

ООО "АМИКОН"

УТВЕРЖДЕН

ПЕРС.26.20.40.140.003РЭ-ЛУ

Программно-аппаратный комплекс

"ФПСУ-IP 3.X"

Руководство по эксплуатации

ПЕРС.26.20.40.140.003РЭ

Листов 371

2023

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением программно-аппаратных комплексов "ФПСУ-IP" (версии ПО 3.20.1, 3.20.2, 3.20.8). В документе содержатся общие 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.

© ООО "АМИКОН", 1994-2023. Все права защищены.

Все авторские права на эксплуатационную документацию защищены.

Документ входит в комплект поставки изделия.

Без специального письменного разрешения ООО "АМИКОН" настоящий документ или его часть в печатном или электронном виде не могут быть скопированы и переданы третьим лицам с коммерческой целью.

Информация, содержащаяся в настоящем документе, может быть изменена разработчиком без специального уведомления, что не является нарушением обязательств по отношению к пользователю со стороны ООО "АМИКОН".

Содержание

1. Список используемых сокращений и определений	8
2. Общие сведения	10
3. Процедуры приемки и безопасной установки	16
3.1. Общий порядок поставки	16
3.2. Организационные условия эксплуатации	16
3.3. Требования к среде функционирования	17
3.4. Выполнение целей безопасности для среды функционирования	18
3.5. Указания для полного или частичного устранения идентифицированных скрытых каналов	20
3.5.1. ISN Evaluation	21
3.5.2. TCP URG Pointer	21
3.5.3. IP ToS Evaluation	22
3.6. Технические условия эксплуатации и хранения	26
3.7. Гарантийные обязательства	27
3.8. Настройки платформ виртуализации	28
3.8.1. Настройка виртуальной машины QEMU/KVM	28
3.8.2. Настройка виртуальной машины VMware	30
3.9. Консольное подключение к ФПСУ-IP	35
3.9.1. Настройки BIOS для консольного подключения	36
3.9.2. Установка драйверов консольного кабеля	40
3.9.3. Подключение к ФПСУ-IP с помощью PuTTY	47
3.10. Установка ПО ФПСУ-IP с дистрибутива	53
3.10.1. Создание загрузочного USB-носителя утилитой restore.exe	54
3.10.2. Установка ПО ФПСУ-IP с установочного носителя	57
4. Настройка параметров и установка драйверов оборудования	62
4.1. Технологический режим ФПСУ-IP	62
4.2. Установка драйверов сетевых адаптеров	63
5. Запуск и режим фильтрации ФПСУ-IP	65
5.1. Запуск ФПСУ-IP	66
5.2. Мониторинг аппаратного состояния и суточная статистика	68
5.3. Окно установки параметров работы с экраном	73
5.4. Окно состояния рабочих LAN портов	73
5.5. Окно состояния ARP-кэша	74

5.6. Окно состояния работы пользователей	76
5.7. Окно состояния VPN-туннелей с другими ФПСУ-IP	81
5.8. Окно состояния связи с удаленными администраторами	83
5.9. Окно мониторинга подключенных ФПСУ-IP/Клиентов	84
5.10. Окно состояния подсистемы "горячего" резервирования	86
5.11. Информационные окна жидкокристаллического экрана	89
6. Контроль целостности программного обеспечения	92
6.1. Проверка целостности программных модулей ФПСУ-IP	93
6.2. Контроль целостности Терминала	94
6.3. Самотестирование функций межсетевых экранов ФПСУ-IP	95
6.4. Проверка контрольных сумм при помощи ФИКС (2.0.2)	96
7. Конфигурация ФПСУ-IP	100
7.1. Общие параметры конфигурации ФПСУ-IP	102
7.2. Установка ключей	111
7.3. Использование ключей	114
7.4. Конфигурация драйверов сетевых адаптеров	115
7.5. Применение 4 порта для доступа удаленного администратора	120
8. Настройка системы	123
8.1. Регистрация ТМ-идентификаторов	123
8.2. Установка дополнений/изменений	126
8.3. Установка пароля администратора	130
8.4. Установка даты и времени	132
8.5. Регистрация Удаленных Администраторов	133
8.5.1. Регистрация удаленного администратора на ФПСУ-IP	135
8.5.2. Ключи аутентификации ФПСУ-IP	138
8.6. Параметры "Горячего резерва"	140
8.6.1. Настройка ФПСУ-IP на работу с партнером по резервированию	142
8.6.2. Замена ключа горячего резерва	144
8.6.3. Принудительная синхронизация данных	149
8.6.4. Параметры проверки линий связи для портов ФПСУ-IP	150
8.6.4.1 Интерфейс настройки проверки линий связи	151
8.6.4.2 Пример работы системы проверки связи	153
8.7. Настройки СКЗИ	156
8.7.1. Отключение автозапуска	158
8.7.2. Переинициализация ПДСЧ	158
8.7.3. Установка времени действия ключей	159

9. Порты ФПСУ	162
9.1. Описание VLAN порта ФПСУ-IP	165
9.2. Описание параметров используемых маршрутизаторов	167
9.3. Описание параметров удаленных ФПСУ-IP	170
9.3.1. Дополнительные параметры соединения ФПСУ-ФПСУ	174
9.3.2. Потоки данных в туннеле между ФПСУ-IP	177
9.3.3. Режим "Мост" между ФПСУ-IP (L2-шифрование)	182
9.3.4. Динамические ФПСУ	185
9.3.5. Описание туннеля типа IP/IP	187
9.4. Описание параметров абонентов	188
9.4.1. Описание абонента "Host"	190
9.4.2. Описание абонента "Подсеть"	197
9.4.3. Описание абонента "Любой Host"	200
9.4.4. Работа со списком абонентов	201
10. Правила трафика межсетевого экрана	207
10.1. Правила трафика	209
10.1.1. Общие настройки правил трафика	211
10.1.2. Вкладки "Источник" и "Назначение" правил трафика	213
10.1.3. Службы в правилах трафика	216
10.2. Службы	219
10.2.1. Протокол ICMP в службах	222
10.2.2. Служба для запрета фрагментированных пакетов	223
10.2.3. Протокол REGEXP в службах	224
10.3. Управление полосой пропускания	232
10.4. Фильтрация трафика по содержимому (DPI)	236
10.4.1. Создание правила фильтрации по содержимому и его общие настройки	238
10.4.2. Исследуемый правилом фильтрации трафика по содержимому протокол	239
10.4.3. Дополнительные фильтры для протокола http	242
10.4.4. Службы в правилах фильтрации трафика по содержимому	245
10.5. Интервалы времени	246
10.6. Группы IP-адресов	249
10.7. Дополнительные параметры и защита от flood-атак	252
11. Клиент для ФПСУ-IP	258
11.1. Установка и удаление общесистемных ключей	260
11.2. Описание логической группы клиентов	261

11.3. Установка правил работы клиентов	262
11.4. Настройка правил работы отдельного клиента	269
12. Служебные протоколы	272
12.1. Общие правила разделения потоков	272
12.2. Учет трафика IPFIX	275
12.3. Syslog-клиент на ФПСУ-IP	277
12.3.1. Настройка SysLog событий ФПСУ-IP	278
12.3.2. Опции работы с SysLog сервером	283
12.3.3. Формат отправляемых SysLog сообщений	286
12.4. SNMP-клиент на ФПСУ-IP	288
12.5. DHCP-Relay	291
12.5.1. Создание списка DHCP-серверов	292
12.5.2. Настройка DHCP-Relay на портах ФПСУ	293
12.6. Http-proxy ФПСУ-IP	296
12.6.1. Авторизация на http-proxy	299
12.7. Взаимодействие со средствами обнаружения вторжений	302
12.8. NTP-клиент ФПСУ-IP	305
12.9. Служебные протоколы и порты на ФПСУ-IP	307
13. Статистика ФПСУ-IP	309
13.1. Просмотр статистики	309
13.2. Выдача журнала изменений конфигурации межсетевого экрана	311
13.3. Ограничение сбора статистики	313
14. Восстановление работы ФПСУ-IP после сбоев	318
15. Примеры настройки ФПСУ-IP	320
15.1. Использование одного ФПСУ-IP для защиты локальной сети	321
15.2. Защита локальной сети, состоящей из двух IP-подсетей	323
15.3. Разделение подсети на два фрагмента средствами ФПСУ-IP	327
15.4. Использование ФПСУ-IP для создания VPN-туннелей	330
15.4.1. Использование отдельных VPN-туннелей	332
15.4.2. Использование совмещенных VPN-туннелей	337
15.5. Использование ФПСУ-IP для создания в одной области двух защищаемых областей	342
16. Способы разрешения возможных проблем при работе ФПСУ-IP	351
16.1. Первый запуск ФПСУ-IP	351
16.2. Устранение неполадок, связанных с работой сетевого оборудования	352

17. Диагностика ошибок ФПСУ-IP	354
17.1. Выдача файла Kmsg	365
18. Удаление программного обеспечения ФПСУ-IP	368
18.1. Удаление СКЗИ ФПСУ-IP	368
18.2. Удаление ПО с помощью USB-носителя со средством восстановления	370

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
СКЗИ	средство криптографической защиты информации
СЗИ НСД	система защиты информации от несанкционированного доступа
ТМ, ТМ-идентификатор	электронный идентификатор "touch-memory": iButton DS1993 – DS1996 или микроэлектронное USB-устройство «ТМ-Кей» ПЕРС.466226.004 производства ООО «АМИКОН»
ФПСУ-IP	программно-аппаратный комплекс "ФПСУ-IP 3.X", средство защиты информации, 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").

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-проxy;
- 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 «ТМ-Кей» 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

<i>Роль/Класс</i>	<i>Разрешенные действия</i>
<i>Пользователь/ /Без идентификации пользователя</i>	<ul style="list-style-type: none">• переинициализация ПДСЧ;• отключение автозапуска.

<i>Роль/Класс</i>	<i>Разрешенные действия</i>
<i>Пользователь/ /Оператор</i>	<ul style="list-style-type: none"> • 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".
<i>Администратор /Инженер</i>	<ul style="list-style-type: none"> • Все права класса <i>Оператор</i> 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).
<i>Администратор/ Администратор</i>	<p>Все права класса <i>Инженер</i> и дополнительно:</p> <ul style="list-style-type: none"> • 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

<i>Роль/Класс</i>	<i>Разрешенные действия</i>
	администраторам; <ul style="list-style-type: none"> • регистрация ТМ-идентификаторов; • 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.
<i>Администратор /Главный администратор</i>	Все права класса <i>Администратор</i> и дополнительно: <ul style="list-style-type: none"> • 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).

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".

3. Процедуры приемки и безопасной установки

3.1. Общий порядок поставки

Комплектность поставки ФПСУ-IP указана в документе «Программно-аппаратный комплекс "ФПСУ-IP 3.X". Формуляр. ПЕРС.26.20.40.140.003ФО».

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

Подсчет контрольных сумм должен выполняться с использованием программы фиксации и контроля исходного состояния программного комплекса «ФИКС» (версия 2.0.2) (сертификат № 1548, выдан ФСТЭК России 15 января 2008 года, действителен до 15 января 2020 года) по алгоритму ВКС, «взвешенное контрольное суммирование».

Проверка выполняется в соответствии с разделом "[Проверка контрольных сумм при помощи ФИКС \(2.0.2\)](#)".

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, используемой 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.26.20.40.140.003ЗБ (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	<p>ПО консоли управления: Putty 0.70</p> <p>ОС консоли управления и для ПО записи дистрибутива ПАК "ФПСУ-IP" на USB: Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10.</p> <p>Вычислительная платформа общего назначения: в соответствии с требованиями операционной системы.</p>
ТМ-идентификатор	<p>Физическим носителем ТМ-идентификатора должно являться:</p> <p>Микроэлектронное устройство контактной памяти iButton DS-1993 (Dallas Semiconductor)</p> <p>или</p> <p>Микроэлектронное USB-устройство «ТМ-Key» ПЕРС.466226.004 (ООО «АМИКОН»).</p>

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](#)):

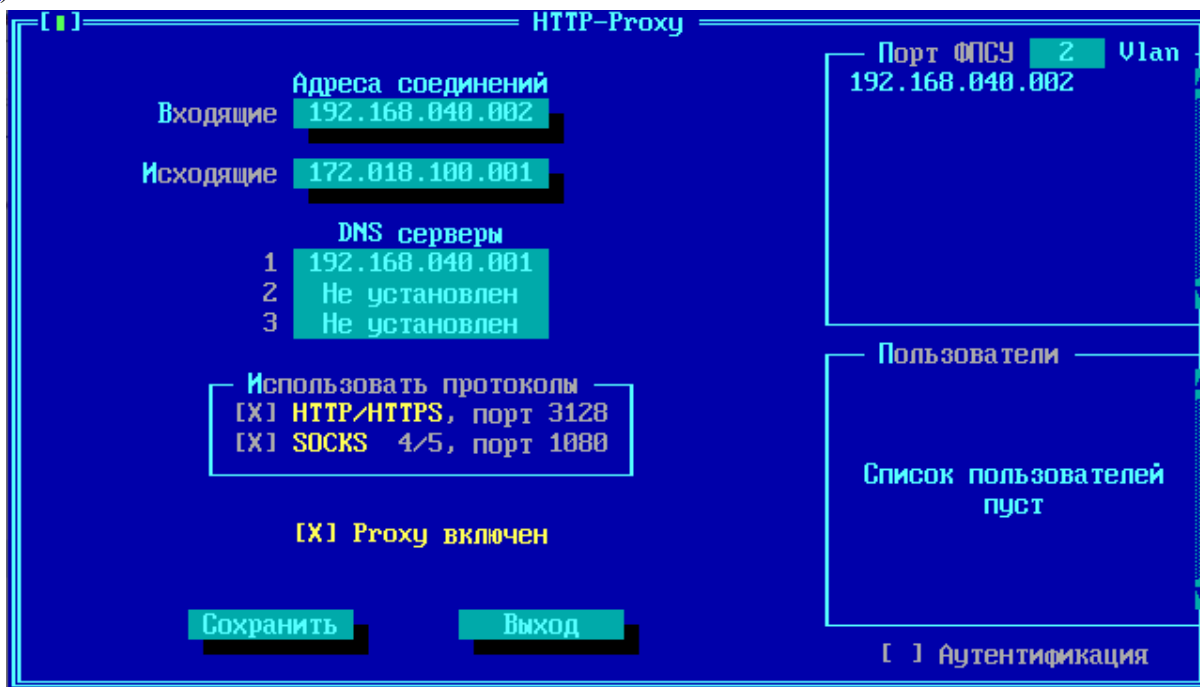


Рисунок 1 - Настройки Proxy

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"\):](#)

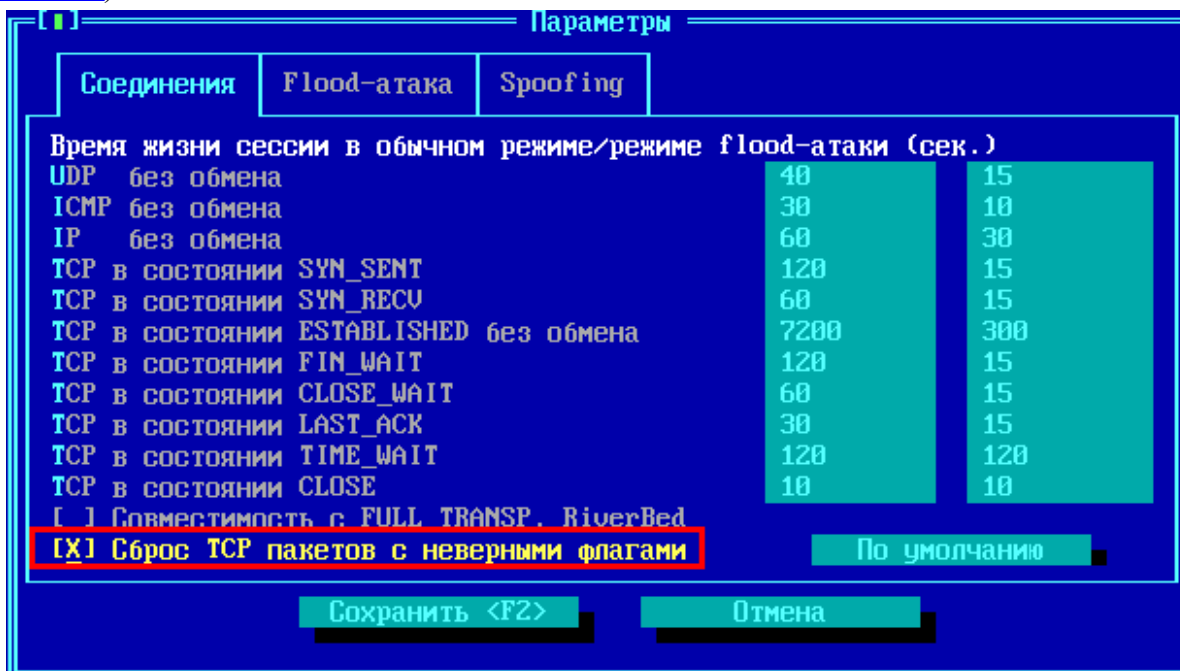


Рисунок 2 - Настройки правил соединения и фильтрации

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 недостижим);

4 – source quench (подавление источника, просьба посылать пакеты медленнее);

11 – time-to-live exceeded (истечение срока жизни пакета);

12 – IP header bad (неправильный IP-заголовок 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):

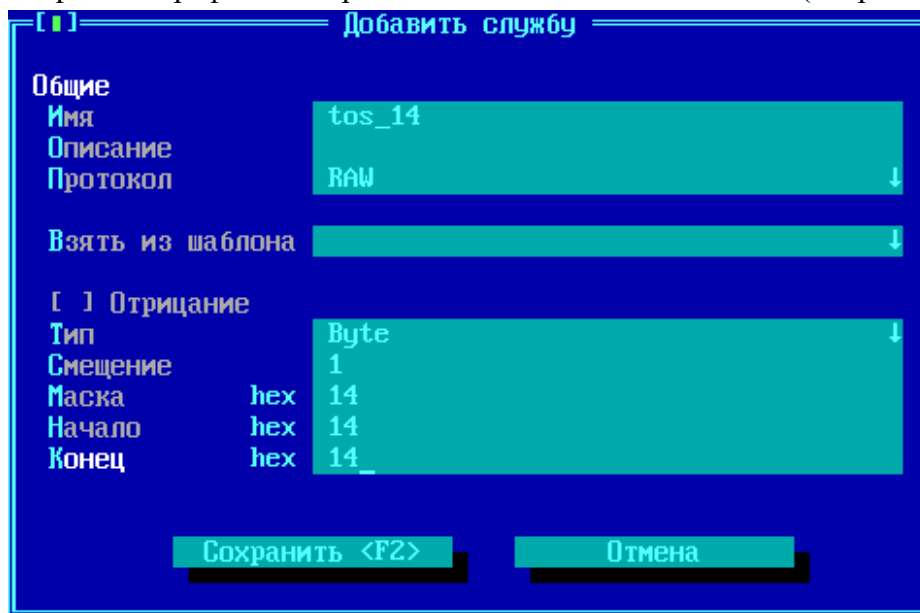


Рисунок 3 - Добавление службы RAW

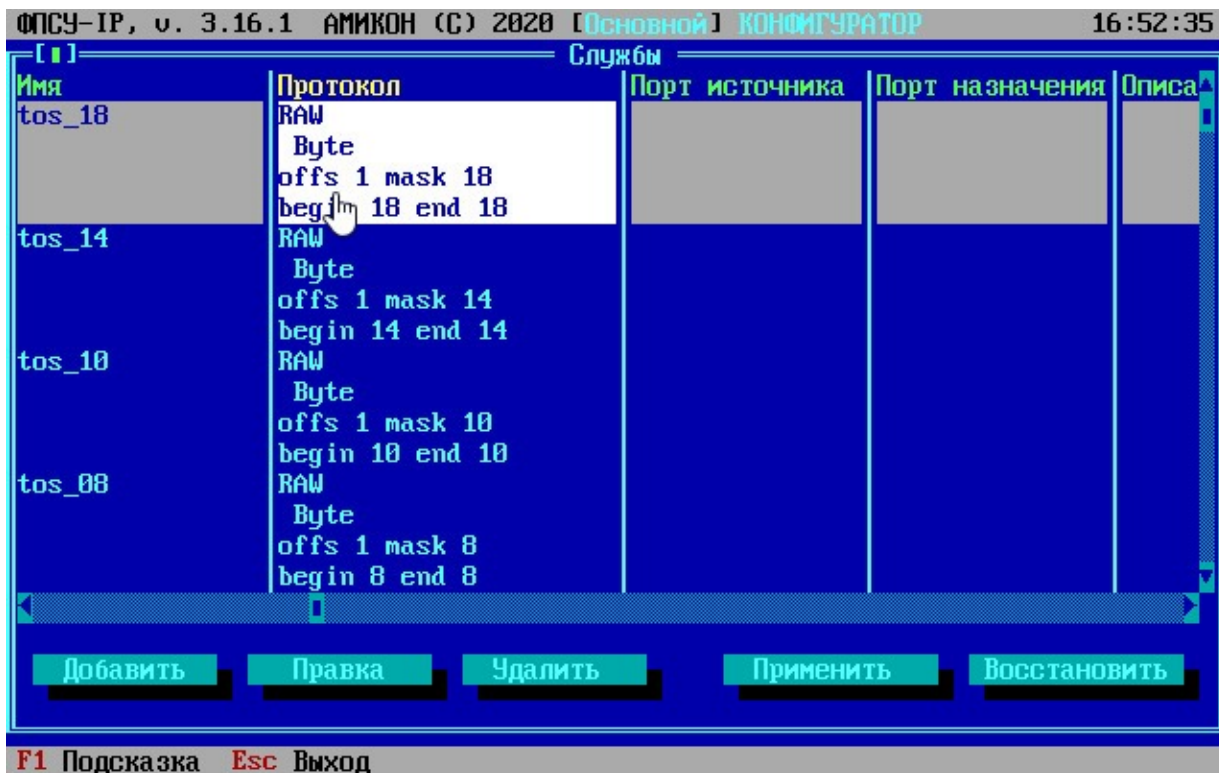


Рисунок 4 - Служба добавлена

Выбрать заранее созданный шаблон фильтра фрагментированных IP-пакетов. (["Службы в правилах фильтрации трафика по содержимому"](#)).

При необходимости изменить правило трафика:

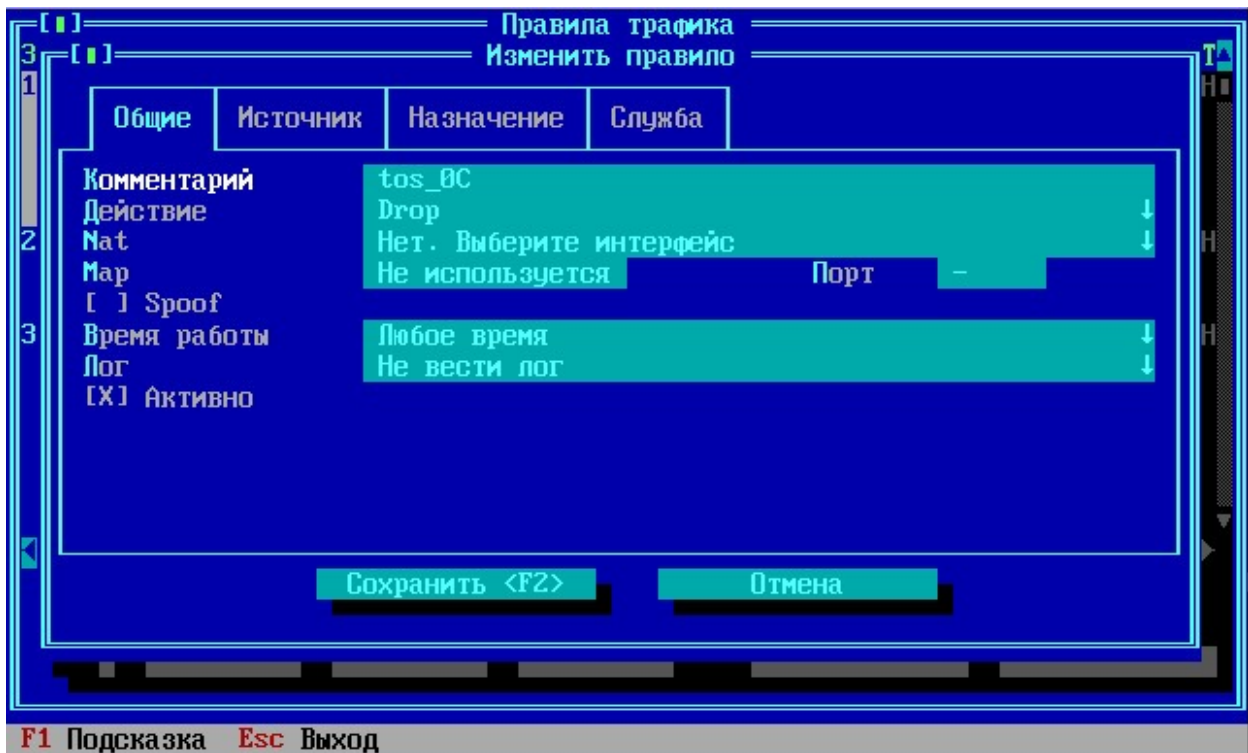


Рисунок 5 - Изменение общих свойств правила

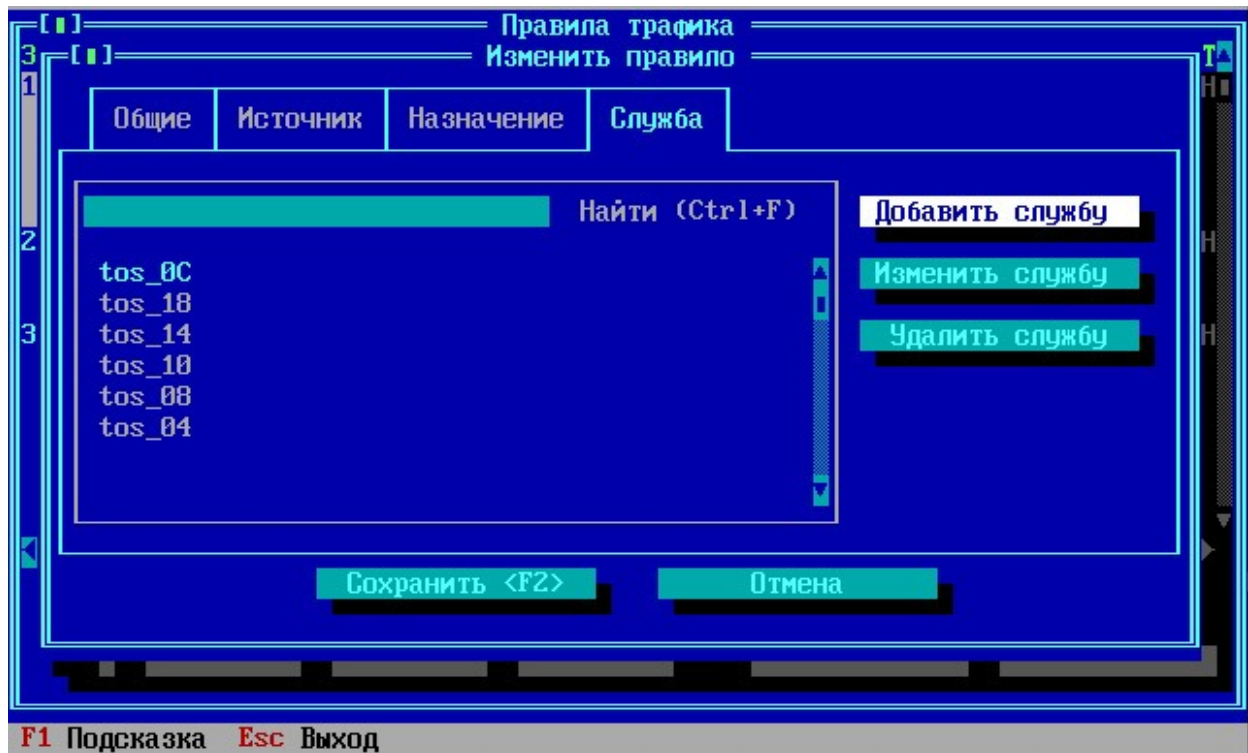


Рисунок 6 - Работа со службами

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 $220 \text{ В} \pm 10\%$, частота тока $50 \text{ Гц} \pm 1\%$, 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 - $20^{\circ}(\pm 15^{\circ}) \text{ C}$;
- относительная влажность окружающего воздуха - $60 (\pm 15)\%$;
- атмосферное давление - от 84 до 107 кПа (630–800 мм рт. ст.);
- запыленность воздуха - не более $0,75 \text{ мг/м}^3$;
- в воздухе не должно быть агрессивных примесей (паров кислот и щелочей), вызывающих коррозию.

Условия хранения.

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

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

3. 7. 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 лицензионном соглашении) 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. 8. Настройки платформ виртуализации

3. 8. 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 (ACCESS-TM SHELL). Настроить сетевые интерфейсы и другие устройства.

Приводится пример установки ФПСУ-IP на Ubuntu 20.04 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 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. Для установки необходимых пакетов введите в строке терминала:

```
sudo apt install kvm libvirt-bin
```

3. После установки пакета libvirt-bin необходимо настроить доступ к управлению виртуальной машиной. В группу libvirtd необходимо добавить пользователя для управления виртуальными машинами. Данный пользователь получит доступ к

расширенным сетевым опциям. Введите команду в терминале:

```
sudo adduser $USER libvirt
```

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

4. Включите поддержку встроенного ПО UEFI для виртуальной машины QEMU/KVM, установив 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`. Для ее установки введите в терминале:

```
sudo apt install virtinst
```

6. Установите гостевую операционную систему ФПСУ-IP в виртуальную машину QEMU/KVM, выполните команду в терминале:

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

Параметр `size=1` убрать, если используется готовый образ диска.

Добавьте в конфигурационный файл USB-носитель с инсталляционным комплектом ФПСУ-IP и проведите установку ПО. Описание процедуры установки ПО ФПСУ-IP находится в разделе [«Установка ПО ФПСУ-IP с установочного носителя»](#).

Если используется образ диска с установленным ФПСУ-IP, то на экране появится окно с главным меню ФПСУ-IP.

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

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

8. Настройте параметры виртуальной машины, введите в терминале:

```
virsh edit vfpsul
```

Откроется редактор с файлом конфигурации виртуальной машины.

9. В файле найдите раздел `<interface>` с параметрами сетевых интерфейсов и изменить 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.

```
<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>
```

10. Для корректной работы QEMU необходимо использовать в качестве дисплея только устройство Cirrus SVGA, проверьте следующие настройки в конфигурационном файле виртуальной машины в разделе <model>.

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

11. Добавьте в конфигурационный файл TM-считыватель или USB-токен.
12. Для управления виртуальной машиной используются различные утилиты. В примере используется пакет virt-manager, который содержит утилиту с графическим интерфейсом для управления локальными и удаленными виртуальными машинами. Для установки virt-manager введите команду в терминале:

```
sudo apt-get install virt-manager
```

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
```

Создание виртуальной машины закончено. Запустите виртуальную машину, введите команду:

