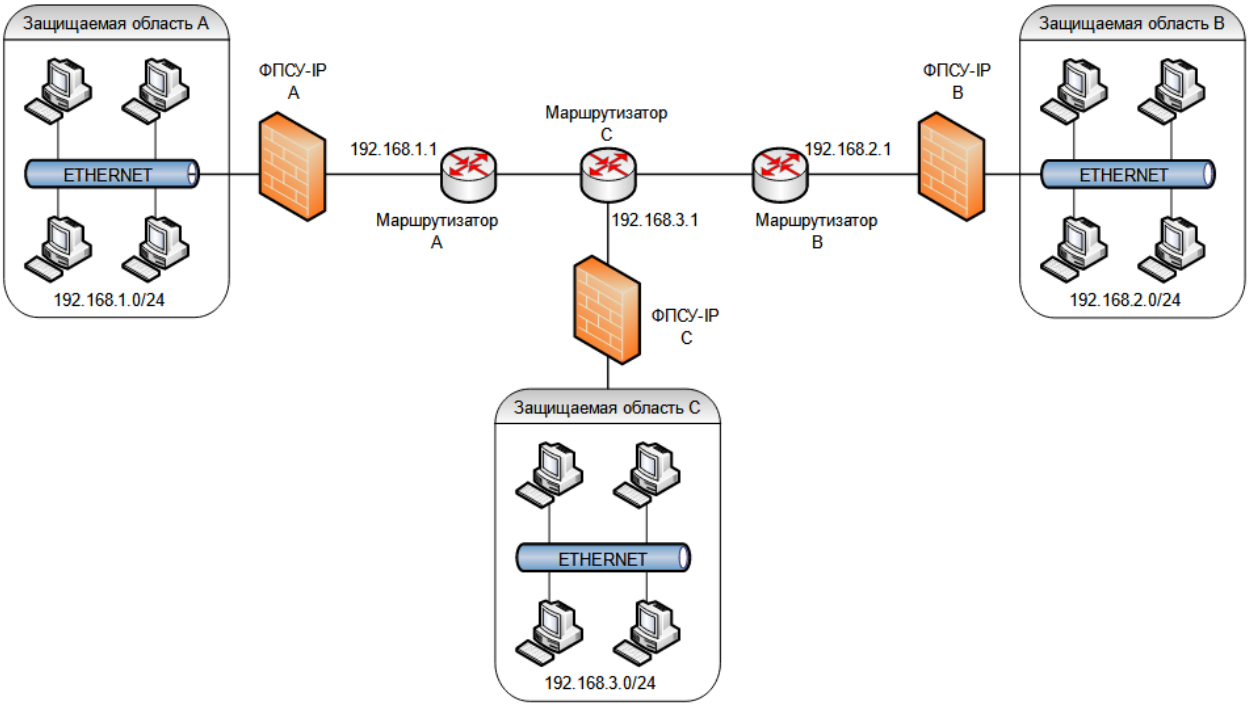

Рисунок 446 - Схема локальной сети с применением ФПСУ-IP

С точки зрения конфигурирования ФПСУ-IP A, B и C для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны внутреннего порта каждого ФПСУ-IP (например, порта 1) существует одна соответствующая IP-подсеть, а со стороны порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы и ФПСУ-IP отсутствуют;
- со стороны порта 2 существуют две IP-подсети, а со стороны порта 1 хостов, принадлежащих этим подсетям, нет; доступ к ним будет осуществляться через соответствующий удаленный ФПСУ-IP;
- обмен между защищаемыми областями должен производиться только внутри организованных ФПСУ-IP VPN-туннелей;
- на каждом ФПСУ-IP должны быть установлены ранее выработанные криптографические ключи парно-выборочной связи. Причем на ФПСУ-IP A указан используемый номер ключа 1, на ФПСУ-IP B - номер 2 и на ФПСУ-IP C - номер 3;
- со стороны внешнего порта ФПСУ-IP установлены пограничные маршрутизаторы, управление которыми должно осуществляться только из защищаемой области C, причем каналы управления маршрутизаторами за пределами их внешних портов должны быть защищены ФПСУ-IP.

В данном случае возможны два различных варианта конфигурации ФПСУ-IP,

которые описаны ниже.

17. 4. 1. Использование раздельных VPN-туннелей

В данном варианте конфигурации на каждом ФПСУ-IP будет создаваться по два VPN-туннеля.

Всего будет создано три VPN-туннеля. При этом для обмена данными защищаемые области будут использовать следующие туннели:

- VPN-1 - обмен области A с областью C;
- VPN-2 - обмен области B с областью C;
- VPN-3 - обмен области A с областью B.

На рисунке ниже показаны организованные VPN-туннели.

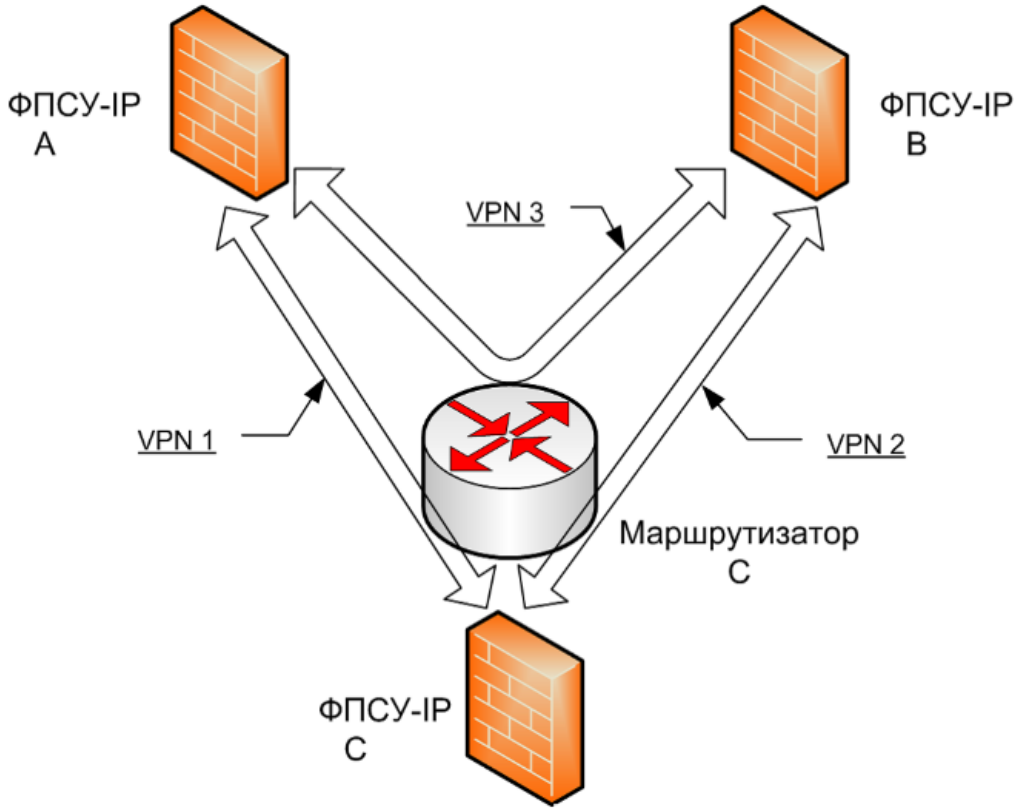

Рисунок 447 - Схема подключения с раздельными туннелями

Как видно из схемы, туннель 3 будет проходить через маршрутизатор C, минуя ФПСУ-IP C, т.е. маршрутизатор C будет осуществлять переброску (маршрутизацию) пакетов с одного из своих интерфейсов на другой для доставки их ФПСУ-IP A или ФПСУ-IP B.

Конфигурация ФПСУ-IP должна содержать следующие установки:

Для ФПСУ-IP А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 в настройках ФПСУ-IP А указаны как используемые.

Порт 1:

Номер 1;
Адрес 192.168.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены.
Абоненты:
Подсеть; 192.168.1.0; 255.255.255.0 (24 разряда),
режим работы - ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ
192.168.2.50, ключевые данные - 2.1; смена через 30 сек,
сжатие и криптозащита - "*желательно*" или "*обязательно*",
через маршрутизатор 192.168.1.1;
192.168.3.50, ключевые данные - 3.1; смена через 30 сек,
сжатие и криптозащита - "*желательно*" или "*обязательно*",
через маршрутизатор 192.168.1.1;
Маршрутизаторы
192.168.1.1;
протоколы маршрутизации - на усмотрение администратора,
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда),
через ФПСУ 192.168.2.50,
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда),

через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Для ФПСУ-IP В:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 в настройках ФПСУ-IP В указаны как используемые.

Порт 1:
Номер 1;
Адрес 192.168.2.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда), ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Порт 2:
Номер 2;
Адрес 192.168.2.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.1.50, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.2.1;
192.168.3.50, ключевые данные - 3.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.2.1;
Маршрутизаторы:
192.168.2.1, протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;

флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть; 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Для ФПСУ-IP С:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3. Ключи номер 3 в настройках ФПСУ-IP С указаны как используемые.

Порт 1:
Номер 1;
Адрес 192.168.3.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть; 192.168.3.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Порт 2:
Номер 2;
Адрес 192.168.3.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.1.50, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 192.168.3.1
192.168.2.50, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 192.168.3.1
Маршрутизаторы:
192.168.3.1, протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:

Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Только на ФПСУ-IP С для подсети 192.168.3.0 должно быть разрешено управление маршрутизаторами 192.168.1.1, 192.168.2.1, 192.168.3.1 (см. пункт «DHCP-Relay»).

Необходимо также перенастроить пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

17. 4. 2. Использование совмещенных VPN-туннелей

ФПСУ-IP С является центральным сервером VPN-сети, организованной по топологии "звезда". В данном варианте конфигурации будут созданы всего два VPN-туннеля, показанные на рисунке ниже:

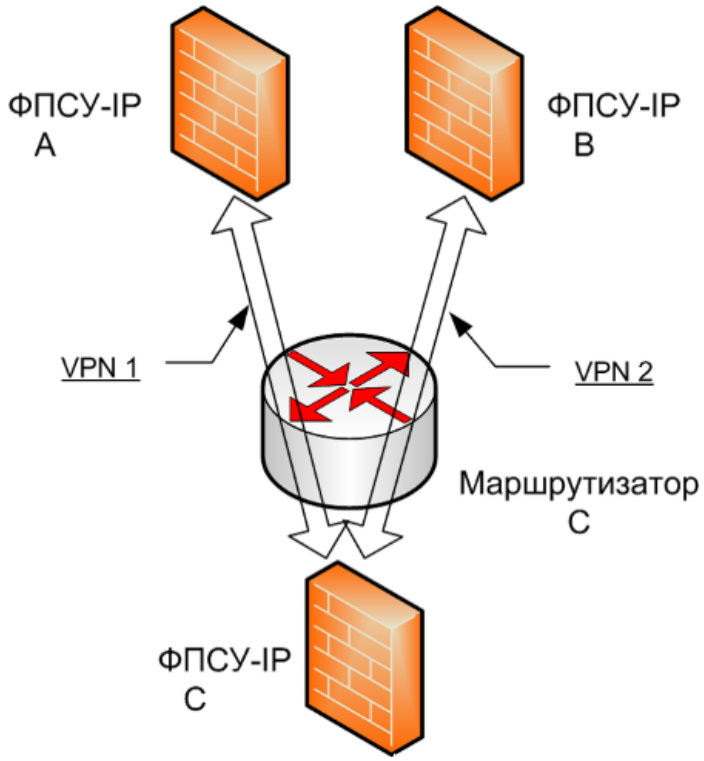

Рисунок 448 - Схема подключения с последовательными туннелями

При этом для обмена данными защищаемыми областями будут использоваться следующие туннели:

- VPN-1 - обмен области A с областью C;
- VPN-2 - обмен области B с областью C;
- VPN-1 и VPN-2 - обмен области A с областью B.

Конфигурация комплексов должна содержать следующие установки:

Для ФПСУ-IP A:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 в настройках ФПСУ-IP A указаны как используемые.

Порт 1:

Номер 1;
Адрес 192.168.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.3.50, ключевые данные - 3.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.1.1;
Маршрутизаторы
192.168.1.1, протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Для ФПСУ-IP B:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 в настройках ФПСУ-IP B указаны как используемые.

Порт 1:

Номер 1;
Адрес 192.168.2.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.2.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.3.50, ключевые данные - 3.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.2.1
Маршрутизаторы:
192.168.2.1, протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Для ФПСУ-IP С:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3. Ключи номер 3 в настройках ФПСУ-IP С указаны как используемые.

Порт 1:

Номер 1;
Адрес 192.168.3.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.3.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.1.50, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.3.1
192.168.2.50, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.3.1
Маршрутизаторы:
192.168.3.1,
протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Только на ФПСУ-IP С для подсети 192.168.3.0 должно быть разрешено управление маршрутизаторами 192.168.1.1, 192.168.2.1, 192.168.3.1 (см. раздел «DHCP-Relay»).

Необходимо также переконфигурировать пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

17. 5. Использование ФПСУ в режиме моста (L2 шифрование)

Предположим, что IP-сеть организации до установки ФПСУ-IP представляла одну

подсеть с IP-адресом 192.168.1.0 и маской 255.255.255.0 (24 разряда), требуется передавать пакеты внутри локальной сети, разделенной географически. Для того, чтобы организовать такую «прозрачную» защищенную передачу данных, достаточно на внешних портах ФПСУ А и ФПСУ В создать описатель партнера по шифрованию и включить режим моста для туннеля ФПСУ А ↔ ФПСУ В.

При этом на внутренних портах ФПСУ А и ФПСУ В не должно быть описано абонентов (хостов, подсетей, записи «любой хост») - пакеты от явно указанных на портах ФПСУ-IP абонентов не передаются в туннель типа «мост» (подробнее см. пункт «Режим «Мост» между ФПСУ-IP (L2-шифрование)»):

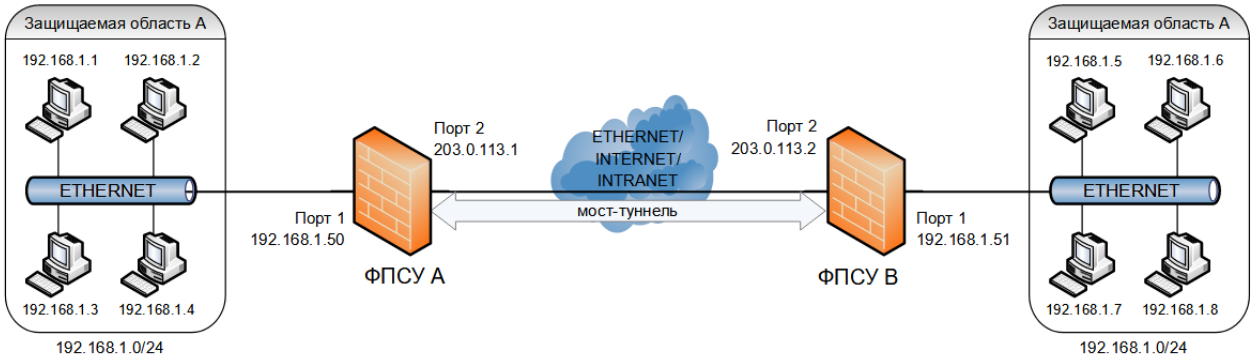

Рисунок 449 - L2-туннель типа "мост"

Используются следующие IP-адреса:

- защищаемая область А - 192.168.1.0, маска 255.255.255.0 (24 бита);
- внутренний порт ФПСУ А -192.168.1.50;
- внешний порт ФПСУ А -203.0.113.1;
- внутренний порт ФПСУ В -192.168.1.51;
- внешний порт ФПСУ В -203.0.113.2.

