ООО «АМИКОН»

УТВЕРЖДЕН

ПЕРС.26.20.40.140.003РА2-ЛУ

Программно-аппаратный комплекс

«ФПСУ-IP 3.X»

Руководство администратора

ПЕРС.26.20.40.140.003РА2

Листов 517

2024

Аннотация

Документ предназначен для системных администраторов и администраторов безопасности систем защиты от несанкционированного доступа с применением программно-аппаратных комплексов «ФПСУ-IP» (версия ПО 3.30.2). В документе содержатся сведения о программно-аппаратном 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 программно-аппаратного комплекса «ФПСУ-IP» и требуемый уровень безопасности, является отсутствие ошибок при конфигурировании комплекса. Поэтому конфигурирование программно-аппаратного 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 программно-аппаратного 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.

Содержание

1. Список используемых сокращений и определений

ARP	«Address Resolution Protocol», протокол для отображения IP-адреса рабочей станции сети по ее аппаратному адресу
ICMP	«Internet Control Message Protocol», протокол для передачи команд и сообщений об ошибках
IP	«Internet Protocol», базовый протокол межсетевого объединения Интернет
MTU	«Maximum transmission unit», параметр, указывающий максимальный размер блока передаваемых данных, который может быть передан протоколом без фрагментации
TCP	«Transmission Control Protocol», протокол транспортного уровня, осуществляющий доставку дейтаграмм с установлением соединения и гарантирующий доставку сообщений
UDP	«User Datagram Protocol», протокол транспортного уровня, не требующий подтверждения доставки дейтаграмм
VPN	«Virtual Private Network», виртуальная частная сеть
VLAN	«Virtual Local Area Network», виртуальная локальная сеть передачи данных
WAN	«Wide-Area Network», глобальная сеть, связывающая географически разделенные рабочие станции и LAN
АРМ УА ФПСУ-IP	Автоматизированное рабочее место удаленного администратора «ФПСУ-IP», являющееся изделием «Автоматизированное рабочее место удаленного администратора» из состава СКЗИ «Программно-аппаратный комплекс шифрования «ФПСУ-IP»
МЭ	межсетевой экран
НСД	несанкционированный доступ к информации
ПЗУ	постоянное запоминающее устройство ФПСУ-IP, твердотельный

	накопитель SSD (solid-state drive)
ПО	программное обеспечение
Сервер лицензирования	программный комплекс «Сервер лицензирования комплексов «ФПСУ-IP/Клиент», реализующий сетевой сервис выдачи и учета лицензий ФПСУ-IP/Клиентам
СЗИ НСД	система защиты информации от несанкционированного доступа
СКЗИ	средство криптографической защиты информации
ТМ, ТМ-идентификатор	электронный идентификатор «touch-memory»: iButton DS1993 – DS1996 или микроэлектронное USB-устройство «TM-Key» ПЕРС.466226.004 производства ООО «АМИКОН»
ФПСУ-IP	программно-аппаратный комплекс «ФПСУ-IP 3.X», средство защиты информации - межсетевой экран, программная компонента которого является изделием Криптомаршрутизатор из состава СКЗИ «Программно-аппаратный комплекс шифрования «ФПСУ-IP»
ЦВК	программно-аппаратный комплекс «Центр выработки ключей», являющийся изделием ЦВК из состава СКЗИ «Программно-аппаратный комплекс шифрования «ФПСУ-IP»
ЦГКК	программное обеспечение «Центр генерации ключей клиентов», являющееся изделием ЦГКК из состава СКЗИ «Программно-аппаратный комплекс шифрования «ФПСУ-IP/Клиент»
ЦПУ	центральное процессорное устройство, процессор
Хост	узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую

2. Общие сведения

Программно-аппаратный комплекс «ФПСУ-IP» (сокращенное название от «Фильтр пакетов сетевого уровня IP протокола») является программно-техническим средством защиты от несанкционированного доступа к информации. ФПСУ-IP реализует функции межсетевого экранирования и функции построения VPN-туннелей.

ФПСУ-IP позволяет выделять в открытой сети защищенные области с ограниченным доступом, а также обеспечивать защищенную передачу данных между защищенными областями.

Программное обеспечение ФПСУ-IP является средством криптографической защиты информации «Программно-аппаратный комплекс шифрования «ФПСУ-IP», изделие Криптомаршрутизатор, сертифицированным ФСБ России.

ФПСУ-IP позволяет осуществить шифрование передаваемой информации в соответствии с ГОСТ 28147-89, ГОСТ 34.12–2015 (блочный шифр «Магма»), ГОСТ Р 1323565.1.026-2019 (МГМ).

ФПСУ-IP работает по протоколу IP и использует формат фрейма Ethernet II.

ФПСУ-IP физически подключается в разрыв цепи между защищаемой локальной подсетью и остальными абонентами таким образом, чтобы все входящие и исходящие из подсети межсетевые потоки данных проходили через ФПСУ-IP.

Основными функциями ФПСУ-IP являются ***фильтрация*** IP-пакетов, заключающаяся в анализе их по совокупности критериев и принятии решения о возможности их дальнейшей передаче (с ***регистрацией*** результатов фильтрации), и ***установка VPN-туннелей с аналогичными ФПСУ-IP*** для организации защищенных режимов передачи данных.

Между прозрачно взаимодействующими через стандартное сетевое оборудование (коммутаторы, модемы, маршрутизаторы) ФПСУ-IP, защищающими IP-подсети, могут быть созданы VPN-туннели. VPN-туннели позволяют ФПСУ-IP скрывать внутреннюю структуру защищаемых сетей. В VPN-туннеле возможно обеспечение средствами ФПСУ-IP сжатия и шифрования передаваемых данных. При создании VPN-туннеля обеспечиваются взаимные ***идентификация и аутентификация*** (как стартовая, так и сеансовая) взаимодействующих комплексов ФПСУ-IP. При включенном режиме шифрования в VPN-туннеле обеспечиваются контроль целостности данных, защита их от просмотра, искажения и подмены. Для формирования межсетевых туннелей на ФПСУ-IP должны быть установлены ключи парно-выборочной связи, выработанные с помощью специального программно-аппаратного комплекса «Центр выработки ключей» (ЦВК).

VPN-туннели могут быть также образованы между ФПСУ-IP и пользователями комплексов «ФПСУ-IP/Клиент», защищающих межсетевое взаимодействие удаленных пользователей. Для формирования туннелей на ФПСУ-IP должны быть установлены общесистемные ключи доступа пользователей комплексов «ФПСУ-IP/Клиент», выработанные с помощью специальной программы «Центр генерации ключей клиентов» (ЦГКК).

В качестве критериев фильтрации пакетов передаваемых данных ФПСУ-IP позволяет задавать:

- IP-адреса отправителя и получателя;
- идентификационные данные клиентов;
- используемые протоколы транспортного и сетевого уровня;
- тип передаваемых данных, мобильный код, протоколы приложений;
- разрешенные режимы работы абонентов;
- разрешенные связи абонентов и маршрутизаторов по конкретным протоколам управления;
- разрешенные информационные взаимодействия абонентов (по пересекающейся совокупности параметров: протоколам, TCP/UDP-портам, интервалам времени дней недели и т.п.), приписанных к соответствующим правилам передачи трафика.

Помимо основных функций, в ФПСУ-IP реализован ряд дополнительных возможностей, в частности:

- возможность безопасного дистанционного контроля и управления работой из любого фрагмента IP-сетей, которая может быть предоставлена нескольким (максимально тридцати двум) зарегистрированным на ФПСУ-IP удаленным администраторам;
- использование технологии DPI (Deep Packet Inspection) для анализа содержимого передаваемых данных;
- встроенный HTTP- и SOCKS-proxy;
- возможность по заданным администратором критериям разделения общего потока посылаемых через VPN-туннель данных. Данные разделяются на несколько (от 1 до 128) различных потоков с целью поддержки соответствующих функций пограничных маршрутизаторов (например, функция установки приоритетов определенным типам IP трафика).

Для повышения надежности и обеспечения бесперебойной работы локальной сети в условиях возможных отказов аппаратуры, два ФПСУ-IP могут работать в режиме горячего резервирования. В режиме горячего резервирования оба ФПСУ-IP подключаются к локальной сети параллельно, с использованием концентраторов (hub) или коммутаторов

(switch) и соединяются между собой отдельной линией передачи данных, при этом обмен информации между ними происходит в защищенном режиме. На каждый момент времени один ФПСУ-IP является активным, выполняя все функциональные операции, а второй находится в резерве в режиме ожидания, периодически проверяя работоспособность первого. В случае отсутствия ответа от активного ФПСУ-IP, или при возникновении аппаратных неполадок на активном, резервный ФПСУ-IP в течение 3 секунд автоматически берет управление на себя. Передача функций резервному ФПСУ-IP может также осуществляться вручную, по команде оператора или удаленного администратора.

Для автоматического возобновления работы после сбоев электропитания (в отсутствие оператора), ФПСУ-IP укомплектован подсистемой автозапуска режима фильтрации.

Программное обеспечение ФПСУ-IP функционирует в собственной изолированной и функционально замкнутой операционной среде, ACCESS-TM SHELL. Среда осуществляет разграничение доступа к операционной системе ФПСУ-IP, защиту программных и информационных модулей на ПЗУ комплекса. ФПСУ-IP предлагает диалоговые средства для управления своей работой (настройки драйверов сетевого оборудования, задания правил фильтрации, установления правил идентификации и аутентификации доступа к операционной системе ФПСУ-IP, просмотра регистрационной информации и т.д.), а также для установки параметров работы.

Разграничение доступа допущенных лиц и контроль их полномочий при запуске ФПСУ-IP и управлении его работой осуществляется подсистемой ACCESS-TM SHELL по предъявляемым допущенными лицами электронным идентификаторам «touch-memory» (в качестве которых могут выступать устройства iButton DS1993 – DS1996, или микроэлектронные USB-устройства «TM-Key» производства ООО «АМИКОН») в соответствии с логическим разделением лиц ФПСУ-IP на две роли и пять условных классов, представленных в нижеследующей таблице:

Таблица 1. Роли и классы пользователей ФПСУ-IP

Роль/Класс	Разрешенные действия
Пользователь/ ***Без идентификации пользователя***	• переинициализация ПДСЧ; • отключение автозапуска.

Роль/Класс	Разрешенные действия
Пользователь/ Оператор	• запуск ФПСУ-IP; • остановка рабочего режима ФПСУ-IP; • просмотр, включение и отключение оповещений о нарушениях правил межсетевого экрана; • передача управления партнеру по горячему резервированию; • удаление текущего соединения из таблицы состояний соединений; • выключение питания ФПСУ-IP по кнопке «Power».
Администратор/ Инженер	Все права класса *Оператор* и дополнительно: • конфигурирование сетевых адаптеров; • конфигурирование IP-адресов портов ФПСУ-IP; • установка даты и времени; • контроль целостности исполняемых программных модулей ФПСУ-IP (только по хранящимся на ФПСУ-IP контрольным суммам с выводом результата на экран); • запуск процесса функционального самотестирования межсетевого экрана ФПСУ-IP; • сохранение текущей конфигурации ФПСУ-IP на USB-flash; • настройка общих параметров работы ФПСУ-IP (watchdog, аварийный перезапуск, переход на резервный, гашение экрана, запрет работы при сбоях жесткого диска, не сообщать об устаревших ключах, контроль сети); • просмотр регистрационной информации (статистики).
Администратор/ Администратор	Все права класса *Инженер* и дополнительно: • восстановление с USB-носителя и редактирование конфигурации ФПСУ-IP; • включение режима «Запрет открытых соединений» в общих параметрах работы ФПСУ-IP; • регистрация и предоставление полномочий на определенные действия удаленным администраторам; • регистрация ТМ-идентификаторов;

Роль/Класс	Разрешенные действия
	• настройка подсистемы автоматического старта; • установка пароля условно-постоянного действия на администрирование; • установка ключей парно-выборочной связи; • установка общесистемных ключей; • установка ключевых данных для реализации защищенного обмена в режиме горячего резервирования; • установка времени действия ключей; • контроль целостности исполняемых программных модулей ФПСУ-IP (без ограничений на варианты проверки); • установка изменений и дополнений к программным модулям ФПСУ-IP; • контроль целостности конфигурации ФПСУ-IP.
Администратор/ Главный администратор	Все права класса *Администратор* и дополнительно: • выдача на USB-носитель системного журнала статистики; • переустановка программного обеспечения ФПСУ-IP со специального средства восстановления (USB-носителя).

Программное обеспечение ФПСУ-IP разработано ООО «АМИКОН» (Лицензия Федеральной службы безопасности Российской Федерации ЛСЗ № 0000055 рег. № 12253 Н от 08 июня 2012 года на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем. Лицензии Федеральной службы по техническому и экспортному контролю №0307 от 21 ноября 2006 г., №0536 от 21 ноября 2006 г: на деятельность по разработке и(или) производству средств защиты конфиденциальной информации; на деятельность по технической защите конфиденциальной информации) и ООО Фирма «ИнфоКрипт» (Лицензия Федеральной службы безопасности Российской Федерации № 4846 П от 06 декабря 2007 года на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем).

ФПСУ-IP является средством криптографической защиты информации «Программно-аппаратный комплекс шифрования «ФПСУ-IP» (изделие Криптомаршрутизатор),

поставляемым в соответствии с формуляром на изделие «Средство криптографической защиты информации «Программно-аппаратный комплекс шифрования «ФПСУ-IP».

ФПСУ-IP следует использовать в соответствии с документом «Правила пользования» изделия «Средство криптографической защиты информации «Программно-аппаратный комплекс шифрования «ФПСУ-IP».

СКЗИ «Программно-аппаратный комплекс шифрования «ФПСУ-IP» разработано ООО Фирма «ИнфоКрипт», имеет сертификат соответствия требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1, КС2 и КС3.

3. Процедуры приемки и безопасной установки

3. 1. Общий порядок поставки

Комплектность поставки ФПСУ-IP указывается в паспорте на изделие.

Перед инсталляцией и началом эксплуатации должна быть выполнена проверка совпадения контрольных сумм файлов дистрибутива с эталонными.

3. 2. Организационные условия эксплуатации

Перед эксплуатацией ФПСУ-IP должно быть обеспечено обязательное выполнение следующих условий эксплуатации:

a) наличие администратора безопасности, отвечающего за правильную эксплуатацию ФПСУ-IP, в том числе:
   - предотвращение несанкционированного доступа к идентификаторам и паролям привилегированных пользователей (администратора безопасности);
   - обеспечение сохранности оборудования и физической целостности ФПСУ-IP;
   - ежедневную проверку программной среды ПЭВМ, использующейся в качестве административной консоли, на наличие вредоносного программного обеспечения;
   - периодический контроль (не реже одного раза в месяц) целостности неизменяемых установленных файлов ФПСУ-IP;
   - периодическое тестирование функций защиты ФПСУ-IP администратором информационной безопасности не реже одного раза в год;

b) администратор безопасности должен провести проверку ФПСУ-IP на отсутствие уязвимостей, а в случае обнаружения уязвимостей необходимо сообщить в службу технической поддержки производителя;

c) администратор безопасности должен проверить информационный ресурс предприятия – производителя (https://www.amicon.ru) на предмет наличия информации, связанной с выпуском обновлений ФПСУ-IP;

d) каналы передачи данных (включая каналы управления), используемые ФПСУ-IP, должны быть либо расположены в пределах контролируемой зоны и защищены с использованием организационно-технических мер, либо, в случае их выхода за пределы контролируемой зоны, должны быть защищены путем применения средств криптографической защиты информации, сертифицированных в системе сертификации ФСБ России;

e) для программ среды функционирования ФПСУ-IP должны быть установлены все актуальные обновления, выпущенные разработчиками данных программ, а также выполнены рекомендации разработчиков по безопасному конфигурированию, направленные на исключение возможности эксплуатации уязвимостей для реализации угроз безопасности информации;

f) должны достигаться цели безопасности для среды функционирования, указанные в разделе 3.1 задания по безопасности ПЕРС.26.20.40.140.0033Б (см. пункт «Выполнение целей безопасности для среды функционирования»);

g) исключить возможность использования ФПСУ-IP для обработки информации, содержащей сведения, составляющие государственную тайну;

h) наличие организационных и технических мер, направленных на исключение несанкционированного доступа к объектам ОС и СУБД, необходимых для функционирования ФПСУ-IP.

3. 3. Требования к среде функционирования

К аппаратному и программному обеспечению, которые используются для установки ПАК «ФПСУ-IP», предъявляются минимальные требования, изложенные в таблице:

Таблица 2. Требования к среде функционирования ФПСУ-IP

Элемент среды функционирования	Параметры
Консоль управления	ПО консоли управления: Putty 0.70 ОС консоли управления и для ПО записи дистрибутива ПАК «ФПСУ-IP» на USB: Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10. Вычислительная платформа общего назначения: в соответствии с требованиями операционной системы.
ТМ-идентификатор	Физическим носителем ТМ-идентификатора должно являться: Микроэлектронное устройство контактной памяти iButton

Элемент среды функционирования	Параметры
	DS-1993 (Dallas Semiconductor) или Микроэлектронное USB-устройство «TM-Key» ПЕРС.466226.004 (ООО «АМИКОН»).

3. 4. Выполнение целей безопасности для среды функционирования

1. Обеспечение доверенного канала

Каналы передачи данных (включая каналы управления), используемые ФПСУ-IP, должны быть либо расположены в пределах контролируемой зоны и защищены с использованием организационно-технических мер, либо, в случае их выхода за пределы контролируемой зоны, должны быть защищены путем применения средств криптографической защиты информации, сертифицированных в системе сертификации ФСБ России.

2. Обеспечение доверенного маршрута

Каналы управления, используемые администраторами безопасности для взаимодействия с ФПСУ-IP, должны быть либо расположены в пределах контролируемой зоны и защищены с использованием организационно-технических мер, либо, в случае их выхода за пределы контролируемой зоны, должны быть защищены путем применения средств криптографической защиты информации, сертифицированных в системе сертификации ФСБ России.

3. Обеспечение условий безопасного функционирования

Администратор безопасности должен проверять отсутствие каналов связи защищаемой автоматизированной системы управления с иными автоматизированными (информационными) системами в обход ФПСУ-IP.

4. Физическая защита

Администратор безопасности должен проверить, что аппаратные средства ФПСУ-IP

и терминалов, с которых выполняется его управление, расположены в пределах контролируемой зоны.

5. Взаимодействие с доверенными продуктами информационных технологий

Администратор безопасности должен проверить, что средства защиты информации (средства обнаружения вторжений), от которых ФПСУ-IP получает управляющие сигналы, сертифицированы на соответствие требованиям безопасности информации не ниже 4 класса защиты.

6. Эксплуатация ФПСУ-IP

Администратор безопасности должен проверить, что установка, конфигурирование и управление объектом оценки выполняется в соответствии с эксплуатационной документацией.

7. Требования к персоналу

Администратор безопасности должен убедиться, что персонал, ответственный за функционирование объекта оценки, обеспечивает надлежащее функционирование объекта оценки, руководствуясь эксплуатационной документацией.

8. Поддержка аудита

Администратор безопасности должен убедиться, что обеспечена поддержка средств аудита, используемых в ФПСУ-IP.

9. Совместимость компонентов ФПСУ-IP с компонентами средств вычислительной техники

Администратор безопасности должен убедиться, что обеспечены совместимость компонентов ФПСУ-IP с компонентами средств вычислительной техники информационной системы, а также выделены необходимые ресурсы для выполнения функций безопасности ФПСУ-IP (в том числе изоляция данных и процессов ФПСУ-IP от иных данных и процессов средства вычислительной техники, на котором он функционирует).

10. Доверенная среда функционирования

Администратор безопасности должен убедиться, что обеспечено функционирование ФПСУ-IP в среде, сертифицированной на соответствие требованиям безопасности информации по соответствующему классу защиты операционной системы, или в среде, защищенной путем принятия мер защиты информации, соответствующих классу защищенности информационной системы (автоматизированной системы управления), для

использования в которой предназначается ФПСУ-IP.

11. Тестирование и контроль целостности среды функционирования

Администратор безопасности должен убедиться, что обеспечены тестирование и контроль целостности аппаратных средств, а также программного обеспечения базовой системы ввода-вывода, загрузчика и операционной системы ФПСУ-IP.

12. Исключение недоверенных компонентов

Администратор безопасности должен убедиться, что ФПСУ-IP не был интегрирован в другое программно-техническое средство.

3. 5. Указания для полного или частичного устранения идентифицированных скрытых каналов

В разделе приведены требования для среды функционирования средства с целью ограничения, мониторинга, полного или частичного устранения идентифицированных скрытых каналов, которые могут возникнуть в информационных (автоматизированных) системах вследствие использования в них средства.

Под скрытым каналом (covert channel) понимается непредусмотренный разработчиком коммуникационный канал, который может быть применен для нарушения политик безопасности в среде информационных технологий.

С помощью скрытых каналов могут быть реализованы следующие нарушения политик безопасности:

- угроза внедрения вредоносных программ и данных;
- угроза подачи нарушителем команд агентом для выполнения его функций;
- угроза утечки криптографических ключей, паролей (несанкционированный доступ к ним) или отдельных информационных объектов.

В результате проведенного анализа возможных скрытых каналов по памяти с использованием стека протоколов TCP/IP были идентифицированы следующие возможные наиболее опасные виды скрытых каналов передачи данных по памяти:

- ISN Evaluation (оценка TCP Initial Sequence Number);
- TCP URG Pointer (указатель TCP URG);
- IP ToS Evaluation (оценка IP-ToS).

Указания для полного или частичного устранения идентифицированных скрытых каналов приводятся в подпунктах ниже.

3. 5. 1. ISN Evaluation

Для предотвращения атаки по скрытому каналу ISN Evaluation необходимо использовать SOCKS прокси (подробнее о настройках прокси см. пункт «Http-proxy ФПСУ-IP»):

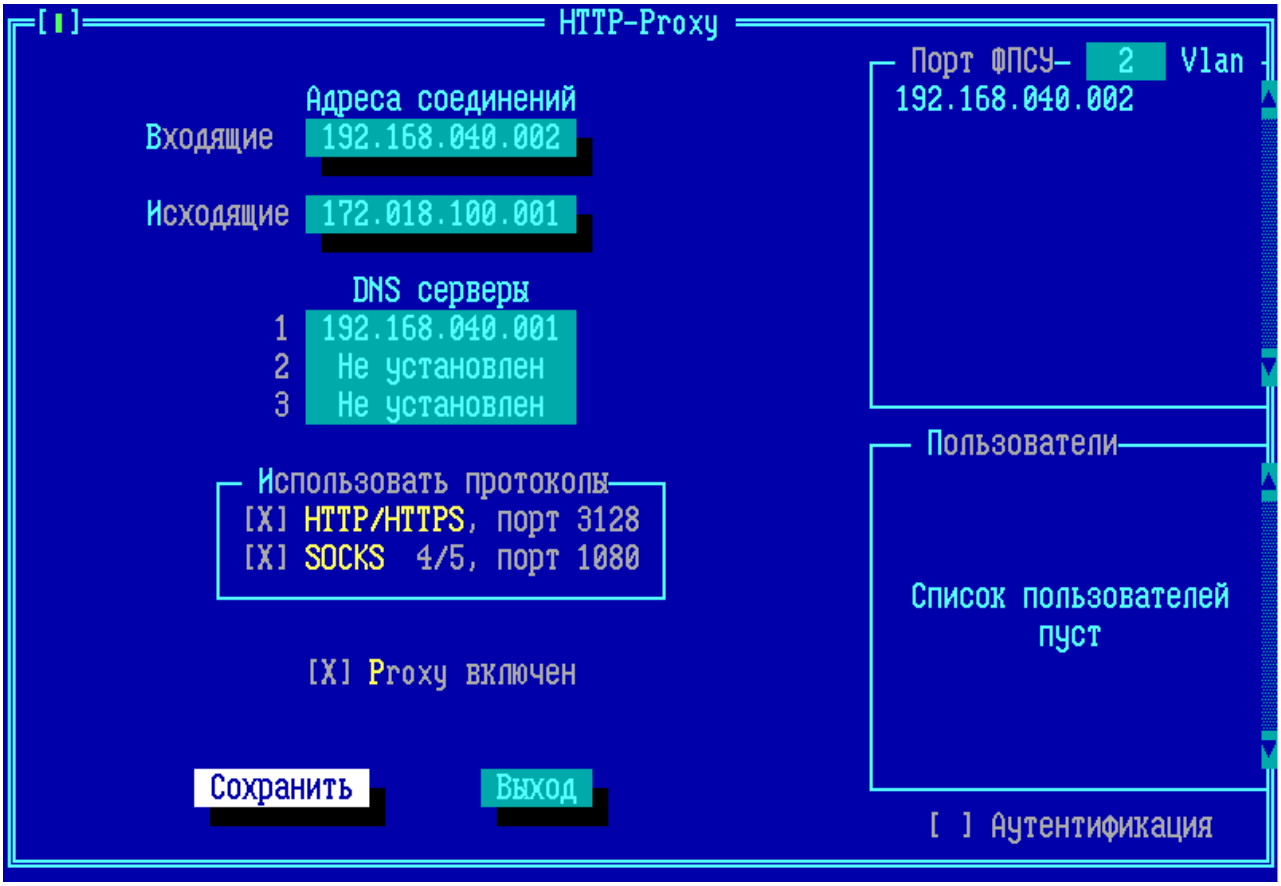


Рисунок 1 - Настройки Proxy

3. 5. 2. TCP URG Pointer

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

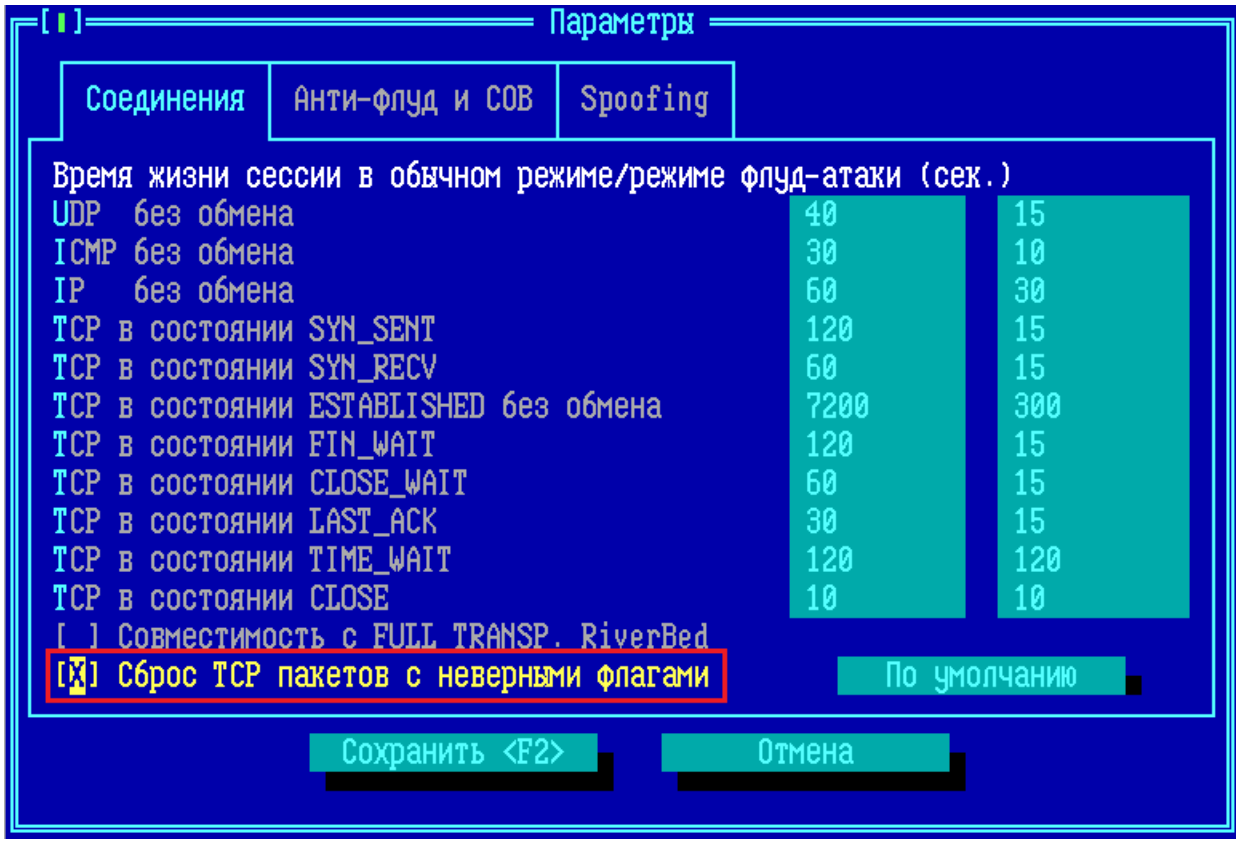


Рисунок 2 - Настройки правил соединения и фильтрации

3. 5. 3. IP ToS Evaluation

В IP-заголовке имеются редко используемые биты – TOS (Type of Service – Тип обслуживания).

Эти биты задают способ обслуживания пакета: «Minimum Delay» (минимальная задержка), «Maximum Throughput» (максимальная пропускная способность), «Maximum Reliability» (максимальная надежность) и «Minimum Cost» (минимальная стоимость канала). Одновременно может быть установлен только один из этих битов.

Как правило, флаг «Minimum Delay» устанавливается в пакетах для telnet и ftp-control, а в пакетах ftp-data – «Maximum Throughput». В ОО необходимо настроить соответствующий способ обслуживания. Также следует разрешить главные типы ICMP протокола (0, 3, 4, 11, 12).

Типы ICMP-сообщений:
0 – echo reply (echo-ответ, пинг);
3 – destination unreachable (адресат недосягаем);
4 – source quench (подавление источника, просьба посылать пакеты медленнее);

11 – time-to-live exceeded (истечение срока жизни пакета);
12 – IP header bad (неправильный заголовок IP-пакета).

Пропускная способность скрытого канала:
1 байт на IP-датаграмму при использовании всего поля ToS;
1 бит на IP-датаграмму, если используется только бит задержки.

Для включения запрещающего правила в ФПСУ-IP необходимо:

Добавить несколько следующих служб протокола RAW (см. раздел «Службы») и включить их в правило трафика с запрещающим основным действием (Drop или Reject):

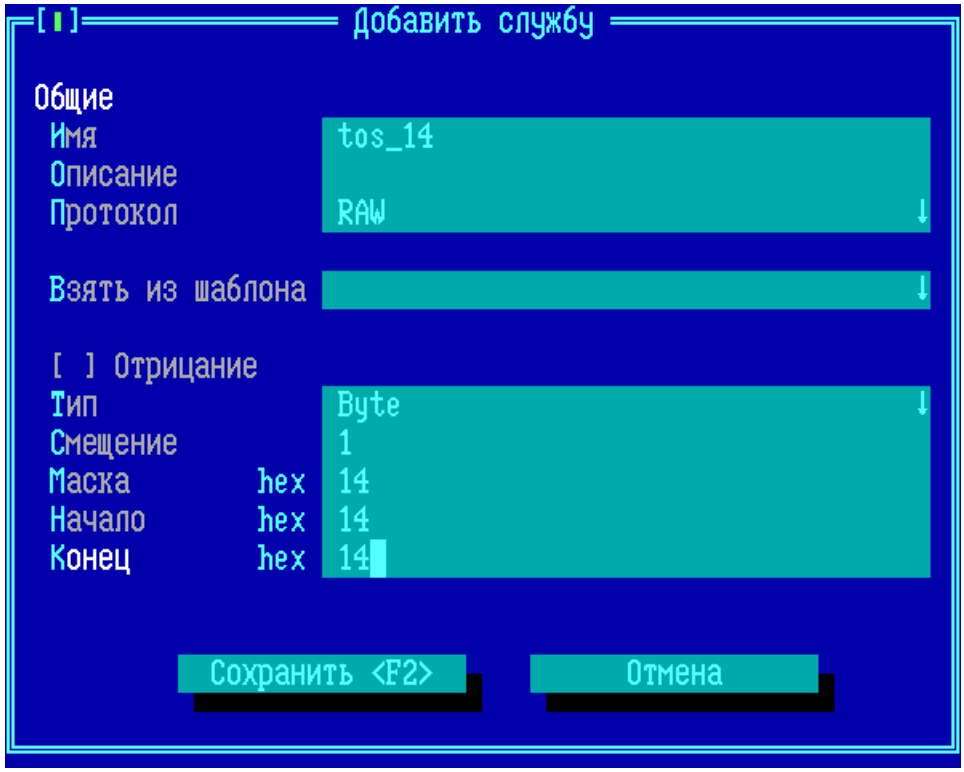


Рисунок 3 - Добавление службы RAW

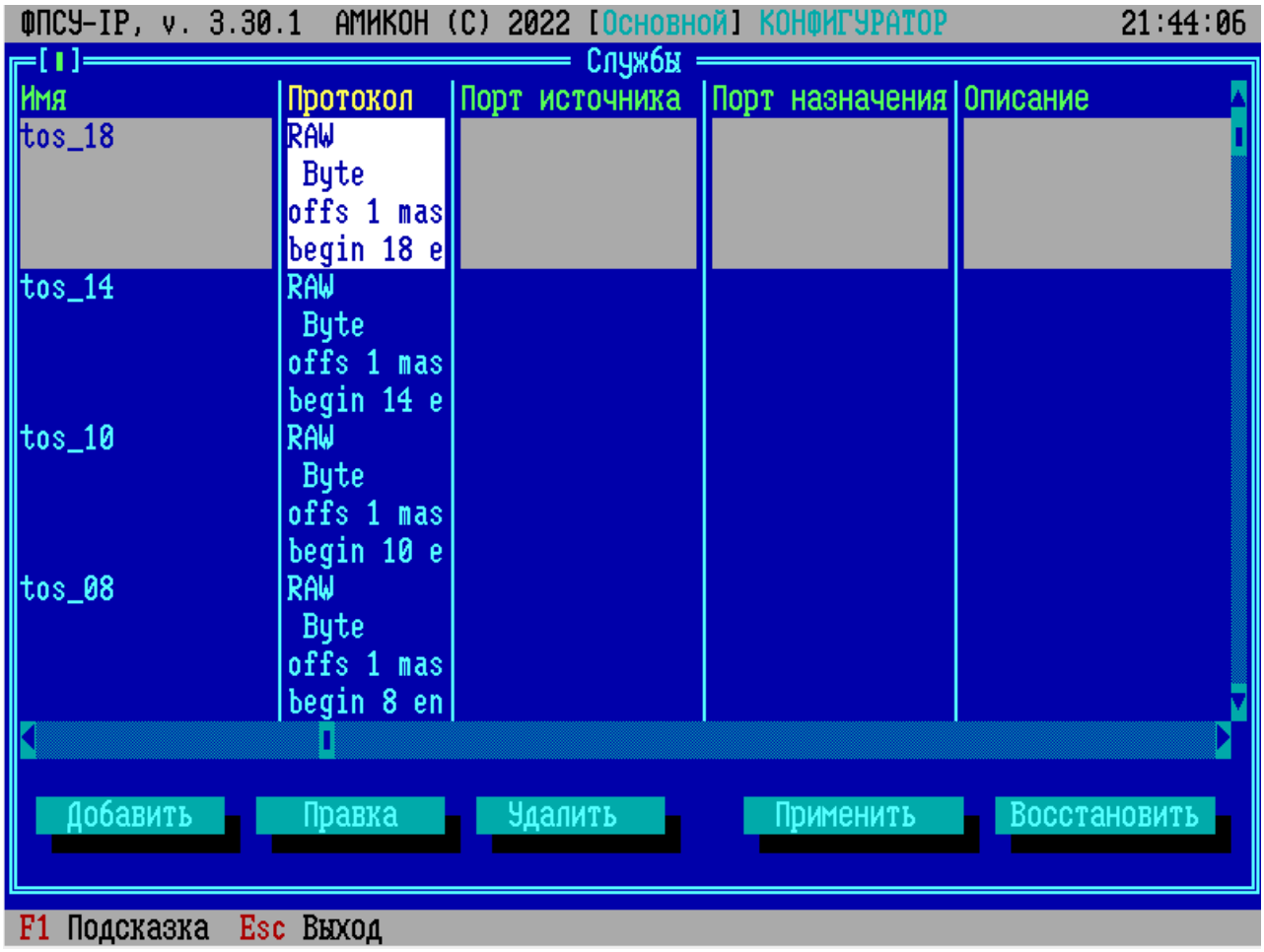


Рисунок 4 - Служба добавлена

Выбрать заранее созданный шаблон фильтра фрагментированных IP-пакетов. («Службы в правилах фильтрации трафика по содержимому»).

При необходимости изменить правило трафика:

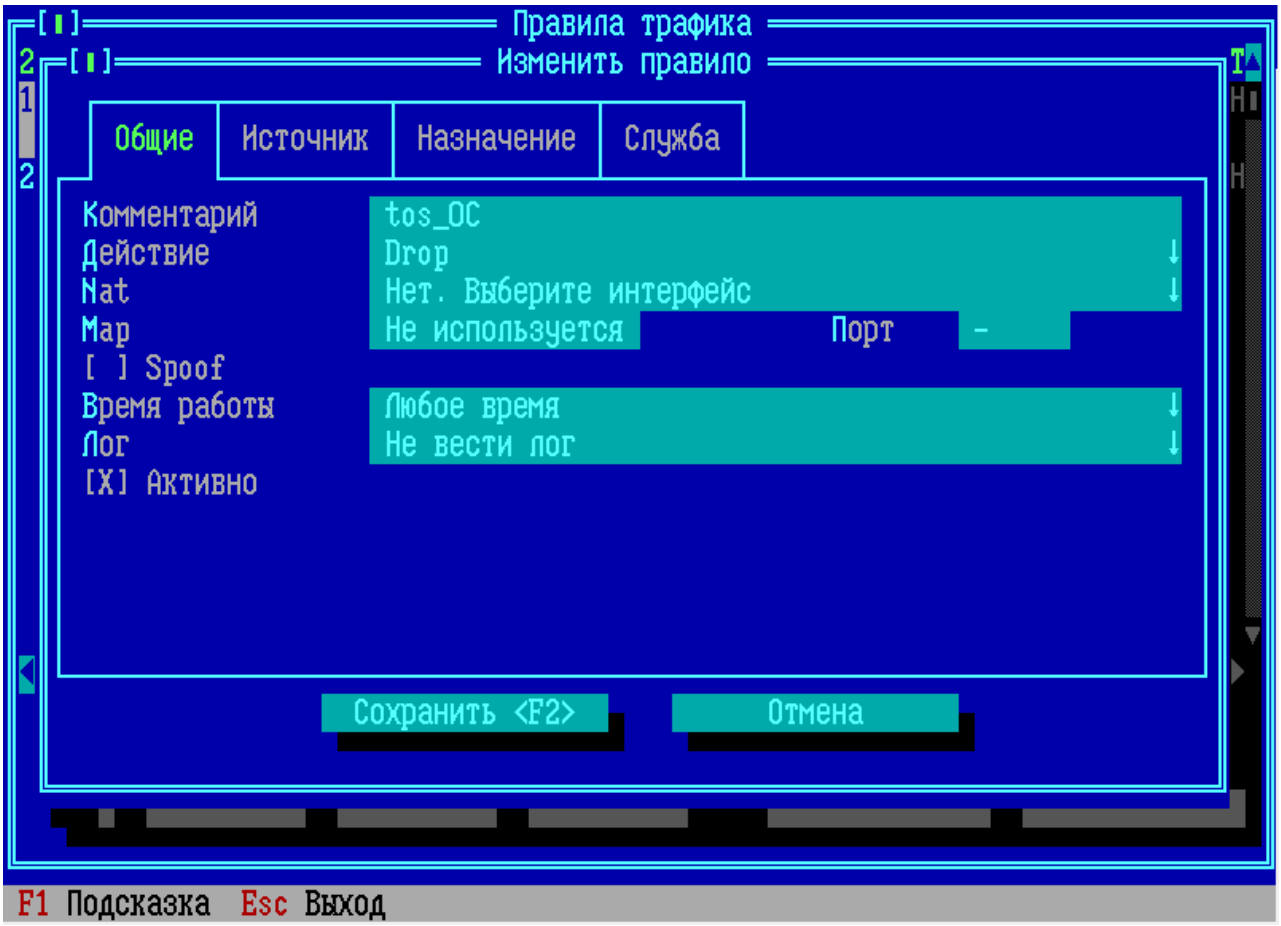


Рисунок 5 - Изменение общих свойств правила

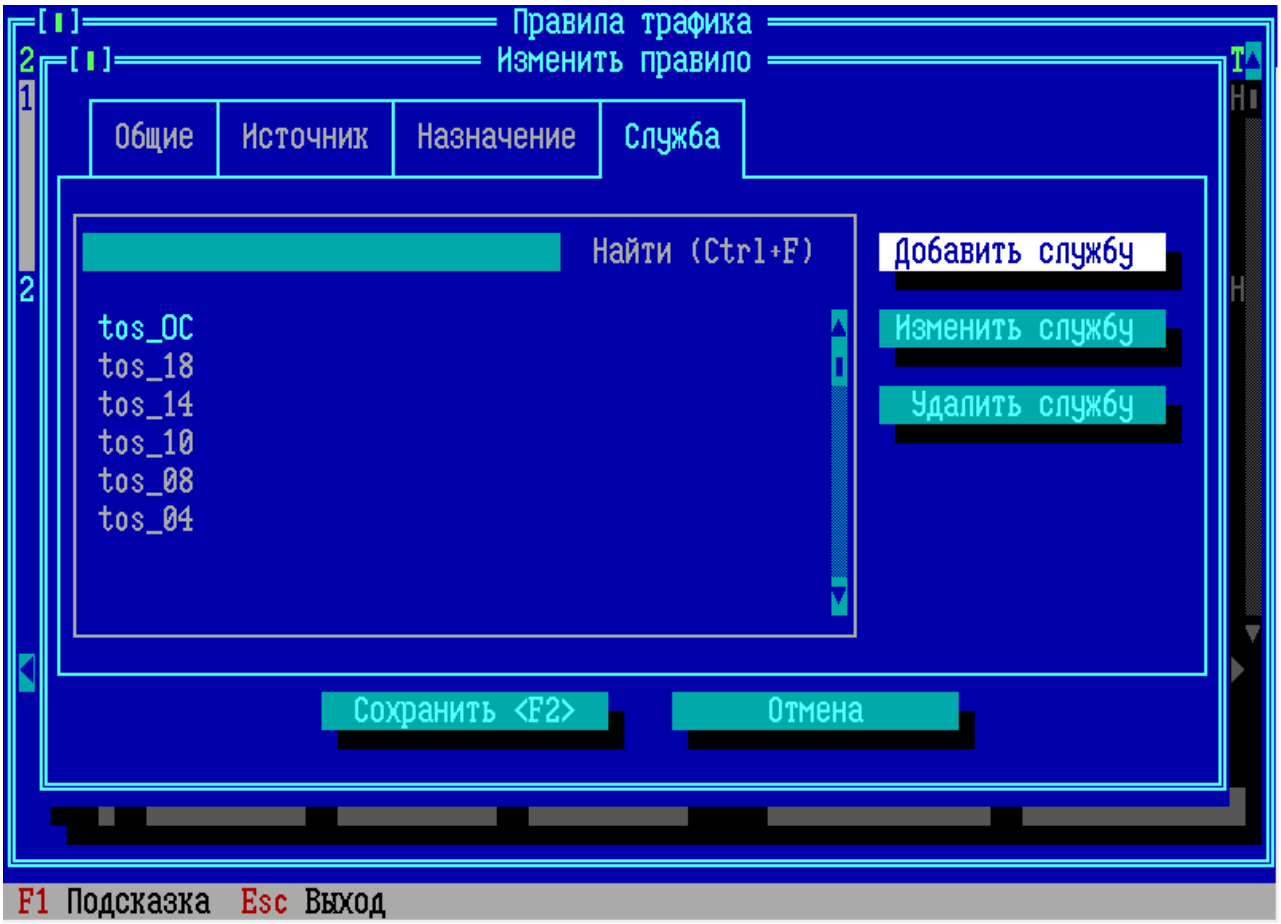


Рисунок 6 - Работа со службами

3. 6. Технические условия эксплуатации и хранения

Электропитание основных технических средств комплекса должно осуществляться от источников гарантированного питания, обеспечивающих автоматический переход на резервные источники при выходе из строя основной энергосистемы, а также фильтрацию от электропомех питающей сети. Напряжение в сети переменного тока должно быть 220 В ± 10%, частота тока 50 Гц ± 1%, качество электрической энергии должно соответствовать ГОСТ 32144-2013.

Запрещается эксплуатация основных технических средств комплекса с неисправным шнуром питания, использование поврежденных розеток, сетевых фильтров и адаптеров.

Аппаратные средства комплекса должны размещаться в охраняемых помещениях с ограниченным доступом.

Аппаратная часть программно-аппаратного комплекса ФПСУ-IP по воздействию климатических факторов относится к 1 группе стойкости к воздействию внешних

климатических факторов в процессе эксплуатации согласно ГОСТ 21552-84, и предназначена для установки в отапливаемых помещениях и эксплуатации в условиях круглосуточной или сменной работы с перерывами на техническое обслуживание в соответствии с регламентом.

Нормальными климатическими условиями эксплуатации аппаратной части комплекса являются:

- температура окружающего воздуха - 20°(±15°) С;
- относительная влажность окружающего воздуха - 60 (±15)%;
- атмосферное давление - от 84 до 107 кПа (630–800 мм рт. ст.);
- запыленность воздуха - не более 0,75 мг/м³;
- в воздухе не должно быть агрессивных примесей (паров кислот и щелочей), вызывающих коррозию.

Допускается эксплуатация ФПСУ-IP в отличных от нормальных климатических условиях. Допустимые отличия указываются в паспорте на поставляемое изделие.

Условия хранения

До ввода в эксплуатацию аппаратные средства комплекса должны храниться в отапливаемых помещениях при температуре воздуха от 5°С до 40°С и относительной влажности не более 80%.

В помещениях для хранения не должно быть агрессивных примесей (паров кислот и щелочей), вызывающих коррозию.

3. 7. Настройки платформ виртуализации

3. 7. 1. Настройка виртуальной машины QEMU/KVM

Подготовка виртуальной машины QEMU/KVM для развертывания ФПСУ-IP.

Поддерживаемые версии: QEMU 4.0.1, QEMU 6.0, QEMU 6.1, QEMU 6.2.

В операционной системе семейства Linux должна быть установлена программа эмуляции аппаратной платформы QEMU. Для использования аппаратной виртуализации KVM необходимо:

- установить библиотеки и ПО;
- настроить доступ к управлению виртуальной машиной;
- создать виртуальную машину с гостевой операционной системой ФПСУ-IP;
- настроить сетевые интерфейсы и другие устройства.

Далее приводится пример установки ФПСУ-IP в QEMU/KVM 4.2.1 на Ubuntu 20.04.05 LTS.

1. Необходимо проверить, поддерживаются ли рабочей станцией необходимые расширения виртуализации для KVM. Для процессоров Intel должна поддерживаться технология Intel VT, для процессоров AMD – AMD SVM. Введите команду в терминале:

```
kvm-ok
```

Если виртуализация поддерживается и включена в BIOS/UEFI, на экран будет выдано сообщение о возможности использовать KVM.

```
INFO: /dev/kvm exists
KVM acceleration can be used
```

В случае, если в сообщении указано что ускорение KVM не может быть использовано, а процессор поддерживает виртуализацию, проверьте, что аппаратная виртуализация включена в BIOS/UEFI материнской платы компьютера.

Если процессор не поддерживает аппаратную виртуализацию, в выводе команды терминала будет возвращено значение 0.

```
egrep -c '(vmx | svm)' /proc/cpuinfo
```

2. В качестве интерфейса к различным технологиям виртуализации используется библиотека libvirt. Перед установкой пакетов рекомендуется обновить список 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 QEMU/KVM, vfpsu1, выполнив команду в терминале:

```
sudo virt-install --name vfpsu1 --memory 2048 --disk disk.qcow2,size=1 --boot uefi
```

Параметр size=1 следует убрать, если используется готовый образ диска на USB-носителе.

Настройка QEMU/KVM отличается для двух вариантов установки ФПСУ-IP - с установочного носителя и с готового образа диска.

Настройка QEMU/KVM для установки ФПСУ-IP с готового образа диска приведена в пунктах 6 - 11.

Настройка QEMU/KVM для установки ФПСУ-IP с установочного носителя приведена в пунктах 12 - 18.

Настройка QEMU/KVM для установки ФПСУ-IP с готового образа диска

6. При создании виртуальной машины необходимо добавить в список оборудования USB Disk 2.0 и TM-Key:

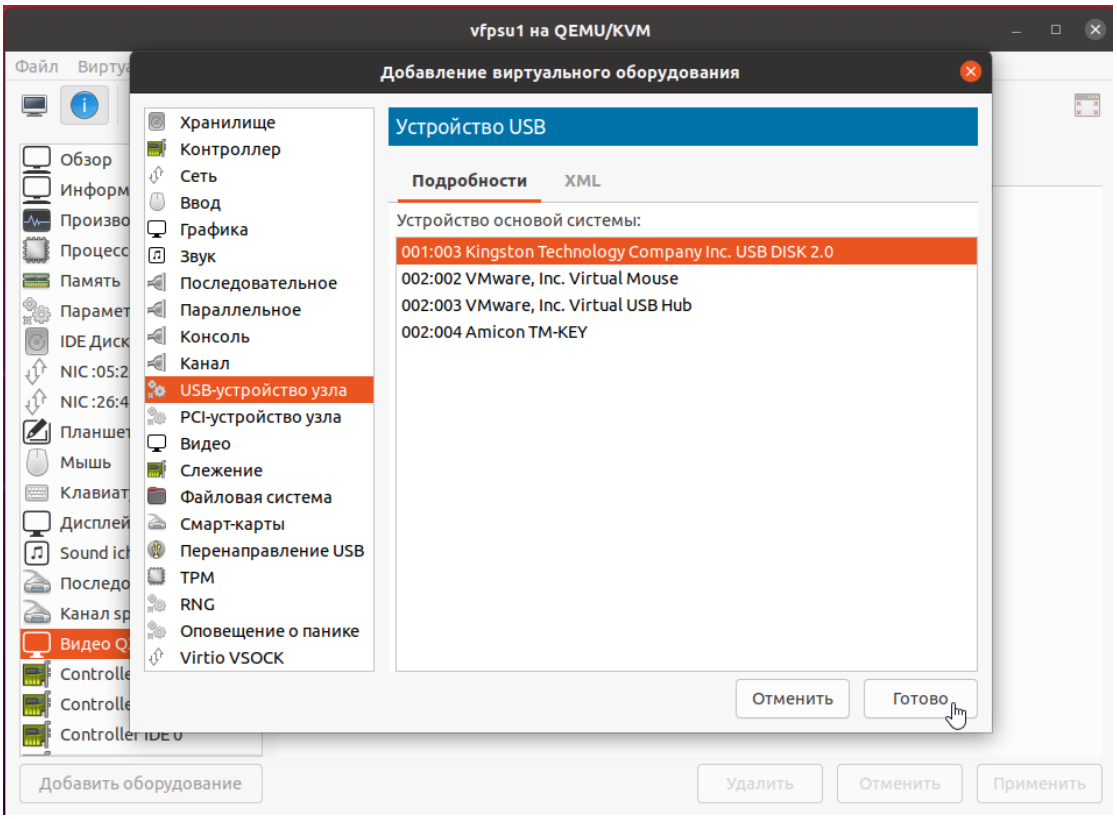


Рисунок 7 - Добавление оборудования

ВНИМАНИЕ! Виртуальная машина должна быть выключена.

7. Добавить второй сетевой интерфейс.

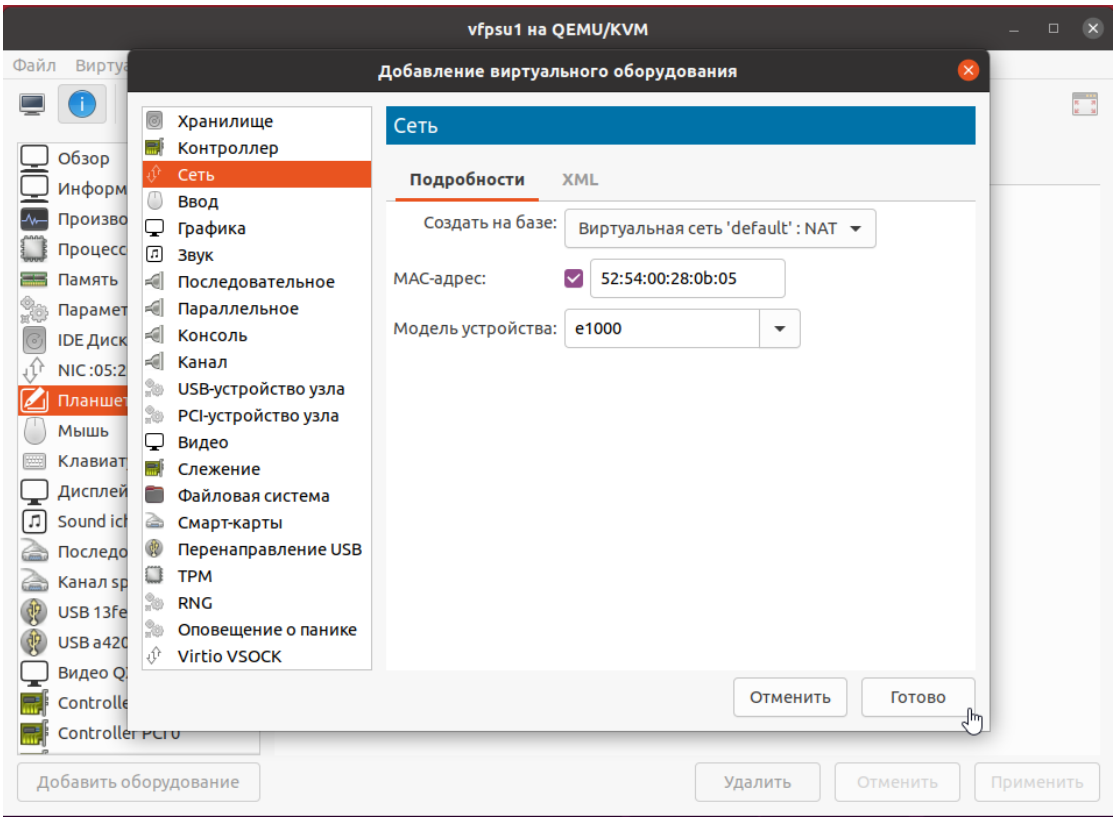


Рисунок 8 - Добавление сетевого интерфейса

8. В настройках процессоров виртуальной машины установите флаг «Копировать конфигурацию ЦП хоста».

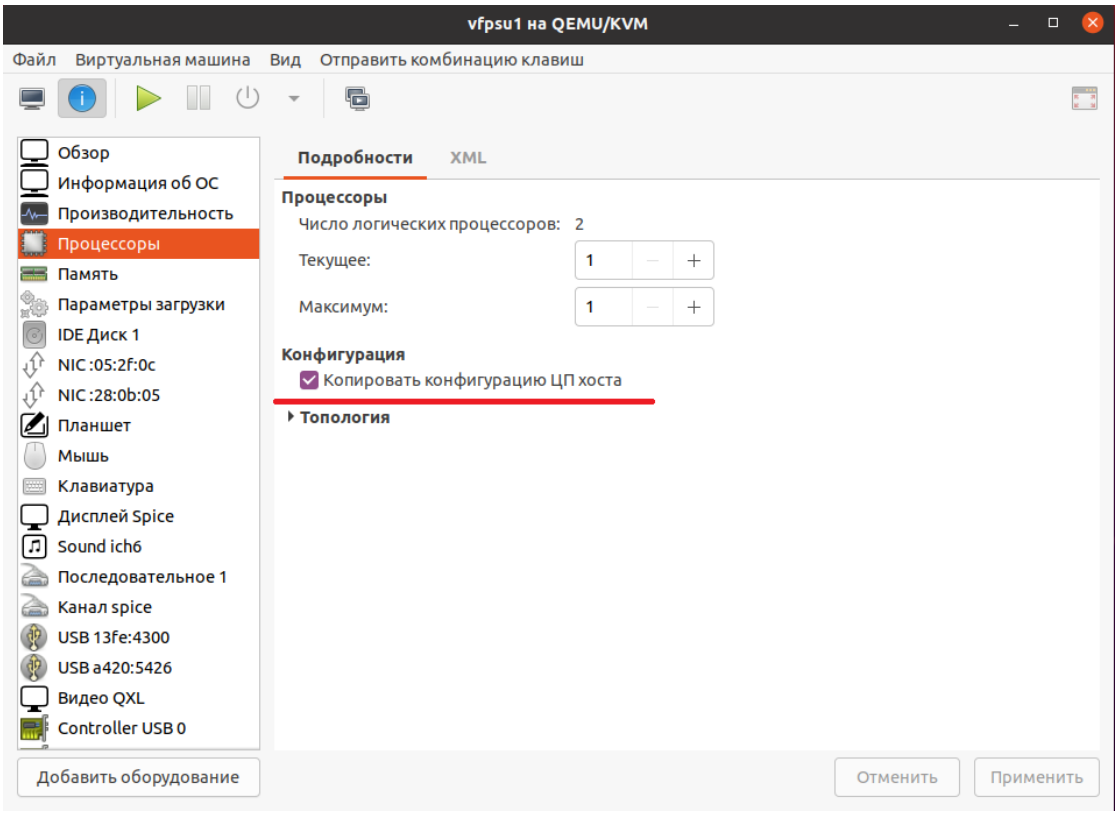


Рисунок 9 - Процессоры

9. В параметрах загрузки виртуальной машины необходимо изменить порядок загрузки дисков, чтобы у USB-носителя с инсталляционным комплектом ФПСУ-IP приоритет был выше. Как показано на рисунке USB-носитель с инсталляционным комплектом ФПСУ-IP будет загружаться первым, отмечен флагом.

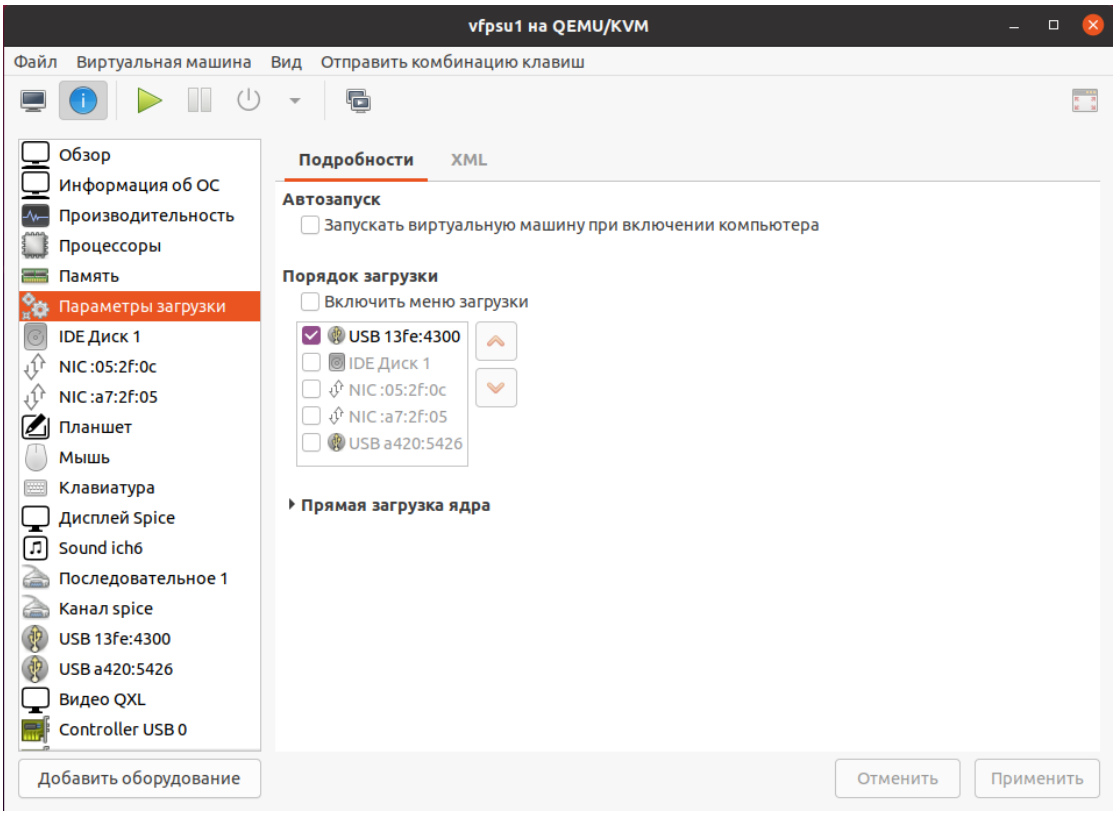


Рисунок 10 - Изменение порядка загрузки дисков

10. Дальнейшие действия по установке ФПСУ-IP с готового образа диска приводятся в пункте «Установка ФПСУ-IP с готового образа диска на USB-носителе в QEMU/KVM».

11. В параметрах загрузки виртуальной машины необходимо вернуть первоначальный порядок загрузки дисков (был изменен в пункте 9).

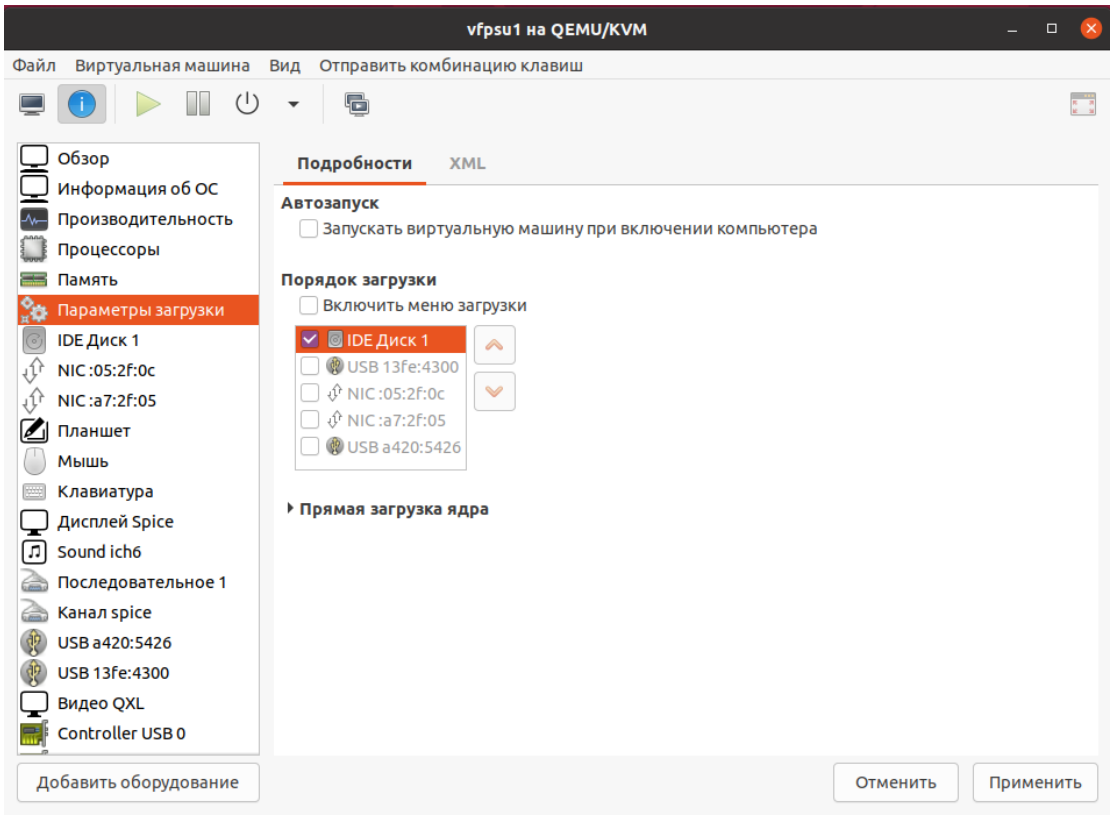


Рисунок 11 - Изменение порядка загрузки дисков

Настройка QEMU/KVM для установки ФПСУ-IP с установочного носителя

12. Виртуальная машина создается с одним сетевым интерфейсом (по умолчанию). Необходимо добавить ещё один сетевой интерфейс командой:

```
virsh attach-interface vfpsu1 --type network --source default --persistent --model e1000
```

или

```
attach-interface vfpsu1 --type bridge --source bridge0 --persistent
```

Второй сетевой интерфейс также может быть добавлен из графического интерфейса виртуальной машины.

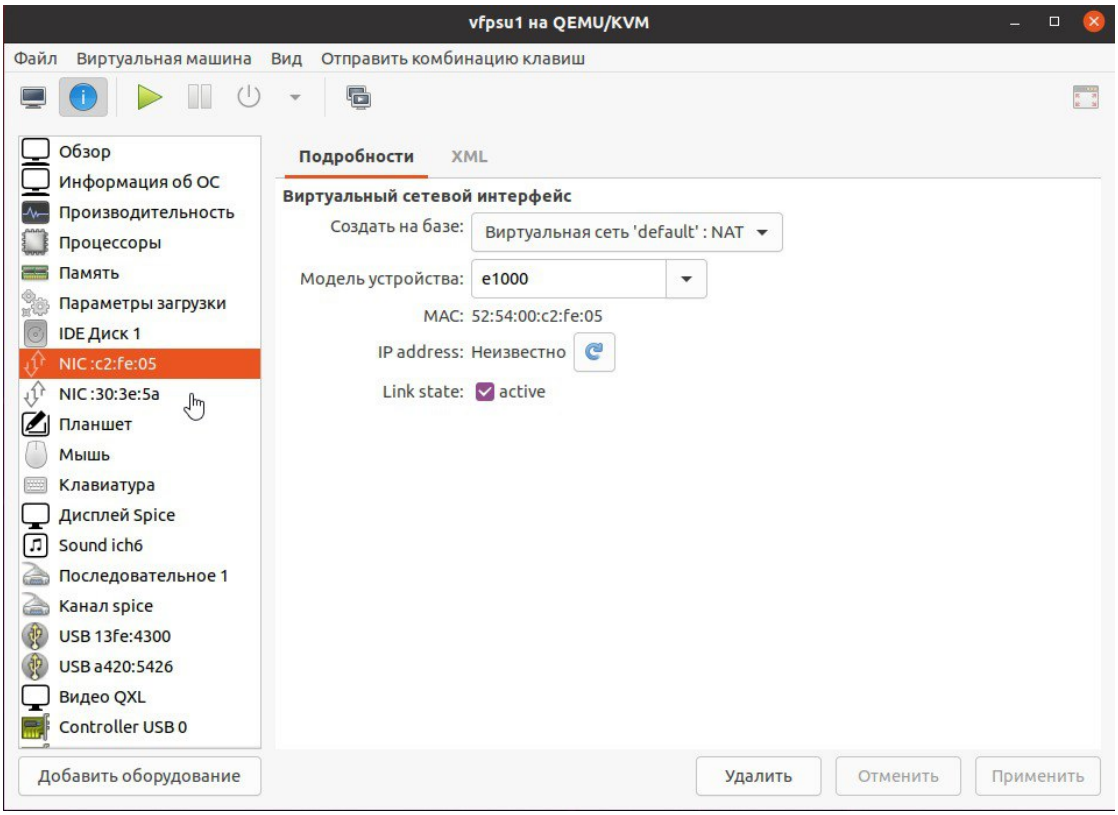


Рисунок 12 - Добавление сетевого интерфейса

13. Параметры виртуальной машины настраиваются в конфигурационном файле. Чтобы открыть для редактирования конфигурационный файл виртуальной машины vfpsu1, введите в терминале:

```
virsh edit vfpsu1
```

Откроется редактор с файлом конфигурации виртуальной машины vfpsu1.

14. В файле найдите раздел <interface> с параметрами сетевых интерфейсов и измените их в зависимости от настроек реальных сетевых адаптеров сервера, на котором запускается виртуальная машина, если это требуется. Для примера приведено описание сетевого адаптера в файле конфигурации виртуальной машины vfpsu1.

```
<interface type='bridge'>
  <mac address='52:54:00:8c:9e:22'/>
  <source bridge='bridge0'/>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
</interface>
```

15. Если в качестве дисплея используется дисплей по умолчанию, но при этом QEMU работает некорректно, рекомендуется использовать в качестве дисплея только устройство

Cirrus SVGA, проверьте следующие настройки в конфигурационном файле виртуальной машины в разделе <model>.

```
<model type='cirrus'/>
```

16. Добавьте в конфигурационный файл в список оборудования USB Disk 2.0 и USB-устройство ТМ (ТМ-считыватель или ТМ-Key). Подробные инструкции приведены в пункте «Добавление USB-устройств в QEMU/KVM».

17. Для управления виртуальной машиной могут быть использованы различные утилиты. В примере используется рекомендуемый пакет virt-manager, который содержит утилиту с графическим интерфейсом для управления локальными и удаленными виртуальными машинами. Данный пакет был установлен в пункте 2.

Пакет virt-manager требует наличия графической среды, рекомендуется ее устанавливать на рабочую станцию или тестовую машину, а не на рабочий сервер. Для подключения к локальному сервису libvirt введите:

```
virt-manager -c qemu:///system
```

18. После добавления в конфигурационный файл виртуальной машины USB-носителя с инсталляционным комплектом ФПСУ-IP поменяйте порядок загрузки, установив загрузку с USB-носителя (действие аналогичное п. 9), и проведите установку ПО. Описание процедуры установки ПО ФПСУ-IP находится в разделе «Установка ПО ФПСУ-IP с установочного носителя». После процедуры установки и первоначальной настройки (см. пункт «Технологический режим ФПСУ-IP») поменяйте обратно порядок загрузки, установив загрузку с диска (действие аналогичное п. 11).

Создание виртуальной машины закончено.

Для запуска ФПСУ-IP в QEMU/KVM введите команду:

```
virsh start vfpsu1
```

На экране отобразится главное меню ФПСУ-IP.

3. 7. 1. 1. Добавление USB-устройств в QEMU/KVM

Для того,чтобы подключить USB-устройства реального хоста в виртуальную машину QEMU/KVM добавьте в конфигурационный файл в список оборудования USB Disk 2.0 и USB-устройство ТМ (ТМ-считыватель или ТМ-Key).

Добавление USB Disk 2.0

Для добавления в конфигурационный файл виртуальной машины в список

оборудования USB Disk 2.0 выполните следующие действия:

1. Подключите USB-носитель с инсталляционным комплектом ФПСУ-IP. Для вывода подключенных USB-устройств введите команду в терминале:

```
lsusb
```

Команда выводит информацию о USB-шинах и подключенных к ним устройствах. Каждое из устройств имеет пару 16-битных идентификаторов: идентификатор производителя (Vendor ID) и идентификатор устройства (Device ID), которые следует использовать для идентификации устройств.

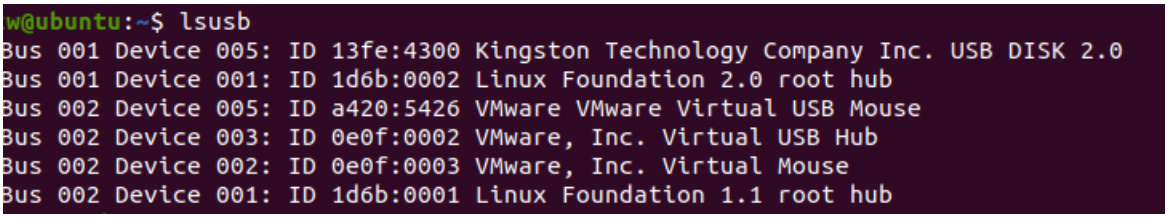


Рисунок 13 - Подключенные USB-устройства

2. Для добавления в конфигурационный файл виртуальной машины USB Disk 2.0, создайте файл /etc/libvirt/qemu/usb1.xml с описанием устройства (укажите параметры Vendor ID, Device ID).

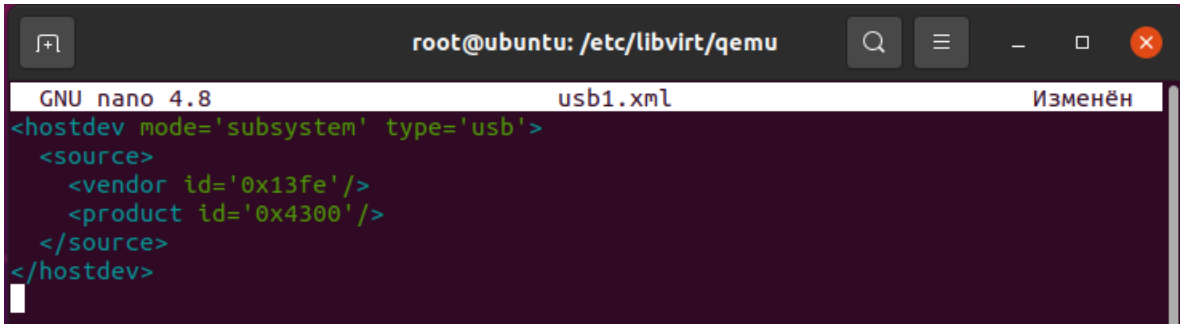


Рисунок 14 - Создание файла с описанием USB-устройства

3. Для проброса USB-устройства с хост-машины в гостевую ОС, виртуальную машину vfpsu1, введите команду в терминале:

```
virsh attach-device vfpsu1 usb1.xml
```

4. Обновите конфигурационный файл виртуальной машины vfpsu1. Введите команду в терминале:

```
virsh dumpxml vfpsu1 > vfpsu1.xml
virsh define vfpsu1.xml
```

Файл конфигурации виртуальной машины будет выведен в файл формата XML. Затем для виртуальной машины vfpsu1 будет переопределен файл конфигурации.

5. Откройте конфигурационный файл и убедитесь, что USB-устройство успешно вмонтировано в виртуальную машину, выполните команду в терминале:

```
virsh edit vfpsu1
```

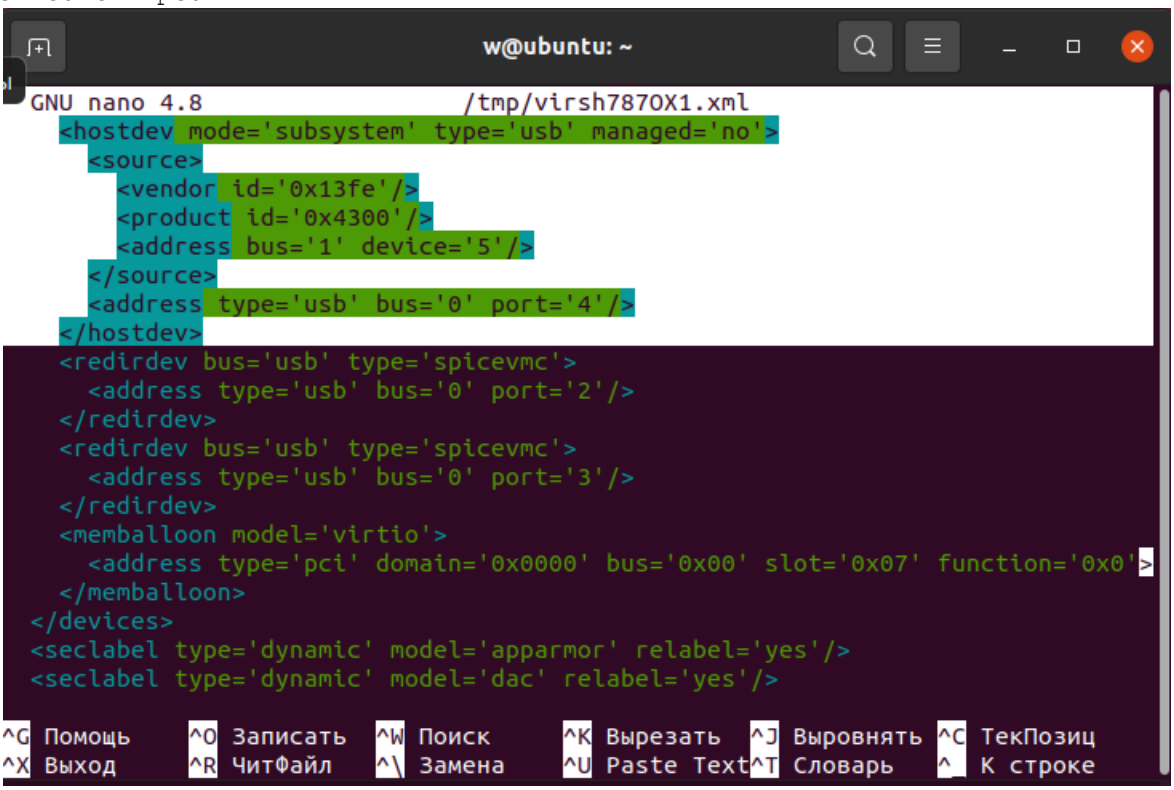


Рисунок 15 - XML файл виртуальной машины

6. При последующем подключении USB-устройства изменяется его номер в системе (параметры Bus, Device), как правило, выводится ошибка (USB-устройство не найдено). Необходимо сверить параметры устройства в конфигурационном файле vfpsu1.xml, выполнив пункт 10.1.

7. В случае несовпадения, замените в файле vfpsu1.xml параметры Bus, Device на актуальные.

8. Удалите USB-устройство из виртуальной машины для переопределения. Выполните шаги 3 - 5.

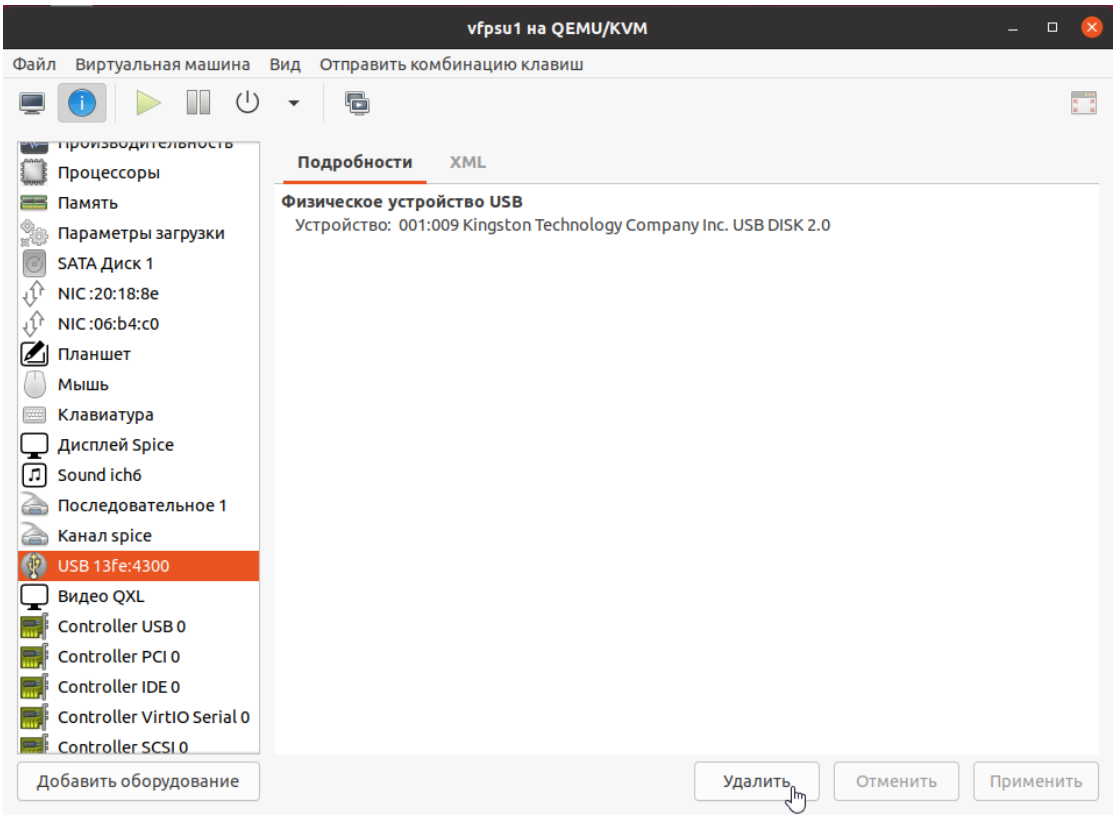


Рисунок 16 - Удаление USB-устройства ТМ подключено

Добавление USB-устройства ТМ

Для добавления в конфигурационный файл виртуальной машины в список оборудования USB-устройства ТМ (ТМ-считыватель или ТМ-Key) выполните следующие действия:

1. Для добавления в конфигурационный файл виртуальной машины USB-устройства ТМ, создайте файл /etc/libvirt/qemu/usb2.xml с описанием устройства (укажите параметры Vendor ID, Device ID).

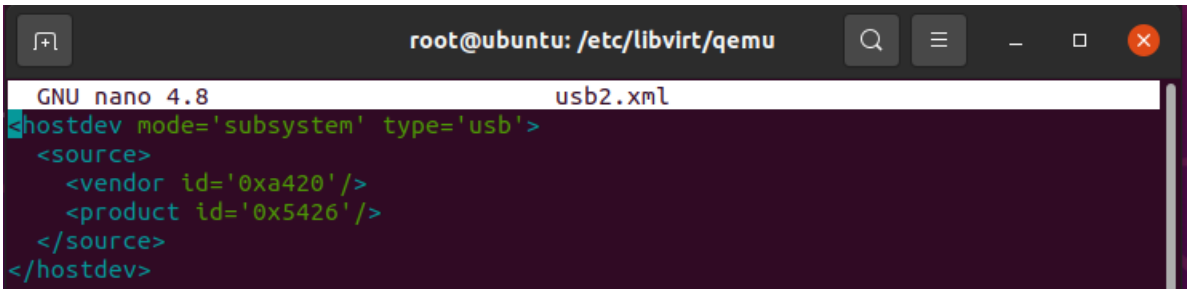


Рисунок 17 - Создание файла с описанием USB-устройства

2. При каждом подключении USB-устройства изменяется его номер в системе, поэтому необходимо чтобы USB-устройство автоматически импортировалось в

виртуальную машину. Для автоматического проброса USB-устройства с хост-машины в гостевую ОС, виртуальную машину vfpsu1, создайте следующее правило в файле /etc/udev/rules.d/90-libvirt-usb.rules:

```
ACTION=="add", \
    SUBSYSTEM=="usb", \
    ENV{ID_VENDOR_ID}=="a420", \
    ENV{ID_MODEL_ID}=="5426", \
    RUN+="/usr/bin/virsh attach-device vfpsu1 /etc/libvirt/qemu/usb2.xml"
ACTION=="remove", \
    SUBSYSTEM=="usb", \
    ENV{ID_VENDOR_ID}=="a420", \
    ENV{ID_MODEL_ID}=="5426", \
    RUN+="/usr/bin/virsh detach-device vfpsu1 /etc/libvirt/qemu/usb2.xml"
```

где /usr/bin/virsh - путь до бинарного файла virsh,

vfpsu1 – имя виртуальной машины, на которую выполняем проброс ТМ,

/etc/libvirt/qemu/usb2.xml – путь до .xml файла с описание устройства ТМ,

ID_VENDOR_ID, ID_MODEL_ID - идентификаторы ТМ, в списке USB-устройств ТМ определяется как a420:5426.

3. Подключите USB-устройство ТМ, добавьте его в список оборудования виртуальной машины.

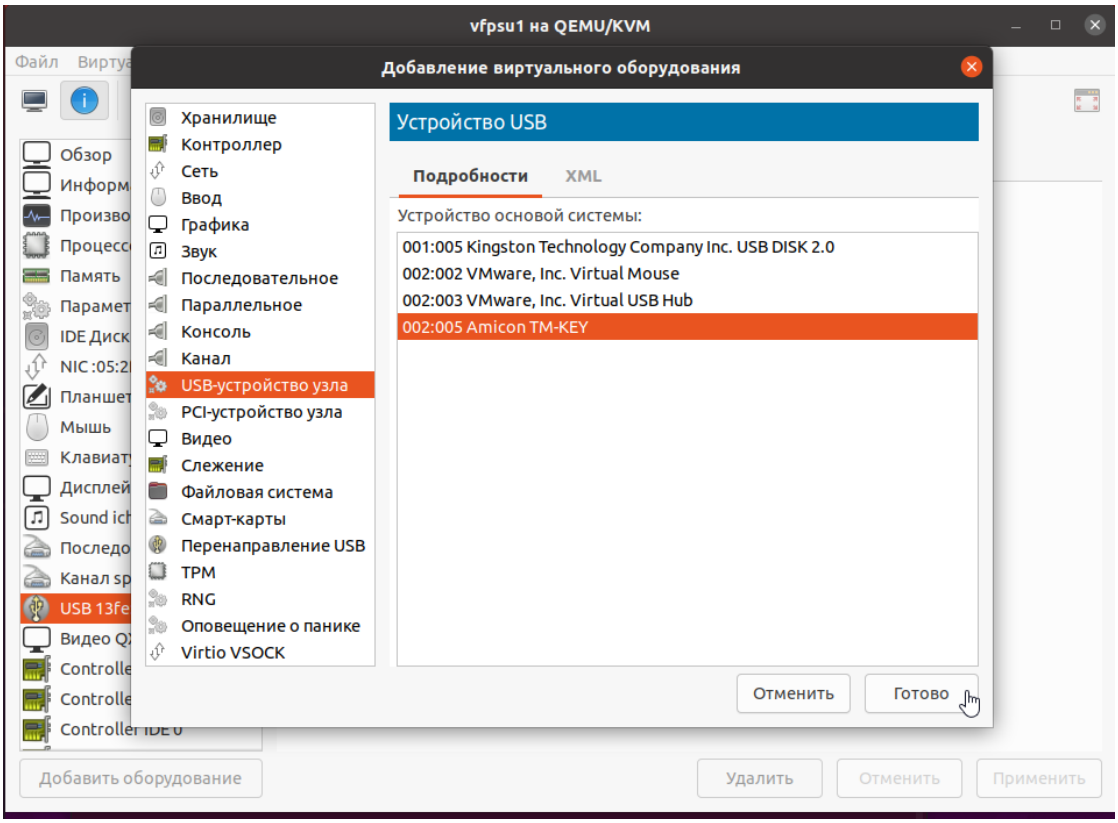


Рисунок 18 - Добавление TM-Key в список оборудования

4. Выполните перезагрузку хост машины, чтобы перезагрузить правила udev, или выполните команду в терминале:

```
udevadm control --reload-rules && udevadm trigger
```

5. Переподключите USB-устройство TM, TM должна автоматически импортироваться в виртуальную машину.

3. 7. 2. Настройка виртуальной машины VMware

Подготовка виртуальной машины VMware Workstation Pro/VMware Workstation/VMware EsXi для развертывания ФПСУ-IP.

Поддерживаемые версии:

- VMware ESXi 6.5, 6.7, 7.0;
- VMware Workstation 14, 15, 16;
- VMware Workstation Pro 14, 15, 16.

Необходимо создать виртуальную машину со следующими характеристиками:

1. Выберите 64-х разрядную операционную систему семейства Linux.

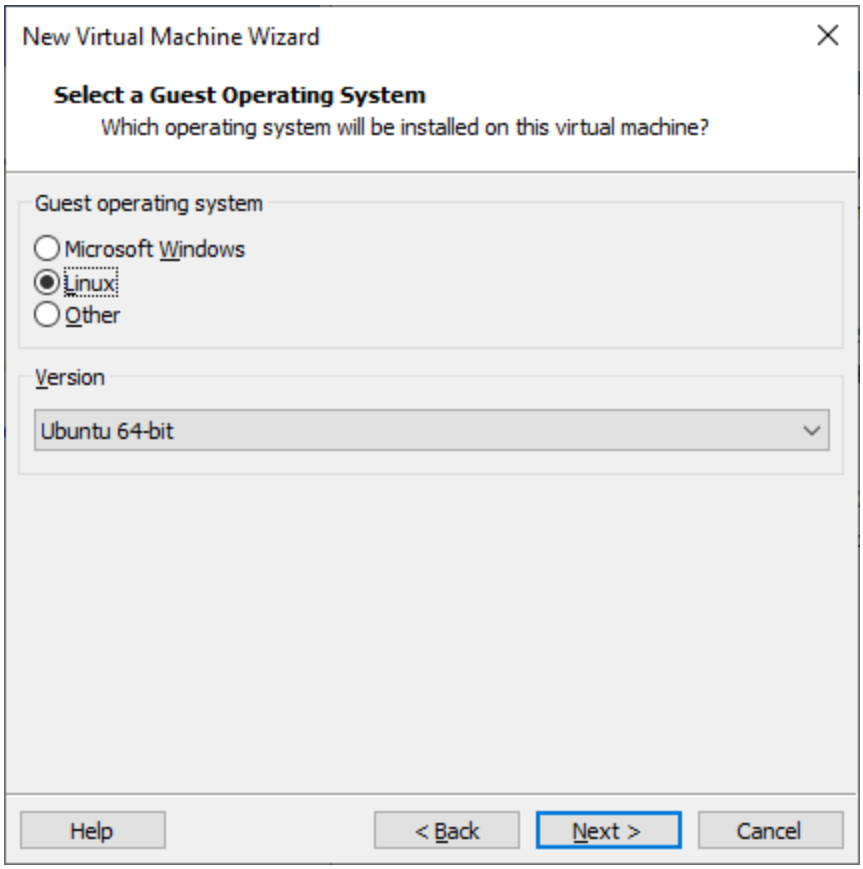


Рисунок 19 - Выбор ОС

2. Количество оперативной памяти, которое выделяется виртуальной машине при создании, должно быть минимум 2 GB. Это же количество памяти будет доступно в гостевой ОС (ОС ФПСУ-IP). Рекомендуется выбирать 4 GB и больше.

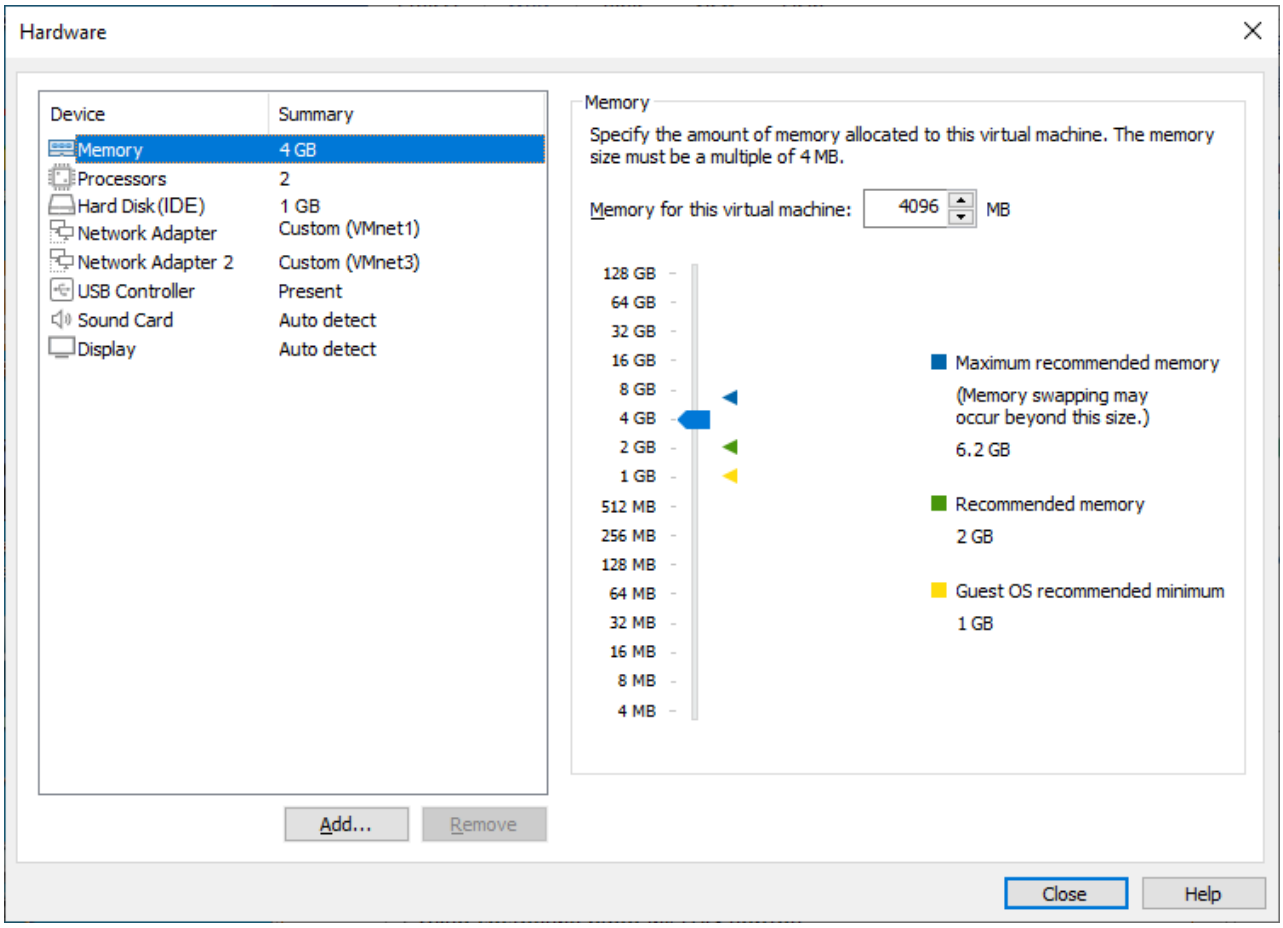


Рисунок 20 - Оперативная память виртуальной машины

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».

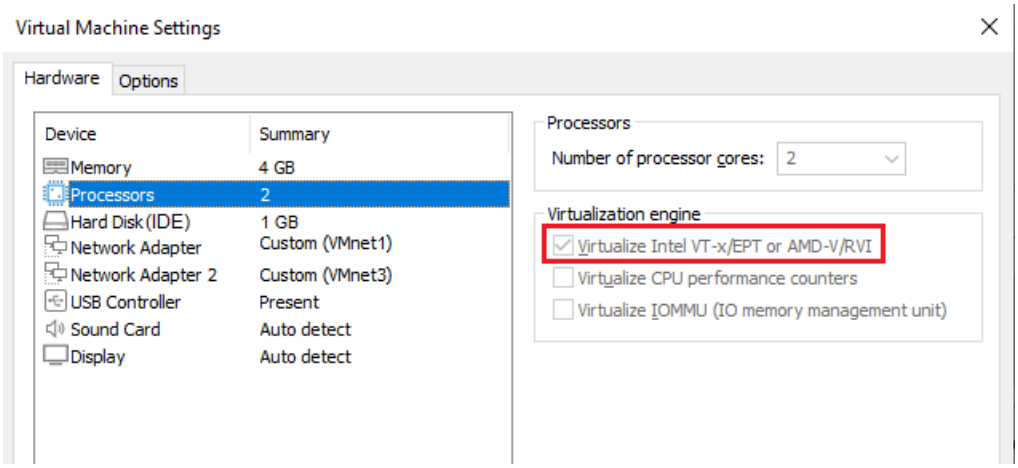


Рисунок 21 - Настройки процессора

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».

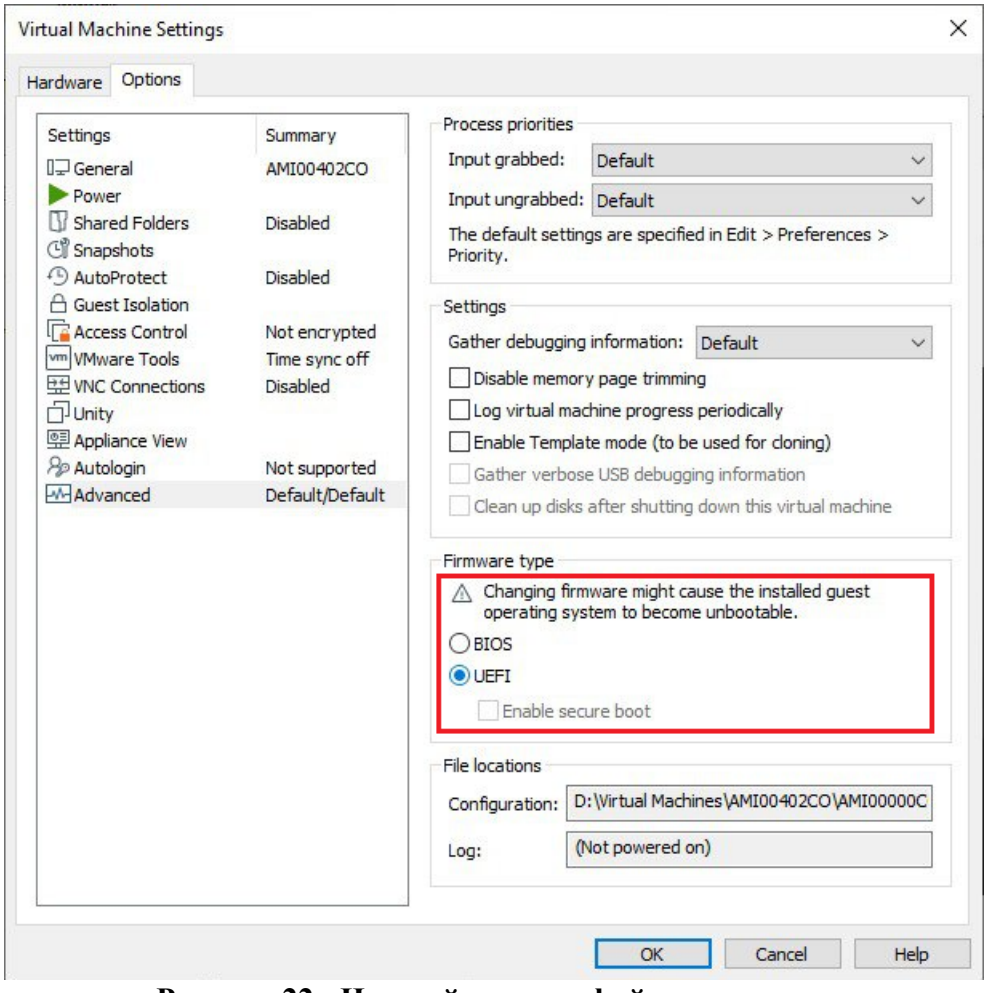


Рисунок 22 - Настройки интерфейса прошивки

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. 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, в таком случае срок указывается в паспорте на изделие) 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);
- в случае ремонта оборудования неуполномоченными лицами.

3. 9. 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). При этом должны выполняться требования к Терминалу, изложенные в документе «Правила пользования» СКЗИ, к которому будет подключаться 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, FPSUIP-EXT-2U, FPSUIP-SRV-1U) — нуль-модемный кабель для COM порта;
3. ФПСУ-IP (FPSUIP-MINI) в компактном корпусе — USB mini-USB кабель.

Возможности работы с интерфейсом ФПСУ-IP аналогичны возможностям работы при локальном администрировании с помощью клавиатуры и монитора, за исключением некоторых сочетаний горячих клавиш:

Обычное управление	**Консольное управление**
Ctrl+Ins	Ctrl+B
Shift+Ins	Ctrl+N
Ctrl+Del	Ctrl+D
Shift+Del	Ctrl+R
Alt+Tab	Ctrl+O

3. 9. 1. Настройки BIOS для консольного подключения

Для использования консольного подключения к ФПСУ-IP требуется внести изменения в BIOS аппаратной платформы ФПСУ-IP, разрешающие консольное подключение по последовательному порту.

После открытия настроек BIOS перейдите на вкладку Server Management и зайдите в пункт Console Redirection. В пункте Console Redirection требуется установить следующие параметры (далее описаны только значимые параметры. Параметры, не указанные в этом пункте, следует оставить в значениях по умолчанию):

Console Redirection — установить значение Serial Port A;

Build Rate — выбрать скорость передачи данных 115.2k;

Terminal type — тип терминала установить значение VT100;
Terminal Resolution — установить значение 80x24.

Примечание. Параметр Terminal Resolution в некоторых BIOS может отсутствовать.

Сохраните внесенные в BIOS изменения и перезапустите ФПСУ-IP.

В примере рассматривается утилита настройки BIOS - Apatio Setup Utility. Название значимых параметров может отличаться от приведенных выше. Откройте утилиту Apatio, перейдите на вкладку Advanced, выберите пункт Serial Port Console Redirection.

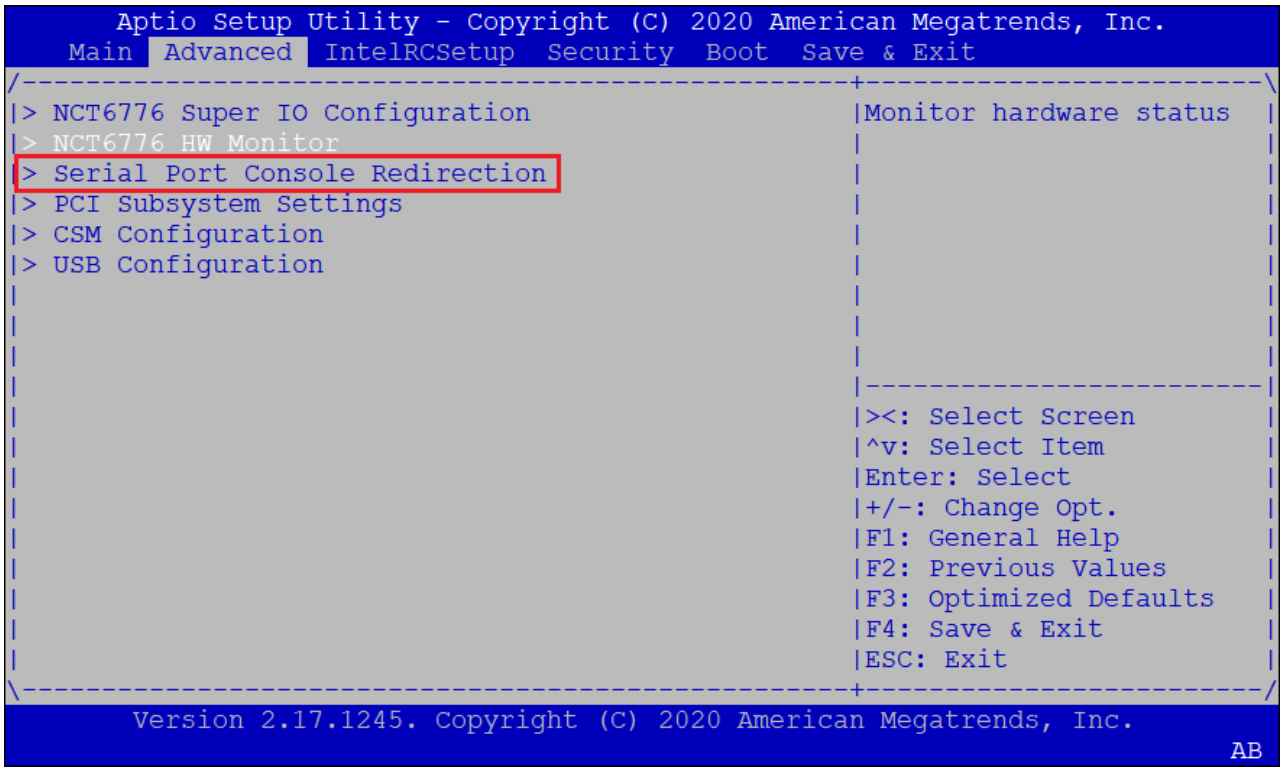


Рисунок 23 - Настройки BIOS

В открывшемся окне активируйте опцию Console Redirection, установив в значение Enabled. Выберите пункт Console Redirection Settings.

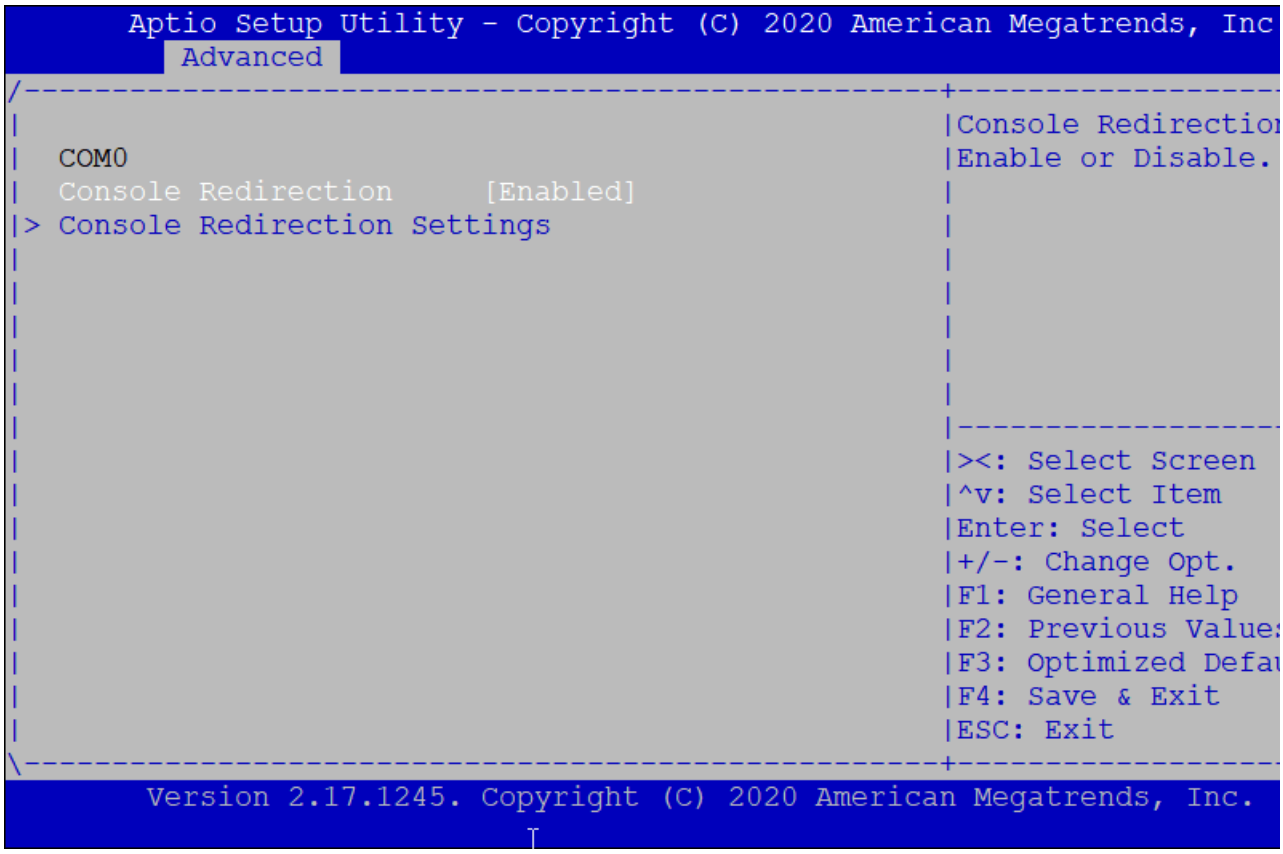


Рисунок 24 - Настройка Console Redirection

В открывшемся окне задайте параметры для выбранного порта:
Terminal Type — тип терминала установить значение VT100+;
Bits per second — выбрать скорость передачи данных 115 200;
Legacy OS Redirection — установить значение 80x24.

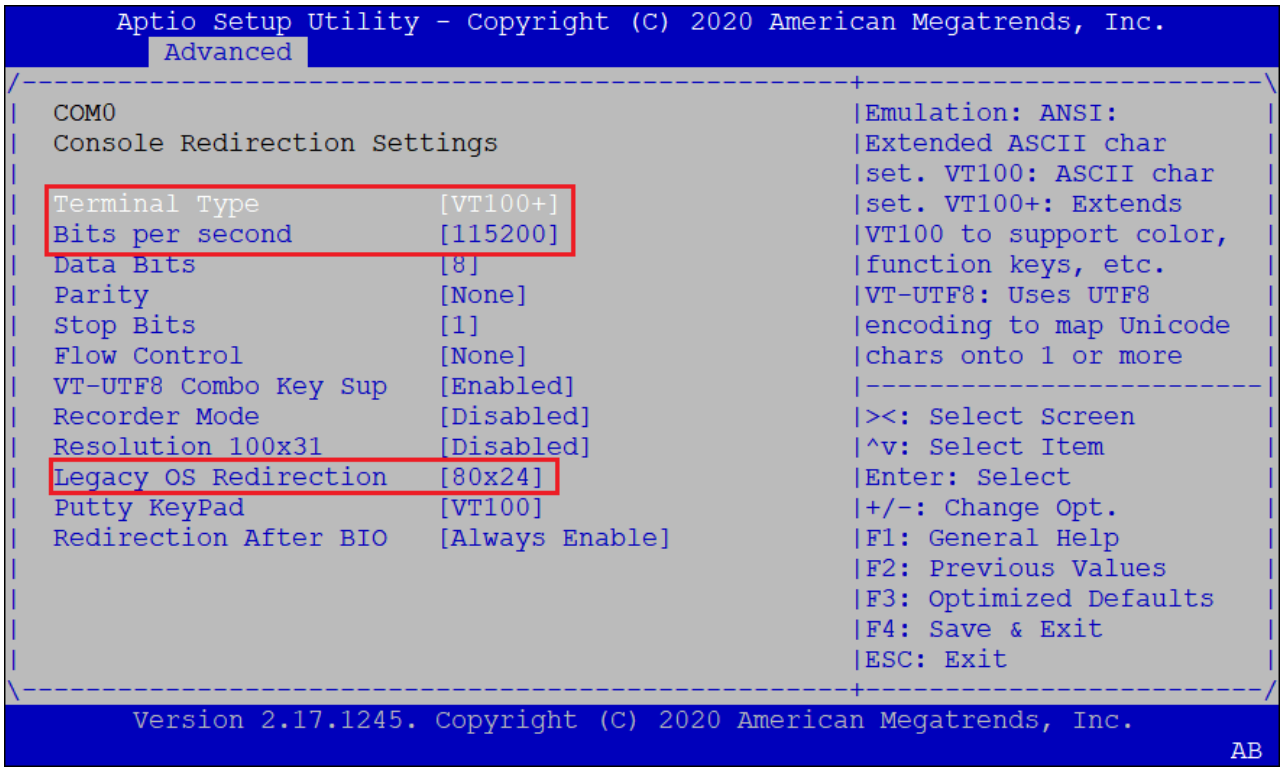


Рисунок 25 - Установка параметров

Сохраните внесенные в BIOS изменения и перезапустите ФПСУ-IP.

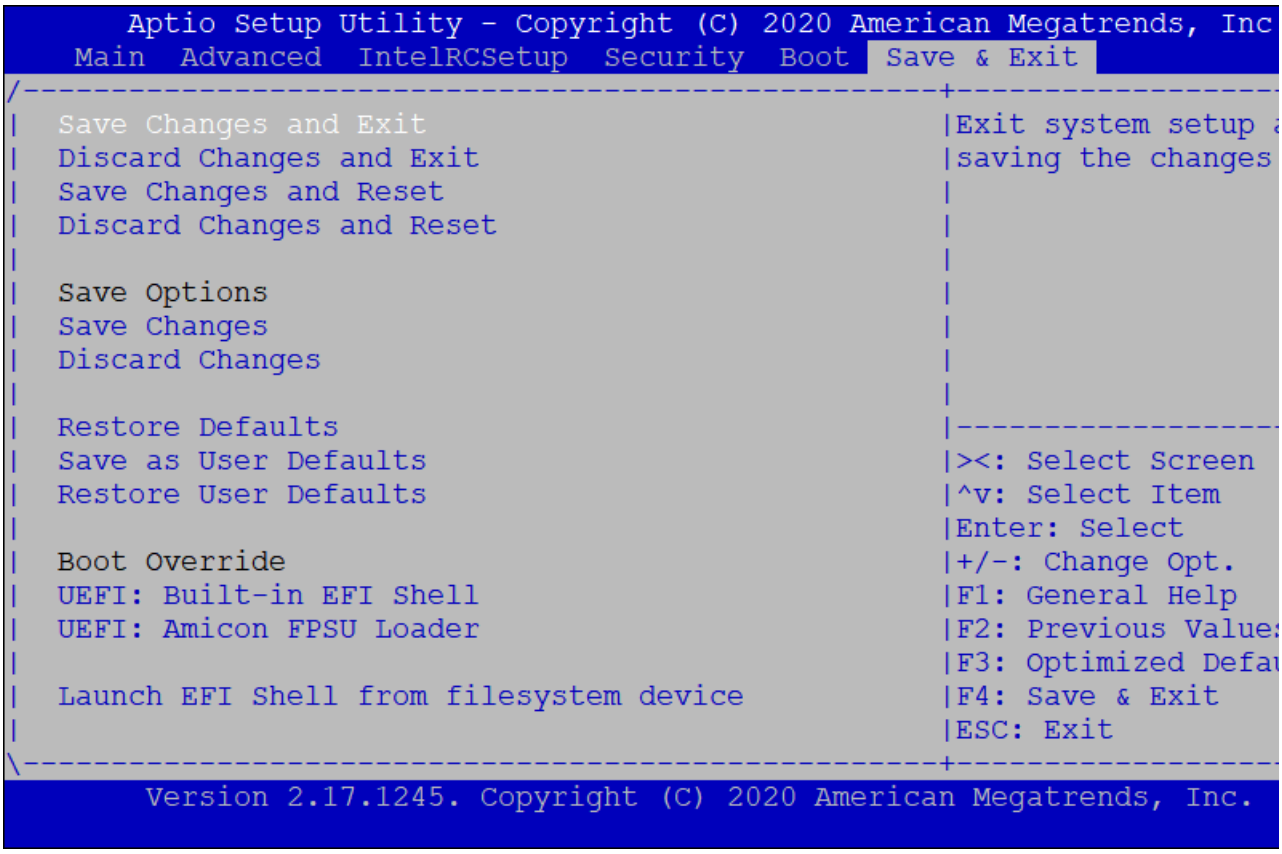


Рисунок 26 - Сохранение настроек BIOS

3. 9. 2. Установка драйверов консольного кабеля

Для использования консольного подключения к ФПСУ-IP требуется подключить консольный кабель к рабочей станции, с которой будет выполняться консольное соединение.

При первом подключении консольного кабеля к рабочей станции Windows драйвер устанавливается автоматически, консольный кабель в диспетчере устройств определяется как USB Serial Port или USB-SERIAL CH340 в группе устройств «Порты (COM и LPT)».

Возможна ситуация, когда при первом подключении к рабочей станции Windows консольный кабель определяется операционной системой ошибочно, и в диспетчере устройств отображается как FT232R USB UART или USB2.0-Ser! в разделе «Другие устройства». В таком случае потребуется вручную установить в операционную систему драйверы кабеля.

Для устройства, определенного в диспетчере устройств Windows как FT232R USB UART, скачайте с официального сайта АМИКОН https://amicon.ru/download.php драйвер для

подключения консоли к ФПСУ-IP для Windows.

Рисунок 27 - Официальный сайт АМИКОН, раздел «Драйверы»

Загрузите и распакуйте архив с файлами драйвера в отдельный каталог. В диспетчере устройств выберите неопознанное устройство FT232R USB UART и по нажатию правой кнопки мыши в контекстном меню выберите пункт «Обновить драйверы» для этого устройства.

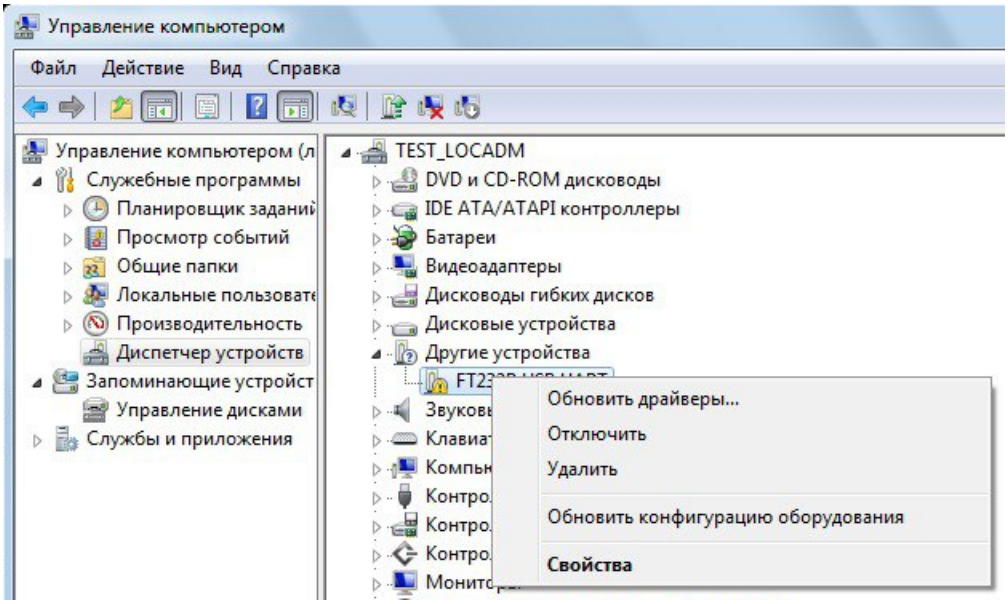


Рисунок 28 - Отображение консольного кабеля в диспетчере устройств

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.

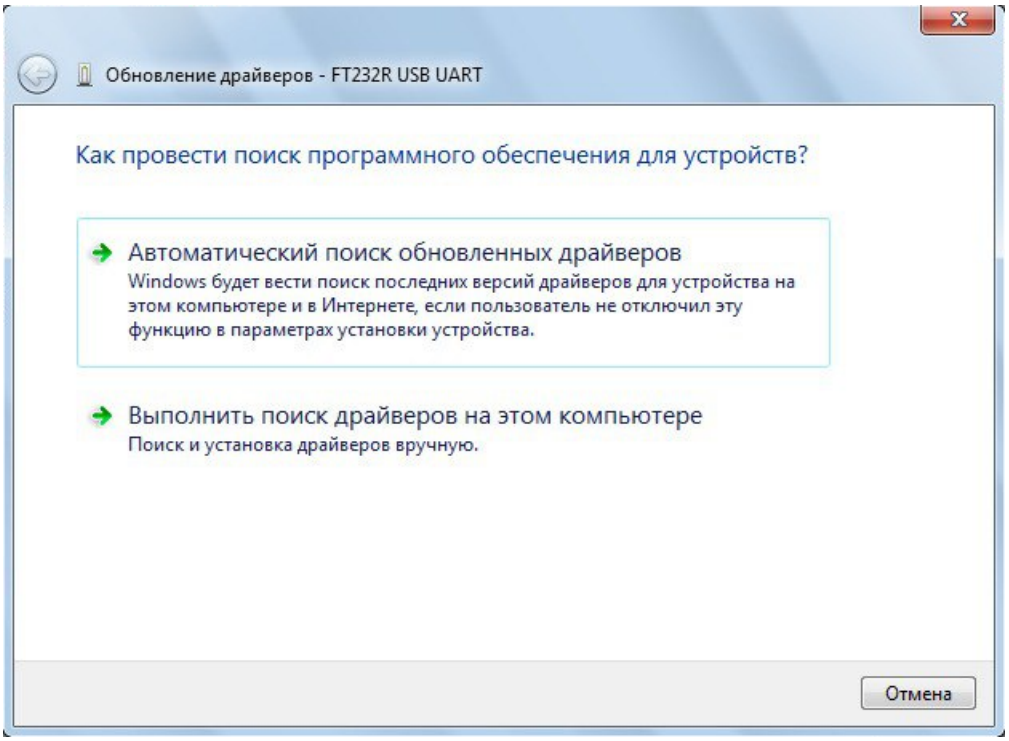


Рисунок 29 - Мастер установки драйвера

Первоначально при установке устройство определяется как USB Serial Converter в разделе «Контроллеры USB».

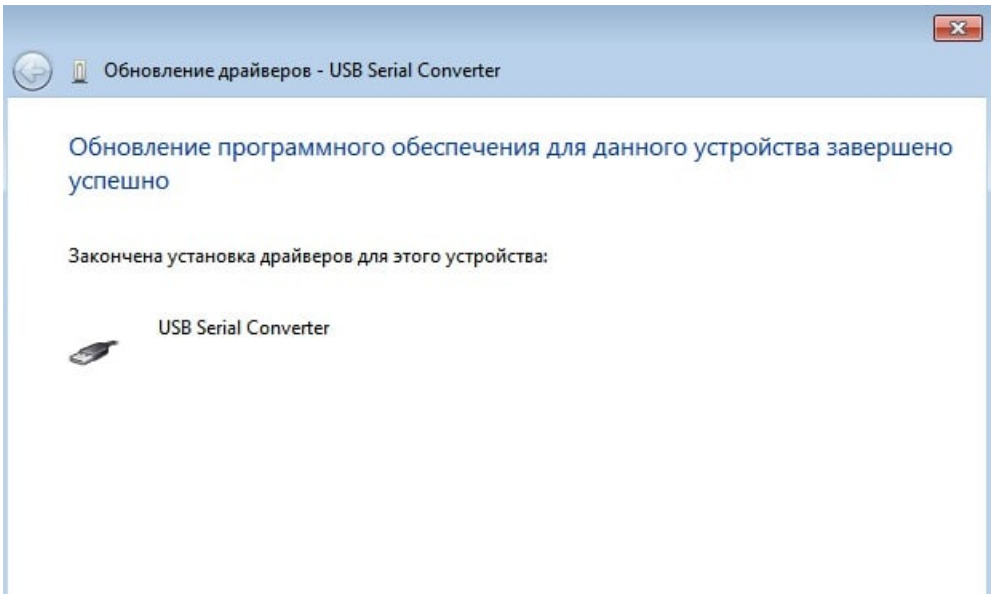


Рисунок 30 - Обновление драйвера консольного кабеля

Требуется еще раз запустить установку драйвера из той же папки. В диспетчере устройств выберите неопознанное устройство USB Serial Port и по нажатию правой кнопки мыши в контекстном меню выберите пункт «Обновить драйверы» для этого устройства.

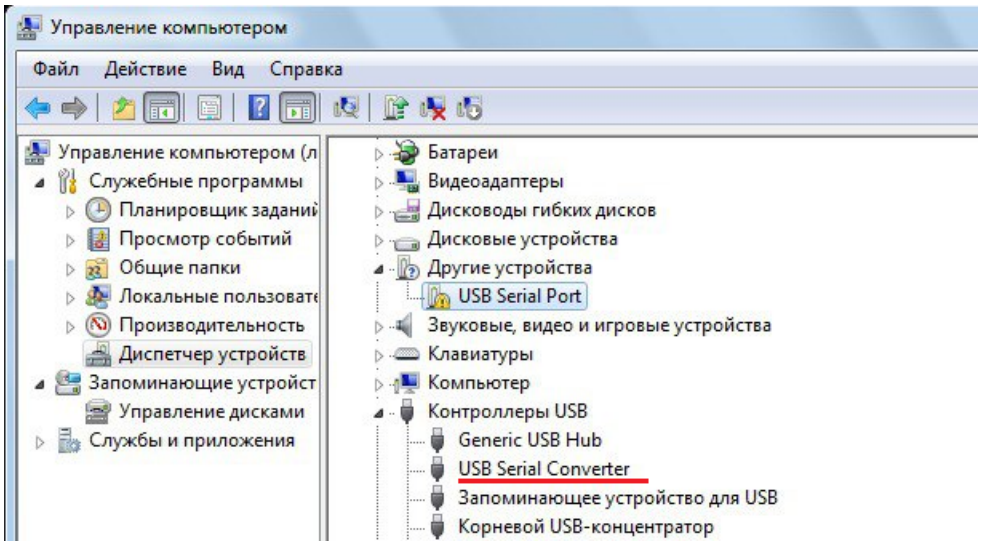


Рисунок 31 - Отображение консольного кабеля после установки драйвера

В диалоговом окне мастера установки выберите поиск драйверов на этом компьютере.

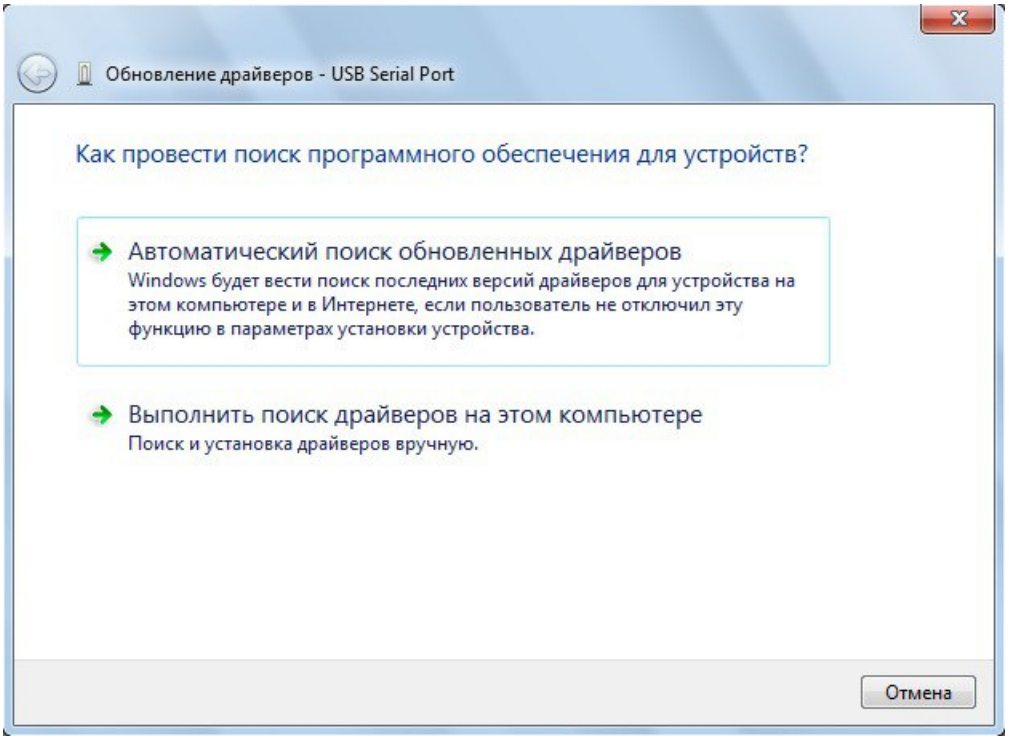


Рисунок 32 - Мастер установки драйвера

Укажите тот же каталог с драйвером. Система установит драйвер и выдаст сообщение об успешном обновлении.

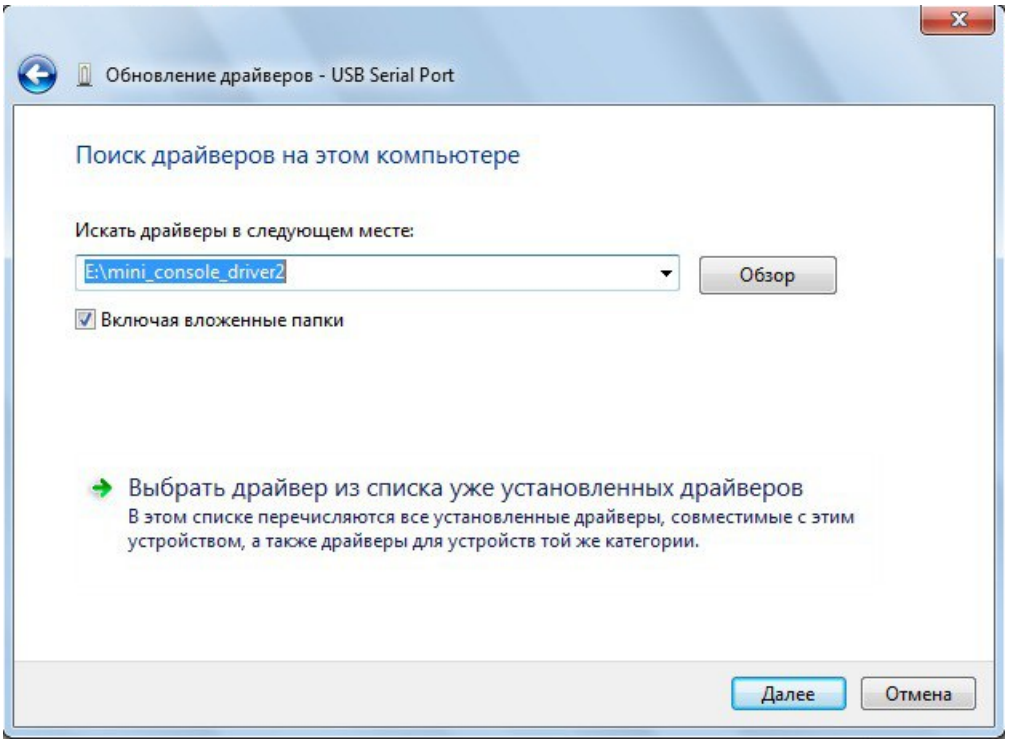


Рисунок 33 - Выбор каталога с драйвером

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

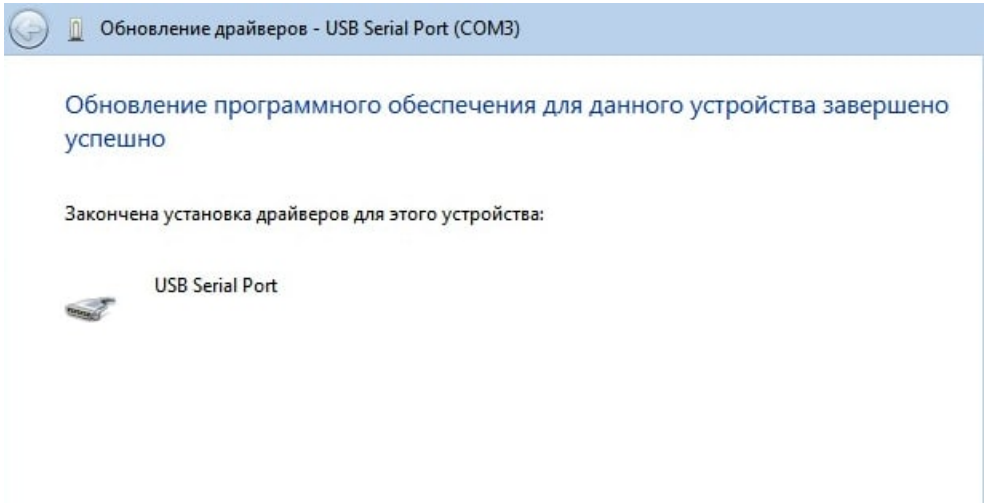


Рисунок 34 - Обновление драйвера консольного кабеля

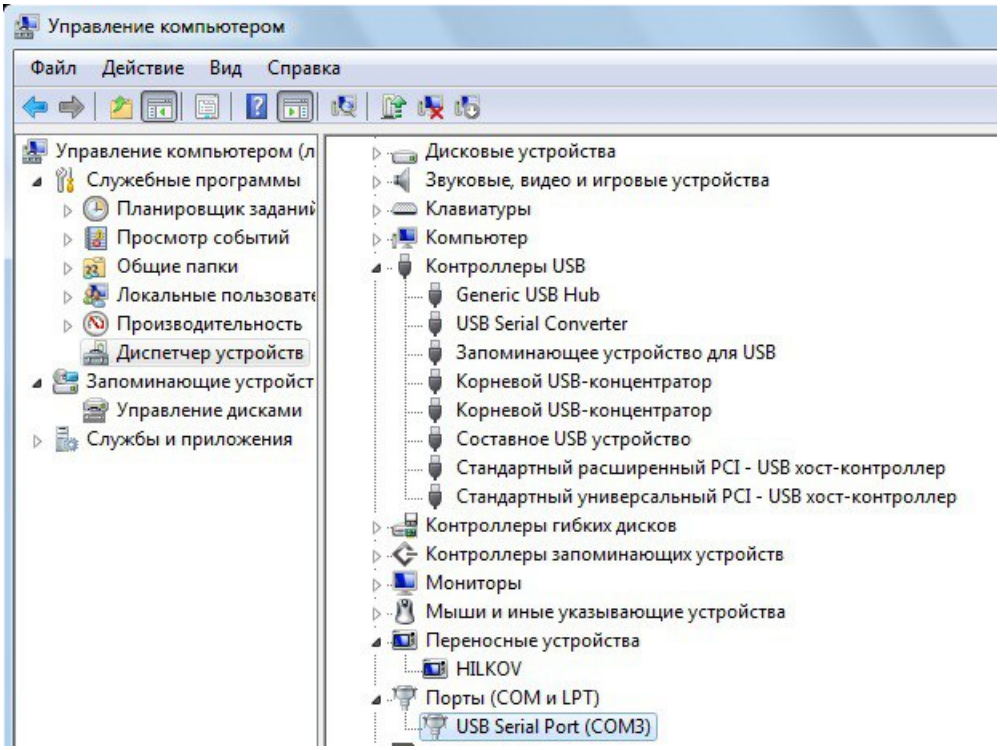


Рисунок 35 - Отображение консольного кабеля после повторной установки драйвера

Для устройства, определенного в диспетчере устройств Windows как USB2.0-Ser! скачайте с официального сайта АМИКОН https://amicon.ru/download.php драйвер для подключения консоли к ФПСУ-IP для Windows с пометкой «CH340».

Загрузите и распакуйте архив с файлами драйвера в отдельный каталог. В диспетчере устройств выберите неопознанное устройство USB2.0-Ser! и по нажатию правой кнопки мыши в контекстном меню выберите пункт «Обновить драйверы» для этого устройства.

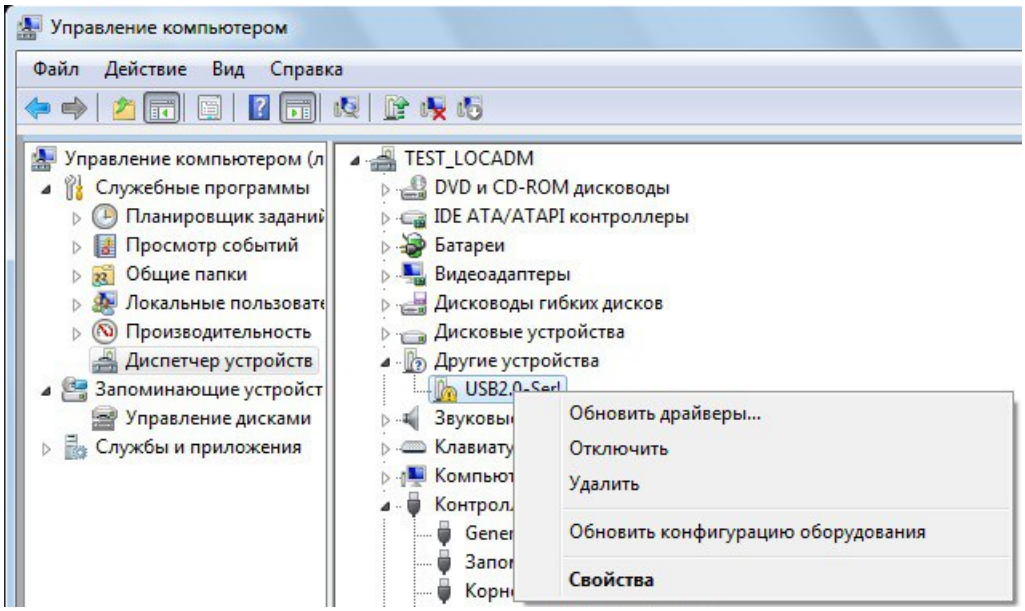


Рисунок 36 - Отображение консольного кабеля в диспетчере устройств

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.

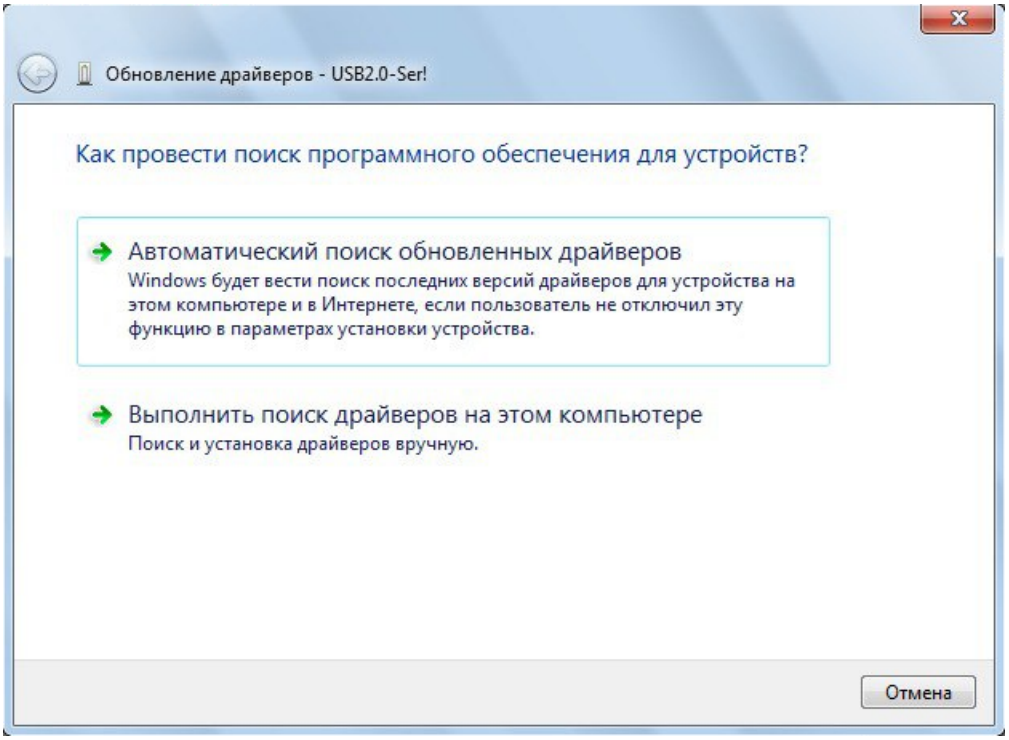


Рисунок 37 - Мастер установки драйвера

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

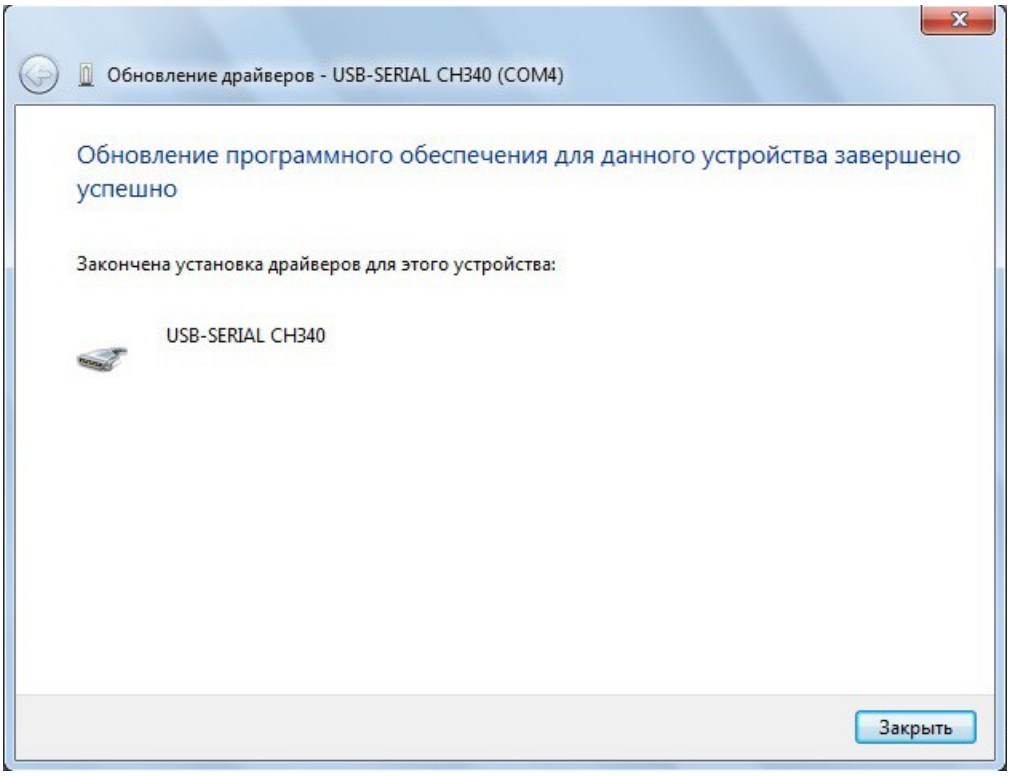


Рисунок 38 - Обновление драйвера консольного кабеля

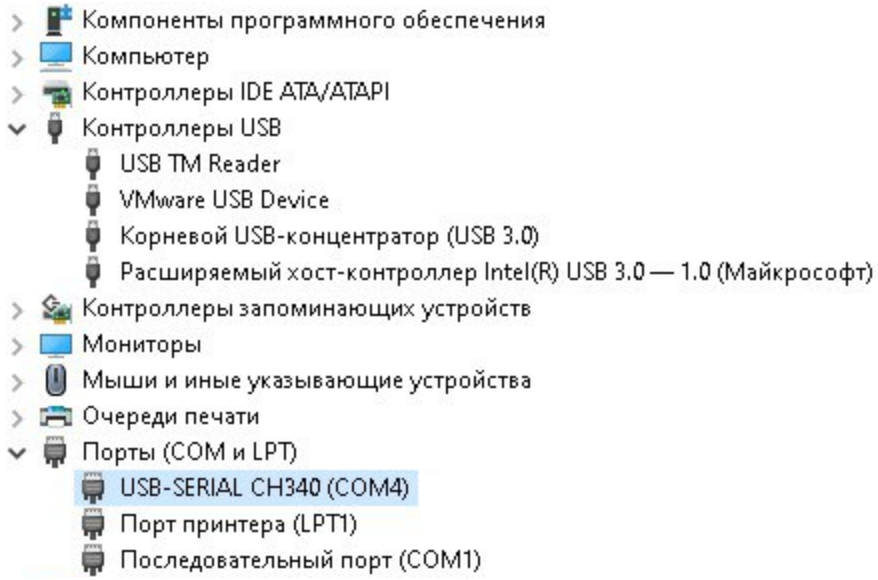


Рисунок 39 - Отображение консольного кабеля после установки драйвера

3. 9. 3. Подключение к ФПСУ-IP с помощью PuTTY

Для консольного подключения к ФПСУ-IP, осуществляемого с Windows станций, следует использовать версию утилиты PuTTY (версии 0.70), входящую в комплектность поставки согласно формуляру на СКЗИ «Программно-аппаратный комплекс шифрования

«ФПСУ-IP». Необходимую версию утилиты PuTTY можно скачать с официального сайта ООО «АМИКОН» (https://amicon.ru/download.php). Кроме того, необходимая версия может быть поставлена по запросу.

Перед запуском утилиты PuTTY соедините консольным кабелем рабочую станцию с ФПСУ-IP. Уточните номер COM порта, зарегистрированного операционной системой для этого последовательного соединения в диспетчере устройств mmc > devmgmt.msc (в примере ниже это COM2). Этот номер потребуется указать в PuTTY при настройке подключения.

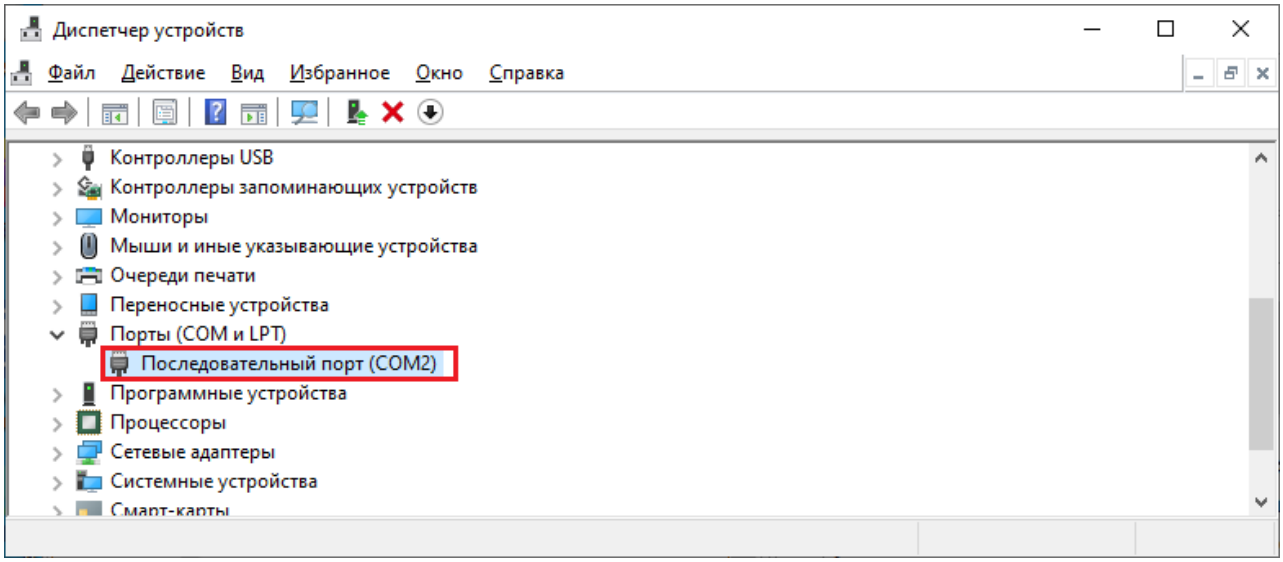


Рисунок 40 - COM порт консольного соединения в диспетчере устройств

Запустите файл PuTTY.exe, выберите тип подключения Serial, укажите номер COM-порта - COM2.