```
virsh start vfpsul
```

На экране отобразится главное меню ФПСУ-IP.

3. 8. 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.

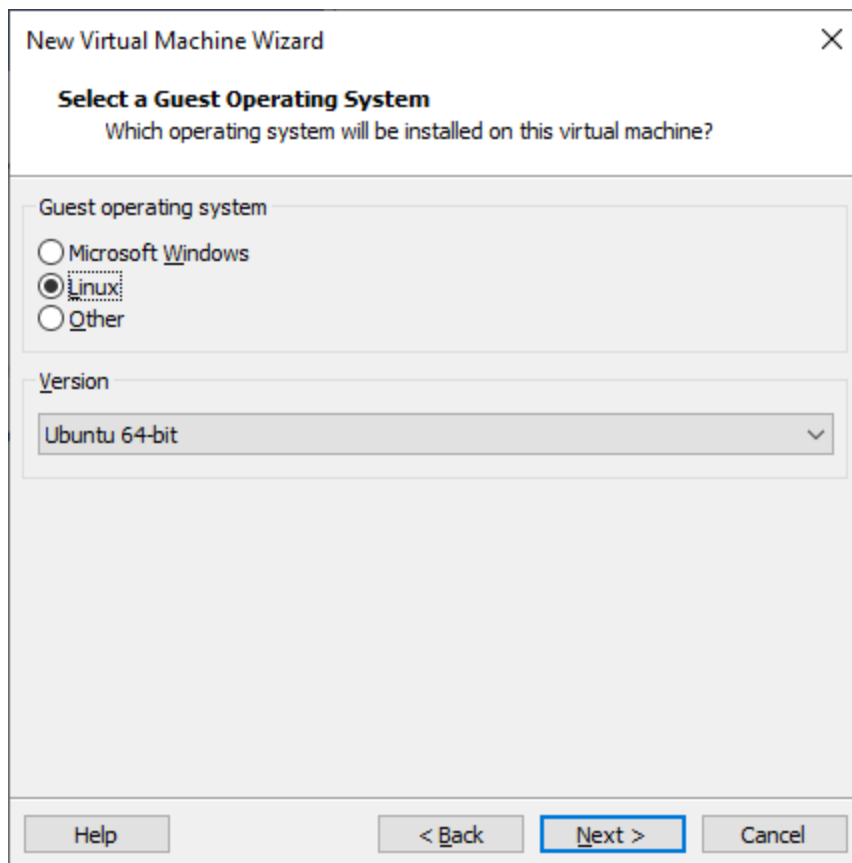


Рисунок 7 - Выбор ОС

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.

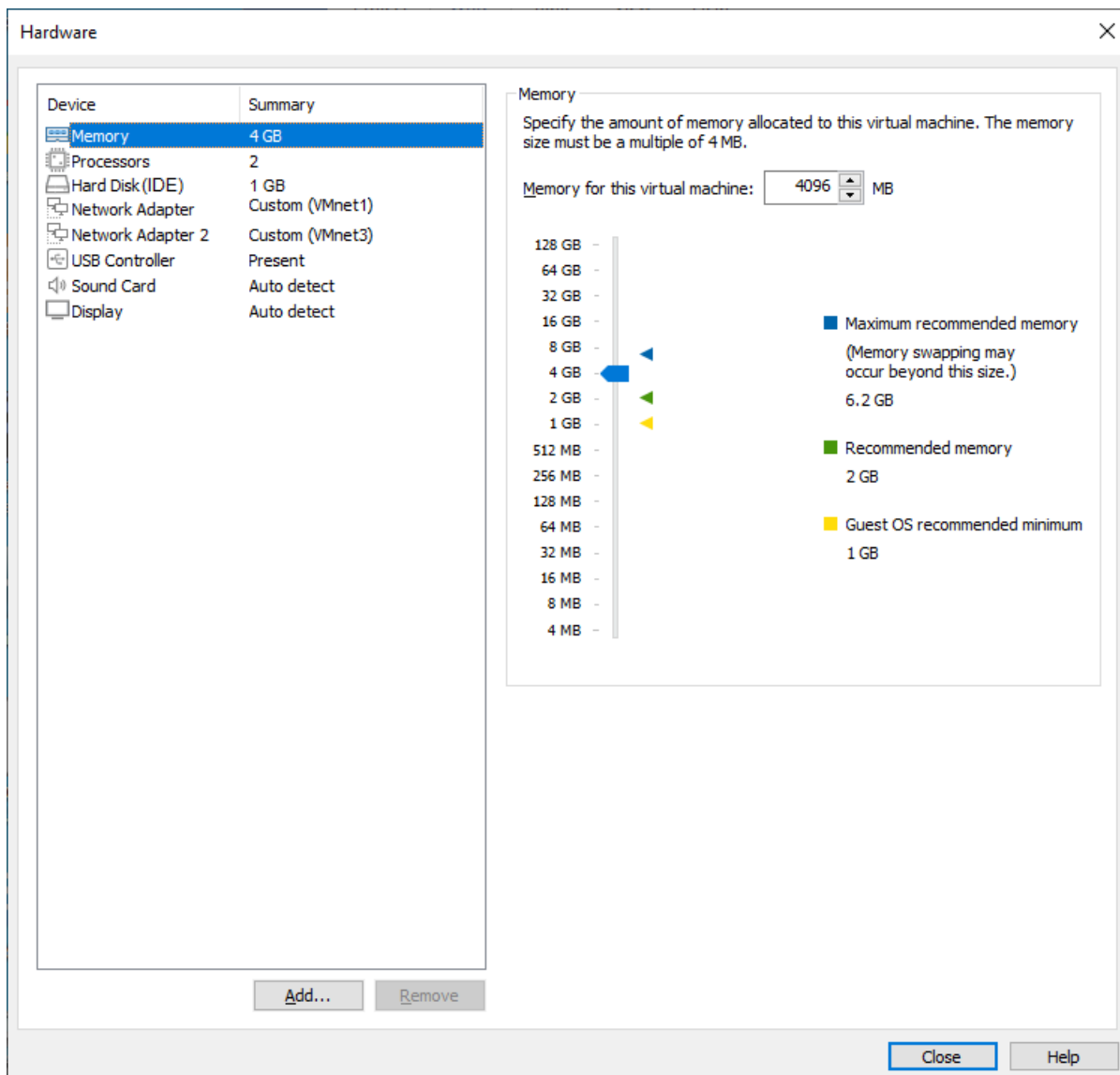
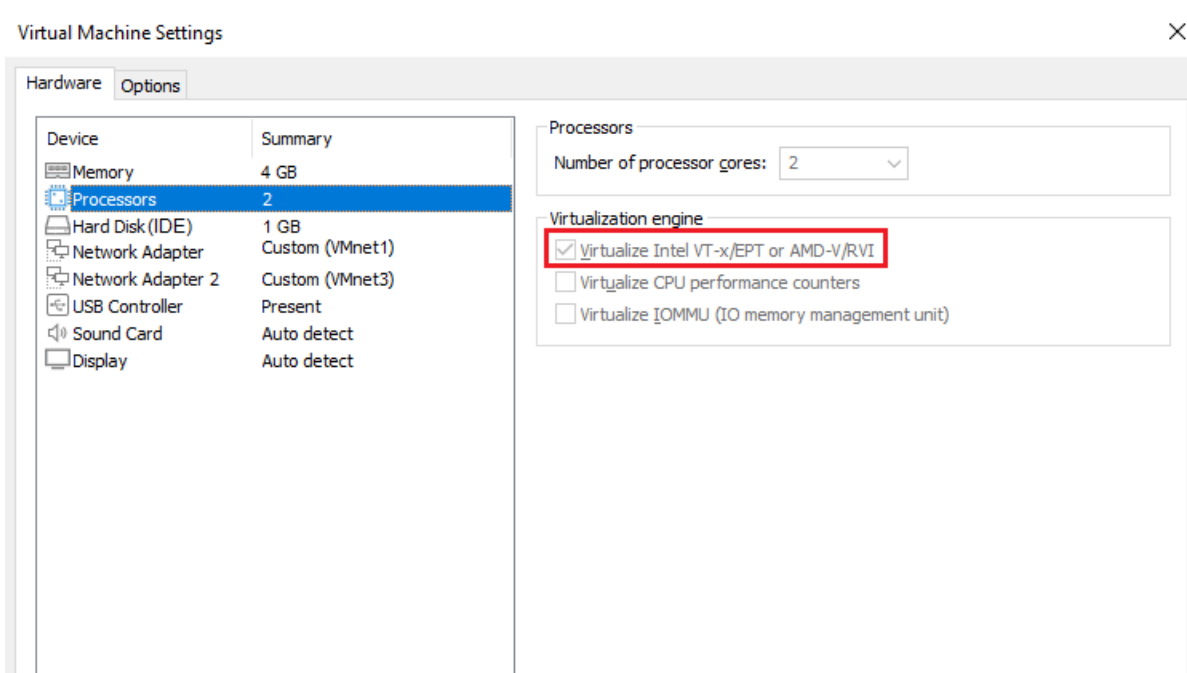


Рисунок 8 - Оперативная память виртуальной машины

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

**Рисунок 9 - 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».

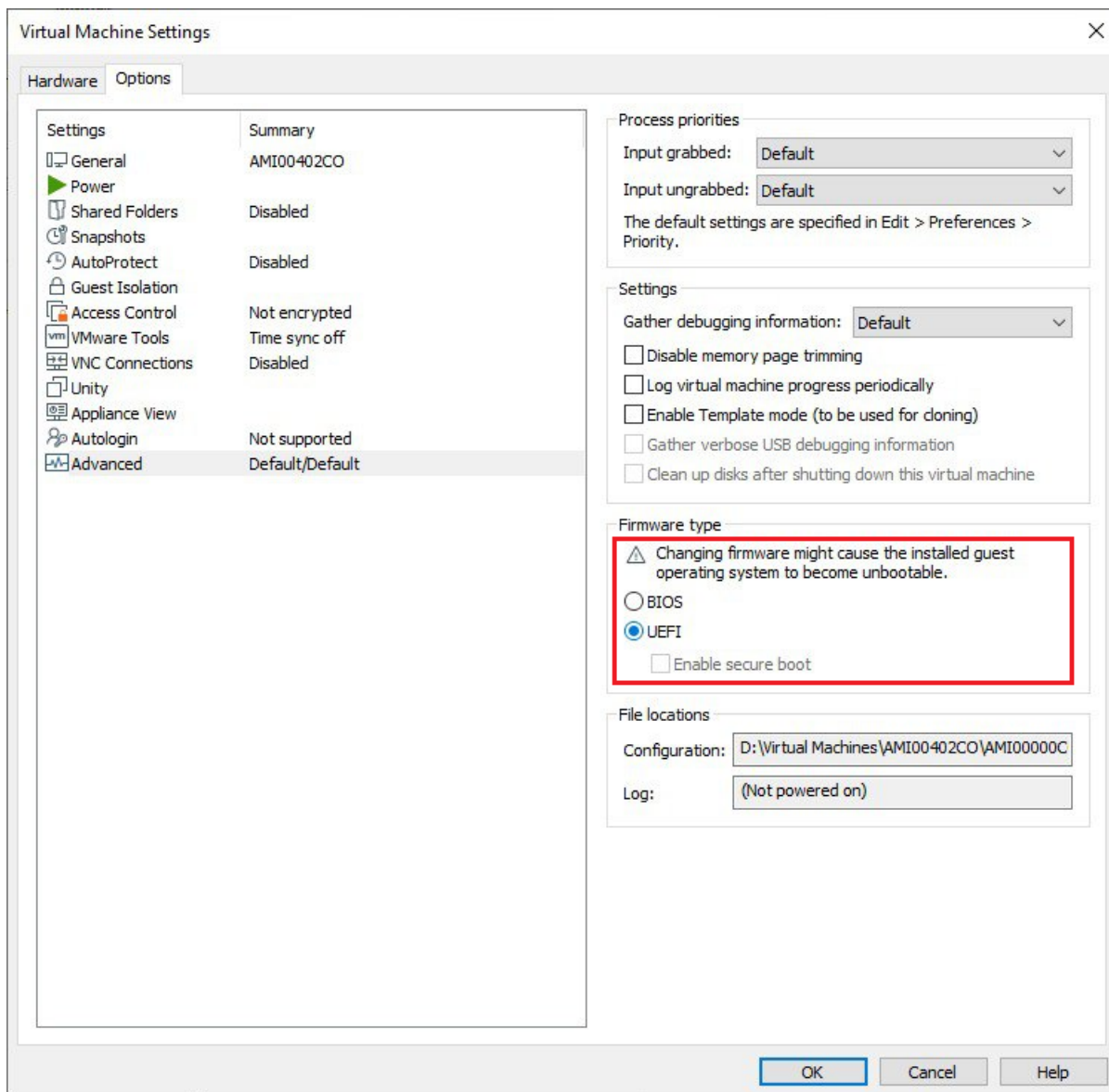


Рисунок 10 - Настройки интерфейса прошивки

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.

- 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. 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 захода в BIOS перейдите на вкладку Server Management и зайдите в пункт Console Redirection. В пункте Console Redirection требуется выставить 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;

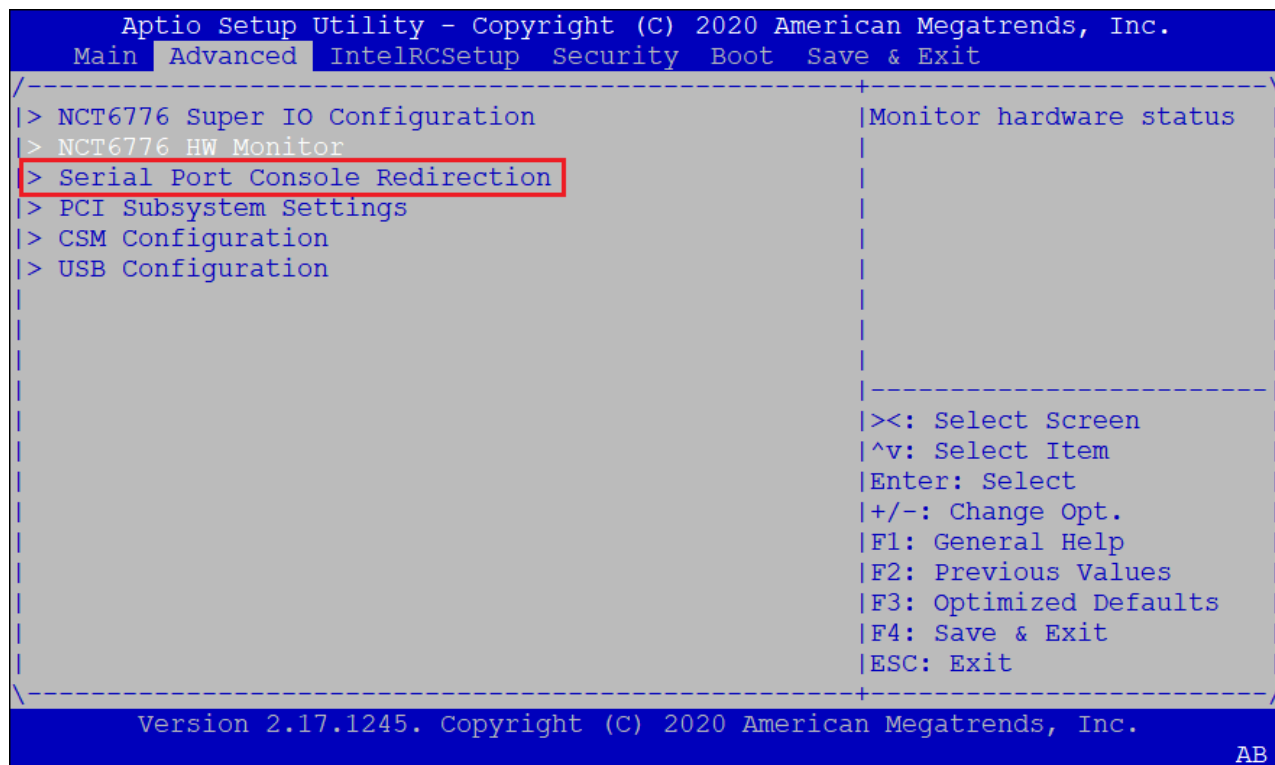
Build Rate — выбрать скорость передачи данных 115.2k;

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 11 - Настройки BIOS**

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



Рисунок 12 - 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.

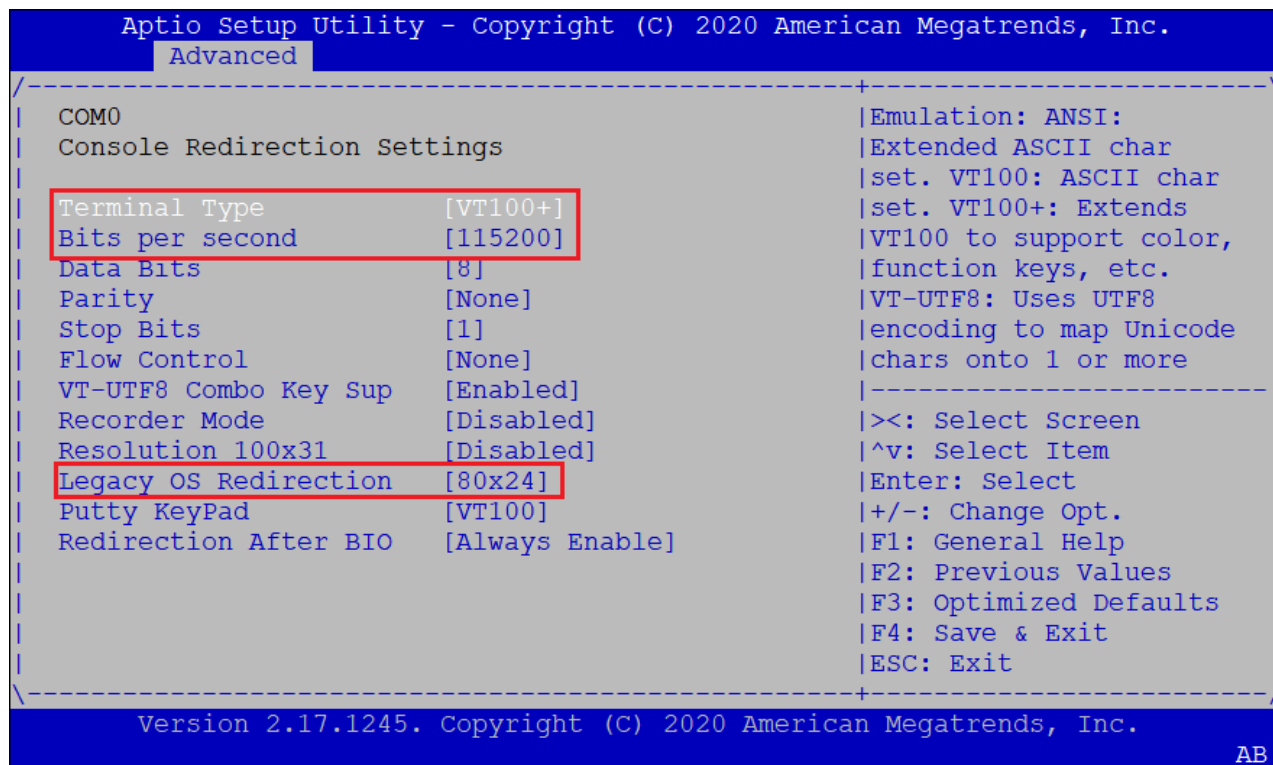


Рисунок 13 - Установка параметров

Сохраните внесенные в BIOS изменения и перезапустите ФПСУ-IP.

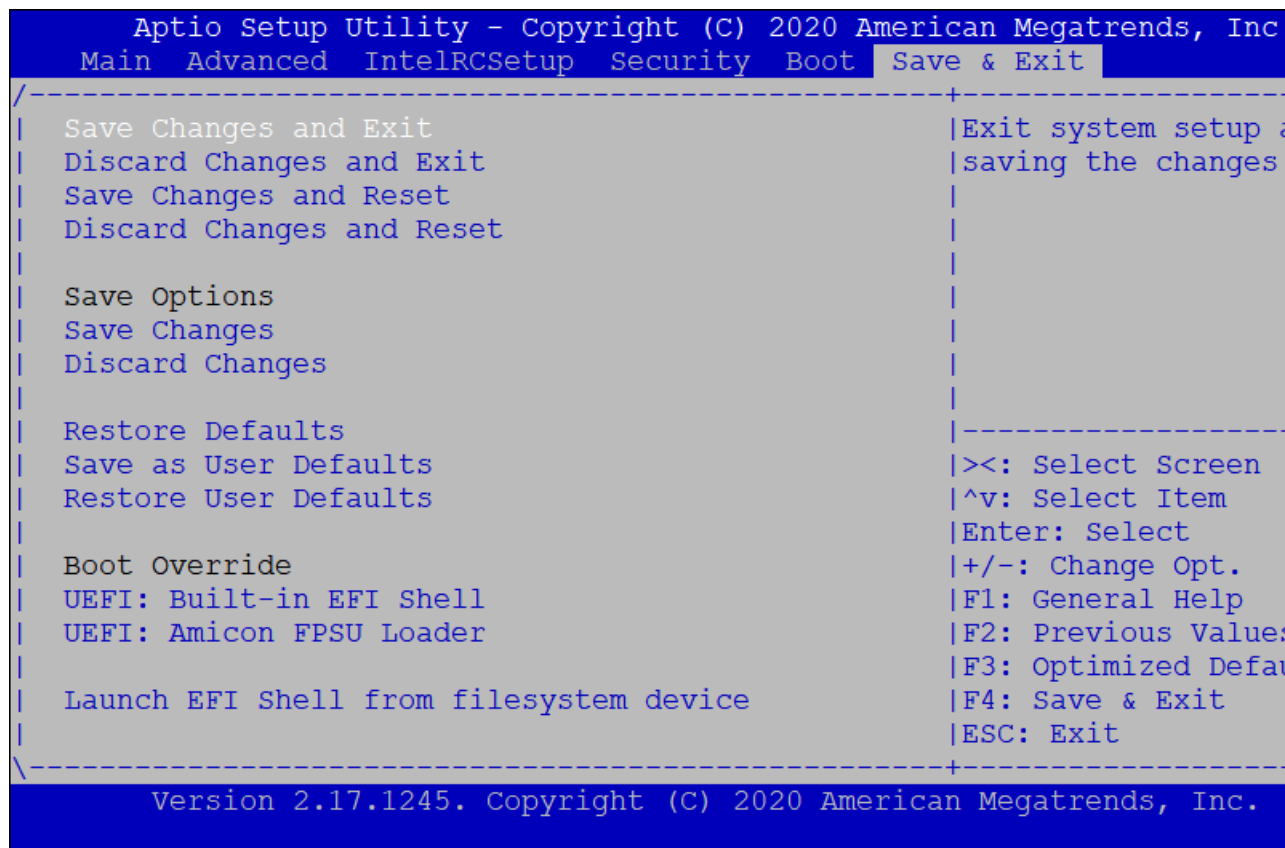


Рисунок 14 - Сохранение настроек BIOS

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.

Консоли

[Драйвер для подключения консоли к ПАК "ФПСУ-IP" для Windows XP \(776 Кб, 07.2012\)](#)

[Драйвер для подключения консоли к ПАК "ФПСУ-IP" для Windows Vista, 7, 8, 10, 11 \(1061 Кб, 11.2016\)](#)

[Драйвер для подключения консоли к ПАК "ФПСУ-IP" для Windows Vista, 7, 8, 10, 11 \(СН340\) \(84 Кб, 11.2016\)](#)

Рисунок 15 - 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.

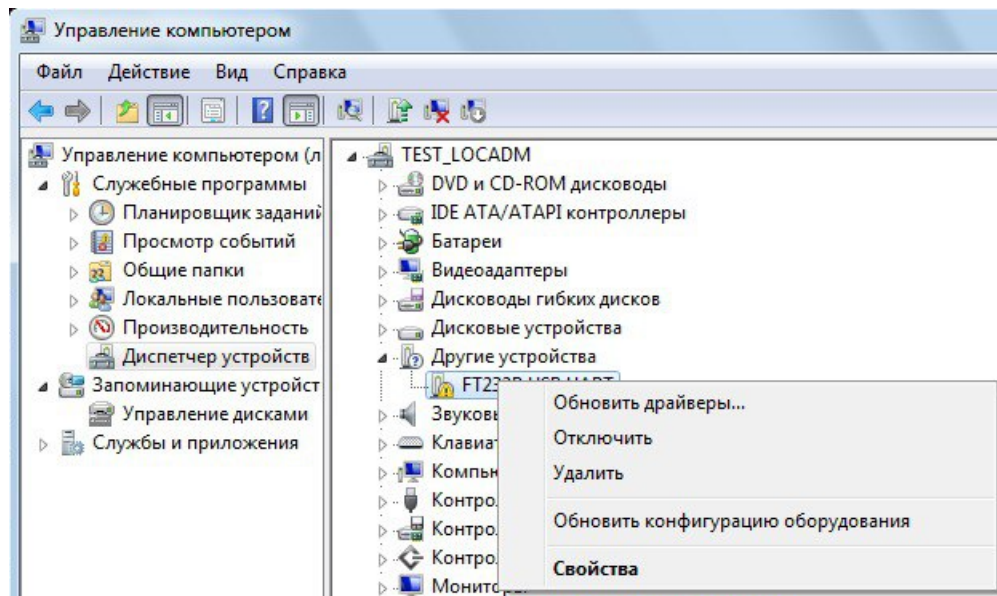


Рисунок 16 - Отображение консольного кабеля в диспетчере устройств

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.

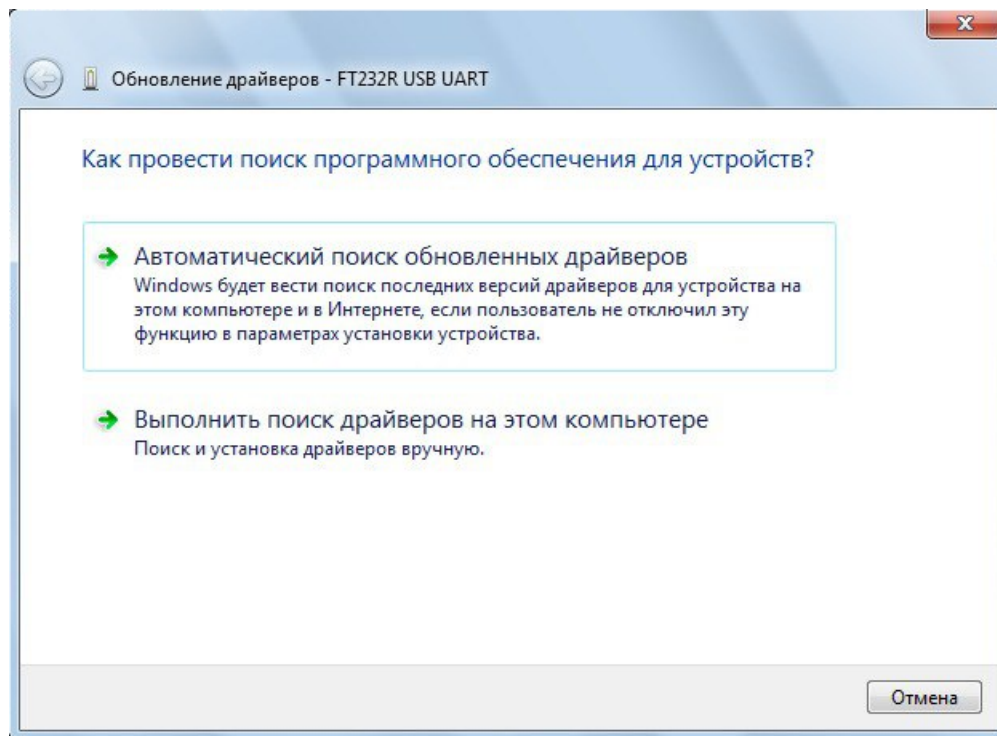


Рисунок 17 - Мастер установки драйвера

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

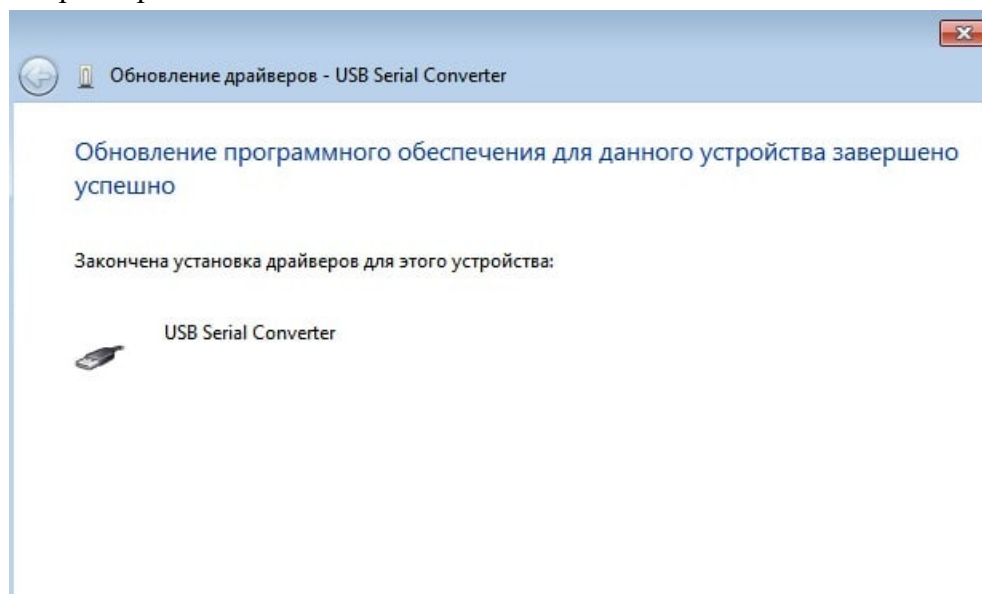


Рисунок 18 - Обновление драйвера консольного кабеля

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.

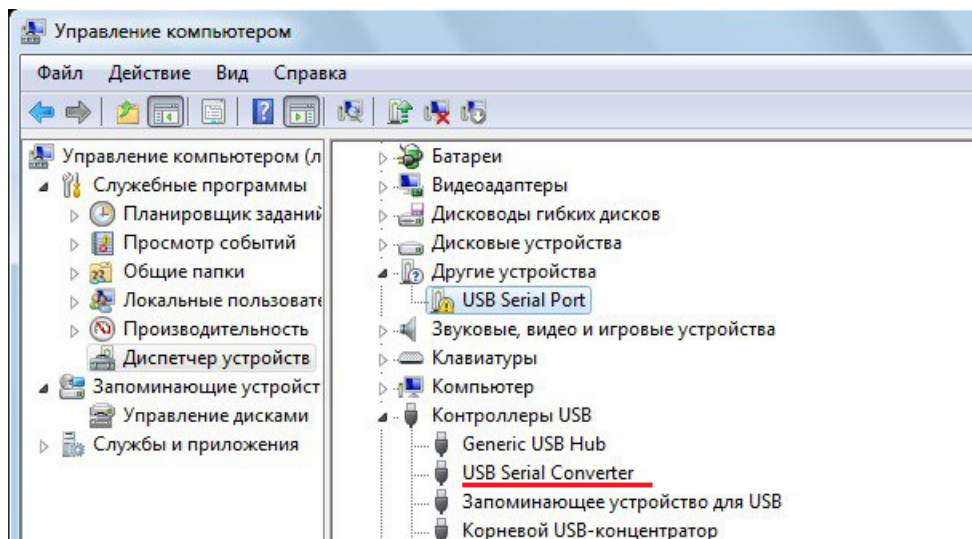


Рисунок 19 - Отображение консольного кабеля после установки драйвера

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

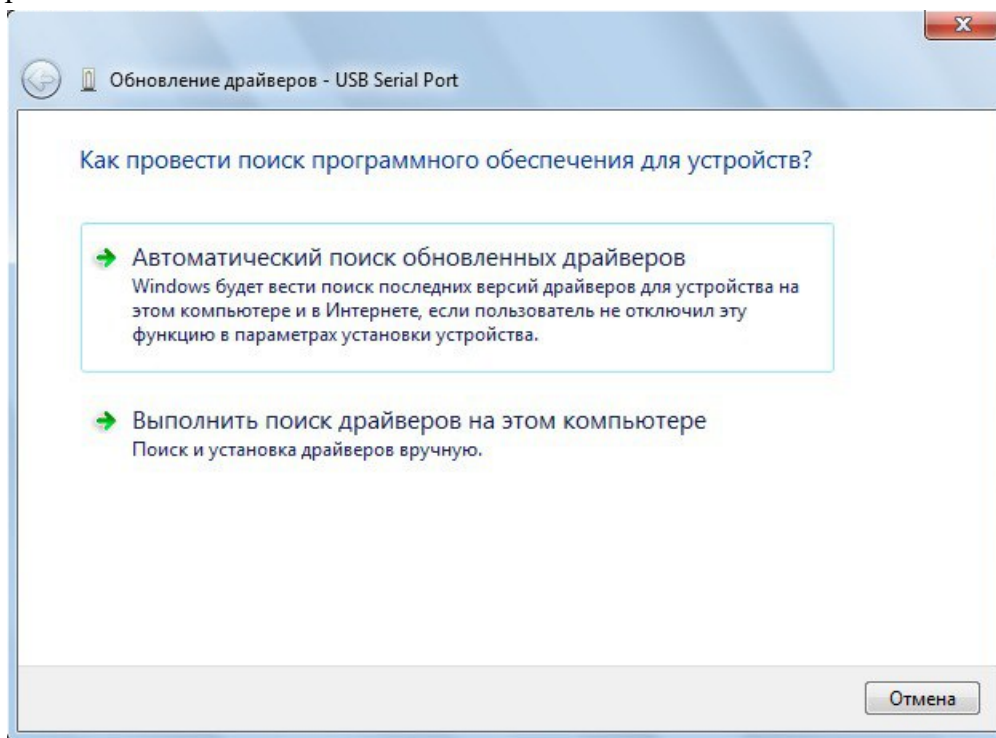


Рисунок 20 - Мастер установки драйвера

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

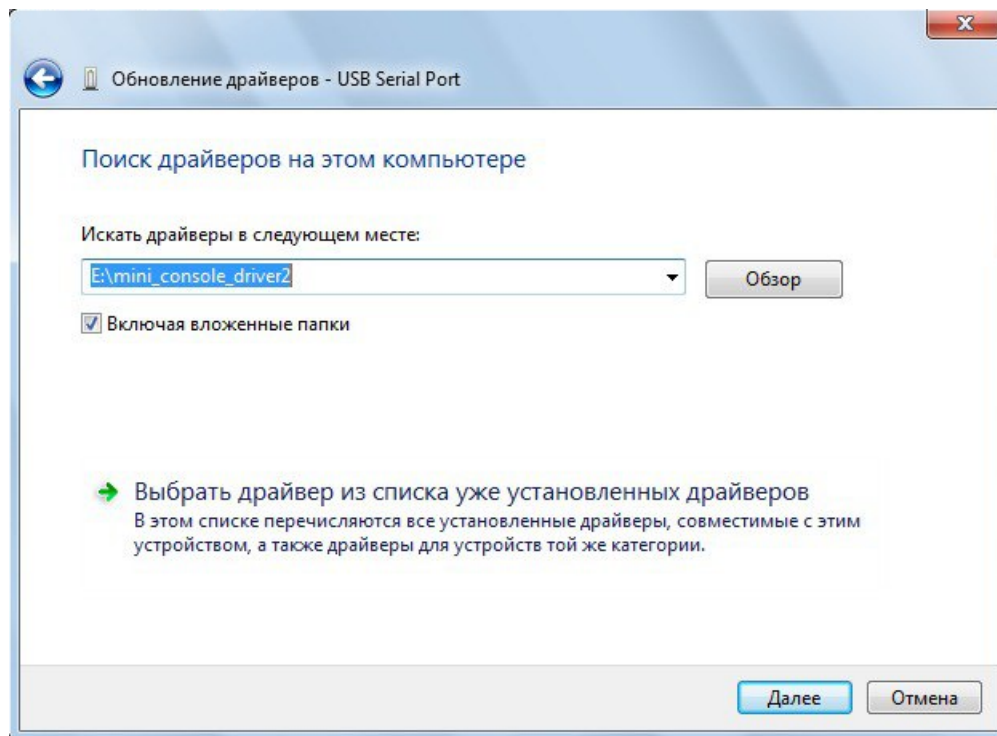


Рисунок 21 - Выбор каталога с драйвером

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

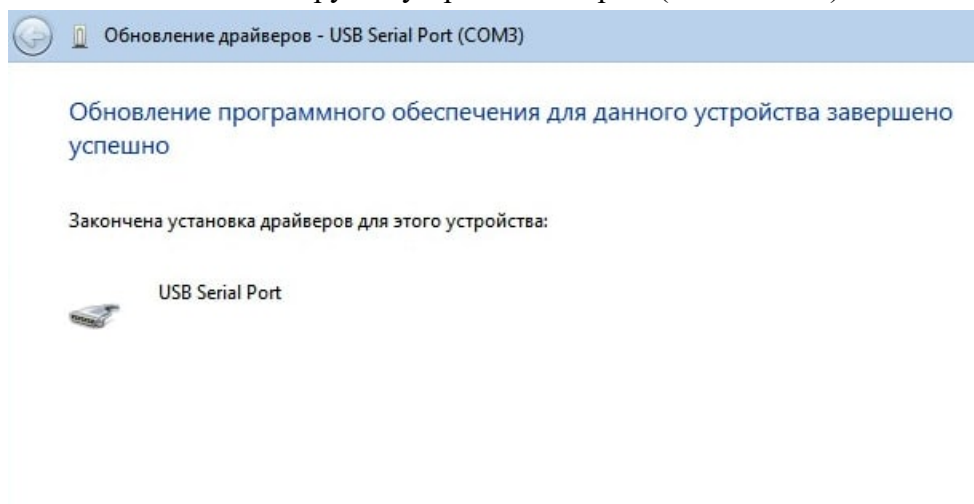


Рисунок 22 - Обновление драйвера консольного кабеля

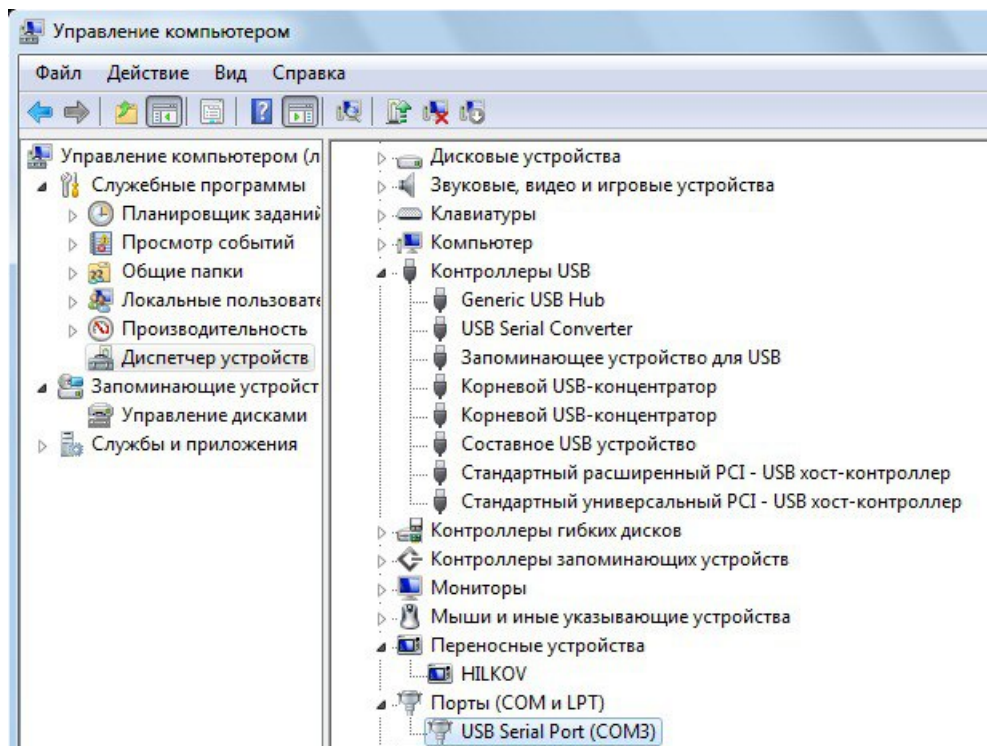


Рисунок 23 - Отображение консольного кабеля после повторной установки драйвера

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.

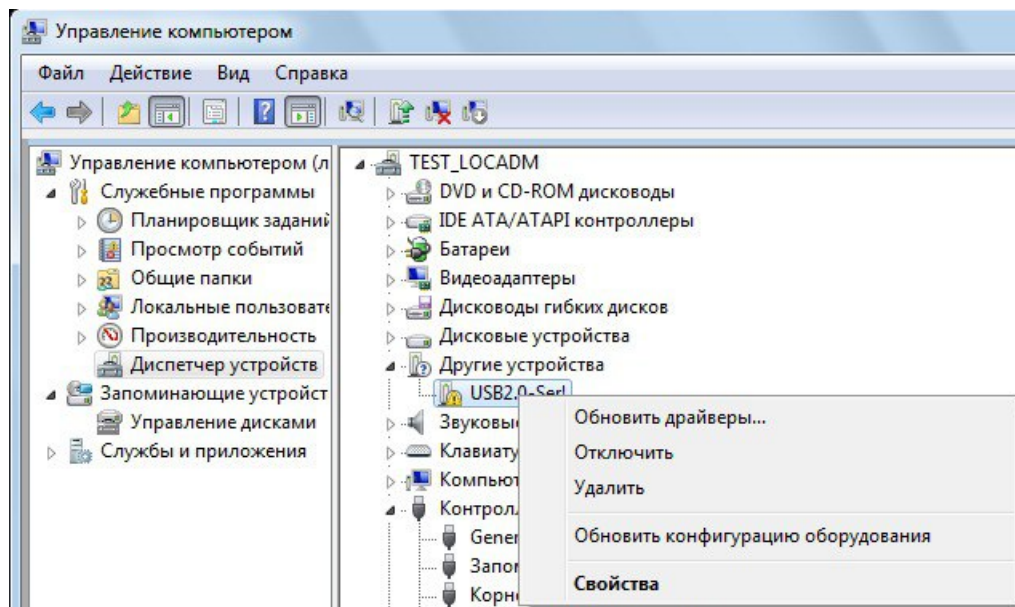


Рисунок 24 - Отображение консольного кабеля в диспетчере устройств

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.

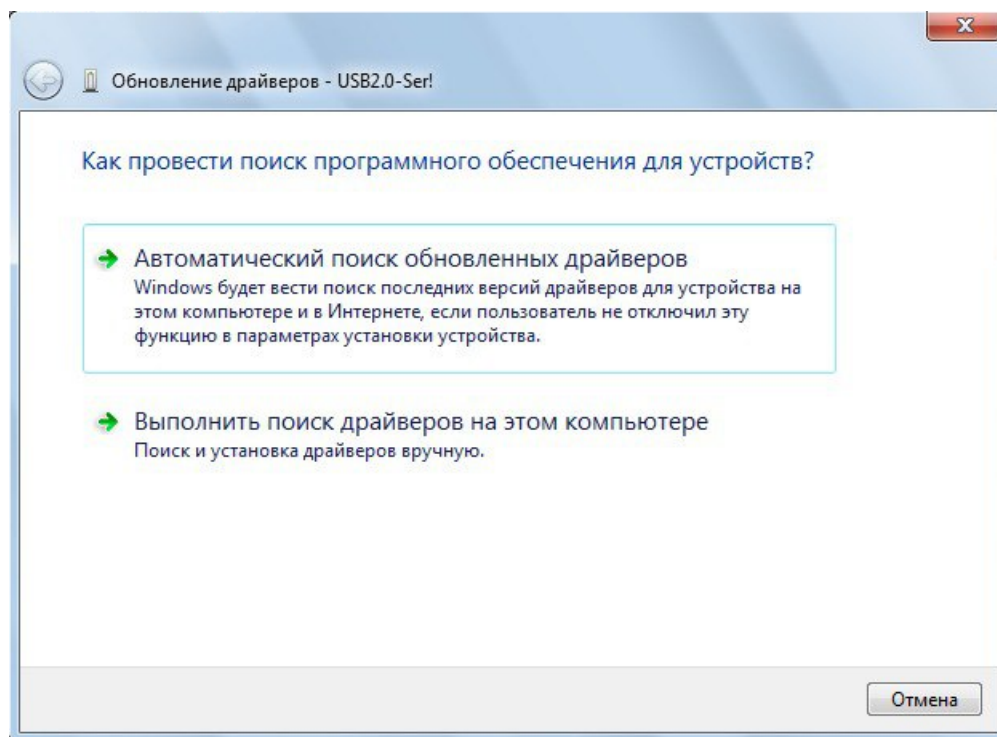


Рисунок 25 - Мастер установки драйвера

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

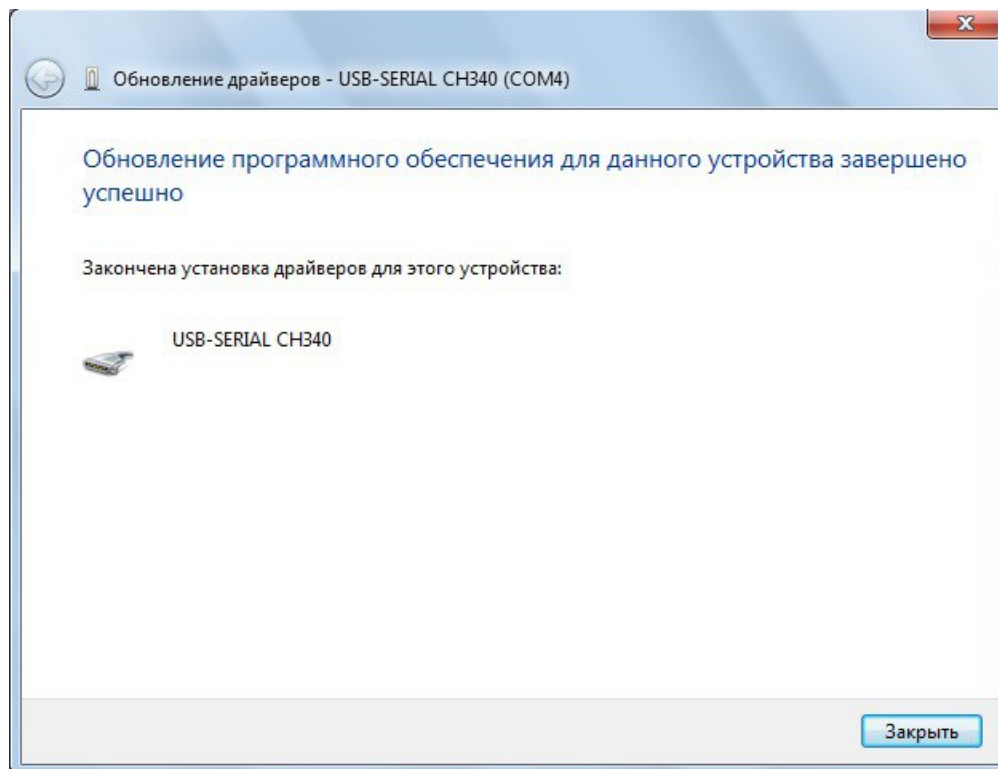


Рисунок 26 - Обновление драйвера консольного кабеля

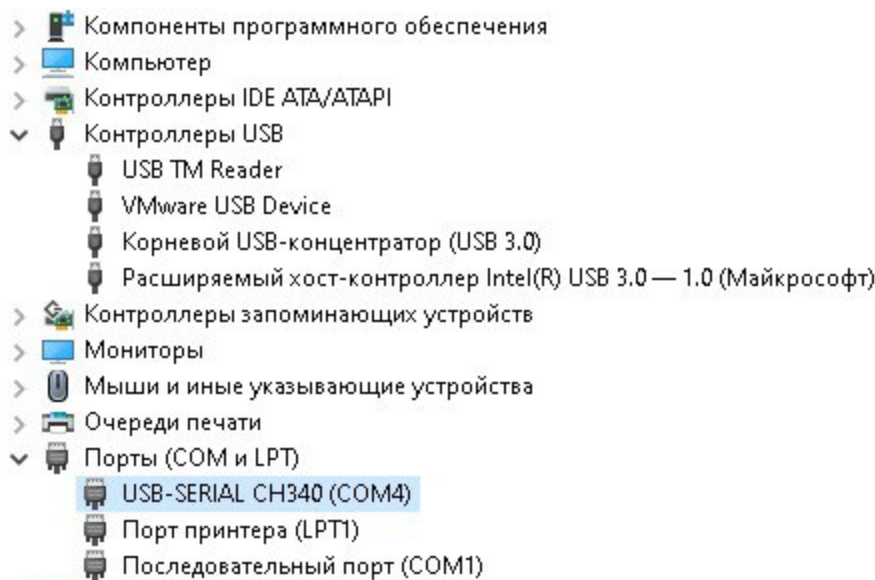


Рисунок 27 - Отображение консольного кабеля после установки драйвера

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.

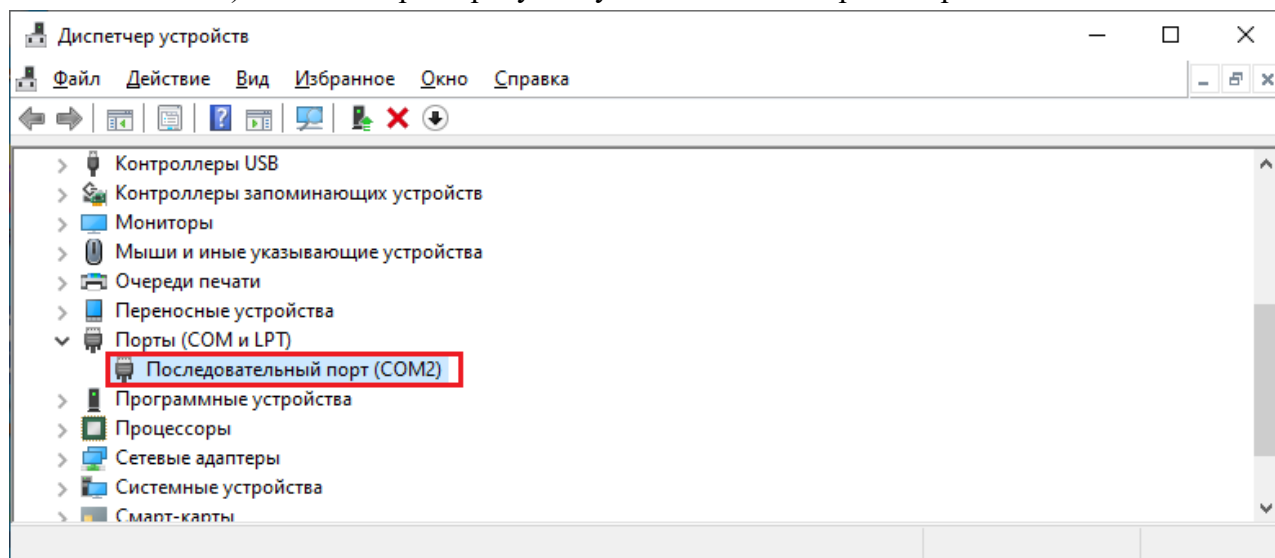
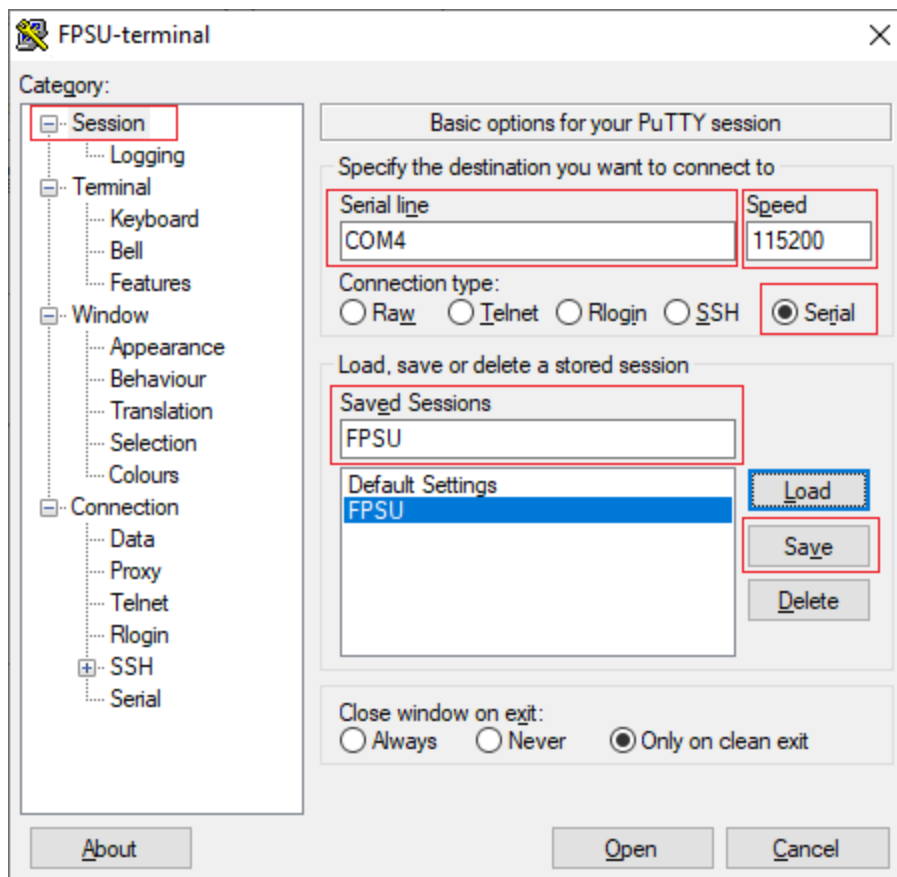


Рисунок 28 - COM порт консольного соединения в диспетчере устройств

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 29 - 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).

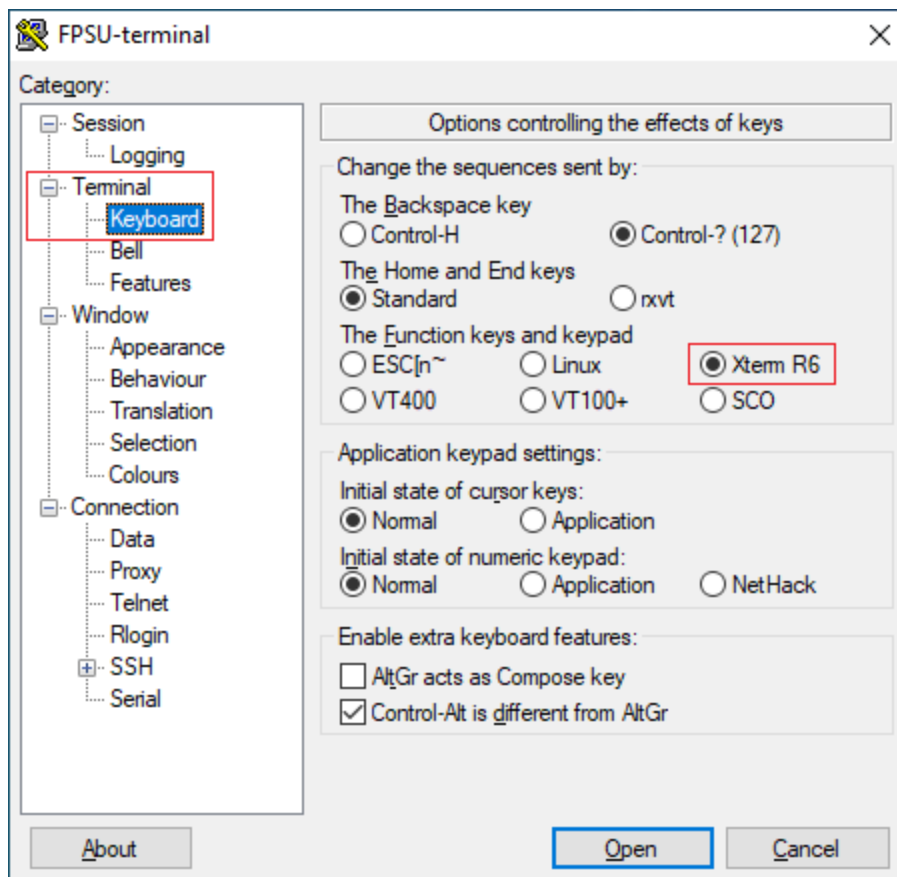


Рисунок 30 - Выбор типа клавиатуры

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

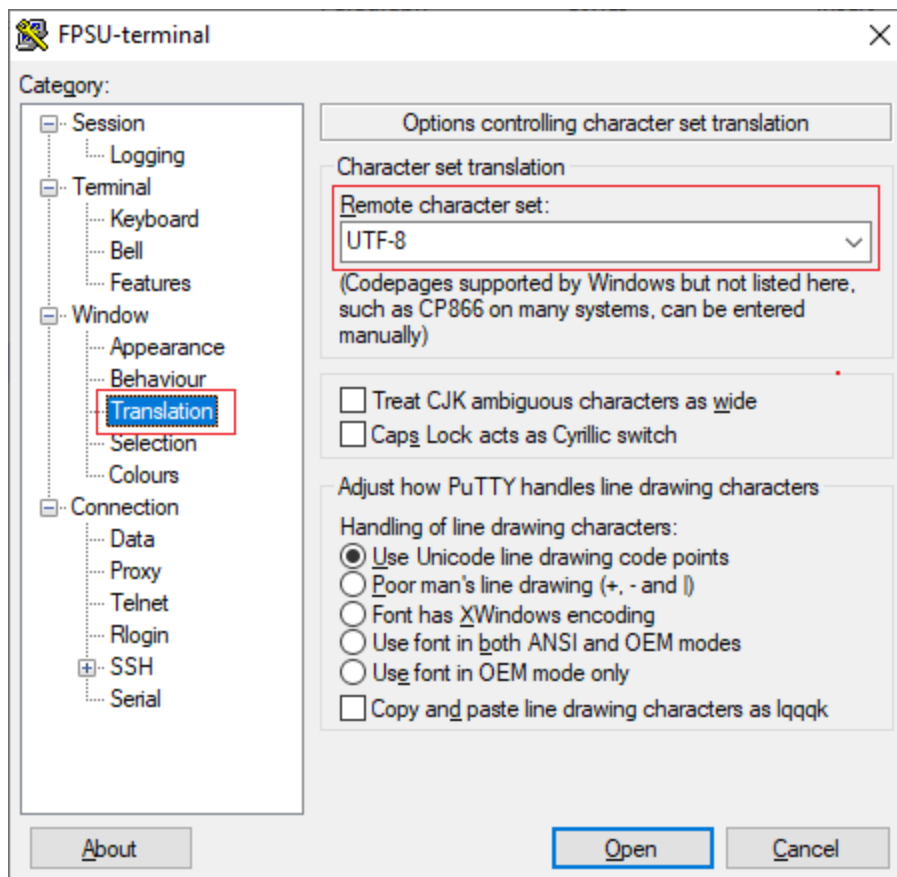


Рисунок 31 - Выбор кодировки

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

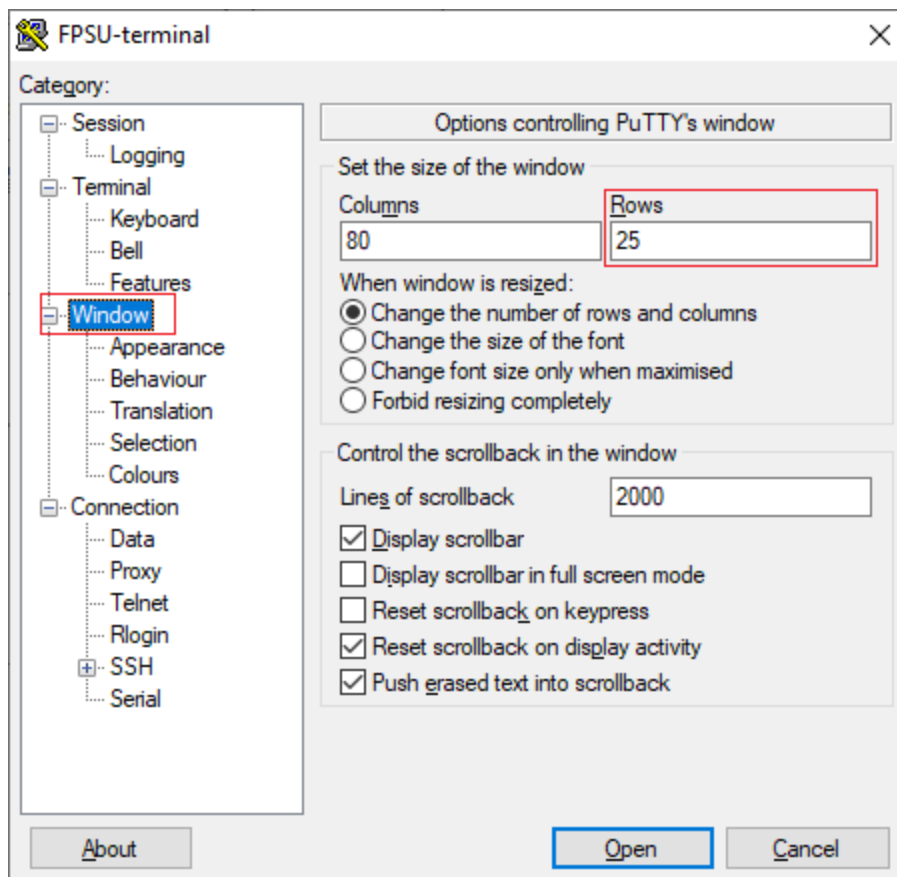


Рисунок 32 - Выбор количества строк

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

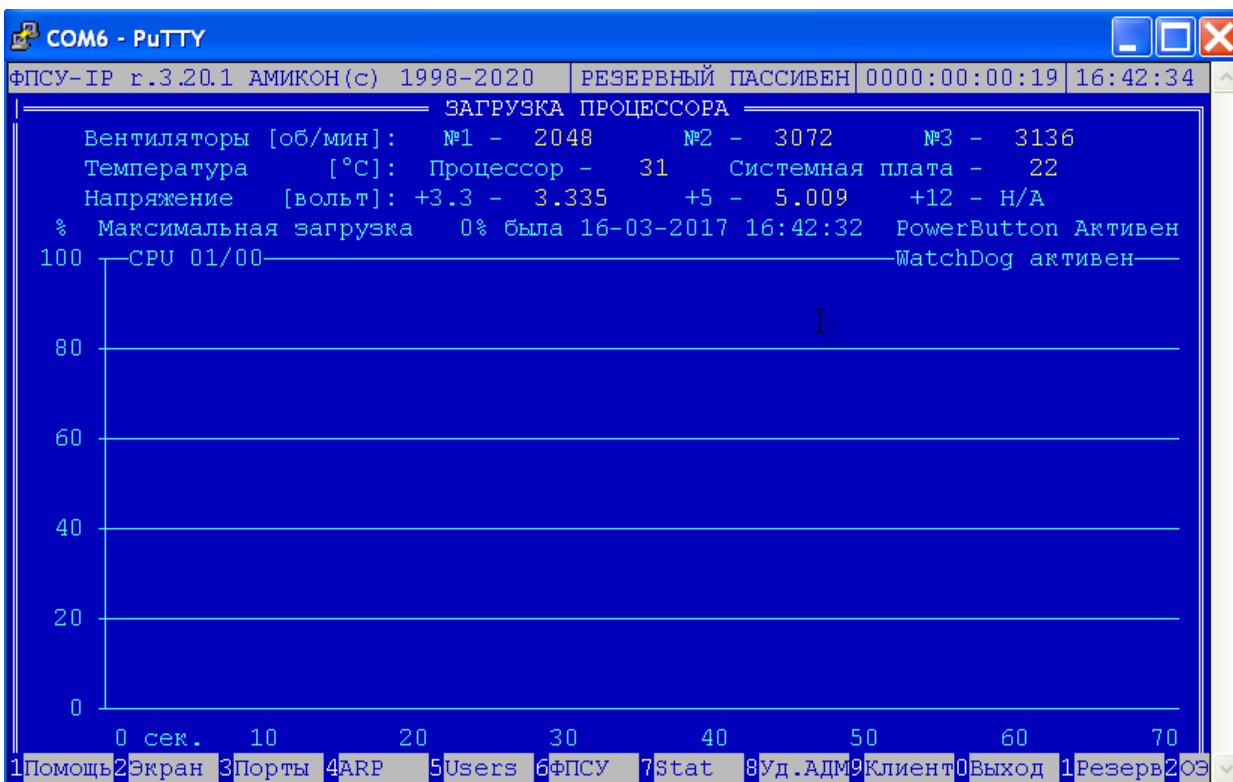


Рисунок 33 - Консольное подключение установлено

3. 10. Установка ПО ФПСУ-IP с дистрибутива

Для установки ФПСУ-IP с дистрибутива администратору потребуется 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 возможностью 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 загрузочного USB-носителя утилитой restore.exe

Первым этапом установки является создание загрузочного 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:

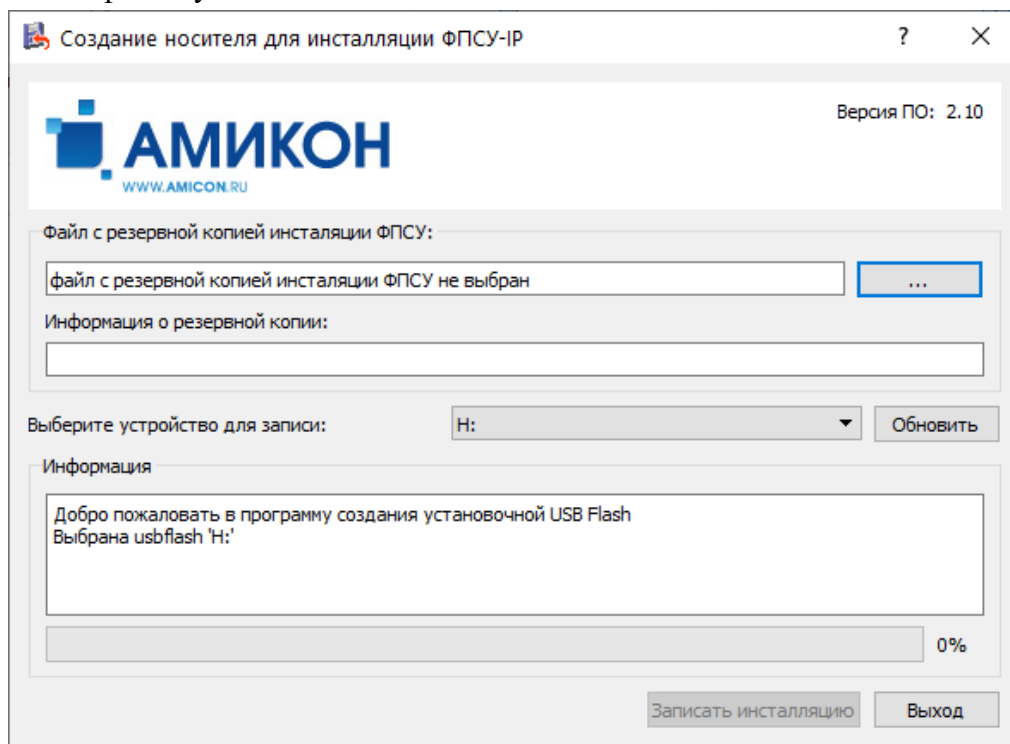


Рисунок 34 - Окно создания носителя

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

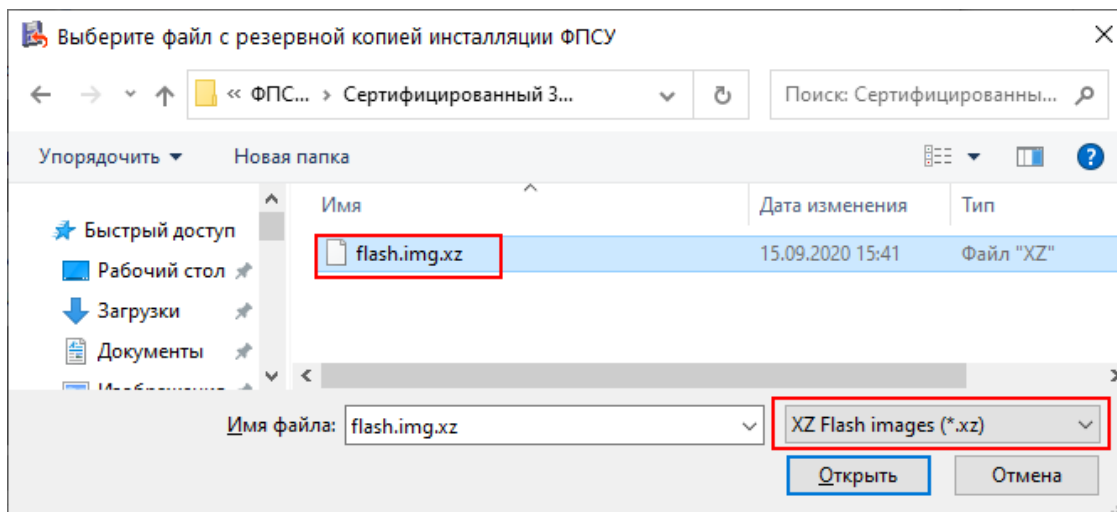


Рисунок 35 - Выбор места хранения эталонного дистрибутива

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

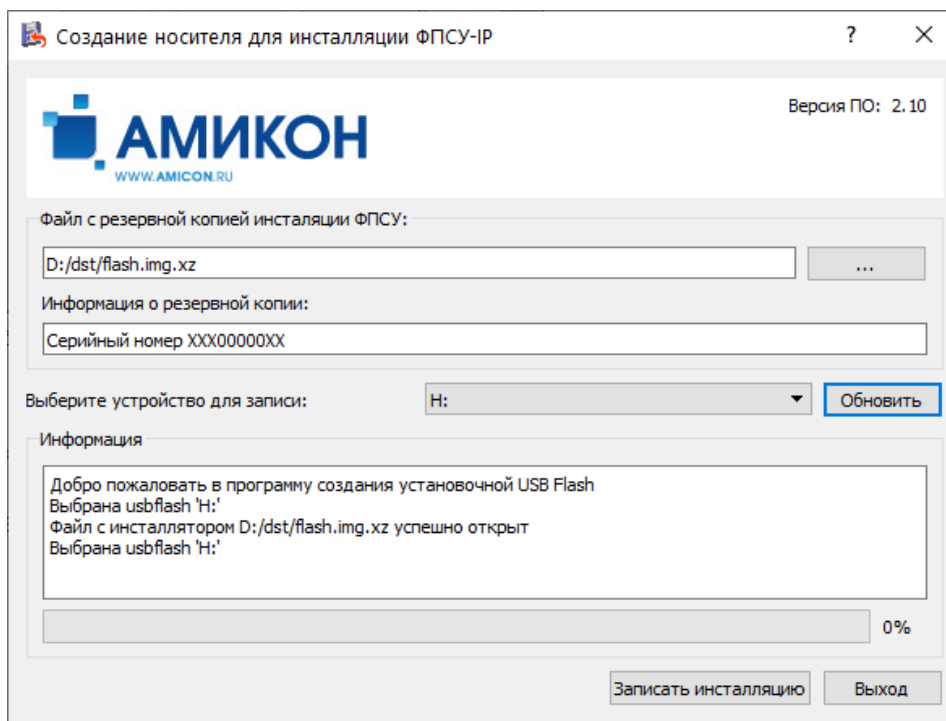


Рисунок 36 - Сообщение о необходимости выбора USB-носителя

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":

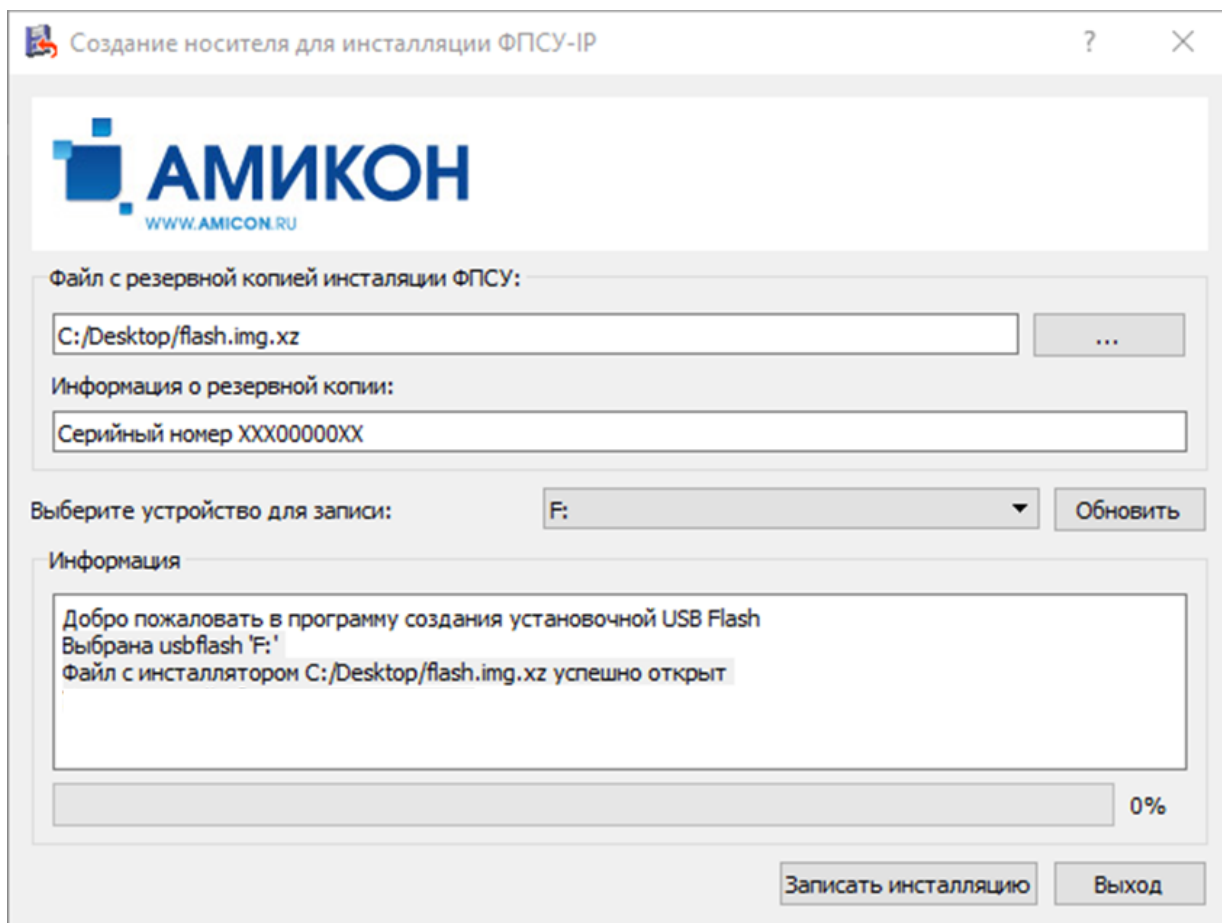


Рисунок 37 - Заполненное окно создания загрузочного носителя

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

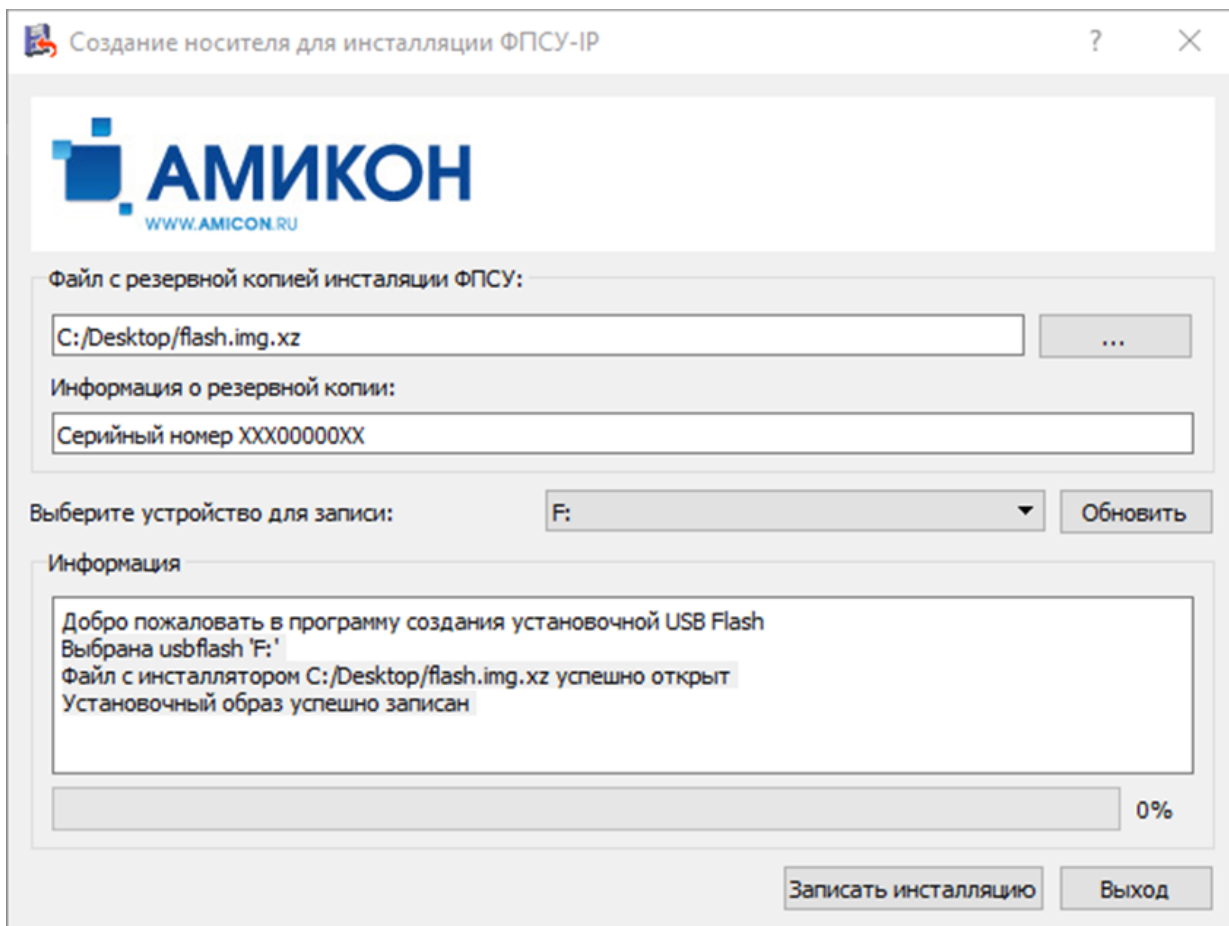


Рисунок 38 - Сообщение об успешном завершении процесса

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 "v" на клавиатуре, иначе загрузка с USB-носителя будет прервана:



Рисунок 39 - 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":

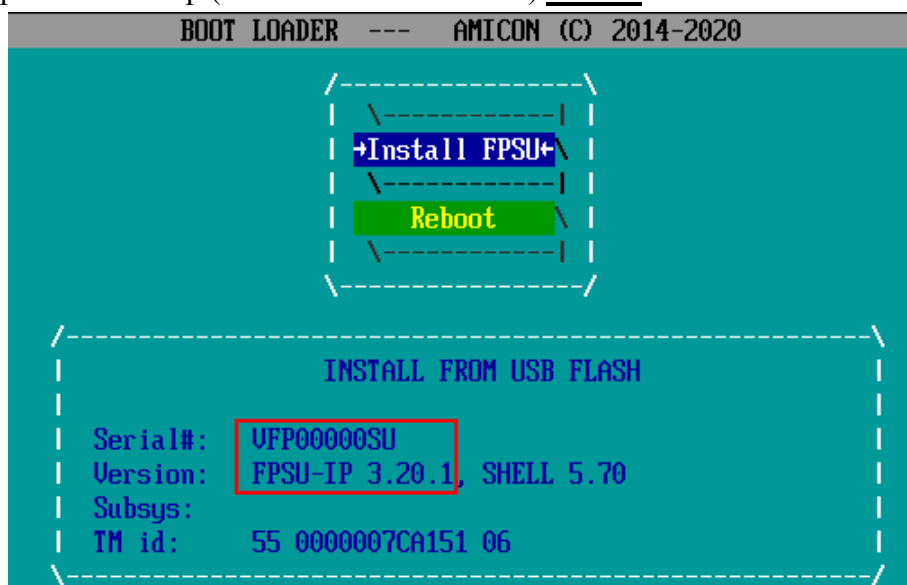


Рисунок 40 - Экран установки ФПСУ-IP

Если серийный номер не совпадает с ожидаемым, следует прекратить установку и заново создать установочный USB-носитель (см. ["Создание загрузочного 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":

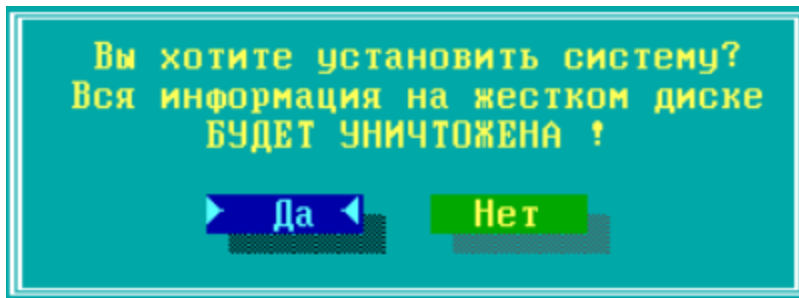


Рисунок 41 - Очистка ПЗУ ФПСУ-IP

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:

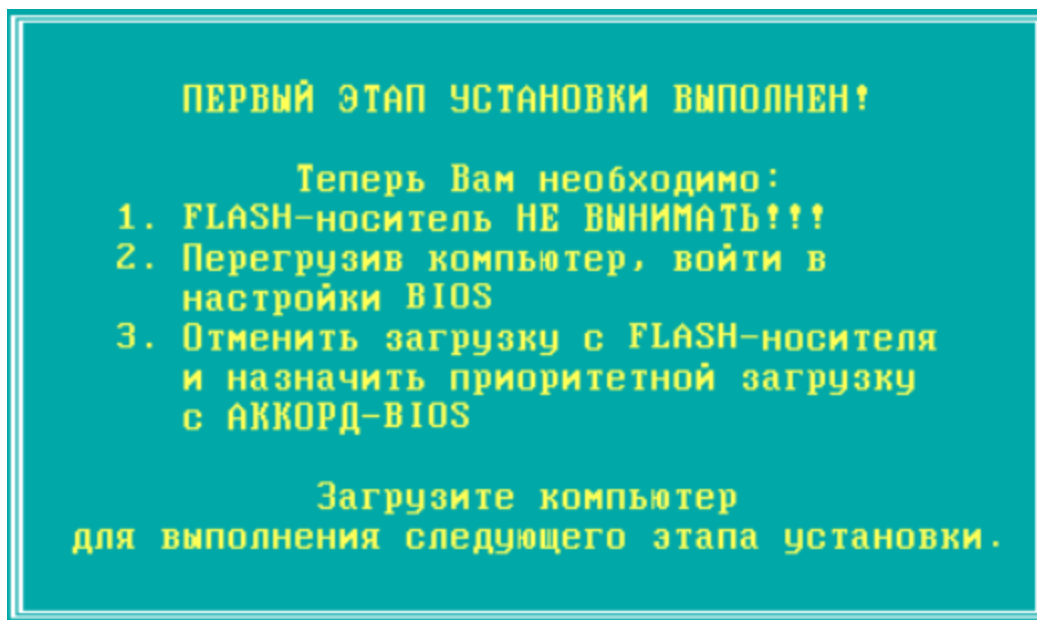


Рисунок 42 - Завершение первого этапа установки

5. После перезагрузки и запуска операционной системы ФПСУ-IP, начнется второй этап установки программного обеспечения. Для продолжения потребуется подтвердить права пользователя класса "Главный администратор", приложив ТМ-идентификатор из инсталляционного комплекта к ТМ-считывателю ФПСУ-IP (или подключив USB ТМ-идентификатор к USB-порту ФПСУ-IP):



Рисунок 43 - 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>.

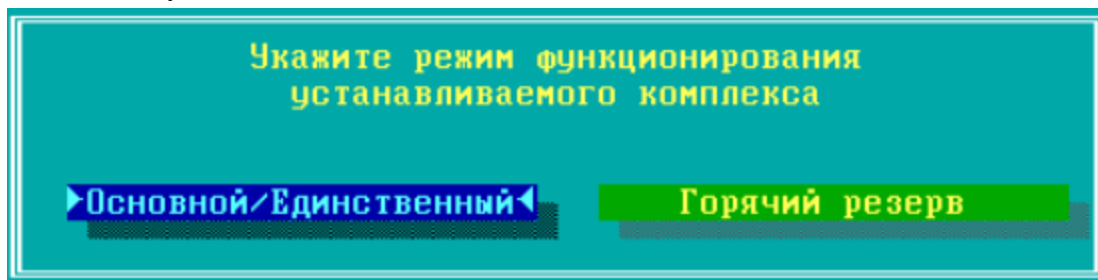


Рисунок 44 - Выбор режима функционирования ФПСУ-IP

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

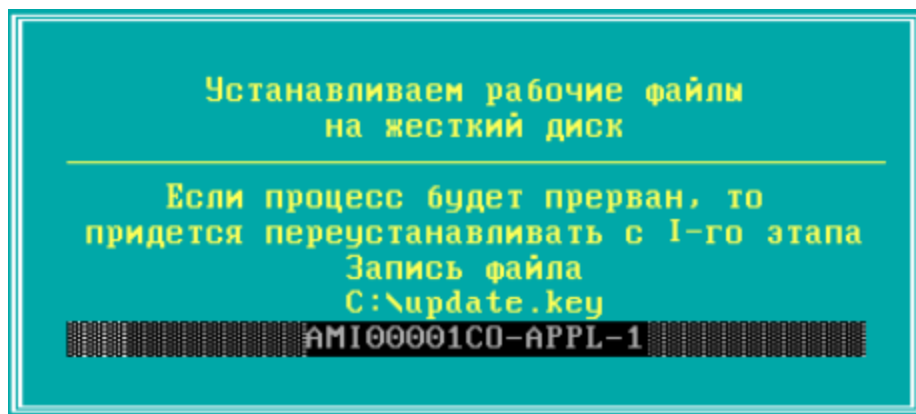


Рисунок 45 - Копирование системных файлов

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"](#)).