С точки зрения конфигурирования ФПСУ-IP А для работы в условиях такой топологии принципиальным является следующее:

- со стороны внутреннего порта ФПСУ-IP А (порта 1 со стороны области А) существует одна IP- подсеть,
- со стороны внешнего порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы отсутствуют; ФПСУ-IP В описан в режиме моста;
- на ФПСУ-IP А должны быть установлены, и указаны как используемые, ранее выработанные ЦВК криптографические ключи номер 1.

С точки зрения конфигурирования ФПСУ-IP В для работы в условиях такой топологии принципиальным является следующее:

- со стороны внутреннего порта ФПСУ-IP В (порта 1 со стороны области В)

существует одна (та же) IP- подсеть,

- со стороны внешнего порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы отсутствуют; ФПСУ-IP А описан в режиме моста;
- на ФПСУ-IP В должны быть установлены, и указаны как используемые, ранее выработанные ЦВК криптографические ключи номер 2;

Конфигурация ФПСУ-IP должна содержать следующие установки:

Для ФПСУ-IP А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 указаны как используемые.

Порт 1:
Номер 1,
Адрес 192.168.1.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:не определены;

Порт 2:
Номер 2,
Адрес 203.0.113.1,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
203.0.113.2, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
мост - включен;
Маршрутизаторы:не определены;
Абоненты:не определены.

Для ФПСУ-IP В:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 указаны как используемые.

Порт 1:
Номер 1,
Адрес 192.168.1.51,

Маска 255.255.255.0 (24 разряда);
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:не определены;

Порт 2:
Номер 2,
Адрес 203.0.113.2,
Маска 255.255.255.0 (24 разряда),
ФПСУ:
203.0.113.1, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
мост - включен;
Маршрутизаторы:не определены;
Абоненты:не определены.

17. 6. Каскадная схема установки ФПСУ-IP в локальной сети

В документе «Описание применения» ПАК ФПСУ-IP приведена каскадная схема установки двух ФПСУ-IP в одной защищаемой области, при которой хосты оконечной области (защищенной двумя ФПСУ-IP) будут обмениваться пакетами с хостами сетевых фрагментов, находящихся со стороны внешнего порта внешнего ФПСУ-IP, через VPN-туннель, создаваемый в самой защищаемой области, а хосты защищаемой области - через внешний ФПСУ-IP защищаемой области. В данном разделе будут рассмотрены особенности конфигурирования работы комплексов в условиях такой сетевой топологии.

Итак, предположим, что сеть организации представляет из себя два территориально разделенных фрагмента, для защиты которых будут применены ФПСУ-IP, причем в одной из подсетей существует особо ответственная IP-сеть, для которой необходимо обеспечить режим усиленной защиты. После установки комплексов сеть организации примет вид, отображенный на рисунке ниже.

Используются следующие IP-адреса:
- защищаемая область A - 192.168.1.0, маска 255.255.255.0 (24 бита);
- защищаемая область B - 192.168.2.0, маска 255.255.255.0 (24 бита);
- защищаемая область C - 192.168.3.0, маска 255.255.255.0 (24 бита);
- внутренний порт маршрутизатора A -192.168.2.1;
- внутренний порт маршрутизатора B -192.168.3.51.

На работу сети наложены следующие ограничения:
- хосты области A должны обмениваться пакетами только с хостами области C и не иметь доступа к другим абонентам;

- управление пограничными маршрутизаторами (A и B) должно осуществляться из защищаемой области B;
- хосты области B имеют доступ в мировую сеть Internet/Intranet и не имеют доступа к другим абонентам.

С точки зрения конфигурирования ФПСУ-IP A для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны внутреннего порта ФПСУ-IP (порта 1 со стороны области A) существует одна IP- подсеть, а со стороны порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы и ФПСУ-IP отсутствуют;
- со стороны порта 2 существуют: IP-подсеть B, доступ к которой необходимо запретить; IP-подсеть C, доступ в которую будет производиться через ФПСУ-IP B, а также мировая сеть, доступ в которую предоставлен не будет; существует также маршрутизатор A, находящийся с внешнего порта ФПСУ-IP B (поскольку он может являться маршрутизатором по умолчанию для хостов области A и является пограничным маршрутизатором);
- обмен между защищаемыми областями A и C должен производиться только внутри двух организованных ФПСУ-IP VPN-туннелей с проведением двусторонней аутентификации и использованием дополнительных процедур сжатия и криптозащиты;
- на ФПСУ-IP A должны быть установлены, и указаны как используемые, ранее выработанные ЦВК криптографические ключи номер 1;
- со стороны внешнего порта ФПСУ-IP (порта 2) присутствует пограничный маршрутизатор A, управление которым из защищаемой области A не должно осуществляться.

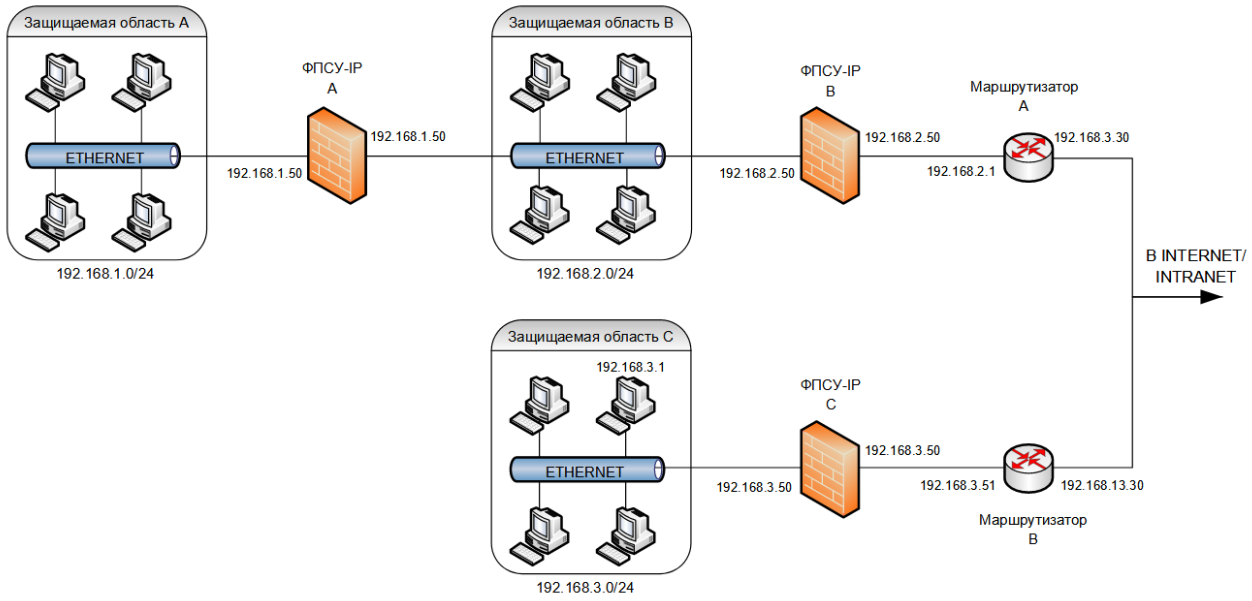

Рисунок 450 - Каскадное подключение ФПСУ-IP

С точки зрения конфигурирования ФПСУ-IP B для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны внутреннего порта (порта 1 со стороны области B) существуют две IP-подсети, доступ в область A должен быть запрещен абонентам B, к абонентам области B доступ будет производиться в режиме ретрансляции; маршрутизаторы отсутствуют; для организации туннеля через область B будет использован ФПСУ-IP A;
- со стороны порта 2 существуют IP-подсеть C, доступ к которой абонентам B должен быть запрещен, а также абоненты общедоступной сети передачи данных; доступ к общедоступной сети передачи данных производится через маршрутизатор A; ФПСУ-IP C существует и доступен через маршрутизатор A;
- на ФПСУ-IP B должны быть установлены, и указаны как используемые, ранее выработанные ЦВК криптографические ключи номер 2;
- со стороны внешнего порта ФПСУ-IP (порта 2) существует пограничный маршрутизатор A, управление которым должно осуществляться только из защищаемой области B, причем каналы управления маршрутизаторами A и B за пределами их внешних портов должны быть защищены ФПСУ-IP B.

С точки зрения конфигурирования ФПСУ-IP C для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны внутреннего порта (порта 1 со стороны области C) существует IP-

подсеть С, а со стороны порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы и ФПСУ-IP отсутствуют;

- со стороны порта 2 (внешнего) существуют: IP-подсеть В, доступ к которой необходимо запретить; IP-подсеть А, доступ в которую будет производиться через ФПСУ-IP В, а также общедоступная сеть, доступ в которую предоставлен не будет; маршрутизатор В является пограничным;
- обмен между защищаемыми областями А и С должен производиться только внутри организованных ФПСУ-IP VPN-туннелей;
- на ФПСУ-IP С должны быть установлены и указаны как используемые ранее выработанные ключи номер 3;
- со стороны внешнего порта ФПСУ-IP С существует пограничный маршрутизатор В, управление которым должно осуществляться только из защищаемой области В, причем канал управления маршрутизатором за пределами его внешнего порта должен быть защищен ФПСУ-IP В.

Конфигурация ФПСУ-IP должна содержать следующие установки:

Для ФПСУ-IP А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 в настройках ФПСУ-IP А указаны как используемые.

Порт 1:

Номер 1,
Адрес 192.168.1.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
A_to_C

Порт 2:

Номер 2,
Адрес 192.168.1.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.2.50, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";

Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.

Правила МЭ:
1 A_to_C
Общие
Действие : Accept
Время работы : Любое
Лог : Не вести лог
Активно : Да
Источник
Сеть : 192.168.001.000 192.168.000.000/24
Назначение
Сеть : 192.168.003.000 192.168.000.000/24
Служба : Любая
2 Block other traffic
Общие
Действие : Drop
Время работы : Любое
Лог : Не вести лог
Активно : Да
Источник : Любой
Назначение : Любой
Служба : Любая

Для ФПСУ-IP B:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 в настройках ФПСУ-IP B указаны как используемые.

Создано и активировано разрешающее правило трафика, в которое включены подсети 192.168.1.0 и 192.168.3.0. Подсети 192.168.2.0 со стороны порта 1 разрешено управление маршрутизатором 192.168.2.1.

Порт 1:
Номер 1,
Адрес 192.168.2.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.1.50, ключевые данные - 1.1; смена через 30 сек;

сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
to routers
Internet_B

Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2,
Адрес 192.168.2.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ:
192.168.3.50, ключевые данные - 3.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 192.168.2.1.
Маршрутизаторы:
192.168.2.1, протоколы маршрутизации - все выключены;
Абоненты:
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.
Любой хост;
флаг "Работа разрешена" включен;
через маршрутизатор 192.168.2.1;
Хост, 192.168.3.51; через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.

Правила МЭ:

1 to routers

Общие
Действие : Accept
Время работы : Любое

```
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Сеть            :   192.168.002.000 192.168.000.000/24
      Назначение
        Хост            :   192.168.002.001 192.168.002.001/32
        Хост            :   192.168.003.051 192.168.003.051/32
      Служба          : Любая
2 Internet_B
      Общие
        Действие        : Accept
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Сеть            :   192.168.002.000 192.168.000.000/24
      Назначение      : Любой
      Служба          : Любая

3 Block other traffic
      Общие
        Действие        : Drop
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник        : Любой
      Назначение      : Любой
      Служба          : Любая
```

Для ФПСУ-IP С:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3. Ключи номер 3 указаны как используемые.

Создано и активировано разрешающее правило трафика, в которое включены подсети 192.168.1.0 и 192.168.3.0. Подсети 192.168.2.0 со стороны порта 2 разрешено управление маршрутизатором 192.168.3.1.

Порт 1:
Номер 1,
Адрес 192.168.3.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда); ретрансляция;

режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
C_to_A

Порт 2:
Номер 2,
Адрес 192.168.3.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.2.50, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 192.168.3.51.
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.

Правила МЭ:
1 C_to_A
Общие
Действие : Accept
Время работы : Любое
Лог : Не вести лог
Активно : Да
Источник
Сеть : 192.168.003.000 192.168.000.000/24
Назначение
Сеть : 192.168.001.000 192.168.000.000/24
Служба : Любая
2 Block other traffic
Общие
Действие : Drop
Время работы : Любое
Лог : Не вести лог
Активно : Да

```
Источник          : Любой
Назначение        : Любой
Служба            : Любая
```

В конфигурациях ФПСУ-IP приведены только необходимые для работоспособности схемы настройки, дополнительно для абонентов должен быть выключен флаг «Только Broadcast», флаг «Отвечать на Ping» устанавливается на усмотрение администратора.

Необходимо также переконфигурировать пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

Поскольку конфигурирование нескольких совместно работающих ФПСУ-IP для разветвленной сетевой топологии может вызвать затруднение у неопытного администратора, рекомендуется после заполнения конфигурационных таблиц произвести аналитическую проверку произведенных установок на предмет соответствия заданным требованиям (ограничениям).

В соответствии с установленной конфигурацией через ФПСУ-IP A:

- абоненты области A не получат доступа к области B, маршрутизатору A и общедоступной сети передачи данных, поскольку все они не описаны со стороны порта 2; кроме того, доступу к ним препятствует также указанный в описателе для абонентов A режим работы с абонентом противоположного порта (только через ФПСУ);
- отсутствие доступа абонентов области A к маршрутизатору A обеспечивается тем, что он не описан со стороны порта 2;
- Доступ от абонентов области A к абонентам области C осуществляется через ФПСУ-IP B, задан правилом трафика, разрешающим доступ в область C.

В соответствии с установленной конфигурацией через ФПСУ-IP B:

- абоненты области B не имеют доступа к области A, поскольку в описателе A на порту 1 нет разрешения работы с абонентами данного порта; кроме того, доступу к A также препятствует то, что для области B не задано правило трафика, разрешающее доступ в область A;
- абонентам области B разрешено управление маршрутизатором A и B, а также доступ в общедоступную сеть передачи данных правилами МЭ;
- доступ к маршрутизатору B от абонентов области B обеспечивается тем, что он указан как абонент на порту 2 и будет осуществляться только через ФПСУ-IP B;
- к абонентам области C (исключая маршрутизатор B, описанный отдельно) абоненты области B доступа не получат, поскольку для области B не задано правило трафика, разрешающее доступ в область C.