Установите Скорость (Speed) в значение 115200, для сохранения настроек задайте название подключения - FPSU и нажмите «Save».

Примечание. В случае, если консольный кабель не переподключался к рабочей станции, при следующем подключении достаточно выбрать подключение из списка сохраненных и нажать «Load».

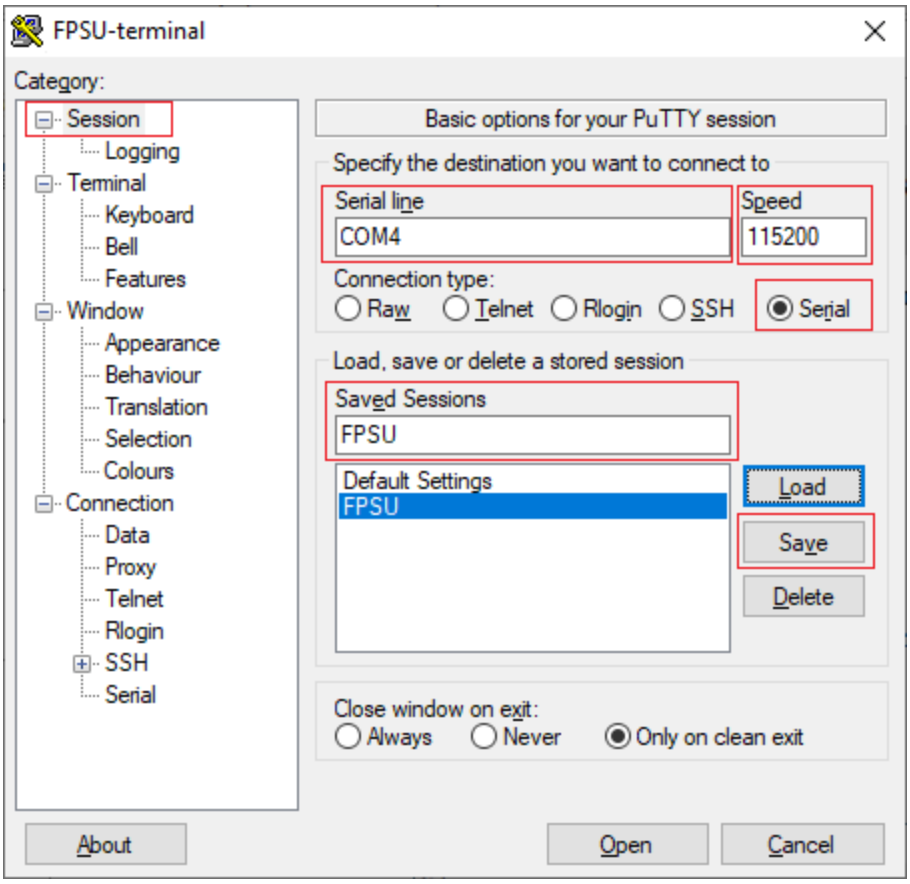


Рисунок 41 - Настройка подключения

Укажите тип используемой в терминале клавиатуры - Xterm R6 или VT100+ (для аппаратной платформы FPSU-ORD4) (устанавливается в интерфейсе PuTTY: Terminal-Keyboard-The Function keys and keypad).

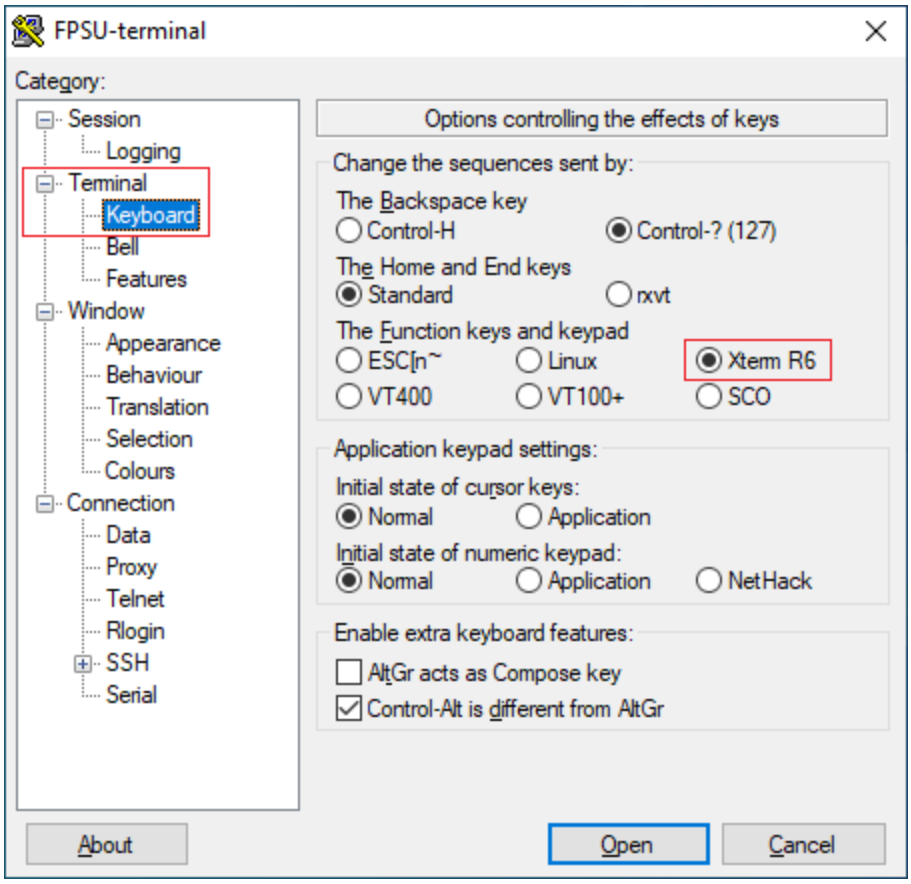


Рисунок 42 - Выбор типа клавиатуры

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

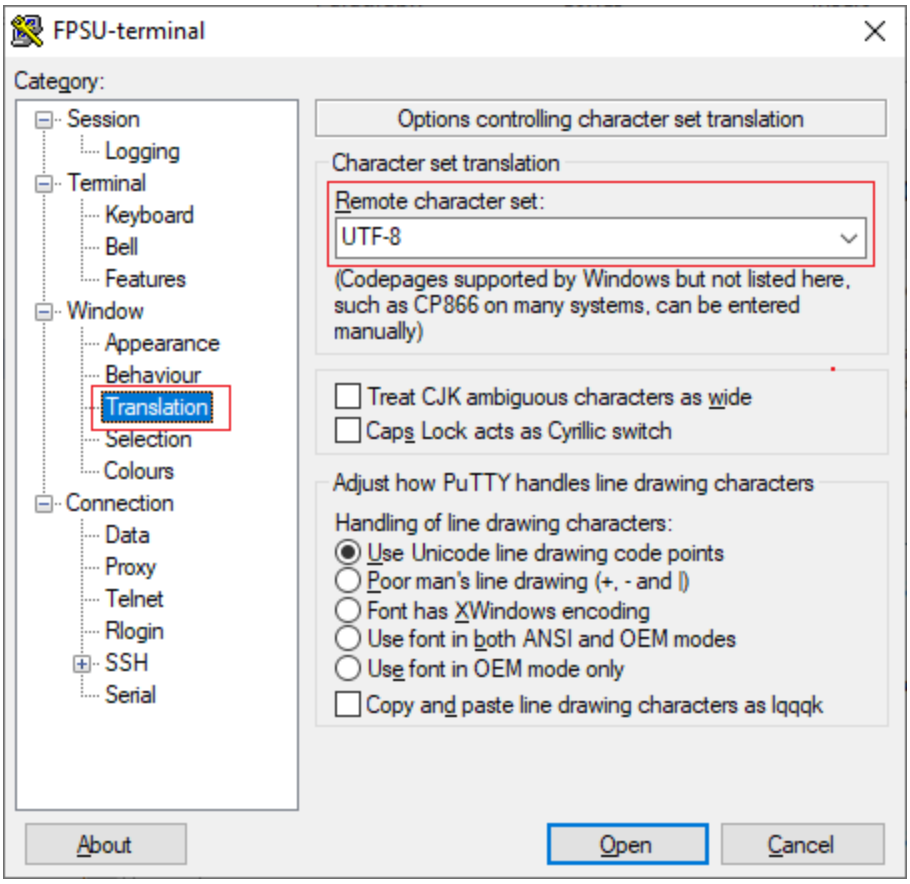


Рисунок 43 - Выбор кодировки

Задайте количество строк – 25 (устанавливается в интерфейсе PuTTY: Window–Rows).

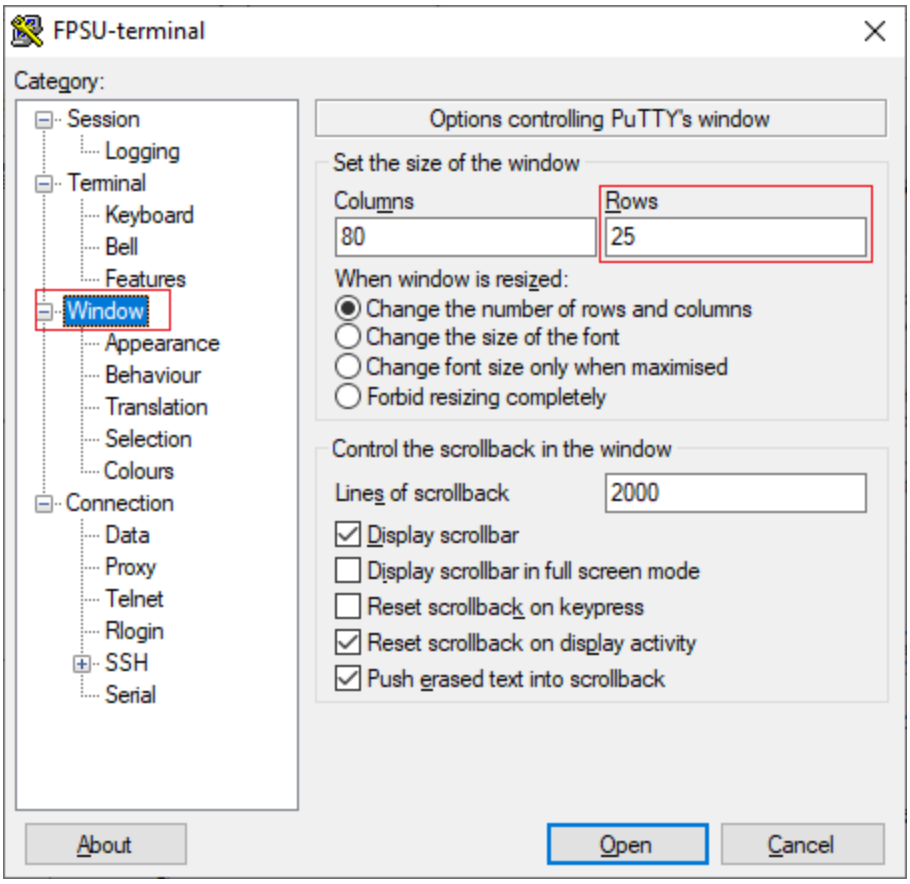


Рисунок 44 - Выбор количества строк

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

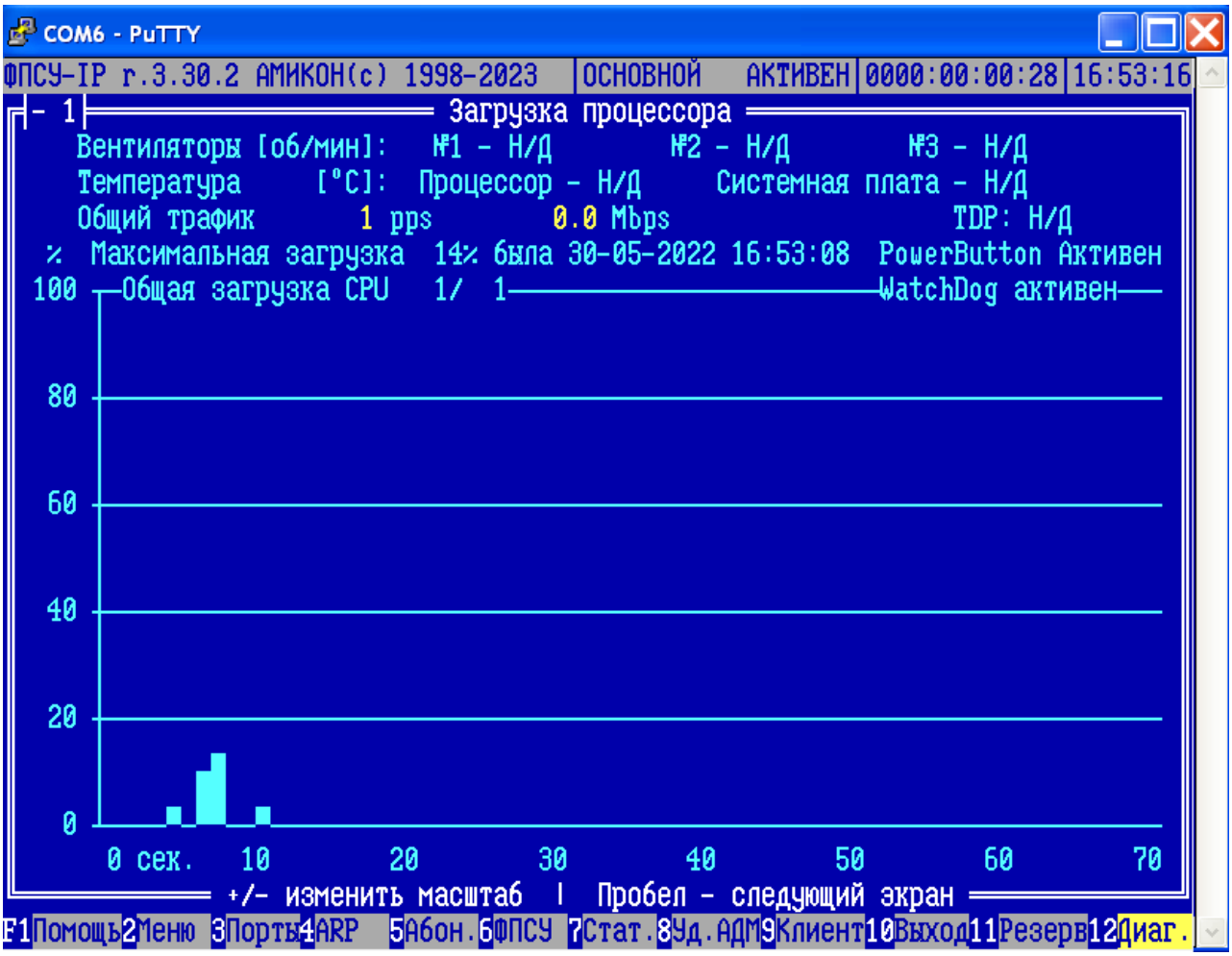


Рисунок 45 - Консольное подключение установлено

3. 10. Установка ПО ФПСУ-IP с дистрибутива

В случае поставки ФПСУ-IP как программно-аппаратного комплекса, ФПСУ-IP поставляется с предустановленным на аппаратную платформу программным обеспечением. У пользователя есть возможность выполнить повторную переустановку программного обеспечения ФПСУ-IP на аппаратную платформу.

Для установки 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:

- эталонного дистрибутива;
- установки серийного номера для данного экземпляра ФПСУ-IP (два файла с расширениями .up0 и .upd, должны находиться в корне дистрибутивного носителя);

- USB-flash накопитель с поддержкой USB 2.0;
- ТМ-идентификатор Главного Администратора ФПСУ-IP;
- Аппаратная платформа ФПСУ-IP, на которую будет установлено ПО ФПСУ-IP.

Перед началом работы, необходимо проверить контрольные суммы утилиты restore.exe и файлов эталонного дистрибутива на соответствие указанным в формуляре.

3. 10. 1. Создание установочного USB-носителя утилитой restore.exe

Первым этапом установки является создание установочного USB-носителя утилитой restore.exe, на основе файла эталонного дистрибутива.

Файл эталонного дистрибутива поставляется на дистрибутивном носителе (CD-диск или USB-flash) вместе с ФПСУ-IP и должен называться «flash.img.xz».

Запустите утилиту restore.exe. Будет выдано окно утилиты, в которой следует указать местоположение файла эталонного дистрибутива и диск USB-flash носителя, на который будут записаны файлы установщика ФПСУ-IP:

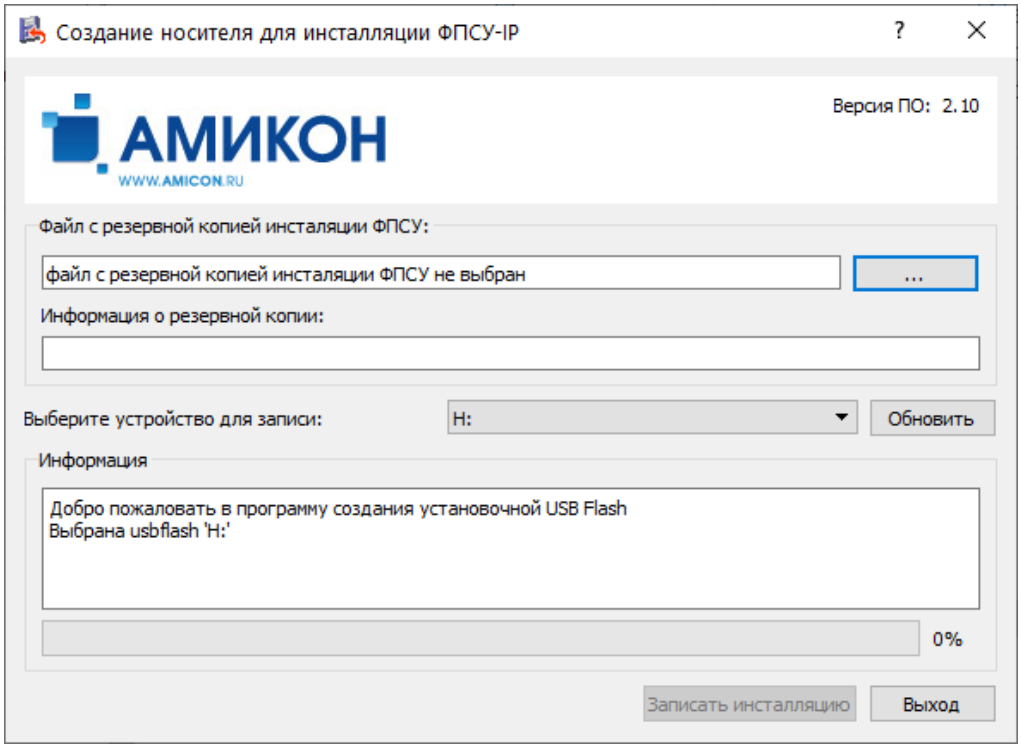


Рисунок 46 - Окно создания носителя

Укажите в интерфейсе стандартного выбора файла Windows, нажав на кнопку «…», место хранения, где находится файл эталонного дистрибутива (в формате архива *.xz) и подтвердите выбор:

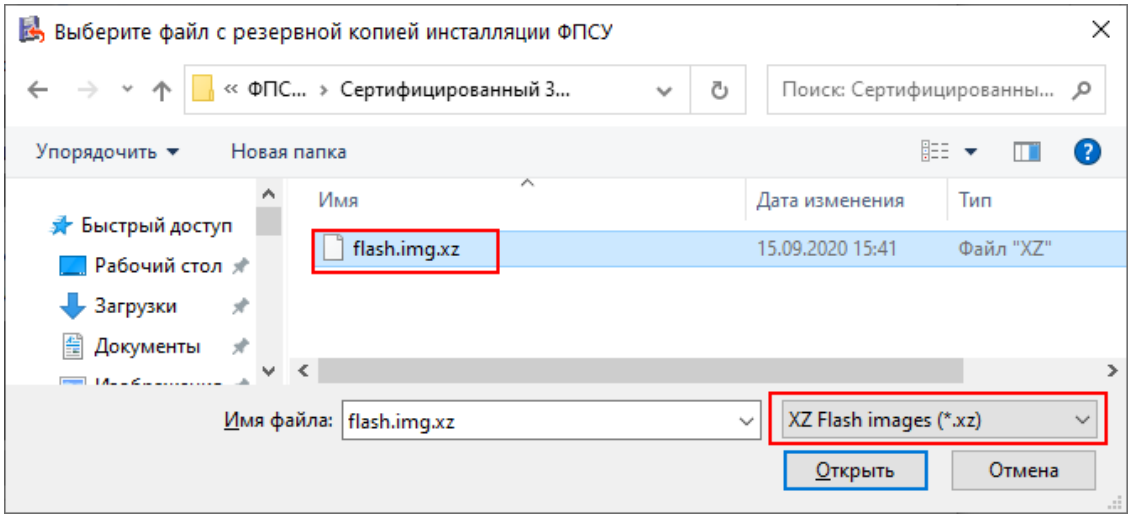


Рисунок 47 - Выбор места хранения эталонного дистрибутива

После выбора файла, утилита отобразит путь к указанному файлу и шаблонный серийный номер (который должен совпадать со значением «XXX00000XX») установочного носителя:

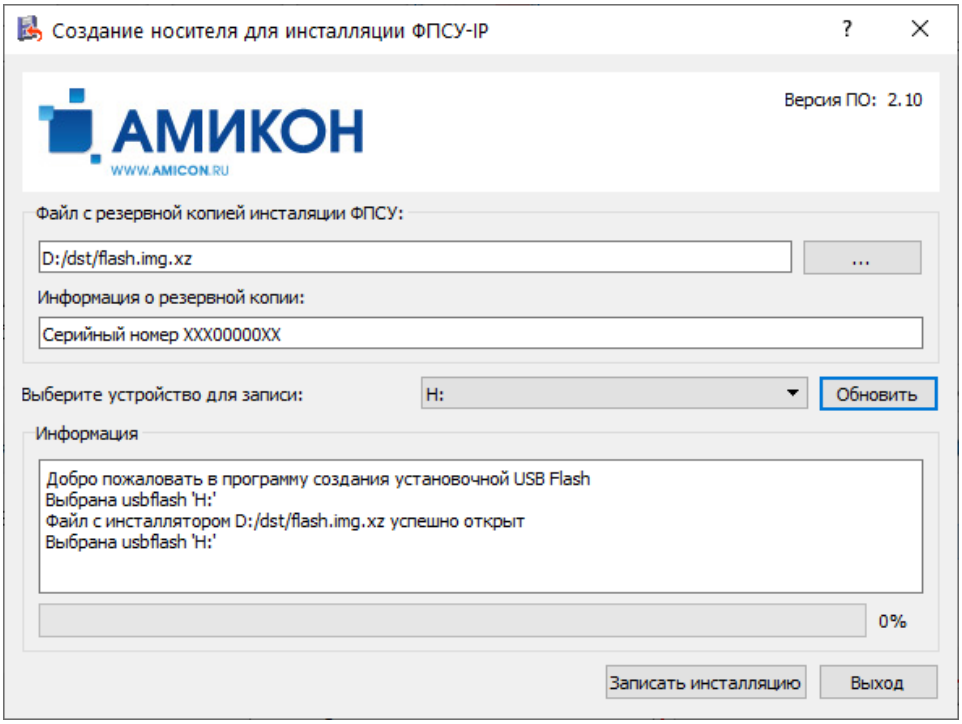


Рисунок 48 - Сообщение о необходимости выбора USB-носителя

Для выбора USB-носителя, подключите USB-flash к ПЭВМ, нажмите кнопку «Обновить», и из выпадающего списка поля «Выберите устройство для записи» укажите найденный USB-flash.

После указания файла дистрибутива и устройства для записи, становится доступной команда «Записать инсталляцию»:

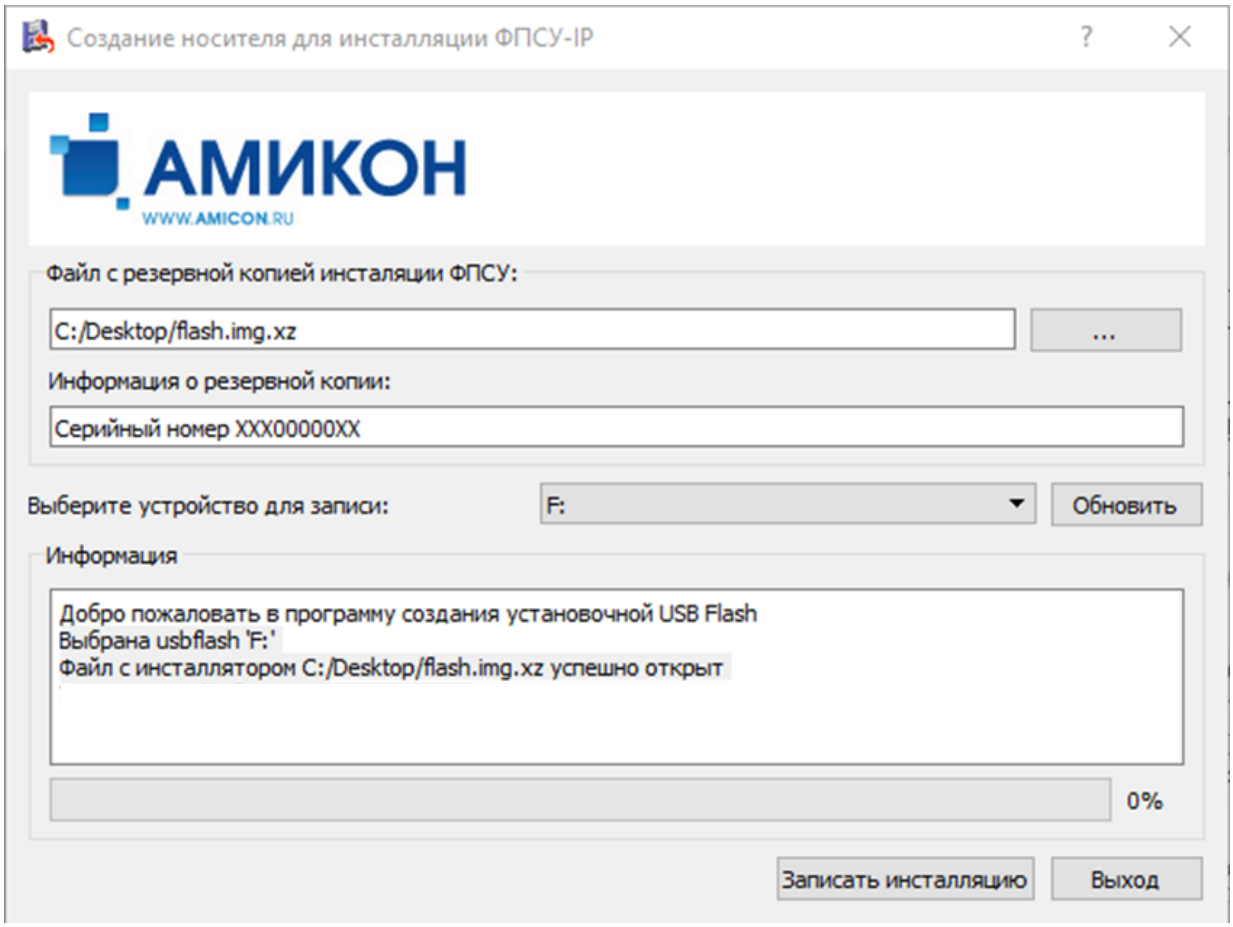


Рисунок 49 - Заполненное окно создания установочного носителя

При выполнении команды «Записать инсталляцию» начнется процесс копирования установочных файлов на USB-носитель. Успешное завершение процесса сопровождается сообщением «Установочный образ успешно записан»:

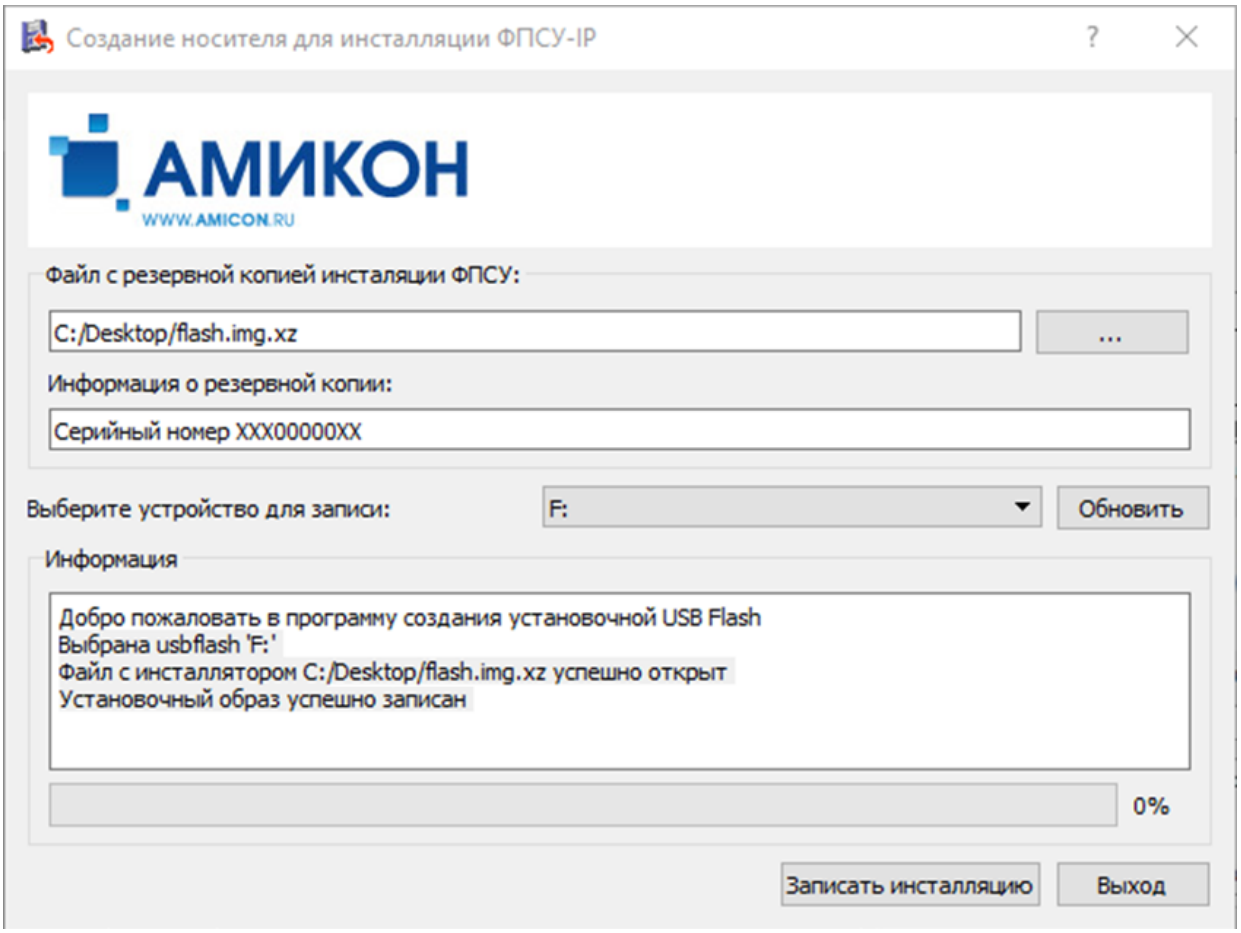


Рисунок 50 - Сообщение об успешном завершении процесса

После создания установочного USB-носителя можно переходить ко второму этапу, установке программного обеспечения ФПСУ-IP с установочного носителя на аппаратную основу или в виртуальную машину.

3. 10. 2. Установка ПО ФПСУ-IP с установочного носителя

Установка ПО ФПСУ-IP на аппаратную платформу ФПСУ-IP (далее АП ФПСУ-IP) или в виртуальную среду заключается в подключении USB-носителя к АП ФПСУ-IP или к виртуальной машине, последующего запуска АП ФПСУ-IP или виртуальной машины, и дальнейшего следования предложениям мастеру установки.

1. Подключите USB-носитель к АП ФПСУ-IP или к виртуальной машине;
2. Запустите АП ФПСУ-IP или виртуальную машину. После выполнения стартовых тестов, на экран будет выдано стартовое окно загрузчика. Требуется нажать клавишу <↓> на клавиатуре, иначе загрузка с USB-носителя будет прервана:

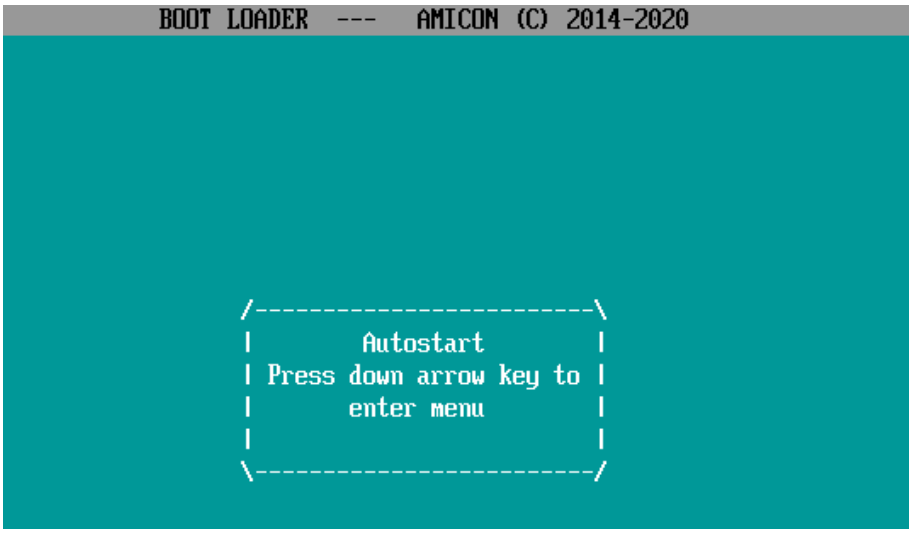


Рисунок 51 - Стартовое окно загрузчика

Откроется экран меню установки, на которой требуется проверить найденный на USB-носителе серийный номер эталонной установки. Для установки в виртуальную среду, серийный номер (значение поля «Serial#») **обязан** быть «VFP00000SU», а для установки на АП ФПСУ-IP серийный номер (значение поля «Serial#») **обязан** быть «XXX00000.XX»:

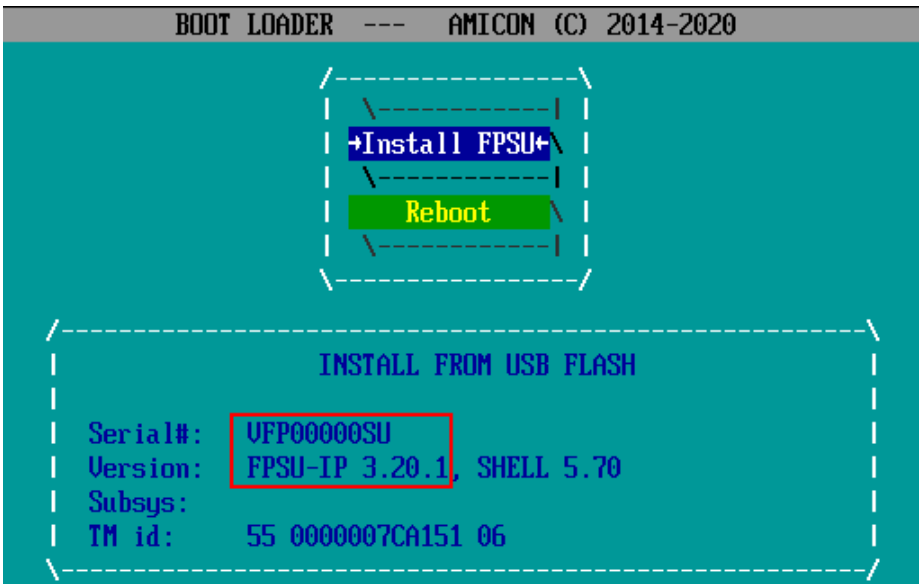


Рисунок 52 - Экран установки ФПСУ-IP

Если серийный номер не совпадает с ожидаемым, следует прекратить установку и заново создать установочный USB-носитель (см. пункт «Создание установочного USB-носителя утилитой restore.exe») с каталога для ожидаемого серийного номера.

Если серийный номер совпадает с ожидаемым, выполните команду «Install FPSU».

3. Установщик продолжит работу. После оповещения и подтверждения решения,

будет запущен процесс форматирования постоянного носителя ФПСУ-IP. Подтвердите продолжение установки выбором команды «Да»:

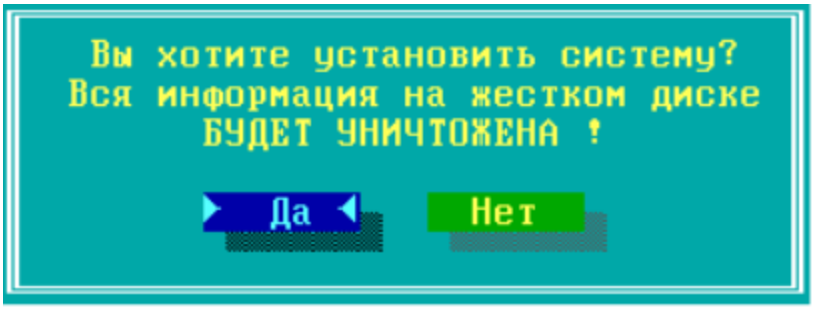


Рисунок 53 - Очистка ПЗУ ФПСУ-IP

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:

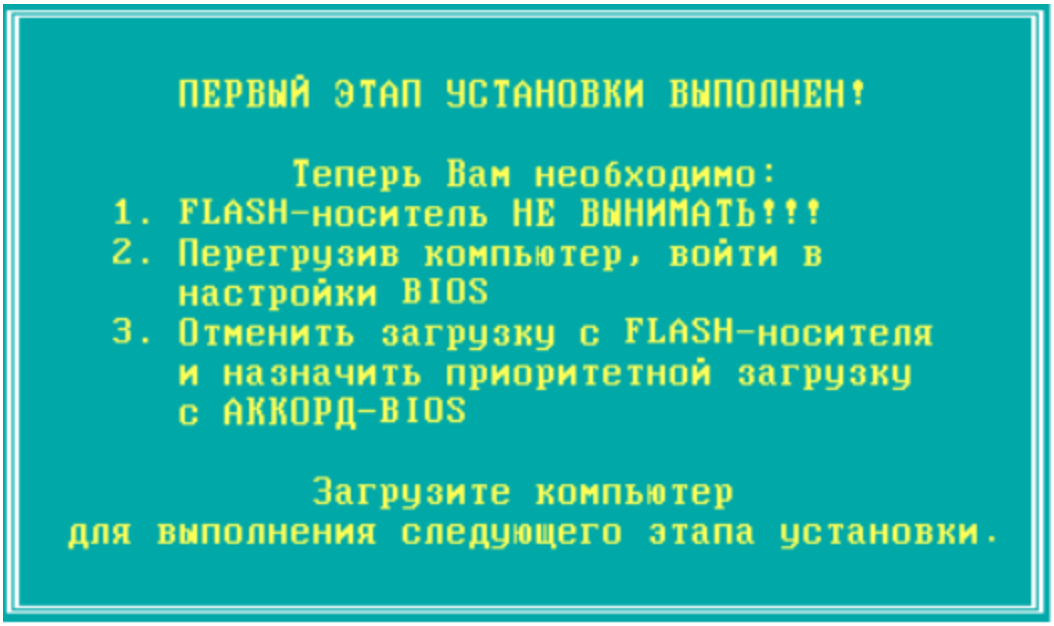


Рисунок 54 - Завершение первого этапа установки

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):

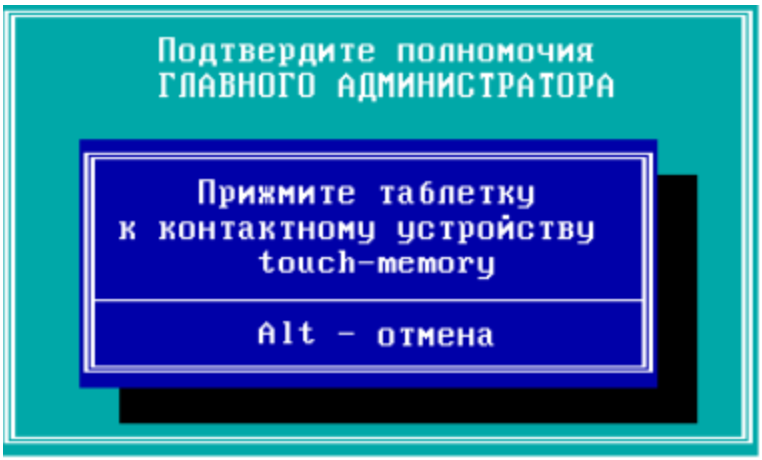


Рисунок 55 - Проверка полномочий Главного администратора

6. Если инсталляционный комплект выдан для ФПСУ-IP с установленной подсистемой «горячего» резервирования, то после проверки полномочий Главного администратора программа установки предложит указать режим функционирования данного ФПСУ-IP в комплексе «горячего» резерва. Выберите требуемый режим — «Основной/Единственный» или «Горячий резерв» и нажмите клавишу <*Enter*>.

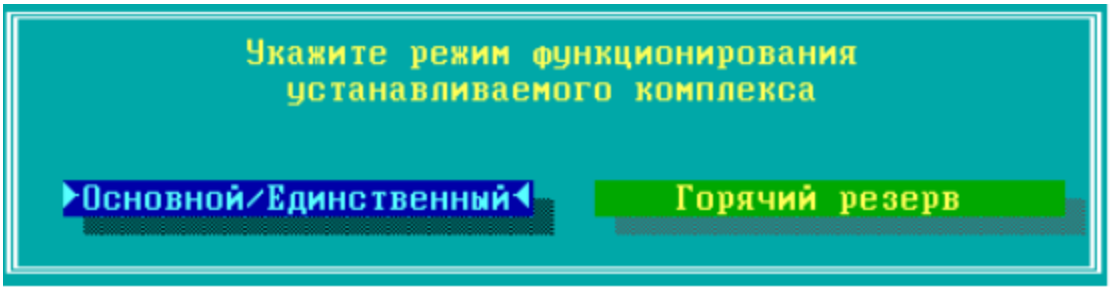


Рисунок 56 - Выбор режима функционирования ФПСУ-IP

7. После выбора режима функционирования ФПСУ-IP в подсистеме «горячего» резервирования, начнется копирование файлов ФПСУ-IP на ПЗУ:

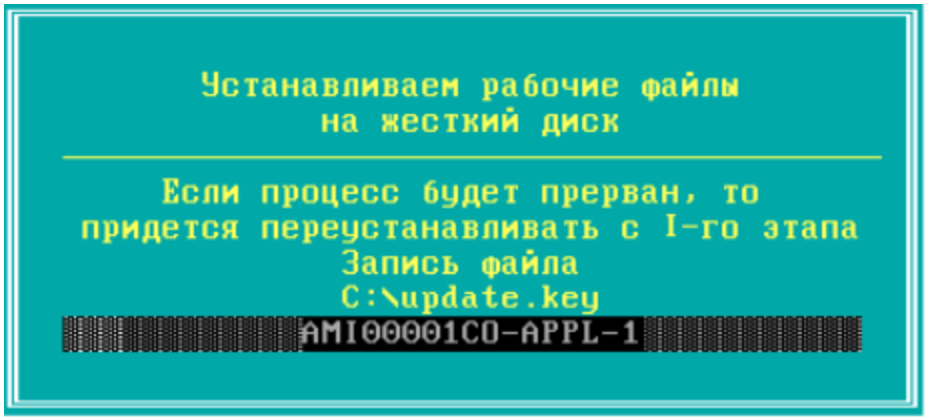


Рисунок 57 - Копирование системных файлов

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. 10. 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).

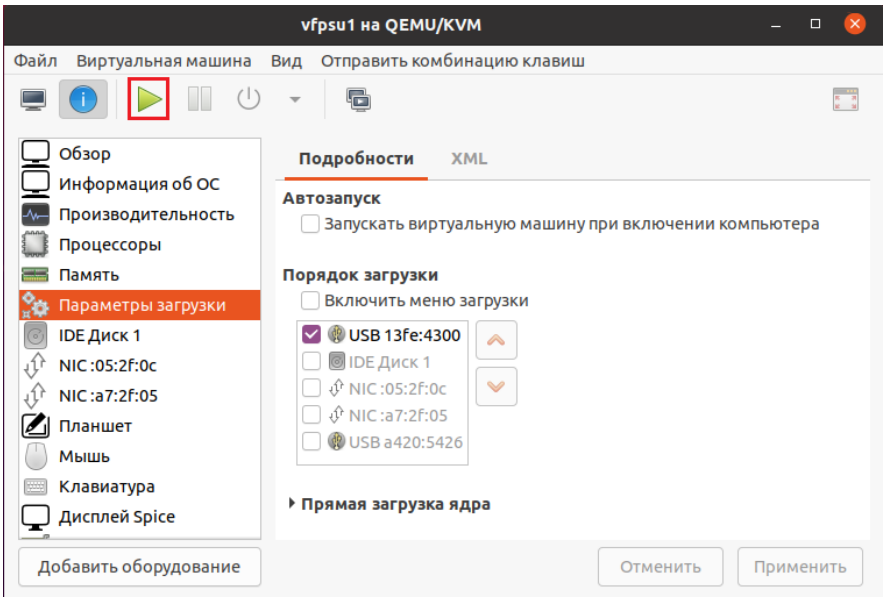


Рисунок 58 - Запуск виртуальной машины

Если инсталляционный комплект выдан для ФПСУ-IP с установленной подсистемой «горячего» резервирования, то после проверки полномочий Главного администратора программа установки предложит указать режим функционирования данного ФПСУ-IP в комплексе «горячего» резерва. Выберите требуемый режим — «Основной/Единственный» или «Горячий резерв» и нажмите клавишу <*Enter*>. Если устанавливаются или переустанавливаются оба комплекса «горячего» резерва, установку рекомендуется начинать с "Основного".

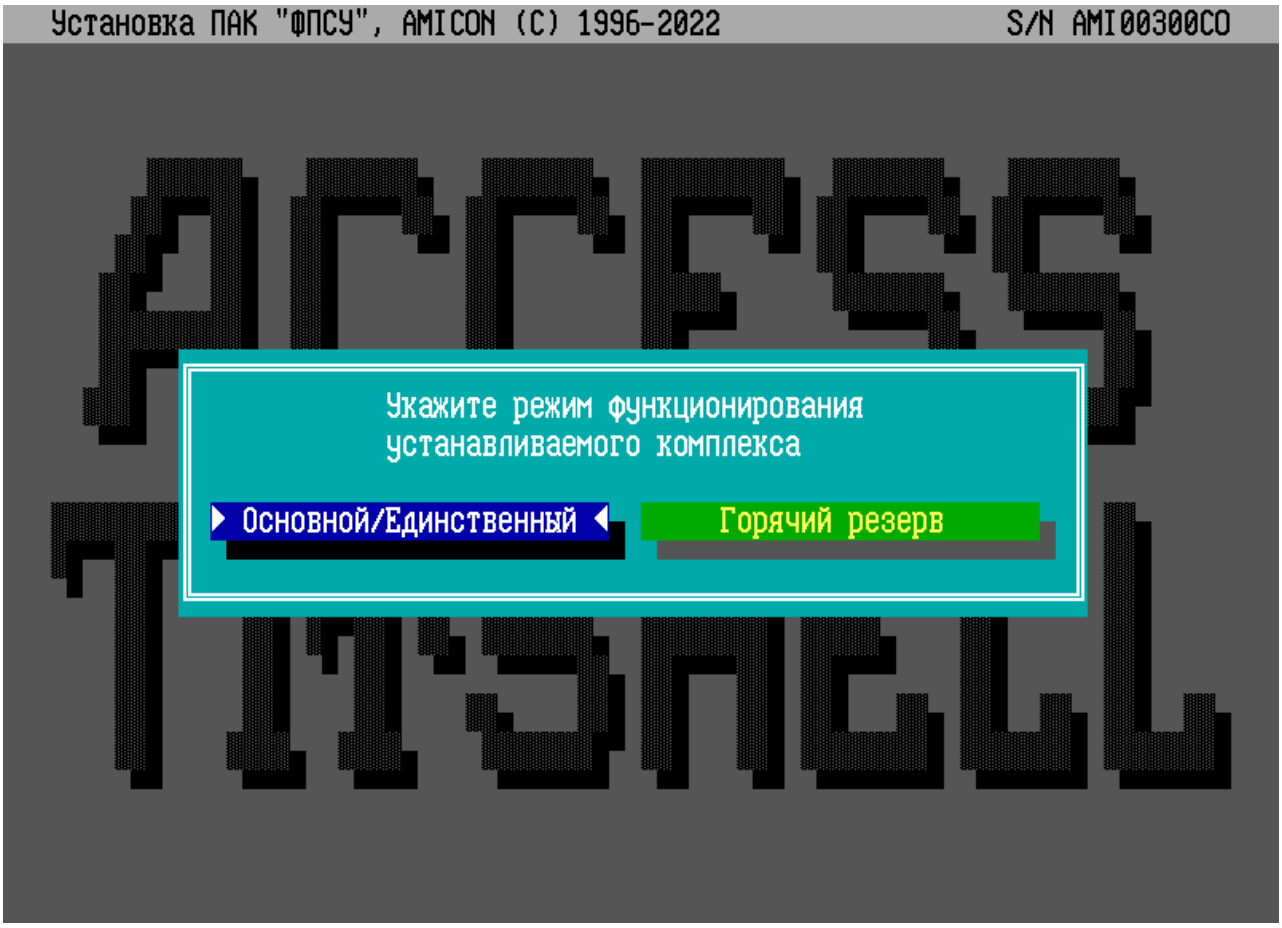


Рисунок 59 - Выбор режима функционирования ФПСУ-IP

После выбора режима функционирования ФПСУ-IP в подсистеме «горячего» резервирования, начнется формирование разделов на диске:

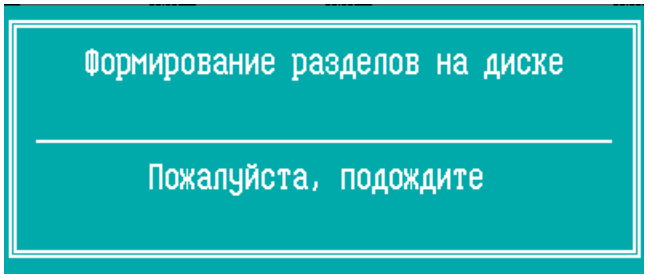


Рисунок 60 - Формирование разделов

Установка программного обеспечения комплекса завершена. ФПСУ-IP будет перезагружен, и после перезагрузки начнет работать в технологическом режиме.

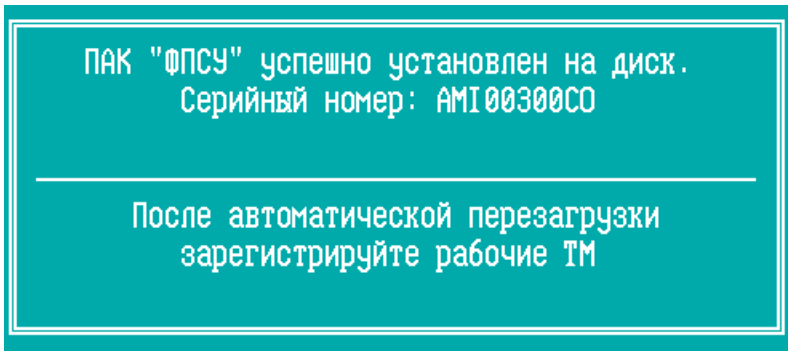


Рисунок 61 - ФПСУ-IP установлен на диск

Отключите USB-носитель с инсталляционным комплектом ФПСУ-IP.

После перезагрузки ФПСУ-IP на экран выдается служебное оповещение о том, что ФПСУ-IP работает в технологическом режиме:

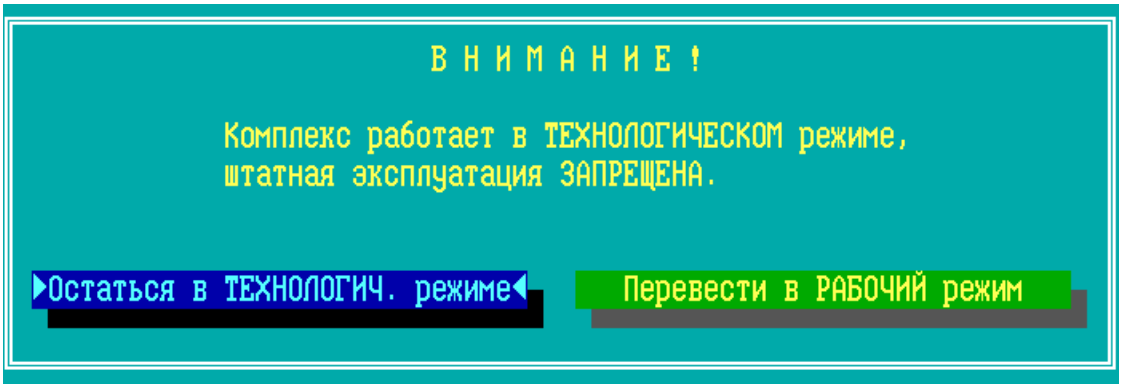


Рисунок 62 - Оповещение о работе в технологическом режиме

Переведите ФПСУ-IP из технологического режима в рабочий, см. пункт «Технологический режим ФПСУ-IP».

Необходимо произвести начальные настройки ФПСУ-IP, зарегистрировать ТМ (см. пункт «Регистрация ТМ-идентификаторов»), сконфигурировать сетевые интерфейсы (см. пункт «Установка драйверов сетевых адаптеров»).

Установка ФПСУ-IP в виртуальную машину QEMU/KVM с USB-носителя с инсталляционным комплектом ФПСУ-IP закончена.

4. Настройка параметров и установка драйверов оборудования

4. 1. Технологический режим ФПСУ-IP

ФПСУ-IP поставляется с установленным программным обеспечением, работающим в технологическом режиме. Кроме этого, технологический режим является режимом по умолчанию после повторной инсталляции программного обеспечения ФПСУ-IP.

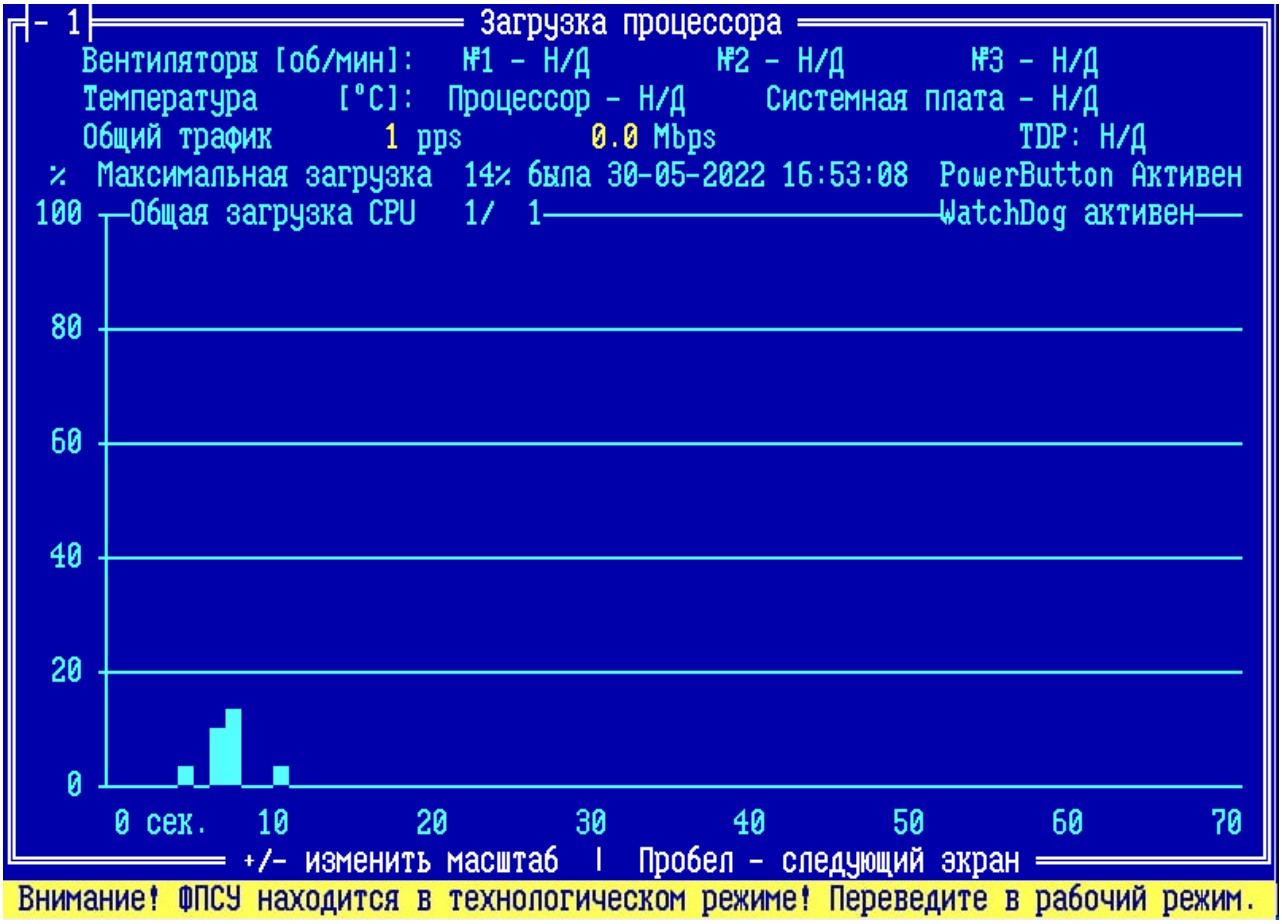


Рисунок 63 - Предупреждение о работе в технологическом режиме

Технологический режим предназначен для первоначальной настройки ФПСУ-IP до ввода в эксплуатацию, и имеет следующие ограничения:

- невозможность работы с подсистемой Клиентов (см. пункт «Клиент для ФПСУ-IP»);
- невозможность работы с подсистемой регистрации ТМ-идентификаторов ФПСУ-IP (см. пункт «Регистрация ТМ-идентификаторов»);
- ограничение работы с ФПСУ-IP горячего резерва (см. пункт «Параметры «Горячего резерва»»). После перевода ФПСУ-IP из технологического режима в рабочий следует повторно провести настройку работы ФПСУ-IP с горячим резервом;

- ограничение работы с ключевыми данными (см. пункты «Установка ключей» и «Использование ключей»). Возможна работа только с тестовыми ключами;
- ограничение взаимодействия с удалёнными ФПСУ-IP в режиме криптозащиты. Возможна работа туннелей только на тестовых, не рабочих ключах.

ВНИМАНИЕ! Тестовые ключи не допускается использовать в рабочем режиме ФПСУ-IP!

При работе в технологическом режиме каждый раз при запуске ФПСУ-IP будет выдаваться служебное оповещение:

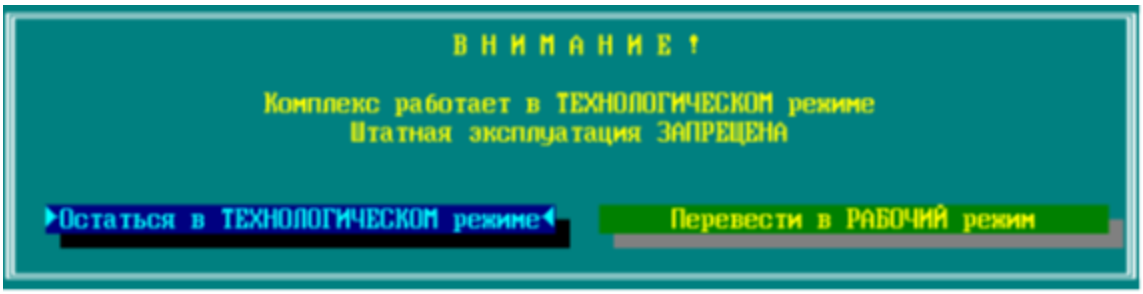


Рисунок 64 - Оповещение о работе в технологическом режиме

Для выхода из технологического режима в штатный, рабочий режим, выберите команду «Перевести в РАБОЧИЙ режим» и нажмите клавишу <*Enter*>. При переводе в рабочий режим ФПСУ-IP требуется произвести инициализацию программно-клавиатурного датчика случайных чисел.

При использовании программно-клавиатурного датчика случайных чисел от администратора требуется ввести указываемые программой цифры (см. рисунок ниже). Дальнейшая работа будет возможна, как только будет осуществлён корректный ввод достаточного числа символов.

Рисунок 65 - Программно-клавиатурный датчик случайных чисел

После инициализации датчика случайных чисел для завершения перехода в рабочий режим будет предложено перерегистрировать ТМ Главного администратора и зарегистрировать ТМ еще одного пользователя (рекомендуется выбрать запасного администратора).

ВНИМАНИЕ! Для корректной работы ФПСУ-IP в режиме криптозащиты следует удалить установленные тестовые ключи парно-выборочной связи и установить рабочие наборы ключевых данных (подробнее см. пункты «Установка ключей» и «Использование ключей»).

4. 2. Установка драйверов сетевых адаптеров

ФПСУ-IP версии 2.65 и выше поддерживает (в зависимости от аппаратной платформы) использование до четырех сетевых адаптеров, работающих в среде передачи данных Ethernet (тип фрейма Ethernet_II). Два адаптера предназначены для передачи данных абонентов, третий и четвертый - для связи с резервным ФПСУ-IP.

Сетевой адаптер, нумерованный в ФПСУ-IP под номером 4, можно использовать для доступа удаленного администратора (см. пункт «Применение 4 порта для доступа удаленного администратора»).

Конкретный тип сетевых адаптеров при их замене должен быть согласован с разработчиком.

Перед установкой или заменой сетевых адаптеров необходимо внимательно изучить документацию на используемое в ФПСУ-IP оборудование с целью его корректной конфигурации, а также во избежание конфликтов в совместной работе.

После установки драйверов необходимо настроить параметры сетевых адаптеров для работы ФПСУ-IP – это будет описано далее, в разделе, «Конфигурация драйверов сетевых адаптеров».

5. 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 66 - Главное меню ФПСУ-IP

В верхней строке окна отображаются: текущая версия операционной среды ACCESS-TM SHELL; режим функционирования ФПСУ-IP в подсистеме горячего резервирования, установленный при инсталляции (Основной или Резервный), а также текущие время и дата на ФПСУ-IP. В нижней строке окна содержится информация об аппаратном обеспечении ФПСУ-IP и времени текущего запуска ФПСУ-IP.

Все команды главного меню описаны подробно в разделах далее.

Команда «Switch to English»/«Переключиться на Русский» позволяет сменить язык в интерфейсе ФПСУ-IP.

5. 1. Запуск ФПСУ-IP

Команда «Запуск ФПСУ» предназначена для перевода ФПСУ-IP из режима конфигурирования в режим фильтрации пакетов. В процессе запуска выполняется загрузка драйверов сетевых адаптеров. Если по какой-либо причине загрузка не может быть

осуществлена, ФПСУ-IP выдаст сообщение об ошибке с диагностикой неисправности. После устранения причины ошибки может быть произведен повторный запуск режима фильтрации.

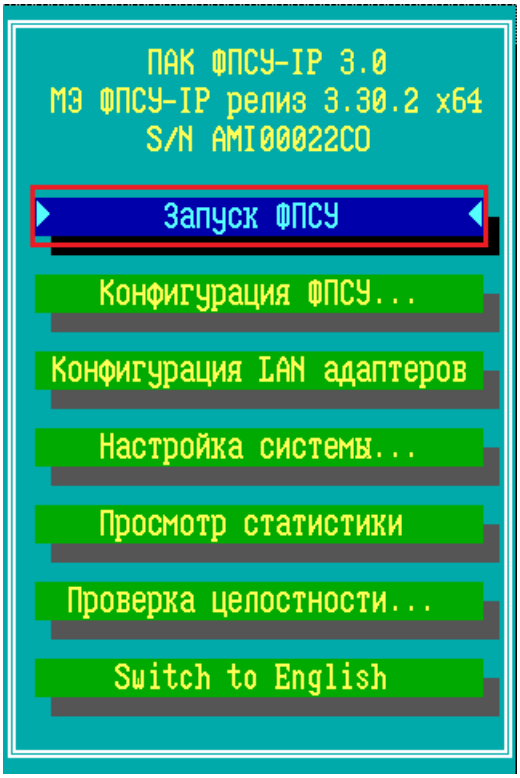


Рисунок 67 - Запуск ФПСУ из главного меню

Команда «Запуск ФПСУ» разрешена допущенным лицам любых классов и выполняется самостоятельно при включении питания ФПСУ-IP в случае задействованной подсистемы автоматического старта.

Если к ФПСУ-IP подключен монитор, во время работы подсистемы фильтрации на экран выводится справочная информация о состоянии сетевых адаптеров, о состоянии ARP-таблицы, о работе подсистемы фильтрации, о взаимодействии с другими ФПСУ-IP и др.

Переключение режимов отображения осуществляется по нажатию функциональных клавиш, информация о назначении которых помещена в статусной строке экрана:

F1 – вывод на экран окна справки о назначении клавиш, информации о версиях (версии и сборке ПО ФПСУ-IP, модели материнской платы), информации об установленных подсистемах (а также количестве ядер процессора), информации об аддонах (dhcp, http-proxy).

F2 – вывод на экран меню управления ключами удаленных администраторов;

F3 – переход на экран отображения состояния сетевых адаптеров рабочих портов;

F4 – переход на экран отображения состояния работы ARP-протокола;

F5 – переход на экран отображения подсистемы фильтрации пакетов абонентов;

F6 – переход на экран отображения состояния взаимодействия с удаленными ФПСУ-IP;

F7 – переход на экран просмотра накопленной за текущие сутки статистики или динамического отображения аппаратного состояния ФПСУ-IP (переключение между режимами осуществляется посредством клавиши <*Пробел*>);

F8 – переход на экран отображения взаимодействия с удаленными администраторами;

F9 – переход на экран отображения состояния связи с клиентами ФПСУ-IP;

F10 – команда завершения работы режима фильтрации и перехода в режим конфигурирования;

F11 – переход на экран отображения состояния «горячего» резервирования;

F12 – переход на диагностический экран для отображения отладочной информации о текущей работе ФПСУ-IP;

ALT+M – нажатие сочетания клавиш включает или отключает вывод на текущий экран мониторинга всплывающих окон с сообщениями о нарушении правил фильтрации.

В верхней строке экрана отображаются текущая версия ПО ФПСУ-IP, текущий статус ФПСУ-IP в процессе «горячего» резервирования, время с момента последнего запуска подсистемы фильтрации и текущее время на ФПСУ-IP.

Для завершения работы режима фильтрации (например, с целью проведения конфигурационных работ или просмотра статистики) нажмите клавишу <*F10*> или сочетание клавиш <*Alt+X*>. После успешной авторизации с помощью ТМ-идентификатора, работа режима фильтрации ФПСУ-IP будет завершена и ФПСУ-IP перейдет в режим конфигурирования.

Примечание. Если подсистема автозапуска ФПСУ-IP задействована, то авторизация для выполнения команды завершения работы режима фильтрации не требуется.

5. 2. Мониторинг аппаратного состояния и суточная статистика

После запуска режима фильтрации (активизации команды «Запуск ФПСУ») ФПСУ-IP переходит в режим динамического отображения состояния аппаратной платформы. Открывается главный экран «Загрузка процессора». Данные для каждого процессора выводятся на отдельном экране. Перемещение между экранами активных процессоров осуществляется нажатием клавиш <→> и <←>.

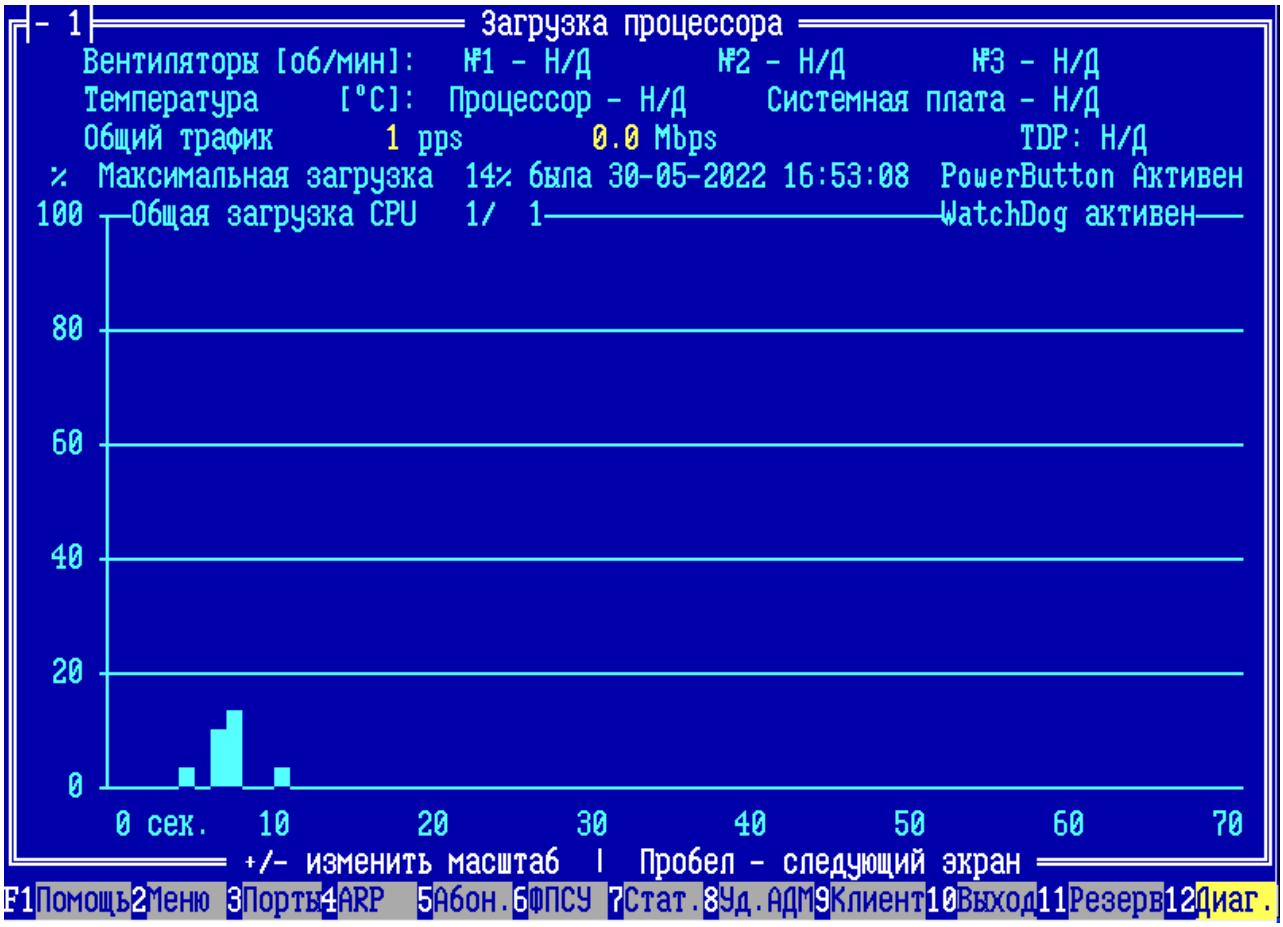


Рисунок 68 - Параметры аппаратного состояния ФПСУ-IP

На экране отображаются параметры (значение параметра «Н/Д» – нет данных или отсутствует):

Вентиляторы - текущая частота вращения вентиляторов в оборотах в минуту.

Температура - текущая температура процессора и системной платы в градусах Цельсия.

Общий трафик - скорость передачи данных в пакетах в секунду и пропускная способность в мегабитах в секунду.

TDP - («thermal design power») потребляемая мощность процессора в ваттах.

Максимальная загрузка - максимальное с момента последнего запуска режима фильтрации значение загрузки процессоров.

PowerButton - индикация активности режима управления кнопкой питания. Значение «Активен» означает, что ФПСУ-IP поддерживает функцию управления кнопкой питания. В этом случае, при нажатии кнопки «Power» на корпусе ФПСУ-IP, программное обеспечение корректно завершит свою работу, передаст управление резервному комплексу (если он доступен), запишет соответствующие сообщения в статистику и отключит электропитание ФПСУ-IP.

WatchDog - индикация активности сторожевого таймера. Значение «Активен» означает, что активирована автоматическая перезагрузка ФПСУ-IP при аппаратном или программном «зависании» комплекса (см. пункт «Общие параметры конфигурации ФПСУ-IP»).

Общая загрузка CPU - количество процессоров (количество активных процессоров/количество процессоров разрешенных в лицензии).

График загрузки процессора. Загрузка (процент использования) процессора за определенный отрезок времени отображается в виде графика, по горизонтальной оси которого откладывается прошедшее время в «секундах тому назад», а по вертикальной – соответствующая этому времени загрузка процессора в процентах. Масштаб изображения можно менять по нажатию клавиш <+> и <−>.

Кроме аппаратного состояния ФПСУ-IP, из данного окна доступен последовательный переход на два дополнительных экрана состояния, «Использование межсетевого экрана» и «Статистика за сутки».

По нажатию клавиши *<Пробел>* на экране «Загрузка процессора» осуществляется переход в окно «Использование межсетевого экрана»:

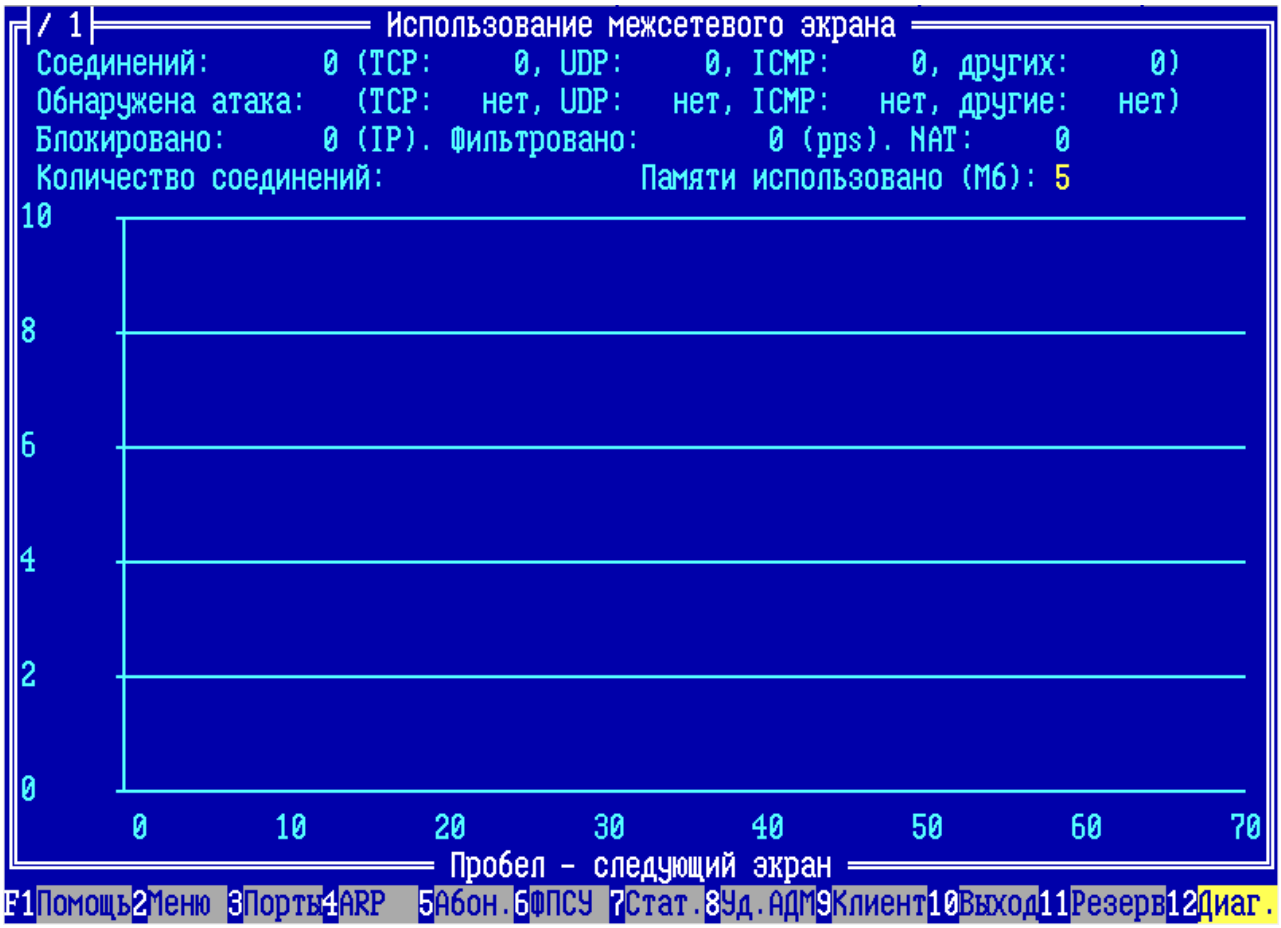


Рисунок 69 - Окно просмотра состояния ФПСУ-IP

Межсетевой экран осуществляет контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. В мониторинге межсетевого экрана выводится отчет об активных соединениях с использованием протоколов транспортного и сетевого уровня, обнаруженных сетевых атаках, блокированных пакетах, скорости фильтрации в пакетах в секунду, используемой памяти для NAT-трансляции в мегабайтах, общем количестве соединений и используемой памяти.

По нажатию клавиши *<Пробел>* в окне «Использование межсетевого экрана» осуществляется переход в режим отображения накопленной с начала суток статистики. Текущая дата отображается вверху окна.

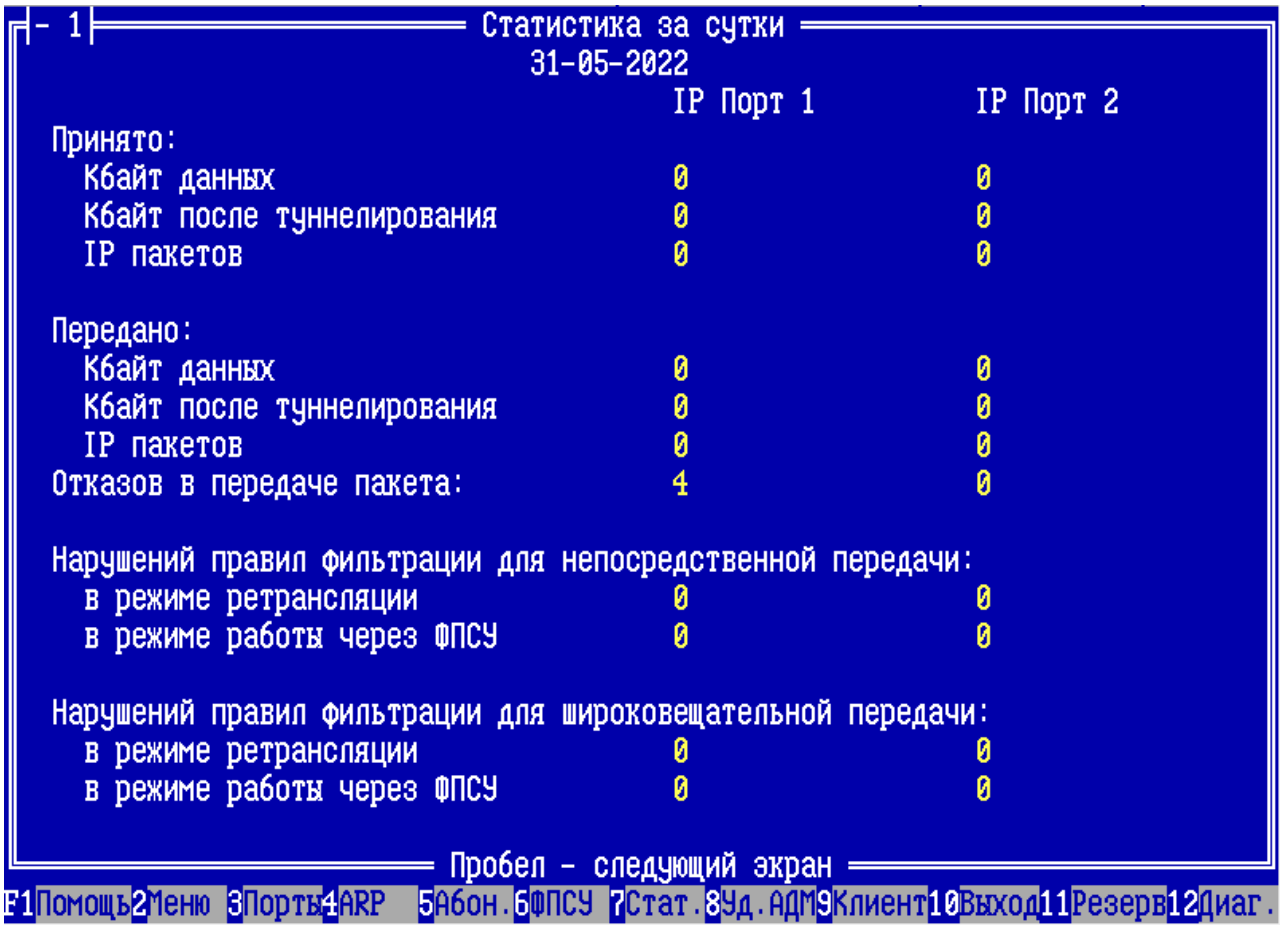


Рисунок 70 - Окно просмотра ежедневной статистки

Для каждого рабочего порта ФПСУ-IP (номера портов отображаются в соответствии с конфигурацией) отображаются сведения:

- количество принятых с этого порта реальных данных абонентов (в килобайтах и IP пакетах), прошедших фильтрацию;
- количество данных в килобайтах, прошедших фильтрацию и полученных из туннеля, возможно зашифрованных и/или сжатых;
- переданные с этого порта абонентские данные в килобайтах и IP-пакетах;
- количество данных в килобайтах, отправленных с этого порта в туннель, возможно зашифрованных и/или сжатых;
- количество отказов в передаче прошедших фильтрацию пакетов по различным причинам, не связанным с фильтрующими функциями ФПСУ-IP: вследствие ошибок фрагментации и дефрагментации, невозможности определить MAC-адрес запрашиваемого абонента, отсутствия соединения с запрашиваемым абонентом и т.д.;
- количество нарушений правил фильтрации со стороны индивидуальных абонентов

для каждого режима работы ФПСУ-IP («Ретрансляция» и «Через ФПСУ»);

- количество нарушений правил фильтрации при широковещательных передачах для каждого режима работы ФПСУ-IP.

По нажатию клавиши <*Пробел*> в окне «Статистика за сутки» осуществляется переход в окно просмотра списка процессов.

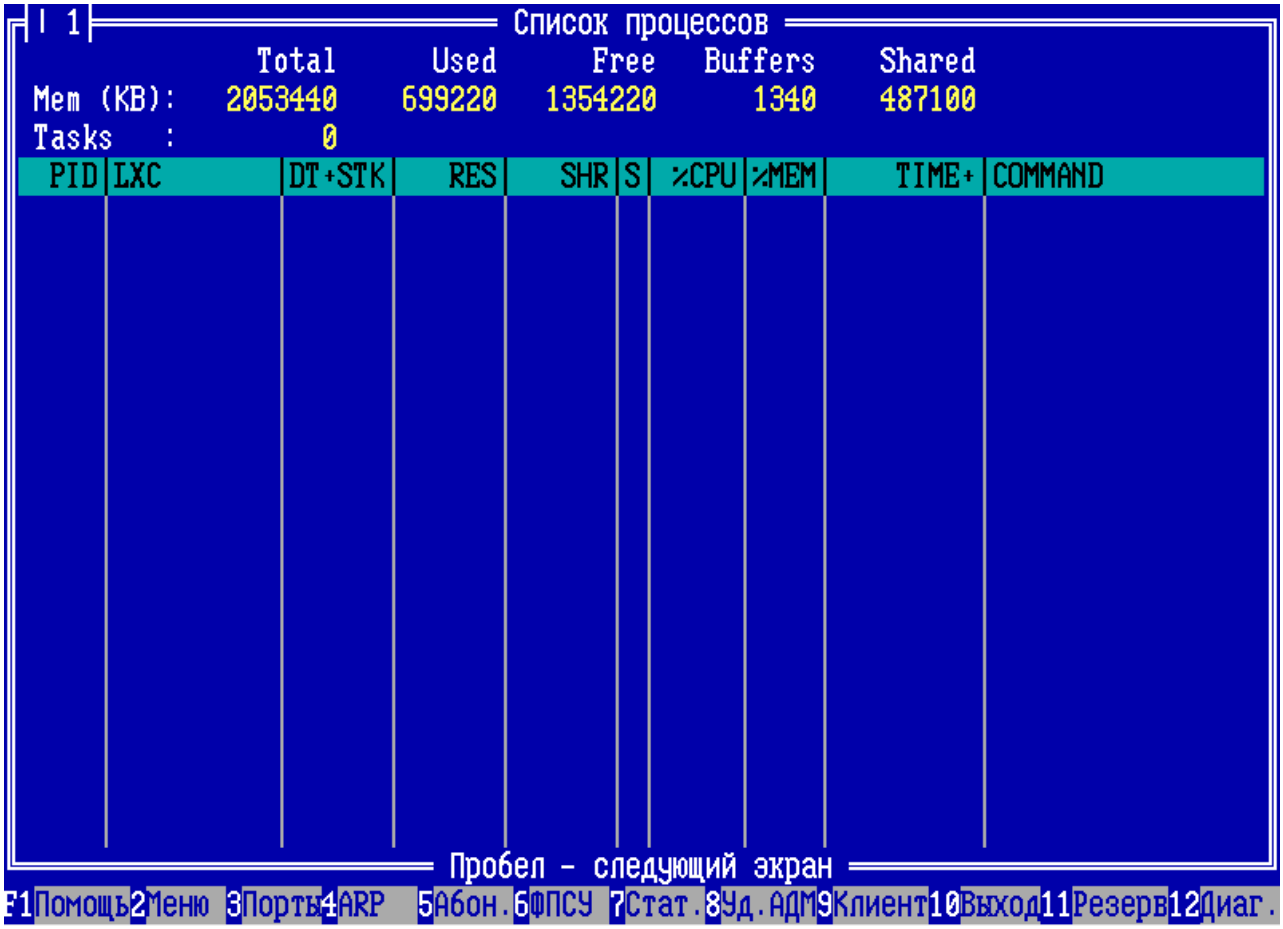


Рисунок 71 - Окно просмотра списка процессов

В окне отображаются сведения о процессах, запущенных подсистемой http-прокси, другими подсистемами и опциональными дополнениями к ПО ФПСУ-IP. Данные аналогичны выводу консольной утилиты top в Linux.

По нажатию клавиши <*Пробел*> на экране «Список процессов» осуществляется переход в окно «Загрузка процессора».

В процессе работы (после перехода в другие информационные окна режима фильтрации) в окно «Загрузка процессора» можно вернуться по нажатию <*F7*>.

5. 3. Окно справки

Вызов окна справочной информации осуществляется по нажатию клавиши *<F1>*, после чего на экран монитора будет выдано меню.

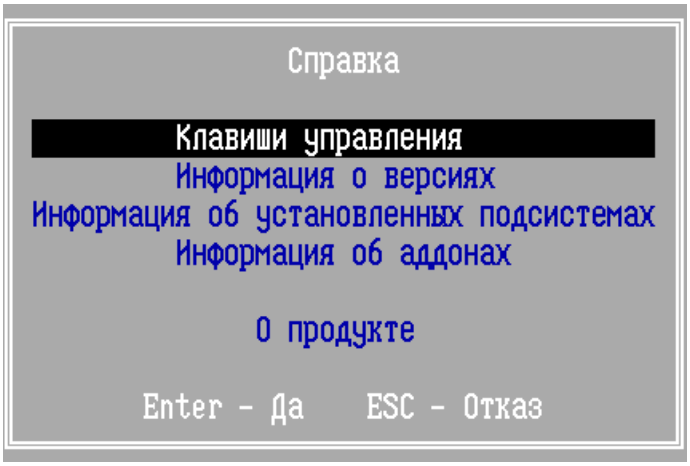


Рисунок 72 - Справочное меню

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.

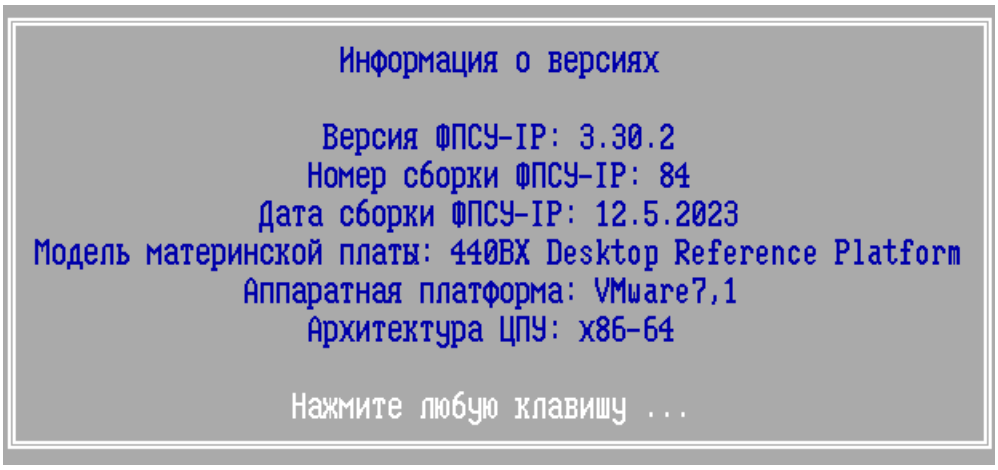


Рисунок 73 - Информация о версиях

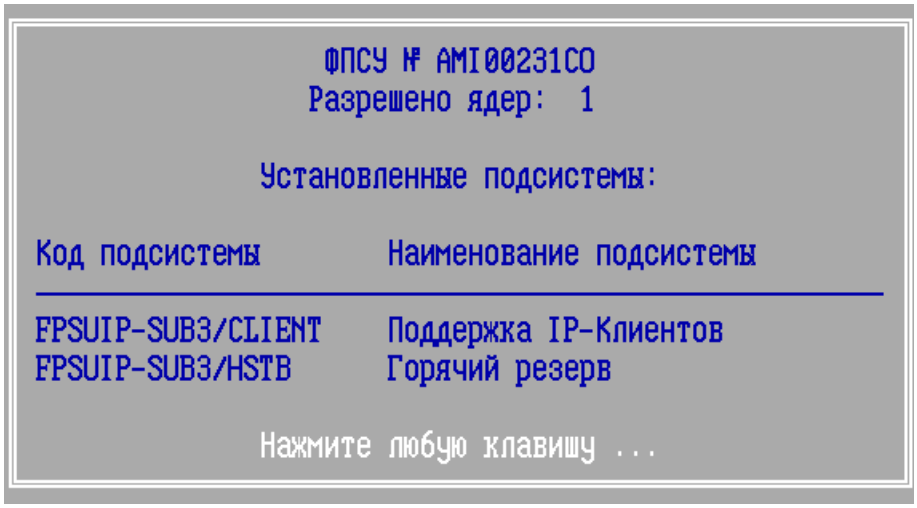


Рисунок 74 - Установленные подсистемы

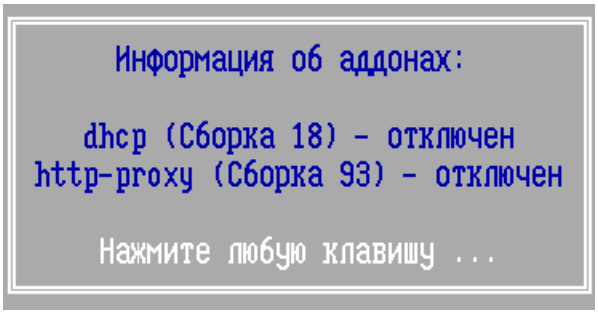


Рисунок 75 - Информация об установленных дополнениях

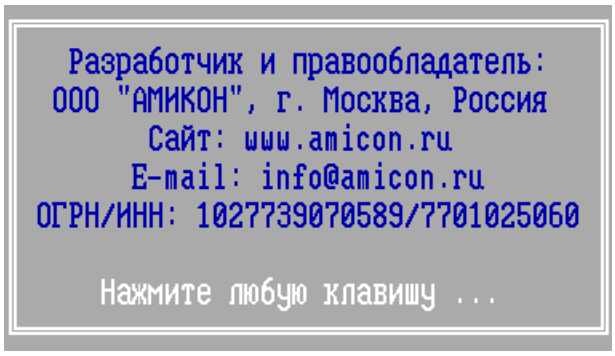


Рисунок 76 - Информация о продукте

5. 4. Меню управления ключами УА

Вызов меню управления ключами удаленных администраторов осуществляется по нажатию клавиши <*F2*>, когда ФПСУ-IP запущен в режиме фильтрация пакетов.

ВНИМАНИЕ! Для платформ с BIOS/Legacy по нажатию клавиши <*F2*> происходит смена языка интерфейса на английский, меню УА недоступно.

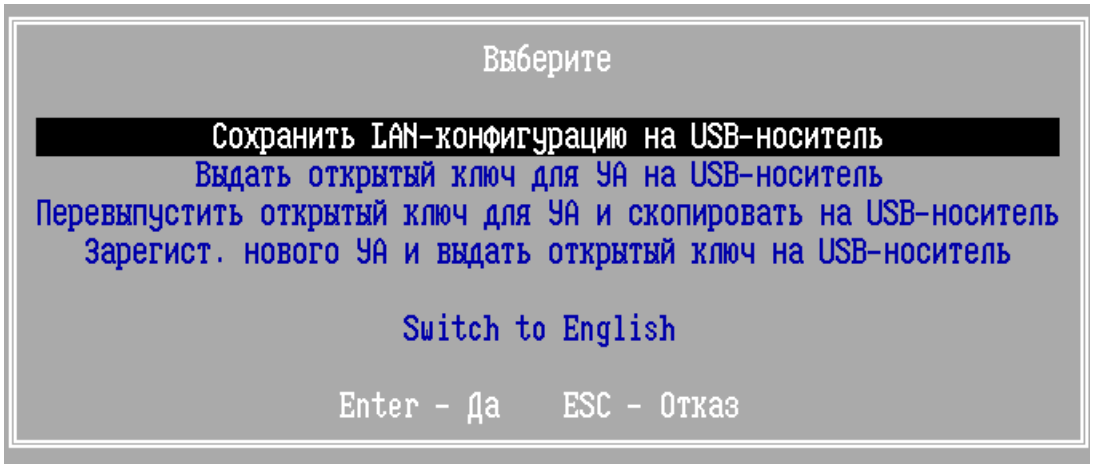


Рисунок 77 - Параметры экрана

Меню УА содержит следующие команды:

- «Сохранить LAN-конфигурацию на USB-носитель» - команда записи текущей конфигурации ФПСУ-IP в специальном формате на съемный носитель без остановки рабочего режима ФПСУ-IP, без перехода в режим конфигурирования. Подключите USB-носитель и выполните команду, будет выдано сообщение об успешном выполнении команды. На внешнем носителе создается каталог с серийным номером ФПСУ-IP с файлом конфигурации с расширением .cfb в разжатом виде. Файл конфигурации .cfb может быть загружен удаленным администратором в программу «Удаленный администратор ФПСУ-IP» для просмотра, изменения и дальнейшей установки на ФПСУ-IP.

- «Выдать открытый ключ для УА на USB-носитель» - команда записи текущего открытого ключа аутентификации ФПСУ-IP на внешний носитель, с целью регистрации его удаленным администратором. Выполняется без остановки рабочего режима ФПСУ-IP, без перехода в режим конфигурирования. Подключите USB-носитель и выполните команду, будет выдано сообщение об успешном выполнении команды. На внешнем носителе создается каталог с серийным номером ФПСУ-IP с файлом с расширением .CO1 - признак основного ФПСУ-IP, .CO2 - горячего резерва. Выдача ключей может быть выполнена также в режиме изменения параметров конфигурации и настройки системы, более подробно см. пункт «Ключи аутентификации ФПСУ-IP».
- «Перевыпустить открытый ключ для УА и скопировать на USB-носитель» - команда выработки нового комплекта ключей аутентификации ФПСУ-IP и записи нового открытого ключа аутентификации ФПСУ-IP на внешний носитель, с целью регистрации его удаленным администратором.
- «Зарегист. нового УА и выдать открытый ключ на USB-носитель» - команда регистрации учетной записи удаленного администратора ФПСУ-IP. На USB-носителе может быть не более одного описателя удаленного администратора, иначе новый удаленный администратор не будет зарегистрирован.
- «Switch to English» - смена языка интерфейса на английский.

5. 5. Окно состояния рабочих LAN портов

Выход в режим отображения состояния рабочих портов ФПСУ-IP осуществляется по нажатию клавиши <*F3*>, после чего будет выведено окно, представленное на рисунке ниже.

Окно разделено на две половины, в каждой из которых отображается состояние одного из портов ФПСУ-IP, используемых для связи локальных подсетей и передачи пакетов абонентов. Выводимые параметры разбиты на три группы.

Первая группа содержит сведения о конфигурационных установках порта - параметрах используемого сетевого адаптера, Ethernet- и IP-адресах порта, маске подсети, связанной с портом, установленном на LAN-адаптере MTU; а также о скорости приема и передачи данных по порту в пакетах в секунду, pps, и в Мбит/с.

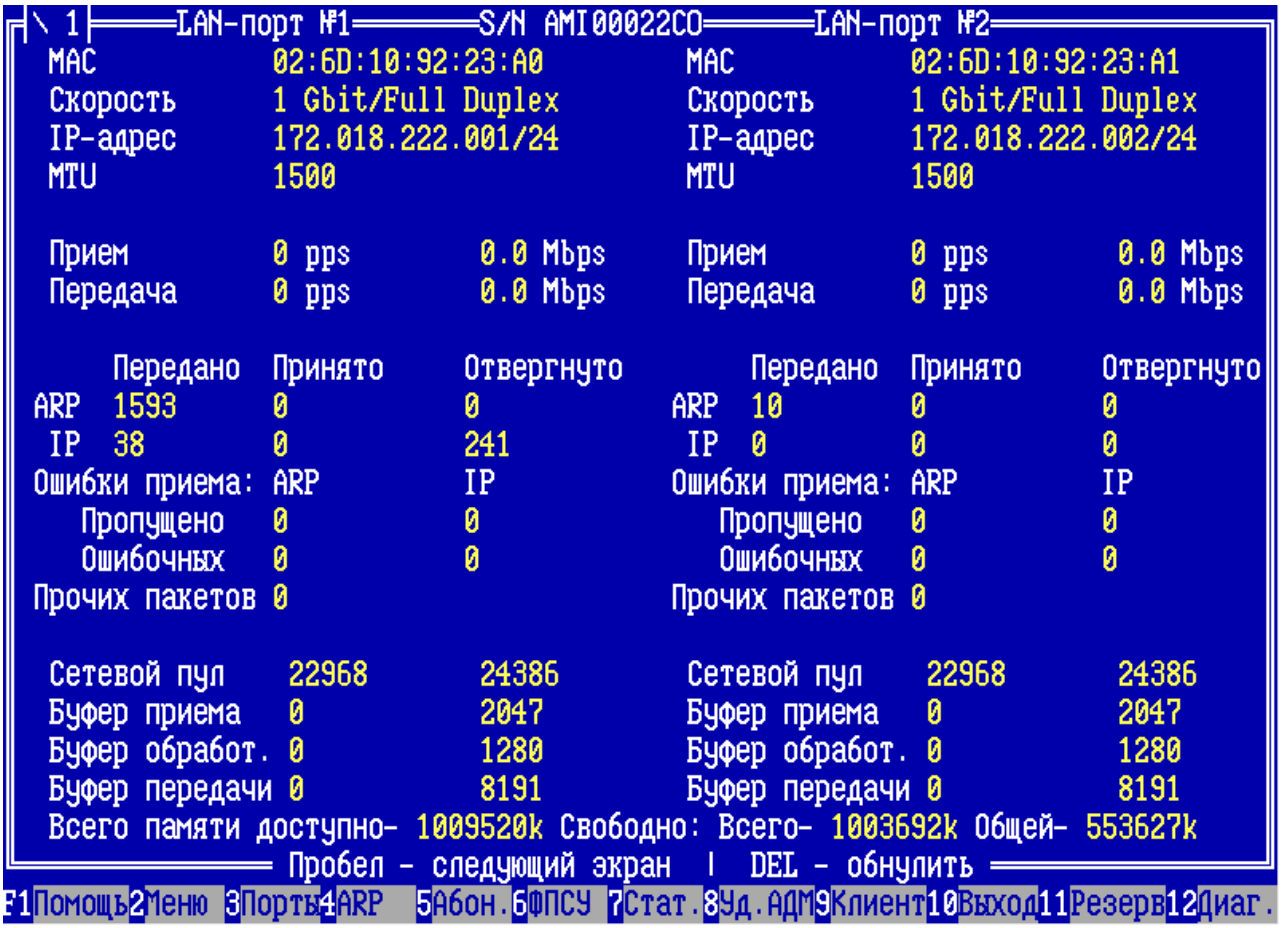


Рисунок 78 - Состояние рабочих портов ФПСУ-IP

Вторая группа отображает статистику событий на сетевом адаптере с момента запуска подсистемы фильтрации. Она содержит сведения о количестве поступивших на сетевой адаптер по сети пакетов различных протоколов (до фильтрации), переданных с этого адаптера в сеть пакетах различных протоколов, отвергнутых пакетах (не прошедших фильтрацию или по причине неполадок сетевого уровня) и пакетах, содержащих ошибки кадрового уровня. Если перед каким-либо значением стоит символ «*» - соответствующий счетчик превысил значение 4294967296 и начал отсчет с нуля. Нажатие клавиши *<Del>* сбрасывает накопленную с момента запуска статистику в нулевые значения.

Третья группа значений демонстрирует состояние динамической памяти протокольного стека и носит справочный характер:

Сетевой пул — количество памяти в ethernet пакетах (фреймах), область выделенная в оперативной памяти ФПСУ-IP, в которую сетевая карта помещает полученные фреймы. Размер пула указан в строке «Сетевой пул». Первое значение - сколько свободных частей памяти для фреймов есть в пуле, второе значение - размер пула. Как правило, один фрейм занимает одно значение в пуле. В зависимости от версии ФПСУ-IP и конфигурации

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»:

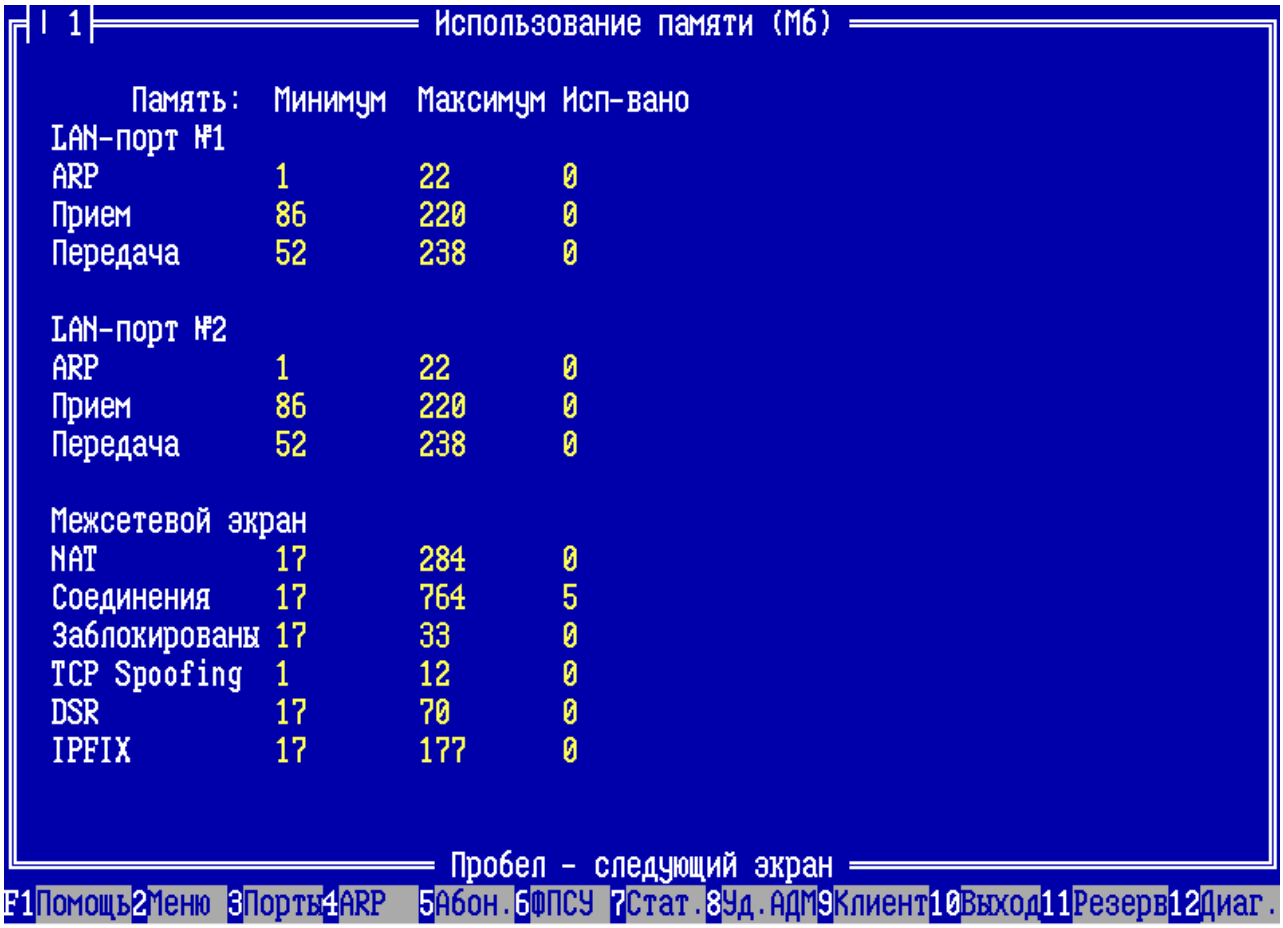


Рисунок 79 - Использование памяти ФПСУ-IP

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»:

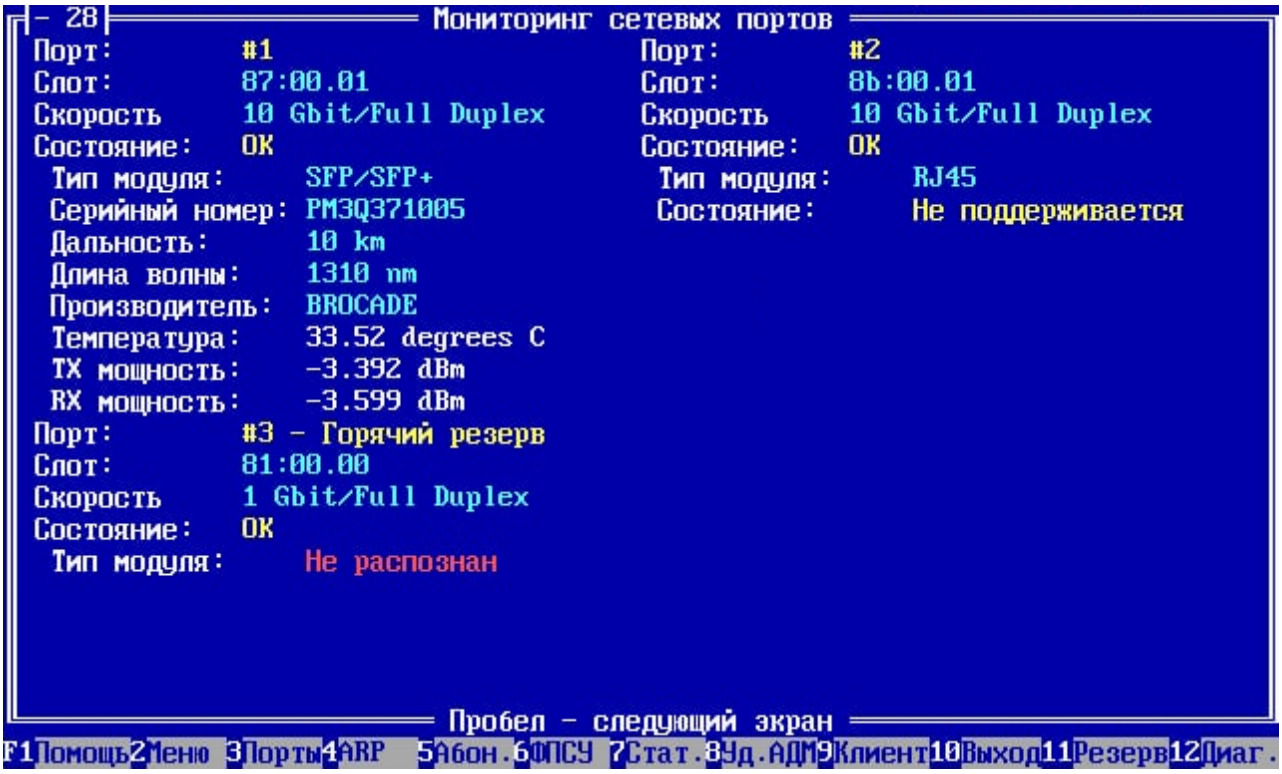


Рисунок 80 - Мониторинг сетевых портов ФПСУ-IP версии 3.30.1

На платформах с версией 3.30.1 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.

Для платформ версий 3.30.2 мониторинг SFP модулей не отображается.

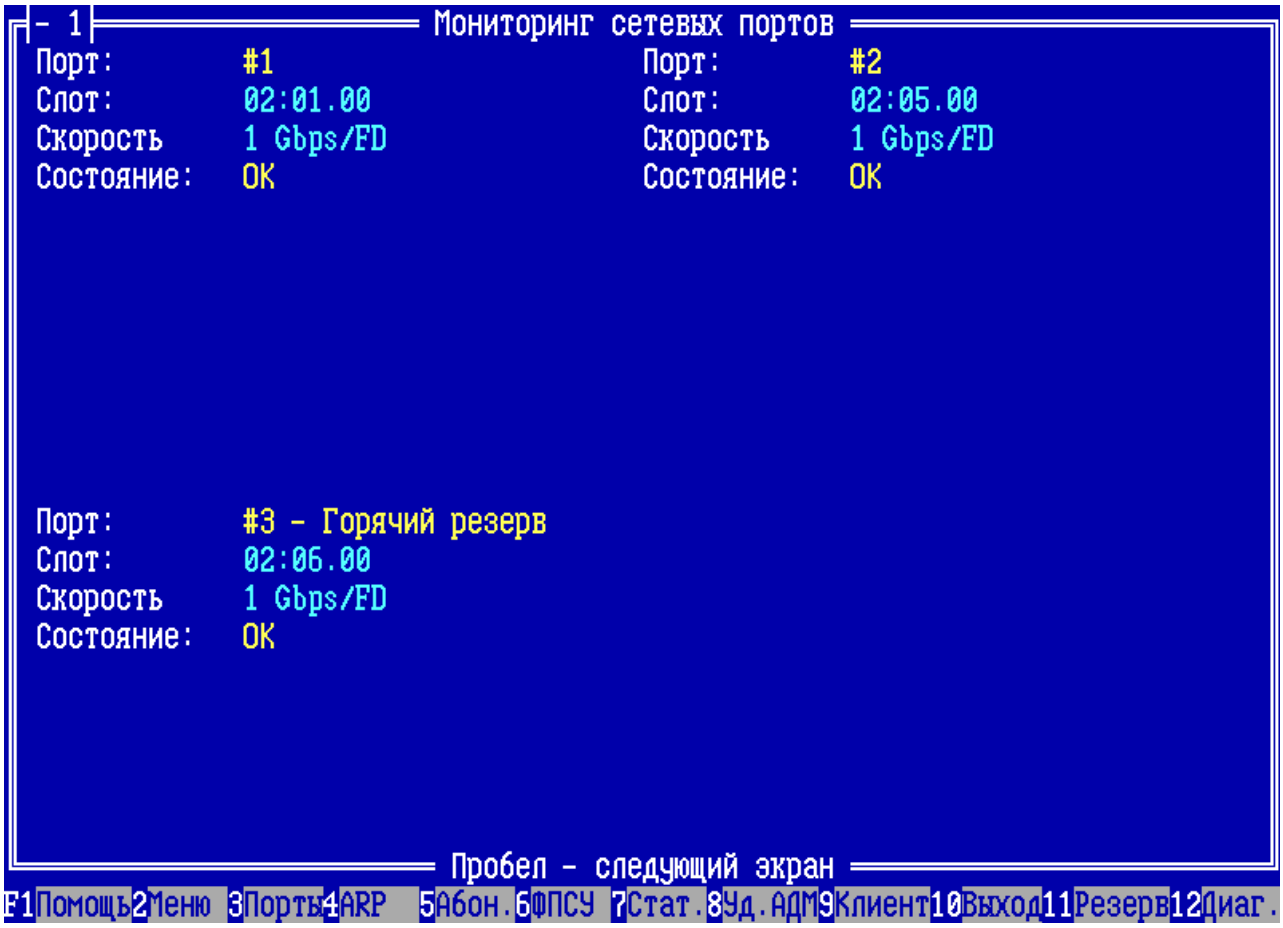


Рисунок 81 - Мониторинг сетевых портов ФПСУ-IP версии 3.30.2

5. 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.

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.

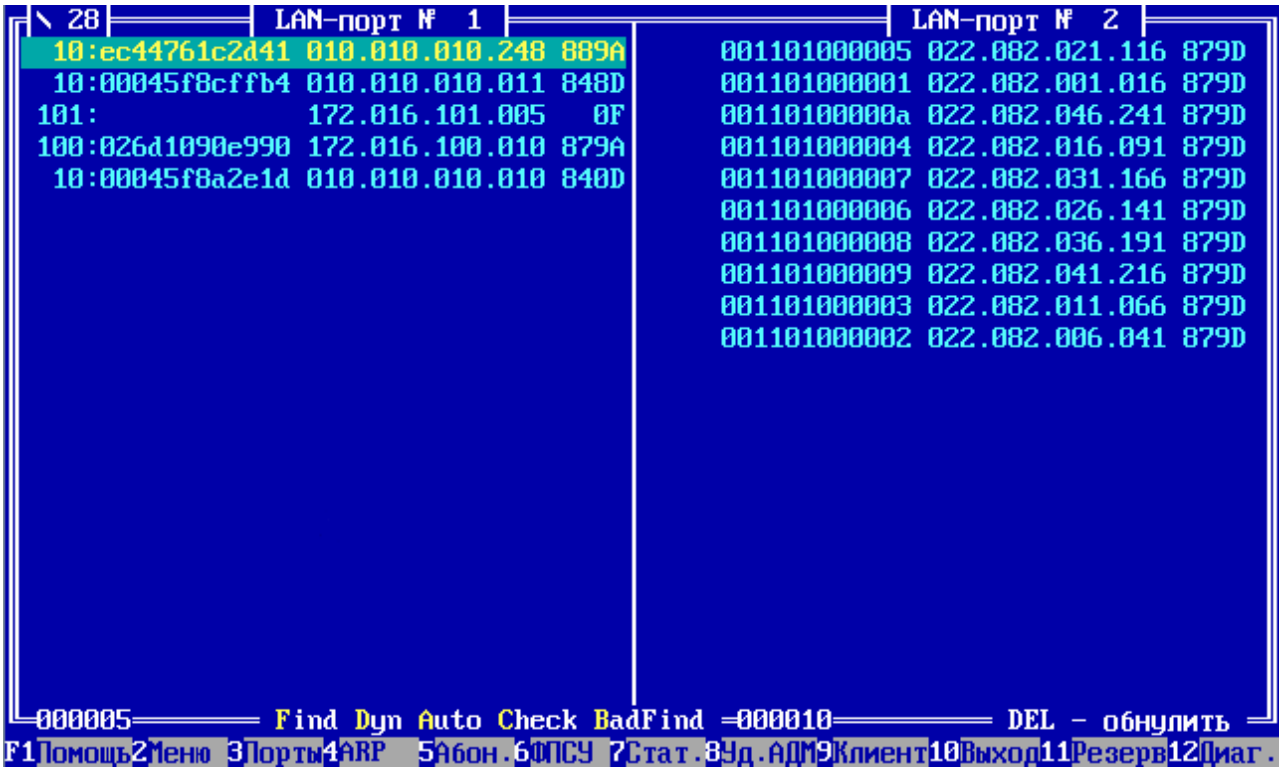


Рисунок 82 - Состояние ARP-кэша

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 <↓>, а между половинами окна - при помощи клавиш <*Tab*>, <←> и <→>.

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

5. 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 <↓>).

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.

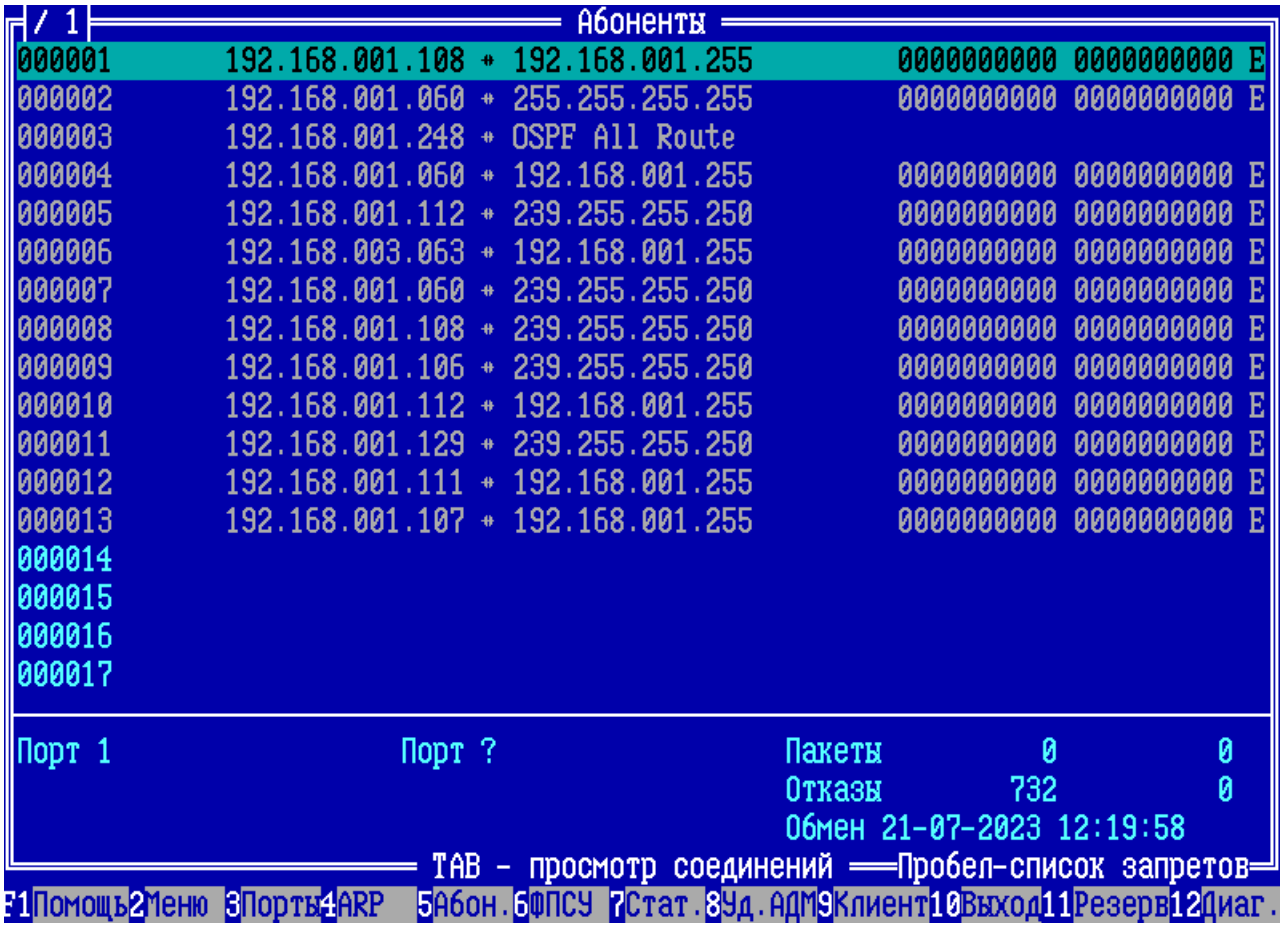
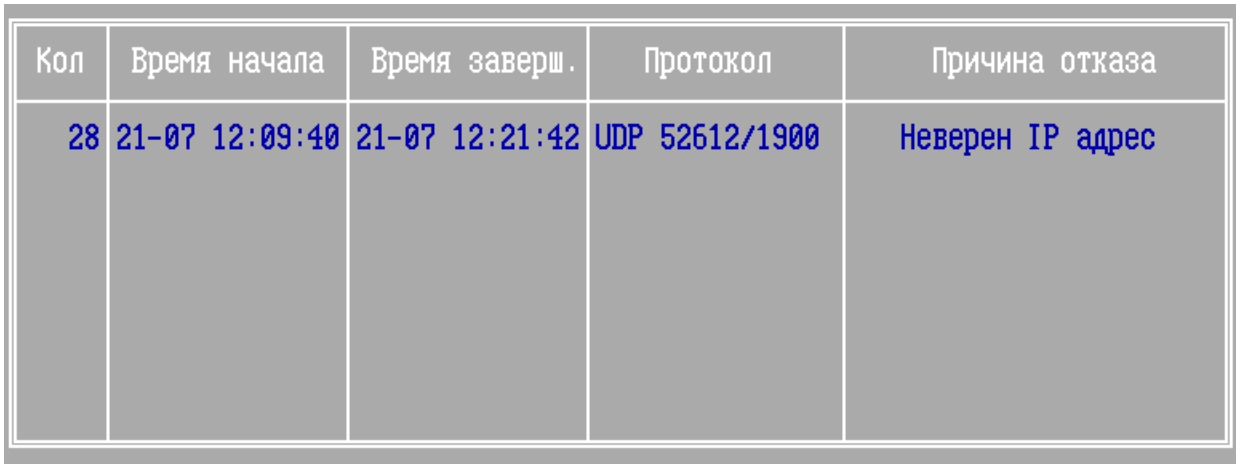


Рисунок 83 - Статистика переданных IP-пакетов

Для записи, в которой стоит признак ошибки («Err»), может быть вызвано окно, содержащее более подробные сведения о работе данной пары абонентов и причине отказа. Для этого нужно установить на строку курсор и нажать клавишу <*Пробел*>.



Кол	Время начала	Время заверш.	Протокол	Причина отказа
28	21-07 12:09:40	21-07 12:21:42	UDP 52612/1900	Неверен IP адрес

Рисунок 84 - Информация об ошибке

В окне отображаются количество отказов для данной пары абонентов, дата и время

первого и последнего отказов, протокол, которому принадлежат пакеты, и причина отказа. Могут быть указаны следующие причины:

Ошибка МЭ	- запрет работы правилами межсетевого экрана (см. пункт «Параметры доступа, правила трафика межсетевого экрана»);
Мало памяти	- недостаточно оперативной памяти для обработки пакета;
Неверен IP адрес	- неверен IP адрес отправителя (широковещательный);
Короткий пакет	- ошибка формата пакета;
Дублирование адресов	- MAC-адрес отправителя равен MAC-адресу LAN-адаптеров ФПСУ-IP;
Входящий не описан	- отправитель пакета не прописан в конфигурации портов ФПСУ-IP (маршрутизации);
Получатель не описан	- получатель пакета не описан в конфигурации портов ФПСУ-IP (маршрутизации);
Запрет работы	- отказ в доступе по причине «запрет работы» в конфигурации портов ФПСУ-IP для одного или обоих абонентов-участников обмена;
Абонент миновал ФПСУ	- абонент в конфигурации портов ФПСУ-IP указан как работающий через VPN-туннель с другим ФПСУ-IP, но его пакеты приходят не из VPN-туннеля;
ФПСУ не работает	- ФПСУ-IP на другой стороне VPN-туннеля не работает, невозможно установить VPN-туннель и отправить пакет абонента;
Маршрут неизвестен	- неизвестен MAC-адрес получателя, невозможно маршрутизировать пакет дальше;
Истекло время	- истекло время жизни пакета (параметр TTL), и пакет в соответствии с правилами работы стека TCP/IP был сброшен;
Ложный ФПСУ	- станция пытается подменить ФПСУ-IP в установки VPN-туннеля;

Протокол недоступен	- обращение к ФПСУ-IP не поддерживаемым протоколом. Пакет не принадлежит к пакетам стека протоколов TCP/IP или другим поддерживаемым протоколам;
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.

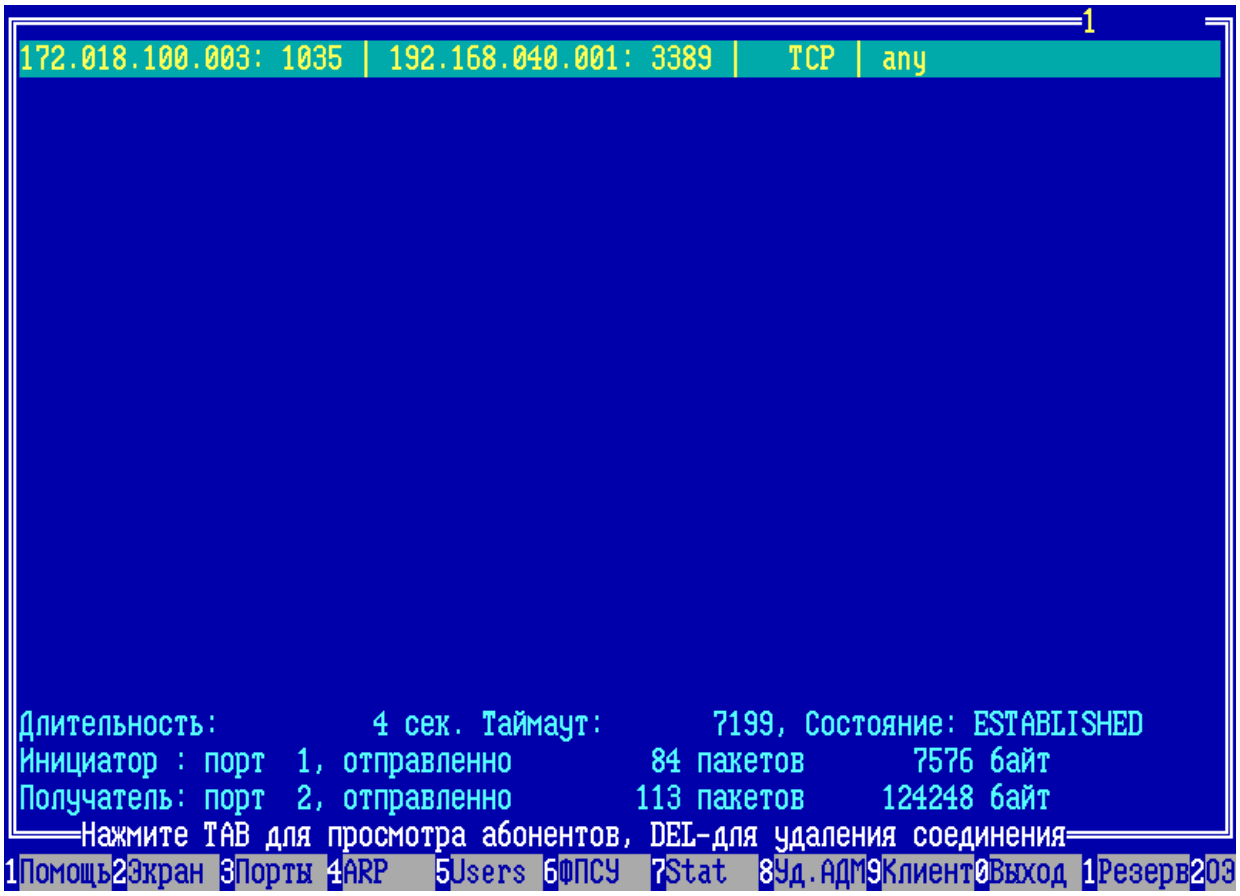


Рисунок 85 - Таблица состояния соединений ФПСУ-IP

В блоке дополнительной информации о соединении в нижней части окна предоставляются следующие сведения:

- длительность соединения;
- таймаут неактивности соединения, время в секундах, по истечении которого соединение будет удалено из таблицы состояний ФПСУ-IP;
- текущее состояние сессии;
- порт инициатора и получателя соединения;
- объем переданных в рамках соединения данных, в пакетах и байтах.

Любой локальный администратор ФПСУ-IP может удалить выбранное курсором соединение, нажав клавишу <Del>. После успешной авторизации с помощью ТМ-идентификатора, выбранное соединение будет удалено из таблицы состояния соединений ФПСУ-IP.

Примечание. Если подсистема автоматического старта ФПСУ-IP задействована, то авторизации администратора для удаления соединения не требуется.

5. 8. Окно состояния VPN-туннелей с другими ФПСУ-IP

Вход в режим отображения состояния работы VPN-туннелей с другими ФПСУ-IP осуществляется по нажатию клавиши *<F6>*. При этом на экран будет выдано справочное окно (см. рисунок ниже).

В окне отображаются сведения о ФПСУ-IP, работающих в паре с данным ФПСУ-IP со стороны каждого из двух рабочих портов. Для каждого порта указан список записей, содержащих IP-адрес удаленного и сведения о состоянии внутреннего протокола обмена между ними.

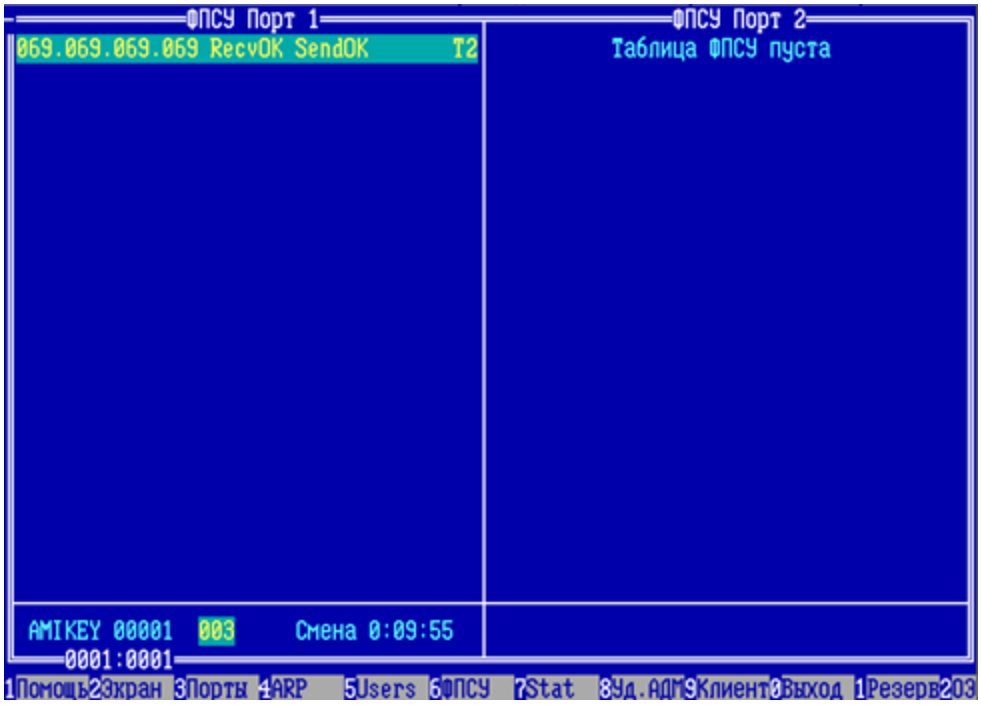


Рисунок 86 - Состояние туннелей с другими ФПСУ-IP

Состояния туннеля могут быть следующими:

- *RecvOk SendOk/Готов* - туннель работоспособен, состояние показывает что соединение с другим ФПСУ-IP прошло успешно и туннель готов принимать и передавать данные абонентов;
- *RecvOk* - прием возможен и разрешен;
- *NoRecv* - прием данных от другого ФПСУ-IP невозможен;
- *SendOk* - передача возможна и разрешена;
- *NoSend* - передача данных другому ФПСУ-IP невозможна;

- *WaitARP/Жду ARP* - прием и передача данных абонентов невозможны, маршрут до удаленного ФПСУ-IP неизвестен (в частности, неизвестен MAC-адрес сетевого устройства, которому требуется передать фрейм для дальнейшей маршрутизации);
- *WaitSynRR* - прием и передача данных абонентов невозможны, ожидается разрешение синхронизации от удаленного ФПСУ-IP. Отображается в случаях ошибок с парно-выборочными ключами на текущем или удаленном ФПСУ-IP (например, не согласованность конфигураций ФПСУ-IP в используемых номерах ключевых данных, серии или криптосети; ошибки чтения файла с ключевыми данными). Также отображается когда по указанному IP-адресу находится не ФПСУ-IP, а другое устройство, с которым невозможно установить VPN-туннель;
- *WaitSynOk* - прием и передача данных абонентов невозможна, ожидается синхронизация с удаленным ФПСУ-IP;
- *Ошибка сериализации* - удаленный и локальный ФПСУ-IP имеют одинаковые серийные номера, установление соединения невозможно.

После разрешения синхронизации возможны следующие дополнительные сообщения:
! - для данного туннеля не задействовано шифрование передаваемых данных;
K - для шифрования данных в VPN-туннеле используется блочный шифр «Кузнечик»;
M - для шифрования данных в VPN-туннеле используется блочный шифр «Магма»;
G - для шифрования данных в VPN-туннеле используется блочный шифр «Магма», используемый в режиме MGM (Multilinear Galois Mode);
L2 - согласован режим VPN-туннеля «мост» между ФПСУ-IP (L2-шифровние);
Aut - ожидается подтверждение на выданный удаленному ФПСУ-IP сеансовый аутентификатор;
C - согласован режим потокового сжатия данных абонентов в VPN-туннеле между двумя ФПСУ-IP;
T - согласован режим криптозащиты данных абонентов в VPN-туннеле между двумя ФПСУ-IP;
P - согласован режим пакетного шифрования данных абонентов. Этот маркер появляется только тогда, когда хотя бы на одном из двух участвующих в построении туннеля ФПСУ-IP установлена версия программного обеспечения меньше 3.0;
Q - для шифрования данных в VPN-туннеле используются квантово-защищенные ключи, полученные от устройств КРК (квантового распределения ключей).
2 – этот маркер означает, что канал построен между двумя ФПСУ-IP с версиями программного обеспечения 3.0 и выше.

В нижней части экрана для текущего удаленного ФПСУ-IP отображаются согласованные используемые им ключи и время, оставшееся до смены сеансовых ключевых данных.

5. 9. Окно состояния связи с удаленными администраторами

Для просмотра состояния работы ФПСУ-IP с удаленными администраторами нажмите клавишу <*F8*>.

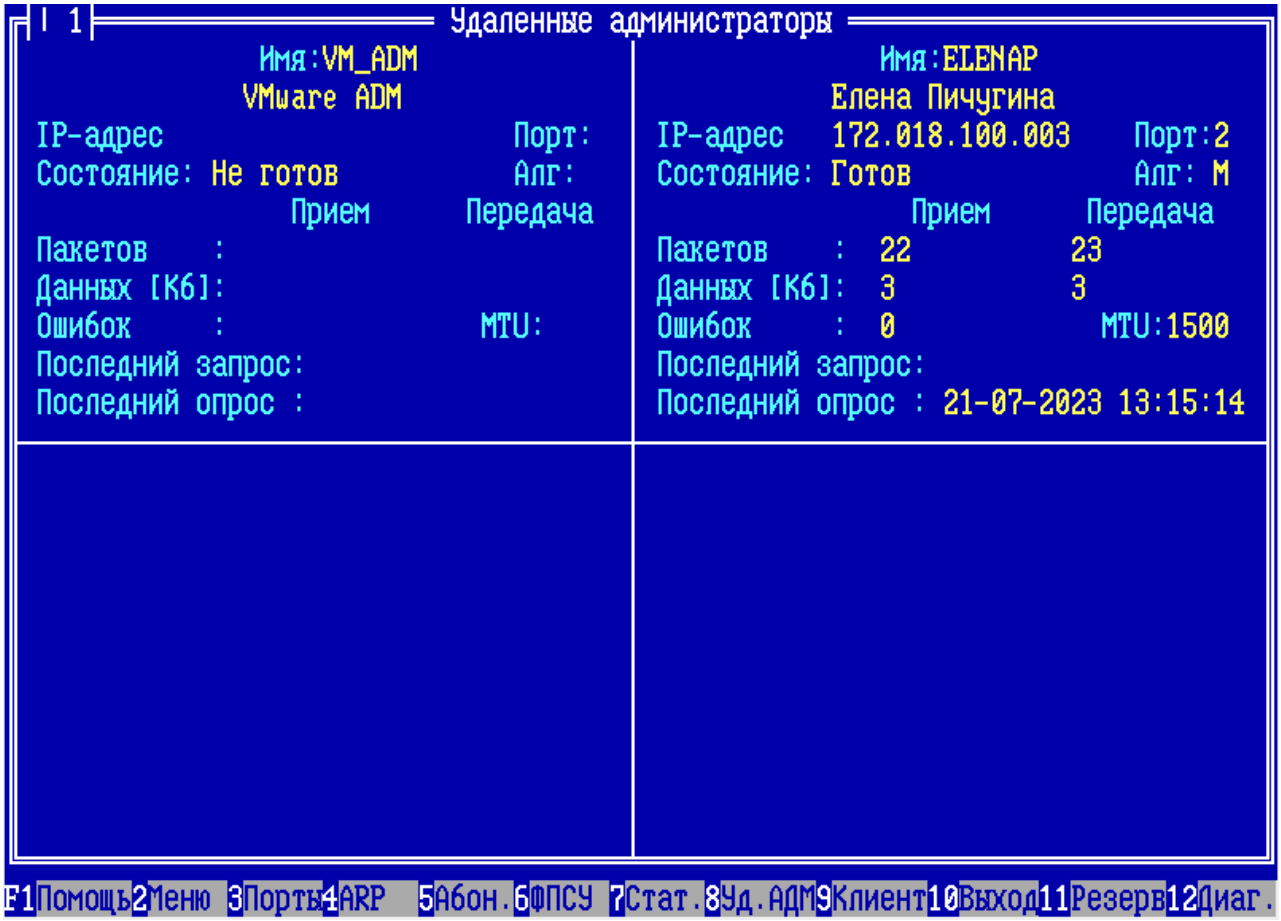


Рисунок 87 - Просмотр состояния удаленных администраторов

ФПСУ-IP отображает сведения обо всех зарегистрированных на нем удаленных администраторах, для каждого администратора указываются:

- имя администратора, комментарий к имени;
- IP-адрес и порт АРМ удаленного администратора;
- текущее состояние соединения ФПСУ-IP с удаленным администратором (готов, не готов, устанавливается);
- алгоритм, по которому строится туннель между ФПСУ-IP и удаленным администратором;
- количество переданных данных за время существования соединения ФПСУ-IP с АРМ удаленного администратора, в байтах и пакетах;
- количество ошибок соединения и запросов за время существования соединения

ФПСУ-IP с АРМ удаленного администратора;

- MTU соединения ФПСУ-IP с АРМ удаленного администратора;
- время и тип последнего запроса с АРМ удаленного администратора к ФПСУ-IP;
- время последнего опроса текущего состояния ФПСУ-IP удаленным администратором.

На экране отображаются два удаленных администраторов из списка зарегистрированных на ФПСУ-IP. Перемещение по списку удаленных администраторов осуществляется с помощью клавиш <*PageUp*> и <*PageDown*>.

5. 10. Окно мониторинга подключенных ФПСУ-IP/Клиентов

Для просмотра информации о текущем взаимодействии ФПСУ-IP как VPN-шлюза с VPN-клиентами, программными и программно-аппаратными комплексами ФПСУ-IP/Клиент, нажмите <*F9*>.

Для каждого ФПСУ-IP/Клиента, работающего в текущий момент времени через ФПСУ-IP, отображаются:

- имя, данное ФПСУ-IP/Клиенту администратором Криптосети Клиентов при генерации ключей ФПСУ-IP/Клиента;
- IP-адрес ФПСУ-IP/Клиента, присвоенный ему администратором ФПСУ-IP (статический NAT-адрес для работы ФПСУ-IP/Клиента в защищенном сегменте IP-сети);
- номер порта ФПСУ-IP, с которым соединён ФПСУ-IP/Клиент в настоящее время;
- количество байт данных, принятых от ФПСУ-IP/Клиента и переданных ему с ФПСУ-IP;
- маркер, указывающий на алгоритм шифрования данных:

  P – пакетное шифрование данных, отображается только когда к ФПСУ-IP подключен ФПСУ-IP/Клиент с версией программного обеспечения меньше 5.0 (использующий СКЗИ «Туннель 2.0»), передаваемые данные между ФПСУ-IP и ФПСУ-IP/Клиентом шифруются по алгоритму ГОСТ 28147-89;

  m – передаваемые данные между ФПСУ-IP и ФПСУ-IP/Клиентом шифруются по алгоритму «Магма»;

  M – передаваемые данные между ФПСУ-IP и ФПСУ-IP/Клиентом шифруются по алгоритму «Магма MGM»;

  C – при передаче данных используется сжатие.

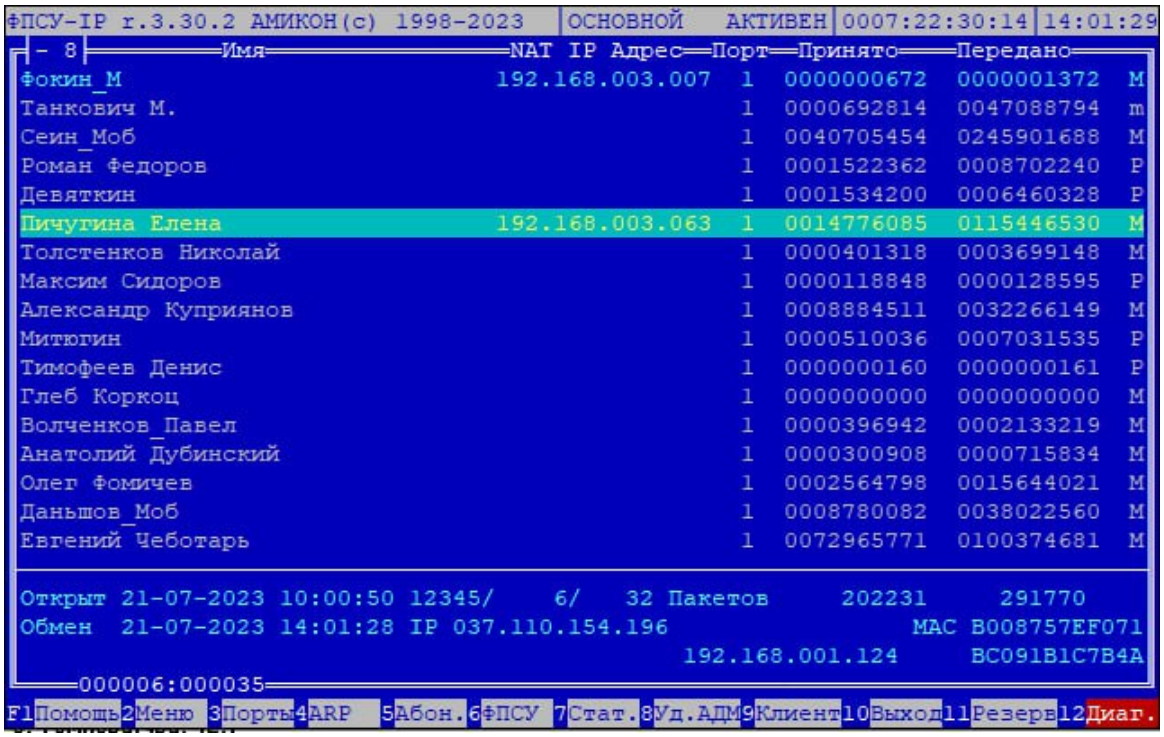


Рисунок 88 - Отображение состояния работы Клиентов

Для выделенного ФПСУ-IP/Клиента списка, в нижней части окна отображаются дополнительные сведения:

- дата и время открытия туннеля - соединения ФПСУ-IP/Клиента с ФПСУ-IP;
- системные идентификаторы ФПСУ-IP/Клиента (номер Криптосети, номер группы в рамках Криптосети и номер пользователя ФПСУ-IP/Клиента в группе);
- количество пакетов, принятых от ФПСУ-IP/Клиента и переданных ему с ФПСУ-IP;
- дата и время последнего обмена данными между ФПСУ-IP и ФПСУ-IP/Клиентом;
- IP-адрес рабочей станции, с которой подключился ФПСУ-IP/Клиент;
- MAC-адрес ФПСУ-IP/Клиента в ARP-таблице ФПСУ-IP.