Обратите 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".

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.

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:

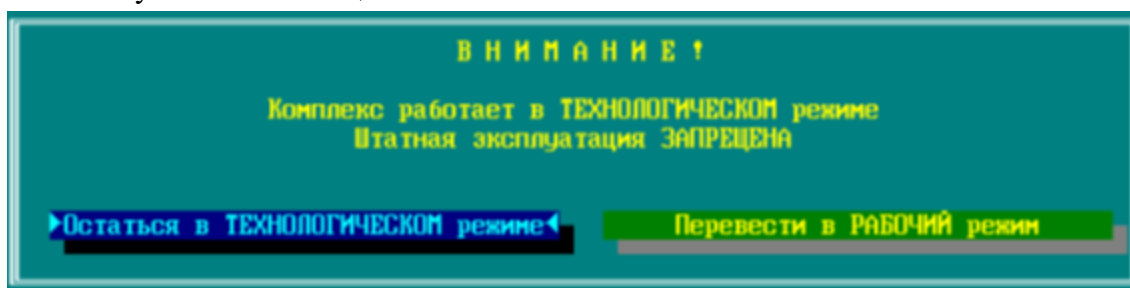


Рисунок 46 - Оповещение о работе в технологическом режиме

Для выхода из технологического режима в штатный, рабочий режим, выберите и нажмите кнопку <Перевести в РАБОЧИЙ режим>. 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.

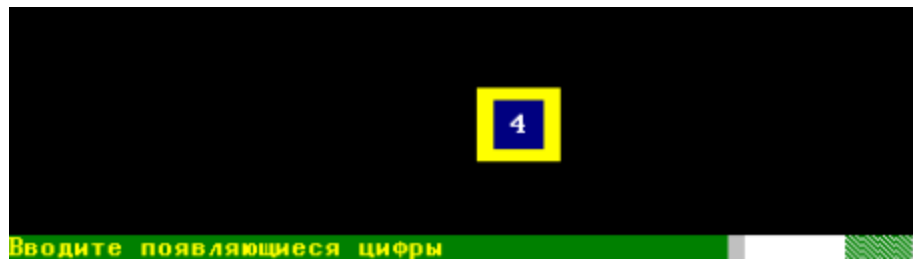


Рисунок 47 - Программно-клавиатурный датчик случайных чисел

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 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 TM-идентификатор (или подключите USB TM-идентификатор к USB-порту ФПСУ-IP) пользователя 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 TM-идентификатора) на запрашиваемые действия (права допущенных лиц различных классов см. раздел [Общие сведения](#)).

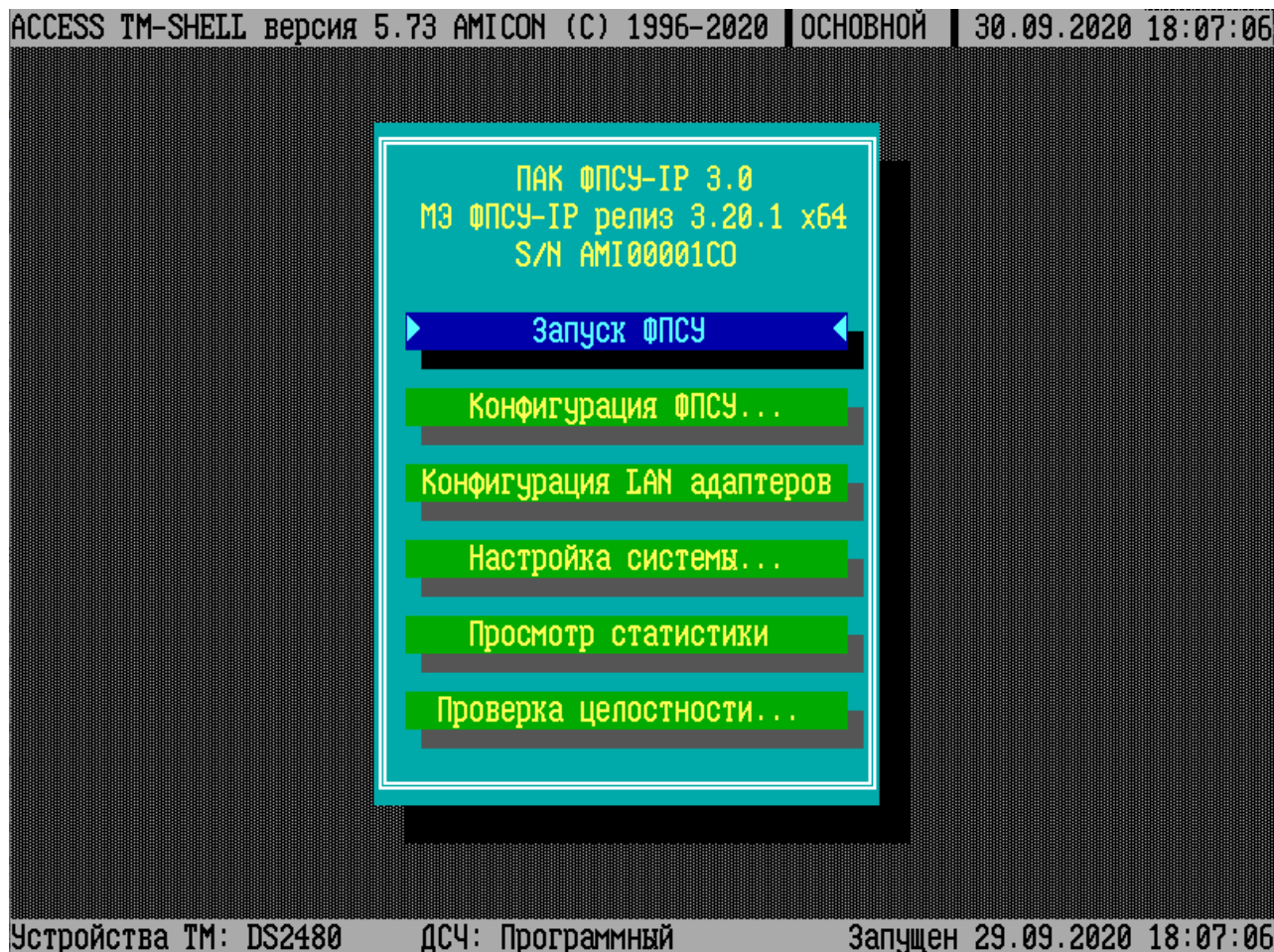


Рисунок 48 - Главное меню ФПСУ-IP

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.

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.

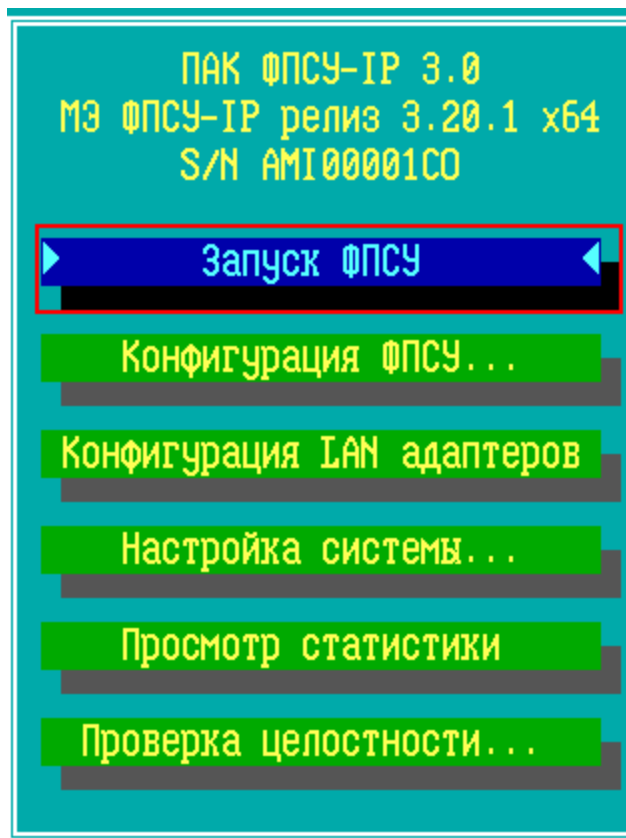


Рисунок 49 - Запуск ФПСУ из главного меню

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, и информации о версии ПО.

F2 – вывод на экран окна настройки параметров отображения экрана;

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

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

F5 – переход на окно отображения подсистемы фильтрации пакетов абонентов;

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

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

F8 – переход на окно отображения взаимодействия с удаленными администраторами;

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

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

F11 – переход на окно отображения состояния "горячего" резервирования;

F12 – переход на окно 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. На

экране ниже отображаются ("н/а" – не активен или отсутствует):

- текущая частота вращения вентиляторов в оборотах в минуту;
- текущая температура процессора и системной платы в градусах Цельсия;
- напряжение, выдаваемое блоком питания;
- загрузка (процент использования) процессоров;
- максимальное с момента последнего запуска режима фильтрации значение загрузки процессоров;
- индикация активности режима управления кнопкой питания.

Строка "PowerButton 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.

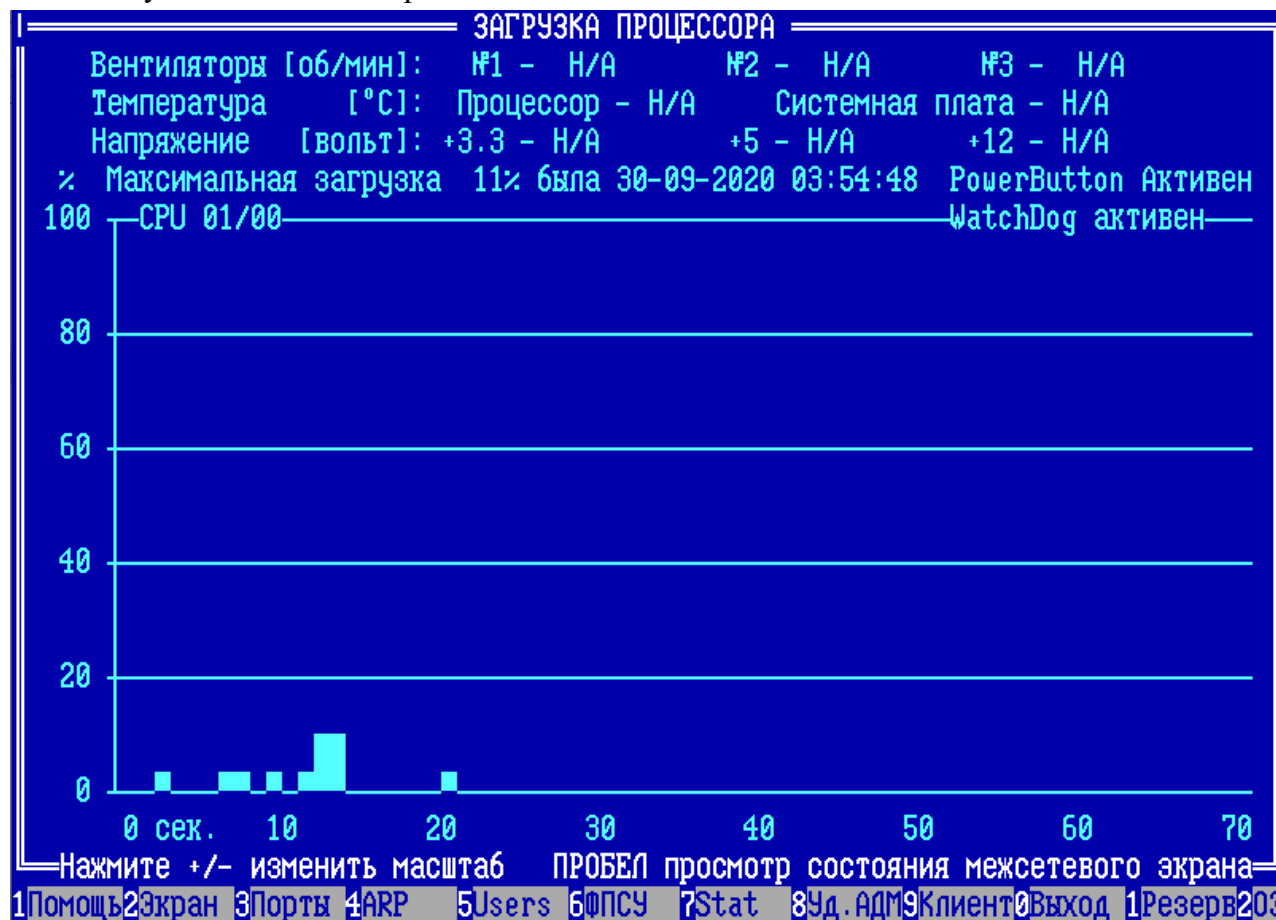


Рисунок 50 - Параметры аппаратного состояния ФПСУ-IP

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 "Просмотр ежедневной статистики".

По нажатию клавиши пробел на экране "Загрузка процессора" осуществляется переход в окно "Использование межсетевого экрана":

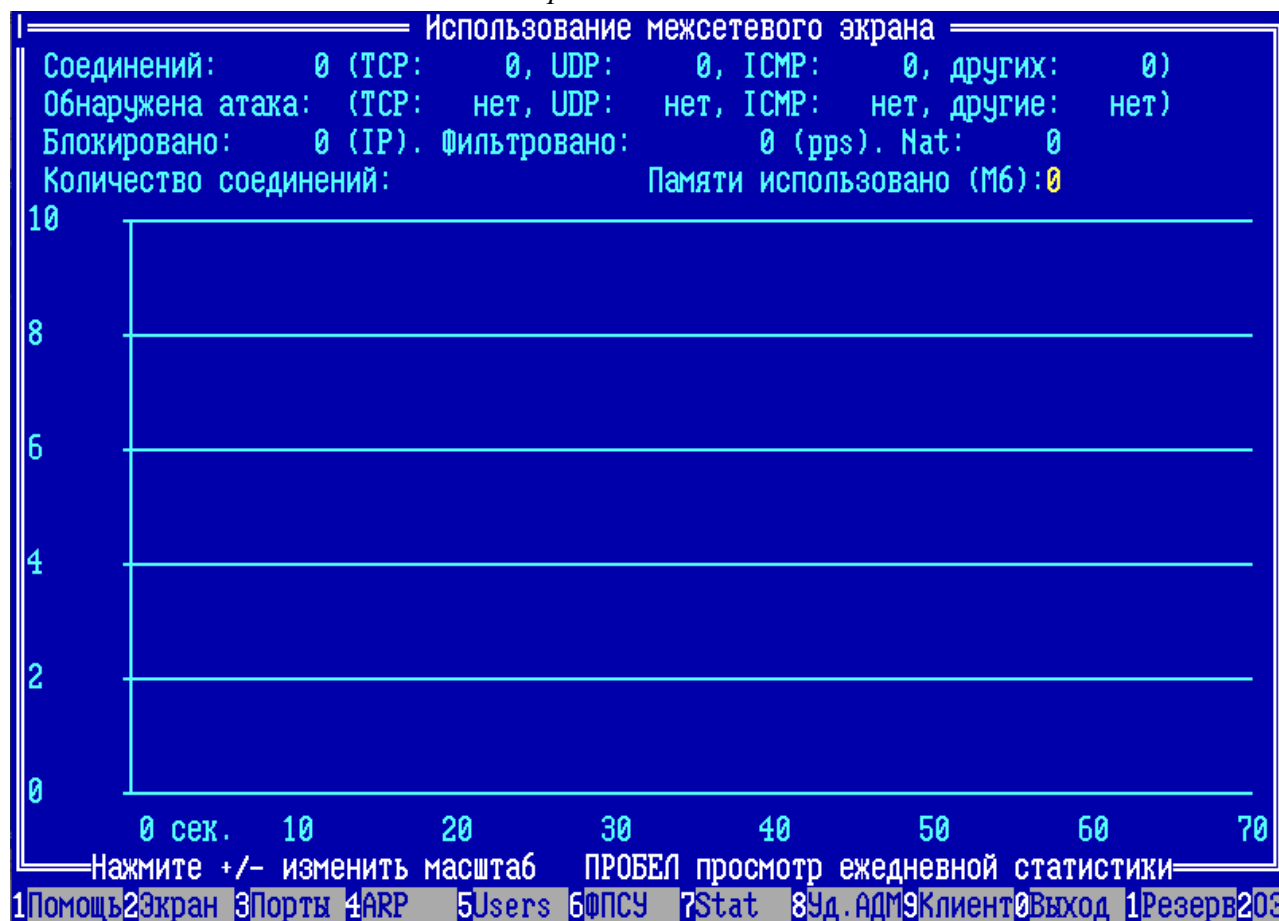


Рисунок 51 - Окно просмотра состояния ФПСУ-IP

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

ПРОСМОТР ЕЖЕДНЕВНОЙ СТАТИСТИКИ		
11-08-2020		
	IP Порт 1	IP Порт 2
Принято:		
Кбайт данных	0	0
Кбайт после туннелирования	0	0
IP пакетов	0	0
Передано:		
Кбайт данных	0	0
Кбайт после туннелирования	0	0
IP пакетов	0	0
Отказов в передаче пакета:	0	0
Нарушений правил фильтрации для непосредственной передачи:		
в режиме ретрансляции	0	0
в режиме работы через ФПСУ	0	0
Нарушений правил фильтрации для широковещательной передачи:		
в режиме ретрансляции	0	0
в режиме работы через ФПСУ	0	0
Нажмите ПРОБЕЛ для просмотра списка процессов		
1Помощь	2Экран	3Порты
4ARP	5Users	6ФПСУ
7Stat	8Уд.Адм	9Клиент
0Выход	1Резерв	203

Рисунок 52 - Окно просмотра ежедневной статистики

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 "Просмотр ежедневной статистики" осуществляется переход в окно просмотра списка процессов.

ПРОСМОТР СПИСКА ПРОЦЕССОВ									
	Total	Used	Free	Buffers			Shared		
Mem (KB):	2358700	780188	1578512	2360			594048		
Tasks :	7								
PID	LXC	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
2782	http-proxy	2276	76	64	S	0.0	0.0	00:00.04	init
2809	http-proxy	2276	72	12	S	0.0	0.0	00:00.00	/bin/syslo
2814	http-proxy	2276	4	0	S	0.0	0.0	00:00.00	/bin/getty
2815	http-proxy	2276	80	12	S	0.0	0.0	00:00.00	init
2819	http-proxy	2276	4	0	S	0.0	0.0	00:00.00	/bin/sh -c
2820	http-proxy	2276	4	0	S	0.0	0.0	00:00.00	{exe} ash
2824	http-proxy	141M	6936	1412	S	0.0	0.3	00:00.07	./3proxy .
Нажмите ПРОБЕЛ для просмотра загрузки процессора									
1Помощь 2Экран 3Порты 4ARP 5Users 6ФПСУ 7Stat 8Уд. АДМ 9Клиент 0Выход 1Резерв 203									

Рисунок 53 - Окно просмотра списка процессов

В окне отображаются сведения о процессах, запущенных подсистемой http-прокси и другими, опциональными, дополнениями к ПО ФПСУ-IP.

По нажатию клавиши пробел на экране "Просмотр списка 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 установки параметров работы с экраном

Вызов окна установки параметров экрана осуществляется по нажатию клавиши <F2>.

Режим предназначен для изменения интервала гашения экрана, установленного при конфигурировании ФПСУ-IP (он отображается в верхней строке окна в скобках), немедленного гашения экрана.

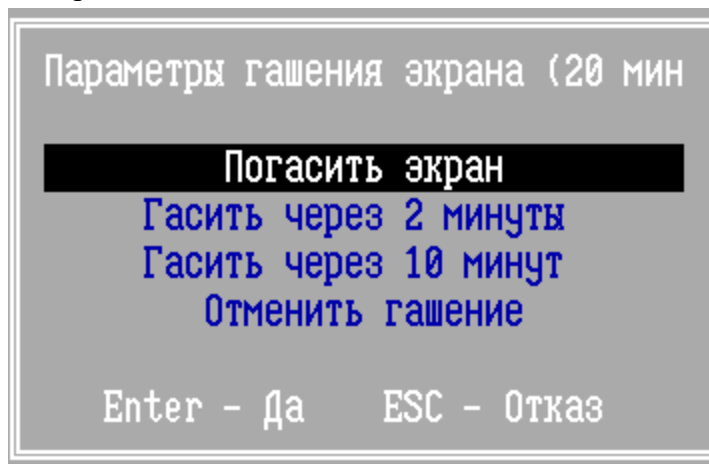


Рисунок 54 - Параметры экрана

Гашение экрана предусмотрено с целью экономии ресурсов компьютера, затрачиваемых на вывод информации на экран монитора, задерживающий работу подсистемы фильтрации. Если наблюдение за работой ФПСУ-IP не производится, экран рекомендуется гасить.

5. 4. 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 передачи данных по порту в пакетах в секунду, "pps", и в "Мбит/с".

LAN карта #1			S/N AMI00003C0	LAN карта #2				
Node Address	026d1892bcc0			Node Address	026d1892bcc1			
Slot Number	0005/00/1			Slot Number	0005/00/0			
Speed	1000 MBit Full Duplex			Speed	1000 MBit Full Duplex			
IP Addr/Mask	192.168.010.001/24			IP Addr/Mask	192.168.001.001/24			
MTU	9000			MTU	15854			
Прием	2 pps	0.001 Mbps		Прием	3 pps	0.001 Mbps		
Передача	2 pps	0.001 Mbps		Передача	3 pps	0.001 Mbps		
	Передано	Принято	Отвергнуто		Передано	Принято	Отвергнуто	
ARP	20	15	3	ARP	202	182	0	
IP	12883	12884	0	IP	12742	12742	0	
Ошибки приема:	ARP	IP		Ошибки приема:	ARP	IP		
Пропущено	0	0		Пропущено	0	0		
Ошибочных	0	0		Ошибочных	0	0		
Прочих пакетов	0			Прочих пакетов	0			
Память:	Минимум	Максимум	Исп-вано	Память:	Минимум	Максимум	Исп-вано	
ARP	1233920	20186913	112	ARP	1233920	20186913	112	
Прием	77120000	19557632	38992	Прием	77120000	19557632	38992	
Передача	46272000	21211072	0	Передача	46272000	21211072	0	
Всего памяти доступно	838795264		Свободно:	Всего	834363676		Общей	469444636
Del-обнулить								

Рисунок 55 - 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 знак "*" - соответствующий счетчик превысил значение 4294967296 и начал отсчет с нуля. Нажатие клавиши сбрасывает накопленную с момента запуска статистику в нулевые значения.

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

5. 5. 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.