В соответствии с установленной конфигурацией через ФПСУ-IP С:

- отсутствие доступа абонентов области С к маршрутизаторам А и в область В обеспечивается тем, что маршрутизатор А не описан как абонент со стороны внешнего порта 2, область С не входит в правило трафика, разрешающее доступ в область В;
- доступ абонентов области С к мировой сети невозможен - они не указаны на порту 2; кроме того, у абонентов С указан режим работы с абонентами противоположного порта только через ФПСУ-IP;
- доступ от абонентов области С к маршрутизатору В невозможен, поскольку, во-первых, управление маршрутизатором не разрешено, во-вторых, он не описан как абонент, в-третьих, у абонентов С указан режим работы с абонентами противоположного порта только через ФПСУ-IP.

17. 7. Использование ФПСУ-IP для контроля доступа в интернет с NAT

Рассмотрим ситуацию, когда сеть организации использует внутренние локальные адреса, доступ ко внешним ресурсам в интернет осуществляется с помощью технологии NAT. ФПСУ-IP выполняет процесс NAT, преобразуя серый IP-адрес в белый IP-адрес из диапазона адресов NAT.

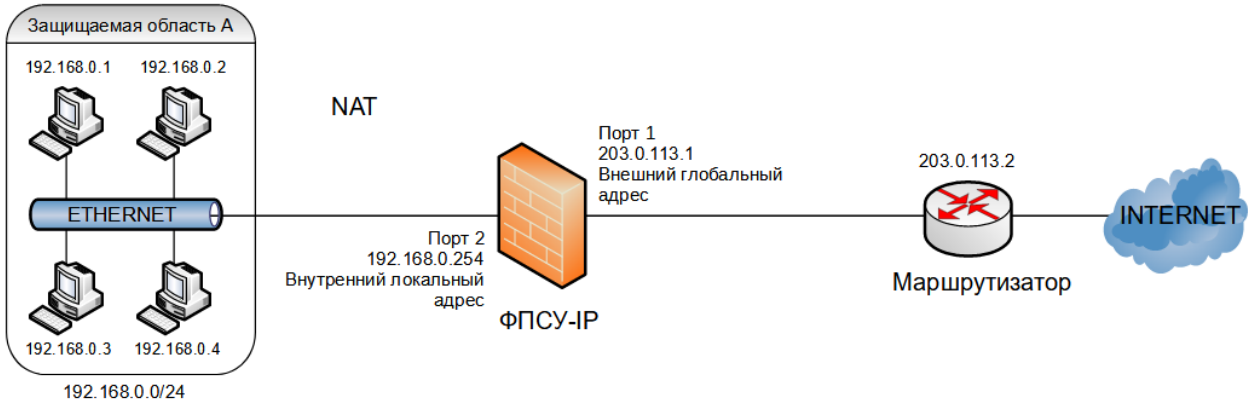

Рисунок 451 - Применение ФПСУ-IP для доступа в интернет с NAT

С точки зрения конфигурирования ФПСУ-IP для работы в условиях такой топологии принципиальным является следующее:

- со стороны внутреннего порта комплекса (порта 2) существует одна IP подсеть, маршрутизаторы отсутствуют;
- со стороны внешнего порта (порта 1) установлен пограничный маршрутизатор, через который осуществляется доступ в интернет;
- межсетевым экраном разрешены исходящие соединения всем хостам IP подсети, кроме хоста 192.168.0.1, в интернет, но запрещены любые входящие соединения из

интернет.

Конфигурация ФПСУ должна содержать следующие установки:

Порт 1:

Номер 1,
Адрес 203.000.113.001,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы:203.000.113.002,
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.

Абоненты:
Хост; Адрес 203.000.113.002; Маска 255.255.255.000 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Хост; Адрес Произвольный (из незаданных)
режим работы ретрансляция;
Доступен через маршрутизатор 203.000.113.002
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2,
Адрес 192.168.000.254,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.000.000; Маска 255.255.255.000;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Правила межсетевого экрана на ФПСУ (подробности см. ниже)
DNS
block 192.168.0.1
Internet_All

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана: (

1. Правило, разрешающее исходящие соединения с порта 2 для службы DNS (DNS-запросы по протоколу TCP/UDP с портом назначения 53);
2. Правило, запрещающее любые межсетевые исходящие соединения абонента 192.168.0.1 (в том числе будет запрещен интернет);
3. Правило, разрешающее исходящие соединения IP подсети через NAT в интернет;
4. Правило "Block other traffic", запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

Правила МЭ:
1 DNS

```
      Общие
        Действие         : Accept
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник
        Интерфейс        :   port2 iface2 192.168.000.254
      Назначение       : Любой
      Служба           : DNS
```

2 block 192.168.0.1

```
      Общие
        Действие         : Drop
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник
        Адрес            :   192.168.000.001/32 192.168.000.001
      Назначение         : Любой
      Служба           : Любая
```

3 Internet_All

```
      Общие
```

```
    Действие        : Accept
    Nat             : port1 iface1 203.000.113.001
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник
    Сеть            :   192.168.000.000 192.168.000.000/24
  Назначение      : Любой
  Служба          : Любая

4 Block other traffic
  Общие
    Действие        : Drop
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник        : Любой
  Назначение      : Любой
  Служба          : Любая

Службы:
  DNS
    Общие
      Протокол        : TCP/UDP
      Порт источника  : Любой
      Порт назначения : 53 (Domain Name Server)
```

17. 8. Использование ФПСУ-IP для контроля доступа ФПСУ-IP/Клиентов

Рассмотрим ситуацию, когда в сеть организации разрешен доступ ФПСУ-IP/Клиентам, которые подключаются удаленно через Интернет. ФПСУ-IP/Клиентам должны быть доступны внутренние ресурсы, но при этом эти ресурсы должны быть закрытыми для общего доступа через Интернет.

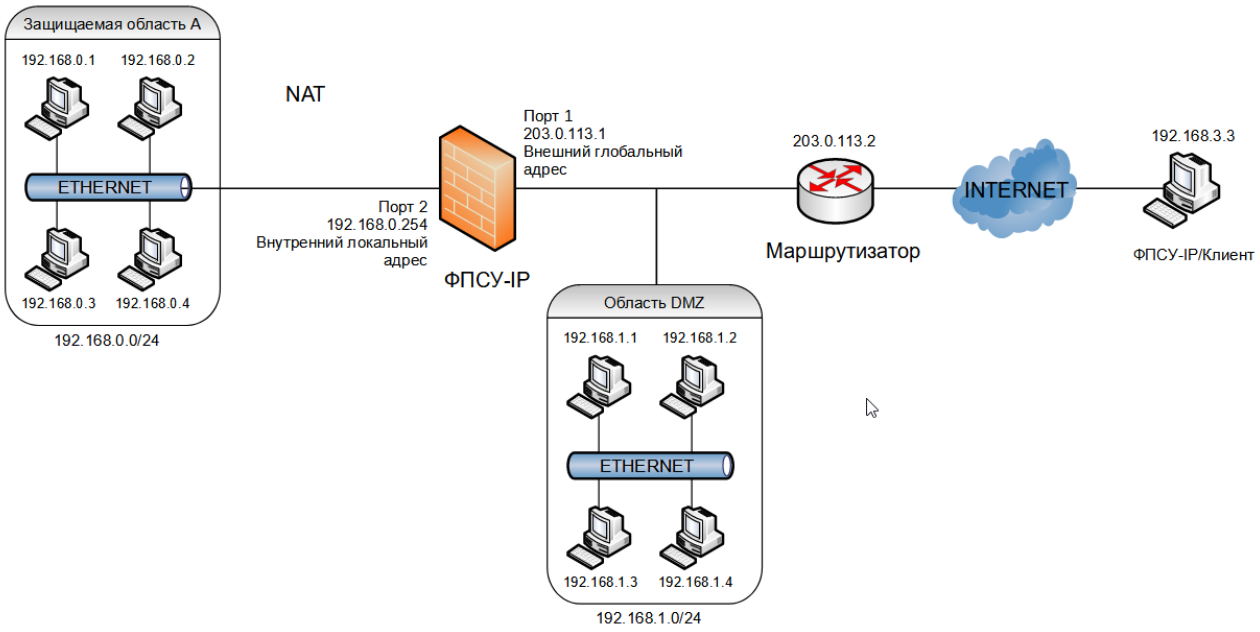

Рисунок 452 - Схема подключения ФПСУ-IP/Клиентов

С точки зрения конфигурирования ФПСУ-IP для работы в условиях такой топологии принципиальным является следующее:

- со стороны внутреннего порта комплекса (порта 2) существует IP подсеть 2, маршрутизаторы отсутствуют;
- со стороны внешнего порта (порта 1) существует содержащий общедоступные сервисы сегмент сети - область DMZ, в которой существует локальная IP подсеть 1, и установлен пограничный маршрутизатор, через который осуществляется доступ в интернет и подключаются Клиенты ФПСУ-IP;
- Клиенты ФПСУ-IP объединены в IP подсеть 3;
- Клиентам ФПСУ-IP разрешен доступ в подсети 1 и 2.

Конфигурация ФПСУ-IP должна содержать следующие установки:

Порт 1:
Номер 1,
Адрес 203.0.113.1,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы:203.0.113.2,
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.
Правила межсетевого экрана для этого маршрутизатора
Client_local

Абоненты:
Хост; Адрес 203.0.113.2; Маска 255.255.255.0 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
Client_local

Подсеть; Адрес 192.168.001.000; Маска 255.255.255.000 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" выключен.

Хост; Адрес Произвольный (из незаданных)
режим работы ретрансляция;
Доступен через маршрутизаторы 203.0.113.2
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Работа разрешена" включен.

Порт 2:
Номер 2,
Адрес 192.168.0.254,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.0.0; Маска 255.255.255.0;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
DNS

```
Client_local
Internet_All
```

ФПСУ-IP/Клиентами при работе с ФПСУ-IP используются два механизма NAT:

- для доступа во внутреннюю сеть, статический NAT (настраивается в описателях Клиентов);
- для работы с интернетом, используя ФПСУ-IP как посредника, динамический NAT (настраивается в правилах МЭ).

Описатель Клиентов:

К-сеть Crypt; **Группа** 1 Для программных устройств
Обслуживание Разрешено
Диапазон номеров 1 .. 25
Описание Активно
Контроль соединения 10 мин

Параметры для портов ФПСУ-IP

Порт 1		Порт 2
NAT при соединении		
192.168.003.001	Начальный адрес	192.168.003.001
255.255.255.000	Маска подсети	255.255.255.000

Правила межсетевого экрана для клиентов этого диапазона
Client_local

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее исходящие соединения с порта 2;
2. Правило, разрешающее исходящие соединения клиентов, программных (мобильных) клиентов и сервиса example.com в подсети 1 и 2 и порты ФПСУ-IP;
3. Правило, разрешающее исходящие соединения подсетей 1 и 2 с NAT в интернет
4. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

Правила МЭ:

1 DNS

```
      Общие
        Действие        : Accept
        Время работы    : Любое
```

```
    Лог             : Не вести лог
    Активно         : Да
  Источник
    Интерфейс       :   port2 iface2 192.168.000.254
  Назначение      : Любой
  Служба          : DNS
```

2 Client_local

```
  Общие
    Действие        : Accept
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник
    Клиент          :     СисCrypt Грп1
    Клиент          :   Мобильные клиенты  СисCrypt Грп1
    Клиент          :   example.com  СисCrypt Грп1
  Назначение
    Сеть            :   192.168.000.000 192.168.000.000/24
    Сеть            :   192.168.001.000 192.168.001.000/24
    Интерфейс       :   port1 iface1 203.0.113.001
    Интерфейс       :   port2 iface2 192.168.000.254
  Служба          : Любая
```

3 Internet_All

```
  Общие
    Действие        : Accept
    Nat             : port1 iface1 203.0.113.1
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник
    Сеть            :   192.168.000.000 192.168.000.000/24
    Сеть            :   192.168.001.000 192.168.001.000/24
  Назначение      : Любой
  Служба          : Любая
```

4 Block other traffic

```
  Общие
    Действие        : Drop
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник        : Любой
```

```
    Назначение      : Любой
    Служба          : Любая

Службы:
  DNS
    Общие
      Протокол        : TCP/UDP
      Порт источника  : Любой
      Порт назначения : 53 (Domain Name Server)
```

17. 9. Использование ФПСУ-IP для объединения офисов с одинаковой внутренней адресацией

Предположим, что есть две территориально разделенные сети с одинаковой адресацией, для защиты которых применяются ФПСУ-IP, необходимо обеспечить доступ хостов одной сети в другую через ФПСУ-туннель. Например, если в одной из сетей расположен сервер, защищенный доступ к которому предоставляется хостам из другой сети.

Такая организация защищаемых подсетей приведет к следующей логике конфигурирования:

- обмен между защищаемыми областями должен производиться только внутри организованного ФПСУ-IP VPN-туннеля;
- на каждом ФПСУ-IP должны быть установлены ранее выработанные криптографические ключи парно-выборочной связи. Причем на ФПСУ-IP A указан используемый номер ключа 1, на ФПСУ-IP B - номер 2;

ФПСУ-IP A

- со стороны внутреннего порта 1 существует одна подсеть; маршрутизаторы и другие ФПСУ-IP, через которые абоненты будут доступны с порта 1, отсутствуют;
- со стороны порта 1 описана подсеть, обмен хостов которой через комплекс производится в режиме ретрансляции;
- со стороны порта 1 описан абонент 192.168.0.1, обмен данными с которым определяется правилом МЭ, в правиле определена трансляция сетевых адресов и задана переадресация порта;
- со стороны внешнего порта 2 определен ФПСУ-IP B и описан как абонент, обмен данными с которым определяется правилом МЭ, в правиле определена трансляция сетевых адресов и задана переадресация порта;

ФПСУ-IP B

- со стороны внутреннего порта 1 существует одна подсеть; маршрутизаторы и другие ФПСУ-IP, через которые абоненты будут доступны с порта 1, отсутствуют;

- со стороны порта 1 описана подсеть с той же адресацией, что и на ФПСУ-IP A, обмен хостов данной подсети через комплекс производится в режиме ретрансляции;
- со стороны внешнего порта 2 определен ФПСУ-IP A, обмен данными с которым определяется правилом МЭ, в правиле задана переадресация порта;
- со стороны порта 2 описан абонент 11.11.11.11, обмен данными с которым определяется правилом МЭ, в правиле задана переадресация порта;

Хост 192.168.0.1 защищаемой области A отправляет эхо-запрос (ping) на внутренний IP-адрес ФПСУ-IP A. Правилом МЭ данный запрос разрешен. На ФПСУ-IP A с помощью NAT IP-адрес отправителя 192.168.0.1 подменяется на 11.11.11.11, с помощью MAP IP-адрес получателя 192.168.0.241 подменяется на внешний IP-адрес ФПСУ-IP B 1.1.1.2. Запрос отправляется на ФПСУ-IP B. Правилом МЭ данный запрос разрешен. На ФПСУ-IP B с помощью MAP IP-адрес получателя 1.1.1.2 подменяется на 192.168.0.1. Запрос отправляется хосту 192.168.0.1 защищаемой области B. Ответ хоста 192.168.0.1 защищаемой области B проходит обратное преобразование при прохождении ФПСУ-IP B и ФПСУ-IP A. На ФПСУ-IP реализовано отслеживание инициатора запроса - возвратный трафик разрешен.