Цифры в нижней строке окна (000001:000001) обозначают номер текущей строки, на которую установлен курсор, и общее количество подключенных ФПСУ-IP/Клиентов в списке.

Окно содержит информацию о соединениях ФПСУ-IP/Клиентов только с ФПСУ-IP. Для того, чтобы проследить за процессом взаимодействия ФПСУ-IP/Клиентов с рабочими станциями назначения, следует по нажатию клавиши <*F5*> перейти в режим мониторинга переданных через ФПСУ-IP пакетов (см. пункт «Окно состояния работы пользователей»).

5. 11. Окно состояния подсистемы «горячего» резервирования

Вызов окна отображения состояния текущей работы ФПСУ-IP с партнером по резервированию осуществляется по нажатию клавиши *<F11>*.

Если подсистема горячего резервирования не была задействована, то на этом экране находится только текст «подсистема горячего резервирования не сконфигурирована». Дальнейший текст в пункте предполагает, что подсистема горячего резервирования ФПСУ-IP была сконфигурирована и задействована (см. пункт «Параметры «Горячего резерва»»).

В окне отображается статистическая информация о количестве и состоянии VPN-туннелей (защищенных каналов связи между наблюдаемым ФПСУ-IP и его партнером по резервированию), через которые происходит взаимодействие между участвующими в системе «горячего» резервирования ФПСУ-IP. Для ФПСУ-IP, начиная с релиза программного обеспечения 2.65, может быть установлено до четырех таких туннелей, до двух через сетевые адаптеры подсистемы горячего резервирования, и до двух через сетевые адаптеры рабочих портов.

На экране порты 1 и 2 - это 3 и 4 LAN-адаптеры в настройках конфигурации для горячего резерва (см. пункт «Конфигурация драйверов сетевых адаптеров» окно «Конфигурация LAN-адаптеров»).

Флаг «M» слева от номера порта означает, что для шифрования данных в VPN-туннеле используется блочный шифр «Магма».

Флаг «A» означает, что порт помимо резерва используется для мониторинга УА.

Символом «*» отмечены туннели, организованные через сетевые адаптеры, которые были специально выделены в конфигурации LAN-адаптеров ФПСУ-IP для работы только с подсистемой «горячего» резервирования (см. пункт «Конфигурация драйверов сетевых адаптеров»).

Не отмеченный символом «*» туннель организован через сетевой адаптер, который в конфигурации ФПСУ-IP настроен в качестве рабочего порта.

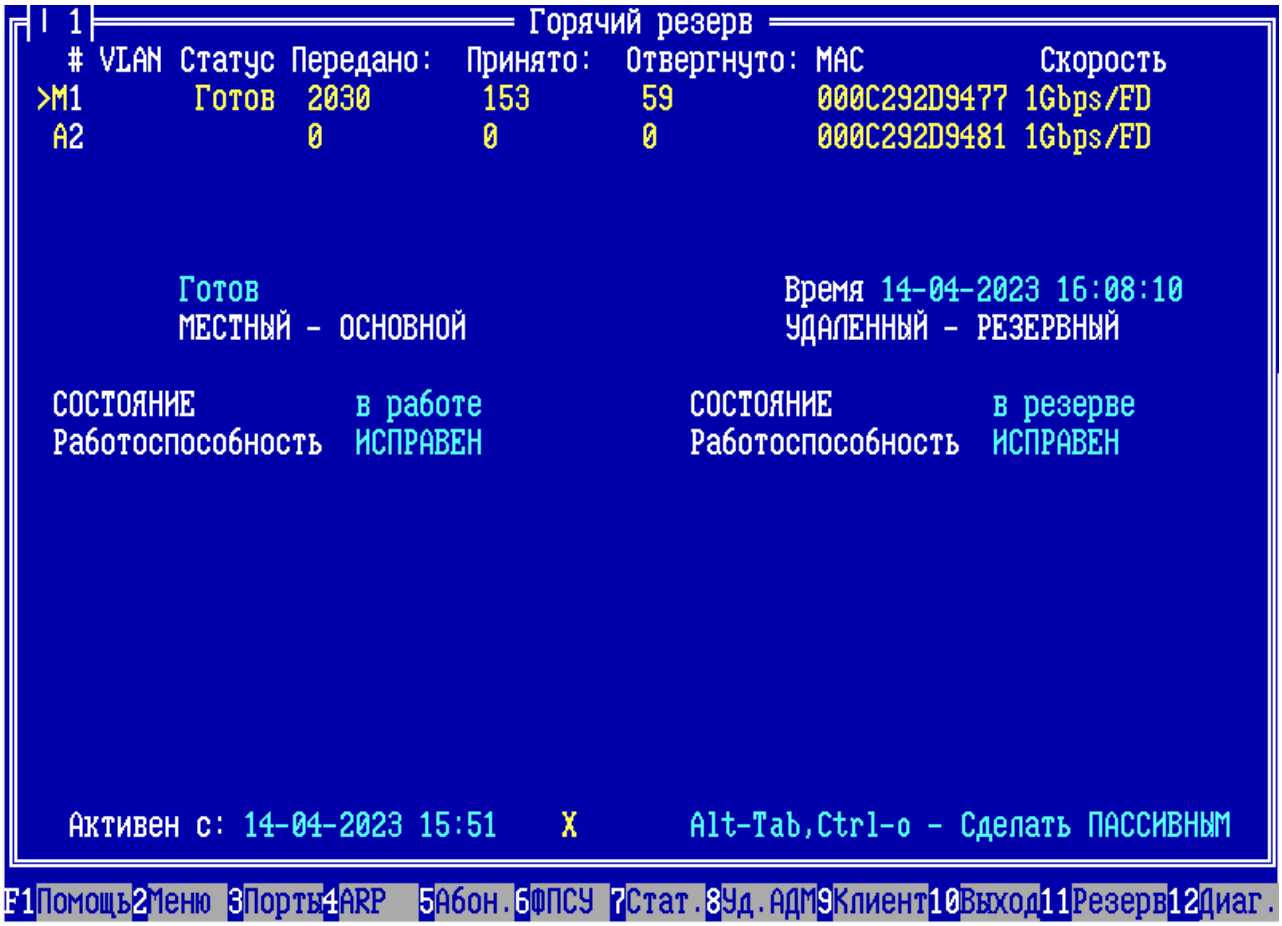


Рисунок 89 - Отображение состояния «горячего» резервирования

Строка «*Статус*» показывает состояние VPN-туннеля «горячего резерва». Туннель может находиться в следующих состояниях:

- Поле «*Статус*» пустое - отсутствует физический канал связи (соединительный кабель не подключен или неисправен).
- *«Устанавливается»* - начат процесс установки туннеля.
- *«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 рабочих портов. Если в течении одной минуты один из сетевых адаптеров рабочих портов находился в состоянии «Speed: No link», то ФПСУ-IP принимает решение, что отсутствие подключения к сети передачи данных на этом сетевом адаптере является штатным режимом взаимодействия ФПСУ-IP с сетью передачи данных и устанавливает локальную оценку состояния ФПСУ-IP в значение «Работоспособность: ИСПРАВЕН» (такое исключение требуется при подключении ФПСУ-IP к сетевому оборудованию не в разрыв сети, а только одним рабочим портом).

Если на ФПСУ-IP задействована система контроля линий связи, то на экране мониторинга *<F11>* дополнительно выводится информация о состоянии проверок каналов связи (подробнее см. пункт «Параметры проверки линий связи для портов ФПСУ-IP»).

В левом нижнем углу указывается информация о длительности текущего функционального статуса ФПСУ-IP, с какого момента он находится в текущем статусе («Активен» или «В резерве»).

Функциональный статус находящихся в горячем резерве комплексов (Активный/Пассивный) администратор может изменить, нажав комбинацию клавиш *<Alt+Tab>* (*<Ctrl+O>*, при управлении ФПСУ-IP через консольное соединение), о чем сообщает подсказка в нижней части экрана. Для выполнения действия требуется успешная авторизация администратору по ТМ-идентификатору.

Примечание. Если подсистема автоматического старта ФПСУ-IP задействована, то авторизации администратора для передачи управления партнеру по горячему резерву не требуется.

5. 12. Информационные окна жидкокристаллического экрана

Программно-аппаратный комплекс «ФПСУ-IP» на базе аппаратной платформы типоразмера 1U (обозначение аппаратной платформы FPSUIP-STD или FPSUIP-EXT) оснащен жидкокристаллическим дисплеем, на который выводится системная информация о работе комплекса.

Рисунок 90 - 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**			**О**	**С**	**Н**	**О**	**В**	**Н**	**О**	**Й**
/		**В**		**Р**	**А**	**Б**	**О**	**Т**	**Е**			**А**	**К**	**Т**	**И**	**В**	**Е**	**Н**	

Первый символ во 2-й строке (вращающаяся «/») предназначен для подтверждения функционирования ФПСУ-IP в рабочем режиме.

Нажатием кнопки «^» и «v» можно перейти на дополнительные информационные окна, окно версий компонентов ФПСУ-IP и окно продолжительности работы и текущей загрузки.

Окно версий компонентов ФПСУ-IP

В информационном окне версий компонентов ФПСУ-IP отображаются:

- версия программного обеспечения ФПСУ-IP;
- обозначение аппаратной платформы ФПСУ-IP.

Пример окна версий компонентов ФПСУ-IP:

П	**О**		**Ф**	**П**	**С**	**У**	**-**	**I**	**P**					**v**	**3**	**.**	**3**	**0**	
H	**W**		**F**	**P**	**S**	**U**	**I**	**P**	**-**	**S**	**T**	**D**	**3**	**-**	**1**	**U**			

Окно продолжительности работы и текущей загрузки

В информационном окне продолжительности работы и текущей загрузки

отображаются:

- время работы ФПСУ-IP после включения питания/последней перезагрузки в днях, часах и секундах;
- текущая загрузка процессора в процентах. Допускается загрузка до 100%. Постоянная высокая (95-100%) загрузка процессора указывает на сильную загруженность траффиком защищаемой ФПСУ-IP линии передачи данных. Возможны сбросы пакетов при увеличении обрабатываемого траффика. Рекомендуется заменить платформу на более производительную.

Пример продолжительности работы и текущей загрузки ФПСУ-IP:

В		**Р**	**А**	**Б**	**О**	**Т**	**Е**	**:**	**1**	**3**	**6**	**4**	**д**	**2**	**3**	**ч**	**5**	**8**	**с**
З	**А**	**Г**	**Р**	**У**	**З**	**К**	**А**		**П**	**Р**	**О**	**Ц**	**:**	**0**	**5**	**0**	**%**		

6. Контроль целостности программного обеспечения

ФПСУ-IP содержит ряд механизмов, обеспечивающих защиту программных модулей от НСД, в частности, автоматический контроль целостности программных модулей, находящихся на ПЗУ комплекса.

Проверка контрольных сумм осуществляется каждый раз при запуске или перезагрузке ФПСУ-IP в обязательном порядке. Если проверка не прошла успешно, перевод ФПСУ-IP в рабочий режим становится невозможен до устранения проблемы путем установки обновления или полной переустановки программного обеспечения ФПСУ-IP.

Администратор имеет возможность осуществить дополнительный контроль целостности программных и информационных частей ФПСУ-IP с использованием специальной подсистемы контроля целостности модулей, в том числе путем сравнения с эталонными контрольными суммами, указанными в формуляре.

Проверку контрольных сумм проводит внутренняя утилита ФПСУ-IP, fpsuhash.exe.

Дополнительная проверка целостности ПО и запуск тестов осуществляется из пункта «Проверка целостности» главного меню ФПСУ-IP.

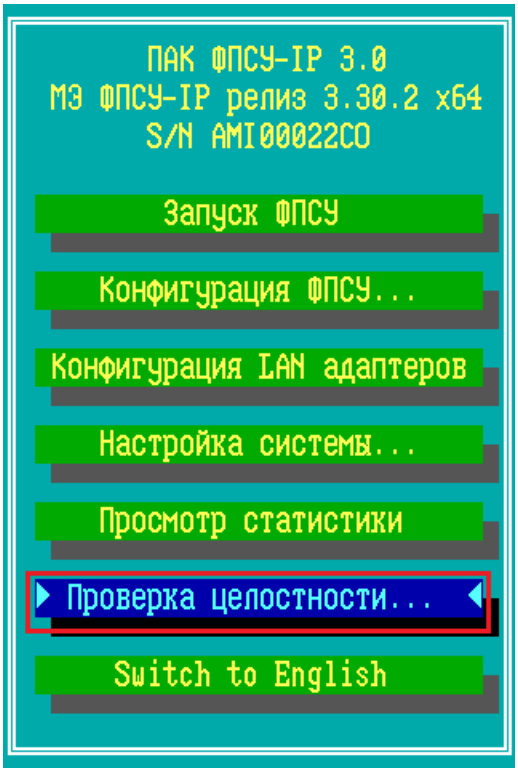


Рисунок 91 - Главное меню ФПСУ-IP

6. 1. Проверка целостности программных модулей ФПСУ-IP

У локального администратора существует три варианта выполнения проверки целостности программных модулей ФПСУ-IP:

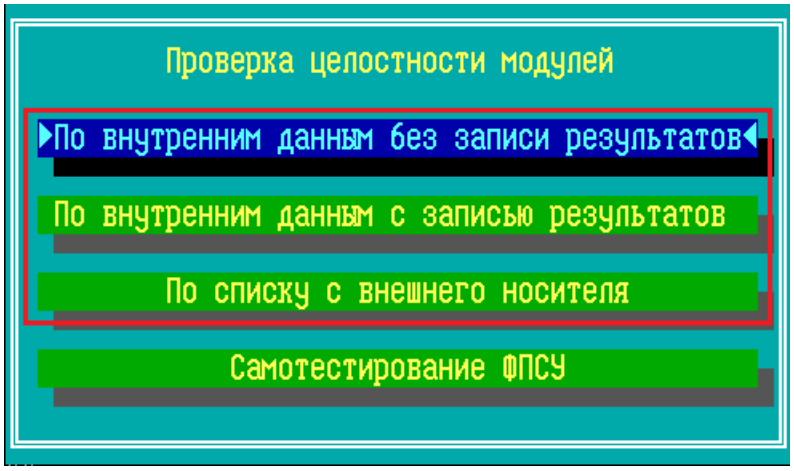


Рисунок 92 - Меню проверки целостности ПО

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 в формуляре СКЗИ, 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.

6. 2. Контроль целостности Терминала

В случае локального управления ФПСУ-IP с помощью консольного подключения через COM-порт от оборудованного программой PuTTy версии 0.70 сборки ООО «АМИКОН» рабочего места под управлением ОС Windows (далее - Терминалом), необходимо выполнять контроль целостности программного обеспечения Терминала.

Первоначальный контроль целостности после установки

Непосредственно после установки ПО Терминала на ПЭВМ следует выполнить первоначальный контроль целостности программных модулей Терминала.

Контроль целостности осуществляется при помощи входящей в состав СКЗИ «Программы контроля целостности файлов», WINFPSUHASH.EXE.

Для выполнения первоначального контроля целостности после установки следует рассчитать с помощью WINFPSUHASH.EXE контрольные суммы на программное обеспечение Терминала и сравнить полученные результаты с эталонными контрольными суммами из формуляра на СКЗИ (подробнее об использовании WINFPSUHASH.EXE см. инструкцию по применению программы контроля целостности файлов).

При нарушении целостности программного модуля Терминала, необходимо повторно установить программу с инсталляционного носителя.

Контроль целостности в процессе эксплуатации

Для использования Терминала для управления ФПСУ как СКЗИ класса КС2 или КС3, контроль целостности программы в процессе эксплуатации следует осуществлять средствами сертифицированного по Требованиям ФСБ АПМДЗ с действующим сертификатом соответствия.

В остальных случаях, контроль целостности Терминала в процессе эксплуатации следует осуществлять программой WINFPSUHASH.EXE.

Контролю целостности в процессе эксплуатации подлежат программные модули Терминала (putty_x86.exe и putty_amd64.exe) исполняемые файлы ОС.

При нарушении целостности контролируемых программных модулей необходимо прекратить работу с Терминалом до восстановления целостности файлов.

6. 3. Самотестирование функций межсетевого экрана ФПСУ-IP

Из пункта меню «Проверка целостности» администратор может выполнить ручную проверку функционала межсетевого экрана ФПСУ-IP, «Самотестирование ФПСУ» (операция доступна администратору класса *«Инженер»* или выше, см. раздел «Общие сведения», таблица 1):

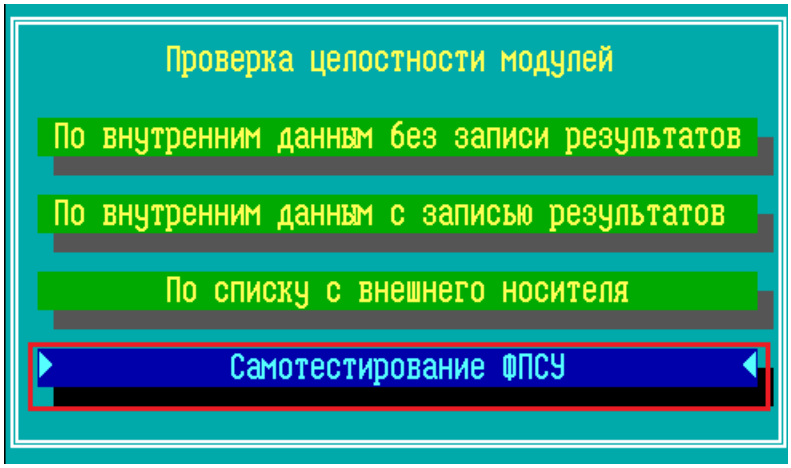


Рисунок 93 - Команда запуска внутреннего теста межсетевого экрана ФПСУ-IP

При выполнении этой команды ФПСУ-IP запускается на специальной тестовой конфигурации и выполняет ряд тестов обработки пакетов по правилам межсетевого экрана тестовой конфигурации.

В процессе выполнения внутренних тестов будет запущен рабочий режим ФПСУ-IP и выведено окно с процессом выполнения самотестирования:

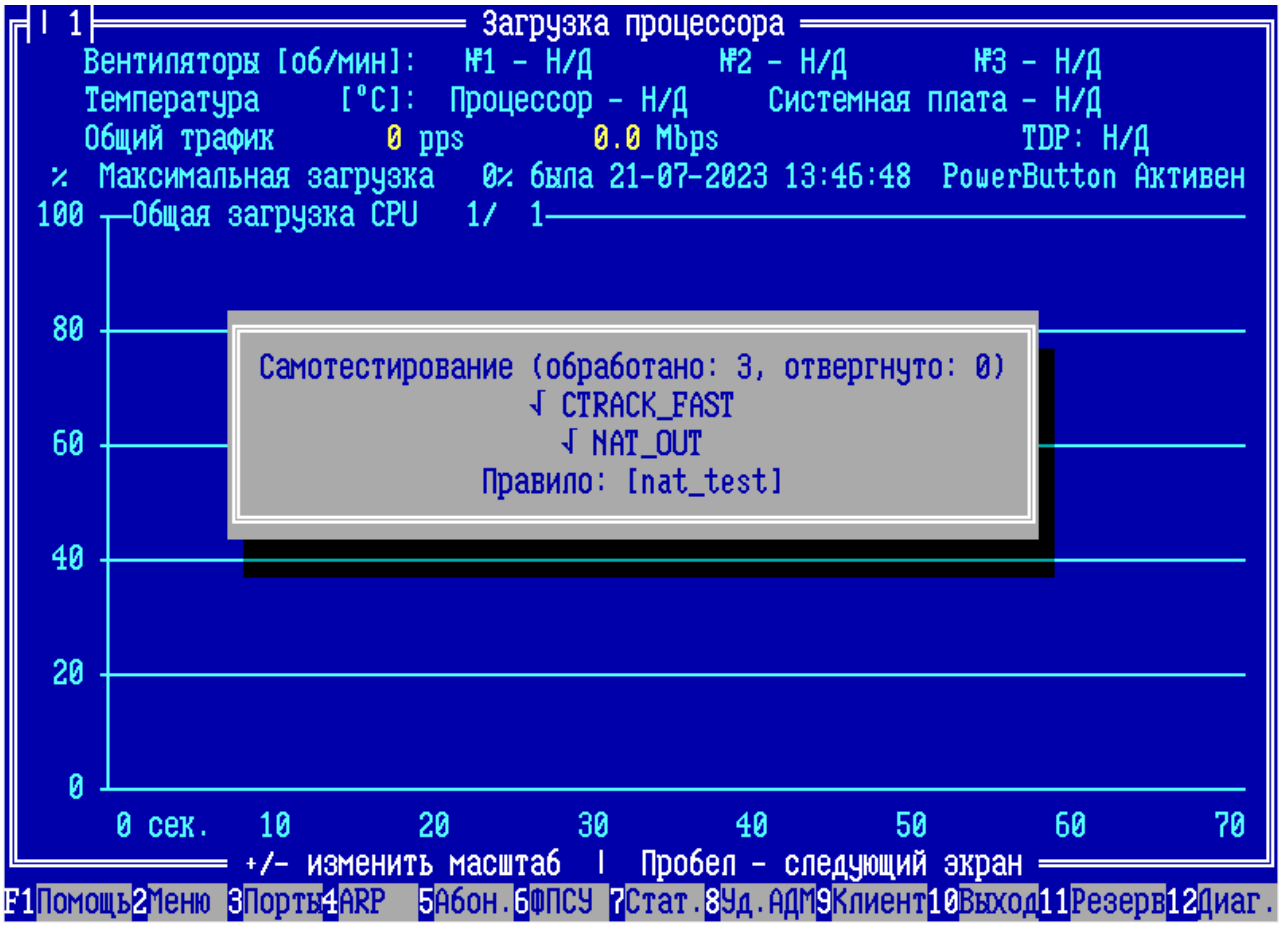


Рисунок 94 - Выполняется самотестирование ФПСУ

В случае успешной проверки, будет выдано оповещение:

Рисунок 95 - 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.

7. Конфигурация ФПСУ-IP

Конфигурирование ФПСУ-IP заключается в определении режимов и правил его работы, позволяющих осуществлять контроль передаваемого трафика данных в соответствии с топологией сети и требуемой степенью безопасности.

Команда главного меню «Конфигурация ФПСУ» предназначена для задания правил фильтрации, режимов работы механизмов аутентификации, сжатия, криптозащиты, правил взаимодействия с клиентами, а также для установки параметров работы ФПСУ-IP:

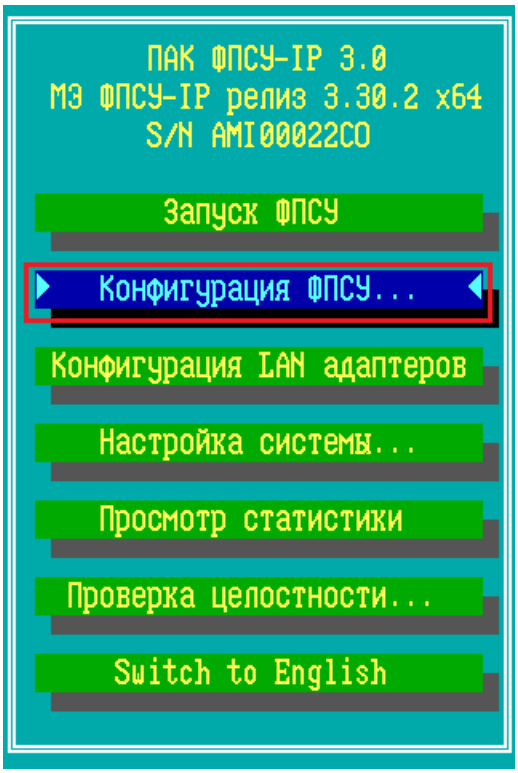


Рисунок 96 - Главное меню ФПСУ

При выборе команды «Конфигурация ФПСУ», на экране появится окно с опциями, которые позволяют производить локальную настройку ФПСУ-IP, а так же, в случае сбоя или аварии внутреннего накопителя (SSD), повлекших переустановку ПО ФПСУ-IP на другой накопитель, быстро восстановить работоспособность ФПСУ-IP. Если заложенные в конфигурацию правила фильтрации являются конфиденциальными, необходимо принять соответствующие меры безопасности к хранению носителя с сохраненной конфигурацией.

Рисунок 97 - Команды работы с конфигурацией

Опции меню «Конфигурация ФПСУ»:

- «Отредактировать» – команда входа в подсистему конфигурирования для внесения изменений в параметры работы ФПСУ-IP.
- «Сохранить на носитель» – команда записи текущей конфигурации ФПСУ-IP в специальном формате на съемный носитель для хранения или переноса на рабочее место удаленного администратора. Опция доступна администраторам классов *«Инженер»* и *«Администратор»* (см. раздел «Общие сведения», таблица 1).
- «Восстановить с носителя» – команда восстановления конфигурации ФПСУ-IP из ранее сохраненной. Опция доступна администратору класса *«Администратор»*.
- «Контроль целостности» – команда проверки внутреннего файла конфигурации ФПСУ-IP по хранящейся на внутреннем накопителе ФПСУ-IP контрольной сумме. Контрольная сумма конфигурации ФПСУ-IP не является неизменной, она пересчитывается каждый раз, когда администратор ФПСУ-IP сохраняет выполненные изменения в конфигурации. Для выполнения команды требуются права роли *«Администратор»*. Результат ручной проверки целостности конфигурации пишется в статистику ФПСУ-IP.

При попытке войти в подсистему конфигурирования (команда «Отредактировать»), ФПСУ-IP потребует прижать к контактному устройству электронный ТМ-идентификатор (или подключить USB ТМ-идентификатор к USB-порту ФПСУ-IP), подтверждающий право администратора на запрашиваемые действия. Администратор класса *«Администратор»* или выше имеет право установки или изменения любых параметров конфигурации, администратору класса *«Инженер»* недоступно изменение правил фильтрации. Кроме того, вход в подсистему может быть защищен паролем (см. раздел «Установка пароля администратора»).

Установленные параметры конфигурации ФПСУ-IP могут впоследствии

редактироваться администратором (имеющим соответствующие полномочия).

Примеры конфигураций ФПСУ-IP приведены в разделе «Примеры настройки ФПСУ-IP».

При входе в подсистему конфигурирования (выполнении команды «Отредактировать») на экране монитора появится меню конфигурации, содержащее описываемые в других разделах возможности настройки ФПСУ-IP:

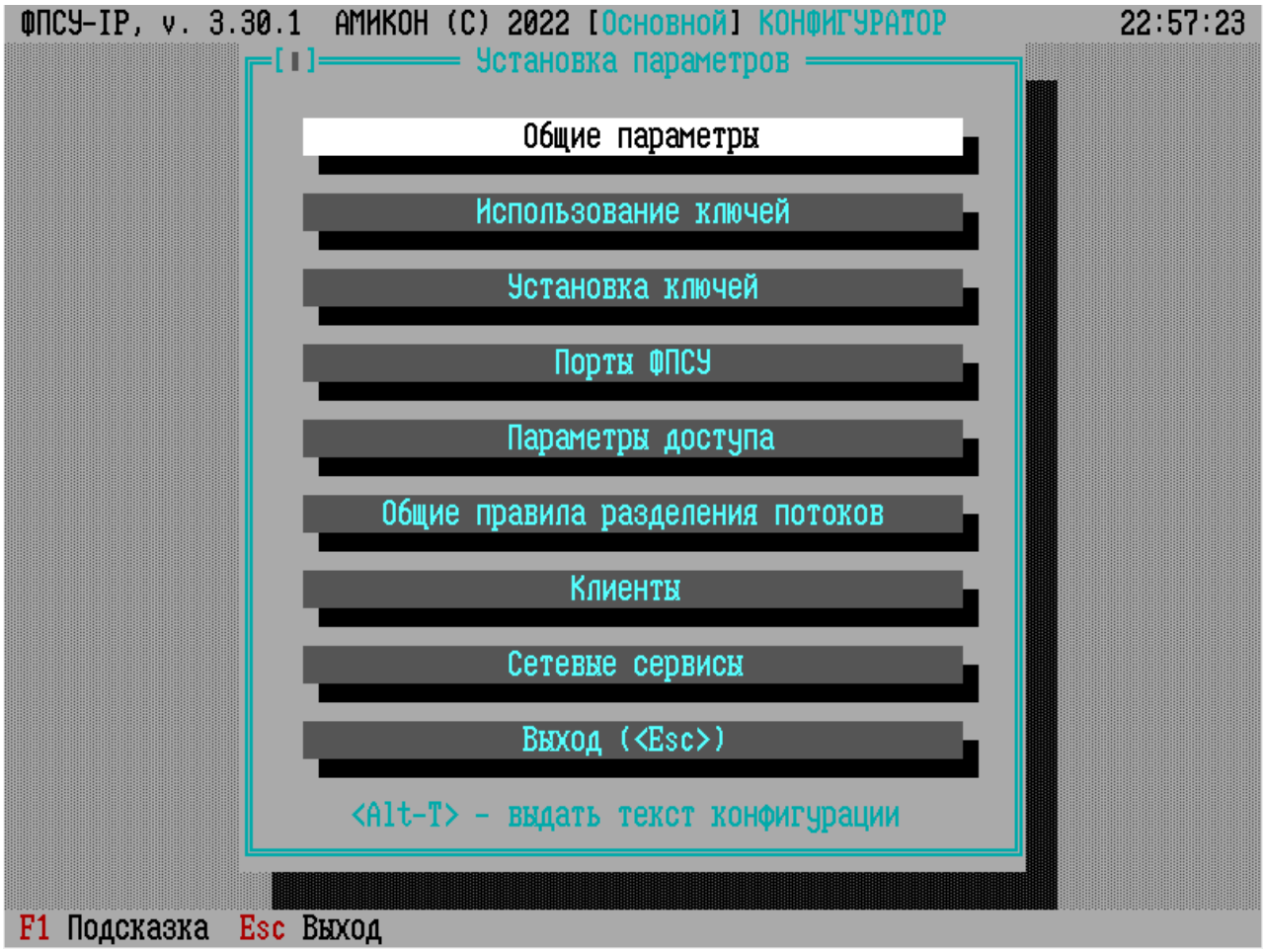


Рисунок 98 - Меню подсистемы конфигурирования ФПСУ-IP

Администратор может выдать конфигурацию в текстовом виде на внешний носитель при помощи комбинации клавиш *<Alt+T>*. Текст конфигурации выдается в файл с именем, образованным из серийного номера ФПСУ-IP с добавлением буквы «t» в конце расширения. Такой файл может быть прочитан и обработан (в частности, распечатан) средствами любого текстового редактора на другом компьютере.

7. 1. Общие параметры конфигурации ФПСУ-IP

Группа установок «Общие параметры» определяет правила работы ФПСУ-IP в различных частных случаях функционирования.

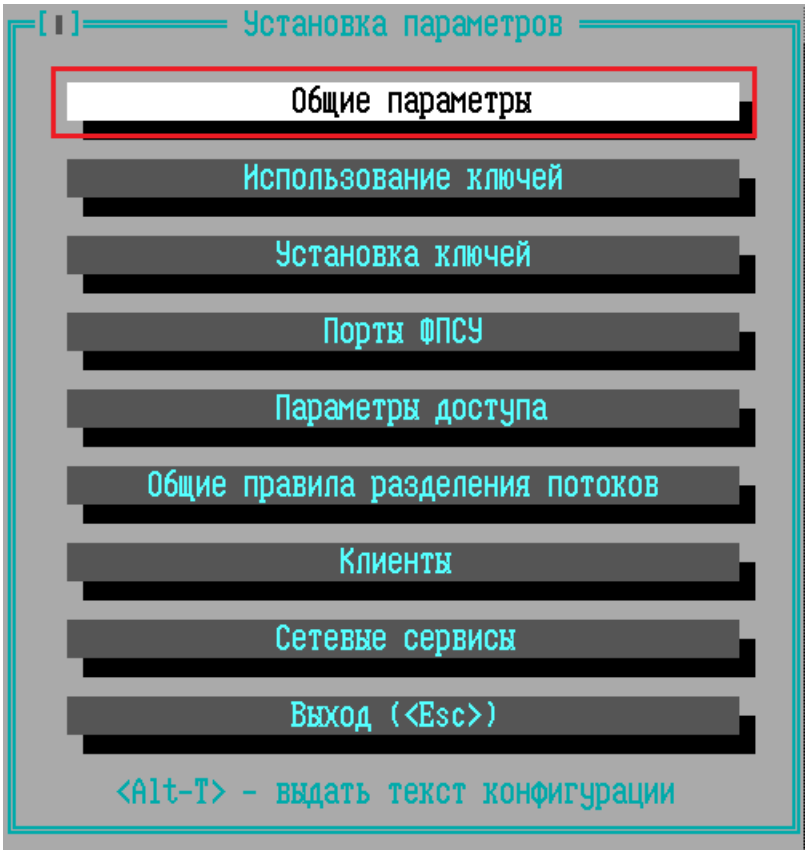


Рисунок 99 - Вход в общие настройки из основного меню конфигурации ФПСУ-IP

Окно установки содержит следующие настраиваемые общие параметры:

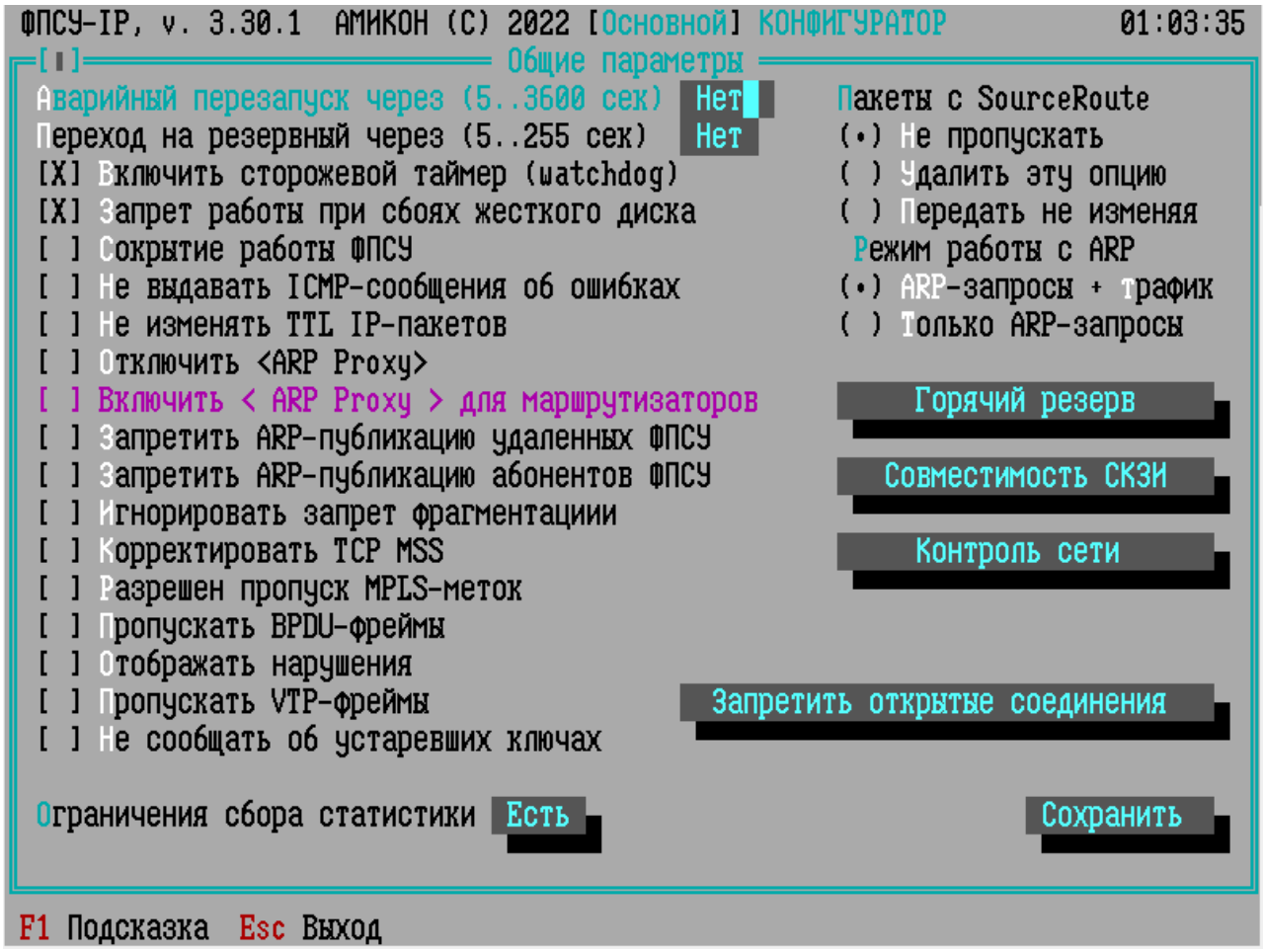


Рисунок 100 - Настройка общих параметров ФПСУ-IP

Включение или выключение опций осуществляется клавишей *<Пробел>*.

Настройки, находящиеся в левой части окна Общие параметры:

Аварийный перезапуск. Если при работе ФПСУ-IP происходит аппаратный сбой сетевых адаптеров, ФПСУ-IP способен детектировать это событие и выдать на экран монитора специальное сообщение, сопровождающееся звуковым сигналом, после чего через некоторое время ПО сетевых адаптеров и ПО ФПСУ-IP автоматически перегрузятся, после чего и ФПСУ-IP попытается восстановить работу режима фильтрации пакетов. В диалоговом поле строки укажите время, в течение которого будет выдаваться сообщение перед перезагрузкой (в диапазоне от 5 секунд до 1 часа).

Если автоматический перезапуск не нужен (например, необходимо ознакомиться с диагностикой неполадок, выданной на экран монитора), оставьте поле пустым; в таком случае при возникновении аппаратного сбоя сообщение, сопровождаемое звуковым сигналом, будет выдаваться до его отмены администратором при локальном управлении.

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.

Не изменять TTL IP-пакетов **—** флаг, позволяющий дать указание ФПСУ-IP не изменять поле «время жизни» в заголовке IP-пакета. Эта опция может быть использована с целью сокрытия работы ФПСУ-IP, а также для передачи через него пакетов, «время жизни» которых равно единице.

Отключить <ARP-proxy>. Для обеспечения «прозрачности» функционирования, в ФПСУ-IP реализован стандартный механизм ARP-proxy со специфичной ARP-фильтрацией, гарантирующей получение ARP-ответа станции, запрашивающей проход через ФПСУ-IP к удаленному ресурсу. Если необходимость в такой функции отсутствует (например, в случае когда по обе стороны ФПСУ-IP установлены маршрутизаторы) или требуется снизить нагрузку на сеть, ARP-proxy можно отключить, установив описываемый флаг. В этом случае ФПСУ-IP будет отвечать только на те ARP-запросы, которые касаются его собственных IP-адресов или адресов клиентов, находящихся в состоянии соединения.

ВНИМАНИЕ! При отключении ARP-proxy для обеспечения работоспособности сети необходимо в конфигурации смежного сетевого оборудования описать конфигурируемый ФПСУ-IP в качестве одного из маршрутизаторов.

Включить <ARP-proxy> для маршрутизаторов **—** флаг, позволяющий при отключении <ARP-proxy> (см. выше) сохранить этот механизм для маршрутизаторов, «прописанных» на портах ФПСУ-IP. Доступен, если опция «*Отключить <ARP-proxy>*» включена.

Запретить ARP-публикацию удаленных ФПСУ **—** флаг, позволяющий с целью снижения нагрузки на сеть отменить ARP-публикацию аппаратных адресов удаленных ФПСУ-IP, описанных со стороны одного из рабочих портов ФПСУ-IP, в локальную сеть со стороны другого порта.

Запретить ARP-публикацию абонентов ФПСУ **—** флаг, позволяющий с целью снижения нагрузки на сеть отменить ARP-публикацию аппаратных адресов абонентов, описанных со стороны одного из рабочих портов ФПСУ-IP, в локальную сеть со стороны другого порта.

Игнорировать запрет фрагментации **—** флаг, работающий в VPN-туннелях между ФПСУ-IP, и в VPN-туннелях между ФПСУ-IP и ФПСУ-IP/Клиент, влияет на обработку пакетов с установленным флагом DF запрета фрагментации. Если опция включена, то пакет, длина которого превышает установленное значение MTU для текущего сетевого соединения или туннеля, будет разбиваться на минимальное количество пакетов примерно равной длины. Производительность ФПСУ-IP при включении опции будет снижена. Если опция выключена – слишком длинный для соединения или туннеля пакет с флагом DF будет сброшен, а отправитель получит ICMP-сообщение о необходимости смены MTU.

Корректировать TCP MSS **—** опция, включающая дополнительный механизм (к имеющемуся PATH MTU DISCOVERY с отсылкой отправителю ICMP-пакета) регулирования MTU IP пакетов, предназначенный для исключения фрагментации или проблем с передачей пакетов при установленном флаге DF. Значение MSS отправляется как опция TCP заголовка в пакетах *TCP SYN* и *SYN ACK*. Каждая сторона при установлении TCP-соединения сообщает свое значение MSS другой стороне. ФПСУ-IP эти значения уменьшает на размер служебных данных туннельного пакета (для ФПСУ-IP - 28 байт). Включение опции позволяет избежать ошибок фрагментации, если при передаче данных используется протокол TCP.

Разрешён пропуск MPLS меток **—** флаг, позволяющий ФПСУ-IP обрабатывать и передавать дальше пакеты с метками MPLS-протокола. При выключенной опции такие пакеты не обрабатываются ФПСУ-IP и сбрасываются.

Пропускать BPDU-фреймы **—** флаг, позволяющий ФПСУ-IP обрабатывать и передавать дальше фреймы BPDU-протокола (Bridge Protocol Data Unit). Включите эту опцию, если ФПСУ-IP подключен в разрыв сети, использующей протокол STP (Spanning Tree Protocol, IEEE 802.1D). При выключенной опции такие пакеты не обрабатываются ФПСУ-IP и сбрасываются, что может вызвать ошибки в работе протокола STP.

Отображать нарушения **—** флаг, при включении которого ФПСУ-IP будет выводить на монитор и в консоль служебные оповещения о сбросе пакетов абонентов по причине запрещающего правила межсетевого экрана. По умолчанию, отключен, и информация о сброшенных пакетах пишется в статистику, но не выводится на экран и в консоль отдельными сообщениями.

Пропускать VTP-фреймы **—** флаг, позволяющий ФПСУ-IP обрабатывать и передавать дальше фреймы VTP-протокола (VLAN Trunking Protocol). Включите эту опцию, если ФПСУ-IP подключен в разрыв сети, использующей технологию VLAN, и VLAN управляется с применением протокола VTP. При выключенной опции такие пакеты не обрабатываются ФПСУ-IP и сбрасываются, что может привести к ошибке вследствие несогласованности в конфигурации VLAN-сетей.

Не сообщать об устаревших ключах — если на ФПСУ-IP установлены ключевые данные класса КС3, то ФПСУ-IP при старте выдает информационное оповещение об истечении срока действия ключей. Для отмены выдачи такого информационного оповещения следует установить флаг «*Не сообщать об устаревших ключах*». По умолчанию, флаг снят.

ВНИМАНИЕ! При использовании ФПСУ-IP по классу КС3, в настройках должен быть включен режим информирования об использовании ключа при превышении срока его

действия (флаг «Не сообщать об устаревших ключах» должен быть снят).

Ограничения по сбору статистики. Эта кнопка позволяет наложить ограничения на сбор регистрационной информации ФПСУ-IP. Подробнее см. пункт «Ограничение сбора статистики».

Настройки, которые находятся в правой части окна Общие параметры:

Пакеты с SourceRoute. Опция SourceRoute, если она содержится в заголовке IP пакета, требует, чтобы пакет следовал по указанному ею маршруту, что может приводить к передаче пакета в обход ФПСУ-IP и нарушению безопасности. С другой стороны, игнорирование этой опции может влиять на работу сети и приводить к каким-либо другим нарушениям. Поэтому администратор в индивидуальном порядке должен решить, как ФПСУ-IP будет обрабатывать эту опцию и указать это в описываемом поле.

ФПСУ-IP предоставляет три возможных способа обработки опции SourceRoute:

- *не пропускать* пакеты, содержащие эту опцию, сбрасывая их без отправки сообщения;
- *удалить эту опцию* - передать пакет получателю (если он удовлетворит требованиям фильтрации), но удалить заданный маршрут и передать пакет по маршруту, который установил при конфигурировании для данного абонента администратор;
- *передать не изменяя* пакет, оставить опцию SourceRoute без изменения.

Включение или выключение радио-кнопки, отображающей выбираемый способ обработки, осуществляется клавишей <*Пробел*>.

Режим работы с ARP — опция, позволяющая выбирать режим формирования ARP-таблицы на ФПСУ-IP. Возможны два варианта настройки:

- *ARP-запросы + трафик* - опция по умолчанию, ARP-таблица формируется из ответов на собственные ARP-запросы, а также из входящих пакетов, передаваемых через ФПСУ;
- *Только ARP-запросы* - при выборе этой опции, ARP-таблица формируется только из ответов на собственные ARP-запросы. Рекомендуется при использовании ФПСУ-IP вместе со сторонними решениями оптимизации передаваемого трафика (таких как Riverbed SteelHead).

Горячий резерв — кнопка перехода в окно настроек работы ФПСУ-IP в подсистеме горячего резерва:

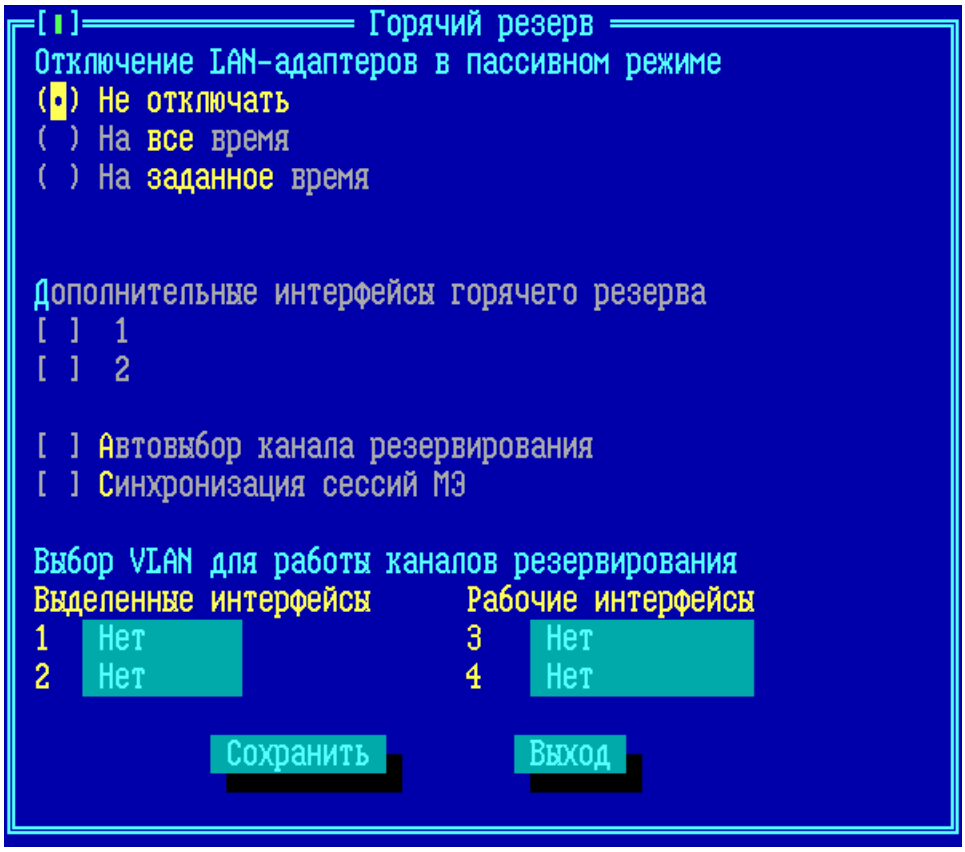


Рисунок 101 - Настройка горячего резерва

- ***Отключение LAN-адаптеров в пассивном режиме*** — опция, относящаяся к схеме горячего резервирования. Включите эту опцию, если хотите, чтобы ФПСУ-IP горячего резерва, который на данный момент работает в пассивном режиме (состояние «в резерве» на экране отображения состояния горячего резервирования, см. «Окно состояния подсистемы «горячего» резервирования»), отключал все сетевые адаптеры, кроме адаптеров, соединяющего с партнером по резервированию. Включение данной опции позволяет сетевым устройствам класса сетевой коммутатор (switch) быстрее обновить таблицу соответствия MAC-адреса ФПСУ-IP физическому порту коммутатора при переключении управления между основным и резервным комплексами.

- ***Дополнительные интерфейсы горячего резерва*** — флаги «[ ] 1» и «[ ] 2». Позволяют комплексу устанавливать через сетевые адаптеры, настроенные как рабочие порты, туннель с партнером горячего резерва. Без включения данной опции туннель между комплексами ФПСУ-IP, работающими в режиме горячего резервирования, устанавливается через специально выделенные для этой цели дополнительные LAN-адаптеры. Опция не работает с включенной опцией ***Отключение LAN-адаптеров в пассивном режиме.*** Опция не работает, если для

рабочего порта ФПСУ-IP настроен работающий в режиме моста туннель (см. пункт «Описание параметров удаленных ФПСУ-IP»).

- ***Автовыбор канала резервирования*** - опция, позволяющая в случае обрыва канального соединения переключаться на следующий активный канал связи с партнером по горячему резервированию (в том числе доступно переключение на резервный канал связи с использованием «рабочих» интерфейсов).

- ***Синхронизация сессий МЭ*** - опция, позволяющая передавать активные сессии абонентов при передаче управления партнеру по горячему резервированию. При включении такой синхронизации работа сетевых сервисов абонентов не прерывается из-за передачи управления горячему резерву.

- ***Выбор VLAN для работы каналов резервирования*** - назначение тега VLAN для каналов «горячего» резервирования. Фреймы «горячего» резервирования будут тегированы соответствующим идентификатором VLAN. Для включения данной опции должен быть задан хотя бы один ***Дополнительный интерфейс горячего резерва***.

- ***Рабочие интерфейсы*** - поля 3 и 4 - это 1 и 2 LAN-адаптеры в настройках конфигурации (окно «Конфигурация LAN-адаптеров», открывается по одноименной команде меню).

- ***Выделенные интерфейсы*** - поля 1 и 2 - это 3 и 4 LAN-адаптеры в настройках конфигурации для горячего резерва (окно «Конфигурация LAN-адаптеров»). Нумерация полей 1 и 2 отображается для адаптеров горячего резерва в настройках ***Дополнительные интерфейсы горячего резерва***, а также в окне «Горячий резерв» (открывается по нажатию клавиши <*F11*>).

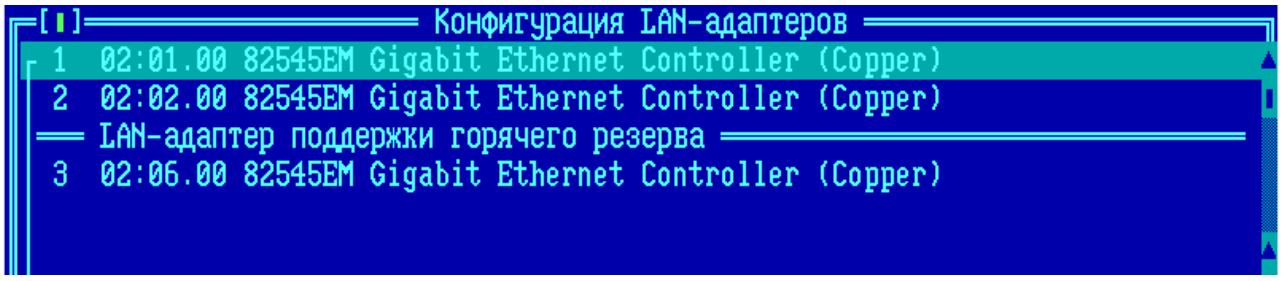


Рисунок 102 - Окно «Конфигурация LAN-адаптеров»

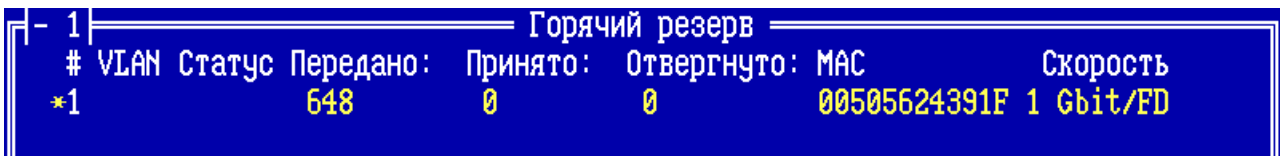


Рисунок 103 - Окно «Горячий резерв»

Совместимость СКЗИ - кнопка перехода в окно настроек алгоритмов шифрования СКЗИ:

Настройка криптопротоколов ФПСУ-Клиент - опции, устанавливающие работу ФПСУ-IP с ФПСУ-IP/Клиентами в режиме шифрования по заданному алгоритму:

- ***Приоритет Магма*** - при установлении флага передаваемые данные между ФПСУ-IP и ФПСУ-IP/Клиентом будут шифроваться по алгоритму «Магма», если и ФПСУ-IP, и ФПСУ-IP/Клиент поддерживают этот алгоритм.

- ***Совместимость с криптопротоколами ФПСУ/Клиент в рамках ГОСТ-89 –*** По умолчанию установлено значение «*Отключена*». Возможные параметры:

КРОМЕ Тун 1 —принимаются пользовательские подключения от ПАК ФПСУ-IP/Клиент, на которых установлена версия СКЗИ, отличная от «Туннель/Клиент».
КРОМЕ Тун 2 — принимаются пользовательские подключения от ПАК ФПСУ-IP/Клиент, на которых установлена версия СКЗИ, отличная от «Туннель 2.0».
Полная — принимаются пользовательские подключения от ПАК ФПСУ-IP/Клиент с любой версией СКЗИ.
Отключена — принимаются пользовательские подключения только от ПАК ФПСУ-IP/Клиент, начиная с версии ПО 6.0.38 (и устройства VPN-Key с версией микрокода 7-й или выше, поддерживающей алгоритм МАГМА).

- ***Запрет ГОСТ-89*** - при установлении флага на ФПСУ-IP будут запрещены любые соединения, использующие алгоритм шифрования ГОСТ 28147-89.

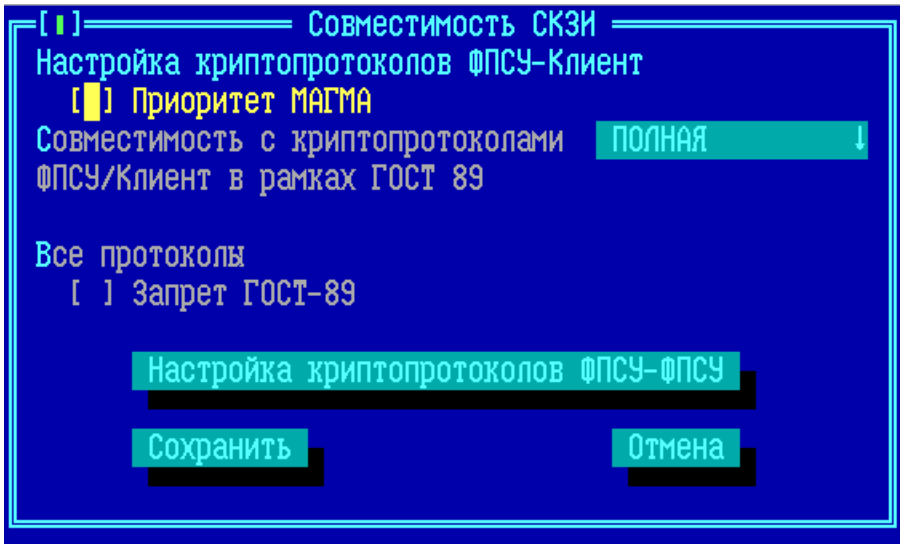


Рисунок 104 - Совместимость СКЗИ

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 MGM» отсутствует, данная опция недоступна (отмечена белым фоном).

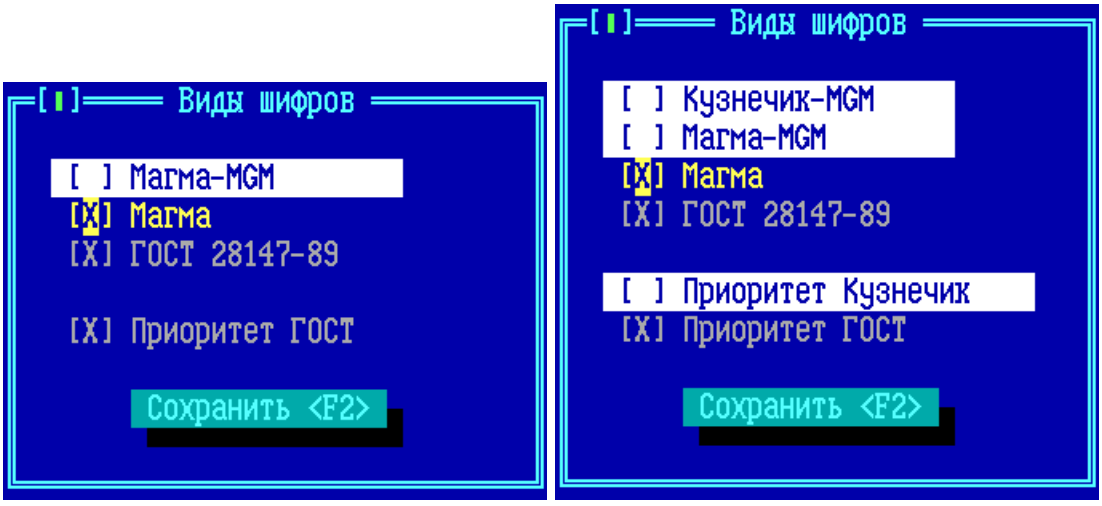


Рисунок 105 - Настройка криптопротоколов ФПСУ-ФПСУ

По умолчанию опции «Магма», «ГОСТ 28147-89» и «Приоритет ГОСТ» установлены.

В случае, когда не установлена ни одна опция, при передаче данных применяется алгоритм шифрования ГОСТ 28147-89.

Контроль сети — кнопка перехода в окно настроек контроля доступности списка IP-адресов, подробнее см. пункт «Параметры проверки линий связи для портов ФПСУ-IP».

Запретить открытые соединения — кнопка, включающая режим *«Запрет открытых соединений»*, в котором вся информация, передаваемая из внутреннего порта ФПСУ-IP на внешний порт ФПСУ-IP (подробнее про внутренние и внешние порты см. пункт «Порты ФПСУ»), и в обратную сторону, в принудительном порядке шифруется, либо передача блокируется. После включения режима он может быть снят только повторной инсталляцией программного обеспечения ФПСУ-IP.

Для исключения утечки через ФПСУ-IP требующей защиты информации объектов защищаемой локальной сети, комплекс во время штатной эксплуатации рекомендуется использовать с включенным режимом «Запрет открытых соединений».

Если режим «Запрет открытых соединений» выключен, то, при установке параметров, позволяющих создавать соединения отличные от криптографически защищенных (выбор режима «запрещено» или «нежелательно» в настройке «Криптозащита», п. «Описание параметров удаленных ФПСУ-IP», или режима абонента «Ретрансляция», п. «Описание абонента «Хост»), должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации или с объектов информатизации в защищаемой ЛВС.

После установки настроек, для их сохранения в конфигурацию, необходимо выполнить команду «***Сохранить»***, после чего произойдет выход в окно установки параметров конфигурации.

7. 2. Установка ключей

Данная команда меню подсистемы конфигурирования ФПСУ-IP предназначена для установки и удаления ключей парно-выборочной связи на ФПСУ. Ключи создаются при помощи программно-аппаратного комплекса СКЗИ «Центр выработки ключей» и предназначены для построения криптографически защищенных туннелей между ФПСУ-IP.

Если при выдаче данных на внешний носитель «Центром выработки ключей» транспортная копия была защищена специальным символьным паролем, при установке на ФПСУ-IP потребует его предъявить.

Одновременно комплекс может участвовать только в шестидесяти четырех (64) криптосетях (то есть, одновременно комплекс может поддерживать работу не более чем шестидесяти четырех различных VPN-сетей).

Выполнение процедуры установки доступно только администраторам классов «*Администратор*» и «*Главный Администратор*» (см. раздел «Общие сведения», таблица 1).

При активизации команды «Установка ключей» открывается диалоговое окно, в левой панели которого отображаются уже установленные на ФПСУ-IP ключевые данные (в случае, если установка производится впервые, окно будет пустым), а правое предназначено для установки новых ключевых данных с носителя.

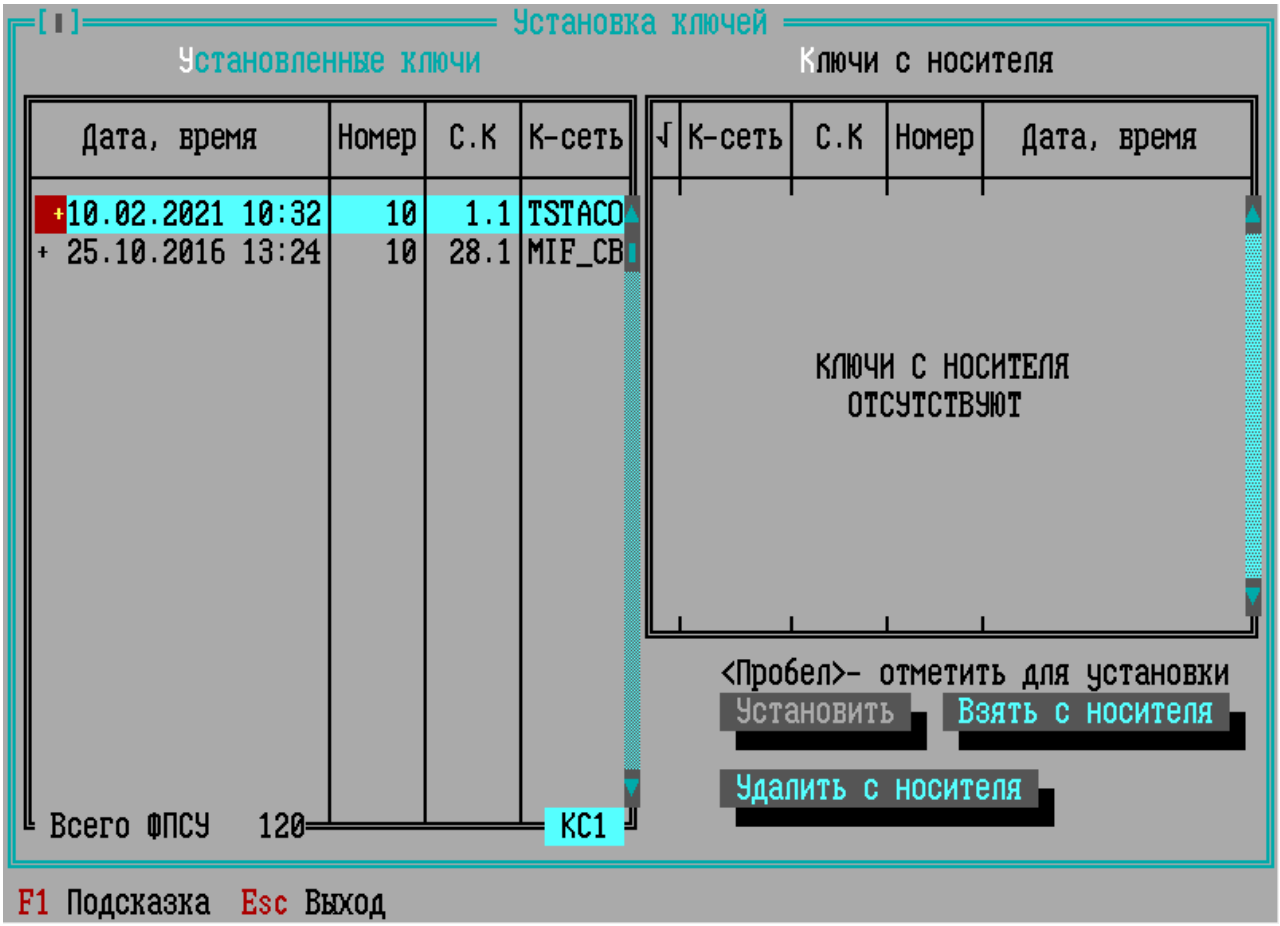


Рисунок 106 - Установка ключей

Для установленных ключевых данных указываются:

- *«Дата, время»* - Время и дата генерации ключевой информации «Центром выработки ключей»;
- *«Номер»* – Номер ключевых данных в рамках криптосети. От 1 до 10 000;
- *«С.К»* – номер серии ключевых данных. Серия предназначена для плановой смены

данных (от 1 до 255, рекомендуется создавать серии по возрастанию). Обозначается в формате N.K, где N - собственно номер серии, предназначенный для данного ФПСУ-IP, а К=1÷4 - номер комплекта данных с в рамках серии и номера;

- *«К-сеть»* – имя криптосети ключевых данных.
- строка *«Всего ФПСУ №№№№»* – при выборе курсором ключевых данных, внизу таблицы указывается общее количество ключей, сгенерированных ЦВК в рамках текущей серии;
- поле «*КС№»* – при выборе курсором ключевых данных, внизу таблицы указывается класс защиты согласно требованиям ФСБ к шифровальным (криптографическим) средствам, КС2 или КС3.
- состояние ключевых данных в конфигурации, перед названием криптосети:
  - «+ » – ключевые данные разрешено использовать в конфигурации ФПСУ-IP;
  - « +» – ключевые данные разрешено использовать в конфигурации ФПСУ-IP и они используются для организации соединений с другими ФПСУ-IP (см. пункт «Описание параметров удаленных ФПСУ-IP»);
  - « - » – лишние ключевые данные, которые **необходимо** удалить прежде чем ФПСУ-IP сможет быть запущен в рабочий режим;
  - если никаких обозначений нет, то ключевые данные только установлены на ФПСУ-IP, но ещё не разрешены к использованию.

При входе в модуль установки правая часть окна, «Данные с носителя» содержит сообщение «Данные с носителя отсутствуют».

Для установки новых ключей подключите к ФПСУ-IP носитель (USB-flash), на который записан ключ, выработанный «Центром выработки ключей», и выполните команду «*Взять с носителя»* в правой нижней части экрана. При этом в окне «Данные с носителя» появится список всех найденных на нем ключевых данных.

Выделите нужные данные курсором, отметьте их клавишей *<Пробел>* (слева от строки появится метка «√») и выполните команду «*Установить отмеченные»*. Отметить и установить на ФПСУ-IP можно только комплекты ключевых данных одного номера для каждой криптосети. На ФПСУ-IP можно отметить и установить два комплекта ключевых данных одной криптосети, только если у них совпадает номер и они отличаются только серией и/или номером комплекта ключевых данных в рамках серии. Например, если на ФПСУ-IP уже стоит комплект ключевых данных «AMITST:10:5.1» (ключ криптосети «AMITST», с номером ключевых данных 10, серии ключевых данных 5 и номером комплекта ключевых данных 1), то на ФПСУ-IP можно поставить комплект ключевых данных «AMITST:10:5.2» (запасной комплект ключевых данных этой же серии) или «AMITST:10:6.1» (новый комплект ключевых данных новой серии), но нельзя поставить

комплект ключевых данных «AMITST:9:5.1» (комплект ключевых данных с другим номером в этой же криптосети) без предварительного удаления комплекта «AMITST:10:5.1».

Для удаления ключевых данных с внутреннего накопителя ФПСУ-IP, установите на них курсор выбора в списке левой части окна, и нажмите клавишу <*Delete*>.

Для удаления ключевых данных с внешнего подключенного к ФПСУ-IP накопителя, выполните в правой нижней части окна команду «*Удалить с носителя*».

На ФПСУ-IP могут быть установлены две серии ключей парно-выборочной связи одновременно на период перехода с текущей серии на новую.

ВНИМАНИЕ! Можно удалить только те ключи, которые на данный момент не используются ФПСУ-IP для создания защищенных межсетевых туннелей. (см. пункт «Описание параметров удаленных ФПСУ-IP»).

7. 3. Использование ключей

Эта команда предназначена для выбора криптографических ключей парно-выборочной связи из установленных на ФПСУ, которые будут использоваться для создания защищенных межсетевых туннелей между парами ФПСУ-IP. Ключи парно-выборочной связи вырабатываются СКЗИ «Центр выработки ключей».

Команда доступна администратору только в случае, если ключи уже были установлены на ФПСУ. В противном случае, необходимо осуществить их установку (см. пункт «Установка ключей»). Если установка ключевых данных была ранее выполнена, при выборе строки с этой командой ФПСУ-IP перейдет в режим отображения установленных на ФПСУ-IP ключевых данных и выдаст на экран монитора следующее окно:

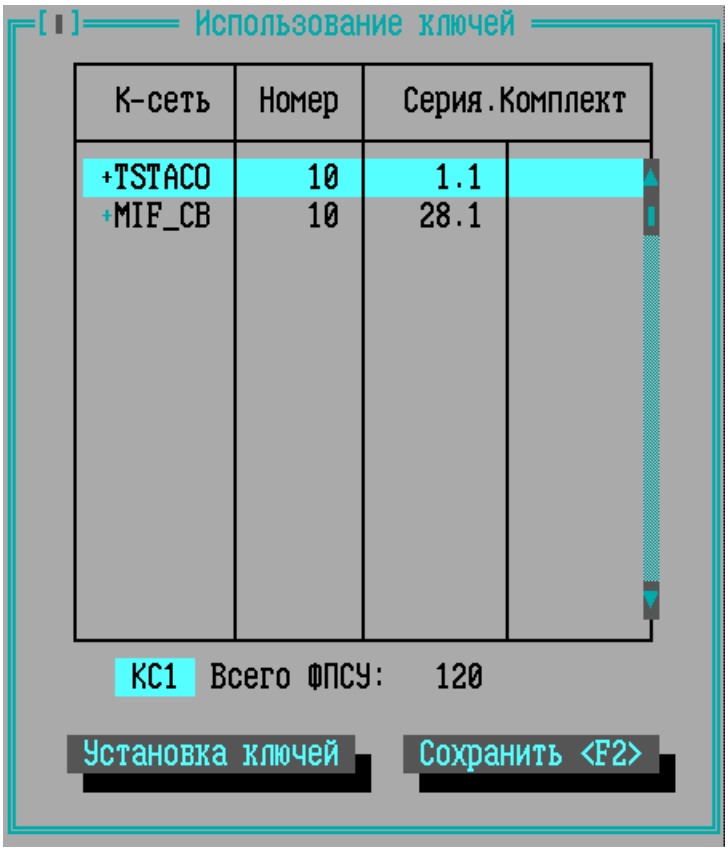


Рисунок 107 - Выбор используемых ключей

Окно содержит список криптосетей, ключи из которых установлены на ФПСУ-IP. Каждая строка содержит информацию о ключевых данных определенной криптосети: её символьное имя, номер установленных ключевых данных в рамках этой криптосети, серия ключевых данных и номер комплекта ключевых данных. На ФПСУ-IP могут быть установлены не более двух комплектов ключевых данных одной криптосети, при этом номер этих комплектов должен совпадать.

При выборе курсором строки с установленным комплектом ключевых данных криптосети, внизу таблицы отображается класс защиты согласно требованиям ФСБ к шифровальным (криптографическим средствам), КС2 или КС3. В строке «Всего ФПСУ» отображается общее количество ключей, сгенерированных ЦВК в рамках текущей серии.

Прежде чем установленные криптографические ключи могут быть использованы в конфигурации ФПСУ-IP, их требуется отметить, как *разрешенные* к применению. Разрешенные к использованию в конфигурации ФПСУ-IP ключи отмечены символом <+> в строке рядом с именем криптосети.

Для разрешения/запрета использования ключевых данных, установите курсор на строке и нажмите клавишу <*Пробел*>. Строка будет отмечена знаком «√». Далее, при

выполнении команды «*Сохранить <F2>*», состояние каждой помеченной строки будет изменено на противоположное – неразрешенные станут разрешенными и наоборот.

Если требуется выйти без сохранения установок, нажмите клавишу <*Esc*>.

Кнопка «*Установка ключей*» используется для перехода в окно интерфейса установки и удаления установленных на ФПСУ-IP ключевых данных (см. пункт «Установка ключей»).

7. 4. Конфигурация драйверов сетевых адаптеров

ФПСУ-IP рассчитан на использование двух сетевых адаптеров для организации двух рабочих портов (для связи локальных сетей) и, опционально, до двух сетевых адаптеров для организации канала резервирования (для связи с резервным ФПСУ-IP, если он есть).

В случае самостоятельной замены установленных на ФПСУ-IP сетевых адаптеров, их тип должен быть согласован с разработчиком.

ФПСУ-IP поставляется с предустановленной, рабочей конфигурацией LAN-адаптеров. Установленная конфигурация LAN-адаптеров может быть отредактирована, если при работе сети обнаруживаются ошибки, или требуется настроить ФПСУ-IP на использование других драйверов, изменить MAC или MTU.

Выбор команды «Конфигурация LAN адаптеров» главного меню открывает окно настройки сетевых адаптеров ФПСУ-IP. Для выполнения команды требуются права администратора класса *«Инженер»* или выше (см. раздел «Общие сведения», таблица 1).

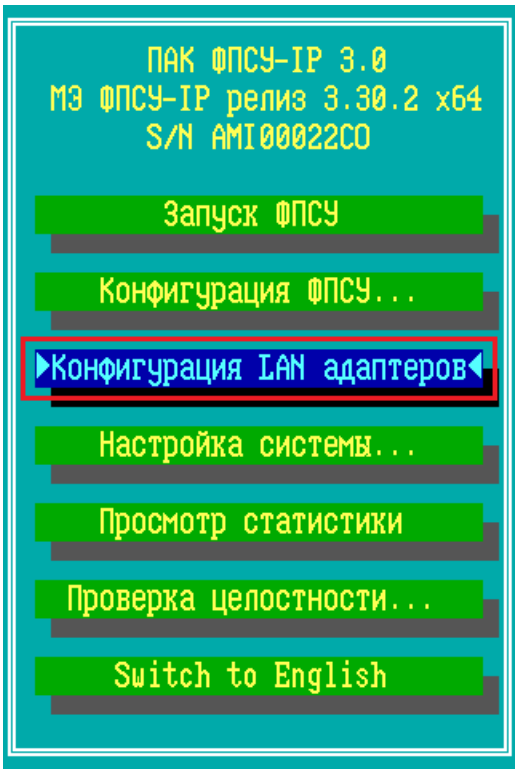


Рисунок 108 - Главное меню ФПСУ-IP

При выборе команды «Конфигурация LAN-адаптеров» и проверки полномочий администратора, система откроет окно установки параметров конфигурации LAN-адаптеров, представленное на рисунке ниже:

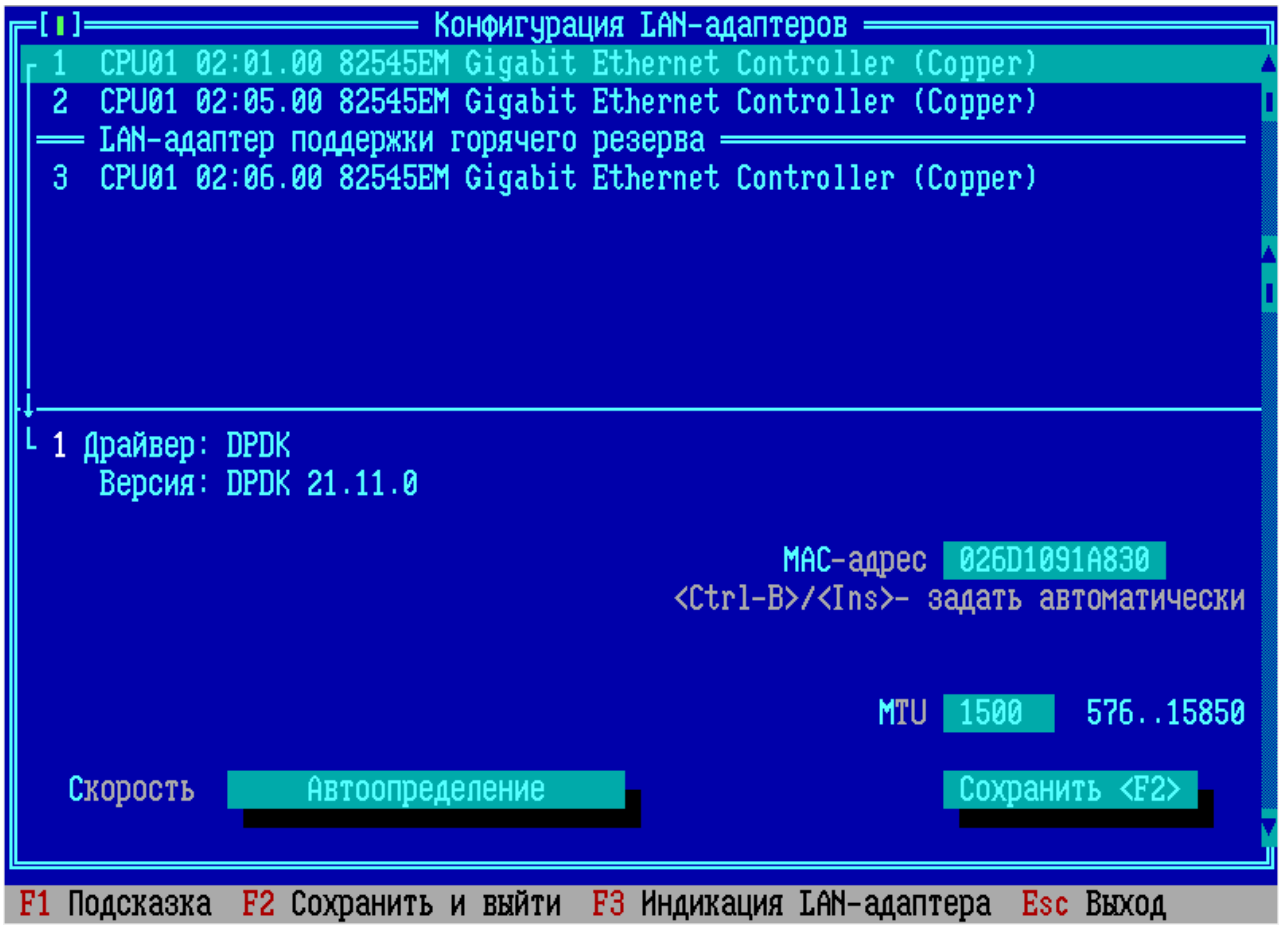


Рисунок 109 - Окно установки параметров конфигурации LAN-адаптеров

Для функционирования ФПСУ-IP требуется установленная конфигурация сетевых адаптеров, используемых для организации рабочих портов (строки с номерами 1 и 2). При этом номер адаптера (номер строки) будет соответствовать номеру порта, установленному для описания локальной сети, подключаемой к ФПСУ-IP через этот сетевой адаптер (см. раздел «Порты ФПСУ»).

Строки с номером 3 и 4, при наличии дополнительных сетевых адаптеров, отображают параметры LAN-адаптеров, применяемых для режима «горячего резерва». При первоначальной настройке в разделе LAN-адаптеров поддержки горячего резерва отображается одна строка такого адаптера, №3. Чтобы настроить запасной LAN-адаптер поддержки горячего резерва, следует установить курсор на строку №3 и нажать клавишу <*Ins*>.

Чтобы выбрать драйвер для какого-либо LAN-порта и установить параметры его работы, установите курсор на соответствующую пронумерованную строку с описателем порта и нажмите <*Enter*> или <*Пробел*>.

Когда на экран будет выдано окно выбора сетевых адаптеров, выделите курсором строку с названием сетевого адаптера, назначаемого для указанного логического порта ФПСУ-IP.

Рисунок 110 - Выбор сетевого адаптера для порта

Если количество обнаруженных драйверов для выбранного LAN-адаптера, отображаемое в нижней строке окна, более одного, войдите в окно выбора драйверов при помощи клавиши <*Пробел*> и укажите используемый драйвер.

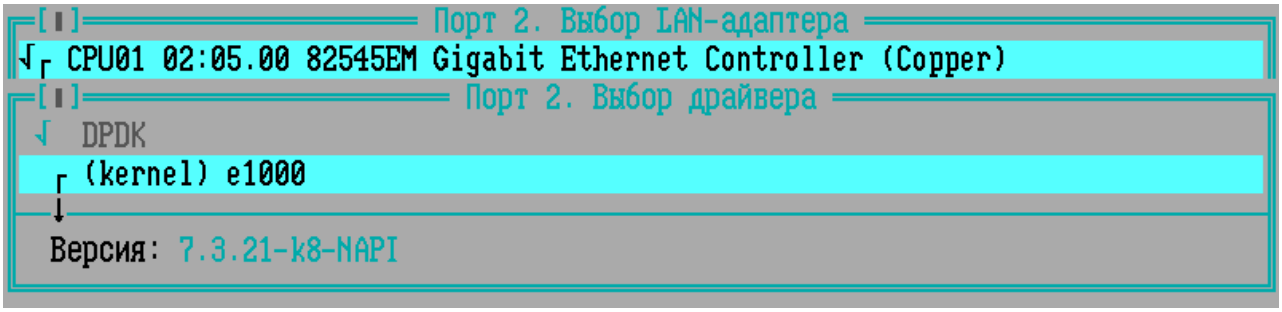


Рисунок 111 - Выбор драйвера для сетевого адаптера

ВНИМАНИЕ! Подсистема http-прокси (см. пункт «Http-proxy ФПСУ-IP») работает только при установленных на сетевых адаптерах драйверах типа **dpdk**.

После выбора используемого драйвера, название указанного адаптера появится в списке LAN-портов, а в нижней части окна установки появится список его параметров и список возможных действий. Необходимо установить два параметра: «Скорость» и «MAC-адрес».

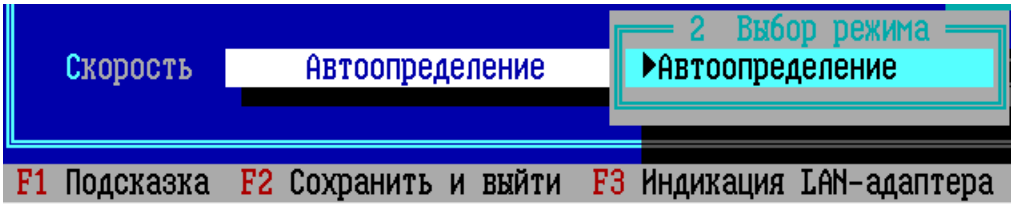


Рисунок 112 - Выбор режима работы адаптера

Для установки скорости выделите его поле курсором при помощи клавиш <*Tab*>, <→> или <←>, затем нажмите <*Пробел*>. В появившемся окне выбора выделите требуемое значение режима работы адаптера. Рекомендуемое значение – «***Автоопределение***».

Для установки MAC-адреса выделите его поле курсором и наберите с клавиатуры желаемое значение. Если драйвер адаптера позволяет, ФПСУ-IP может автоматически определить аппаратный адрес – в таком случае под строкой с MAC-адресом будет содержаться соответствующее предложение системы. При нажатии комбинации клавиш <*Ctrl+Ins*> будет сформирован и установлен адрес, уникальный для данного серийного номера ФПСУ-IP. Автоматическая установка MAC-адреса является обязательной для организации работы горячего резерва: обеспечивает идентичность аппаратных адресов для основного и резервного ФПСУ-IP.

ВНИМАНИЕ! Автоматическую установку MAC-адреса следует выполнять ПОСЛЕ установления на ФПСУ-IP обновления с серийным номером!

Дополнительным действием, отображаемым в статусной строке окна «Конфигурация LAN-адаптеров», является команда «*F3 Индикация LAN-адаптера*». Для визуальной индикации адаптера нажмите клавишу <*F3*>. При этом LED-светодиод сетевого адаптера (в случае наличия) начнет мигать, указывая на конфигурируемое устройство.

MTU каждого сетевого адаптера установлен в значение по умолчанию, 1500. При необходимости, это значение можно изменить в рамках допустимого для выбранного сетевого адаптера (в примере на рисунке ниже MTU выбранного сетевого адаптера может быть установлен в пределах от 576 до 15850 байт).

По окончании установки параметров выбранного сетевого адаптера нажмите кнопку «*Сохранить <F2>*» в нижней части окна. При этом настройки рабочих портов (с номерами 1 и 2) могут быть сохранены только в паре, в противном случае (при попытке сохранения настроек только одного порта) на экран будет выдано сообщение о невозможности сохранения установок.

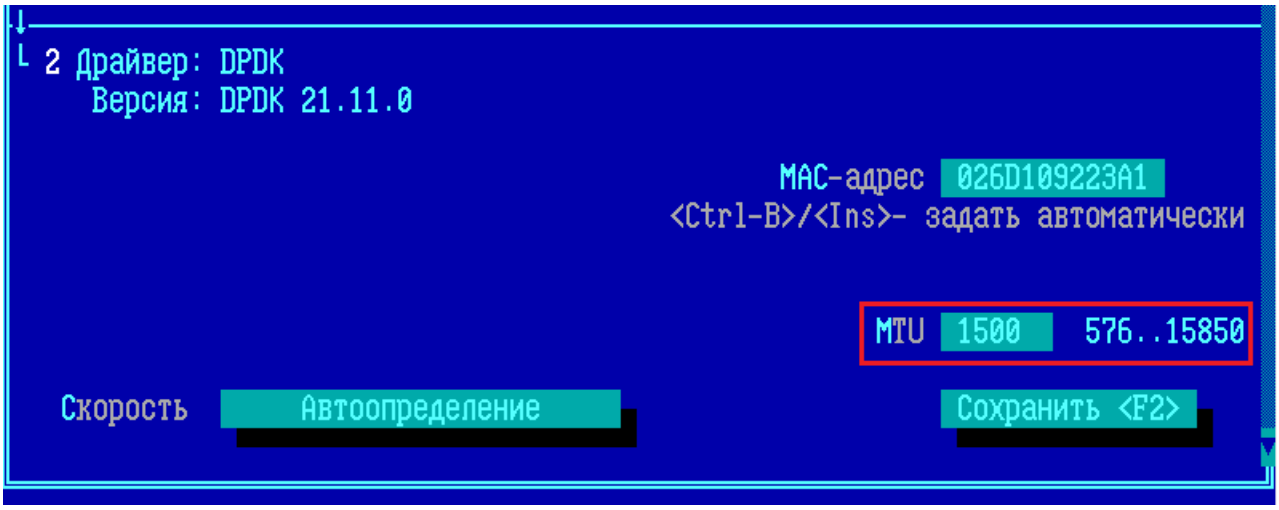


Рисунок 113 - Изменение параметра MTU сетевого адаптера с DPDK драйвером

Выбор любого установленного адаптера можно отменить, воспользовавшись клавишей <*Del*>. Выдав запрос на подтверждение операции, система удалит существующие установки и очистит строку, после чего порт можно настраивать заново, как было описано выше.

При необходимости изменить нумерацию уже настроенных портов выделите нужную строку и переместите ее вверх или вниз при помощи комбинации клавиш <*Ctrl* ↓> или <*Ctrl* ↑> соответственно.

Выход без сохранения выполненных настроек осуществляется по клавише <*Esc*>.

ВНИМАНИЕ! Некорректное конфигурирование адаптеров локальной сети может привести к неправильной или неэффективной работе всего участка сети. Устранение некоторых неполадок, связанных с конфликтом оборудования ФПСУ-IP, описано в разделе «Устранение неполадок, связанных с работой сетевого оборудования».

7. 4. 1. Агрегированный сетевой адаптер

При конфигурировании LAN-адаптеров может быть применена технология объединения нескольких физических сетевых адаптеров в агрегированный сетевой адаптер, Link Aggregation. Поддерживается три режима агрегации каналов - LACP (IEEE 802.3AD/802.1AX), Balance XOR и Active Backup.

Чтобы сконфигурировать агрегированный сетевой адаптер, необходимо добавить LAN-адаптер по нажатию клавиши <*Ins*>, либо сбросить настройки выбранного LAN-адаптера по нажатию клавиши <*Del*>.

Выберите LAN-адаптер в состоянии «LAN-адаптер не выбран», по нажатию клавиши <*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*>.

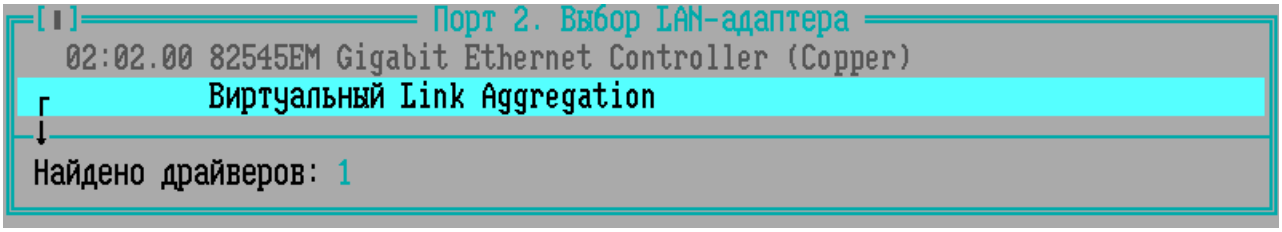


Рисунок 114 - Выбор сетевого адаптера для порта

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

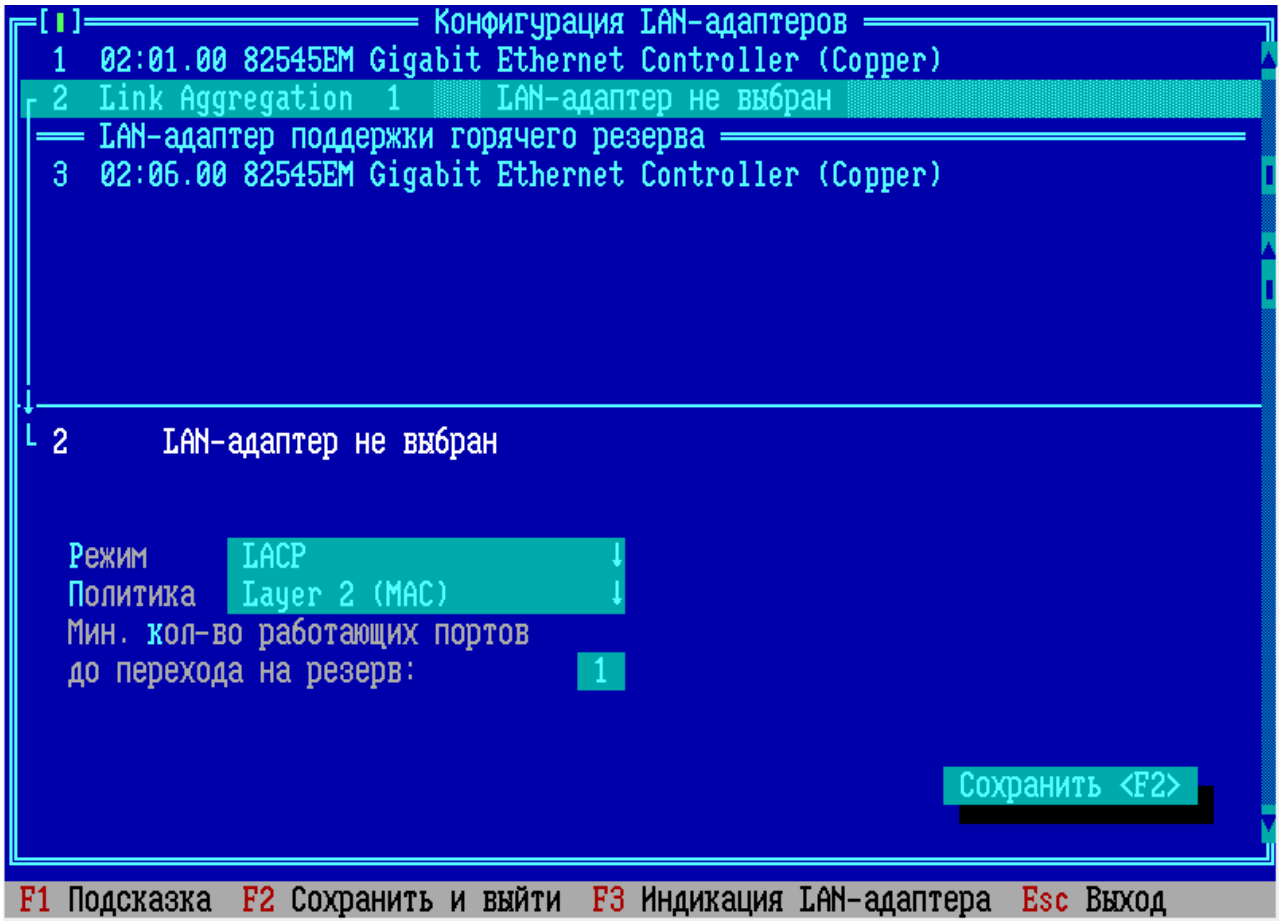


Рисунок 115 - Агрегированный сетевой адаптер

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*>.

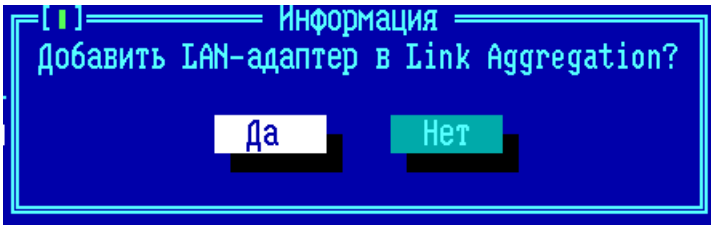
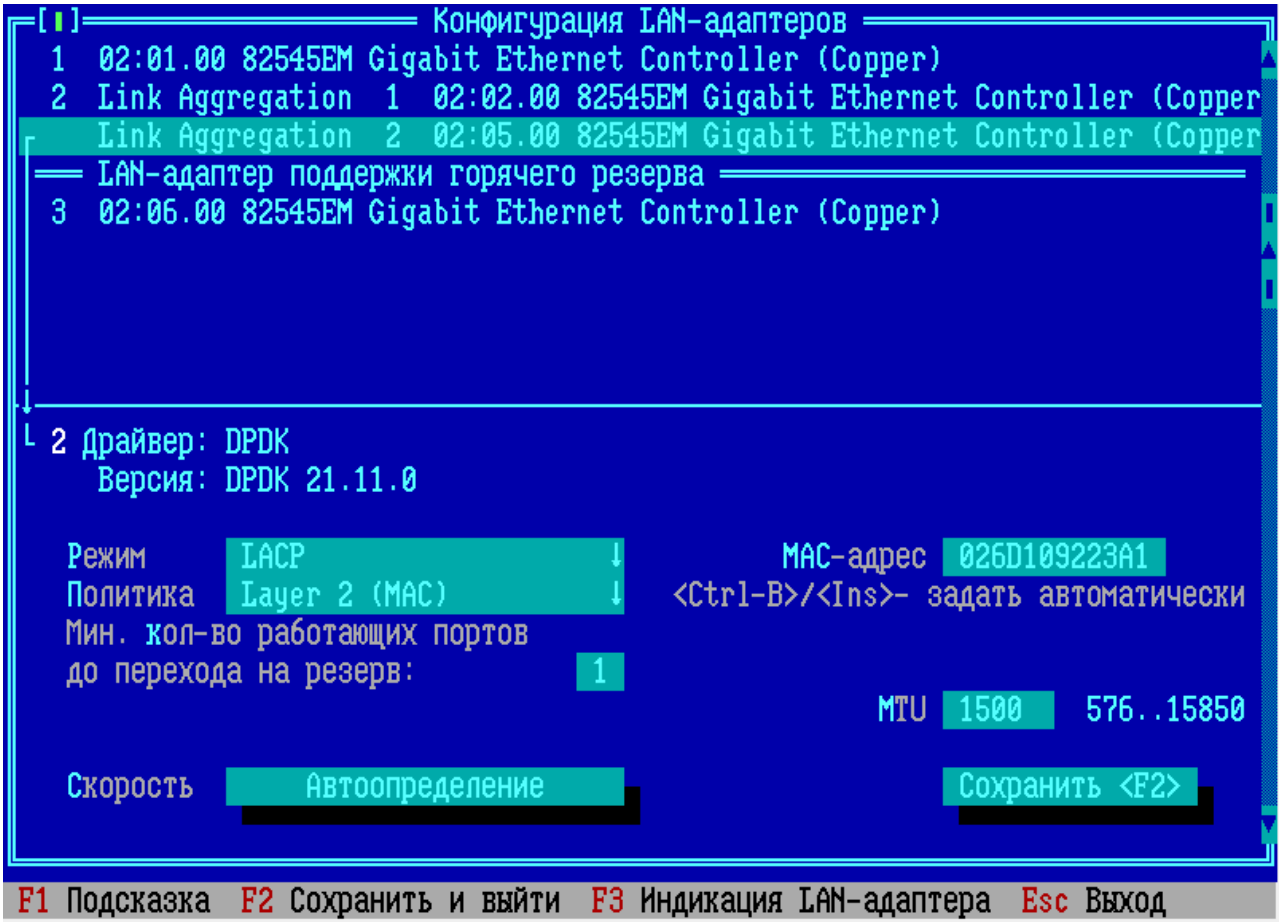


Рисунок 116 - Добавление LAN-адаптера

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 «↓», по нажатию клавиши <*Пробел*> открывается выпадающий список. Перемещение по списку осуществляется клавишами <↓> и <↑>, для выбора значения из списка выделите строку значения и нажмите клавишу <*Enter*>.



Примечание. Для агрегированного сетевого адаптера рекомендуется использовать LAN-адаптеры одинаковых типов с одинаковыми настройками (скорости, дуплекса, VLAN, типа порта).

Для сетевого адаптера необходимо задать следующие параметры:

Режим - режимы работы агрегированного сетевого адаптера:
Active Backup - режим, при котором активен только один порт, если он выходит из строя, оборудование переключается на другой работающий. Обеспечивается отказоустойчивость без увеличения скорости.
Balance XOR - режим, при котором активны несколько портов, исходящие пакеты

распределяются по нескольким линиям исходя из Политики (см. ниже). Обеспечивается балансировка нагрузки при передаче пакетов и отказоустойчивость.
LACP - динамическое объединение каналов в соответствии со спецификацией 802.3ad. Режим, при котором активны несколько портов, исходящие пакеты распределяются по нескольким линиям исходя из Политики (см. ниже), линии могут назначаться только для приема или только для передачи.

Политика определяет способ распределения пакетов по линиям для режимов «Balance XOR» и «LACP»:
L2 - балансировка на основе MAC-адреса отправителя;
L2-L3 - балансировка на основе MAC-адреса и IP адреса отправителя или получателя;
L3-L4 - балансировка на основе IP-адреса и TCP/UDP порта отправителя или получателя.

Минимальное количество работающих портов до перехода на резерв - от 2 до 22 в зависимости от аппаратной платформы. Управление ФПСУ-IP передается «горячему» резерву, в случае если количества работающих портов меньше указанного.

Задание параметров «Скорость», «MAC-адрес», «MTU» подробно описано в пункте «Конфигурация драйверов сетевых адаптеров».

7. 5. Применение 4 порта для доступа удаленного администратора

Сетевой адаптер, внесенный под номером 4 в список используемых ФПСУ-IP сетевых адаптеров, может быть задействован для предоставления доступа удаленного администратора к этому ФПСУ-IP. При этом взаимодействие с горячим резервом не блокируется и не ограничивается.

Если требуется, чтобы MAC-адрес сетевого адаптера №4 публиковался в ответ на запросы сетевого оборудования, то тип драйвера сетевого адаптера №4 должен быть выбран из предлагаемых вариантов для типа kernel (не dpdk!).

Для использования сетевого адаптера №4 в качестве выделенного адаптера для доступа удаленного администратора к ФПСУ-IP требуется выполнить следующие действия:

1. Задействовать подсистему горячего резервирования (активировать флаг «Резервирование активно» и **создать ключ горячего резерва**, см пункт «Настройка ФПСУ-IP на работу с партнером по резервированию»).
2. Включить опцию в конфигурации LAN-адаптеров «Интерфейс для удаленного управления ФПСУ»:

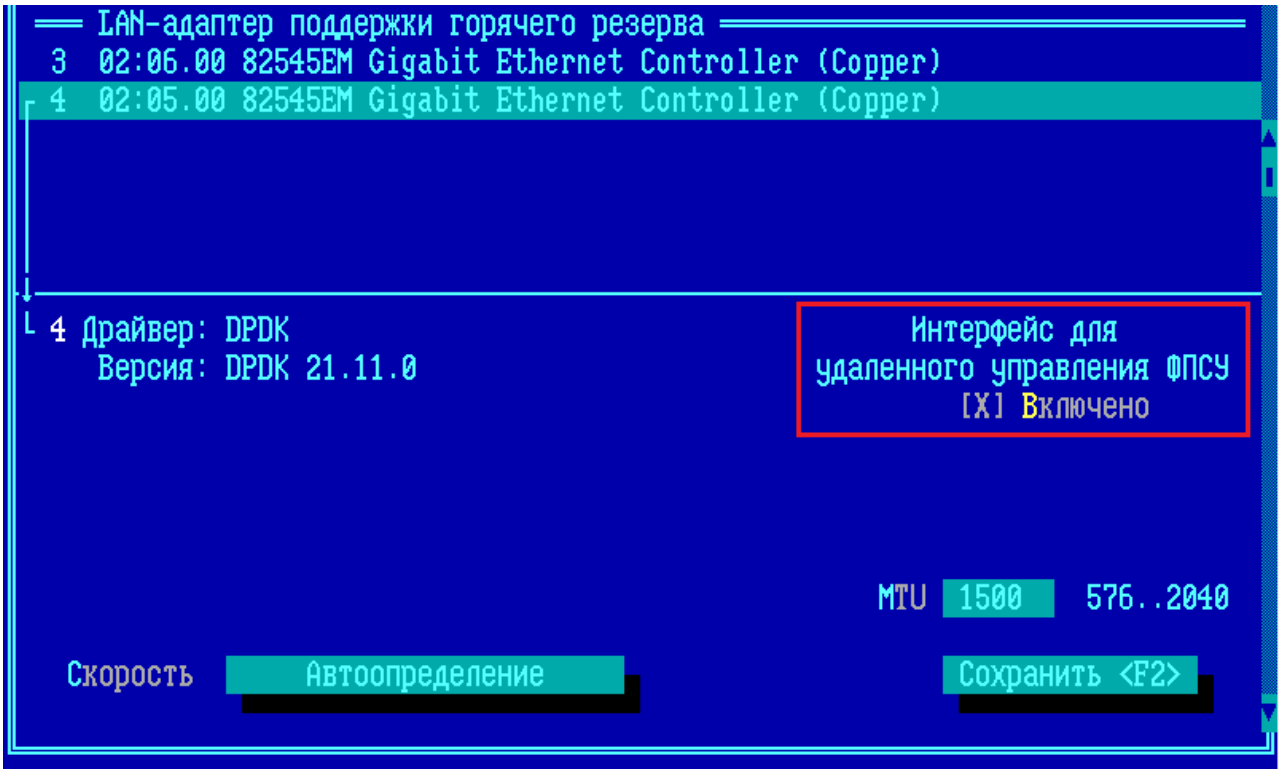


Рисунок 117 - LAN-адаптер №4 для удаленного администрирования подготовлен

3. Добавить в описание порта 1 (обязательно порт 1, не порт 2!) ФПСУ-IP дополнительный IP-адрес ФПСУ-IP, назначенный VLAN №4093 (см. пункт «Описание VLAN порта ФПСУ-IP»). Этот IP-адрес будет использоваться на УА ФПСУ-IP для доступа к ФПСУ-IP (к единственному, или основному, если задействована система горячего резервирования):

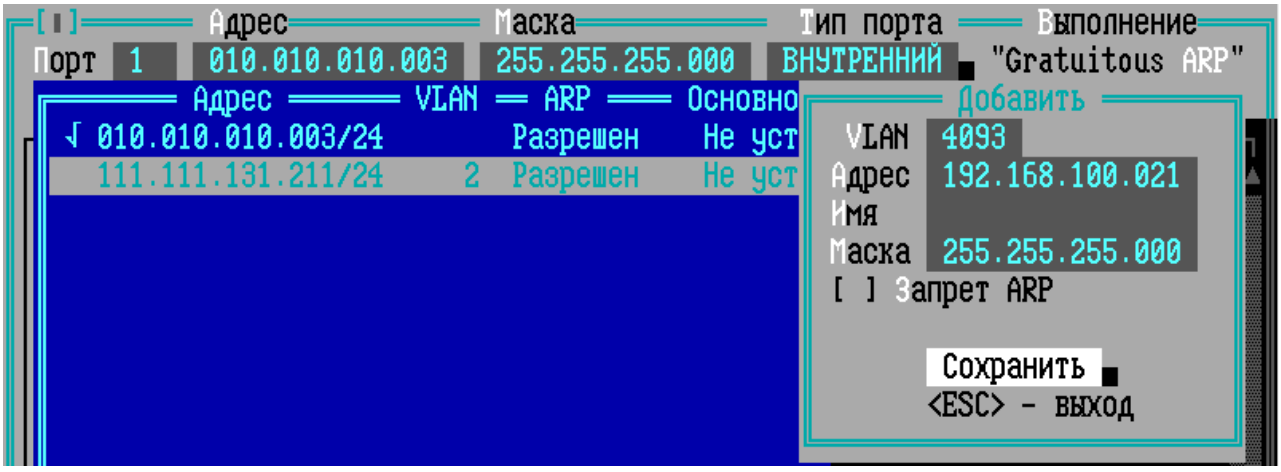


Рисунок 118 - Добавления IP-адреса порту ФПСУ в VLAN №4093

4. Добавить, если используется система горячего резервирования, в описание порта 1 (обязательно порт 1, не порт 2!) дополнительный IP-адрес ФПСУ-IP, назначенный VLAN №4094. Этот IP-адрес будет использоваться на УА ФПСУ-IP в качестве

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

После активации опции «Интерфейс для удаленного управления ФПСУ» сетевого адаптера №4, 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 сетевой адаптер №4.

Использование сетевого адаптера №4 для доступа удаленных администраторов можно проверить, 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 (за него отвечает сетевой адаптер №4 из используемых ФПСУ-IP):

Рисунок 119 - Адаптер №4 готов принимать соединения с удаленными администраторами

8. Настройка системы

По команде «Настройка системы» главного меню ФПСУ-IP, доступны установки параметров и режимов работы с обслуживающими подсистемами ФПСУ-IP: подсистемой разграничения доступа, подсистемой учета электронных идентификаторов, подсистемой регистрации удаленных администраторов, подсистемой аутентификации, СКЗИ и т.д. Выполнение команд меню «Настройка системы» позволит работать с ТМ-идентификаторами, принять дополнительные меры безопасности (установить пароль администратора), установить дополнительное или обновить существующее программное обеспечение (полученное от разработчика для данного ФПСУ-IP), а также определить рабочие параметры резервирования.

К этой же группе команд отнесена опция изменения (корректировки) текущих даты и времени ФПСУ-IP.

Команды, доступные из меню «Настройка системы» (описываются в подпунктах далее):

Рисунок 120 - Меню «Настройка системы»

8. 1. Регистрация ТМ-идентификаторов

Команда «Регистрация ТМ-идентификаторов» доступна из меню «Настройки системы» ФПСУ-IP.

Для выполнения команды требуются права класса «*Администратор*» или выше (см. раздел «Общие сведения», таблица 1).

Рисунок 121 - Выбор пункта «Регистрация ТМ-идентификаторов»

При выполнении, команда вызывает окно регистратора ТМ-идентификаторов, из которого доступны следующие операции:

- регистрация ТМ-идентификаторов новых администраторов ФПСУ-IP;
- удаление записанной на потерявших актуальность или скомпрометированных ТМ-идентификаторах ключевой информации;
- проверка ТМ-идентификаторов на исправность и корректность хранимой в них информации;
- включение или отключение подсистемы автозапуска ФПСУ-IP.

Окно регистратора содержит таблицу, показывающую наличие зарегистрированных ТМ-идентификаторов, а также состояние подсистемы автозапуска.

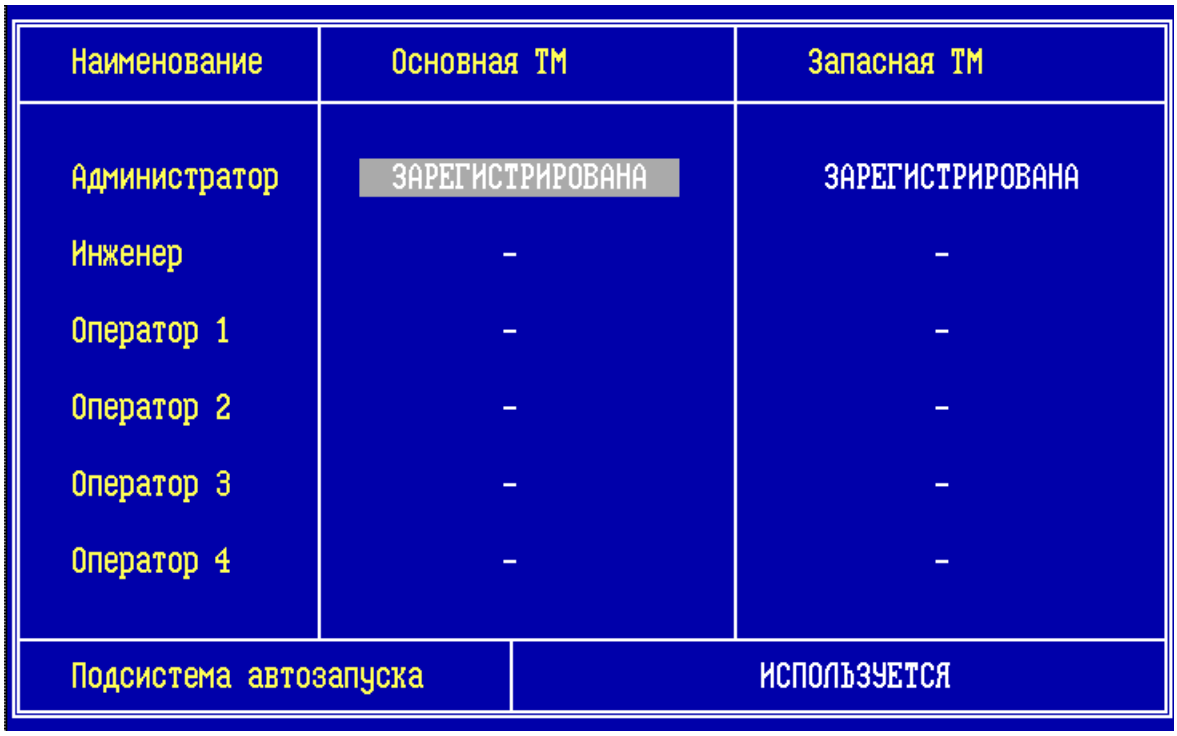


Рисунок 122 - Окно управления ТМ-идентификаторами ФПСУ-IP

Для включения подсистемы автозапуска перейдите в поле «Подсистема автозапуска» и нажмите клавишу <*Insert*>. Подтвердите на появившемся окне выполнение включения режима автозапуска. При включении электропитания ФПСУ-IP с активированной подсистемой автозапуска, ФПСУ-IP будет переведен режим фильтрации, как если бы эту команду выполнил пользователь с правами учетной записи «*Оператор*».

Для выключения подсистемы автозапуска перейдите в поле «Подсистема автозапуска» и нажмите клавишу <*Delete*>. Подтвердите на появившемся окне запрещение использования подсистемы автозапуска.

Для зарегистрированных ТМ-идентификаторов могут быть осуществлены следующие операции:

- «Основной» ТМ-идентификатор строки «Администратор», выдается администратору класса «Главный администратор», может быть только проверен;
- остальные ТМ идентификаторы – проверены, очищены или повторно зарегистрированы, с новой ключевой информацией.

Новый ТМ-идентификатор может быть только зарегистрирован как «запасная ТМ» для строки «Администратор», или «основная ТМ»/«запасная ТМ» для любого другого наименования пользователей. ***Основной ТМ-идентификатор администратора зарегистрирован быть не может, он перерегистрируется только при повторной***

инсталляции или переходе ФПСУ-IP из технологического в рабочий режим, и только на ТМ-идентификатор, поставляемый вместе с дистрибутивом ФПСУ-IP и маркированный как ТМ-идентификатор Главного администратора.

Разрешенные для текущей записи действия выполняются при помощи клавиш, указанных в динамически меняющейся строке подсказки в нижней части экрана.

Для удаления записанной на потерявшем актуальность или скомпрометированном ТМ-идентификаторе ключевой информации перейдите в соответствующее ТМ-идентификатору поле таблицы и нажмите клавишу <*Delete*>. Подтвердите в появившемся окне очистку ТМ-идентификатора. При этом соответствующий ТМ-идентификатору ключ запуска будет удален с ФПСУ-IP.

При выполнении операций по регистрации или очистке система будет требовать подтверждения полномочий администратора (посредством прижатия соответствующей touch-memory к считывателю ТМ или подключения TM-Key) с целью предотвращения несанкционированных действий.

8. 2. Установка дополнений/изменений

Опция «Установка дополнений/изменений» меню «Настройка системы» предназначена для установки новых программных модулей, опциональных подсистем, или обновлений существующих модулей ФПСУ-IP (операции доступны администраторам класса «*Администратор*» или выше, см. раздел «Общие сведения», таблица 1).

Рисунок 123 - Выбор пункта «Установка дополнений/изменений»

При получении информации о выходе обновления программного обеспечения ФПСУ-IP, администратор безопасности должен определить необходимость установки данного обновления и обратиться в службу технической поддержки организации-поставщика или производителя ФПСУ-IP за получением обновления.

Все изменения или дополнения для ФПСУ-IP представляются в двух файлах: файл списка (расширение .up0) и файл, содержащий изменения, разрешенные для данного серийного номера ФПСУ-IP (расширение .upd).

Файлы с изменениями должны сопровождаться контрольными суммами, которые следует проверить перед установкой обновлений или дополнений.

Для установки дополнений/изменений выполните следующие действия:

1. Выберите пункт меню «Установка дополнений/изменений». Для продолжения потребуется подтвердить полномочия администратора, приложив ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-IP (или подключив USB ТМ-идентификатор к USB-порту ФПСУ-IP).

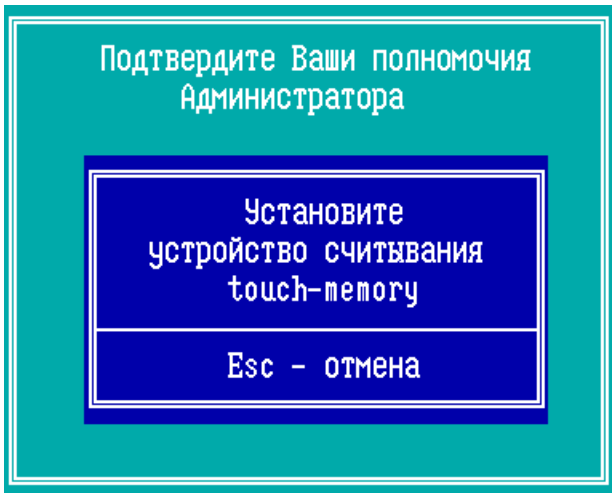


Рисунок 124 - Подтверждение полномочий администратора

2. Подключите USB-носитель к АП ФПСУ-IP или к виртуальной машине.

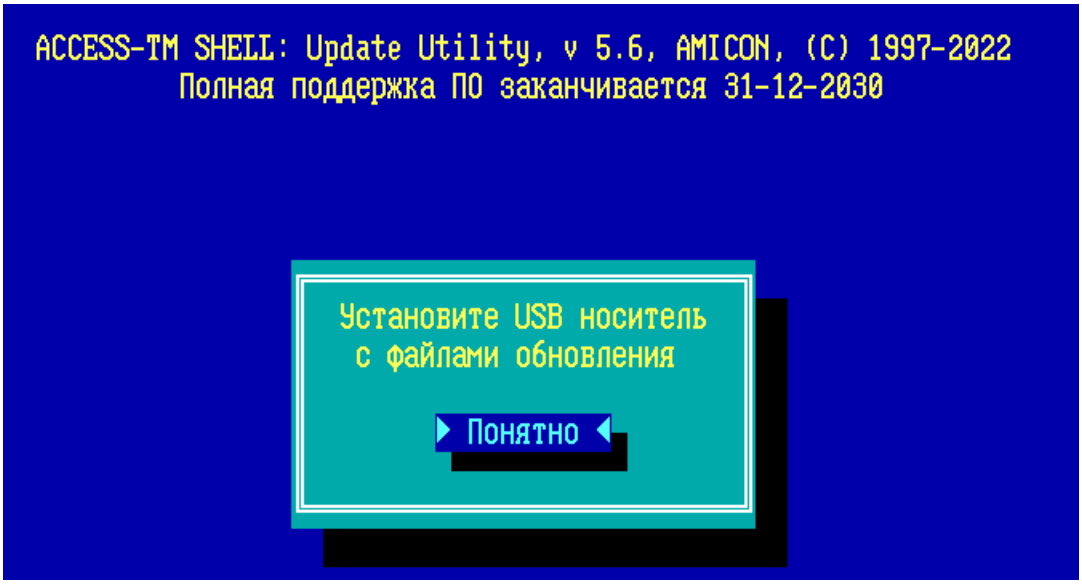


Рисунок 125 - Подключение USB-носителя

3. Выберите файл обновления и нажмите клавишу <*Enter*>.

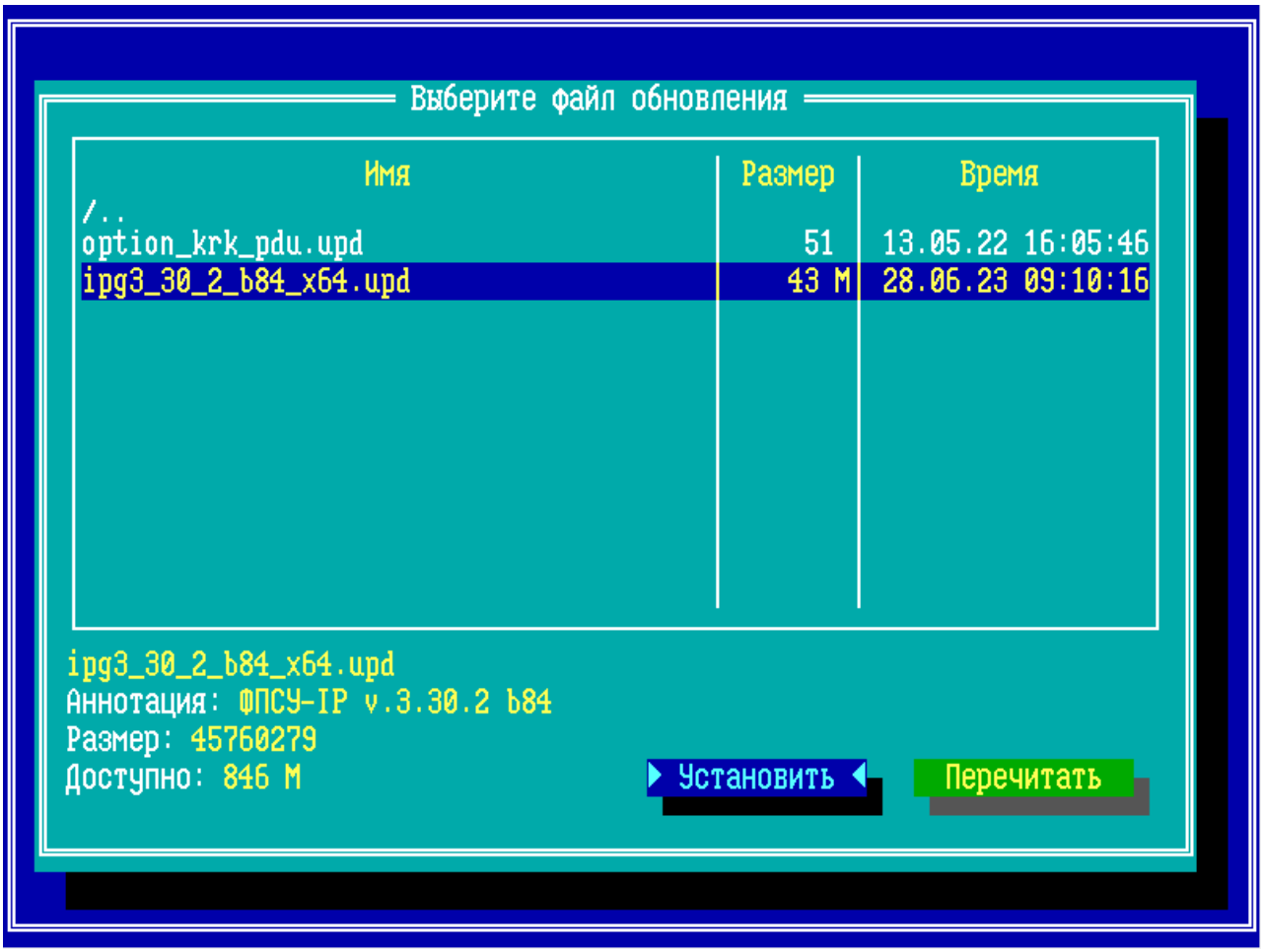


Рисунок 126 - Выбор файла обновления

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

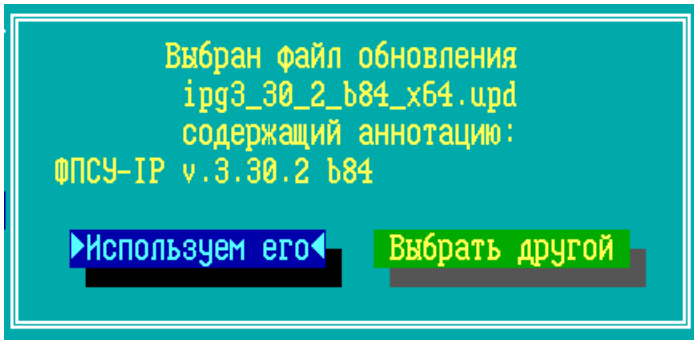


Рисунок 127 - Подтверждение обновления

Начнется процесс установки обновления, необходимо подтверждать этапы установки.

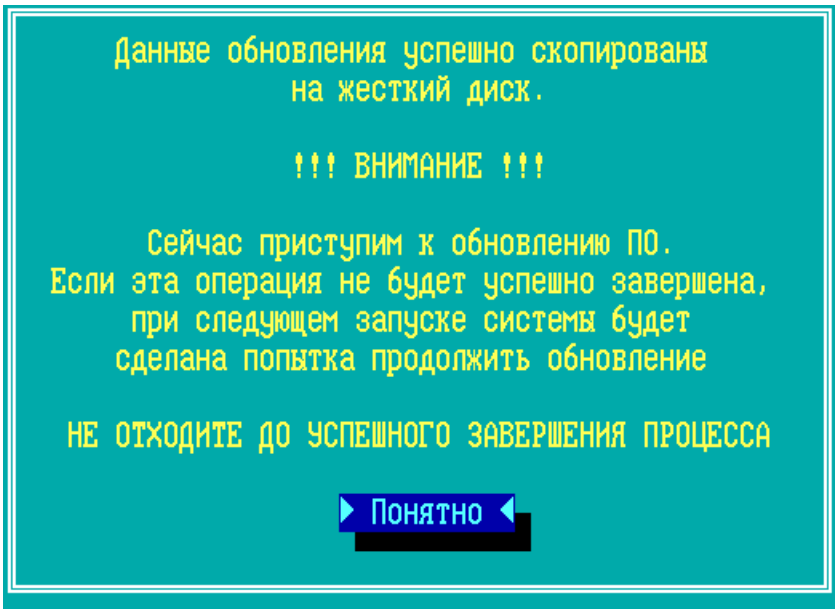


Рисунок 128 - Процесс установки обновления

После установки обновления система будет перезагружена автоматически.

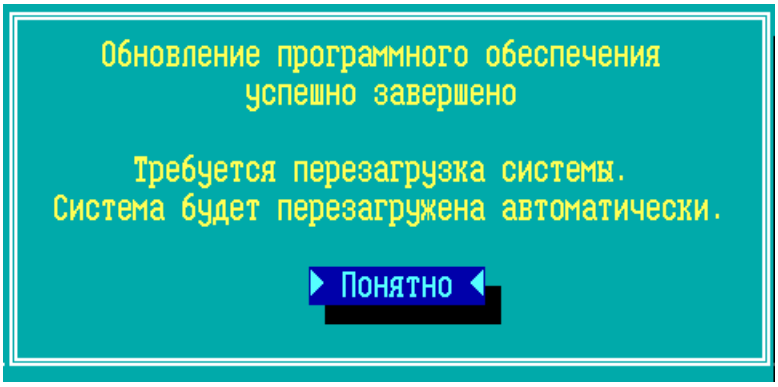


Рисунок 129 - Завершение процесса установки

После перезагрузки на экране будет выдано сообщение для выбора режима ФПСУ-IP – настройки и изменения конфигурации или фильтрации пакетов.

Рисунок 130 - Автовключение фильтрации

Для запуска ФПСУ-IP в режиме фильтрации пакетов нажмите кнопку «Понятно». Для отображения главного меню с командами настройки и запуска ФПСУ-IP нажмите <*Enter*>.

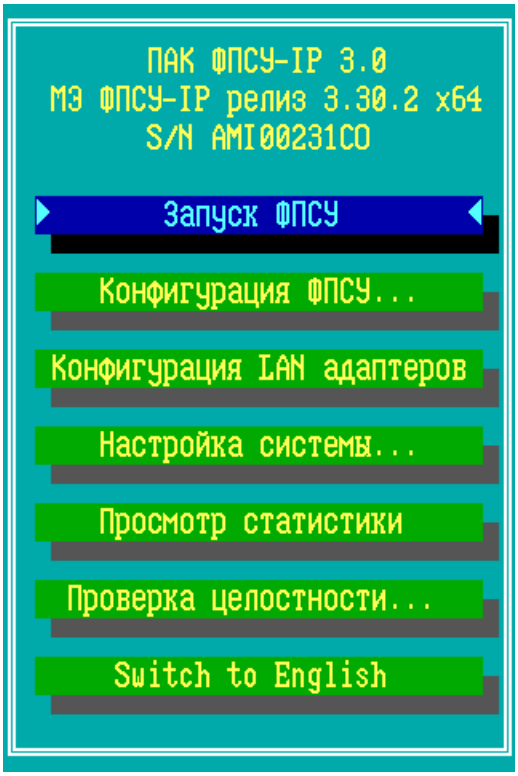


Рисунок 131 - Главное меню

8. 3. Установка пароля администратора

Команда «Установка пароля администратора» меню «Настройка системы» предназначена для задействования, изменения или отмены пароля на вход в подсистемы конфигурирования ФПСУ-IP и сетевых адаптеров. Операции доступны администраторам класса «*Администратор*» и выше (см. раздел «Общие сведения», таблица 1).

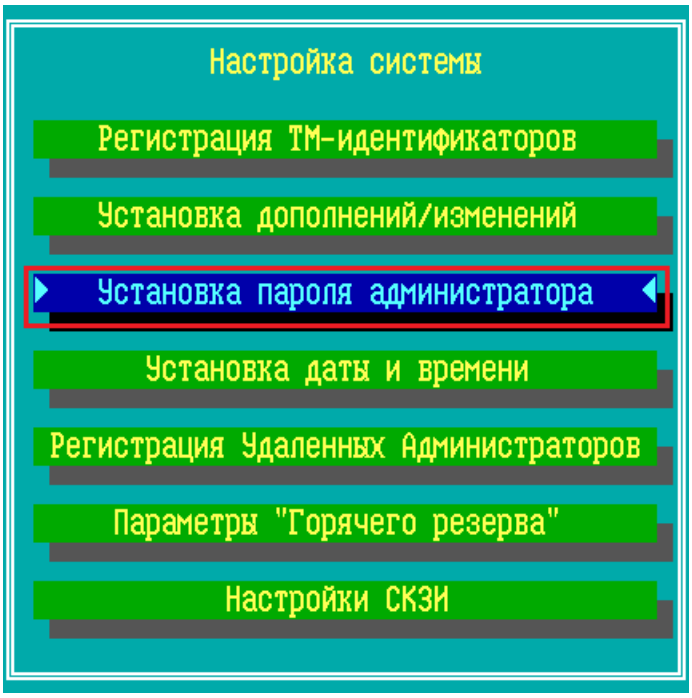


Рисунок 132 - Команда «Установка пароля администратора»

При выборе опции откроется окно, в поле редактирования которого следует ввести пароль - комбинацию из 5 - 15 символов.

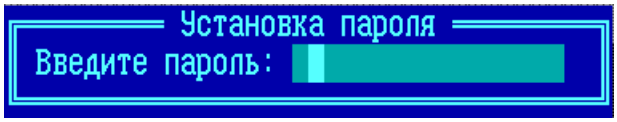


Рисунок 133 - Установка пароля администратора

Поскольку вводимые символы не будут отображаться на экране, подсистема попросит ввести пароль еще раз с целью исключения возможной ошибки. Установка будет произведена только после повторного введения идентичной комбинации символов.

В операции проверки пароля участвуют ASCII-коды символов, поэтому администратор должен быть внимателен к набору символов в определенных регистре и алфавите.

После установки пароля при попытке изменить конфигурацию ФПСУ-IP (выборе соответствующей команды) подсистема будет блокировать любые действия администратора до ввода установленного пароля.

Администратор может отменить установку пароля. Для этого он должен выбрать ту же команду «*Установка пароля администратора*», оставить поле пустым (не вводить символы), и нажать <*Enter*>. Отмену пароля он сможет осуществить только после введения текущего пароля, который запросит подсистема.

Пароль также может быть изменен администратором, для чего команде «*Установка пароля администратора»* он должен по запросу подсистемы подтвердить текущий пароль, а затем дважды ввести новый пароль.

ВНИМАНИЕ! Если администратор забыл пароль, то для возможности внесения любых изменений в конфигурацию или режим работы ФПСУ-IP потребуется повторная установка ФПСУ-IP с дистрибутива.

8. 4. Установка даты и времени

Команда меню «Настройка системы» → «Установка даты и времени» предназначена для ручной корректировки или изменения текущего времени и текущей даты, установленных на ФПСУ-IP, в условиях функционирования собственной изолированной операционной среды ФПСУ-IP.

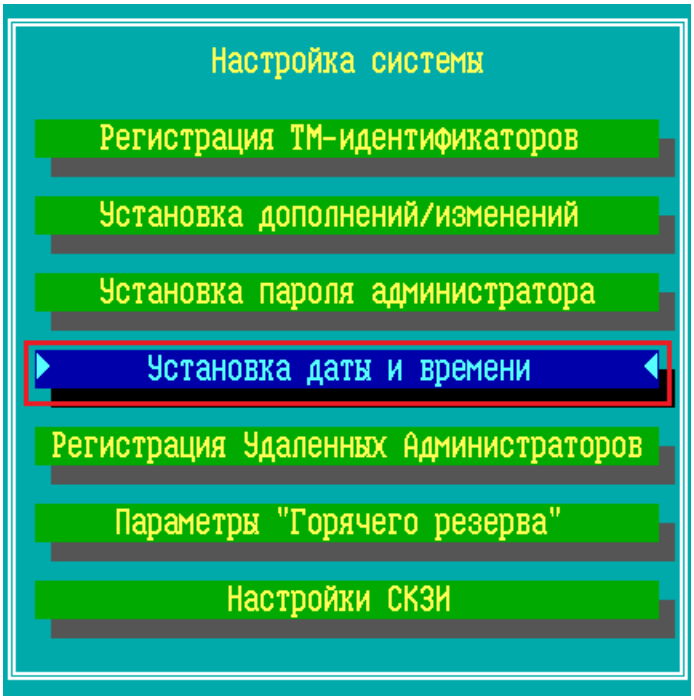


Рисунок 134 - Команда «Установка даты и времени»

При активизации команды на экран будет выдано диалоговое окно:

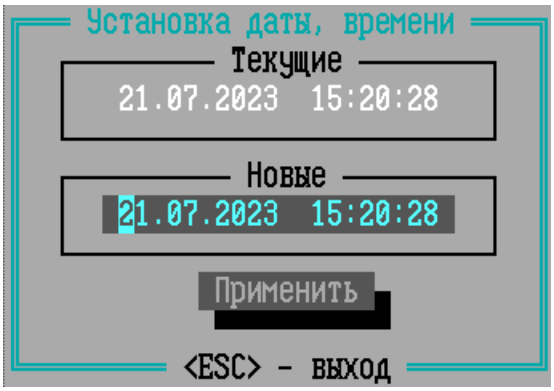


Рисунок 135 - Установка даты и времени на ФПСУ-IP

В окне отображаются текущие дата и время, а также содержатся два поля ввода (соответственно для даты и для времени) и кнопка команды «*Применить*». При обращении к данной опции поля ввода содержат дублированные значения текущих даты и времени. Перемещение внутри каждого окна осуществляется при помощи клавиш управления горизонтальным движением курсора, перемещение между окнами - при помощи клавиши <*Tab*>.

Значения устанавливаются в режиме замены: чтобы изменить отображаемый в поле ввода символ, следует установить на него курсор и нажать клавишу с нужной цифрой, после чего старый символ будет заменен на новый.

Чтобы новое значение параметров вступило в силу, следует выделить курсором команду «*Применить*» и нажать клавишу <*Enter*>.

Для наиболее точной установки времени рекомендуется ввести в соответствующее поле значение, немного превышающее текущее время и отметить курсором команду «*Применить*» (при этом значение поля будет оставаться постоянным). В момент, когда реальное время на часах, служащих эталоном для установки, достигнет отображаемого значения, следует нажать клавишу <*Enter*>, после чего текущее время будет установлено и начнется отсчет секунд.

Выход из режима установки даты и времени производится по нажатию клавиши <*Esc*>.

8. 5. Регистрация Удаленных Администраторов

Команда меню «Настройка системы» → «Регистрация Удаленных Администраторов» предназначена для:

- регистрации учетных записей удаленных администраторов ФПСУ-IP;
- предоставления или отмены им прав на доступ к подсистемам ФПСУ-IP;

- удаления ранее зарегистрированных удаленных администраторов;
- выдачи ключа аутентификации ФПСУ-IP для удаленного администратора;
- повторной генерации ключей аутентификации ФПСУ-IP, используемых в подсистеме удаленного управления.

Рисунок 136 - Команда «Регистрация Удаленных Администраторов»

Операции доступны администраторам класса «*Администратор*» и выше (см. раздел «Общие сведения», таблица 1).

Если был установлен пароль на вход в подсистему регистрации удаленных администраторов (см. раздел «Установка пароля администратора»), при выборе команды необходимо ввести пароль.

Взаимная регистрация ФПСУ-IP и удаленного администратора производится следующим образом:

1. локальным администратором ФПСУ-IP выдается на внешний USB-flash носитель файл с ключом аутентификации ФПСУ-IP;
2. файл с ключом аутентификации ФПСУ-IP отправляется удаленному администратору (передача файла с аутентификатором по незащищенной сети передачи данных запрещается);
3. получив файл с ключом аутентификации, администратор регистрирует у себя данный ФПСУ-IP в программе «Удаленный администратор ФПСУ-IP»;
4. удаленный администратор с помощью программы «Удаленный администратор 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»).

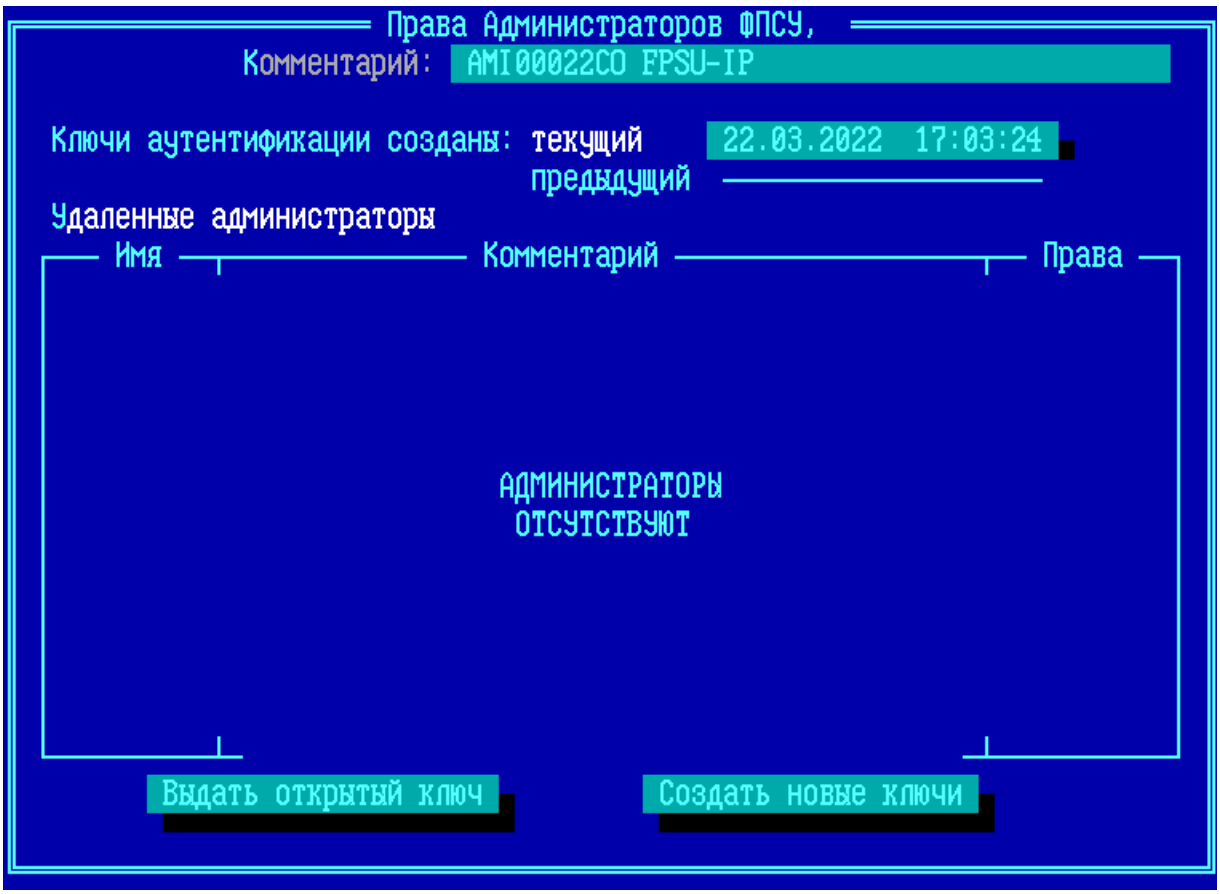


Рисунок 137 - Список удаленных администраторов

Количество удаленных администраторов, зарегистрированных на ФПСУ-IP, не может превышать 128.

Выход из подсистемы регистрации удаленных администраторов осуществляется

клавишами <*Alt+X*> или <*Esc*>.

8. 5. 1. Регистрация удаленного администратора на ФПСУ-IP

Для регистрации первой учетной записи удаленного администратора на ФПСУ-IP нажмите клавишу <*Ins*>, установив курсор на текст «Администраторы отсутствуют». Подсистема запросит установить носитель с ключами аутентификации удаленных администраторов, которые должны быть предварительно получены от удаленного администратора. Подключите USB-flash с ключами аутентификации удаленных администраторов и нажмите кнопку «*OK*», или клавишу <*Enter*>.

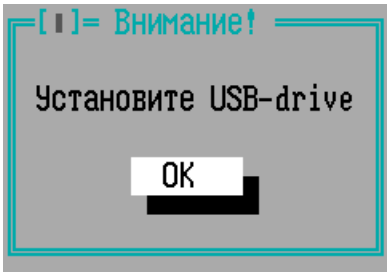


Рисунок 138 - Выбор USB-носителя с ключами аутентификации

Когда подсистема опознает и считает ключи аутентификации удаленных администраторов, она выдаст окно, содержащее список их описателей. В окне «Обнаружены данные» необходимо сначала отметить регистрируемые учетные записи администраторов клавишей <*Пробел*> (рядом с регистрируемой учетной записью проставляется знак «√»), а потом выполнить команду «*Добавить отмеченные*».

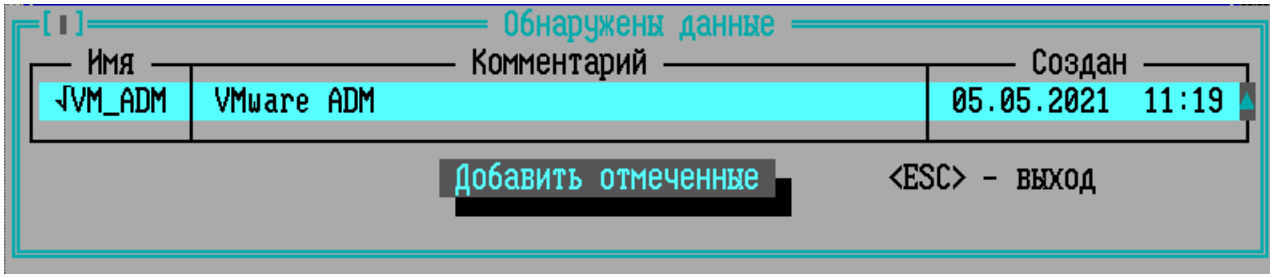


Рисунок 139 - Найденные аутентификаторы удаленного администратора

После выполнения команды зарегистрированные удаленные администраторы появятся в списке окна «Права администраторов».

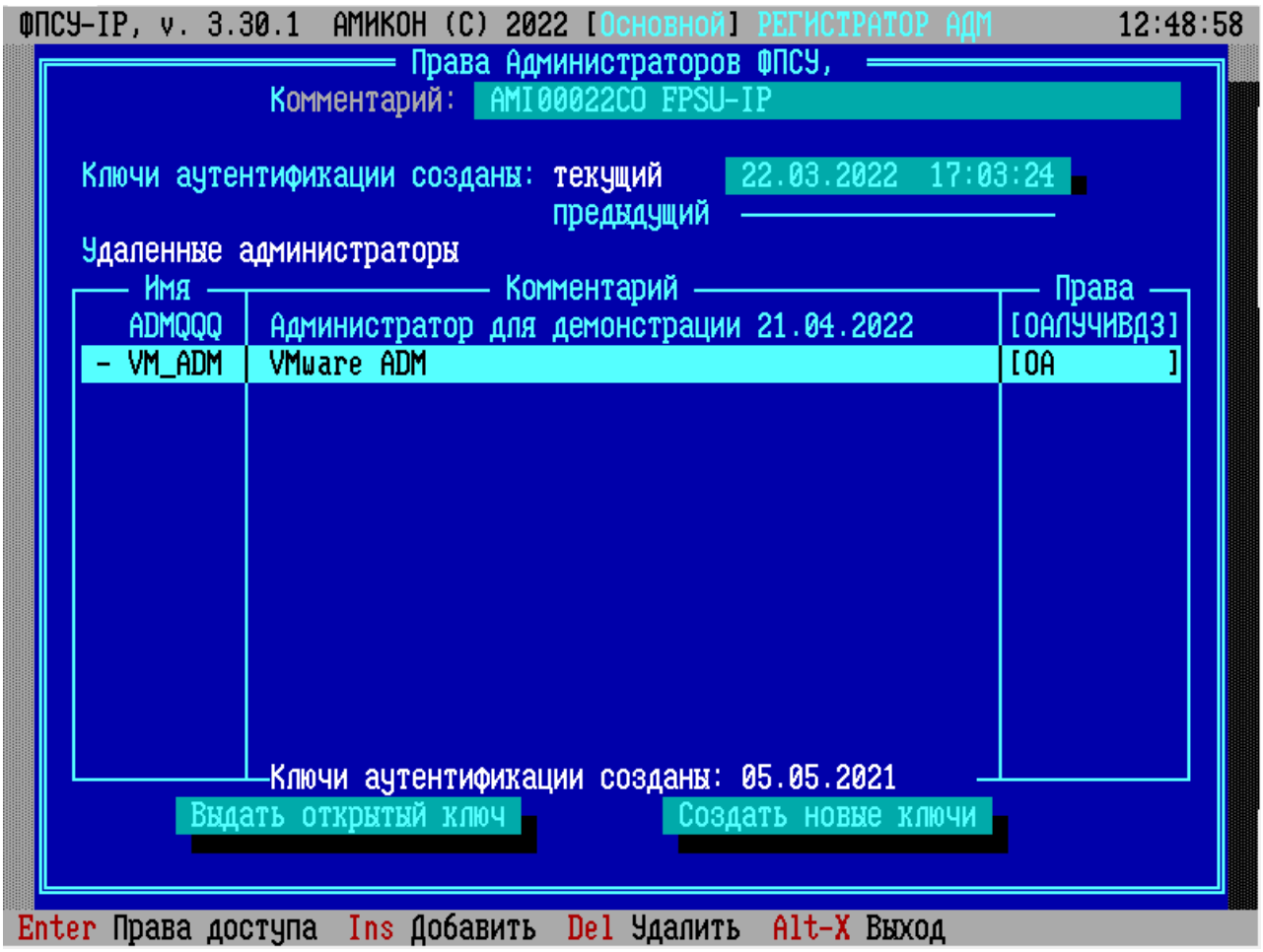


Рисунок 140 - Зарегистрирован удаленный администратор

Для каждого зарегистрированного удаленного администратора будет отображаться имя, комментарий к имени, права на доступ к подсистемам ФПСУ-IP и дата создания ключа аутентификации удаленного администратора.