```

LAN карта #1
4:000427150081 010.010.002.245 889A
11:000427150081 010.010.011.245 880A
000427150081 010.010.015.245 880A
010.010.002.245 1B
98: 172.024.196.177 1B
98: 172.024.012.193 2B
11:000427150081 089.175.054.121 821A

LAN карта #2
4:0007E9395C07 010.010.002.003 888D
4:0004278EDD00 010.010.002.200 821A

000007 Find Dyn Auto Check BadFind =000002 Del-обнулить
1Помощь2Экран3Порты4ARF5Users6ФПСУ7Stat8Уд.АДМ9Клиент0Выход1Резерв203

```

Рисунок 56 - Состояние ARP-кэша

Цифры внизу ("000007" и "000002" на рисунке) означают общее количество записей в ARP-кэше для каждого порта.

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

Нажатие клавиши вызывает процедуру обновления ARP-кэша на ФПСУ-IP.

5. 6. 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	Егг
------	-------------------	-------------------	------	-----------------------------	-----------------------------	-----

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

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

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

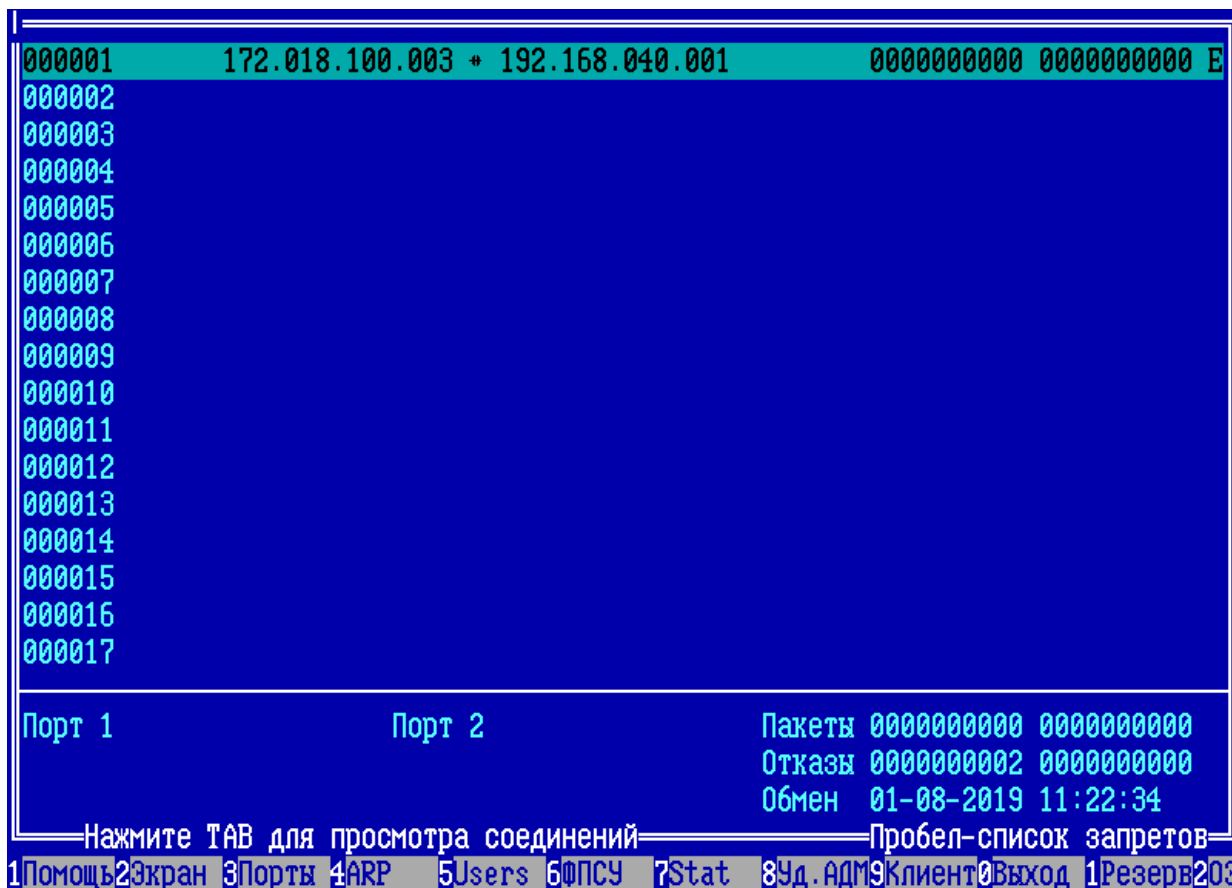


Рисунок 57 - Статистика переданных IP-пакетов

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 конца	Протокол	Причина отказа
14	15-10 16:41:48	15-10 16:43:48	VPN FPSU-IP	Нет ФПСУ-туннеля

Рисунок 58 - 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 "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 межсетевых экранов 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 межсетевое экрана, которое разрешает текущее соединение.

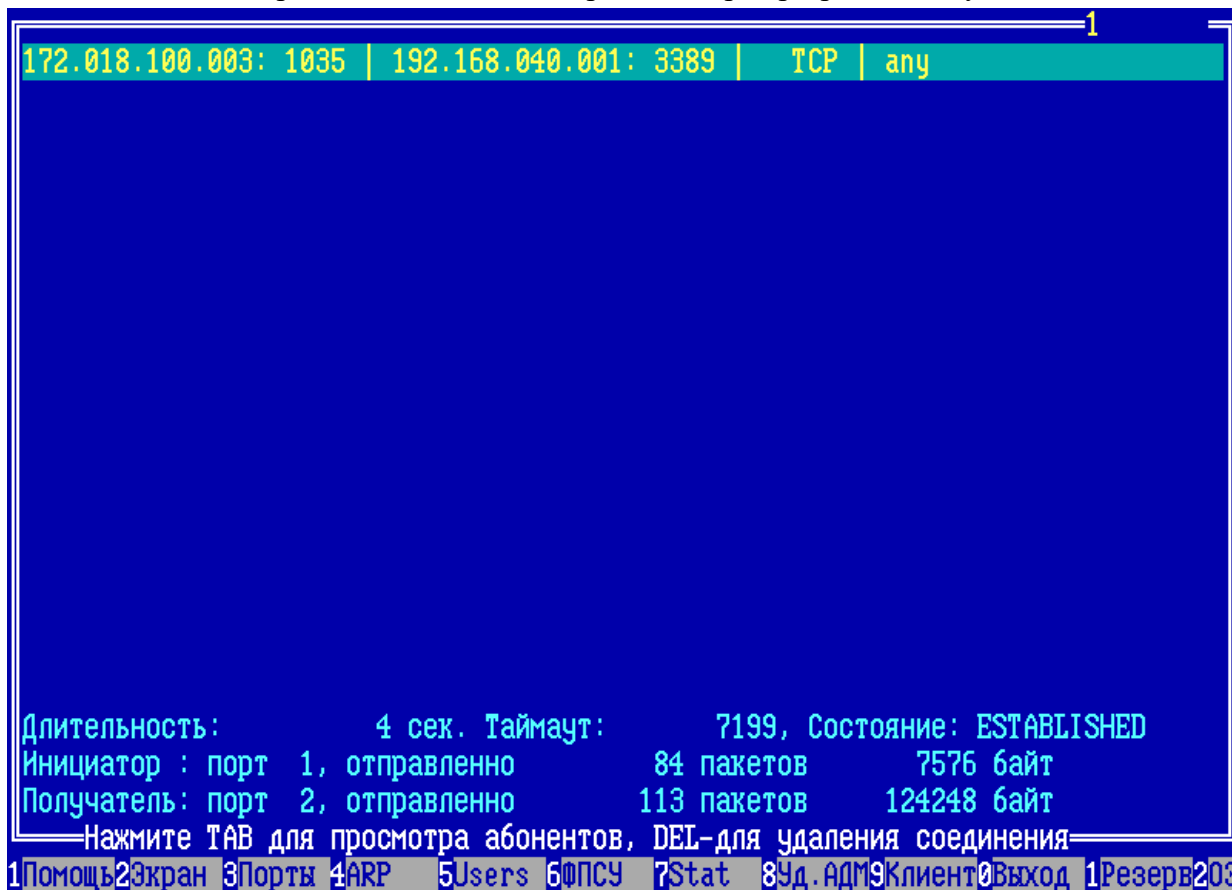


Рисунок 59 - Таблица состояния соединений ФПСУ-IP

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 . 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. 7. 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.

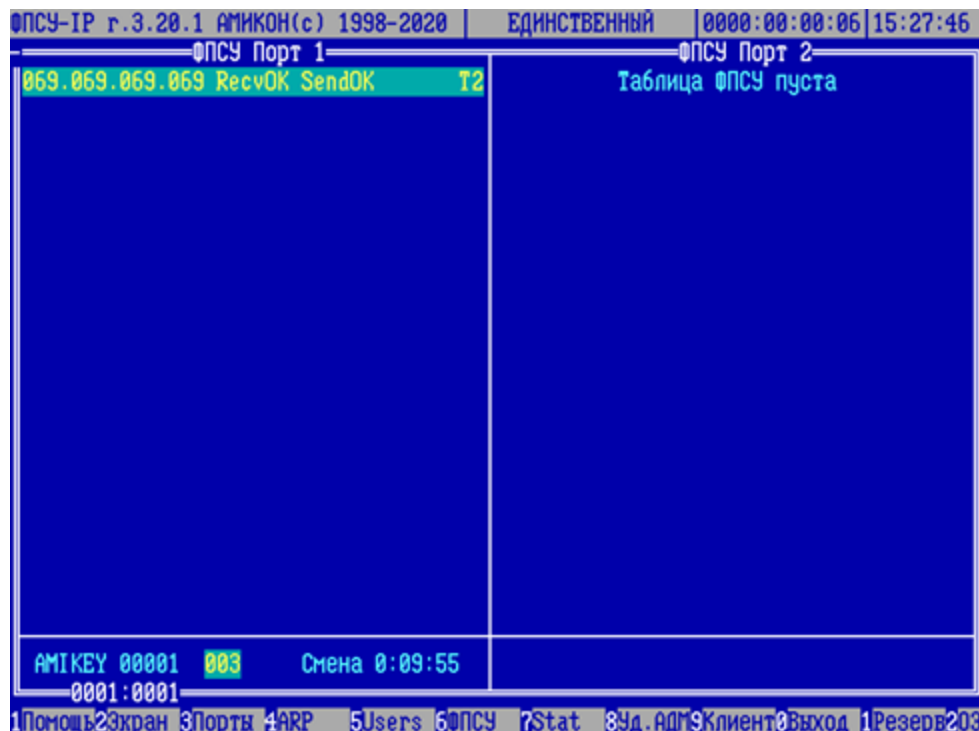


Рисунок 60 - Состояние туннелей с другими ФПСУ-IP

Состояния могут быть следующими:

RecvOk SendOk - 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 - 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). Так же 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:

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-шифрование);

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.

Цифры в рамке означают текущий номер записи и общее количество записей в списке.

5. 8. Окно состояния связи с удаленными администраторами

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

ПРОСМОТР СОСТОЯНИЯ УДАЛЕННЫХ АДМИНИСТРАТОРОВ					
Имя:ADMQQQ asda			Имя:ADM_MX Fpsu admin		
IP Адрес :	Порт:		IP Адрес :	Порт:	
Состояние: Не готов	Прием	Передача	Состояние: Не готов	Прием	Передача
Пакетов :			Пакетов :		
Данных [Кб]:		MTU:	Данных [Кб]:		MTU:
Ошибок :			Ошибок :		
Последний запрос:			Последний запрос:		
Последний опрос :			Последний опрос :		
Имя:ARM_UA test arm ua			Имя:ARMINM Fpsu admin m		
IP Адрес :	Порт:		IP Адрес :	Порт:	
Состояние: Не готов	Прием	Передача	Состояние: Не готов	Прием	Передача
Пакетов :			Пакетов :		
Данных [Кб]:		MTU:	Данных [Кб]:		MTU:
Ошибок :			Ошибок :		
Последний запрос:			Последний запрос:		
Последний опрос :			Последний опрос :		
1 Помощь 2 Экран 3 Порты 4 ARP 5 Users 6 ФПСУ 7 Stat 8 Уд.Адм 9 Клиент 0 Выход 1 Резерв 2 13					

Рисунок 61 - 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 АРМ удаленного администратора и порта соединения с ФПСУ-IP;
- текущее состояние соединения ФПСУ-IP с удаленным администратором (готов, не готов, устанавливается);
- номер порта ФПСУ-IP, по которому осуществляется связь с 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 четверо первых удаленных администраторов из списка зарегистрированных на ФПСУ-IP. Для просмотра состояния остальных удаленных администраторов следует использовать клавиши <PageUp> и <PageDown>.

5. 9. 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 пакетного шифрования данных, "P". Отображается только когда к ФПСУ-IP подключен ФПСУ-IP/Клиент с версией программного обеспечения меньше 5.0 (использующий СКЗИ "Туннель 2.0").

Имя	NAT	IP Адрес	Порт	Принято	Передано
otk_technol		192.168.015.001	2	0000000120	0000000120 P

Открыт	11-08-2020	16:54:54	12345/00004/00002	Пакетов	0000000003	0000000003
Обмен	11-08-2020	16:55:08	IP 192.168.000.085			MAC 080027e24af7

000001:000001

Рисунок 62 - 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. 10. 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.

"Звездочкой" 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 "звездочкой" туннель организован через сетевой адаптер, который в конфигурации ФПСУ-IP настроен в качестве рабочего порта.

#	Статус	Передано	Принято	Ошибочных	Node Address	Speed
*1		34	0	0	001B216E3998	No link
*2		34	0	0	0002B3881C8C	No link
3	Готов	64	47	13	026D10918440	100 Мbps F
4	Готов	45	62	0	026D10918441	1000 Мbps F
Готов		Время 10-12-2013 13:01:14				
МЕСТНЫЙ - РЕЗЕРВНЫЙ		УДАЛЕННЫЙ - ОСНОВНОЙ				
СОСТОЯНИЕ		в резерве		СОСТОЯНИЕ		в работе
Работоспособность		ИСПРАВЕН		Работоспособность		ИСПРАВЕН
Активен с: 16:22:36 07.03.2020				Alt-Tab - Сделать АКТИВНЫМ		

1 Помощь 2 Экран 3 Порты 4 ARP 5 Users 6 ФПСУ 7 Stat 8 Уд. АДМ 9 Клиент 0 Выход 1 Резерв 2 ОЗ

Рисунок 63 - 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 нем 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. 11. 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 64 - Жидкокристаллический дисплей ФПСУ-IP

На экран выводится текстовая информация, две строки по двадцать символов в каждой. Далее 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 "АМ100001СО";
- режим ФПСУ-IP в системе горячего резервирования, значение выбирается из списка *основной / резервный / единств.* (единственный);
- статус ФПСУ-IP: *в работе*;
- текущее состояние ФПСУ-IP в системе горячего резервирования, значение выбирается из списка *активен / пассивен / блок.* (блокирован ввиду ошибок).

Схематичный пример основного информационного окна:

А	М	1	0	0	0	0	1	С	О			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 "Λ" 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	-	І	Р				v	3	.	2	0		
Н	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.

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.

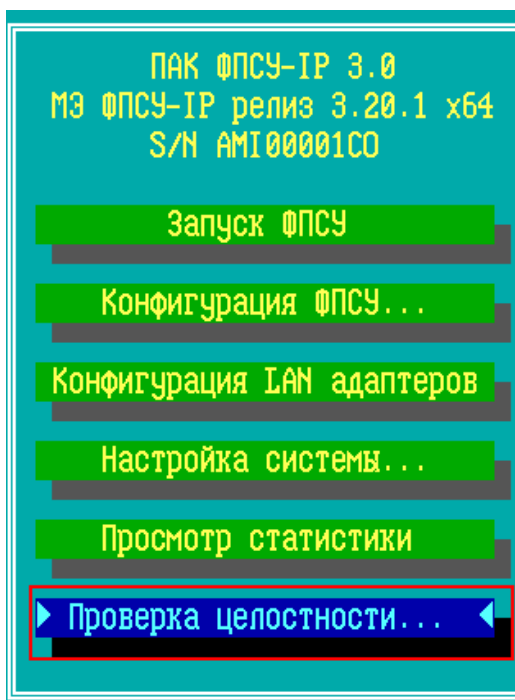


Рисунок 65 - Главное меню ФПСУ-IP

6. 1. Проверка целостности программных модулей ФПСУ-IP

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

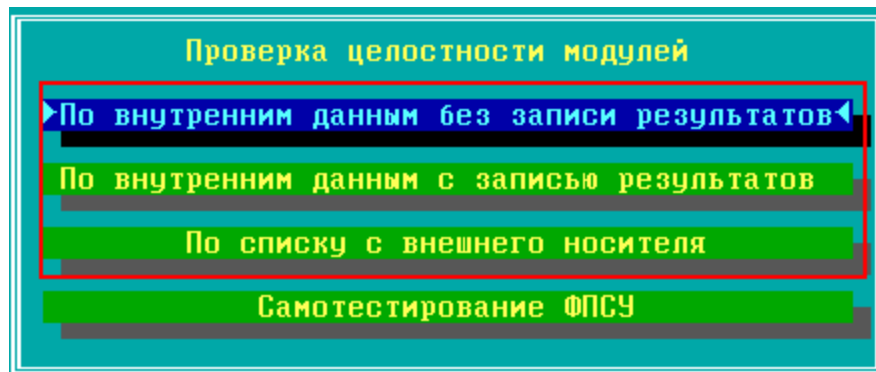


Рисунок 66 - Меню проверки целостности ПО

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

При выборе пункта **"По внутренним данным с записью результатов"** проверка 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.

При выборе пункта **"По списку с внешнего носителя"** проверка 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 главного меню **"Проверка целостности"** и команды **"По списку с внешнего носителя"** открывшегося подменю 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.

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 "Проверка целостности" администратор может выполнить ручную проверку функционала межсетевого экрана ФПСУ-IP, "Самотестирование ФПСУ" (операция доступна администратору класса "Инженер" или выше):

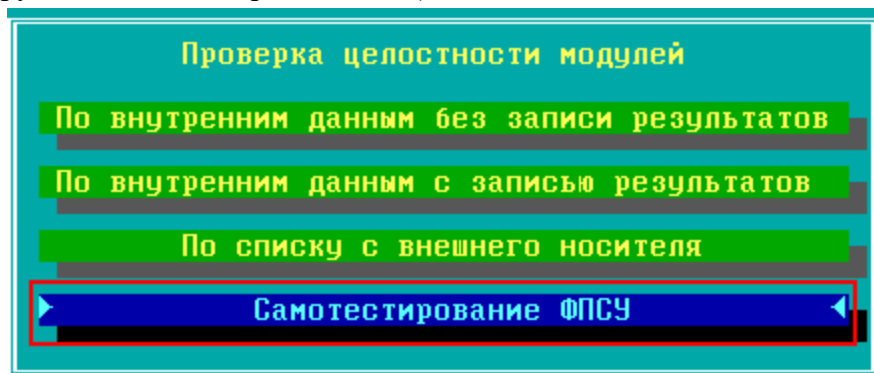


Рисунок 67 - Команда запуска внутреннего теста межсетевого экрана ФПСУ-IP

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:

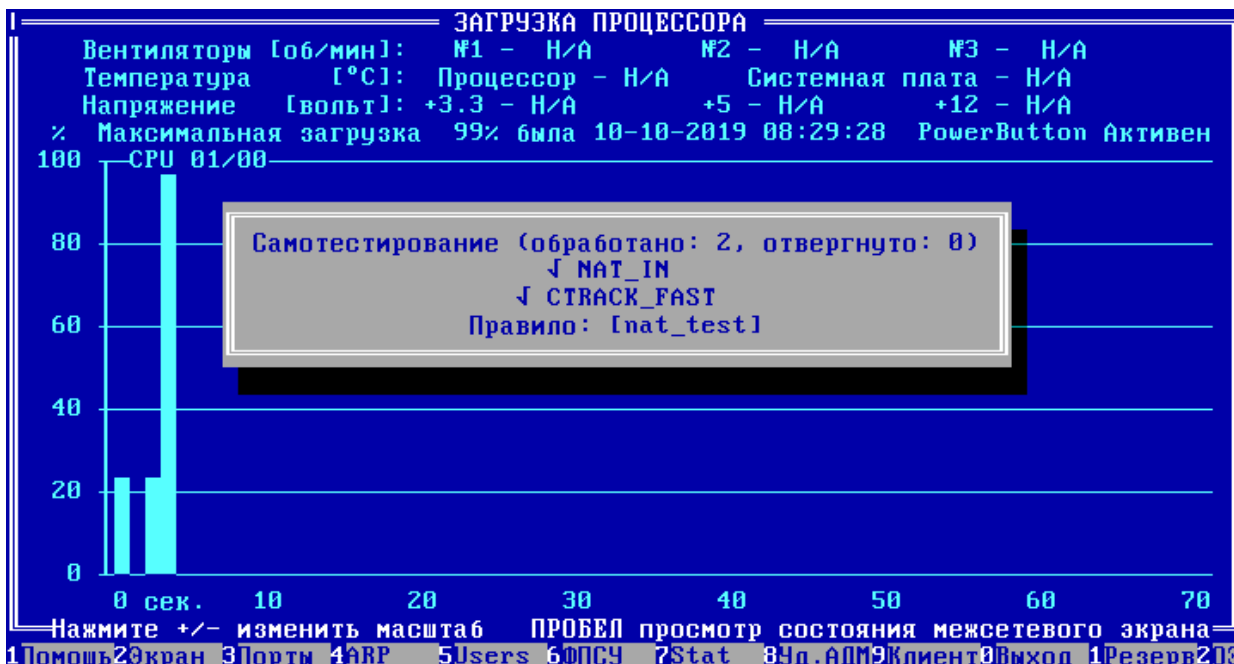


Рисунок 68 - Выполняется самотестирование ФПСУ

В случае успешной проверки, будет выдано оповещение:

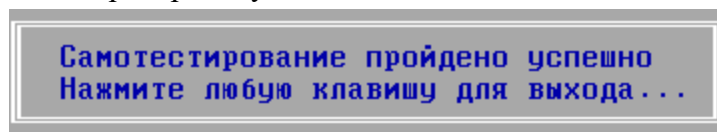


Рисунок 69 - Сообщение об успешно пройденном самотестировании

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

Результат прохождения самотестирования записывается в статистику ФПСУ-IP.

6. 4. Проверка контрольных сумм при помощи ФИКС (2.0.2)

Часть неизменяемых файлов, поставляемых с ФПСУ-IP, не устанавливается на аппаратную платформу ФПСУ-IP, а запускается с консоли управления. Такими файлами из комплекта поставки являются файлы "прошивки" BIOS аппаратных платформ ФПСУ-IP и утилита Restore.exe, предназначенная для записи дистрибутива ПАК "ФПСУ IP" на USB-flash.

Для проверки контрольных сумм, эти файлы предварительно требуется скопировать с консоли управления или дистрибутивного носителя на рабочее место с установленной "Программой фиксации и контроля исходного состояния программного комплекса "ФИКС" (версия 2.0.2)" (далее ФИКС). Допускается установка ФИКС на консоль управления

ФПСУ-IP. ФИКС следует использовать в соответствии с эксплуатационными документами на программу.

Для проверки контрольных сумм:

1. Скопируйте на рабочую станцию с установленной ФИКС проверяемые файл или файлы (например, restore.exe);

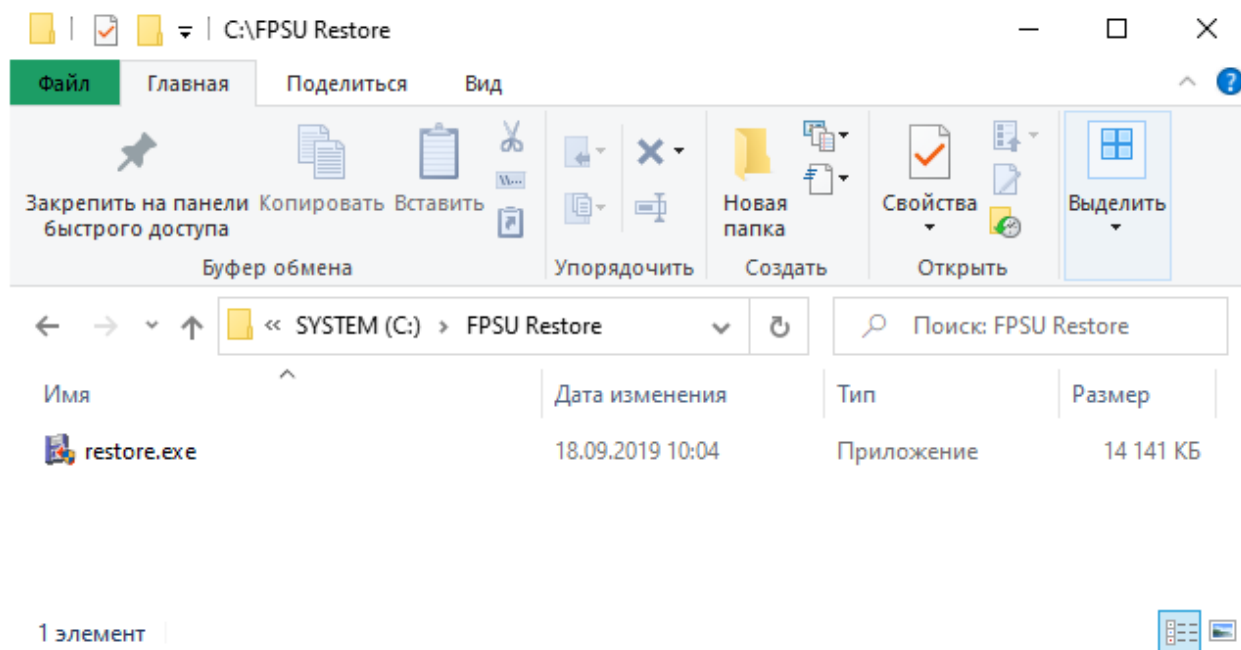


Рисунок 70 - Файл скопирован для проверки ФИКС

2. Запустите ФИКС и укажите каталог, в котором находится скопированный проверяемый файл. Установите следующие параметры работы ФИКС: Режим – Фиксация версии, Алгоритм КС – "ВКС". Остальные параметры следует оставить установленными в значения по умолчанию

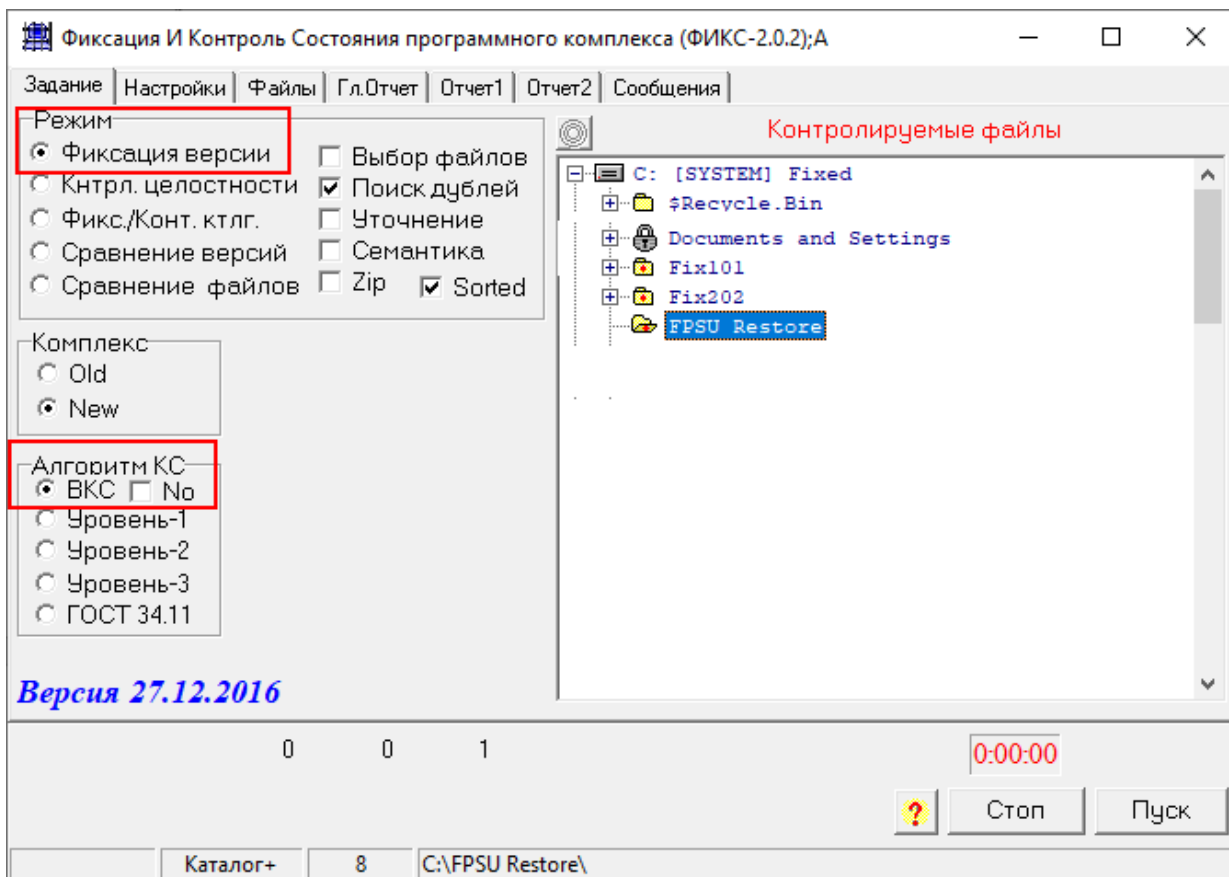


Рисунок 71 - Параметры ФИКС

3. Выполните команду "Пуск" программы ФИКС. Подтвердите необходимость работы по указанному каталогу, включая подкаталоги. ФИКС произведет подсчет контрольных сумм и выдаст результат в отчет:

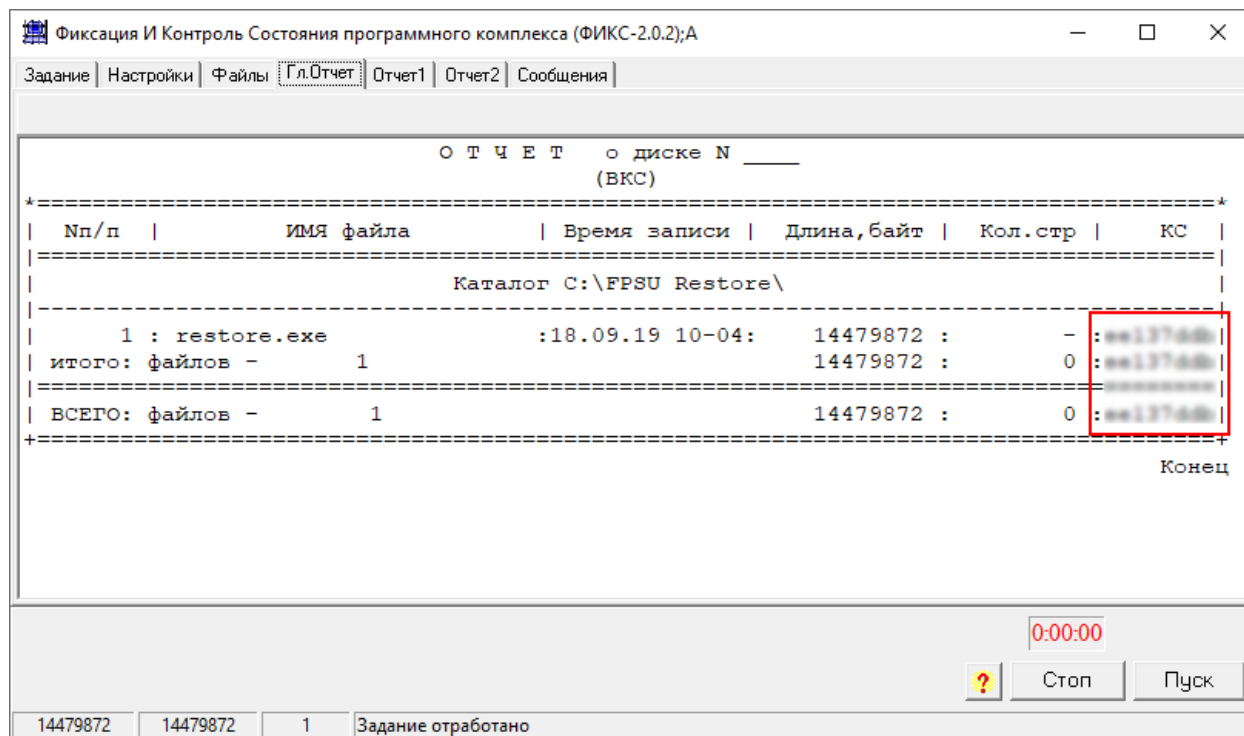


Рисунок 72 - Результат расчета контрольных сумм

Подсчитанные ФИКС контрольные суммы следует сравнить с указанными в формуляре на ФПСУ-IP эталонными суммами. В случае несовпадения контрольных сумм с указанными в формуляре, использовать файлы с не прошедшими проверку контрольными суммами запрещается.

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:

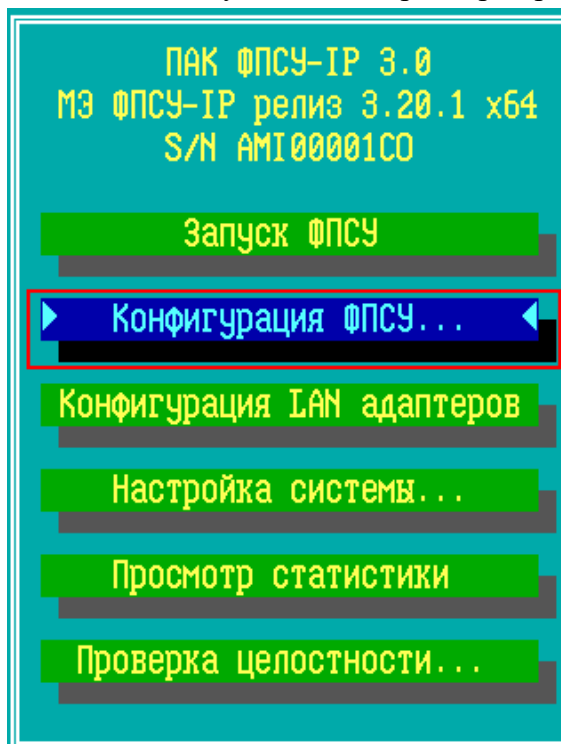


Рисунок 73 - Главное меню ФПСУ

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.

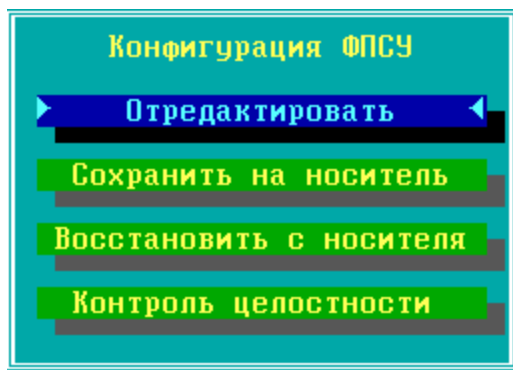


Рисунок 74 - Команды работы с конфигурацией

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*".

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:

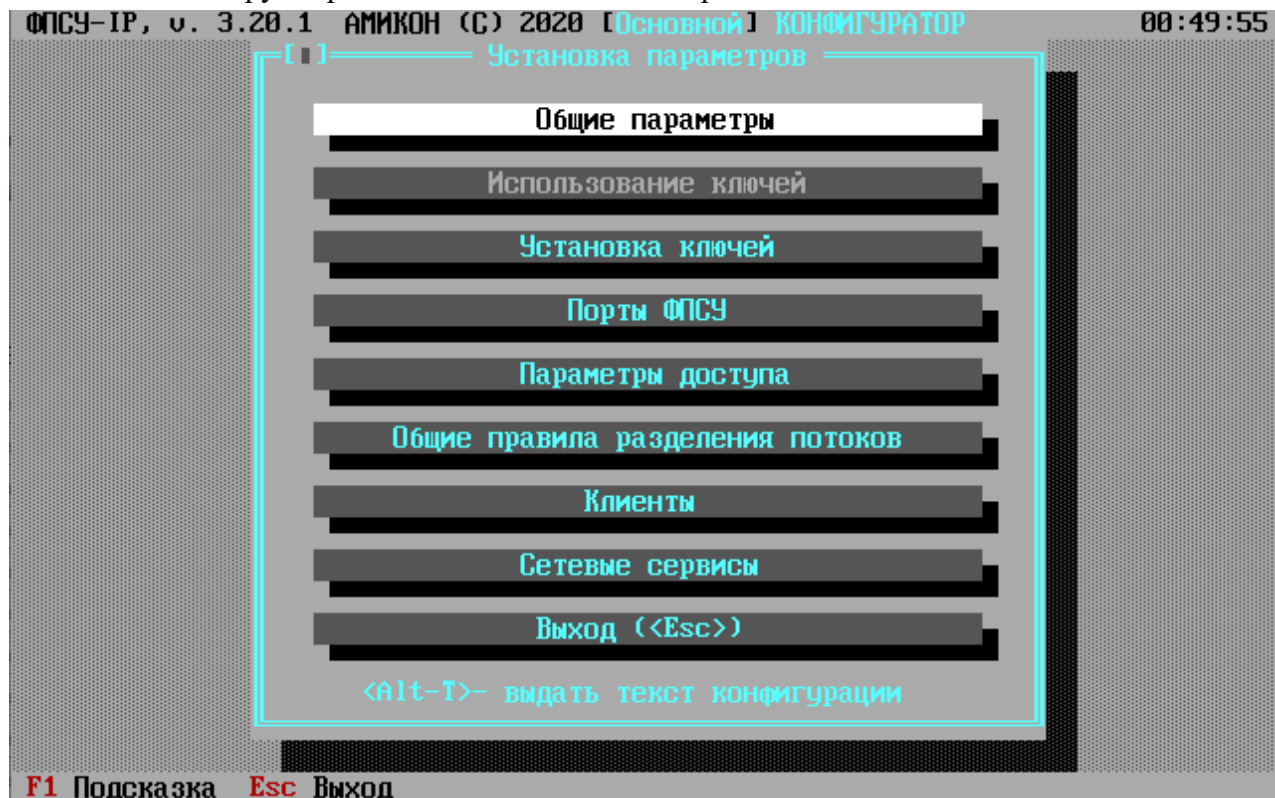


Рисунок 75 - Меню подсистемы конфигурирования ФПСУ-IP

Администратор может выдать конфигурацию в текстовом виде на внешний носитель при помощи комбинации клавиш $\langle Alt + T \rangle$. Текст конфигурации выдается в файл с именем, образованным из серийного номера ФПСУ-IP с добавлением буквы "Т" 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.

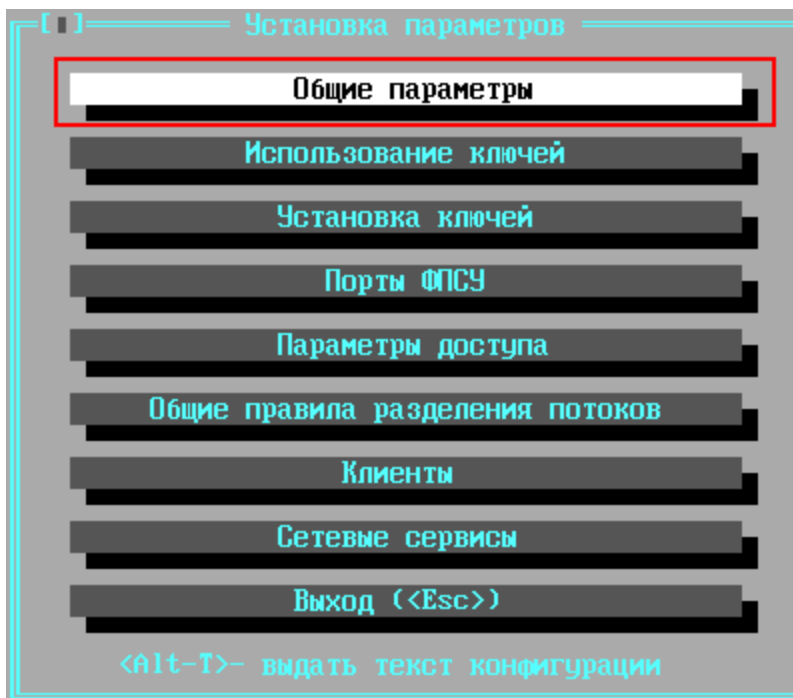


Рисунок 76 - Вход в общие настройки из основного меню конфигурации ФПСУ-IP

Окно установки содержит следующие настраиваемые общие параметры:

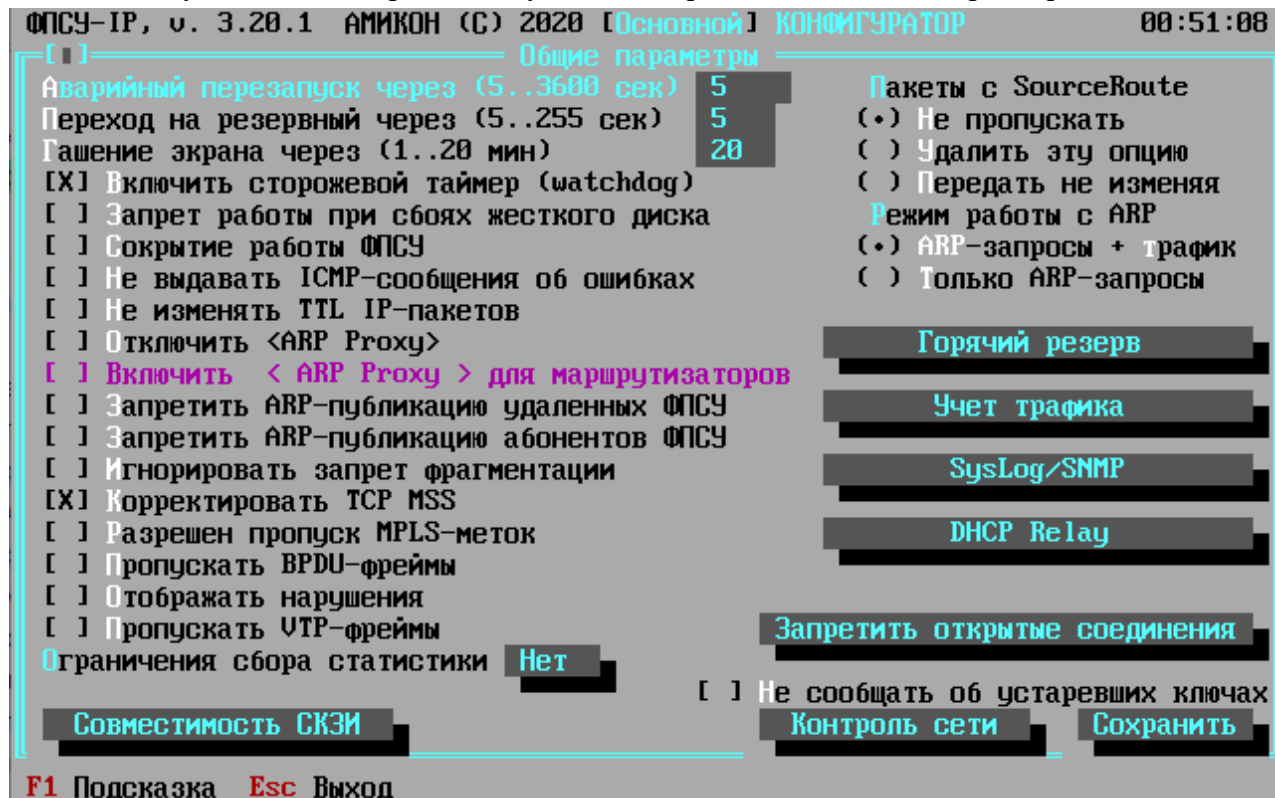


Рисунок 77 - Настройка общих параметров ФПСУ-IP

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.

Гашение экрана. В ряде случаев при работе ФПСУ-IP возникает необходимость визуально отслеживать происходящие на экране события. Если такой необходимости нет, с точки зрения сбережения ресурсов монитора и повышения быстродействия ФПСУ-IP целесообразно прибегать к гашению экрана. В поле ввода справа от строки введите время (от 1 до 20 минут), по истечении которого с момента последнего действия администратора (обращения к клавиатуре или к консоли) экран монитора будет автоматически погашен до следующего обращения. Если оставить поле пустым, гашение экрана производиться не будет.

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 переключатель. Включение или выключение опции запрета осуществляется клавишей <Пробел>.

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.

Соккрытие работы ФПСУ. В зависимости от требуемой степени защиты администратор может включить переключатель конфигурации, указывающий ФПСУ-IP, что он должен работать в режиме сокрытия своих защитных (фильтрующих) функций. При включенном переключателе 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. Включение или выключение опции сокрытия осуществляется клавишей <Пробел>.

Не выдавать ICMP-сообщения об ошибках. Если переключатель выставлен, ФПСУ-IP никогда не будет генерировать ICMP-сообщения, кроме сообщений о необходимости изменения MTU. Включение или выключение опции осуществляется клавишей <Пробел>.

Не изменять TTL IP-пакетов — переключатель, 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. Включение или выключение опции осуществляется клавишей <Пробел>.

Отключить <ARP-проху>. Для обеспечения "прозрачности" функционирования, в ФПСУ-IP реализован стандартный механизм ARP-проху 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-проху можно отключить, выставив описываемый переключатель. 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. Включение или выключение опции осуществляется клавишей <Пробел>.

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

Включить <ARP-proxy> для маршрутизаторов — переключатель, позволяющий при отключении <ARP-proxy> (см. выше) сохранить этот механизм для маршрутизаторов, "прописанных" на портах ФПСУ-IP. Доступен, если опция "Отключить <ARP-proxy>" включена. Включение или выключение опции осуществляется клавишей <Пробел>.

Запретить ARP-публикацию удаленных ФПСУ — переключатель, 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. Включение или выключение опции осуществляется клавишей <Пробел>.

Запретить ARP-публикацию абонентов ФПСУ — переключатель, 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. Включение или выключение опции осуществляется клавишей <Пробел>.

Игнорировать запрет фрагментации — переключатель, 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. Включение или выключение опции осуществляется клавишей <Пробел>.

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 — переключатель, позволяющий ФПСУ-IP обрабатывать и передавать дальше пакеты с метками MPLS-протокола. При выключенной опции такие пакеты не обрабатываются ФПСУ-IP и сбрасываются.

Пропустить BPDU-фреймы — переключатель, 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 — переключатель, 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.

Пропустить VTP-фреймы — переключатель, 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.