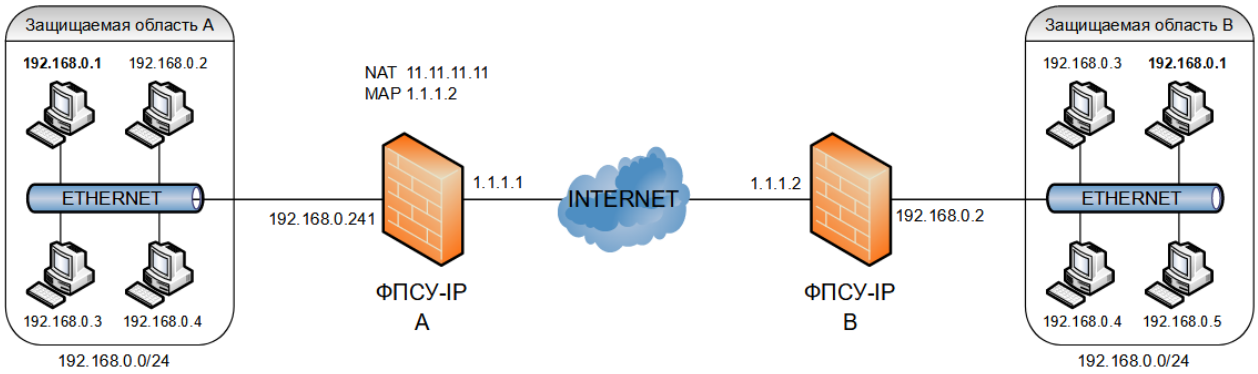

Рисунок 453 - Схема подключения ФПСУ-IP/Клиентов

ФПСУ-IP A

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 указаны на ФПСУ A как используемые.

Порт 1:
Номер 1,
Адрес 192.168.000.241,
Маска 255.255.255.000 (24 разряда),
VLAN Нет;
ФПСУ не определены,
Маршрутизаторы: не определены,
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.

Абоненты:
Подсеть; Адрес 192.000.000.000; Маска 255.000.000.000 (8 разряда);
режим работы ретрансляция;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен.

Хост; Адрес 192.168.000.001;
режим работы ретрансляция;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен;
Правила межсетевого экрана для этого абонента
ping over nat.

Порт 2:
Номер 2,
Адрес 001.001.001.001,
Маска 255.255.255.000 (24 разряда),
VLAN Нет;
Адрес 011.011.011.011,
Маска 255.255.255.000 (24 разряда),
VLAN 111;
ФПСУ:
001.001.001.002, ключевые данные - 1; смена через 120 сек;
сжатие и криптозащита - "запрещено" и "обязательно";
мост - выключен;
Маршрутизаторы:не определены,
протоколы маршрутизации выключены;

Абоненты:
Хост; Адрес 192.168.000.002;
режим работы Через ФПСУ 001.001.001.002;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен;

Правила межсетевого экрана для этого ФПСУ-IP
ping over nat.

Службы межсетевого экрана для этого ФПСУ-IP:
PING

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее исходящие соединения по протоколу ICMP хоста 192.168.0.1 на внутренний порт ФПСУ-IP A, IP-адрес источника и назначения преобразуются по заданным правилам NAT и MAP;
2. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

```
Правила МЭ:
1. ping over nat
      Общие
        Действие         : Accept
        Nat              : port2 iface2 vlan111 011.011.011.011
        Map              : 001.001.001.002 port -
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник
        Адрес            :   192.168.000.001/32 192.168.000.001
      Назначение
        Интерфейс        :   port1 iface1 192.168.000.241
      Служба
        PING

2. Block other traffic
      Общие
        Действие         : Drop
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник         : Любой
      Назначение       : Любой
      Служба           : Любая

Службы
1. PING
        Описание         : Internet Control Message Protocol
        Протокол         : ICMP
      Тип сообщения ICMP: Любой
```

ФПСУ B

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 указаны на ФПСУ В как используемые.

Порт 1:

Номер 1,
Адрес 192.168.000.002,
Маска 255.255.255.000 (24 разряда),
VLAN Нет;
ФПСУ не определены,
Маршрутизаторы:не определены,
протоколы маршрутизации выключены;

Абоненты:
Подсеть; Адрес 192.168.000.000; Маска 255.255.255.000 (24 разряда);
режим работы ретрансляция;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен.

Порт 2:

Номер 1,
Адрес 001.001.001.002,
Маска 255.255.255.000 (24 разряда),
VLAN Нет;
ФПСУ:
001.001.001.001, ключевые данные - 2.1; смена через 120 сек;
сжатие и криптозащита - "запрещено" и "обязательно";
мост - выключен;
Правила межсетевого экрана для этого ФПСУ-IP
map.

Маршрутизаторы:не определены,
протоколы маршрутизации выключены;

Абоненты:
Хост; Адрес 011.011.011.011;
режим работы Через ФПСУ 001.001.001.001;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен;

Правила межсетевого экрана для этого ФПСУ-IP
map

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее входящие соединения по протоколу ICMP с IP-адреса 11.11.11.11 на внешний порт ФПСУ-IP B, IP-адрес назначения подменяется по заданному правилу MAP;
2. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

```
Правила МЭ:
1. map
      Общие
        Действие         : Accept
        Map              : 192.168.000.001
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник
        Адрес            :   011.011.011.011/32 011.011.011.011
      Назначение
        Интерфейс        :   port2 iface2 001.001.001.002
      Служба
        PING

2. Block other traffic
      Общие
        Действие         : Drop
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник         : Любой
      Назначение       : Любой
      Служба           : Любая
```

В конфигурациях ФПСУ-IP приведены только необходимые для работоспособности схемы настройки, дополнительно для абонентов должен быть выключен флаг «Только Broadcast», флаг «Отвечать на Ping» устанавливается на усмотрение администратора.

17. 10. Использование ФПСУ-IP для смены порта назначения трафика, направляемого в адрес абонента

В качестве назначения MAP в правиле межсетевого экрана можно ставить одиночный адрес, равный MAP-адресу с установкой порта назначения. При такой настройке

ФПСУ-IP будет менять порт назначения у всех пакетов, подпадающих под действие правила, на указанный администратором.

Рассмотрим пример использования ФПСУ-IP для переназначения порта у пакетов, отправленных в адрес внутреннего сервера. ФПСУ-IP получает пакет в адрес сервера 192.168.10.10 на порт 80 и изменяет порт получателя на 1080. Таким образом, входящие клиентские соединения можно перенаправлять на другой порт сервера.

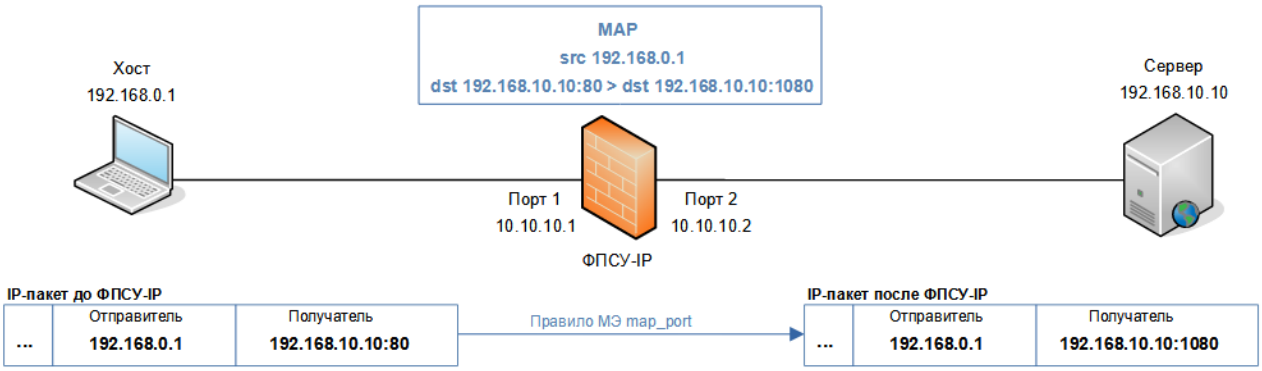

Рисунок 454 - Схема перенаправления пакетов на другой порт сервера

В настройках конфигурации ФПСУ-IP порта 1 (IP- адрес 10.10.10.1) необходимо описать хост или подсеть, в которую входит хост 192.168.0.1, отправляющий запросы серверу, как абонента порта. В настройках конфигурации ФПСУ-IP порта 2 (IP- адрес 10.10.10.2) должен быть описан в качестве абонента сервер 192.168.10.10 или подсеть, в которой расположен сервер, принимающий запросы клиентов. Переназначение номеров портов входящих соединений клиентов задается правилом трафика межсетевого экрана, в котором указывается:

- в поле опции MAP, IP-адрес назначения и новый порт;
- IP-адрес отправителя в списке отправителей, пакеты которого требуется отслеживать и изменять порт назначения;
- только один IP-адрес сервера в списке назначений правила;
- служба, распространяющая действие правила только на пакеты TCP/UDP порта номер 80;
- правило разрешается (accept, активно).

Конфигурация ФПСУ-IP должна содержать следующие установки:

```
Порт 1      Адрес            Маска         VLAN
        010.010.010.001  255.255.255.000   Нет

АБОНЕНТЫ
 Адрес 192.168.000.001   Хост
 Имя   192.168.000.001
```

```
Режим работы     Ретрансляция
Режим партнера
 Данного порта   Ретрансляция  Через ФПСУ
 Другого порта   Ретрансляция  Через ФПСУ
Работа разрешена

Адрес 192.168.000.000   Маска 255.255.255.000
Имя   192.168.000.000
Режим работы     Ретрансляция
Режим партнера
 Данного порта   Ретрансляция  Через ФПСУ
 Другого порта   Ретрансляция  Через ФПСУ
Работа разрешена
```

Порт 2 Адрес Маска VLAN
010.010.010.002 255.255.255.000 Нет

АБОНЕНТЫ

```
Адрес 192.168.010.010   Хост
Имя   192.168.010.010
Режим работы     Ретрансляция
Режим партнера
 Данного порта   Ретрансляция  Через ФПСУ
 Другого порта   Ретрансляция  Через ФПСУ
Работа разрешена
Правила межсетевого экрана для этого абонента
 map_port
```

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее любые входящие соединения по протоколу TCP/UDP с портом назначения 80, для указанных соединений порт назначения преобразуется по заданному правилу MAP на номер 1080. В правиле межсетевого экрана во вкладке «Назначение» должен быть указан один и только один адрес назначения, адрес сервера. Во вкладке «Источник» может быть явно указан хост или подсеть, отправляющие запросы. Если вкладка «Источник» пустая, ФПСУ-IP будет принимать и менять порт у любых входящих соединений с сервером и портом назначения 80. Во вкладке «Общие» в поле «MAP» указывается тот же IP-адрес сервера, что и во вкладке назначения, и новый порт 1080, на который должны перенаправляться запросы. Данное правило применяется на порту 2 ФПСУ-IP к абоненту сервер, указанному как хост;
2. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

Межсетевой экран активен: Да

Правила трафика

1. map_port

Общие
Действие : Accept
Map : 192.168.010.010 1080
Время работы : Любое
Лог : Не вести лог
Активно : Да
Источник : Любой
Назначение
Адрес : 192.168.010.010 192.168.010.010
Служба
TCP/UDP

2. Block other traffic

Общие
Действие : Drop
Время работы : Любое
Лог : Не вести лог
Активно : Да
Источник : Любой
Назначение : Любой
Служба : Любая

Службы

1. TCP/UDP

Общие
Описание :
Протокол : TCP/UDP
Порт источника : Любой
Порт назначения : 80 (World Wide Web HTTP)

17. 11. Использование ФПСУ-IP для балансировки нагрузки на порты внутреннего сервера

Рассмотрим пример с балансировкой нагрузки на порты внутреннего сервера. Входящие клиентские соединения можно распределять по разным портам сервера.

ФПСУ-IP отслеживает входящие пакеты в адрес сервера 192.168.10.10 на порт 80 и в

зависимости от источника получения запроса изменяет порт получателя у входящего соединения. Хост 1 отправляет запросы серверу 192.168.10.10 на порт 80 по умолчанию, запросы данного хоста сервер получает на порт по умолчанию. Хосты 2 и 3 отправляют запросы серверу 192.168.10.10 на порт 80 по умолчанию, ФПСУ-IP по правилу МЭ с применением перенаправления порта MAP меняет порт назначения входящего соединения и сервер получает запросы данного хоста на другой указанный порт соответственно 1080 и 2080.

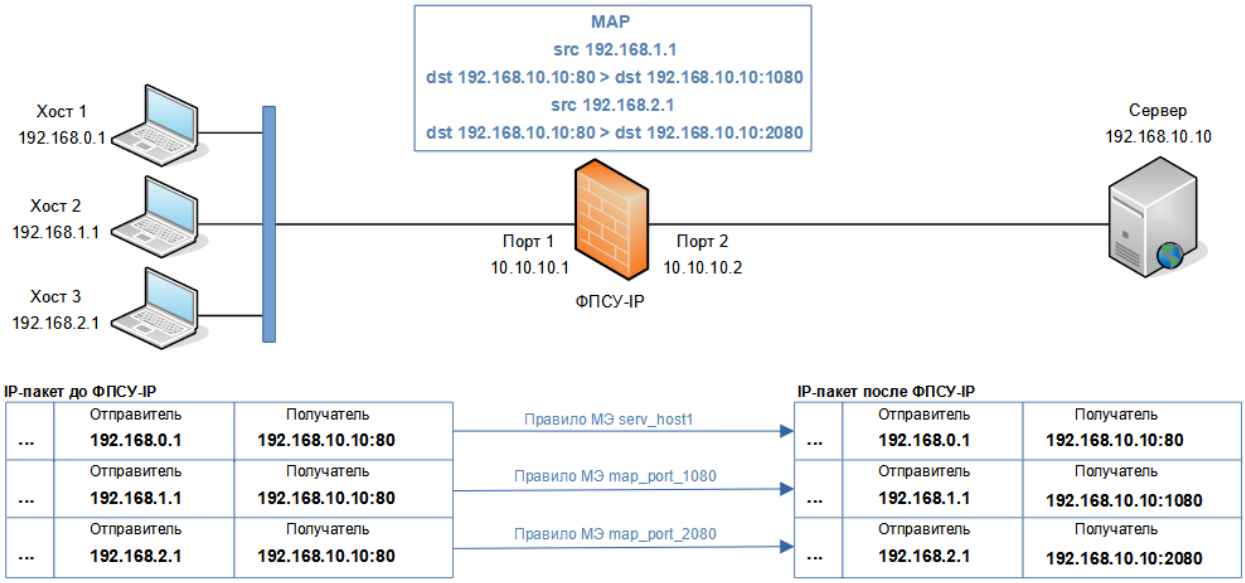

Рисунок 455 - Схема перенаправления пакетов на другой порт сервера

В настройках конфигурации ФПСУ-IP порта 1 (IP- адрес 10.10.10.1) необходимо описать хосты 192.168.0.1, 192.168.1.1, 192.168.2.1 или подсети, в которые они входят, как абоненты порта. В настройках конфигурации ФПСУ-IP порта 2 (IP- адрес 10.10.10.2) должен быть описан в качестве абонента сервер 192.168.10.10 или подсеть, в которой расположен сервер, принимающий запросы клиентов. Переназначение номеров портов входящих соединений клиентов задается правилами трафика межсетевого экрана, в которых указывается:

- в поле опции MAP, IP-адрес назначения и новый порт;
- IP-адрес отправителя в списке отправителей, пакеты которого требуется отслеживать и изменять порт назначения;
- только один IP-адрес сервера в списке назначений правила;
- служба, распространяющая действие правила только на пакеты TCP/UDP порта номер 80;
- правило разрешается (accept, активно).