Новый удаленный администратор регистрируется на ФПСУ-IP не только с минимальными правами, но и в состоянии «Временно запрещен».

В статусной строке окна динамически (в зависимости от производимой операции) отображаются варианты возможных действий с учетными записями удаленных администраторов: установить или изменить права (<*Enter*>), зарегистрировать новые (<*Ins*>), удалить имеющиеся из списка (<*Del*>) или выйти из подсистемы регистрации (<*Alt+X*> или <*Esc*>).

Для присвоения удаленному администратору прав на доступ к подсистемам ФПСУ-IP или изменения существующих, отметьте его в списке и нажмите <*Enter*>. В появившемся окне можно установить или изменить права (права на опрос текущего состояния и

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

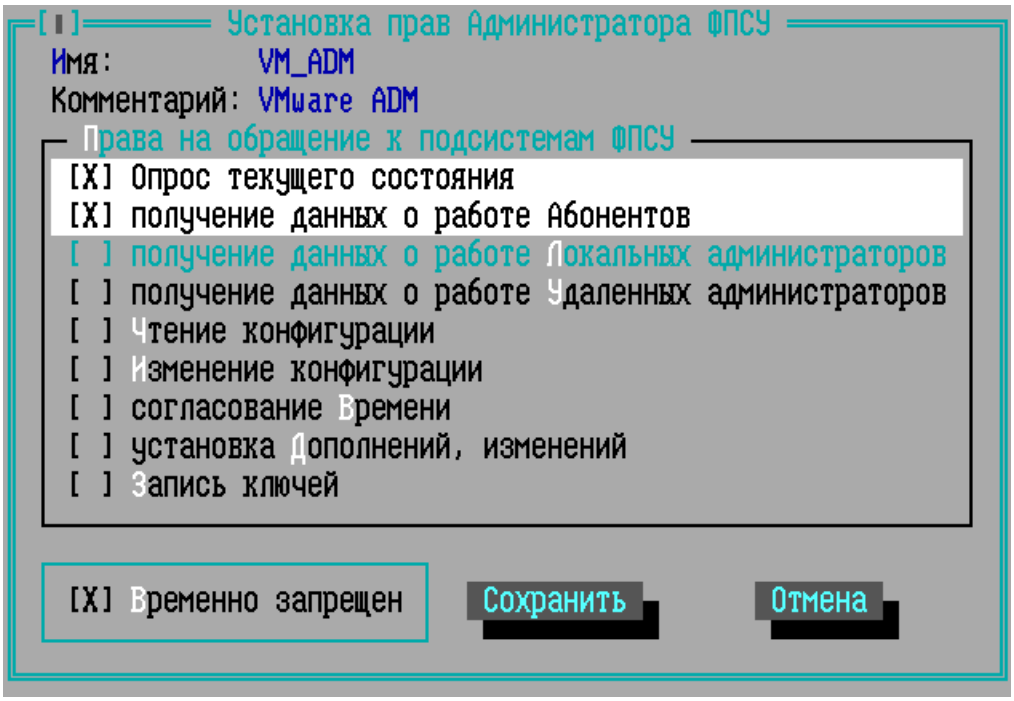


Рисунок 141 - Назначение прав удаленному администратору

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!

ВНИМАНИЕ! Синхронизация времени через УА будет отключена при работающей синхронизации через NTP.

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

8. 5. 2. Ключи аутентификации ФПСУ-IP

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

Ключи аутентификации ФПСУ-IP могут иметь статус «текущие» и «предыдущие». И «текущие» и «предыдущие» ключи аутентификации являются действительными для установления соединения с удаленным администратором. При создании нового комплекта ключей аутентификации ФПСУ-IP, «текущие» ключи становятся «предыдущими», а «предыдущие» становятся недействительными.

Для записи текущего ключа аутентификации ФПСУ-IP на внешний носитель, с целью регистрации его удаленным администратором, нажмите, находясь в окне списка зарегистрированных удаленных администраторов, кнопку «*Выдать открытый ключ*». Выдать предыдущий ключ аутентификации ФПСУ-IP нельзя.

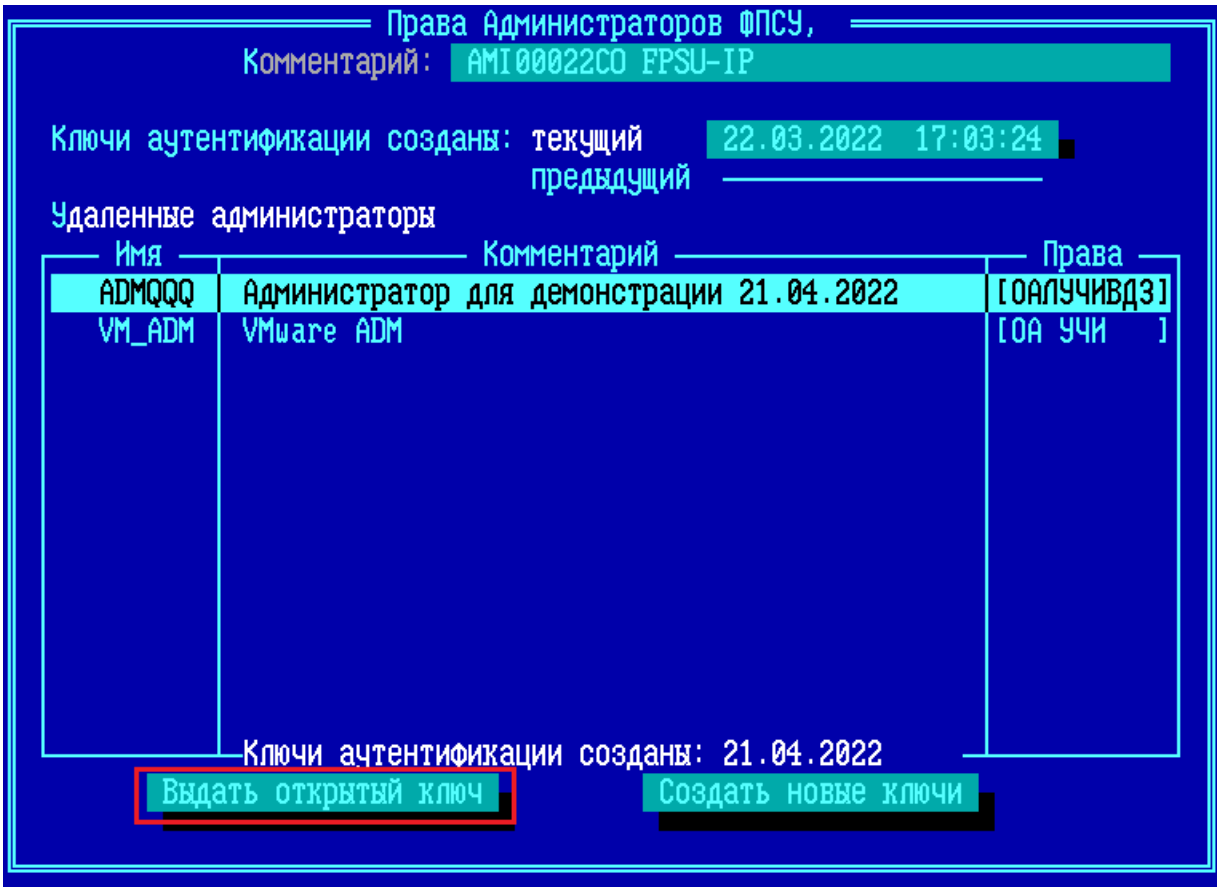


Рисунок 142 - Команда выдачи открытого ключа аутентификации ФПСУ-IP

Для выработки нового комплекта ключей аутентификации ФПСУ-IP, выполните команду «*Создать новые ключи*». В случае компрометации «текущих» ключей

аутентификации этой командой придется воспользоваться два раза (сначала сделать «текущие» ключи «предыдущими», а затем недействительными).

После генерации новых ключей аутентификации ФПСУ-IP, доступ всех удаленных администраторов к ФПСУ-IP будет заблокирован. Удаленным администраторам потребуется выполнить повторную регистрацию ФПСУ-IP, с новыми ключами аутентификации.

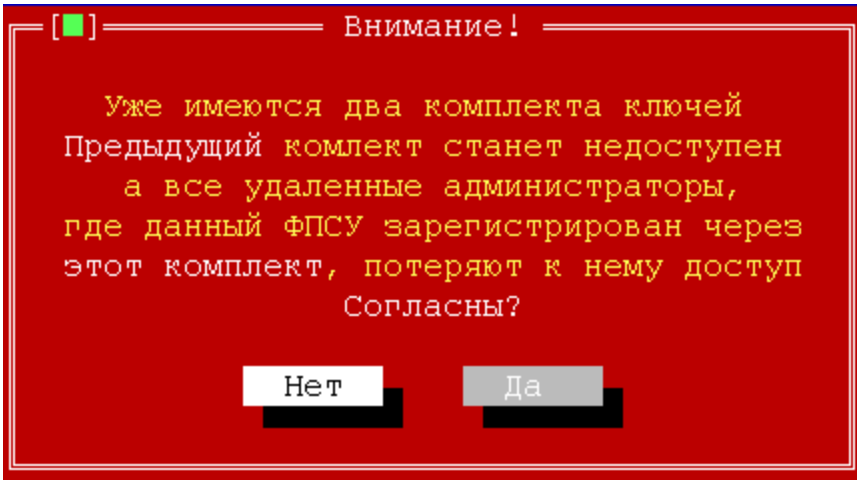


Рисунок 143 - Предупреждение при создании нового ключа аутентификации ФПСУ-IP

8. 6. Параметры «Горячего резерва»

Команда «Параметры «Горячего резерва» меню «Настройка системы» присутствует в интерфейсе в том случае, если в состав ПО ФПСУ-IP входит подсистема «горячего» резервирования. Команда предназначена для:

- активизации режима горячего резервирования работы ФПСУ-IP;
- разовой принудительной синхронизации данных основного и резервного ФПСУ-IP системы горячего резерва;
- взаимной регистрации ФПСУ-IP и его партнера по резервированию.

Рисунок 144 - Команда «Параметры «Горячего резерва»

Запуск команды доступен администраторам класса «*Администратор*» и выше (см. раздел «Общие сведения», табл. 1).

Для функционирования пары ФПСУ-IP в режиме резервирования необходимо соединить кабелем передачи данных их сетевые адаптеры, конфигурированные как порты резервирования (см. раздел «Конфигурация драйверов сетевых адаптеров»). В «разрыв цепи» между локальными подсетями оба ФПСУ-IP обычно подключаются через коммутаторы (switch) или концентраторы (hub).

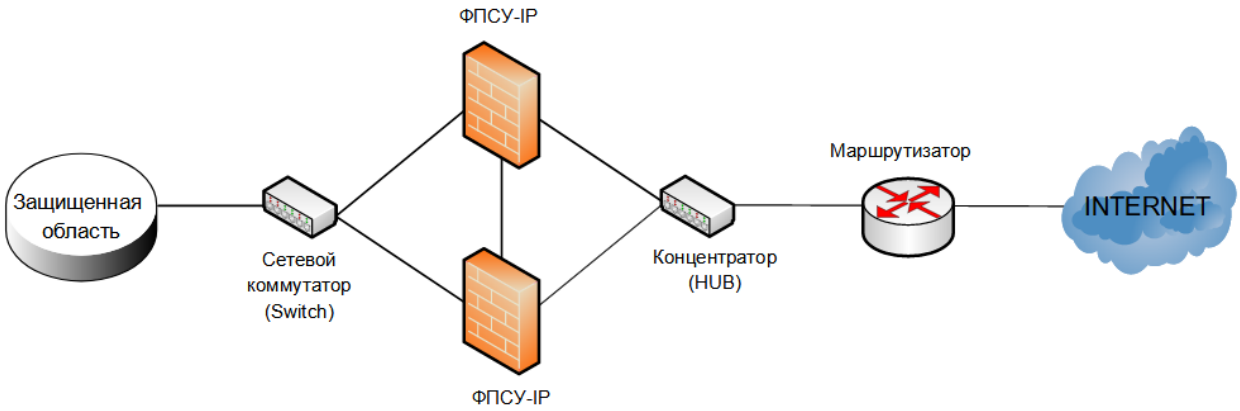


Рисунок 145 - Пример схемы подключения горячего резерва ФПСУ-IP

ВНИМАНИЕ! В конфигурационных установках обоих ФПСУ-IP MAC-адреса сетевых адаптеров с одинаковыми номерами должны совпадать (см. раздел «Конфигурация

драйверов сетевых адаптеров»).

ВНИМАНИЕ! При включении режима «мост» разрешается использовать горячий резерв по основным портам.

Маркер каждого из ФПСУ-IP («основной» или «резервный» в схеме горячего резервирования) устанавливается один раз при инсталляции ПО ФПСУ-IP, а функциональный статус может меняться в процессе работы: каждый из ФПСУ-IP может быть «активным» (осуществлять функции по обработке и передаче данных), в то время как другой («пассивный») работает в режиме ожидания.

В процессе функционирования оба ФПСУ-IP производят периодический опрос работоспособности друг друга. При отсутствии ответа от активного ФПСУ-IP или при получении сообщения об аппаратных неполадках на активном, пассивный ФПСУ-IP забирает управление, становится активным, и начинает работу по обработке и передаче данных. При необходимости, допущенное лицо с правами класса *«Оператор»* и выше может поменять текущий функциональный статус ФПСУ-IP вручную (см. раздел «Окно состояния подсистемы «горячего» резервирования»).

Фактическая работа подсистемы резервирования происходит только тогда, когда оба ФПСУ-IP запущены в режим фильтрации пакетов.

В процессе взаимодействия основной и резервный ФПСУ-IP производят автоматическую синхронизацию следующих рабочих данных:

- модулей программного обеспечения ФПСУ-IP;
- конфигурационной информации, включая ключевые данные смежных ФПСУ-IP и клиентов (то есть всей совокупности параметров, устанавливаемых через опцию меню «Конфигурация ФПСУ»);
- текущего времени ФПСУ-IP;
- ключевых данных удаленных администраторов.

Автоматическая синхронизация производится по последнему произведенному на каком-либо из ФПСУ-IP изменению. При этом ФПСУ-IP, передающий изменения партнеру, автоматически переходит в статус «активный». В случае необходимости администратор класса «*Администратор»* и выше может осуществить принудительную синхронизацию изменений (см. раздел «Принудительная синхронизация данных»).

Часть рабочих данных каждого из ФПСУ-IP остается автономной:

- настройки LAN-адаптеров;
- информация подсистемы регистрации и статистики;
- пароль администратора;

- данные о зарегистрированных на ФПСУ-IP ТМ-идентификаторах (кроме Главного администратора, его ТМ-идентификатор общий для обоих ФПСУ-IP).

Для защиты обменов служебной информацией во время работы подсистемы резервирования между ФПСУ-IP создается VPN-туннель, по которому данные передаются в защищенном виде. Для этого на одном из ФПСУ-IP вырабатывается и выдается на ТМ-идентификатор ключ горячего резерва, который затем должен быть установлен на второй ФПСУ-IP.

8. 6. 1. Настройка ФПСУ-IP на работу с партнером по резервированию

Перед непосредственной настройкой конфигурации ФПСУ-IP на работу с партнером по резервированию, администратору следует проверить, что:

- для настройки выбраны именно те два комплекса ФПСУ-IP, которые предназначены для работы в резерве, основной и резервный (см. предыдущий пункт). Первые 10 символов серийных номеров таких ФПСУ-IP должны совпадать;
- основной и резервный комплексы ФПСУ-IP соединены кабелем передачи данных друг с другом посредством портов, предназначенных для резервирования (см. пункт «Конфигурация драйверов сетевых адаптеров»).

Для настройки работы ФПСУ-IP в режиме «горячего» резервирования:

1. Активизируйте команду «Настройка системы» → «Параметры «Горячего резерва»;
2. Установите флаг «Резервирование активно» при помощи клавиши <Пробел>;
3. Активизируйте команду «Начать работу с ключом». Если ключи не установлены, основной ФПСУ-IP может либо создать ключ горячего резерва и выдать его на ТМ-идентификатор для установки на резервный ФПСУ-IP, либо считать ключ с предъявленного ТМ-идентификатора (если он был ранее выдан на этот ТМ-идентификатор администратором основного ФПСУ-IP) и зарегистрировать его у себя в качестве ключа горячего резерва. Резервный ФПСУ-IP может только считать ключ с предъявленного ТМ-идентификатора.

ВНИМАНИЕ! Выданный на ТМ-идентификатор ключ горячего резерва остается там и после регистрации ключа на резервном ФПСУ-IP и его можно повторно использовать при аварийном восстановлении конфигурации.

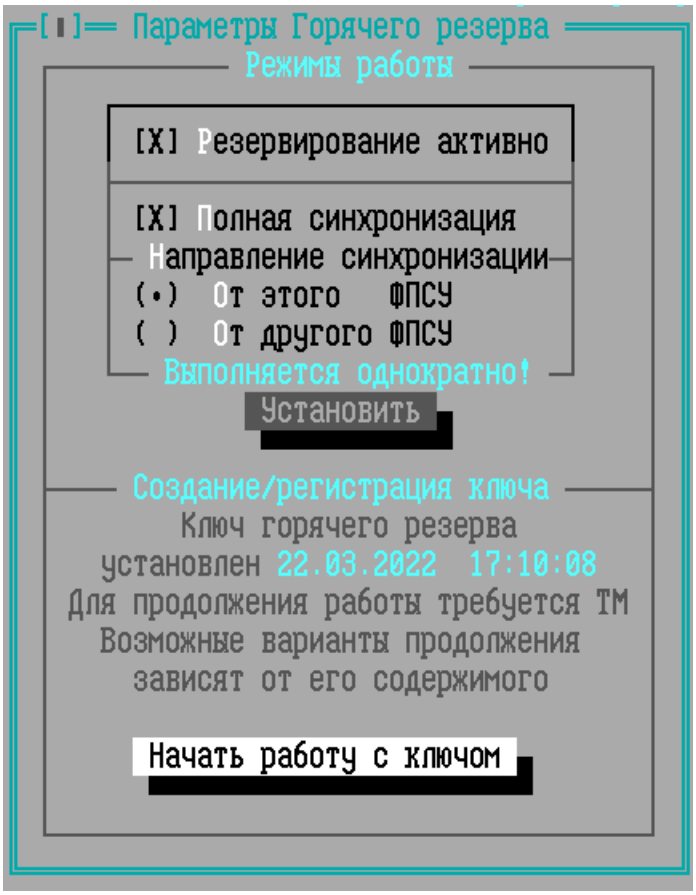


Рисунок 146 - Окно настроек работы горячего резерва

ВНИМАНИЕ! При переходе из технологического режима работы ФПСУ-IP в рабочий (см. пункт «Технологический режим ФПСУ-IP») настройки, описанные в этом пункте, необходимо выполнить повторно ввиду перехода с тестовых на рабочие ключи!

8. 6. 2. Замена ключа горячего резерва

Ключ горячего резерва подлежит замене в ряде случаев: завершение установленного срока действия ключа, утеря или компрометация ТМ-идентификатора с ключом.

Для замены ключа горячего резерва следует выполнить следующие действия (начиная с основного ФПСУ-IP системы горячего резерва!):

1. В окне «Параметры Горячего резерва» основного ФПСУ-IP нажмите кнопку «Начать работу с ключом»:

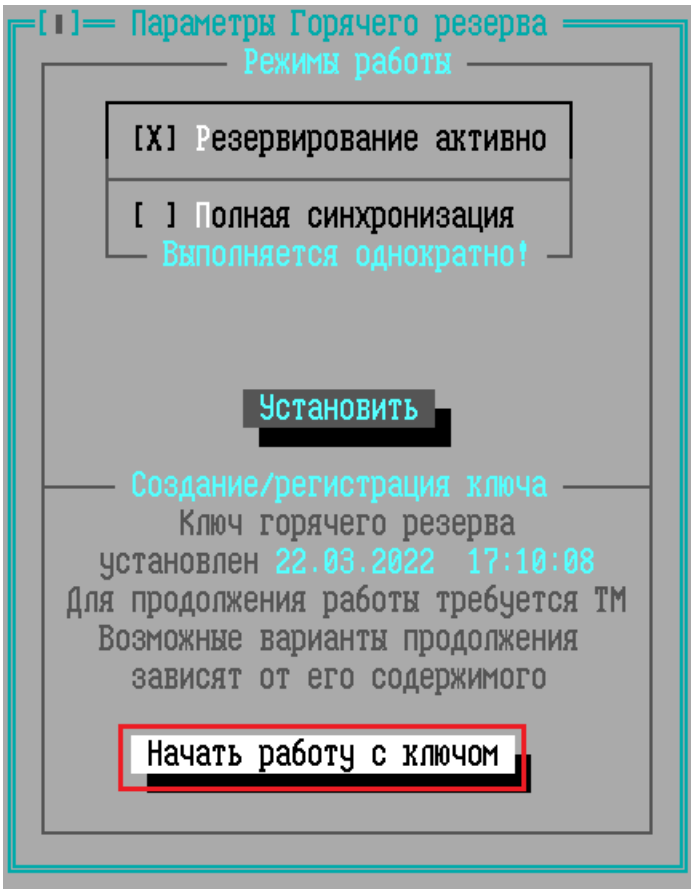


Рисунок 147 - Окно настроек горячего резерва

2. Предъявите предназначенный для ключа горячего резерва ТМ-идентификатор по запросу системы.

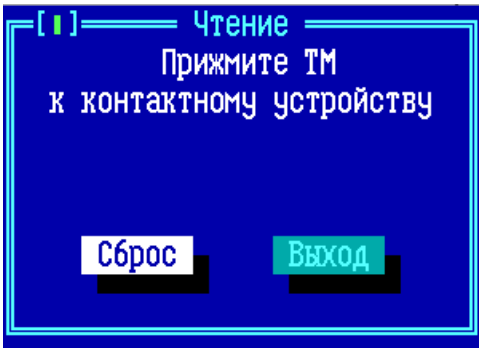


Рисунок 148 - Требование предъявить ТМ-идентификатор для ключа горячего резерва

На экран будет выдано сообщение об уже имеющемся ключе горячего резерва, записанном на ТМ-идентификатор. Для смены ключа горячего резерва требуется нажать кнопку «Да»;

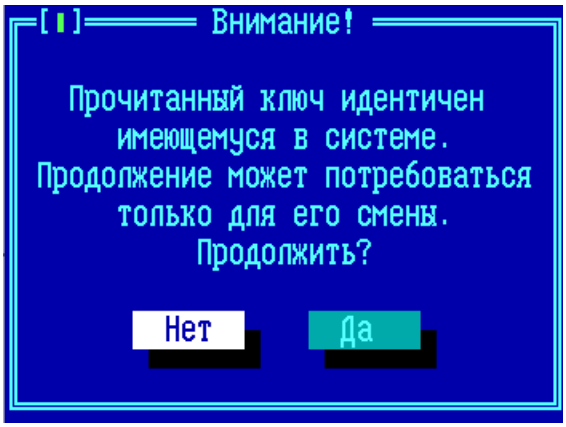


Рисунок 149 - Сообщение об имеющемся ключе горячего резерва

3. Выберите и выполните команду «Создать и выдать новый ключ»:

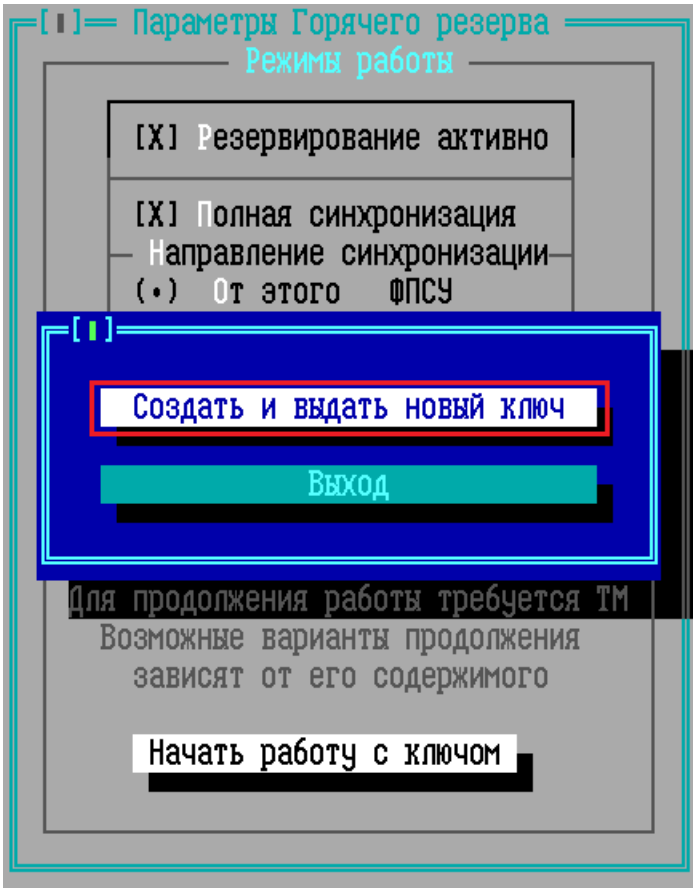


Рисунок 150 - Команда создания нового ключа горячего резерва

4. Прочитайте появившееся предупреждение и подтвердите выполнение команды создания нового ключа, нажмите кнопку «Да»;

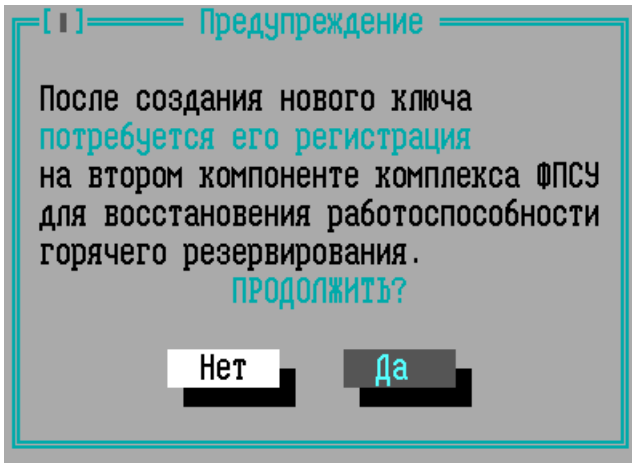


Рисунок 151 - Подтверждение выполнения команды

5. Ключ горячего резерва будет создан и начнется его запись в предъявленный ТМ-идентификатор. В случае успешной записи ключа горячего резерва появится служебное предупреждение:

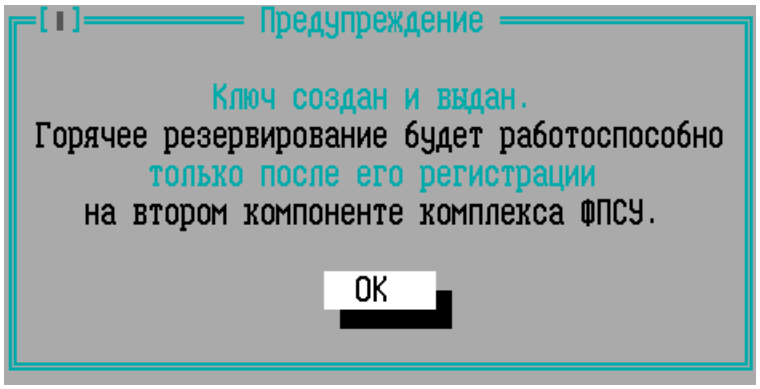


Рисунок 152 - Новый ключ горячего резерва создан и выдан на ТМ

6. Перейдите к конфигурированию резервного ФПСУ-IP. В окне «Параметры Горячего резерва» резервного ФПСУ-IP нажмите кнопку «Начать работу с ключом»;

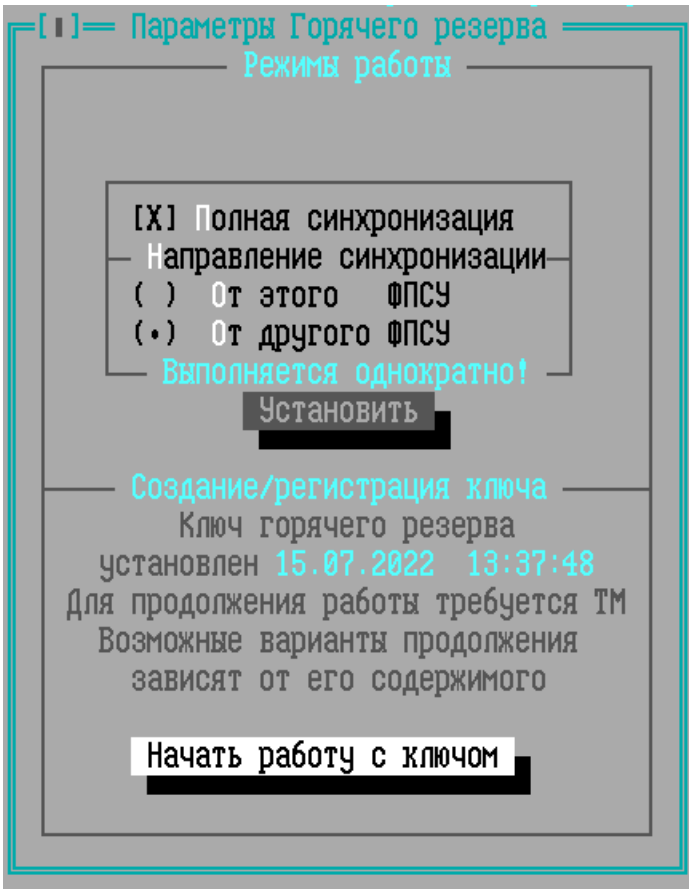


Рисунок 153 - Окно настроек горячего резерва на резервном ФПСУ-IP

7. Предъявите резервному ФПСУ-IP ТМ-идентификатор с новым ключом горячего резерва по запросу системы;

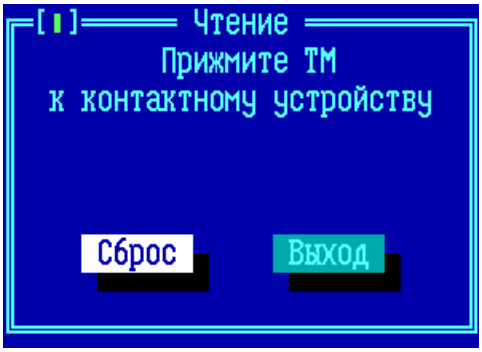


Рисунок 154 - Требование предъявить ТМ-идентификатор с новым ключом горячего резерва

8. Зарегистрировать считанный с ТМ-идентификатора ключ горячего резерва на резервном ФПСУ-IP.

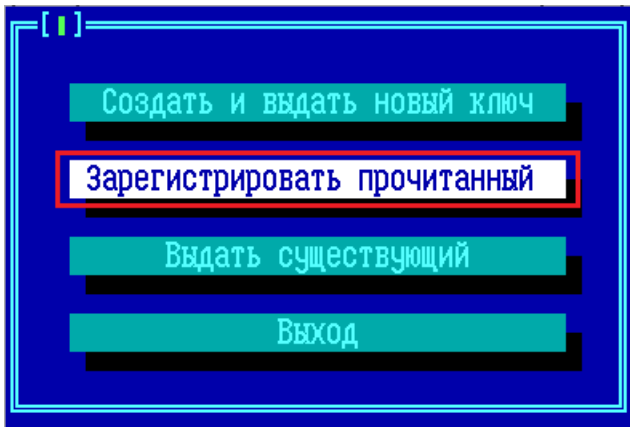


Рисунок 155 - Команда регистрации нового ключа горячего резерва на резервном ФПСУ

9. Процедура завершена. Ключ горячего резерва заменен на обоих ФПСУ-IP системы горячего резервирования.

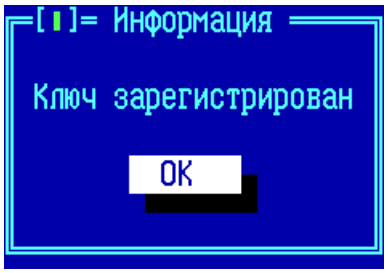


Рисунок 156 - Окончание регистрации нового ключа горячего резерва на резервном ФПСУ

После выполнения такой процедуры замены ключа горячего резерва на новый, выданный ранее ключ горячего резерва становится нерабочим: ФПСУ-IP не смогут построить туннели горячего резервирования на старом ключе.

Если ТМ-идентификатор с ключом горячего резерва был скомпрометирован, а выполнить процедуру замены ключа горячего резерва невозможно по тем или иным причинам, администратору следует прекратив работу ФПСУ-IP на скомпрометированом ключе, сняв флаг «Резервирование активно» и сохранив конфигурацию с отключенной системой горячего резервирования.

8. 6. 3. Принудительная синхронизация данных

Принудительную однократную синхронизацию данных основного и резервного ФПСУ-IP рекомендуется производить в следующих случаях:

1. При установке и настройке ПО одного из ФПСУ-IP с целью сокращения времени работы и исключения ошибок конфигурирования;

2. При восстановлении работы одного из ФПСУ-IP после аварий и сбоев оборудования;
3. Если при внесении изменений на один из ФПСУ-IP администратор не был уверен, что за время его работы никто не редактировал рабочие данные активного комплекса.

В двух первых перечисленных случаях на настраиваемый ФПСУ-IP достаточно инсталлировать ПО ФПСУ-IP, содержащее подсистему резервирования, установить параметры резервирования (см. предыдущий раздел, «Настройка ФПСУ-IP на работу с партнером по резервированию»), конфигурировать его LAN-порты и ввести номера и IP-адреса ФПСУ-портов, после чего дать указание принудительной синхронизации от работающего ФПСУ-IP.

Для выполнения однократной синхронизации:

1. Выполните команду главного меню «*Настройка системы*»;
2. Выполните команду меню настройки системы «*Параметры «Горячего резерва»*;
3. Выделите курсором флаг «*Полная синхронизация*» и включите его при помощи клавиши <*Пробел*>;
4. В открывшемся поле укажите направление синхронизации: если необходимо передать свои данные от конфигурируемого ФПСУ-IP, отметьте при помощи клавиши <*Пробел*> команду «*От этого ФПСУ*», если на ФПСУ-IP устанавливаются данные партнера, отметьте «*От другого ФПСУ*»;
5. Активизируйте команду «*Установить*»;
6. Выйдите из опции настройки в главное меню ФПСУ-IP и запустите подсистему фильтрации.

Убедитесь в том, что обмен служебной информацией между ФПСУ-IP происходит нормально, то есть статус соединения между ФПСУ-IP горячего резерва отображается как «*Готов*» (см. подраздел «Окно состояния подсистемы «горячего» резервирования»).

Синхронизация данных (в частности, тех изменений, которые могли быть сделаны после установления флага однократной синхронизации и до запуска подсистемы фильтрации) будет произведена после взаимного обмена между основным и резервным ФПСУ-IP. После этого флаг в поле «*Полная синхронизация*» будет снят.

8. 6. 4. Параметры проверки линий связи для портов ФПСУ-IP

Одним из параметров работоспособности ФПСУ-IP в системе горячего резервирования является успешная проверка указанных администратором ФПСУ-IP линий связи (по умолчанию отключена). Если проверка включена, то она начинает выполняться

через 15 секунд после запуска ФПСУ-IP в рабочий режим или перехода из пассивного в активный.

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».

8. 6. 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»:

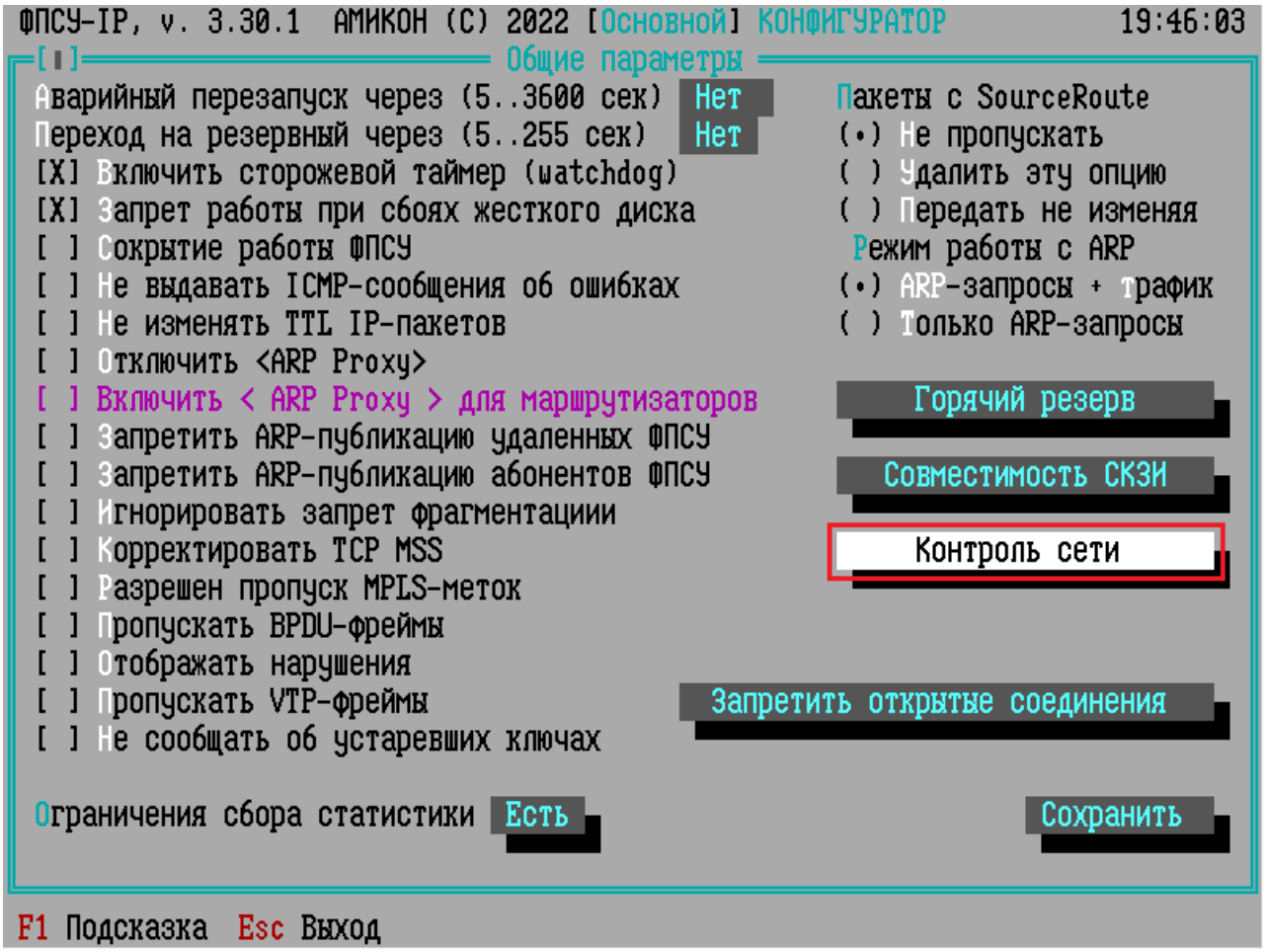


Рисунок 157 - Общие параметры ФПСУ-IP

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».

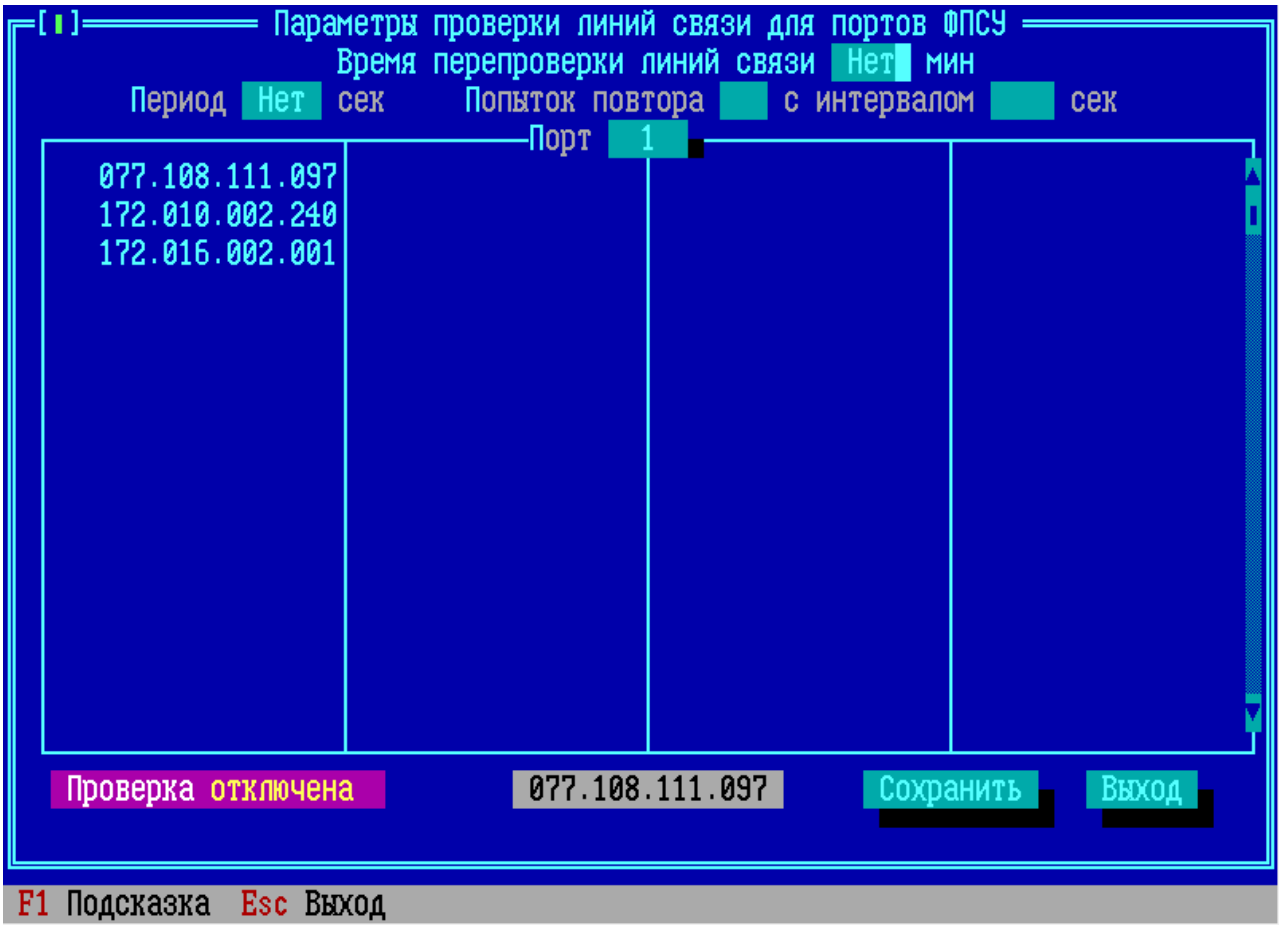


Рисунок 158 - Окно настройки параметров контроля связи

Для включения проверки контроля сети следует установить параметры проверки и выбрать из списка абонентов типа «хост» тех, доступность которых будет проверяться. На каждом порту ФПСУ-IP может быть выбрано до 8 абонентов для контроля сети.

Параметры, которые необходимо установить:

Время перепроверки линии связи – время в минутах (от 1-й до 255-и), по прошествии которого **ставший активным ФПСУ-IP** запустит ещё одну серию проверок доступности контролируемых IP-адресов, то есть первую попытку проверки и все повторные попытки в указанном количестве.

Этот же параметр, **время перепроверки линии связи** (умноженный на пять при первом случае передачи управления по причине неудачной проверки линии связи), указывает время, в течении которого отдавший управление комплекс горячего резерва не будет принимать управление от партнера;

Период – временной интервал отправки эхо-запросов в заданные администратором IP-адреса. Устанавливается в пределах от 3-х до 255-и секунд. ФПСУ-IP ожидает заданный

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

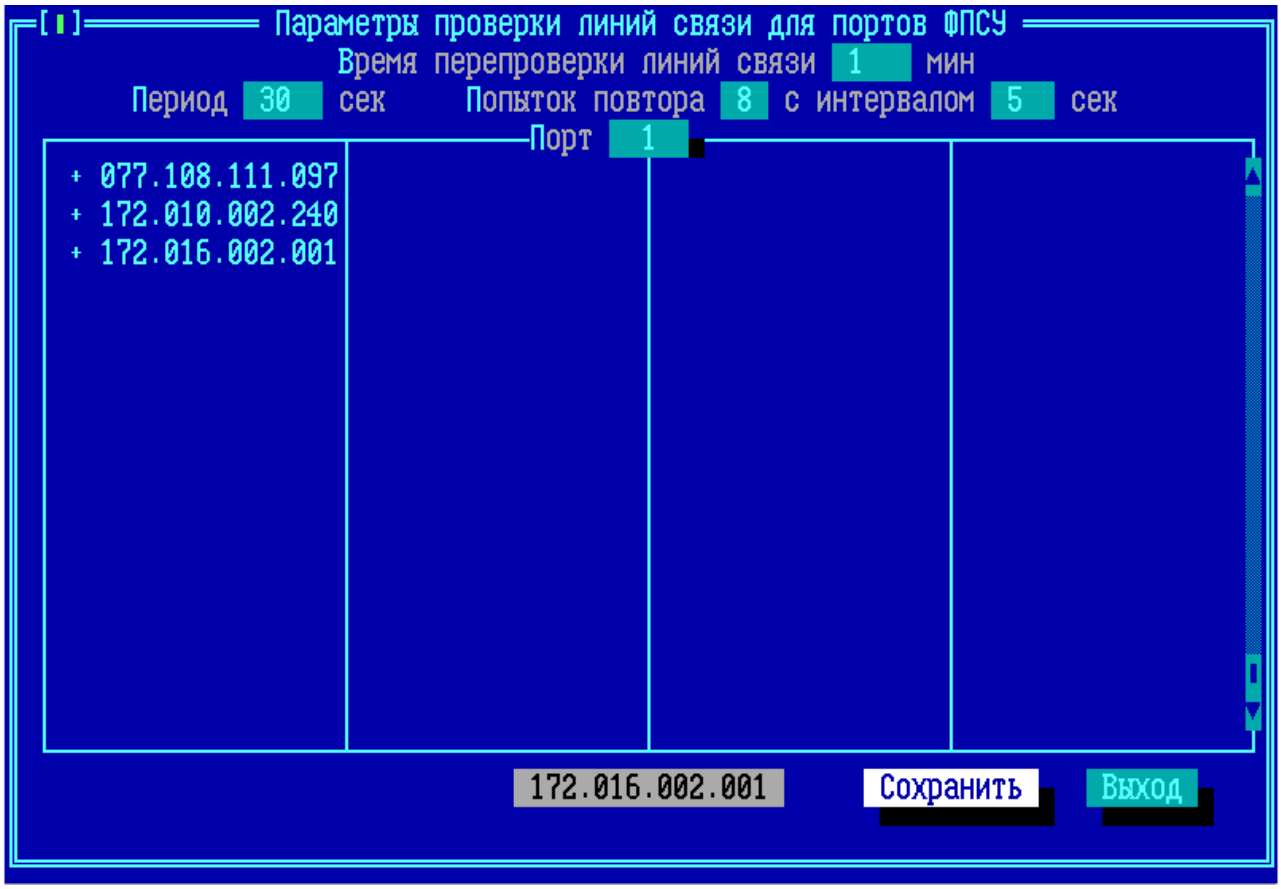
Попыток повтора – количество повторных попыток отправки эхо-запросов, которые будет выполнять активный ФПСУ-IP, в случае если ни от одного из IP-адресов контролируемого списка не пришел ответ. Только после исчерпания попыток повтора активный ФПСУ-IP передаст управление партнеру по горячему резерву. Количество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

8. 6. 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:


Параметры проверки линий связи для портов ФПСУ
Время перепроверки линий связи 1 мин
Период 30 сек
Попыток повтора 8 с интервалом 5 сек
Порт 1
+ 077.108.111.097
+ 172.010.002.240
+ 172.016.002.001
172.016.002.001
Сохранить
Выход

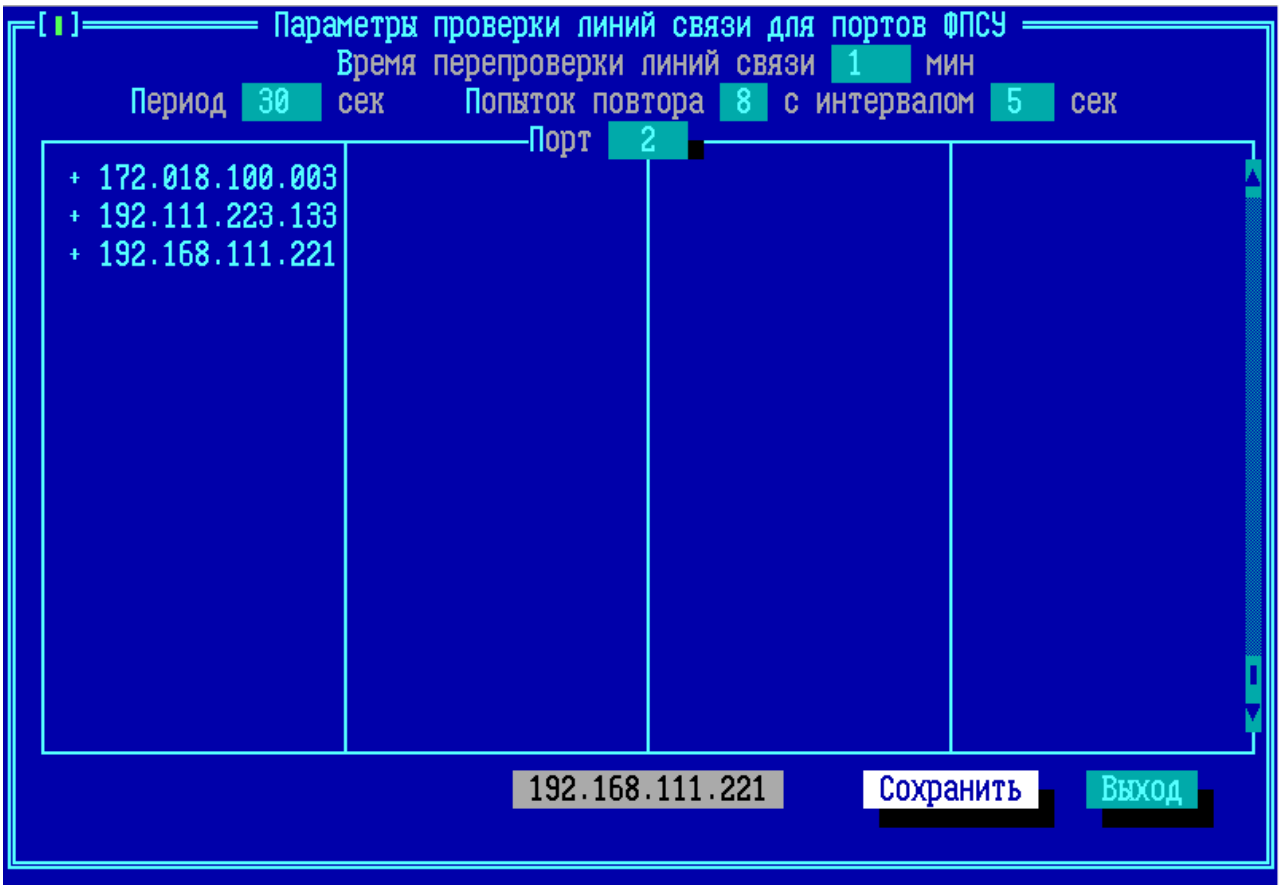


Рисунок 159 - Пример настройки системы проверки линий связи

Активный комплекс ФПСУ-IP системы горячего резерва (далее **ФПСУ№1**) каждые **30 секунд** будет направлять эхо-запросы в адрес хостов первого порта **077.108.111.097**, **172.010.002.240**, **172.016.002.001**, и эхо-запросы в адрес хостов второго порта **172.018.100.003**, **198.111.223.133**, **192.168.111.211**. Проверки доступности хостов каждого порта проводятся независимо друг от друга.

Если все хосты, указанные на первом порту в качестве отслеживаемых, не отвечают на эхо-запросы (порт «замолчал»), **ФПСУ№1** начинает выполнять **8 повторных рассылок** эхо-запросов на хосты первого порта, каждая с интервалом в **5 секунд**. То же самое происходит, если перестали отвечать на запросы отслеживаемые хосты второго порта: **ФПСУ№1** начинает выполнять **8 повторных рассылок** эхо-запросов на хосты второго порта, каждая с интервалом в **5 секунд**.

Если в результате **8 повторных рассылок** не был получен эхо-ответ от хотя бы одного хоста «замолчавшего» порта, **ФПСУ№1** отдает управление другому комплексу горячего резерва (далее **ФПСУ№2**), становясь пассивным и устанавливая **5-минутный** (1 минута параметра **время перепроверки линий связи** умножается на 5, поскольку это первая передача управления по причине неуспешной проверки линии связи) таймер, запрещающий

принимать активное управление обратно. В течении работы таймера состояние **ФПСУ№1** в системе горячего резервирования устанавливается как «*Работоспособность: частичная*» с дополнительной строкой сообщения «*нет канала связи*», что можно отследить на экране отображения состояния горячего резерва.

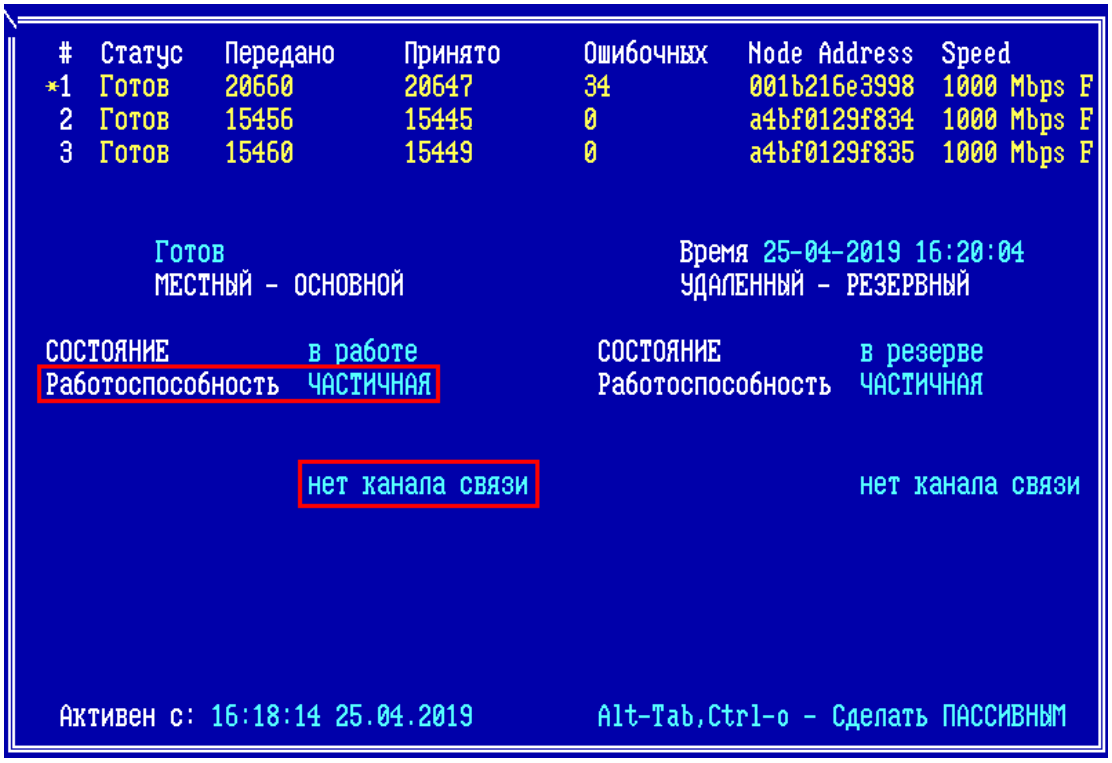


Рисунок 160 - Проверка линии связи неуспешна

Через 15 секунд (постоянный параметр) после становления активным, **ФПСУ№2** начинает проверку доступности хостов первого порта **077.108.111.097**, **172.010.002.240, 172.016.002.001** и проверку доступности хостов второго порта **172.018.100.003**, **198.111.223.133, 192.168.111.211**.

Если ответ с проверяемых хостов «замолчавшего» порта не был получен в результате первой проверки или в результате **8 повторных проверок** с интервалом в **5 секунд**, то **ФПСУ№2** устанавливает себе состояние «*Работоспособность: частичная*», «*нет канала связи*» и запрашивает **ФПСУ№1** о возможности передать управление комплексом. Если на **ФПСУ№1** все ещё действует таймер запрета передачи управления, то **ФПСУ№2**. остается активным комплексом и ждет через **1 минуту** (параметр **время перепроверки линий связи**) перед запуском следующей серии проверок доступности хостов.

После каждой неуспешной серии проверок **ФПСУ№2** запрашивает **ФПСУ№1** о возможности передать управление комплексом. Если во время такого запроса таймер запрета передачи управления на **ФПСУ№1** уже закончился, то **ФПСУ№2** передает управление на

ФПСУ№1 и устанавливает собственный таймер запрета передачи управления, равный **5 минутам** (1 минута параметра **время перепроверки линий связи** умножается на 5, поскольку это первая передача управления по причине неуспешной проверки линии связи).

ФПСУ№1 становится активным и через 15 секунд (постоянный параметр) запускает первую серию проверок доступности хостов, и так же будет пытаться передать управление **ФПСУ№2** в случае неуспешного результата проверки. Единственным отличием будет длительность таймера запрета передачи управления, который будет установлен в 1 минуту (1 минута параметра **время перепроверки линий связи** без умножения на первичный коэффициент 5).

Такая схема передачи управления и поочередной проверки доступности хостов будет повторяться до тех пор, пока **ФПСУ№1** или **ФПСУ№2** не получит хотя бы один эхо-ответ с хостов «замолчавшего» порта.

8. 7. Настройки СКЗИ

Команда «Настройки СКЗИ» меню «Настройка системы» предназначена для перехода в интерфейс отключения подсистемы автозапуска, повторной инициализации программно-клавиатурного датчика случайных чисел, управления сроками действия ключевых данных ФПСУ-IP, удаления СКЗИ с ПЗУ ФПСУ-IP.

Рисунок 161 - Меню настройки системы ФПСУ-IP

При выполнении команды «Настройки СКЗИ» происходит переход в меню «Настройки СКЗИ», содержащее следующие пункты:

Рисунок 162 - Меню настройки СКЗИ ФПСУ-IP

- «Отключение автозапуска» – переход в окно регистрации ТМ-идентификаторов для отключения подсистемы автозапуска ФПСУ-IP (см. пункт «Отключение автозапуска»);
- «Переинициализация ПДСЧ» – команда запуска процедуры повторной инициализации программно-клавиатурного датчика случайных чисел (см. пункт «Переинициализация ПДСЧ»);
- «Установка времени действия ключей» – переход в окно управления сроками действия ключевых данных ФПСУ-IP (см. пункт «Установка времени действия ключей»);
- «Удаление СКЗИ» – запуск процедуры удаления программных модулей ФПСУ-IP и форматирования внутреннего носителя (см. пункт «Удаление СКЗИ ФПСУ-IP»).

Возвращение в меню «Настройка системы» осуществляется по клавише <*Esc*>.

8. 7. 1. Отключение автозапуска

Команда «Отключение Автозапуска» предназначена для отключения подсистемы автозапуска, если она была ранее задействована локальным администратором. Выполнение команды при включенной подсистеме автозапуска не требует авторизации и может быть выполнена любым пользователем.

При выполнении команды осуществляется переход в окно регистрации ТМ-идентификаторов, где система предлагает пользователю подтвердить или отклонить отключение подсистемы автозапуска:

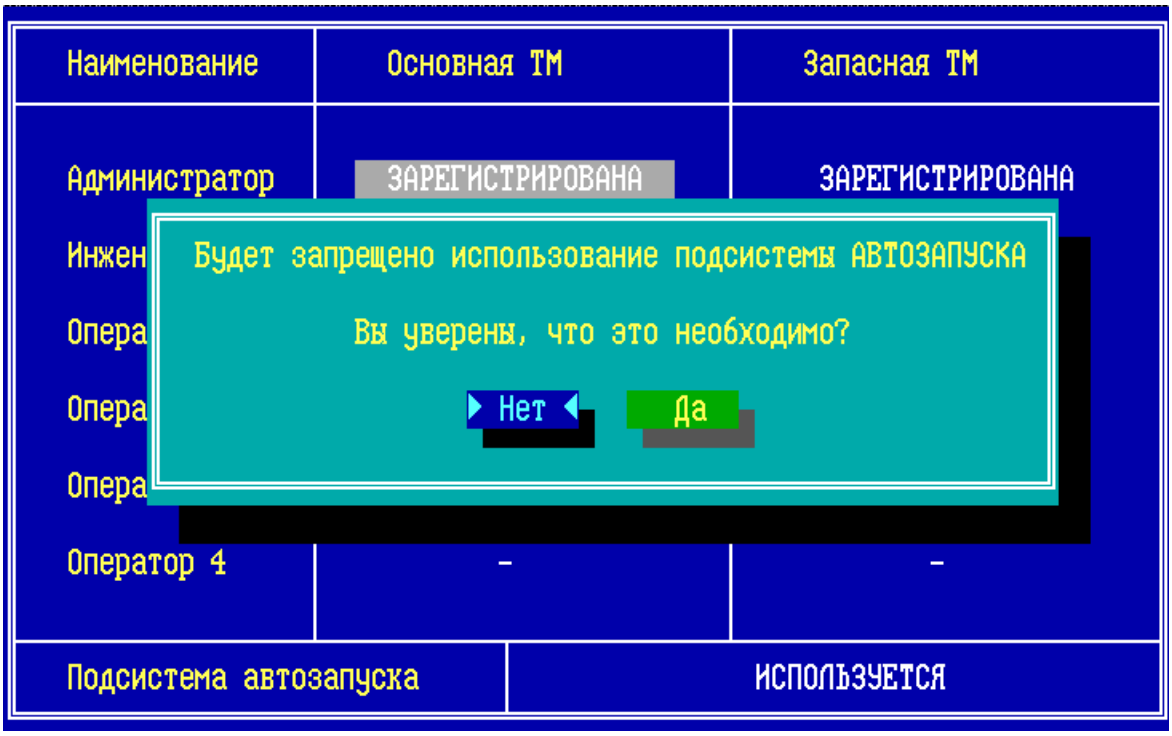


Рисунок 163 - Подтверждение отключения подсистемы автозапуска

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

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

8. 7. 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 164 - Команда повторной инициализации ДСЧ

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

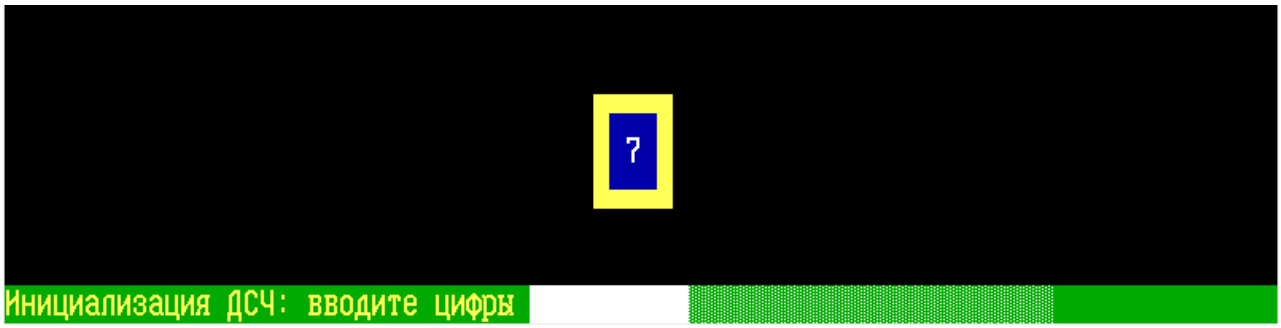


Рисунок 165 - Программно-клавиатурный датчик случайных чисел

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».

8. 7. 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 166 - Команда «Установка времени действия ключей»

При выполнении команды будет предложен выбор типа ключа, для которого будут выполнены настройки сроков действия. Настройки для каждого типа ключа выполняются и сохраняются отдельно:

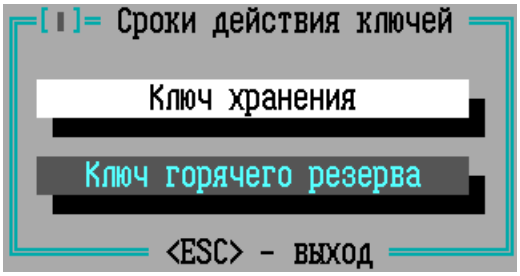


Рисунок 167 - Выбор типа ключа

При выборе пункта меню «Ключ хранения» или «Ключ горячего резерва» открывается окно настроек сроков действия выбранного ключа, в котором указывается дата создания ключа и текущие настройки.

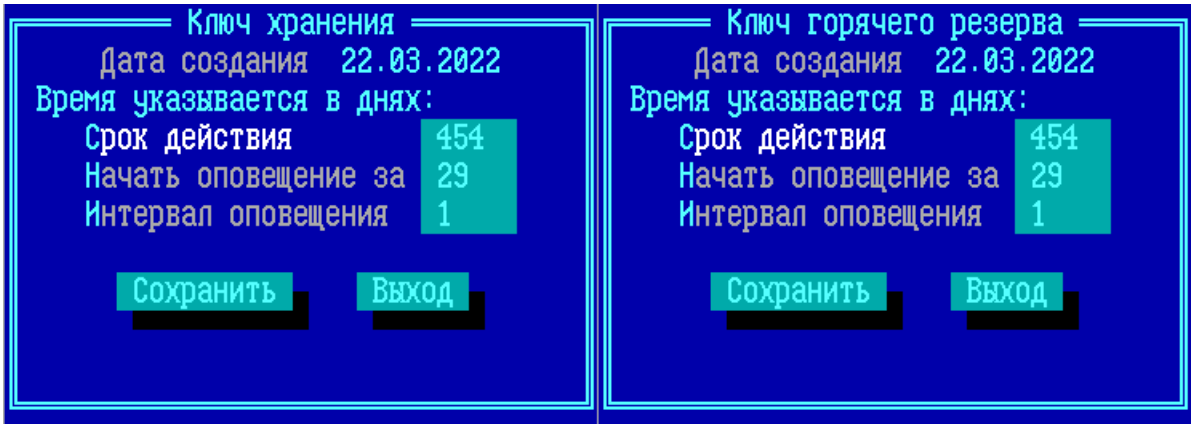


Рисунок 168 - Настройка сроков действия выбранного ключа

Параметры, доступные администратору для изменения:

Срок действия – число, обозначающее количество дней с даты создания, в течение которого ключ будет считаться рабочим;

Начать оповещение за – число, обозначающее количество дней до срока прекращения действия ключа, с которого администратору ФПСУ-IP будет при запуске ФПСУ-IP выводится сообщение о приближающемся окончании срока действия ключа;

Интервал оповещения – число от 1 до 14, обозначающее количество дней, через которое оповещение о приближающемся сроке прекращение действия ключа будет повторяться.

9. Порты ФПСУ

Команда «Порты ФПСУ» меню конфигурации предназначена для задания основных правил фильтрации и маршрутизации абонентского трафика, и указания способа последующей передачи данных через ФПСУ-IP.

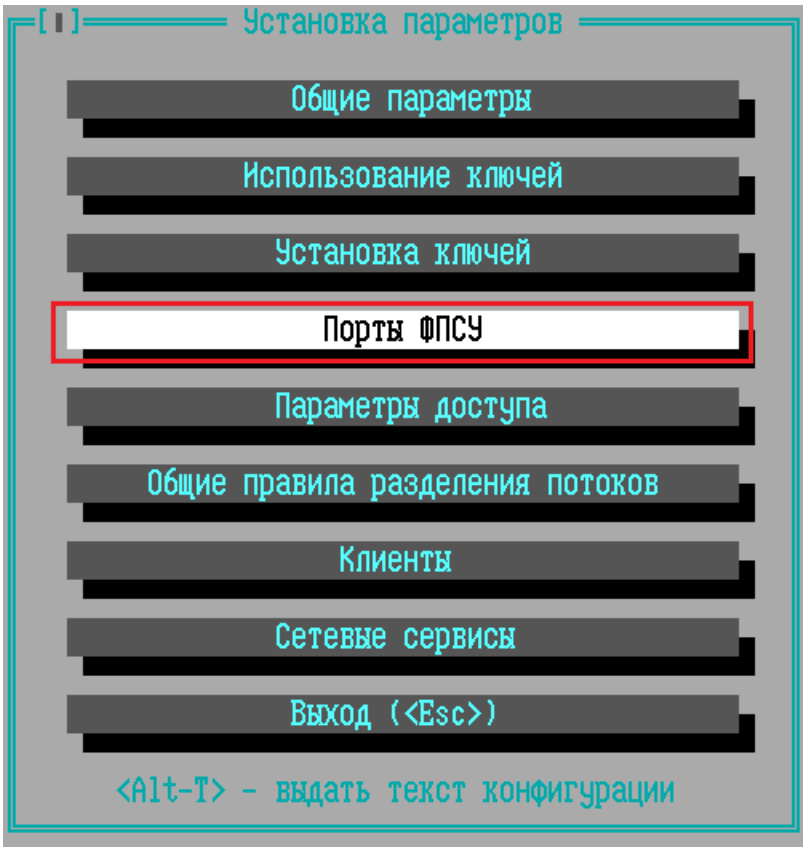


Рисунок 169 - Меню конфигурации ФПСУ-IP

Статическая маршрутизация

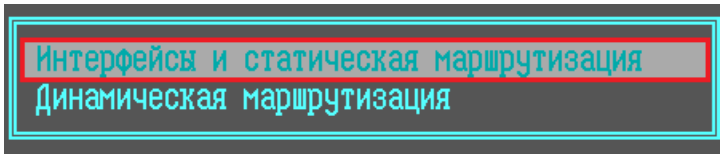


Рисунок 170 - Подменю команды «Порты ФПСУ»

Для каждого рабочего порта ФПСУ-IP необходимо создать список абонентов, которым разрешается подключаться к ФПСУ-IP со стороны этого порта, указать ФПСУ-IP, с которыми будут устанавливаться VPN-туннели, маршрутизаторы, через которые абоненты будут доступны, и установить правила их работы.

ФПСУ-IP работает по принципу **«все, что явно не разрешено – запрещено»**, поэтому если на каком-либо из портов не указано ни одного абонента, то передача данных

через ФПСУ-IP производиться не будет.

При выполнении команды появится окно «Порты ФПСУ», отображающее общие установки для каждого из рабочих портов ФПСУ-IP.

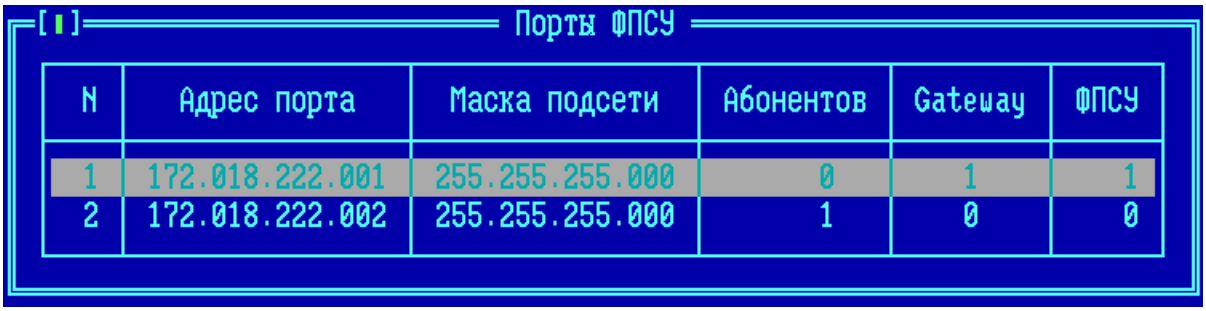


Рисунок 171 - Порты ФПСУ-IP

Необходимо строго следить за тем, чтобы номер описываемого порта в списке был тем же, что и номер соответствующего ему сетевого адаптера, установленный при конфигурировании последнего (см. раздел «Конфигурация драйверов сетевых адаптеров») – это указание для ФПСУ-IP, какой адаптер связан с каким сегментом IP-сети.

При первом запуске подсистемы конфигурирования таблица будет пустой. Чтобы осуществить необходимые установки (или отредактировать существующие), выберите строку с нужным номером порта и нажмите *<Пробел>*, после чего на экран будет выдано диалоговое окно настроек порта, в котором указываются сетевые параметры абонентов, других ФПСУ и маршрутизаторов.

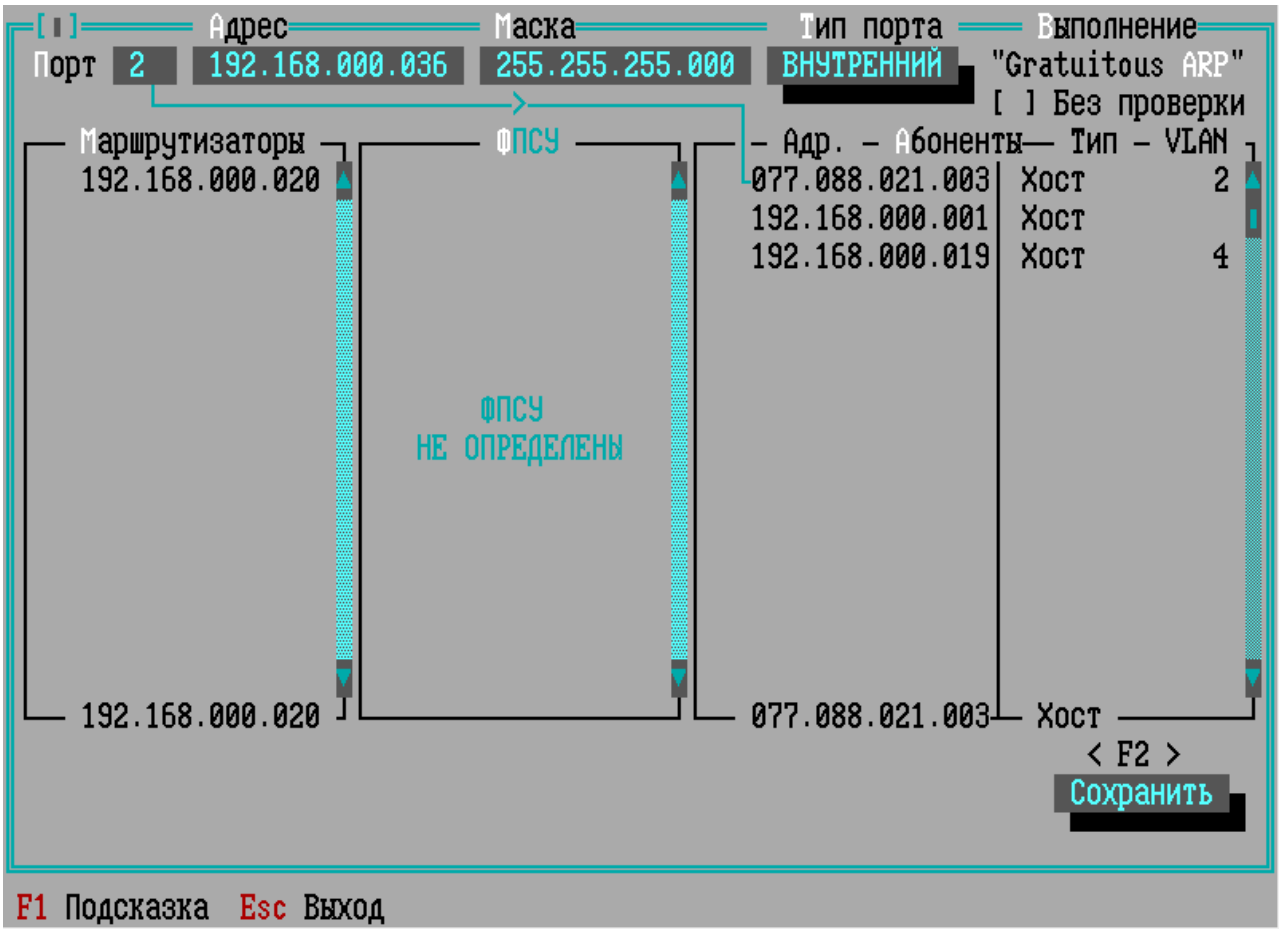


Рисунок 172 - Установка параметров порта

Передвижение по одиночным полям окна осуществляется клавишами <↓>, <↑>, <*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».

Маска подсети — IP-маска в представлении «dotted-decimal» подсети со стороны данного порта. Маску подсети рекомендуется устанавливать в соответствии с топологией локальной подсети. Маска подсети должна иметь формат, соответствующий стандарту IP-подсетей.

Введите значение рассчитанной маски непосредственно или выделите поле ввода и нажмите <*Пробел*>, после чего введите в появившемся окне число необходимых значащих разрядов (от 8 до 30), в таком случае ФПСУ-IP рассчитает значение маски автоматически.

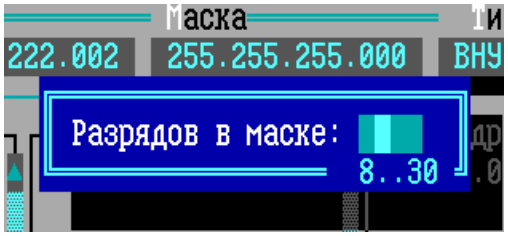


Рисунок 173 - Ввод числа необходимых разрядов

Примечание. Оба порта ФПСУ-IP, и 1, и 2, могут иметь один и тот же IP-адрес в одной и той же подсети, в этом случае ни одному порту ФПСУ-IP не получится назначить DHCP-Relay!

Тип порта — указатель на значимость порта по отношению к режиму работы *«Запрет открытых соединений»* (см. пункт «Общие параметры конфигурации ФПСУ-IP»). Внутренний порт логически обозначает сетевой интерфейс, к которому подключается защищаемая локальная сеть, к внешнему порту подключается открытая (не защищённая) сеть передачи данных, например, Internet/Intranet. При включенном режиме *«Запрет открытых соединений»* автоматически не допускаются открытые (без шифрования) соединения абонентов внутреннего порта с абонентами внешнего порта ФПСУ-IP. Если оба порта ФПСУ-IP помечены как «Внутренние», то открытые соединения абонентов через ФПСУ-IP допускаются.

По умолчанию все порты помечены как «Внутренние». Перевод порта из внешнего во внутренний и наоборот доступен только локальному администратору. Локальному администратору для каждого порта ФПСУ-IP следует:

- определить согласно политике безопасности организации: является порт внутренним или внешним;
- установить значение поля «Тип порта» в соответствующее значение.

«Gratuitous ARP». Без проверки — способ обработки принятого «Gratuitous ARP» запроса/ответа. При снятом флаге ФПСУ-IP через 0,5 секунд после получения запроса начнет проверять доступность ранее работоспособной сетевой станции в течении 4 секунд и только при неудаче начнет широковещательный запрос этого MAC-адреса в локальной сети. При

установленном флаге ФПСУ-IP разрешено сразу изменить значение MAC-адреса в таблице ARP.

9. 1. Описание VLAN порта ФПСУ-IP

Логический порт ФПСУ-IP может принимать участие в построении VLAN (IEEE 802.1Q). Один порт может быть участником 4093 VLAN (номера от 2 до 4094). По умолчанию, подсистема VLAN на ФПСУ-IP не сконфигурирована, и указанный в поле «Адрес» IP-адрес порта не участвует в VLAN.

Переход к интерфейсу настройки используемых VLAN на порту ФПСУ-IP осуществляется нажатием клавиши <*Пробел*>, при установленном курсоре на поле IP-адреса порта, «Адрес».

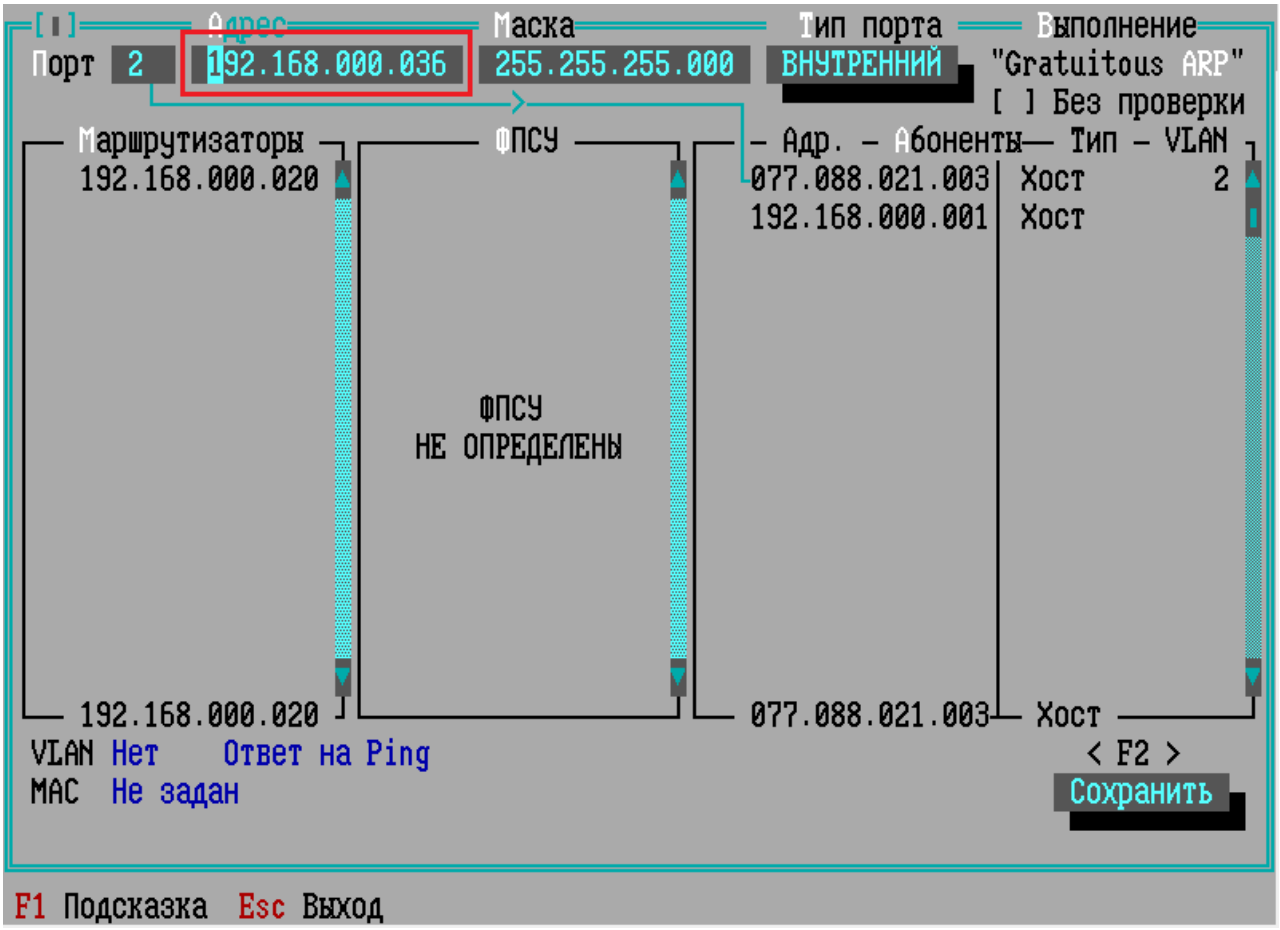


Рисунок 174 - Порт ФПСУ-IP

В открывшемся окне находится список VLAN, в которых участвует данный порт ФПСУ-IP (список по умолчанию пустой). Для добавления описателя VLAN следует нажать клавишу <*Ins*>, и в открывшемся окне «Добавить» указать требуемые параметры:

- ***VLAN*** — идентификатор описываемого VLAN. Указывает, какому VLAN 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.

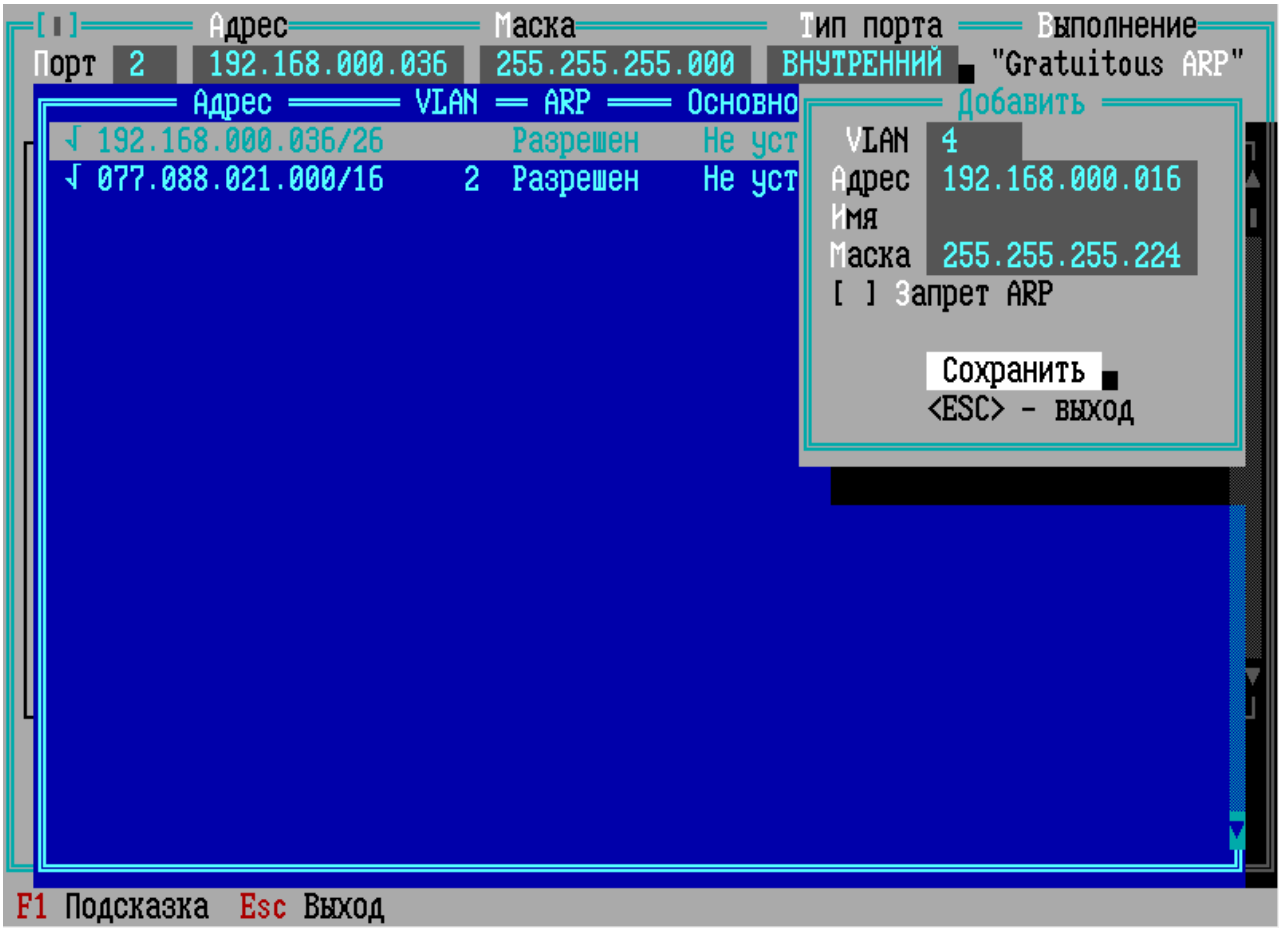


Рисунок 175 - Настройка VLAN на порту ФПСУ-IP

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*>.

9. 2. Описание параметров используемых маршрутизаторов

Поле ***Маршрутизаторы*** окна портов предназначено для ведения на ФПСУ-IP описателей маршрутизаторов, через которые могут быть доступны абоненты или другие ФПСУ-IP со стороны данного порта.

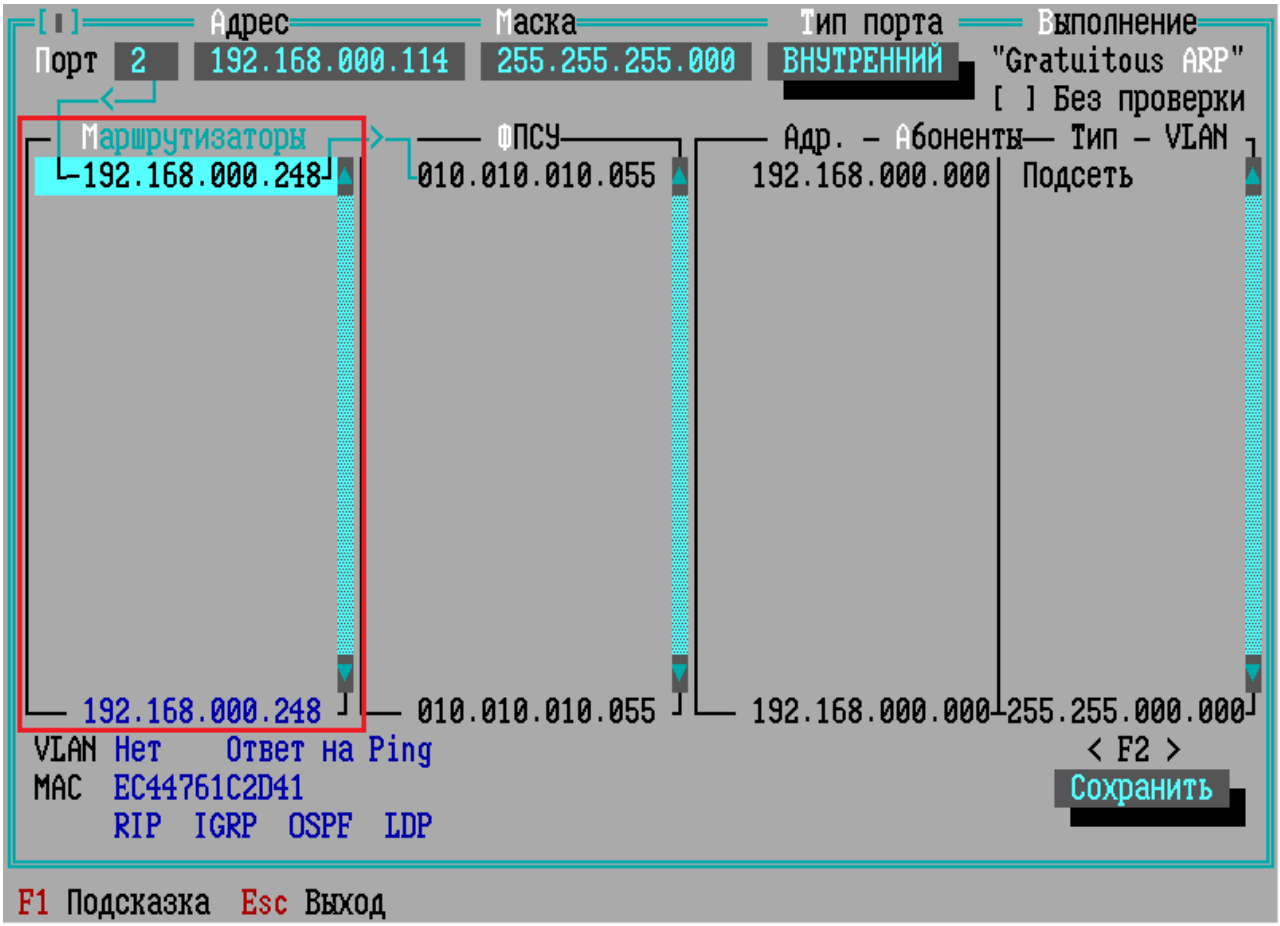


Рисунок 176 - Маршрутизаторы порта ФПСУ-IP

Описатели маршрутизаторов **обязательно** создавать на порту в следующих случаях:

- если они являются пограничными (то есть расположены между описываемым портом ФПСУ-IP и общей сетью) и внесены в конфигурацию TCP/IP стека каких-либо рабочих станций защищаемой области (в противном случае может потребоваться переконфигурирование соответствующих параметров рабочих станций и указание на рабочих станциях в качестве шлюза адреса внутреннего порта ФПСУ-IP);
- если необходимо пропускать через сообщения протоколов маршрутизации, исходящих от маршрутизаторов, находящихся со стороны разных портов ФПСУ-IP;
- если ФПСУ-IP разрешено принимать от данных маршрутизаторов ICMP-сообщения

переадресации (Redirect) в свой адрес или адреса абонентов защищаемой области;

- если эти маршрутизаторы могут быть использованы для передачи данных при получении внешним портом ФПСУ-IP ICMP-сообщений переадресации (Redirect) от уполномоченных маршрутизаторов;
- если рабочие станции защищаемых областей будут осуществлять управление этими маршрутизаторами (только для ФПСУ-IP с более ранними версиями программного обеспечения, чем 3.0, см. раздел «DHCP-Relay»).

Для введения нового описателя выделите заголовок «*Маршрутизаторы*» и нажмите клавишу <*Ins*>, а для редактирования существующего адреса отметьте его и нажмите <*Пробел*>. В открывшемся окне укажите:

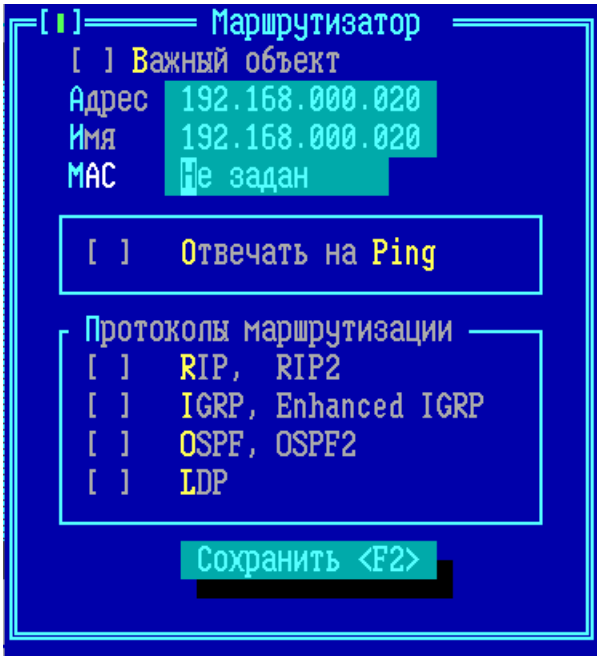


Рисунок 177 - Параметры маршрутизатора

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

Адрес – основной IP-адрес порта маршрутизатора, связанного с описываемым портом ФПСУ-IP;

Имя – название маршрутизатора, которое будет отображаться в списке;

MAC – аппаратный адрес порта маршрутизатора, связанного с ФПСУ-IP.

Отвечать на Ping - указание для ФПСУ-IP: отвечать на ICMP (ECHO) запросы,

направленные от описываемого маршрутизатора в IP-адреса портов конфигурируемого ФПСУ-IP. Отметка (разрешение отвечать на запросы) производится по нажатию клавиши <*Пробел*>. ВНИМАНИЕ! ФПСУ-IP отвечает только на те ICMP (ECHO) запросы, которые поступают одним IP-пакетом (т.е. не были фрагментированы в процессе доставки). Это означает, что размер пакета, на который 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.

Протоколы маршрутизации - протоколы маршрутизации, которые описываемый маршрутизатор может использовать для обменов данными с маршрутизаторами, находящимися со стороны противоположного порта ФПСУ-IP.

Используемый маршрутизаторами протокол (протоколы) необходимо отметить клавишей <*Пробел*>, при этом в квадратных скобках слева от него появится знак [X], свидетельствующий о разрешении обменов данными этого протокола с маршрутизаторами противоположного порта. Снятие отметки также производится клавишей <*Пробел*>.

ВНИМАНИЕ! Если со стороны другого порта конфигурируемого ФПСУ-IP отсутствуют описания маршрутизаторов, использующих один из устанавливаемых протоколов маршрутизации, IP-пакеты этого протокола маршрутизации **не будут проходить через ФПСУ-IP**.

Поддерживается корректная фильтрация и обработка протоколов маршрутизации RIP, RIP2, IGRP, EIGRP, OSPF, OSPF2, LDP.

Когда все параметры в окне «Маршрутизатор» установлены, нажмите кнопку «*Сохранить <F2>*» (или клавишу <*F2*>), после чего осуществится выход в список маршрутизаторов, где появится новая запись маршрутизатора, а внизу окна установки параметров порта будут отображаться введенные параметры.

Если маршрутизатор больше не участвует в работе и его описатель администратору не нужен, выберите его и нажмите <*Del*> для удаления из списка.

Для перехода к списку ФПСУ-IP нажмите <*Tab*>. По нажатию <→> произойдет переход либо к списку ФПСУ-IP, либо к абоненту, с которым связан данный маршрутизатор.

На каждом порту можно создать не больше 32 описателей для маршрутизаторов.

9. 3. Описание параметров удаленных ФПСУ-IP

В поле ***ФПСУ*** порта ФПСУ-IP необходимо описать все другие ФПСУ-IP, которые

будут участвовать в создании VPN-туннелей передачи данных между защищаемыми ими абонентами (сетями) и абонентами настраиваемого ФПСУ-IP.

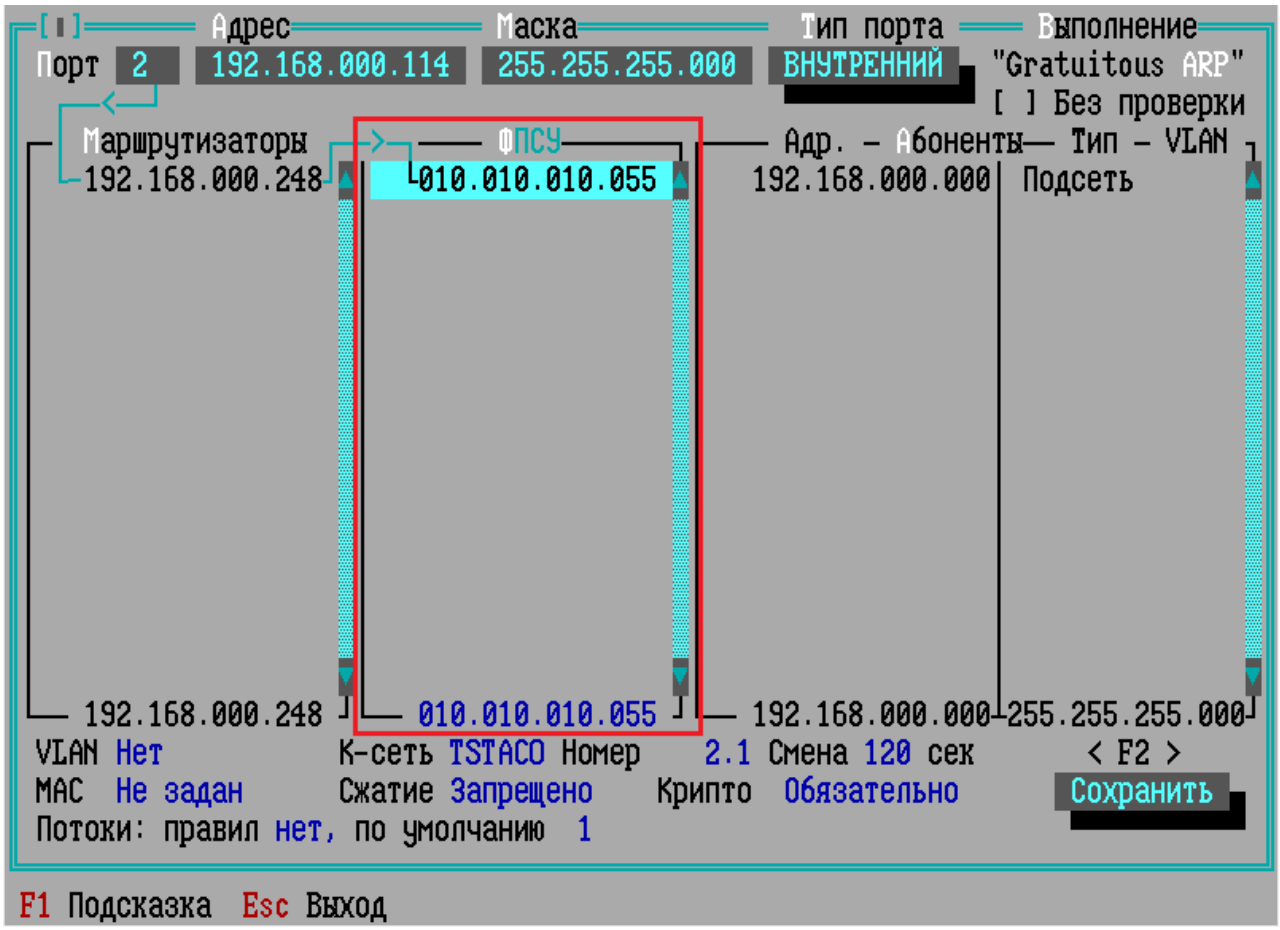


Рисунок 178 - Описатели удаленных ФПСУ порта

Сохранить созданный описатель другого ФПСУ-IP возможно только в том случае, если соответствующие ключи, полученные от «Центра выработки ключей», установлены на ФПСУ-IP и указаны к использованию (см. разделы «Установка ключей» и «Использование ключей»).

Максимальное количество ФПСУ-IP, которое может быть описано на порту — 1024.

Примечание. Для модификации ULT10G при дополнительном лицензировании максимальное количество ФПСУ-IP, описанных в конфигурации может быть увеличено до 10240.

Чтобы создать новый описатель, установите курсор на поле «ФПСУ» и нажмите <*Ins*>, а чтобы отредактировать отмеченный описатель – нажмите клавишу <*Enter*> или <*Пробел*> при установленном на нём курсоре. В окне установки параметров укажите следующие основные параметры, необходимые для установки соединения между ФПСУ-IP:

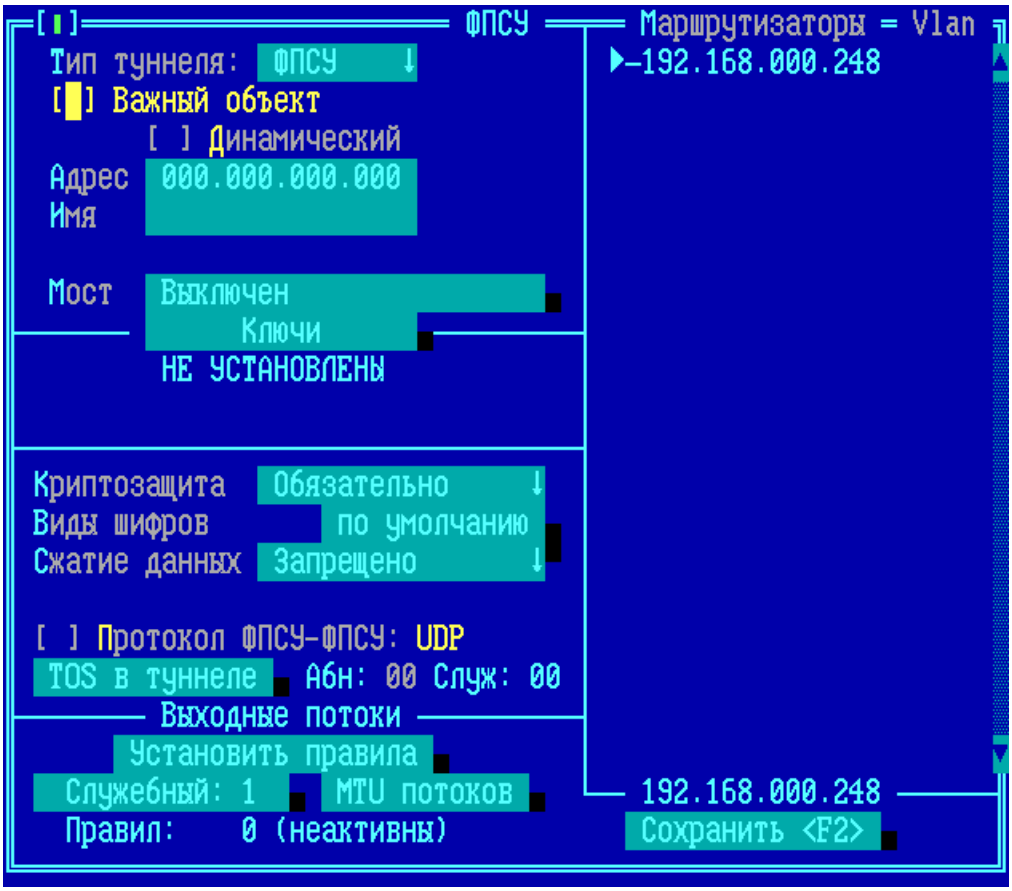


Рисунок 179 - Настройка удаленного ФПСУ-IP

Адрес **—** IP-адрес ФПСУ-IP, с которым будет устанавливаться туннель;

Имя **—** символьное имя этого ФПСУ-IP, оно будет отображаться в списке ФПСУ-IP на экране порта. По умолчанию совпадает со значением поля «Адрес».

Ключи **—** ***обязательный параметр***, определяющий какие именно ключи парно-выборочной связи, из числа установленных и разрешенных к использованию на ФПСУ-IP, будут применяться в процессе шифрования.

Для перехода к установке выделите курсором строку «Ключи» и нажмите *<Пробел>*. В открывшемся окне укажите криптосеть, номер и комплект используемых другим ФПСУ-IP ключей (комплект указывается только для ключей класса КС2).

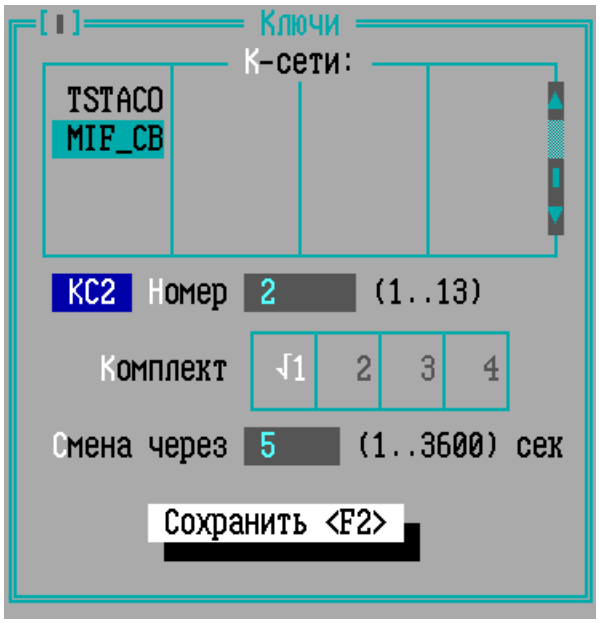


Рисунок 180 - Указание ключевых данных партнера

Определите время, по истечении которого при взаимодействии другого ФПСУ-IP с конфигурируемым на основе выделенных ключей парно-выборочной связи будут вырабатываться новые сеансовые ключи (от 1 до 3600 секунд). Фактически, это время является временем проверки работоспособности VPN-соединения между двумя ФПСУ-IP, поэтому установка большого промежутка времени смены ключей может привести к увеличению времени реакции на потерю соединения (передаваемого на службы мониторинга SysLog или удаленного администратора ФПСУ-IP).

При установке времени смены необходимо учитывать, что при выработке новых сеансовых ключей между двумя ФПСУ-IP будут производиться обмены данными (по два IP-пакета общим размером 80 байт). «Времена смены» могут быть различны на двух ФПСУ-IP, участвующих в процессе образования и поддержания VPN-туннеля.

Затем воспользуйтесь командой «*Сохранить <F2>*», после чего произойдет возврат в окно «ФПСУ».

Маршрутизаторы - маршрутизаторы, через которые может осуществляться связь с описываемым удаленным ФПСУ-IP. Окно содержит список маршрутизаторов, которые заранее были созданы администратором (см. пункт «Описание параметров используемых маршрутизаторов»).

ФПСУ-IP из списка можно приписывать к различным маршрутизаторам, регламентируя тем самым нагрузку на маршрутизаторы. Следует особо отметить ситуацию, когда конфигурируемый ФПСУ-IP имеет несколько смежных маршрутизаторов, которые могут направлять ему ICMP-сообщения переадресации (Redirect) на другой маршрутизатор.

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.

9. 3. 1. Дополнительные параметры соединения ФПСУ-ФПСУ

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

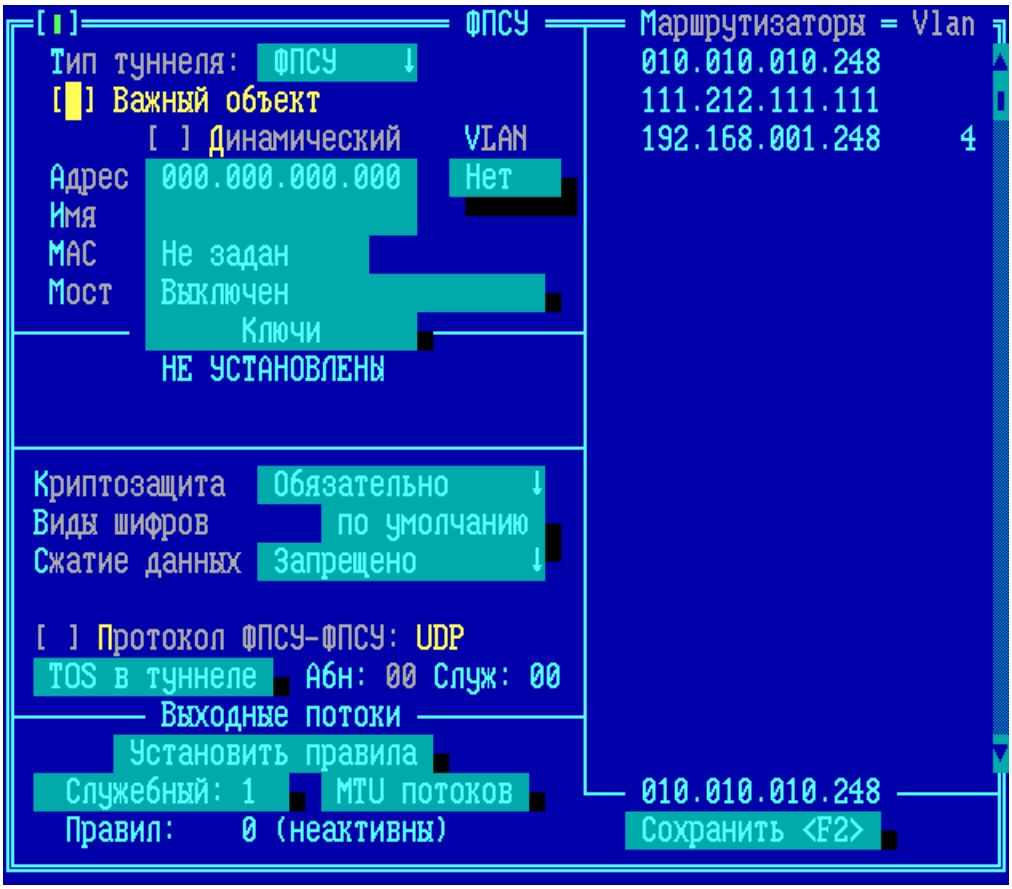


Рисунок 181 - Настройка удаленного ФПСУ-IP

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

Тип туннеля – задается тип туннеля, который строит ФПСУ-IP с другим объектом взаимодействия.

- *ФПСУ* – ФПСУ-туннель устанавливается между двумя ФПСУ-IP, передача данных осуществляется в зашифрованном виде, выполняется инкапсуляция данных в собственный протокол VPN FPSU-IP;
- *IPIP* – ФПСУ-IP строит IPIP-туннель с ФПСУ-IP или другим устройством, поддерживающим протокол инкапсуляции, таким как маршрутизатор или МЭ, передача данных осуществляется в незашифрованном виде (подробнее см. пункт «Описание туннеля типа IPIP»).

Мост – туннель между настраиваемым и удаленным ФПСУ-IP может работать в режиме «моста» (bridge). Описание работы режима моста находится далее, в пункте «Режим «Мост» между ФПСУ-IP (L2-шифрование)».

VLAN **—** номер виртуальной локальной сети, в которой участвует ФПСУ-IP, если требуется. Если маршрут к удаленному ФПСУ-IP указывается через конкретный маршрутизатор (один из маршрутизаторов в поле «Маршрутизаторы» отмечен символом «→»), то VLAN не указывается. Если в маршруте к удаленному ФПСУ-IP маршрутизатор не выбран (ни один из маршрутизаторов не отмечен символом «→»), то VLAN указывается при необходимости тэгировать передаваемый к ФПСУ-IP трафик определенным VLAN (подробнее о выборе маршрутизатора см. пункт «Описание параметров удаленных ФПСУ-IP»).

Криптозащита – указание ФПСУ-IP, каким образом при работе с описываемым партнером согласовывать использование режима шифрования передаваемой информации в соответствии с ГОСТ 28147-89.

Сжатие данных – указание ФПСУ-IP при работе с удаленным ФПСУ-IP использовать режим проходного архивирования передаваемых данных, уменьшая объем передаваемого трафика. ВНИМАНИЕ! Использовать этот режим по умолчанию не рекомендуется, поскольку он уменьшает общую скорость передачи данных между двумя ФПСУ-IP. Рекомендуется к применению на медленных каналах связи (например, ADSL или спутниковых).

Возможные варианты установки каждого из режимов сжатия и шифрования:

- *запрещено* – режим запрещен для канала передачи данных;
- *нежелательно* – использование режима нежелательно, но допускается по конфигурации удаленного ФПСУ-IP;
- *желательно* – режим желателен, но может быть использован только при соответствующих установках на удаленном ФПСУ-IP. Он является режимом по умолчанию;
- *обязательно* – для канала передачи данных режим является обязательным.

Ответственность за согласование конфигураций двух ФПСУ-IP, через которые осуществляется соединение абонентов, и за соответствие установленных на них режимов **несет администратор**. Реальный режим будет зависеть от конфигурации обоих ФПСУ-IP, а ошибка администратора при установке режима может привести к несоблюдению требуемой степени защиты и даже к невозможности передачи данных.

Представленная ниже таблица отображает фактический режим передачи данных абонентов, который будет являться результатом объединения установок работы каждого из двух участвующих в процессе передачи данных ФПСУ-IP с удаленным партнером.

Таблица 3. Режимы взаимодействия ФПСУ

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.

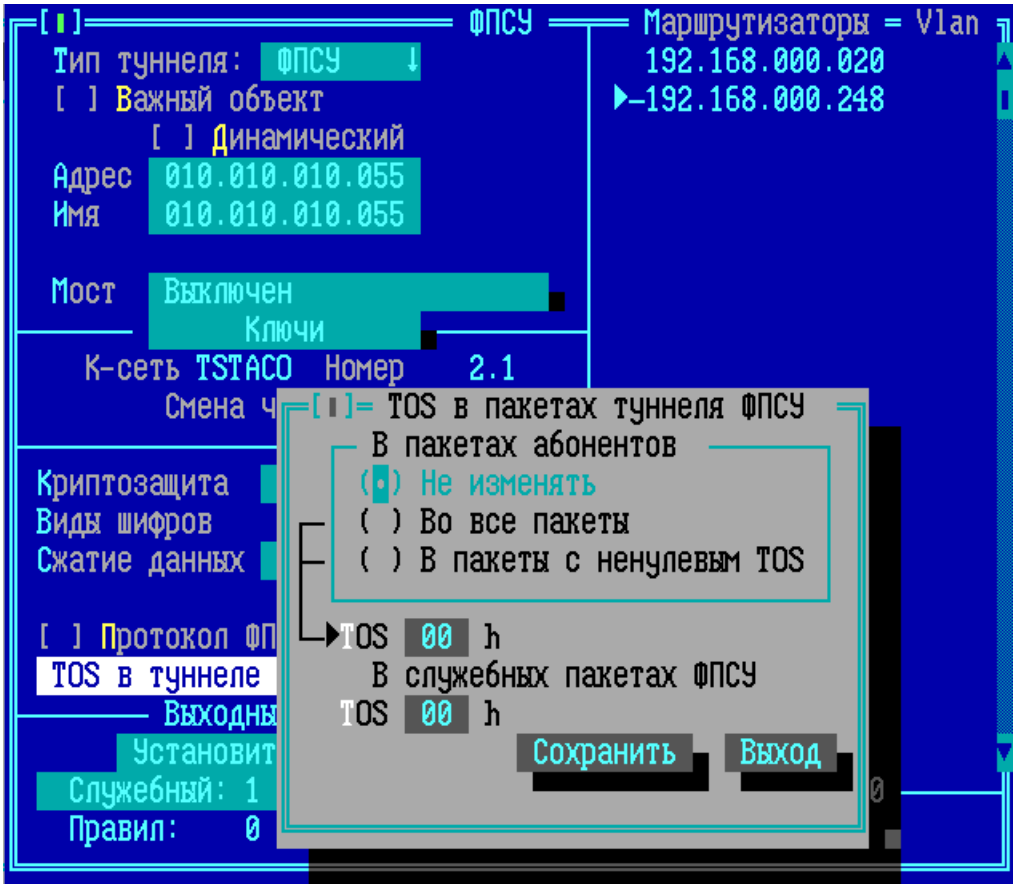


Рисунок 182 - Настройка типа обслуживания в туннеле

9. 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 потока, в который будут направляться служебные данные при взаимодействии ФПСУ-IP с удаленным партнером.

Для перехода в окно управления выходными потоками в туннеле с описываемым ФПСУ-IP нажмите кнопку «*Установить правила*»:

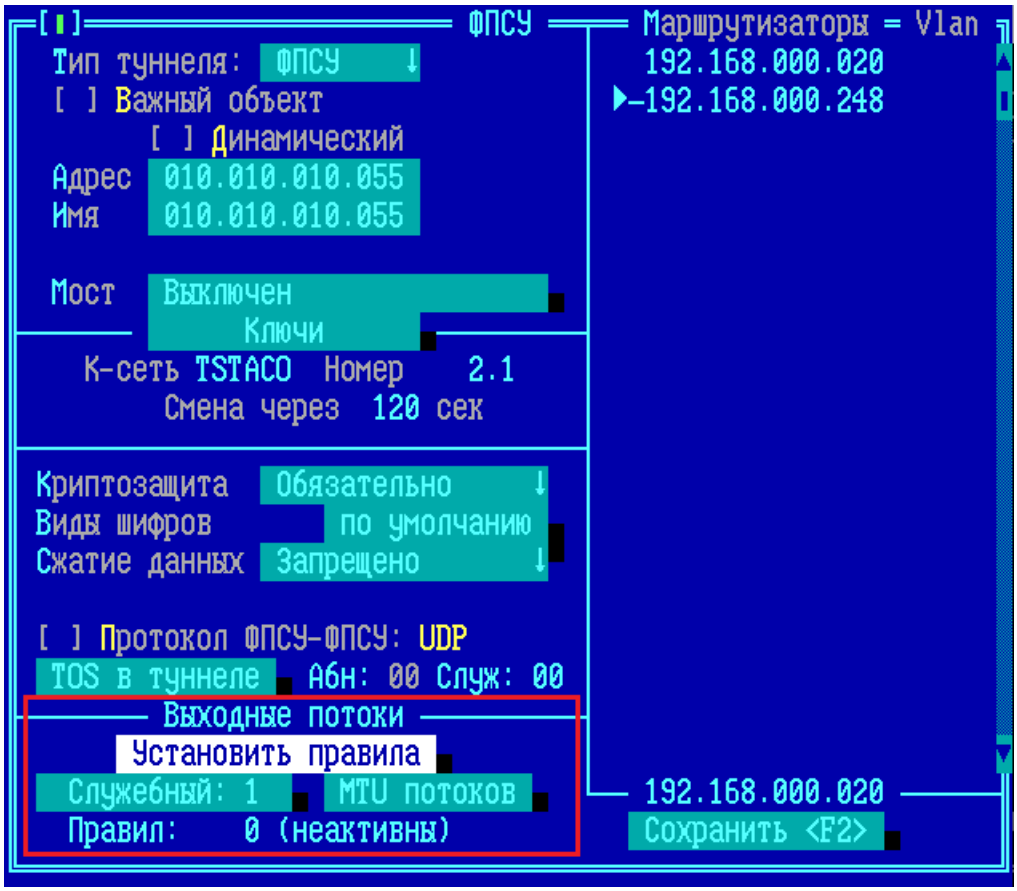


Рисунок 183 - Поле настроек выходных потоков в туннеле между ФПСУ-IP

На экран будет выдано окно, содержащее список правил разделения потоков для VPN туннеля между конфигурируемым ФПСУ-IP и его партнером (пустое по умолчанию, если правила еще не устанавливались).

Правила в списке индивидуальных правил должны располагаться в определенном порядке (в порядке убывания степени детализации условий). Это необходимо для определения приоритетного правила в случае удовлетворения параметров передаваемых IP-пакетов критериям нескольких выходных потоков. При принятии решения о направлении пакета в тот или иной выходной поток правила просматриваются в порядке списка сверху

вниз и при первом совпадении параметров пакета с текущим правилом поток считается выбранным. В случае, когда параметры передаваемого пакета не удовлетворяют критериям ни одного из правил списка, пакет направляется в так называемый поток по умолчанию, номер которого должен быть указан администратором в поле «*Поток по умолчанию*»:

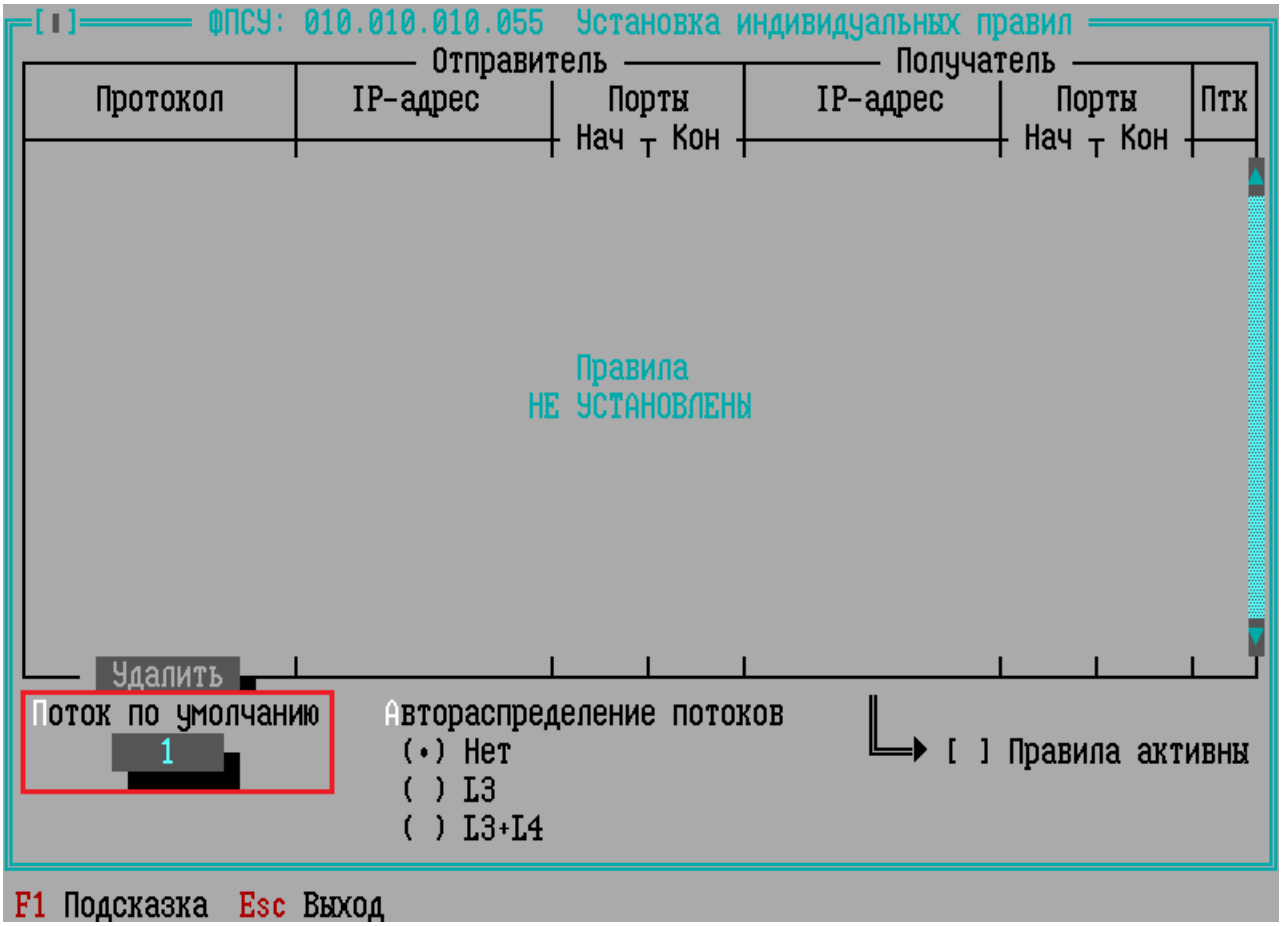


Рисунок 184 - Окно установки правил потоков для удаленного ФПСУ-IP

Потоки могут распределятся вручную администратором, исходя из индивидуальных устанавливаемых правил. Альтернативный вариант: автоматическое случайное распределение пакетов по потокам, которое включает опция «*Авторапределение потоков*» (по умолчанию не задействованная, значение опции установлено в положение «Нет»).

Автоматическое случайное распределение пакетов по потокам было реализовано для оптимизации использования смежного сетевого оборудования: программное обеспечение отдельных многоядерных маршрутизаторов обрабатывало пакеты одного соединения на одном ядре. А поскольку туннелированный трафик между двумя ФПСУ-IP является однотипным с точки зрения IP уровня (один и тот же IP-адрес отправителя и получателя, один и тот же номер IP-протокола), то такие маршрутизаторы работали крайне

неэффективно.

При установке опции «Авторасределение потоков» в значение «L3» или «L3+L4» появляется поле с дополнительной настройкой «Всего потоков»: в нем указывается, на какое количество потоков следует распределять туннелируемый трафик между двумя ФПСУ. Если используется «Авторасределение потоков» для оптимизации использования многоядерных маршрутизаторов, то рекомендуется устанавливать значение, которое равно или превышает число ядер маршрутизатора.

L3 авторасределение использует потоки на сетевом уровне, меняя значения номера IP-протокола (IP№53 и 110-227).

L3+L4 авторасределение использует потоки на транспортном уровне, меняя значения номера UDP-протокола (UDP: №№: 55 000 - 55 127).

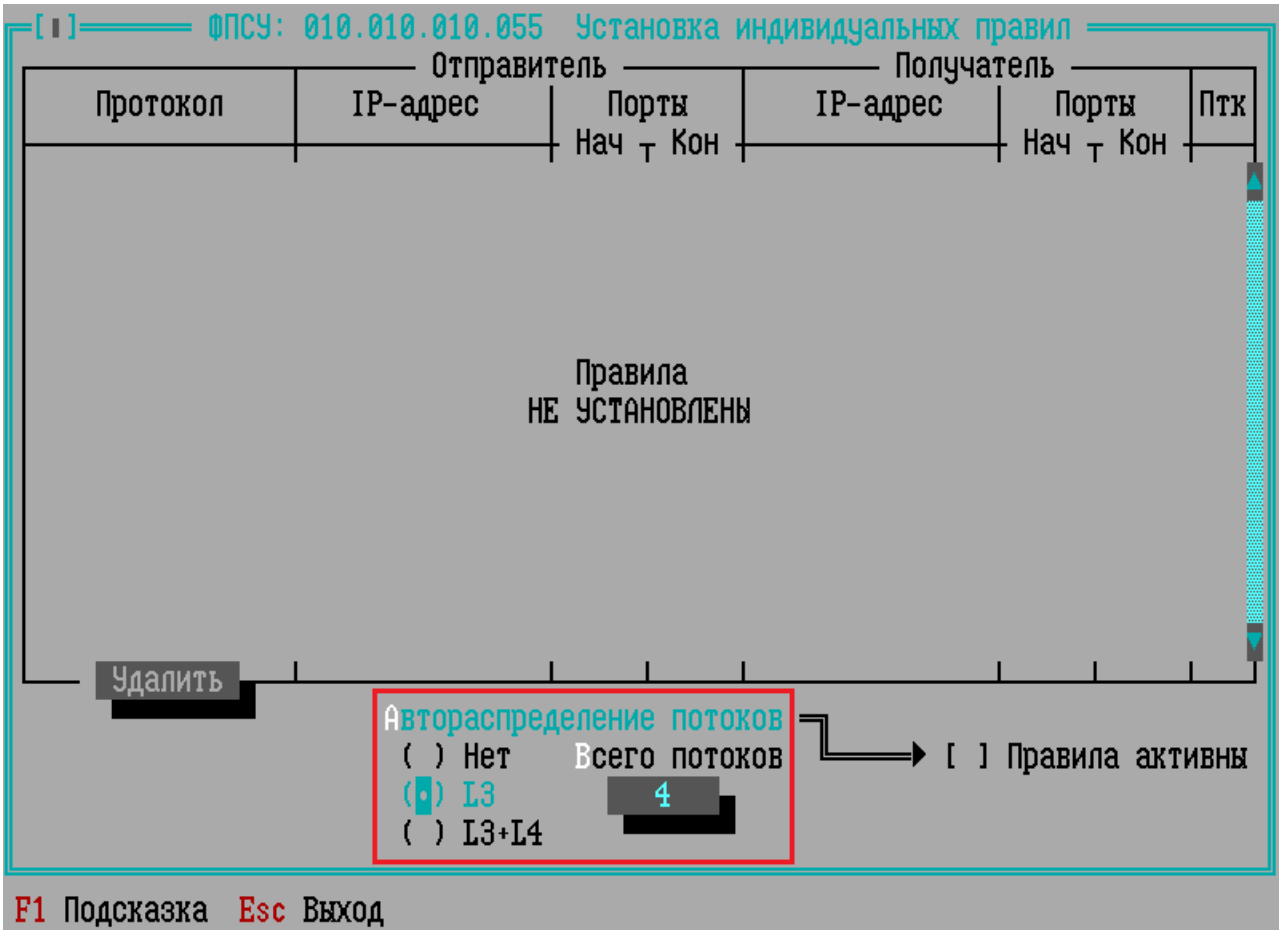


Рисунок 185 - Окно установки правил потоков для удаленного ФПСУ-IP

Если администратор поставил опцию «*Авторасределение потоков*» в значение «*Нет*» (вариант по умолчанию), то можно распределять данные в выходные потоки

вручную. Для того чтобы упорядочить список индивидуальных правил, используются клавиши цифровой части клавиатуры <+> (перемещение правила на позицию вверх) и <-> (перемещение правила на позицию вниз).

По нажатию клавиши <*Ins*> открывается окно установки нового правила, в котором можно установить требуемые параметры вручную, а можно (по нажатию <*Ins*>) вызвать список установленных общих правил (если они есть) и использовать любое из них в качестве заготовки.

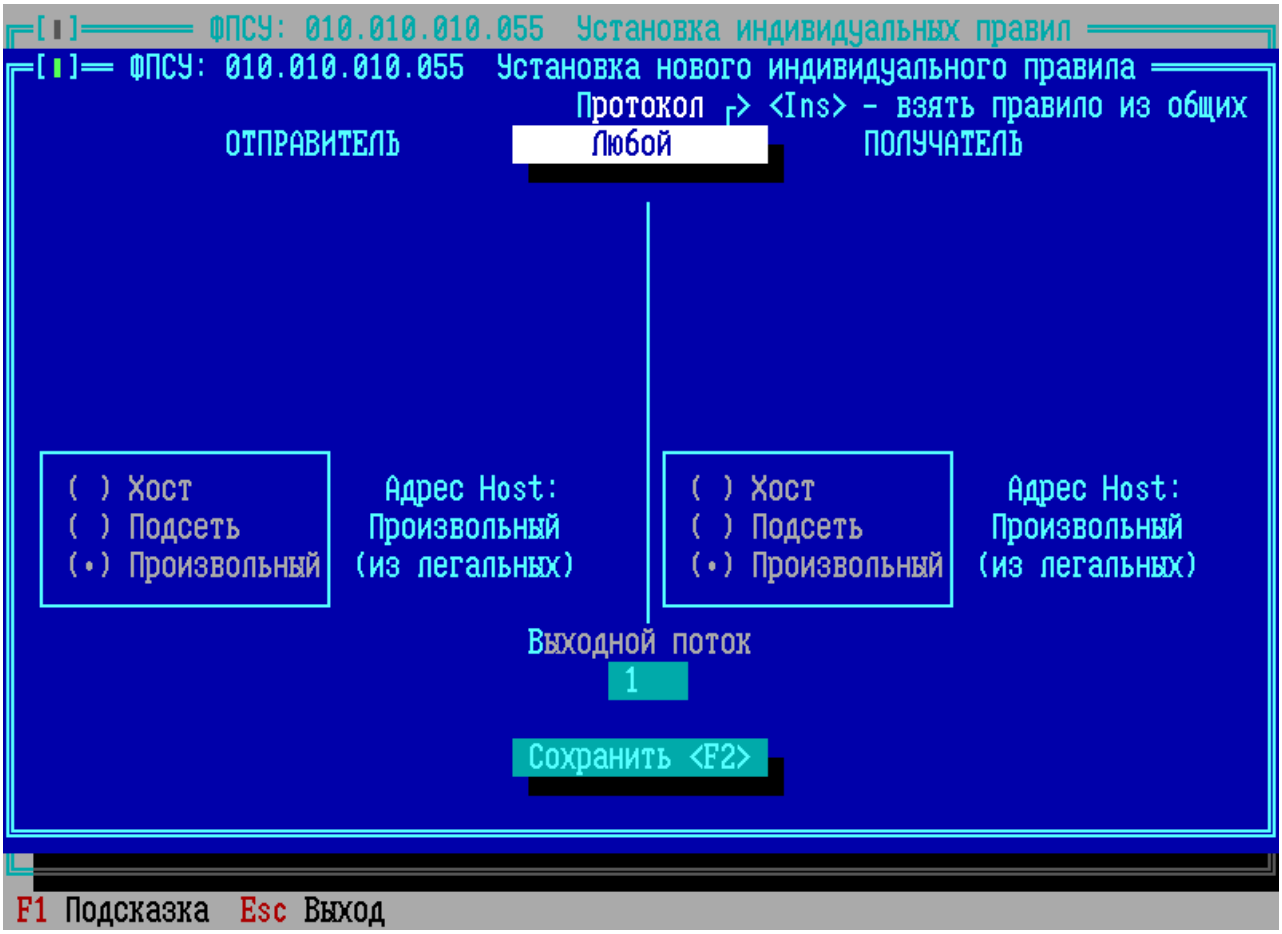


Рисунок 186 - Окно задания правила для нового потока

Для задания протокола для правила нажмите кнопку «Любой». Откроется окно «Установка протокола».

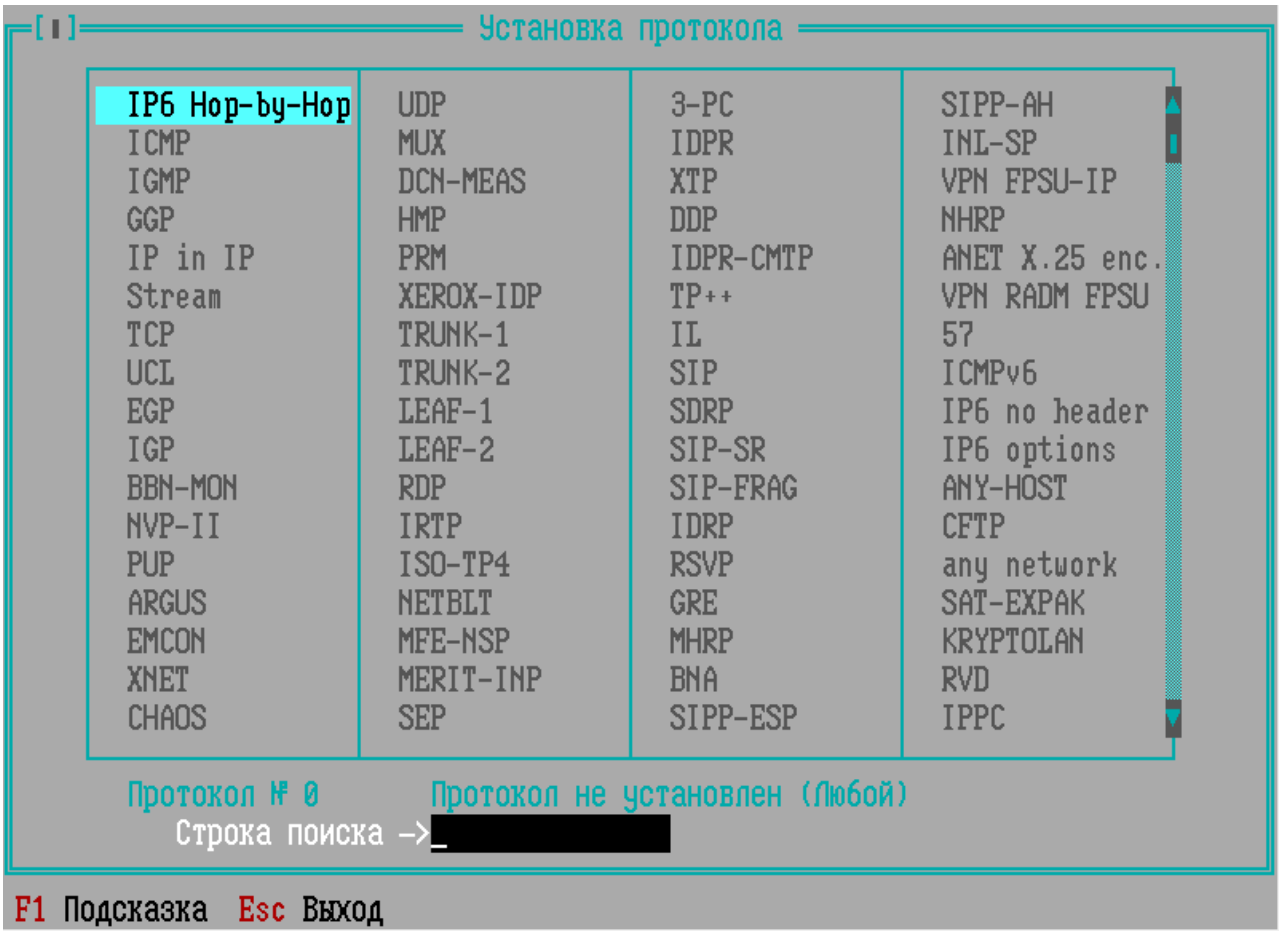


Рисунок 187 - Окно установления протокола для нового потока

Выберите протокол из списка, в окне «Установка нового индивидуального правила» отобразятся дополнительные поля в зависимости от выбранного протокола.

В приведенном примере на рисунке ниже, задается правило для потока. Для правила устанавливается протокол TCP, для которого в дополнительных полях требуется указать начальный и конечный порты для отправителя и получателя. Для правила необходимо задать абонента для отправителя и получателя, выбран по умолчанию - «Произвольный». Необходимо задать выходной поток, выбран по умолчанию - 1. Правило необходимо сохранить по кнопке «Сохранить <F2>».

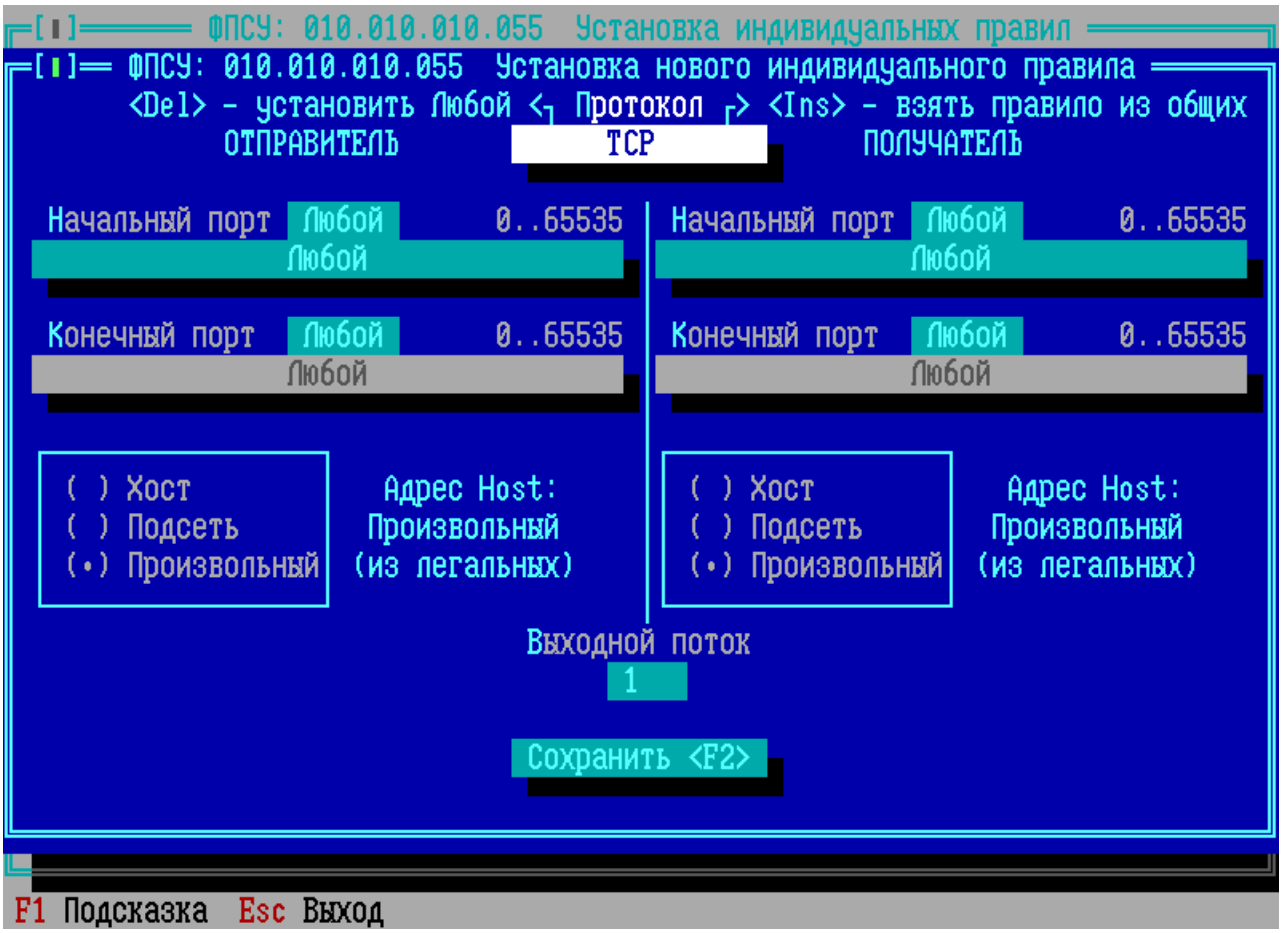


Рисунок 188 - Дополнительные поля для протокола TCP

Чтобы все описанные правила (или авторасределение потоков) использовались при работе VPN-туннеля, необходимо включить флаг «*Правила активны*» в окне «Установка индивидуальных правил».