Ограничения по сбору статистики. Эта кнопка позволяет наложить ограничения на сбор регистрационной информации ФПСУ-IP. Подробнее см. пункт "[Ограничение сбора статистики](#)".

Совместимость с предыдущими версиями СКЗИ Туннель/Клиент — опция, разрешающая тестовую работу ФПСУ-IP с пользователями ПАК ФПСУ-IP/Клиент, которые используют СКЗИ предыдущих версий. По умолчанию переключатель установлен в положение "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 с последней версией СКЗИ.

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;
- 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 пакет, оставив опцию 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 так же 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 SteelHand).

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

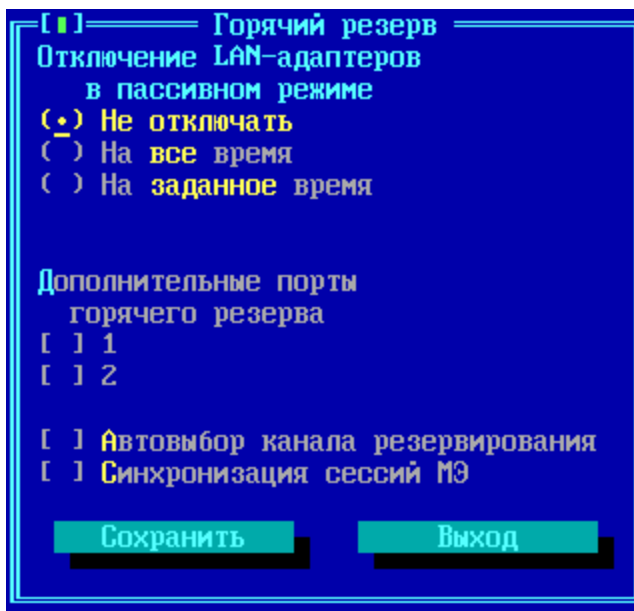


Рисунок 78 - Настройка горячего резерва

- **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 порты горячего резерва** — переключатели "[] 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 со 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 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.

Учет трафика — кнопка перехода в окно настроек работы сенсора IPFIX на ФПСУ-IP, подробная информация находится в пункте [Учет трафика IPFIX](#)

SysLog/SNMP — кнопка, при нажатии которой происходит переход в окно настроек отправки сообщений SysLog и SNMP серверу о происходящих на ФПСУ-IP событиях. Подробные настройки этой опциональной подсистемы ФПСУ-IP описаны в пунктах "[Syslog-клиент на ФПСУ-IP](#)" и "[SNMP-клиент на ФПСУ-IP](#)". Если ни одна из подсистем SysLog/SNMP не установлена, кнопка не отображается.

DHCP Relay — кнопка, вызывающая окно "*DHCP Relay*". В нем администратором ФПСУ-IP включается поддержка DHCP Relay и ведется список IP-адресов хостов, используемых абонентами ФПСУ-IP в качестве DHCP-серверов.

Детальная информация по настройке и работе DHCP Relay на ФПСУ-IP находится в пункте "[DHCP-Relay](#)".

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. п. "[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 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 "Host"](#)"), должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации или с объектов информатизации в

защищаемой ЛВС.

Не сообщать об устаревших ключах — если на ФПСУ-IP установлены ключевые данные класса КСЗ, 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.

Примечание! При использовании ФПСУ-IP по классу КСЗ, в настройках должен быть включен режим информирования об использовании ключа при превышении срока его действия (флаг "**Не сообщать об устаревших ключах**" должен быть снят).

Контроль сети — кнопка перехода в окно настроек контроля доступности списка IP-адресов, подробнее см. пункт "[Параметры проверки линий связи для портов ФПСУ-IP](#)".

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 пользователям классов "**Администратор**" и "**Главный Администратор**".

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

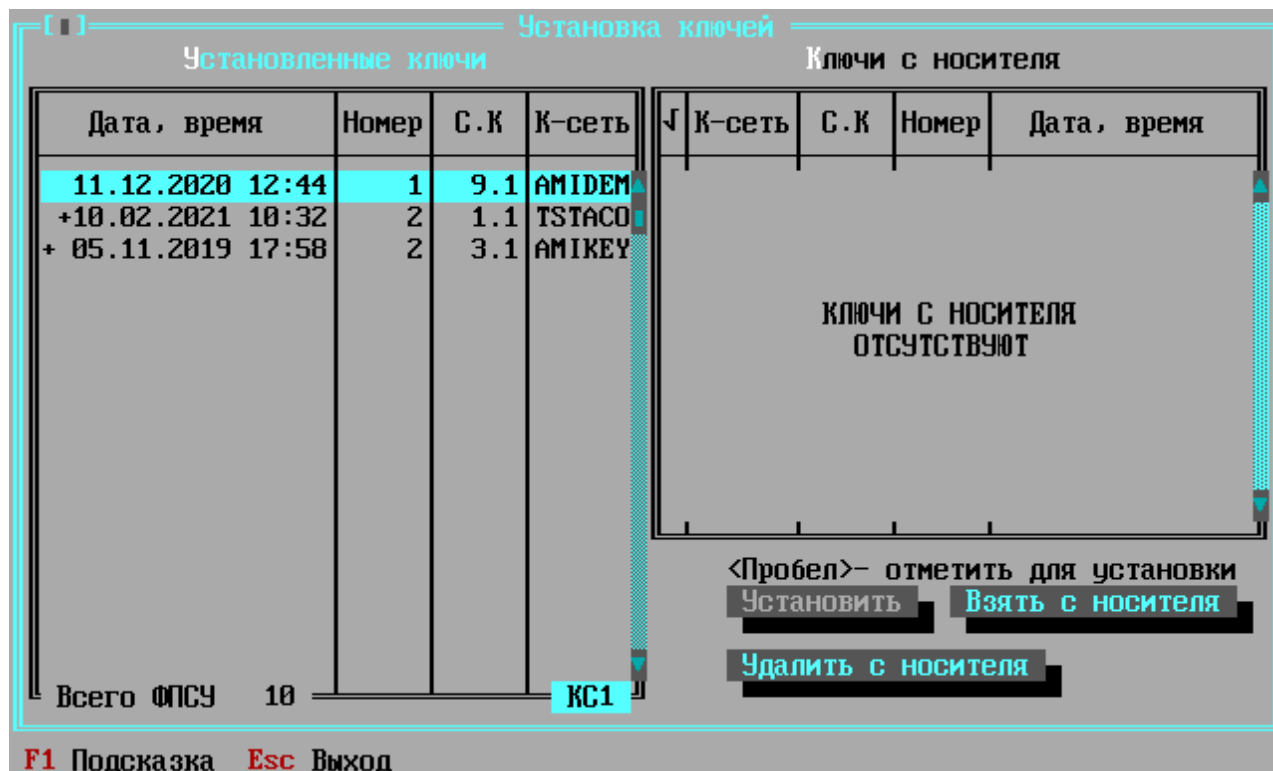


Рисунок 79 - Установка ключей

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 K=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. ["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 "v") 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, только если у них совпадает номер в рамках криптосети, 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 рамках 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".

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 80 - Выбор используемых ключей

Окно содержит список криптосетей, ключи из которых установлены на ФПСУ-IP. Каждая строка содержит информацию об 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.

Так же 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.

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 символом "v". 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 пользователя **Инженер** или выше.

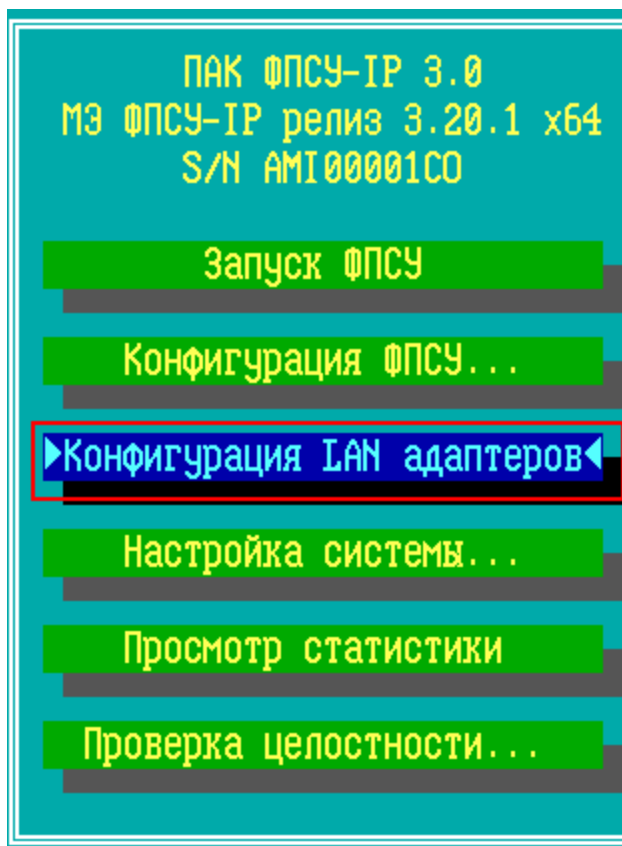


Рисунок 81 - Главное меню ФПСУ-IP

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

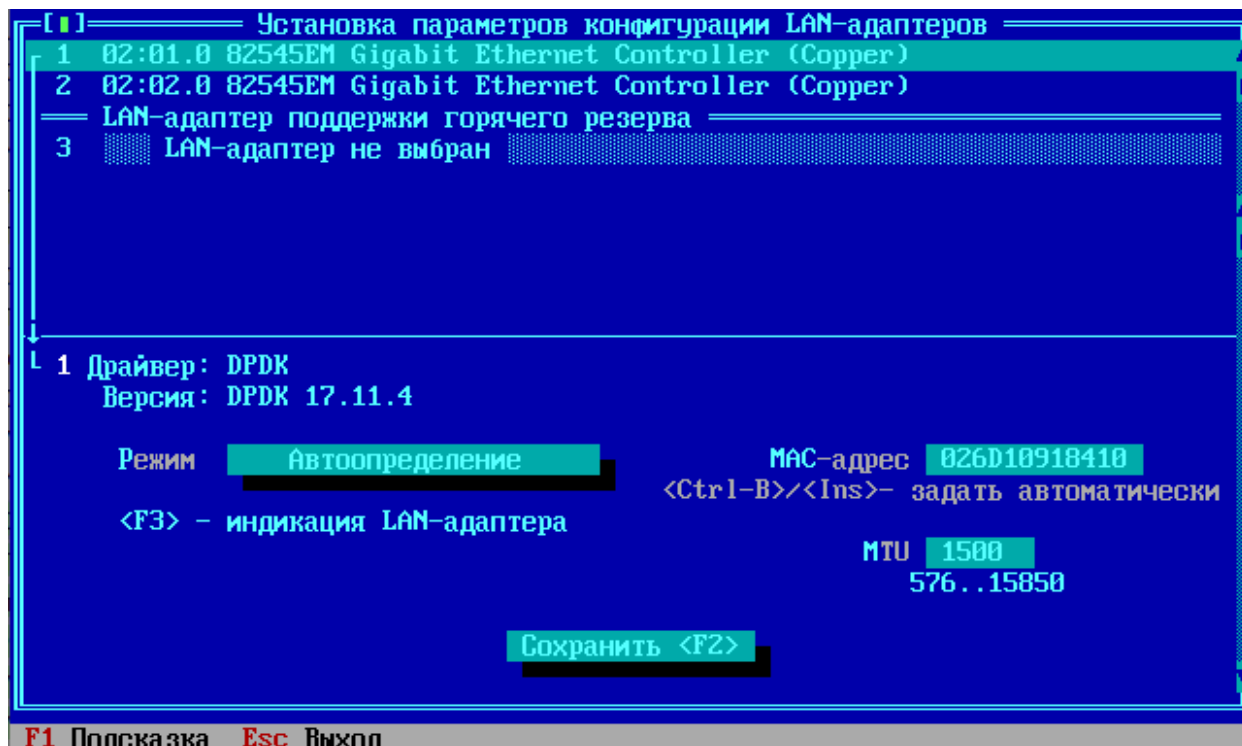


Рисунок 82 - Окно установки параметров конфигурации LAN-адаптеров

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 описанием 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.

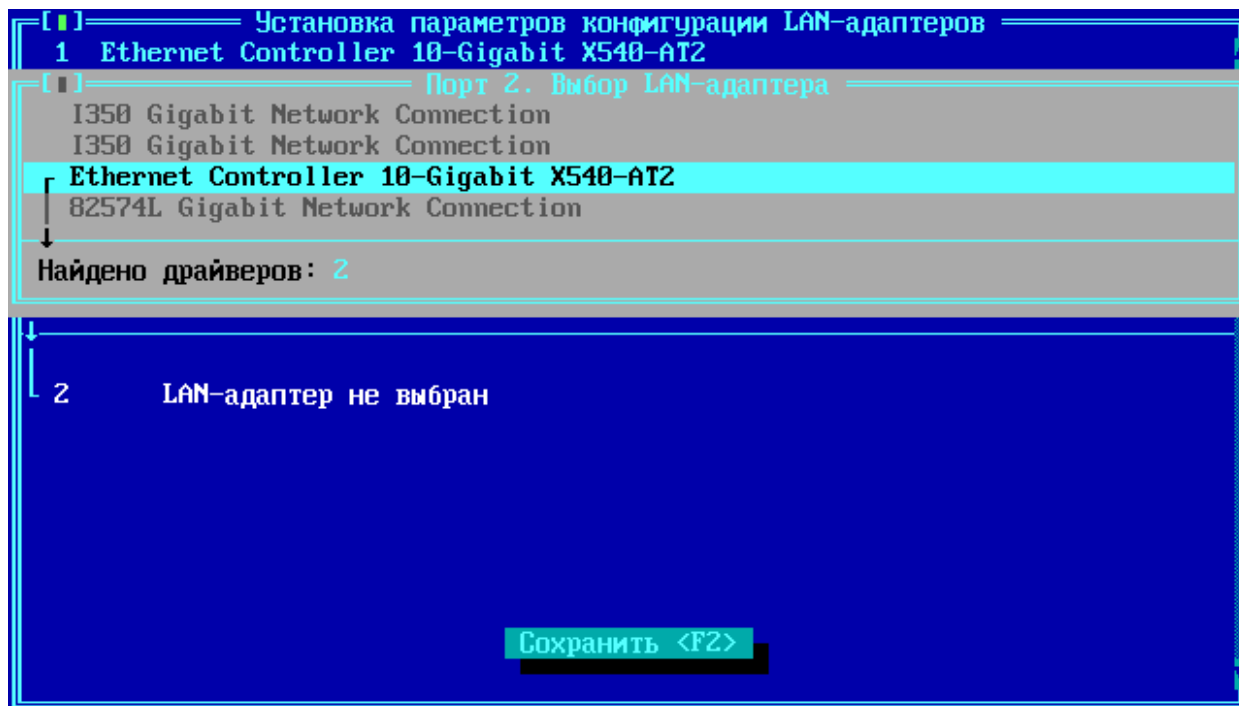


Рисунок 83 - Выбор сетевого адаптера для порта

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.

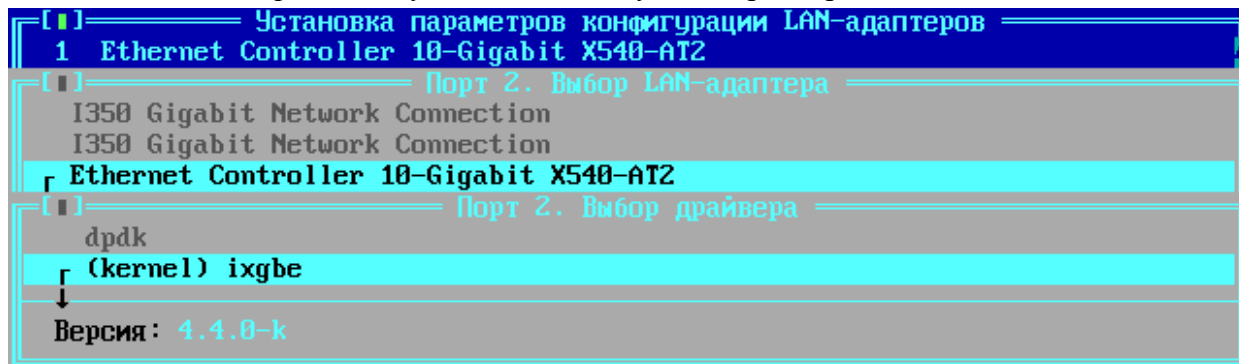


Рисунок 84 - Выбор драйвера для сетевого адаптера

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: "**Режим**" и "**MAC-адрес**".

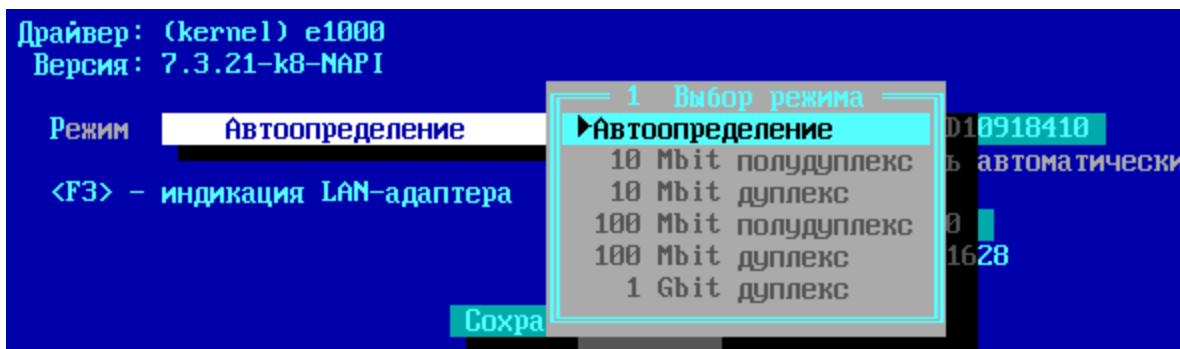


Рисунок 85 - Выбор режима работы адаптера

Для установки режима 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.

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

Дополнительным действием, отображаемым в нижней части окна установки параметров, 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 15854 байт).

По окончании установки параметров выбранного сетевого адаптера нажмите клавишу **"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.

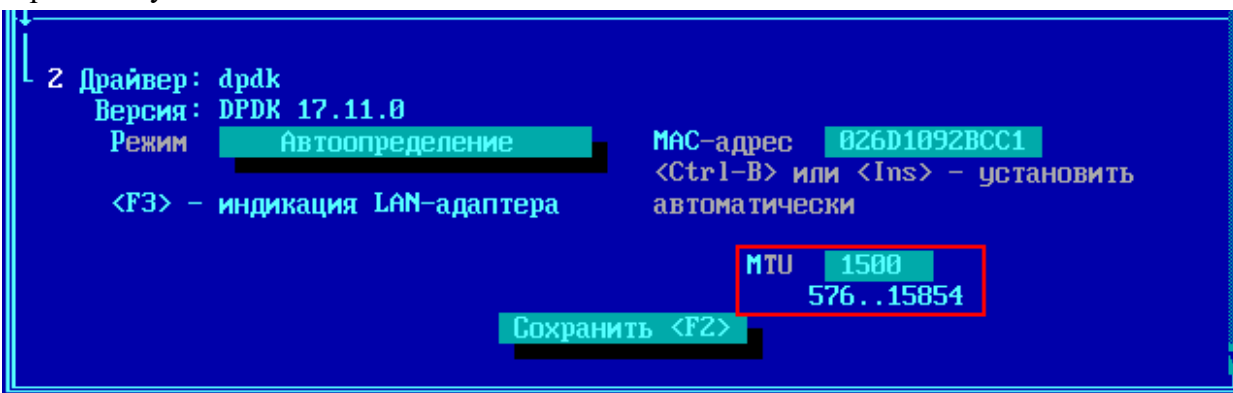


Рисунок 86 - Изменение параметра MTU сетевого адаптера с DPDK драйвером

Выбор любого установленного адаптера можно отменить, воспользовавшись клавишей . 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+v> 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. 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 переключатель "Резервирование активно" и **создать ключ горячего резерва**, см "[Настройка ФПСУ-IP на работу с партнером по резервированию](#)").
2. Включить опцию в конфигурации LAN-адаптеров "Интерфейс для удаленного управления ФПСУ":

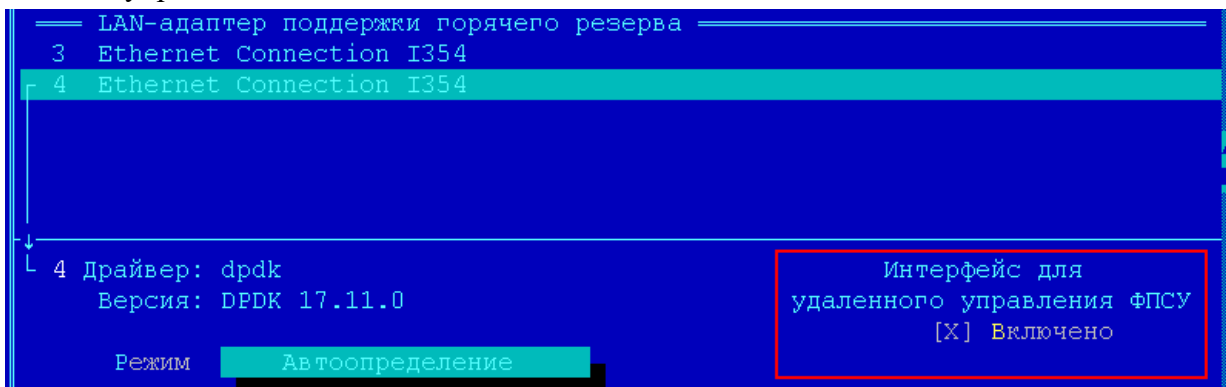


Рисунок 87 - LAN-адаптер №4 для удаленного администрирования подготовлен

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):

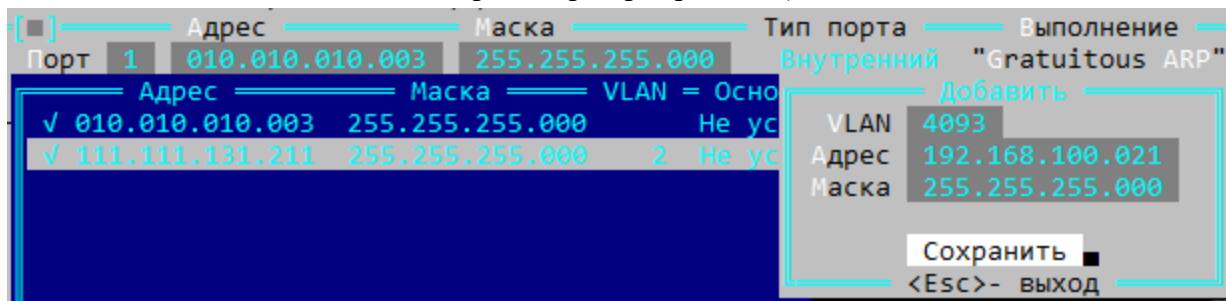


Рисунок 88 - Добавления IP-адреса порту ФПСУ в VLAN №4093

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):

#	Статус	Передано	Принято	Ошибочных	Node Address	Speed
*1	Готов	125010	124812	1	00900b6c5725	1000 Mbps F
A2		21529	0	0	00900b6c5726	100 Mbps F

Готов
МЕСТНЫЙ - РЕЗЕРВНЫЙ

Время 19-12-2018 13:54:35
УДАЛЕННЫЙ - ОСНОВНОЙ

СОСТОЯНИЕ в работе
Работоспособность ИСПРАВЕН

СОСТОЯНИЕ в резерве
Работоспособность ИСПРАВЕН

Рисунок 89 - Адаптер №4 готов принимать соединения с удаленными администраторами

8. Настройка системы

Из интерфейса меню "Настройка системы", вызываемом из "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 "Настройки 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):

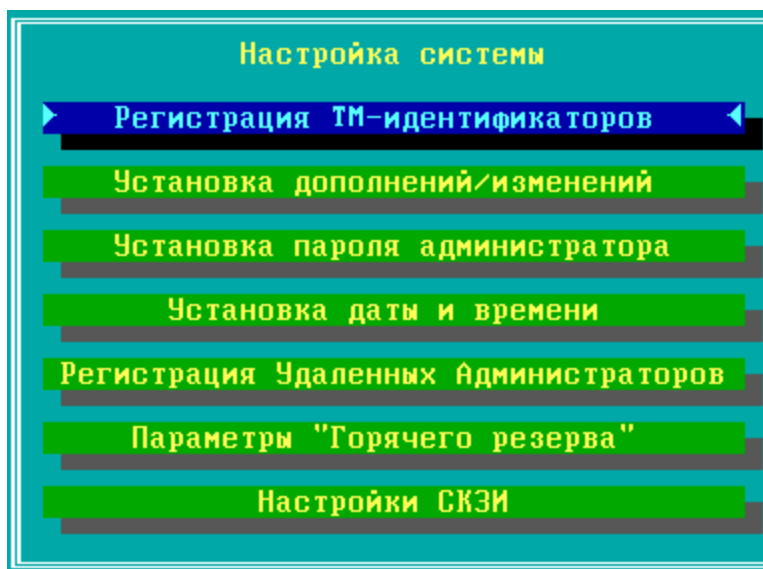


Рисунок 90 - Меню "Настройка системы"

8. 1. Регистрация ТМ-идентификаторов

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

Для выполнения команды требуются права роли "Администратор" или выше.

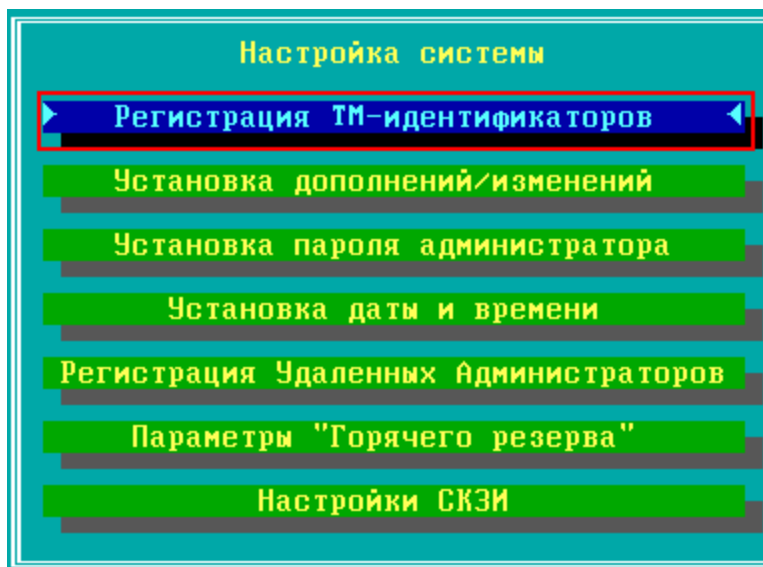


Рисунок 91 - Выбор пункта "Регистрация ТМ-идентификаторов"

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.

Наименование	Основная ТМ	Запасная ТМ
Администратор	ЗАРЕГИСТРИРОВАНА	ЗАРЕГИСТРИРОВАНА
Инженер	-	-
Оператор 1	-	-
Оператор 2	-	-
Оператор 3	-	-
Оператор 4	-	-
Подсистема автозапуска	ИСПОЛЬЗУЕТСЯ	

Рисунок 92 - 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 пользователю с ролью "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 установке 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 на 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-методу к считывателю ТМ или подключения ТМ-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 пользователям класса "Администратор" или выше, см. раздел [«Общие сведения»](#), таблица 1).

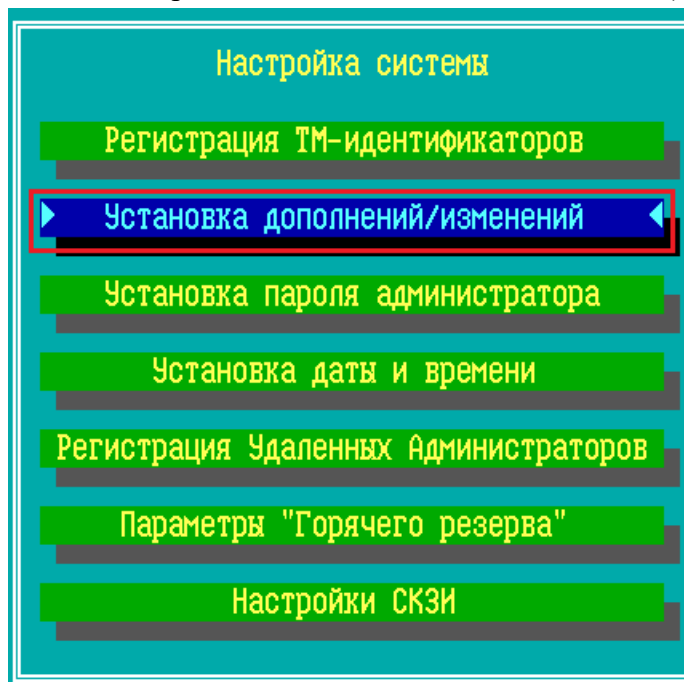


Рисунок 93 - Выбор пункта «Установка дополнений/изменений»

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).

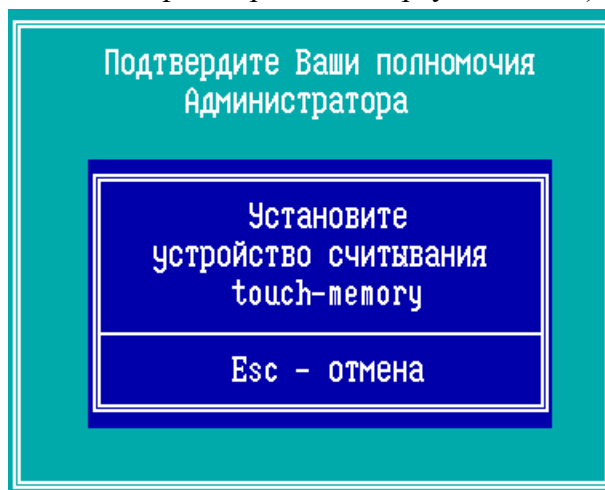


Рисунок 94 - Подтверждение полномочий администратора

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

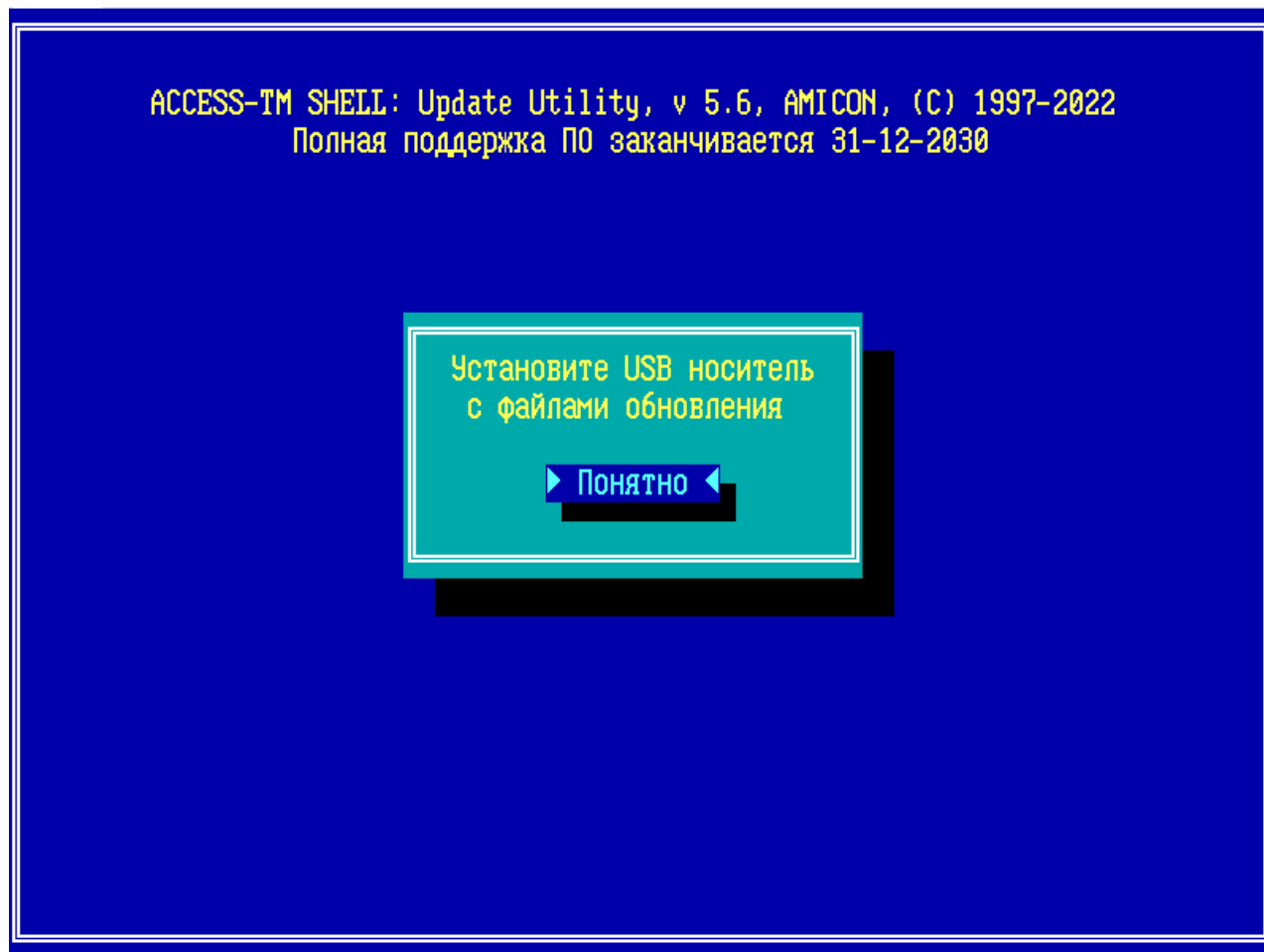


Рисунок 95 - Подключение USB-носителя

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

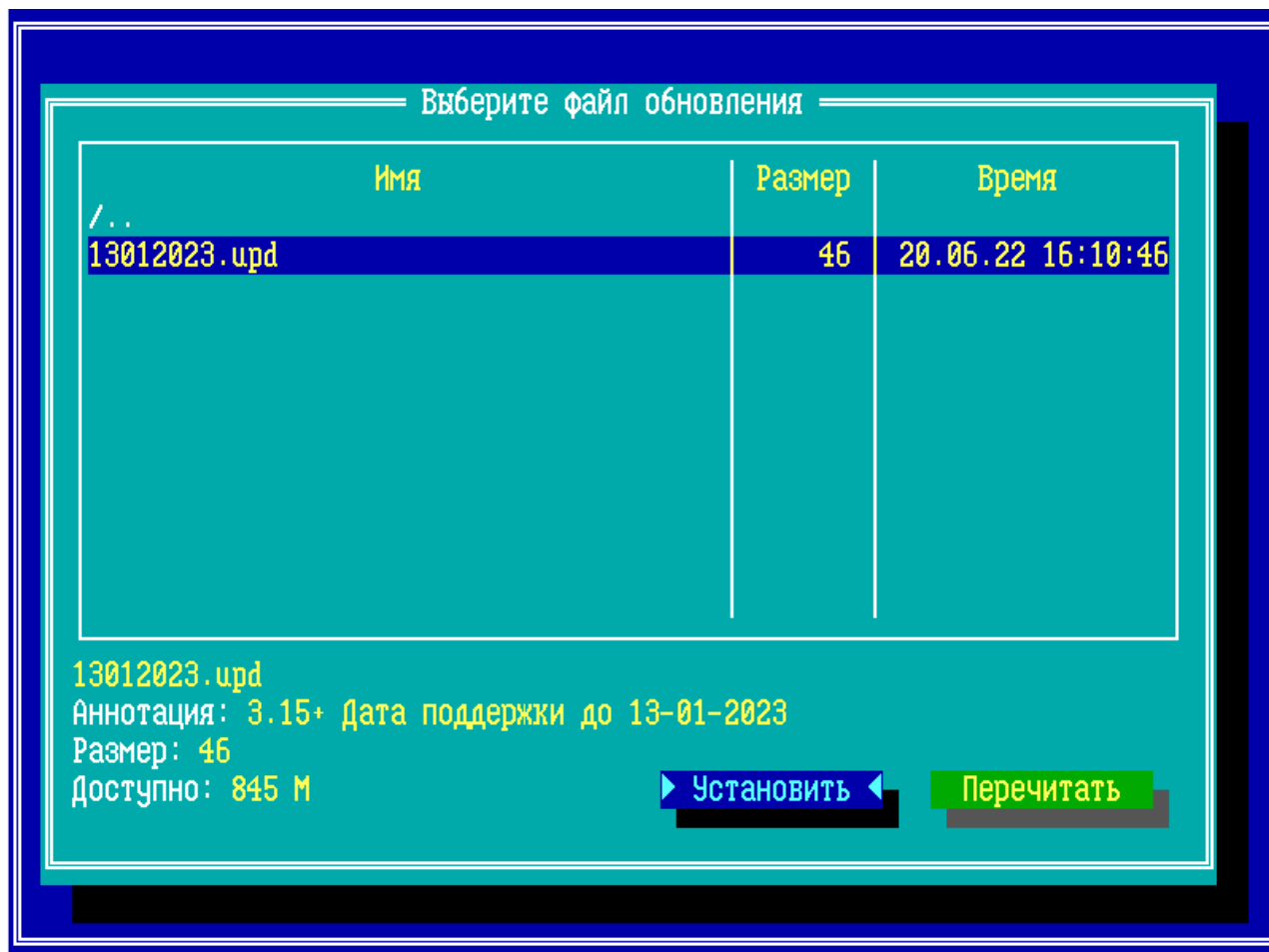


Рисунок 96 - Выбор файла обновления

4. Требуется подтвердить выбор обновления, либо вернуться к выбору другого файла обновления.

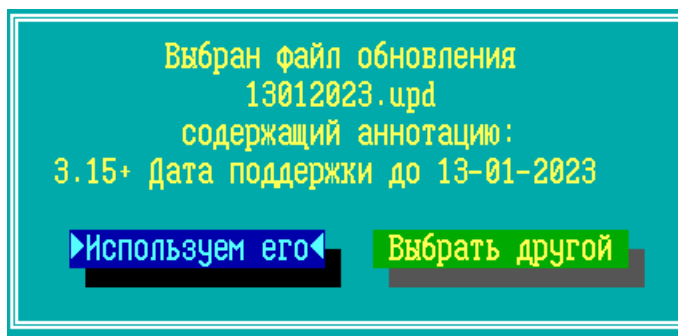


Рисунок 97 - Подтверждение обновления

Начнется процесс установки обновления, необходимо контролировать процесс установки.

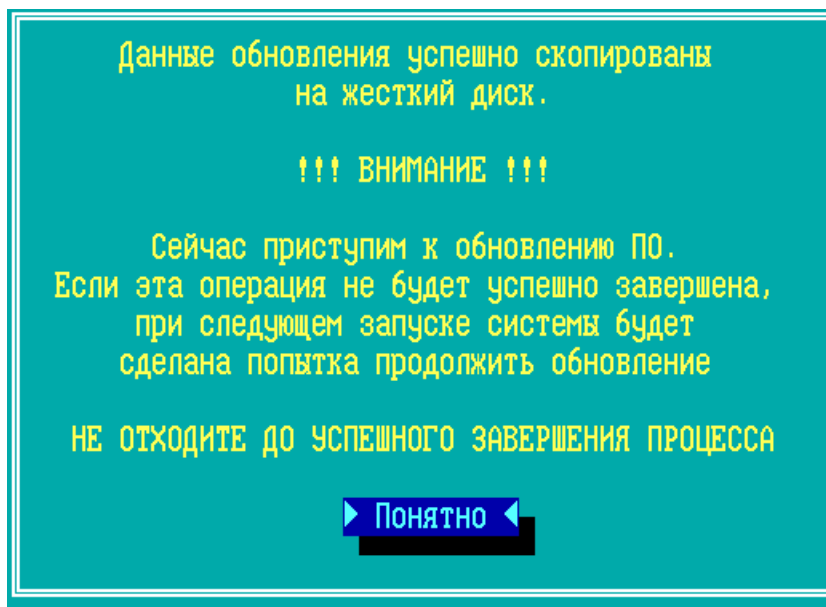


Рисунок 98 - Процесс установки обновления

После установки обновления система будет перезагружена автоматически.

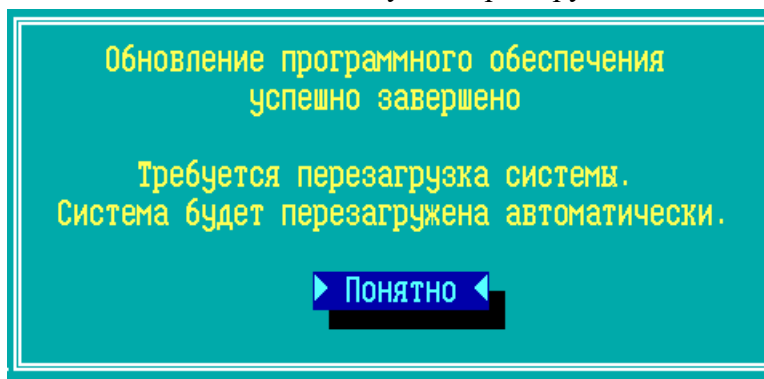


Рисунок 99 - Завершение процесса установки

Обновление установилось успешно, если после перезагрузки отобразится главное меню ФПСУ-IP.

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 пользователям роли "Администратор" и выше.

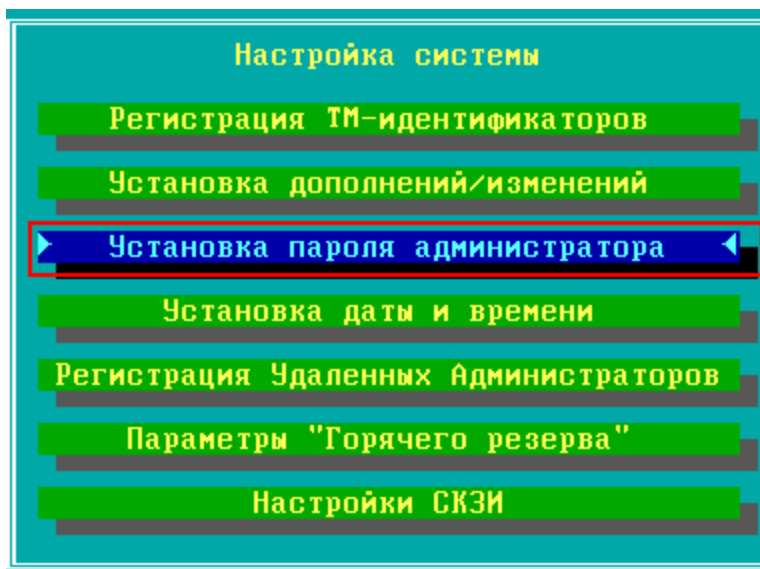


Рисунок 100 - Команда "Установка пароля администратора"

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

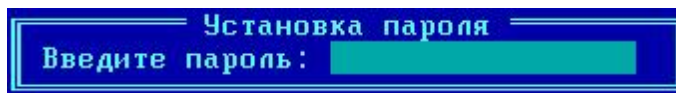


Рисунок 101 - Установка пароля администратора

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

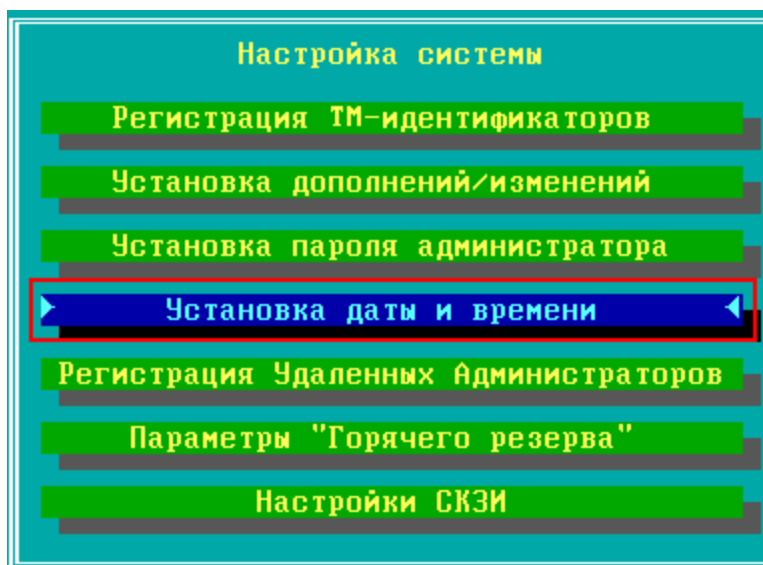


Рисунок 102 - Команда "Установка даты и времени"

При активизации команды на экран будет выдано диалоговое окно:

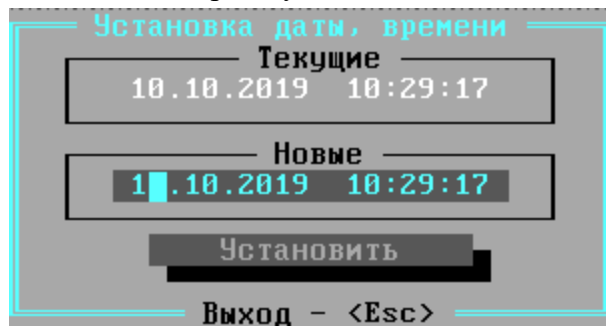


Рисунок 103 - Установка даты и времени на ФПСУ-IP

В окне отображаются текущие дата и время, а также содержатся два поля ввода

(соответственно для даты и для времени) и кнопка команды "Установить". 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 "Установить" и нажать клавишу <Enter>.

Для наиболее точной установки времени рекомендуется ввести в соответствующее поле значение, немного превышающее текущее время и отметить курсором команду "Установить" (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 "Регистрация Удаленных Администраторов" меню "Настройка системы" 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.

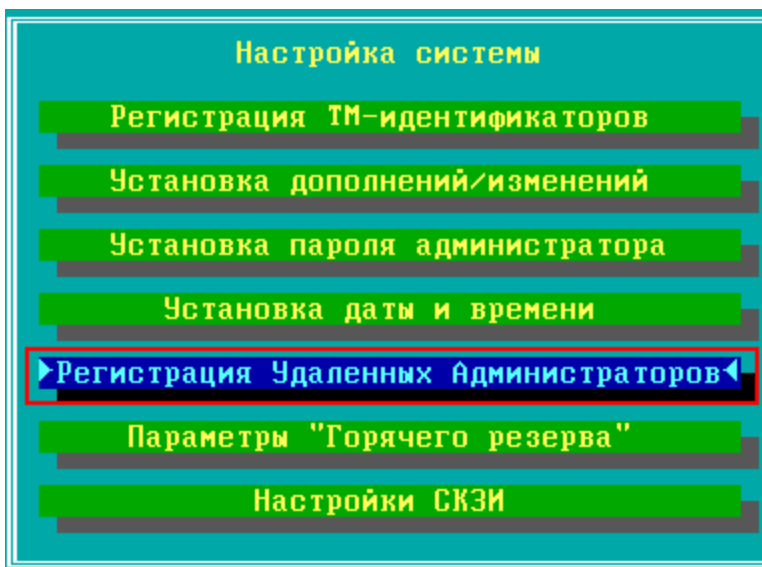


Рисунок 104 - Команда "Регистрация Удаленных Администраторов"

Операции доступны пользователям класса "Администратор" и выше. 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:

- локальным администратором ФПСУ-IP выдается на внешний USB-flash носитель файл с ключом аутентификации ФПСУ-IP;
- файл с ключом аутентификации ФПСУ-IP отправляется удаленному администратору (передача файла с аутентификатором по незащищенной сети передачи данных запрещается);
- получив файл с ключом аутентификации, администратор регистрирует у себя данный ФПСУ-IP в программе "Удаленный администратор ФПСУ-IP";
- удаленный администратор с помощью программы "Удаленный администратор ФПСУ-IP" выдает на внешний носитель файл с ключом аутентификации удаленного администратора;
- файл с ключом аутентификации удаленного администратора отправляется локальному администратору ФПСУ-IP (передача файла с аутентификатором по незащищенной сети передачи данных запрещается);
- 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 регистрирует удаленный администратор, а также список уже зарегистрированных удаленных администраторов ФПСУ-IP (по умолчанию, пустой, с текстом "Администраторы отсутствуют").

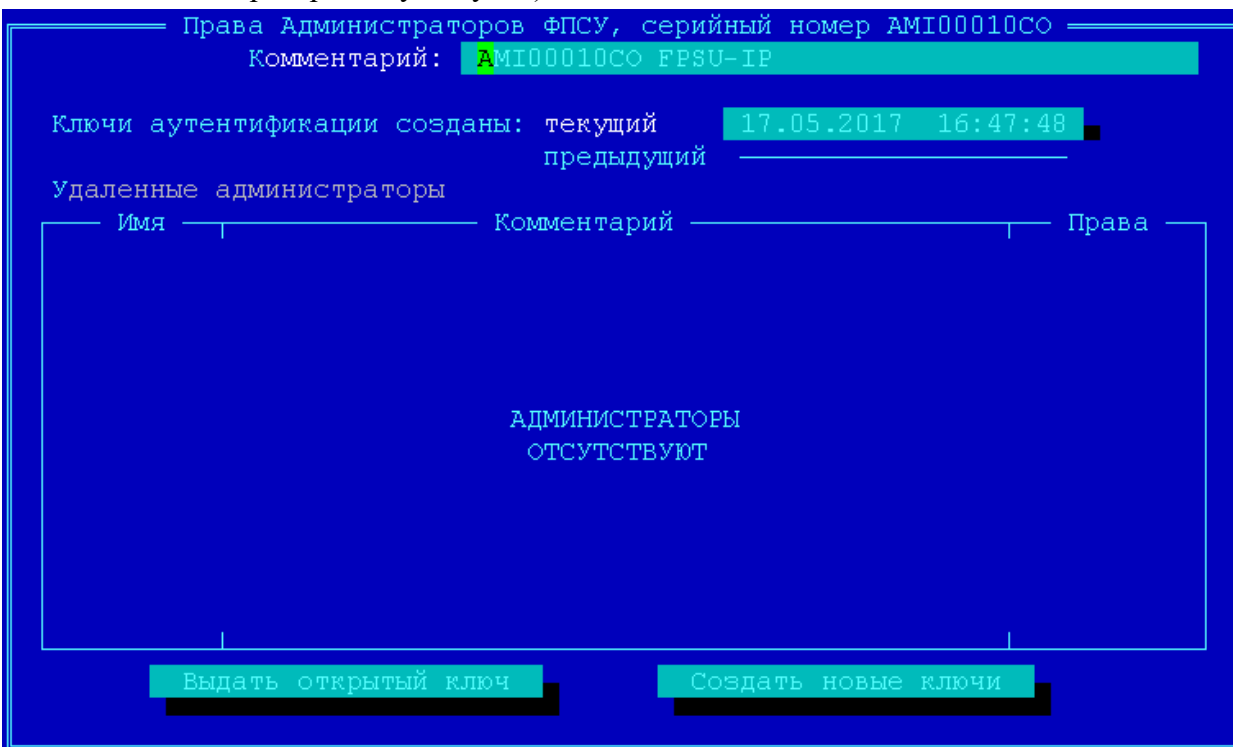


Рисунок 105 - Список удаленных администраторов

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

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>.

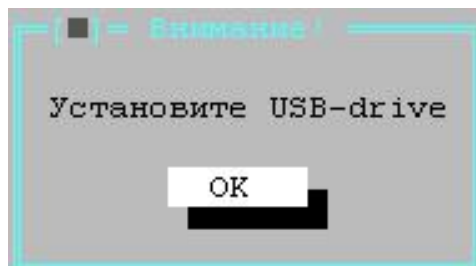
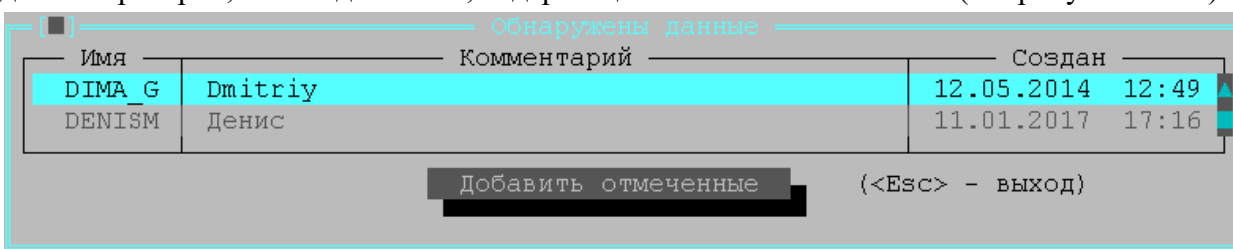


Рисунок 106 - Выбор носителя ключей аутентификации

Когда подсистема опознает и считает ключи аутентификации удаленных администраторов, она выдаст окно, содержащее список их описателей (см. рисунок ниже):



Имя	Комментарий	Создан
DIMA_G	Dmitriy	12.05.2014 12:49
DENISM	Денис	11.01.2017 17:16

Добавить отмеченные (<Esc> - выход)

Рисунок 107 - Найденные аутентификаторы удаленного администратора

В окне "Обнаружены данные" необходимо сначала отметить регистрируемые учетные записи администраторов клавишей <Пробел>, а потом выполнить команду "Добавить отмеченные". После выполнения команды зарегистрированные удаленные администраторы появятся в списке окна "Права администраторов".

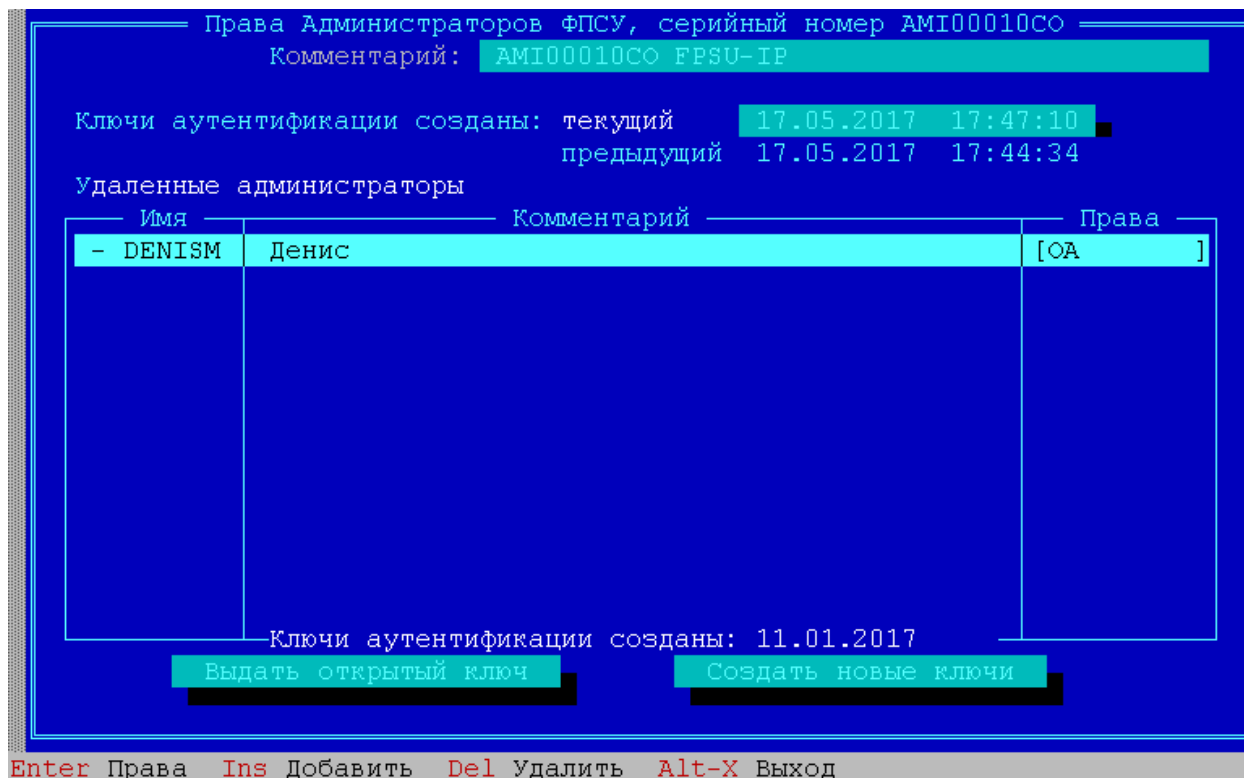


Рисунок 108 - Зарегистрирован удаленный администратор

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 () 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.

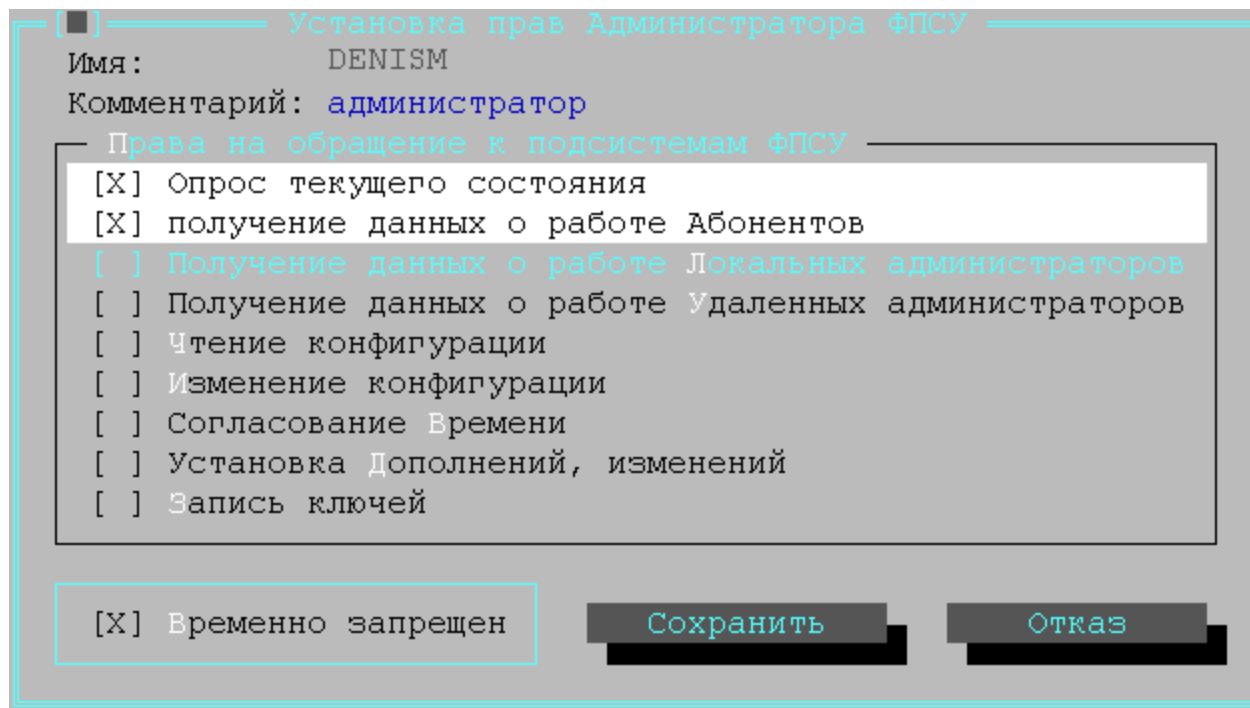


Рисунок 109 - Назначение прав удаленному администратору

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 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 (см. пункт "[NTP-клиент ФПСУ-IP](#)") и синхронизацию времени ФПСУ с удаленным администратором!

Отметив соответствующие выдаваемым правам строки с переключателями 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.

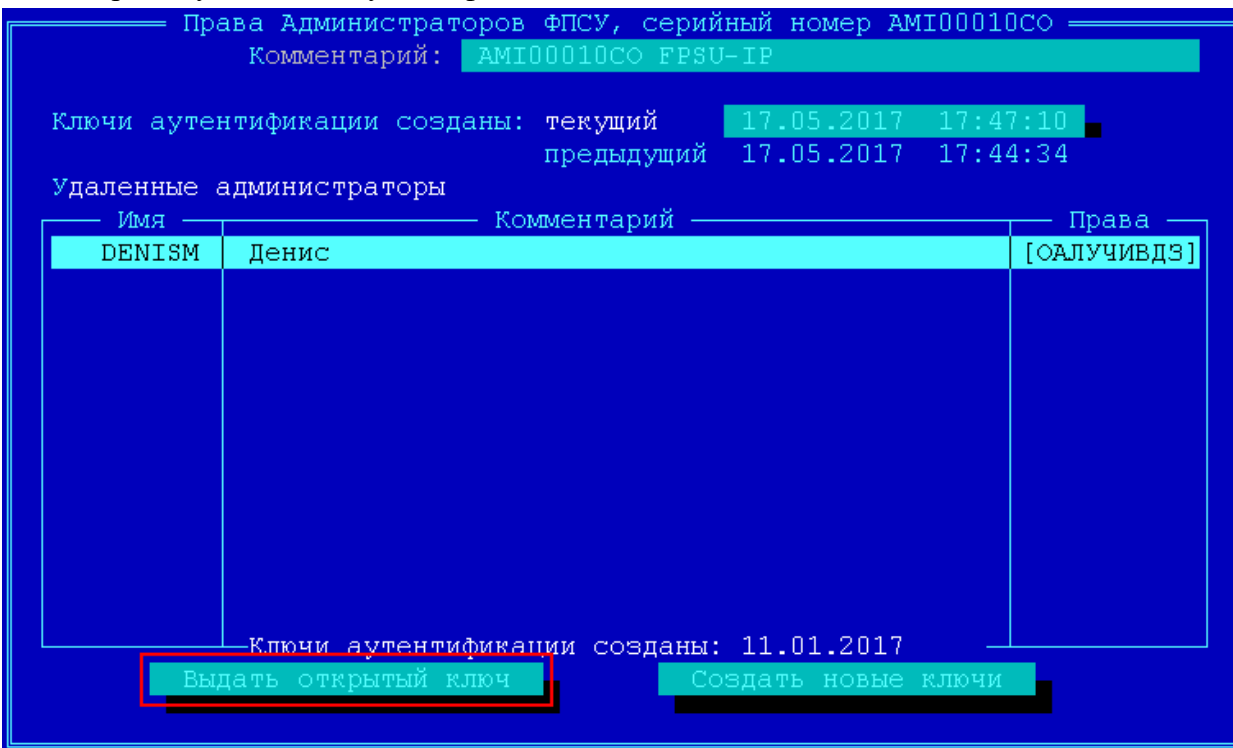


Рисунок 110 - Команда выдачи открытого ключа аутентификации ФПСУ-IP

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.

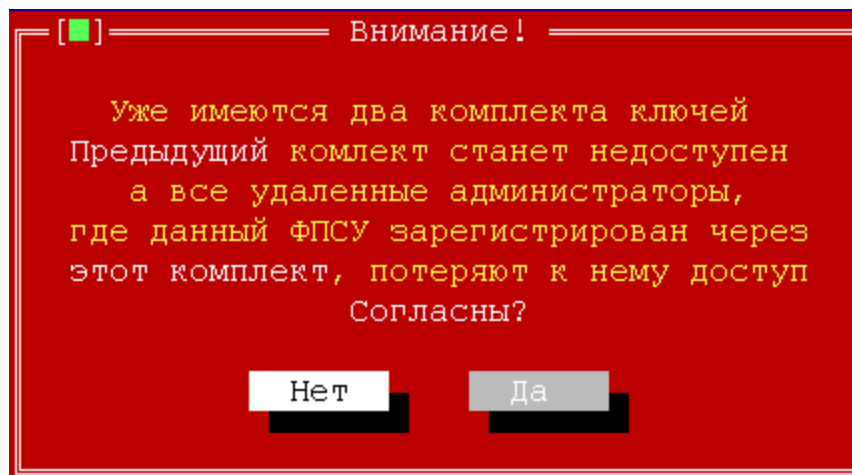


Рисунок 111 - Предупреждение при создании нового ключа аутентификации ФПСУ-IP

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.

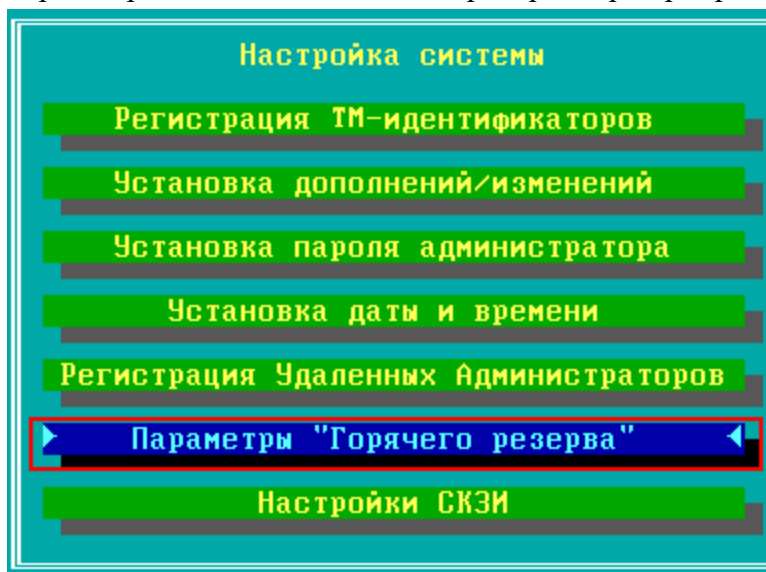


Рисунок 112 - Команда "Параметры "Горячего резерва"

Запуск команды доступен пользователям роли "Администратор" и выше. Для

функционирования пары ФПСУ-IP в режиме резервирования необходимо соединить кабелем передачи данных их сетевые адаптеры, сконфигурированные 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).

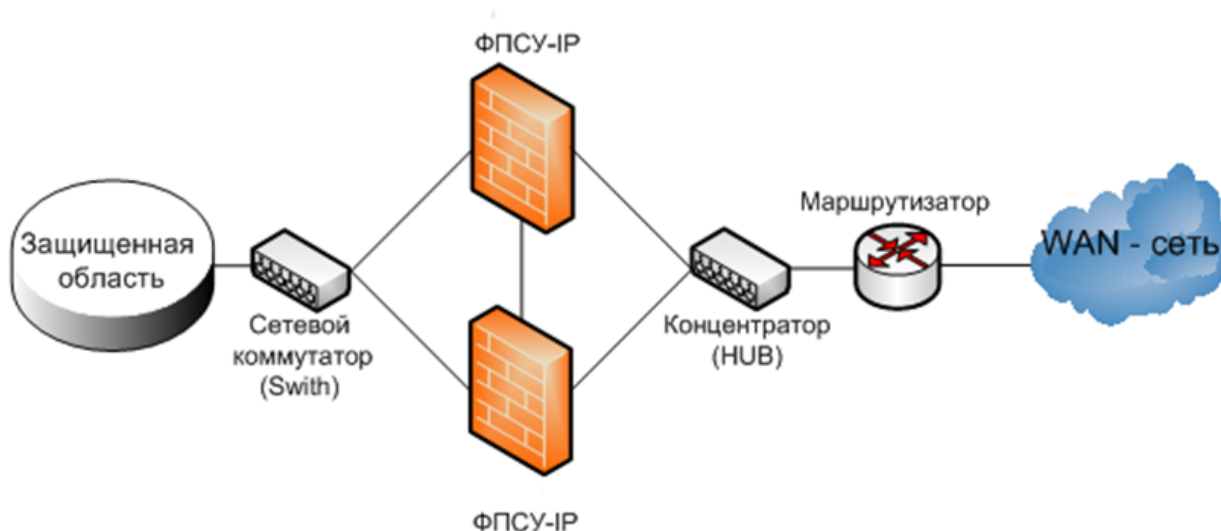


Рисунок 113 - Пример схемы подключения горячего резерва ФПСУ-IP

Обратите внимание на то, что в конфигурационных установках обоих ФПСУ-IP MAC-адреса сетевых адаптеров с одинаковыми номерами должны совпадать (см. раздел ["Конфигурация драйверов сетевых адаптеров"](#)).