Конфигурация ФПСУ-IP должна содержать следующие установки:

```
Порт 1      Адрес            Маска        VLAN
        010.010.010.001  255.255.255.000   Нет

  АБОНЕНТЫ
Адрес 192.168.000.001   Хост
   Имя   192.168.001.001
   MAC   Не задан
   Режим работы     Ретрансляция
   Режим партнера
    Данного порта   Ретрансляция  Через ФПСУ
    Другого порта   Ретрансляция  Через ФПСУ
   Работа разрешена
   Правила межсетевого экрана для этого абонента
    serv_host1

Адрес 192.168.001.001   Хост
   Имя   192.168.001.001
   MAC   Не задан
   Режим работы     Ретрансляция
   Режим партнера
    Данного порта   Ретрансляция  Через ФПСУ
    Другого порта   Ретрансляция  Через ФПСУ
   Работа разрешена
   Правила межсетевого экрана для этого абонента
    map_port_1080

   Адрес 192.168.002.001   Хост
   Имя   192.168.002.001
   MAC   Не задан
   Режим работы     Ретрансляция
   Режим партнера
    Данного порта   Ретрансляция  Через ФПСУ
    Другого порта   Ретрансляция  Через ФПСУ
   Работа разрешена
   Правила межсетевого экрана для этого абонента
    map_port_2080

 Порт 2      Адрес            Маска        VLAN
        010.010.010.002  255.255.255.000   Нет
  АБОНЕНТЫ
Адрес 192.168.010.010   Хост
   Имя   192.168.010.010
   MAC   Не задан
   Режим работы     Ретрансляция
```

```
Режим партнера
 Данного порта   Ретрансляция  Через ФПСУ
 Другого порта   Ретрансляция  Через ФПСУ
Работа разрешена
Правила межсетевого экрана для этого абонента
 serv_host1
 map_port_1080
 map_port_2080
```

Межсетевой экран ФПСУ-IP должен быть задействован. Должны быть созданы и задействованы следующие правила межсетевого экрана:

1. Правило, разрешающее входящие соединения по протоколу TCP/UDP хоста 192.168.0.1 в адрес сервера 192.168.10.10 на порт 80 (по умолчанию). Данное правило будет применено к абоненту 192.168.0.1 на порту 1 ФПСУ-IP, а также на порту 2 ФПСУ-IP к абоненту сервер 192.168.10.10, указанному как хост;
2. Правило, разрешающее входящие соединения по протоколу TCP/UDP хоста 192.168.1.1 в адрес сервера 192.168.10.10, порт IP-адреса назначения - по умолчанию 80 подменяется на другой порт 1080 по заданному правилу MAP. В правиле во вкладке «Назначение» обязательно должен быть указан один и только один IP-адрес - адрес сервера. Во вкладке «Источник» явно указан источник - хост 192.168.1.1. Во вкладке «Общие» в поле MAP необходимо указать тот же IP-адрес сервера, что указан в адресе назначения, и новый порт 1080. Данное правило будет применено к абоненту 192.168.1.1 на порту 1 ФПСУ-IP, а также на порту 2 ФПСУ-IP к абоненту сервер 192.168.10.10;
3. Правило, разрешающее входящие соединения по протоколу TCP/UDP хоста 192.168.2.1 в адрес сервера 192.168.10.10, порт IP-адреса назначения - по умолчанию 80 подменяется на другой порт 2080 по заданному правилу MAP. В правиле во вкладке «Назначение» обязательно должен быть указан один и только один IP-адрес - адрес сервера. Во вкладке «Источник» явно указан источник - хост 192.168.2.1. Во вкладке «Общие» в поле MAP необходимо указать тот же IP-адрес сервера, что указан в адресе назначения, и новый порт 2080. Данное правило будет применено к абоненту 192.168.2.1 на порту 1 ФПСУ-IP, а также на порту 2 ФПСУ-IP к абоненту сервер 192.168.10.10;
4. Правило, запрещающее все остальные не указанные выше входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

Межсетевой экран активен: Да

Правила трафика

```
1. serv_host1
      Общие
        Действие        : Accept
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Адрес           :   192.168.000.001 192.168.000.001
      Назначение
        Адрес           :   192.168.010.010 192.168.010.010
      Служба
        TCP/UDP

2. map_port_1080
      Общие
        Действие        : Accept
        Map             : 192.168.010.010 1080
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Адрес           :   192.168.001.001 192.168.001.001
      Назначение
        Адрес           :   192.168.010.010 192.168.010.010
      Служба
        TCP/UDP

3. map_port_2080
      Общие
        Действие        : Accept
        Map             : 192.168.010.010 2080
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Адрес           :   192.168.002.001 192.168.002.001
      Назначение
        Адрес           :   192.168.010.010 192.168.010.010
      Служба
        TCP/UDP

4. Block other traffic
      Общие
        Действие        : Drop
```

```
    Время работы     : Любое
    Лог              : Не вести лог
    Активно          : Да
  Источник         : Любой
  Назначение       : Любой
  Служба           : Любая
```

Службы

```
1. TCP/UDP
    Общие
      Описание         :
      Протокол         : TCP/UDP
      Порт источника   : Любой
      Порт назначения : 80 (World Wide Web HTTP)
```

В конфигурациях ФПСУ-IP приведены только необходимые для работоспособности схемы настройки, дополнительно для абонентов должен быть выключен флаг «Только Broadcast», флаг «Отвечать на Ping» устанавливается на усмотрение администратора.

17. 12. Использование ФПСУ-IP на медленных каналах. Спутник, spoofing

Рассмотрим ситуацию, когда сеть организации представляет отдельные локальные IP-подсети, разделенные территориально и для передачи данных используется спутниковый канал связи. Защищенное взаимодействие каждой из локальных подсетей обеспечивается ФПСУ-IP, подключенного со стороны внутреннего порта пограничного маршрутизатора, предоставляющего доступ к сети Интернет с использованием технологий спутниковой связи (подробнее о настройках см. пункт «Дополнительные параметры и защита от flood-атак»).

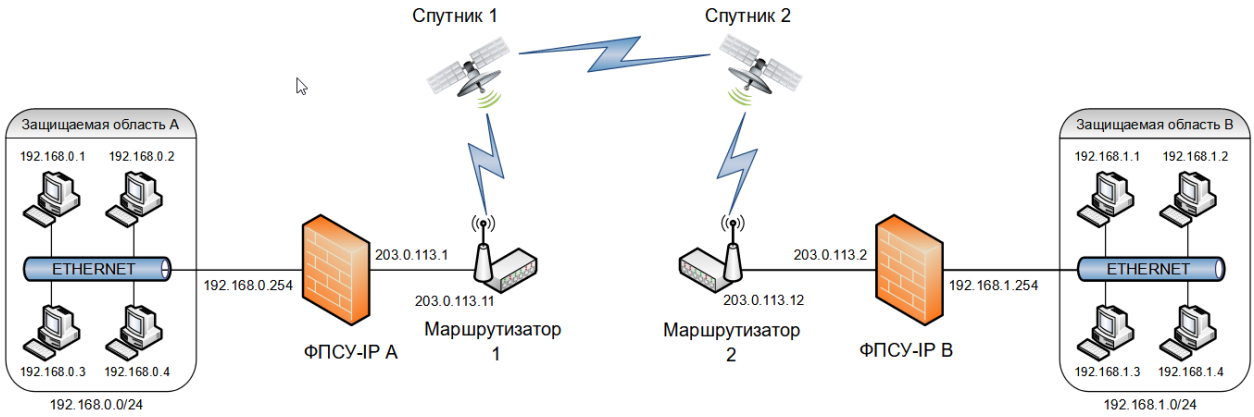

Рисунок 456 - Передача данных через спутниковый канал связи

Рассмотрим пример, когда абонент области А отправляет данные абоненту области В. При настройке спуфинга важно учитывать в каком направлении строится сессия TCP.

Настройки спуфинга устанавливаются на принимающей стороне, ФПСУ-IP B. Необходимо задать правило МЭ для входящего трафика от абонентов области A с включением функции спуфинга, включить настройки спуфинга в параметрах доступа на ФПСУ-IP B. Спуфинг позволяет ФПСУ-IP B отправлять подтверждение о получении TCP пакета от абонента области A не дожидаясь подтверждения его получения. На ФПСУ-IP A достаточно задать правило МЭ для исходящего трафика. При обмене пакетами спуфинг на ФПСУ-IP A включается автоматически, с настройками спуфинга по умолчанию.

Используются следующие IP-адреса:

- защищаемая область A - 192.168.0.0, маска 255.255.255.0 (24 бита);
- защищаемая область B - 192.168.1.0, маска 255.255.255.0 (24 бита).

Конфигурация ФПСУ-IP должна содержать следующие установки:

⇒ Для ФПСУ-IP A:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 указаны как используемые.

Порт 1:
Номер 1,
Адрес 203.000.113.001,
Маска 255.255.255.000 (24 разряда),
ФПСУ
203.000.113.2, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы:203.000.113.011,
протоколы маршрутизации выключены;

Абоненты:
Адрес 192.168.001.000; Маска 255.255.255.000;
Доступен через маршрутизатор 203.000.113.011
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.

Порт 2:
Номер 2,

Адрес 192.168.000.254,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.000.000; Маска 255.255.255.000;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
Change

Правила МЭ:

1 Change

```
      Общие
        Действие        : Accept
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Сеть            :   192.168.000.000 192.168.000.000/24
      Назначение
        Сеть            :   192.168.001.000 192.168.001.000/24
      Служба          : Любая
```

2 Block other traffic

```
      Общие
        Действие        : Drop
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник        : Любой
      Назначение      : Любой
      Служба          : Любая
```

Для ФПСУ-IP B:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 указаны как используемые.

Порт 1:

Номер 1,

Адрес 203.000.113.002,
Маска 255.255.255.000 (24 разряда),
ФПСУ
203.000.113.1, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы:203.000.113.012,
протоколы маршрутизации выключены;

Абоненты:
Адрес 192.168.000.000; Маска 255.255.255.000;
Доступен через маршрутизатор 203.000.113.012
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.

Порт 2:
Номер 2,
Адрес 192.168.001.254,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.001.000; Маска 255.255.255.000;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
Spoof

Правила МЭ:
1 Spoof
Общие
Действие : Accept
Время работы : Любое
Лог : Не вести лог
Spoof : Да
Активно : Да
Источник
Сеть : 192.168.000.000 192.168.000.000/24
Назначение
Сеть : 192.168.001.000 192.168.001.000/24

```
      Служба          : TCP

2 Block other traffic
      Общие
        Действие        : Drop
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник        : Любой
      Назначение      : Любой
      Служба          : Любая

Службы:
    1. TCP
      Общие
        Протокол        : TCP
        Порт источника  : Любой
        Порт назначения : Любой

меню Параметры доступа→Параметры→Spoofing:
Таймаут повторной пересылки задержанного пакета 250,
Шаг увеличения таймаута 125,
```

В конфигурациях ФПСУ-IP приведены только необходимые для работоспособности схемы настройки, дополнительно для абонентов должен быть выключен флаг «Только Broadcast», флаг «Отвечать на Ping» устанавливается на усмотрение администратора.

Достаточно настроить спуфинг на одном ФПСУ-IP, где используется спутниковая связь. Межсетевой экран ФПСУ-IP должен быть задействован. Созданное правило межсетевого экрана должно быть задействовано. Межсетевым экраном контролируется каждая сессия, поэтому достаточно описать правило трафика из защищенной области А в защищенную область В.

17. 13. Применение prefix-list в протоколе BGP

Рассмотрим пример базовой настройки протокола BGP, ограничение трафика из одной автономной системы в другую организуется с помощью prefix-list. ФПСУ-IP расположены в разных автономных системах.

Для установления eBGP-сессии между двумя ФПСУ-IP необходимо на каждом ФПСУ-IP:

- указать номер автономной системы Local AS, в которой находится ФПСУ-IP;
- задать идентификатор Router ID для включения ФПСУ-IP в протокол BGP;

- включить протокол BGP на вкладке «General»;
- объявить подсети в данной автономной системе;
- предварительно создать prefix-list для входящих и исходящих маршрутов (по необходимости);
- задать соседа на вкладке «Peers»;
- запустить ФПСУ-IP.

Ограничим исходящие и входящие маршруты в таблицах маршрутизации ФПСУ-IP:

- В таблицах маршрутизации ФПСУ-IP описаны по 5 подсетей.
- ФПСУ-IP A объявляет ФПСУ-IP B только подсеть 100.0.1.0/24 по протоколу eBGP.
- ФПСУ-IP A отклоняет объявление подсетей 100.0.2.0/24 и 200.0.2.0/24 от ФПСУ-IP B по протоколу eBGP.