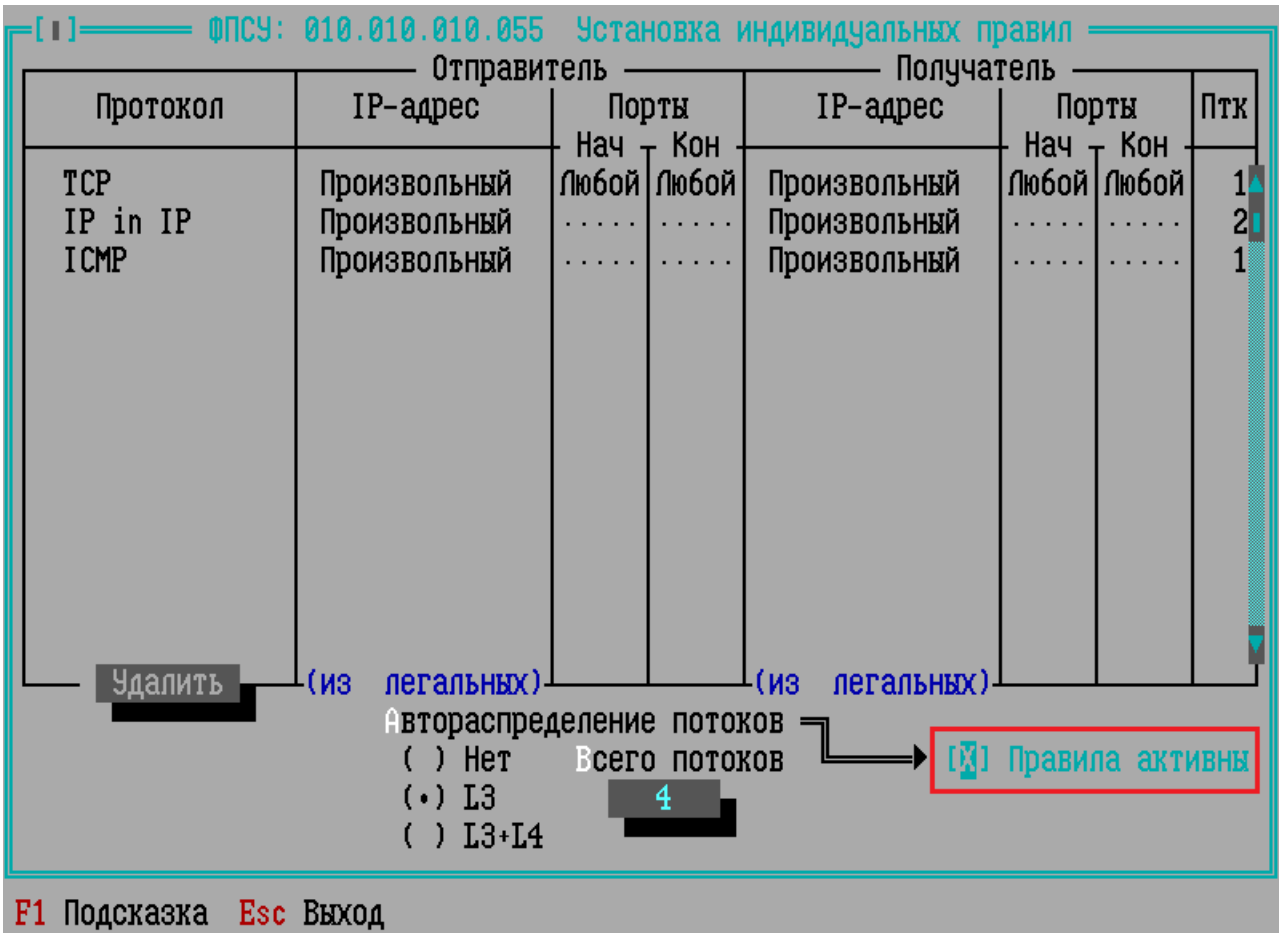


Рисунок 189 - Установка флага «Правила активны»

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.

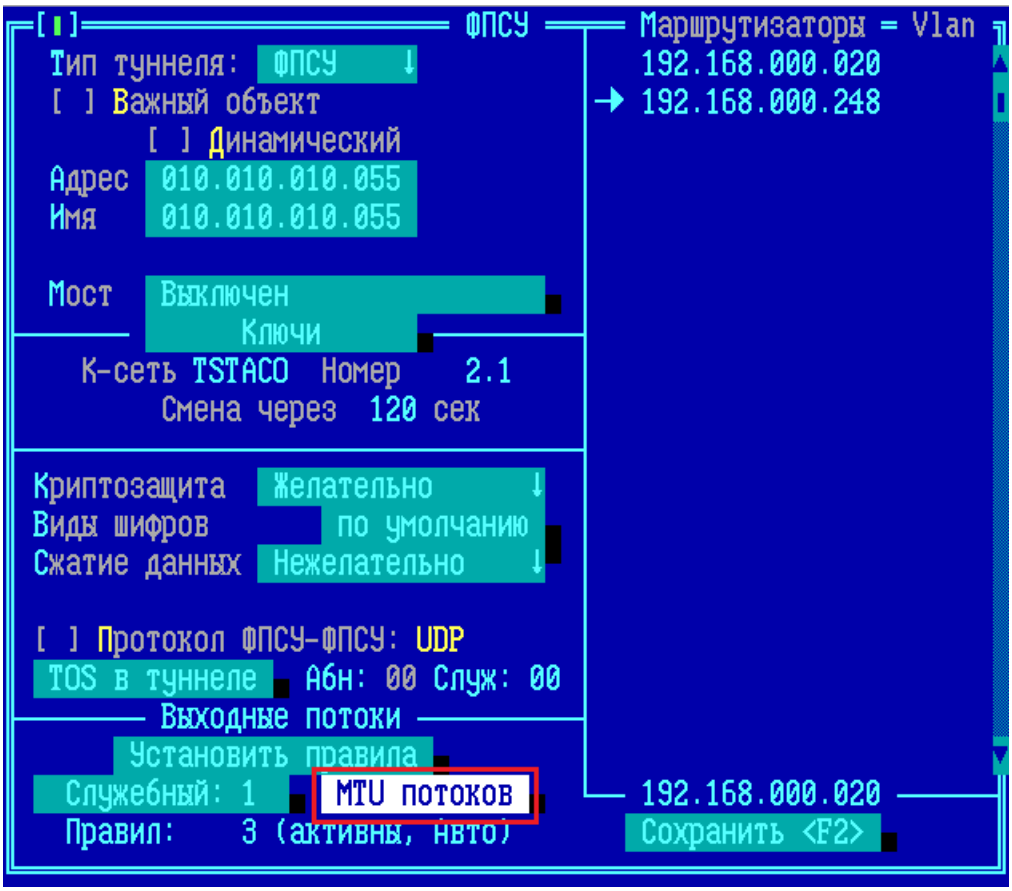


Рисунок 190 - Настройка удаленного ФПСУ-IP

MTU **-** максимальный размер IP-пакетов (в байтах), которые будут передаваться с конфигурируемого порта ФПСУ-IP удаленному ФПСУ-IP через VPN-туннель. Значение этого поля возможно установить в диапазоне от 576 до размера 65535 байт (ВНИМАНИЕ! Фактический MTU будет не выше значения, установленного в настройках сетевого адаптера, см. пункт «Конфигурация драйверов сетевых адаптеров»). По умолчанию («От LAN-платы») будет использоваться значение MTU, которое конфигурируемый ФПСУ-IP автоматически получит от сетевого адаптера описываемого порта. Установка значения, отличного от значения по умолчанию, может потребоваться только в случае наличия достаточно большого количества маршрутизаторов (в конфигурации которых установлено значение MTU менее 1480 байт) по маршруту к описываемому удаленному ФПСУ-IP на загруженных «медленных» магистральных линиях связи. Обычно характерным проявлением такой ситуации является появление на удаленном ФПСУ-IP сообщений (в рабочем окне абонентов, см. Раздел «Окно состояния работы пользователей») об истечении времени жизни пакета от адреса конфигурируемого ФПСУ-IP в собственный адрес удаленного ФПСУ-IP. Необходимо также учитывать, что при уменьшении значения MTU производительность магистральной линии связи между двумя ФПСУ-IP МОЖЕТ СНИЖАТЬСЯ.

9. 3. 3. Режим «Мост» между ФПСУ-IP (L2-шифрование)

Режим моста предназначен для передачи **всех** входящих сетевых фреймов (L2) с одного порта ФПСУ-IP в туннель к другому ФПСУ-IP **без дополнительной проверки и фильтрации**. Режим моста может быть включен только для одного туннеля между ФПСУ-IP.

Для перехода в окно выбора действующего режима следует установить курсор на поле «Мост» и нажать клавишу <*Пробел*>.

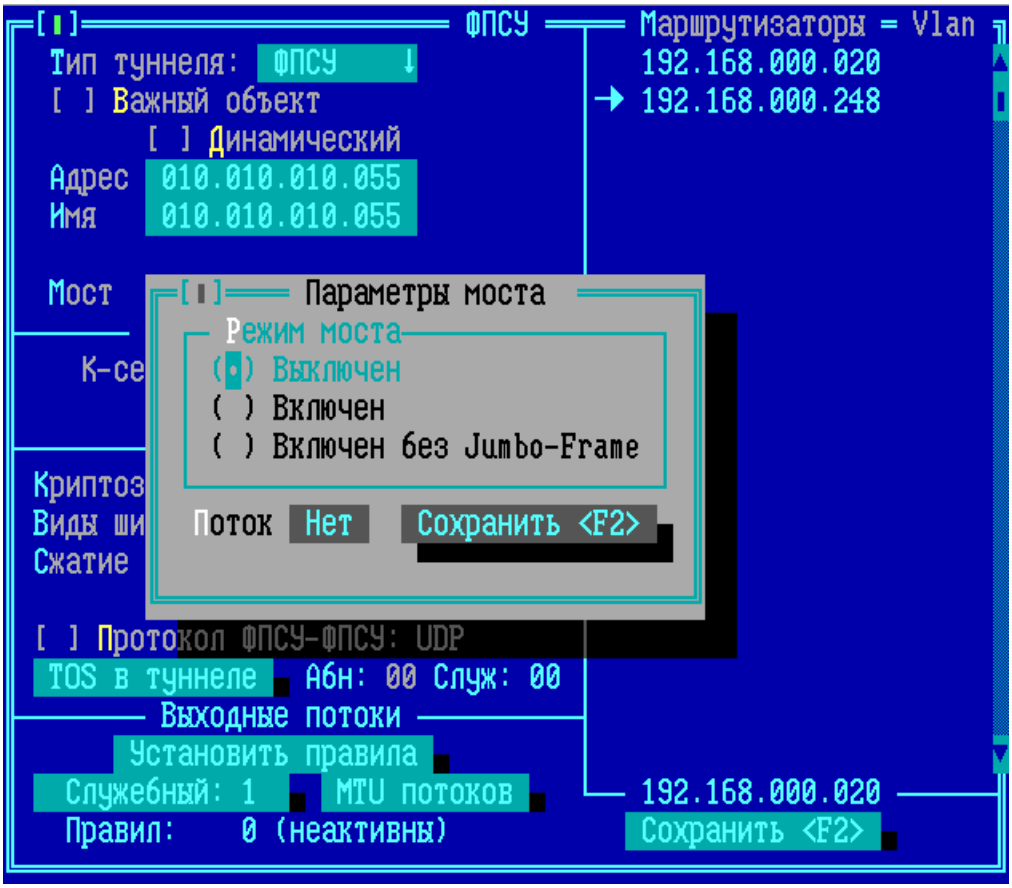


Рисунок 191 - Режим моста ФПСУ-ФПСУ

Режим моста для туннеля между ФПСУ-IP может находиться в следующих состояниях:

Выключен — в туннеле между двумя ФПСУ-IP не используется режим моста.

Включен — в туннеле используется режим моста; ФПСУ-IP будет использовать пакеты увеличенного размера (Jumbo-Frame) для передачи инкапсулированных фреймов, размером до 15854 байт, в зависимости от типа сетевого адаптера. Предназначен для создания «моста» с удаленным ФПСУ-IP. ВНИМАНИЕ! Передача Jumbo-Frame корректно работает только при выборе DPDK драйверов для сетевых

адаптеров! (см. пункт «Конфигурация драйверов сетевых адаптеров»).

Включен без Jumbo-Frame — в туннеле используется режим моста; в этом режиме IP пакеты обычной длины (пакеты размером более 1460 байт, в зависимости от настроек MTU туннеля между ФПСУ-IP и задействованных Ethernet сервисов) после инкапсуляции превысят 1500 байт и будут разбиты на два пакета, что и может вызвать ухудшение скоростных характеристик.

Поток — опциональный параметр. Укажите номер выходного потока (см. пункт «Общие правила разделения потоков»), в который будут инкапсулированы передаваемые в режиме моста пакеты. ВНИМАНИЕ! Для задания отличного от автоматически определенного MTU передаваемых в режиме моста данных, требуется обязательно установить номер потока (от 1 до 8), и затем в настройках выходных потоков туннеля указать для установленного потока желаемый MTU.

При включенном для туннеля между ФПСУ-IP режиме *моста,* все приходящие на другой порт ФПСУ-IP кадры будут приняты и ретранслированы в данный туннель, кроме следующих:

- кадров, отправленные в MAC-адрес портов ФПСУ-IP;
- пакетов от абонентов, описанных на портах ФПСУ-IP.

Полученные из работающего в режиме *моста* туннеля пакеты, отправленные не в MAC-адрес портов ФПСУ-IP, будут ретранслированы на другой порт, вне зависимости от типа кадра (unicast, broadcast) или содержимого верхнего уровня.

Передаваемые в работающий в режиме моста туннель данные инкапсулируются вместе с заголовком канального уровня, в отличие от обычного режима туннеля, когда инкапсулируются данные только начиная с сетевого уровня (выполняется инкапсуляция Ethernet в IP, а не IP в IP).

ВНИМАНИЕ! ФПСУ-IP не выполняет фильтрацию пакетов, ретранслируемых в работающий в режиме моста туннель и получаемых из работающего в режиме моста пакетов, если эти пакеты были направлены не в MAC-адрес портов ФПСУ-IP. Для пакетов, отправленных в MAC-адрес портов ФПСУ-IP, фильтрация по правилам ФПСУ-IP выполняется в обычном порядке.

ВНИМАНИЕ! ФПСУ-IP, работающий в режиме моста, запрещается указывать в качестве основного шлюза на рабочей станции!

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 только один туннель может быть настроен на работу в режиме моста.

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.

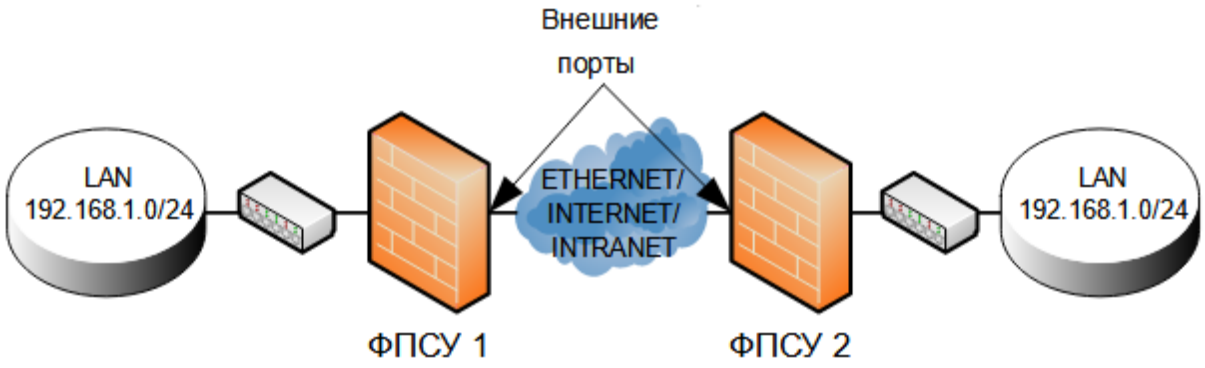


Рисунок 192 - Режим моста в туннеле ФПСУ-ФПСУ

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.

Нажмите кнопку *«Сохранить»* или клавишу *<F2>* для выхода из окна с сохранением выполненных изменений, и клавишу *<Esc>* для выхода без сохранения.

ВНИМАНИЕ! При включении режима «мост» разрешается использовать горячий резерв по основным портам.

9. 3. 4. Динамические ФПСУ

Стандартный вариант построения VPN-туннеля между двумя ФПСУ-IP предполагает, что администратору местного ФПСУ-IP известен постоянный IP-адрес удаленного ФПСУ-IP.

В случае, когда удаленный ФПСУ-IP подключается к сегменту сети передачи данных через провайдера, выдающего сетевым устройствам временный IP-адрес, стандартный вариант построения VPN-туннеля не подходит. Администратор ФПСУ-IP может отметить такой удаленный ФПСУ-IP как «Динамический», разрешая установление туннеля с произвольного IP-адреса.

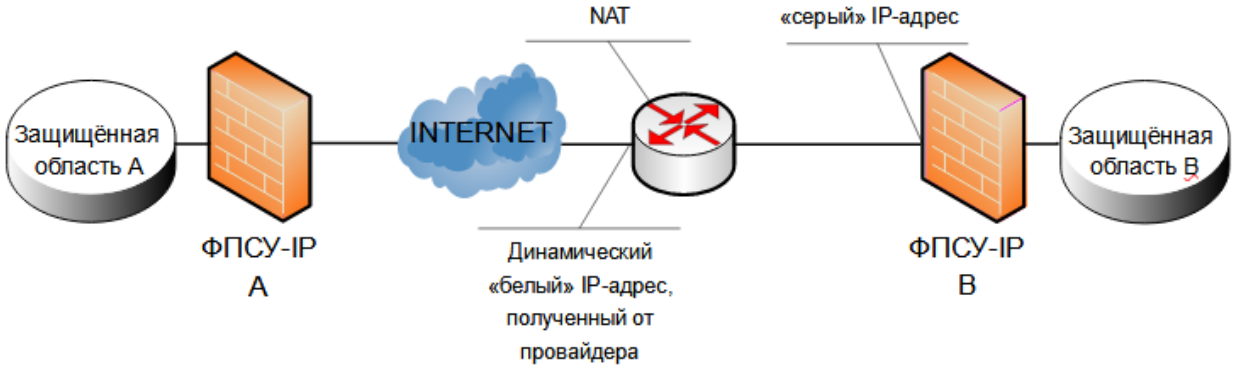


Рисунок 193 - Схема при установлении динамического туннеля с другим ФПСУ-IP

Опция «Динамический» для ФПСУ-IP может быть задействована только в случае использования ключей класса КС1 или КС3. Если на ФПСУ-IP используются только ключи класса КС2, не получится указать ФПСУ-IP как «Динамический».

Признак «Динамического» удаленного ФПСУ-IP устанавливается в описателе ФПСУ-IP:

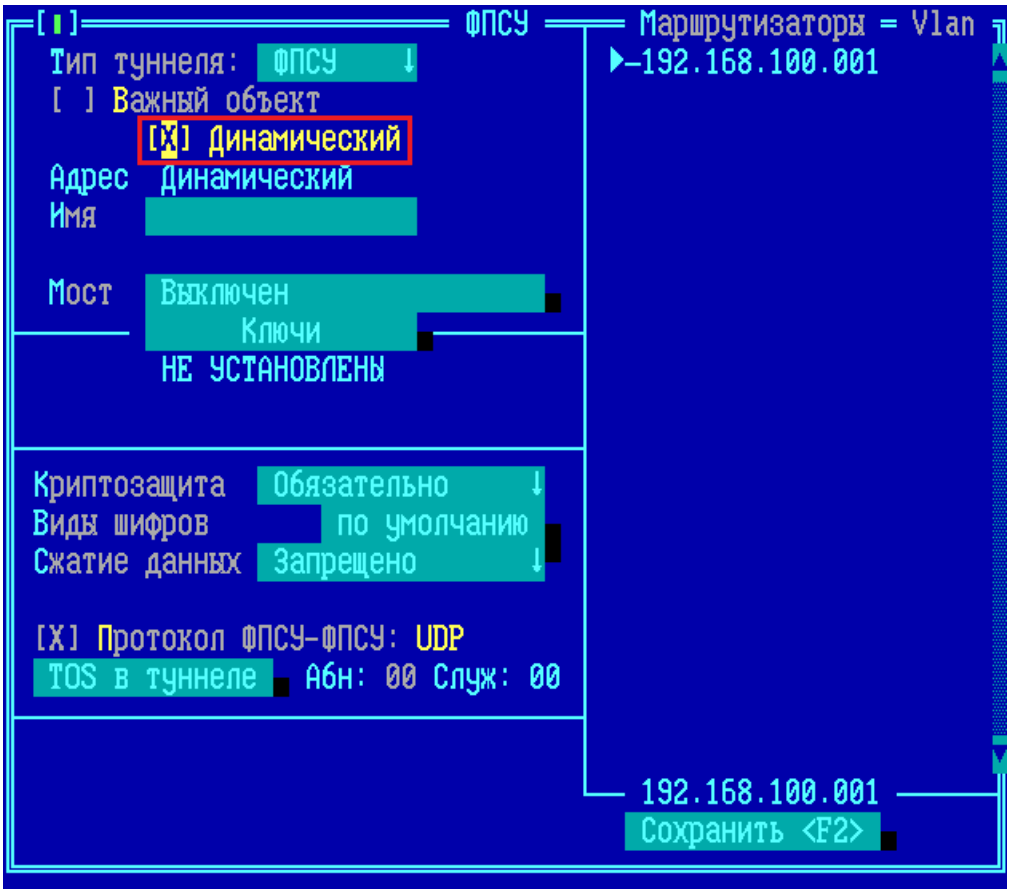


Рисунок 194 - Динамический туннель с другим ФПСУ-IP

При использовании опции описателя ФПСУ-IP - «Динамический», следует учитывать следующие отличия такого VPN-туннеля от стандартного:

- динамический ФПСУ-IP может быть указан только как доступный через маршрутизатор;
- местный ФПСУ-IP никогда не будет выступать инициатором установления туннеля с динамическим ФПСУ-IP, ожидая подключения со стороны динамического;
- протокол VPN-туннеля для взаимодействия с динамическим ФПСУ-IP обязательно должен быть UDP. Установление соединения по сетевому протоколу IP№53 не поддерживается;
- для установления соединения с динамическими ФПСУ-IP, основной слушает порт UDP:30004. После успешной авторизации динамического ФПСУ-IP, VPN-туннелю выделяется UDP-порт из диапазона UDP:40000 - UDP:50000;
- разделение VPN-туннеля на потоки не поддерживается для динамического ФПСУ-IP;
- создавать отдельное правило межсетевого экрана разрешения установления соединений для таких VPN-туннелей не требуется.

ВНИМАНИЕ! Если администраторы обоих ФПСУ-IP указали партнера по VPN-туннелю как «Динамического», VPN-туннель не будет установлен.

9. 3. 5. Описание туннеля типа IPIP

На ФПСУ-IP поддерживается дополнительный тип туннеля — IPIP-туннель. ФПСУ-IP строит IPIP-туннель с ФПСУ-IP или другим устройством, поддерживающим протокол инкапсуляции, таким как маршрутизатор или межсетевой экран. При построении IPIP-туннеля ФПСУ-IP реализован протокол IP in IP, используется механизм инкапсуляции, регламентированный стандартом RFC 2003. В IPIP-туннеле не используются шифрование передаваемых данных и аутентификация участвующих в построении туннеля устройств.

В IPIP-туннеле каждый IP-пакет инкапсулируется в другой IP-пакет и оправляется другому участнику соединения. На обеих сторонах IPIP-туннеля должны использоваться белые IP-адреса, либо участники соединения должны находиться в одной локальной сети, при этом не используется трансляция адресов NAT.

В IPIP-туннеле любой трафик (пользовательский или служебный) пересылается по общим правилам межсетевого экрана на ФПСУ-IP. После извлечения из туннеля трафик маршрутизируется по общим правилам ммежсетевого экрана на ФПСУ-IP.

При разрыве соединения досыл данных в IPIP-туннель не производится.

IPIP-туннель может использоваться во VLAN. Допустимый диапазон используемых идентификаторов VLAN от 2 до 4092.

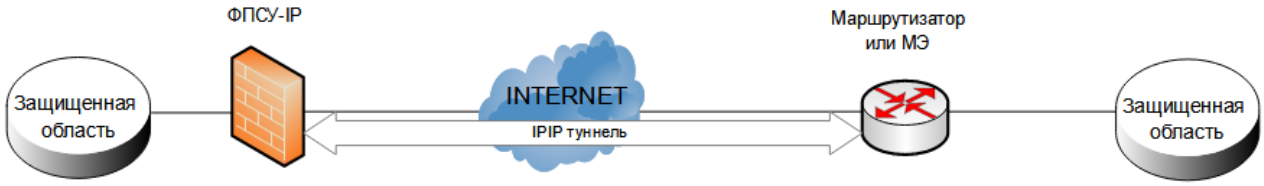


Рисунок 195 - Режим IPIP-туннеля ФПСУ-ФПСУ

9. 4. Описание параметров абонентов

В поле ***Абоненты*** содержится список абонентов со стороны данного порта ФПСУ-IP, для которых будет разрешен обмен пакетами с другими абонентами ФПСУ-IP.

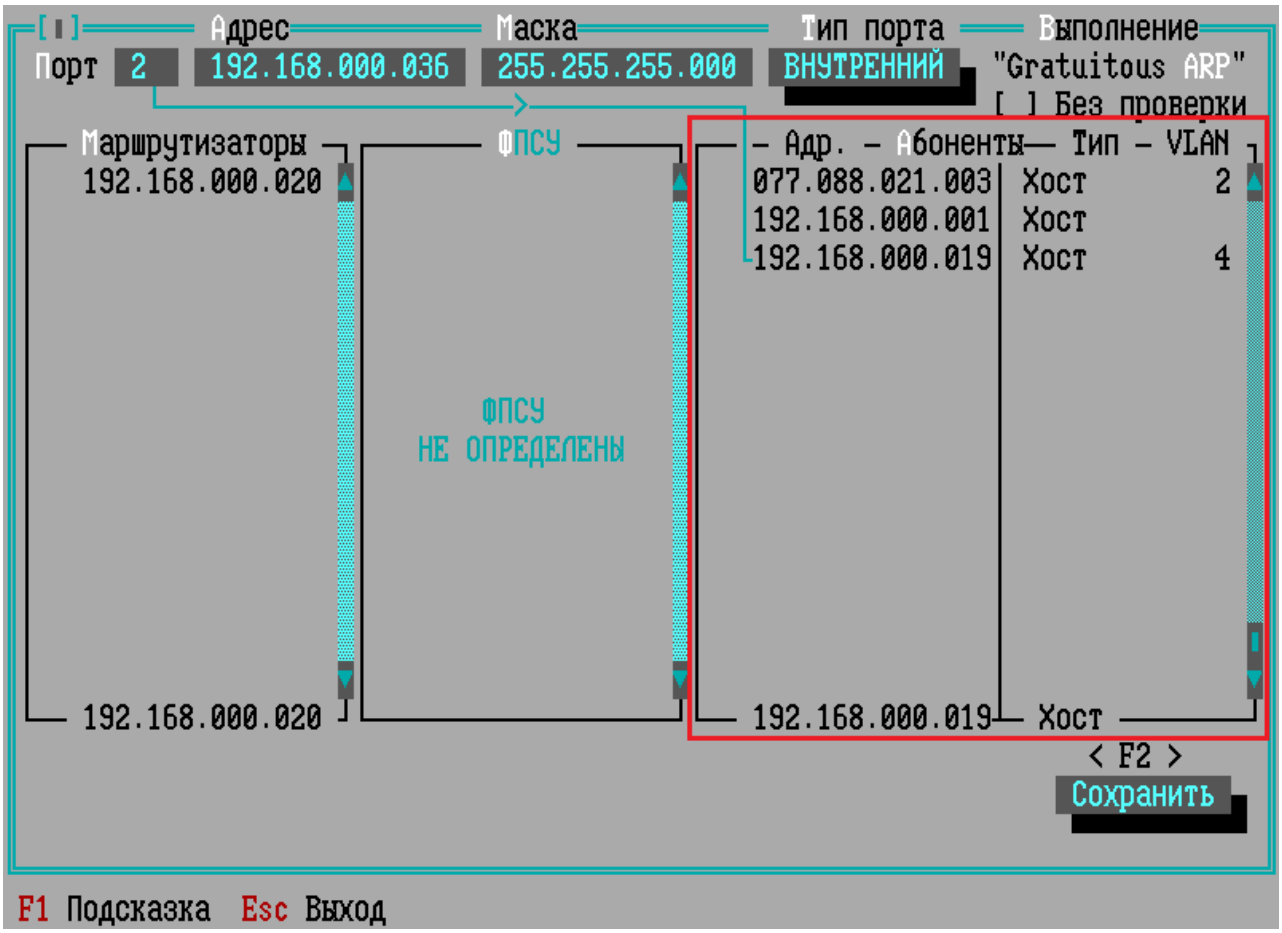


Рисунок 196 - Абоненты порта ФПСУ-IP

Если со стороны одного порта не указано ни одного абонента, ФПСУ-IP не сможет передавать данные через себя. Смогут функционировать и взаимодействовать между собой только IP-адреса, указанные как абоненты на другом порту.

В списке абонентов порта используются три типа записей:

- отдельные рабочие станции (запись типа «Хост»);
- пары адрес/маска подсети (запись типа «Подсеть»);
- специальный адрес «Любой Хост».

Адрес одного и того же абонента может содержаться в нескольких записях (абонент имеет собственный IP-адрес, он может входить в «прописанную» подсеть, которая входит в другую «прописанную» подсеть, кроме того, он попадает в категорию «Любой Хост», если она указана).

При проверке проходящего через ФПСУ-IP пакета, поиск адреса в таблице (и соответствующая фильтрация для этого адреса) производится по принципу «наибольшего совпадения», то есть в описателях конфигурации данного порта ищется «самый

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.

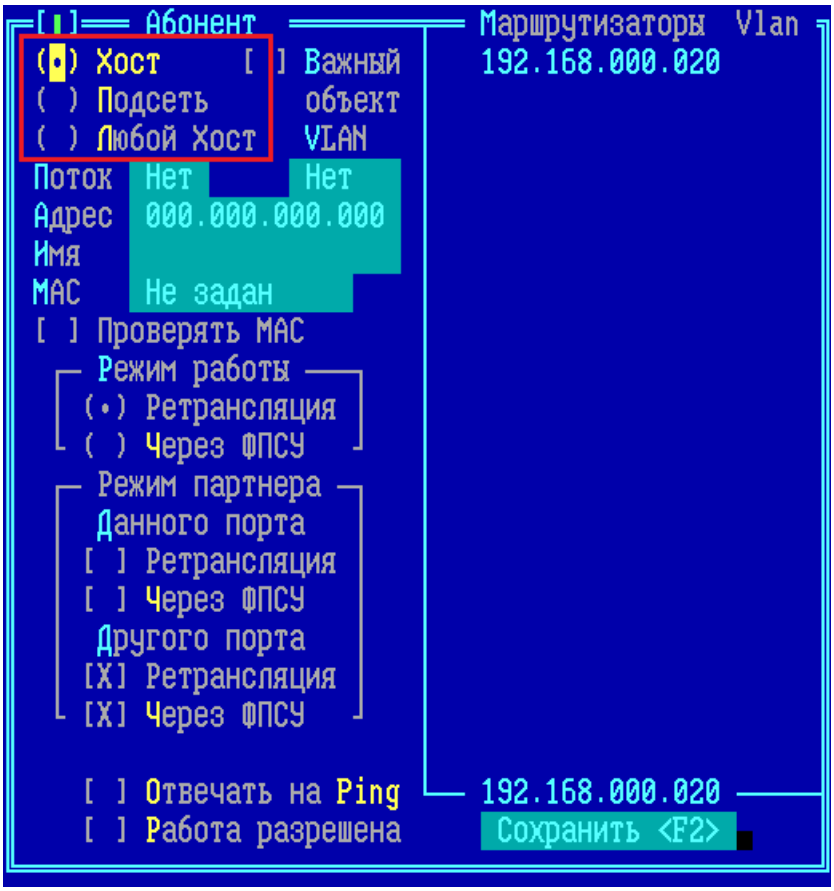


Рисунок 197 - Окно «Абонент»

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».

9. 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:

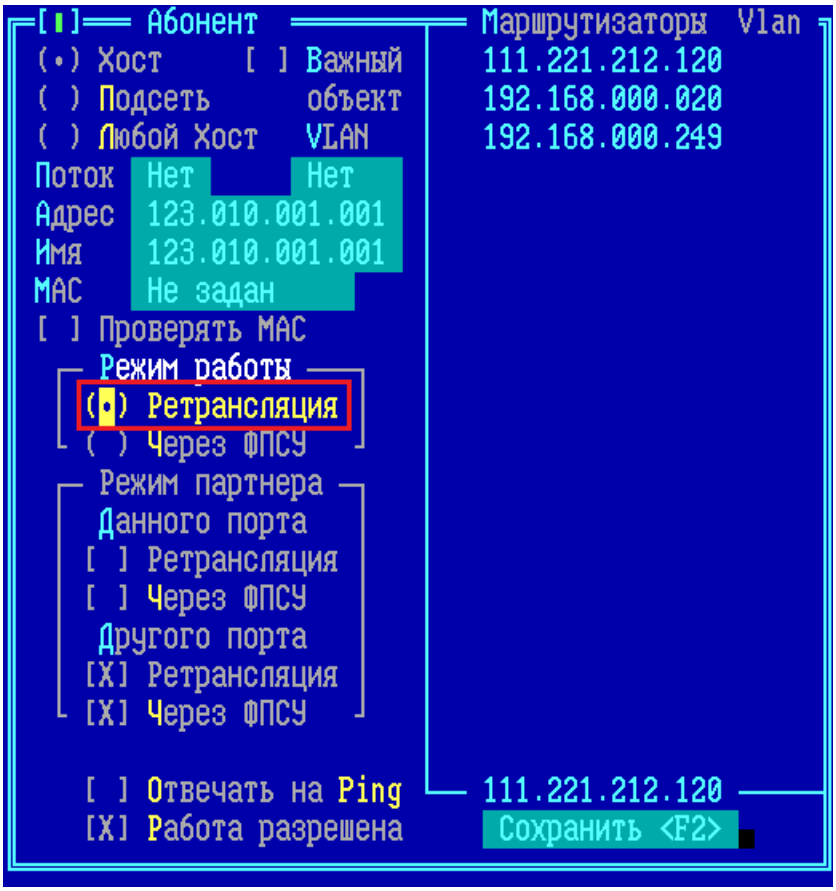


Рисунок 198 - Параметры абонента типа хост, режим «Ретрансляция»

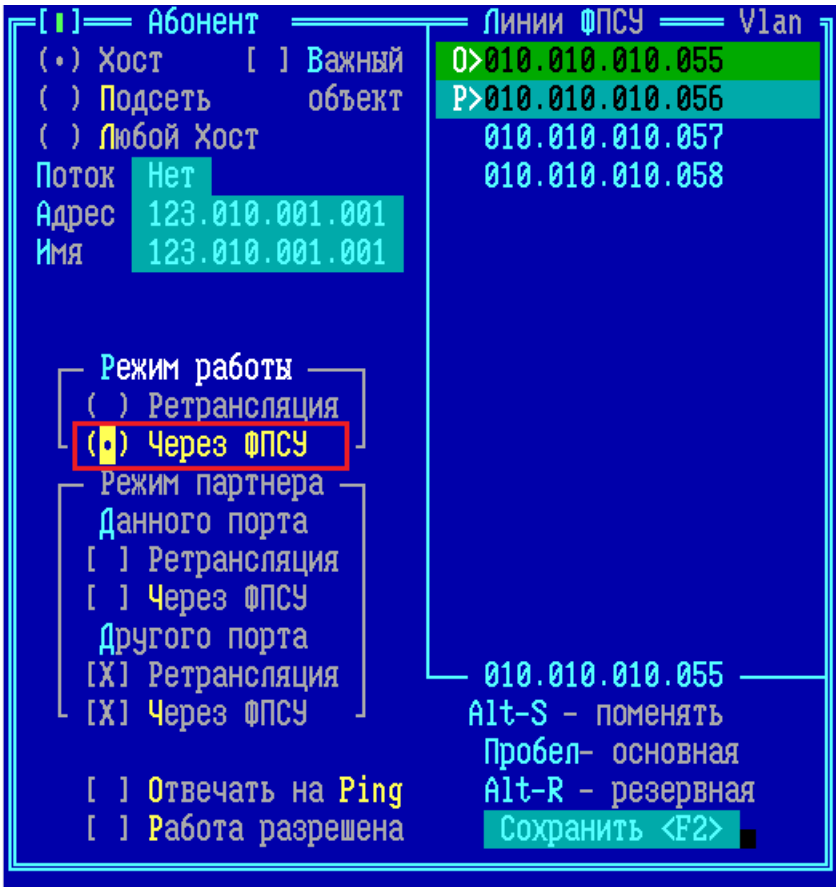


Рисунок 199 - Параметры абонента типа хост, режим «Через ФПСУ»

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-

адресу. Если MAC-адрес полученного пакета от IP-адреса описываемого абонента не совпадает с указанным в поле «MAC», пакет будет сброшен.

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

Режим работы: «Ретрансляция» (фильтрация без аутентификации) или «Через ФПСУ» (обмен между абонентом и портом ФПСУ-IP будет производиться через туннель со смежным ФПСУ-IP. В этом режиме возможно включение механизмов шифрования и/или сжатия передаваемых данных).

- ***«Ретрансляция»*** (обмен данных ФПСУ-IP с абонентом осуществляется без шифрования, соединения с ним только фильтруются межсетевым экраном).

Выберите этот режим, если описываемый абонент подключен к настраиваемому ФПСУ-IP напрямую, то есть пакеты от него приходят в обычном виде, а не через VPN-туннель. Например, на рисунке ниже для ФПСУ-IP A это будут абоненты «a1», «a2», «b1»и «b2»; для ФПСУ-IP B это будут абоненты «b1», «b2», «In1» и «In2»; а для ФПСУ-IP C это будут абоненты «c1», «c2», «In1» и «In2».

При выборе режима «Ретрансляция», в правой части окна будет отображаться список маршрутизаторов, описанных со стороны данного порта. Если абонент доступен через какой-либо маршрутизатор, то такой маршрутизатор следует отметить нажатием клавиши <*Пробел*> (если в списке нет маршрутизаторов, необходимо сначала описать их). Заметим, что администратор может регламентировать нагрузку на маршрутизаторы, приписывая различных абонентов к определенным маршрутизаторам. При передаче IP-пакетов описываемому абоненту ФПСУ-IP будет учитывать ICMP сообщения переадресации (см. пункт «Описание параметров удаленных ФПСУ-IP»).

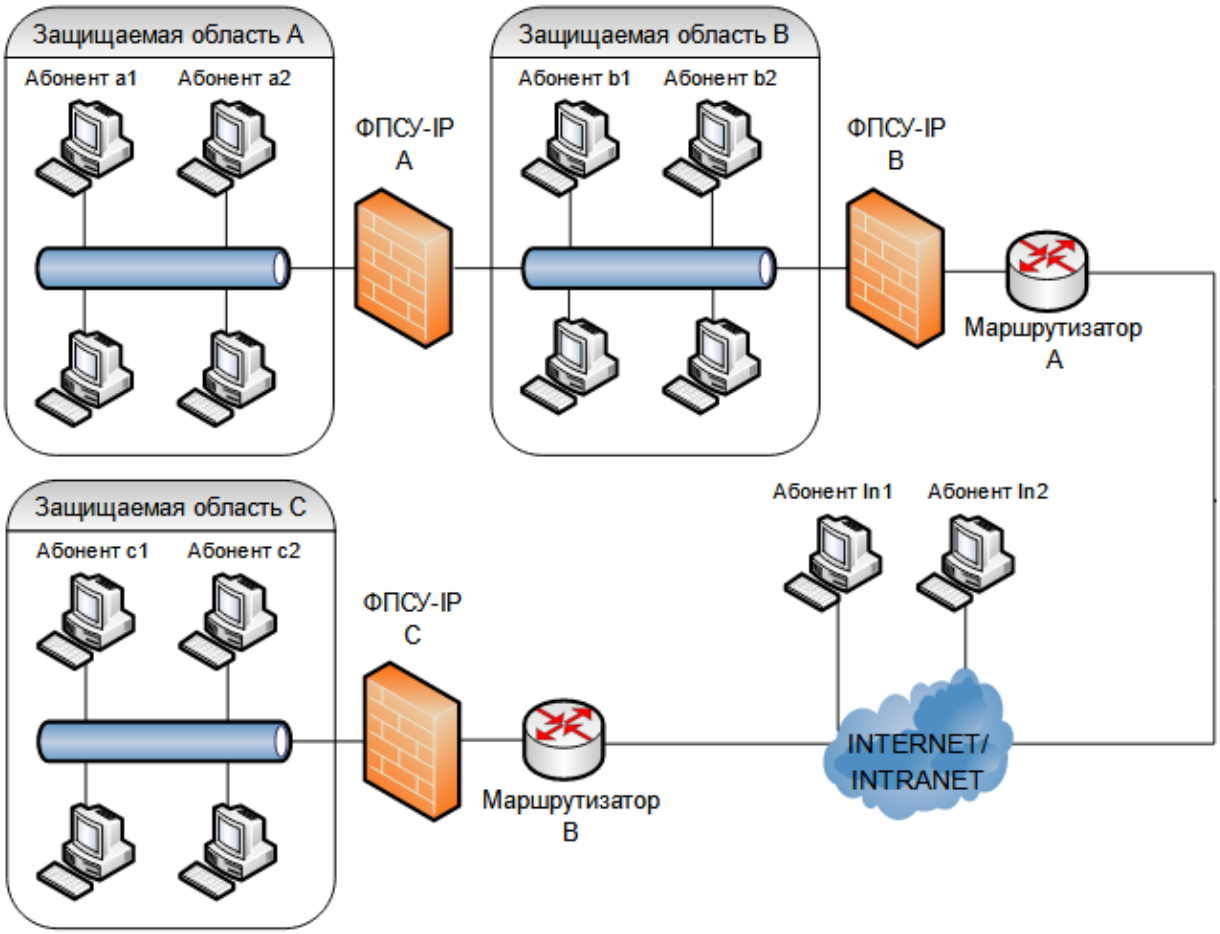


Рисунок 200 - Режим работы партнеров абонента

- «***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).

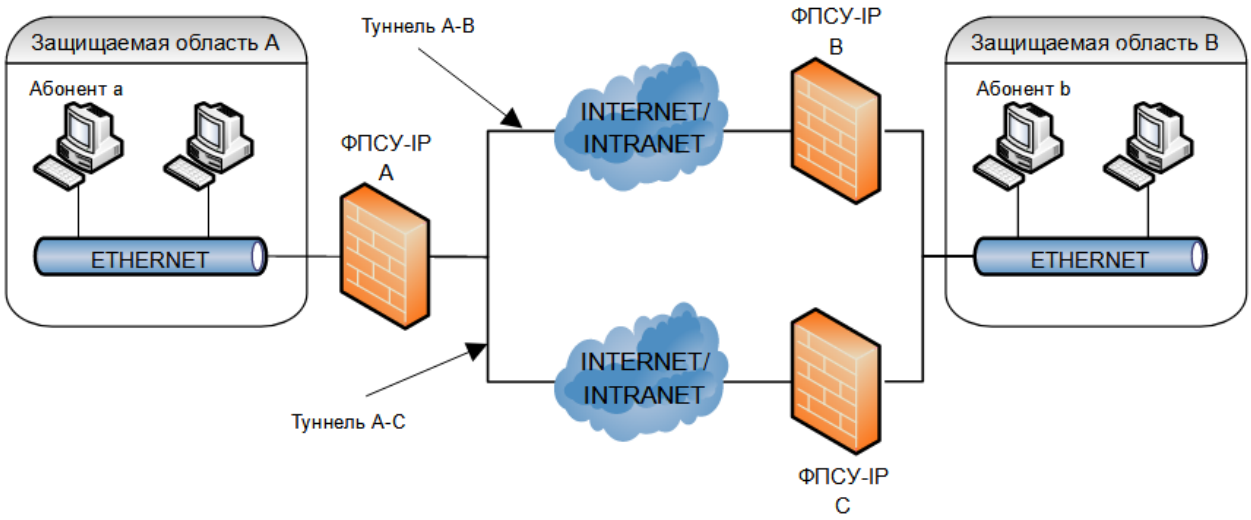


Рисунок 201 - Использование основной и резервной (запасной) линий ФПСУ-IP

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».

Режим партнера - режим работы, указываемый для партнера (абонента), с которым может обмениваться пакетами данный абонент. Знак [X] около соответствующей строки означает отсутствие, для данного абонента, принципиального запрета возможности работать с партнерами, для которых установлен указанный режим работы на одном из портов.

Партнер данного порта — это абонент, зарегистрированный на том же логическом порту ФПСУ, что и описываемый абонент (например, при добавлении абонента на логический порт с номером 1 партнерами данного порта являются все абоненты, описанные на логическом порте с номером 1 настраиваемого ФПСУ).

Партнер данного порта в режиме «Ретрансляция» — это абонент, зарегистрированный на том же логическом порту, что и описываемый абонент, который подключен к настраиваемому ФПСУ-IP напрямую. Например, на рис. «Режим работы партнеров абонента» для ФПСУ-IP C и описываемого на нем «Абонента a1» партнером данного порта в режиме ретрансляция является «Абонент In1» или «Абонент In2»; для ФПСУ-IP B и описываемого «Абонента a2» таким партнером является «Абонент b2».

Партнер данного порта в режиме «Через ФПСУ» — это абонент, зарегистрированный на том же логическом порту, что и описываемый абонент, который подключен к настраиваемому ФПСУ-IP через установленный VPN-туннель с другим ФПСУ-IP. Например, на рис. «Режим работы партнеров абонента» для ФПСУ-IP C и описываемого на нем «Абонента c1» партнером данного порта в режиме «Через ФПСУ» является «Абонент b2» или «Абонент a1»; для ФПСУ-IP A и описываемого на нем «Абонента b1» таким партнером является «Абонент In2» или «Абонент c2».

Партнер другого порта — это абонент, зарегистрированный на другом логическом порту ФПСУ, относительно описываемого абонента (например, при добавлении абонента на первый логический порт партнерами другого порта являются все абоненты, описанные на втором логическом порту).

Партнер другого порта в режиме «Ретрансляция» — это абонент, зарегистрированный на другом логическом порту ФПСУ-IP, относительно описываемого абонента, который подключен к настраиваемому ФПСУ-IP напрямую. Например, для ФПСУ-IP B и описываемого «Абонента b1» партнером другого порта в режиме «Ретрансляция» является «Абонент In1» или «Абонент In2»; для ФПСУ-IP C и описываемого «Абонента c1» таким партнерами тоже являются «Абонент In1» или «Абонент In2».

Партнер другого порта в режиме «Через ФПСУ» — это абонент, зарегистрированный на другом логическом порту ФПСУ-IP относительно описываемого абонента, который подключен к настраиваемому ФПСУ-IP через установленный VPN-туннель с другим ФПСУ-IP. Например, для ФПСУ-IP A и описываемого «Абонента a1»

партнерами другого порта в режиме «Через ФПСУ» являются «Абонент c1» или «Абонент in1»; для ФПСУ-IP C и описываемого «Абонента c2» такими партнерами являются «Абонент a2» или «Абонент b2».

Режим партнера устанавливается отдельно для каждого абонента порта комплекса, причем:

- для партнера со стороны данного (своего) порта могут быть разрешены один или оба режима, а отказ от обоих режимов означает запрещение описываемому абоненту обмениваться IP пакетами с абонентами со стороны своего порта;
- для партнера со стороны противоположного порта должен быть разрешен хотя бы один режим работы, иначе пакеты данного абонента не смогут быть переданы через комплекс (о чем подсистема выдаст сообщение при последующей попытке сохранить установки), отметка обоих режимов работы означает отсутствие ограничения по режиму работы.

Отвечать на Ping - указание конфигурируемому ФПСУ-IP отвечать на ICMP (ECHO) пакеты, направленные от IP-адреса описываемого абонента в IP-адреса портов ФПСУ-IP. Отметка (разрешение отвечать на запросы) производится по нажатию клавиши *<Пробел>*. Необходимо заметить, что 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 который 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.

Повторное описание абонента с IP-адресом, совпадающим с ранее определенным адресом, недопустимо (подсистема конфигурирования выдаст соответствующее предупреждение).

9. 4. 2. Описание абонента «Подсеть»

Записи типа «Подсеть» предназначены для указания группового адреса абонентов (IP адреса и маски подсети, которой они принадлежат) со стороны данного порта, которым будет разрешена передача данных абонентам противоположного и/или данного порта в случае соблюдения совокупности правил фильтрации, определенной для них администратором - фильтрации по IP-адресам, режимам работы с партнером и правилам трафика межсетевого экрана (см. раздел «Параметры доступа, правила трафика межсетевого экрана»).

Отдельным хостам из этой подсети можно назначить права, отличающиеся от прав

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.

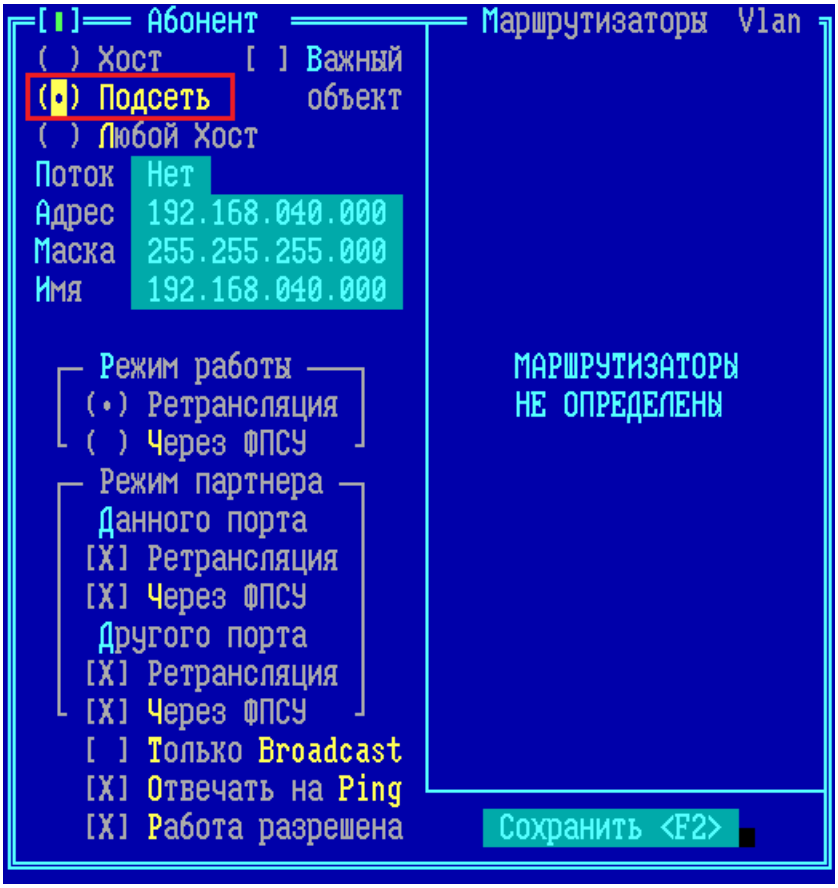


Рисунок 202 - Описание абонента ФПСУ-IP типа «Подсеть»

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 8 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.

Пояснение работы параметра «Только Broadcast»

Существует сетевая конфигурация, которую необходимо рассмотреть отдельно, при которой параметры абонентов для ФПСУ-IP настраиваются особым образом. Предположим, что со стороны одного порта ФПСУ-IP находится IP-подсеть, а со стороны другого порта - один или несколько хостов с адресами, входящими в диапазон адресов этой подсети, которые должны получать широковещательные IP-пакеты из этой IP-подсети. В таком случае со стороны первого порта нужно было бы описать групповой адрес подсети, а со стороны второго - индивидуальные адреса хостов или групповой адрес части данной IP-подсети, находящейся с этой стороны.

Однако при таком описании абоненты смогут обмениваться только индивидуальными IP-пакетами, а широковещательные пакеты от абонентов первого порта абонентам второго порта не смогут быть переданы через ФПСУ-IP. Для обработки подобной ситуации предусмотрена следующая последовательность установок:

- со стороны первого порта описывается групповой адрес IP-подсети. При этом для этой записи устанавливается режим «Только Broadcast», а из всех установок доступной будет только установка «Режим работы»;
- со стороны второго порта создается отдельная запись типа «Подсеть», содержащая тот же групповой адрес (это единственный возможный случай повторного описания адреса).

Необходимо отметить, что в данном случае ФПСУ-IP не будет отвечать на ARP-запросы, направленные в адрес абонентов, входящих в фиктивную запись.

9. 4. 3. Описание абонента «Любой Хост»

Специальный адрес «Любой Хост» может быть описан только один раз со стороны любого порта и предназначен для реализации возможности обмена пакетами через ФПСУ-IP с абонентами произвольных IP-адресов, принадлежащими всей сети Internet/Intranet. Использование или неиспользование адреса этого типа определяется политикой безопасности организации.

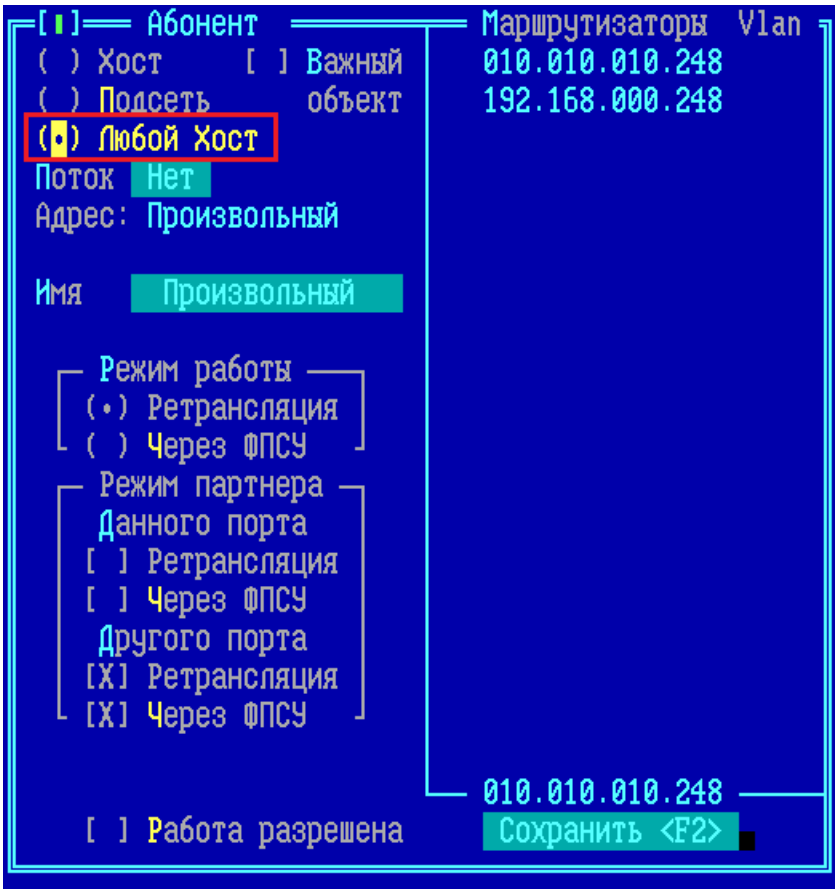


Рисунок 203 - Абонент «Любой Хост», режим «Ретрансляция»

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.

9. 4. 4. Работа со списком абонентов

Работа со списком абонентов осуществляется с помощью «горячих» клавиш.

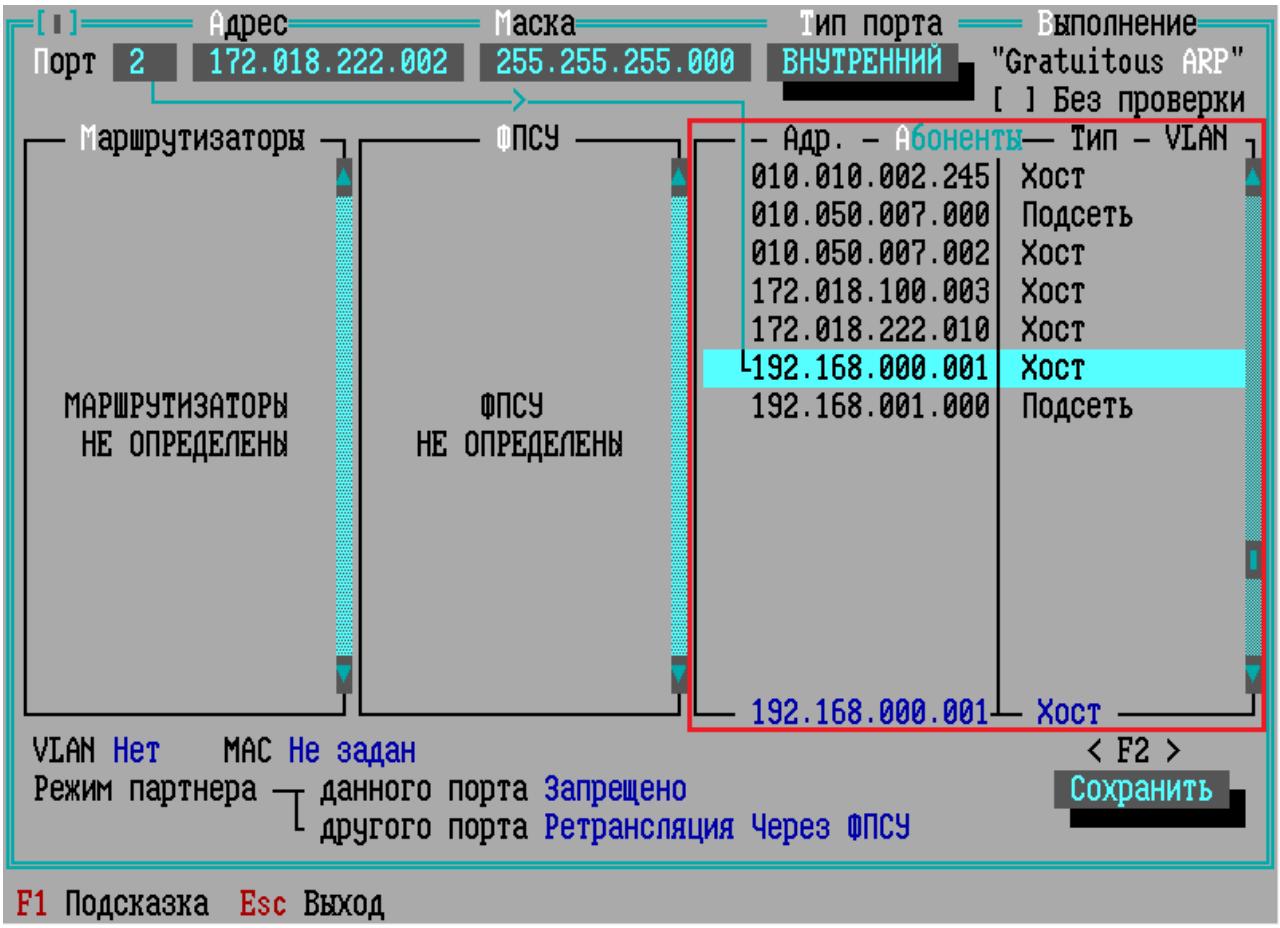


Рисунок 204 - Абоненты порта ФПСУ-IP

Переход к списку туннелей ФПСУ-IP осуществляется клавишей <←> или сочетанием клавиш <*Shift+Tab*>.

Если абонент указан, как находящийся за маршрутизатором, переход к маршрутизатору осуществляется клавишей <←>.

Для сортировки списка абонентов по имени нажмите сочетание клавиш <*Alt+N*>.

Рисунок 205 - Сортировка списка абонентов по имени

Для сортировки списка абонентов по IP-адресу нажмите сочетание клавиш <*Alt+A*>.

Поиск абонента в списке ведётся по клавише <*Alt+F*>.

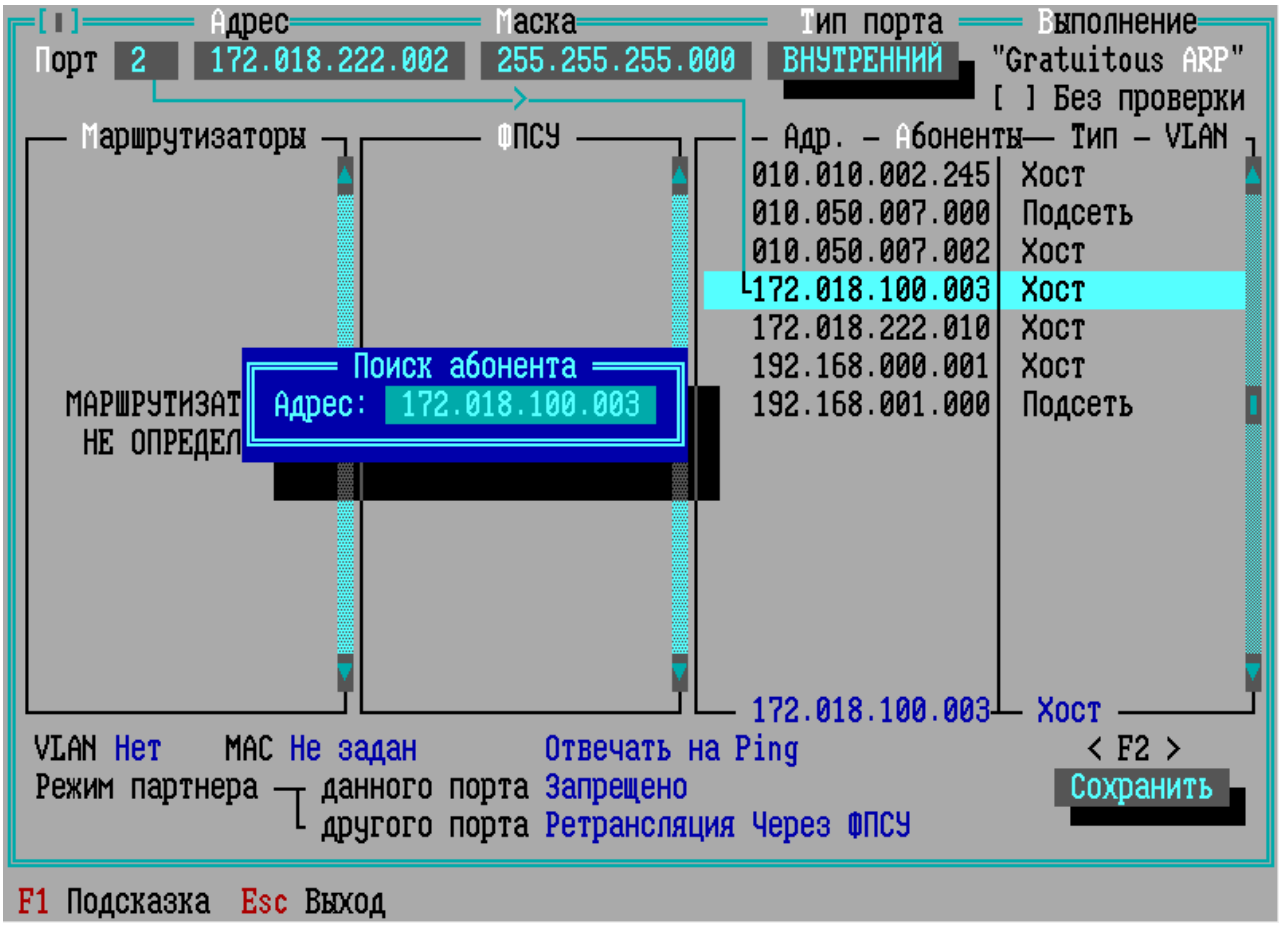


Рисунок 206 - Поиск абонента в списке

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.

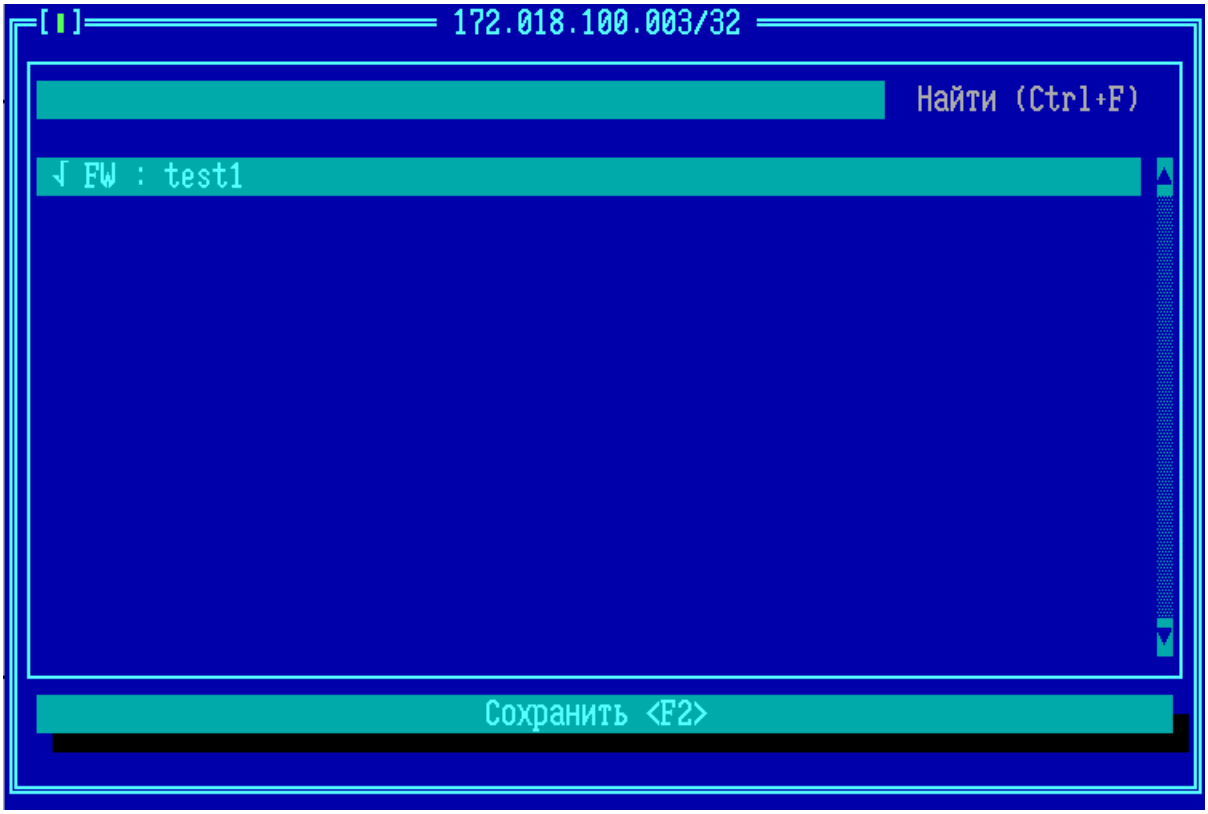


Рисунок 207 - Поиск абонента в правилах МЭ

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.

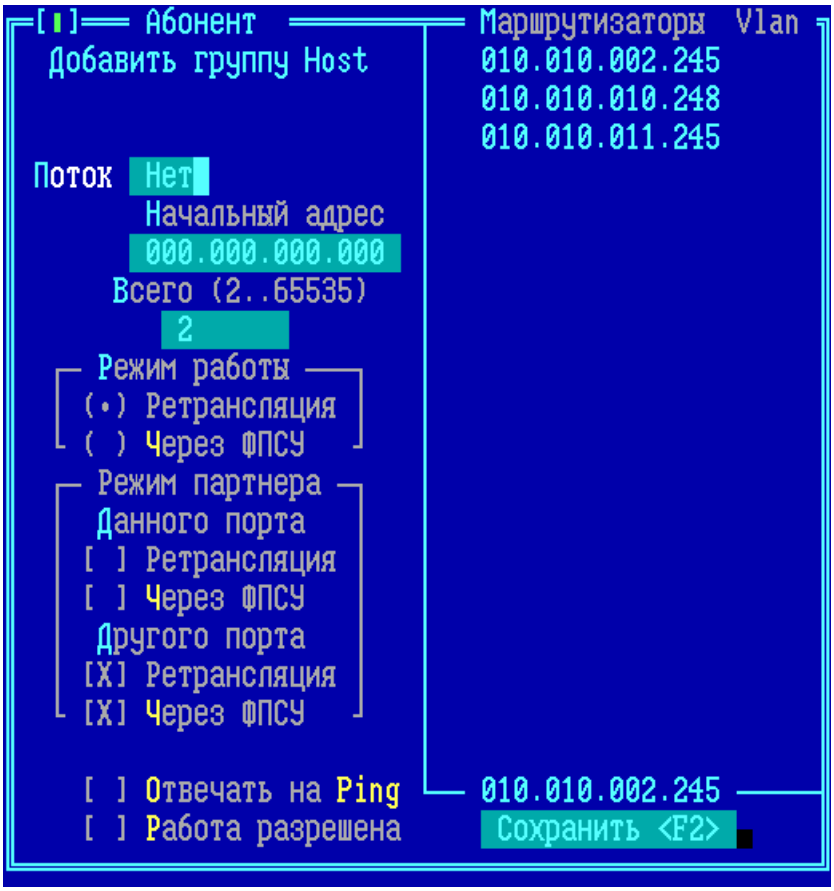


Рисунок 208 - Окно добавления группы описателей типа «хост»

В поле «Всего (2…)» устанавливается количество описателей хост-абонентов с одинаковыми параметрами, которые будут добавлены в список при выполнении команды «*Сохранить*».

Удаление абонентов

Для удаления описателя абонента из списка, выделите его курсором, нажмите клавишу <*Del*> и подтвердите выполнение команды.

Для удаления нескольких абонентов одновременно, находясь курсором в списке абонентов, нажмите сочетание клавиш <*Ctrl+Del*> или <*Ctrl+D*>. Появится окно со списком абонентов порта.

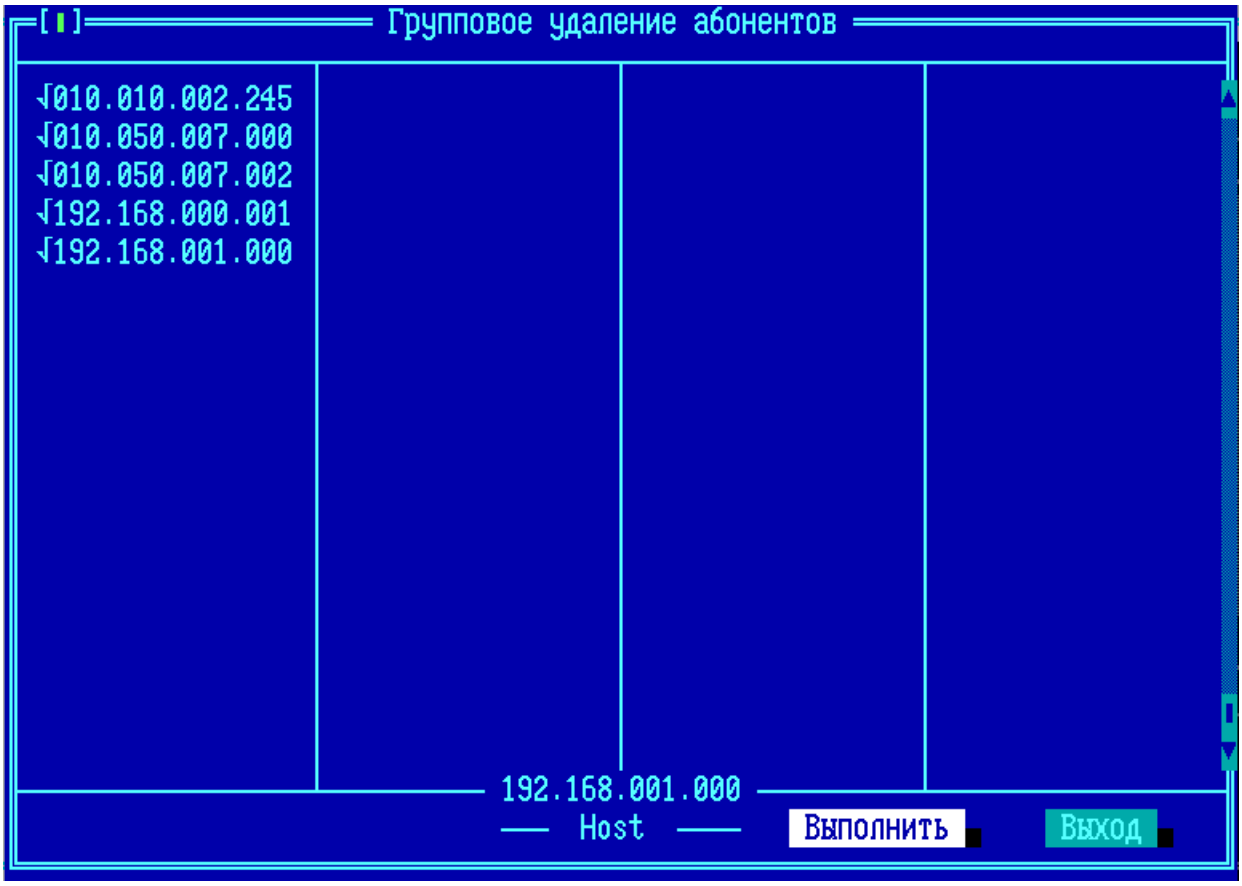


Рисунок 209 - Групповое удаление абонентов

При нажатии кнопки *«Выполнить»*, все отмеченные описатели будут удалены. Для пометки знаком «√» 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.

10. Параметры доступа, правила трафика межсетевого экрана

В разделе «Параметры доступа» меню конфигурации ФПСУ-IP находятся опциональные настройки межсетевого экрана, позволяющие администратору вести фильтрацию передаваемого трафика по ряду критериев.

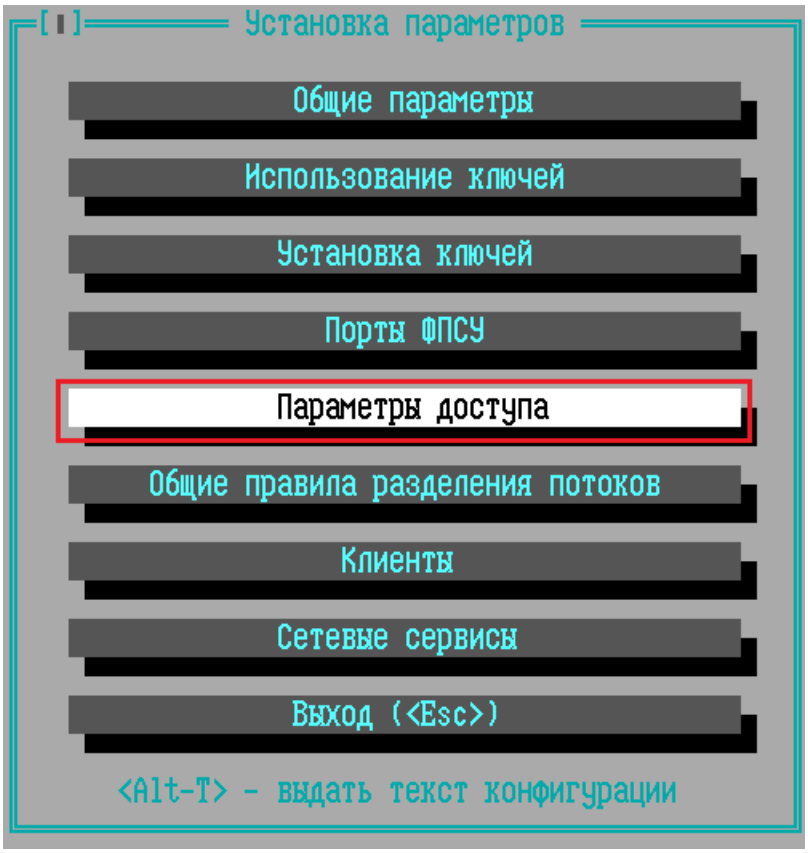


Рисунок 210 - Меню конфигурации ФПСУ-IP

Настраиваемые здесь правила доступа работают в дополнение к правилам маршрутизации, заданных администратором в пункте главного меню «Порты ФПСУ». Любой сетевой объект, используемый в интерфейсе параметров доступа, должен быть сначала описан в интерфейсе «Порты ФПСУ».

Администратор ФПСУ-IP может создавать правила передачи трафика, применяемые к одному и/или нескольким IP-адресам, одной и/или нескольким подсетям и логическим группам IP-адресов. Таким образом, трафик абонентов маршрутизации может быть логически разделен, например, по функциональному признаку, и для каждого правила могут быть установлены свои ограничения.

Для каждого создаваемого правила указываются сетевые объекты, к которым это правило применяется (IP-адреса, группы IP-адресов, ФПСУ-IP/Клиенты). Для правила могут

быть указаны диапазоны времени разрешенной работы объектов, к которым это правило применяется, а также разрешенные протоколы передачи данных. Правило может быть разрешительным (Accept) или запретительным (Reject, Drop).

Межсетевым экраном отслеживается инициатор установления соединения, возвратный трафик разрешается.

Правила располагаются в списке правил трафика по приоритету, и в случае возникновения взаимоисключающих настроек, будет работать правило, находящееся выше по списку.

ВНИМАНИЕ! По умолчанию, правила дополнительной фильтрации выключены, и трафик абонентов передается без дополнительных проверок. После создания администратором ФПСУ-IP как минимум одного правила трафика (см. пункт «Правила трафика»), активируется также правило по умолчанию «**Block other traffic»**, запрещающее передачу пакетов, не разрешенных хотя бы одним из правил дополнительной фильтрации. Правило по умолчанию «**Block other traffic»** всегда имеет самый низкий приоритет.

После нажатия кнопки главного меню «Параметры доступа» происходит переход в подменю «Настройки» правил дополнительной фильтрации.

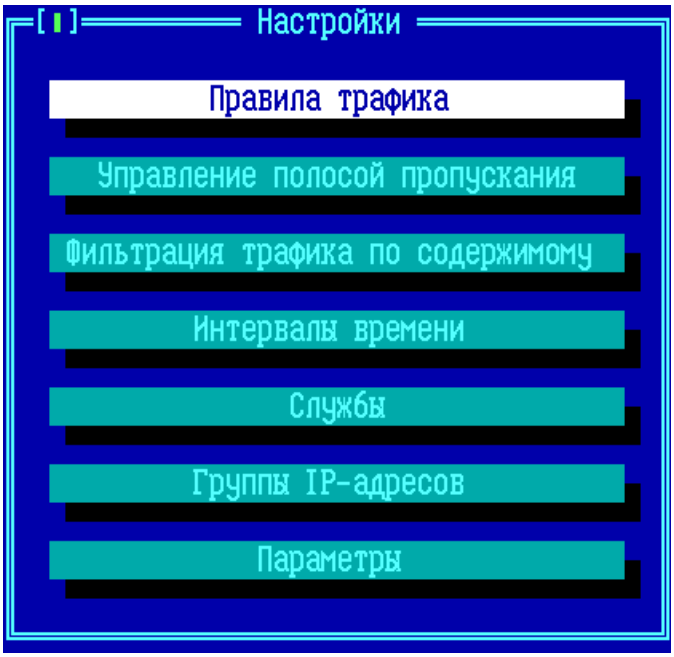


Рисунок 211 - Команды меню «Параметры доступа»

Меню «Параметры доступа» правил дополнительной фильтрации содержит следующие команды:

- «Правила трафика» — переход в основное окно управления списком существующих

правил фильтрации межсетевого экрана, подробнее см. пункт «Правила трафика»;

- «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*>.

10. 1. Правила трафика

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

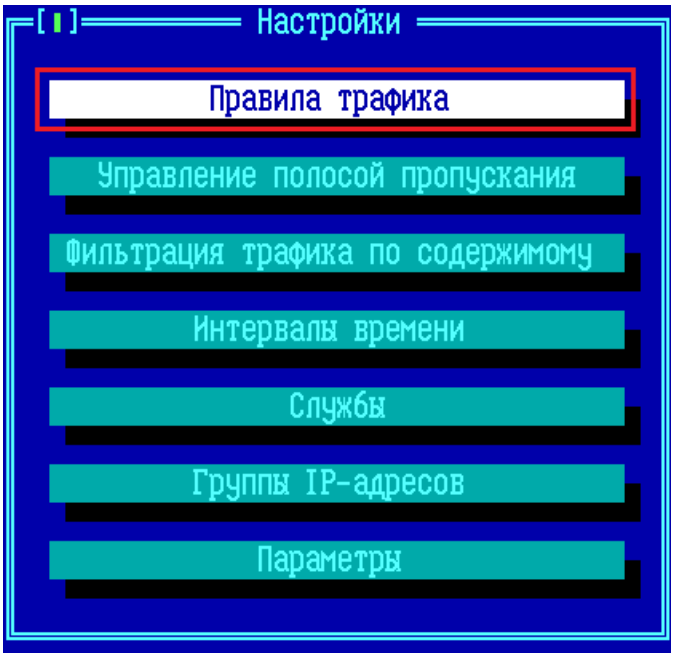


Рисунок 212 - Меню «Параметры доступа» → «Правила трафика»

После выполнения команды «Правила трафика», происходит переход в окно, где отображен список используемых на ФПСУ-IP правил дополнительной фильтрации. Правило по умолчанию — **Block other traffic —** носит запретительный характер, указывая сбрасывать без оповещения (Drop) все пакеты всех абонентов, для которых не создано ни одного разрешительного правила.

ВНИМАНИЕ! Если ни один администратор ФПСУ-IP не добавлял в список ни одного правила, то есть список правил пуст, то ограничений на передачу трафика нет, в том числе выключено и правило по умолчанию **Block other traffic**. В этом случае все пакеты передаются в соответствии с маршрутизацией, заданной в пункте «Порты ФПСУ».

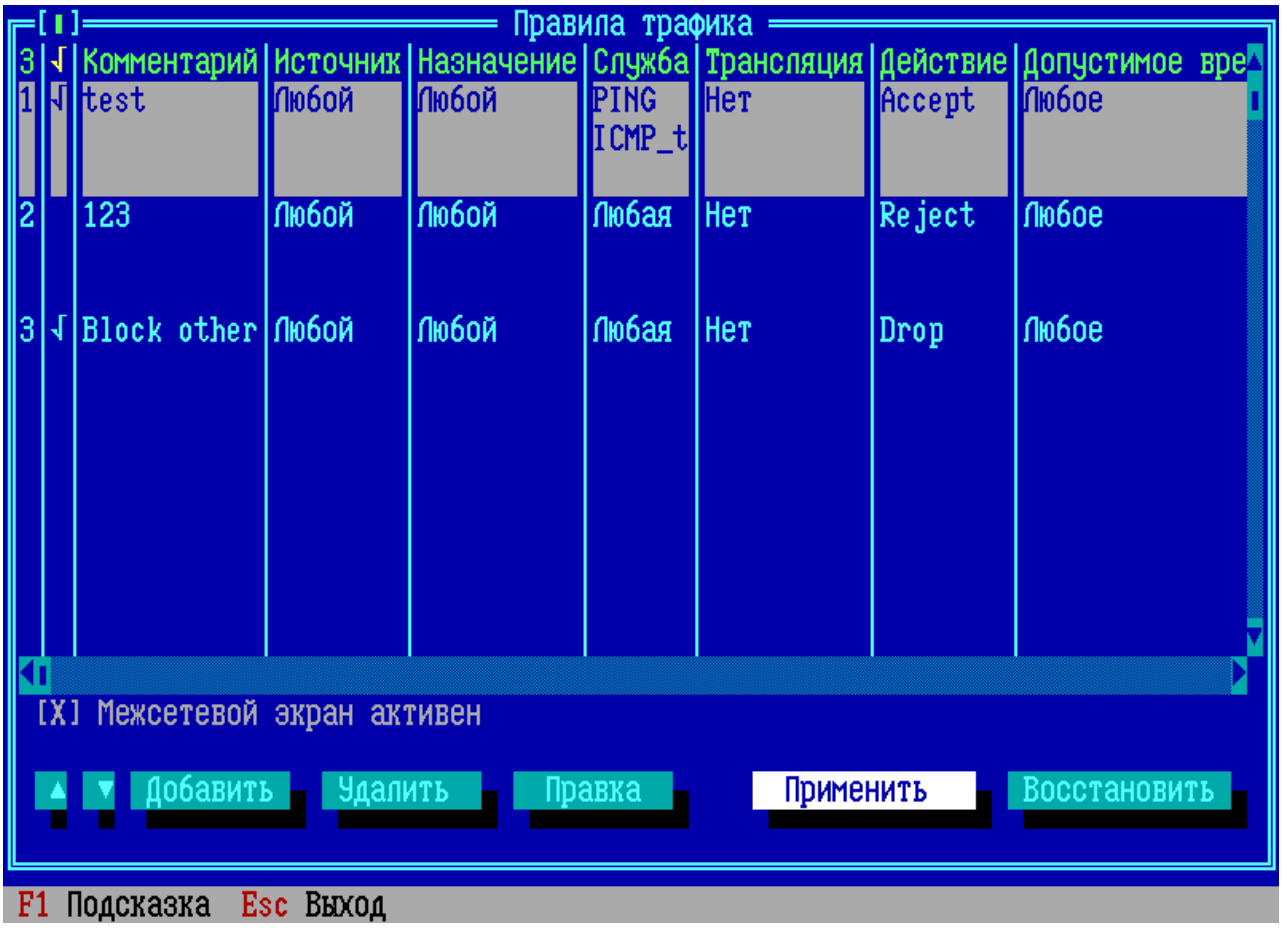


Рисунок 213 - Список правил трафика на ФПСУ-IP

Правила трафика работают в зависимости от направления передачи пакета. В нем в качестве критериев срабатывания фильтрации указываются разрешенные IP-адреса отправителей пакетов, IP-адреса получателей пакетов, разрешенный протокол передачи (***служба*** в терминологии интерфейса дополнительной фильтрации ФПСУ-IP), диапазон разрешенного времени работы, и основное действие с пакетом: разрешить передачу (Accept) или запретить (Drop или Reject).

Флаг «*Межсетевой экран активен*» включает работу дополнительных правил фильтрации. Без установленного флага работают только основные правила маршрутизации списка абонентов, заданные администратором в пункте главного меню «Порты ФПСУ».

Для внесения изменений в конфигурацию без выхода из окна, нажмите клавишу «*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 «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 <↓>, 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* ↓>.

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

10. 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 «↓» в конце настраиваемого поля обозначает наличие выпадающего списка, вызываемого нажатием клавиши *<Пробел>* при установленном на поле курсоре.

Вкладка **Общие** содержит следующие настраиваемые опции:

Комментарий — обязательное произвольное текстовое поле для пояснения правила.

Действие — обязательное правило, определяющее, как поступить с передаваемым пакетом. В выпадающем меню могут быть выбраны следующие варианты основного действия:

- *Drop* — действие по умолчанию, пакет данных будет сброшен, ICMP-оповещение об отказе передачи пакета не будет передано отправителю;
- *Reject* — пакет данных будет сброшен, отправителю будет передано ICMP-оповещение об отказе передачи пакета;
- *Accept* — пакет данных будет передан по назначению.

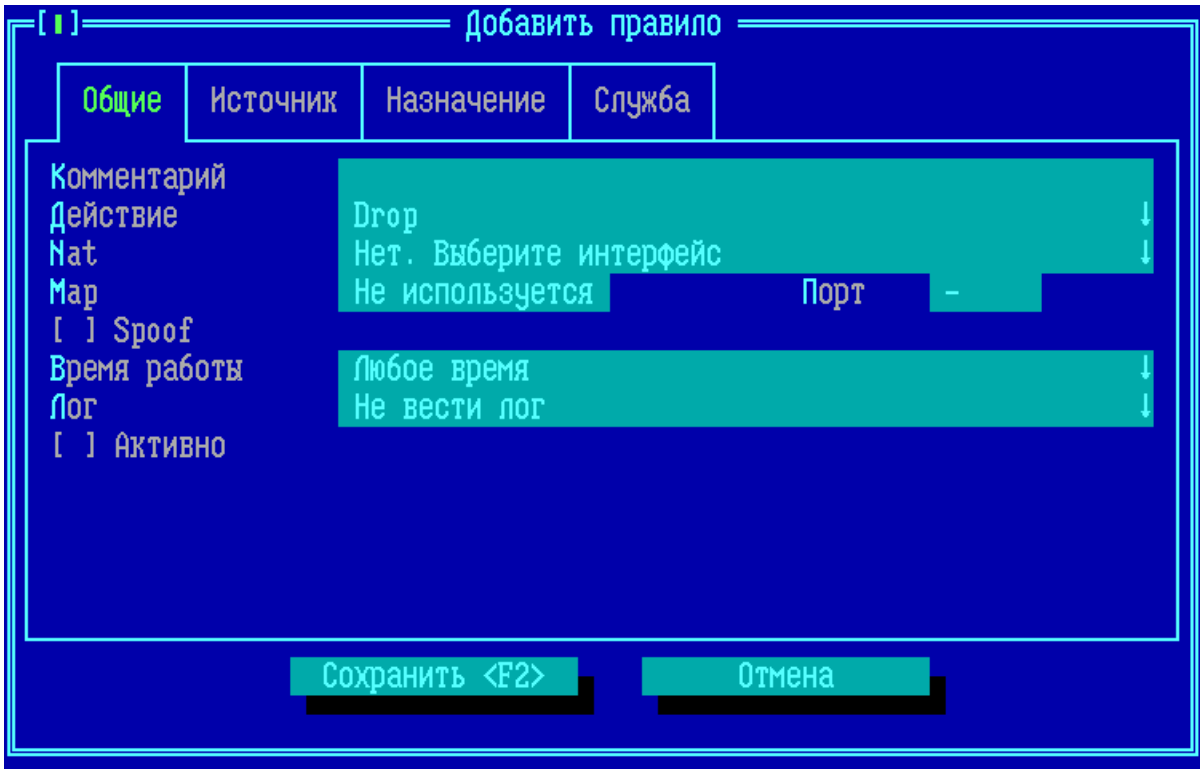


Рисунок 214 - Добавление нового правила трафика

Кроме основного действия с пакетом, в правиле могут быть сконфигурированы и использованы дополнительные опции.

NAT. Правило, включающее в себя дополнительную опцию трансляции адресов при

передаче данных от источника к получателю. В поле опции (где по умолчанию стоит текст «*Нет. Выберите интерфейс*») с помощью выпадающего списка следует указать, какой из портов ФПСУ-IP будет использован для трансляции адреса источника при передаче пакета получателю.

MAP, Порт. Правило, включающее в себя дополнительную опцию MAP, позволяет перенаправить полученные ФПСУ-IP пакеты, где получателем пакета являются собственные IP-адреса ФПСУ-IP (при этом во вкладке «Назначение» IP-адрес порта ФПСУ-IP должен быть добавлен как объект «Интерфейс»), на другой, указанный в поле этой опции, IP-адрес. В поле ***Порт*** указывается номер порта протоколов TCP/UDP. Если в поле ***Порт*** установлено отличное от нуля значение, то трафик будет перенаправляться, изменяя порт назначения транспортного протокола на указанный номер. Если в поле ***Порт*** опции ***MAP*** стоит значение 0, то трафик на указанный в поле ***MAP*** IP-адрес будет перенаправлен без изменения порта назначения.

Примеры применения правил NAT и MAP можно посмотреть в пунктах «Использование ФПСУ-IP для контроля доступа в интернет с NAT», «Использование ФПСУ-IP для объединения офисов с одинаковой внутренней адресацией», «Использование ФПСУ-IP для смены порта назначения трафика, направляемого в адрес абонента», «Использование ФПСУ-IP для балансировки нагрузки на порты внутреннего сервера».

Spoof – опция для сетевых соединений на медленных каналах передачи данных с большими задержками (спутник, например). Если задействована опция подтверждения получения данных ACK, то ФПСУ-IP отвечает отправителю самостоятельно, не дожидаясь подтверждения от получателя сегмента.

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* или *Вести лог, писать заголовки пакетов*. Значение по умолчанию - *Не вести лог*.

Для того, чтобы все указанные в правиле настройки после сохранения были задействованы, следует перед выходом установить флаг *«Активно»*.

Помимо общих настроек, можно указать параметры на других вкладках создаваемого правила. Перемещение между вкладками осуществляется установлением курсора на вкладку

и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

10. 1. 2. Вкладки «Источник» и «Назначение» правил трафика

Правило трафика применяется только к тем пакетам, IP-адреса источника и назначения которых указаны в соответствующих вкладках. Исключение: если во вкладках **Источник** и **Назначение** нет ни одной записи (список пуст), то правило трафика применяется ко всем пакетам.

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.

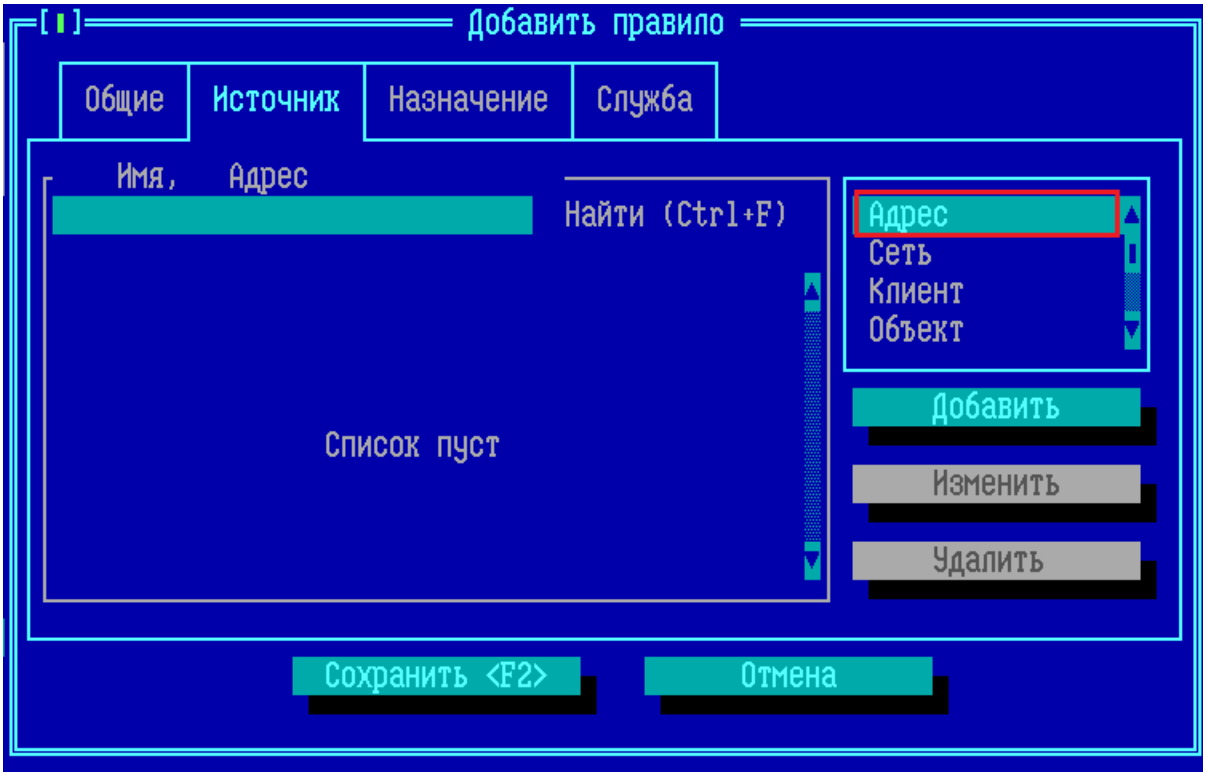


Рисунок 215 - Назначение источников для правила трафика

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

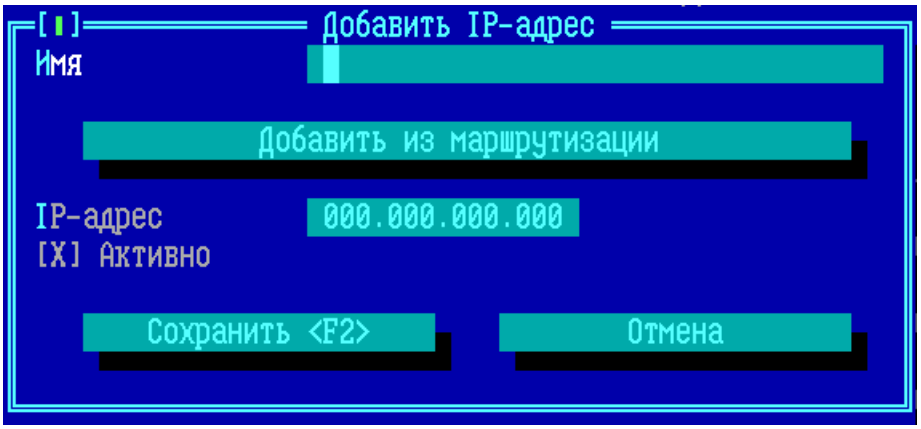


Рисунок 216 - Команда «Добавить» для отдельного IP-адреса

Из выпадающего меню, открывающегося по команде *«Добавить из маршрутизации»*, курсором может быть выбран ранее описанный на «Портах ФПСУ» сетевой объект:

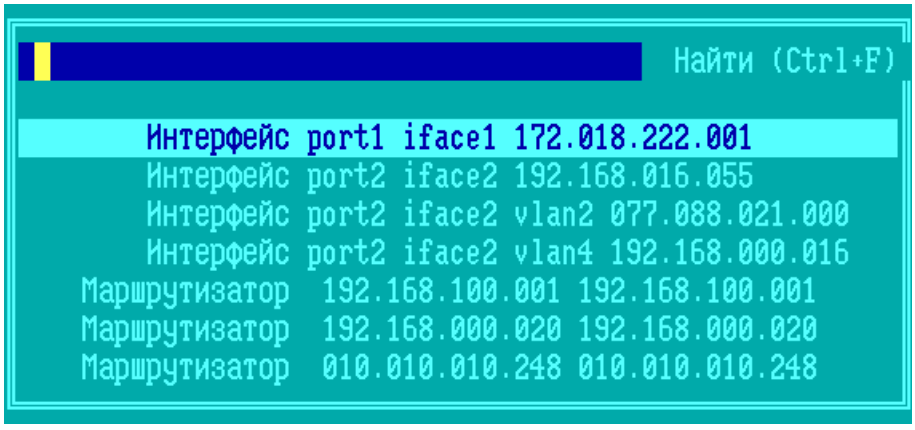


Рисунок 217 - Список найденных объектов в маршрутизации (Портах ФПСУ)

Перемещение по списку осуществляется клавишами <↑> и <↓>, выбор осуществляется нажатием клавиши <*Enter*> или <*Пробел*> Например, при выборе объекта «Абонент 010.010.010.248 010.010.010.248», интерфейс добавления IP-адреса автоматически заполнится данными, взятыми из списка маршрутизации:

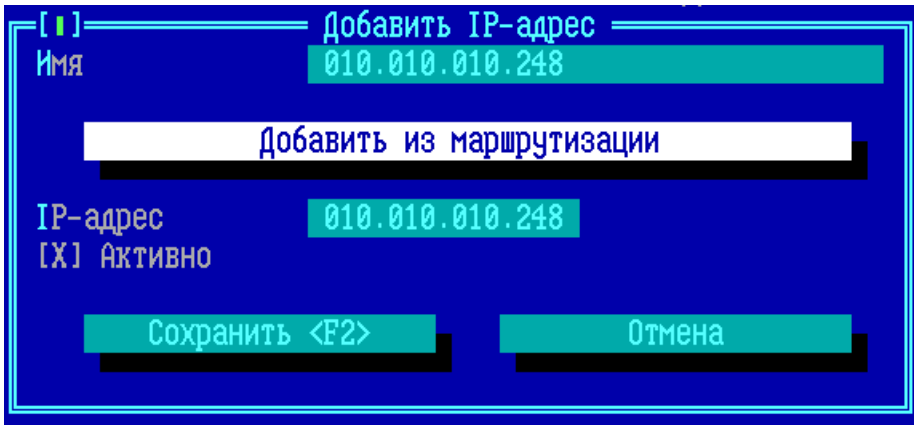


Рисунок 218 - Данные взяты из списка маршрутизации

ВНИМАНИЕ! Если флаг *«Активно»* выключен, то IP-адрес будет добавлен в список, но правило трафика по нему отрабатывать не будет.

После нажатия клавиши *<F2>* или выполнении команды *«Сохранить <F2>»*, IP-адрес будет добавлен в список вкладки **Источник**:

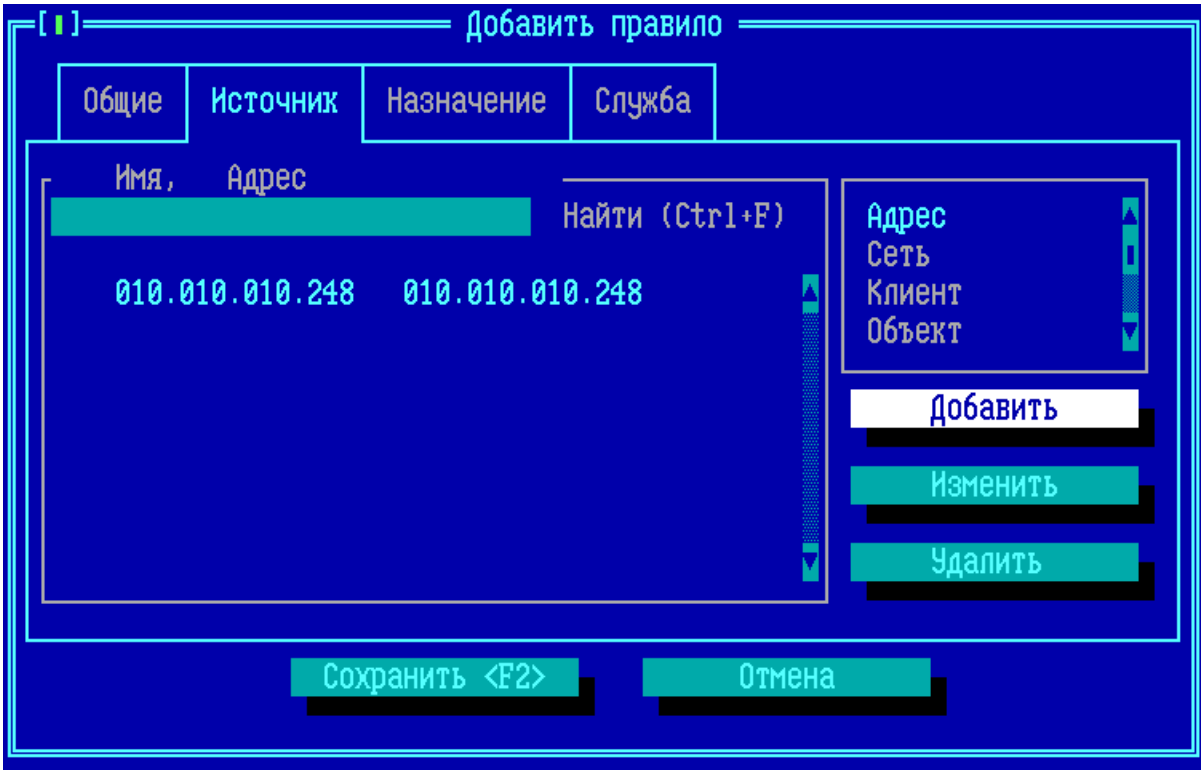


Рисунок 219 - В список «Источник» правила трафика добавлена новая запись

Сеть — для добавления в список обрабатываемых правилом источников подсети IP-адресов, следует установить курсор на строке «Сеть», затем по нажатию клавиши *<Tab>* перейти на кнопку *«Добавить»* и нажать *<Enter>*. Подсеть должна быть выбрана из

диапазона подсетей, прописанных в маршрутизации на портах ФПСУ-IP, либо входить в такую.

Клиент — для добавления в список обрабатываемых правилом источников трафика данных, поступающих от ФПСУ-IP/Клиентов, следует установить курсор на строке «Клиент», затем по нажатию клавиши <*Tab*> перейти на кнопку «*Добавить*» и нажать <*Enter*>. Описатель клиента должен быть выбран из заранее сконфигурированной на ФПСУ-IP группы клиентов зарегистрированной Криптосети.

Объект — в список может быть добавлена заранее созданная логическая группа IP-адресов и подсетей (подробнее см. пункт «Группы IP-адресов»). Для добавления в список обрабатываемых правилом источников трафика от ФПСУ-IP/Клиента, следует установить курсор на строке «Объект», затем по нажатию клавиши <*Tab*> перейти на кнопку «*Добавить*» и нажать <*Enter*>.

Интерфейс — в список обрабатываемых правилом источников передаваемых пакетов может быть выбран один из логических интерфейсов ФПСУ-IP (IP-адрес «Порта ФПСУ» №1 и №2, а также IP-адреса портов ФПСУ-IP, назначенные VLAN). Для добавления в список IP-адреса интерфейса ФПСУ-IP, следует установить курсор на строке «Интерфейс», затем по нажатию клавиши <*Tab*> перейти на кнопку «*Добавить*» и нажать <*Enter*>.

ВНИМАНИЕ! Суммарно в правилах МЭ может быть описано не более 1024*1024 записей в источнике.

Каждая запись списка вкладок **Источник** или **Назначение** может быть временно исключена из проверяемых фильтров, при снятии включенного по умолчанию флага «*Активно*».

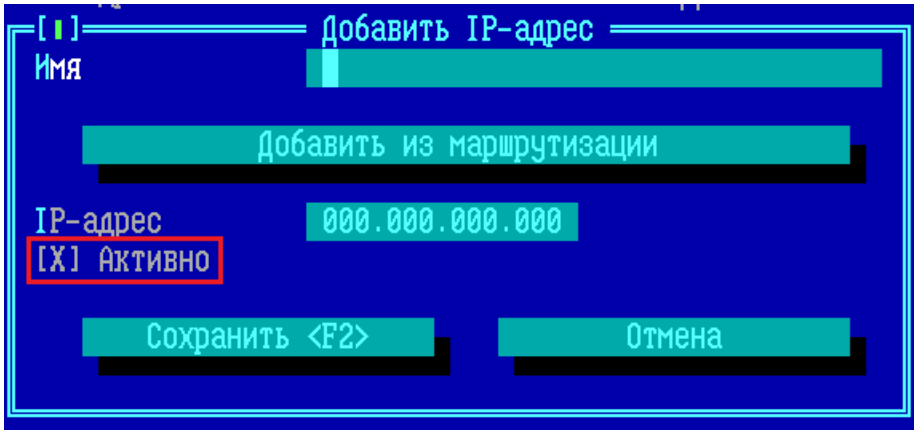


Рисунок 220 - Активизация добавленного адреса

10. 1. 3. Службы в правилах трафика

Правило трафика по умолчанию применяется ко всем пакетам, источник и назначение 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:

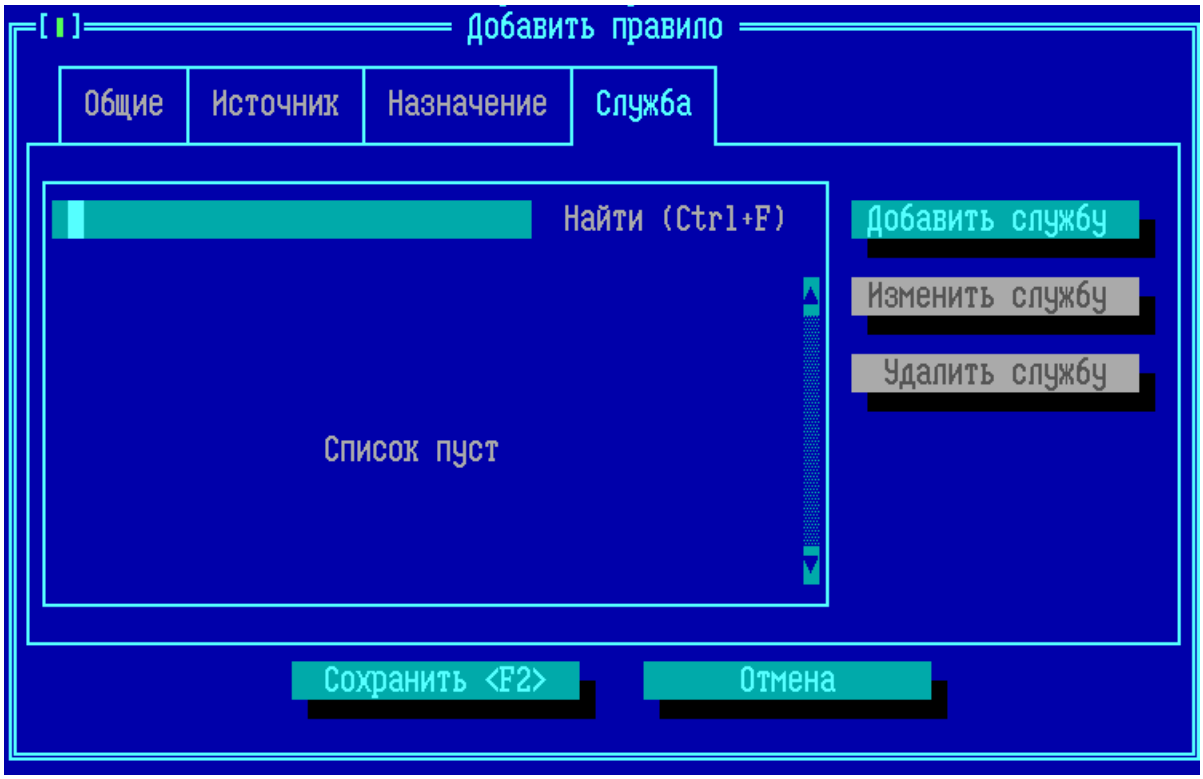


Рисунок 221 - Пустой список служб у нового добавляемого правила

Для внесения новой службы в список, нажмите кнопку *«Добавить службу»* и выберите из появившегося перечня заранее созданных служб (на примере в конфигурации ФПСУ-IP заранее создана служба с именем «TCP 80»):

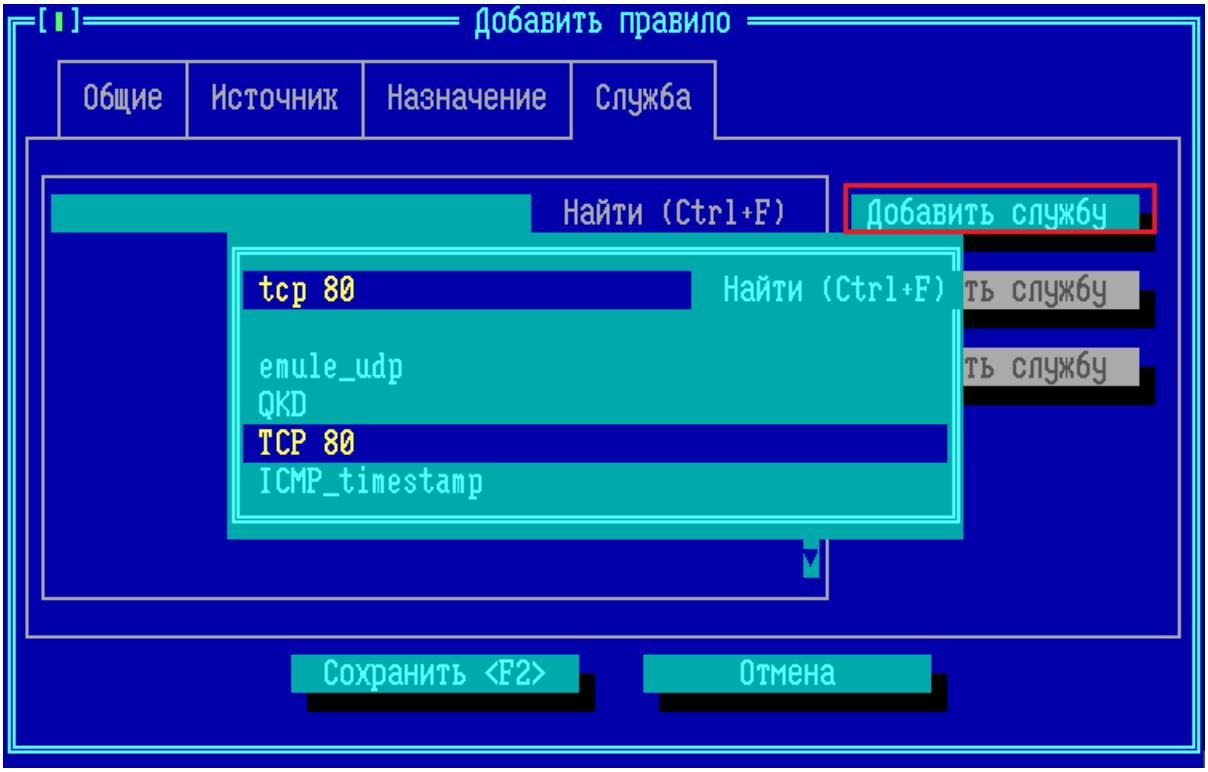


Рисунок 222 - Добавление службы в правило трафика

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:

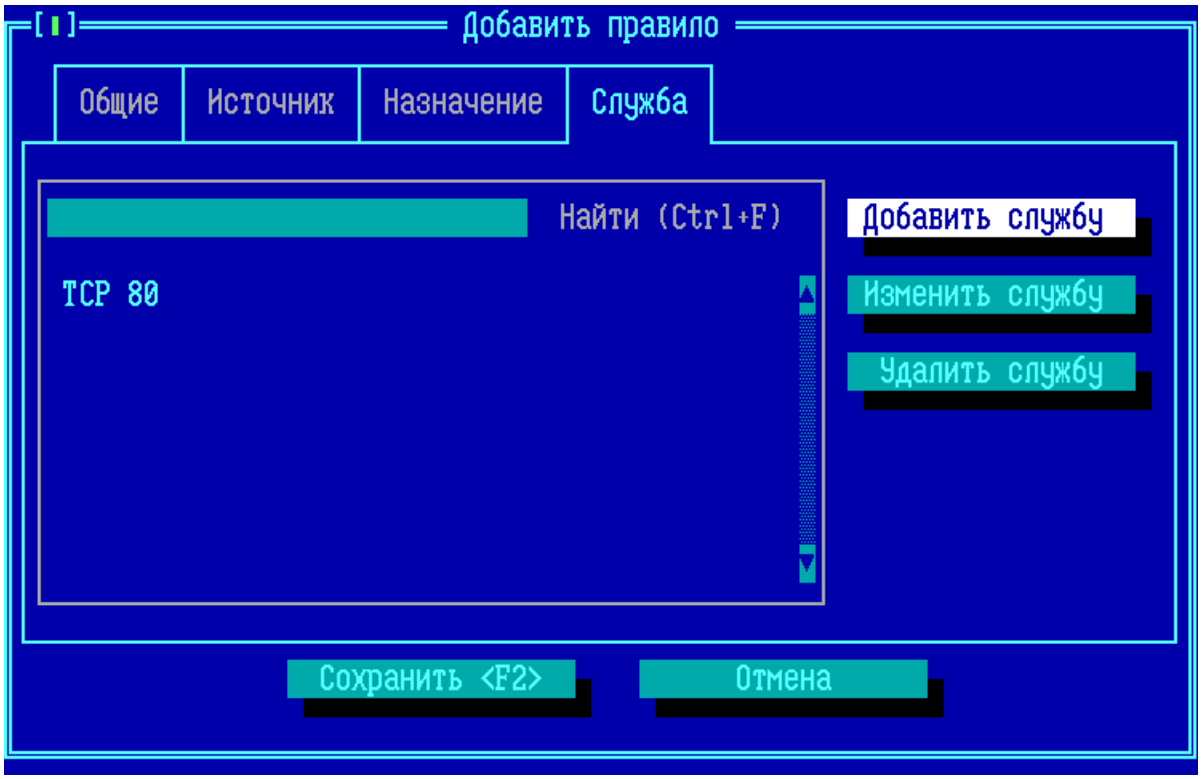


Рисунок 223 - Вкладка со списком служб правила трафика

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»):

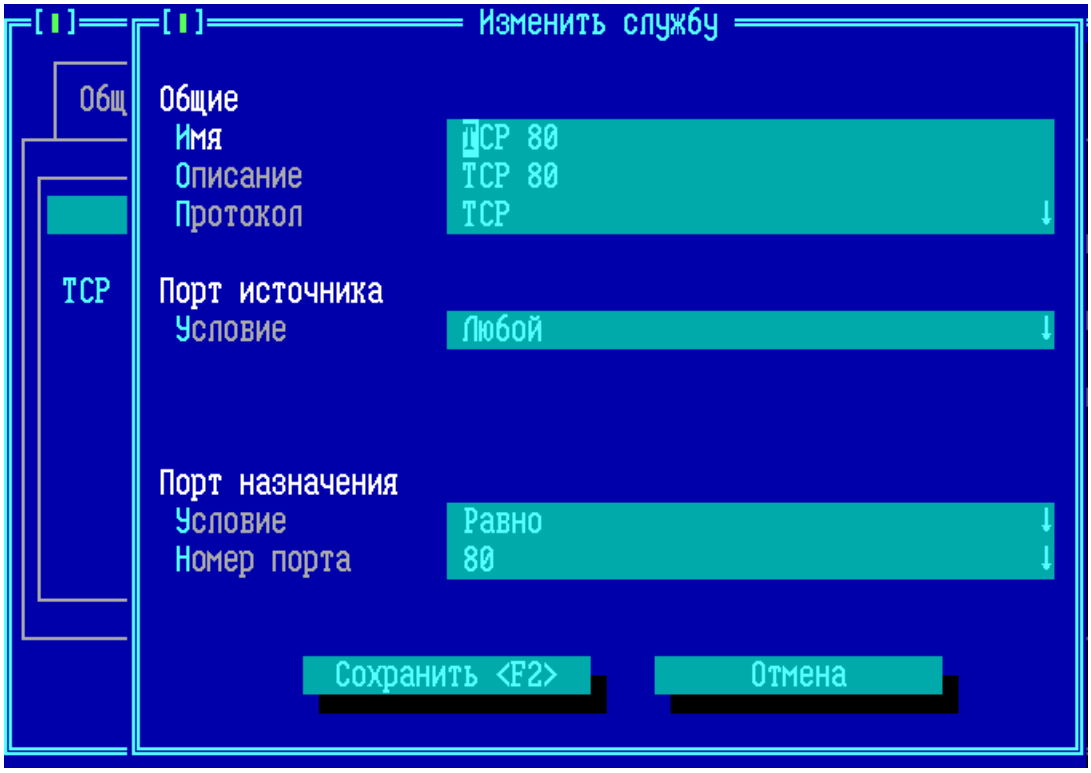


Рисунок 224 - Изменение службы из окна настроек правила доступа

10. 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 225 - Команда «Службы» настроек правил доступа

В списке служб по умолчанию отображаются шаблоны популярных служб.

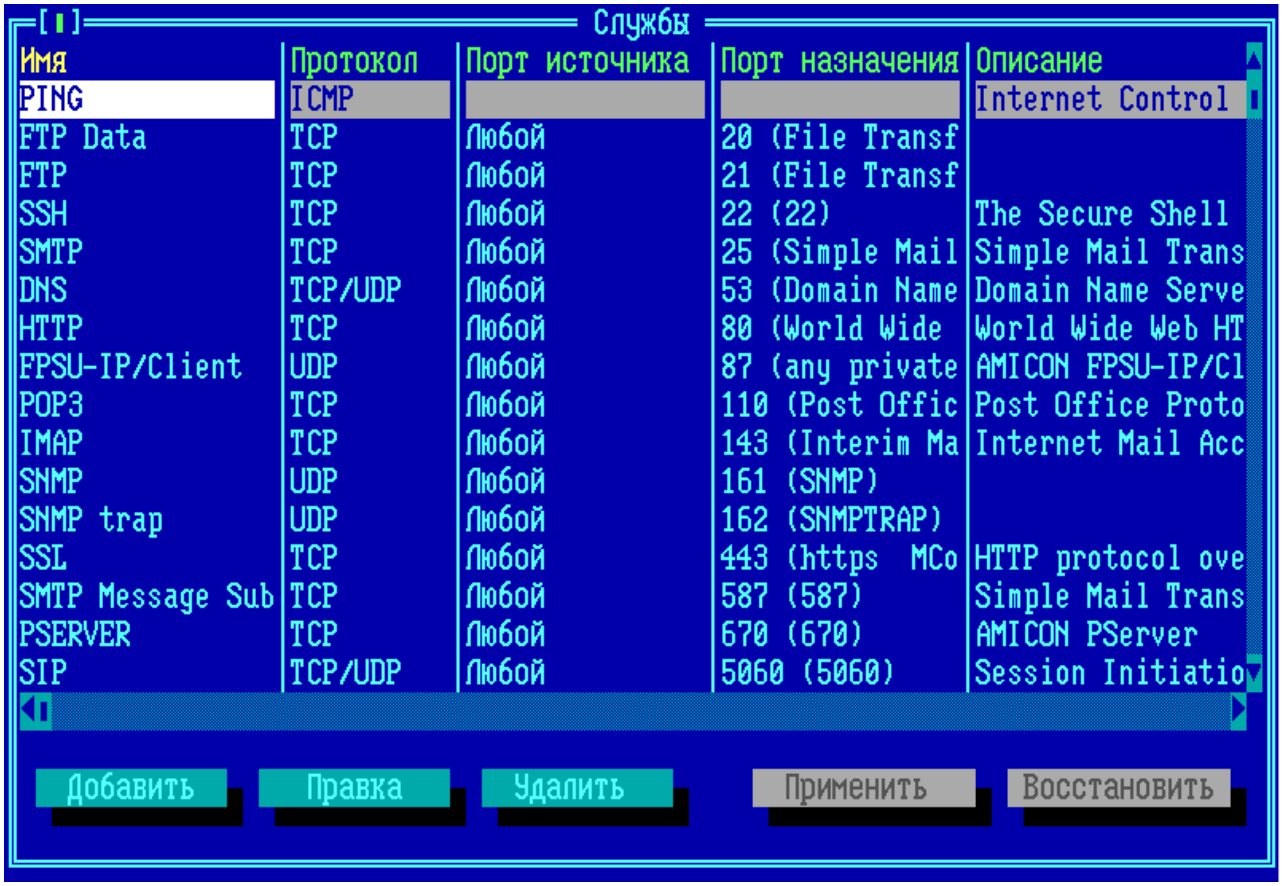


Рисунок 226 - Список служб

Каждая создаваемая служба может быть привязана к определенному протоколу передачи данных — IP, ICMP, TCP и/или UDP, и номеру или порту используемого протокола. С помощью служб, выбираемых при создании правила трафика (пункт «Правила трафика»), можно гибче управлять разрешениями или запретами передаваемых данных, разрешая или запрещая к передаче не весь трафик между абонентами, а только тот, который использует указанные в службах протоколы.

Для создания новой службы нажмите кнопку «*Добавить*» или клавишу <*Ins*>. По умолчанию, интерфейс предлагает создать службу, привязанную к протоколу TCP, этот выбор по умолчанию можно далее поменять.

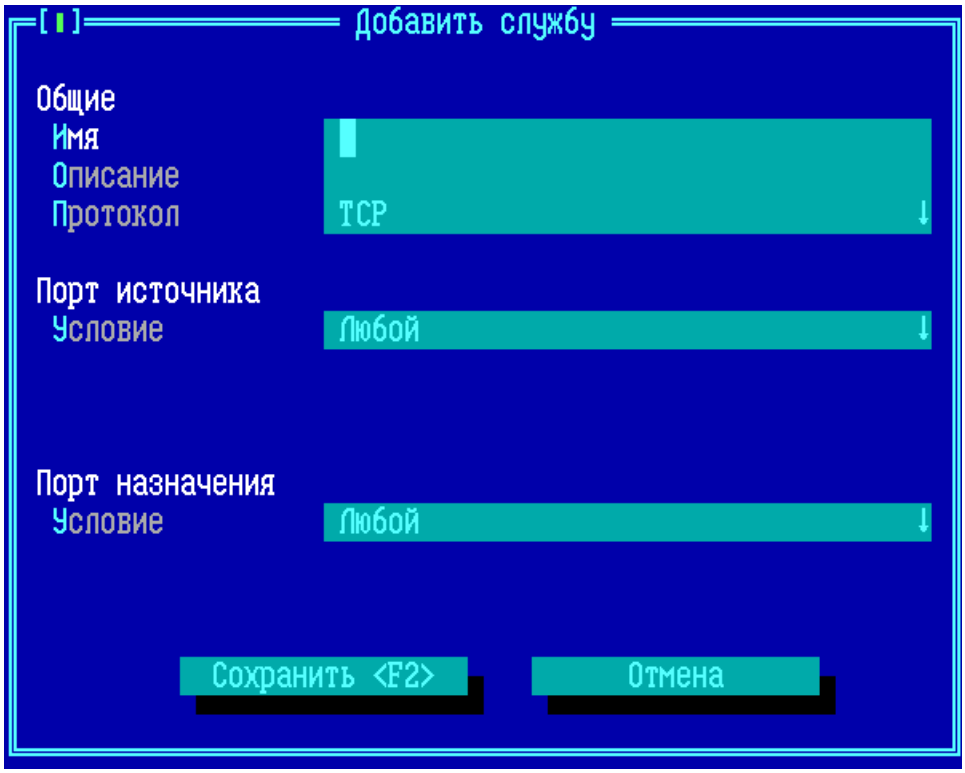


Рисунок 227 - Добавление службы в список

В открывшемся окне указываются следующие параметры службы:

Имя — обязательный параметр, символьное название службы. Это имя будет потом использоваться администратором для прикрепления службы к правилу трафика, поэтому стоит выдавать как можно более точное название (например «TCP:80», если правило будет распространяться на протокол TCP, обращающийся к назначению по 80-му порту протокола TCP);

Описание — произвольное текстовое описание службы, опционально;

Протокол — поле выбора из выпадающего списка протокола передачи данных

создаваемой службы. В качестве протокола могут быть выбраны следующие:

- *TCP* – служба ограничивает правило трафиком, передаваемым с помощью протокола Transmission Control Protocol;
- *UDP* – служба ограничивает правило трафиком, передаваемым с помощью протокола User Datagram Protocol;
- *TCP/UDP* – служба ограничивает правило трафиком, передаваемым с помощью протоколов TCP или UDP;
- *ICMP* – служба ограничивает правило трафиком, передаваемым с помощью протокола ICMP (см. пункт «Протокол ICMP в службах»);
- *Другие (IP)* – служба ограничивает правило трафиком, передаваемым с помощью протокола IP;
- *DSCP* – служба ограничивает правило трафиком, указанным в поле приоритета согласно RFC 2474 (значение от 0 до 63);
- *RAW* – служба, предназначенная для установки произвольных фильтров на основе значений битов заголовков сетевого уровня (пример использования протокола RAW см. пункт «Служба для запрета фрагментированных пакетов»);
- *REGEXP* – служба, предназначенная для установки произвольных фильтров на основе символьных строк и регулярных выражений (подробнее см. пункт «Протокол REGEXP в службах»).

Порт источника и порт назначения — при выборе TCP, UDP или TCP/UDP протоколов, следует определить дополнительные условия: порт отправителя и порт получателя данных. Можно указать отдельный номер порта или диапазон. Установленное значение **любой** обозначает, что служба будет задействована при передаче любого трафика указанного транспортного протокола.

Номер протокола — при выборе значения поля протокола «*Другие*», указывается номер сетевого протокола, привязанный к создаваемой службе. Установленное значение **любой** обозначает, что служба будет задействована при передаче любого IP трафика.

Для внесения произведенных изменений в конфигурацию, нажмите кнопку «*Сохранить*» или клавишу <*F2*>, для выхода без сохранения изменений нажмите кнопку «*Отмена*» или клавишу <*Esc*>.

10. 2. 1. Протокол ICMP в службах

Тип сообщения ICMP **—** при выборе в качестве сетевого протокола ICMP, следует указать, какие именно ICMP-сообщения будут обрабатываться создаваемой службой. Установленное значение «**[X] Любой»** обозначает, что служба включает передачу любого

ICMP трафика, всех типов и кодов.

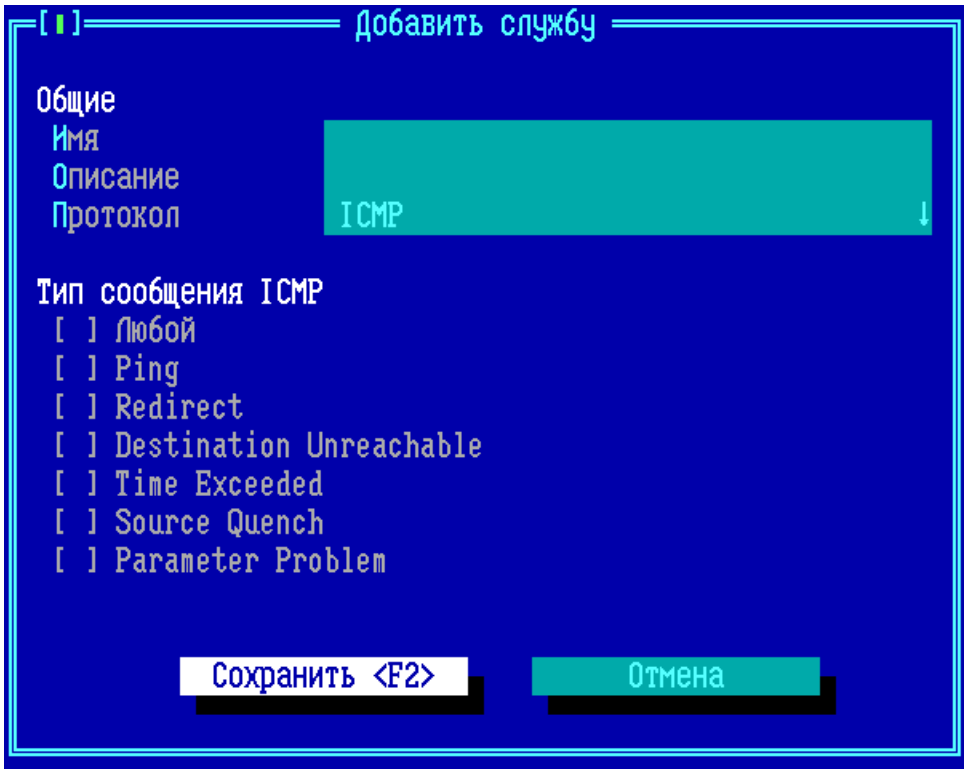


Рисунок 228 - Выбор сообщений ICMP в службе

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.

10. 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».

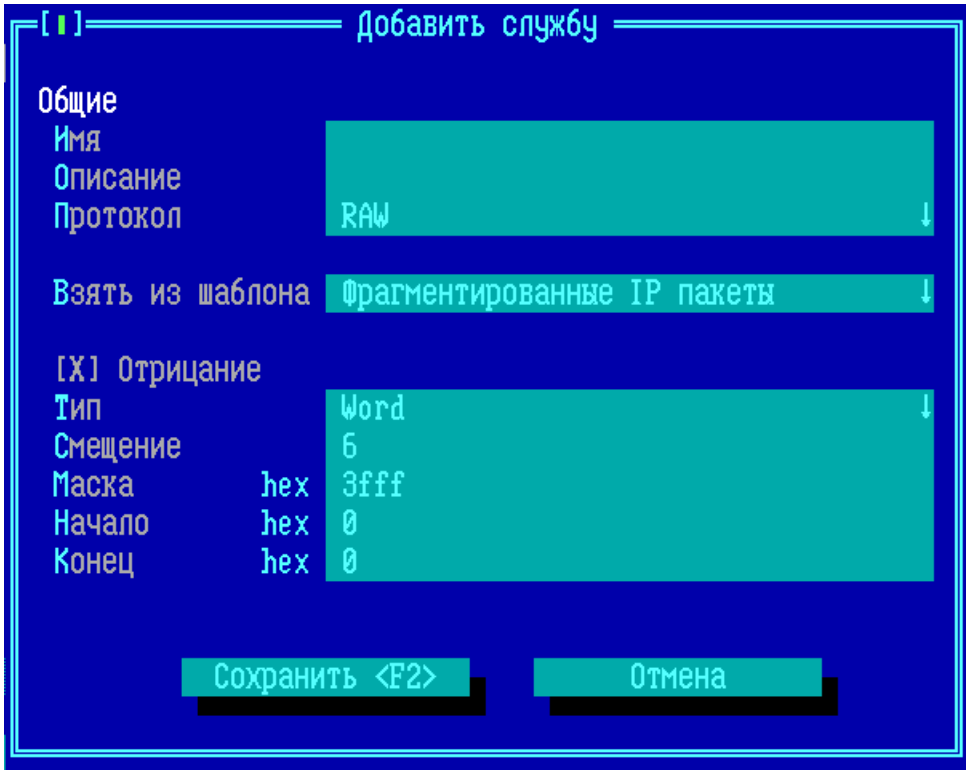


Рисунок 229 - Шаблон для фильтра фрагментированных IP-пакетов

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.

10. 2. 3. Протокол REGEXP в службах

Протокол REGEXP в службах предназначен для установки произвольных фильтров на основе символьных строк и регулярных выражений. Фильтр протокола REGEXP исследует наличие символьной строки или регулярных выражений в передаваемом пакете, начиная с IP-заголовка и заканчивая передаваемыми данными прикладного протокола.

При выборе в добавлении/изменении службы типа протокола REGEXP появляется блок со списком регулярных выражений, по умолчанию пустой:

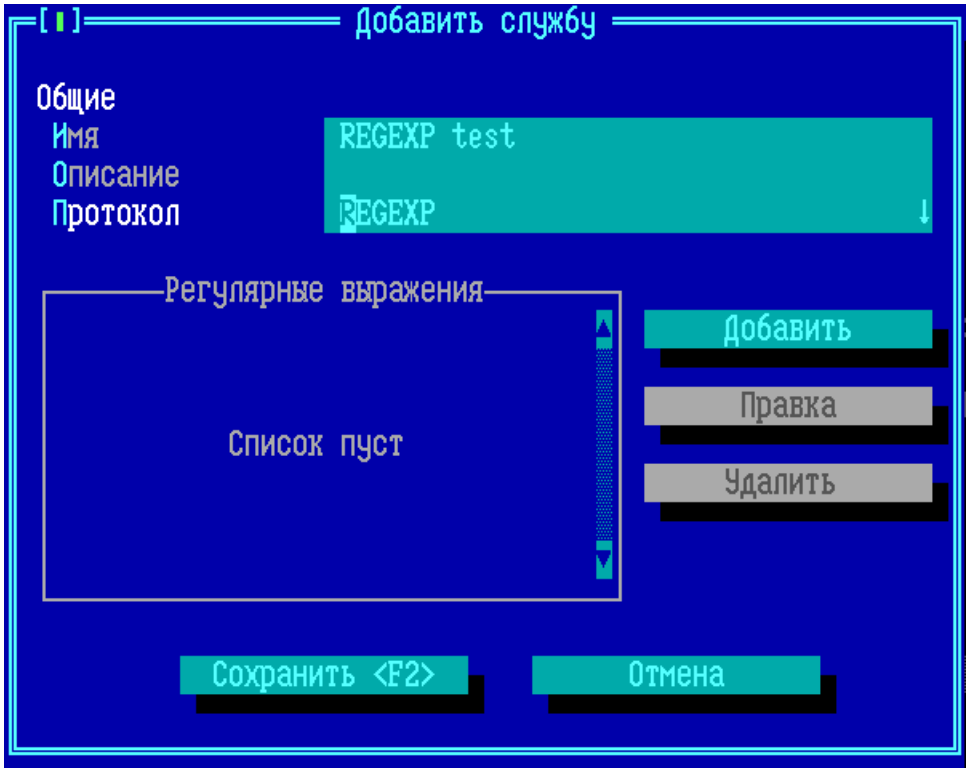


Рисунок 230 - Добавление службы REGEXP

В список «*Регулярные выражения*» службы должны быть добавлены символьные строки или регулярные выражения, которые межсетевой экран будет искать в IP-пакете, начиная с IP-заголовка и заканчивая данными прикладного протокола.

Для добавления новой символьной строки или регулярного выражения в список службы нажмите кнопку «Добавить» или клавишу <*Ins*>. В появившемся окне требуется указать следующие опции:

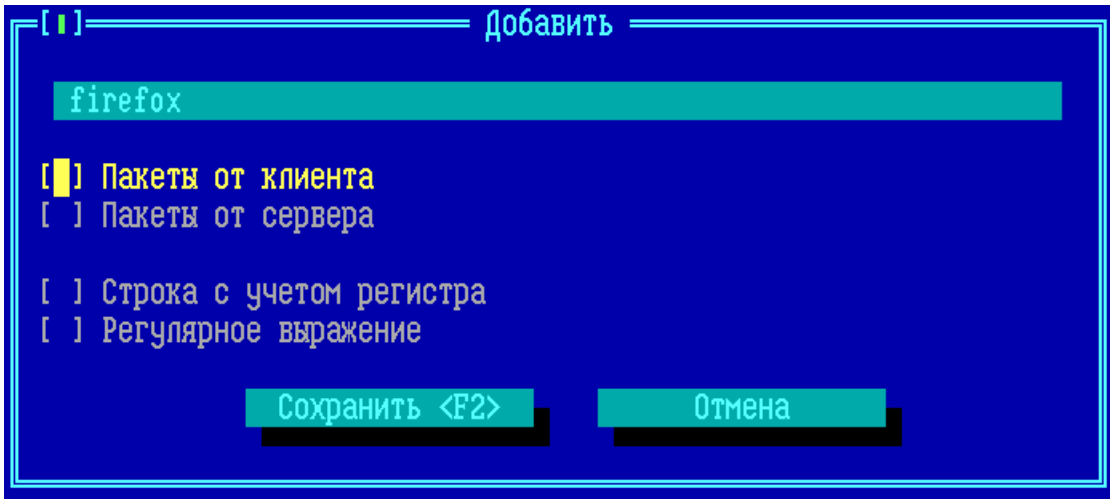


Рисунок 231 - Добавление службы REGEXP

Поле ввода окна «Добавить» - символьная строка или регулярное выражение, обязательная опция. Поле не должно быть пустым. Именно на наличие в IP-пакете указанной в поле ввода символьной строки/регулярного выражения межсетевой экран будет исследовать передаваемые пакеты. Количество символов в поле ограничено 1024. Символьная строка ищется в кодировке cp866. Если требуется искать символьную строку в другой кодировке, то следует использовать запись в кодах Unicode через символ «\u» с включенной опцией ***Регулярное выражение***. Например, для поиска сочетания латинской буквы A с латинской буквой B (символьной строки AB) следует написать в поле значение «\u0041\u0042».

Пакеты от клиента - опция, указывает на то, что символьную строку/регулярное выражение стоит искать только в пакетах, передающихся от инициатора соединения (клиента) к принимающей соединение стороне (серверу).

Пакеты от сервера - опция, указывает на то, что символьную строку/регулярное выражение стоит искать только в пакетах, передающихся от принимающей соединение стороны (сервера) к инициатору соединения (клиенту).

ВНИМАНИЕ! Должна быть задействована хотя бы одна из опций «Пакеты от клиента» или «Пакеты от сервера» (могут быть задействованы обе)!

Строка с учетом регистра - необязательная опция. Указывает на то, что в анализируемой символьной строке важен регистр (прописные или ЗАГЛАВНЫЕ символы).

Регулярное выражение - необязательная опция. Указывает на то, что в поле ввода указана не символьная строка, а регулярное выражение. Используются регулярные выражения библиотеки glibc (подробнее можно посмотреть в официальной документации на регулярные выражения glibc, https://www.gnu.org/software/libc/manual/html_node/Regular-

Expressions.html). Включение опции «Регулярное выражение» отключает опцию «Строка с учетом регистра».

Для выхода и возвращения в окно «Добавить службу» с сохранением выполненных настроек, нажмите кнопку «*Сохранить (F2)*» или клавишу <*F2*>.

Для выхода из окна и без внесения в конфигурацию сделанных изменений, нажмите кнопку «*Отмена*» или клавишу <*Esc*>.

После выхода с сохранением выполненных настроек, в списке «*Регулярные выражения*» окна «Добавить службу» появится новая запись:

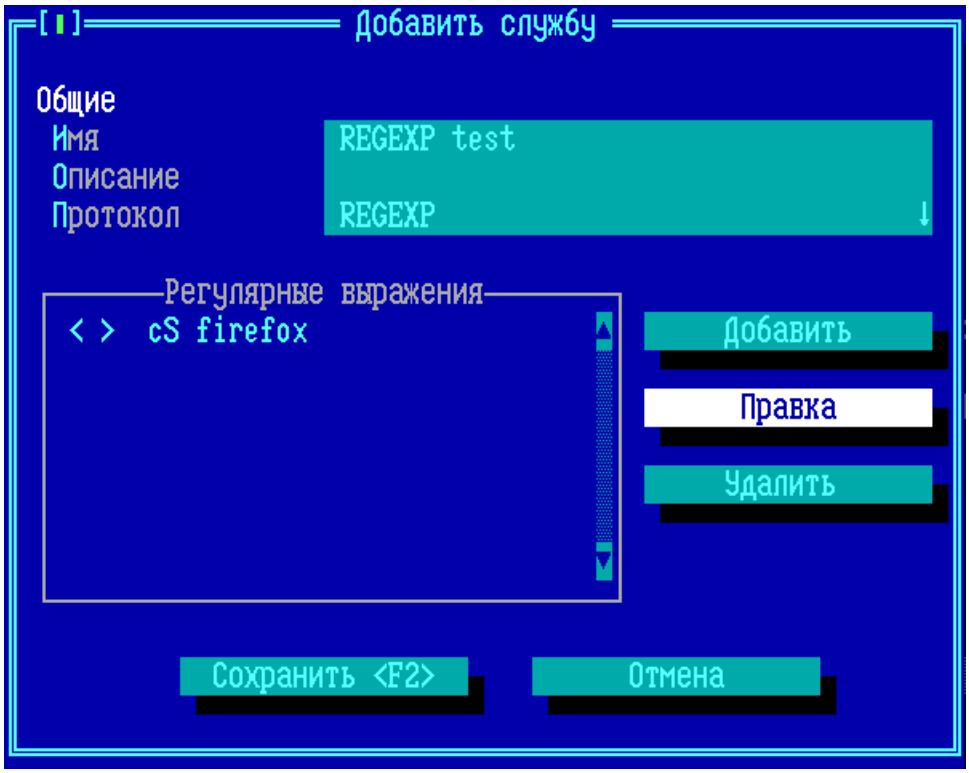


Рисунок 232 - Добавление службы REGEXP

Новая запись содержит следующие условные обозначения:

- Символ «<» - указатель на включенную опцию «Пакеты от клиента»;
- Символ «>» - указатель на включенную опцию «Пакеты от сервера»;
- Символы «cS» - указатель на включенную опцию «Строка с учетом регистра»;
- Символы «??» - указатель на включенную опцию «Регулярное выражение»;
- Текст после условных обозначений - символьная строка или регулярное выражение записи списка.