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, оператор (любого класса) 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.

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 оператор 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 команды "Настройка системы" и "Параметры "Горячего резерва"";
2. Выставьте переключатель "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. Обратите внимание, что 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.

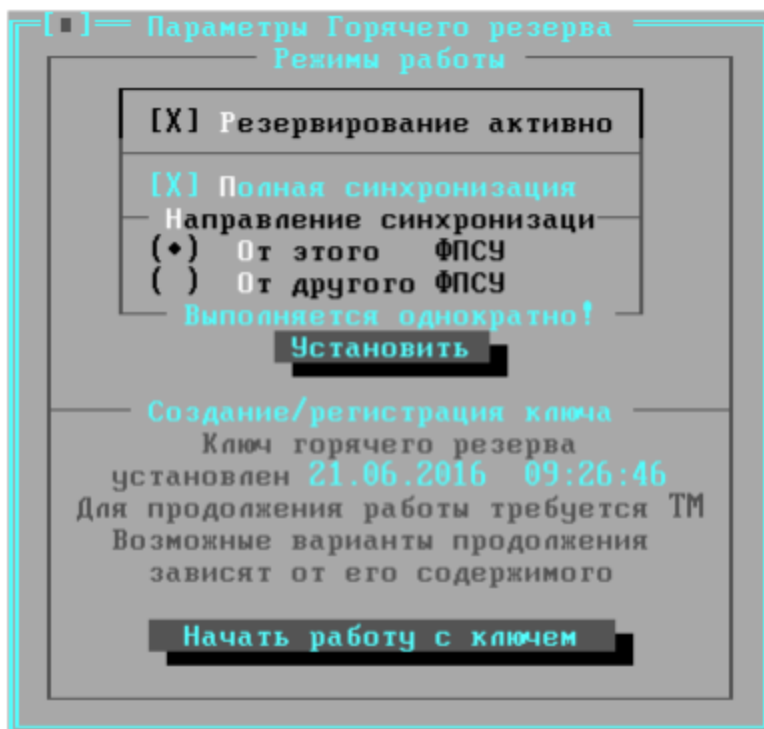


Рисунок 114 - Окно настроек работы горячего резерва

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»:

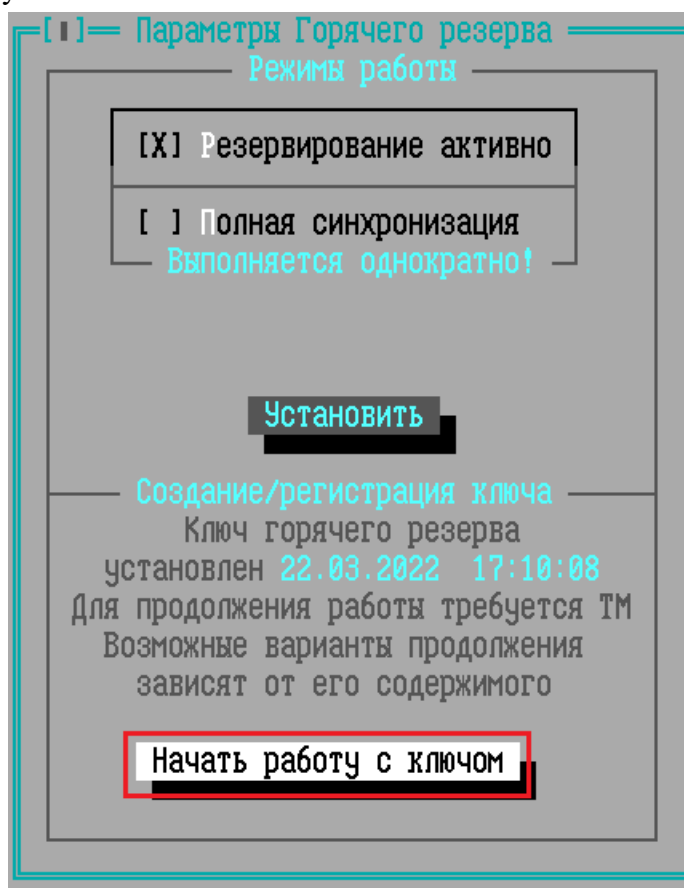


Рисунок 115 - Окно настроек горячего резерва

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

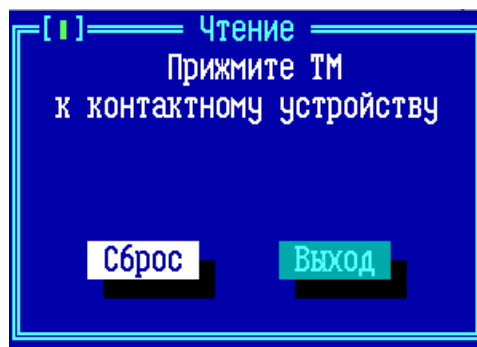


Рисунок 116 - Требование предъявить ТМ-идентификатор для ключа горячего резерва

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

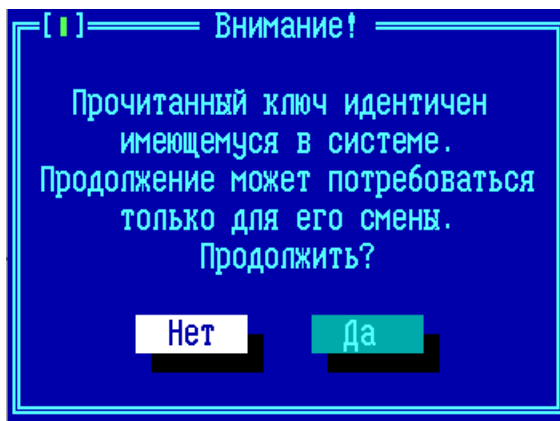


Рисунок 117 - Сообщение об имеющемся ключе горячего резерва

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

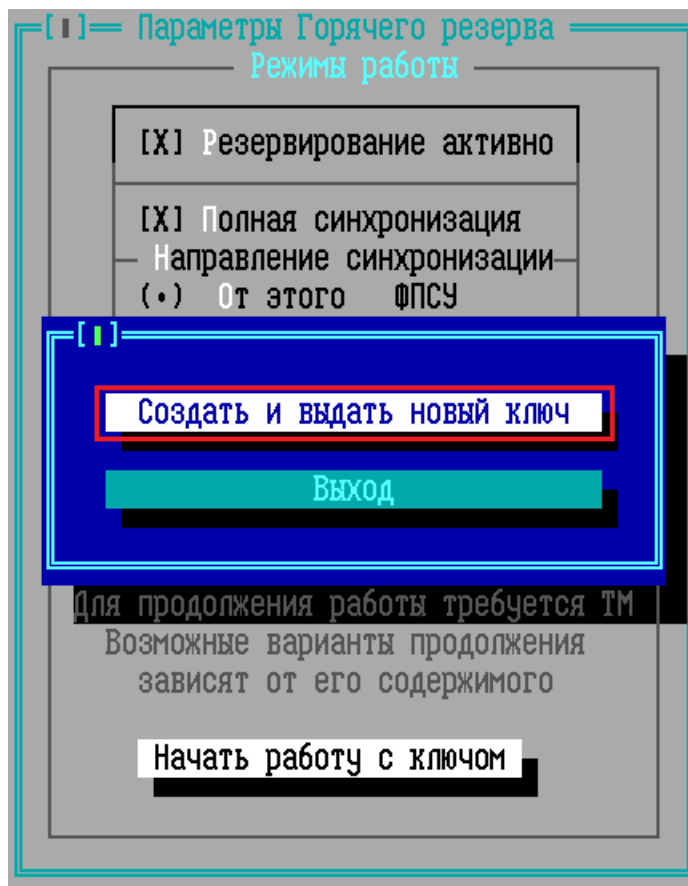


Рисунок 118 - Команда создания нового ключа горячего резерва

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

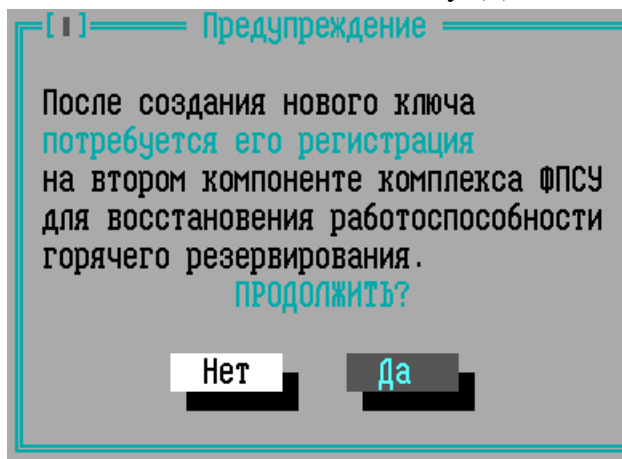


Рисунок 119 - Подтверждение выполнения команды

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

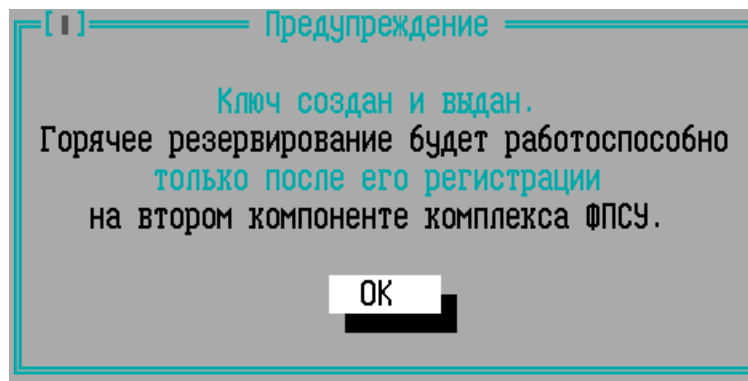


Рисунок 120 - Новый ключ горячего резерва создан и выдан на ТМ

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

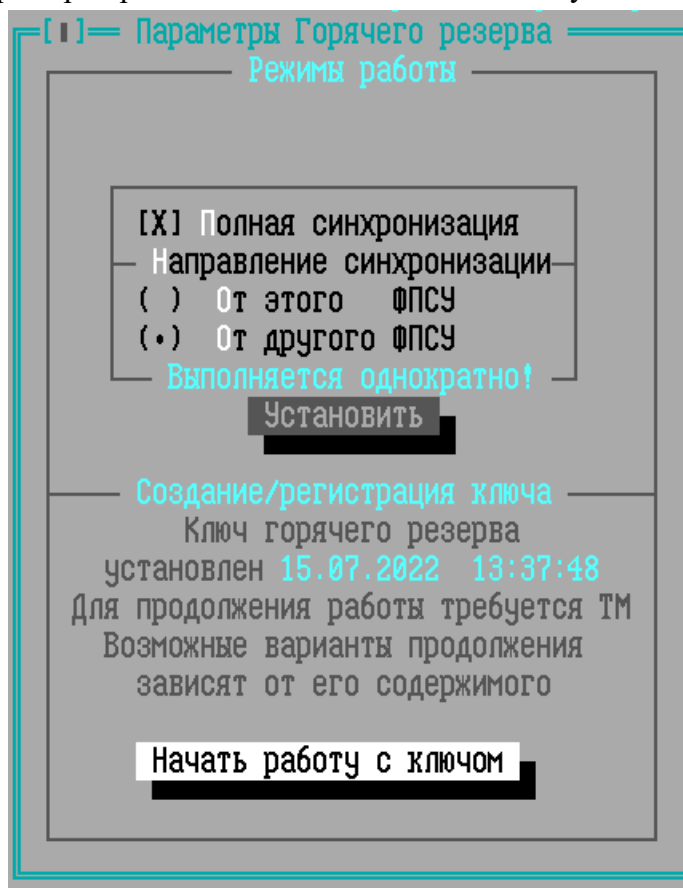


Рисунок 121 - Окно настроек горячего резерва на резервном ФПСУ-IP

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

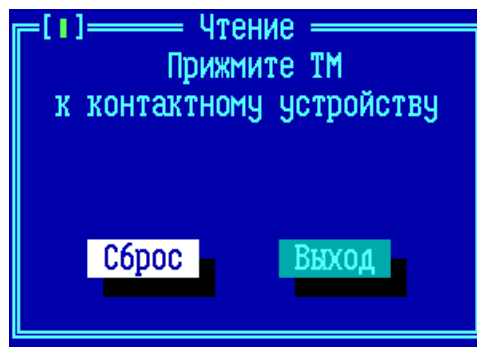


Рисунок 122 - Требование предъявить ТМ-идентификатор с новым ключом горячего резерва

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

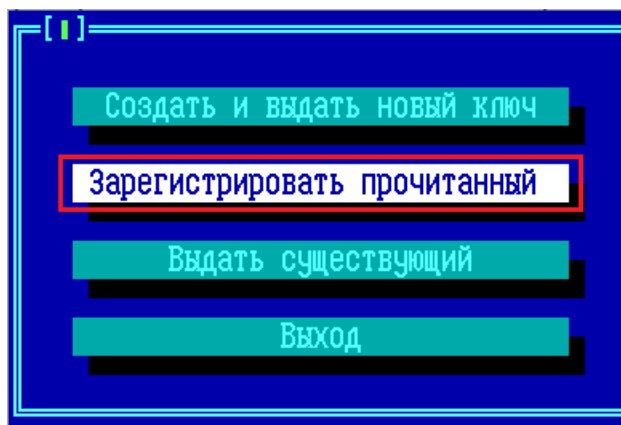


Рисунок 123 - Команда регистрации нового ключа горячего резерва на резервном ФПСУ

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

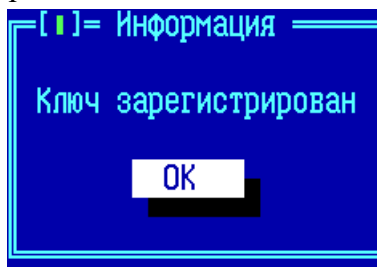


Рисунок 124 - Окончание регистрации нового ключа горячего резерва на резервном ФПСУ

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 прекратить работу ФПСУ-IP на скомпрометированном 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 установить 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. Установите курсор на переключатель *"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 выставления переключателя однократной синхронизации и до запуска подсистемы фильтрации) будет произведена после взаимного обмена между основным и резервным ФПСУ-IP. После этого флажок 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 отсутствия

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":

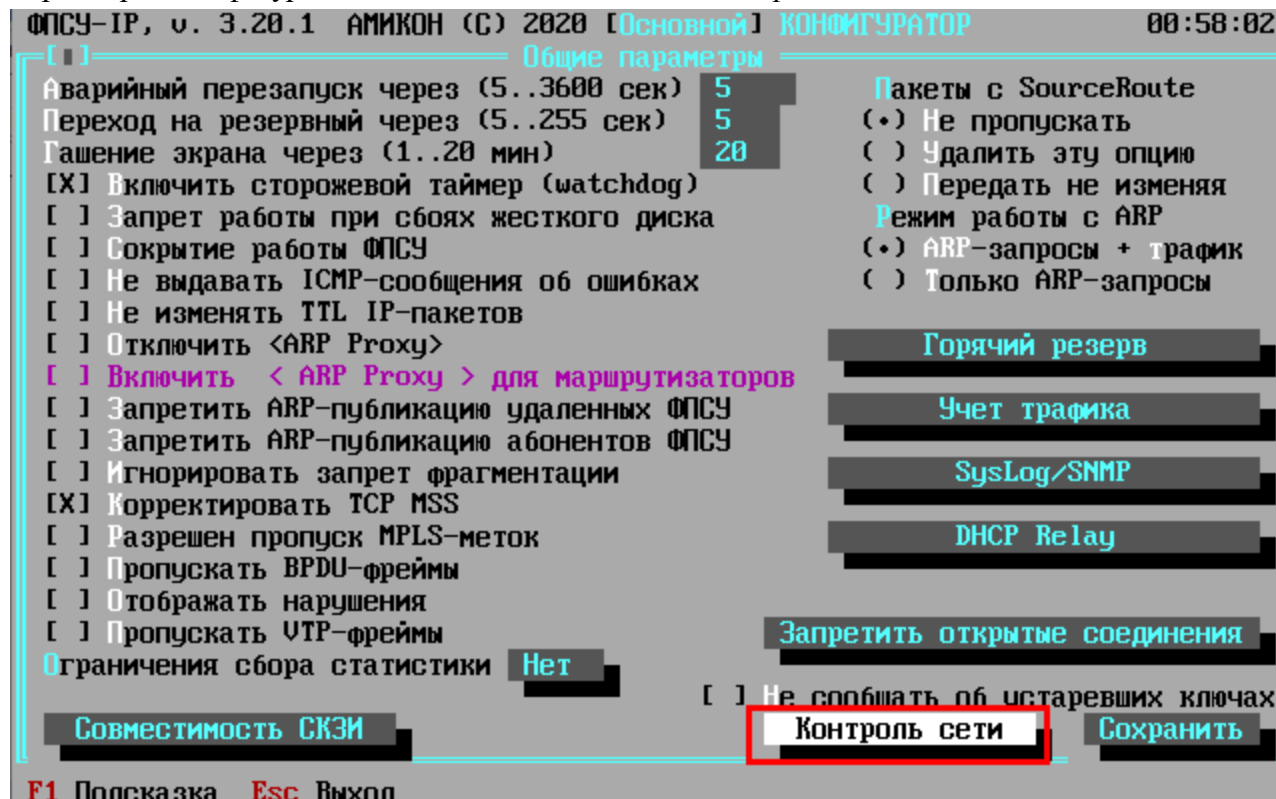


Рисунок 125 - Общие параметры ФПСУ-IP

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 "Host"](#)"). 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".

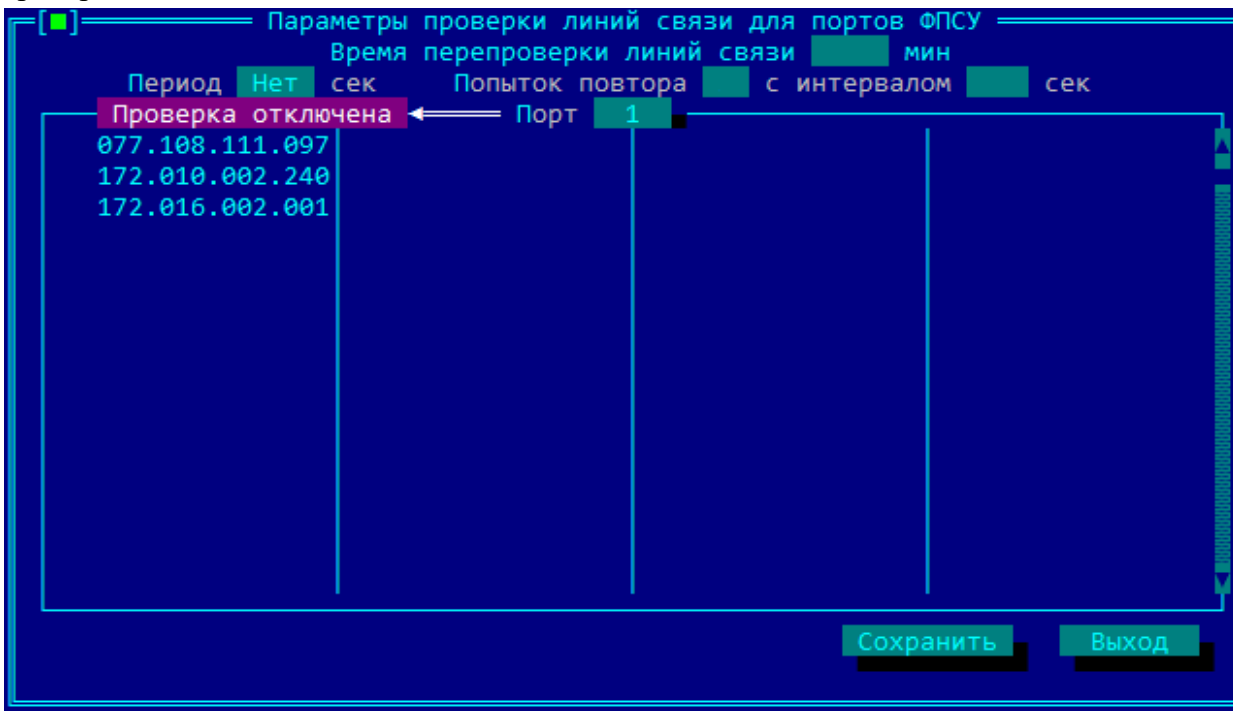


Рисунок 126 - Окно настройки параметров контроля связи

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 пере проверки 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 пере проверки 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, работающий в режиме горячего резервирования, будет проводить отдельную проверку для каждого порта следующим образом:

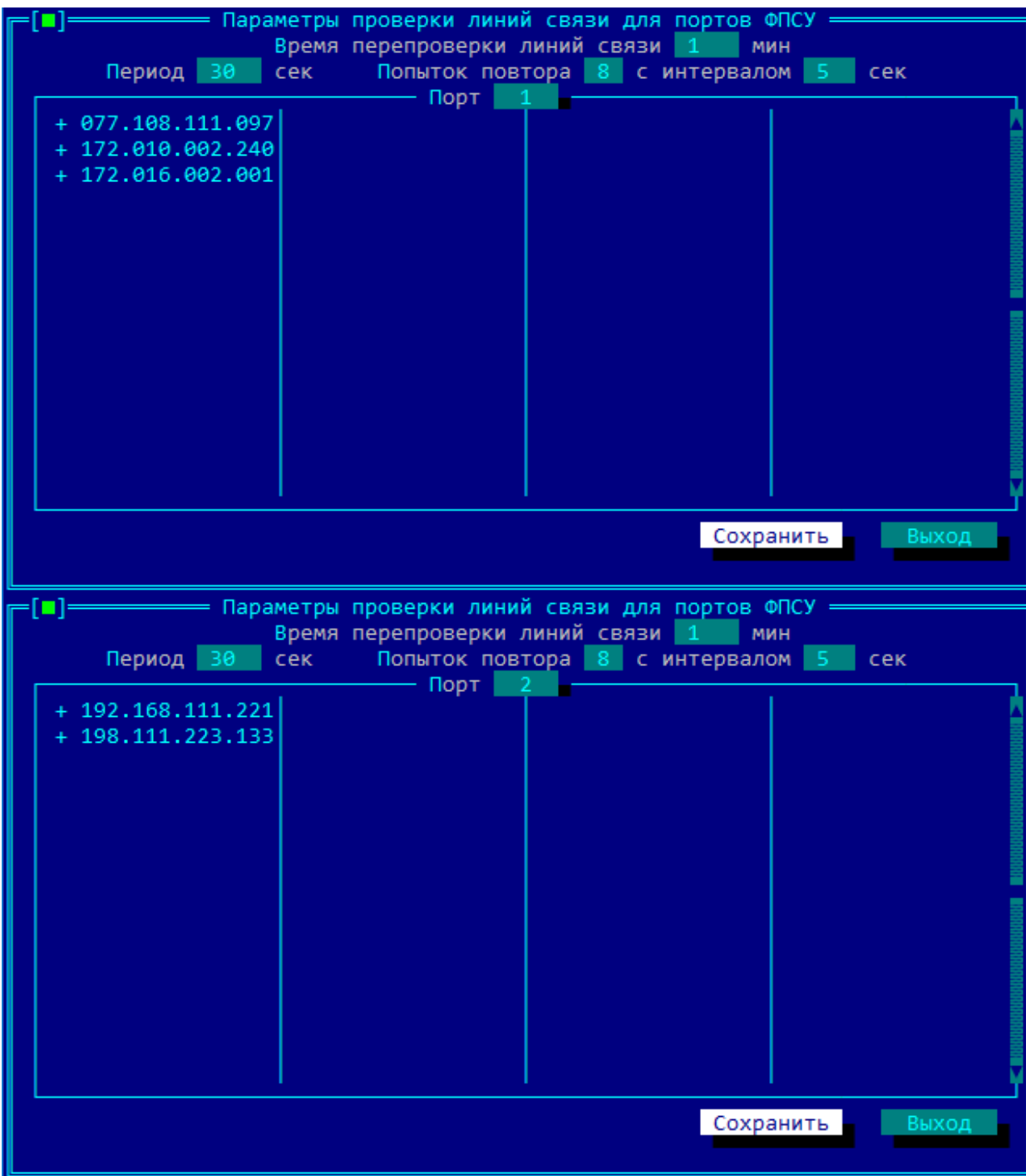


Рисунок 127 - Пример настройки системы проверки линий связи

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**, **172.016.002.001**, **172.010.002.240**, и эхо-запросы в адрес хостов второго порта **192.168.111.211**, **198.111.223.133**. 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.

#	Статус	Передано	Принято	Ошибочных	Node Address	Speed
*1	Готов	20660	20647	34	001b216e3998	1000 Mbps F
2	Готов	15456	15445	0	a4bf0129f834	1000 Mbps F
3	Готов	15460	15449	0	a4bf0129f835	1000 Mbps F

Готов	Время 25-04-2019 16:20:04
МЕСТНЫЙ - ОСНОВНОЙ	УДАЛЕННЫЙ - РЕЗЕРВНЫЙ
СОСТОЯНИЕ	СОСТОЯНИЕ
Работоспособность	Работоспособность
в работе	в резерве
ЧАСТИЧНАЯ	ЧАСТИЧНАЯ
нет канала связи	нет канала связи

Активен с: 16:18:14 25.04.2019 Alt-Tab, Ctrl-o - Сделать ПАССИВНЫМ

Рисунок 128 - Проверка линии связи неуспешна

Через 15 секунд (постоянный параметр) после становления активным, **ФПСУ№2**

начинает проверку доступности хостов первого порта **077.108.111.097**, **172.016.002.001**, **172.010.002.240** и проверку доступности хостов второго порта **192.168.111.211**, **198.111.223.133**.

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 таймер 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 "Настройка 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 129 - Меню настройки системы ФПСУ-IP

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



Рисунок 130 - 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 Настройки 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:

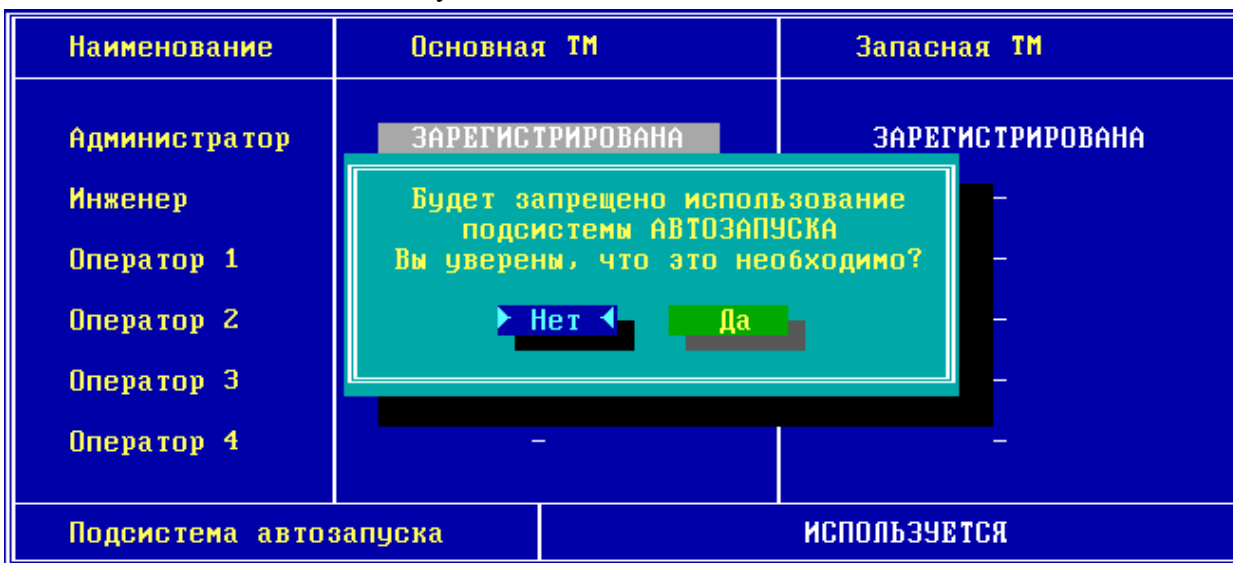


Рисунок 131 - Подтверждение отключения подсистемы автозапуска

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.

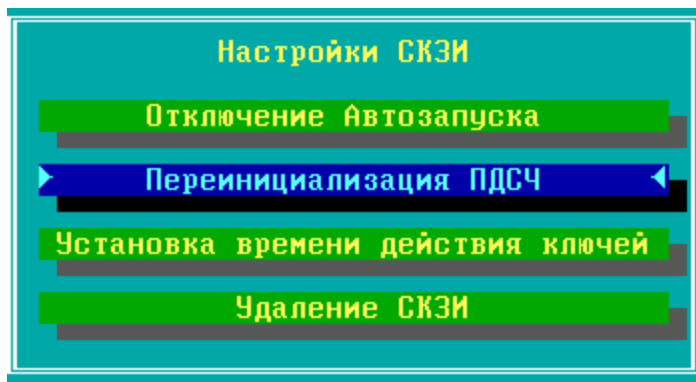


Рисунок 132 - Команда повторной инициализации ДСЧ

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



Рисунок 133 - 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.

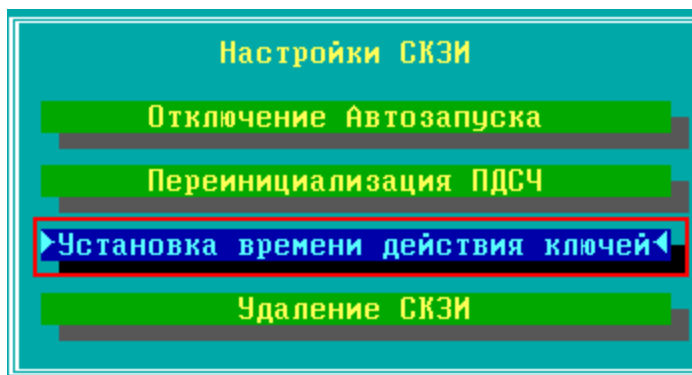


Рисунок 134 - Команда "Установка времени действия ключей"

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

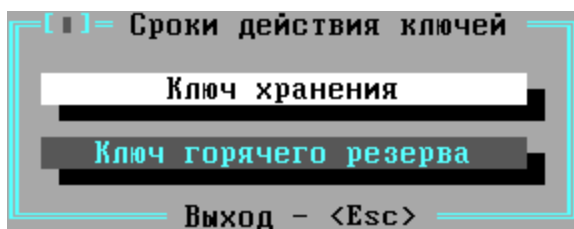


Рисунок 135 - Выбор типа ключа

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.

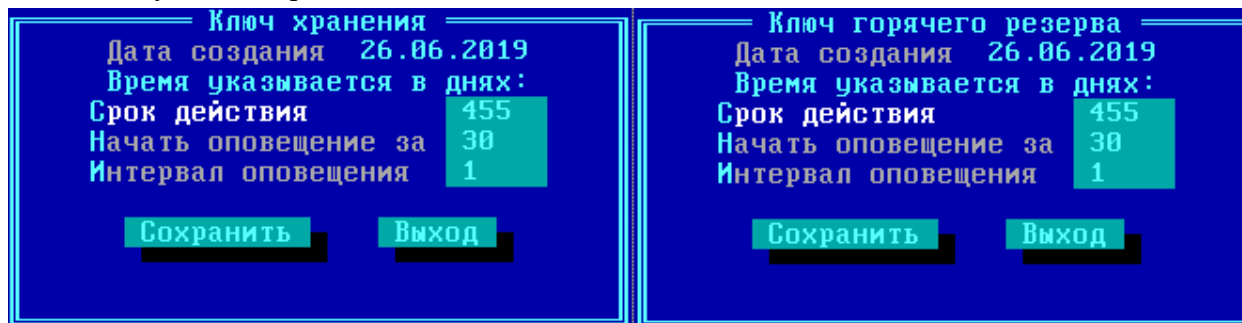


Рисунок 136 - Настройка сроков действия выбранного ключа

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 прекращения 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.

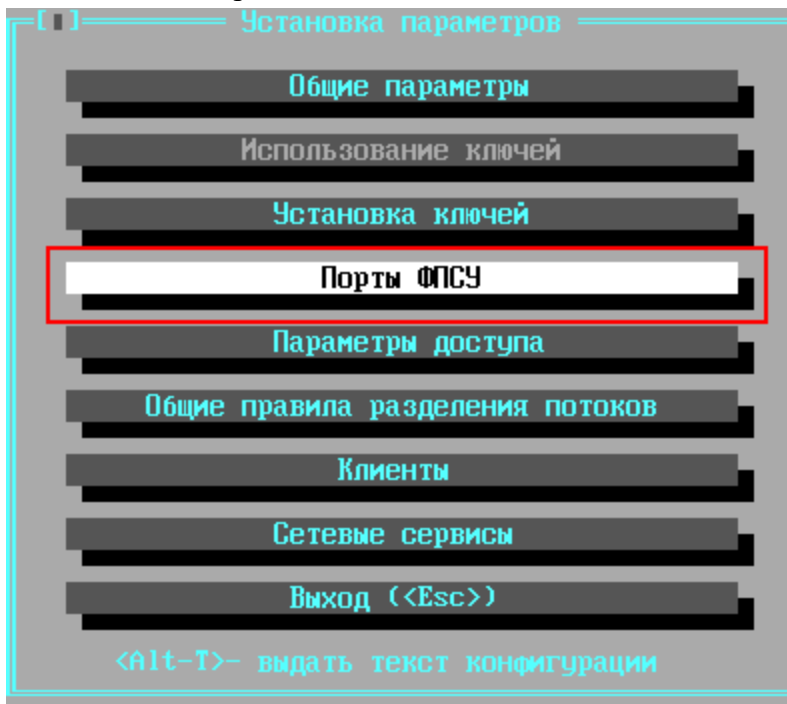


Рисунок 137 - Меню конфигурации ФПСУ-IP

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.

Порты ФПСУ					
N	Адрес порта	Маска подсети	Абонентов	Gateway	ФПСУ
1	010.010.010.003	255.255.255.000	11	1	1
2	100.000.000.001	255.255.255.000	0	0	0

Рисунок 138 - 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.

Порт 2 Адрес 192.168.000.036 Маска 255.255.255.000 Тип порта ВНУТРЕННИЙ Выполнение "Gratuitous ARP" [] Без проверки

Маршрутизаторы
192.168.000.020

ФПСУ
ФПСУ НЕ ОПРЕДЕЛЕНА

Имя	Абоненты	Тип	VLAN
077.088.021.003	Хост		2
192.168.000.001	Хост		
192.168.000.019	Хост		4

192.168.000.020 192.168.000.001 Хост

< F2 >
Сохранить

F1 Подсказка Esc Выход 363393

Рисунок 139 - Установка параметров порта

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

по нажатию клавиш << > или <> >.

Окно содержит следующие параметры порта ФПСУ-IP:

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

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, и настройки DHCP-Relay для адресов этого порта. 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](#)". По умолчанию, DHCP-Relay для порта не работает, информацию о настройке DHCP-Relay см. пункт "[DHCP-Relay](#)".

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 в появившемся окне число необходимых значащих разрядов (от 8 до 30), в таком случае ФПСУ-IP рассчитает значение маски автоматически.

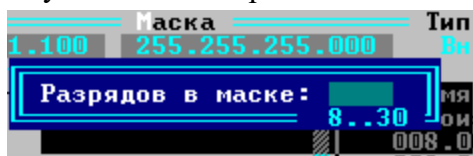


Рисунок 140 - Ввод числа необходимых разрядов

Оба порта ФПСУ-IP, и 1, и 2, могут иметь один и тот же IP-адрес в одной и той же подсети (Примечание: 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. п. "[Общие параметры конфигурации ФПСУ-IP](#)"). Внутренний порт логически обозначает сетевой интерфейс, к которому подключается защищаемая локальной сети, 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".

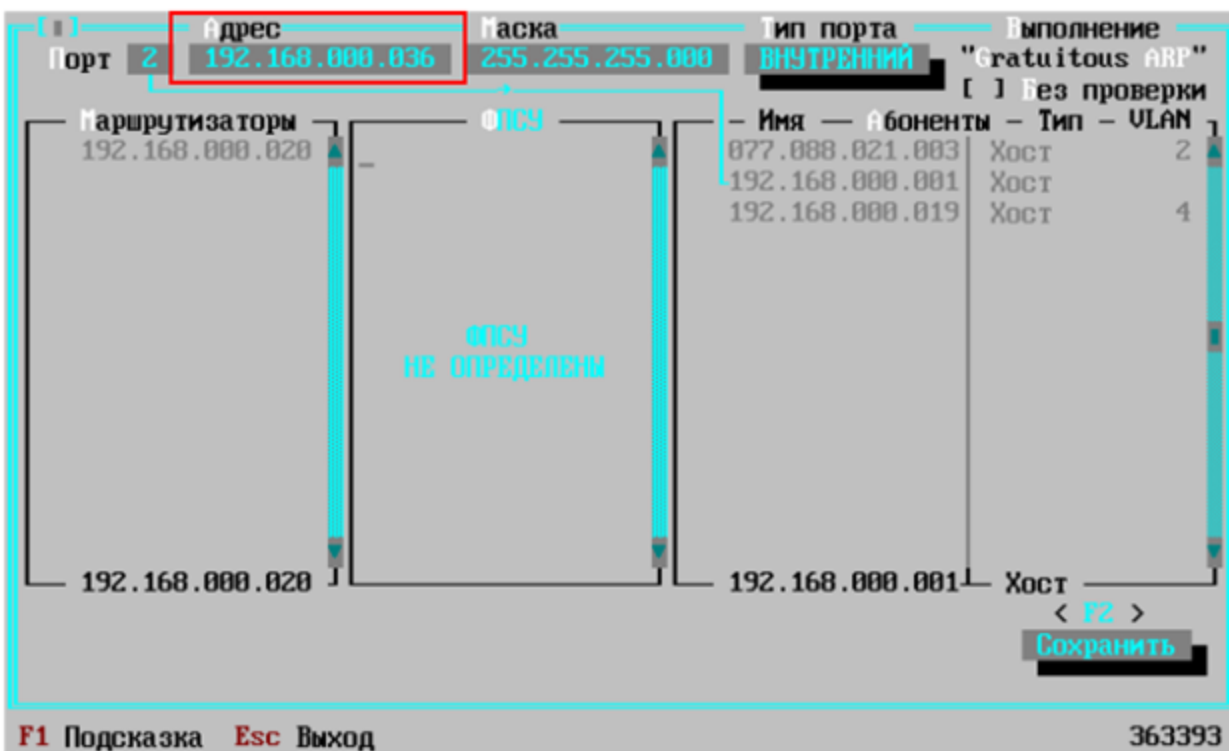


Рисунок 141 - Порт ФПСУ-IP

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;
- **Маска** — маска IP-адреса порта ФПСУ-IP в описываемом VLAN;
- **DHCP Relay** — необязательная опция, позволяющая выбрать основной и дополнительный сервер, куда будут ретранслироваться DHCP-запросы абонентов данного VLAN (подробнее см. пункт "[DHCP-Relay](#)").

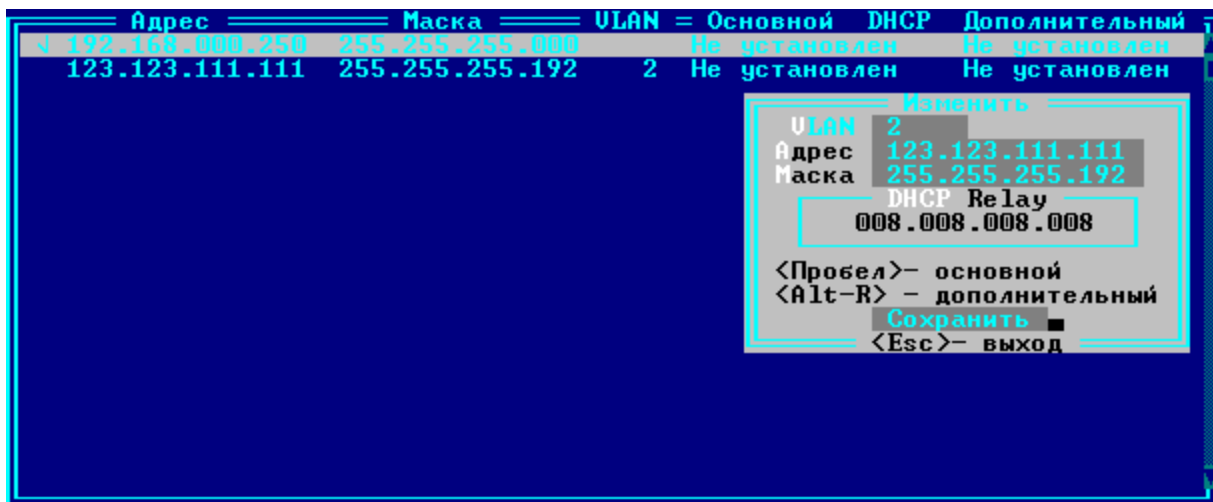


Рисунок 142 - Настройка VLAN на порту ФПСУ-IP

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 .

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.

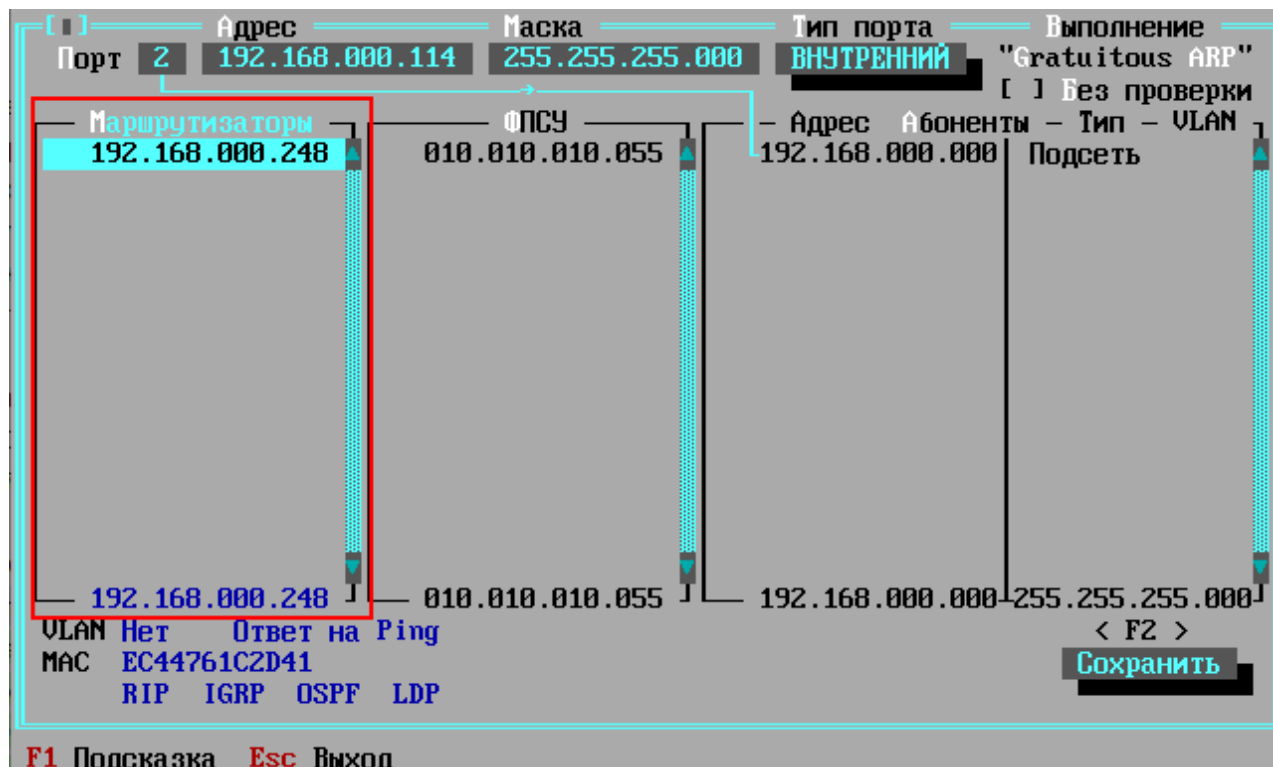


Рисунок 143 - Маршрутизаторы порта ФПСУ-IP

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:

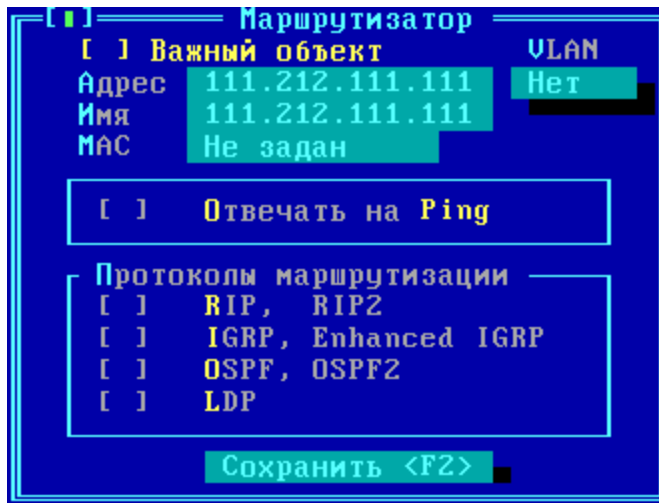


Рисунок 144 - Параметры маршрутизатора

Важный объект – переключатель, который 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;

VLAN – номер виртуальной локальной сети, в которой участвует маршрутизатор, если требуется;

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>. Обратите внимание, что 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 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.

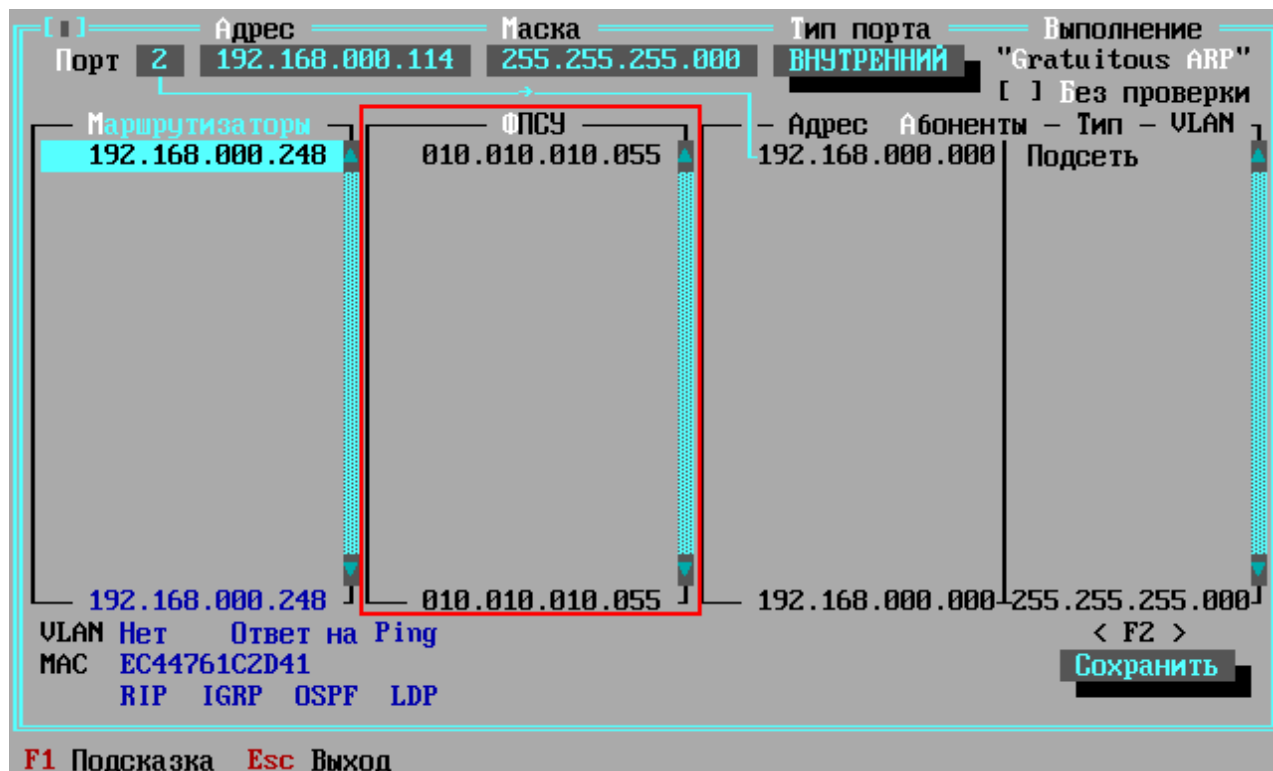


Рисунок 145 - описатели удаленных ФПСУ порта

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.

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:

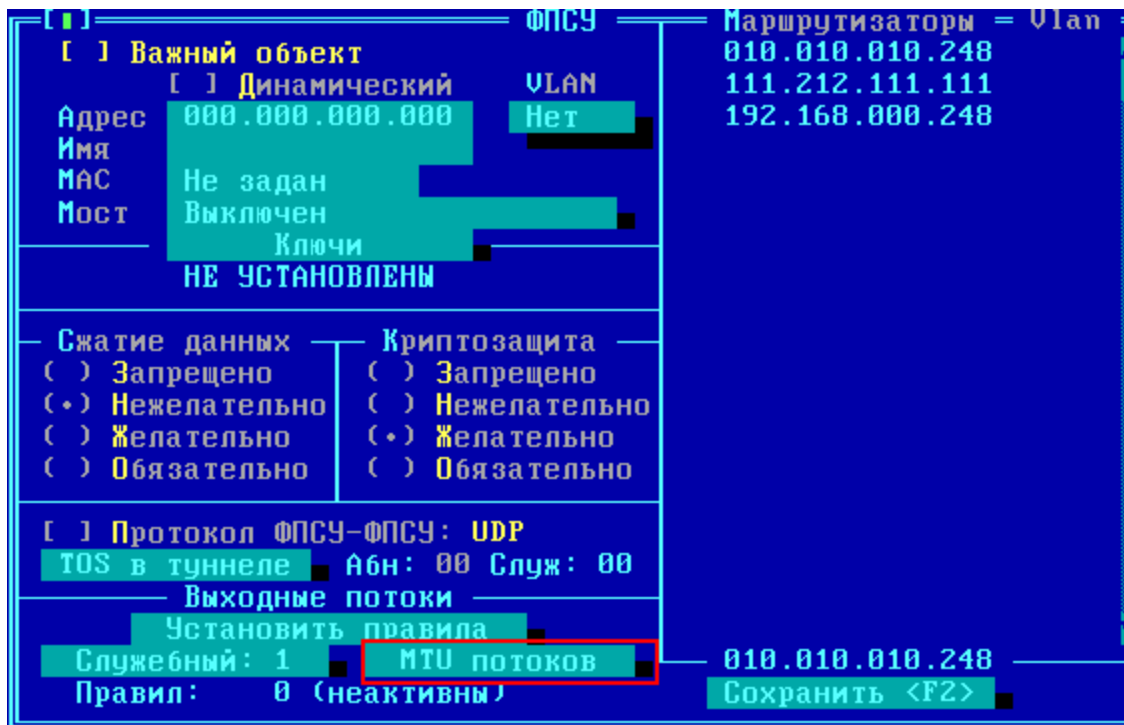


Рисунок 146 - Настройка удаленного ФПСУ-IP

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 одноименную строку и нажмите <Пробел>. В открывшемся окне укажите криптосеть, номер и комплект используемых другим ФПСУ-IP ключей (комплект указывается только для ключей класса КС2).



Рисунок 147 - 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 "Установить" (клавишей <F2>), после чего произойдет возврат в окно "Параметры ФПСУ".

Маршрутизаторы - маршрутизаторы, через которые может осуществляться связь с описываемым удаленным ФПСУ-IP. Окно содержит список маршрутизаторов, которые ранее 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 (знаком "> "), 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.

Когда все требуемые параметры в окне "*Параметры ФПСУ*" определены, следует активизировать команду "*Установить*" 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 отображены 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 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:

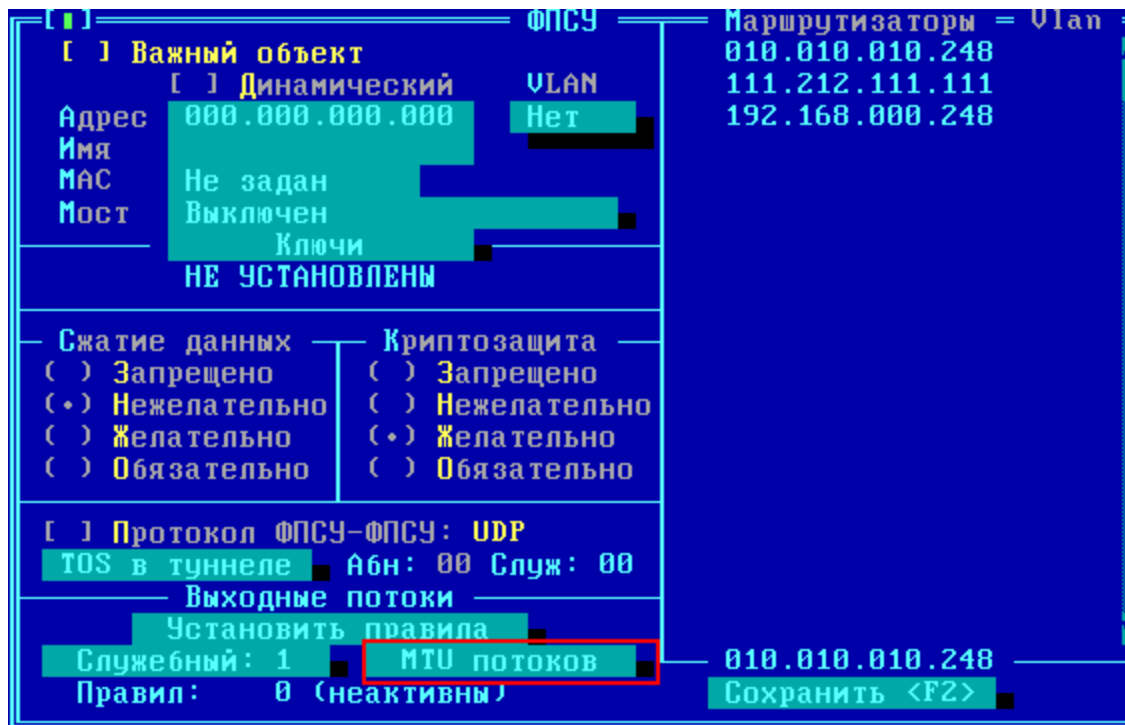


Рисунок 148 - Настройка удаленного ФПСУ-IP

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

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

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.

MAC-адрес — аппаратный адрес удаленного ФПСУ-IP, устанавливается в справочных целях. По указанному адресу конфигурируемый ФПСУ-IP будет выполнять первичный ARP-запрос. Если не установлен, то физический адрес партнера ФПСУ-IP по туннелированию будет определен в обычном режиме.

Сжатие - указание ФПСУ-IP при работе с удаленным ФПСУ-IP использовать режим

проходного архивирования передаваемых данных, уменьшая объем передаваемого трафика. Обратите внимание, что 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).

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

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			
	<i>запрещено</i>	<i>нежелательно</i>	<i>желательно</i>	<i>обязательно</i>
<i>запрещено</i>	не используется	не используется	не используется	<u>соединение не состоится</u>
<i>нежелательно</i>	не используется	не используется	используется	используется
<i>желательно</i>	не используется	используется	используется	используется
<i>обязательно</i>	<u>соединение не состоится</u>	используется	используется	используется

9.3.2. Потоки 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":

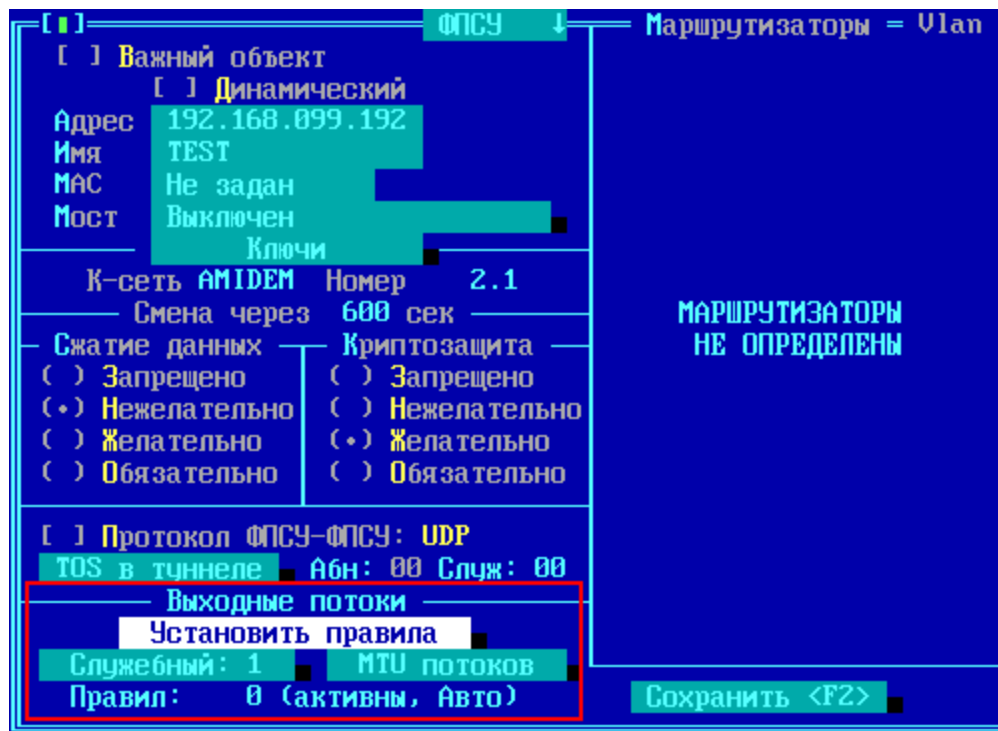


Рисунок 149 - Поле настроек выходных потоков в туннеле между ФПСУ-IP

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 150 - Окно установки правил потоков для удаленного ФПСУ-IP

Потоки могут распределяться вручную администратором, исходя из индивидуальных устанавливаемых правил. Альтернативный вариант: автоматическое случайное распределение пакетов по потокам, которое включает опция "Автораспределение 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 "Автораспределение 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 "Автораспределение потоков" для оптимизации использования многоядерных маршрутизаторов, то рекомендуется устанавливать значение, которое равно или превышает число ядер маршрутизатора.

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

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

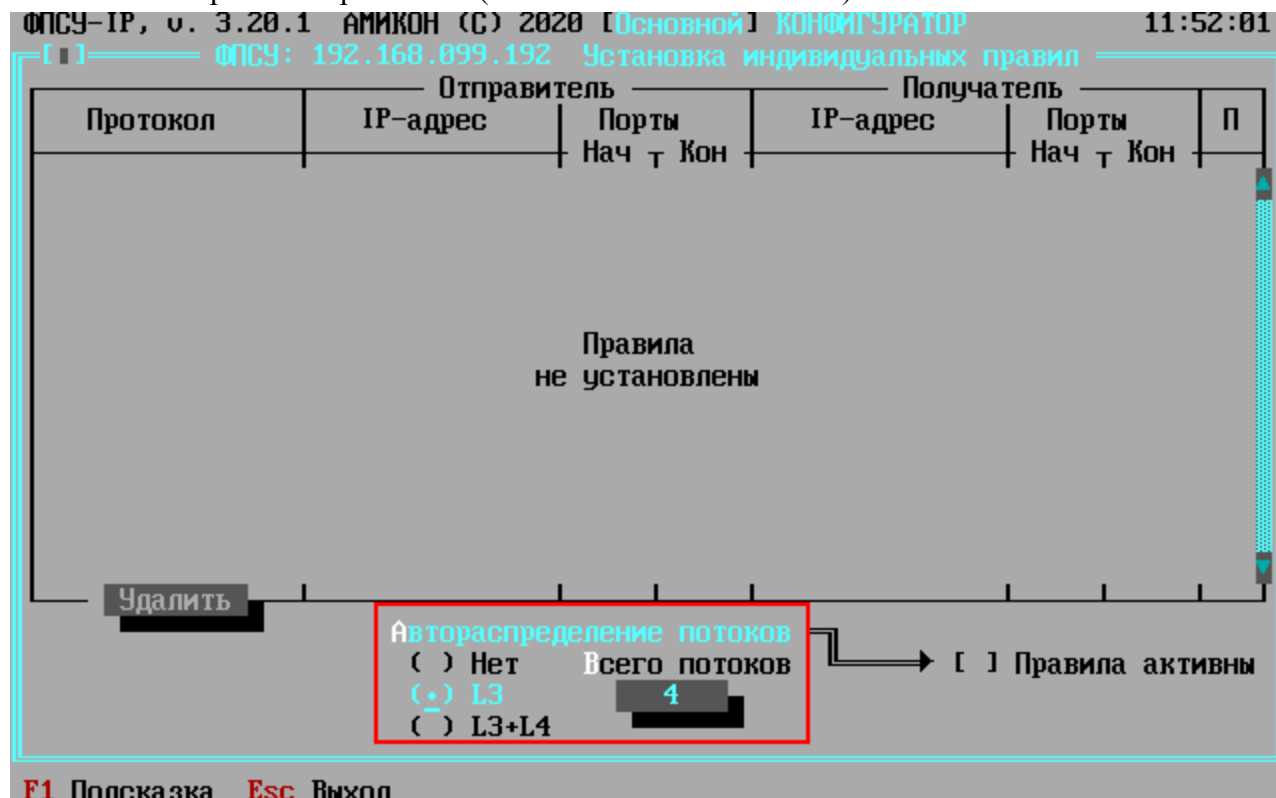


Рисунок 151 - Окно установки правил потоков для удаленного ФПСУ-IP

Если администратор поставил опцию "Автораспределение 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 152 - Окно создания правила для нового потока

Чтобы все описанные правила (или автораспределение потоков) использовались при работе VPN-туннеля, необходимо включить переключатель "Правила активны" в окне "Установка индивидуальных правил".

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.

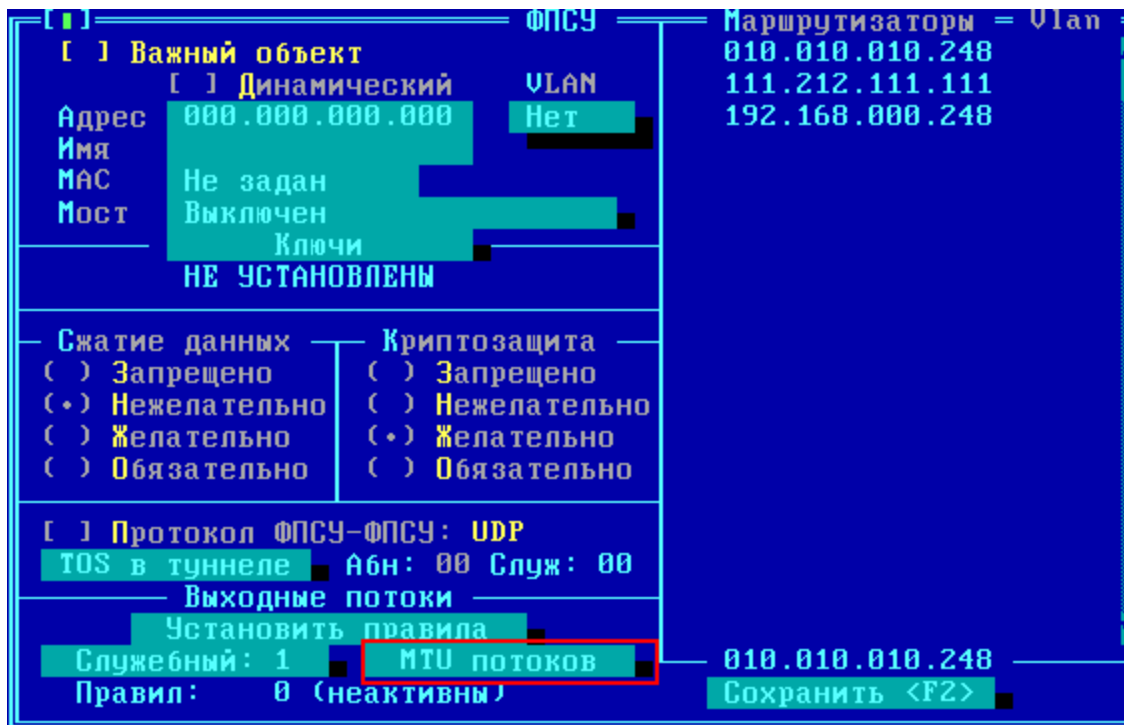


Рисунок 153 - Настройка удаленного ФПСУ-IP

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 (Обратите внимание, что 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>.

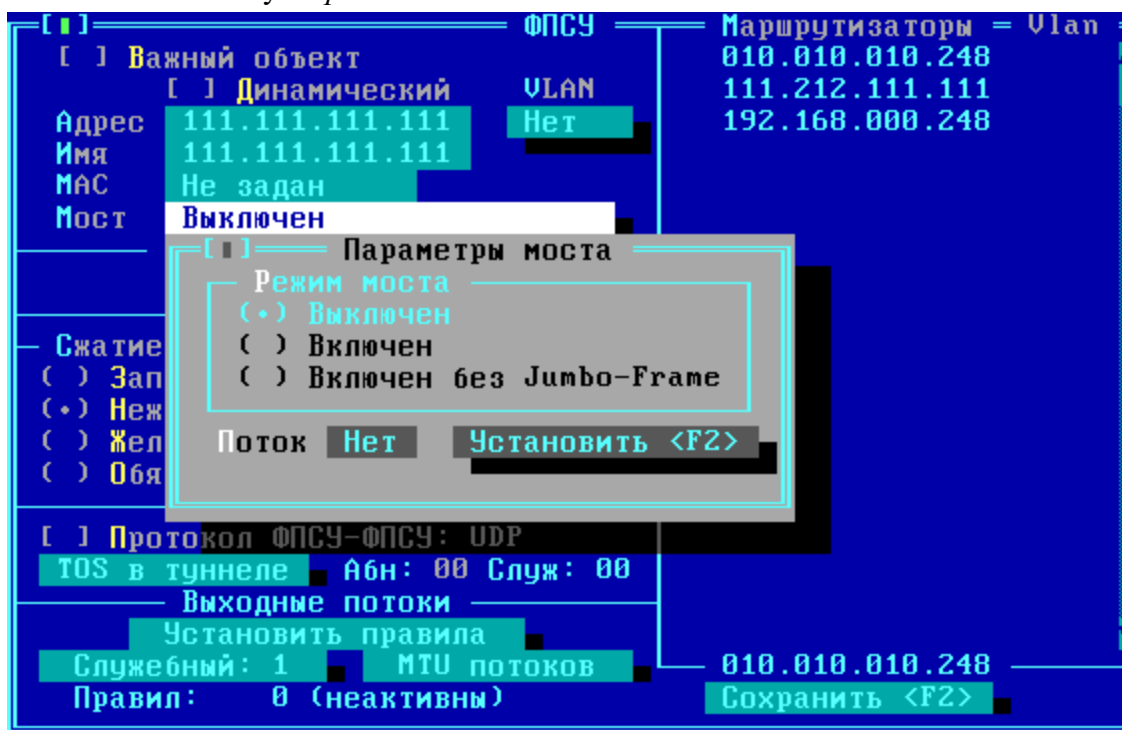


Рисунок 154 - Режим моста ФПСУ-ФПСУ

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. **Обратите 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. "[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 входящие 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, 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. Для пакетов, отправленных в MAC-адрес портов ФПСУ, 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, имеющему мостовой туннель. При задействованном механизме ARP-прогу в локальной сети может произойти обновление ARP-таблиц рабочих станций, и абоненты начнут обращаться в MAC-адрес ФПСУ, 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.

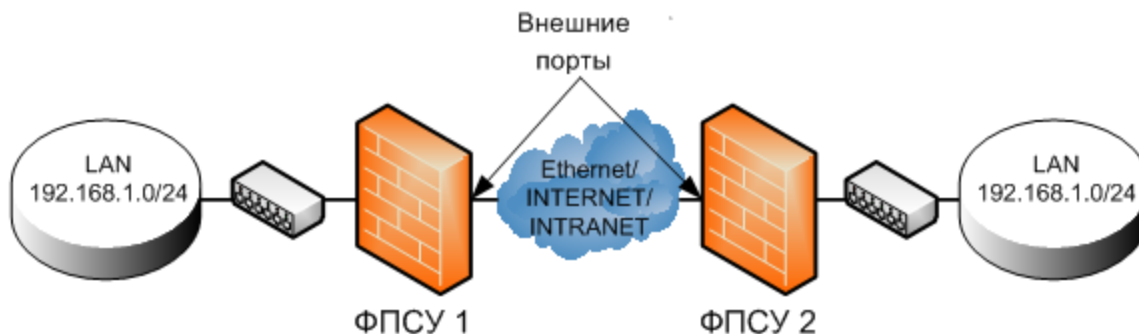


Рисунок 155 - Режим моста в туннеле ФПСУ-ФПСУ