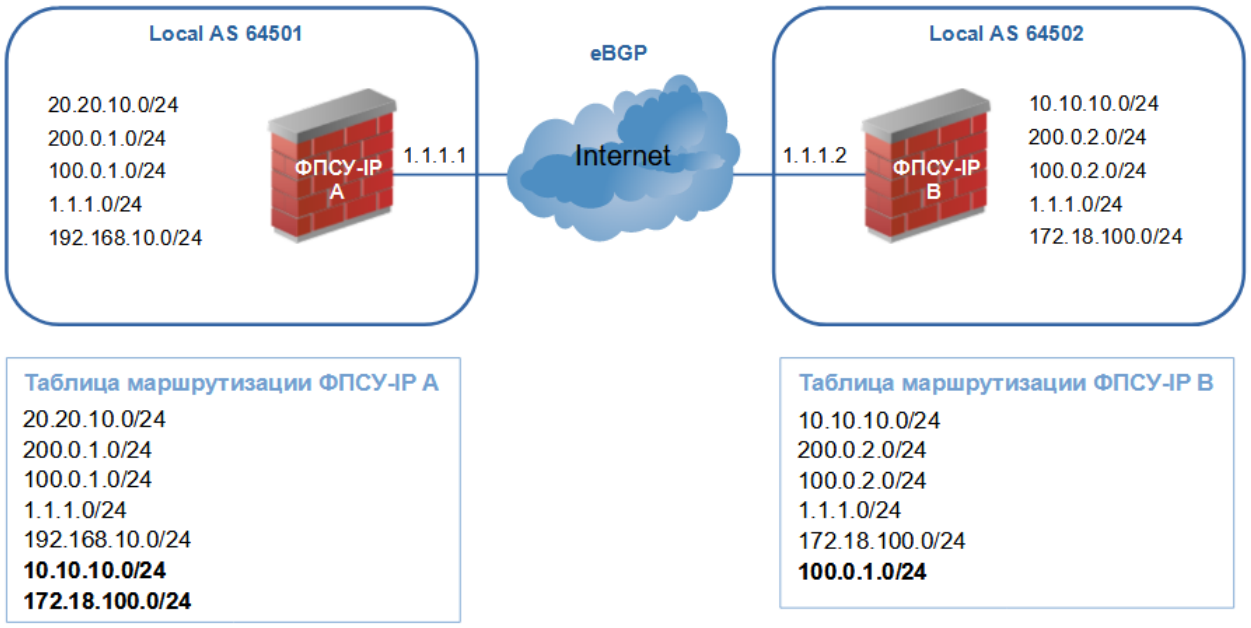

Рисунок 457 - Ограничение исходящих и входящих маршрутов на ФПСУ-IP A

ФПСУ A

Local AS 64501
Router ID 1.1.1.1
Graceful restart X
Require police on eBGP X
Активно X

Networks
1.1.1.0/24, описание N1, Активно X
100.0.1.0/24, описание N2, Активно X
200.0.1.0/24, описание N3, Активно X

20.20.10.0/24, описание N4, Активно X
192.168.10.0/24, описание N5, Активно X

Peers
Адрес 1.1.1.2, описание ФПСУ B
Remote AS 64502
Keepalive time 60
Hold time 180
Graceful restart X
prefix-list pref1
Активно X

Prefix-list
Имя pref1, описание out
Prefix
Sequence 100, action Permit, адрес 100.0.1.0, маска 255.255.255.0

Имя pref1, описание in
Prefix
Sequence 100, action Deny, адрес 200.0.2.0, маска 255.255.255.0
Sequence 110, action Deny, адрес 100.0.2.0, маска 255.255.255.0
Sequence 120, action Permit, Any

ФПСУ B

Local AS 64502
Router ID 1.1.1.2
Graceful restart X
Require police on eBGP X
Активно X

Networks
10.10.10.0/24, описание N1, Активно X
100.0.2.0/24, описание N2, Активно X
200.0.2.0/24, описание N3, Активно X
1.1.1.0/24, описание N4, Активно X
172.18.100.0/24, описание N5, Активно X

Peers
Адрес 1.1.1.1, описание ФПСУ A
Remote AS 64501
Keepalive time 60
Hold time 180
Graceful restart X
Активно X

18. Способы разрешения возможных проблем при работе ФПСУ-IP

18. 1. Первый запуск ФПСУ-IP

Несмотря на то, что установка ФПСУ-IP не требует переконфигурирования сетевого оборудования, при первом его запуске (при подключении его к сети) возможны ситуации, когда для нормализации работы сети необходимо предпринять специальные действия.

Это обусловлено тем, что ARP-таблицы сетевого оборудования после установки ФПСУ-IP будут содержать устаревшие сведения (ARP-записи) об адресах сетевых адаптеров хостов или другого сетевого оборудования, которые могут обновиться только после истечения «времени жизни» записи. Это время задается в конфигурации сетевого оборудования и может оказаться достаточно большим (например, у маршрутизаторов фирмы Cisco это время может быть равно 4 часам). Понятно, что в течение периода «жизни» устаревших записей необходимо предпринять специальные меры, чтобы восстановить прежнее состояние работы сети и доступ к некоторым хостам защищаемой области.

В ПО ФПСУ-IP введены специальные процедуры, позволяющие обновлять «недостоверные» ARP-записи в ARP-таблицах как пограничных маршрутизаторов, так и хостов, находящихся со сторон его портов. Однако обновление производится только при попытке обмена пакетами хостов защищаемой области с другими хостами или сетевым оборудованием (когда установленный комплекс «знакомится» с хостами или оборудованием, смежными с ним). Если в защищаемой области окажется сервер (передающий пакеты только в ответ на посылаемый запрос, которого он не может получить, поскольку маршрутизирующему оборудованию известен «недостоверный» адрес сетевого адаптера сервера, которому он должен передавать запросы) или другой хост, работающий в пассивном режиме, они будут недоступны в течение «времени старения» соответствующих записей в ARP-таблицах.

Для нормализации работы сети в данной ситуации рекомендуется принять следующие меры:

1. В случае, если ФПСУ-IP устанавливается между защищаемой областью и ее пограничными маршрутизаторами - очистить ARP-таблицы пограничных маршрутизаторов или перезапустить маршрутизаторы;
2. Если между защищаемой областью и ФПСУ-IP пограничные маршрутизаторы отсутствуют — очистить ARP-таблицы «пассивных» хостов или сетевого оборудования, либо перезапустить их, либо осуществить с них попытку обмена пакетами с другими хостами или сетевым оборудованием.

18. 2. Устранение неполадок, связанных с работой сетевого оборудования

Одна из возможных причин возникновения большого количества ошибок в работе сети, или неэффективной работы ФПСУ-IP, выражающейся в резком падении скорости приема/передачи пакетов, связана с несовместимыми режимами работы сетевых адаптеров как самого ФПСУ-IP, так и адаптеров пограничного сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и т.п.). Ошибки также могут быть связаны с неправильным подбором сетевого кабеля. Многие сетевые LAN-адаптеры при соответствующих установках могут автоматически определять скорость передачи данных по линии и возможность использования полнодуплексного режима приема/передачи.

Однако, при использовании сетевых адаптеров различных фирм-производителей в совместной работе автоматическое определение не всегда производится корректно. Рекомендуется в таком случае отказаться от таких установок и задавать параметры адаптеров вручную в соответствии с требуемым режимом работы.

Таблица обобщает возможные причины возникновения неполадок и рекомендуемые методы проверки аппаратуры или коррекции конфигурации оборудования.

Таблица 458. Причины возникновения неполадок

Неполадки	Возможные причины неполадок	Методы определения и/или устранения
Отсутствие принимаемых пакетов на соответствующем порту ФПСУ-IP.	Несоответствующий тип соединительного кабеля между ФПСУ-IP и смежным оборудованием	Проверить тип применяемого кабеля и убедиться в его соответствии подключенному оборудованию
Отсутствие принимаемых пакетов на соответствующем порту ФПСУ-IP или появление большого количества ошибочных пакетов (см. пункт «Окно состояния рабочих LAN портов»)	Дефект соединительного кабеля между ФПСУ-IP и смежным оборудованием	Проверить работоспособность применяемого кабеля и при обнаружении неисправности заменить кабель

Отсутствие принимаемых пакетов на соответствующем порту ФПСУ-IP	Неправильно указанная (или определенная адаптером) скорость работы линии на сетевом адаптере	Установить в конфигурации соответствующего LAN-порта необходимую скорость работы линии
Появление на соответствующем порту ФПСУ-IP большого количества ошибочных пакетов (см. пункт «Окно состояния рабочих LAN портов») снижение скорости передачи или невозможность передачи данных через ФПСУ-IP.	Неправильное указание дуплексного режима работы линии (полный дуплекс или полудуплекс) или несовместимость режима одного из адаптеров комплекса с адаптерами смежного оборудования сети	Установить в конфигурации соответствующего LAN-порта или конфигурации смежного оборудования правильный дуплексный режим работы линии.

19. Диагностика ошибок ФПСУ-IP

При отладке работы ФПСУ-IP сразу после его установки, а также в процессе его дальнейшей работы администратор имеет возможность отслеживать процессы, происходящие в различных подсистемах ФПСУ-IP. Сообщения об ошибках или неполадках, обнаруженных работающим ФПСУ-IP, выдаются на экран монитора (если к ФПСУ-IP подключен монитор) и в регистрационные записи статистики (см. разделы «Окно состояния работы пользователей» и «Просмотр статистики»). Данный раздел поясняет выдаваемые диагностические сообщения и представляет возможные причины возникновения ошибок и методы их устранения.

Таблица 459. Ошибки формата принимаемых IP-пакетов

Диагностика	Пояснение	Причина возникновения
Короткий пакет	Длина принятых данных короче, чем указано в IP заголовке принятого пакета.	Сбой или коллизии локальной сети; сбой у станции отправителя.
Ошибка фрагментации	Суммарная длина собранного из фрагментов IP-пакета больше 65536 байт.	Некорректная работа программного обеспечения станции-отправителя. Если при передаче данных используется протокол TCP, ошибки можно избежать, включив опцию «Корректировать TCP MSS» (см. пункт «Общие параметры конфигурации ФПСУ-IP»)
Отмена фрагментации	Размер пакета превышает максимальный размер пакета, MTU, но установленный флаг запрета фрагментации не дает разбивать его на несколько пакетов.	Такая ситуация обычно возникает при попытке передачи пакетов TCP/UDP по протоколу FTP и некоторым другим протоколам, и носит временный характер. Если ошибка возникает постоянно, необходимо проанализировать (и, при необходимости, скорректировать) конфигурацию сетевых адаптеров и/или уменьшить MTU до 1400 байт на оборудовании, от которого приходят большие пакеты с флагом запрета фрагментации.

Диагностика	Пояснение	Причина возникновения
Ошибочный фрагмент	Начало фрагментированного пакета не выровнено на 8 байтовую границу.	Некорректная работа программного обеспечения станции-отправителя.
Неверен список опций	Список IP-опций в заголовке IP пакета не отвечает принятым в сообществе Интернет правилам.	Некорректная работа программного обеспечения станции-отправителя.
Мало памяти	Недостаточно оперативной памяти для приема и/или обработки пакета.	Если такая ошибка указывается для разных IP адресов, причина возникновения - «шторм» в IP сети. Если ошибка возникает только для одного конкретного адреса - вероятно проведение атаки на ФПСУ-IP с целью вывода его из строя через создание сетевой перегрузки.

Таблица 460. Ошибки, связанные с обработкой принимаемых пакетов

Диагностика	Пояснение	Причина возникновения
Маршрут неизвестен	Не известен адрес сетевого адаптера для соответствующего IP-адреса абонента-получателя.	Если ошибка возникает постоянно - либо станции с таким IP-адресом в сети нет или она не работает, либо режимы смежных сетевых адаптеров несовместимы. Если ошибка возникает эпизодически - неполадки отсутствуют, в момент поступления запроса адрес сетевого адаптера был неизвестен, после чего он был автоматически определен ФПСУ-IP за непродолжительное время.

Диагностика	Пояснение	Причина возникновения
Сбой LAN карты	Сбой указанного сетевого адаптера при попытке передачи фрейма	Неустойчивая работа сбойного сетевого адаптера - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.
MAC-адрес станции совпадает с адресом ФПСУ-IP	получен фрейм, MAC-адрес отправителя которого совпадает с MAC-адресом одного из сетевых портов ФПСУ-IP	Сетевые пакеты от станции, MAC-адрес которой совпадает с MAC-адресом одного из портов ФПСУ-IP, будут сброшены. Требуется изменить MAC-адрес у рабочей станции или у ФПСУ-IP.
Дублирование адресов	В сети со стороны указанного порта обнаружена станция, имеющая IP адрес, совпадающий с одним из портов ФПСУ-IP, или адрес сетевого адаптера которой совпадает с адресом сетевого адаптера ФПСУ-IP.	Это может произойти при образовании маршрутной петли - проверьте правильность конфигурации маршрутизирующего оборудования. В сети на самом деле существует такая станция — смените адреса на ФПСУ-IP или указанной станции.
Неверен IP адрес	Неверен один из IP-адресов в заголовке IP пакета.	IP-адрес отправителя является широковещательным в известные ФПСУ-IP подсети. Отправитель пакета не является известным ФПСУ-IP маршрутизатором, а IP-адрес получателя является либо групповым (multicast), либо широковещательным во все подсети (255.255.255.255). IP-адрес отправителя пакета — 255.255.255.255.
Истекло время	Время жизни пакета истекло, или исчерпан лимит времени ожидания сборки пакета	У принятого пакета истекает время жизни.

Диагностика	Пояснение	Причина возникновения
		Если данная ошибка проявляется часто, причем получателем является данный ФПСУ-IP, а отправителем - другой ФПСУ-IP, рекомендуется в конфигурации обоих ФПСУ-IP изменить значение MTU (см. раздел «Описание параметров удаленных ФПСУ-IP»)
Протокол недоступен	Обращение к одному из портов ФПСУ-IP по протоколу, который ФПСУ-IP не поддерживает.	ФПСУ-IP не принимает для обработки пакеты никаких протоколов, кроме собственных протоколов поддержки VPN и администрирования, а также протокола ICMP ECHO REQUEST (Ping) при условии, если это разрешено в конфигурации ФПСУ-IP.

Таблица 461. Ошибки, связанные с попытками нарушения установленных правил фильтрации

Диагностика	Пояснение	Причина возникновения
Входящий не описан	Отправитель пакета не описан в конфигурации	Отправитель пакета не описан в конфигурации портов ФПСУ-IP.
Получатель не описан	Получатель пакета не описан в конфигурации.	Не описан абонент-получатель в конфигурации портов ФПСУ-IP. Для межмаршрутизаторного обмена - нет маршрутизаторов со стороны противоположного порта, использующих данный протокол.
Запрет работы	Отказ в доступе абоненту-отправителю пакета	Выключен флаг «Работа Разрешена» у отправителя или получателя пакета. Попытка приема или передачи в индивидуальный адрес при включенном флаге «Только Broadcast».

Диагностика	Пояснение	Причина возникновения
		Попытка межмаршрутизаторного обмена по неразрешенному протоколу маршрутизации для маршрутизатора-отправителя пакета. «Ping» - попытка ФПСУ-IP от прописанного абонента или маршрутизатора при выключенном флаге «Отвечать на Ping». «Ping» - попытка ФПСУ-IP длинным пакетом. Не «Ping» - попытка обращения прописанного абонента к удаленному ФПСУ-IP или абонент не является удаленным администратором или ФПСУ-IP.
Запрет по доступу	Запрет по режиму работы с партнером.	Запрет по режиму работы с партнером данного или противоположного порта.
Запрет SourceRoute	Запрет доступа по опции SourceRoute в IP-пакете.	В принятом IP-пакете присутствует одна из опций, требующая записывать маршрут прохождения пакета, а в конфигурации ФПСУ-IP установлен флаг «Пакеты с опцией SourceRoute» - «Не пропускать».
Абонент через ФПСУ	Абонент должен работать в режиме ретрансляции.	Принят пакет из VPN-туннеля от абонента, для которого на данном ФПСУ-IP установлен режим работы «Ретрансляция».
Абонент миновал ФПСУ	Абонент должен работать через ФПСУ.	Принят пакет не из VPN-туннеля от абонента, для которого на данном ФПСУ-IP установлен режим работы «Через ФПСУ».
ФПСУ не работает	Удаленный ФПСУ-IP не работает.	Не включен удаленный ФПСУ-IP или с ним нет связи. Не работает сетевой адаптер - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.