В одну службу с типом протокола REGEXP можно добавить 255 записей символьных

строк или регулярных выражений. В этом случае будет анализироваться наличие в IP-пакете 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:

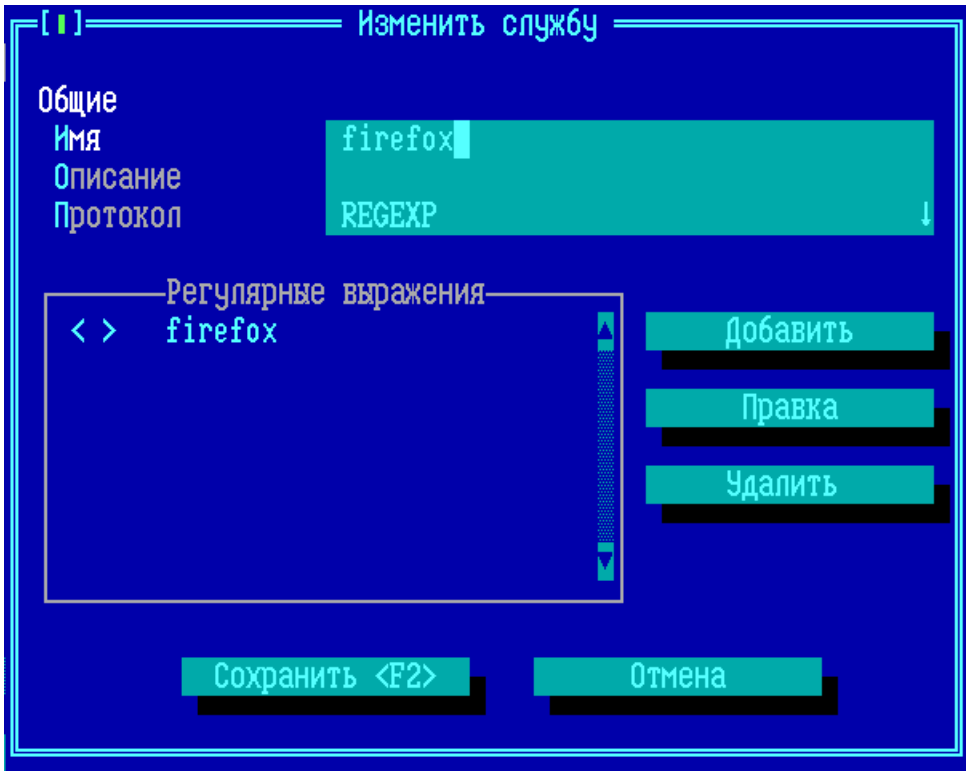


Рисунок 233 - Блокировка браузера Mozilla Firefox, правило 1

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

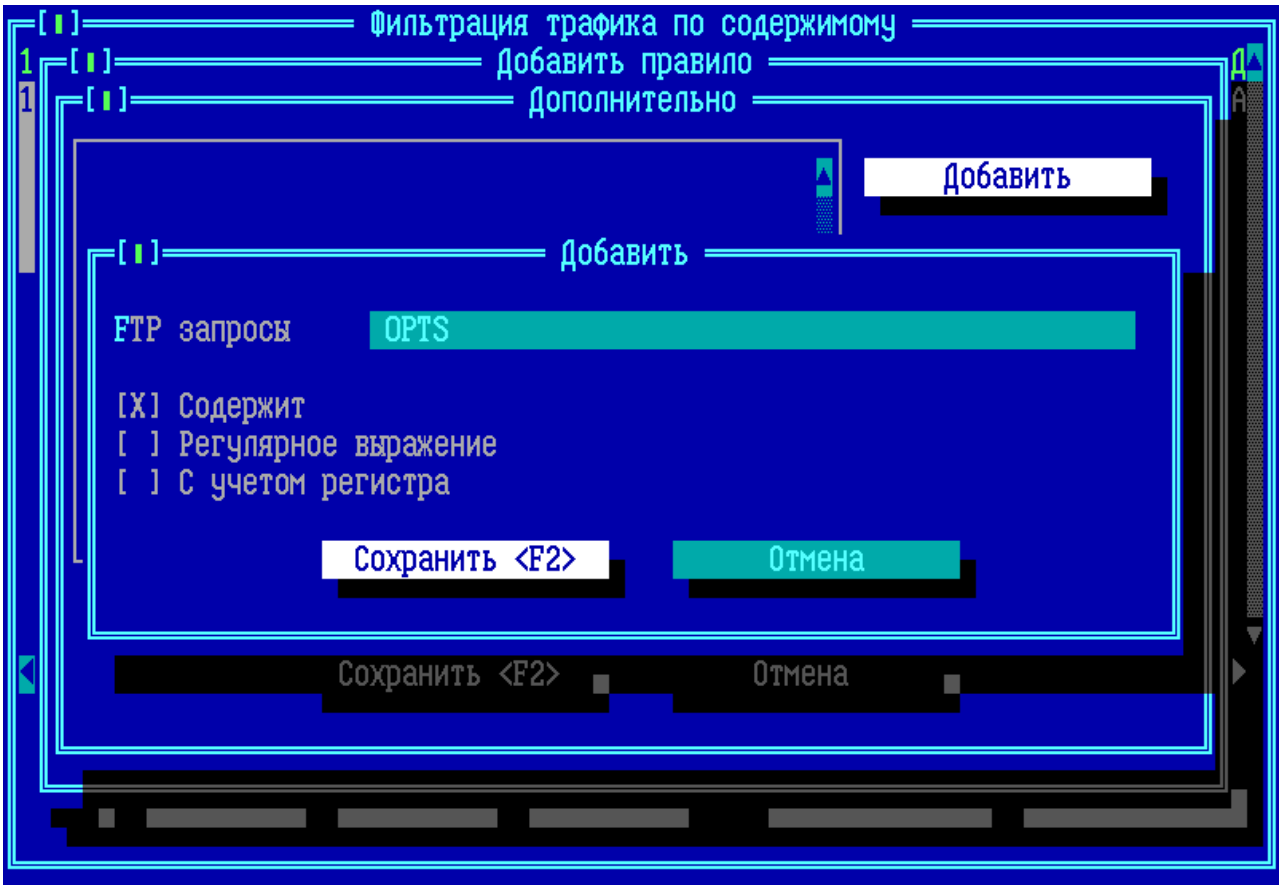


Рисунок 234 - Блокировка браузера Mozilla Firefox, правило 2

Для блокировки сетевой работы браузера Google Chrome следует создать 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:

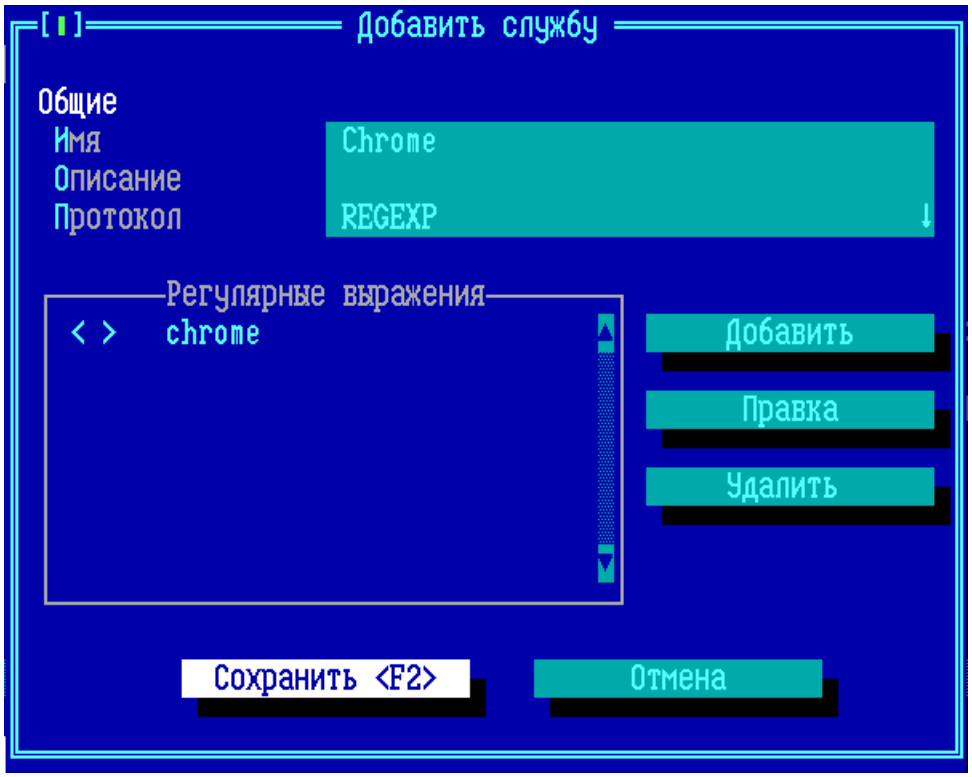


Рисунок 235 - Блокировка браузера Google Chrome, правило 1

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

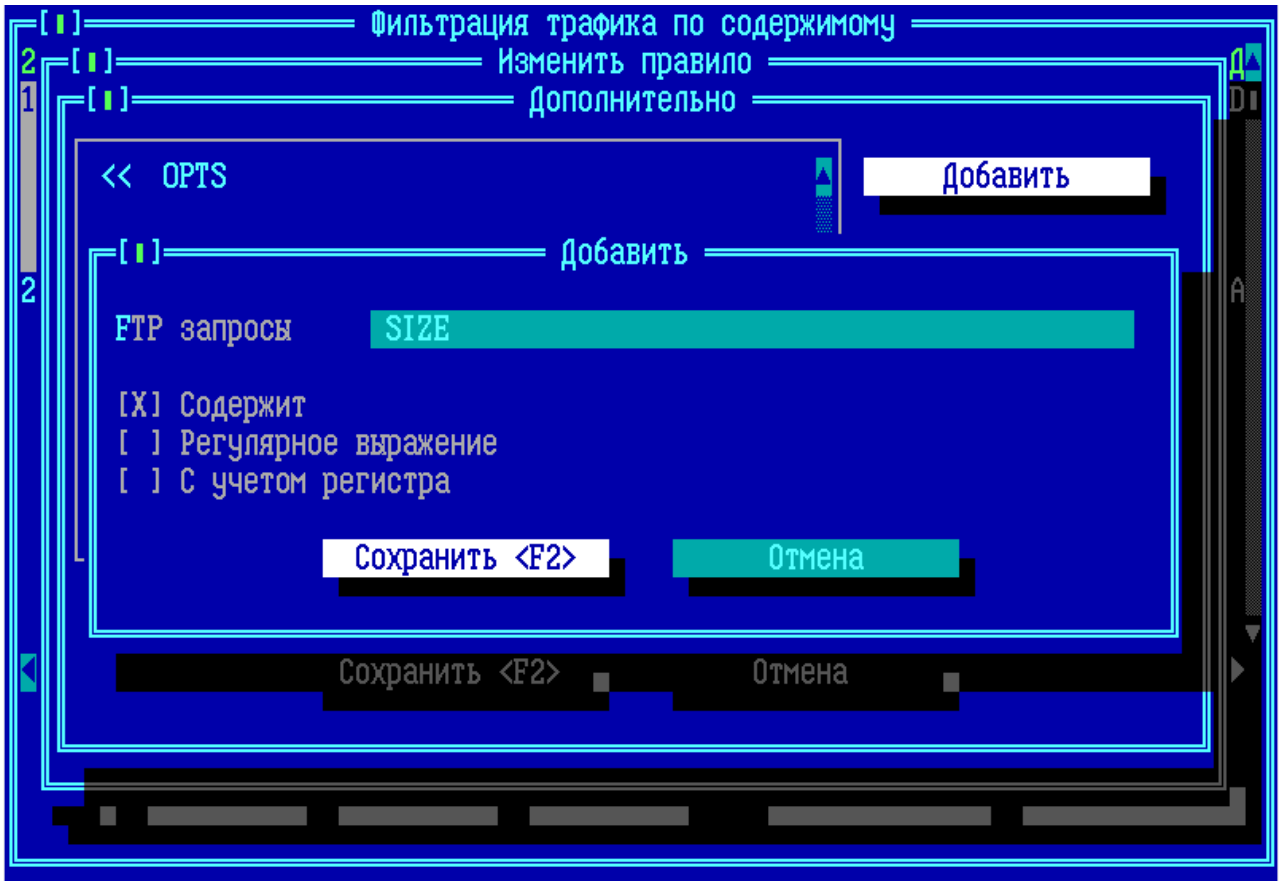


Рисунок 236 - Блокировка браузера Google Chrome, правило 2

Примеры для частичной блокировки работы приложения:

Для частичной блокировки сетевой работы почтового клиента Dreammail, 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:

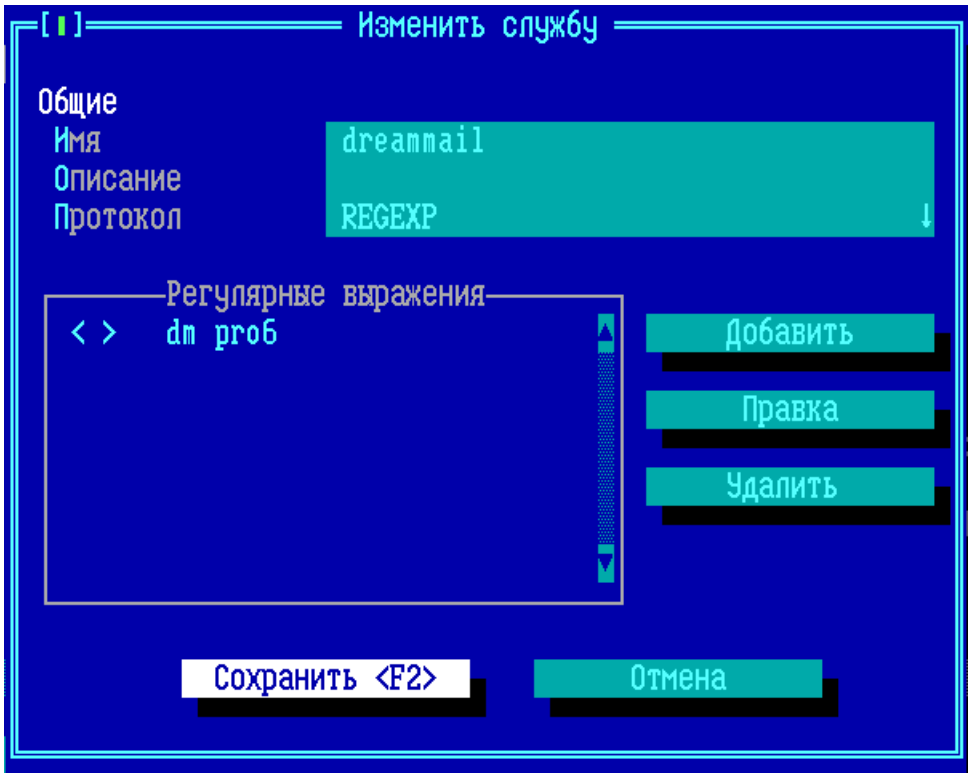


Рисунок 237 - Блокировка работы почтового клиента Dreammail по протоколу SMTP

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:

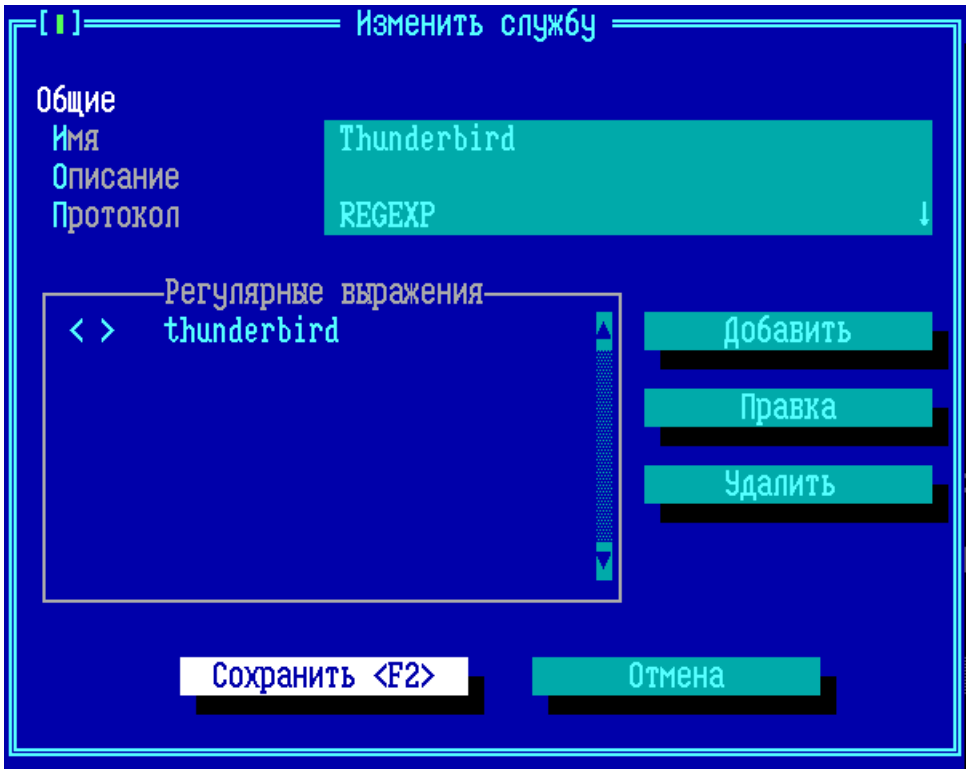


Рисунок 238 - Блокировка работы почтового клиента Thunderbird по протоколу SMTP

10. 3. Управление полосой пропускания

Скорость передаваемых через ФПСУ-IP абонентских данных может контролироваться межсетевым экраном. Для этого в конфигурации параметров доступа ФПСУ-IP создаются специальные правила управления полосой пропускания:

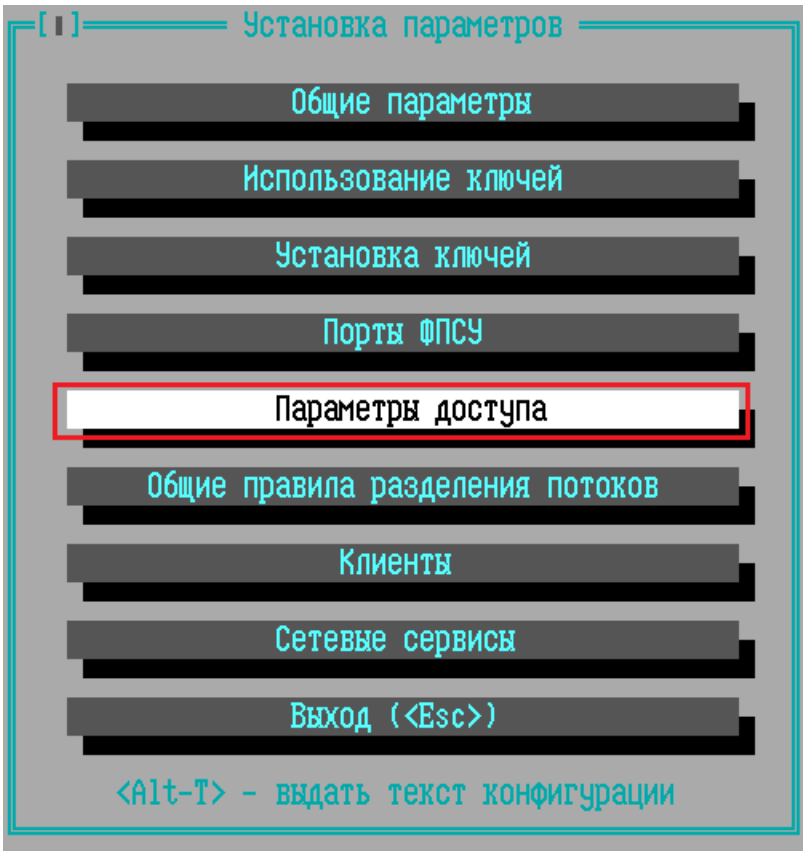


Рисунок 239 - Команды «Параметры доступа» и «Управление полосой пропускания»

Управление ограничением скорости передаваемых через ФПСУ-IP пользовательских

данных реализовано следующим образом: администратор ФПСУ-IP создает список правил, 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.

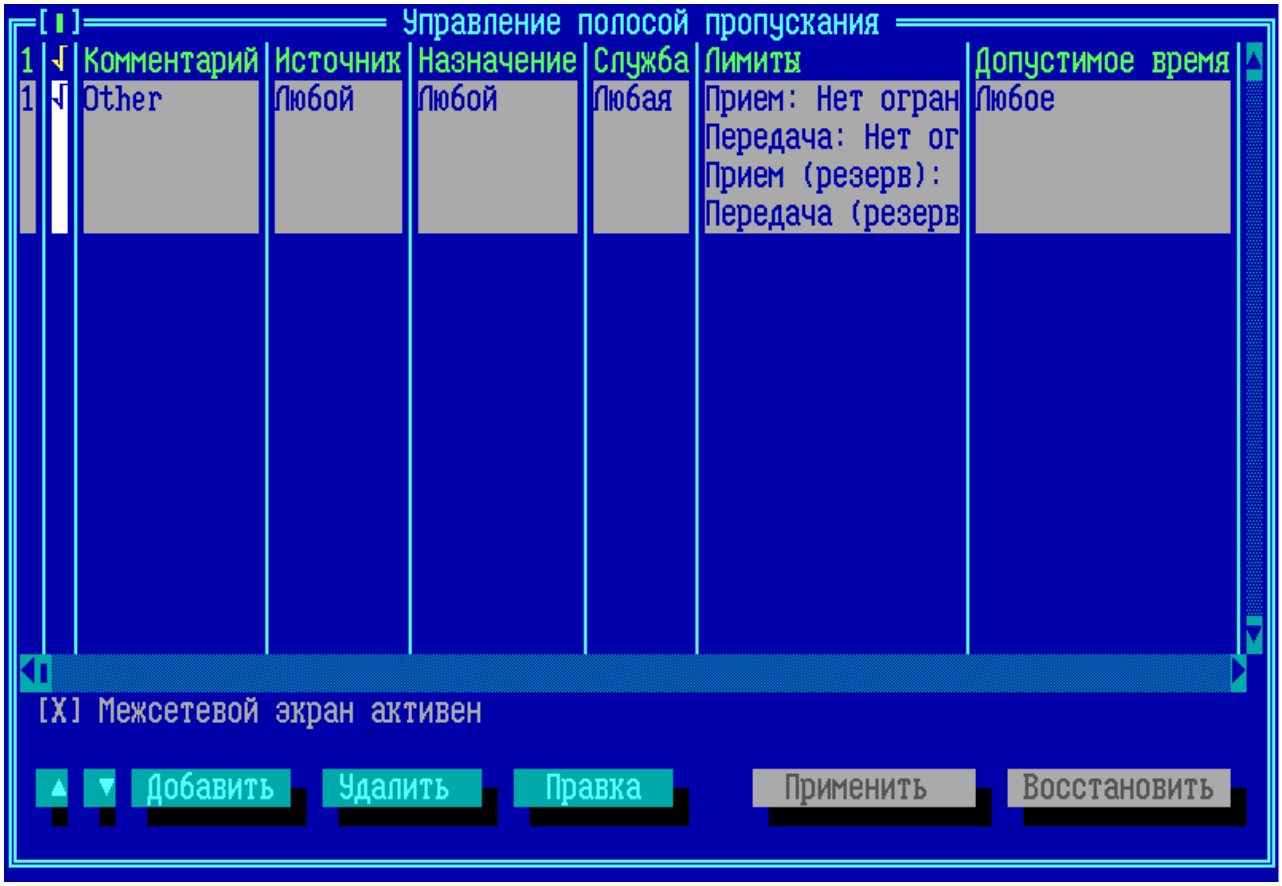


Рисунок 240 - Окно списка правил управления полосой пропускания

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».

Для создания нового правила управления полосой пропускания, следует нажать клавишу <*Ins*> или кнопку «*Добавить*». В появившемся окне «Добавить правило» находятся четыре вкладки с настраиваемыми опциями. Переход с активной вкладки на соседнюю осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

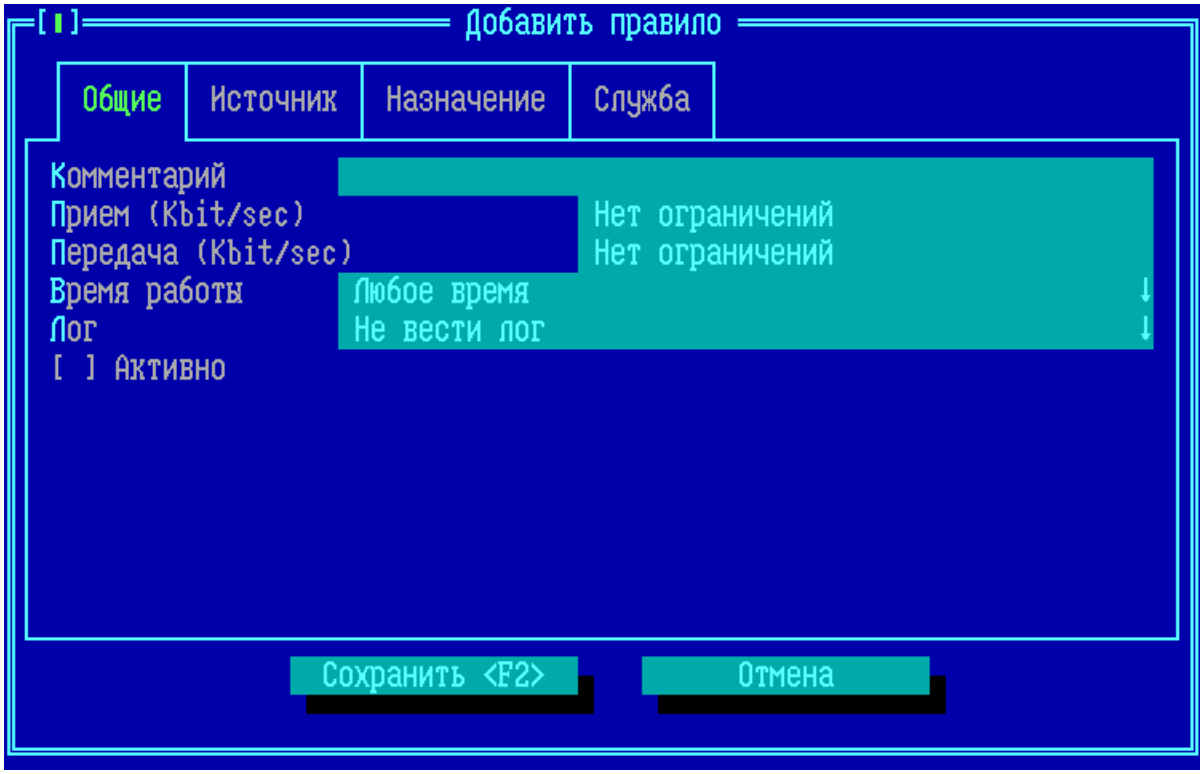


Рисунок 241 - Создание нового правила ограничения скорости передачи данных

Для каждого создаваемого правила требуется указать ограничение приема и передачи данных, а также к каким именно передачам данных такое ограничение будет применено: определить источник и назначение передачи, и тип ограничиваемого трафика.

Вкладка **Общие** предназначена для выбора разрешенной скорости передачи данных, и опциональных дополнительных настроек. Символом «↓» в конце настраиваемого поля обозначается наличие выпадающего списка, вызываемого нажатием клавиши <*Пробел*> при установленном на поле курсоре.

Вкладка **Общие** содержит следующие настраиваемые опции:

Комментарий — обязательное произвольное текстовое поле для пояснения правила.

Прием (Kbit/sec) — установка разрешенной скорости приема данных от источника к

назначению, килобит в секунду (ВНИМАНИЕ! На ФПСУ-IP используется метрика 1 Kbit/sec = 1024 bit/sec). По умолчанию, не ограничено.

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*».

10. 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»:

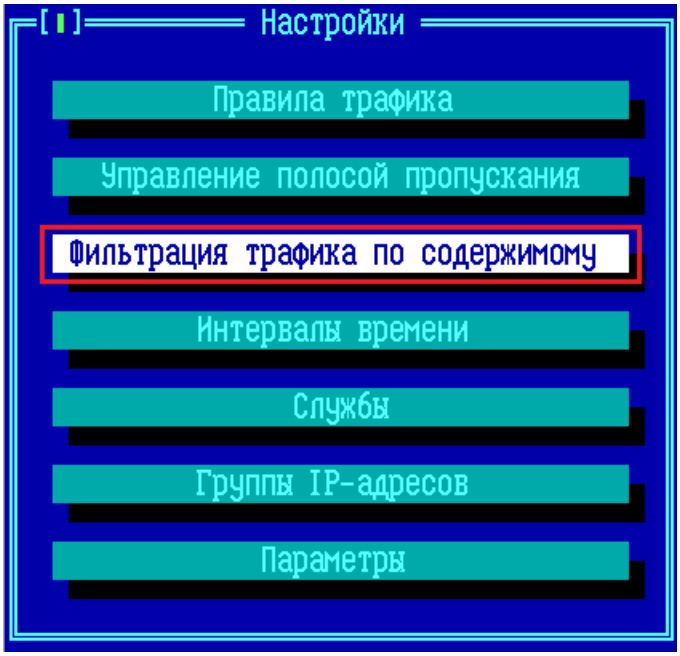


Рисунок 242 - Меню настройки межсетевого экрана ФПСУ-IP

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.

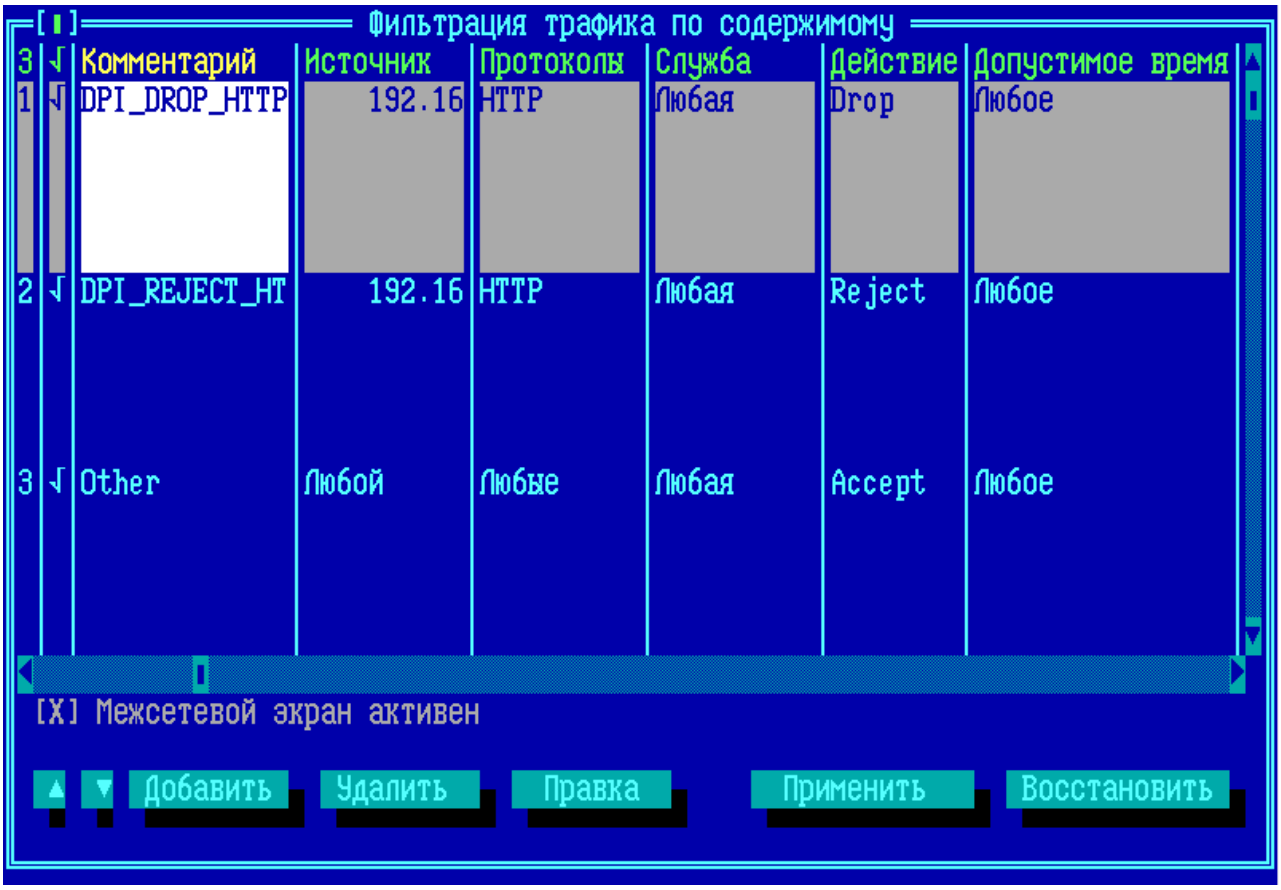


Рисунок 243 - Окно списка правил фильтрации трафика по содержимому

Фильтрация трафика по содержимому осуществляется только при активном межсетевом экране ФПСУ-IP. Флаг «*Межсетевой экран активен*» указывает на работу дополнительных правил фильтрации, в том числе правил фильтрации трафика по содержимому.

Для внесения изменений в конфигурацию без выхода из окна, нажмите кнопку «*Применить*». Сохранение изменений с выходом в подменю «Настройки» осуществляется по нажатию 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 «Правила трафика».

10. 4. 1. Создание правила фильтрации по содержимому и его общие настройки

Для создания нового правила фильтрации по содержимому, следует нажать клавишу <*Ins*> или кнопку «*Добавить*» в окне списка правил фильтрации по содержимому.

В появившемся окне «Добавить правило» находятся вкладки с настраиваемыми параметрами правила, которые определяют, как и какой тип трафика будет исследоваться. Переход с активной вкладки на соседнюю осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

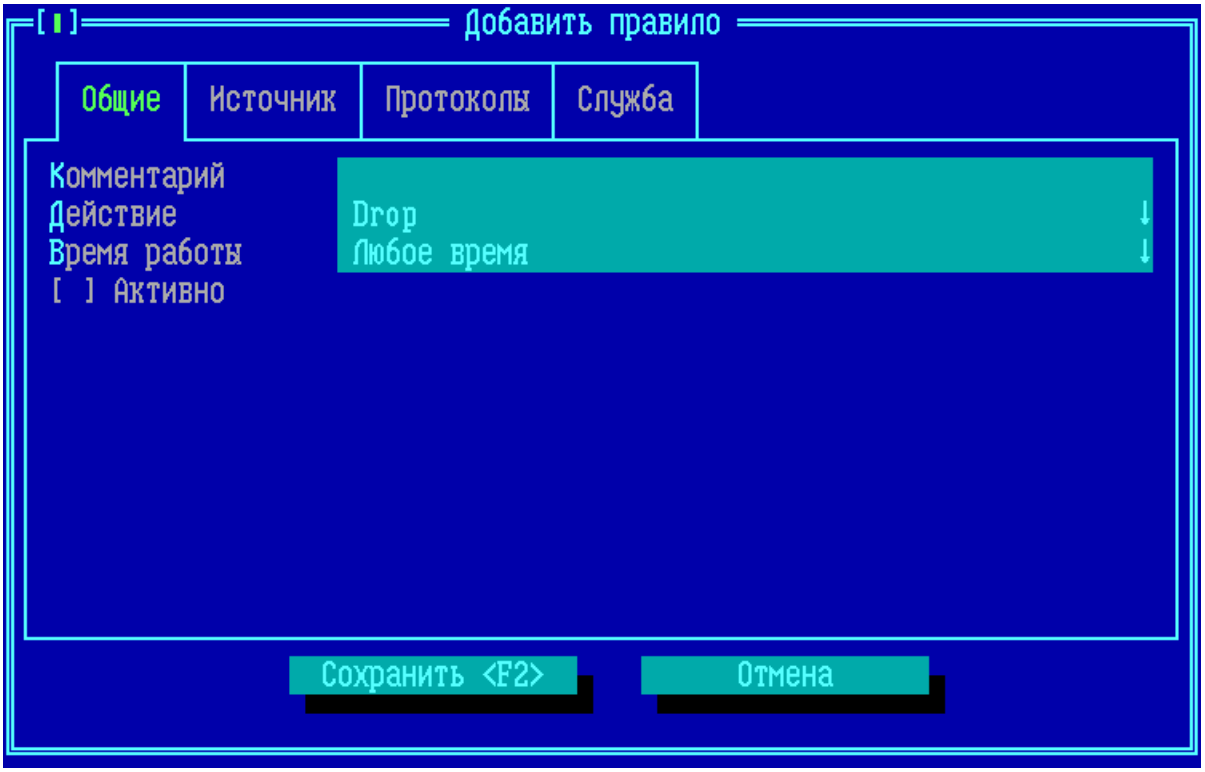


Рисунок 244 - Добавление нового правила фильтрации по содержимому

Для каждого создаваемого правила требуется указать действие, как поступить с попавшим под критерии правила фильтрации по содержимому пакетом, к каким именно передачам данных такое ограничение будет применено: определить источник передачи, и фильтры, по которым будет анализироваться передаваемый трафик.

Вкладка **Общие** содержит следующие настраиваемые опции:

Комментарий — обязательное произвольное текстовое поле для пояснения правила.

Действие — обязательная настройка, определяющая, как поступить с передаваемым пакетом. В выпадающем меню могут быть выбраны следующие варианты действия:

- *Drop* — действие по умолчанию, пакет данных будет сброшен, оповещение об отказе передачи пакета не будет передано отправителю;
- *Reject* — пакет данных будет сброшен, отправителю будет передано ICMP-оповещение об отказе передачи пакета.

Символом «↓» в конце настраиваемого поля обозначается наличие выпадающего списка, вызываемого нажатием клавиши <*Пробел*> при установленном на поле курсоре.

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»).

10. 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).

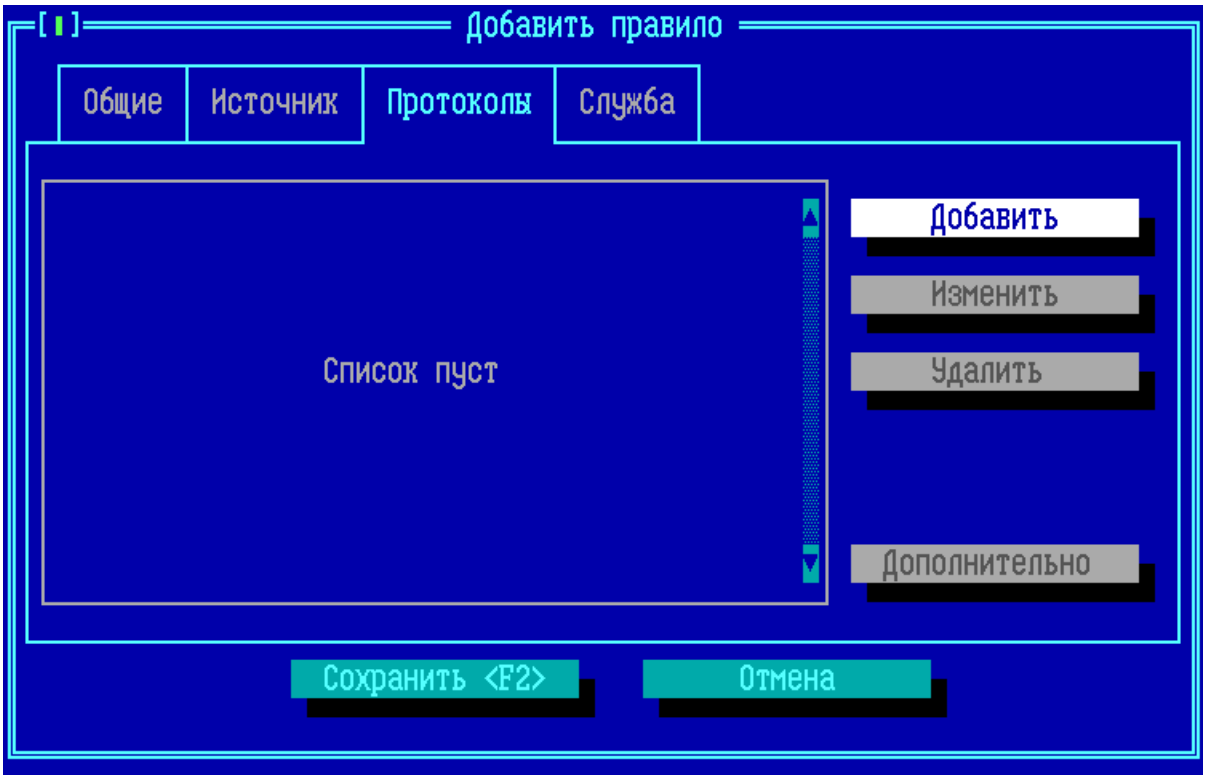


Рисунок 245 - Вкладка «Протоколы»

Для каждого правила фильтрации трафика по содержимому должен быть установлен один и только один исследуемый протокол. Если список пустой (настройка нового правила по умолчанию), дополнительный анализ на формат используемого протокола и тип передаваемых данных проводиться не будет.

Для занесения в список исследуемого правилом протокола, нажмите кнопку «*Добавить*».

Рисунок 246 - Окно выбора исследуемого протокола

Из выпадающего списка поля «Протокол» следует выбрать один из доступных для

анализа протоколов:

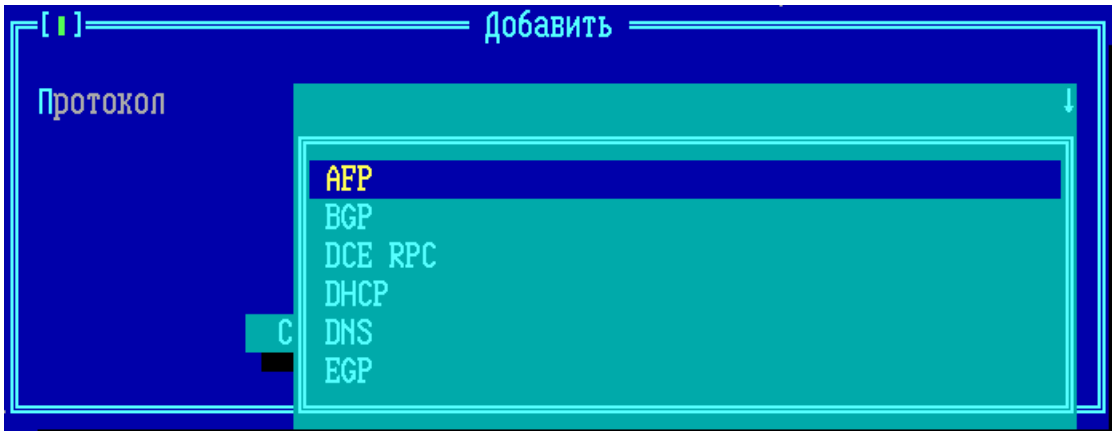
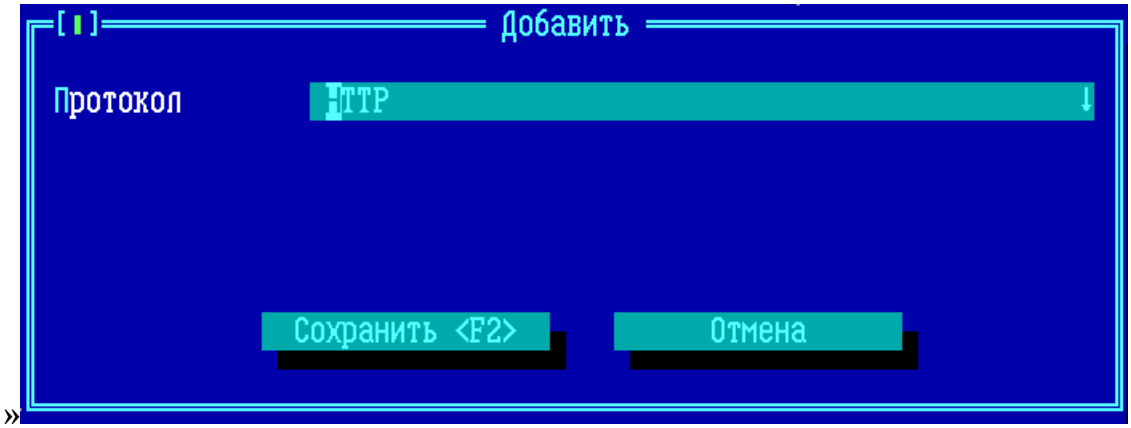


Рисунок 247 - Выбор исследуемого протокола

После выбора курсором одного из предлагаемых протоколов, нажмите клавишу *<Enter>* для подтверждения выбора. Выбранный протокол будет указан в поле «Протокол» окна (в примере - HTTP):



»

Рисунок 248 - Выбран протокол для исследования

Нажмите клавишу *<F2>* или кнопку *«Сохранить <F2>»* для возврата в интерфейс настройки правила фильтрации трафика по содержимому. Выбранный протокол будет указан в списке:

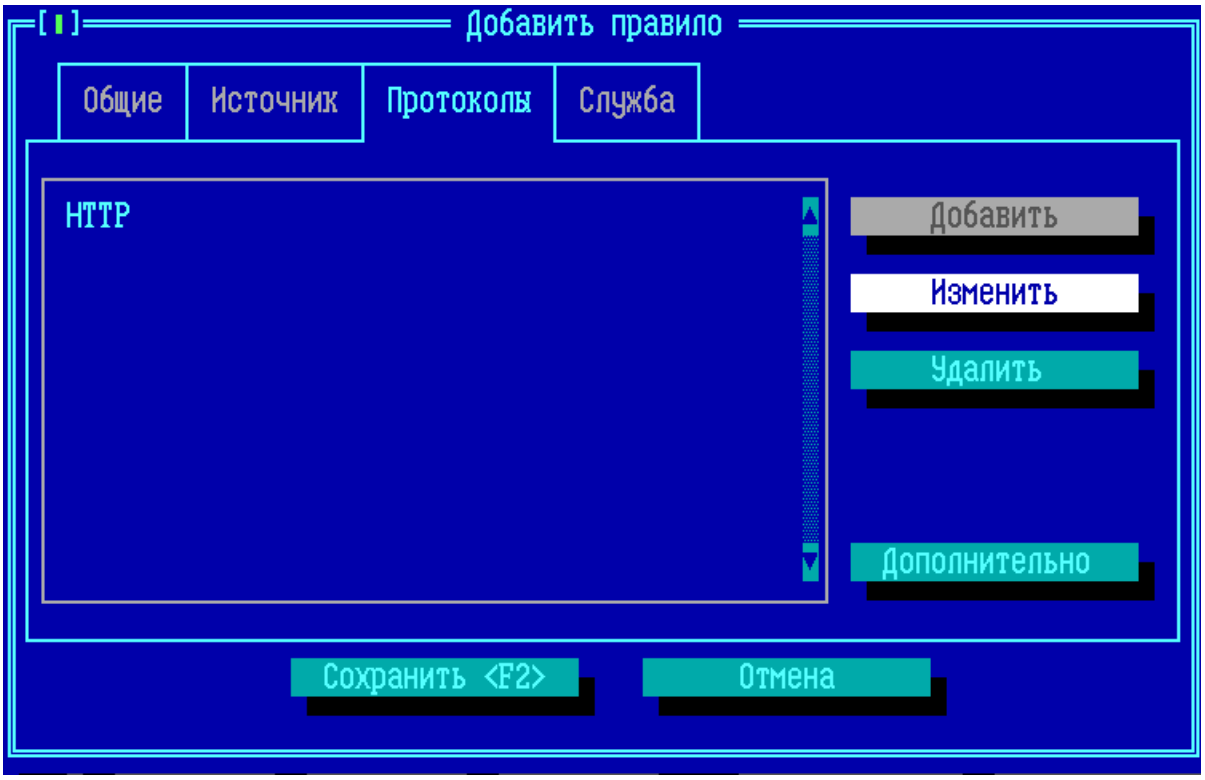


Рисунок 249 - Протокол, исследуемый правилом

Выбор протокола можно поменять командой *«Изменить»* или отменить командой *«Удалить»*. Если в протоколе доступны дополнительные настройки для анализа не всего протокола, а исследование передаваемого содержимого по контенту, командам или другим параметрам, то кнопка ***Дополнительно*** становится активной.

10. 4. 3. Дополнительные фильтры для протокола http

Протокол HTTP может дополнительно исследовать на список используемых в http-соединении методов, типов содержимого (контент, content type) и URL-адресов. Для протокола HTTP может быть использован фильтр, содержащий несколько дополнительных опций (например, исследоваться будет и по методу, и по контенту). При нажатии кнопки *«Дополнительно»* будет выведено окно выбора опций фильтра для выбранного протокола:

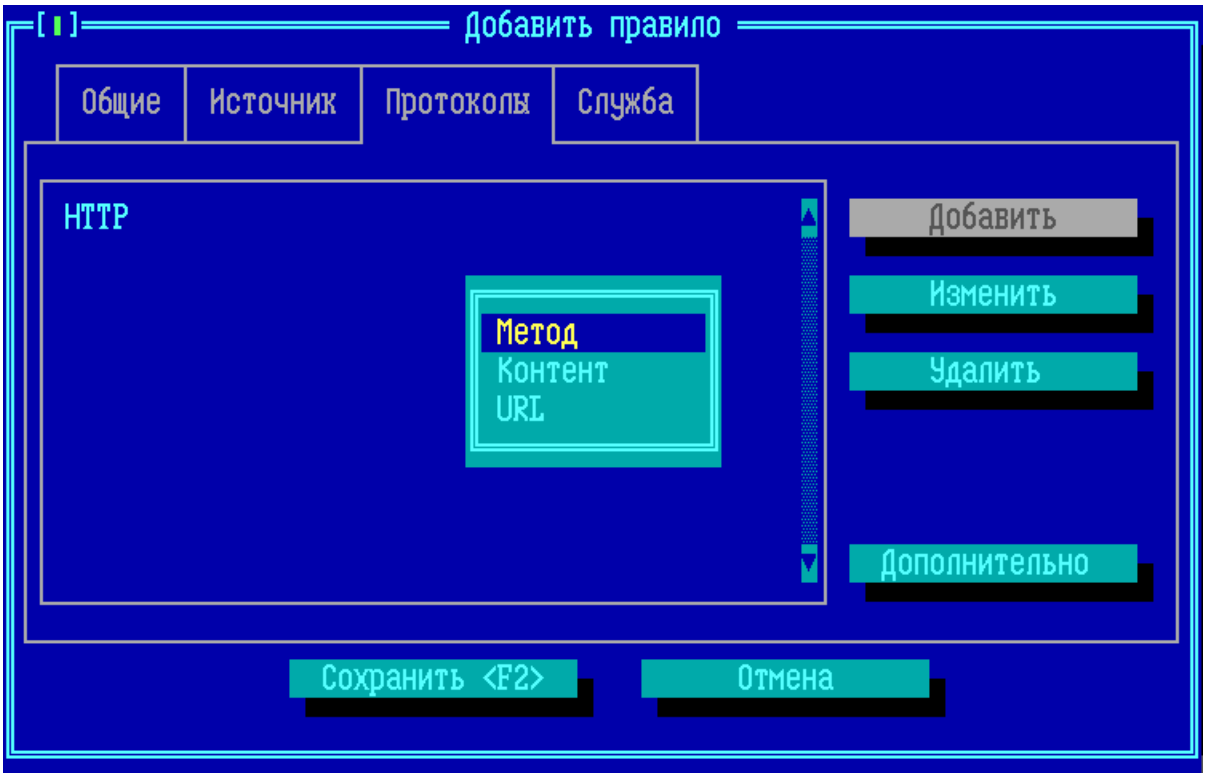


Рисунок 250 - Доступные опции исследования протокола HTTP

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

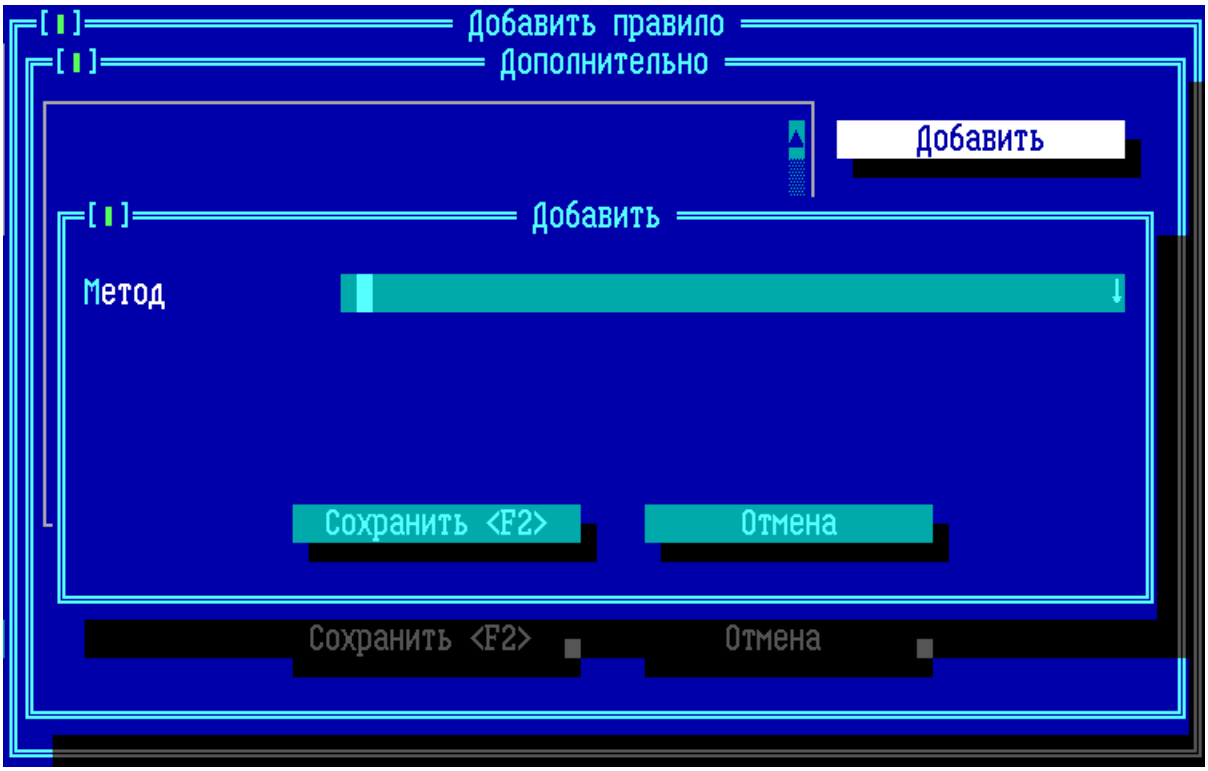


Рисунок 251 - Добавление фильтруемого метода протокола http

В качестве фильтруемых *методов* могут быть установлены методы запроса http-протокола *OPTIONS*, *GET*, *HEAD*, *POST*, *PUT*, *DELETE*, *TRACE*, *CONNECT*. Параметр метода *UNKNOWN* является специальным. Он означает, что будет фильтроваться метод, неизвестный межсетевому экрану, то есть ни один из перечисленных выше.

В качестве фильтруемого типа содержимого (*контент*) может быть установлена символьная строка, которую использует протокол для обозначения типа передаваемых данных (например, установить значение «*application/javascript*» для фильтрации соединения, в рамках которого выполняется попытка передать мобильный код JavaScript):

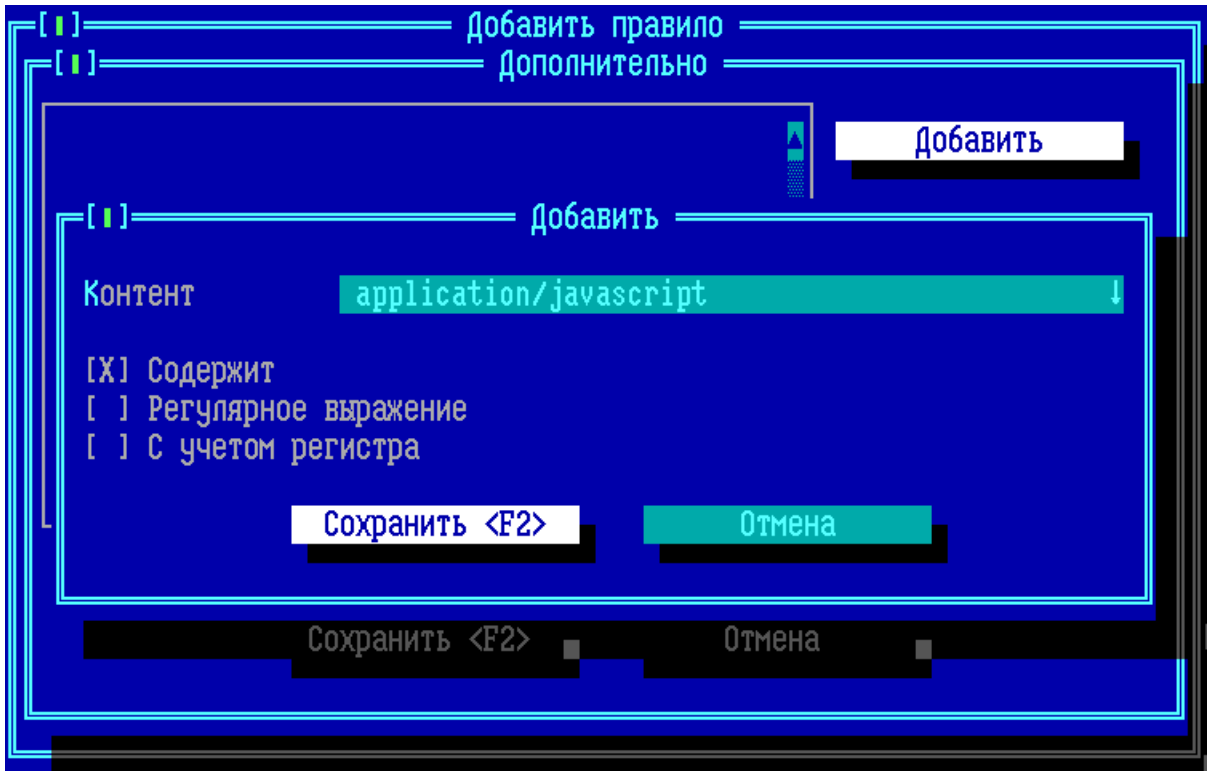


Рисунок 252 - Добавление фильтруемого контента протокола http

В качестве фильтруемого URL-адреса может стоять как точное символьное выражение (например, *example.com*), так и встречающаяся в нём строка или регулярное выражение.

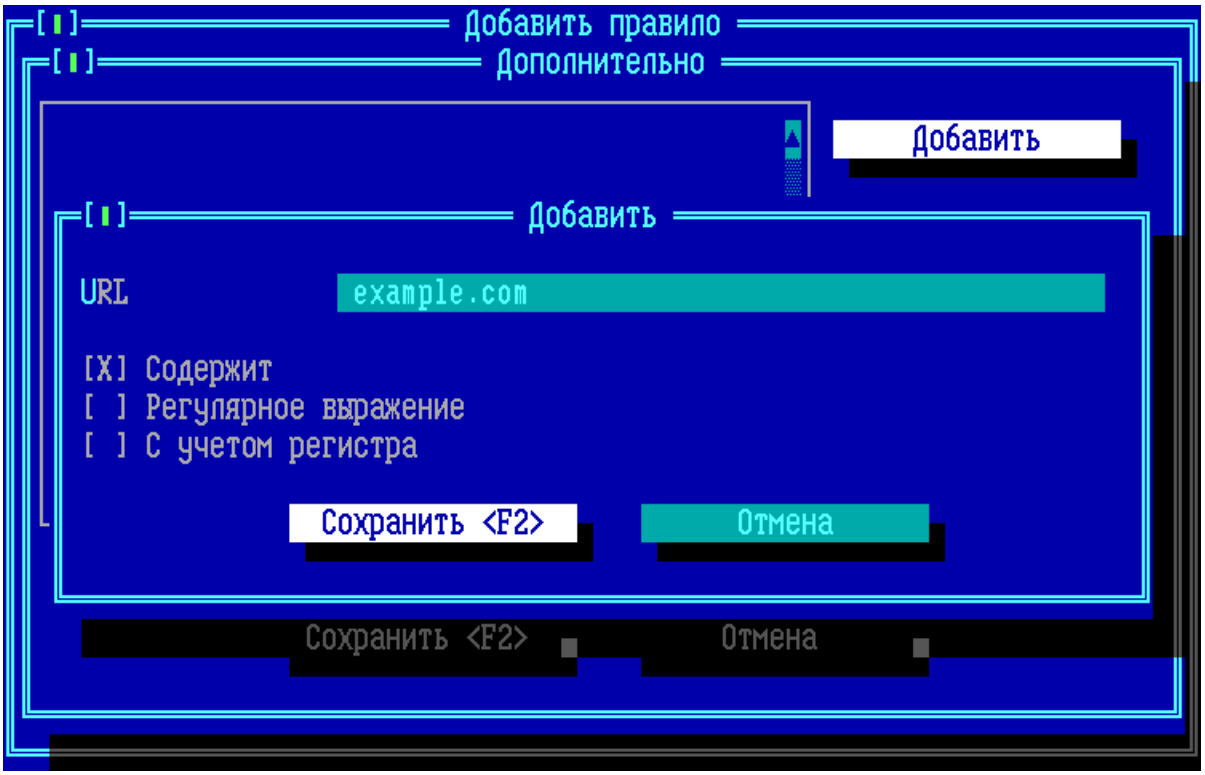


Рисунок 253 - Добавление фильтруемого URL-адреса протокола http

После сохранения дополнительных опций, которые задействуют несколько фильтров, в интерфейсе фильтруемого протокола будет указан признак, что исследуется трафик http-протокола несколькими фильтрами:

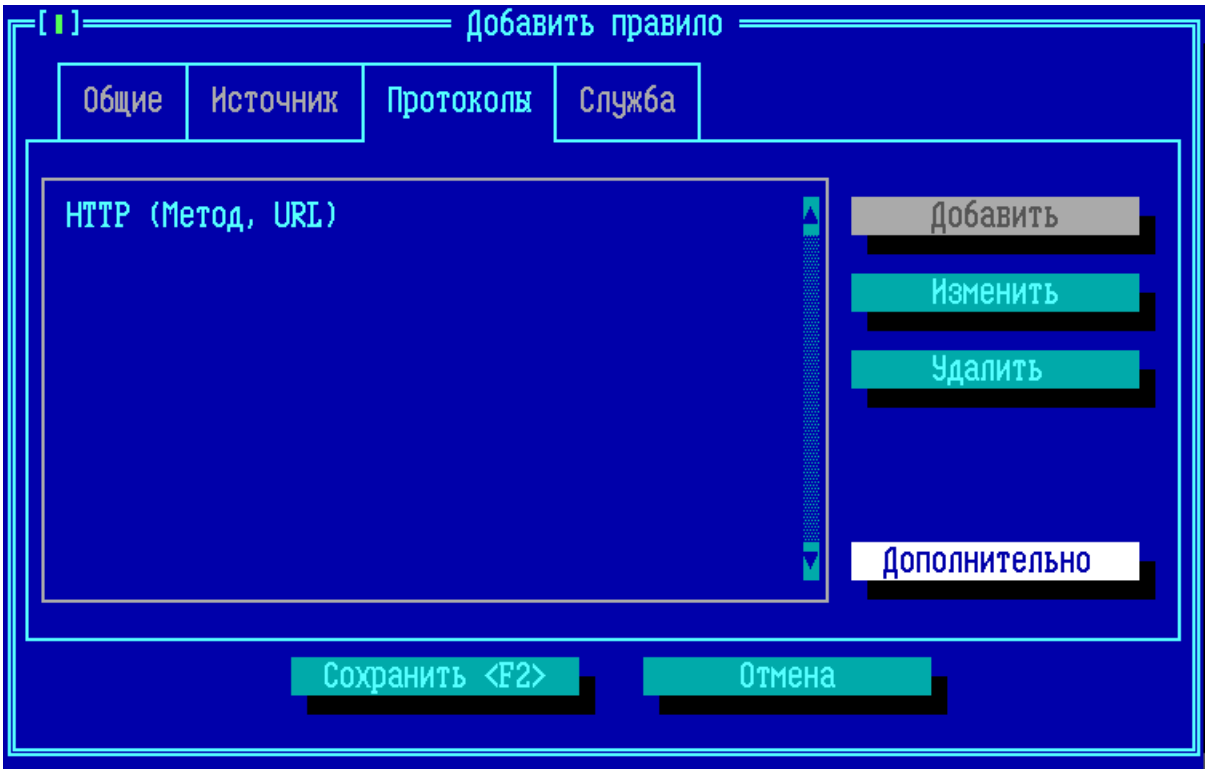


Рисунок 254 - Правило с дополнительными фильтрами протокола http

10. 4. 4. Службы в правилах фильтрации трафика по содержимому

В правилах фильтрации трафика по содержимому могут быть использованы только службы типа протокола RAW (подробнее см. пункт «Службы»). Службы для остальных типов протоколов не могут быть добавлены к правилу фильтрации по содержимому.

Особенности конфигурации:

1. Если правило фильтрации трафика по содержимому исследует передаваемые от **Источника** пакеты только по добавленным в список **Службы** RAW-фильтрам, то достаточно одного правила фильтрации трафика по содержимому.

Например, для фильтрации всего трафика на предмет наличия фрагментированных пакетов достаточно будет добавить одно активное правило фильтрации трафика по содержимому, с пустыми вкладками **Источник** и **Протоколы**, где во вкладке **Службы** указана ссылка на службу фильтрации фрагментированных пакетов (см. пункт «Служба для запрета фрагментированных пакетов»).

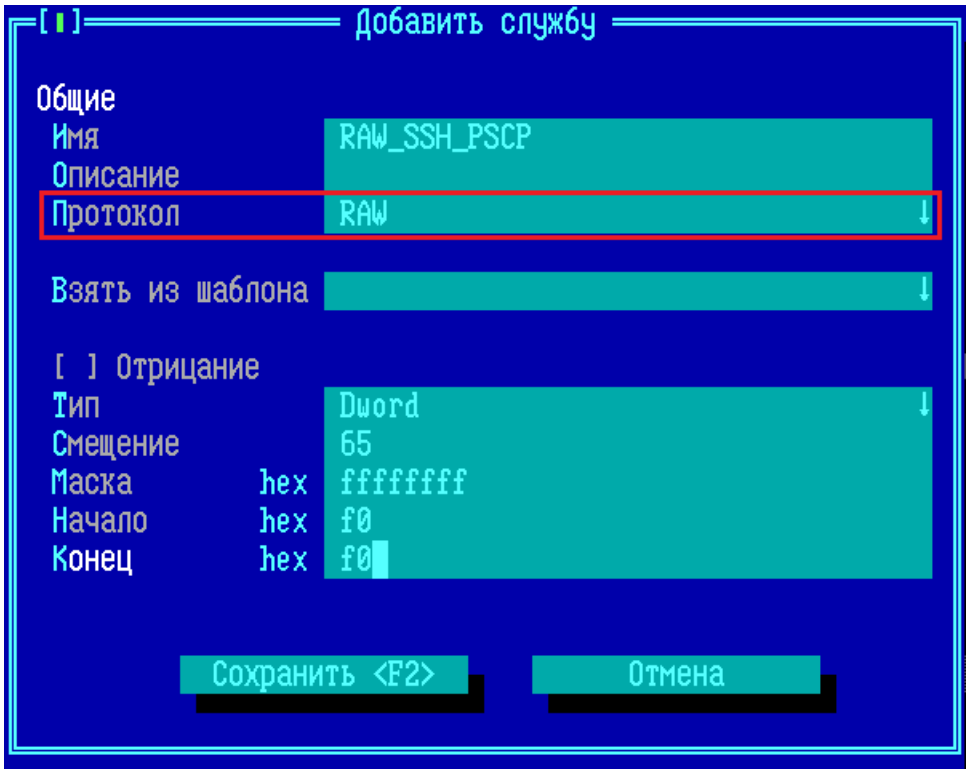


Рисунок 255 - Служба для протокола RAW

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.

10. 5. Интервалы времени

Пункт «Интервалы времени» меню правил доступа предназначен для создания и управления используемых правилами трафика и правилами фильтрации по содержимому временных интервалов.

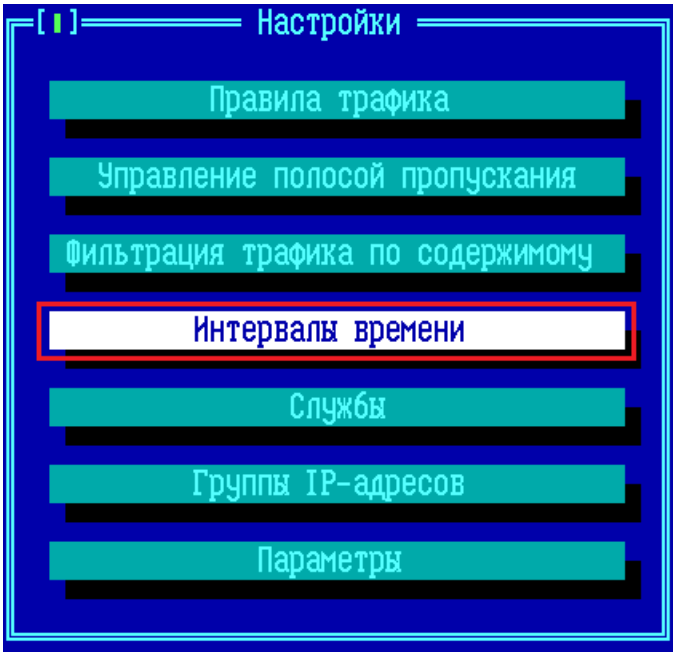


Рисунок 256 - Команда «Интервалы времени»

В окне управления списком разрешенных интервалов работы создаются используемые в правилах трафика ограничения по дням недели и времени суток при передаче данных. В каждом создаваемом интервале основным параметром является день недели, в который передача данных разрешена.

В окне содержится список созданных администратором интервалов времени разрешенной работы абонентов (по умолчанию пустой):

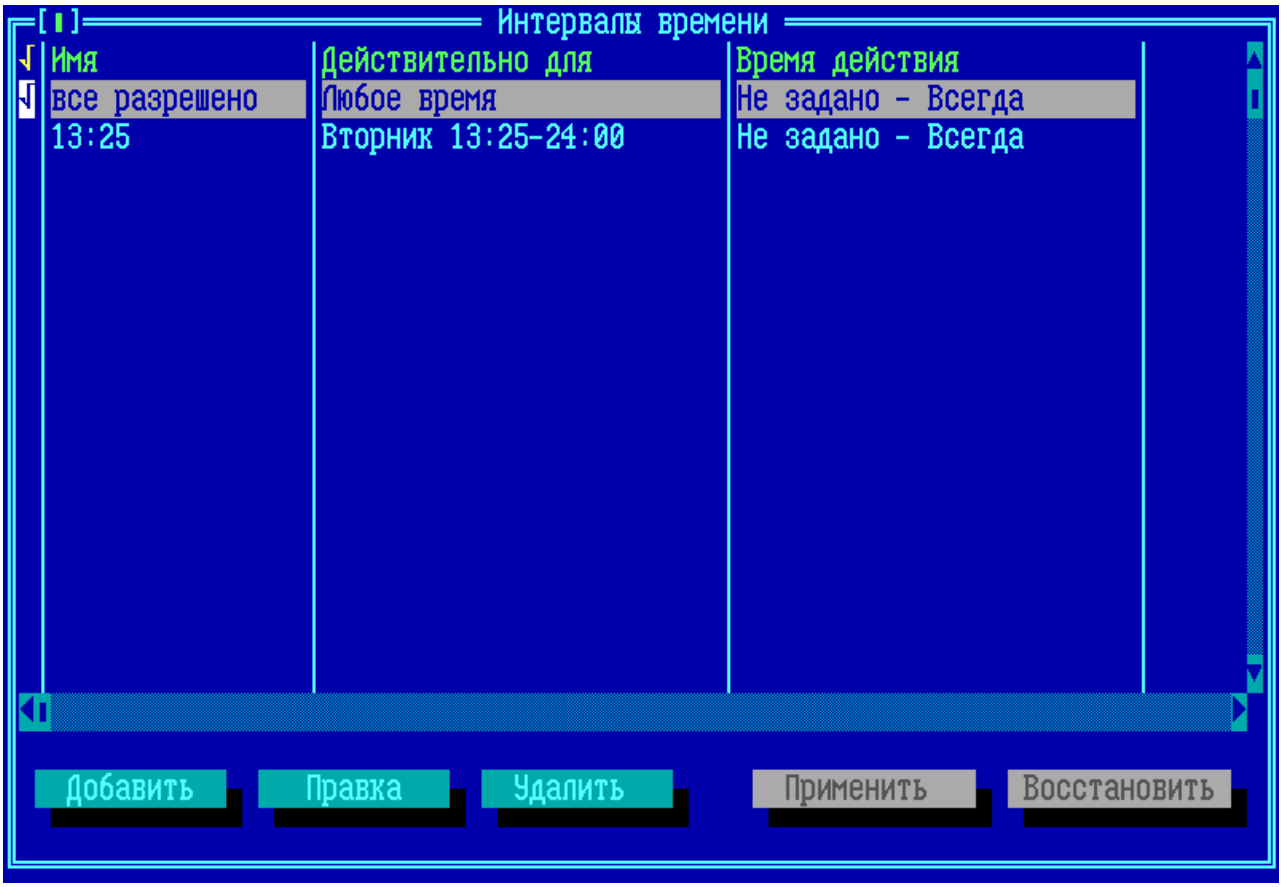


Рисунок 257 - Список определенных интервалов времени

Команды окна управления списком интервалов:

Добавить **—** кнопка, по нажатию который происходит вызов окна создания нового интервала времени.

Правка — кнопка, по нажатию которой (или клавиши <*Enter*>) происходит вызов окна параметров ранее созданного интервала времени.

Удалить — по нажатию кнопки происходит удаление интервала времени, отмеченного курсором.

Применить — при внесении изменений в существующие интервалы времени следует подтвердить изменения, нажав эту кнопку (или клавишу <*F2*>). ВНИМАНИЕ! При выходе из окна управления списком интервалов времени по клавише <*Esc*> или сочетанию клавиш <*Alt+X*>, изменения не сохраняются!

Восстановить — по нажатию этой кнопки будут отменены все выполненные в этот сеанс работы изменения в существующих интервалах времени.

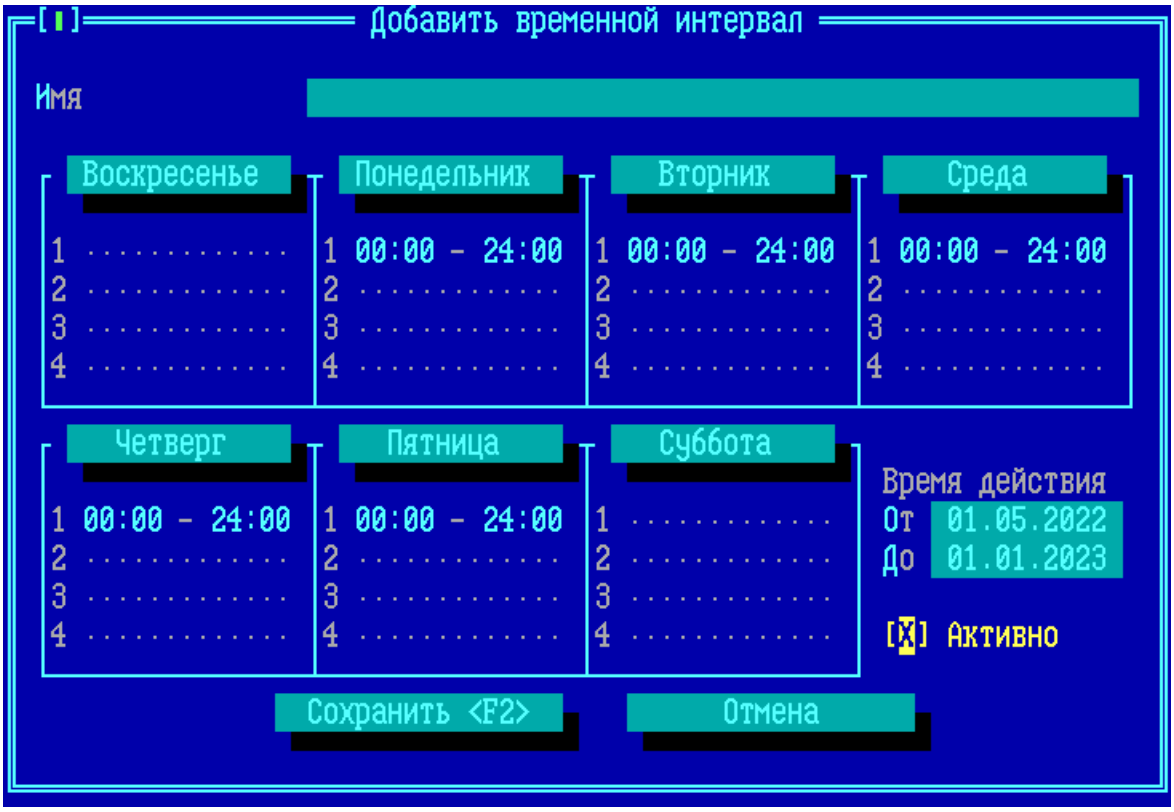


Рисунок 258 - Параметры временного интервала

Для каждого дня недели можно указать до четырех временных интервалов, в которые разрешен обмен пакетами. Если ограничений нет - устанавливается интервал 00:00 - 24:00, если работа не разрешена - временные интервалы должны быть пусты. Удаления значений в каждом из интервалов работы производится нажатием клавиши <*Del*>. После определения всех интервалов следует включить флаг «*Активно*» (при помощи клавиши <*Пробел*>) для активации сделанных ограничений.

Во временном интервале может быть опционально установлено время действия правила в масштабе временных дат. В графе «Время действия» в таком случае следует указать дату начала и дату завершения разрешенного периода действия временного интервала.

Сохраните сделанные установки нажатием клавиши <*F2*> (или выйдите без сохранения при помощи <*Esc*>).

10. 6. Группы IP-адресов

Действие создаваемого правила трафика (пункт «Правила трафика») можно ограничить, установив его действие не на все передаваемые данные между указанными отправителями и получателями, а только на те, которые дополнительно входят и в диапазон

указанных во вкладке «Группы IP-адресов».

В окне, вызываемом по выполнению команды «Группы IP-адресов» меню настройки конфигурации «Параметры доступа» правил дополнительной фильтрации, находится список созданных администраторами ФПСУ-IP групп IP-адресов (по умолчанию пустой).

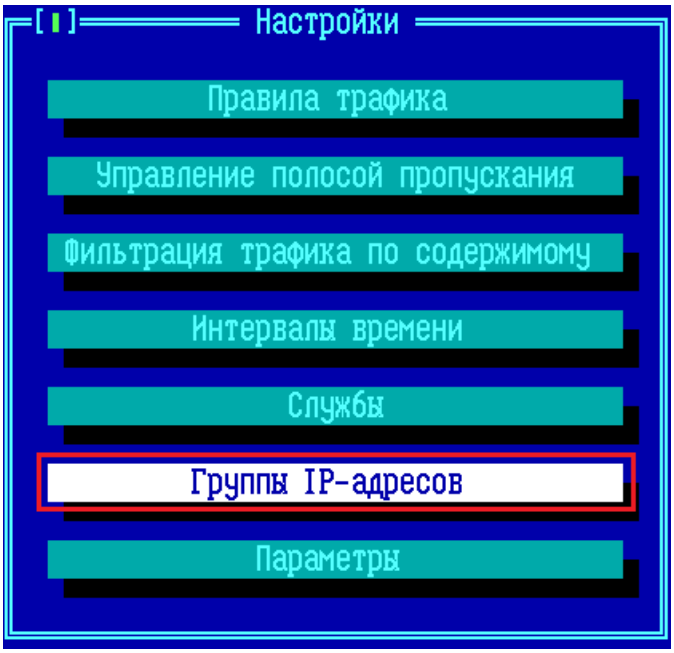


Рисунок 259 - Команда настройки групп IP-адресов параметров доступа

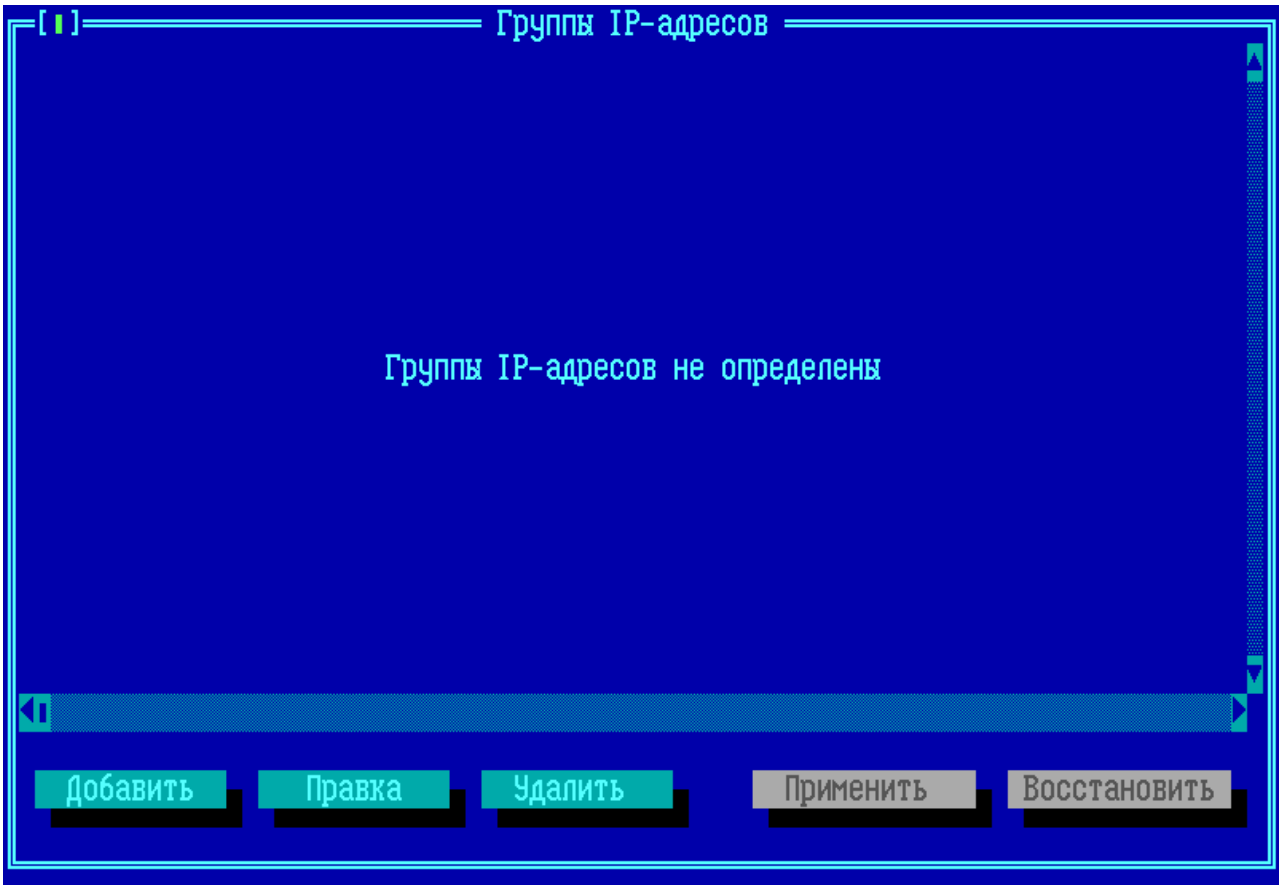


Рисунок 260 - Окно со списком групп IP-адресов

Находящиеся в списке группы IP-адресов используются при создании и изменении правил трафика (см. пункт «Вкладки «Источник» и «Назначение» правил трафика», описание последовательности действий «*Объект → Добавить*»).

Для добавления новой группы IP-адресов в список, нажмите в окне списка групп IP-адресов кнопку «*Добавить*» или клавишу <*Ins*>.

В открывшемся окне «Добавить группу» расположено несколько вкладок с параметрами создаваемой группы. Переход с активной вкладки на соседнюю осуществляется установлением курсора на вкладке и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

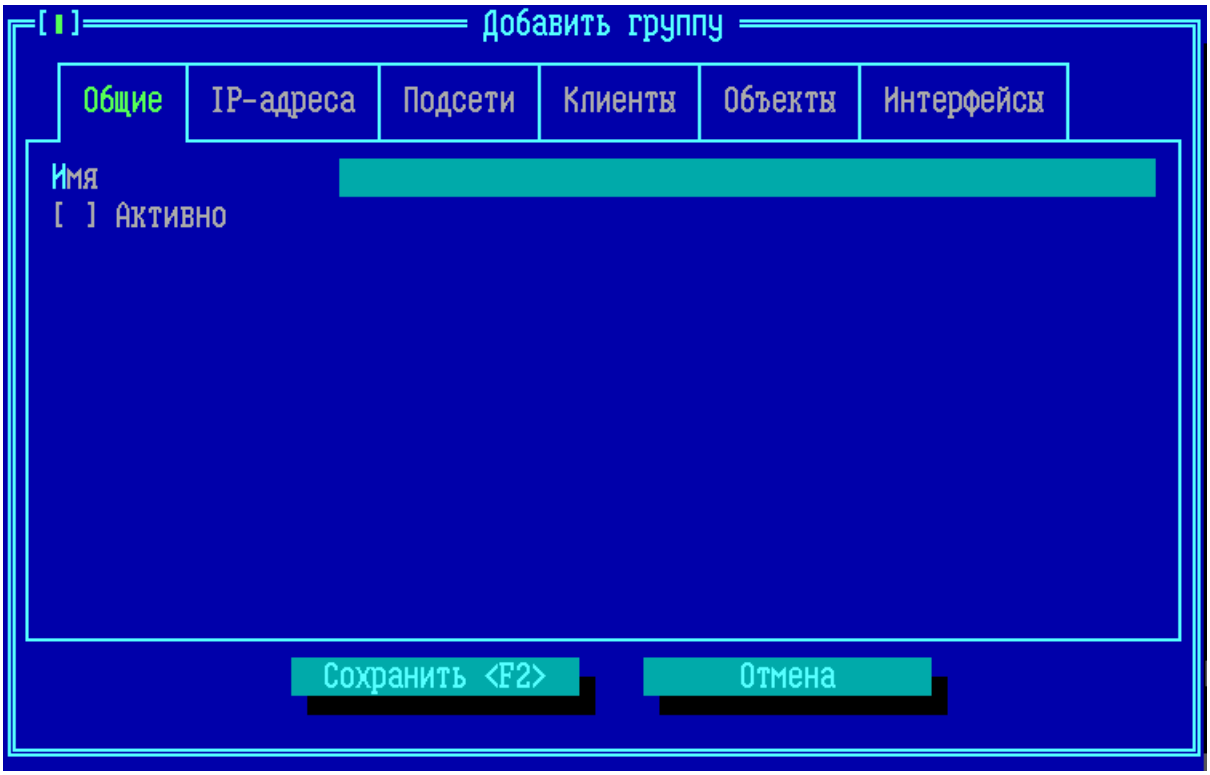


Рисунок 261 - Создание новой группы IP-адресов

Вкладка **Общие** содержит символьное название создаваемой группы, которое будет использоваться для привязки группы IP-адресов к тому или иному правилу трафика, и флаг «*Активно*», подтверждающий действие внесенных в группу изменений.

Вкладка **IP-адреса** содержит список входящих в группу отдельных IP-адресов (по умолчанию пустой). IP-адреса, вносимые в список, должны принадлежать диапазону описанных и разрешенных к маршрутизации IP-адресов (см. раздел «Порты ФПСУ»).

Вкладка **Подсети** содержит список входящих в группу подсетей, выбранных из маршрутизации (по умолчанию пустой). Подсети IP-адресов, вносимые в список должны принадлежать диапазону описанных и разрешенных к маршрутизации IP-адресов (см. раздел «Порты ФПСУ»).

Вкладка **Клиенты** содержит список (по умолчанию пустой) входящих в группу описателей ФПСУ-IP/Клиентов, выбранных из списка зарегистрированных на данном ФПСУ-IP криптосетей и групп клиентов.

Вкладка **Объекты** содержит список входящих в создаваемую группу других групп IP адресов (по умолчанию пустой).

Вкладка **Интерфейсы** содержит список входящих в создаваемую группу интерфейсов ФПСУ-IP (по умолчанию пустой).

После сохранения группы, она помещается в окно списка:

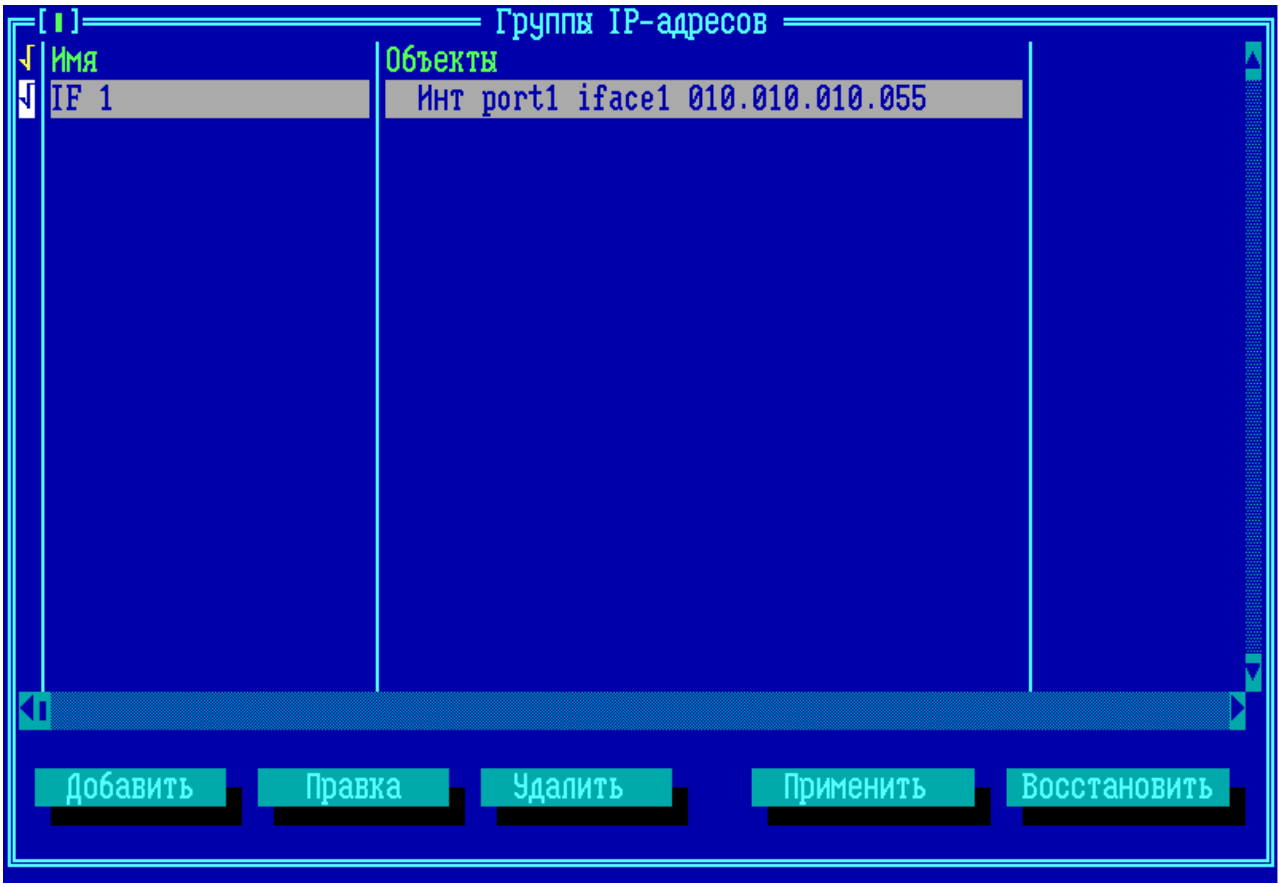


Рисунок 262 - В список групп IP-адресов добавлена новая запись

10. 7. Дополнительные параметры и защита от flood-атак

Команда «Параметры» меню «Параметры доступа» правил дополнительной фильтрации содержит список дополнительных опций межсетевого экрана.

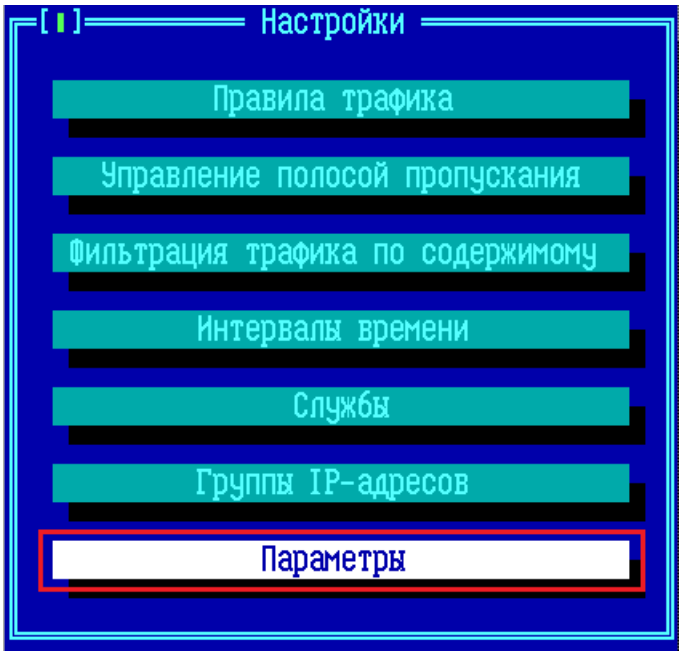


Рисунок 263 - Дополнительные параметры межсетевого экрана ФПСУ-IP

Окно состоит из трех вкладок. Первые две, **Соединения** и **Анти-флуд и СОВ**, предназначены для настройки системы защиты ФПСУ-IP от атак отказа в обслуживании (flood-атак). Переход между вкладками осуществляется установлением курсора на вкладке и нажатием сочетания клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

Вкладка **Соединения** содержит установленные по умолчанию параметры работы межсетевого экрана ФПСУ-IP с IP/TCP/UDP соединениями в обычном режиме и в режиме после обнаружения атаки.

Здесь настраиваются таймауты, по истечению которых неактивное соединение будет удалено из внутренней таблицы контроля соединений межсетевого экрана. Указывается два типа таймаутов – время удаления записи о соединении из таблицы при штатном режиме работы ФПСУ-IP (первый столбец), и время обнаружения атаки отказа в обслуживании (второй столбец).

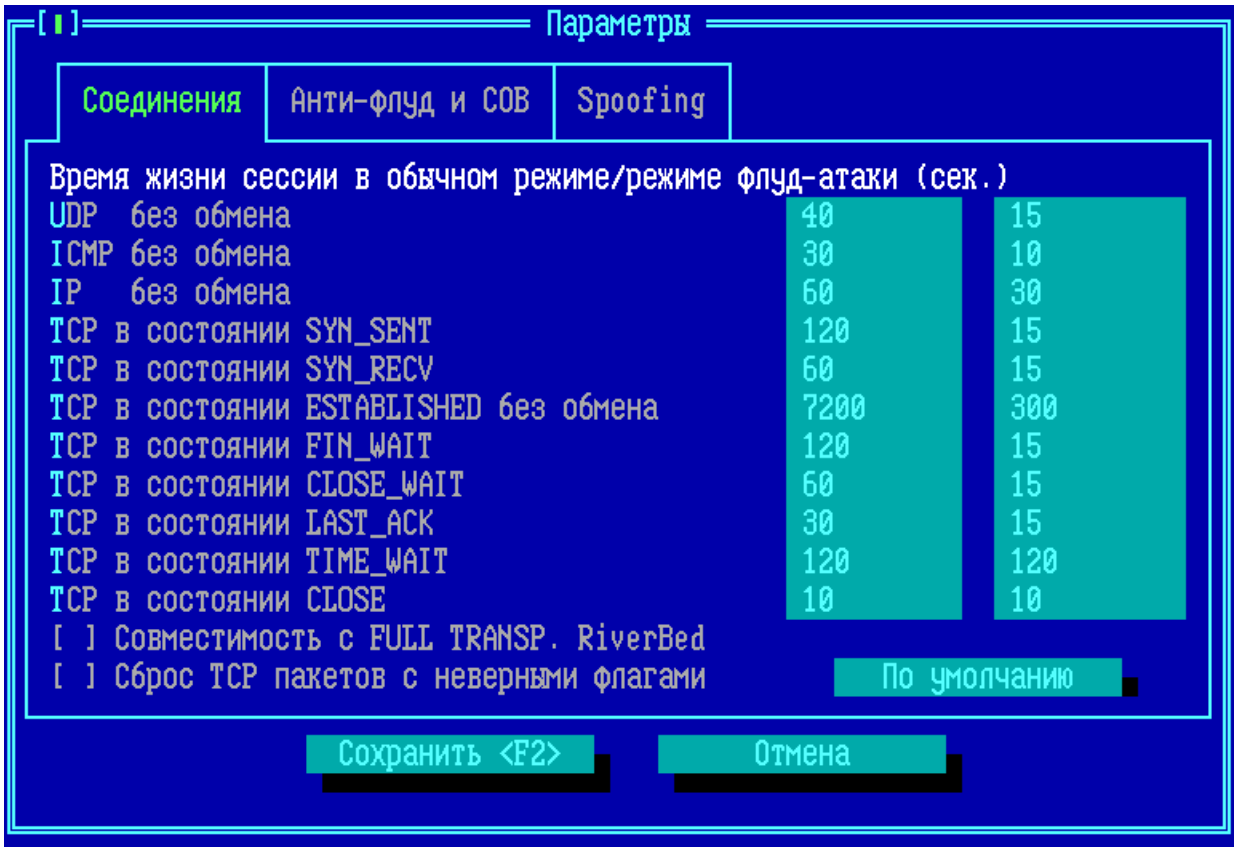


Рисунок 264 - Параметры ограничения соединений

Учитываются таймауты удаления из таблицы контроля соединения межсетевого экрана для следующих типов соединений:

UDP без обмена – соединением в этом случае считается трафик между уникальными UDP портами разных IP-адресов абонентов ФПСУ-IP. В случае отсутствия UDP-трафика по указанным портам, по таймауту запись о соединении удаляется из таблицы;

ICMP без обмена – соединением в этом случае считается ICMP обмен между двумя абонентами ФПСУ-IP. В случае отсутствия обмена ICMP-сообщениями в течение указанного таймаута, запись о соединении удаляется из таблицы;

IP без обмена – соединением в этом случае считаются все прочие виды трафика между двумя абонентами, не являющиеся TCP, UDP или ICMP. Запись удаляется из таблицы по таймауту при отсутствии новых обменов;

TCP в состоянии … – учитывается каждое соединение с разными TCP портами отправителя и получателя между любой парой абонентов ФПСУ-IP. По таймауту запись будет удалена из таблицы, и дальнейшее взаимодействие между этой парой абонентов должно будет начаться с повторного установления TCP-соединения. Новые пакеты, не

относящиеся к установлению TCP-соединения, после удаления записи из таблицы будут 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.

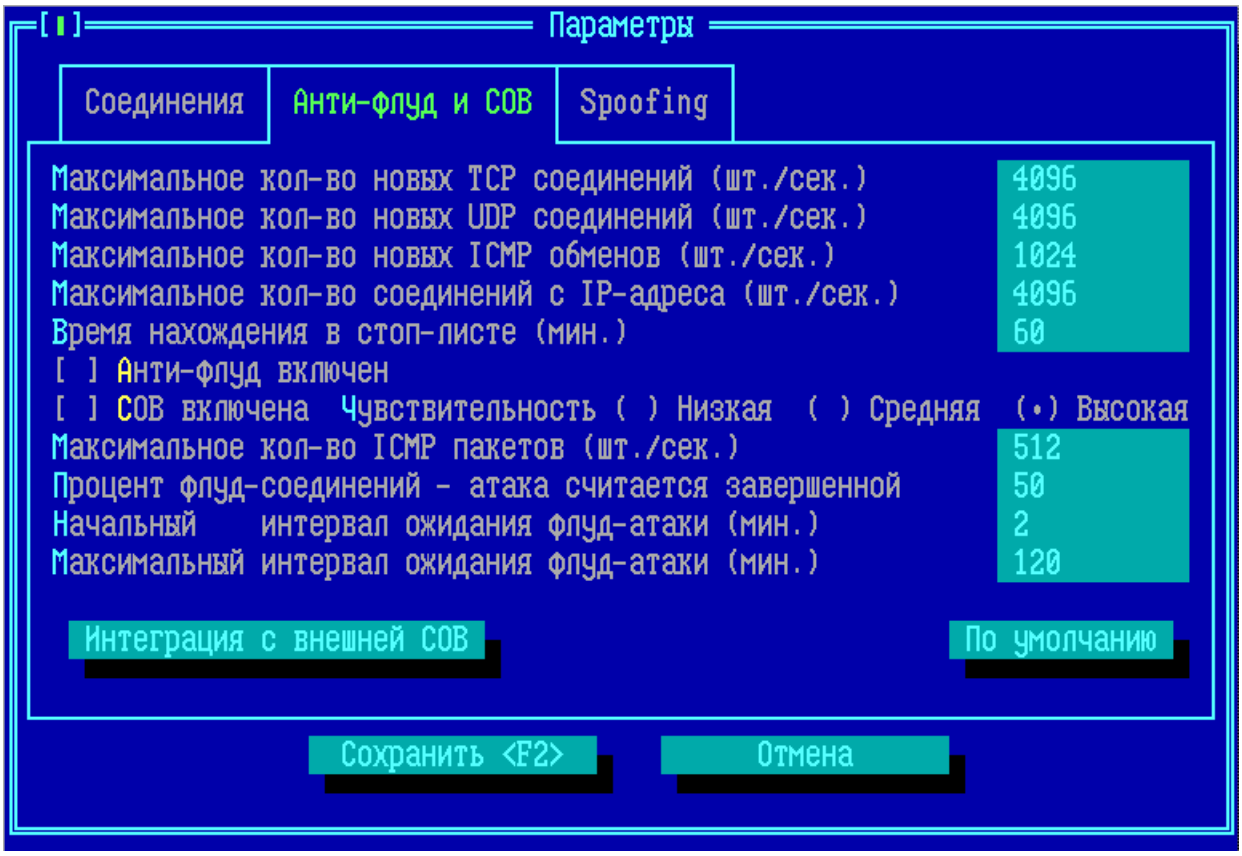


Рисунок 265 - Параметры работы ФПСУ-IP во время flood атаки

ФПСУ-IP переходит в режим защиты от атаки, если превышен хотя бы один из следующих критериев:

Максимальное кол-во новых TCP соединений (шт./сек.) – количество новых, то есть отсутствующих в таблице контроля соединений межсетевого экрана, TCP- соединений в секунду;

Максимальное кол-во новых UDP соединений (шт./сек.) – количество новых, то есть между новыми парами IP-адрес: UDP-порт, UDP- обменов в секунду;

Максимальное кол-во новых ICMP обменов (шт./сек.) – количество новых ICMP-обменов в секунду;

Максимальное кол-во новых ICMP пакетов (шт./сек.) – общее количество ICMP *эхо-запросов* (и только эхо-запросов) в секунду.

Во время защиты от flood-атаки, ФПСУ-IP начинает считать количество пакетов в секунду, отправленных с IP-адресов абонентов. Если это число превышает параметр ***«Максимальное кол-во соединений с IP-адреса (шт./сек.)»***, то этот IP-адрес заносится в стоп-лист, то есть все исходящие от него пакеты будут блокироваться.

Анти-флуд включен. Если флаг *«Анти-флуд включен»* установлен, то IP-адрес будет находится в стоп-листе время, указанное в поле ***«Время нахождения в стоп-листе (мин.)»***. Если флаг *«Анти-флуд включен»* не установлен, то IP-адрес будет находится в стоп-листе до перезагрузки ФПСУ-IP.

Флаг *«Анти-флуд включен»* влияет на действие/бездействие параметров ***«Максимальное кол-во новых TCP соединений (шт./сек.)»***, ***«Максимальное кол-во новых UDP соединений (шт./сек.)»***, ***«Максимальное кол-во новых ICMP обменов (шт./сек.)»***, ***«Максимальное кол-во соединений с IP-адреса (шт./сек.)»***. Если флаг снят, то ФПСУ-IP будет переходить в режим защиты от flood-атаки только в случаях полной загрузки оперативной памяти и в случае превышения порога ICMP эхо-запросов.

СОВ включена. Опция недоступна в данной версии.

Интеграция с внешней СОВ – команда перехода в интерфейс настройки взаимодействия ФПСУ-IP со сторонними средствами обнаружения вторжений (подробнее см. пункт «Взаимодействие со средствами обнаружения вторжений»).

На момент начала атаки ФПСУ-IP запоминает общее количество всех типов соединений – это значение потребуется для определения времени завершения атаки. Для начала выхода ФПСУ-IP из режима защиты от flood-атак, общее количество соединений сначала должно упасть до указанной в поле ***«Процент flood-соединений – атака считается завершенной»*** доли соединений, по сравнению с количеством соединений на начало атаки.

После *первоначального* уменьшения соединений до процентного значения, указанного в поле ***«Процент flood-соединений – атака считается завершенной»***, ФПСУ-IP запускает таймер обратного отсчета, с указанным в поле ***«Начальный интервал ожидания flood-атаки (мин.)»*** значением. Если в течение этого времени общее количество соединений не поднялось обратно выше порога, то атака считается завершенной и ФПСУ-IP переходит в обычный режим работы.

Если общее количество соединений за указанное время превысило пороговое значение, то ФПСУ-IP остается в режиме защиты от flood-атаки, таймер **увеличивается в полтора раза** и запускается заново. Максимальное значение таймера указывается в поле ***«Максимальный интервал ожидания Flood-атаки (мин.)»***.

Вкладка **Spoofing** содержит параметры, отвечающие за работу ФПСУ-IP с TCP-соединениями в режиме spoofing на медленных каналах связи.

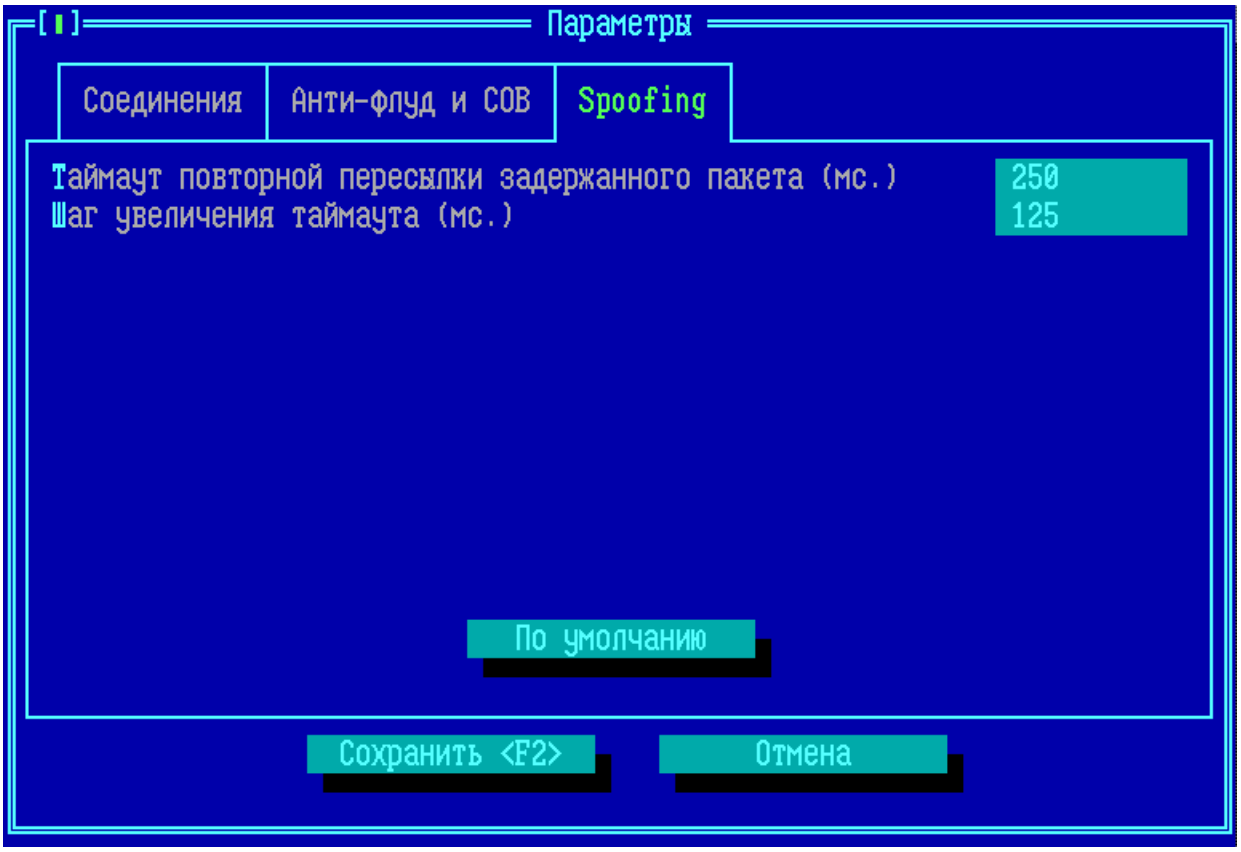


Рисунок 266 - Параметры передачи подтверждений в режиме Spoofing

Если в общих настройках правила трафика выключена опция *Spoof* (см. пункт «Общие настройки правил трафика»), то настройки на вкладке **Spoofing** никак не влияют на обработку и передачу пакетов, подпадающих под описываемое правило.

Если опция *Spoof* включена в общих настройках правила трафика, то ФПСУ-IP отправляет подтверждение о передаче пакета получателем отправителю самостоятельно, не дожидаясь такого подтверждения от получателя. После этого ФПСУ-IP буферизирует пакеты отправителя и периодически отправляет их получателю, повторяя при необходимости отправку в отсутствие подтверждения о получении.

Некоторые параметры такой отправки можно изменить:

Таймаут повторной пересылки задержанного пакета (мс.) – время в миллисекундах, через которое ФПСУ-IP будет проводить повторную пересылку пакета, в отсутствие ответа от получателя;

Шаг увеличения таймаута (мс.) – с каждым разом повторной отправки пакета, время очередного повтора пересылки увеличивается на указанное в этом параметре количество миллисекунд.

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 входящие Интернет-соединения, а также передавать ей список IP-адресов, к которым клиент может запрашивать доступ.

При передаче запросов клиентов ФПСУ-IP может производить трансляцию сетевого адреса (Network Address Translation - NAT) клиента во внутренний адрес защищаемой сети. Это обеспечивает клиентам возможность мобильной работы из любой точки сети (независимо от IP адреса) по предъявлению устройства, содержащего его идентификационные и ключевые данные (устройства VPN-Key). Администратор ФПСУ-IP может ограничить «миграцию» клиентов, указав IP- и MAC-адреса рабочих станций, с которых работа разрешена.

Для настройки ФПСУ-IP в части работы с клиентами выберите команду меню конфигурации «*Клиенты*». На экран будет выдано окно со списком зарегистрированных на ФПСУ-IP групп Криптосетей, пустое (при первом запуске) или содержащее список пар Криптосеть /логическая группа клиентов, которые будут обслуживаться ФПСУ-IP. На одном ФПСУ-IP может быть описано не более 128 логических групп, принадлежащих одной или нескольким Криптосетям Клиентов, в одной группе может быть зарегистрировано не более 1024 Клиентов.

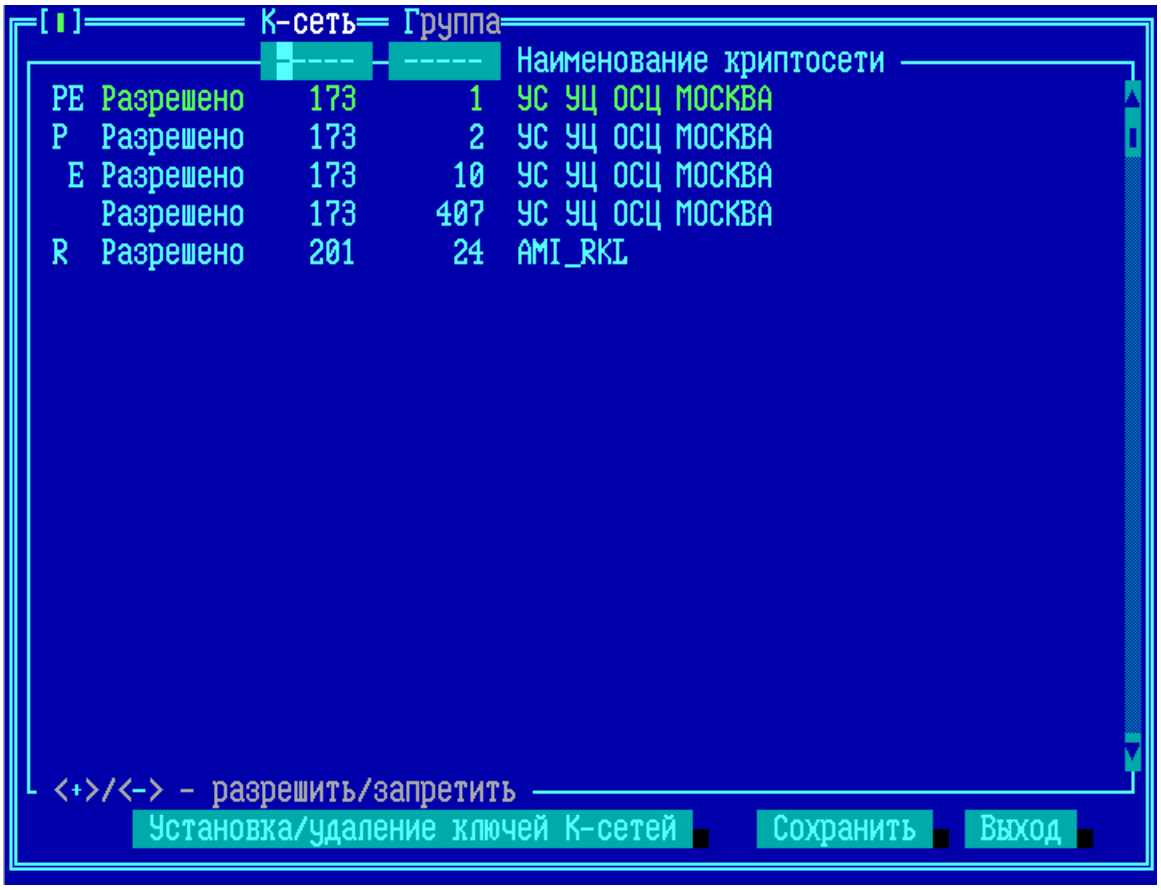


Рисунок 267 - Список групп Клиентов на ФПСУ-IP

Для установки или изменения правил работы клиентов, входящих в одну из групп списка, отметьте ее строкой выбора и нажмите клавишу <*Enter*> - см. пункт «Установка правил работы клиентов».

Для удаления записи логической группы отметьте его и нажмите <*Del*>. Для того чтобы разрешить (запретить) работу через ФПСУ-IP всех клиентов логической группы, правила работы которых уже установлены, выберите группу и нажмите клавишу <+> (<–>).

Для создания записи новой логической группы Клиентов, переведите курсор в список групп и нажмите клавишу <*Ins*> - см. раздел «Описание логической группы клиентов». Добавить группу можно только в том случае, если общесистемные ключи Криптосети установлены на ФПСУ-IP.

Для установки общесистемных ключей активизируйте опцию «*Установка/удаление ключей К-сетей*» – см. раздел «Установка и удаление общесистемных ключей».

Переход курсора на опцию «*Установка/удаление ключей К-сетей*» осуществляется по клавише <→>, <*Tab*>.

Для перехода к полям поиска группы нажмите клавишу <←→>. В полях задайте номер Криптосети и номер искомой группы, нажмите <*Enter*>, в списке групп будет выделена строка с найденной группой.

11. 1. Установка и удаление общесистемных ключей

По умолчанию, общесистемных ключей на ФПСУ-IP не установлено. Без установленных общесистемных ключей ФПСУ-IP не будет принимать соединения Клиентов.

Для установки нового общесистемного ключа на ФПСУ-IP выполните следующие действия:

В окне списка групп Криптосетей нажмите кнопку «*Установка/удаление ключей К-сетей*», после чего на экран монитора будет выдан список Криптосетей Клиентов, ключи которых были установлены на ФПСУ-IP.

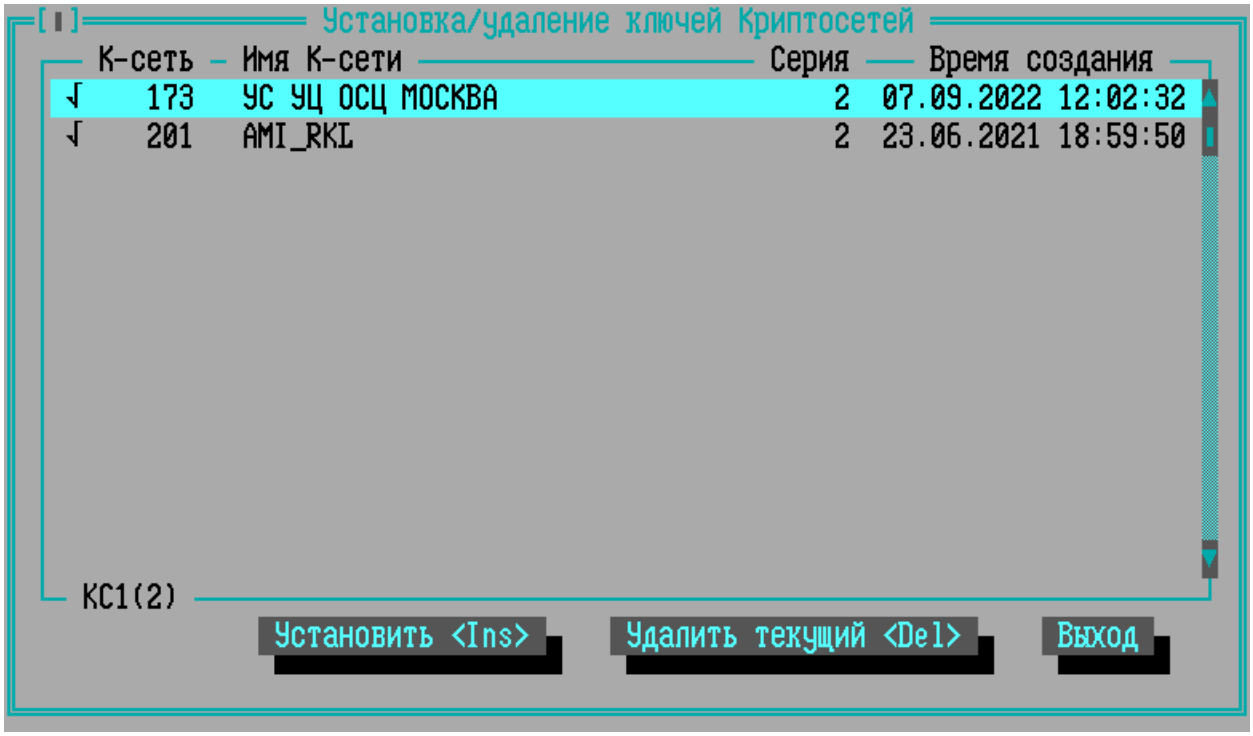


Рисунок 268 - Установленные на ФПСУ-IP общесистемные ключи Криптосетей Клиентов

Если строка слева помечена символом «√» – это означает, что ключи уже зарегистрированы на ФПСУ-IP, то есть для Криптосети создана хотя бы одна запись логической группы и определены правила работы клиентов. Такие ключи можно удалить

только после того, как удалены записи всех логических групп, принадлежащих данной 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 269 - 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.

В окне используемых на ФПСУ-IP Криптосетей и Групп ЦГКК нажмите клавишу <*Ins*>, после чего на экран будет выдан список Криптосетей, общесистемные ключи которых были ранее установлены на ФПСУ-IP.

В списке слева от Криптосети отметка «**R**» означает признак RKL-Криптосети, Клиенты такой Криптосети могут осуществлять удаленную загрузку ключевых данных Клиентов других Криптосетей. На ФПСУ-IP может быть активна только одна RKL-Криптосеть.

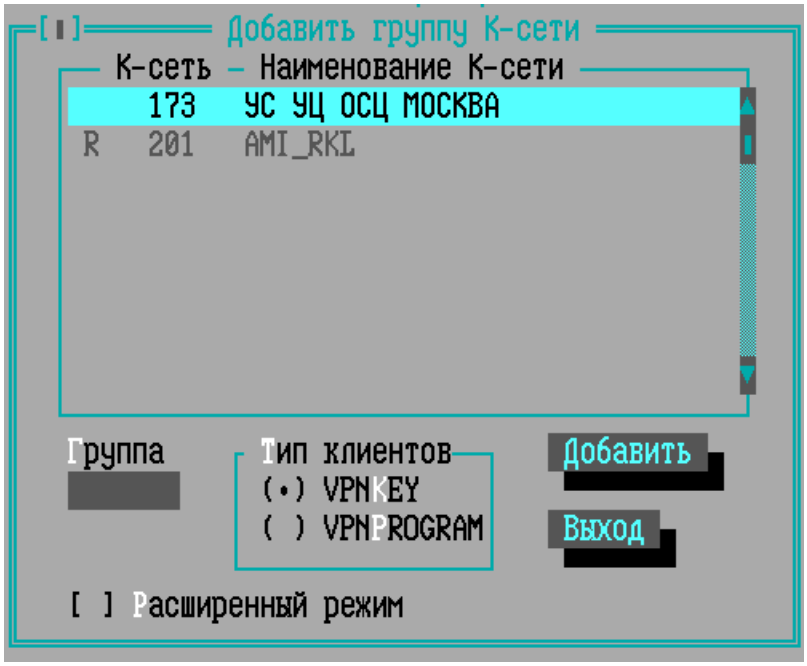


Рисунок 270 - Добавление группы клиентов

Выберите Криптосеть Клиентов, которой будет принадлежать описываемая группа, затем при помощи клавиши <→> или <*Tab*> переместитесь в поле «*Группа*», где следует ввести номер группы. Номер группы должен совпадать с логическим номером, присвоенным описываемой группе администратором программы ЦГКК.

Потом следует выбрать тип клиентов в создаваемой группе:

- VPNKEY – пользователи ПАК «ФПСУ-IP/Клиент», стандартный тип клиентов, ключевые данные которых хранятся в USB-устройстве VPN-Key. Далее по документу, если будет говориться о «клиенте» без уточнения, следует считать, что идет описание именно клиента типа VPN-Key.
- VPNPROGRAM – пользователи программного комплекса «ФПСУ-IP/Клиент», не использующие USB-устройство VPN-Key. Далее по документу, данный

пользователь будут упоминаться как «программный клиент» или «мобильный клиент».

ВНИМАНИЕ! Для поддержки пользовательских подключений VPNPROGRAM на ФПСУ-IP необходимо установить специальное обновление активации программных клиентов ФПСУ-IP!

Для групп RKL-Криптосети тип клиентов предустановлен, всегда VPNKEY.

Расширенный режим - при установлении флага клиенты данной группы смогут осуществлять взаимодействие с ЦРМК, ЦРМК-RKL, внешней системой RKL. Расширенный режим позволяет вести учет ключевых данных для устройств с установленным ПО ФПСУ-IP/Клиент с помощью ЦРМК-RKL.

После введения номера и указания типа группы клиентов нажмите кнопку «*Добавить*». В открывшемся окне введите имя для описателя группы клиентов и нажмите кнопку «*Сохранить*».

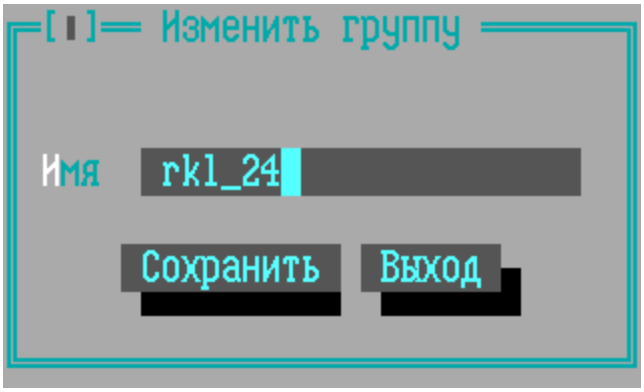


Рисунок 271 - Наименование группы клиентов

В результате выполнения команды пустая запись группы появится в окне групп ЦГКК.

На созданную группу будет по умолчанию выставлена метка «ЗАПРЕЩЕНО». Пока она выставлена, пользователям из указанной группы и криптосети будет запрещено выполнять соединение с ФПСУ-IP.

Если группа содержит описатели программных клиентов типа VPNPROGRAM, то она будет отмечена буквой «**P**» (program).

Если при создании группы был активирован флаг «Расширенный режим», то она будет отмечена буквой «**E**» (extended).

Группа RKL-Криптосети отмечается в списке буквой «**R**».

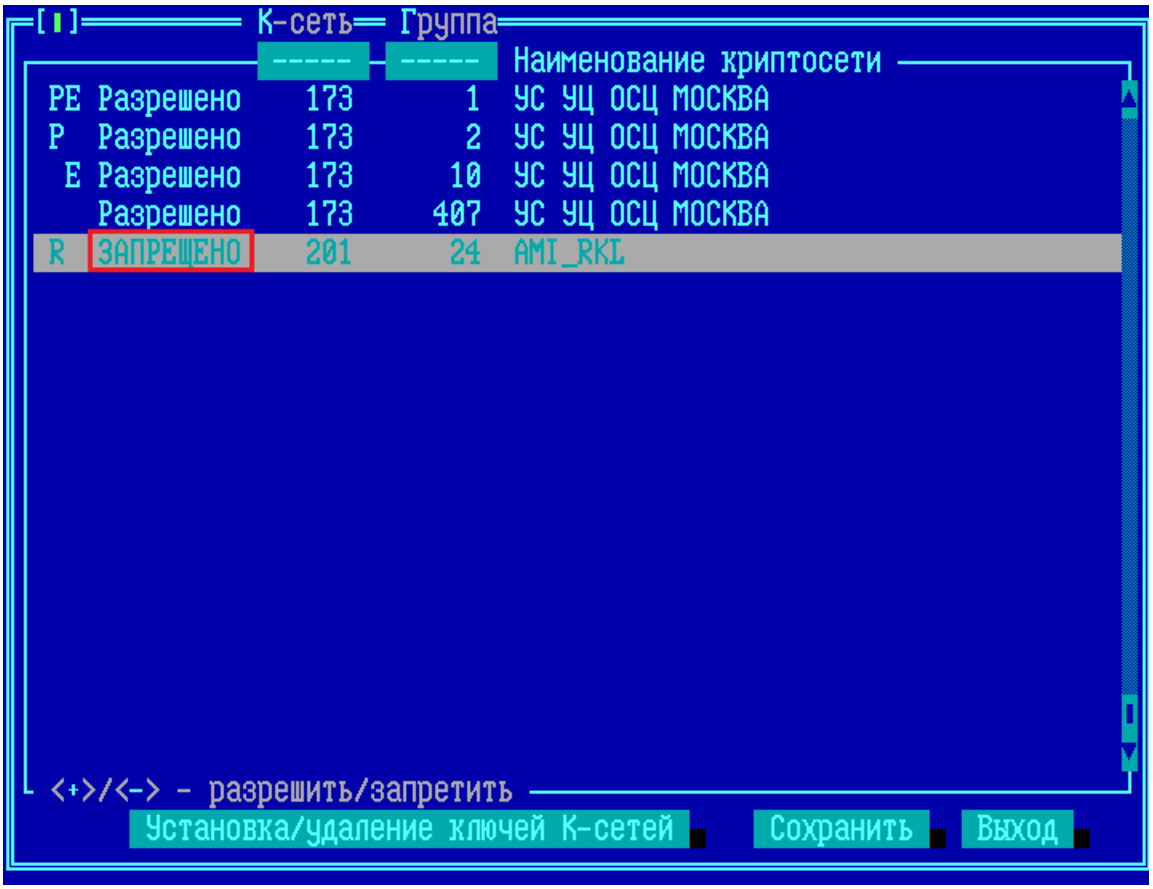


Рисунок 272 - Создана новая группа клиентов

Для разрешения соединений необходимо в группе создать хотя бы одно описание с правилами работы клиентов (см. пункт «Установка правил работы клиентов»), после чего установить курсор на группе в списке групп, и нажать клавишу <+>. Выдать разрешение на работу пустой группе невозможно.

11. 3. Установка правил работы клиентов

Параметры соединений клиентов группы с ФПСУ-IP определяются специальными записями – описаниями. Для перехода к списку существующих в группе описаний, выберите группу в окне списка групп криптосетей и нажмите клавишу <*Enter*>. В открывшемся окне списка описаний клиентов, пустом по умолчанию, администратор может создавать, удалять и разделять описания правил работы клиентов.

В левой верхней части окна выводится символы признака группы: «**P**» (группа мобильных клиентов), «**E**» (группа клиентов с расширенным режимом RKL), «**R**» (группа RKL-клиентов), подробнее см. пункт «Описание логической группы клиентов».

Для каждой логической группы может быть создано от одного до 64 описаний правил

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

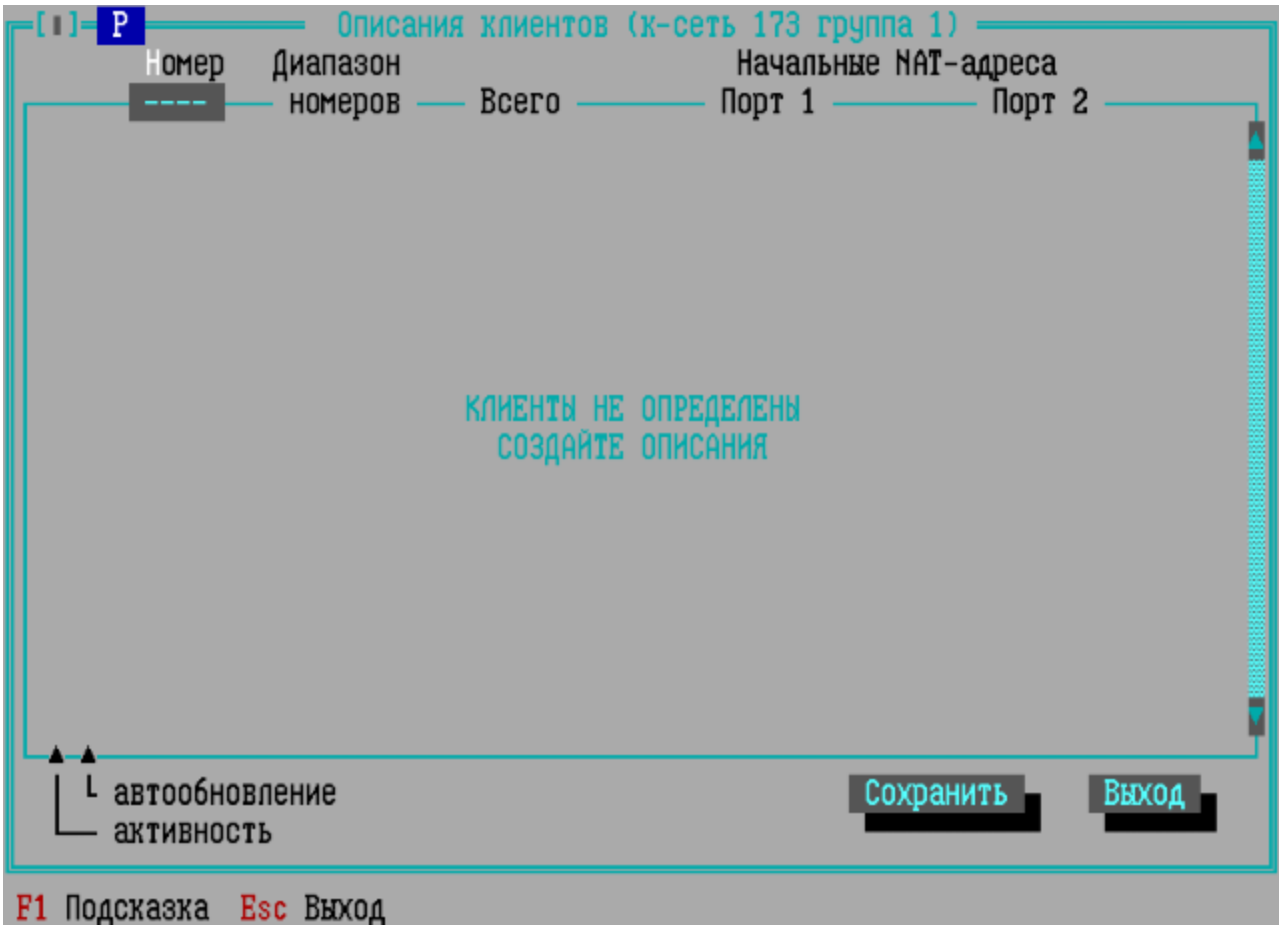


Рисунок 273 - Пустой список описаний новой группы

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»*.

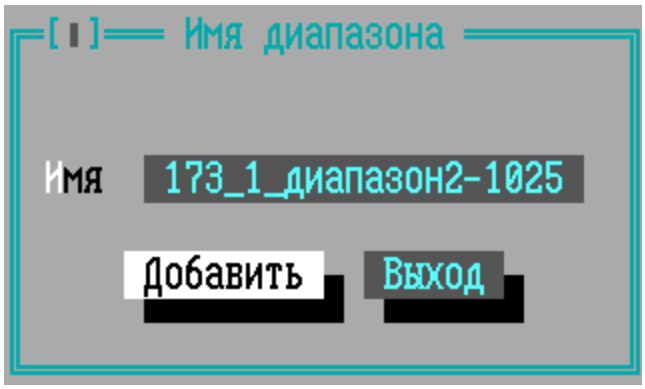


Рисунок 274 - Наименование диапазона номеров

Появится окно указания параметров взаимодействия клиентов и ФПСУ-IP.

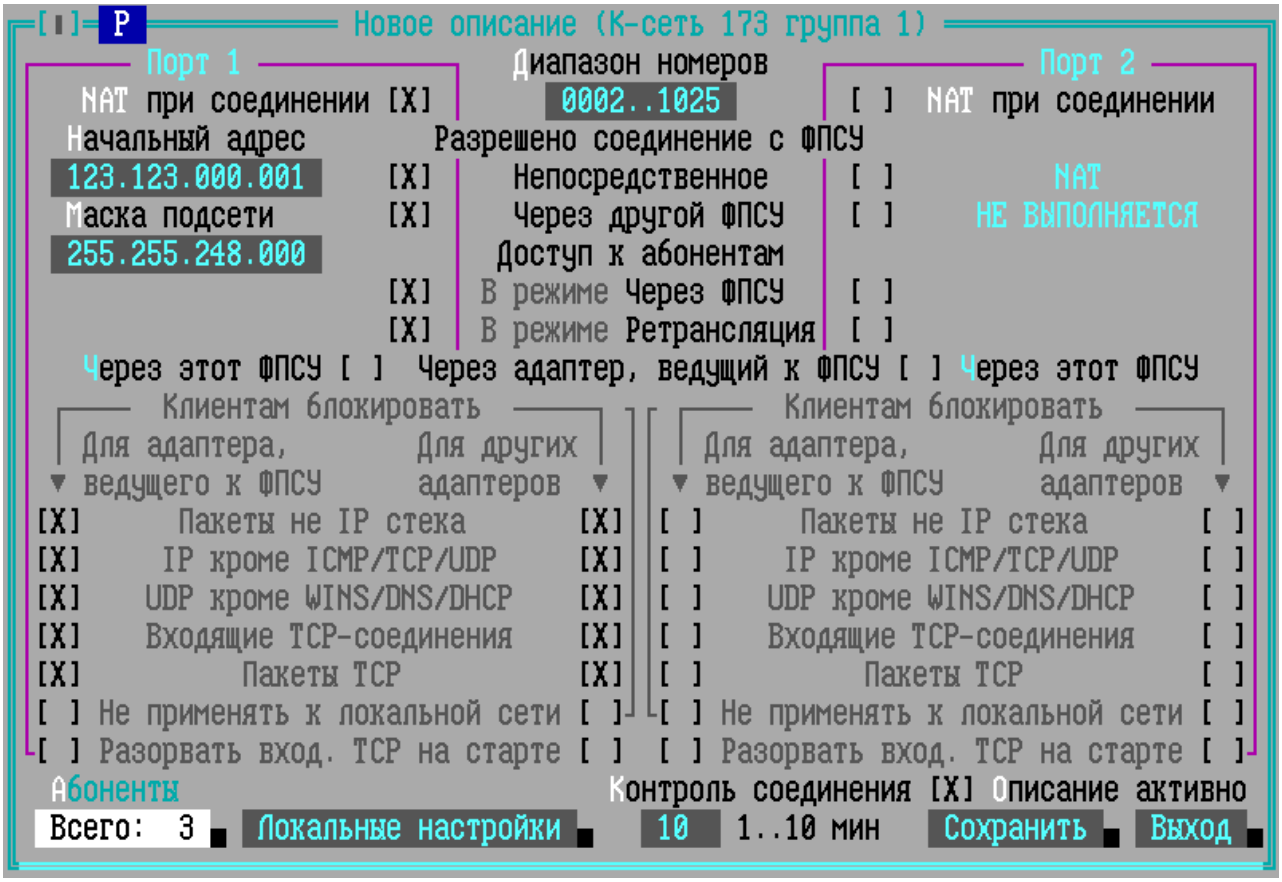


Рисунок 275 - Описание параметров работы диапазона Клиентов

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.

В поля открывшегося окна описания введите:

Параметр	Описание параметра
Диапазон номеров	- диапазон уникальных номеров клиентов, для которых устанавливаются правила. Диапазоны номеров различных описаний не могут пересекаться;
NAT при соединении	- указание ФПСУ-IP производить трансляцию реальных IP адресов клиентов описываемого диапазона во внутренние (виртуальные) адреса защищаемой подсети при соединениях со стороны данного порта;
Начальный адрес	- в случае применения NAT-трансляции первый из IP адресов внутренней подсети, в который будет транслироваться реальный IP-адрес первого клиента описываемого диапазона;
Маска подсети	- в случае применения NAT-трансляции используется маска внутренней подсети, рассчитанная на количество клиентов описываемого диапазона. ВНИМАНИЕ! В диапазон адресов, образованный начальным адресом и маской, не должен попадать ни один реально существующий IP-адрес, указанный в конфигурации ФПСУ-IP;
Разрешено соединение через ФПСУ	- разрешение ФПСУ-IP производить соединения с клиентами со стороны данного порта в задаваемом режиме (обмениваться данными с описываемыми клиентами непосредственно или через другой ФПСУ-IP). Если режим соединений с клиентами не регламентируется, включите при помощи клавиши <*Пробел*> оба флага. Если ни один флаг не установлен – доступ клиентам со стороны данного порта ФПСУ-IP предоставляться не будет;
Разрешен доступ к абонентам	- разрешение ФПСУ-IP предоставлять клиентам, работающим со стороны данного порта, доступ к станциям назначения (со стороны любого порта) только в задаваемом режиме. Если режим соединений ФПСУ-IP с рабочими станциями не регламентируется, включите при помощи клавиши <*Пробел*> оба флага. Если ни один флаг не

Параметр	Описание параметра
	установлен, доступ клиентам со стороны данного порта ФПСУ-IP к другим рабочим станциям предоставляться не будет;
Через адаптер, ведущий к ФПСУ	- опция, изменяющая сетевые настройки на стороне рабочей станции Клиента. После её включения, все IP-пакеты, отправляемые рабочей станцией Клиента через сетевой адаптер, ведущий к ФПСУ-IP, будут зашифрованы и отправлены в туннель к ФПСУ-IP. ВНИМАНИЕ! При включении опции открытые соединения рабочей станции Клиента через ведущий к ФПСУ-IP сетевой адаптер будут невозможны;
Клиентам блокировать	- указание клиентам при работе со стороны данного порта ФПСУ-IP блокировать соответствующие соединения. Установленные администратором ФПСУ-IP ограничения будут выполняться на всех указанных сетевых адаптерах рабочих станций клиентов принудительно, независимо от собственных установок клиентов. ВНИМАНИЕ! Для клиентов типа VPNPROGRAM такой вид дополнительной настройки недоступен;
Не применять к локальной сети	- флаг, разрешающий не применять указанные блокировки опции «Клиентам блокировать» для сетевых взаимодействий в пределах локальной сети рабочей станции Клиента.
Разорвать вход. TCP на старте	- указание принудительного разрыва всех входящих TCP сессий на рабочей станции Клиента, в момент установления соединения с ФПСУ.
Абоненты	- список IP-адресов абонентов, к которым клиенты могут запрашивать доступ при соединении с ФПСУ-IP. Этот список будет передаваться клиентам при установке туннеля и дополнять их собственные списки абонентов.
Локальные настройки	- устанавливаемые для ФПСУ-IP/Клиентов локальные настройки, передаются с ФПСУ-IP в момент соединения с ФПСУ-IP/Клиентом;

Параметр	Описание параметра
Контроль соединения	- временной интервал (от 1 до 10 минут), по истечении которого после получения последних данных от клиента ФПСУ-IP будет производить контроль соединения с ним. В случае отсутствия связи соединение будет сброшено. Для клиентов RKL-Криптосети временной интервал (от 1 до 255 минут), поле может быть пустым, если контроль не требуется. 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.

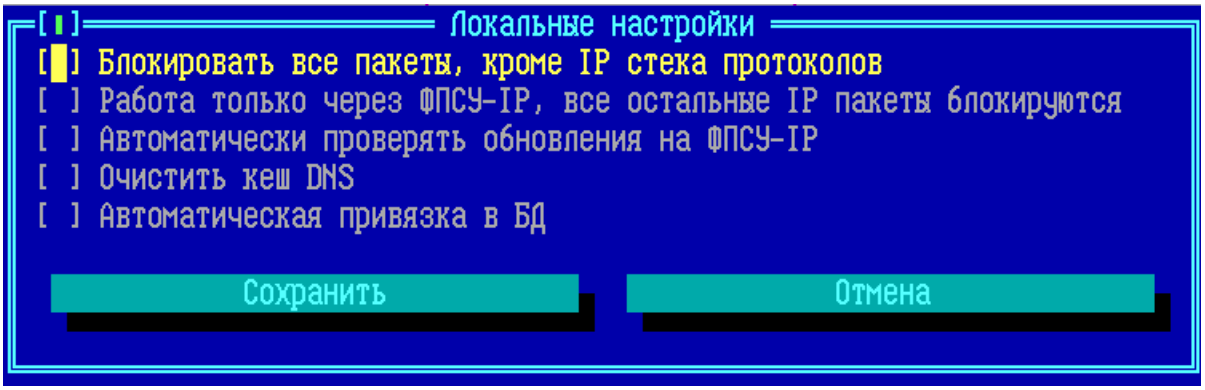


Рисунок 276 - Локальные настройки ФПСУ-IP/Клиента, устанавливаемые на ФПСУ-IP

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.

Автоматически проверять обновления на ФПСУ-IP - флаг, при установке которого при каждом соединении с ФПСУ-IP (основным или дополнительным) ФПСУ-IP/Клиент будет запрашивать у него наличие новых версий программного обеспечения ФПСУ-IP/Клиента.

Очистить кэш DNS - флаг, при установке которого выполняется сброс кэша DNS на рабочей станции ФПСУ-IP/Клиента при установления соединения с ФПСУ-IP.

Автоматическая привязка в БД - установленный флаг позволяет привязать Клиента к рабочей станции или устройству с установленным программным обеспечением ФПСУ-IP/Клиент, чтобы пользователь мог работать с этим Клиентом только на одном АРМ. Привязка клиента хранит данные о серийных номерах ОС (только для Windows), материнской платы и системного диска устройства с установленным программным обеспечением ФПСУ-IP/Клиент в базе данных на ФПСУ-IP. Каждый раз при подключении ФПСУ-IP/Клиента к ФПСУ-IP эти данные сверяются, в случае подключения клиента с другого устройства работа данного клиента блокируется. База данных с привязками клиентов синхронизируется с дополнительным ФПСУ-IP, заданным в настройках ФПСУ-IP/Клиента.

Нажатие кнопки *«Сохранить»* или клавиши *<F2>* сохраняет локальные настройки и возвращает в окно описания диапазона номеров группы клиентов.

Для создания или корректировки списка абонентов, нажмите кнопку «Абоненты», после чего откроется окно списка передаваемых клиенту IP-адресов.

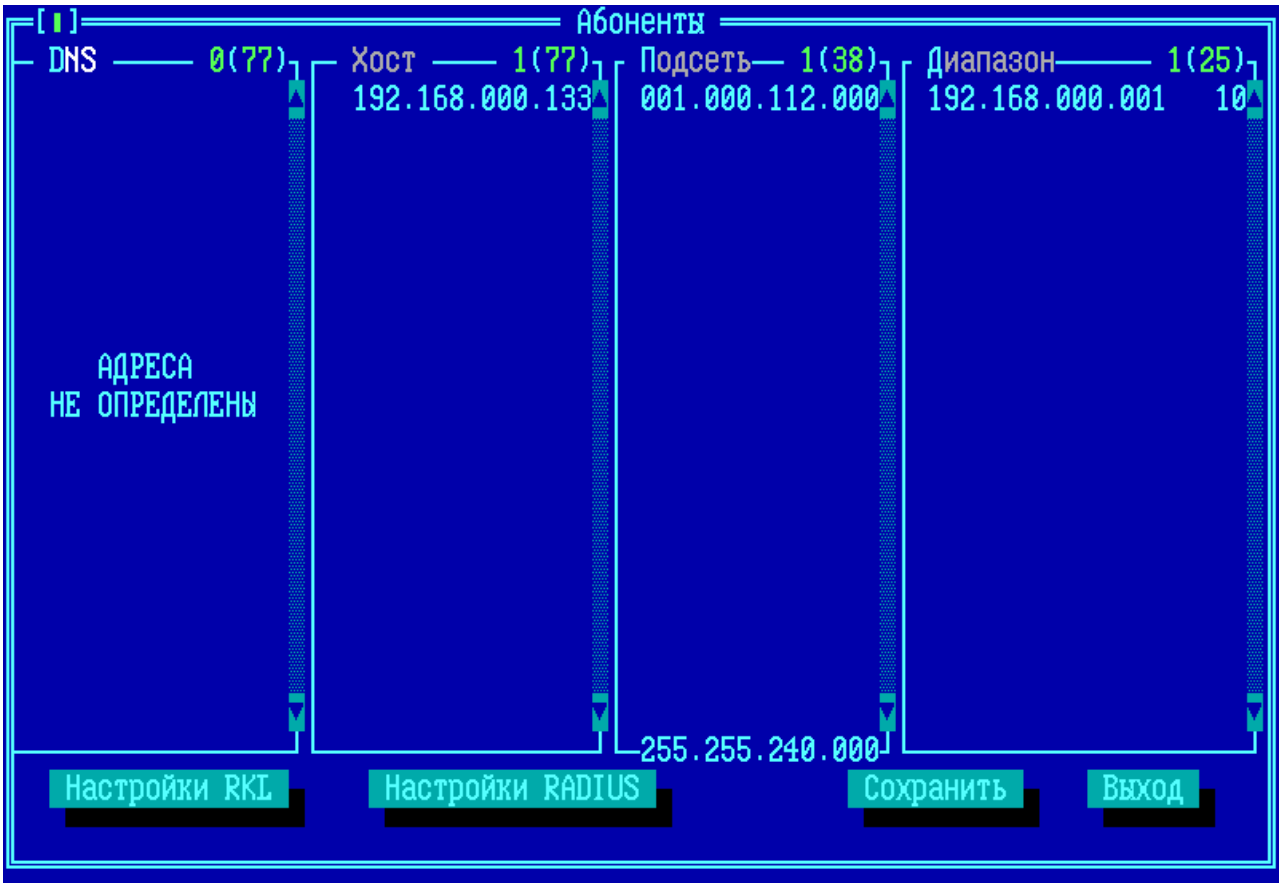


Рисунок 277 - Абоненты ФПСУ-IP, доступные ФПСУ-IP/Клиенту

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 «было_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

Сервер лицензирования доступен в сети (см.пункт «было_Настройка диапазона клиентов на работу с Сервером лицензирования»).