Диагностика	Пояснение	Причина возникновения
Нет ФПСУ-туннеля	Отсутствие взаимодействия между ФПСУ-IP.	VPN-туннель между двумя ФПСУ-IP не установлен к моменту попытки передачи через него пакетов от абонентов. Не включен удаленный ФПСУ-IP или с ним нет связи. Неустойчивая работа сбойного сетевого адаптера - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.
Ложный ФПСУ	Станция-отправитель использует ошибочный протокол установки соединения или поддержания VPN-туннеля	Попытка передачи пакетов в IP-адрес местного ФПСУ-IP от рабочей станции, зарегистрированной как удаленный ФПСУ-IP, но не являющейся таковой.
Ошибочный ФПСУ-пакет	Ошибочный пакет от ФПСУ-IP.	На местном или удаленном ФПСУ-IP указаны неверные значения номеров ключевых данных удаленных ФПСУ-IP. В процессе установки или поддержания VPN-туннеля произошел кратковременный сбой, что обычно очень редко проявляется в момент первичной установки VPN-туннеля. Попытка навязывания местному ФПСУ-IP VPN-данных или повторения ранее переданных удаленным ФПСУ-IP данных от «вредоносной» станции.
Ошибка клиент-пакет	Искажены или повреждены находящиеся в полученном от ФПСУ-IP/Клиента пакете данные.	Сообщение возникает на экране мониторинга подключенных ФПСУ-IP/Клиентов. Такие пакеты будут сброшены ФПСУ-IP.

Таблица 462. Ошибки, связанные с ключевыми данными

Служебное сообщение	Пояснение	Действия администратора
The TM does not contain the key	Ошибка возникает при попытке запуска ФПСУ-IP с помощью ТМ-идентификатора, на котором находится искаженный ключ запуска.	Если искажен ключ запуска Главного администратора - обратитесь к поставщику ФПСУ-IP для замены ТМ-идентификатора Главного администратора. Если искажен ключ запуска пользователя другого класса - повторно перезапишите ТМ-идентификатор пользователя средствами ФПСУ-IP (Настройка системы - Регистрация ТМ-идентификаторов)
Внимание! Повреждены критические компоненты комплекса. ВСЕ установленные ключевые данные и ТМ утрачены. Комплекс переведен в технологический режим. Возможно потребуется переустановка комплекса	ПО ФПСУ-IP обнаружило искажение ключа для хранения долговременных ключей. Требуется вмешательство администратора	Требуется выполнить повторный перевод ФПСУ-IP из технологического режима в рабочий режим, заново зарегистрировать все ТМ-идентификаторы пользователей и переустановить ключевые данные ЦВК и удаленных администраторов. В случае ошибки перевода ФПСУ-IP из технологического режима в рабочий режим, выполнить полную переустановку ПО ФПСУ-IP.
Внимание! Поврежден компонент комплекса. Необходима инициализация ДСЧ	ПО ФПСУ-IP обнаружило искажение ключа ПДСЧ. Требуется вмешательство администратора	Требуется выполнить повторный перевод ФПСУ-IP из технологического режима в рабочий режим.
Внимание! ФПСУ не работоспособен. Искажены данные конфигурации.	ПО ФПСУ-IP обнаружило искажение конфигурации ФПСУ-IP	Восстановить конфигурацию ФПСУ-IP любым из следующих способов: • локально с помощью резервной копии конфигурации;

Служебное сообщение	**Пояснение**	**Действия администратора**
Ожидание восстановления конфигурации с резервного комплекса или удаленного администратора		• подключить к ФПСУ-IP комплекс горячего резерва; • установить на ФПСУ-IP новую конфигурацию средствами удаленного администратора.
Ошибка инициализации! Служебный описатель искажен	Сообщение об ошибке выводится на экран просмотра состояний удаленных администраторов ФПСУ-IP. ПО ФПСУ-IP обнаружило искажение секретного ключа ФПСУ-IP подсистемы удаленного администрирования или открытых ключей удаленных администраторов. Удаленное управление ФПСУ-IP с такой ошибкой невозможно.	Заново зарегистрировать удаленных администраторов на ФПСУ-IP. Перерегистрировать ФПСУ-IP на всех удаленных администраторах.
Описатель удаленных администраторов испорчен или несовместимая версия!	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ-IP.	Заново зарегистрировать удаленных администраторов на ФПСУ-IP. Перерегистрировать ФПСУ-IP на всех удаленных администраторах.

Служебное сообщение	**Пояснение**	**Действия администратора**
	ПО ФПСУ-IP обнаружило искажение секретного ключа ФПСУ-IP подсистемы удаленного администрирования или открытых ключей удаленных администраторов Удаленное управление ФПСУ-IP с такой ошибкой невозможно.	
**Имя_файла_с_открытым_ключом_удаленного_администратора*----> Поврежден*	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ-IP при попытке зарегистрировать нового удаленного администратора. Причина - искажен или поврежден предъявленный на внешнем USB-носителе открытый ключ удаленного администратора	Заново получить от администратора АРМ УА открытый ключ удаленного администратора и повторить процедуру регистрации удаленного администратора на ФПСУ-IP
Состояние туннеля с другим ФПСУ-IP "WaitSynRR" с дополнительными сообщениями в журнале статистики	Хранящиеся на внутреннем накопителе ФПСУ-IP парно-выборочные ключи были искажены.	Заново установить на ФПСУ-IP полученные от администратора ЦВК парно-выборочные ключи.

Служебное сообщение	**Пояснение**	**Действия администратора**
"Аварийное состояние ключей/нештатные действия: Ошибка при зачитывании установленных ключей"	Требуется вмешательство администратора	
Данные искажены, пропускаю!	Сообщение об ошибке выводится на экране установки ключей меню конфигурации ФПСУ-IP. Возникает при искажении предъявленного на внешнем USB-носителе парно-выборочного ключа	Заново получить от администратора ЦВК парно-выборочный ключ взамен искаженного.
Испорчены служебные данные горячего резервирования	Сообщение об ошибке выводится на экране мониторинга состояния горячего резерва ФПСУ-IP (основной комплекс системы горячего резервирования). Ошибка возникает при искажении хранящегося на внутреннем накопителе ФПСУ-IP ключа горячего резерва	Считать на ТМ-идентификатор ключ горячего резерва с исправного комплекса (меню локального конфигурирования ФПСУ-IP «Настройка системы» - «Параметры горячего резерва»). Если ключ горячего резерва не считывается с исправного комплекса, создать новый ключ горячего резерва. Повторно зарегистрировать ключ горячего резерва на сообщившем об ошибке ФПСУ-IP.

Служебное сообщение	Пояснение	Действия администратора
ФАТАЛЬНАЯ ОШИБКА. Резервный комплекс не может функционировать, так как испорчены служебные данные горячего резервирования. Возможно потребуется переустановка комплекса	Сообщение об ошибке выводится при запуске ФПСУ-IP (резервный комплекс системы горячего резервирования). Ошибка возникает при искажении хранящегося на внутреннем накопителе ФПСУ-IP ключа горячего резерва	Считать на ТМ-идентификатор ключ горячего резерва с исправного комплекса (меню локального конфигурирования ФПСУ-IP «Настройка системы» - «Параметры горячего резерва»). Если ключ горячего резерва не считывается с исправного комплекса, создать новый ключ горячего резерва. Повторно зарегистрировать ключ горячего резерва на сообщившем об ошибке ФПСУ-IP.
Испорчен или не установлен ключ центра	Сообщение об ошибке выводится на экране мониторинга действий ФПСУ-IP\Клиентов. Искажен общесистемный ключ Криптосети Клиентов. ФПСУ-IP\Клиенты не могут соединиться с ФПСУ-IP	Заново установить на ФПСУ-IP общесистемный ключ Криптосети Клиентов вместо искаженного.
ТМ испорчена	Сообщение об ошибке выводится при попытке зарегистрировать общесистемный ключ Криптосети Клиентов на ФПСУ-IP. Находящийся на ТМ-идентификаторе общесистемный ключ Криптосети Клиентов искажен или испорчен.	Заново получить от администратора ЦГКК общесистемный ключ Криптосети Клиентов и повторить процедуру регистрации общесистемного ключа Криптосети Клиентов на ФПСУ-IP

Таблица 463. Ошибки при соединении ФПСУ-IP

Диагностика	Пояснение	Причина возникновения
Не совпадают RKL роли клиент/ФПСУ-IP	Оба участника ФПСУ-IP/Клиент и ФПСУ-IP при соединении должны поддерживать удаленную загрузку ключевых данных	На ФПСУ-IP с установленной подсистемой RKL (подсистемой удаленной загрузки ключевых данных) пытается соединиться ФПСУ-IP/Клиент, VPN-Key которого не поддерживает удаленную загрузку ключевых данных, или наоборот, к ФПСУ-IP без подсистемы RKL соединяется ФПСУ-IP/Клиент, VPN-Key которого поддерживает удаленную загрузку ключевых данных

19. 1. Выдача файла Kmsg

Команда «Выдать kmsg» окна просмотра статистики ФПСУ-IP («Статистика ФПСУ-IP») позволяет выдать на внешний носитель (USB-flash) файл для анализа сообщений ядра и использования памяти в случае падения ядра Linux.

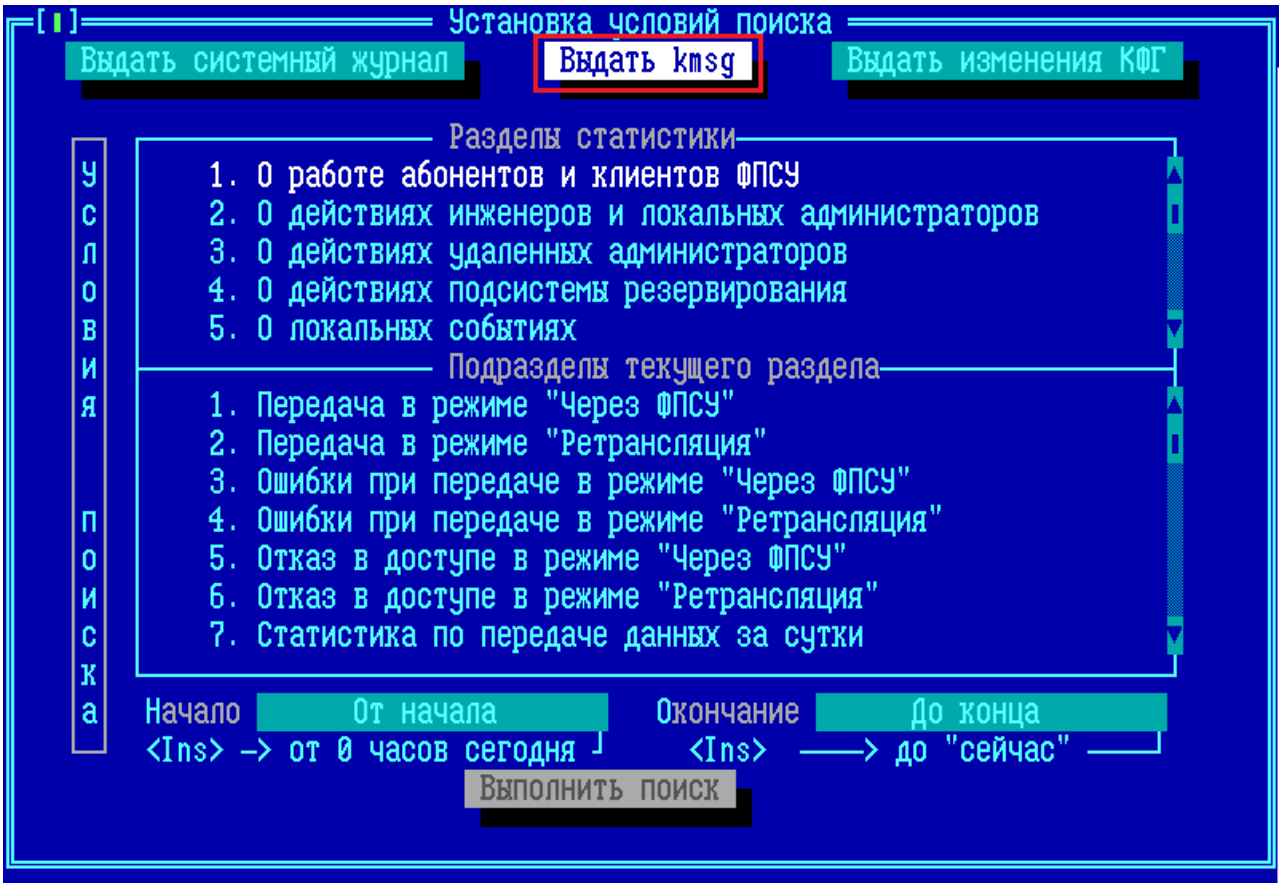

Рисунок 464 - Команда выдачи журнала изменений конфигурации межсетевого экрана

После выполнения команды система предложит подключить USB-носитель, на который будет выдан файл, к ФПСУ-IP:

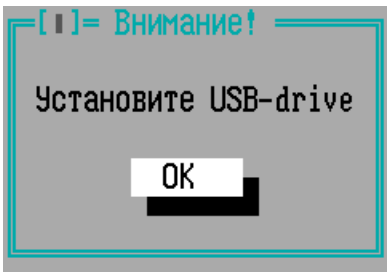

Рисунок 465 - Предложение подключить USB-носитель

Подключите носитель к ФПСУ-IP и подтвердите выполнение команды, нажав клавишу Enter. Если USB-носитель будет обнаружен ФПСУ-IP, то откроется окно диалога, в котором следует выбрать каталог на носителе.