Настройки RADIUS – устанавливаются для аутентификации ФПСУ-IP/Клиентов в сети (см. пункт «Настройка диапазона клиентов на работу с Radius»).

После установки всех параметров в окне «Абоненты» активизируйте поле «*Сохранить*», после чего будет произведен выход в окно списка описаний клиентов в группе.

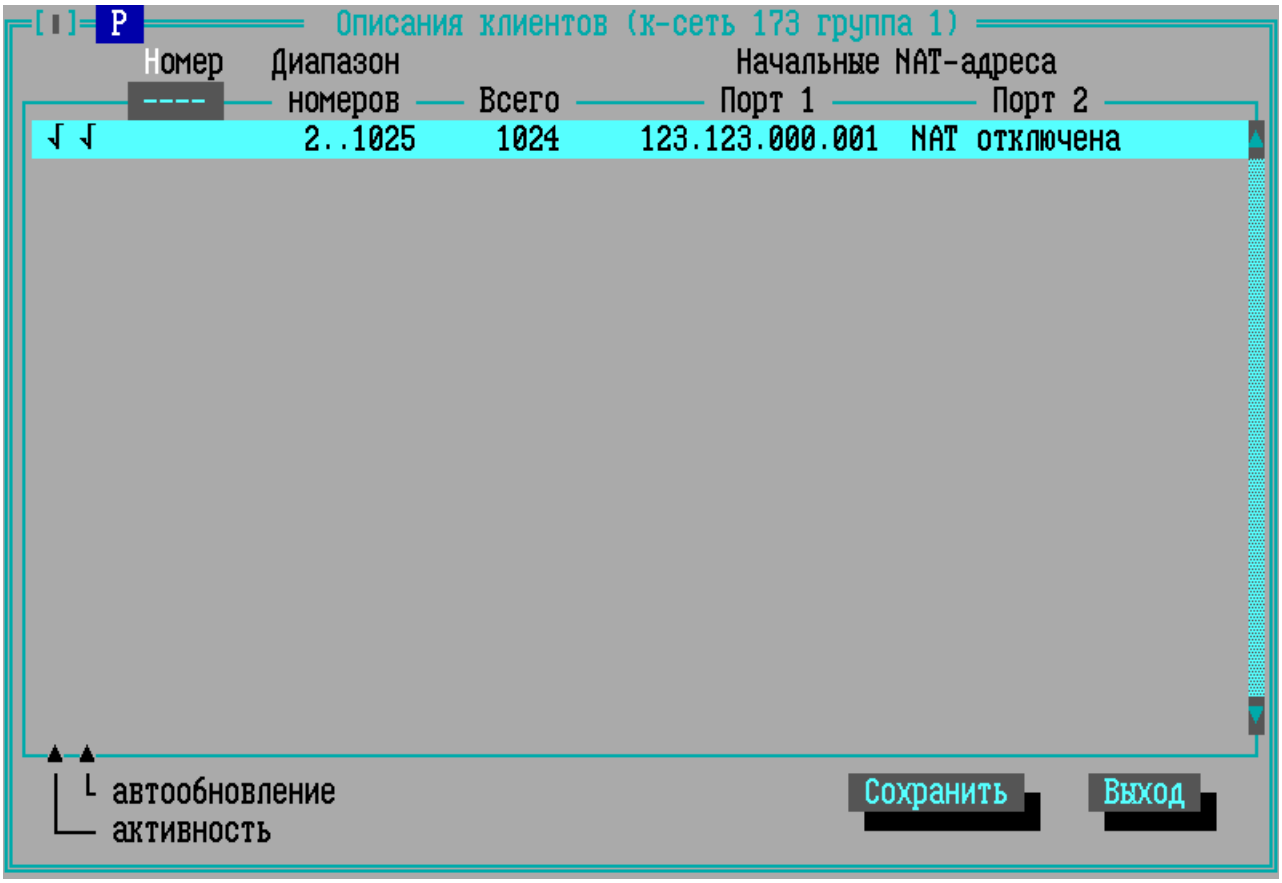


Рисунок 278 - Список описаний диапазонов Клиентов

Для перехода к форме списка описаний отдельного клиента нажмите клавишу <*Пробел*>.

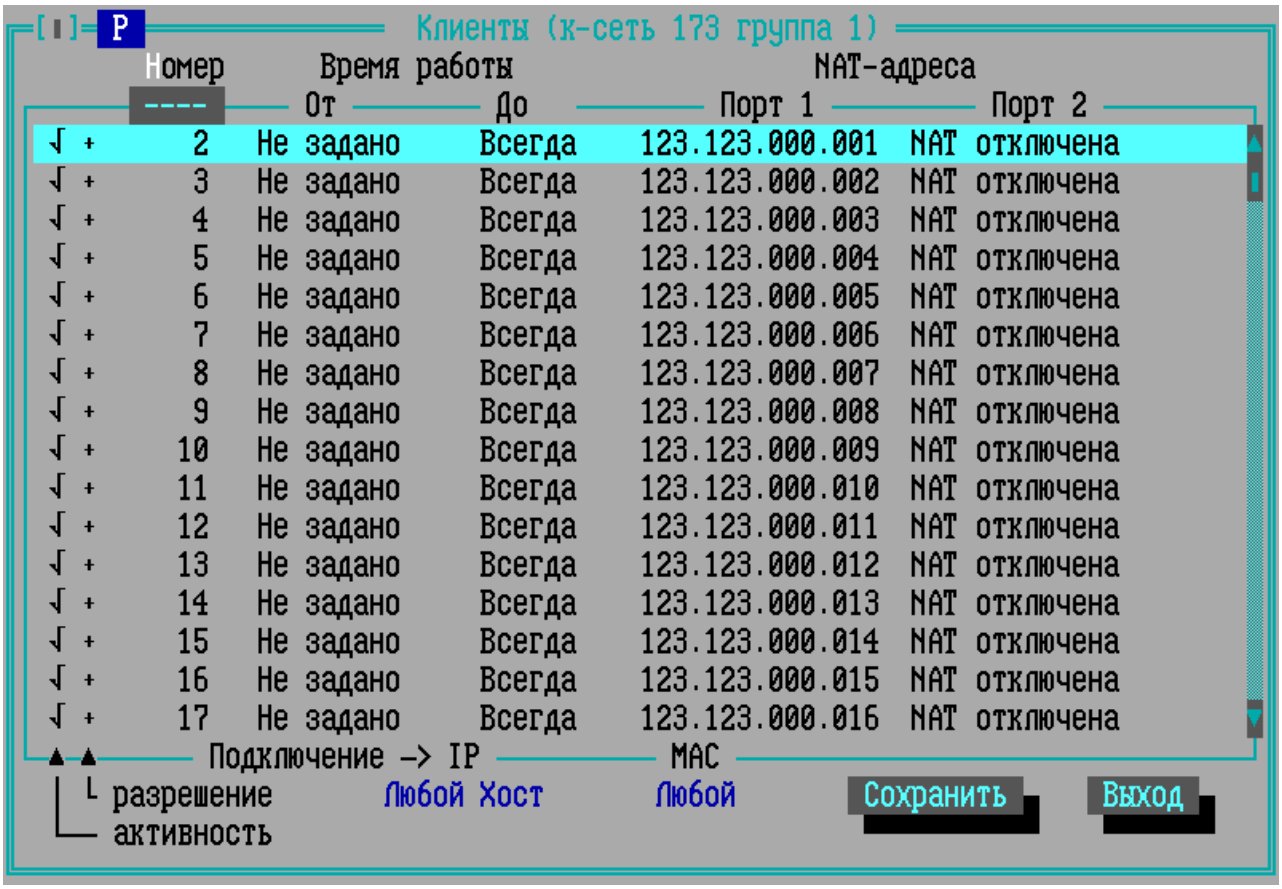


Рисунок 279 - Список зарегистрированных в группе Клиентов

Знак «√» 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* ↑↓> (<*Alt* ↑↓>).

11. 4. RKL для обновления ключевых данных клиентов

Настройки RKL доступны на ФПСУ-IP с установленной подсистемой RKL, позволяют проводить удаленную загрузку ключевых данных клиентов с ФПСУ-IP на устройства с установленным ПО ФПСУ-IP/Клиент.

Удаленная загрузка ключевых данных проводится в двух режимах, получения/обновления ключевых данных по запросу с использованием RKL-токена и автоматического обновления ключевых данных при обнаружении новой серии ключевых данных на ФПСУ-IP.

При получении/обновлении ключевых данных по запросу необходимо подключение RKL-токена в USB-порт рабочей станции или устройства с установленным программным обеспечением ФПСУ-IP/Клиент. ФПСУ-IP/Клиент осуществляет взаимодействие с ФПСУ-RKL, все другие соединения блокируются. Взаимодействие осуществляется по следующей схеме:

- ФПСУ-IP/Клиент с RKL-токеном запрашивает ключевые данные у ФПСУ-RKL.
- В расширенном режиме ФПСУ-RKL запрашивает разрешение получения/обновления ключевых данных на ЦРМК-RKL.
- ЦРМК-RKL разрешает получение/обновление ключевых данных.
- ФПСУ-RKL выдает новый ключ ФПСУ-IP/Клиенту и ключ устанавливается на ФПСУ-IP/Клиенте.
- RKL-токен извлекается, ФПСУ-IP/Клиент устанавливает соединение с ФПСУ-IP на новой серии ключа.

В расширенном схеме взаимодействия ЦРМК-RKL позволяет вести учет ключевых данных для устройств с установленным ПО ФПСУ-IP/Клиент. ЦРМК-RKL хранит данные о ФПСУ-IP/Клиенте, его VPN-профиле, выданных ключевых данных.

В упрощенной схеме взаимодействия запрос ключевых данных не перенаправляется на ЦРМК-RKL, учет ключевых данных не ведётся (шаги 2,3 на схеме исключаются).

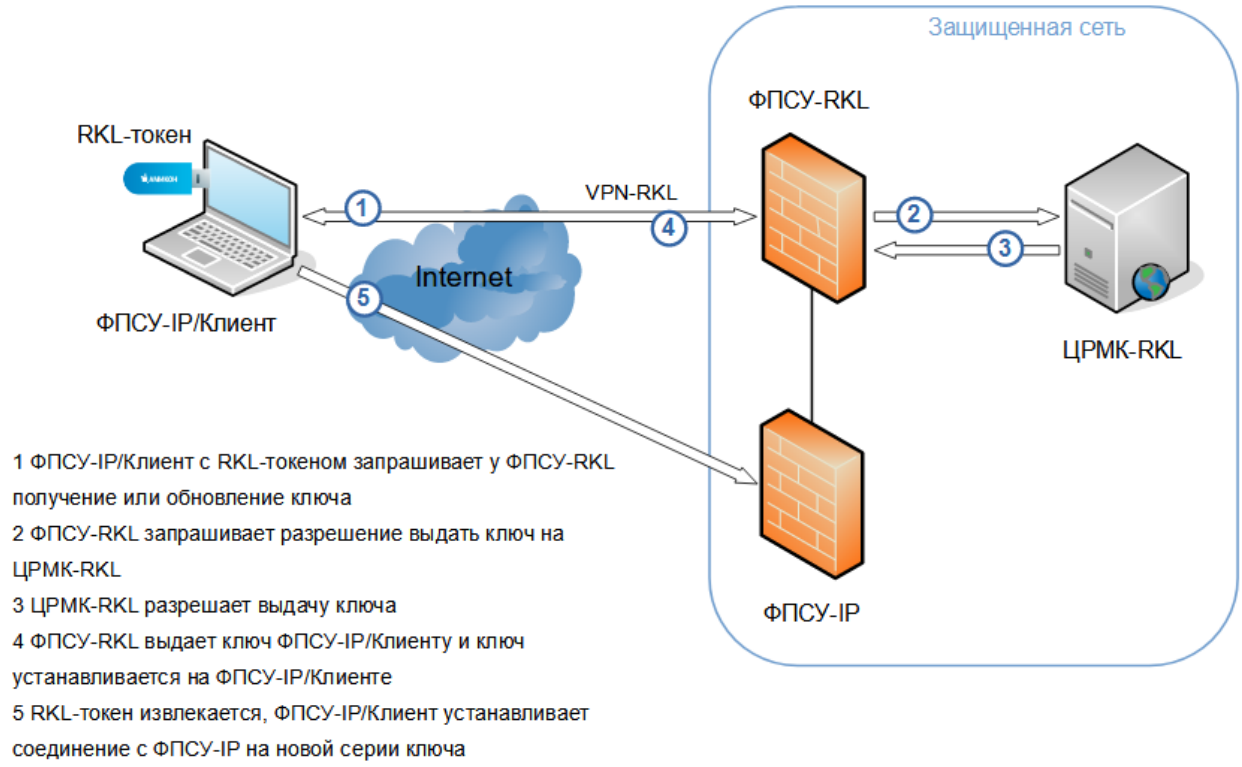


Рисунок 280 - Схема получения/обновления ключа по запросу с RKL-токеном

При автоматическом обновлении ключевых данных ФПСУ-IP/Клиент запрашивает обновление ключа у ФПСУ-RKL при обнаружении новой серии ключевых данных на ФПСУ-IP. ФПСУ-IP/Клиент осуществляет взаимодействие с ФПСУ-RKL через ФПСУ-IP. Взаимодействие осуществляется по следующей схеме:

- ФПСУ-IP/Клиент устанавливает соединение с ФПСУ-IP.
- ФПСУ-IP сообщает о наличии новой серии ключа.
- ФПСУ-IP/Клиент запрашивает у ФПСУ-RKL смену ключевых данных, ФПСУ-IP перенаправляет запрос ФПСУ-RKL.
- ФПСУ-RKL запрашивает разрешение выдать ключ на ЦРМК-RKL.
- ЦРМК-RKL разрешает обновление ключа.
- ФПСУ-RKL выдает ключ ФПСУ-IP/Клиенту через канал с ФПСУ-IP и ключ устанавливается на ФПСУ-IP/Клиенте.
- ФПСУ-IP/Клиент устанавливает соединение с ФПСУ-IP на новой серии ключа.

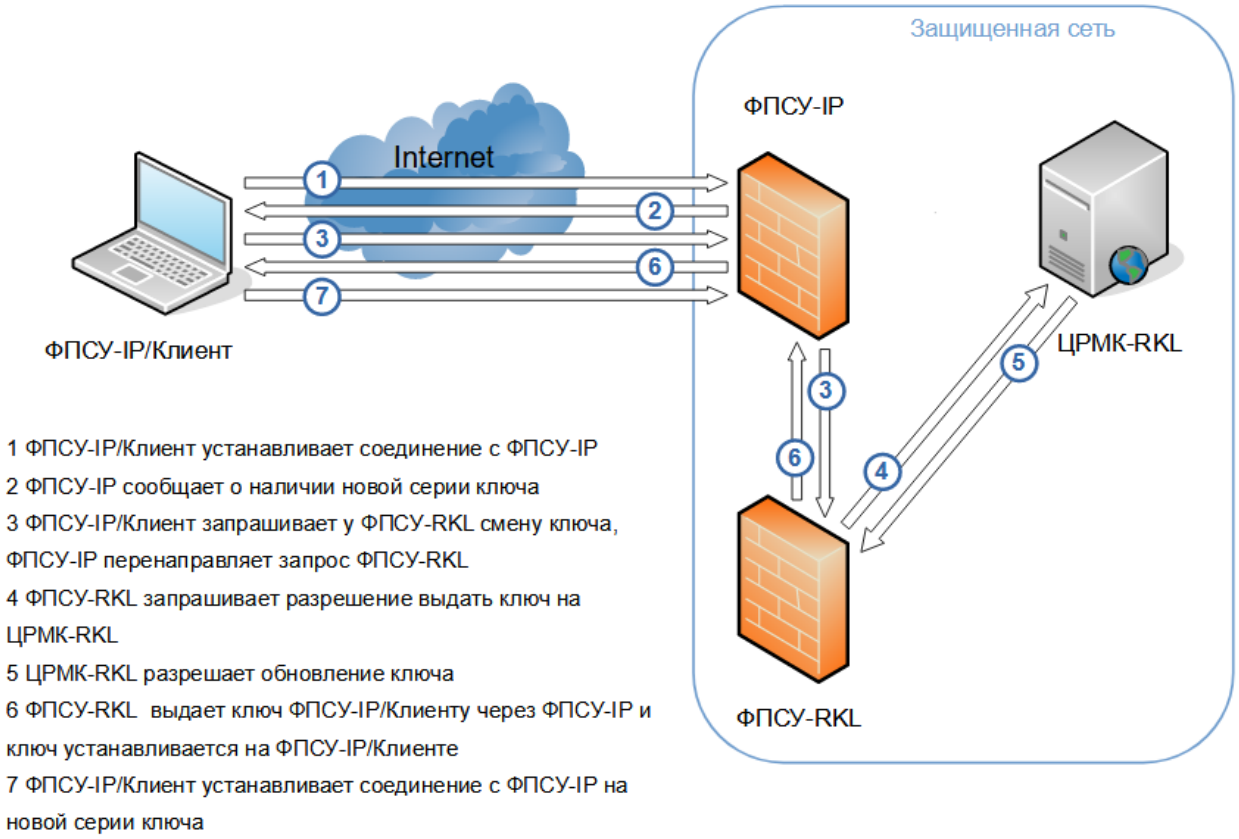


Рисунок 281 - Схема автоматического обновления ключа («зацепление»)

Рекомендуемый порядок действий при настройке:

Подсистема RKL для работы с ЦРМК и сервером лицензирования требует установки аддона rkl.

Настройка клиентов RKL-токенов требуется только при получении/обновлении ключевых данных с подключением RKL-токена.

1. Построить туннель между ФПСУ-IP и ФПСУ-RKL (см. раздел «Описание параметров удаленных ФПСУ-IP»).

2. В упрощенном режиме на ЦГКК, в расширенном режиме на ЦРМК зарегистрировать две Криптосети Клиентов, одну с признаком RKL для клиентов RKL-токенов, другую для целевых клиентов с VPN-Key. Изготовить VPN-ключи для клиентов этих Криптосетей.

на ФПСУ-RKL:

3. Установить подсистему RKL, для расширенного режима установить дополнение

rkl. Описание установки приведено в пункте «Установка дополнений/изменений». Должна быть предустановлена подсистема CLIENT.

4. Загрузить общесистемные ключевые данные RKL-Криптосети Клиентов и целевой Криптосети Клиентов (см. пункт «Установка и удаление общесистемных ключей»).

5. Создать группы клиентов этих Криптосетей (см. пункт «Описание логической группы клиентов»).

6. В группе RKL-Криптосети задать клиентов RKL-токенов и установить для них настройки RKL (см. пункты «Установка правил работы клиентов» и «Настройка диапазона клиентов на работу с RKL»).

7. В группе целевой Криптосети задать клиентов VPN-Key и установить для них настройки RKL.

8. Для расширенного режима настроить ЦРМК. В меню выбрать пункт «Сетевые сервисы → Серверы ЦРМК», задать URL ЦРМК для группы или диапазона групп обеих Криптосетей. Описание приведено в пункте «Серверы ЦРМК и Сервер лицензирования».

на ФПСУ-IP целевом:

9. Должна быть предустановлена подсистема CLIENT.

10. Загрузить общесистемные ключевые данные целевой Криптосети Клиентов.

11. Создать группу клиентов целевой Криптосети.

12. В группе целевой Криптосети задать клиентов VPN-Key и установить для них настройки RKL.

11. 4. 1. Настройка диапазона клиентов на работу с RKL

В зависимости от используемой схемы обновления ключевых данных на ФПСУ-IP/Клиентах (см. пункт «RKL для обновления ключевых данных клиентов») установите на целевом ФПСУ-IP и на ФПСУ-RKL настройки RKL для клиентов VPN-Key и клиентов RKL-токенов.

Настройки RKL устанавливаются для диапазона клиентов из группы Криптосети, чтобы перейти к параметрам необходимо:

- выбрать пункт меню «Клиенты»;
- в открывшемся окне групп Криптосетей выбрать группу;
- по нажатию клавиши <*Enter*> перейти в окно «Описание клиентов», где

перечислены диапазоны номеров клиентов;

- выбрать диапазон номеров клиентов, по нажатию клавиши <*Enter*> перейти в окно параметров диапазона;
- выбрать опцию Абоненты, по нажатию кнопки *«Всего»* перейти в окно «Абоненты»;
- нажать кнопку *«Настройки RKL»*, перейти в окно «Настройки RKL для диапазона».

В окне «Настройки RKL для диапазона» на вкладке «RKL» доступны следующие параметры:

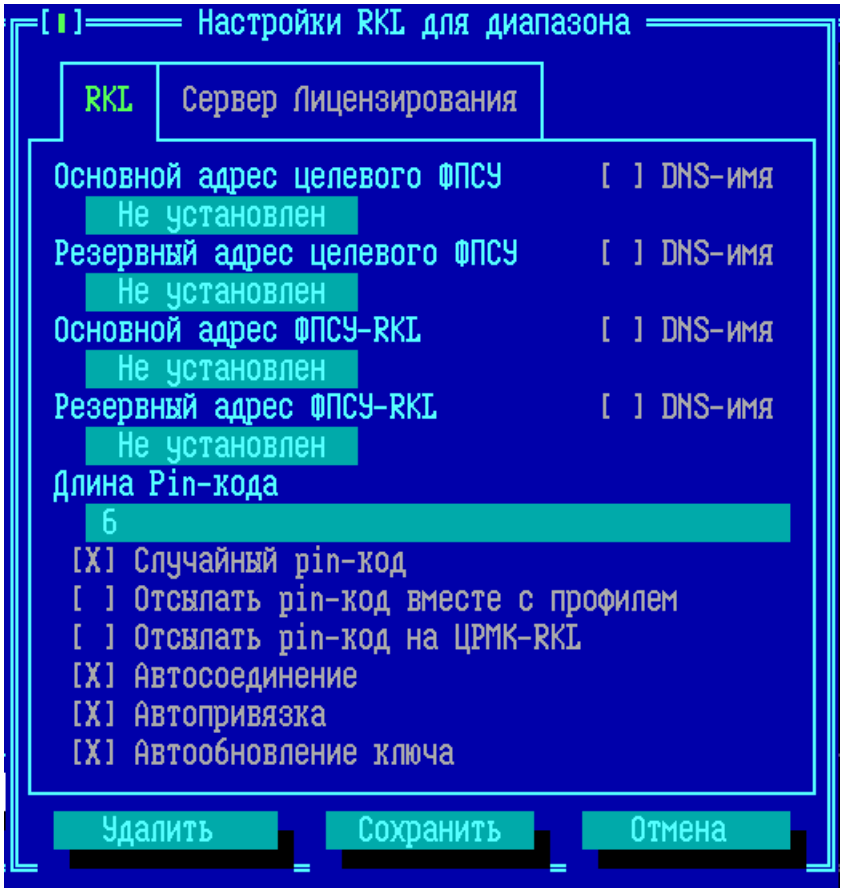


Рисунок 282 - Настройки RKL

Основной адрес целевого ФПСУ – в поле необходимо ввести IP-адрес ФПСУ-IP, через который будет осуществляться доступ ФПСУ-IP/Клиента к защищенным хостам.

DNS-имя – флаг, позволяющий вместо указания IP-адреса ФПСУ-IP сохранить в настройках DNS-имя. Служба DNS должна поддерживаться устройством с установленным ПО ФПСУ-IP/Клиент. В этом случае перед установлением соединения ФПСУ-IP/Клиента с ФПСУ-IP будет каждый раз выполняться DNS-запрос на получение IP-адреса ФПСУ-IP у обслуживающего данное устройство DNS-сервера.

Резервный адрес целевого ФПСУ – в поле необходимо ввести IP-адрес дополнительного ФПСУ-IP, если в локальной сети имеется еще один ФПСУ-IP, который может предоставить доступ ФПСУ-IP/Клиенту в случае отсутствия связи с основным.

Основной адрес ФПСУ-RKL – в поле необходимо ввести IP-адрес ФПСУ-IP, через который будет осуществляться взаимодействие целевого ФПСУ-IP с ЦРМК-RKL.

Резервный адрес ФПСУ-RKL – в поле необходимо ввести IP-адрес дополнительного ФПСУ-IP, через который будет осуществляться взаимодействие целевого ФПСУ-IP с ЦРМК-RKL в случае отсутствия связи с основным.

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 обновления ключей достаточно выпустить новую серию общесистемных ключей. К моменту наступления срока обновления ключа на ЦГКК должен быть создан общесистемный ключ новой серии, на целевом ФПСУ-IP и ФПСУ-RKL должны быть установлены две серии ключей текущая и новая, выработанная на ЦГКК. Для ФПСУ-IP/Клиента при соединении с целевым ФПСУ-IP проверяется наличие новой серии ключей на целевом ФПСУ-IP. В случае если новая серия обнаружена, ФПСУ-IP/Клиент обращается к ФПСУ-RKL с запросом обновления ключей. При наличии на ФПСУ-RKL новой серии ключей для клиента, запрос перенаправляется в ЦРМК-RKL. ЦРМК-RKL выдает разрешение на обновление ключей. На ФПСУ-IP/Клиенте обновляется серия общесистемных ключей без участия Администратора. Клиент пересоединяется с ФПСУ-IP, используя новую серию ключа.

Нажатие кнопки *«Сохранить»* или клавиши *<F2>* сохраняет настройки вкладок RKL и Сервера лицензирования и возвращает в окно описания абонентов для диапазона номеров. Сбросить установленные настройки можно по нажатию кнопки *«Удалить»* или клавиши *<Del>*, отменить внесенные изменения – по нажатию кнопки *«Отмена».*

11. 4. 2. Настройка диапазона клиентов на работу с Сервером лицензирования

Сервер лицензирования используется для учета и выдачи программных лицензий ФПСУ-IP/Клиентов.

Настройки Сервера лицензирования позволяют проводить автоматическую удаленную загрузку лицензий до истечения срока действия с Сервера лицензирования на устройства с установленным ПО ФПСУ-IP/Клиент.

Удаленная загрузка лицензий проводится в двух режимах, получения лицензии по запросу с использованием RKL-токена и автоматического обновления лицензии при истечении срока действия лицензии.

При получении лицензии по запросу необходимо подключение RKL-токена в USB-порт рабочей станции или устройства с установленным программным обеспечением ФПСУ-IP/Клиент. ФПСУ-IP/Клиент осуществляет взаимодействие с ФПСУ-RKL, все другие соединения блокируются. Взаимодействие осуществляется по следующей схеме:

- ФПСУ-IP/Клиент с RKL-токеном устанавливает защищенное соединение с ФПСУ-RKL.
- ФПСУ-IP/Клиент запрашивает лицензию у ФПСУ-RKL.
- ФПСУ-RKL отправляет запрос на получение лицензии на Сервер лицензирования.
- Сервер лицензирования выдает лицензию ФПСУ-IP/Клиенту.

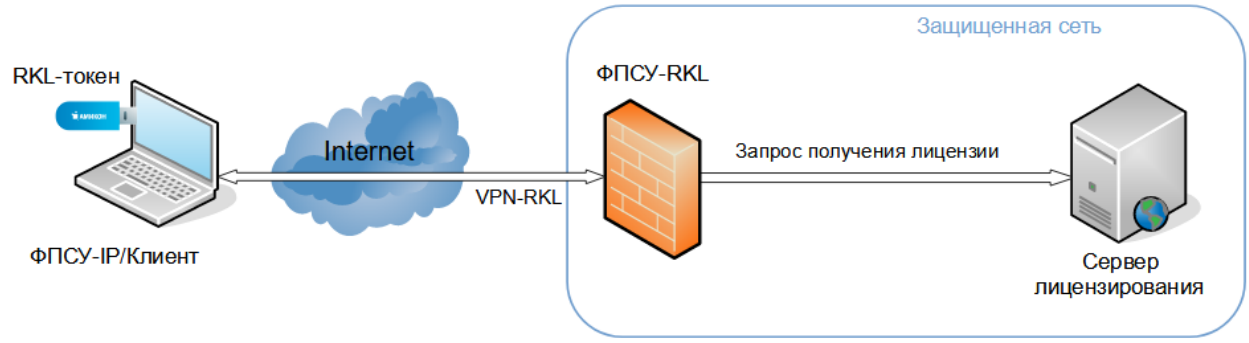


Рисунок 283 - Схема получения лицензии с Сервера лицензирования

При автоматическом обновлении лицензии ФПСУ-IP/Клиент в момент подключении к ФПСУ-IP проверяется срок истечения лицензии, запрос обновления лицензии отправляется с ФПСУ-IP за указанное количество дней до окончании поддержки на Сервер лицензирования. Сервер лицензирования выдает лицензию ФПСУ-IP/Клиенту. На ФПСУ-IP/Клиенте обновляется лицензия.

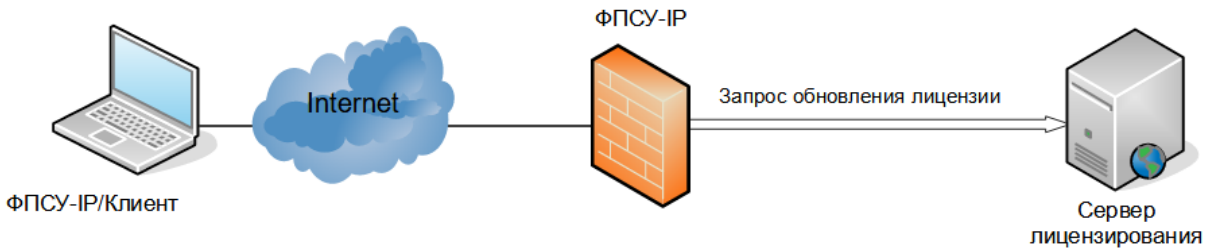


Рисунок 284 - Схема обновления лицензии с Сервера лицензирования

В зависимости от используемого режима получения или обновления лицензии на ФПСУ-IP/Клиентах установите на ФПСУ-IP или/и на ФПСУ-RKL настройки Сервера лицензирования для диапазона клиентов из группы Криптосети на вкладке «Сервер лицензирования» и в пункте меню «Сетевые сервисы → Серверы ЦРМК» (см.пункт «Серверы ЦРМК и Сервер лицензирования»).

Настройки Сервера лицензирования устанавливаются для диапазона клиентов из группы Криптосети, чтобы перейти к параметрам необходимо:

- выбрать пункт меню «Клиенты»;
- в открывшемся окне групп Криптосетей выбрать группу;
- по нажатию клавиши <*Enter*> перейти в окно «Описание клиентов», где перечислены диапазоны номеров клиентов;
- выбрать диапазон номеров клиентов, по нажатию клавиши <*Enter*> перейти в окно параметров диапазона;
- выбрать опцию Абоненты, по нажатию кнопки *«Всего»* перейти в окно «Абоненты»;
- нажать кнопку *«Настройки RKL»*, перейти в окно «Настройки RKL для диапазона».

В окне «Настройки RKL для диапазона» на вкладке «Сервер лицензирования» доступны следующие параметры:

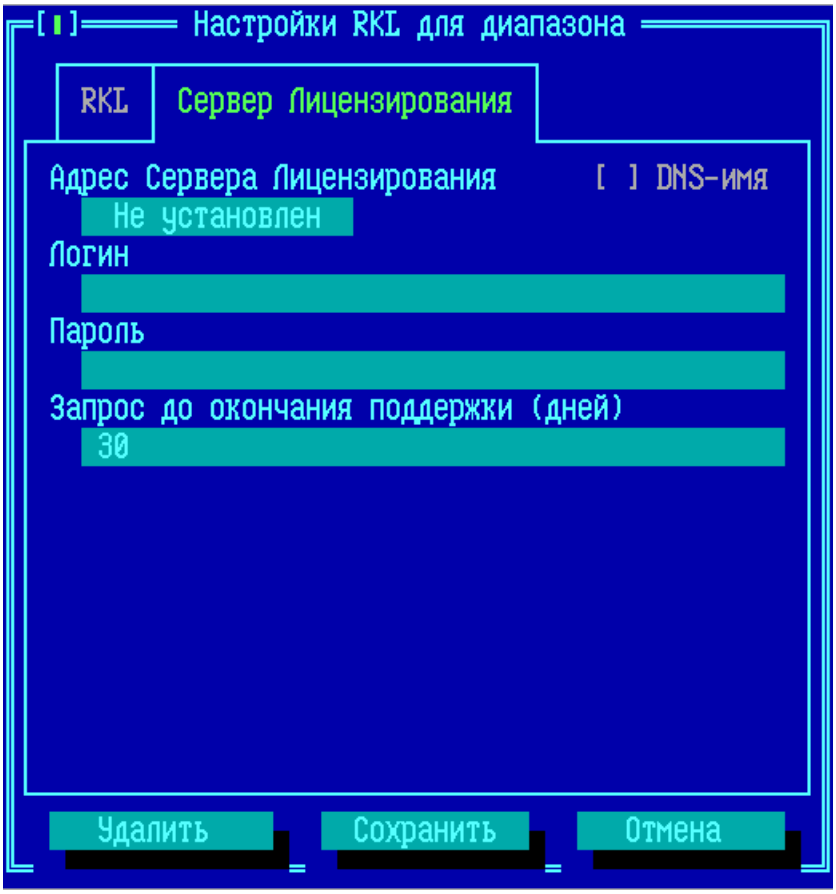


Рисунок 285 - Настройки RKL. Вкладка Сервер Лицензирования

Адрес Сервера лицензирования – в поле необходимо ввести IP-адрес Сервера лицензирования или ФПСУ-RKL при использовании ЦРМК-RKL.

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

На Сервере лицензирования может быть установлена аутентификация, заданы ***Логин*** и ***Пароль***, для получения Клиентом лицензии.

Запрос до окончания поддержки – При старте ФПСУ-IP/Клиент проверяет дату окончания поддержки лицензии. За указанный период до её окончания отправляется запрос на Сервер лицензирования для автоматического обновления лицензии, по умолчанию за 30 дней.

Нажатие кнопки *«Сохранить»* или клавиши *<F2>* сохраняет настройки вкладок RKL и Сервера лицензирования и возвращает в окно описания абонентов для диапазона номеров. Сбросить установленные настройки можно по нажатию кнопки *«Удалить»* или клавиши *<Del>*, отменить внесенные изменения – по нажатию кнопки *«Отмена»*.

11. 4. 3. Серверы ЦРМК и Сервер лицензирования

Для расширенного режима при получении/обновлении ключевых данных требуется организовать взаимодействие с ЦРМК, необходимо указать сервер ЦРМК на ФПСУ-RKL.

При автоматическом удаленном получении/обновлении лицензий лицензии загружаются с Сервера лицензирования, в зависимости от схемы взаимодействия с сервером необходимо указать Сервер лицензирования на ФПСУ-IP и/или на ФПСУ-RKL. Схемы взаимодействия с сервером описаны в пункте «Настройка диапазона клиентов на работу с Сервером лицензирования».

Настройка сервера ЦРМК и Сервера лицензирования выполняется из пункта меню «Сетевые сервисы → Серверы ЦРМК».

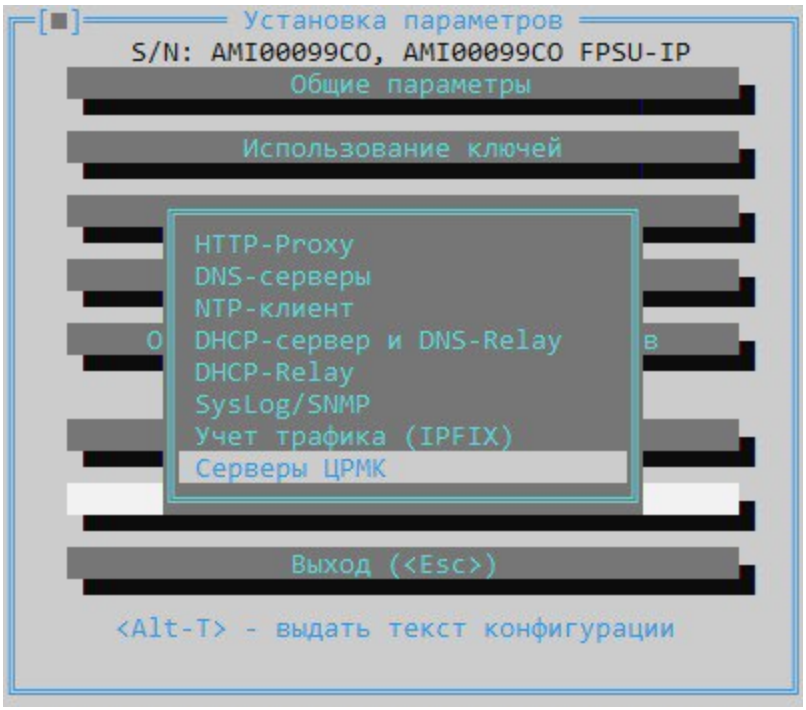


Рисунок 286 - Меню подсистемы конфигурирования ФПСУ-IP

Для задания Сервера лицензирования в поле «Сервер лицензий» следует ввести IP-адрес сервера и порт подключения к серверу.

Для задания сервера ЦРМК необходимо задать диапазон групп Криптосетей и напротив ввести URL сервера ЦРМК.

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*».

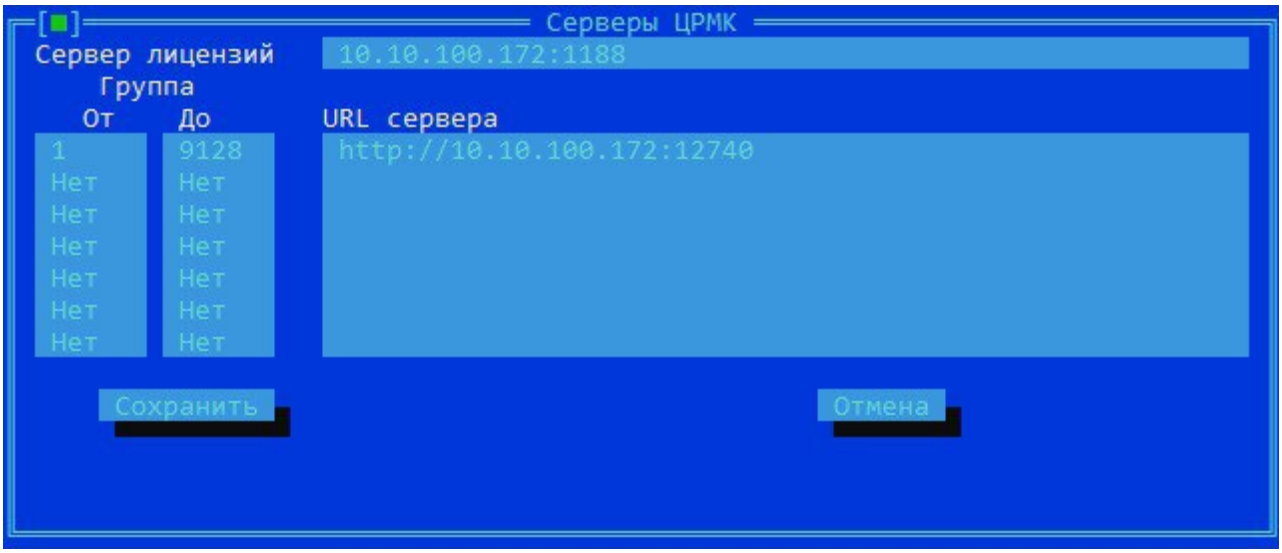


Рисунок 287 - Настройка ЦРМК и Сервера лицензирования

11. 5. Настройка диапазона клиентов на работу с Radius

Настройки RADIUS позволяют установить дополнительные требования к аутентификации ФПСУ-IP/Клиентов при попытке соединения с ФПСУ-IP для доступа в защищаемую сеть.

Аутентификация ФПСУ-IP на сервере RADIUS проводится согласно RFC 2865.

Аутентификация ФПСУ-IP/Клиента на сервере RADIUS проходит по следующей схеме:

- ФПСУ-IP/Клиент отправляет запрос ФПСУ-IP, который является сервером сетевого доступа, чтобы получить доступ к защищенной области, используя имя пользователя и пароль.
- ФПСУ-IP отправляет сообщение с запросом доступа RADIUS, на сервер RADIUS, запрашивая авторизацию для предоставления доступа.
- Сервером RADIUS подтверждается личность пользователя, а также права доступа к сетевым службам. Сервер RADIUS разрешает или запрещает доступ.
- В случае успешной аутентификации ФПСУ-IP/Клиент получает доступ к запрошенному сетевому ресурсу, защищенной области А.

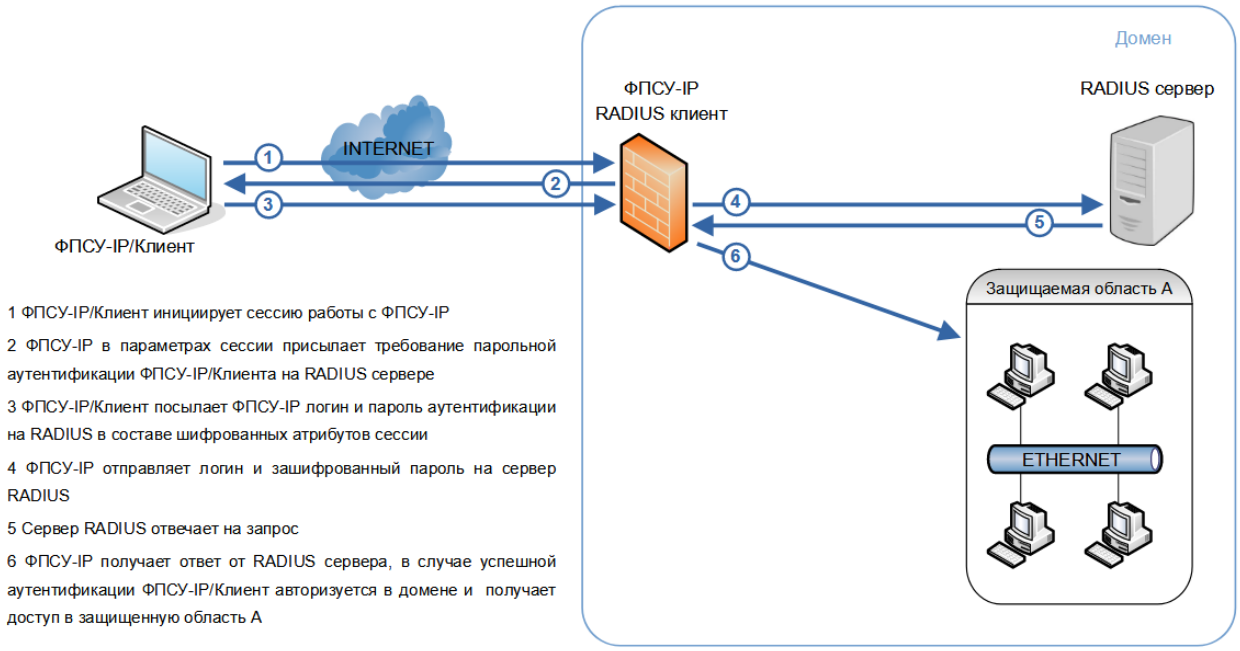


Рисунок 288 - Схема взаимодействия ФПСУ-IP при аутентификации на сервере RADIUS

Установите следующие настройки:

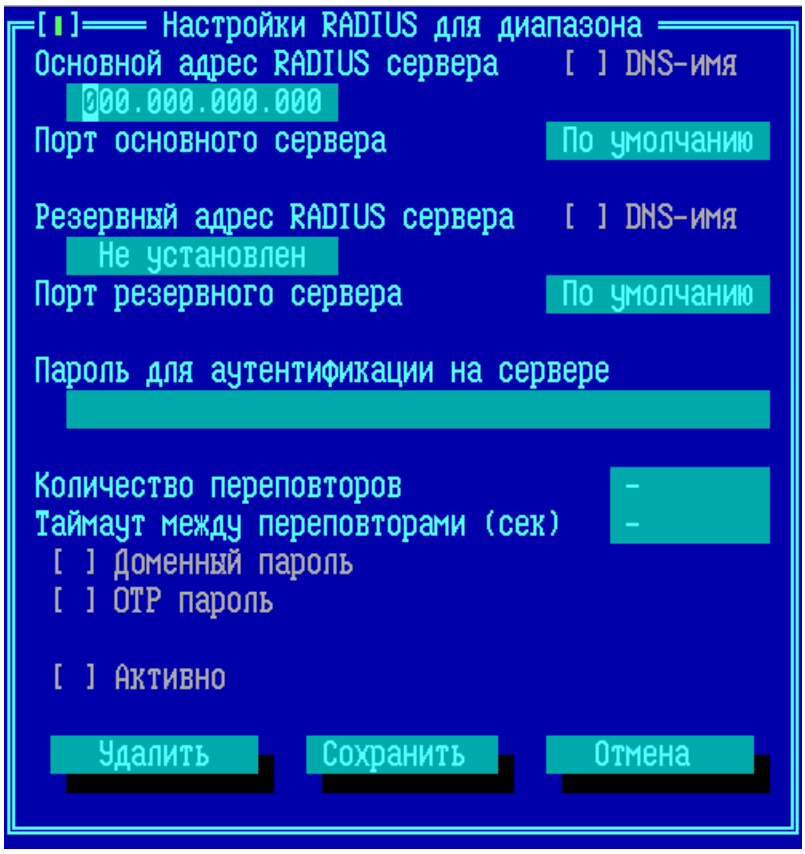


Рисунок 289 - Настройки RADIUS

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:

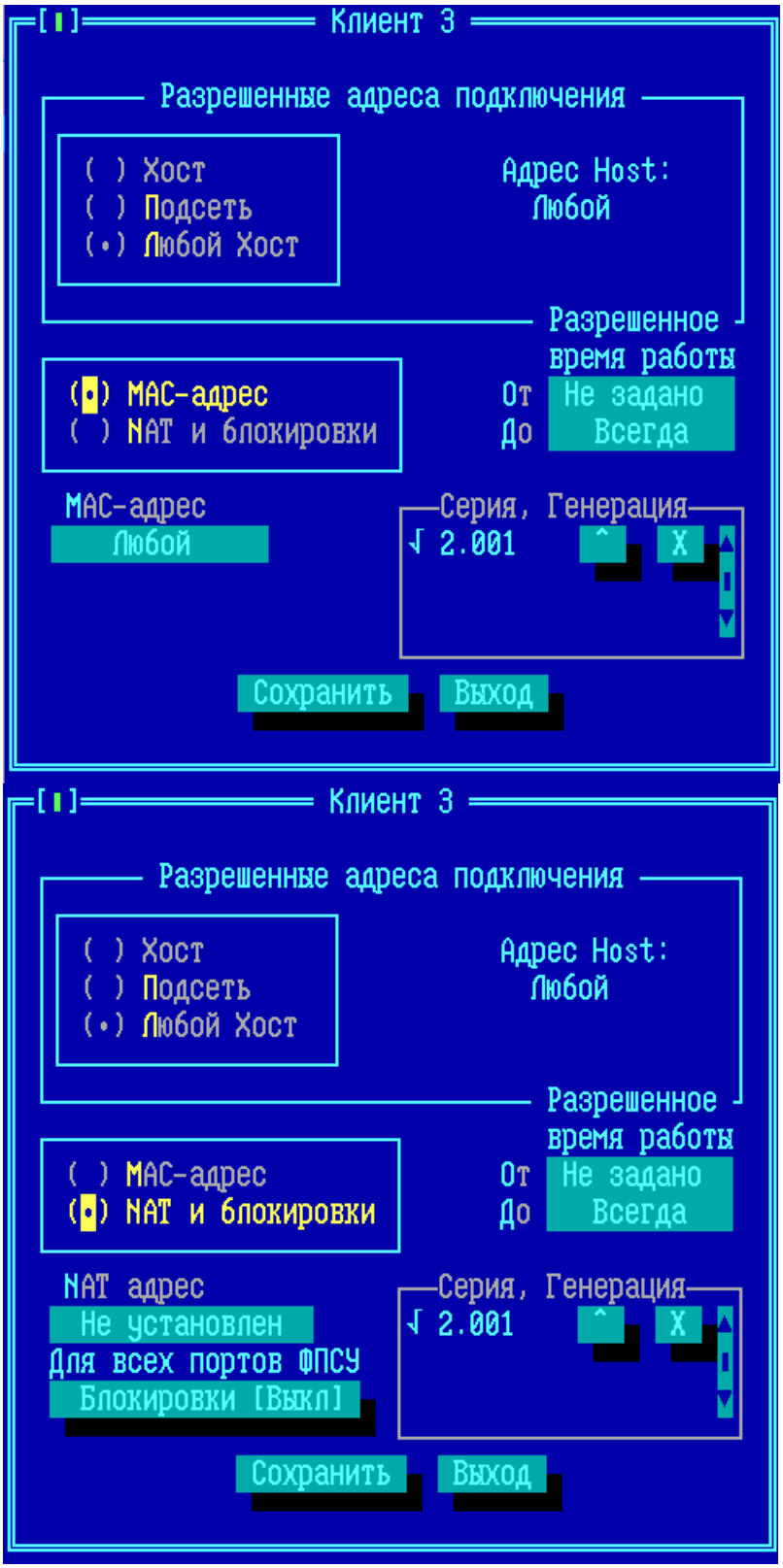


Рисунок 290 - Параметры работы отдельного Клиента

Разрешенные адреса подключения – выбор диапазона IP-адресов, с которого данному Клиенту разрешено подключение к ФПСУ-IP:

- *Хост* – Клиенту разрешено подключение только с одного указанного IP-адреса;
- *Подсеть* – Клиенту разрешено подключение только из указанной IP-подсети;
- *Любой хост* – настройка по умолчанию, Клиенту разрешено подключение к ФПСУ-IP с любого IP-адреса.

Разрешенное время работы – выбор начальной (поле «*От*») и конечной (поле «*До*») даты периода, в течение которого Клиенту разрешено подключение к ФПСУ-IP.

Серия – уникальный числовой идентификатор общесистемного ключа Криптосети.

Генерация – уникальный числовой идентификатор ключа Клиента, от 1 до 256.

Серия и генерация отображаются в виде X.YYY, где X - номер серии, YYY - номер генерации.

Знак «√» слева от серии ключа означает, что ключ Клиента Криптосети с данной серией и генерацией используется для установления соединения ФПСУ-IP/Клиента и ФПСУ-IP.

В случае компрометации ключа Клиента необходимо сменить ключ Клиента, повысив номер генерации. Для увеличения номера генерации на единицу выделите кнопку «^» курсором и нажмите <*Enter*>. Данная операция необратима. Ключ Клиента со старым номером генерации блокируется.

В случае компрометации общесистемного ключа Криптосети необходимо сменить общесистемный ключ, для этого установить запрет на использование текущей серии и повысить номер серии. Для запрета серии ключа Криптосети выделите кнопку «***X***» курсором и нажмите <*Enter*>. Данная операция необратима. Смена серии общесистемного ключа производится на ЦГКК, подробно описана в руководстве «Центр генерации ключей клиентов» (процедуры установки полученного от администратора ЦГКК нового общесистемного ключа - см. пункт «Установка и удаление общесистемных ключей»).

MAC-адрес – флаг, при включении которого можно ограничить подключение клиента с только определенного MAC-адреса, указав ниже в поле «*MAC адрес*» ожидаемое значение физического адреса, с которого приходят IP-пакеты Клиента.

При установленном флаге «*MAC-адрес*» не работают настройки, ранее выполненные в полях «*NAT и блокировки*» (см. далее).

NAT и блокировки – флаг, при включении которого можно указать исключения в

работе данного Клиента из общих настроек, сделанных в описании диапазона Клиентов (см. пункт «Установка правил работы клиентов»).

При установленном флаге «*NAT и блокировки*» в поле ***NAT адрес*** может быть указан транслируемый IP-адрес (NAT) для данного Клиента, если требуется для отдельного Клиента ФПСУ-IP выдать отдельный NAT адрес, отличающийся от заданного в описании диапазона Клиентов.

При включенном флаге «*NAT и блокировки*» также могут быть указаны отличные от выставленных в описании всего диапазона Клиентов блокировки. Для этого выполните переход в окно индивидуальных блокировок, нажав в поле ***Для всех портов ФПСУ*** кнопку «*Блокировки*».

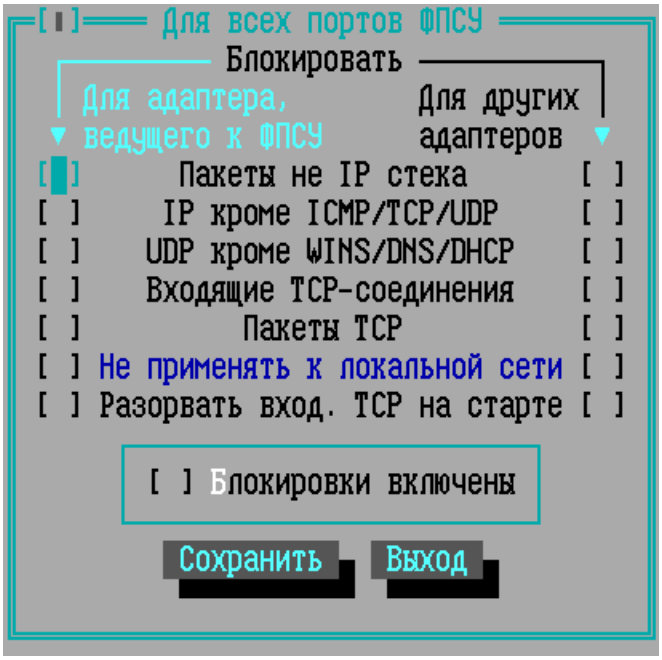


Рисунок 291 - Индивидуальные блокировки Клиента

В окне индивидуальных блокировок отдельного Клиента, при установлении флага «*Блокировки включены*», к данному клиенту будут применены указанные в этом окне параметры фильтрации трафика, полностью заменяя находящиеся в описании диапазона Клиентов (см. пункт «Установка правил работы клиентов») блокировки. Указанные блокировки будут действовать вне зависимости от того, с каким портом ФПСУ-IP соединился Клиент.

При установленном флаге «*NAT и блокировки*» не работают ранее выполненные настройки, указанные в поле «*MAC адрес*».

Примечание. Для клиентов типа VPNPROGRAM такой вид дополнительной

настройки блокировок недоступен.

12. Служебные протоколы

12. 1. Общие правила разделения потоков

При обмене информацией между двумя ФПСУ-IP, работающими в паре, данные передаются по сети в туннелированном виде, так что любая рабочая станция на пути следования IP пакетов от одного ФПСУ-IP к другому, включая пограничные маршрутизаторы, может «видеть» в их IP-заголовках только IP-адреса отправляющего и получающего ФПСУ-IP и номер IP-протокола, по которому осуществляется обмен между ФПСУ-IP.

Таким образом, если на пути следования пакетов находится пограничный маршрутизатор, конфигурированный на формирование нескольких различных потоков с различными маршрутами следования или ограничения полосы их пропускания (функция «shaping»), этот маршрутизатор не сможет вычленить из пакетов данных необходимую информацию и выполнить указанные функции.

Для устранения этой проблемы и согласования работы ФПСУ-IP и пограничных маршрутизаторов разработана специальная подсистема, позволяющая разделить поступающие в VPN-туннель данные на несколько (максимально сто двадцать восемь) различных потоков и связать номера этих потоков с различными номерами IP-протоколов. Соответствие номеров потоков данных, отправляемых с ФПСУ-IP, номерам IP-протоколов, по которым они будут отправлены, выглядит следующим образом:

Поток №1 (поток по умолчанию) — 53 номер IP протокола или UDP:30004 (если протокол между ФПСУ-IP выбран UDP).

Остальные потоки идут подряд, начиная с 110 номера IP протокола или UDP:55 000:
Поток №2 — 110 номер IP протокола / UDP:55 000;
Поток №3 — 111 номер IP протокола / UDP:55 001;
…
Поток №128 — 226 номер IP протокола / UDP:55 126.

Обратите внимание, что для эффективной совместной работы ФПСУ-IP и пограничных маршрутизаторов по формированию потоков требуется согласование их конфигураций. Однако если это условие не выполняется, фатальных ошибок при передаче данных не произойдет и данные по VPN-туннелю будут доставлены в любом случае. Если ФПСУ-IP конфигурирован на разделение потоков, а один из пограничных маршрутизаторов (или даже все) - не конфигурирован, удаленный ФПСУ-IP получит посылаемые с конфигурируемого ФПСУ-IP данные в IP-пакетах с номером протокола 53 в заголовке пакета (по маршруту, который конфигурирован на пограничных маршрутизаторах для этого

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.

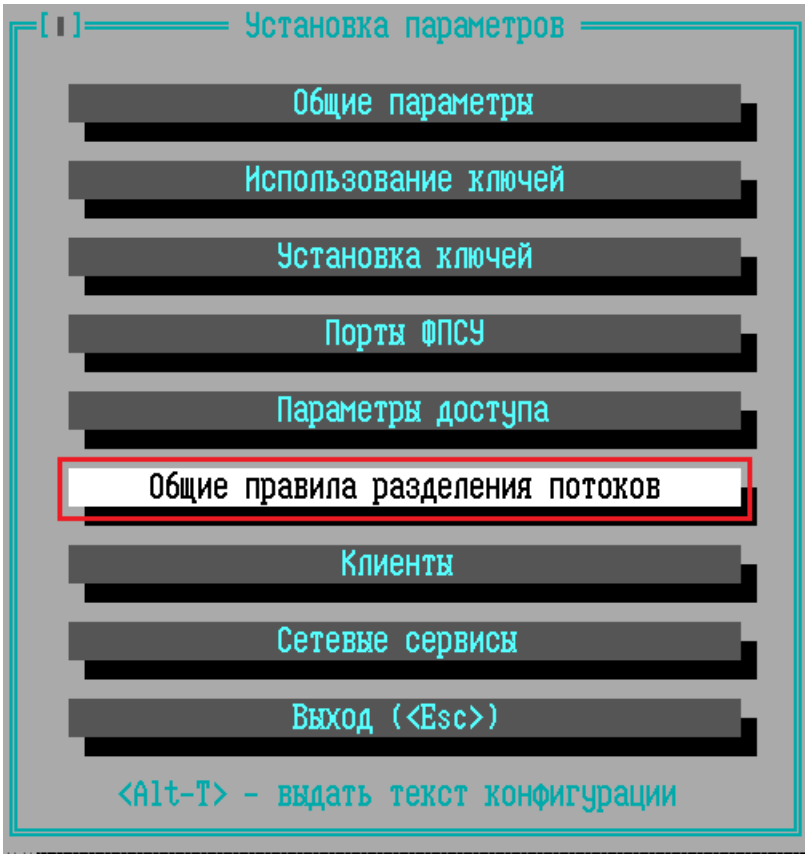


Рисунок 292 - Меню подсистемы конфигурирования ФПСУ-IP

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

описывались.

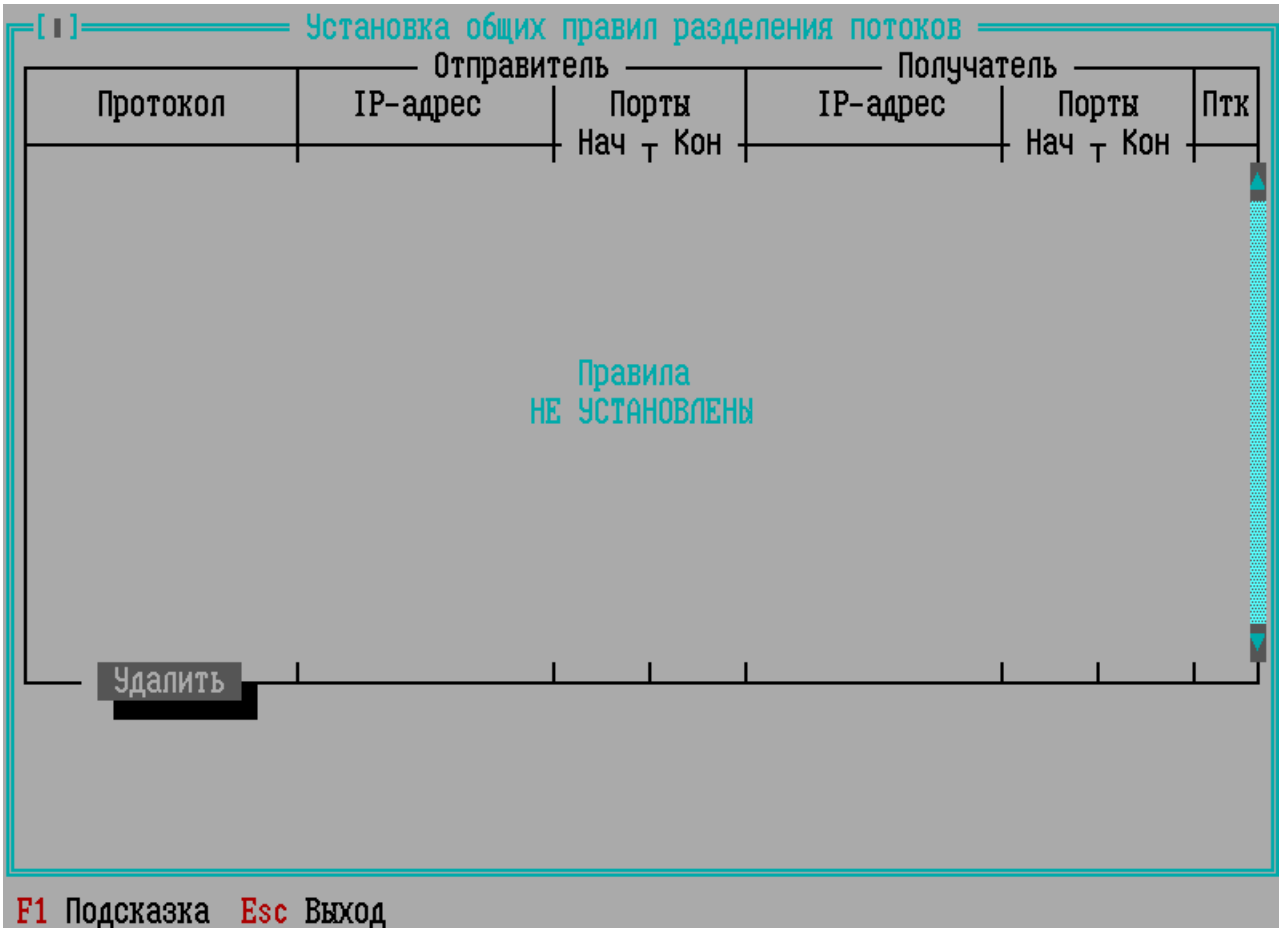


Рисунок 293 - Окно «Установка общих правил разделения потоков»

Чтобы добавить новое общее правило, следует нажать клавишу <*Ins*>, после чего открывается окно «*Установка нового общего правила разделения потоков*».

Чтобы установить правило, по которому поступающий в VPN-туннель со стороны конфигурируемого ФПСУ-IP IP-пакет будет направлен в определенный выходной поток, следует указать ФПСУ-IP номер IP-протокола, данные которого будут содержать пакет, IP-адрес (или диапазон адресов) отправителя (абонента, посылающего пакет со стороны конфигурируемого ФПСУ-IP) и адрес (или диапазон адресов) получателя (абонента, которому предназначается пакет).

Если какой-либо критерий правила не имеет значения для направления пакета в тот или иной выходной поток (например, в поток направляются любые данные, отправляемые любыми абонентами по конкретному IP-адресу), в соответствующих полях устанавливаются значения «*Любой*» (для протокола) или «*Произвольный*» (для адресов).

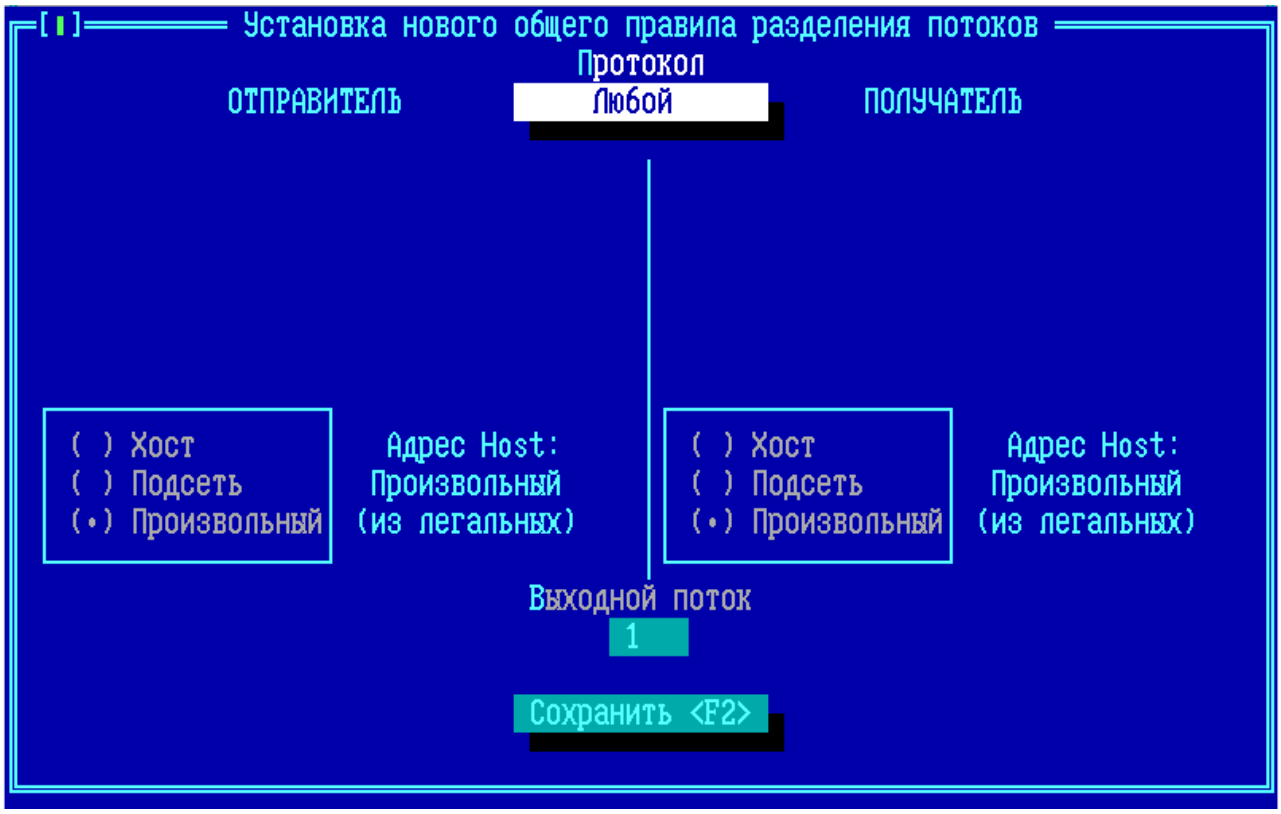


Рисунок 294 - Создание нового общего правила разделения потоков

Чтобы установить для выходного потока какой-либо конкретный протокол, нужно установить курсор на строку «Любой» под заголовком «Протокол» и нажать клавишу <*Пробел*>, затем в открывшемся списке протоколов установить курсор на нужный протокол и нажать <*Enter*> или <*Пробел*>, после чего будет осуществлен выход в окно установки описываемого правила. Если указанный протокол требует установки дополнительных параметров (например, номера начального и конечного портов для протоколов TCP или UDP), в окне появятся соответствующие поля ввода, в которые можно ввести либо номера портов (после чего в нижележащей строке будет отображено название «прикрепленного» к этому порту протокола, если оно есть), либо установить курсор на строку под полем ввода и нажать <*Пробел*>, после чего в появившемся списке отметить номер (или соответствующий протокол) нужного порта (в случае, если номер порта не превышает 1023).

Для установки IP-адресов отправителей и получателей следует поместить курсор на нужную строку, нажать <*Пробел*> и набрать в появившихся полях ввода адрес и маску (если в качестве отправителя и/или получателя могут выступать подсети).

После описания всех критериев правила следует выбрать номер выходного потока, для чего требуется перейти в поле «*Выходной поток*», и указать номер (номер выходного потока должен соответствовать номеру протокола, который будет использован для

формирования данного потока при конфигурировании пограничного маршрутизатора). По активизации поля «*Сохранить*» подсистема конфигурирования осуществит выход в окно списка установленных общих правил.

Над установленными общими правилами в списке можно осуществить следующие операции:

- редактировать текущее правило (по нажатию <*Enter*>);
- удалить текущее правило (по нажатию <*Del*>).

ВНИМАНИЕ! При выделении в отдельный поток данных протоколов, допускающих динамическое изменение номеров портов (например, FTP), правила направления IP-пакетов в этот поток могут работать некорректно (хотя пакеты в любом случае будут доставлены удаленному комплексу ФПСУ-IP). Если администратору обязательно требуется сформировать отдельный FTP-поток, рекомендуется использовать с этой целью поток по умолчанию (см. раздел Описание параметров удаленных ФПСУ-IP). Для этого все прочие данные распределяются по каким-либо определенным потокам, а в качестве потока по умолчания устанавливается поток, соответствующий номеру протокола, конфигурированного на пограничном маршрутизаторе для требуемого маршрута передачи данных FTP-протокола.

12. 2. Учет трафика IPFIX

ФПСУ-IP может выступать в качестве сенсора сетевой структуры IPFIX (выступать в качестве IPFIX Device согласно RFC 5470).

ФПСУ-IP может собирать информацию о проходящем через него трафике, создавать на основе полученной информации шаблоны с данными IP-потоков, и периодически отправлять эти шаблоны на указанные IP-адреса коллекторов IPFIX.

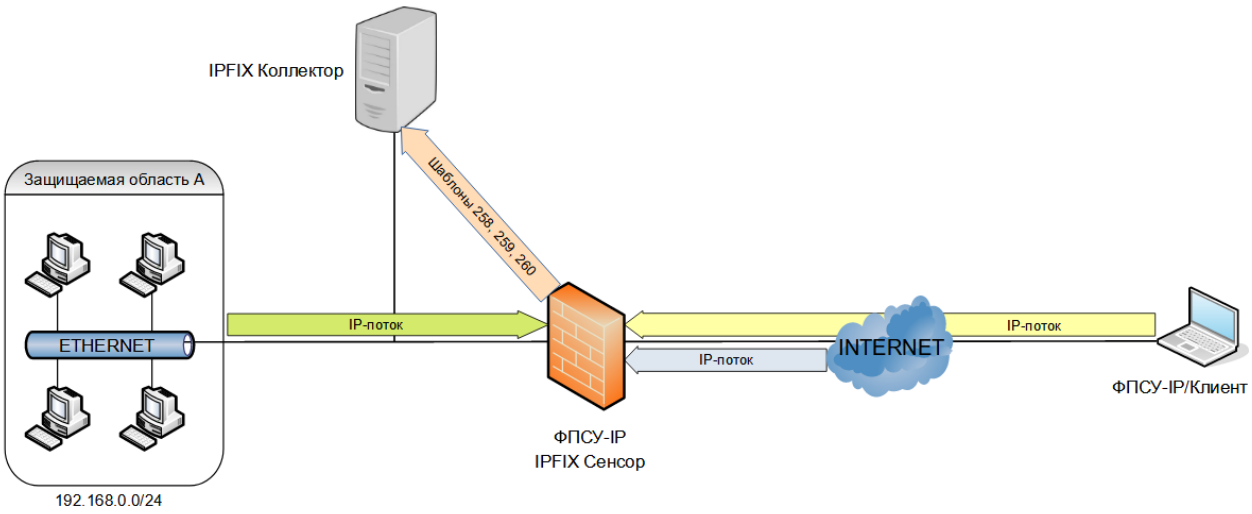


Рисунок 295 - ФПСУ-IP в качестве сенсора IPFIX

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)*».

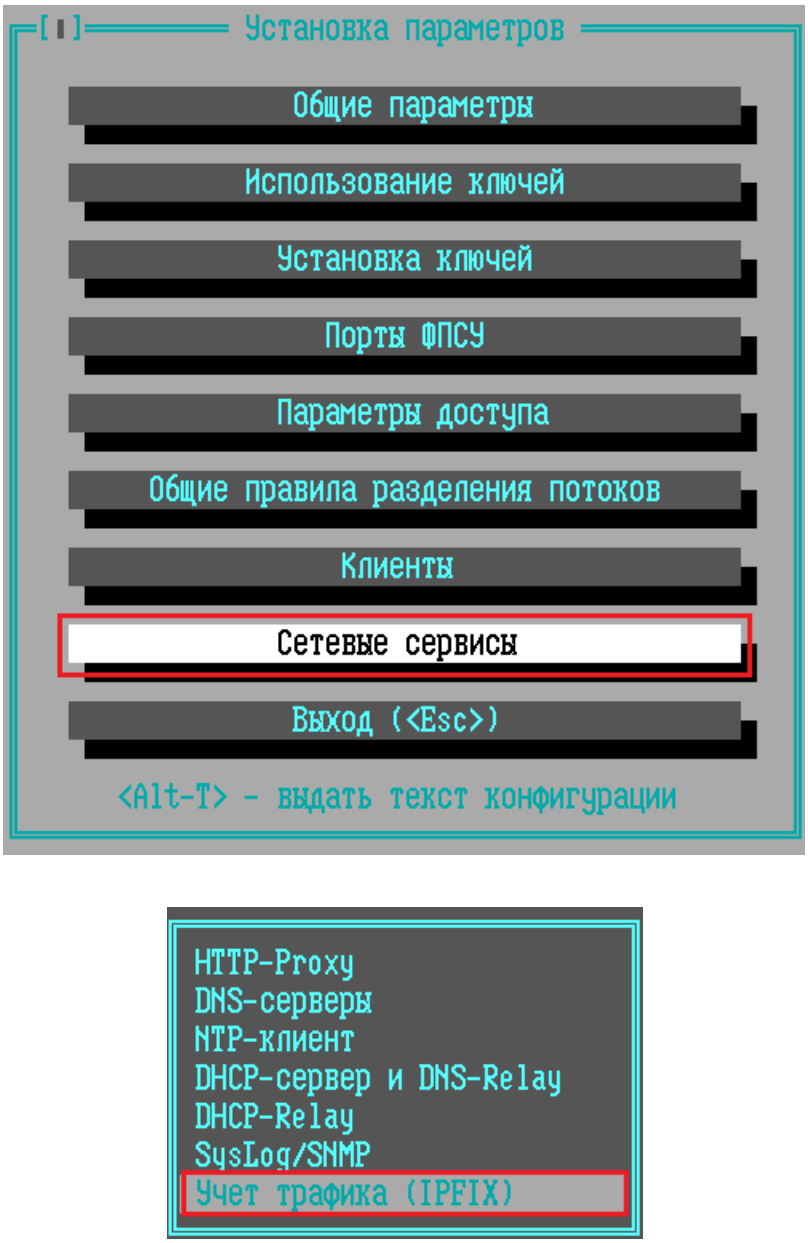


Рисунок 296 - Команда меню «Сетевые сервисы» → «Учет трафика (IPFIX)»

По команде меню открывается окно со списком коллекторов IPFIX, по умолчанию список пустой.

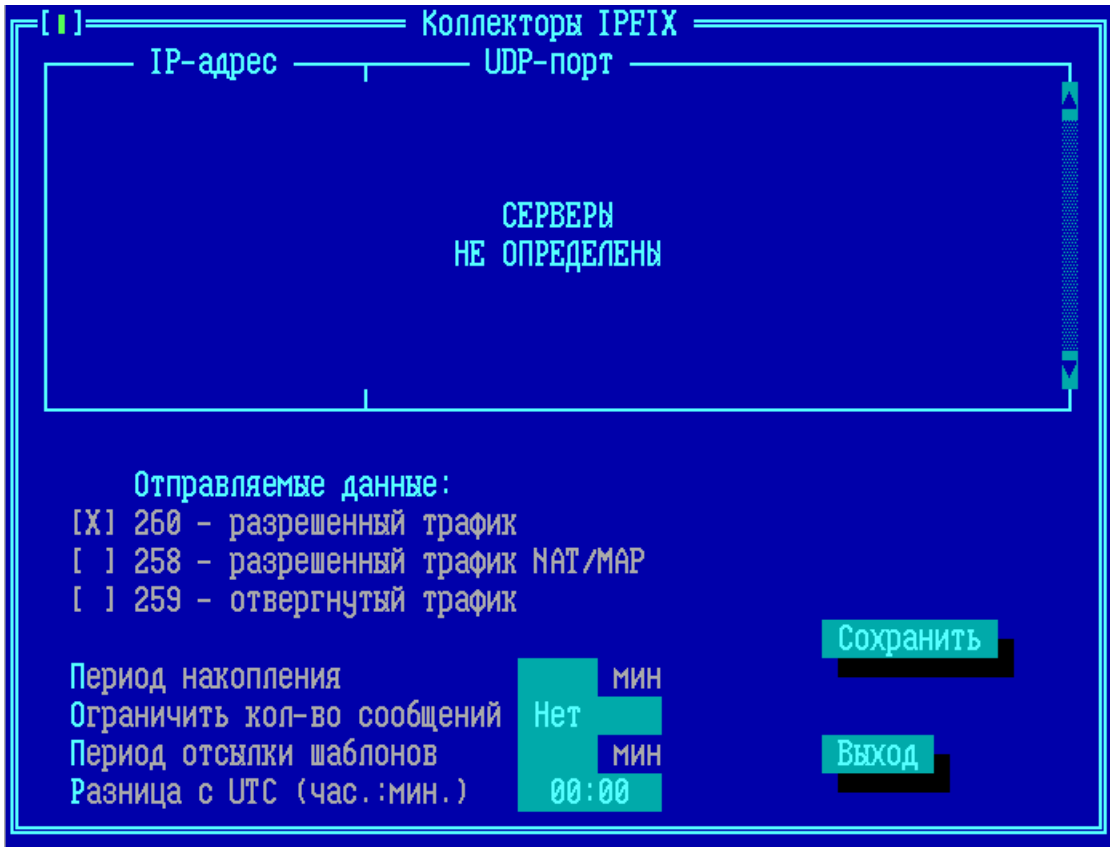


Рисунок 297 - Общие параметры, вызов окна настроек учета трафика IPFIX

Включение поддержки IPFIX может замедлять работу межсетевого экрана ФПСУ-IP.

Для добавления нового коллектора IPFIX следует нажать клавишу <*Ins*>. Откроется окно, в котором задается IP-адрес коллектора и UDP-порт, по умолчанию 4739.

Флаг *«Работа запрещена»* при включении запрещает отправку шаблонов на указанный IP-адрес коллектора IPFIX.

Рисунок 298 - Добавление коллектора IPFIX

Отправляемые данные распределяются по нескольким шаблонам в зависимости от типа трафика:

Шаблон 258 - трафик с NAT-адреса;

Шаблон 259 - отвергнутый трафик;

Шаблон 260 - разрешенный трафик.

Устанавливаются периоды накопления и отсылки шаблонов в минутах. Может быть задано ограничение на количество сообщений в шаблоне. Устанавливается разница временного пояса, в котором работает ФПСУ-IP, с UTC временем.

12. 2. 1. Коды IPFIX, используемые в шаблонах

В таблице приведены коды IPFIX, используемые в шаблонах при экспорте информации о потоке IP.

Таблица 4. Информационные коды IPFIX

Код	Наименование кода	Типоразмер	Единицы	Описание
1	octetDeltaCount	unsigned64	octets	Количество октетов с момента предыдущего отчета (если есть) во входящих пакетах для этого потока в точке наблюдения. Количество октетов включает IP-заголовок(и) и полезную нагрузку IP
2	packetDeltaCount	unsigned64	packets	Количество входящих пакетов с момента предыдущего отчета (если есть) для этого потока в точке наблюдения
4	protocolIdentifier	unsigned8		Идентификатор протокола
6	tcpControlBits	unsigned16		Наблюдаемые управляющие биты TCP для пакетов этого потока. Эта информация кодируется в виде битового поля; для каждого управляющего бита TCP в этом наборе есть бит. Бит устанавливается равным 1, если для любого наблюдаемого пакета этого потока

Код	Наименование кода	Типоразмер	Единицы	Описание
				установлен соответствующий бит управления TCP, равный 1. В противном случае бит будет очищен до 0. Значения каждого бита показаны ниже в соответствии с определением битов в заголовке TCP [RFC9293] [RFC3168]: MSb LSb 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ | | | N | C | E | U | A | P | R | S | F / | Нулевой | Будущий | S | W | C | R | C | S | S / Y | I | | (Смещение данных) | Использовать | | R | E | G | K | H | T / N | N | +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ битовый флаг значение имя описание ------+----- +----------

Код	Наименование кода	Типоразмер	Единицы	Описание
				0x8000 Ноль (см. tcpHeaderLength) 0x4000 Ноль (см. tcpHeaderLength) 0x2000 Ноль (см. tcpHeaderLength) 0x1000 Ноль (см. tcpHeaderLength) 0x0800 Будущее использование 0x0400 Будущее использование 0x0200 Будущее использование 0x0100 NS ECN одноразовая сумма Уменьшено окно перегрузки 0x0080 CWR 0x0040 ECE ECN Echo 0x0020 URG Поле срочного указателя значимо 0x0010 Поле подтверждения подтверждения значимо Функция Push 0x0008 PSH 0x0004 СНАЧАЛА сбросьте соединение 0x0002 SYN Синхронизирует порядковые номера 0x0001 FIN Больше нет данных от отправителя Поскольку наиболее значимые 4 бита октетов 12 и 13 (считая от нуля) заголовка TCP [RFC9293]

Код	Наименование кода	Типоразмер	Единицы	Описание
				используются для кодирования смещения данных TCP (длины заголовка), соответствующие биты в этой информации Элемент ДОЛЖЕН быть экспортирован как ноль и ДОЛЖЕН игнорироваться сборщиком. Используйте информационный элемент tcpHeaderLength для кодирования этого значения. Каждый из 3 битов (0x800, 0x400 и 0x200), которые зарезервированы для будущего использования в [RFC9293], СЛЕДУЕТ экспортировать, как указано в заголовках TCP пакетов этого потока. При экспорте в виде одного октета с кодировкой уменьшенного размера этот информационный элемент охватывает октет младшего порядка этого поля (т.Е. биты от 0x80 до 0x01), исключая одноразовую сумму ECN и три бита будущего использования. Сборщик, получающий этот информационный элемент с кодировкой уменьшенного размера, не должен ничего предполагать о содержимом этих четырех битов.

Код	Наименование кода	Типоразмер	Единицы	Описание
				Экспортирующие процессы, экспортирующие этот информационный элемент от имени процесса учета, который не способен отслеживать какие-либо биты одноразового номера ECN или биты будущего использования, ДОЛЖНЫ использовать кодирование уменьшенного размера и экспортировать только 8 младших значащих битов этого информационного элемента. Обратите внимание, что в предыдущих версиях определения этого информационного элемента указывалось, что биты CWR и ECE должны экспортироваться как нулевые, даже если они соблюдены. Поэтому сборщики не должны предполагать, что нулевое значение для этих битов в этом информационном элементе указывает, что биты никогда не устанавливались в наблюдаемом трафике, особенно если эти биты равны нулю в каждой записи потока, отправленной данным экспортером.
7	sourceTransportPort	unsigned16		TCP/UDP-порт отправителя

Код	Наименование кода	Типоразмер	Единицы	Описание
8	sourceIPv4Address	ipv4Address		IP-адрес отправителя
10	ingressInterface	unsigned8		Номер порта ФПСУ-IP, на который были приняты пакеты
11	destinationTransportPort	unsigned16		TCP/UDP-порт получателя
12	destinationIPv4Address	ipv4Address		IP-адрес получателя
14	egressInterface	unsigned8		Номер порта ФПСУ-IP, через который пакеты должны быть отправлены, либо 0, если это неизвестно
32	icmp_typecode	unsigned16		Тип/код сообщения для ICMP протокола см. пункт «Особенности реализации ICMP протокола» , таблица «Типы ICMP-ответов ФПСУ-IP»
44	sourceIPv4Prefix	ipv4Address		Адрес ФПСУ-IP, если абонент-отправитель прописан за ФПСУ-IP, либо 0
45	destinationIPv4Prefix	ipv4Address		Адрес ФПСУ-IP, если абонент-получатель прописан через ФПСУ-IP, либо 0
89	forwardingStatus	unsigned8		Способ обработки пакета. Проставляется: Dropped + код ошибки, см. таблица «Кодирование ошибок»

Код	Наименование кода	Типоразмер	Единицы	Описание
133	droppedPacketDeltaCount	unsigned64	packets	Количество пакетов с момента последнего отчета
135	droppedPacketTotalCount	unsigned64	packets	Общее кол-во пакетов в серии
150	flowStartSeconds	Milliseconds (64)	seconds	Время появления первого пакета в серии
151	flowEndSeconds	Milliseconds (64)	seconds	Время появления последнего пакета в серии
152	flowStartMilliseconds	dateTimeMilliseconds	milliseconds	Абсолютная временная метка первого пакета этого потока
153	flowEndMilliseconds	dateTimeMilliseconds	milliseconds	Абсолютная временная метка последнего пакета этого потока
225	postNATSourceIPv4Address	ipv4Address		Определение этого информационного элемента идентично определению информационного элемента 'sourceIPv4Address', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока NAT после того, как пакет прошел точку наблюдения
226	postNATDestinationIPv4Address	ipv4Address		Определение этого информационного элемента идентично определению информационного элемента

Код	Наименование кода	Типоразмер	Единицы	Описание
				'destinationIPv4Address', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока NAT после того, как пакет прошел точку наблюдения
227	postNAPTSourceTransportPort	unsigned16		Определение этого информационного элемента идентично определению информационного элемента 'sourceTransportPort', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока преобразования сетевого адреса (NAPT) после того, как пакет прошел точку наблюдения
228	postNAPTDestinationTransportPort	unsigned16		Определение этого информационного элемента идентично определению информационного элемента 'destinationTransportPort', за исключением того, что он сообщает об измененном значении, вызванном функцией промежуточного блока преобразования сетевого адреса (NAPT) после того, как пакет прошел точку наблюдения.
231	initiatorOctets	unsigned64	octets	Общее количество байтов полезной нагрузки уровня 4 в потоке от

Код	Наименование кода	Типоразмер	Единицы	Описание
				инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и остается неизменным в течение срока действия сеанса.
232	responderOctets	unsigned64	octets	Общее количество байтов полезной нагрузки уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик - это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса.
233	firewallEvent	unsigned8		Код события: 3 → flow_denied Указывает на событие брандмауэра. Допустимые значения перечислены в реестре firewallEvent: Значение Описание 0 Ignore (invalid) 1 Flow Created 2 Flow Deleted 3 Flow Denied 4 Flow Alert 5 Flow Update 6-255 Unassigned
298	initiatorPackets	unsigned64	packets	Общее количество пакетов уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и

Код	Наименование кода	Типоразмер	Единицы	Описание
				остается неизменным в течение всего срока действия сеанса.
299	responderPackets	unsigned64	packets	Общее количество пакетов уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик - это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса.

Таблица 5. Кодирование ошибок (для статуса пересылки 89)

Статус	Описание статуса	Hex код ответа	Описание ответа	№ ошибки на ФПСУ-IP	Внутреннее обозначение	Описание ошибки на ФПСУ-IP
00b	Unknown	0x00-0x3F	Unassigned			
01b	Forwarded	0x40	Unknown			
		0x41	Fragmented			
		0x42	Not Fragmente			

Статус	**Описание статуса**	**Hex код ответа**	**Описание ответа**	**№ ошибки на ФПСУ-IP**	**Внутреннее обозначение**	**Описание ошибки на ФПСУ-IP**
			d			
		0x43	Tunneled			
		0x44-0x7F	Unassigned			
10b	Dropped	0x81	ACL deny	7	AERR_PROHIBIT	Абонент запрещен
		0x82	ACL drop	17	AERR_PROHCONNECT	Запрет МЭ
		0x83	Unroutable	10	AERR_NOROUTE	Маршрут неизвестен (нет MAC-адреса)
		0x84	Adjacency			
		0x85	Fragmentation and DF set	19	AERR_CANTFRAG	Требуется фрагментация
		0x86	Bad header checksum			

Статус	Описание статуса	Нех код ответа	Описание ответа	№ ошибки на ФПСУ-IP	Внутреннее обозначение	Описание ошибки на ФПСУ-IP
		0x87	Bad total Length	3	AERR_SHORTPACK	Слишком короткий пакет
		0x88	Bad header length			
		0x89	Bad TTL	13	AERR_TTL	Истекло время жизни
		0x8A	Policer			
		0x8B	WRED			
		0x8C	RPF			
		0x8D	For us			
		0x8E	Bad output interface			
		0x8F	0x8F, Hardware	16	AERR_LAN	Сбой LAN-адаптера
		Коды AMICON (свободный диапазон 0x90-0xBF):				

Статус	Описание статуса	Нех код ответа	Описание ответа	№ ошибки на ФПСУ-IP	Внутреннее обозначение	Описание ошибки на ФПСУ-IP
		0x91	Unknown 17	1	AERR_NOMEM	Нет памяти для обработки пакета
		0x92	Unknown 18	2	AERR_BADADDR	Не верен IP адрес
		0x94	Unknown 20	4	AERR_DBLADDR	Дублирование адресов ФПСУ-IP
		0x95	Unknown 21	5	AERR_UNKNOWN	Отправитель не зарегистрирован на ФПСУ-IP
		0x96	Unknown 22	6	AERR_REMOTEUNKNOWN	Получатель не зарегистрирован на ФПСУ-IP
		0x98	Unknown 24	8	AERR_GUARDNEEDED	Абонент должен работать через ФПСУ-IP
		0x99	Unknown 25	9	AERR_GUARDNOTREADY	Удаленный ФПСУ-IP не работает
		0x9B	Unknown 27	11	AERR_IFACE	Запрет по интерфейсам доступа
		0x9C	Unknown 28	12	AERR_MODEWORK	Запрет по режиму работы с партнером
		0x9	Unknown	14	AERR_BADGUARD	Ложный ФПСУ-IP

Статус	Описание статуса	Hex код ответа	Описание ответа	№ ошибки на ФПСУ-IP	Внутреннее обозначение	Описание ошибки на ФПСУ-IP
		E	30			
		0x9F	Unknown 31	15	AERR_UNSUPREQ	Обращение с неподдерживаемым протоколом
		0xA2	Unknown 34	18	AERR_LENPACK	Длина фрагмента > 65536
		0xA4	Unknown 36	20	AERR_GUARDNOTNEEDED	Абонент должен работать в открытом виде, а пришел из туннеля с ФПСУ-IP
		0xA5	Unknown 37	21	AERR_TCPUDP	Запрет доступа по TCP/UDP портам
		0xA6	Unknown 38	22	AERR_SOURCEROUTE	Запрет доступа по SourceRoute
		0xA7	Unknown 39	23	AERR_INVALIDTOTLEN	Фрагмент не кратен 8
		0xA8	Unknown 40	24	AERR_INVALIDOPLIST	Неверен список опций
		0xA9	Unknown 41	25	AERR_GUARDIGNORE	Нет ФПСУ-IP туннеля
		0xAA	Unknown 42	26	AERR_GUARDREMERR	Ошибочный пакет ФПСУ-IP

Статус	Описание статуса	Hex код ответа	Описание ответа	№ ошибки на ФПСУ-IP	Внутреннее обозначение	Описание ошибки на ФПСУ-IP
		0xAB	Unknown 43	27	AERR_SERIALIZATION	Ошибка сериализации
		0xAC	Unknown 44	28	AERR_REDIRECT	Bad REDIRECT от XXX.XXX.XXX.XXX
		0xAD	Unknown 45	29	AERR_CLIBADPACK	Ошибочный пакет от клиента
		0xAE	Unknown 46	30	AERR_CLINOTCONNECT	ФПСУ-IP/Клиент не соединен
		0xAF	Unknown 47	31	AERR_IFACECLIENTUSER	Запрет доступа клиента к абоненту
		0xB0	Unknown 48	32	AERR_IFACECLIENTCLIENT	Запрет доступа клиента к клиенту
		0xB1	Unknown 49	33	AERR_VLANUNKNOWN	VLAN не прописан
		0xB2	Unknown 50	34	AERR_BRIDGELONGPACK	Длинный пакет для моста
		0xB3	Unknown 51	35	AERR_PROHMACADDR	Запрет работы по MAC адресу станции
11b	Consumed	0xC0	Unknown			

Статус	Описание статуса	Hex код ответа	Описание ответа	№ ошибки на ФПСУ-IP	Внутреннее обозначение	Описание ошибки на ФПСУ-IP
		0xC1	Punt Adjacency			
		0xC2	Incomplete Adjacency			
		0xC3	For us			
		0xC4-0xFF	Unassigned			

12. 2. 2. Отвергнутый трафик

Таблица 6. Шаблон 259

№ п/п	Код	Наименование кода	Типоразмер	Описание
1	10	ingressInterface	unsigned8	Номер порта ФПСУ-IP, на который были приняты пакеты
2	14	egressInterface	unsigned8	Номер порта ФПСУ-IP, через который пакеты должны быть отправлены, либо 0, если это неизвестно
3	8	sourceIPv4Addres	ipv4Address	IP-адрес отправителя

		s		
4	7	sourceTransportPort	unsigned16	TCP/UDP-порт отправителя
5	12	destinationIPv4Address	ipv4Address	IP-адрес получателя
6	11	destinationTransportPort	unsigned16	TCP/UDP-порт получателя
7	4	protocolIdentifier	unsigned8	Идентификатор протокола
8	150	flowStartSeconds	Milliseconds (64)	Время появления первого пакета в серии
9	151	flowEndSeconds	Milliseconds (64)	Время появления последнего пакета в серии
10	32	icmp_typecode	unsigned16	Тип/код сообщения для ICMP протокола см. пункт «Особенности реализации ICMP протокола» , таблица «Типы ICMP-ответов ФПСУ-IP»
11	44	sourceIPv4Prefix	ipv4Address	Адрес ФПСУ-IP, если абонент-отправитель прописан за ФПСУ-IP (либо 0)
12	45	destinationIPv4Prefix	ipv4Address	Адрес ФПСУ-IP, если абонент-получатель прописан через ФПСУ-IP (либо 0)
13	233	firewallEvent	unsigned8	Код события: 3 - flow_denied
14	89	forwardingStatus	unsigned8	Способ обработки пакета. Проставляется: Dropped + код ошибки, см. пункт «Коды IPFIX, используемые в шаблонах», таблица «Кодирование ошибок»
15	135	droppedPacketTotalCount	unsigned64	Общее количество пакетов в серии
16	133	droppedPacketDel	unsigned64	Количество пакетов с момента последнего отчета

		taCount		

12. 2. 3. Разрешенный трафик

Таблица 7. Шаблон 260

№ п/п	Код	Наименование кода	Типоразмер	Описание
1	1	octetDeltaCount	unsigned64	Количество октетов с момента предыдущего отчета (если есть) во входящих пакетах для этого потока в точке наблюдения. Количество октетов включает IP-заголовок(и) и полезную нагрузку IP
2	2	packetDeltaCount	unsigned64	Количество входящих пакетов с момента предыдущего отчета (если есть) для этого потока в точке наблюдения
3	4	protocolIdentifier	unsigned8	Идентификатор протокола
4	6	tcpControlBits	unsigned16	Наблюдаемые управляющие биты TCP для пакетов этого потока. Эта информация кодируется в виде битового поля; для каждого управляющего бита TCP в этом наборе есть бит. Бит устанавливается равным 1, если для любого наблюдаемого пакета этого потока установлен соответствующий бит управления TCP, равный 1. В противном случае бит будет очищен до 0. Значения каждого бита показаны ниже в соответствии с определением битов в заголовке TCP [RFC9293][RFC3168]: MSb LSb

				0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ | | | N | C | E | U | A | P | R | S | F / | Нулевой | Будущий | S | W | C | R | C | S | S / Y | I | | (Смещение данных) | Использовать | | R | E | G | K | H | T / N | N | +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ битовый флаг значение имя описание ------+-----+---------- 0x8000 Ноль (см. tcpHeaderLength) 0x4000 Ноль (см. tcpHeaderLength) 0x2000 Ноль (см. tcpHeaderLength) 0x1000 Ноль (см. tcpHeaderLength) 0x0800 Будущее использование 0x0400 Будущее использование 0x0200 Будущее использование 0x0100 NS ECN одноразовая сумма Уменьшено окно перегрузки 0x0080 CWR 0x0040 ECE ECN Echo 0x0020 URG Поле срочного указателя значимо 0x0010 Поле подтверждения подтверждения значимо

				Функция Push 0x0008 PSH 0x0004 СНАЧАЛА сбросьте соединение 0x0002 SYN Синхронизирует порядковые номера 0x0001 FIN Больше нет данных от отправителя Поскольку наиболее значимые 4 бита октетов 12 и 13 (считая от нуля) заголовка TCP [RFC9293] используются для кодирования смещения данных TCP (длины заголовка), соответствующие биты в этой информации Элемент ДОЛЖЕН быть экспортирован как ноль и ДОЛЖЕН игнорироваться сборщиком. Используйте информационный элемент tcpHeaderLength для кодирования этого значения. Каждый из 3 битов (0x800, 0x400 и 0x200), которые зарезервированы для будущего использования в [RFC9293], СЛЕДУЕТ экспортировать, как указано в заголовках TCP пакетов этого потока. При экспорте в виде одного октета с кодировкой уменьшенного размера этот информационный элемент охватывает октет младшего порядка этого поля (т.Е. биты от 0x80 до 0x01), исключая одноразовую сумму ECN и три бита будущего использования. Сборщик, получающий этот информационный элемент с кодировкой уменьшенного размера, не должен ничего предполагать о содержимом этих четырех битов. Экспортирующие процессы, экспортирующие этот информационный элемент от имени процесса учета, который не способен отслеживать какие-

				либо биты одноразового номера ECN или биты будущего использования, ДОЛЖНЫ использовать кодирование уменьшенного размера и экспортировать только 8 младших значащих битов этого информационного элемента. Обратите внимание, что в предыдущих версиях определения этого информационного элемента указывалось, что биты CWR и ECE должны экспортироваться как нулевые, даже если они соблюдены. Поэтому сборщики не должны предполагать, что нулевое значение для этих битов в этом информационном элементе указывает, что биты никогда не устанавливались в наблюдаемом трафике, особенно если эти биты равны нулю в каждой записи потока, отправленной данным экспортером.
5	7	sourceTransportPort	unsigned16	TCP/UDP-порт отправителя
6	8	sourceIPv4Address	ipv4Address	IP-адрес отправителя
7	10	ingressInterface	unsigned32	Номер порта ФПСУ-IP, на который были приняты пакеты
8	11	destinationTransportPort	unsigned16	TCP/UDP-порт получателя
9	12	destinationIPv4Address	ipv4Address	IP-адрес получателя
10	14	egressInterface	unsigned32	Номер порта ФПСУ-IP, через который пакеты должны быть отправлены, либо 0, если это неизвестно
11	32	icmpTypeCodeIPv4	unsigned16	Тип/код сообщения для ICMP протокола

				см. пункт «Особенности реализации ICMP протокола» , таблица «Типы ICMP-ответов ФПСУ-IP»
12	44	sourceIPv4Prefix	ipv4Address	Адрес ФПСУ-IP, если абонент-отправитель прописан за ФПСУ-IP, либо 0
13	45	destinationIPv4Prefix	ipv4Address	Адрес ФПСУ-IP, если абонент-получатель прописан через ФПСУ-IP, либо 0
14	152	flowStartMilliseconds	dateTimeMilliseconds	Абсолютная временная метка первого пакета этого потока
15	153	flowEndMilliseconds	dateTimeMilliseconds	Абсолютная временная метка последнего пакета этого потока
16	231	initiatorOctets	unsigned64	Общее количество байтов полезной нагрузки уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и остается неизменным в течение срока действия сеанса
17	232	responderOctets	unsigned64	Общее количество байтов полезной нагрузки уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик - это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса
18	233	firewallEvent		Код события: 3 → flow_denied Указывает на событие брандмауэра. Допустимые значения перечислены в реестре firewallEvent: Значение Описание 0 Ignore (invalid) 1 Flow Created 2 Flow Deleted 3 Flow Denied 4 Flow Alert 5 Flow Update

				6-255 Unassigned
19	298	initiatorPackets	unsigned64	Общее количество пакетов уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и остается неизменным в течение всего срока действия сеанса
20	299	responderPackets	unsigned64	Общее количество пакетов уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик - это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса

12. 2. 4. Трафик с NAT

Таблица 8. Шаблон 258

№ п/п	Код	Наименование кода	Типоразмер	Описание
1	1	octetDeltaCount	unsigned64	Количество октетов с момента предыдущего отчета (если есть) во входящих пакетах для этого потока в точке наблюдения. Количество октетов включает IP-заголовок(и) и полезную нагрузку IP
2	2	packetDeltaCount	unsigned64	Количество входящих пакетов с момента предыдущего отчета (если есть) для этого потока в точке наблюдения
3	4	protocolIdentifier	unsigned8	Идентификатор протокола
4	6	tcpControlBits	unsigned16	Наблюдаемые управляющие биты TCP для пакетов этого потока. Эта информация кодируется в виде битового поля; для каждого

				управляющего бита TCP в этом наборе есть бит. Бит устанавливается равным 1, если для любого наблюдаемого пакета этого потока установлен соответствующий бит управления TCP, равный 1. В противном случае бит будет очищен до 0. Значения каждого бита показаны ниже в соответствии с определением битов в заголовке TCP [RFC9293][RFC3168]: MSb LSb 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ | | | N | C | E | U | A | P | R | S | F / | Нулевой | Будущий | S | W | C | R | C | S | S / Y | I | | (Смещение данных) | Использовать | | R | E | G | K | H | T / N | N | +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ битовый флаг значение имя описание ------+-----+---------- 0x8000 Ноль (см. tcpHeaderLength) 0x4000 Ноль (см. tcpHeaderLength)

				0x2000 Ноль (см. tcpHeaderLength) 0x1000 Ноль (см. tcpHeaderLength) 0x0800 Будущее использование 0x0400 Будущее использование 0x0200 Будущее использование 0x0100 NS ECN одноразовая сумма Уменьшено окно перегрузки 0x0080 CWR 0x0040 ECE ECN Echo 0x0020 URG Поле срочного указателя значимо 0x0010 Поле подтверждения подтверждения значимо Функция Push 0x0008 PSH 0x0004 СНАЧАЛА сбросьте соединение 0x0002 SYN Синхронизирует порядковые номера 0x0001 FIN Больше нет данных от отправителя Поскольку наиболее значимые 4 бита октетов 12 и 13 (считая от нуля) заголовка TCP [RFC9293] используются для кодирования смещения данных TCP (длины заголовка), соответствующие биты в этой информации Элемент ДОЛЖЕН быть экспортирован как ноль и ДОЛЖЕН игнорироваться сборщиком. Используйте информационный элемент tcpHeaderLength для кодирования этого значения. Каждый из 3 битов (0x800, 0x400 и 0x200),

				которые зарезервированы для будущего использования в [RFC9293], СЛЕДУЕТ экспортировать, как указано в заголовках TCP пакетов этого потока. При экспорте в виде одного октета с кодировкой уменьшенного размера этот информационный элемент охватывает октет младшего порядка этого поля (т.Е. биты от 0x80 до 0x01), исключая одноразовую сумму ECN и три бита будущего использования. Сборщик, получающий этот информационный элемент с кодировкой уменьшенного размера, не должен ничего предполагать о содержимом этих четырех битов. Экспортирующие процессы, экспортирующие этот информационный элемент от имени процесса учета, который не способен отслеживать какие-либо биты одноразового номера ECN или биты будущего использования, ДОЛЖНЫ использовать кодирование уменьшенного размера и экспортировать только 8 младших значащих битов этого информационного элемента. Обратите внимание, что в предыдущих версиях определения этого информационного элемента указывалось, что биты CWR и ECE должны экспортироваться как нулевые, даже если они соблюдены. Поэтому сборщики не должны предполагать, что нулевое значение для этих битов в этом информационном элементе указывает, что биты никогда не

				устанавливались в наблюдаемом трафике, особенно если эти биты равны нулю в каждой записи потока, отправленной данным экспортером.
5	7	sourceTransportPort	unsigned16	TCP/UDP-порт отправителя
6	8	sourceIPv4Address	ipv4Address	IP-адрес отправителя
78	10	ingressInterface	unsigned32	Номер порта ФПСУ-IP, на который были приняты пакеты
9	11	destinationTransportPort	unsigned16	TCP/UDP-порт получателя
10	12	destinationIPv4Address	ipv4Address	IP-адрес получателя
11	14	egressInterface	unsigned32	Номер порта ФПСУ-IP, через который пакеты должны быть отправлены, либо 0, если это неизвестно
12	32	icmpTypeCodeIPv4	unsigned16	Тип/код сообщения для ICMP протокола см. пункт «Особенности реализации ICMP протокола» , таблица «Типы ICMP-ответов ФПСУ-IP»
13	44	sourceIPv4Prefix	ipv4Address	Адрес ФПСУ-IP, если абонент-отправитель прописан за ФПСУ-IP, либо 0
14	45	destinationIPv4Prefix	ipv4Address	Адрес ФПСУ-IP, если абонент-получатель прописан через ФПСУ-IP, либо 0
15	152	flowStartMilliseconds	dateTimeMilliseconds	Абсолютная временная метка первого пакета этого потока
16	153	flowEndMilliseconds	dateTimeMilliseconds	Абсолютная временная метка последнего пакета этого потока
17	225	postNATSourceIPv4Ad	ipv4Address	Определение этого информационного

		dress		элемента идентично определению информационного элемента 'sourceIPv4Address', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока NAT после того, как пакет прошел точку наблюдения
18	226	postNATDestinationIPv4Address	ipv4Address	Определение этого информационного элемента идентично определению информационного элемента 'destinationIPv4Address', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока NAT после того, как пакет прошел точку наблюдения
19	227	postNAPTSourceTransportPort	unsigned16	Определение этого информационного элемента идентично определению информационного элемента 'sourceTransportPort', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока преобразования сетевого адреса (NAPT) после того, как пакет прошел точку наблюдения
20	228	postNAPTDestinationTransportPort	unsigned16	Определение этого информационного элемента идентично определению информационного элемента 'destinationTransportPort', за исключением того, что он сообщает об измененном значении, вызванном функцией промежуточного блока преобразования сетевого адреса (NAPT) после того, как пакет прошел точку наблюдения.
21	231	initiatorOctets	unsigned64	Общее количество байтов полезной нагрузки уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и остается неизменным в течение срока

				действия сеанса.
22	232	responderOctets	unsigned64	Общее количество байтов полезной нагрузки уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик - это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса.
23	233	firewallEvent		Код события: 3 → flow_denied Указывает на событие брандмауэра. Допустимые значения перечислены в реестре firewallEvent: Значение Описание 0 Ignore (invalid) 1 Flow Created 2 Flow Deleted 3 Flow Denied 4 Flow Alert 5 Flow Update 6-255 Unassigned
24	298	initiatorPackets	unsigned64	Общее количество пакетов уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и остается неизменным в течение всего срока действия сеанса.
25	299	responderPackets	unsigned64	Общее количество пакетов уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик - это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса.

12. 3. Syslog-клиент на ФПСУ-IP

ФПСУ-IP поддерживает возможность отправки сообщений о происходящих на ФПСУ-IP событиях по протоколу SysLog. Для этого реализована подсистема, которая отслеживает происходящие на ФПСУ-IP события и отправляет их на внешний SysLog-сервер.

Сообщения отправляются в кодировке OEM/DOS (866) по умолчанию (может быть переключена на UTF-8).

Для настройки SysLog-клиента на ФПСУ-IP следует указать IP-адрес SysLog сервера, на который будут отправляться сообщения, настроить список и параметры для регистрируемых событий. **ВНИМАНИЕ!** IP-адрес SysLog сервера должен быть ранее внесен в список абонентов порта как разрешенный к работе IP-адрес (см. пункт «Описание параметров абонентов»).

Доступ к окну настроек параметров SysLog на ФПСУ-IP предоставляется из меню *«Сетевые сервисы»* конфигурации ФПСУ-IP при выборе в подменю команды *«SysLog/SNMP»*.

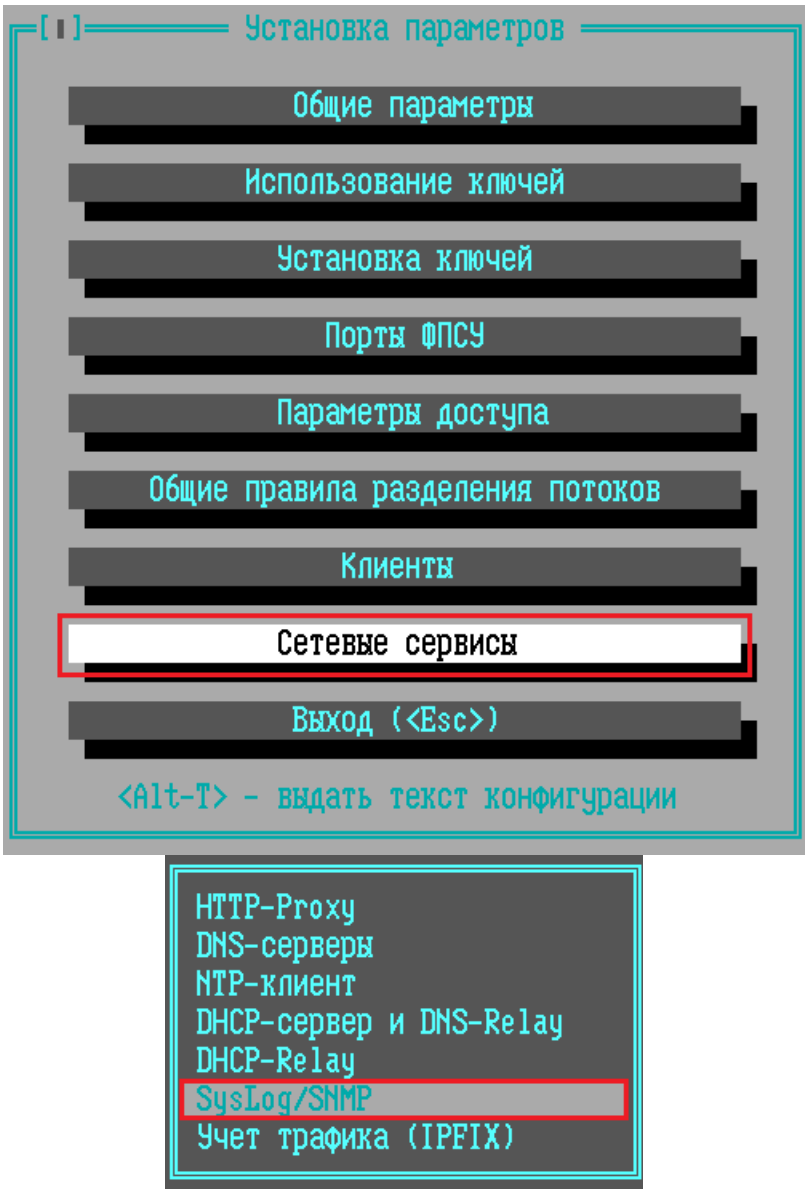


Рисунок 299 - Команда меню «Сетевые сервисы» → «SysLog/SNMP»

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.

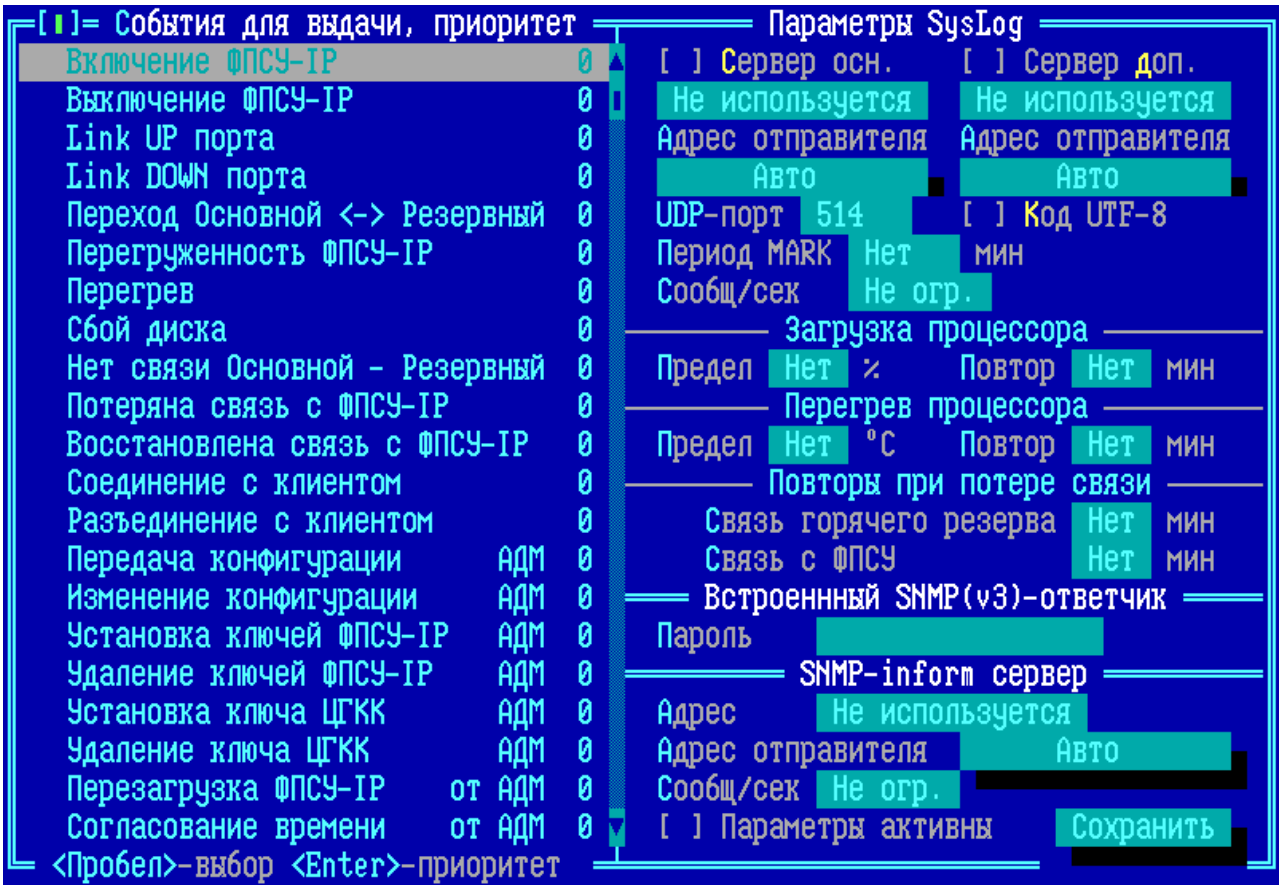


Рисунок 300 - Настройка параметров SysLog

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 9. 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	100003	Удаленный администратор ФПСУ-IP передал на

Название события	**Код события в тексте SysLog сообщения**	**Причина**
конфигурации АДМ		ФПСУ-IP и активизировал изменённую конфигурацию
Установка ключей ФПСУ АДМ	100004	Удаленный администратор ФПСУ-IP выполнил установку на ФПСУ-IP ключей парно-выборочной связи
Удаление ключей ФПСУ АДМ	100005	Удаленный администратор ФПСУ-IP выполнил удаление с ФПСУ-IP ключей парно-выборочной связи
Установка ключа ЦГКК АДМ	100006	Удаленный администратор ФПСУ-IP выполнил установку на ФПСУ-IP общесистемного ключа Криптосети Клиентов
Удаление ключа ЦГКК АДМ	100007	Удаленный администратор ФПСУ-IP выполнил удаление с ФПСУ-IP общесистемного ключа Криптосети Клиентов
Перезагрузка ФПСУ-IP АДМ	100008	Удаленным администратором произведена перезагрузка комплекса ФПСУ-IP
Согласование времени с АДМ	100009	Время на ФПСУ-IP было синхронизировано со временем на АРМ УА ФПСУ-IP
Подключение УА	100010	Удаленный администратор подключился к ФПСУ-IP
Локальная установка	110001	Локальный администратор ФПСУ-IP выполнил установку на ФПСУ-IP ключей парно-выборочной

Название события	**Код события в тексте SysLog сообщения**	**Причина**
ключей ФПСУ		связи
Локальное удаление ключей ФПСУ АДМ	110002	Локальный администратор ФПСУ-IP выполнил удаление с ФПСУ-IP ключей парно-выборочной связи
Локальная установка ключа ЦГКК	110003	Локальный администратор ФПСУ-IP выполнил установку на ФПСУ-IP общесистемного ключа Криптосети Клиентов
Локальное удаление ключа ЦГКК	110004	Локальный администратор ФПСУ-IP выполнил удаление с ФПСУ-IP общесистемного ключа Криптосети Клиентов
Локальное изменение конфигурации	110005	Локальный администратор ФПСУ-IP изменил конфигурацию
Изменение конфигурации LAN-адаптеров	110006	Локальный администратор ФПСУ-IP изменил конфигурацию LAN-адаптеров
Потеряна связь с ФПСУ	200001	Произошло разъединение защищенного соединения (туннеля) с удаленным ФПСУ-IP
Восстановлена связь с ФПСУ	200002	Установлен туннель с удалённым ФПСУ-IP

Название события	**Код события в тексте SysLog сообщения**	**Причина**
Включение ФПСУ	200003	Включение работы ФПСУ-IP в режим фильтрации
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 ФПСУ-IP/Клиентом	300001	Установлено защищенное соединение (туннель) с комплексом ФПСУ-IP/Клиент
Разъединение с ФПСУ-IP/Клиентом	300002	Произошло разъединение защищенного соединения (туннеля) с комплексом ФПСУ-IP/Клиент
События удаленной загрузки ключей	300010	Запрос получения ключа ФПСУ-IP/Клиентом
	300011	Запрос обновления ключа на ФПСУ-IP/Клиенте
	300012	Подтверждение получения ключа ФПСУ-IP/Клиентом
Авторизация ФПСУ-IP/Клиента	300020	Произошла авторизация ФПСУ-IP/Клиента на сервере RADIUS
Переход Основной -	400001	Произошла передача управления партнёру по горячему резервированию

Название события	Код события в тексте SysLog сообщения	Причина
Резервный		
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
Перегрев	500003	Температура ЦПУ ФПСУ-IP достигла порогового значения, указанного в параметре «Перегрев процессора, Температура»
Сбой диска	500004	Произошла ошибка при обращении к внутреннему накопителю информации ФПСУ-IP, обычно при попытке записи статистической информации
Текущая температура	500005	Периодическое отправление сообщения с текущим уровнем нагрева ЦПУ ФПСУ-IP, периодичность отправки указывается в параметре «Перегрев процессора, Повтор»
Окончание поддержки	500006	Заканчивается текущий срок поддержки программно-аппаратного комплекса ФПСУ-IP
Журнал ARP-	510001	MAC-адрес добавлен в ARP-таблицу

Название события	**Код события в тексте SysLog сообщения**	**Причина**
записей	510002	MAC-адрес исключен из ARP-таблицы
События МЭ	700001	Соединение разрешено МЭ
	700002	Соединение запрещено МЭ
Блокировка абонента МЭ (flood)	700003	Абонент заблокирован МЭ (flood)
	700004	Абонент разблокирован МЭ (flood)
Блокировка ресурсов	700007	Блокировка абонента межсетевым экраном ФПСУ-IP
	700008	Разблокировка абонента межсетевым экраном ФПСУ-IP
Соединение запрещено МЭ (DPI)	700013	Соединение было сброшено межсетевым экраном ФПСУ-IP по одному из правил DPI

Каждому из событий в соответствии с протоколом SysLog назначается его приоритет, от 0 до 7. Приоритет имеет значение для принимающего сообщение SysLog сервера, и интерпретируется следующим образом:

Таблица 10. Приоритеты Syslog-сообщений

Приоритет	**Описание**
0	Авария: система неработоспособна (экстренная ситуация или останов системы);
1	Тревога: действия должны быть предприняты немедленно (Срочные ситуации);
2	Критично: критические условия и состояния;

3	Ошибка: состояния ошибок (условия ошибки);
4	Предупреждение: условия предупреждений;
5	Извещение: нормальное рабочее состояние, но заслуживающее внимания условие (необычные состояния);
6	Информация: информационные сообщения;
7	Отладка: сообщения диагностического уровня.

Приоритет каждому событию может быть назначен администратором ФПСУ-IP в значения по умолчанию, а также выставлен вручную для каждого события. Для установки приоритетов по умолчанию нажмите в окне «Параметры SysLog» сочетание клавиш <*Ctrl+Enter*> и выберите в появившемся служебном окне предупреждения ответ «Да». Для установки приоритета событию вручную установите курсор на событии, нажмите <*Enter*>, и выберите новый приоритет события.

12. 3. 2. Опции работы с SysLog сервером

Кроме списка отправляемых серверу событий, в окне настроек, в правой части, находится ряд опций работы с сервером SysLog, где находятся следующие настраиваемые параметры:

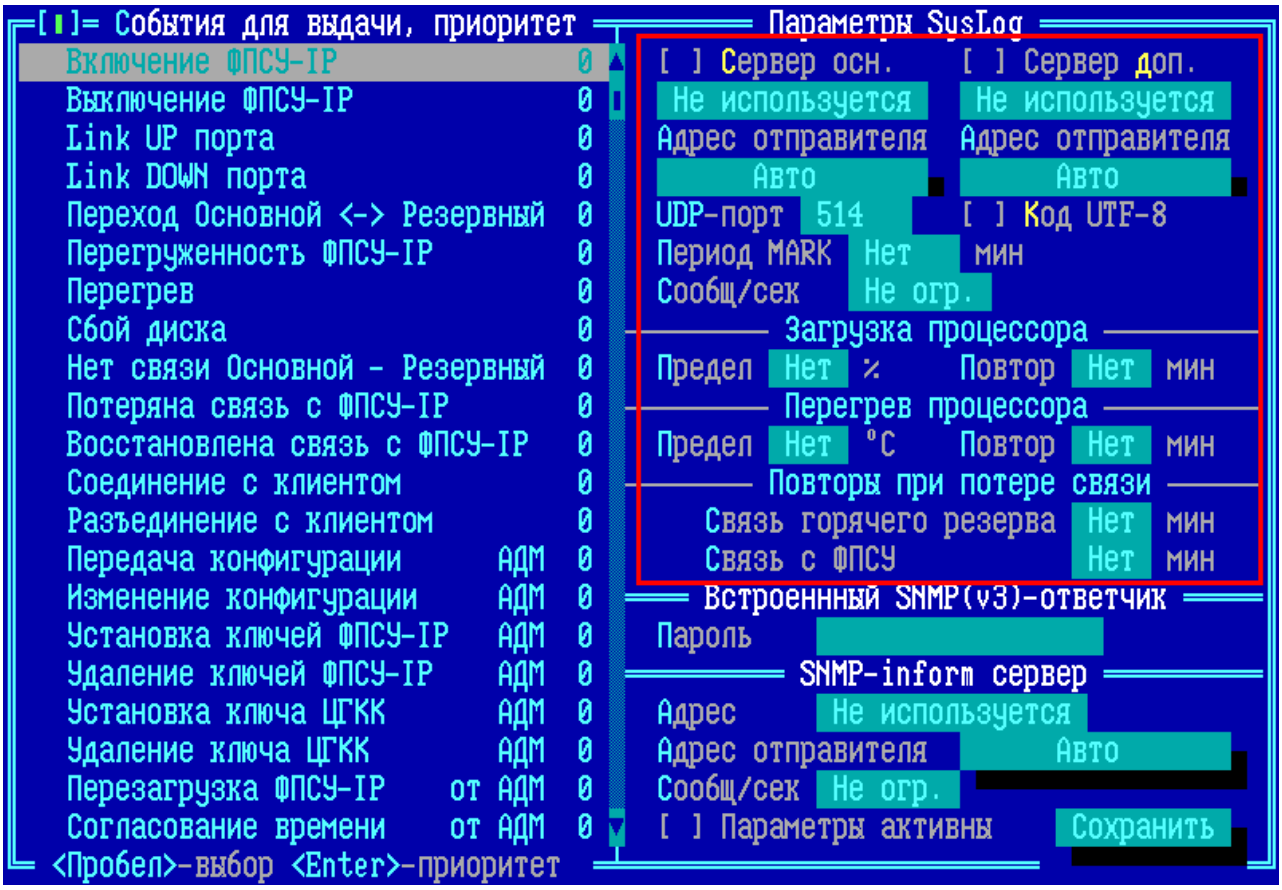


Рисунок 301 - Параметры SysLog

Сервер осн., Сервер доп. — при включении флага в поле ниже указывается IP-адрес SysLog сервера основного и дополнительного, на них будут отправляться SysLog-сообщения.

UDP порт — поле выбора UDP-порта принимающего сообщения SysLog сервера. По умолчанию - рекомендуемый UDP:514.

Код UTF-8 — если флаг задействован, сообщения отправляются в кодировке UTF-8 (кодировкой по умолчанию со снятым флагом является OEM/DOS (866).

Адрес отправителя — порт ФПСУ-IP, чей IP-адрес будет указан в качестве отправителя SysLog-сообщений. По умолчанию, режима «*Авто*», в качестве отправителя будет указан тот порт, на котором описан принадлежащий Syslog-серверу IP-адрес. Администратор может безусловно указать, что сообщения следует отправлять от IP-адреса 1 или 2 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 — если флаг задействован, сообщения отправляются в кодировке UTF-8 (кодировкой по умолчанию со снятым флагом является 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 11. 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
Служебное число	Дата и время в формате Мес ДД ЧЧ:ММ:СС	Серийный номер ФПСУ-IP, отправившего сообщение	Текст [FPSU]:	Код события в соответствии с таблицей 4	Текст, содержащий название события	Дополнительные поля, в зависимости от события	1, если основной/ единственный ФПСУ;

							2, резервный

Кроме полей заголовка, к сообщению прикрепляется дополнительная информация, в зависимости от произошедшего события:

100001 Передача конфигурации АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора, текстовый комментарий удаленного администратора;

100003 Изменение конфигурации АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора, текстовый комментарий удаленного администратора;

100004 Установка ключей ФПСУ АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора, служебный текст «Ключ» имя группы ключей, номер серии ключей, номер комплекта ключей, текстовый комментарий удаленного администратора;

100005 Удаление ключей ФПСУ АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора, служебный текст «Ключ» имя группы ключей, номер серии ключей, номер комплекта ключей, текстовый комментарий удаленного администратора;

100006 Установка ключа ЦГКК АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора, служебный текст «Криптосеть номер» номер установленной Криптосети Клиентов, текстовый комментарий удаленного администратора;

100007 Удаление ключа ЦГКК АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора, служебный текст «Криптосеть номер» номер удалённой Криптосети Клиентов, текстовый комментарий удаленного администратора;

100008 Перезагрузка ФПСУ АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора;

100009 Согласование времени с АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора, текстовый

комментарий удаленного администратора;

100010 Подключение УА – служебный текст «Удаленный администратор», имя удаленного администратора, служебный текст «подключился с IP-адреса» IP адрес удалённого администратора, «на порт» PORT;

110001 Локальная установка ключей ФПСУ – служебный текст «Локальная установка ключей ФПСУ, Ключ», имя группы ключей, номер ключа, служебный текст «Серия» номер серии ключей, служебный текст «предъявлен токен» имя(роль) локального администратора;

110002 Локальное удаление ключей ФПСУ АДМ – служебный текст «Локальное удаление ключей ФПСУ, Ключ», имя группы ключей, номер ключа, служебный текст «Серия» номер серии ключей, служебный текст «предъявлен токен» имя(роль) локального администратора;

110003 Локальная установка ключа ЦГКК – служебный текст «Локальная установка ключей клиентов, Криптосеть», имя Криптосети, служебный текст «Серия» номер серии ключей, служебный текст «предъявлен токен» имя(роль) локального администратора;

110004 Локальное удаление ключа ЦГКК – служебный текст «Локальное удаление ключей клиентов, Криптосеть», имя Криптосети, служебный текст «Серия» номер серии ключей, служебный текст «предъявлен токен» имя(роль) локального администратора;

110005 Локальное изменение конфигурации – служебный текст «Локальное изменение конфигурации», служебный текст «предъявлен токен» имя(роль) локального администратора;

110006 Изменение конфигурации LAN-адаптеров – служебный текст «Локальное изменение конфигурации LAN-адаптеров», служебный текст «предъявлен токен» имя локального администратора;

200001 Потеряна связь с ФПСУ – серийный номер и IP-адрес ФПСУ-IP, с которым потеряно защищенное соединение;

200002 Восстановлена связь с ФПСУ – серийный номер и IP-адрес ФПСУ-IP, с которым восстановлено защищенное соединение;

200003 Включение ФПСУ – дополнительные поля отсутствуют;

200004 Выключение ФПСУ – дополнительные поля отсутствуют;

200005 Перегруженность ФПСУ – загрузка ЦПУ, в процентах;

200007 Период <MARK> – служебный текст «CPU(%)», загрузка ЦПУ, «Температура», температура ЦПУ по шкале Цельсия;

300001 Соединение с клиентом – имя подключившегося Клиента, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, серийный номер устройства VPN-Key/Client, служебный текст «Порт», номер порта ФПСУ-IP, к

которому произошло подключение; служебный текст «IP», IP-адрес порта ФПСУ-IP, к которому произошло подключение; служебный текст «IP-адрес NAT/Real», выданный от ФПСУ-IP NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети, MAC-адрес подключившегося Клиента, служебный текст «HW vers:», версия микрокода устройства VPN-Key/Клиент, служебный текст «SW vers:» версия программного обеспечения ФПСУ-IP/Клиента, служебный текст «OS vers:» название и версия операционной системы рабочей станции подключившегося Клиента;

300002 Разъединение с клиентом – имя отключившегося Клиента, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, серийный номер устройства VPN-Key/Client, служебный текст «Port», номер порта ФПСУ-IP, от которого произошло отключение; служебный текст «IP», IP-адрес порта ФПСУ-IP, от которого произошло отключение; служебный текст «IP-адрес NAT/Real», полученный от ФПСУ-IP NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети, MAC-адрес отключившегося Клиента;

300010 – служебный текст «RKL: Запрос на получение ключа» имя группы ключей, номер ключа, служебный текст «токен» имя(роль) локального администратора, O/C, ID, ключ, лицензия, администратор;

300011 – служебный текст «RKL: Запрос на обновление ключа» имя группы ключей, номер ключа, служебный текст «токен» имя(роль) локального администратора, O/C, ID, ключ, лицензия, администратор;

300012 – служебный текст «RKL: Подтверждение получения ключа» имя группы ключей, номер ключа, ID, терминал;

300020 – служебный текст «Авторизация RADIUS» имя Клиента, логин на сервере RADIUS, номер Криптосети Клиента - номер Группы Клиента - номер Клиента в группе, служебный текст «s/n», серийный номер устройства VPN-Key/Client, служебный текст «Port», номер порта ФПСУ-IP, с которого произошла авторизация; служебный текст «IP», IP-адрес порта ФПСУ-IP, с которого произошла авторизация; служебный текст «IP-адрес NAT/Real», полученный от ФПСУ-IP NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети;

400001 Переход Основной - Резервный – режим функционирования ФПСУ-IP горячего резерва, на который произошло переключение (основной или резервный);

400002 Нет связи Основной - Резервный – режим функционирования ФПСУ-IP горячего резерва, с которым не удаётся установить связь (основной или резервный);

400003 Нет канала Основной - Резервный – служебный текст «Нет связи на порту», номер порта ФПСУ-IP, служебный текст «горячего резерва»;

500001 Link UP порта – логический номер LAN-порта, а также его IP-адрес;

500002 Link DOWN порта – логический номер LAN-порта, а также его IP-адрес;

500003 Перегрев – температура ЦПУ по шкале Цельсия;

500004 Сбой диска – дополнительные поля отсутствуют;
500005 Текущая температура – служебный текст «Температура», температура ЦПУ по шкале Цельсия;
500006 Окончание поддержки – служебный текст «Поддержка комплекса истекает», дата;
510001 MAC-адрес занесен в ARP-таблицу – служебный текст «MAC-адрес добавлен» MAC-адрес станции, IP-адрес станции, «Порт ФПСУ» PORT, «VLAN ID» VLAN;
510002 MAC-адрес исключен из ARP-таблицы – служебный текст «MAC-адрес удален» MAC-адрес станции, IP-адрес станции, «Порт ФПСУ» PORT, «VLAN ID» VLAN;
700001 Соединение разрешено МЭ – Служебный текст «Соединение разрешено МЭ» ,«SRC IP:port» IP:port «(SRC NAT/MAP » IP:port «)», «DST IP:port» IP:port «(DST NAT/MAP » IP:port «)», «Протокол» PROTO, «Правило» Rules name, «SRC данные/пакеты» byte/pkt, «DST данные/пакеты» byte/pkt, «Входящий порт ФПСУ» PORT, «Исходящий порт ФПСУ» PORT, «Длительность» work time «сек»;
700002 Соединение запрещено МЭ – Служебный текст «Соединение запрещено МЭ» , «SRC IP:port» IP:port, «DST IP:port» IP:port, «Протокол» PROTO, «Правило» Rule name (FLOOD/IPS/RADM), «Порт ФПСУ» PORT, time;
700003 Абонент заблокирован МЭ (flood) – Служебный текст "FLOOD заблокировал", IP-адрес, период блокировки «с до» в формате hh:mm:ss;
700004 Абонент разблокирован МЭ (flood) – Служебный текст "FLOOD разблокировал", IP-адрес, время в формате hh:mm:ss;
700007 Блокировка абонента МЭ ФПСУ-IP – служебный текст «Администратор» удаленный администратор, «заблокировал IP» IP-адрес, период блокировки «с до» в формате mm-dd-yyyy hh:mm:ss;
700008 Разблокировка абонента МЭ ФПСУ-IP – служебный текст «Администратор» удаленный администратор, «разблокировал IP» IP-адрес, период разблокировки «с» в формате mm-dd-yyyy hh:mm:ss;
700013 Соединение запрещено МЭ (DPI) – служебный текст «Соединение заблокировано подсистемой DPI, правило», правило, IP:port источника, IP:port назначения, «PROTO» протокол, «Правило» Rule name DPI, time.

12. 4. SNMP-клиент на ФПСУ-IP

ФПСУ-IP поддерживает возможность отправки сообщений о происходящих на ФПСУ-IP событиях по протоколу SNMP. Для этого реализована подсистема, которая отслеживает происходящие на ФПСУ-IP события и отправляет их в ответ на запросы

SNMP-менеджера.

Доступ к окну настроек параметров SNMP-клиента на ФПСУ-IP предоставляется меню «*Сетевые сервисы*» конфигурации ФПСУ-IP при выборе в подменю команды «*SysLog/SNMP*».

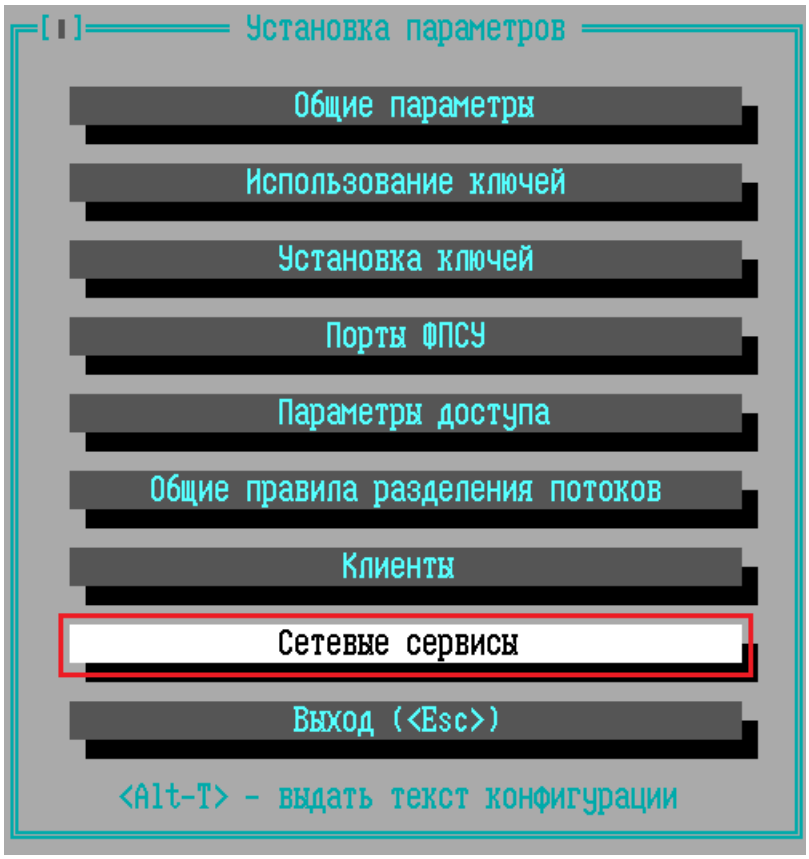


Рисунок 302 - Команда меню «Сетевые сервисы» → «SysLog/SNMP»

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.

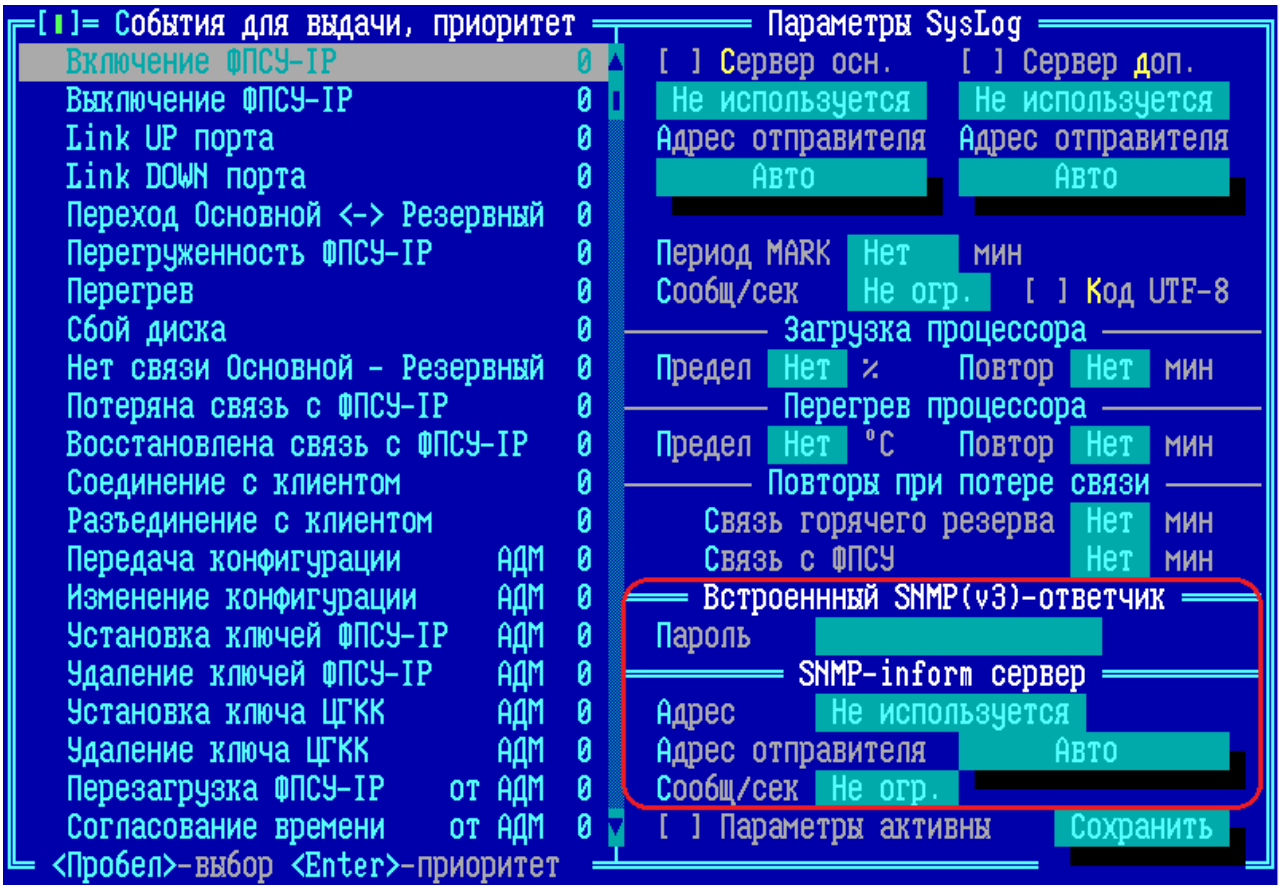


Рисунок 303 - Интерфейс настройки SNMP

Настраиваемые параметры SNMP-клиента:

Встроенный SNMP(v3)-ответчик, Пароль — символьный пароль, указание которого требуется при направлении запроса к SNMP-агенту, работающего на ФПСУ-IP, от SNMP-менеджера. Поле можно оставить пустым, в таком случае пароль не будет установлен.

SNMP-inform сервер, Адрес — IP-адрес SNMP-менеджера, на него будут отправляться SNMP TRAP сообщения;

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

SNMP-inform сервер, Сообщений/сек — максимальное количество SysLog-сообщений о событиях на настраиваемом ФПСУ-IP, отправляемое в секунду. Рекомендуется

устанавливать значение не более 100. По умолчанию не ограничено;

Параметры активны — флаг, при установлении которого включается обработка и отправка сообщений в ответ на SNMP-запросы и выполнение SNMP TRAP, в поле «*Адрес*» должен быть задан IP-адрес SNMP-менеджера. При выключенном флаге обработка и отправка сообщений в ответ на SNMP-запросы и выполнение SNMP TRAP не происходит. Включение или выключение осуществляется клавишей <*Пробел*>.

Помимо настроек на стороне ФПСУ-IP, на стороне SNMP-менеджера требуется указать определенные параметры для подключения:

- MIB база ФПСУ-IP доступна для скачивания через Internet по адресу https://amicon.ru/download.php;
- поддерживаемая версия SNMP-протокола — 3;
- в настройках SNMP-агента используемого SNMP-менеджера следует указать определенное имя пользователя — «***authOnlyUser***». Обратитесь к руководству пользователя используемого SNMP-менеджера для уточнения настраиваемых параметров;
- информация о событиях на ФПСУ-IP доступна в ветке OID - .1.3.6.1.4.1.37249.

Например, для SNMP-менеджера iReasoning MIB Browser параметры управляемого SNMP-агента выглядят следующим образом:

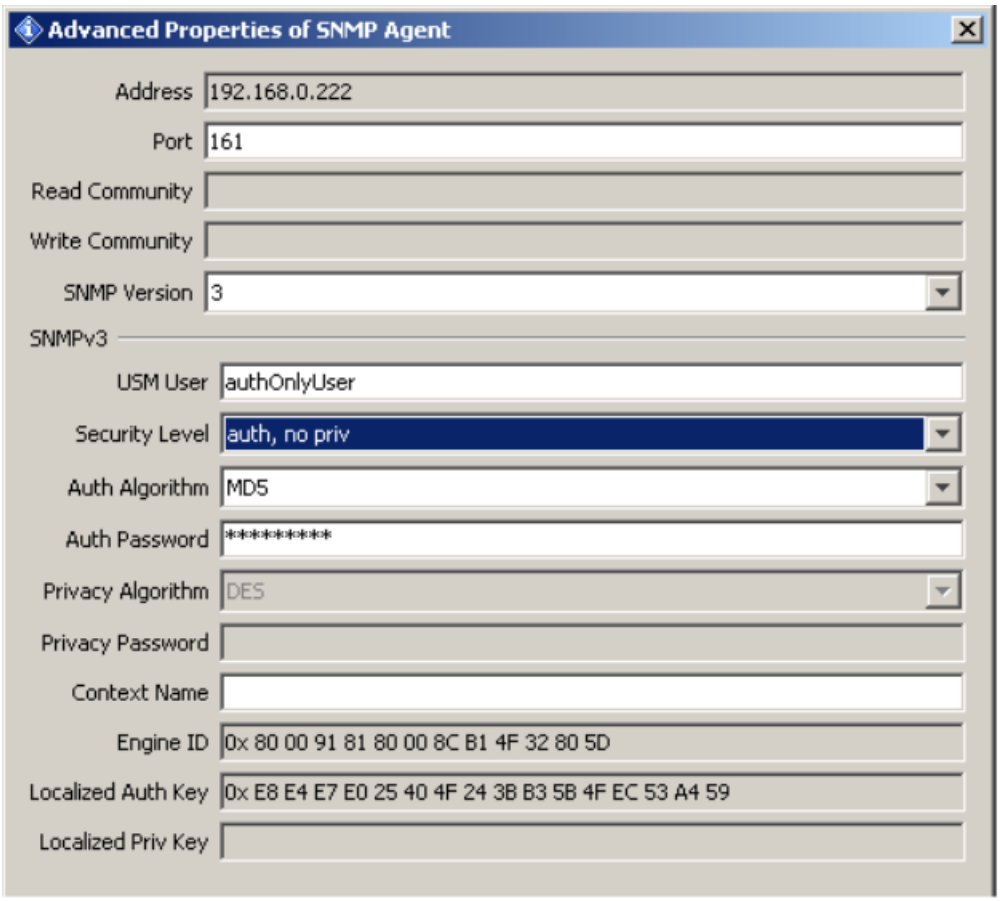


Рисунок 304 - Настройки SNMP-агента ФПСУ-IP в iReasoning MIB Browser

12. 5. DNS-серверы

ФПСУ-IP поддерживает стандартный протокол DNS для некоторых установленных подсистем, используется для разрешения сетевых имён. При подключенной системе удаленной загрузки ключевых данных клиентов (RKL) на ФПСУ-IP необходимо задать DNS-сервер.