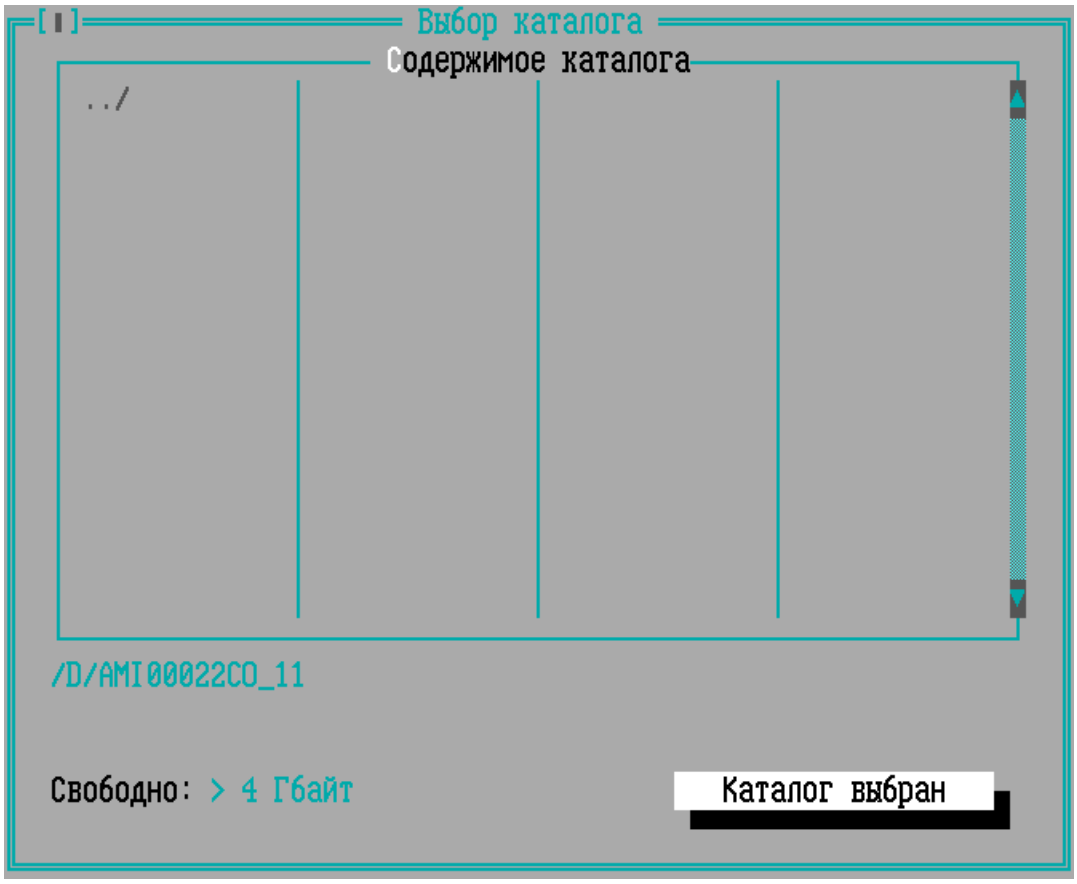

Рисунок 466 - Выбор каталога для выгрузки файла

Подтвердите место выгрузки файла, выполнив команду «Каталог выбран».

После выгрузки файла, ФПСУ-IP выдаст системное оповещение о завершении процедуры:

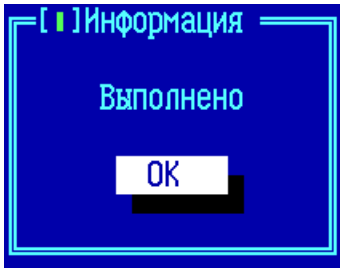

Рисунок 467 - Сообщение о завершении процедуры

19. 2. Выдача файла отладки OSPF

Команда меню «Настройка дополнений → Configure frr → copy logs» позволяет выдать на внешний носитель (USB-flash) файл отладки OSPF. Перед выполнением команды необходимо подключить USB-носитель, на который будет выдан файл, к ФПСУ-IP и запустить команду. На внешнем носителе будет создан каталог frr.log и записан отладочный

файл ospf.log.

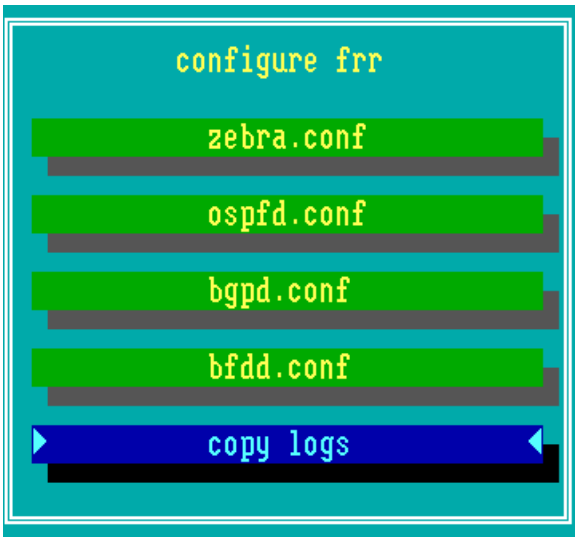

Рисунок 468 - Меню «Configure frr»

20. Удаление программного обеспечения ФПСУ-IP

20. 1. Удаление СКЗИ ФПСУ-IP

Локальному администратору ФПСУ-IP классов *«Администратор»* или *«Главный администратор»* доступна возможность форматирования внутреннего накопителя ФПСУ-IP с удалением операционной системы ФПСУ-IP и хранящихся файлов, в том числе ключевой информации СКЗИ, программных и служебных модулей СКЗИ, и программного обеспечения BIOS/UEFI.

Для запуска процедуры форматирования внутреннего накопителя:

1. Выполните команду «Настройка системы» главного меню:

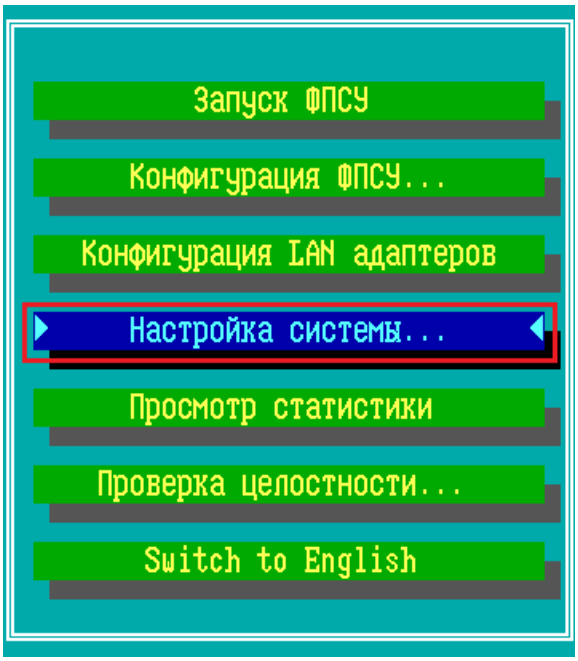

Рисунок 469 - Главное меню ФПСУ-IP

2. Выполните команду «Настройки СКЗИ» меню настройки системы:

Рисунок 470 - Меню настройки системы ФПСУ-IP

3. Выполните команду «Удаление СКЗИ» меню настройки СКЗИ.

ВНИМАНИЕ! Если при выполнении команды «Удаление СКЗИ» к ФПСУ-IP подключен USB ТМ-идентификатор ТМ-Key с правами *«Администратор»* или *«Главный администратор»,* то последующего окна к подтверждением полномочий не будет выведено на экран. Процедура удаления СКЗИ начнется сразу после выполнения команды «Удаление СКЗИ»!

Рисунок 471 - Запуск процедуры удаления СКЗИ

Если USB ТМ-идентификатор ТМ-Key не был подключен к ФПСУ-IP, появится окно с предложением подтвердить полномочия администратора или Главного администратора (права классов *«Администратор»* или *«Главный администратор»,* см. раздел «Общие

сведения», таблица 1).

ВНИМАНИЕ! Сразу после приложения к ТМ-считывателю ФПСУ-IP ТМ-идентификатора, подтверждающего права классов *«Администратор»* или *«Главный администратор»*, будет запущен необратимый процесс форматирования внутреннего накопителя!

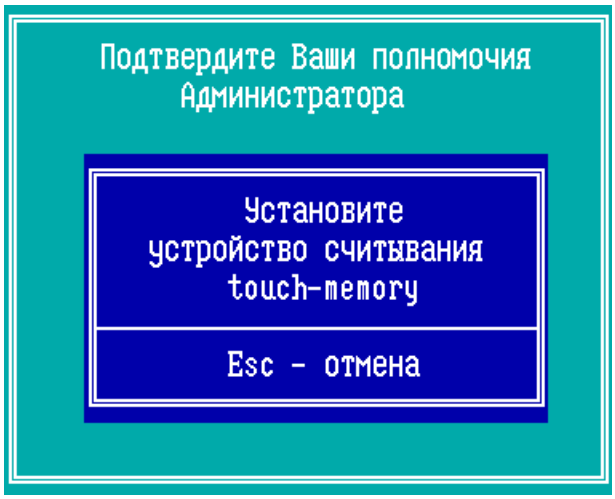

Рисунок 472 - Подтвердите полномочия для удаления СКЗИ

После подтверждения прав администратора, ФПСУ-IP начнет форматирование внутреннего накопителя, после чего перезагрузит операционную систему. Удаление операционной системы ФПСУ-IP и хранящихся на внутреннем накопителе файлов, в том числе ключевой информации СКЗИ, программных и служебных модулей СКЗИ, и программного обеспечения BIOS/UEFI, завершено.

20. 2. Удаление ПО с помощью USB-носителя со средством восстановления

Для полного удаления программного обеспечения ФПСУ-IP с его ПЗУ, следует запустить процедуру повторной установки программного обеспечения (см. пункт «Установка ПО ФПСУ-IP с установочного носителя»). Для успешного удаления программного обеспечения потребуются:

- ФПСУ-IP;
- инсталляционный комплект программного обеспечения ФПСУ-IP, состоящий из USB-носителя с дистрибутивом.

Порядок действий при удалении программного обеспечения с ПЗУ ФПСУ-IP следующий:

1. Подключите USB-носитель с дистрибутивом программного обеспечения к ФПСУ-IP.

2. При включении ФПСУ-IP следует отменить загрузку подсистемы контроля ACCESS BIOS (названия могут меняться, например на Access Bios/PnP или FPSU Access BIOS), запрещающей загружать операционную систему иначе как с защищенной внутренней памяти, и выбрать загрузку с USB. Это можно сделать при выборе Boot Options (обычно при нажатии F10) после включения ФПСУ-IP, или напрямую зайдя в BIOS и установив в Boot Options загрузку **USB2.0** вместо **Access BIOS**.

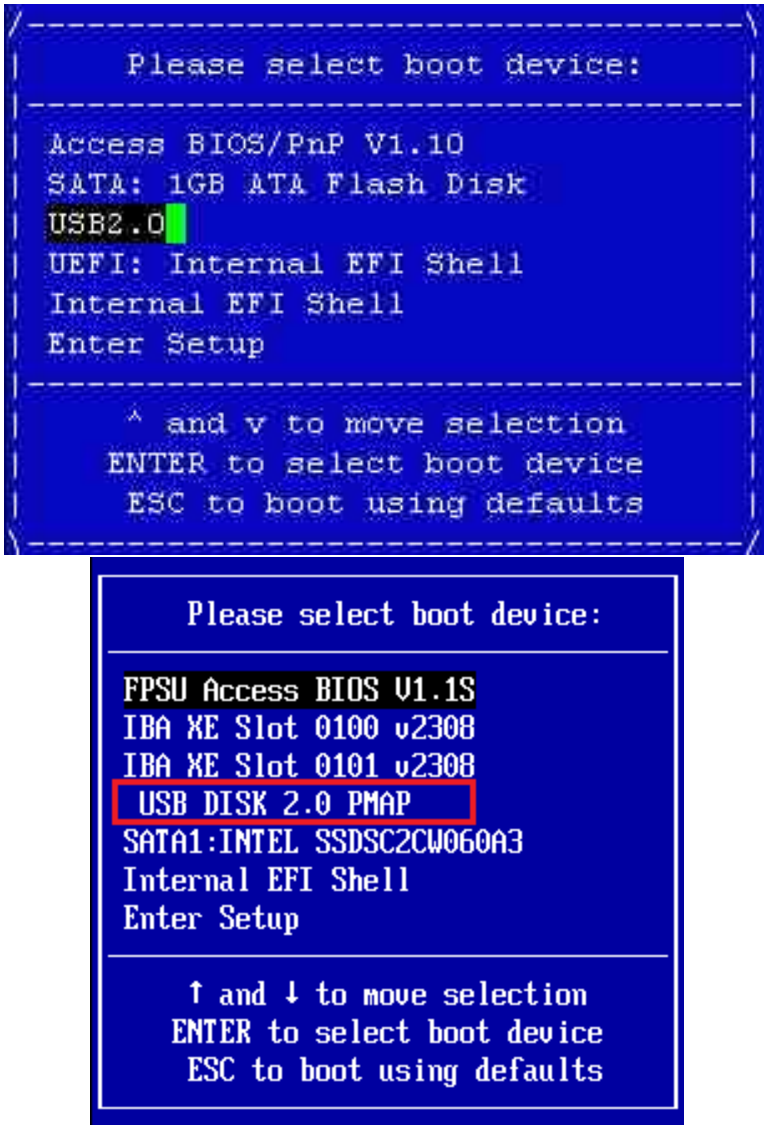

Рисунок 473 - Выбор загрузки с USB

3. Загруженная с инсталляционного USB-носителя программа начнет первый этап установки с проверки ранее установленного программного обеспечения ФПСУ-IP. Если система была ранее установлена на комплекс, будет выдано следующее сообщение:

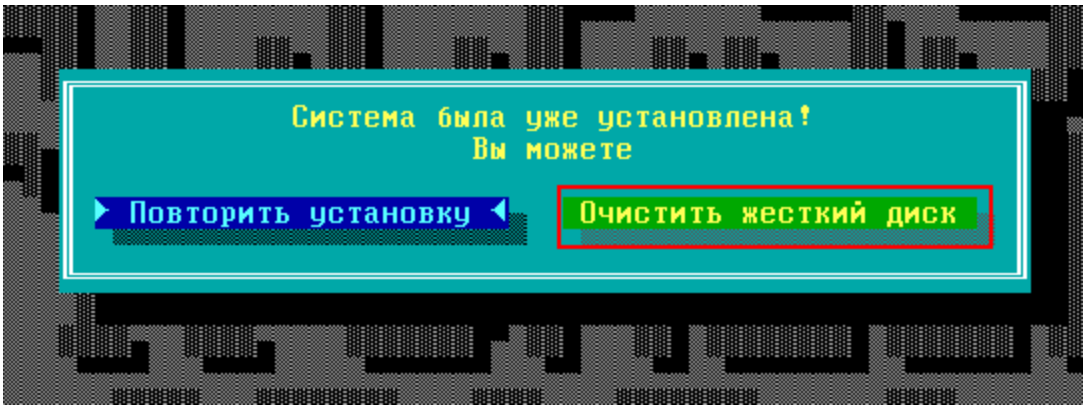

Рисунок 474 - Операционная система ФПСУ-IP уже установлена

4. Выберите команду *<Очистить жесткий диск>* и подтвердите выполнение операции.

После выполнения операции «Очистить жесткий диск», питание ФПСУ-IP можно выключать. Операционная система, ключевая информация СКЗИ, программные и служебные модули СКЗИ полностью удалены с ПЗУ ФПСУ-IP.

Уничтожение программных модулей СКЗИ на дистрибутивном USB-носителе осуществляется путем расплющивания USB-носителя молотком на наковальне.