Для указания DNS-сервера выберите в меню «Сетевые сервисы» конфигурации ФПСУ-IP команду *«DNS-серверы»*:

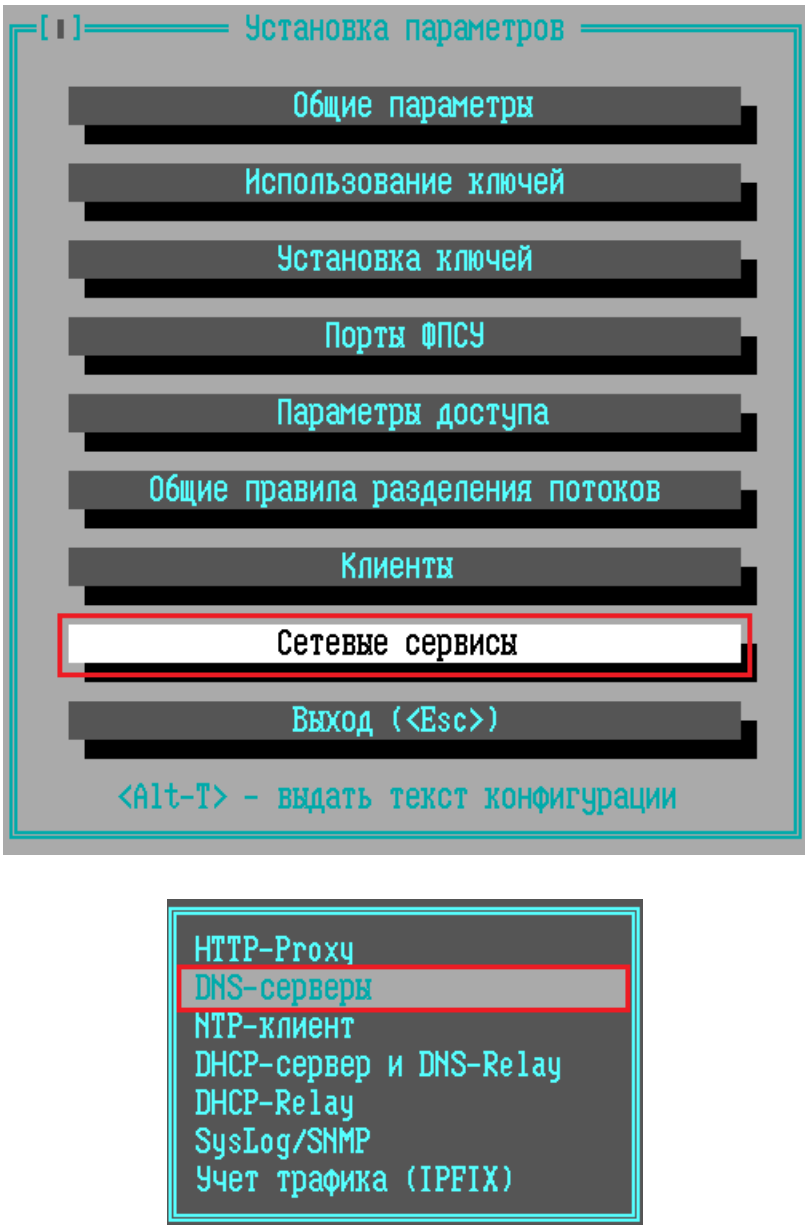


Рисунок 305 - Команда меню «Сетевые сервисы» → «DNS-серверы»

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»).

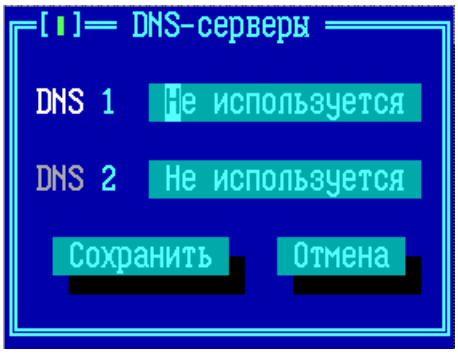


Рисунок 306 - Окно «DNS-серверы»

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

12. 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*»:

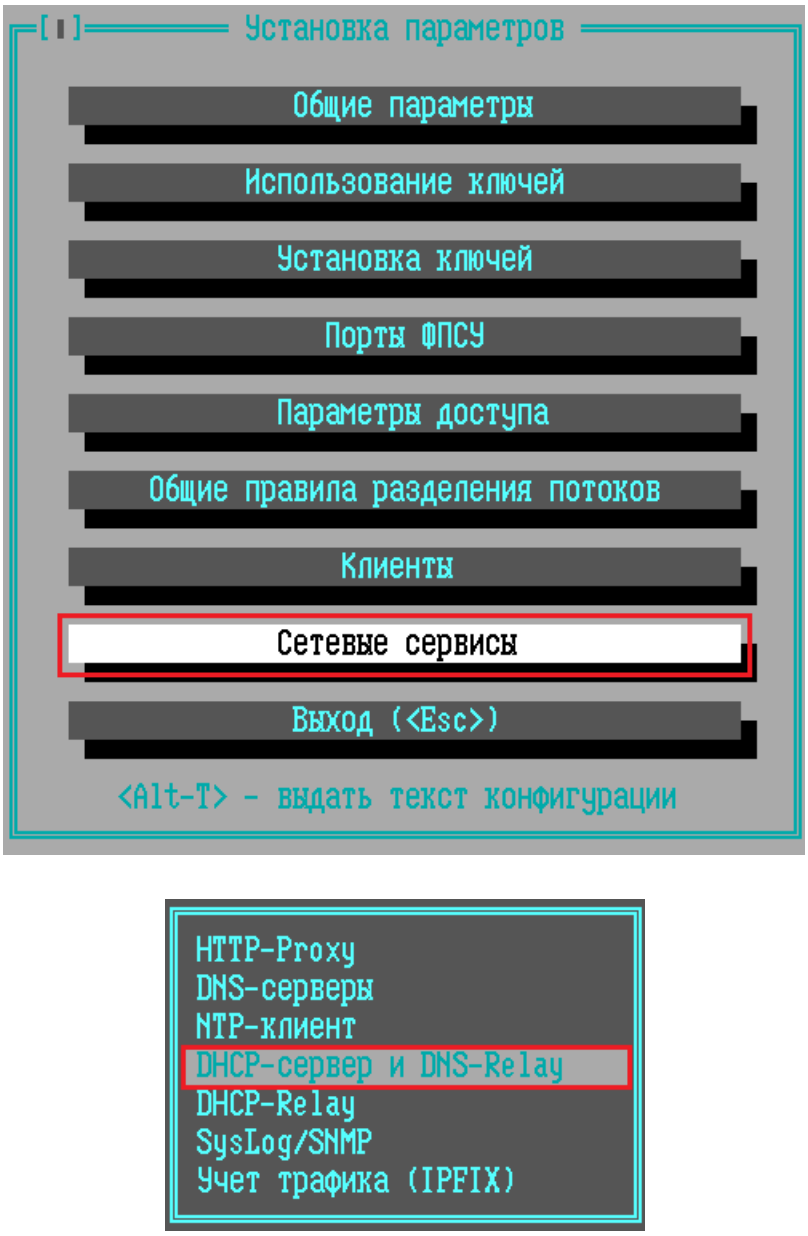


Рисунок 307 - Команда меню «Сетевые сервисы» → «DHCP-сервер и DNS-Relay»

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

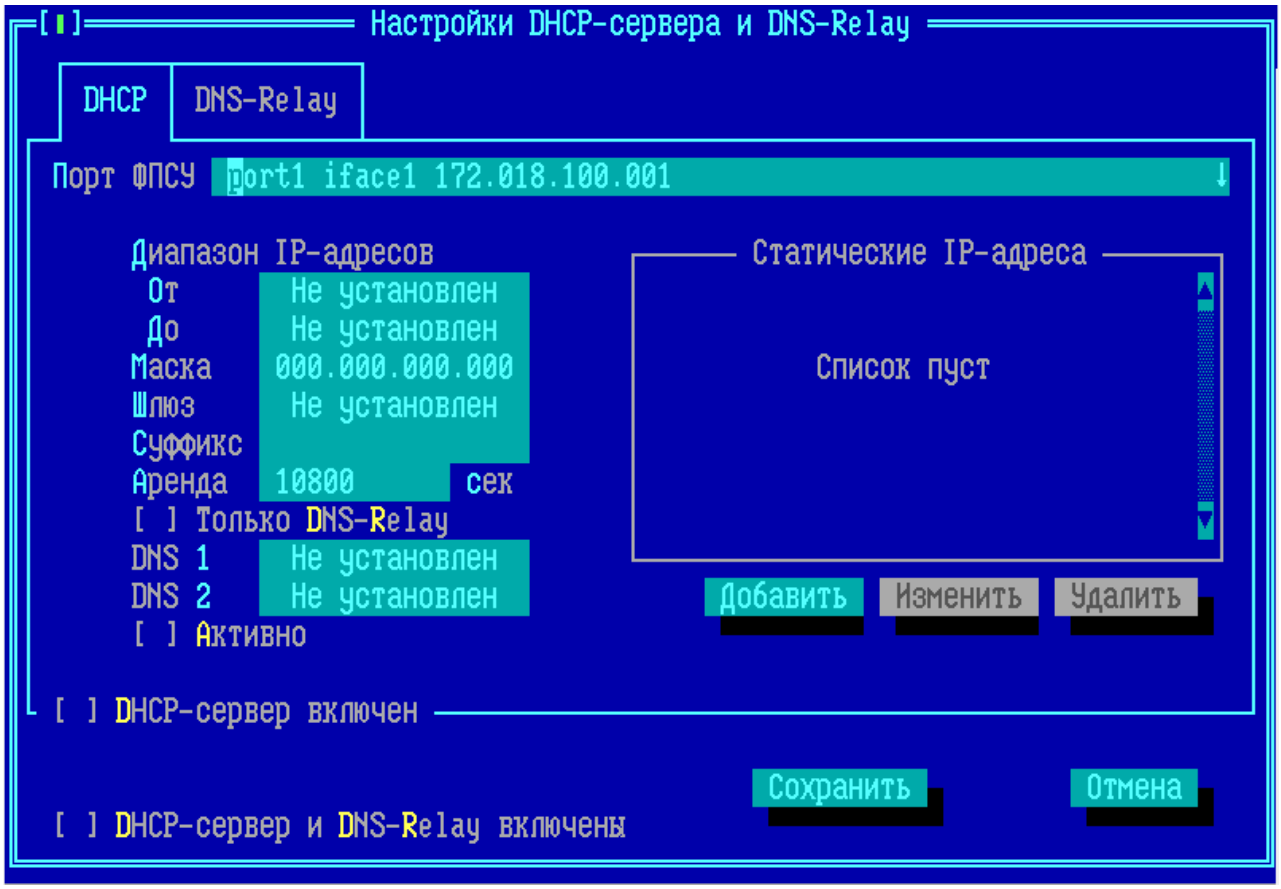


Рисунок 308 - Вкладка «DHCP»

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 309 - 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.

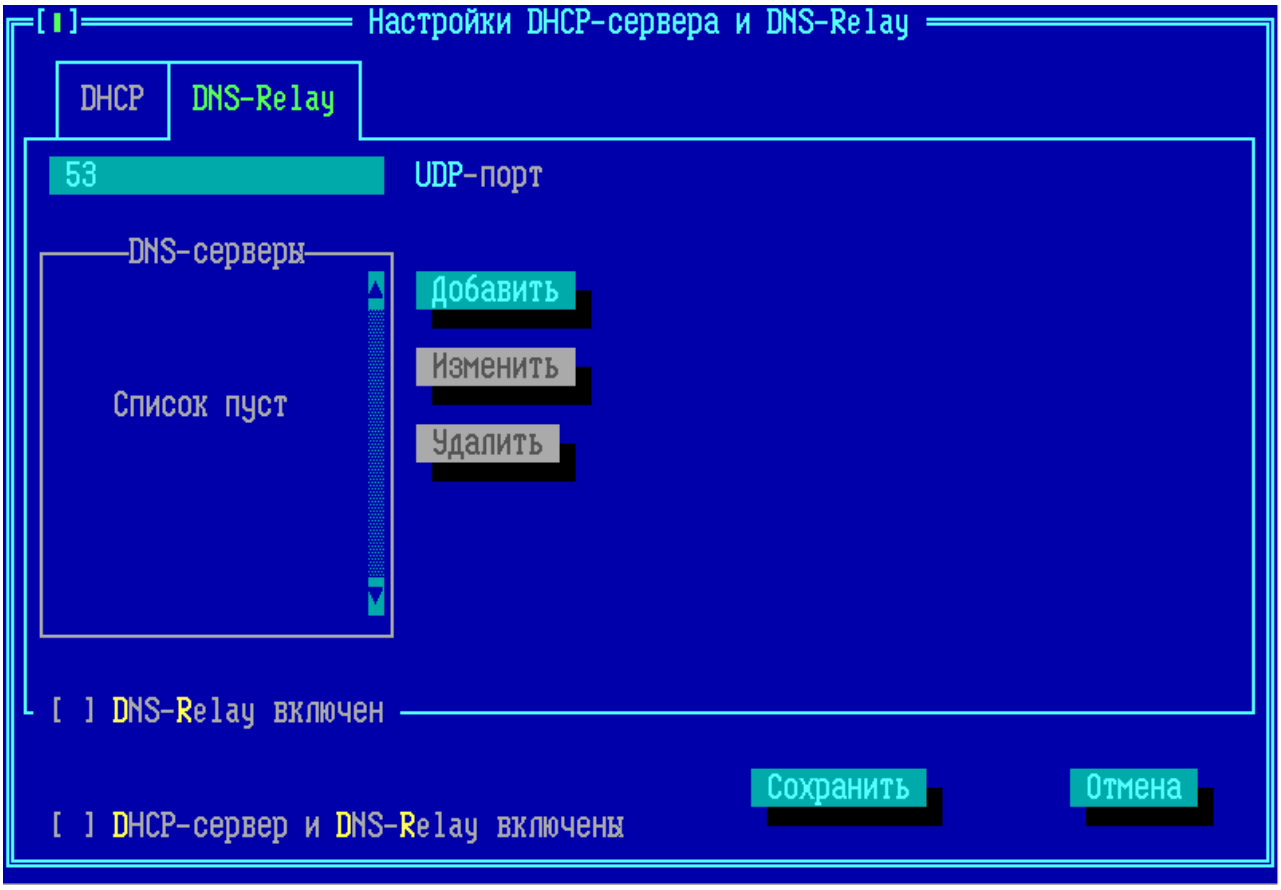


Рисунок 310 - Вкладка «DNS-Relay»

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 311 - 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.

12. 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.

12. 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»*:

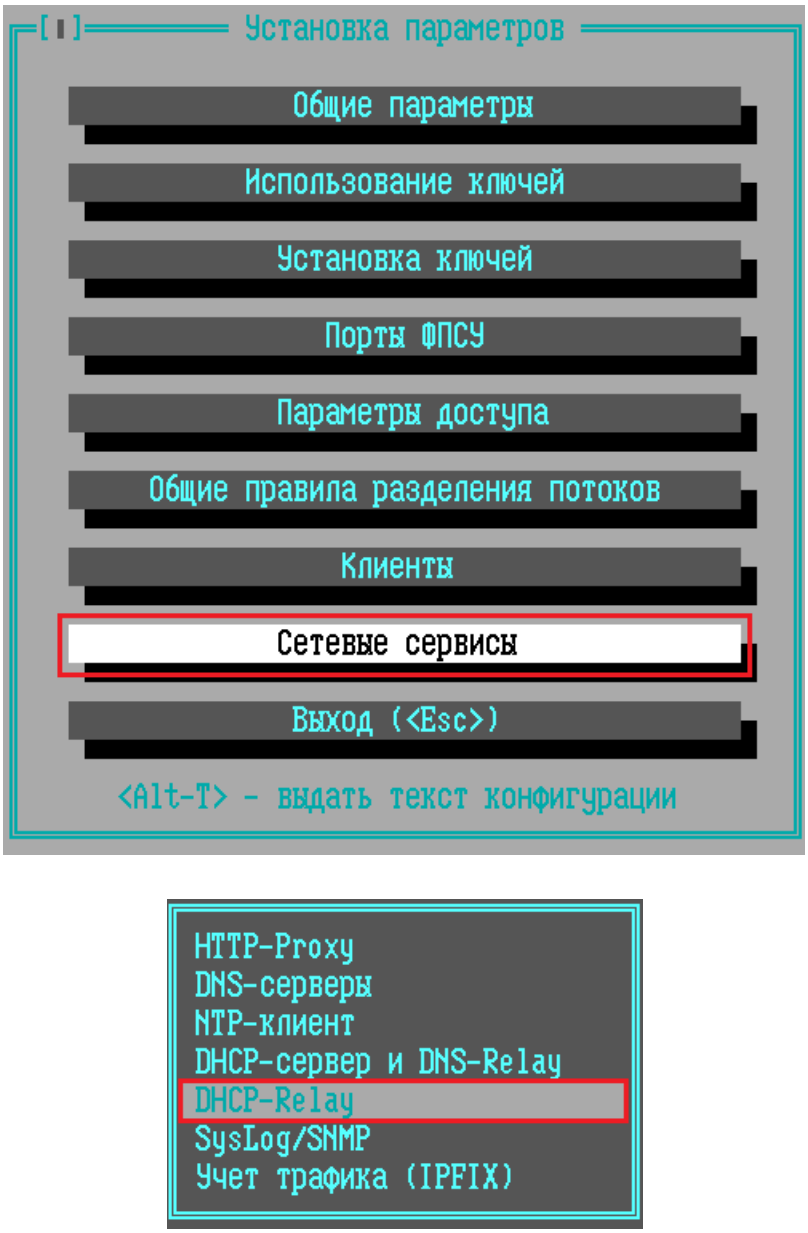


Рисунок 312 - Команда меню «Сетевые сервисы» → «DHCP-Relay»

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 313 - Список DHCP-серверов

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

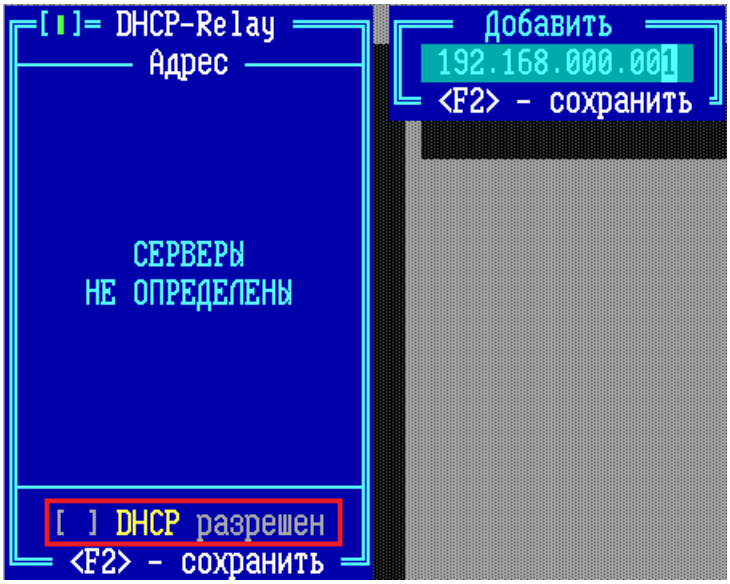


Рисунок 314 - Добавление DHCP-сервера

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.

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.

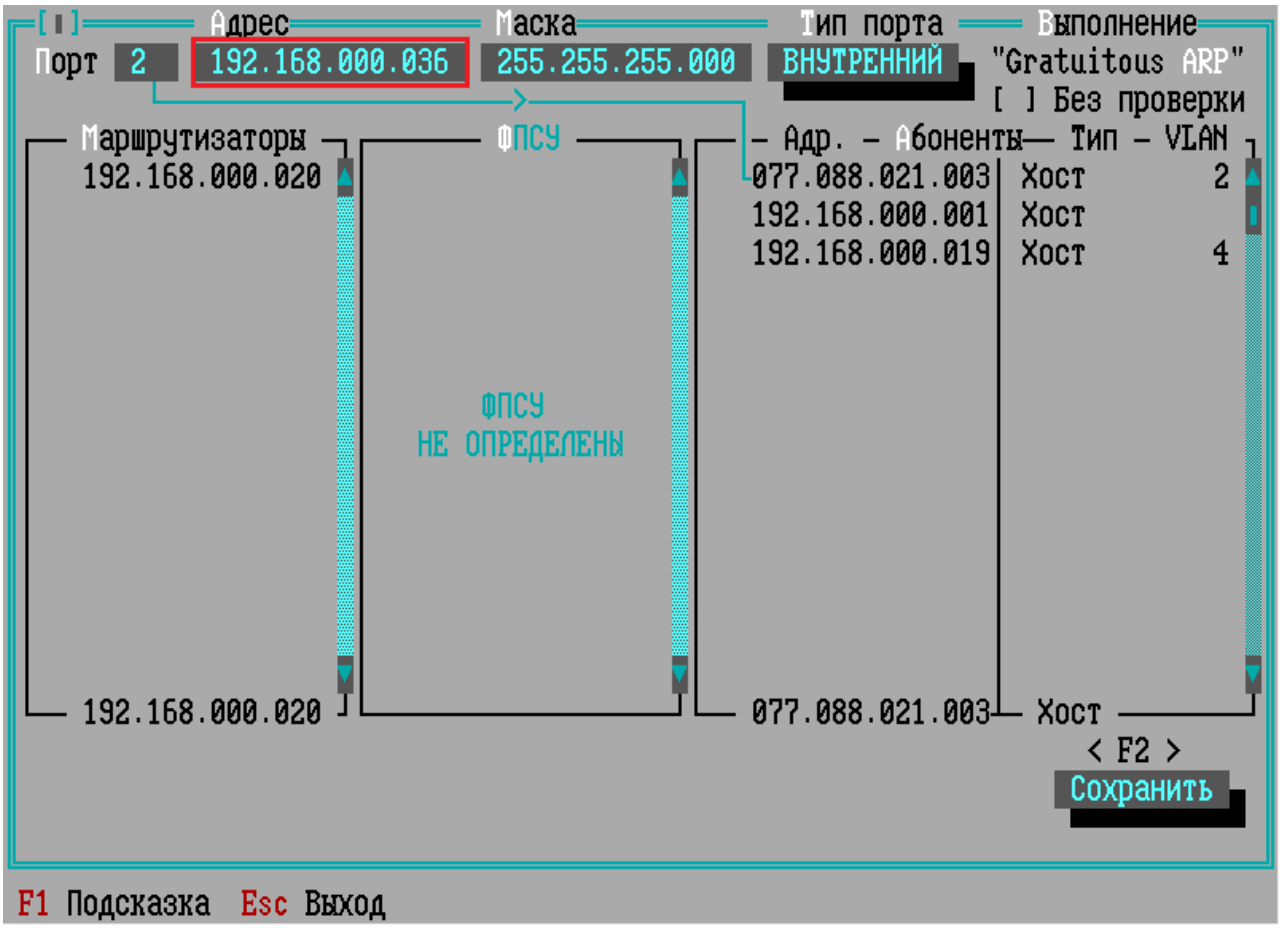


Рисунок 315 - Параметры порта ФПСУ-IP

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 316 - 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.

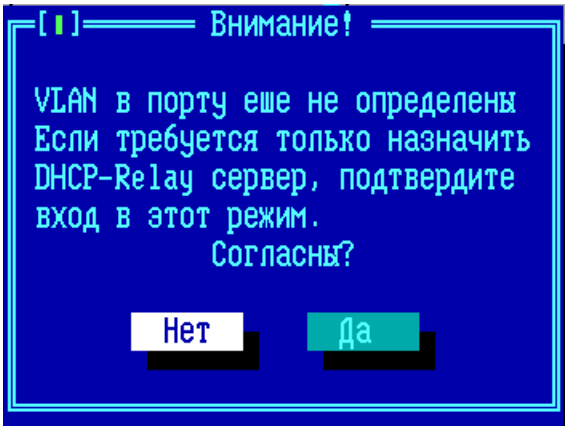


Рисунок 317 - Служебное оповещение

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.

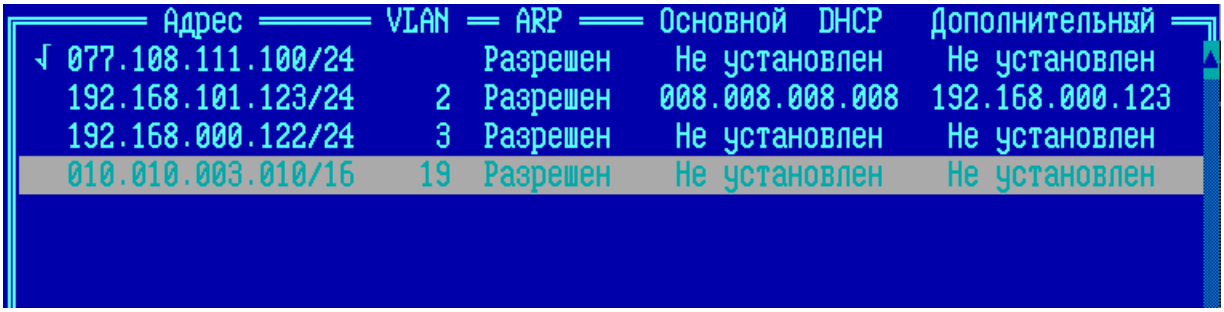


Рисунок 318 - Настройка DHCP на порту с определенными VLAN

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

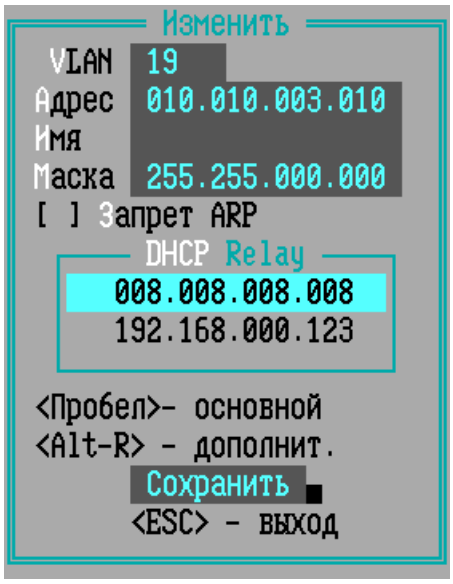


Рисунок 319 - Настройка DHCP-сервера для отдельного VLAN порта

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.

12. 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:

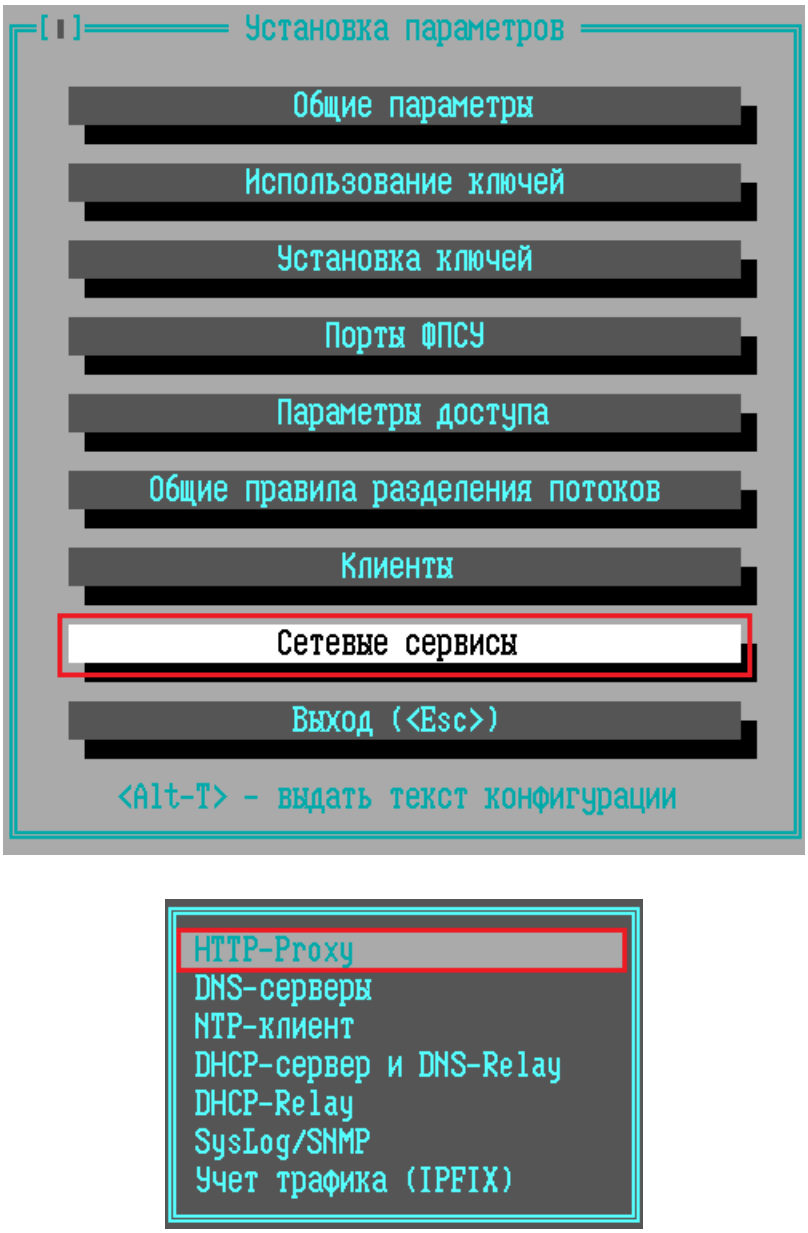


Рисунок 320 - Команда перехода в конфигурацию proxy на ФПСУ-IP

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:

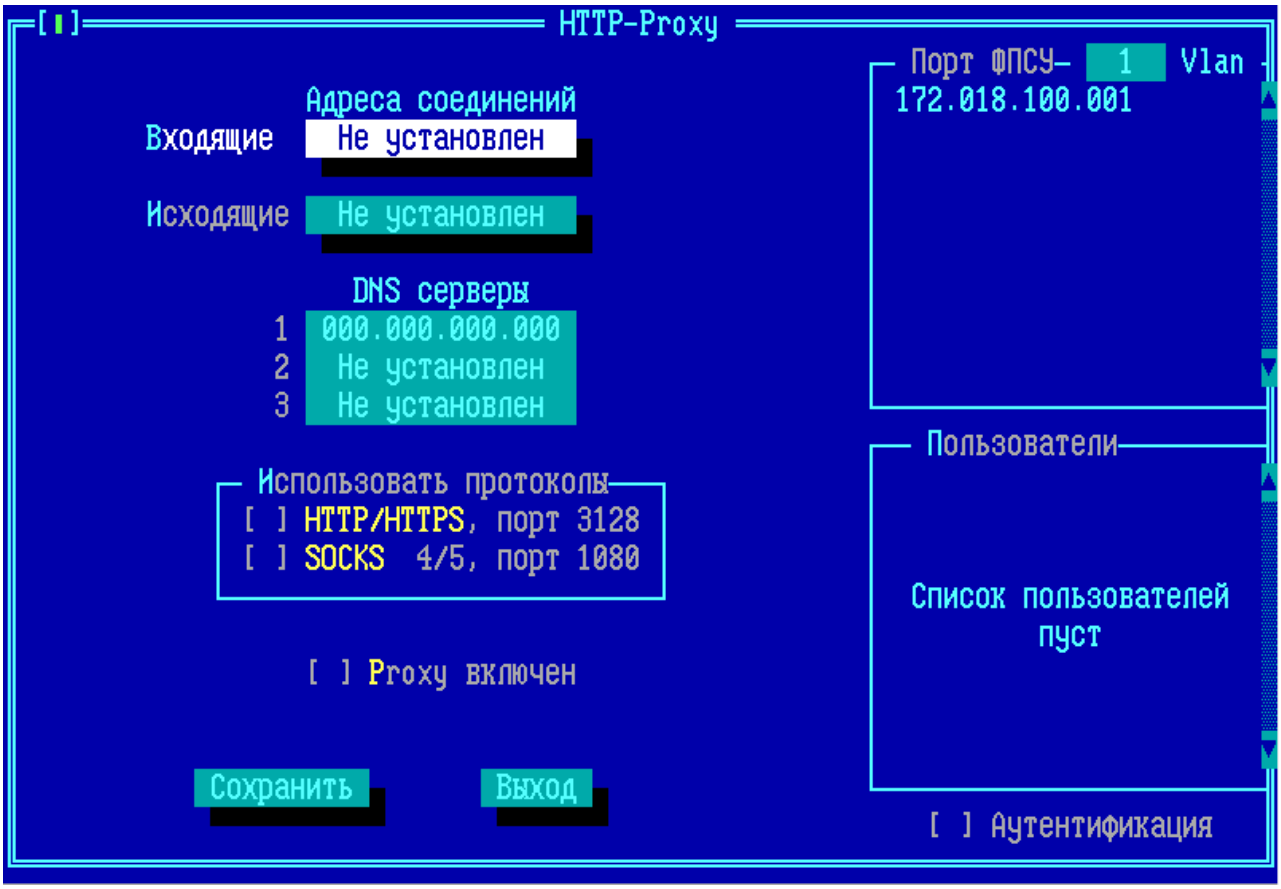


Рисунок 321 - Окно настроек HTTP-proxy

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.

12. 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:

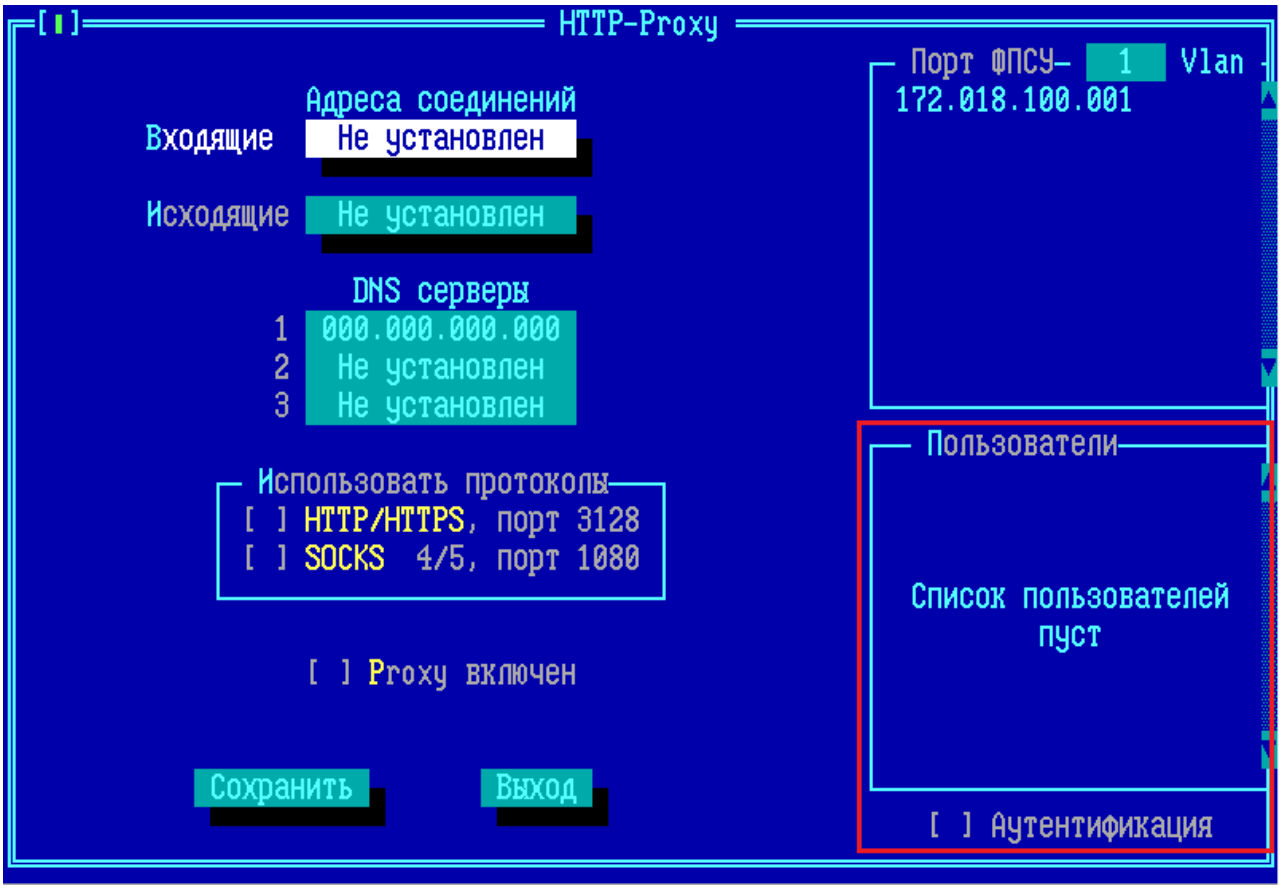


Рисунок 322 - Блок настройки пользователей proxy ФПСУ-IP

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:

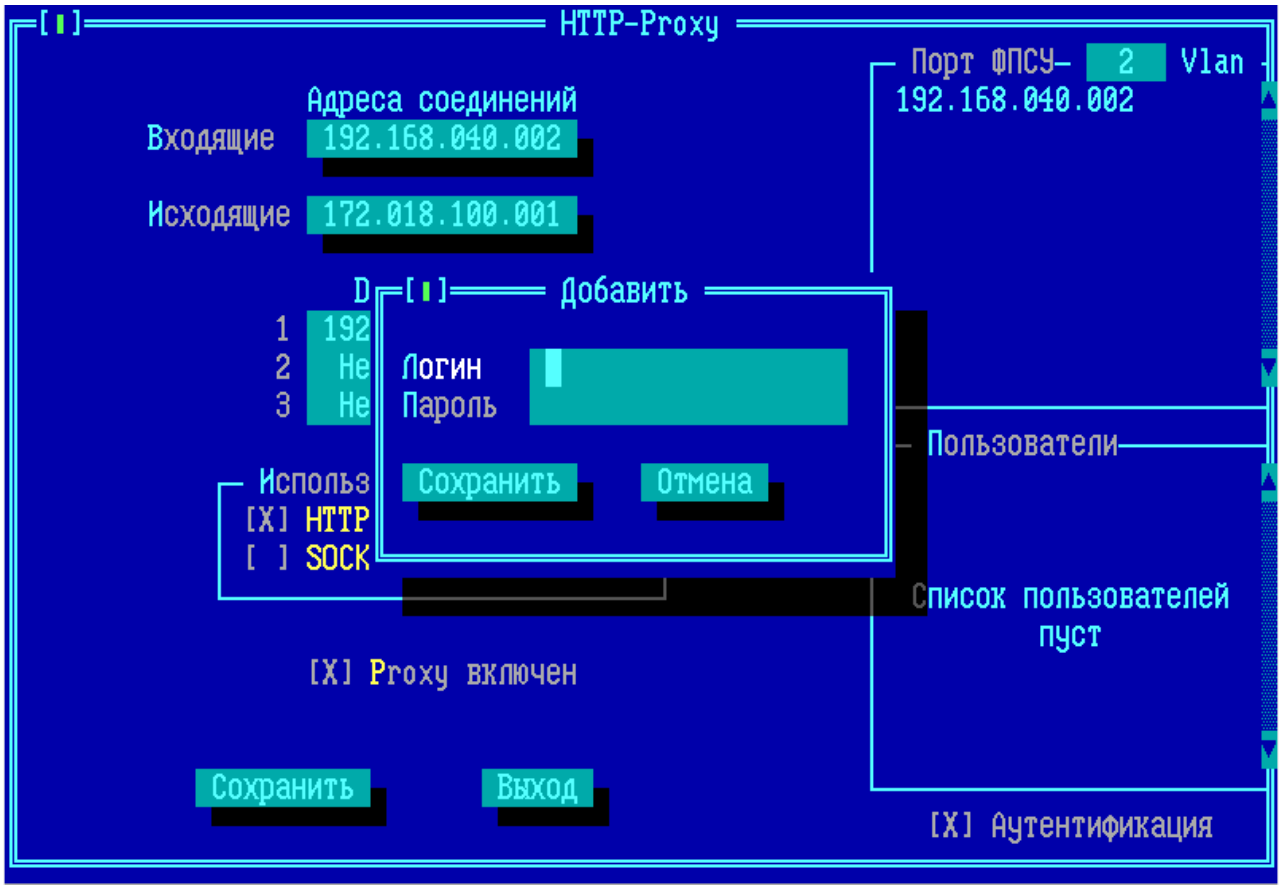


Рисунок 323 - Добавление учетной записи нового пользователя proxy ФПСУ-IP

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:

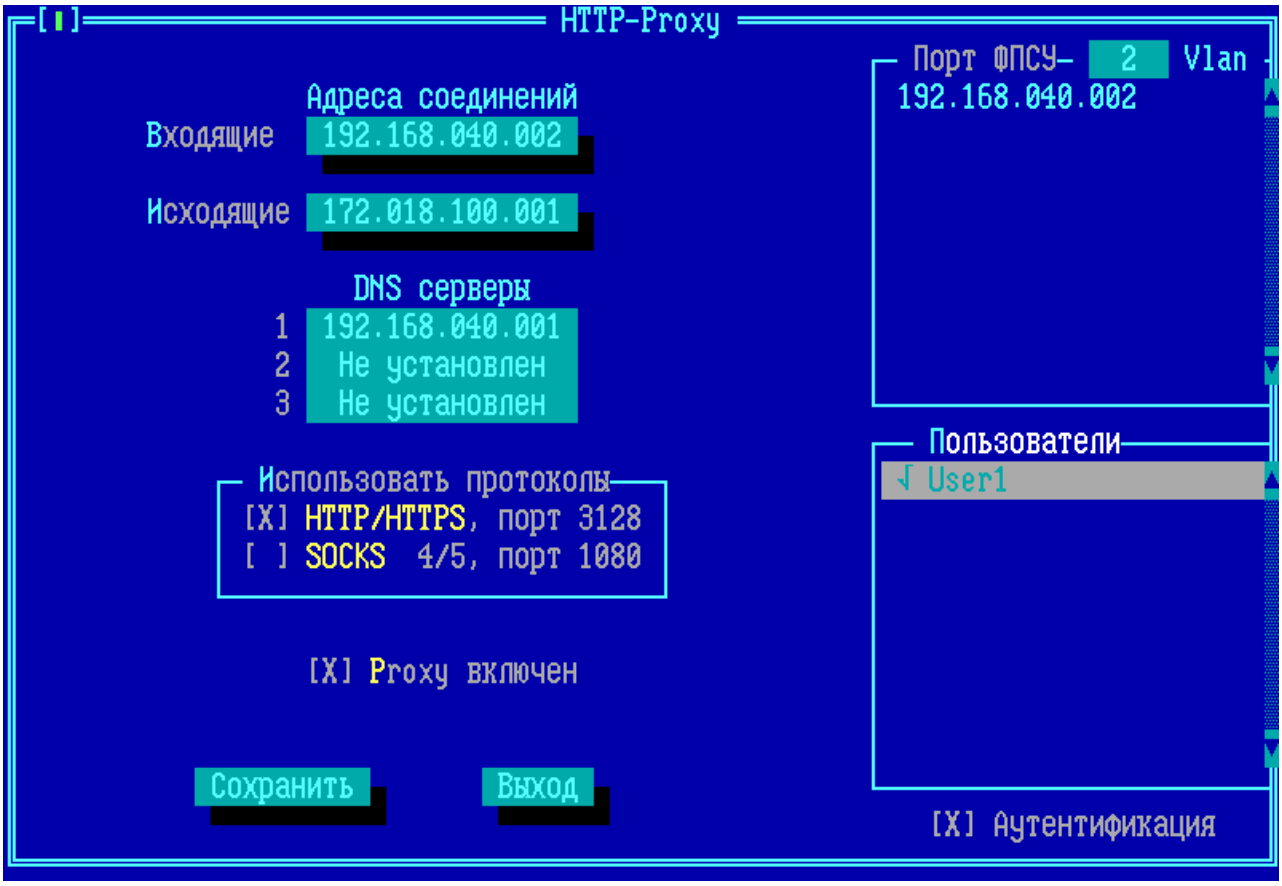


Рисунок 324 - Новый пользователь proxy ФПСУ-IP добавлен

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, 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.

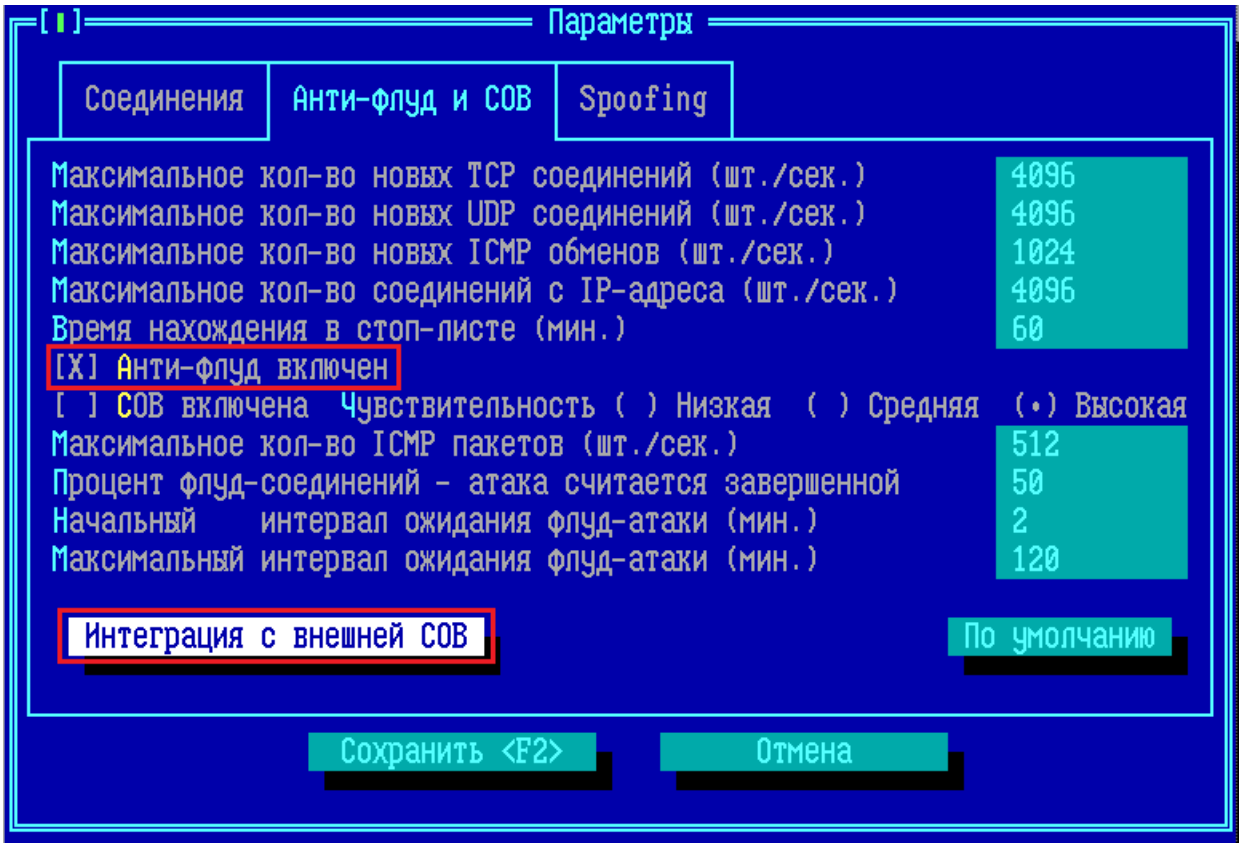


Рисунок 325 - Вызов интерфейса настройки взаимодействия с СОВ

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

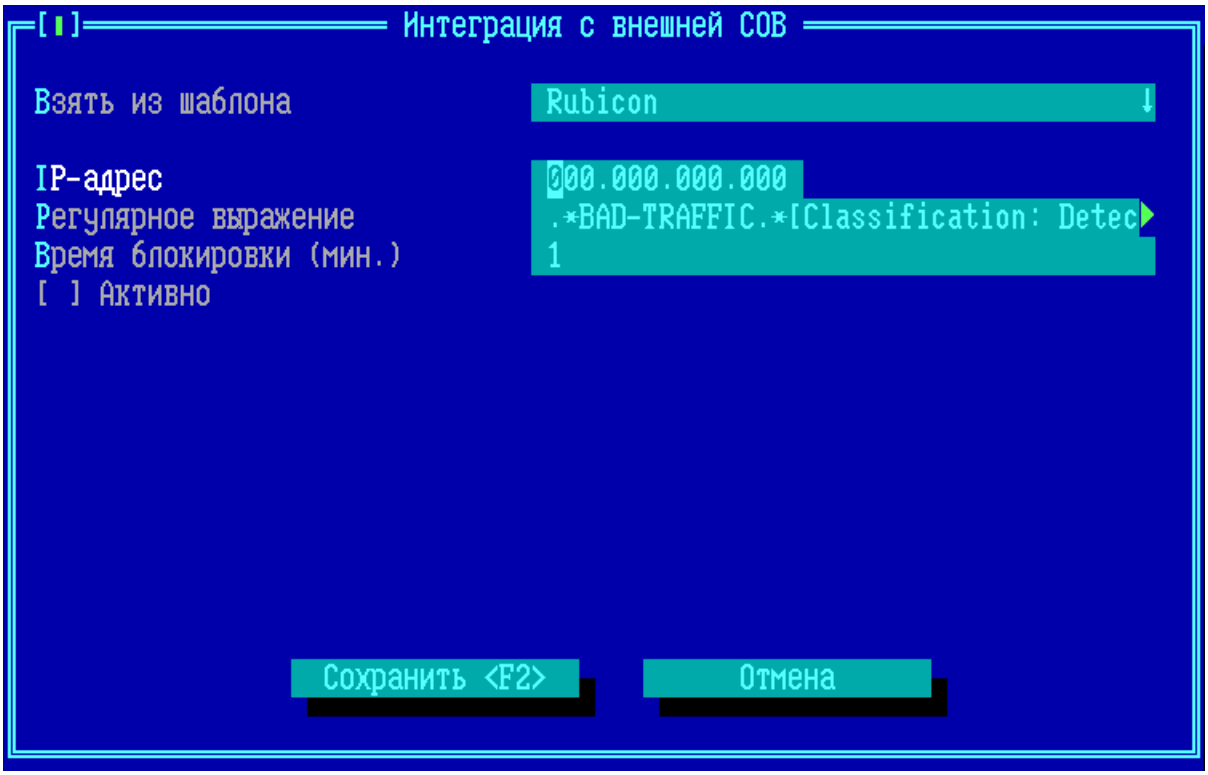


Рисунок 326 - Параметры взаимодействия с СОВ

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).

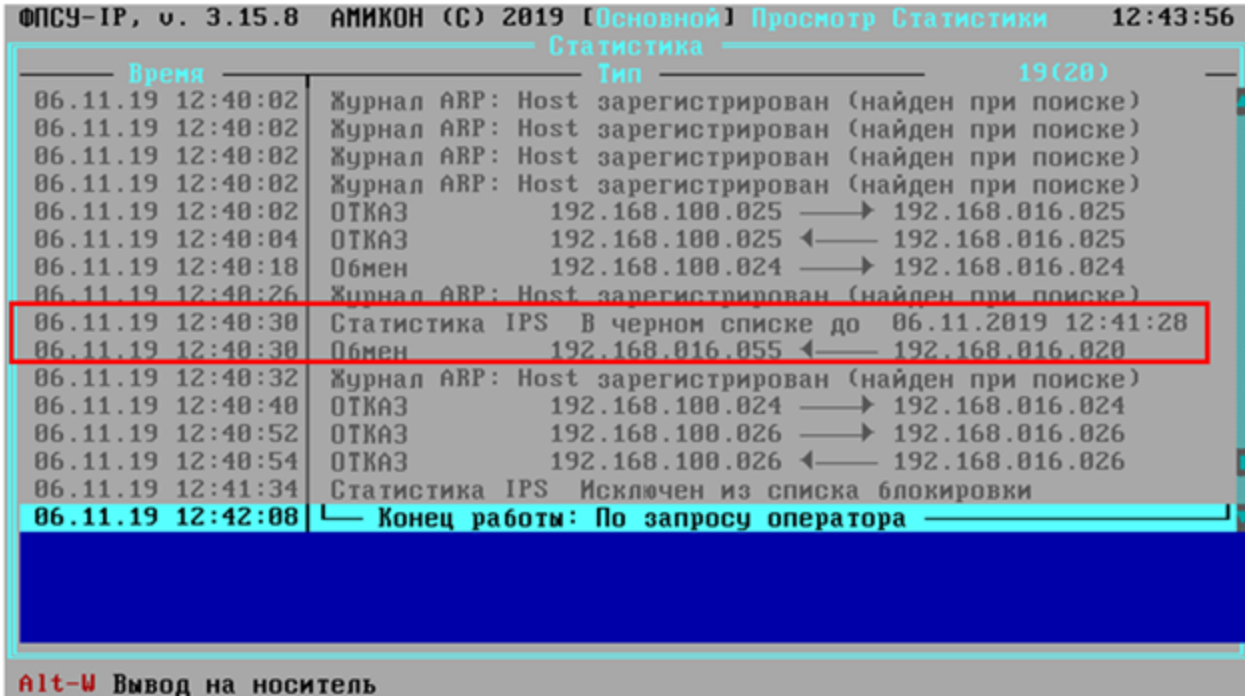


Рисунок 327 - Получено управляющее сообщение от СОВ

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%».

12. 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»)!

ВНИМАНИЕ! Синхронизация времени через УА будет отключена при работающей синхронизации через NTP.

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

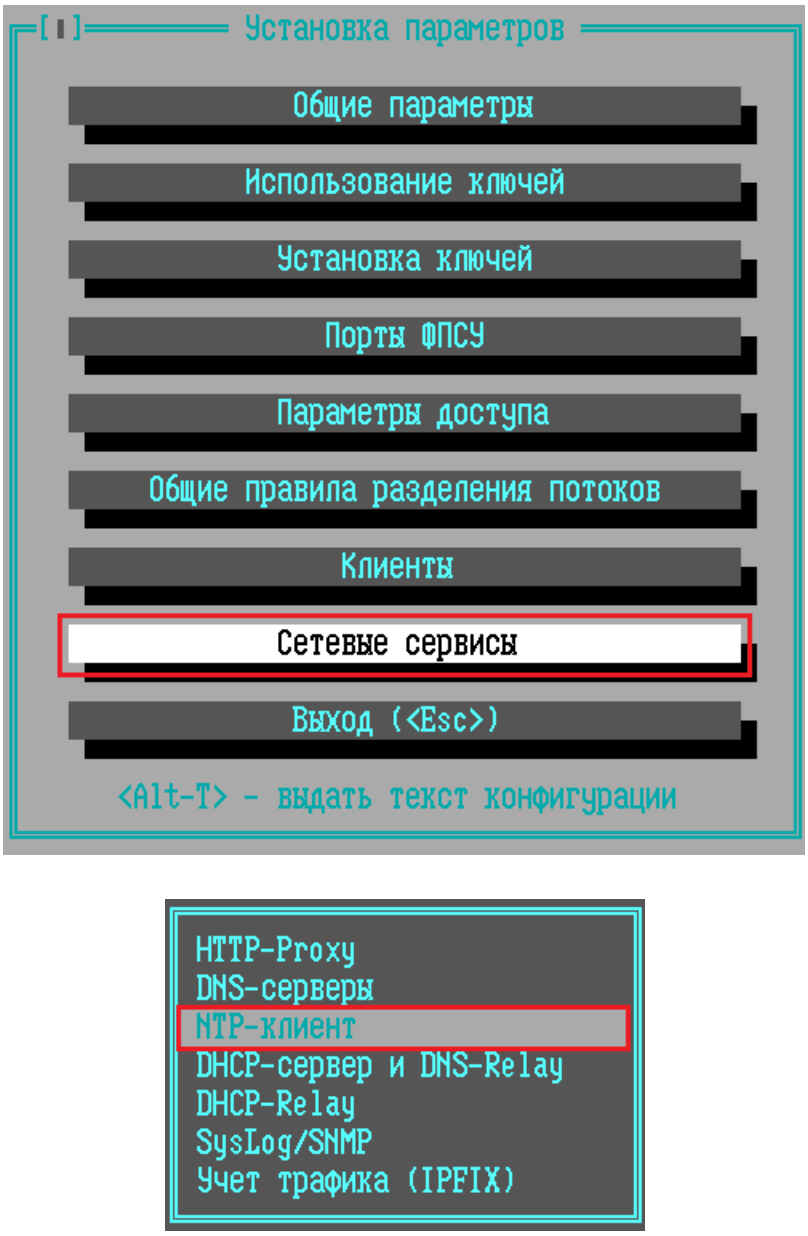


Рисунок 328 - Команда меню «Сетевые сервисы» → «NTP-клиент»

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

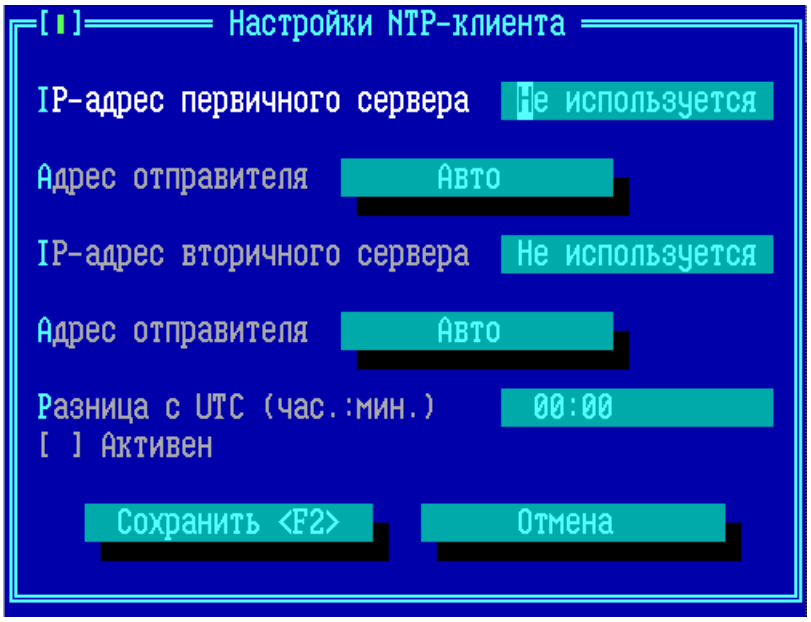


Рисунок 329 - Настройки NTP-клиента по умолчанию

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*».

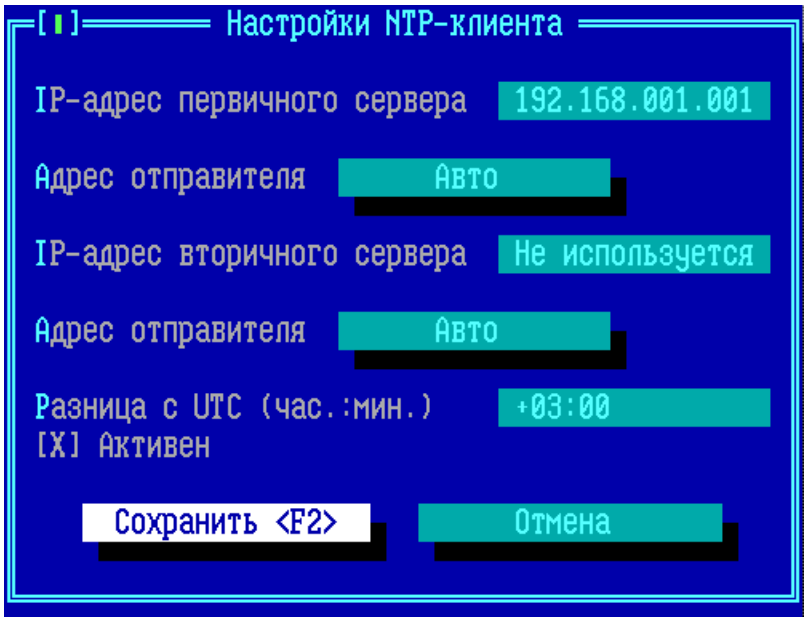


Рисунок 330 - Пример настроек NTP-клиента

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.

12. 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 12. 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»).

12. 12. Поддержка Wake-on-Lan

На ФПСУ-IP начиная с версии программного обеспечения 3.30.2 поддерживается технология удаленного включения Wake-on-LAN, позволяющая удаленно управлять включением рабочих станций.

Отправление команд Wake-on-LAN осуществляется только удаленным администратором, возможности отправить такой

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».

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

Таблица 13. 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

Описание	Номер протокола или порта
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
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

13. 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.

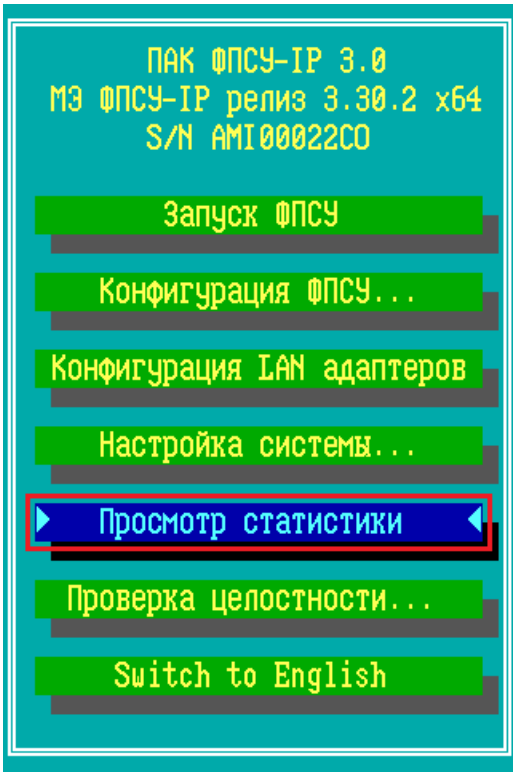


Рисунок 331 - Главное меню ФПСУ-IP

13. 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:

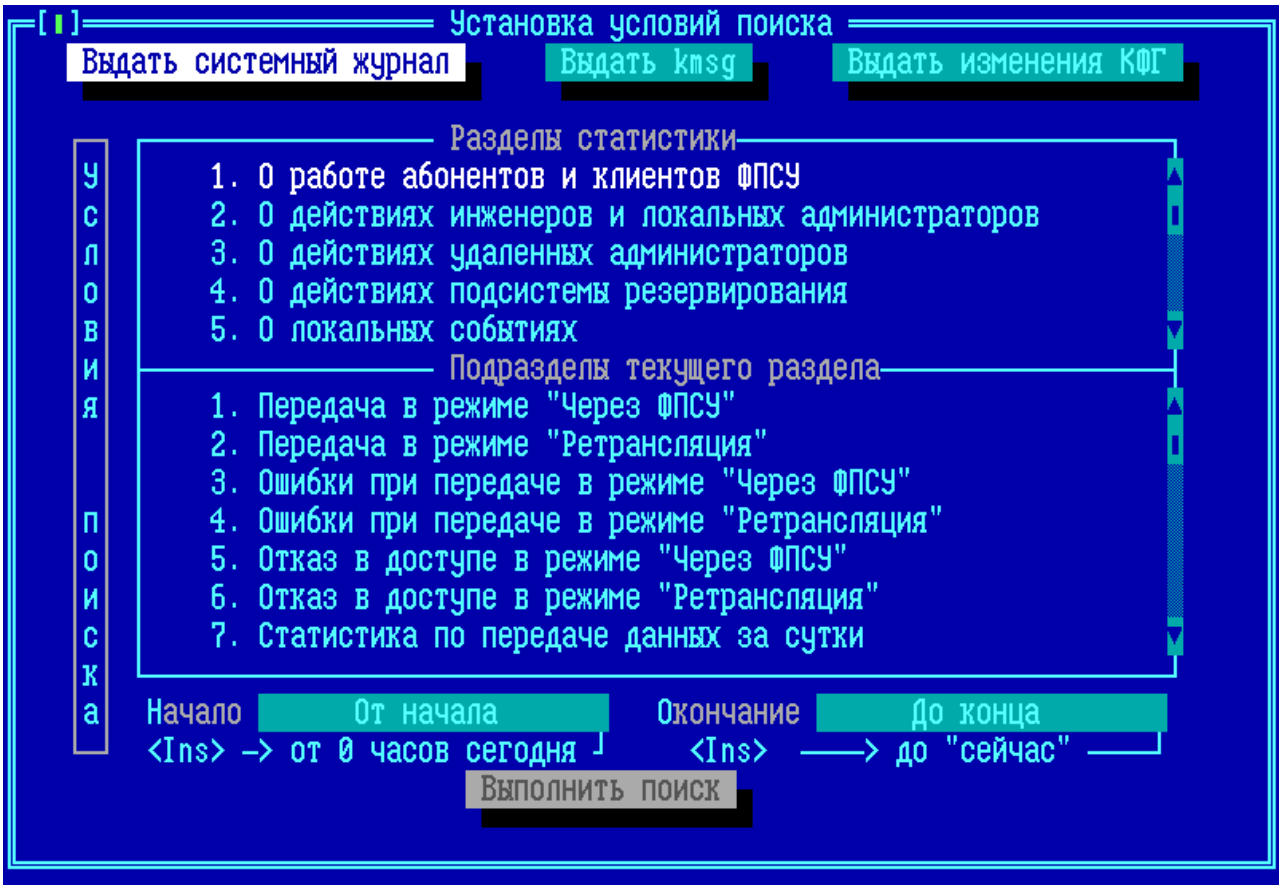


Рисунок 332 - Окно создания запроса на получение статистики

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:

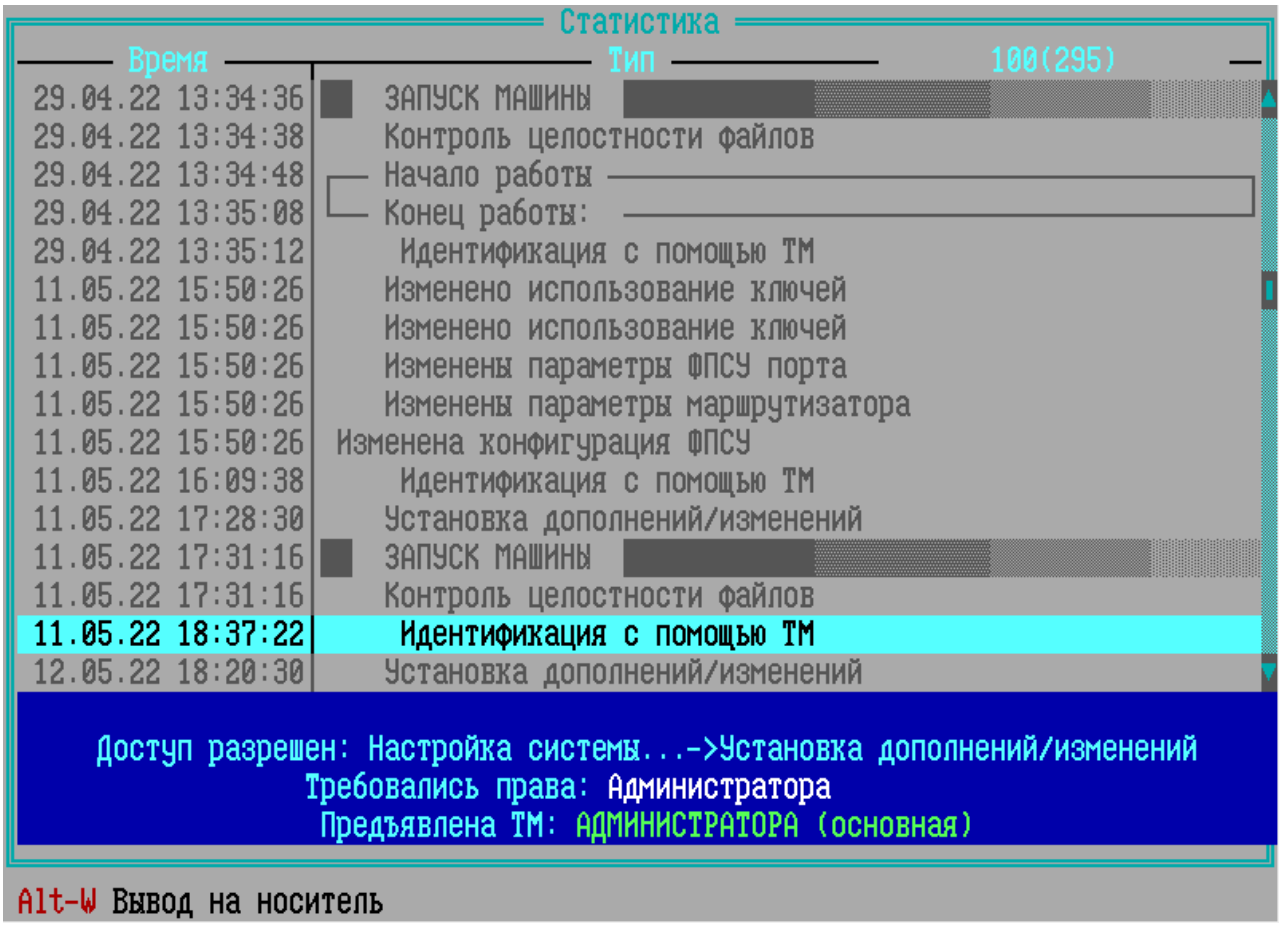


Рисунок 333 - Результат запроса статистики

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.

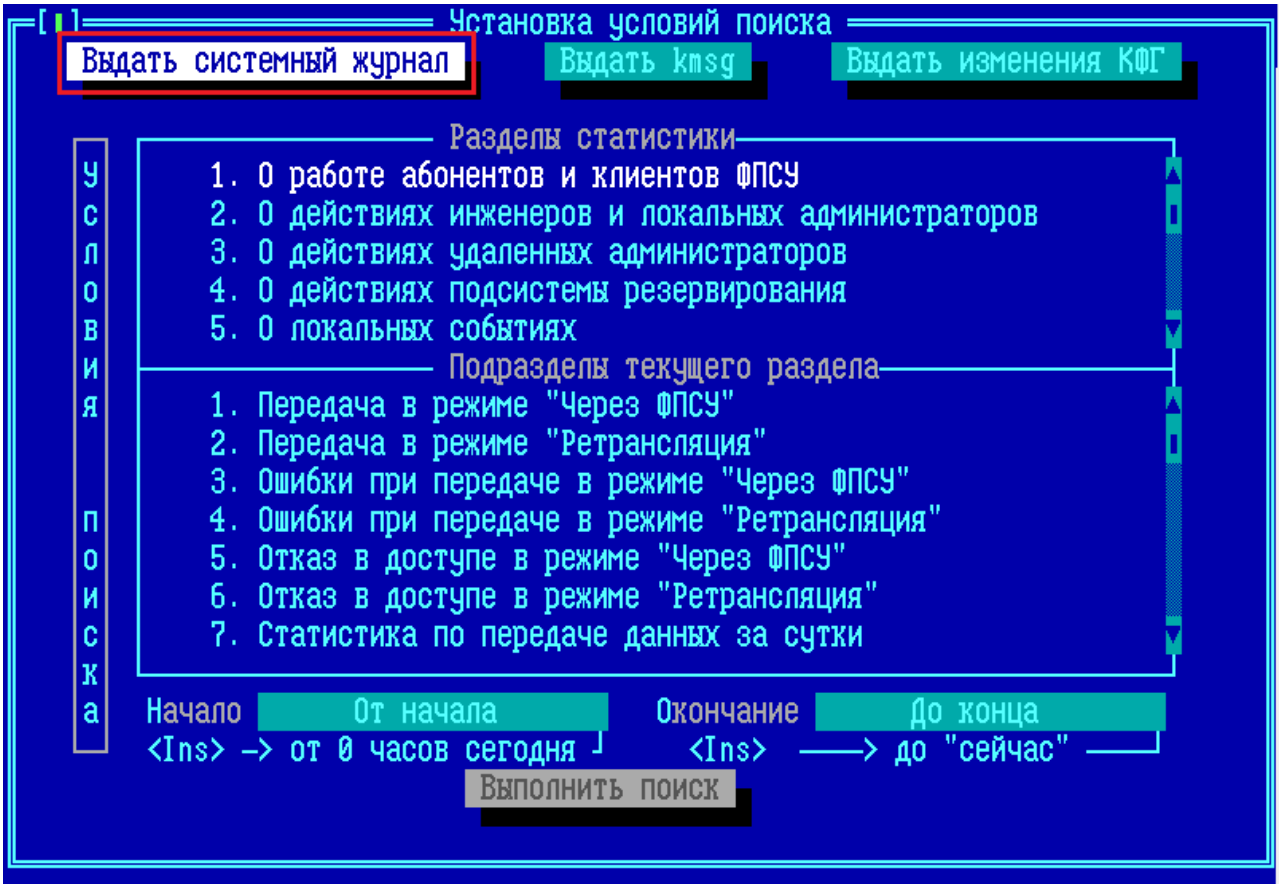


Рисунок 334 - Команда выдачи журнала изменений конфигурации межсетевого экрана

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

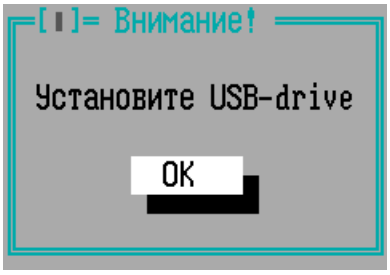


Рисунок 335 - Предложение подключить USB-носитель

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.

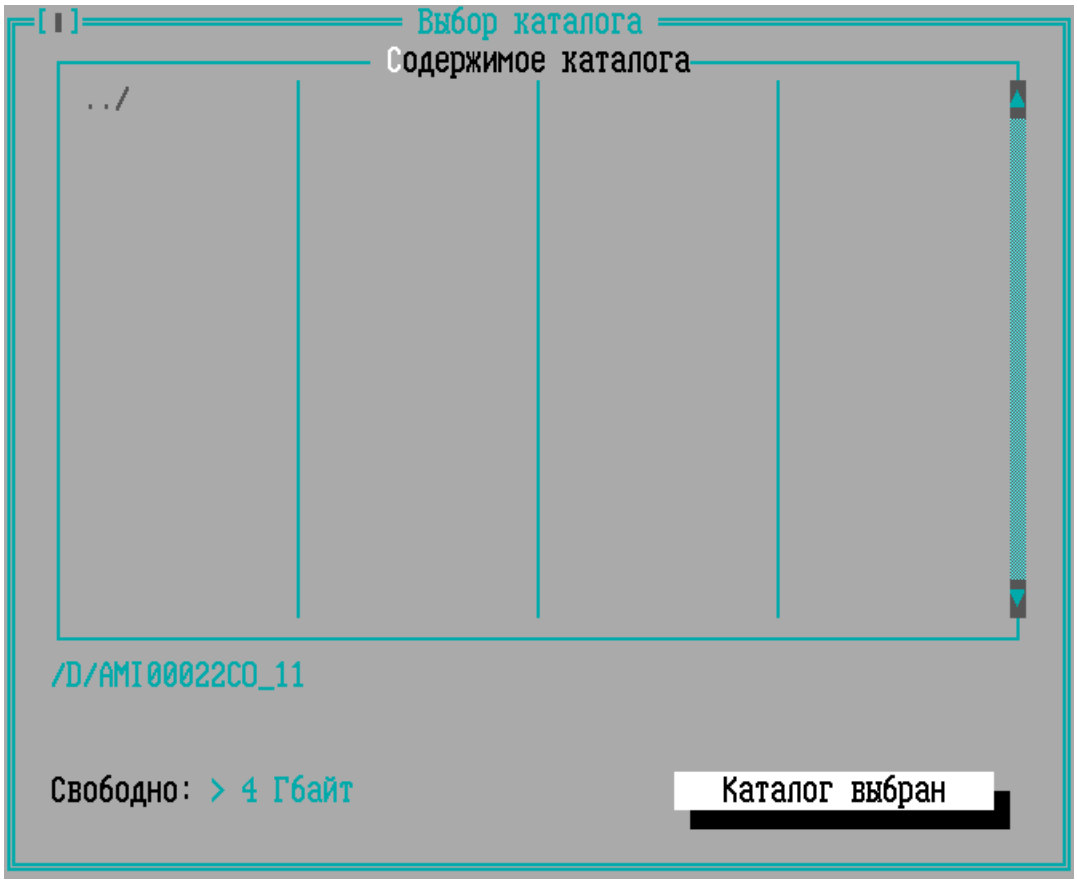


Рисунок 336 - Выбор каталога для выгрузки файла

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

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

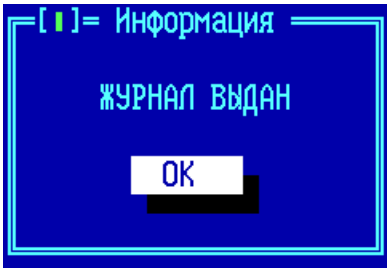


Рисунок 337 - Сообщение о завершении процедуры

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.

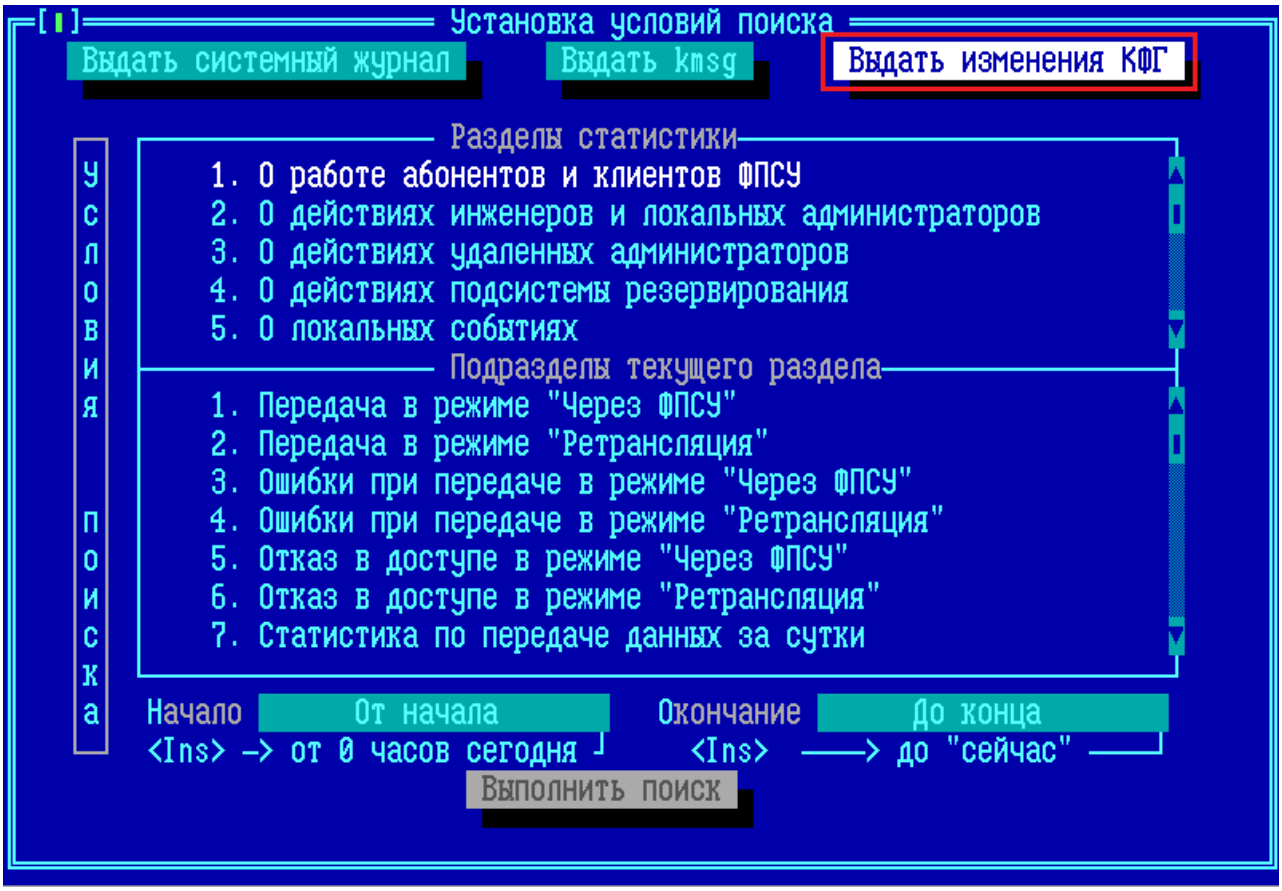


Рисунок 338 - Команда выдачи журнала изменений конфигурации межсетевого экрана

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

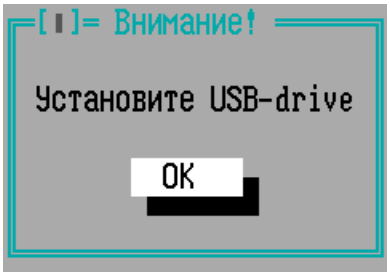


Рисунок 339 - Предложение подключить внешний носитель

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.

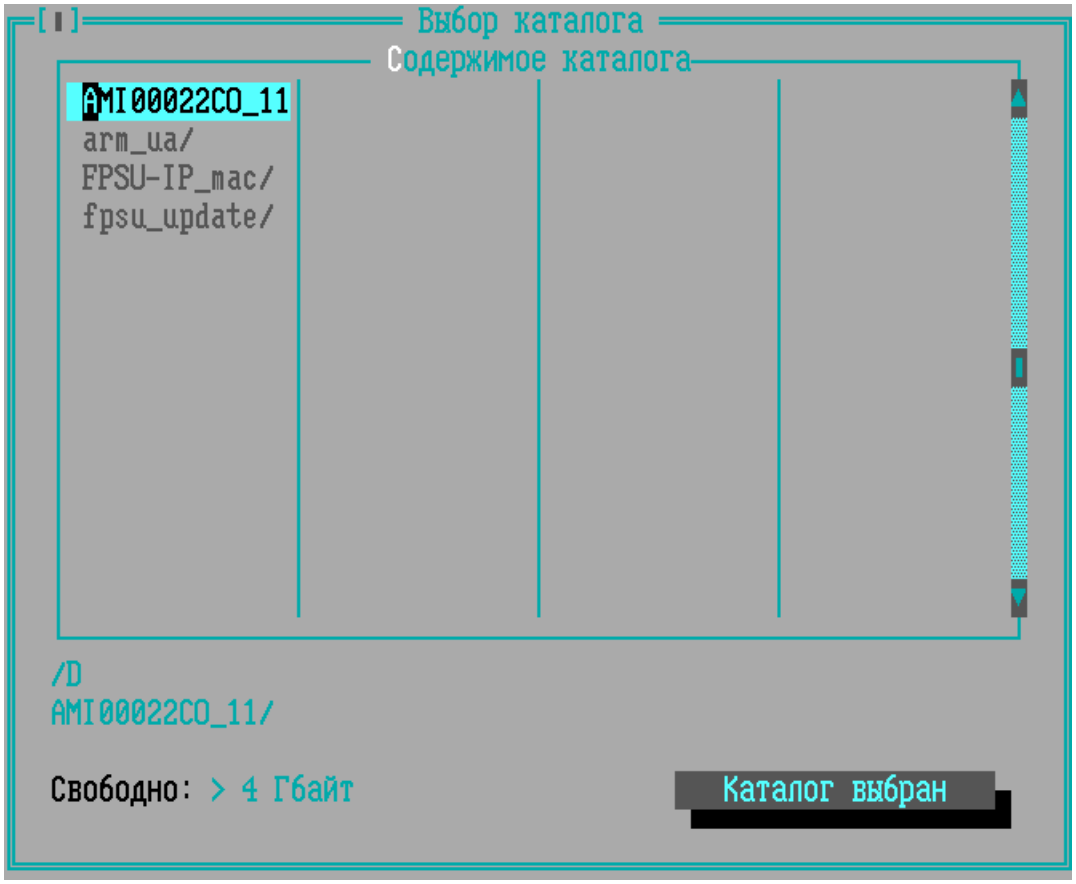


Рисунок 340 - Выбор каталога для выгрузки журнала

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

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

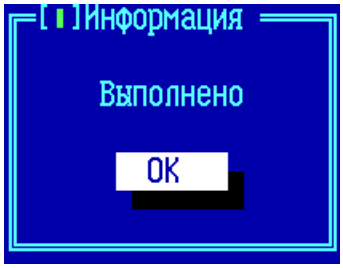


Рисунок 341 - Сообщение о завершении процедуры

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

13. 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.

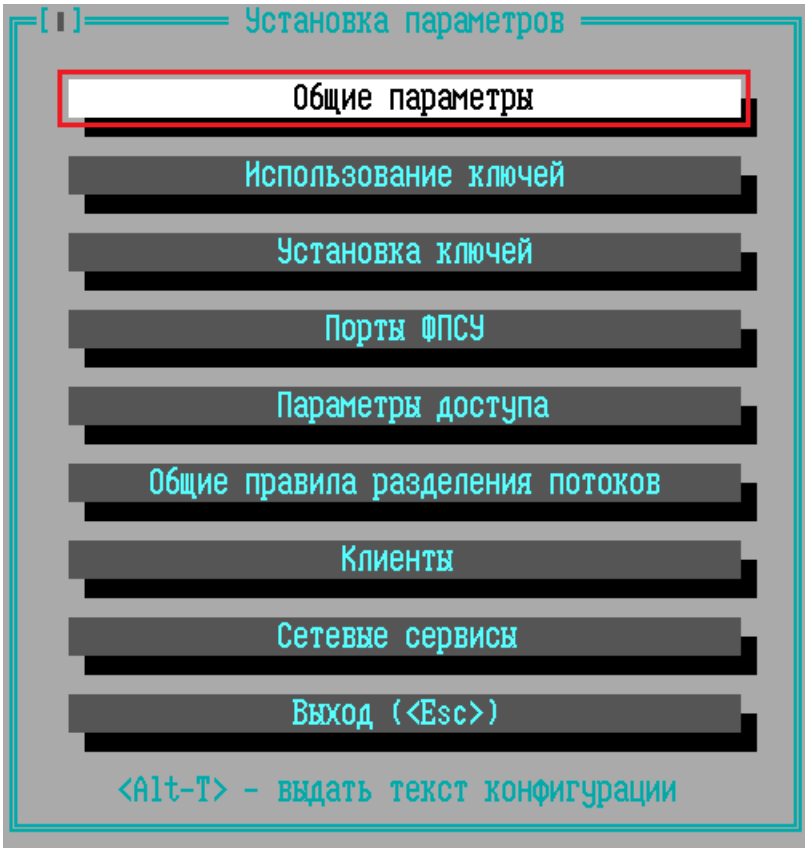


Рисунок 342 - Вход в общие настройки из основного меню конфигурации ФПСУ-IP

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

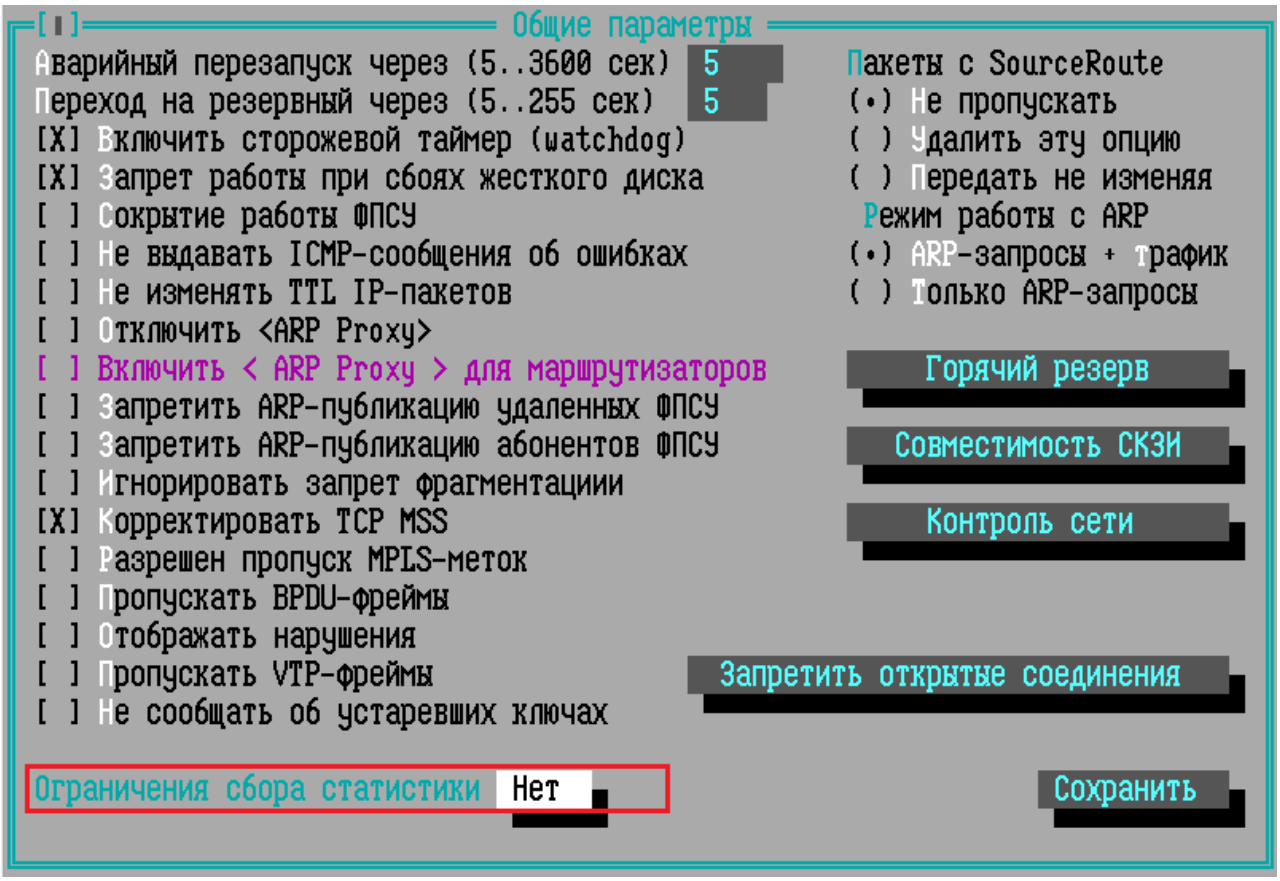


Рисунок 343 - Окно общих параметров ФПСУ-IP

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

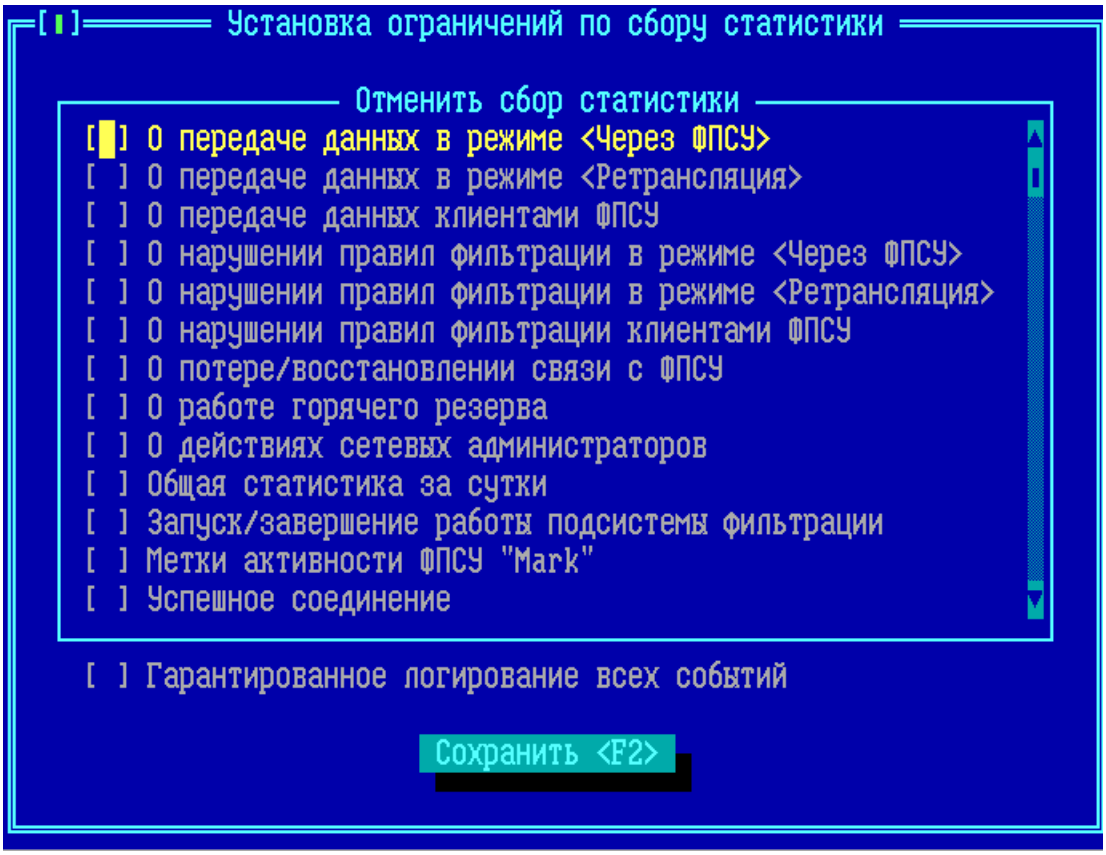


Рисунок 344 - Окно ограничения сбора статистики

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. Гарантированное логирование всех событий по умолчанию не задействовано.

ВНИМАНИЕ! Все отказы в статистике значительно увеличивают нагрузку на ЦПУ и

могут приводить к снижению производительности комплекса, особенно это заметно в случае включенного МЭ. В таких случаях рекомендуется выключить сбор статистики по отказам и настроить учёт отвергнутого трафика в IPFIX drop.

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

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»).

15. 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).

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.

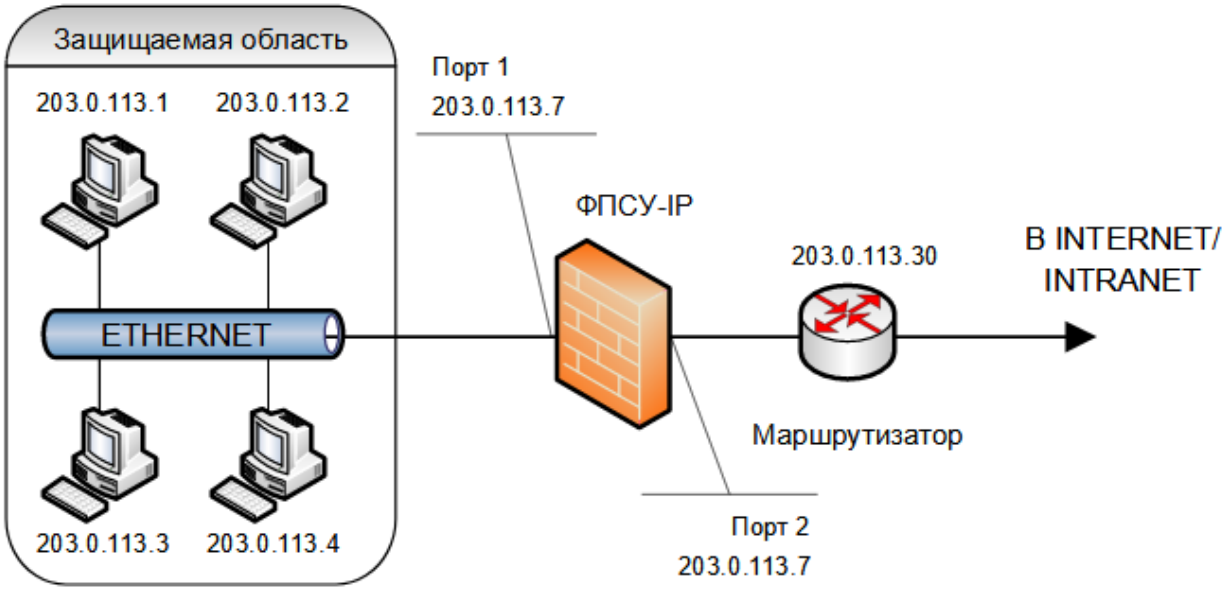


Рисунок 345 - Применение ФПСУ-IP для защиты оконечной области

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.

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.

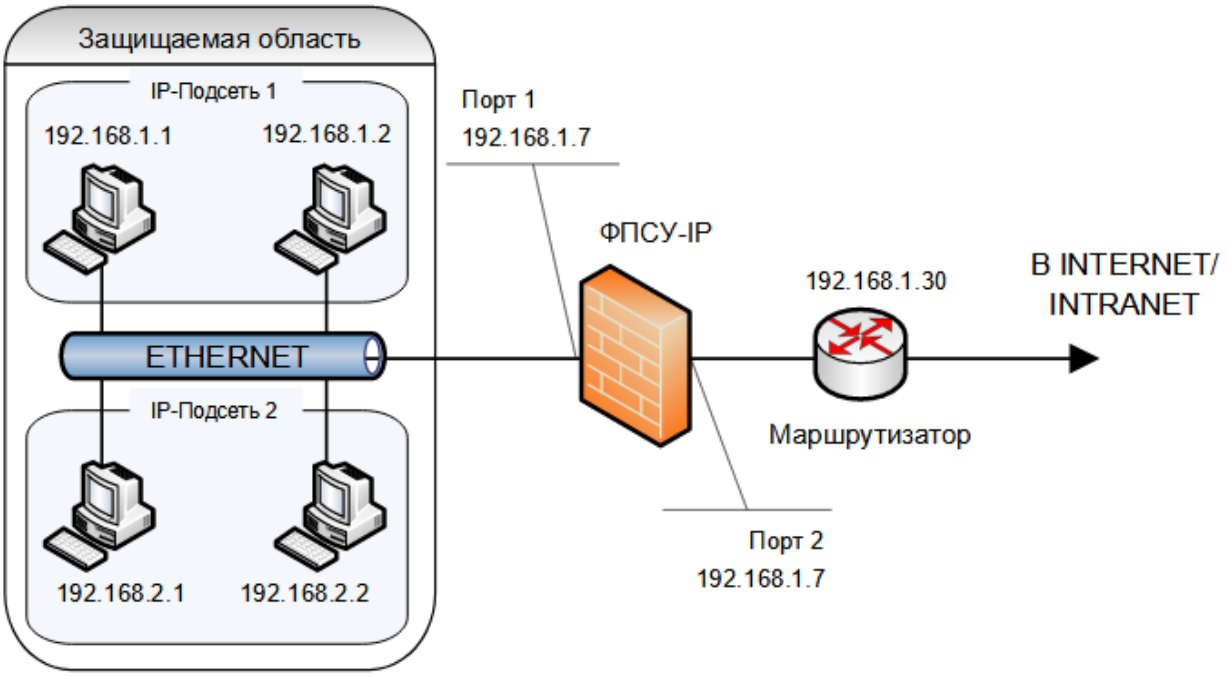


Рисунок 346 - Защита двух подсетей

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.

15. 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.

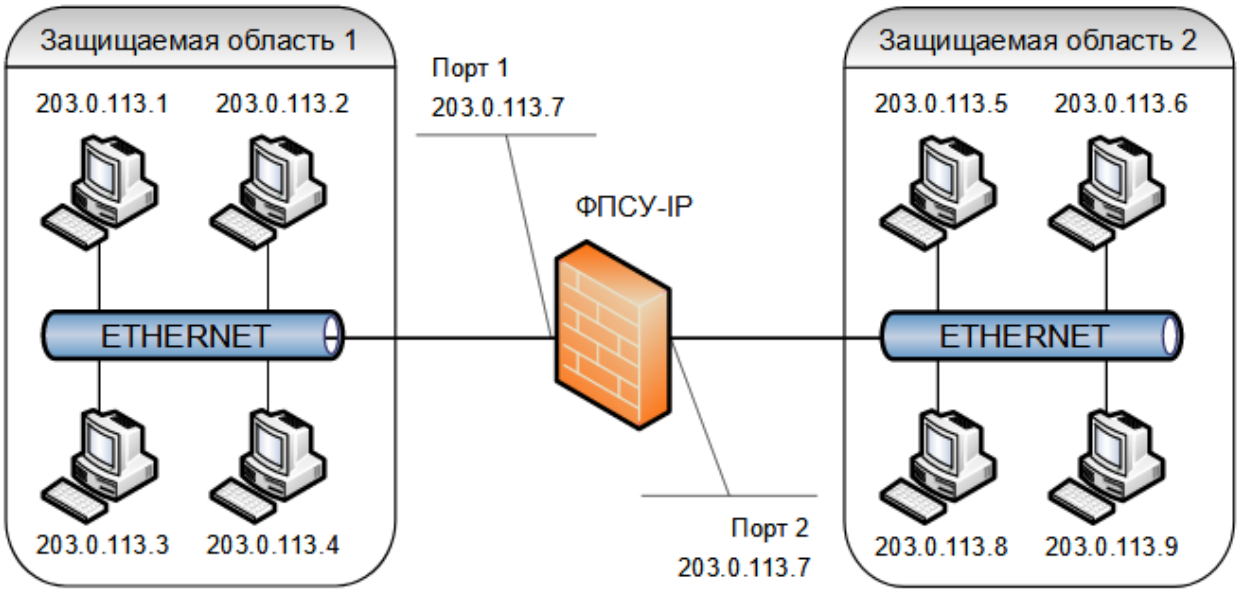


Рисунок 347 - Разбиение сети на фрагменты

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».

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.

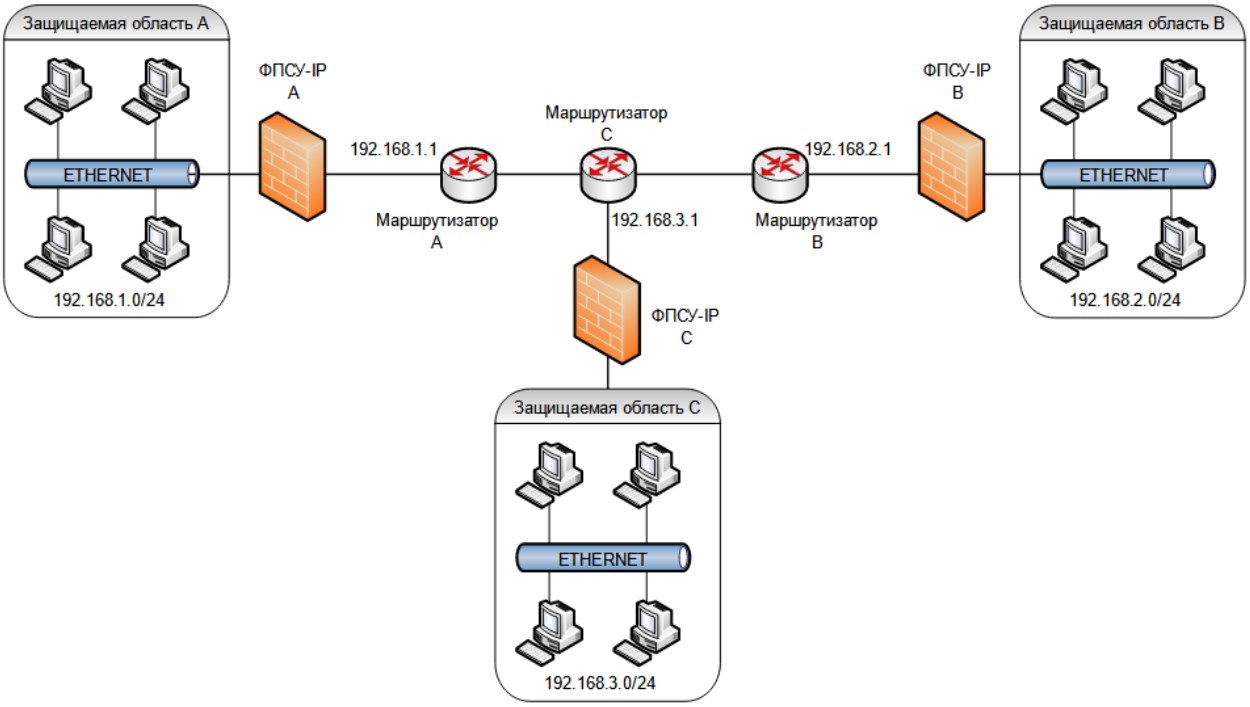


Рисунок 348 - Схема локальной сети с применением ФПСУ-IP

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.

15. 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.

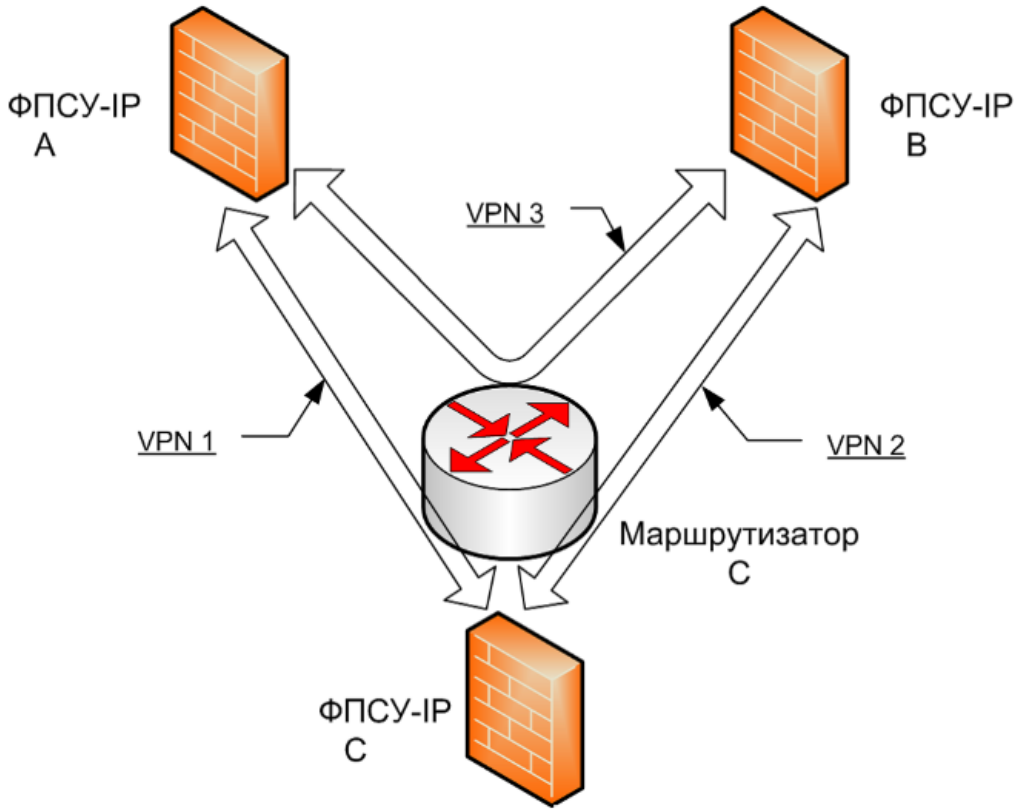


Рисунок 349 - Схема подключения с раздельными туннелями

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 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:
192.168.1.50, 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.

15. 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:

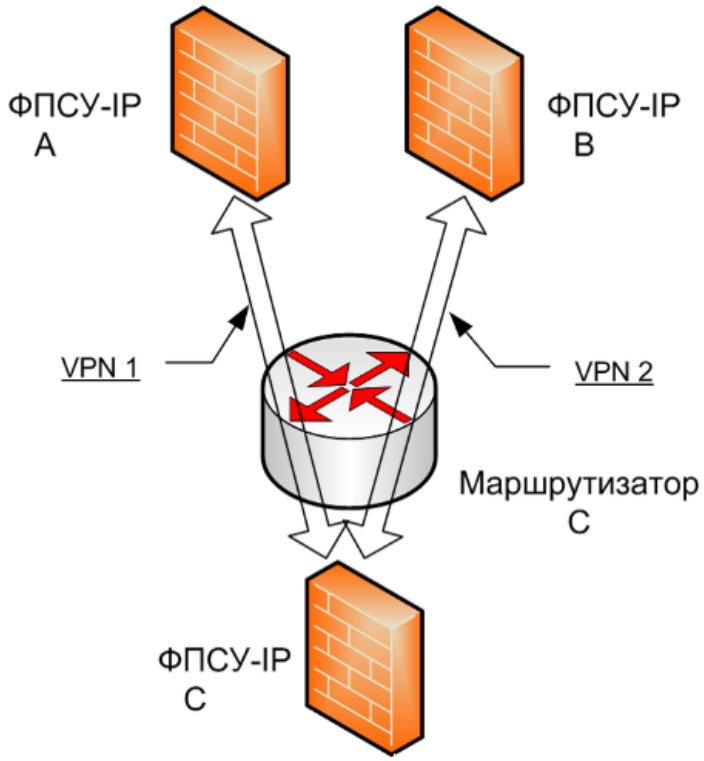


Рисунок 350 - Схема подключения с последовательными туннелями

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.

15. 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)»):

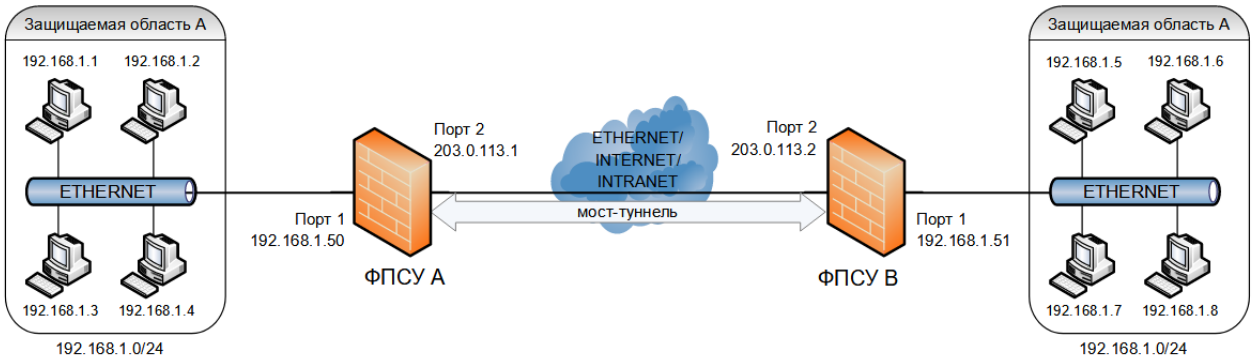


Рисунок 351 - L2-туннель типа "мост"

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 B для работы в условиях такой топологии принципиальным является следующее:

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

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 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 B:

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.

15. 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.

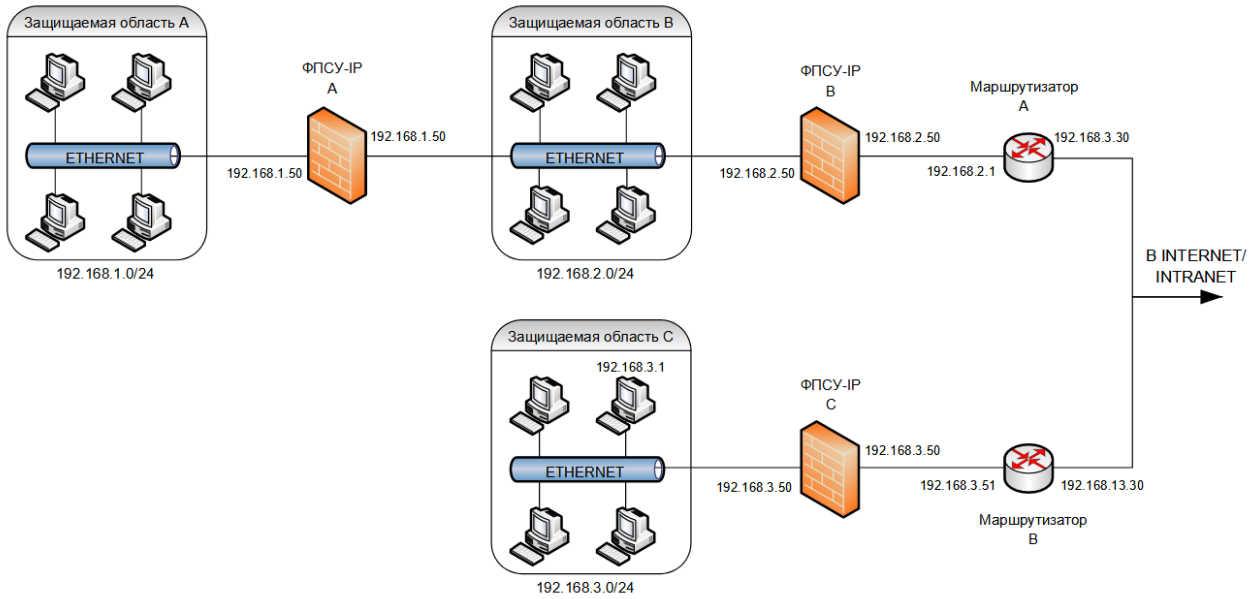


Рисунок 352 - Каскадное подключение ФПСУ-IP

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 C:

- отсутствие доступа абонентов области C к маршрутизаторам A и в область B обеспечивается тем, что маршрутизатор A не описан как абонент со стороны внешнего порта 2, область C не входит в правило трафика, разрешающее доступ в область B;
- доступ абонентов области C к мировой сети невозможен - они не указаны на порту 2; кроме того, у абонентов C указан режим работы с абонентами противоположного порта только через ФПСУ-IP;
- доступ от абонентов области C к маршрутизатору B невозможен, поскольку, во-первых, управление маршрутизатором не разрешено, во-вторых, он не описан как абонент, в-третьих, у абонентов C указан режим работы с абонентами противоположного порта только через ФПСУ-IP.

15. 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.

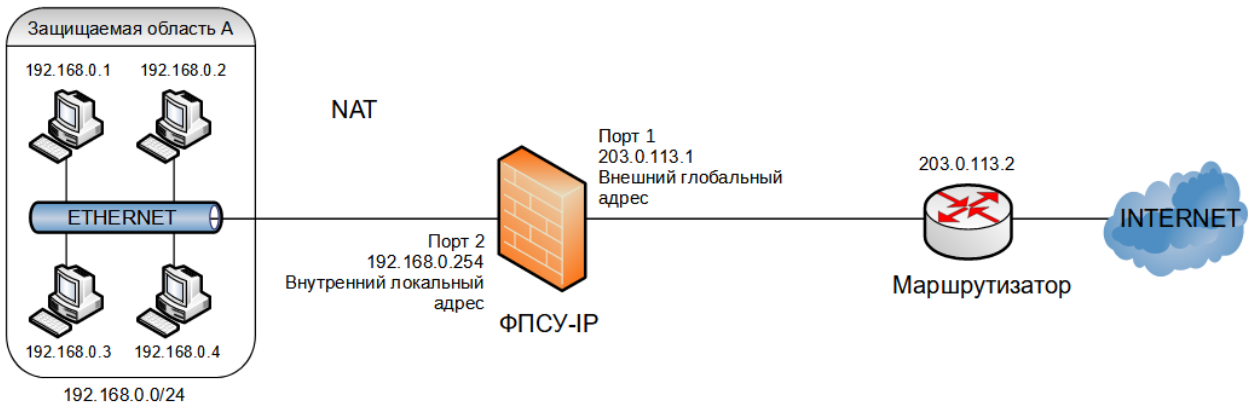


Рисунок 353 - Применение ФПСУ-IP для доступа в интернет с NAT

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)
```

15. 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.

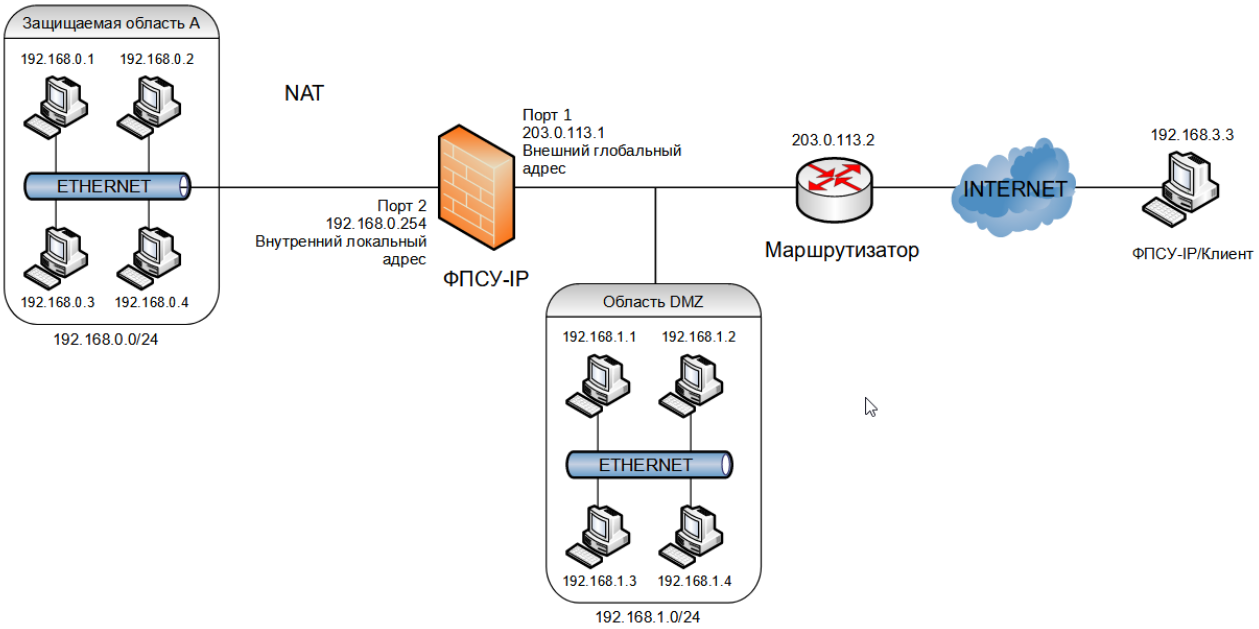


Рисунок 354 - Схема подключения ФПСУ-IP/Клиентов

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)
```

15. 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 А, обмен хостов данной подсети через комплекс производится в режиме ретрансляции;
- со стороны внешнего порта 2 определен ФПСУ-IP А, 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 А отправляет эхо-запрос (ping) на внутренний IP-адрес ФПСУ-IP А. Правилом МЭ данный запрос разрешен. На ФПСУ-IP А 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 В 1.1.1.2. Запрос отправляется на ФПСУ-IP В. Правилом МЭ данный запрос разрешен. На ФПСУ-IP В 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 В. Ответ хоста 192.168.0.1 защищаемой области В проходит обратное преобразование при прохождении ФПСУ-IP В и ФПСУ-IP А. На ФПСУ-IP реализовано отслеживание инициатора запроса - возвратный трафик разрешен.

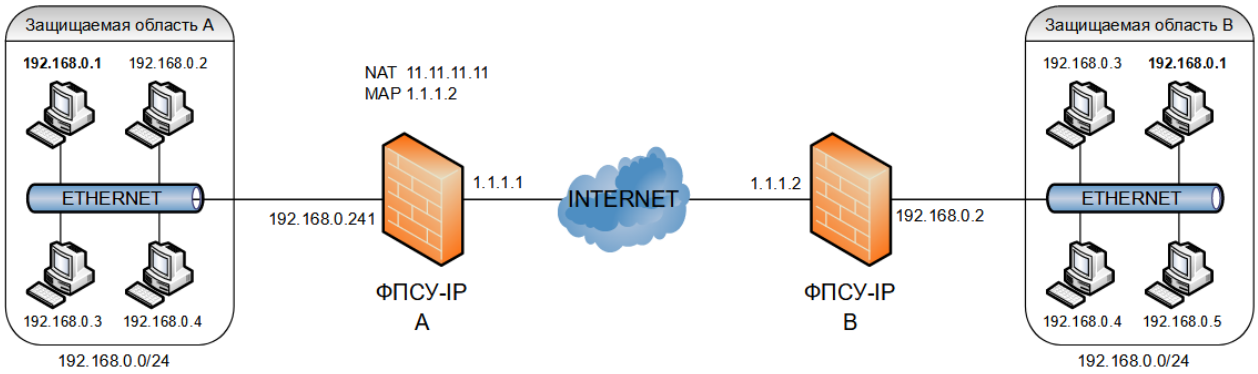


Рисунок 355 - Схема подключения ФПСУ-IP/Клиентов

ФПСУ-IP А

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 указаны на ФПСУ А 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 В

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.

15. 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.

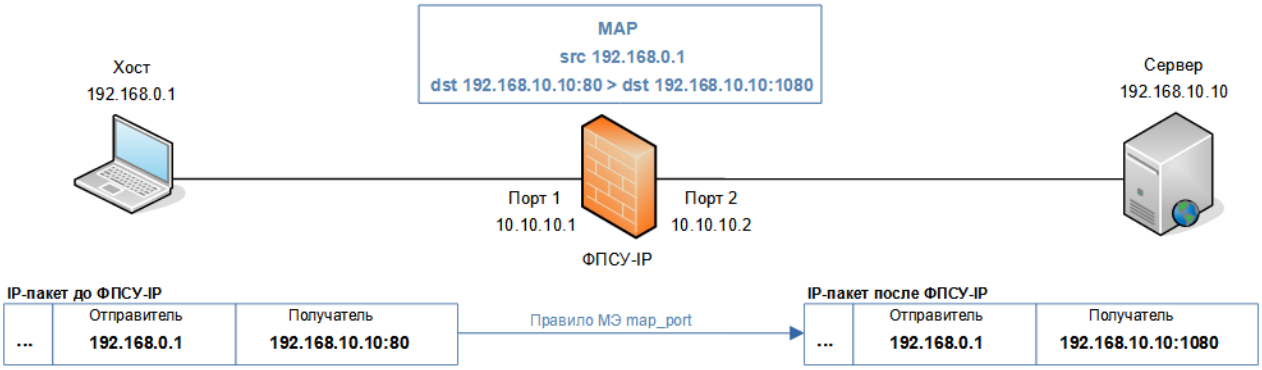


Рисунок 356 - Схема перенаправления пакетов на другой порт сервера

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
       Мар             : 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.

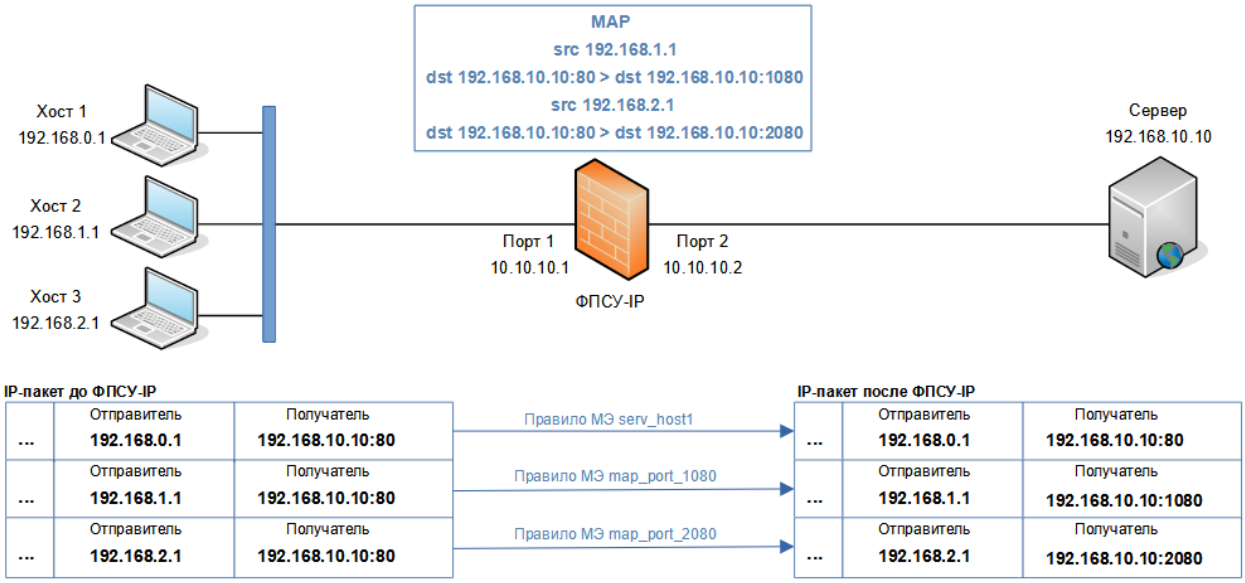


Рисунок 357 - Схема перенаправления пакетов на другой порт сервера

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
        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
        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.

15. 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»).

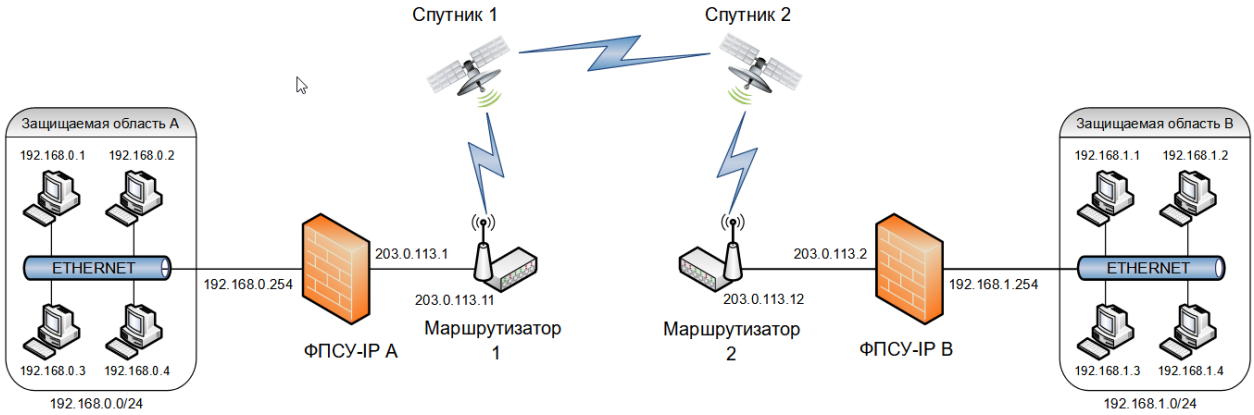


Рисунок 358 - Передача данных через спутниковый канал связи

Рассмотрим пример, когда абонент области A отправляет данные абоненту области B. 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 A в защищенную область B.

16. Способы разрешения возможных проблем при работе ФПСУ-IP

16. 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.

16. 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 14. 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	Неправильно указанная	Установить в конфигурации

пакетов на соответствующем порту ФПСУ-IP	(или определенная адаптером) скорость работы линии на сетевом адаптере	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.

17. 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 15. 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.
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 16. Ошибки, связанные с обработкой принимаемых IP-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.
Сбой	Сбой указанного сетевого	Неустойчивая работа сбойного сетевого

Диагностика	Пояснение	Причина возникновения
LAN карты	адаптера при попытке передачи фрейма	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	У принятого пакета истекает время жизни. Если данная ошибка проявляется часто, причем

Диагностика	Пояснение	Причина возникновения
	лимит времени ожидания сборки пакета	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 17. 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.

Диагностика	Пояснение	Причина возникновения
		Несовместимые режимы работы смежных сетевых адаптеров.
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.

Диагностика	Пояснение	Причина возникновения
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 18. 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	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.

Служебное сообщение	Пояснение	Действия администратора
комплекса		
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. Ожидание восстановления конфигурации с резервного комплекса или удаленного администратора	ПО ФПСУ-IP обнаружило искажение конфигурации ФПСУ-IP	Восстановить конфигурацию ФПСУ-IP любым из следующих способов: • локально с помощью резервной копии конфигурации; • 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	Заново зарегистрировать удаленных администраторов на ФПСУ-IP. Перерегистрировать ФПСУ-IP на всех удаленных администраторах.

Служебное сообщение	**Пояснение**	**Действия администратора**
	открытых ключей удаленных администраторов. Удаленное управление ФПСУ-IP с такой ошибкой невозможно.	
Описатель удаленных администраторов испорчен или несовместимая версия!	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы 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.
**Имя_файла_с_открытым_ключом_удаленного_администратора*----> Поврежден*	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ-IP при попытке	Заново получить от администратора АРМ УА открытый ключ удаленного администратора и повторить процедуру регистрации удаленного администратора на ФПСУ-IP

Служебное сообщение	**Пояснение**	**Действия администратора**
	зарегистрировать нового удаленного администратора. Причина - искажен или поврежден предъявленный на внешнем USB-носителе открытый ключ удаленного администратора	
Состояние туннеля с другим ФПСУ-IP "WaitSynRR" с дополнительными сообщениями в журнале статистики "Аварийное состояние ключей/нештатные действия: Ошибка при зачитывании установленных ключей"	Хранящиеся на внутреннем накопителе ФПСУ-IP парно-выборочные ключи были искажены. Требуется вмешательство администратора	Заново установить на ФПСУ-IP полученные от администратора ЦВК парно-выборочные ключи.
Данные искажены, пропускаю!	Сообщение об ошибке выводится на экране установки ключей меню конфигурации ФПСУ-IP. Возникает при искажении предъявленного на внешнем USB-носителе	Заново получить от администратора ЦВК парно-выборочный ключ взамен искаженного.

Служебное сообщение	**Пояснение**	**Действия администратора**
	парно-выборочного ключа	
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.
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.	Заново установить на ФПСУ-IP общесистемный ключ Криптосети Клиентов вместо искаженного.

Служебное сообщение	Пояснение	Действия администратора
	Искажен общесистемный ключ Криптосети Клиентов. ФПСУ-IP\Клиенты не могут соединиться с ФПСУ-IP	
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 19. 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.

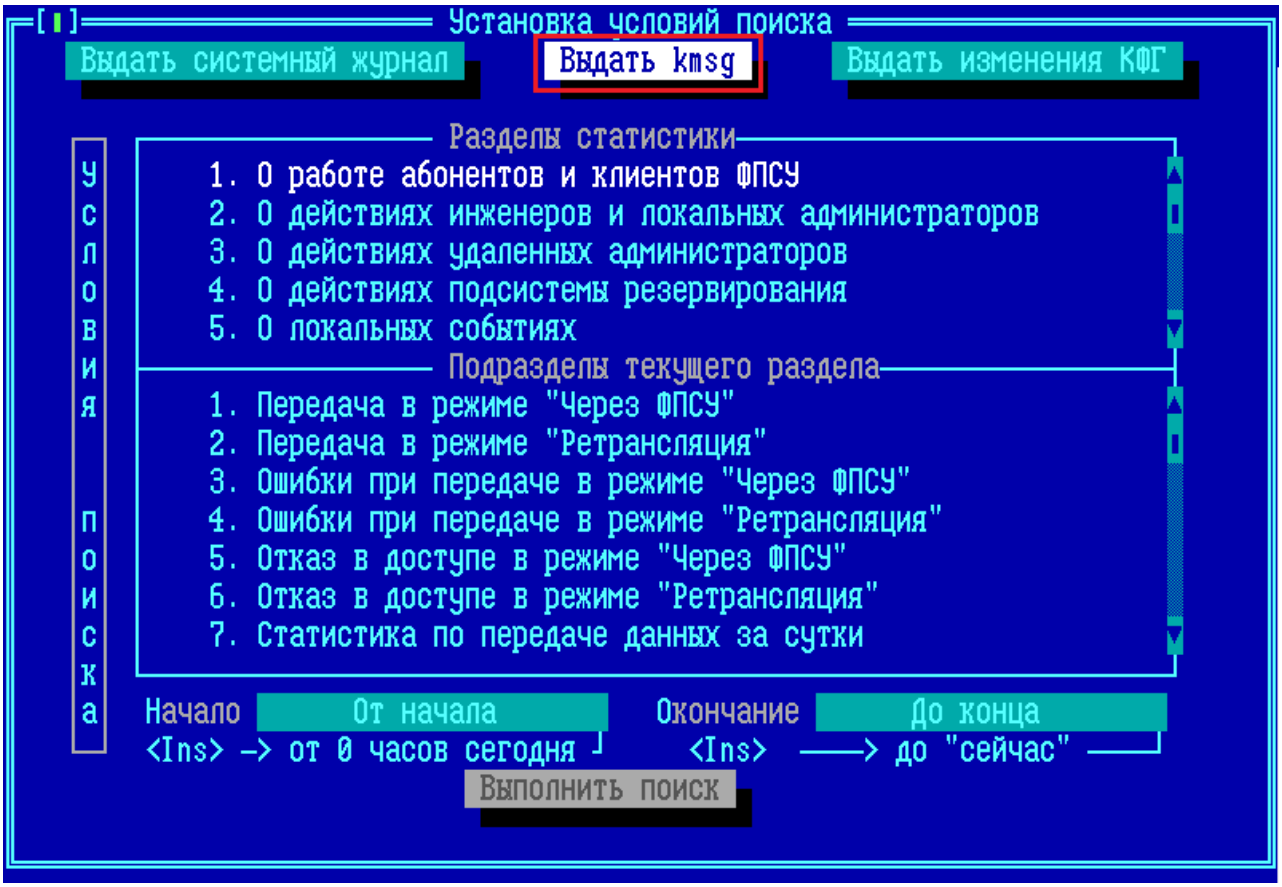


Рисунок 359 - Команда выдачи журнала изменений конфигурации межсетевого экрана

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

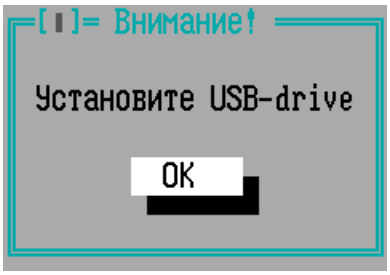


Рисунок 360 - Предложение подключить USB-носитель

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.

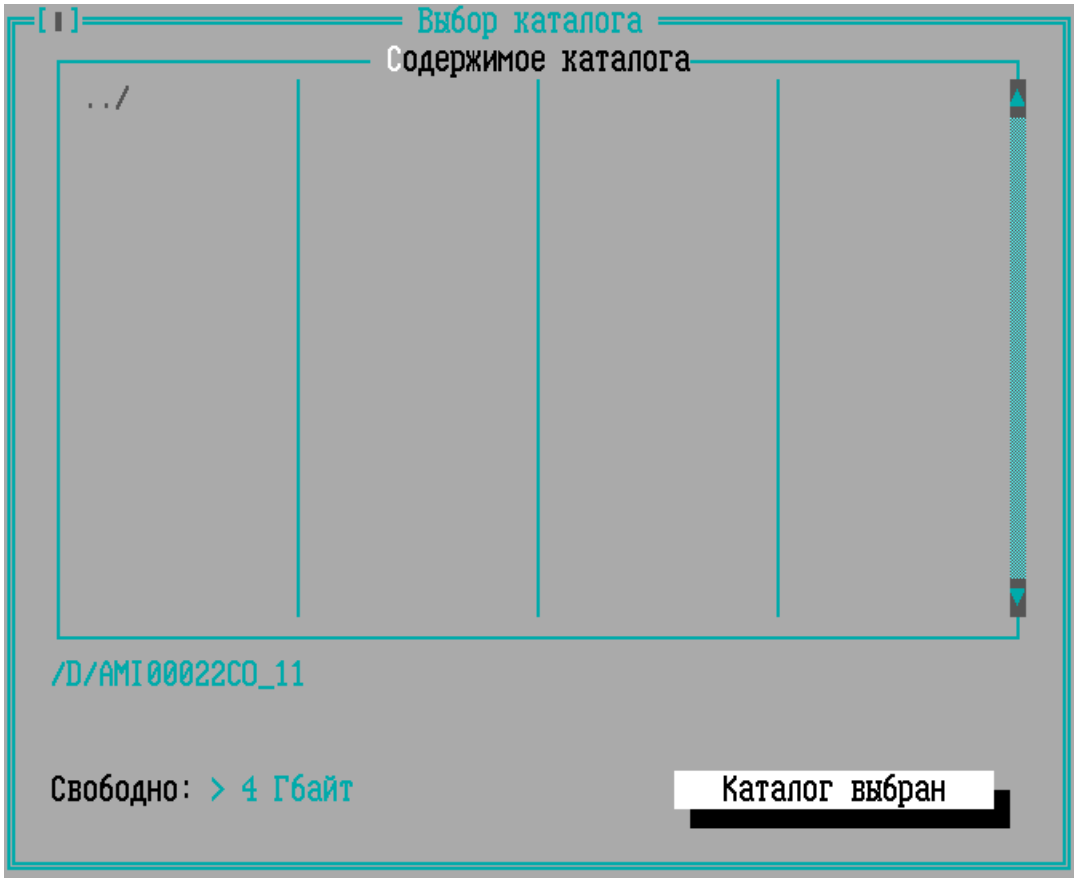


Рисунок 361 - Выбор каталога для выгрузки файла

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

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

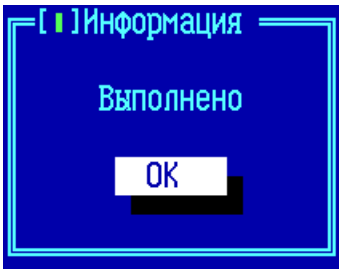


Рисунок 362 - Сообщение о завершении процедуры

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 следует выполнить:

1. Команду «Настройка системы» главного меню:

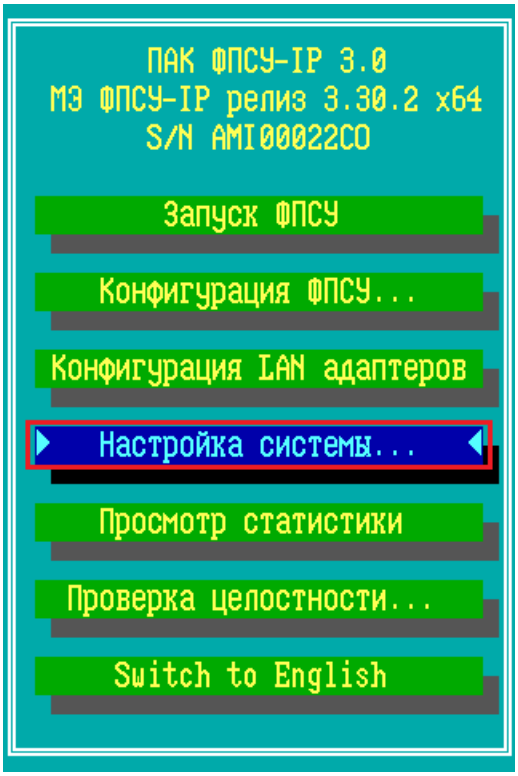


Рисунок 363 - Главное меню ФПСУ-IP

2. Команду «Настройки СКЗИ» меню настройки системы:

Рисунок 364 - Меню настройки системы ФПСУ-IP

3. Команду «Удаление СКЗИ» меню настройки СКЗИ.

Рисунок 365 - Запуск процедуры удаления СКЗИ

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!

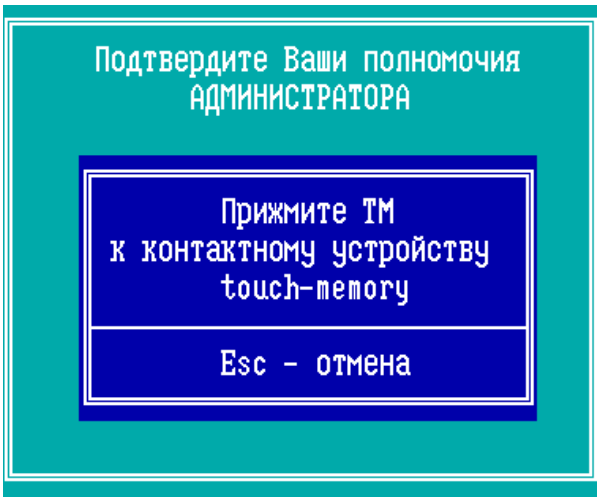


Рисунок 366 - Подтвердите полномочия для удаления СКЗИ

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.

18. 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.

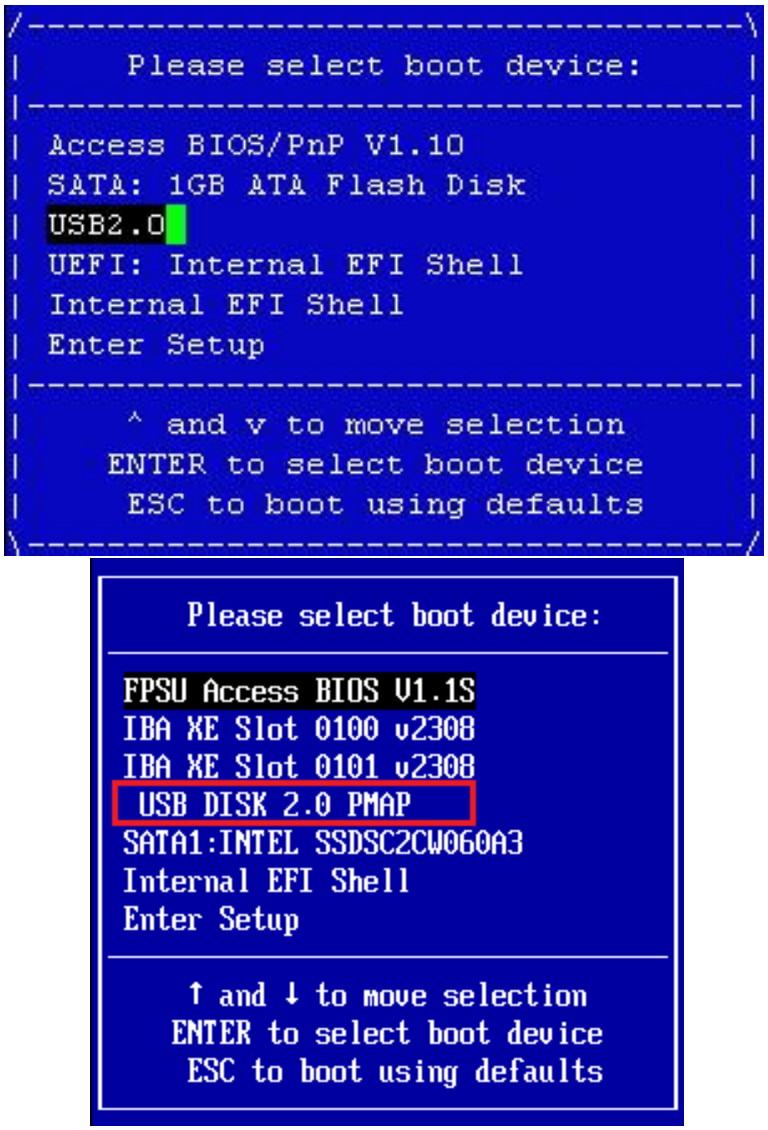


Рисунок 367 - Выбор загрузки с USB

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:

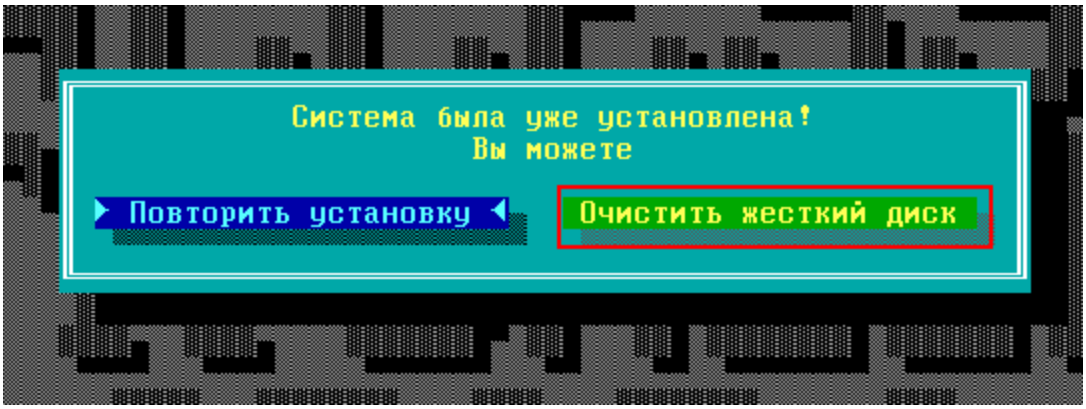


Рисунок 368 - Операционная система ФПСУ-IP уже установлена

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.