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-IP 1 и ФПСУ-IP 2 создать описатель партнера по шифрованию и включить режим моста для туннеля ФПСУ-IP 1 - ФПСУ-IP 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".

Нажмите кнопку "Установить" или клавишу <F2> для выхода из окна с сохранением выполненных изменений, и клавишу <Esc> для выхода без сохранения.

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.

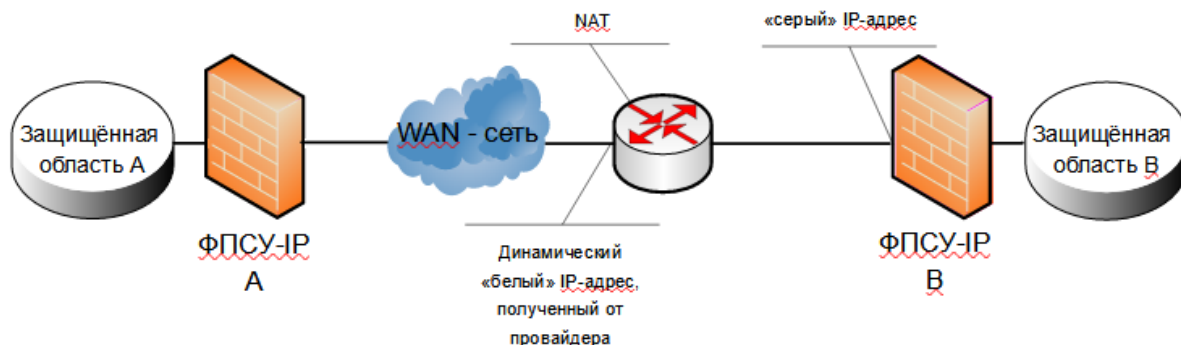


Рисунок 156 - Схема при установлении динамического туннеля с другим ФПСУ-IP

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:

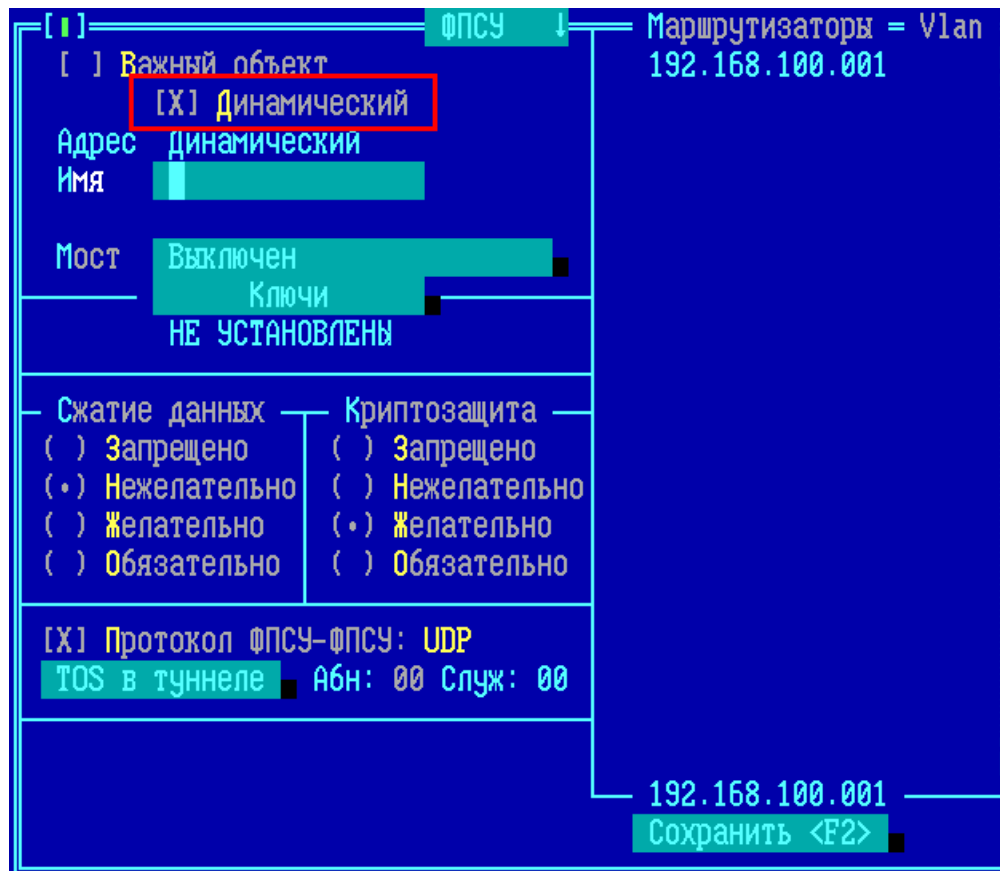


Рисунок 157 - Динамический туннель с другим ФПСУ-IP

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 отправляется 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 межсетевого экрана на ФПСУ-IP.

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

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

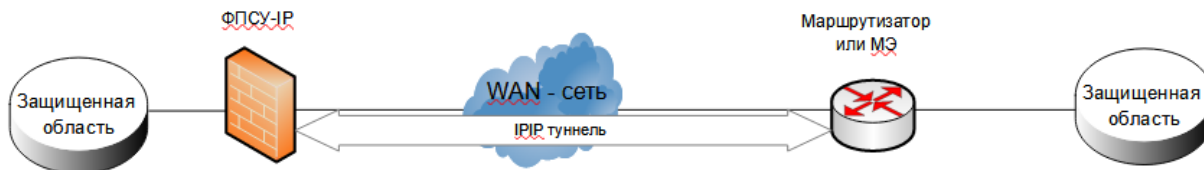


Рисунок 158 - Режим IP-туннеля ФПСУ-ФПСУ

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.

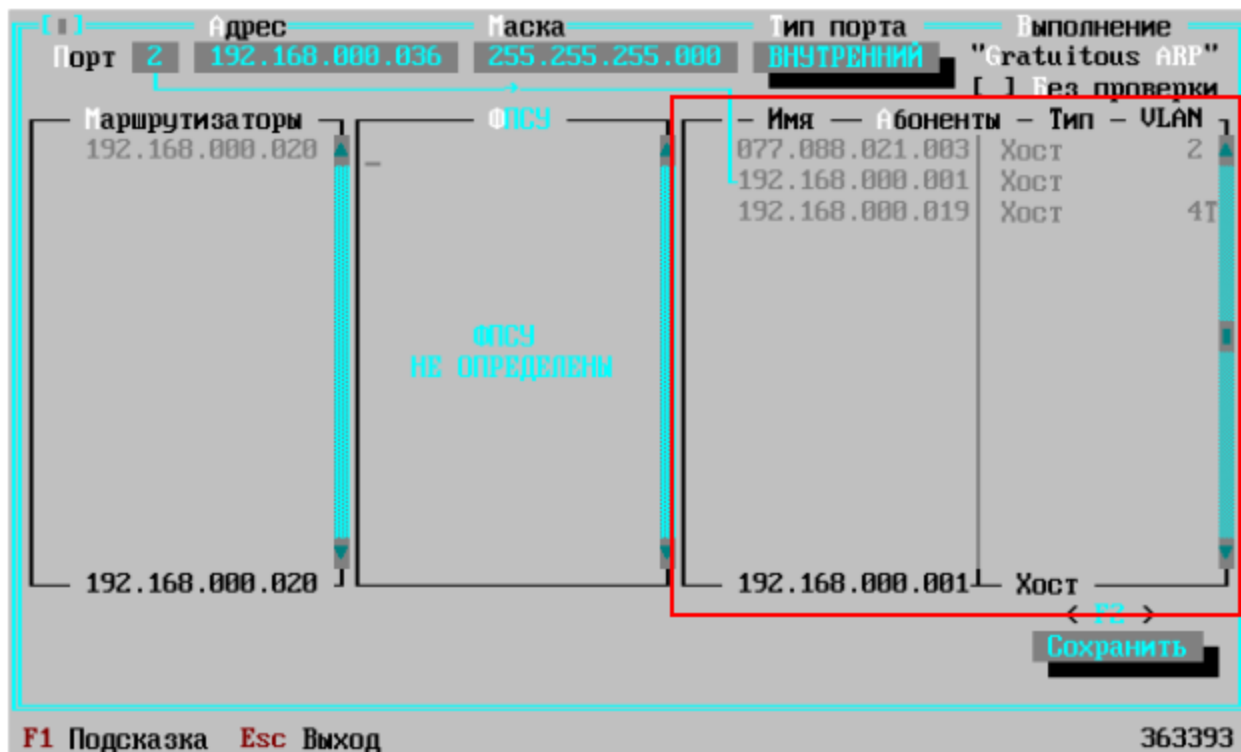


Рисунок 159 - Абоненты порта ФПСУ-IP

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 "[Host](#)");
- пары адрес/маска подсети (запись типа "[Подсеть](#)");
- специальный адрес "[Любой Host](#)".

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 32768 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 "*Параметры абонента*", 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 "*Параметры абонента*" установите тип адреса

абонента.

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 "Host"](#)", "[Описание абонента "Подсеть"](#)" и "[Описание абонента "Любой Host"](#)".

Для удаления описателя абонента из списка, выделите его курсором, нажмите клавишу и подтвердите выполнение команды.

Для удаления нескольких абонентов одновременно нажмите сочетание клавиш <Ctrl- Del> или <Ctrl-D>. Появится окно со списком абонентов порта.

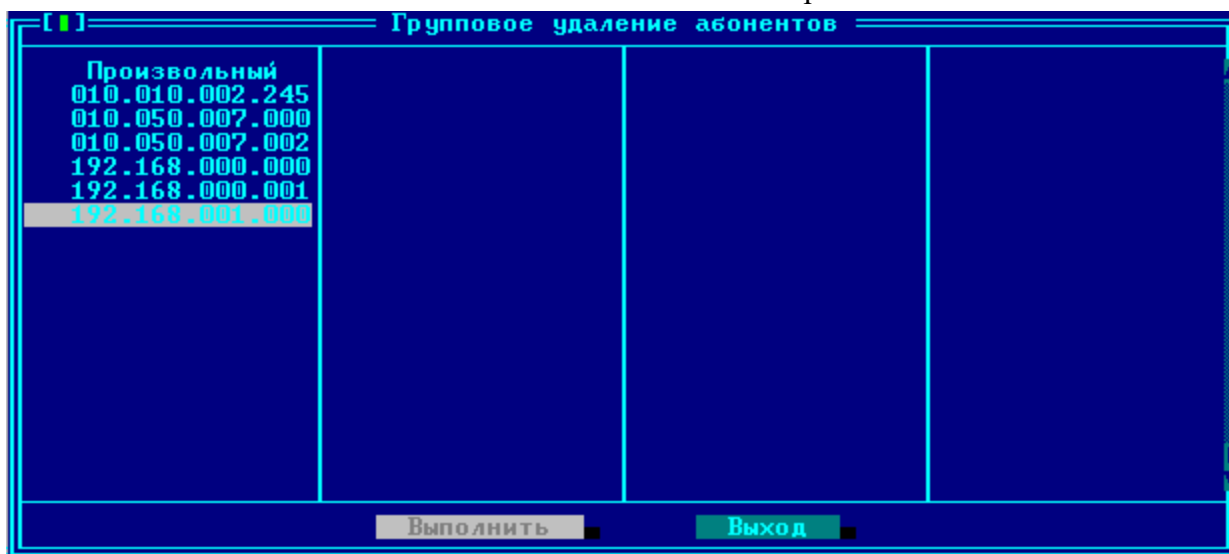


Рисунок 160 - Групповое удаление абонентов

При нажатии кнопки "Выполнить", все отмеченные описатели будут удалены. Для пометки 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 к окну порта ФПСУ-IP.

9. 4. 1. Описание абонента "Host"

Записи типа "Host" 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:

Абонент		Маршрутизаторы	Ulan
(*) Host	<input type="checkbox"/> Важный	111.221.212.120	
() Подсеть	объект	192.168.000.249	
() Любой Host			
Поток	Нет		
Адрес	123.010.001.001		
Имя	123.010.001.001		
MAC	Не задан		
<input type="checkbox"/> Проверять MAC			
Режим работы			
<input checked="" type="radio"/> Ретрансляция			
() Через ФПСУ			
Режим партнера			
Данного порта			
<input type="checkbox"/> Ретрансляция			
<input type="checkbox"/> Через ФПСУ			
Другого порта			
<input checked="" type="checkbox"/> Ретрансляция			
<input checked="" type="checkbox"/> Через ФПСУ			
<input type="checkbox"/> Отвечать на Ping		192.168.000.249	
<input checked="" type="checkbox"/> Работа разрешена			Сохранить <F2>

Рисунок 161 - Параметры абонента типа хост, режим "Ретрансляция"

Абонент		Линии ФПСУ	Ulan
(*) Host	<input type="checkbox"/> Важный	0→010.010.010.055	
() Подсеть	объект	P→010.010.010.056	
() Любой Host		010.010.010.057	
Поток	Нет	010.010.010.058	
Адрес	123.010.001.001		
Имя	123.010.001.001		
Режим работы			
() Ретрансляция			
<input checked="" type="radio"/> Через ФПСУ			
Режим партнера			
Данного порта			
<input type="checkbox"/> Ретрансляция			
<input type="checkbox"/> Через ФПСУ			
Другого порта			
<input checked="" type="checkbox"/> Ретрансляция			
<input checked="" type="checkbox"/> Через ФПСУ			
<input type="checkbox"/> Отвечать на Ping		010.010.010.055	
<input checked="" type="checkbox"/> Работа разрешена		Alt-S - поменять	
		Пробел - основная	
		Alt-R - резервная	
		Сохранить <F2>	

Рисунок 162 - Параметры абонента типа хост, режим "Через ФПСУ"

Важный объект – переключатель, который 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;

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.

Проверить MAC – Только для абонентов типа "Хост", работающих в режиме "Ретрансляция". Требуется заполненное поле **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).

Режим работы "*Ретрансляция*" (фильтрация без аутентификации).

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 А" это будут абоненты "a1", "a2", "b1" и "b2"; для "ФПСУ-IP В" это будут абоненты "b1", "b2", "In1" и "In2"; а для ФПСУ-С 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. п. ["Описание параметров удаленных ФПСУ-IP"](#)).

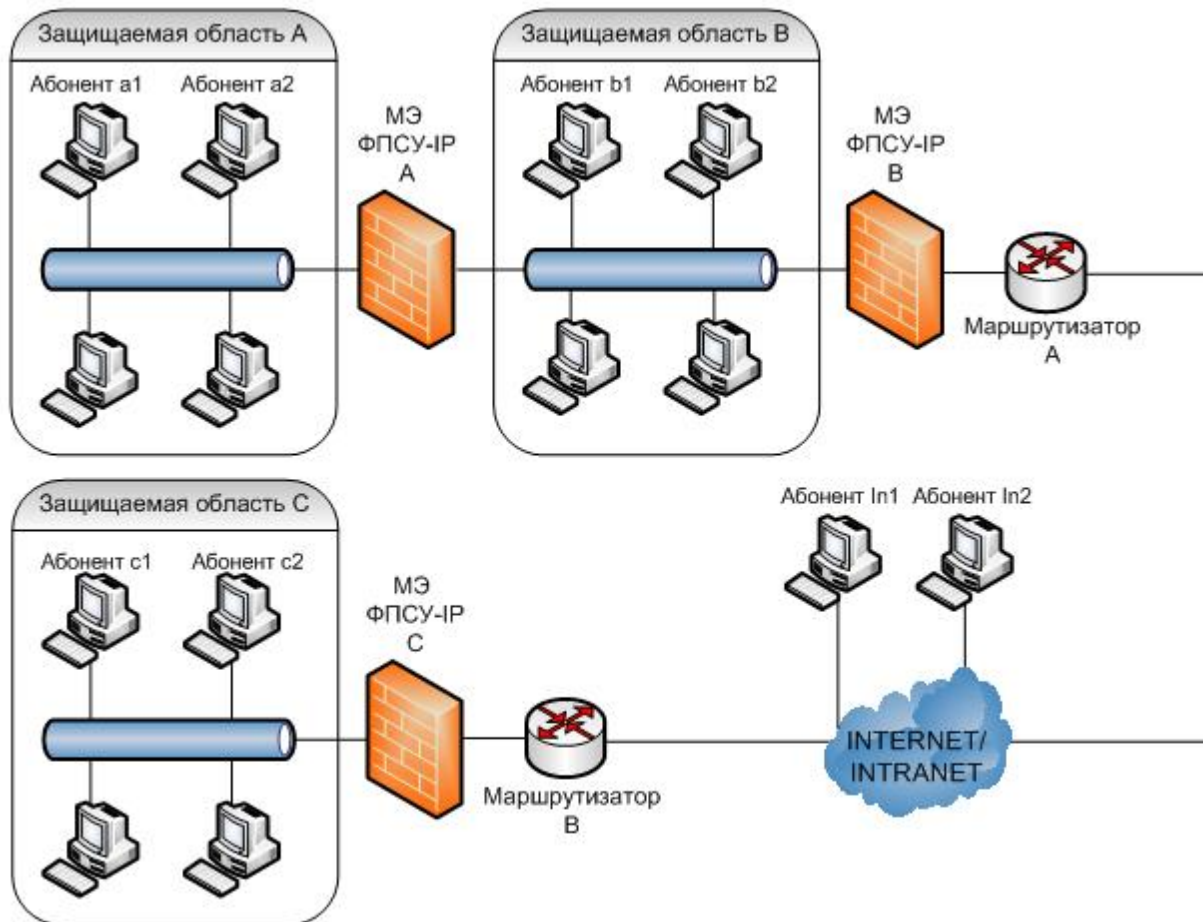


Рисунок 163 - Режим работы партнеров абонента

- "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 А это будут ""Абонент In1" через ФПСУ-IP В" или ""Абонент c1" через ФПСУ-IP В"; для ФПСУ-IP В это будут ""Абонент c1" через ФПСУ-IP С" или ""Абонент a2" через ФПСУ-IP А"; для ФПСУ-IP С это будут ""Абонент a2" через ФПСУ-IP В" 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, 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. 164 "Использование основной и резервной (запасной) линий ФПСУ-IP" данные от "Абонент а" до "Абонент b" могут идти двумя путями:

- "Абонент а" > ФПСУ-IP А > туннель А-В > ФПСУ-IP В > "Абонент b";
- "Абонент а" > ФПСУ-IP А > туннель А-С > ФПСУ-IP С > "Абонент b".

В таком случае, "Абонент b" может быть описан на ФПСУ-IP А как абонент, работающий в режиме "Через ФПСУ" с указанием основной линии, идущей через ФПСУ-IP В и резервной (запасной) линии, идущей через ФПСУ-С.

Если абонент подключается через цепочку туннелей к настраиваемому ФПСУ-IP (как, например "Абонент с1" на рис. "Режим работы партнеров абонента" при настройке взаимодействия через ФПСУ-IP А, подключается через два туннеля — туннель **ФПСУ С-ФПСУ В** и туннель **ФПСУ В-ФПСУ А**), то указывать следует ближайший ФПСУ-IP (в приведенном примере это ФПСУ-IP В).

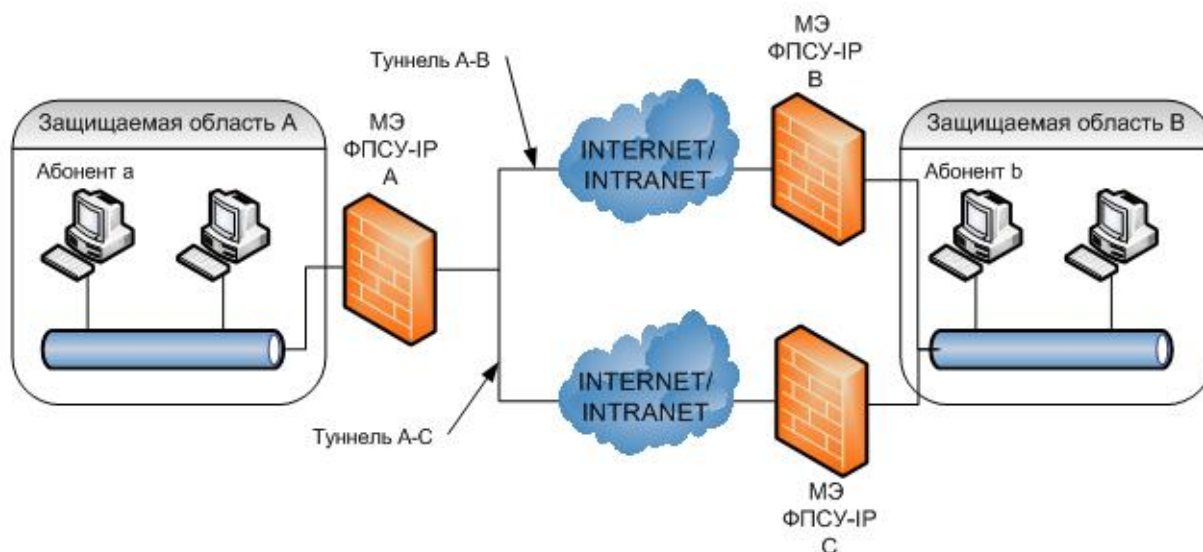


Рисунок 164 - Использование основной и резервной (запасной) линий ФПСУ-IP

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 С и описываемого на нем "Абонента а1" партнером данного порта в режиме ретрансляция является "Абонент In1" или "Абонент In2"; для ФПСУ-IP В и описываемого "абонента а2" 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 С и описываемого на нем "Абонента с1" партнером данного порта в режиме "Через ФПСУ" является "Абонент b2" или "Абонент a1"; для ФПСУ-IP А и описываемого на нем "Абонента b1" таким партнером является "Абонент In2" или "Абонент с2".

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 В и описываемого Абонента b1 партнером другого порта в режиме "Ретрансляция" является "Абонент In1" или "Абонент In2"; для ФПСУ-IP С и описываемого "Абонента с1" 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 А и описываемого "Абонента a1" партнерами другого порта в режиме "Через ФПСУ" являются "Абонент с1" или "Абонент in1"; для ФПСУ-IP С и описываемого "Абонента с2" 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).

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 host-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.

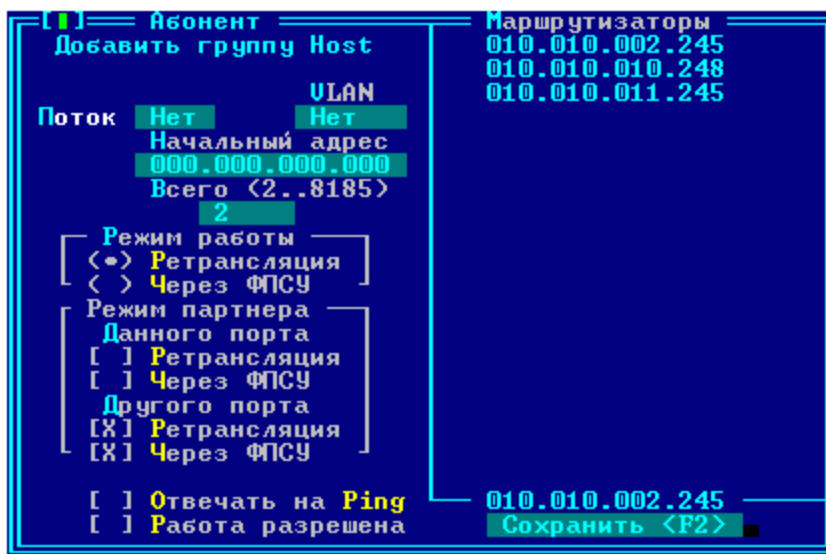


Рисунок 165 - Окно добавления группы описателей типа "хост"

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

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 "[Правила трафика межсетевого экрана](#)").

Отдельным хостам из этой подсети можно назначить права, отличающиеся от прав данной подсети, описав их отдельно (см. подраздел "[Описание абонента "Host"](#)"). Такая запись отдельного хоста будет иметь больший приоритет, чем описание всей подсети, включающей в себя IP-адрес хоста.

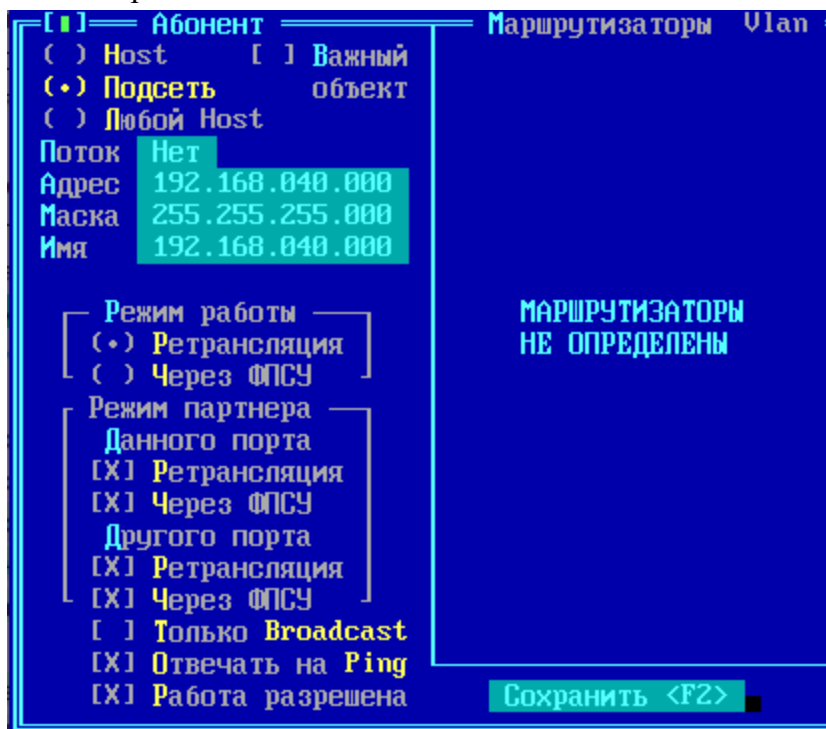


Рисунок 166 - Описание абонента ФПСУ-IP типа "Подсеть"

Для описания **подсети** заполните следующие поля:

- **Важный объект** – переключатель, который 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 подсеть, если требуется;
- **Поток** — аналогично описанию потока для абонента-хоста;
- **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 24), в таком случае ФПСУ-IP рассчитает значение маски автоматически.

- **Имя** – имя подсети (произвольное), которое будет отображаться в списке абонентов порта.
- **MAC** – аппаратный адрес подсети.
- **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.

Только Broadcast - переключатель, указывающий ФПСУ-IP, что данная запись типа "подсеть" создана специально для определения правил работы с ширококвещательными передачами. Если переключатель выключен - описываемая подсеть по установленным правилам будет обмениваться с партнерами как ширококвещательными 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 ширококвещательных передач, вся подсеть может быть описана одной записью и переключатель включать не нужно. В противном случае, если получение ширококвещательных пакетов желательно, но небезопасно для отдельных хостов подсети, следует создать специальную запись для передачи только ширококвещательных пакетов в описываемую подсеть (включив в ней переключатель "**Только Broadcast**"), а для описания отдельных рабочих станций этой подсети создать отдельные записи (см. пункт ["Описание абонента "Host"](#)).

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

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 Host"

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.

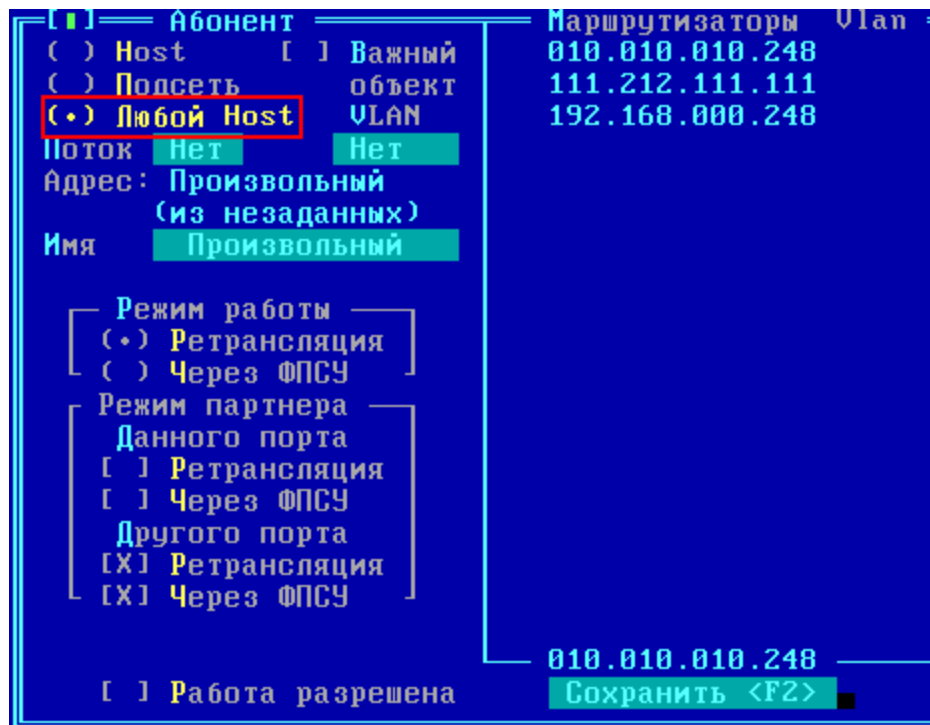


Рисунок 167 - Абонент вида "Любой Host", режим "Ретрансляция"

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 "[Правила трафика межсетевых экранов](#)"), 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.

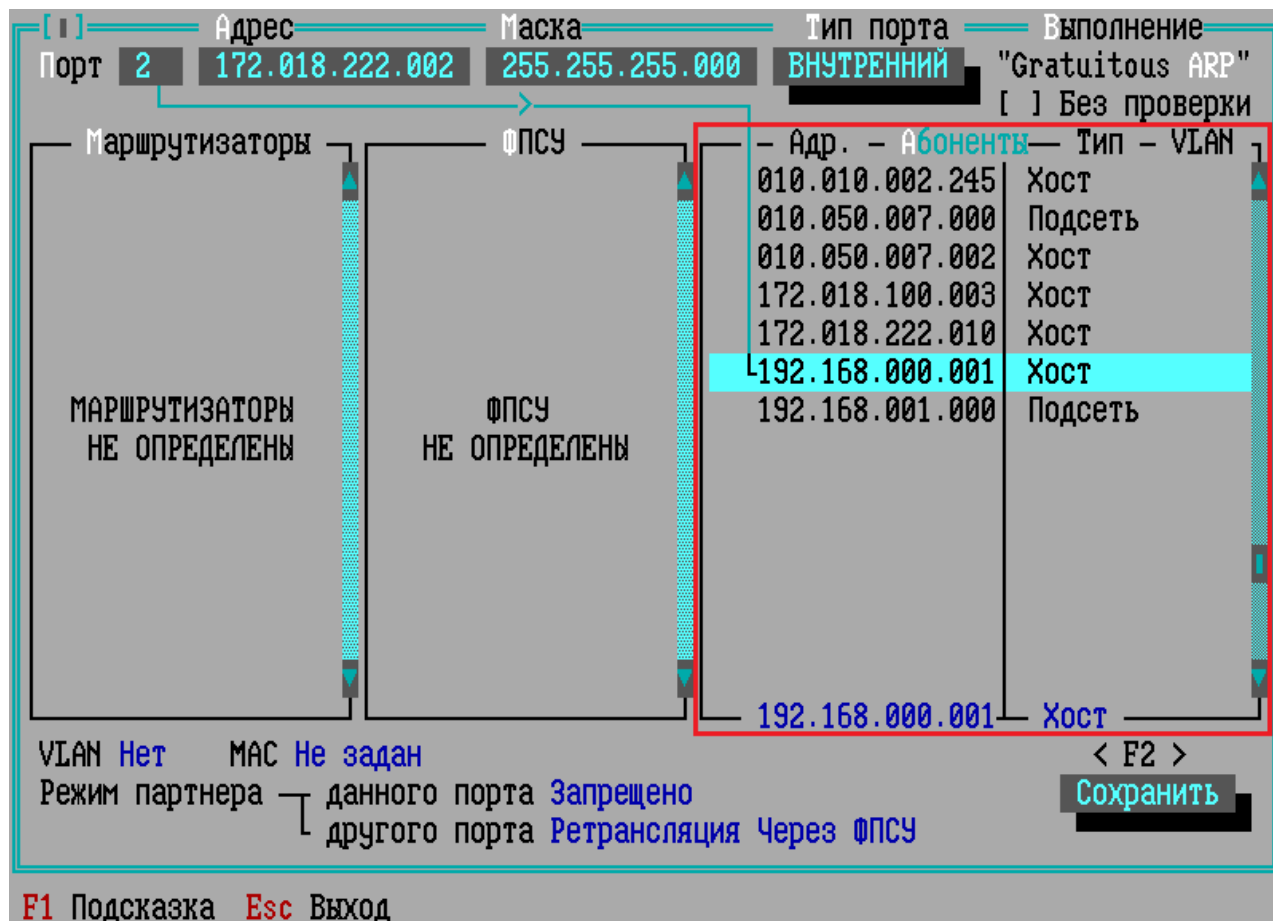


Рисунок 168 - Абоненты порта ФПСУ-IP

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>.

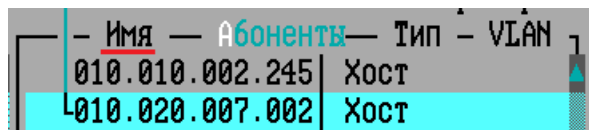


Рисунок 169 - Сортировка списка абонентов по имени

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

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

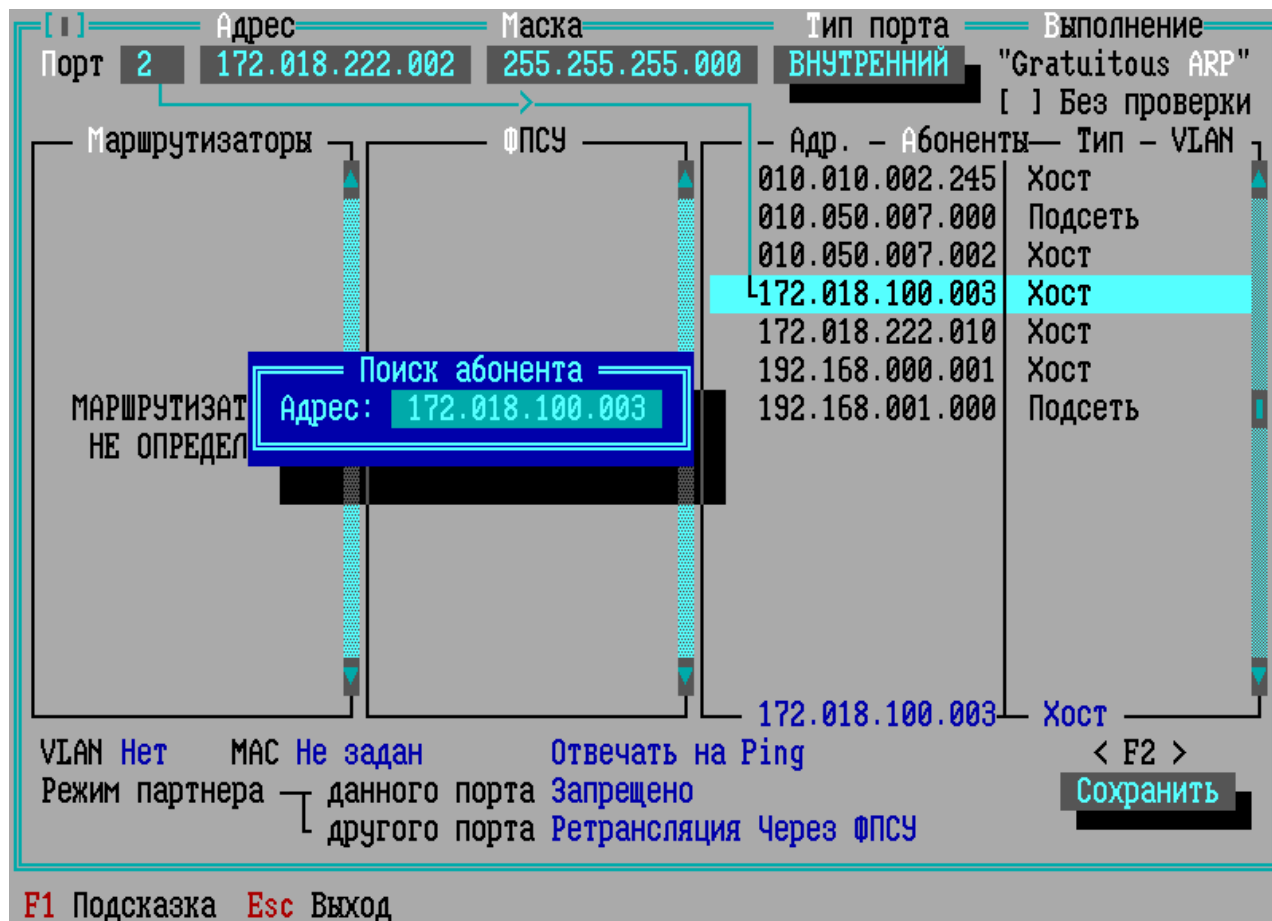


Рисунок 170 - Поиск абонента в списке

Поиск абонента в правилах межсетевых экранов ведется 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.

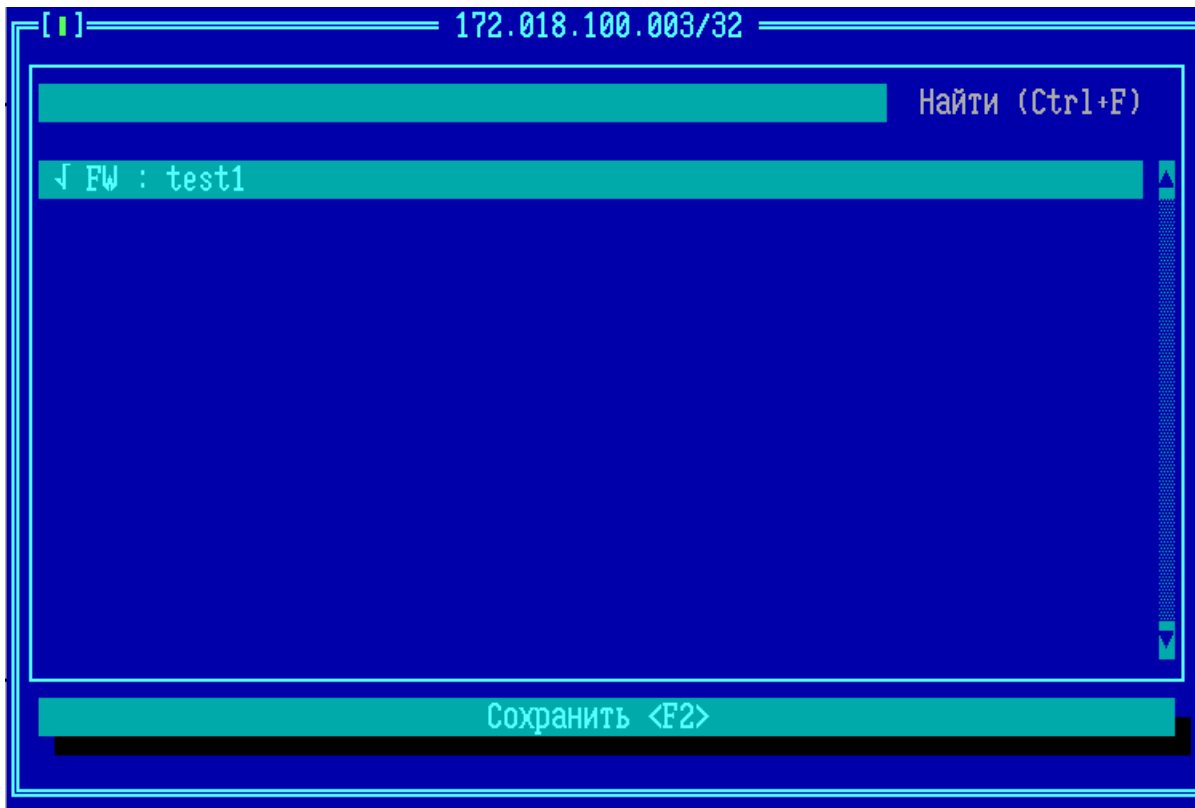


Рисунок 171 - Поиск абонента в правилах МЭ

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.

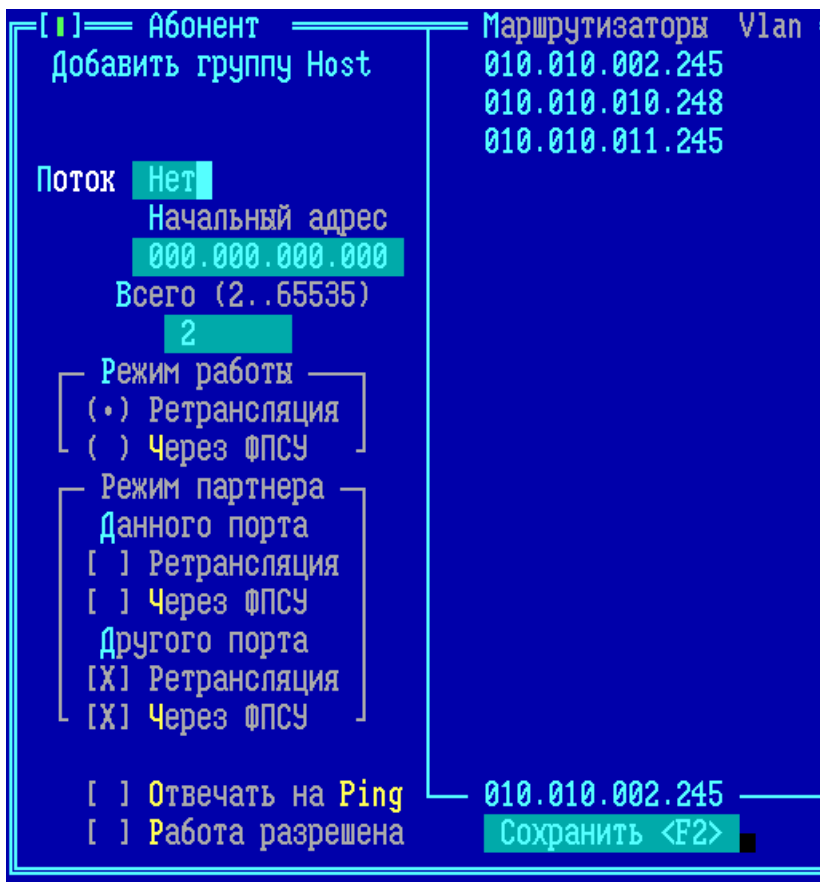


Рисунок 172 - Окно добавления группы описателей типа «хост»

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 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.

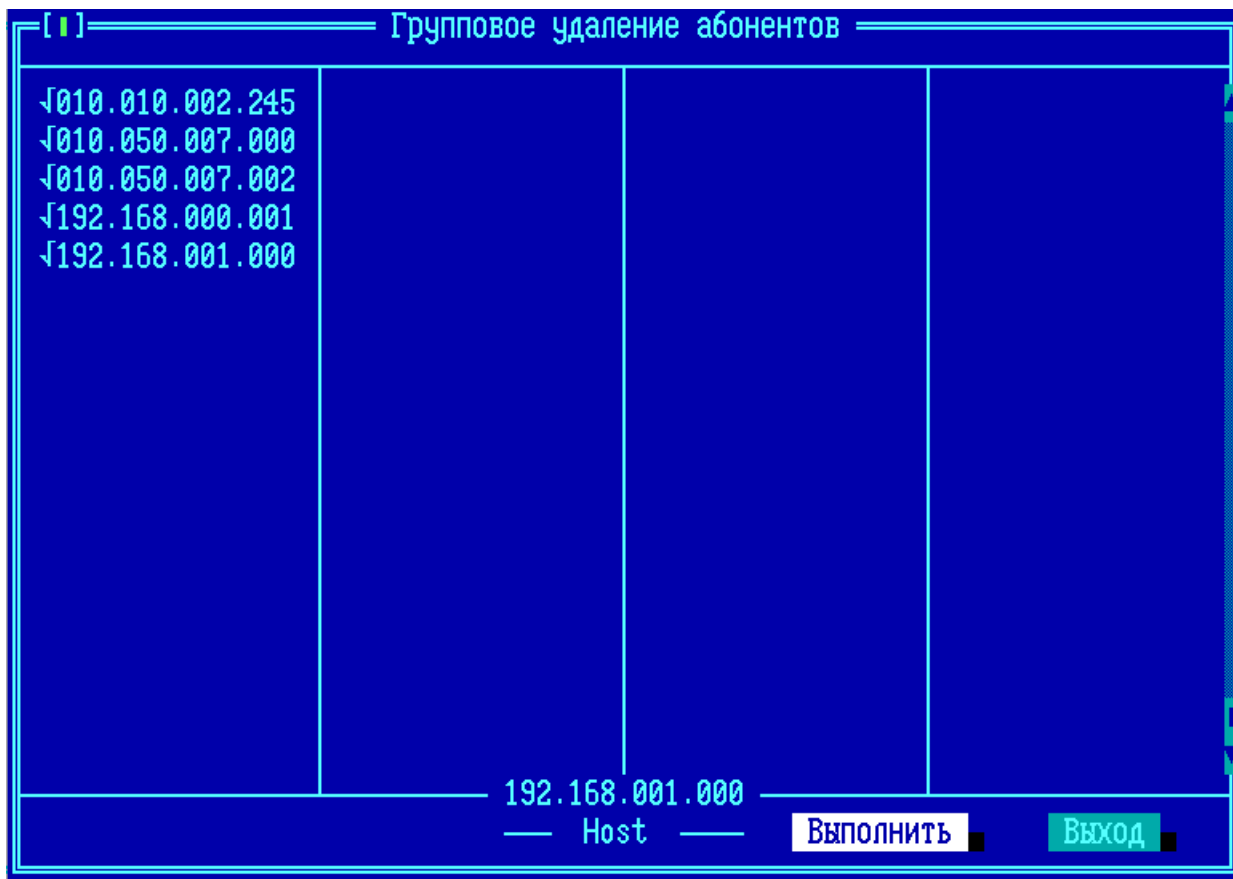


Рисунок 173 - Групповое удаление абонентов

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. 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.

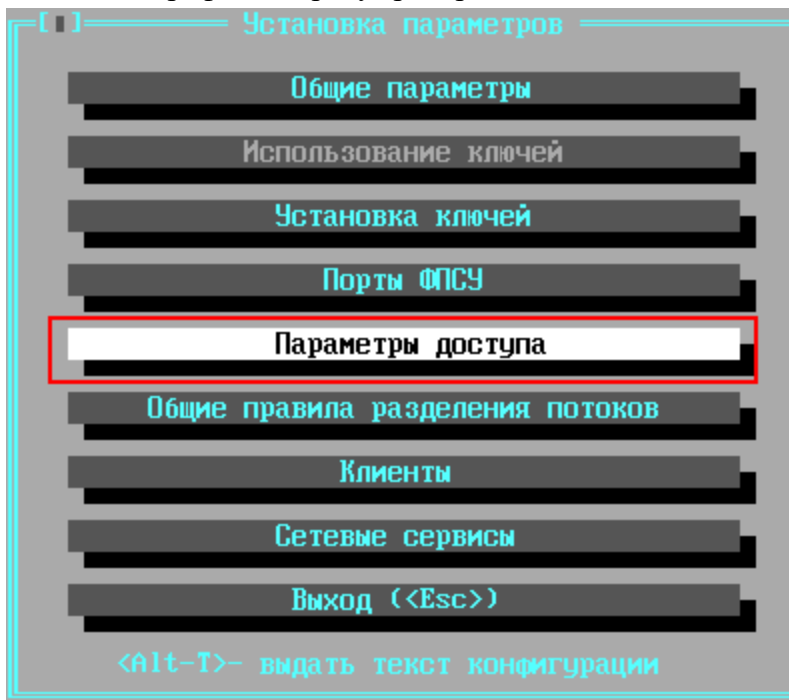


Рисунок 174 - Меню конфигурации ФПСУ-IP

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).

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 так же 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.

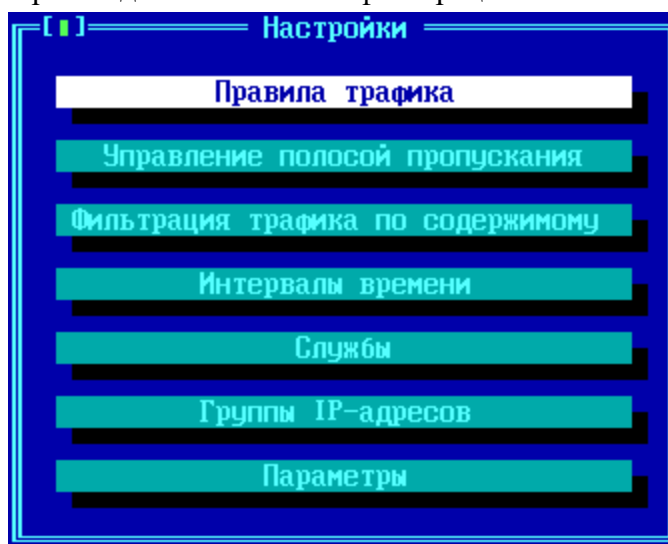


Рисунок 175 - Команды меню "Параметры доступа"

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":

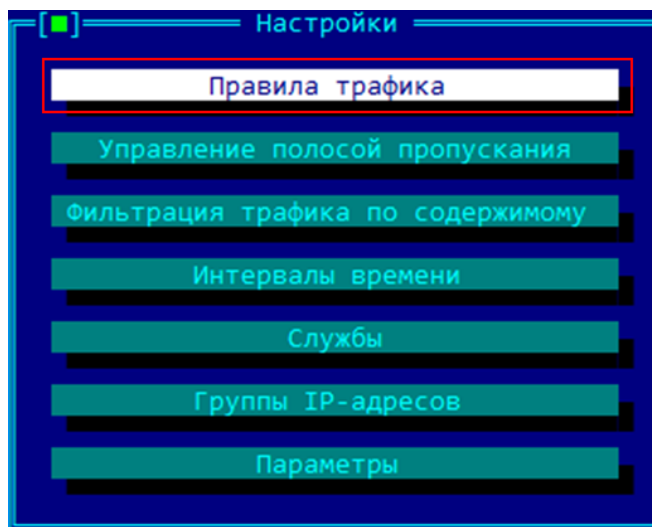
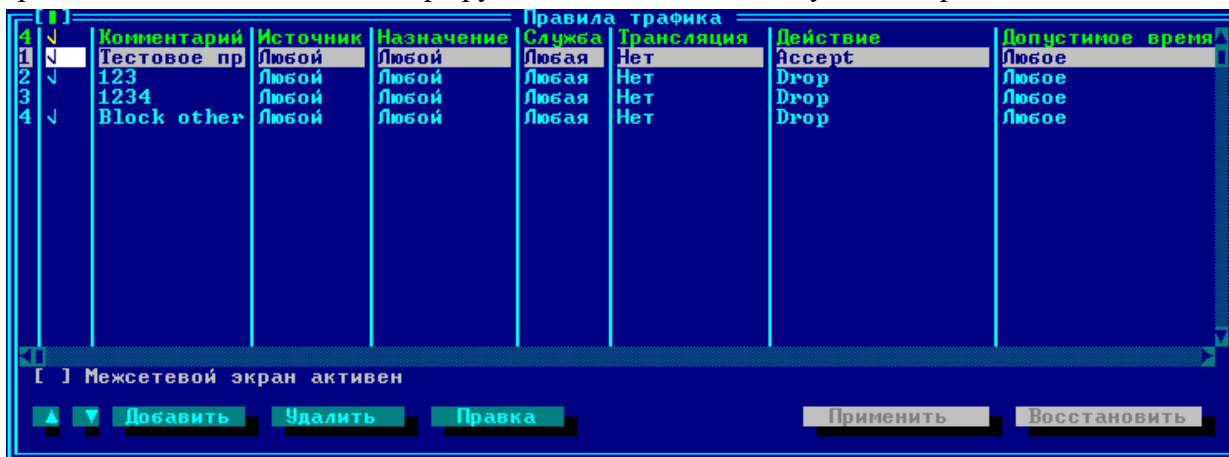


Рисунок 176 - Меню "Параметры доступа" – команда Правила трафика

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".



	Комментарий	Источник	Назначение	Служба	Трансляция	Действие	Допустимое время
1	Тестовое пр	Любой	Любой	Любая	Нет	Accept	Любое
2	1234	Любой	Любой	Любая	Нет	Drop	Любое
3	Block other	Любой	Любой	Любая	Нет	Drop	Любое

Рисунок 177 - 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 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».

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 ** или кнопку «Удалить».

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

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

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

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

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

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

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

10. 1. 1. Общие настройки правил трафика

В окне "Добавить правило" находятся четыре вкладки с настраиваемыми опциями. Переход с активной вкладки на соседнюю осуществляется нажатием сочетаний клавиш *<Ctrl> + <> >* и *<Ctrl> + << >*.

Вкладка **Общие** (настройки) предназначена для выбора обязательного основного действия с передаваемым пакетом (сбросить или пропустить), и опциональных дополнительных действий. Символом "v" 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.

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.

Общие	Источник	Назначение	Служба
Комментарий			
Действие	Drop ↓		
Nat	Нет. Выберите интерфейс ↓		
Мар	Не используется	Порт	—
[] Spoof			
Время работы	Любое время ↓		
Лог	Не вести лог ↓		
[] Активно			

Сохранить <F2> Отмена

Рисунок 178 - 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.

МАР (Порт). Правило, включающее в себя дополнительную опцию МАР, 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.

Переключатель **Sproof** – опция для сетевых соединений на медленных каналах передачи данных с большими задержками (спутник, например). Если задействована опция подтверждения получения данных АСК, 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 переключатель у поля **Активно**.

Помимо общих настроек, можно указать параметры на других вкладках создаваемого правила. Перемещение между вкладками осуществляется нажатием сочетаний клавиш <Ctrl> + < > и <Ctrl> + << >.

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 её. Указываемый в открывшемся окне IP-адрес

должен быть предварительно описан в интерфейсе "Порты ФПСУ" как абонент любого типа, другой ФПСУ-IP, или маршрутизатор.

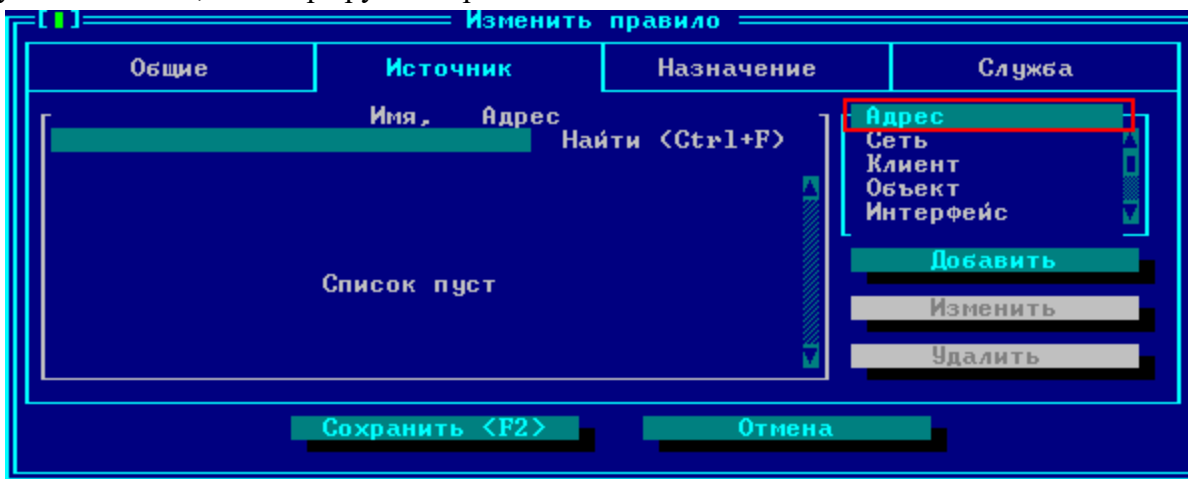


Рисунок 179 - Назначение источников для правила трафика

После выполнения команды добавить следует указать Имя и IP-адрес добавляемого объекта, либо выбрать из списка маршрутизации:

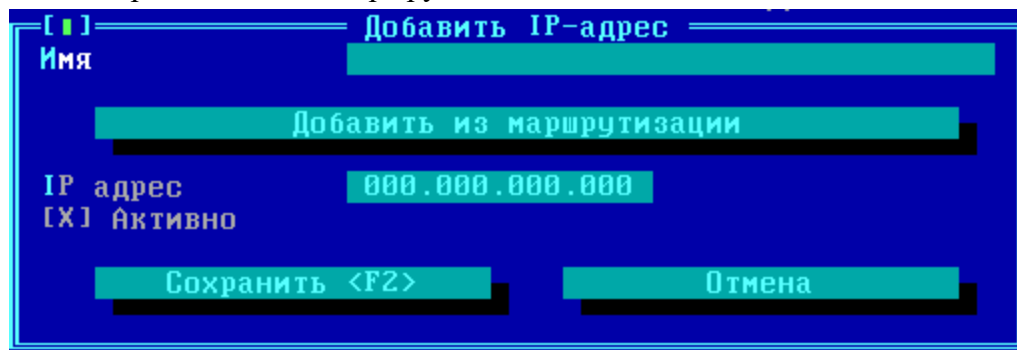


Рисунок 180 - Команда "Добавить" для отдельного IP-адреса

Из выпадающего меню, открывающегося по команде "Добавить из маршрутизации", курсором может быть выбран ранее описанный на "Портах ФПСУ" сетевой объект:

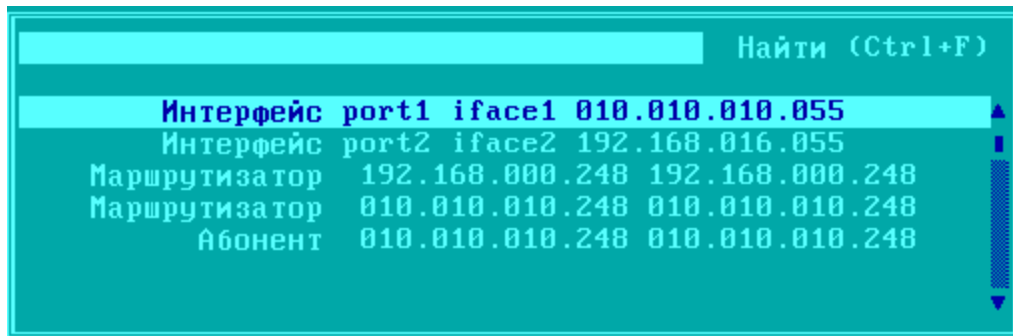


Рисунок 181 - Список найденных объектов в маршрутизации (Портах ФПСУ)

Перемещение по списку осуществляется клавишами " " и "v", 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:

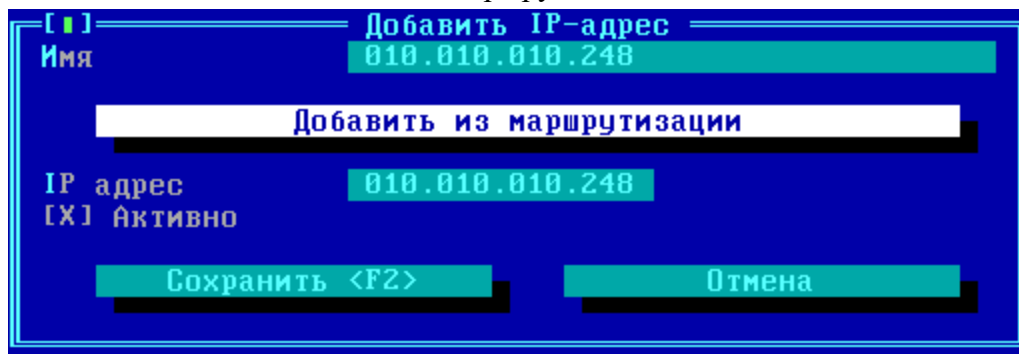


Рисунок 182 - Данные взяты из списка маршрутизации

Обратите внимание, что если переключатель "Активно" выключен, то IP-адрес будет добавлен в список, но правило трафика по нему обрабатывать не будет.

После нажатия клавиши <F2> или выполнении команды "Сохранить <F2>", IP-адрес будет добавлен в список вкладки **Источник**:

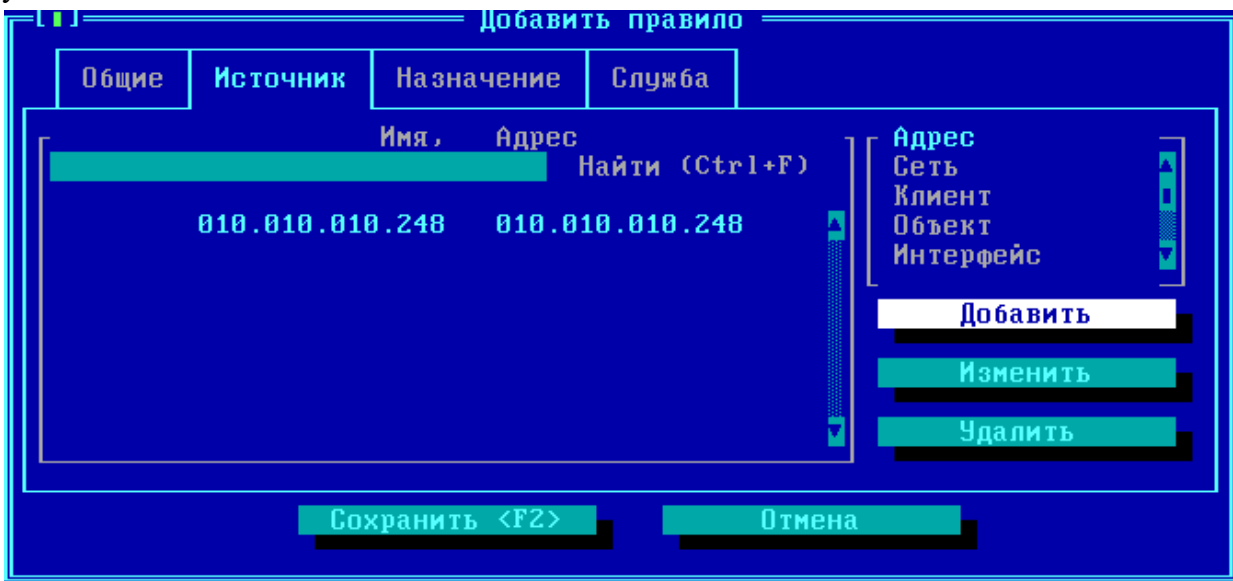


Рисунок 183 - В список "Источник" правила трафика добавлена новая запись

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 её. 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 её. 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 её.

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 так же 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 её.

Каждая запись списка вкладок **Источник** или **Назначение** может быть временно исключена из проверяемых фильтров, при снятии включенного по умолчанию переключателя "Активно"

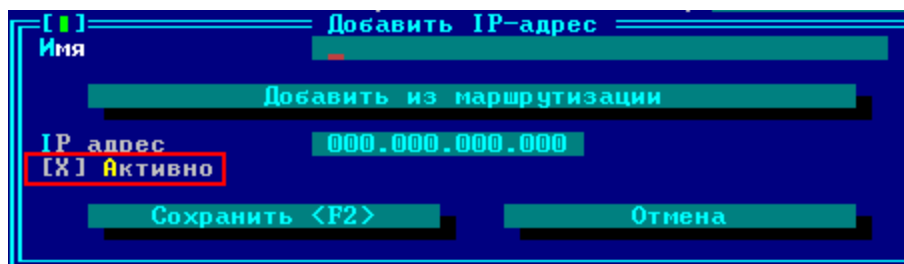


Рисунок 184 - Активизация добавленного адреса

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:

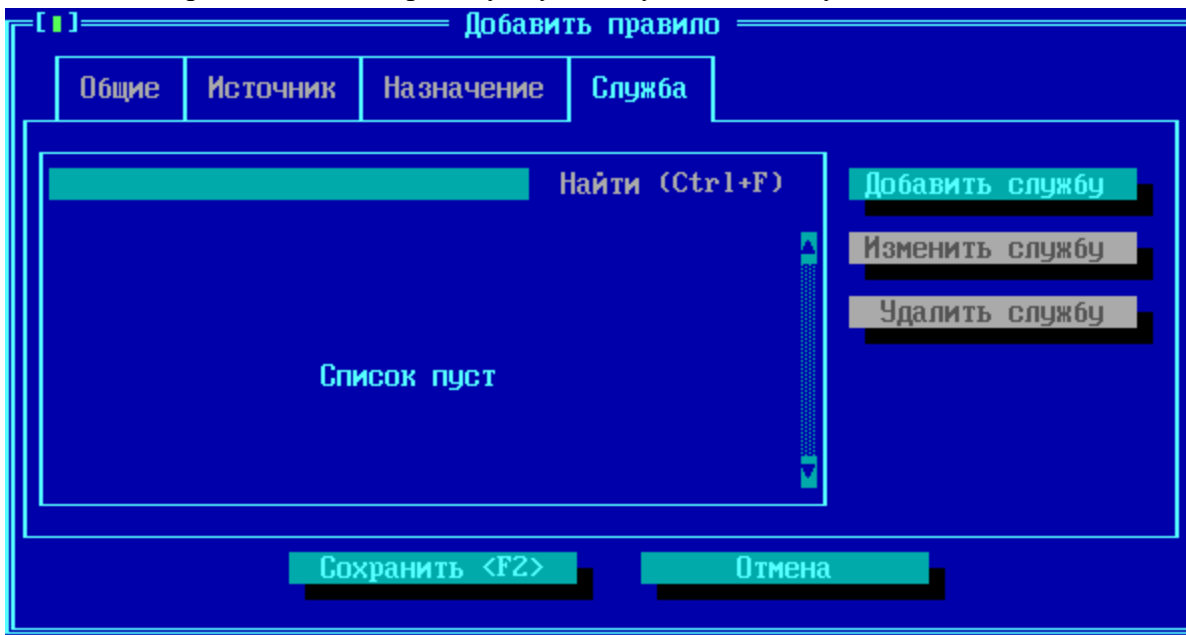


Рисунок 185 - Пустой список служб у нового добавляемого правила

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 только одна служба с именем "TCP 80"):

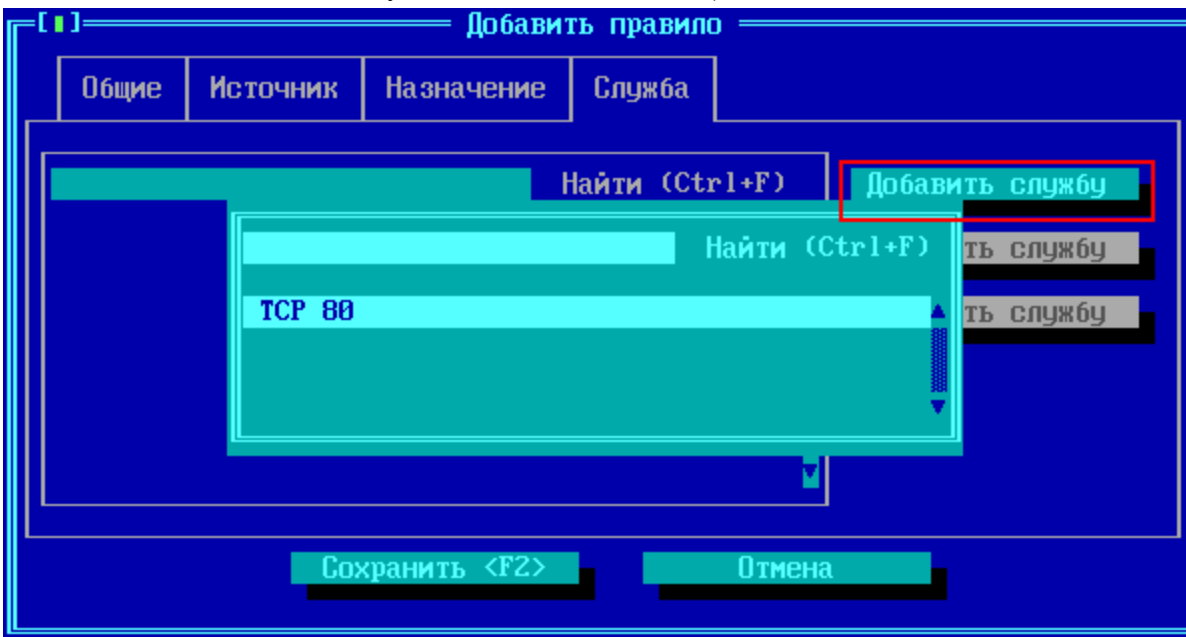


Рисунок 186 - Добавление службы в правило трафика

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

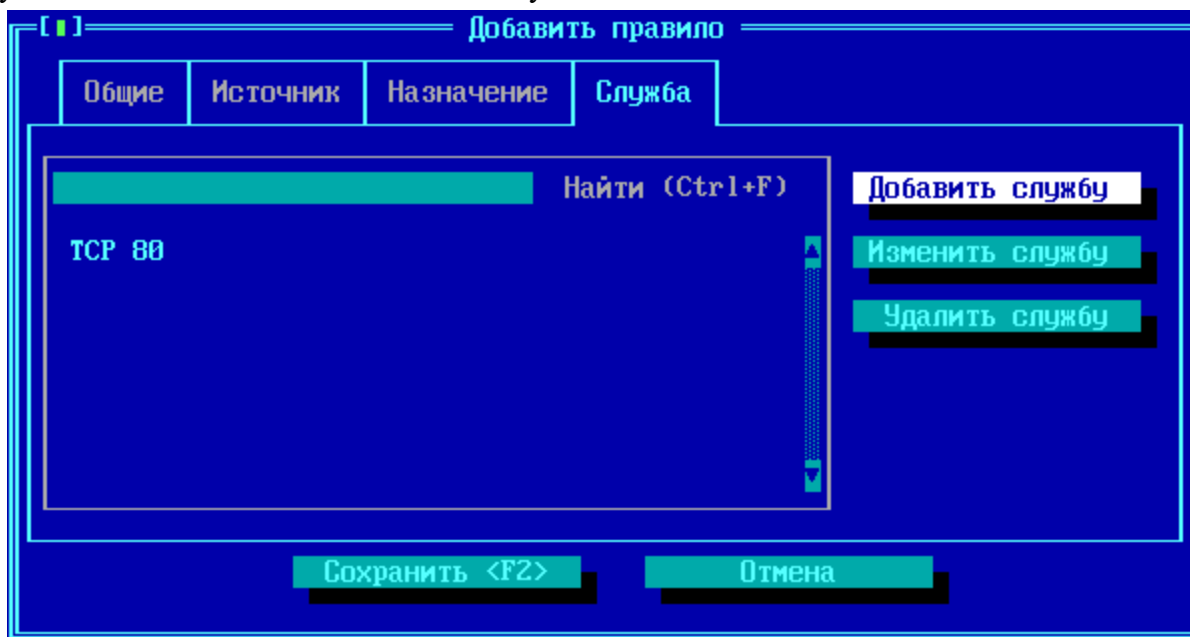


Рисунок 187 - Вкладка со списком служб правила трафика

Внести изменения в параметры выбранной курсором службы можно, нажав клавишу **Изменить службу** — при этом происходит переход в окно изменения настроек обрабатываемых протоколов (подробнее см. пункт "[Службы](#)"):

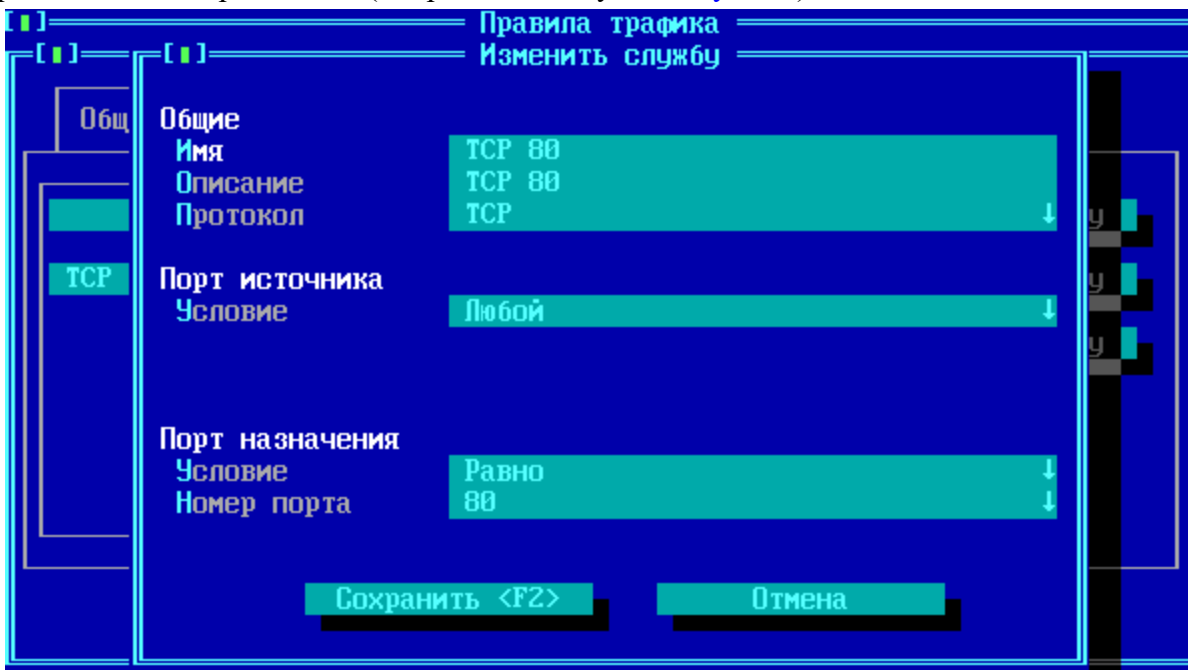


Рисунок 188 - Изменение службы из окна настроек правила доступа

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 "Службы" меню "Настройки Параметров доступа":

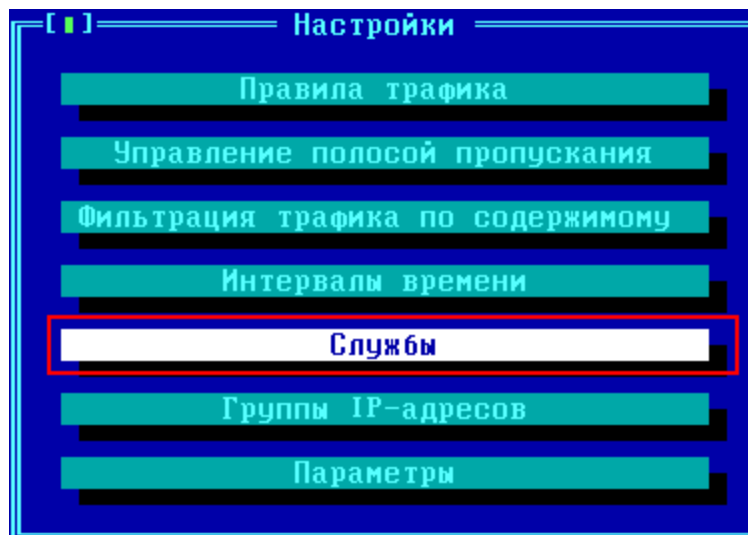


Рисунок 189 - Команда "Службы" настроек правил доступа

Список служб по умолчанию пустой.

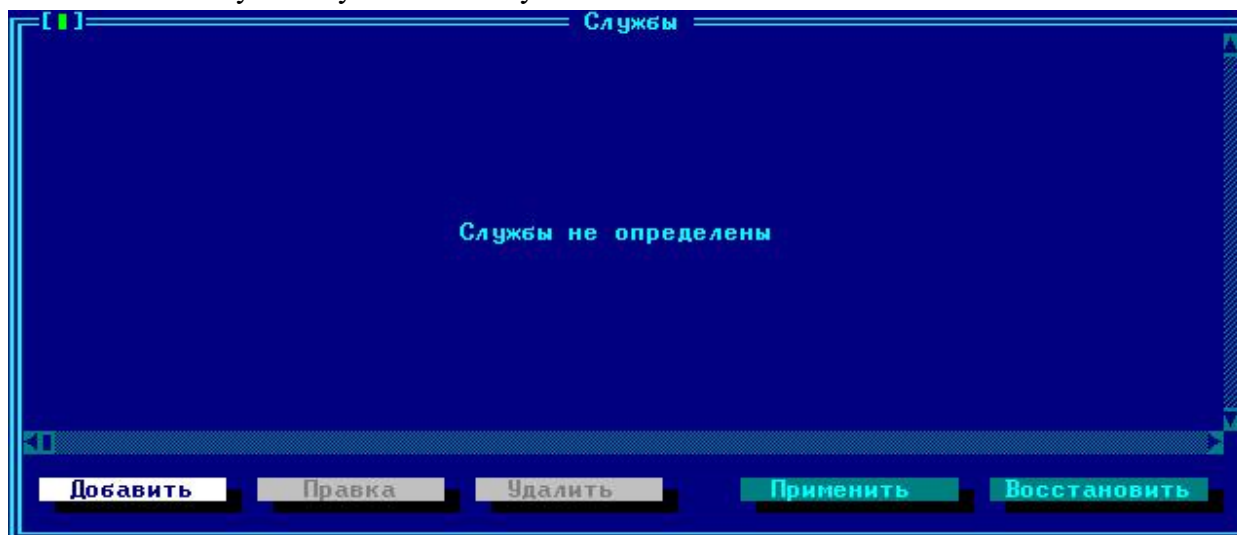


Рисунок 190 - Список служб

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 191 - 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](#)");
- *RAW* – 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.

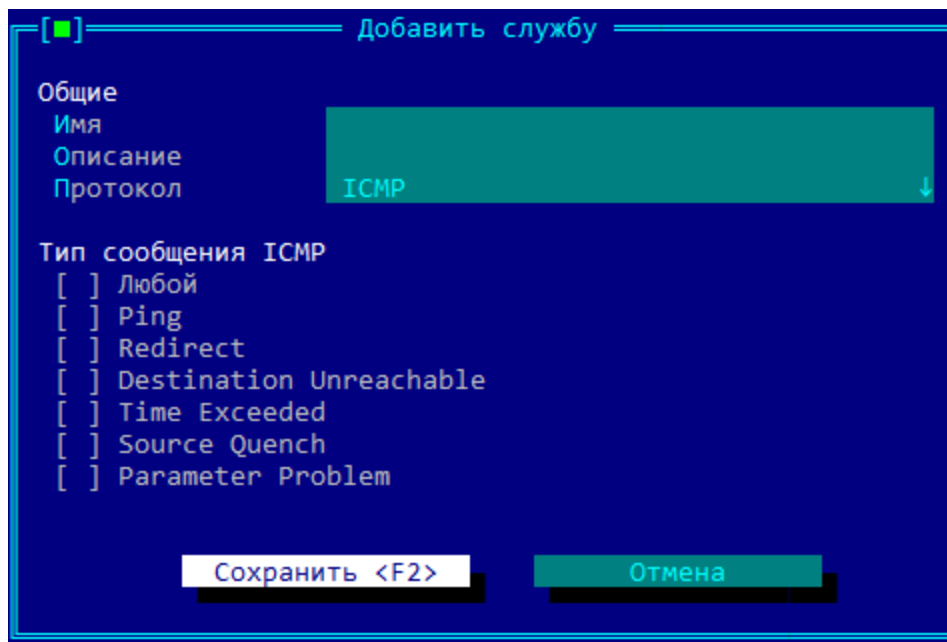


Рисунок 192 - Выбор сообщений ICMP в службе

Если правило трафика не должно применяться ко всем типам ICMP-сообщений, в службе при выборе протокола ICMP не следует выставлять переключатель "[] 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:

- переключатель "Отрицание" – задействован;
- тип "Word";
- смещение "6";
- маска "3fff";
- начало "0";
- конец "0".

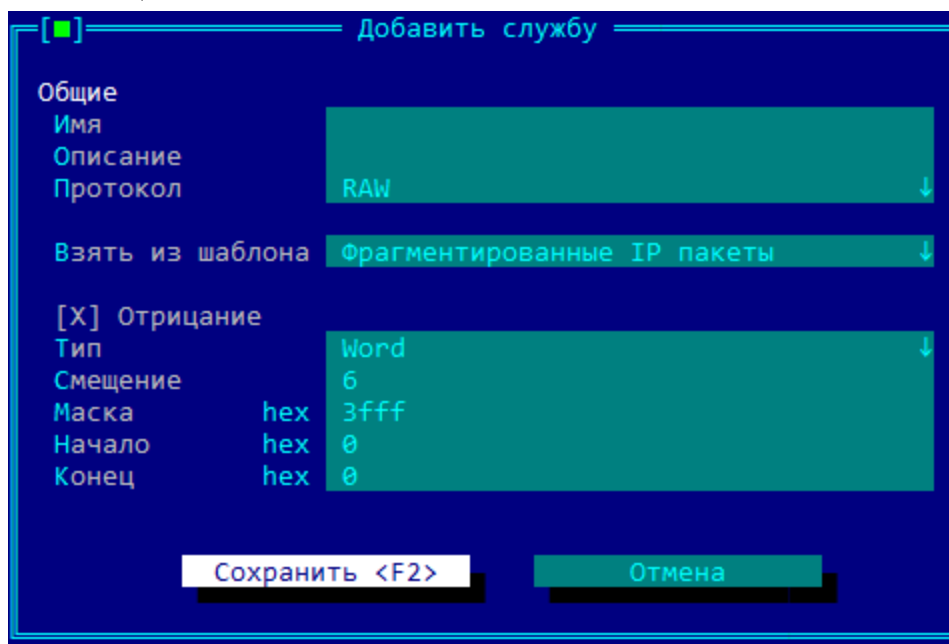


Рисунок 193 - Шаблон для фильтра фрагментированных IP-пакетов

После сохранения службы, её можно добавить к любому правилу **фильтрации трафика по содержимому** (см. "[Фильтрация трафика по содержимому \(DPI\)](#)") межсетевое экрана ФПСУ-IP.

При добавлении такой службы к правилу фильтрации трафика по содержимому межсетевое 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:

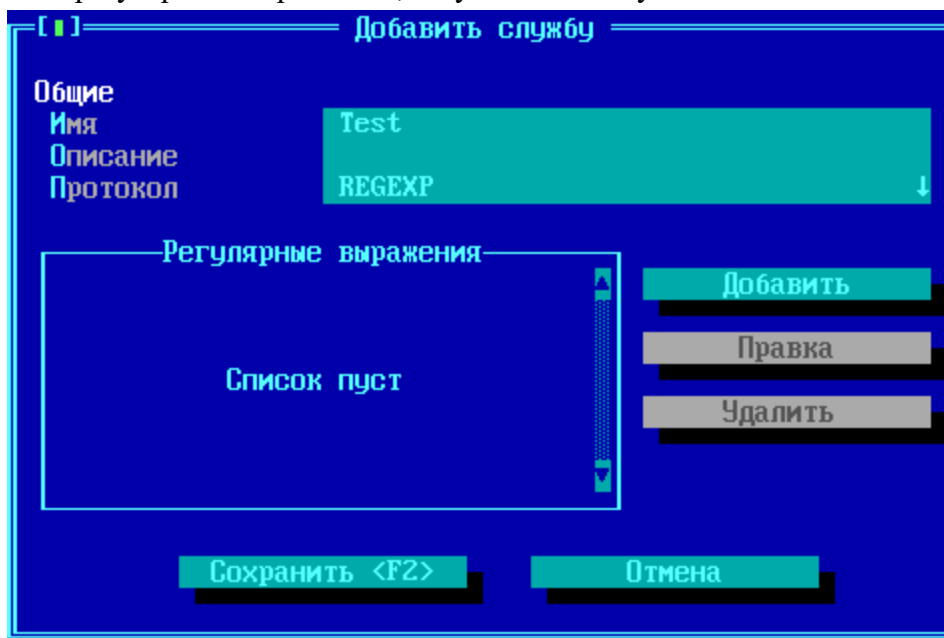


Рисунок 194 - Добавление службы REGEXP

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:

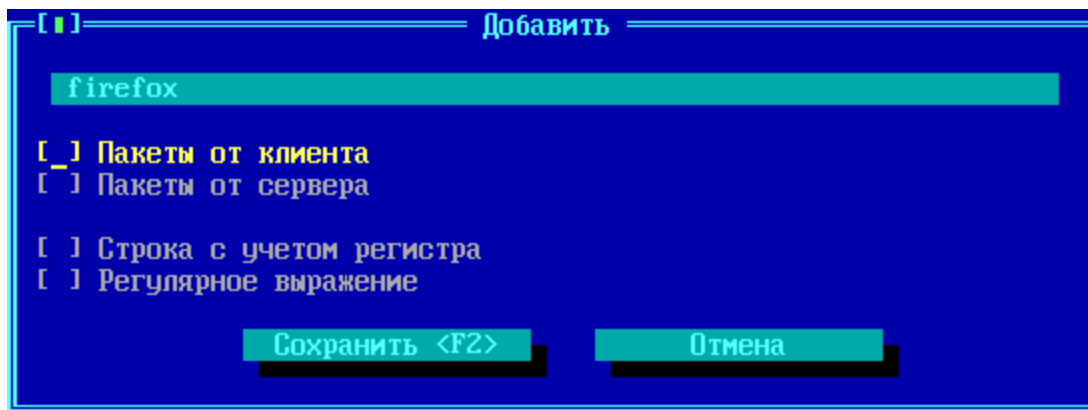


Рисунок 195 - Добавление службы REGEXP

Поле ввода под названием окна *Добавить* - символьную строку или регулярное выражение, обязательная опция. Поле не должно быть пустым. Именно на наличие в IP-пакете указанной в поле символьной строке/регулярном выражении 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 А с латинской буквой В (символьной строки АВ) 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 (клиенту) к принимающей соединению стороне (сервера).

Пакеты от сервера - опция, указывает на то, что символьную строку/регулярное выражение стоит искать только в пакетах, передающихся от принимающей соединению стороны (сервера) к инициатору соединения (клиенту).

ОБРАТИТЕ 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:

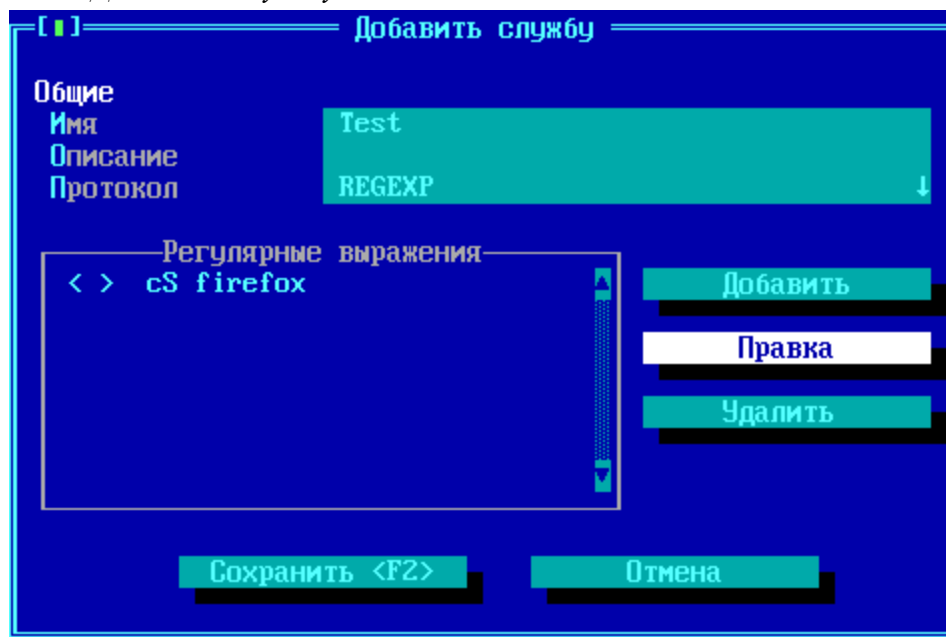


Рисунок 196 - Добавление службы REGEXP

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 .

Применение протокола REGEXP для частично 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:

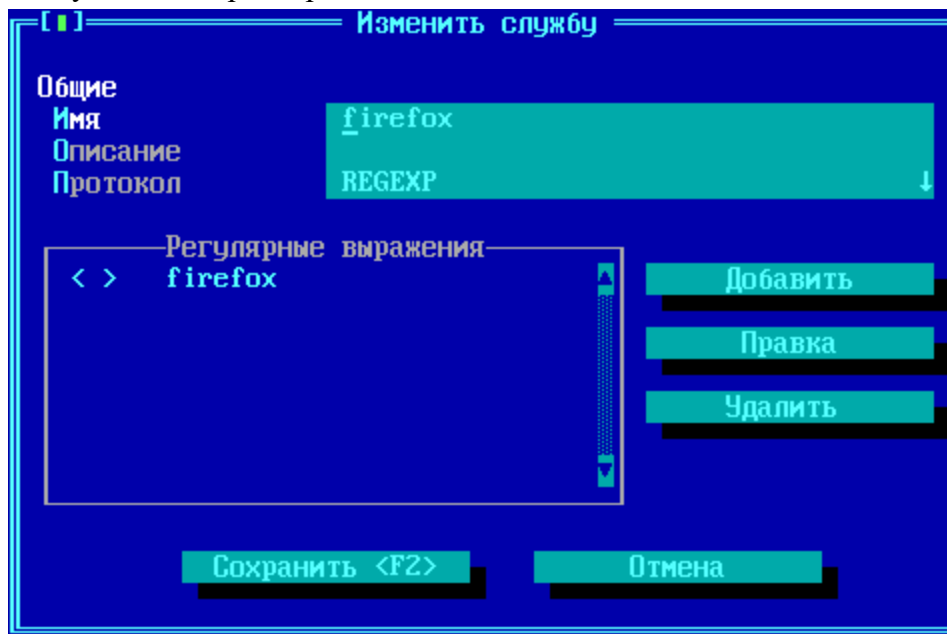


Рисунок 197 - Блокировка браузера Mozilla Firefox, правило 1

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

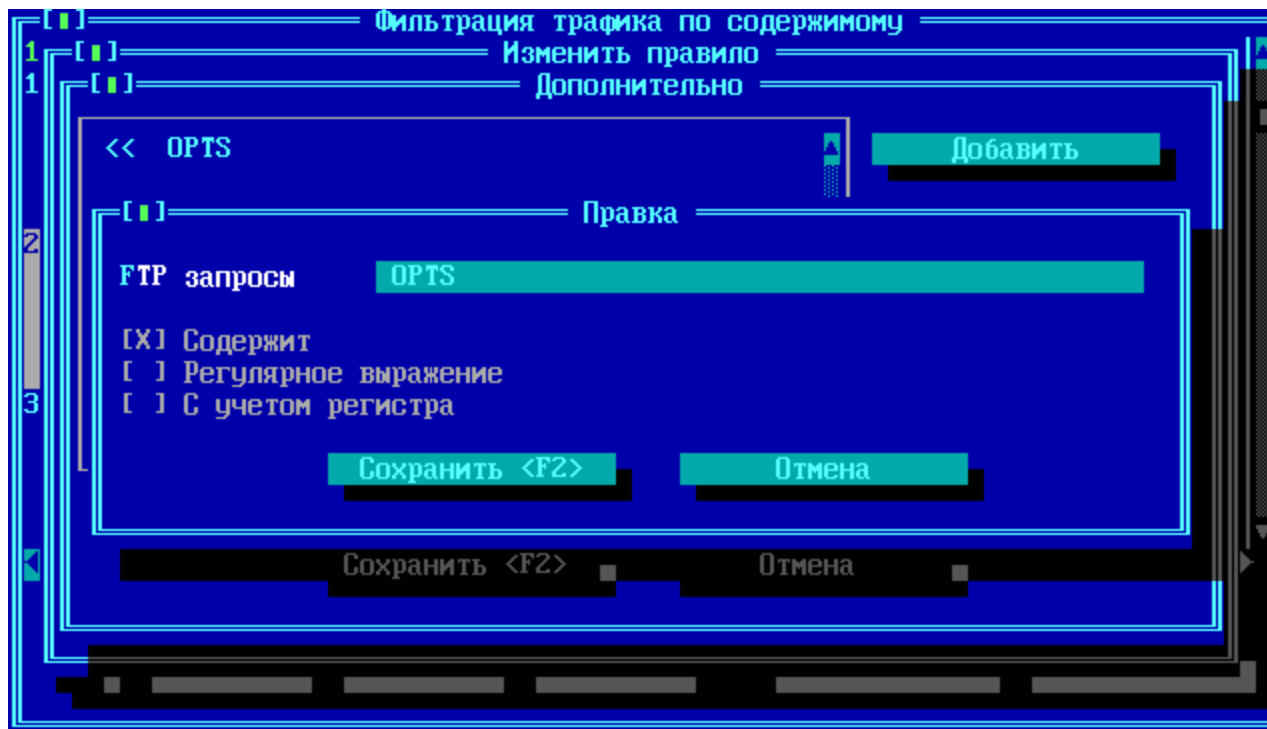


Рисунок 198 - Блокировка браузера Mozilla Firefox, правило 2

Для блокировки сетевой работы браузера Google Chrome 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:

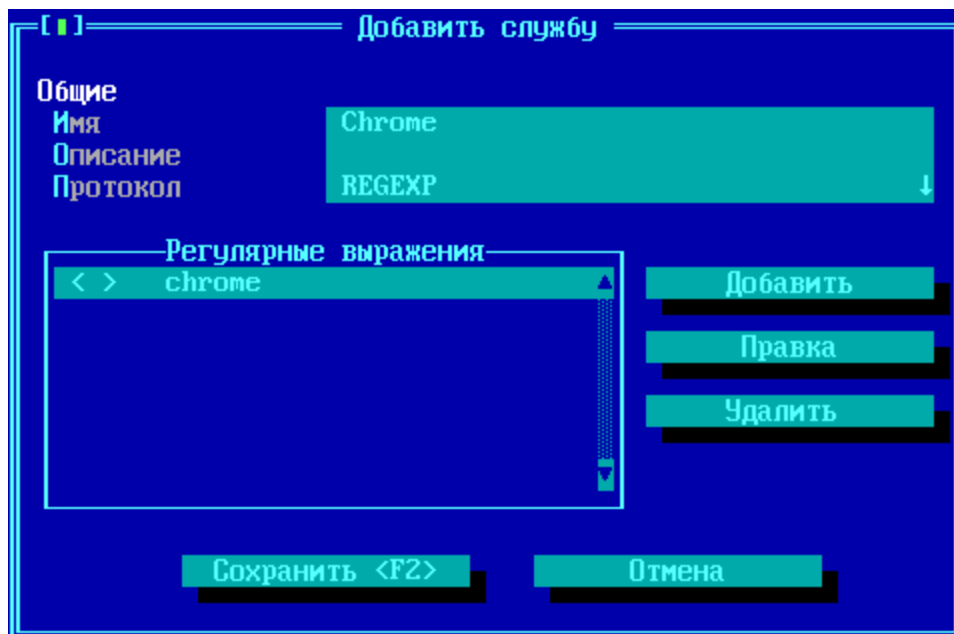


Рисунок 199 - Блокировка браузера Google Chrome, правило 1

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

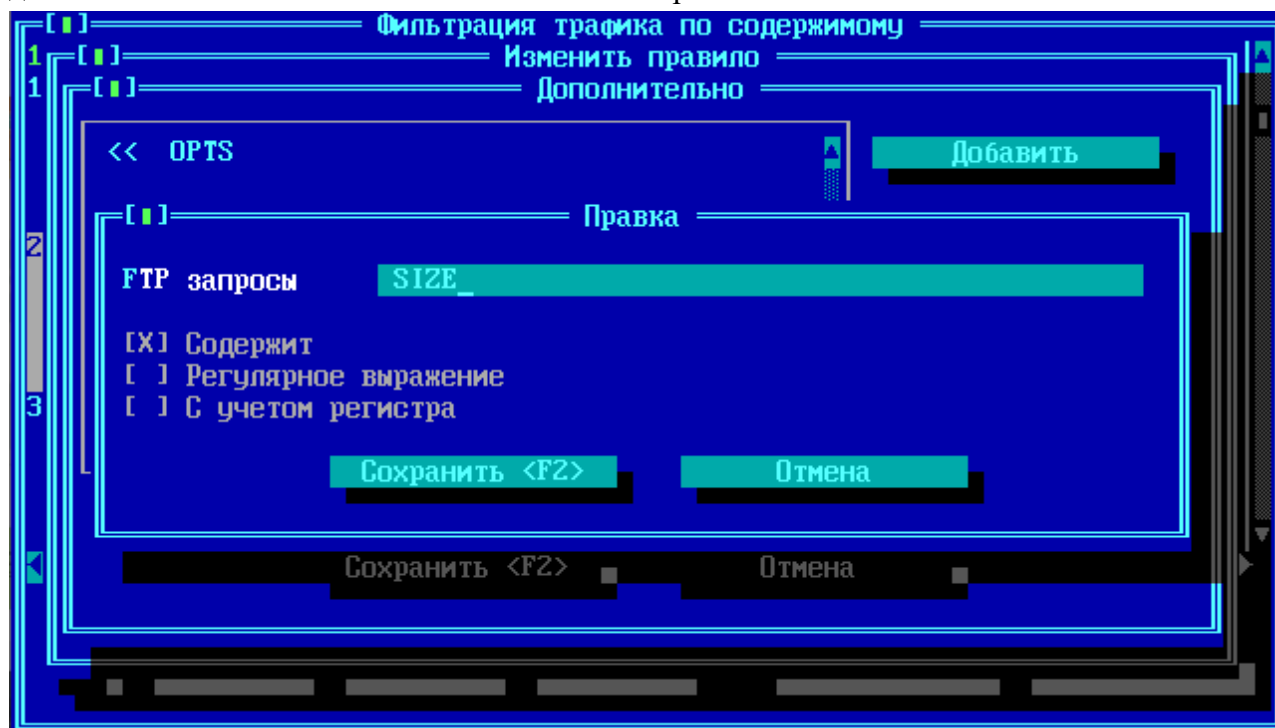


Рисунок 200 - Блокировка браузера Google Chrome, правило 2

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:

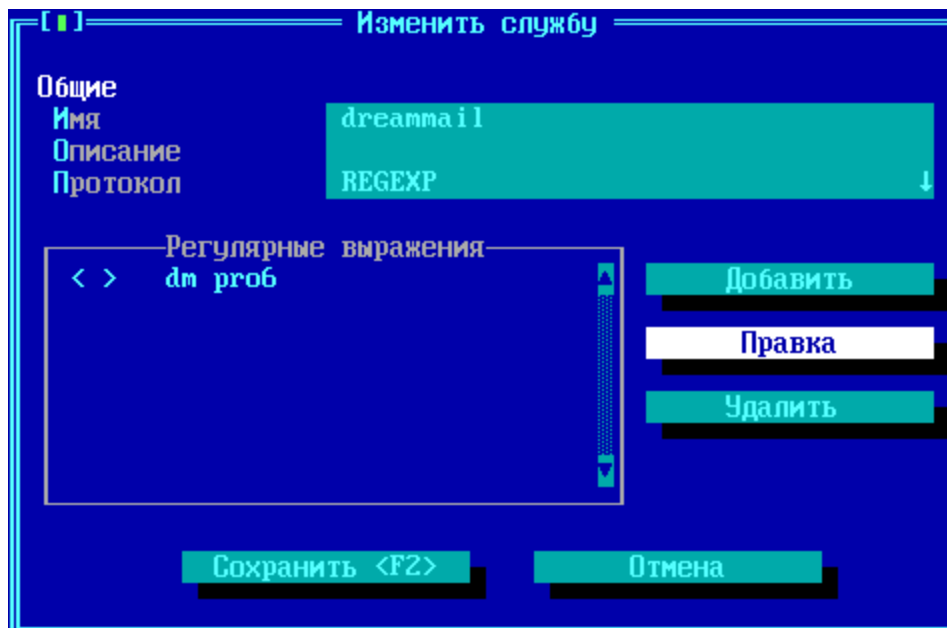


Рисунок 201 - Блокировка работы почтового клиента Dreammail по протоколу SMTP

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 202 - 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:

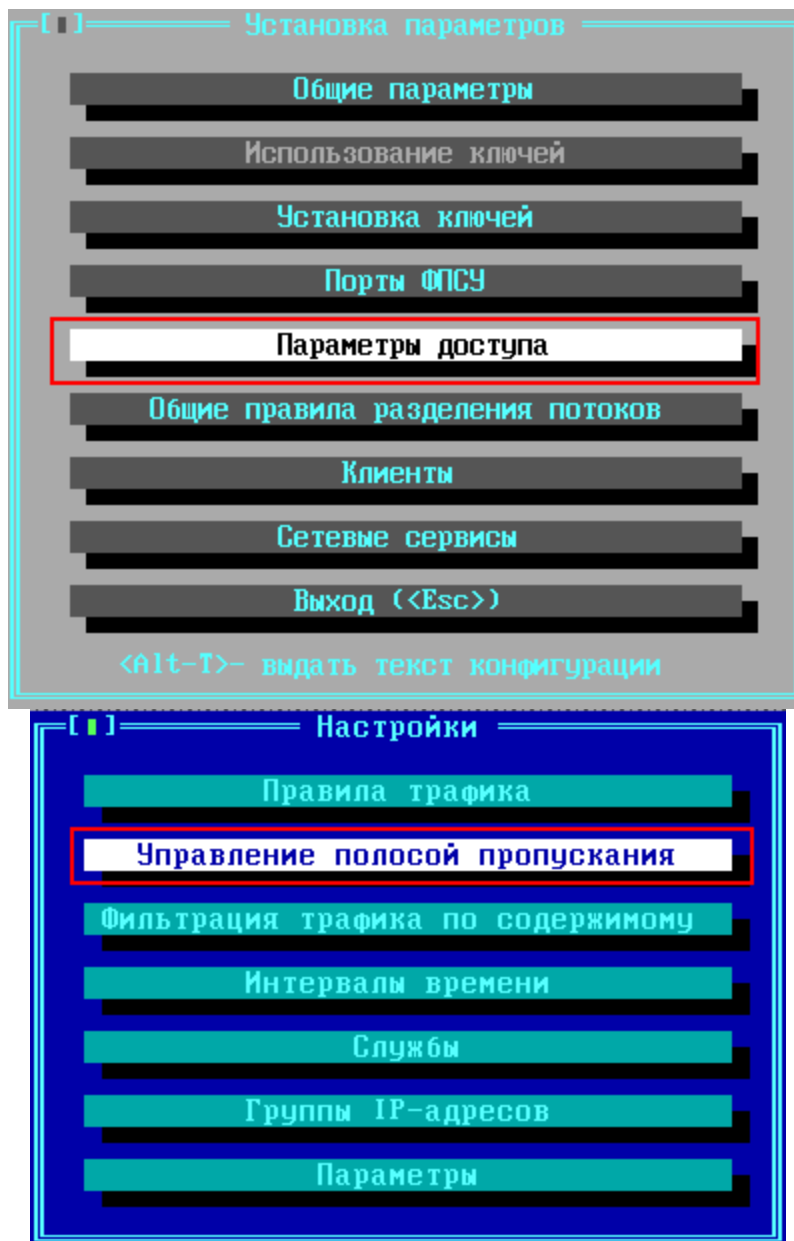


Рисунок 203 - Команды "Параметры доступа" и "Управление полосой пропускания"

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. Переключатель "Межсетевой экран активен" указывает на работу дополнительных правил фильтрации и правил ограничений скорости передачи данных.

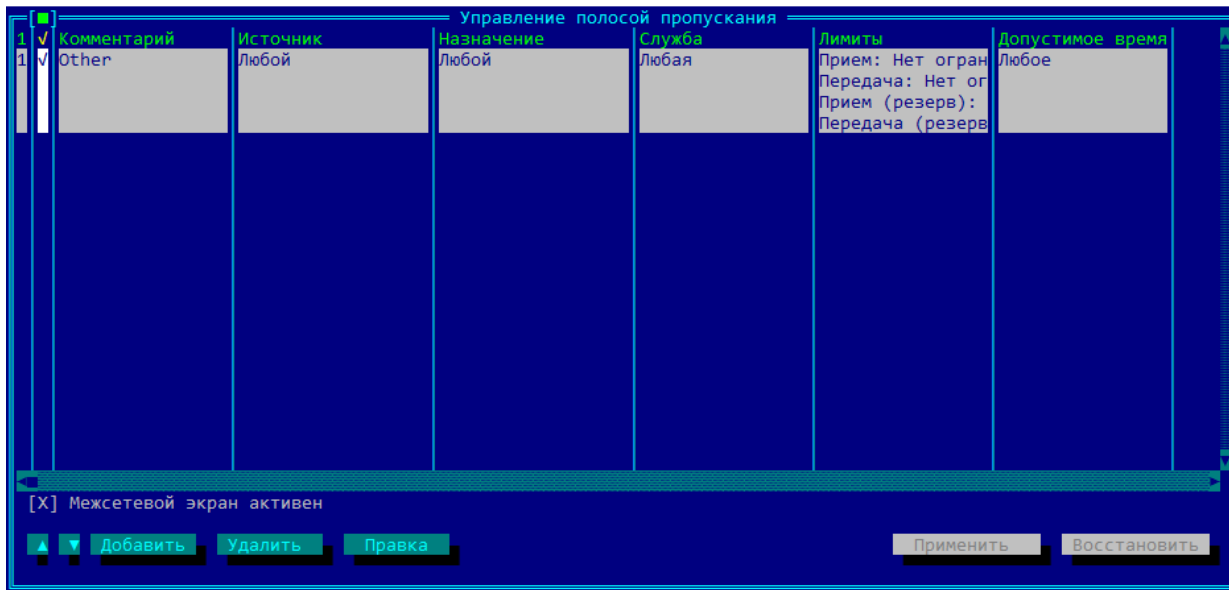


Рисунок 204 - Окно списка правил управления полосой пропускания

Для внесения изменений в конфигурацию без выхода из окна, нажмите клавишу "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 "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 нажатием сочетаний клавиш <Ctrl> + <> и <Ctrl> + <<>.

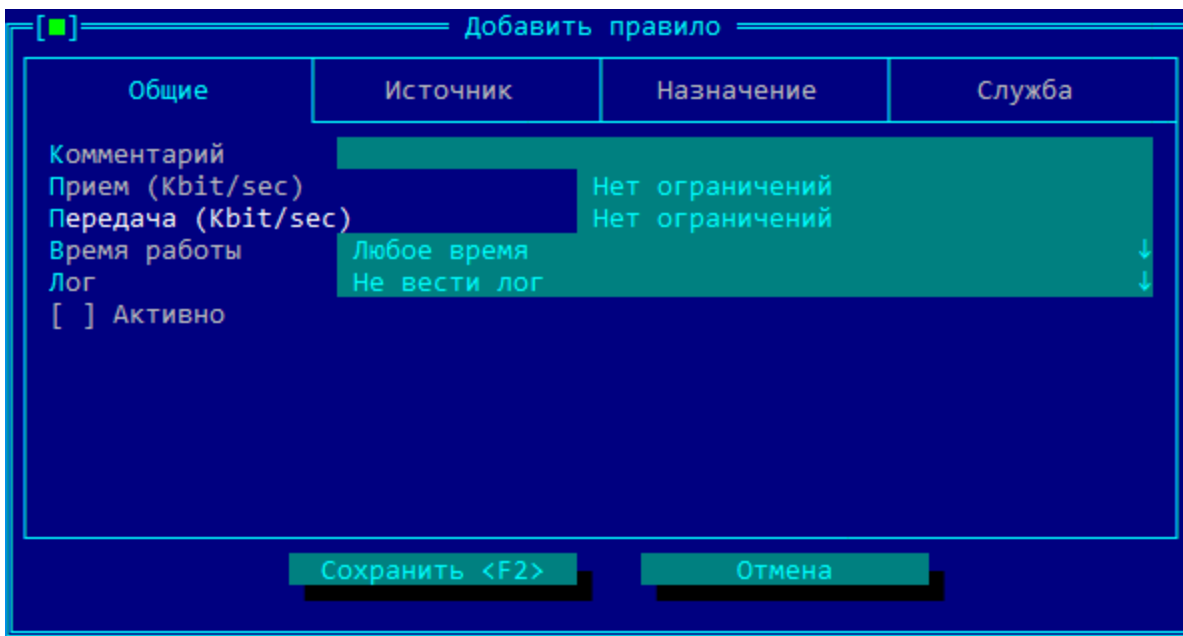


Рисунок 205 - Создание нового правила ограничения скорости передачи данных

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 "v" 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 $1 \text{ Kbit/sec} = 1024 \text{ bit/sec}$). 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 $1 \text{ Kbit/sec} = 1024 \text{ bit/sec}$). 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 "Службы" 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 нажатием сочетаний клавиш <Ctrl> + <> и <Ctrl> + << >.

Для того, чтобы все указанные в правиле после выхода с сохранением (F2) были задействованы, следует перед выходом установить переключатель у поля **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 решение 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 по нажатию кнопки "Фильтрация трафика по содержимому" подменю "Настройки":

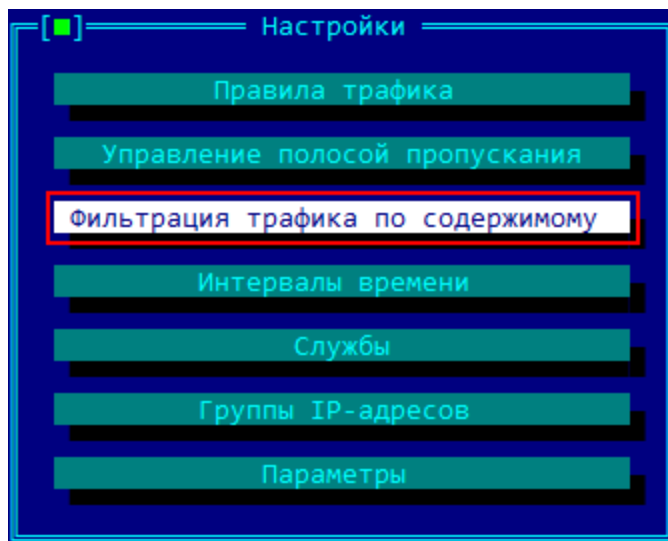


Рисунок 206 - Меню настройки межсетевое экрана ФПСУ-IP

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.

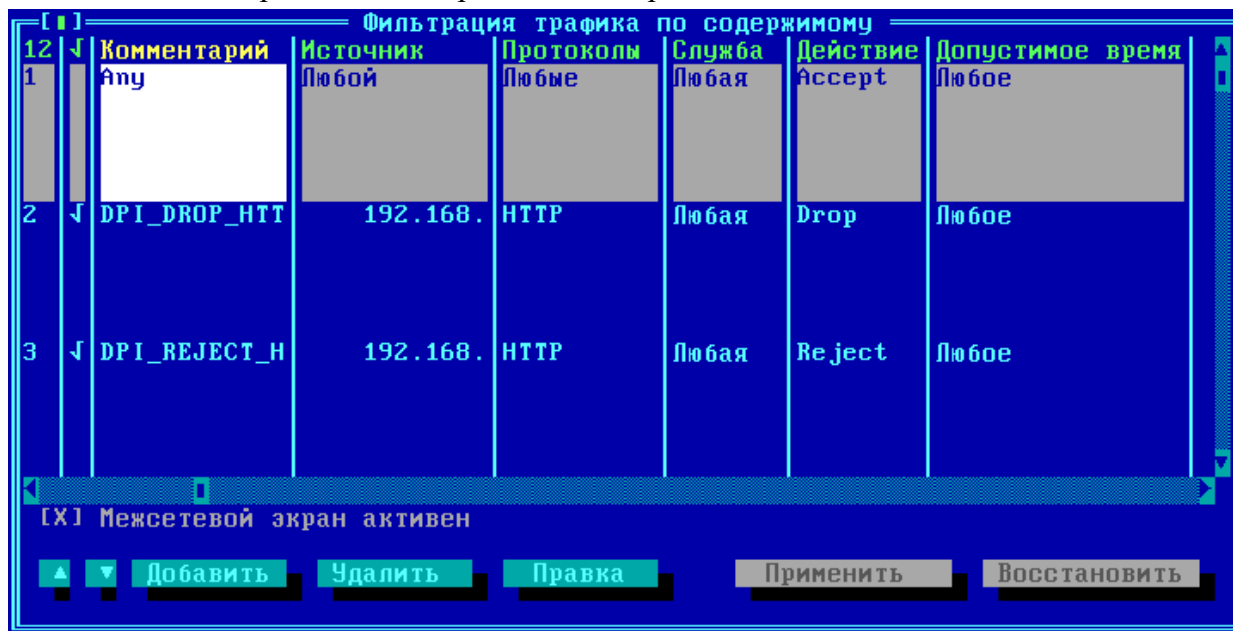


Рисунок 207 - Окно списка правил фильтрации трафика по содержимому

Фильтрация трафика по содержимому осуществляется только при активном межсетевом экране ФПСУ-IP. Переключатель "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 клавишу "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 нажатием сочетаний клавиш <Ctrl> + < > и <Ctrl> + << >.

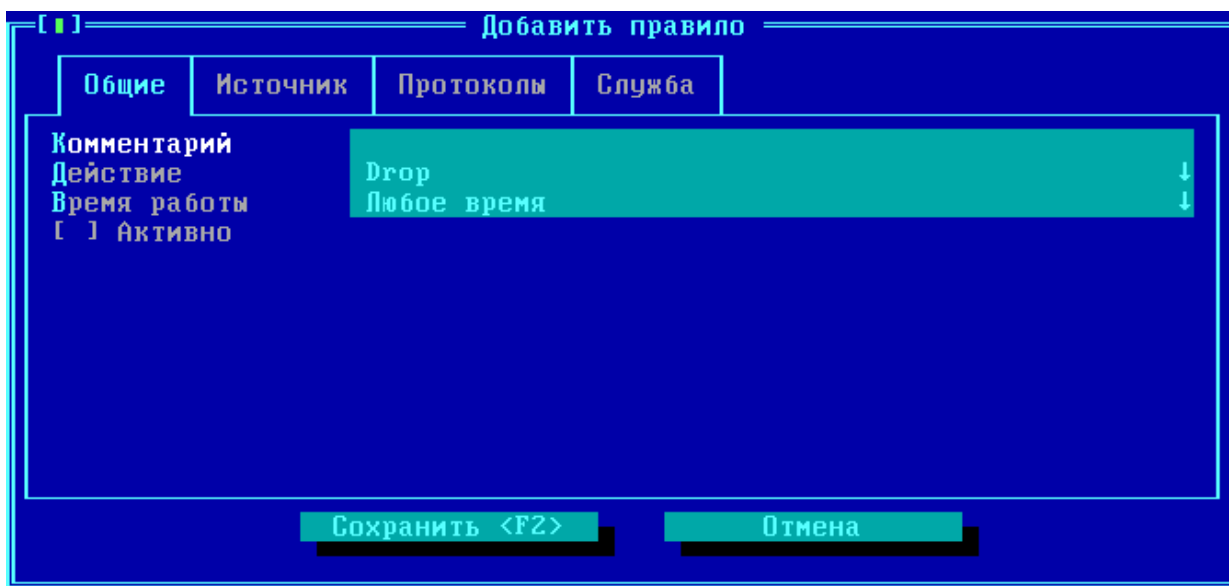


Рисунок 208 - Добавление нового правила фильтрации по содержимому

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 "v" 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 – переключатель, который указывает на то, что данное правило следует задействовать при работе межсетевого экрана.

Перемещение между вкладками осуществляется нажатием сочетаний клавиш <Ctrl> + <> и <Ctrl> + <<>.

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 **Источника** 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).

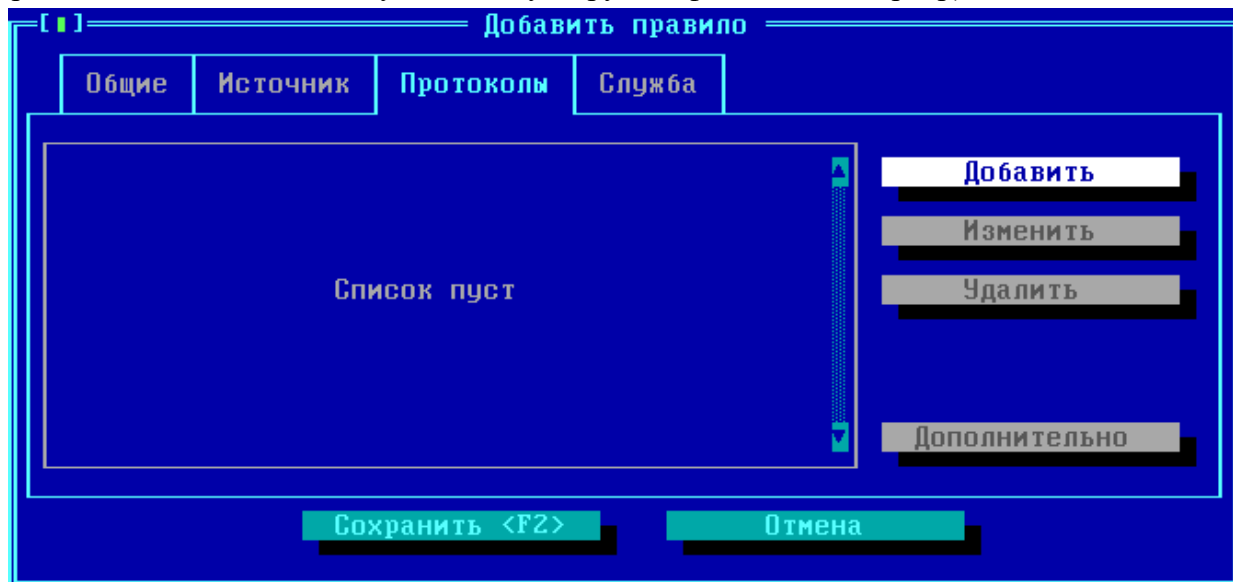


Рисунок 209 - Вкладка "Протоколы"

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".

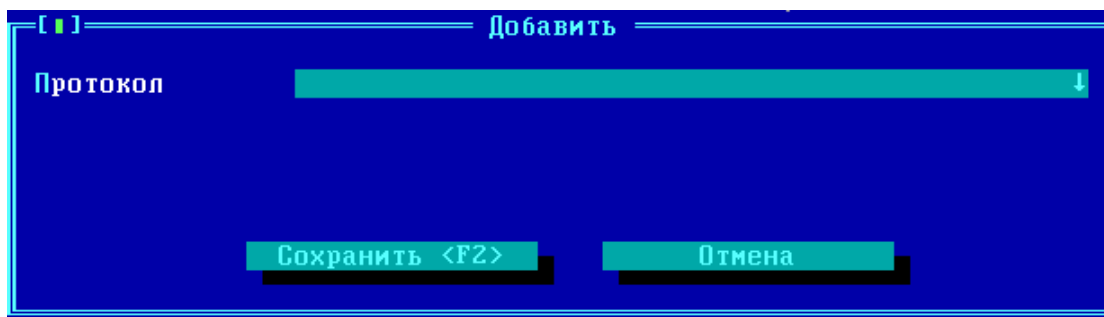


Рисунок 210 - Окно выбора исследуемого протокола

Из выпадающего списка поля "Протокол" следует выбрать один из доступных для анализа протоколов:

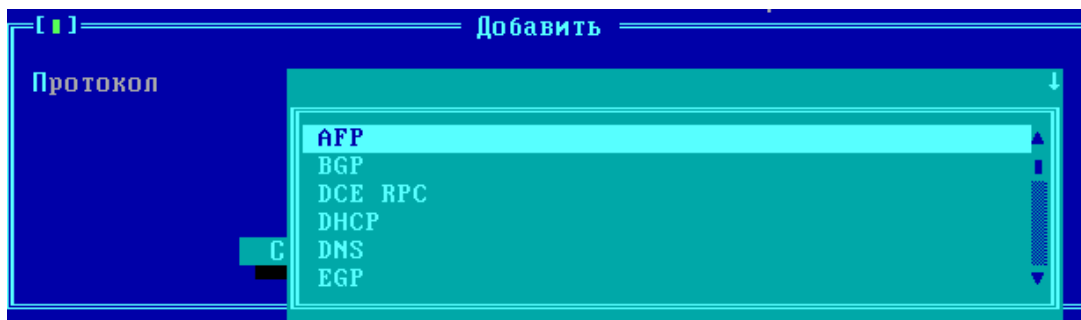


Рисунок 211 - Выбор исследуемого протокола

После выбора курсором одного из предлагаемых протоколов, нажмите клавишу Enter для подтверждения выбора. Выбранный протокол будет указан в поле "Протокол" окна (в примере - HTTP):

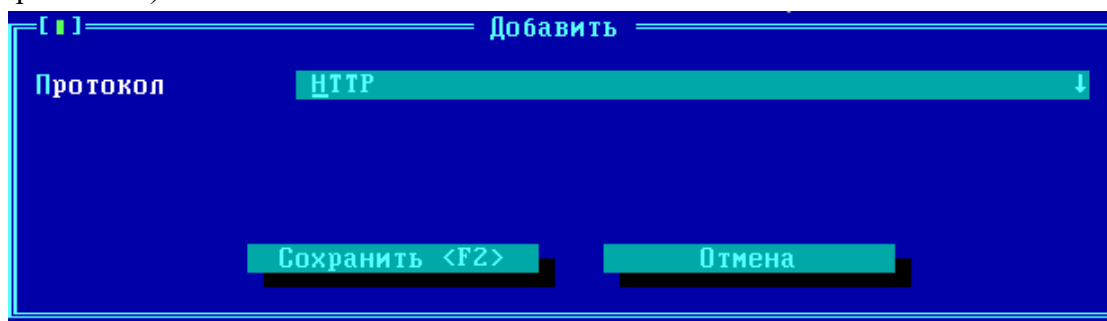


Рисунок 212 - Выбран протокол для исследования

Нажмите клавишу <F2> или кнопку "Сохранить F2" для возврата в интерфейс настройки правила фильтрации трафика по содержимому. Выбранный протокол будет указан в списке:

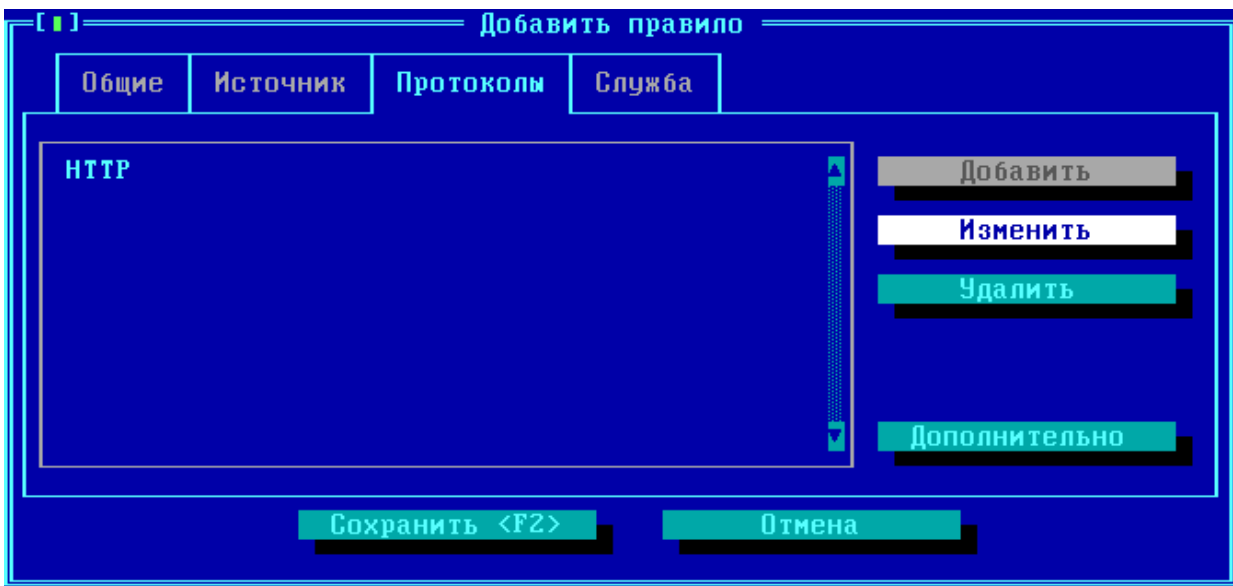


Рисунок 213 - Протокол, исследуемый правилом

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:

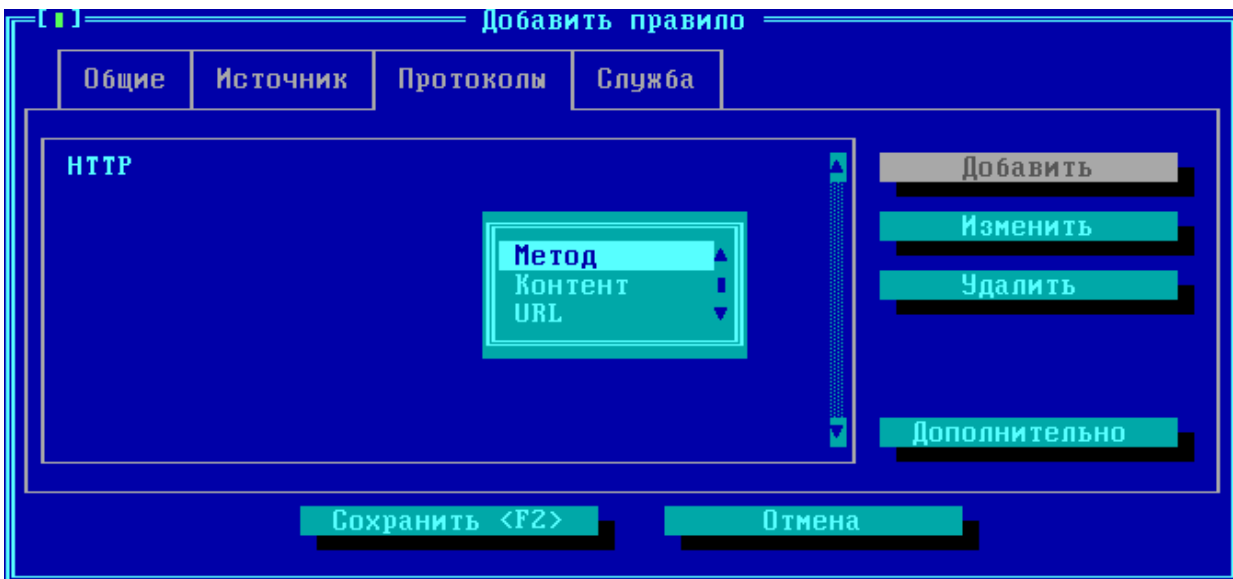


Рисунок 214 - Доступные опции исследования протокола HTTP

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

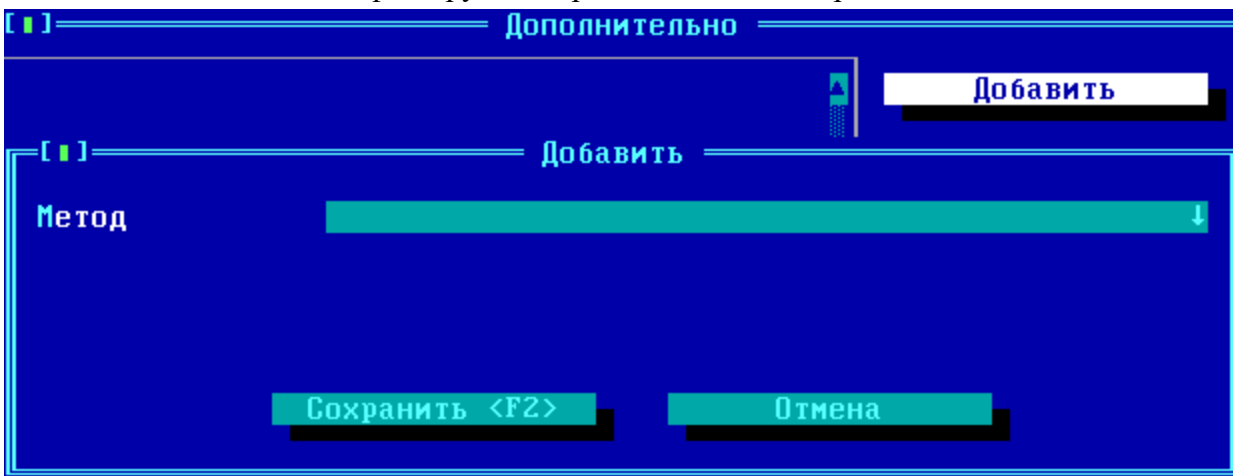


Рисунок 215 - Добавление фильтруемого метода протокола http

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):

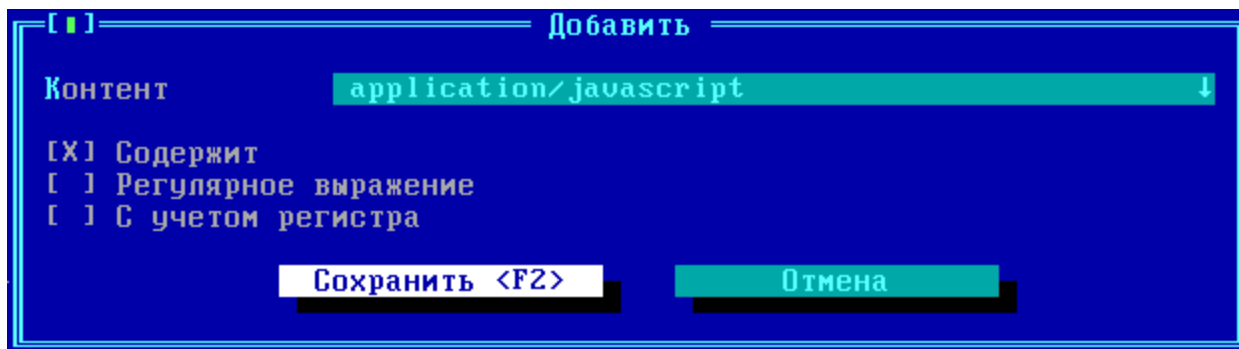


Рисунок 216 - Добавление фильтруемого контента протокола http

В качестве фильтруемого URL-адреса может стоять как точное символьное выражение (например, *example.com*), так и встречающаяся в нём строка или регулярное выражение.

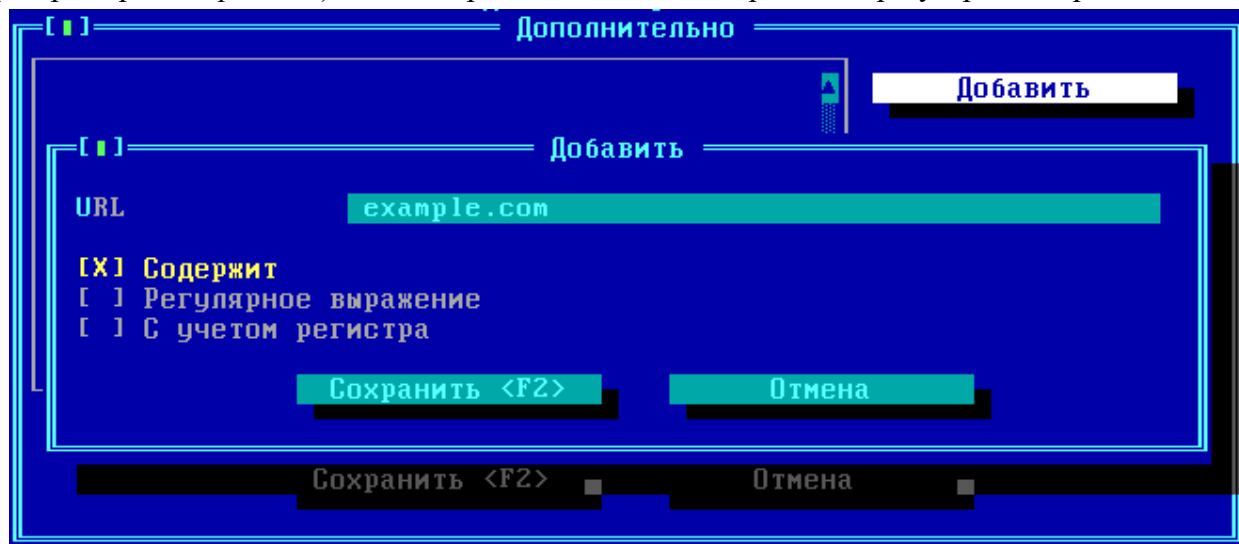


Рисунок 217 - Добавление фильтруемого URL-адреса протокола http

После сохранения дополнительных опций, которые задействуют несколько фильтров, в интерфейсе фильтруемого протокола будет указан признак, что исследуется трафик http-протокола несколькими фильтрами:

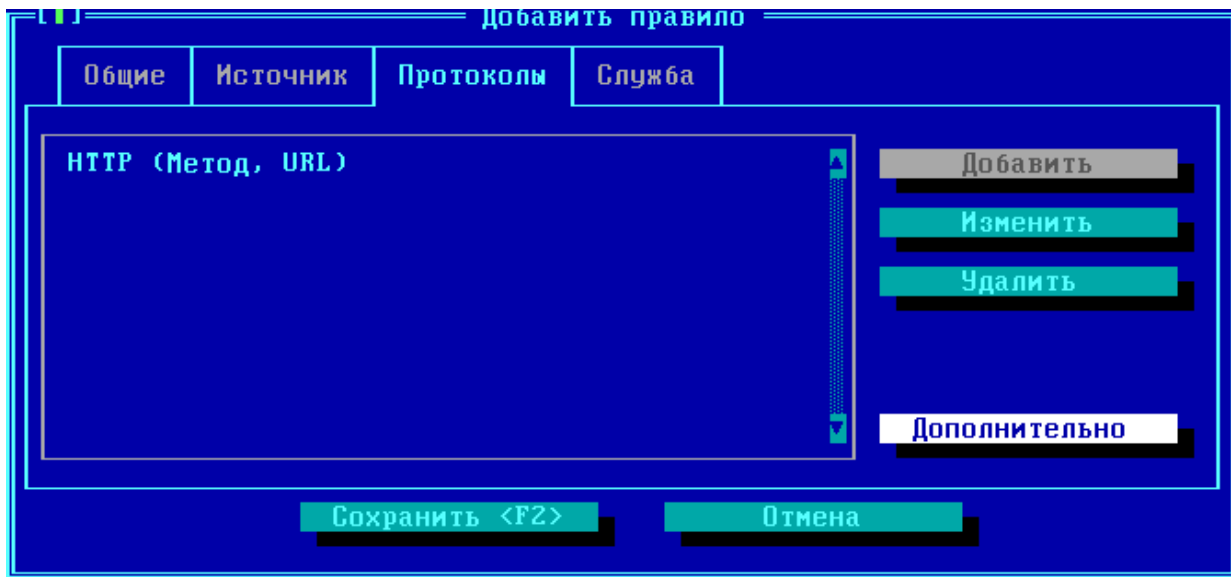


Рисунок 218 - Правило с дополнительными фильтрами протокола http

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](#)").

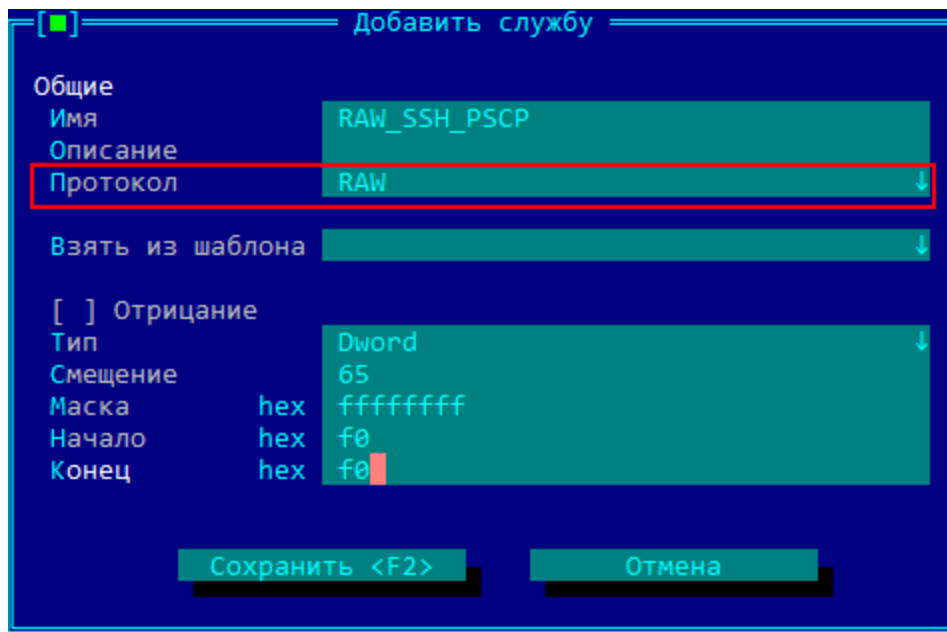


Рисунок 219 - Служба для протокола RAW

2. Если требуется выполнить фильтрацию трафика по содержимому одновременно и по **Службам**, и по **Протоколу**, то потребуются 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.

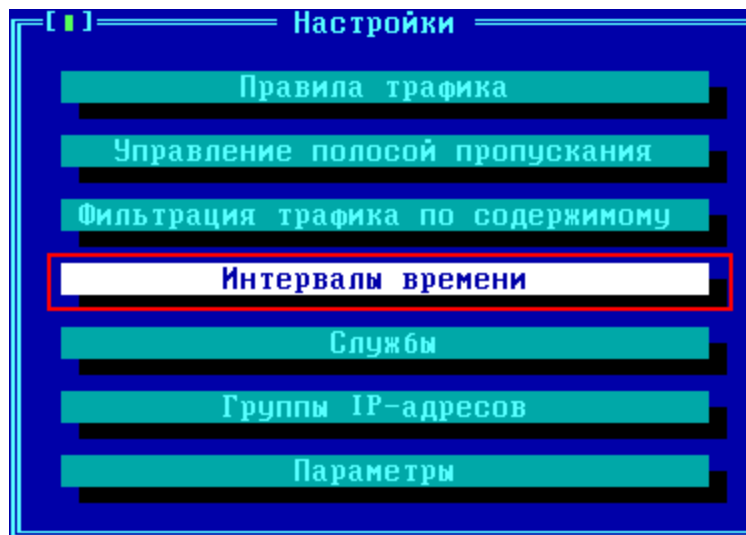


Рисунок 220 - Команда "Интервалы времени"

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):

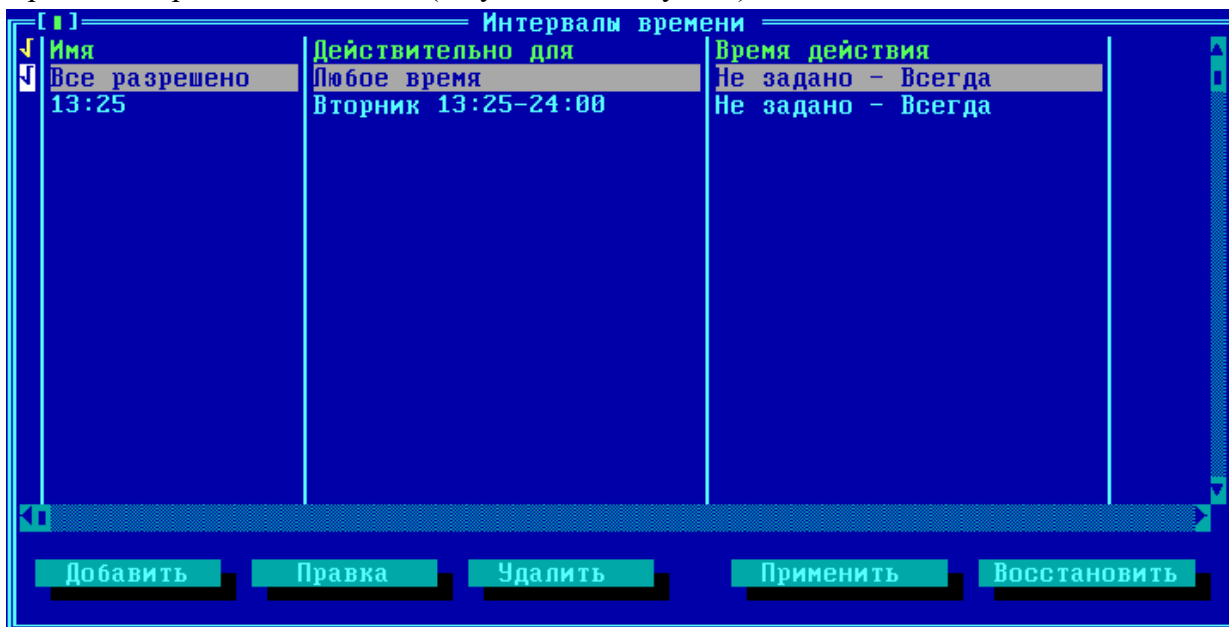


Рисунок 221 - Список определенных интервалов времени

Команды окна управления списком интервалов:

Добавить — кнопка, по нажатию которой 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 этой 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 222 - 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 . После определения всех интервалов следует отметить знаком [X] (при помощи клавиши <Пробел>) переключатель включения сделанных ограничений, "Активно".

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 Параметров доступа" правил дополнительной фильтрации, находится список созданных администраторами ФПСУ-IP групп IP-адресов (по умолчанию пустой).

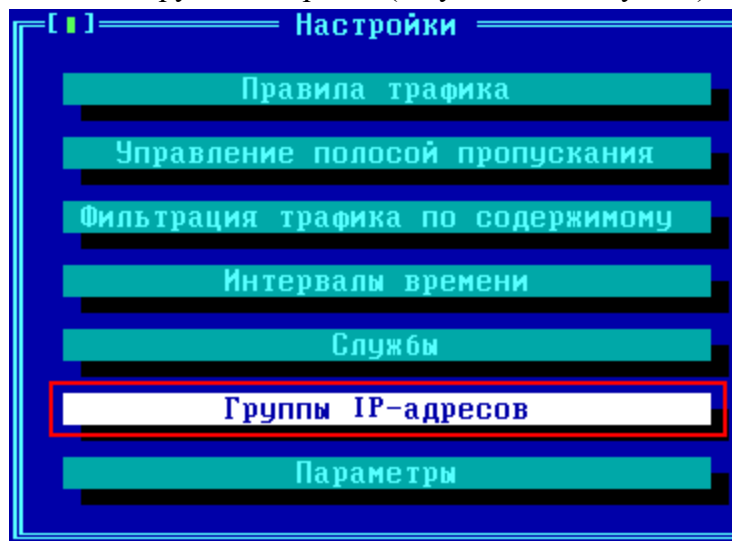


Рисунок 223 - Команда настройки групп IP-адресов параметров доступа

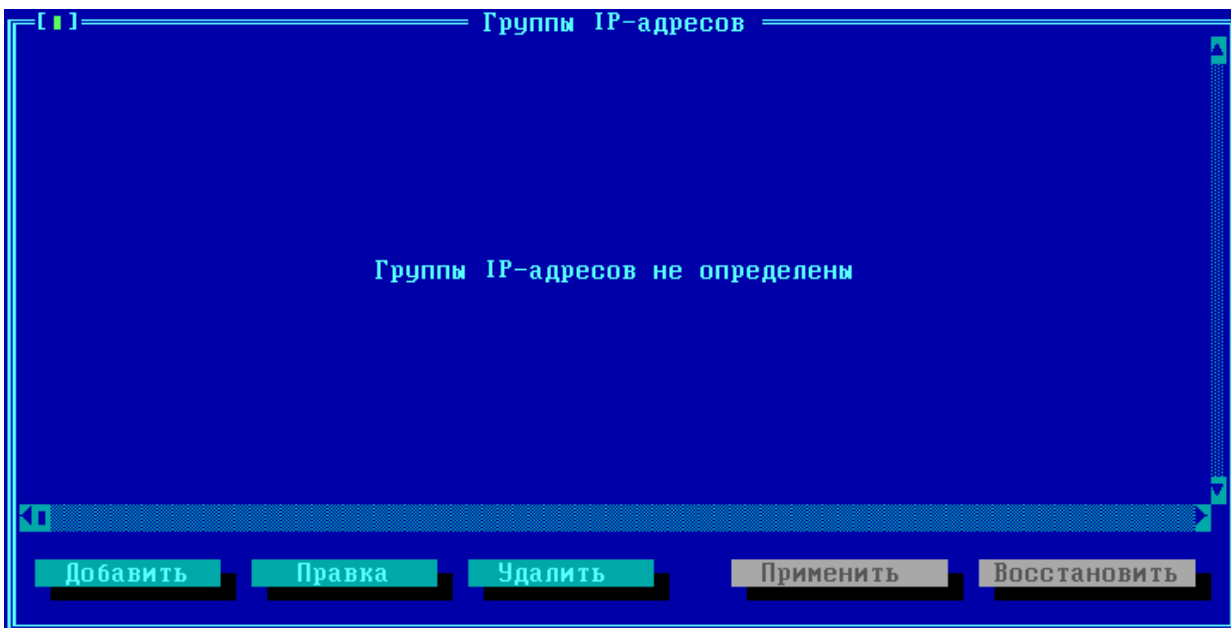


Рисунок 224 - Окно со списком групп IP-адресов

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 нажатием сочетаний клавиш *<Ctrl> + <>* и *<Ctrl> + <<>*.

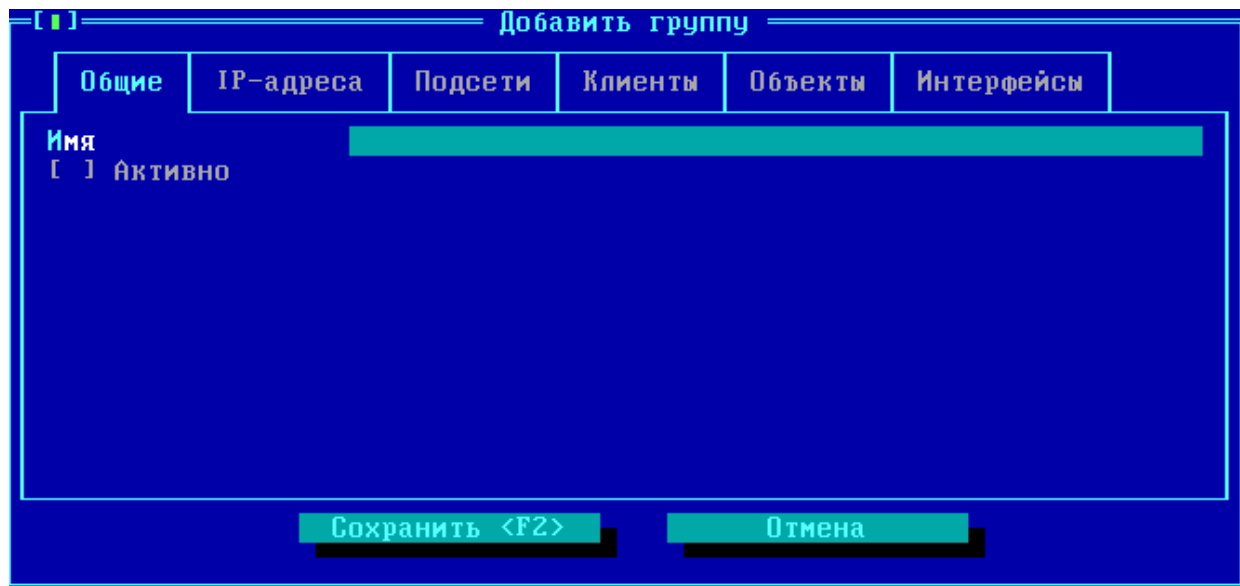


Рисунок 225 - Создание новой группы IP-адресов

Вкладка **Общие** содержит символьное название создаваемой группы, которое будет использоваться для привязки группы IP-адресов к тому или иному правилу трафика, и переключатель *<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:

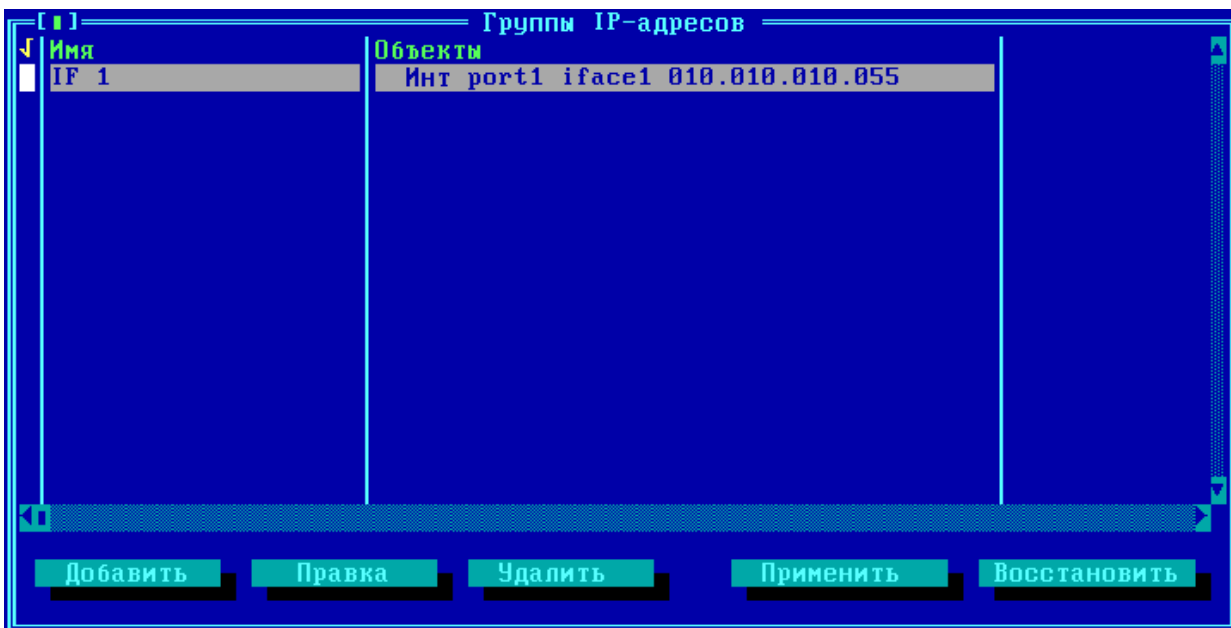


Рисунок 226 - В список Групп IP-адресов добавлена новая запись

10. 7. Дополнительные параметры и защита от flood-атак

Окно "Параметры" подменю "Настройки" правил дополнительной фильтрации содержит список дополнительных опций межсетевого экрана.

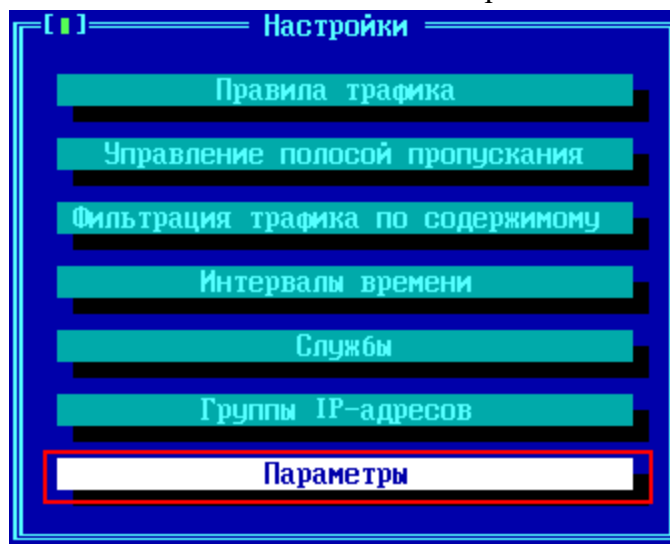


Рисунок 227 - Дополнительные параметры межсетевого экрана ФПСУ-IP

Окно состоит из трех вкладок. Первые две, "Соединения" и "Flood-атака", предназначены для настройки системы защиты ФПСУ-IP от атак отказа в обслуживании (flood-атак). Переход между вкладками осуществляется нажатием сочетания клавиш <Ctrl +

> > и <Ctrl + < >.

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).

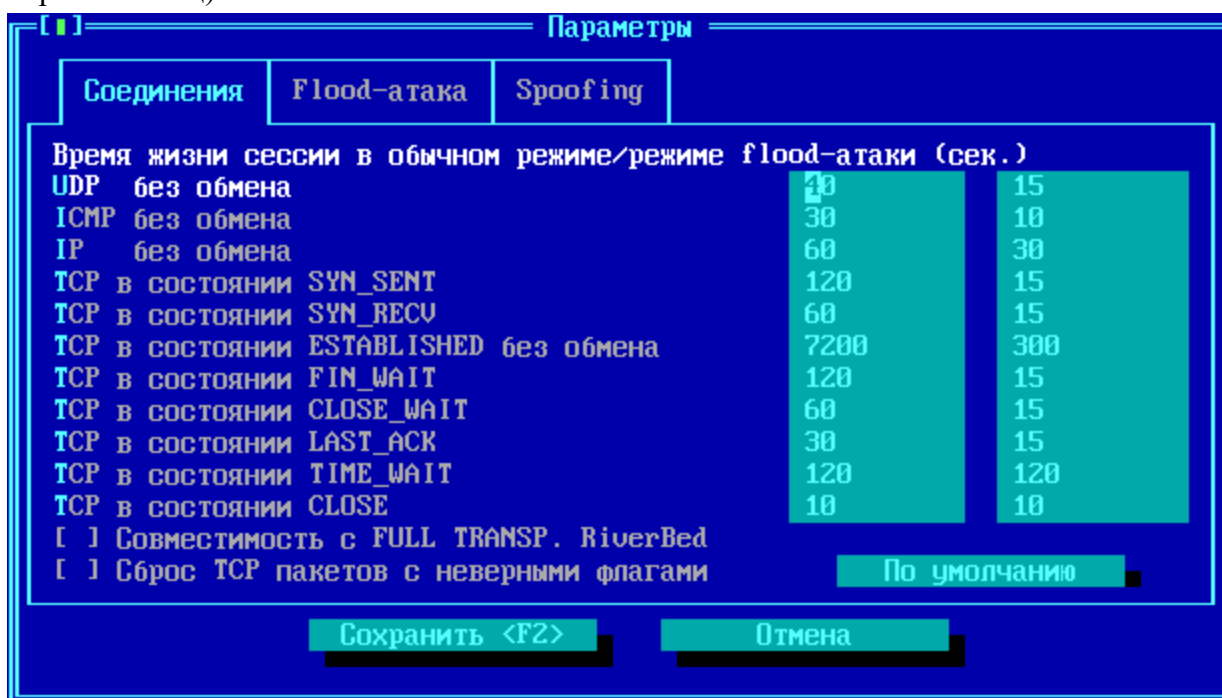


Рисунок 228 - Параметры ограничения соединений

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 межсетевое экрана ФПСУ-IP, но таймауты различаются.

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

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

Вкладка **Flood-атака** 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.

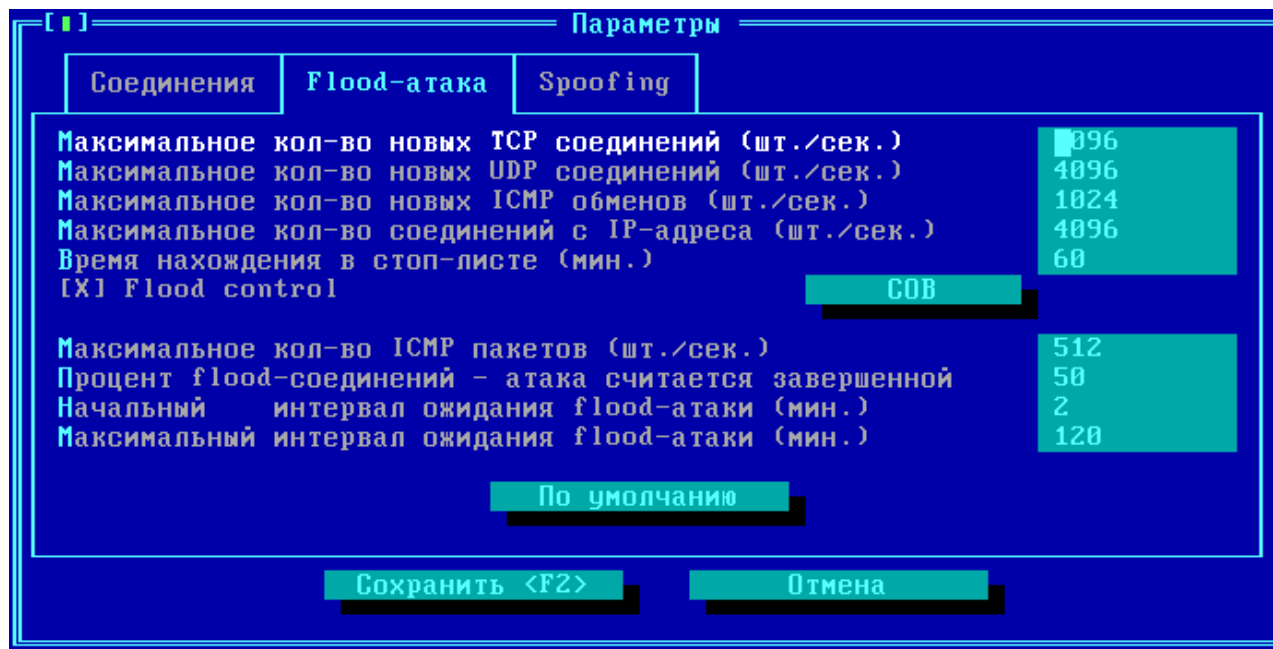


Рисунок 229 - Параметры работы ФПСУ-IP во время flood атаки

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.

Если переключатель "[] Flood control" установлен, то IP-адрес будет находится в стоп-листе время, указанное в поле "Время нахождения в стоп-листе (мин.)". Если переключатель "[] Flood control" не установлен, то IP-адрес будет находится в стоп-листе до перезагрузки ФПСУ-IP.

Переключатель "[] Flood control" 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 переключатель 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 – 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.

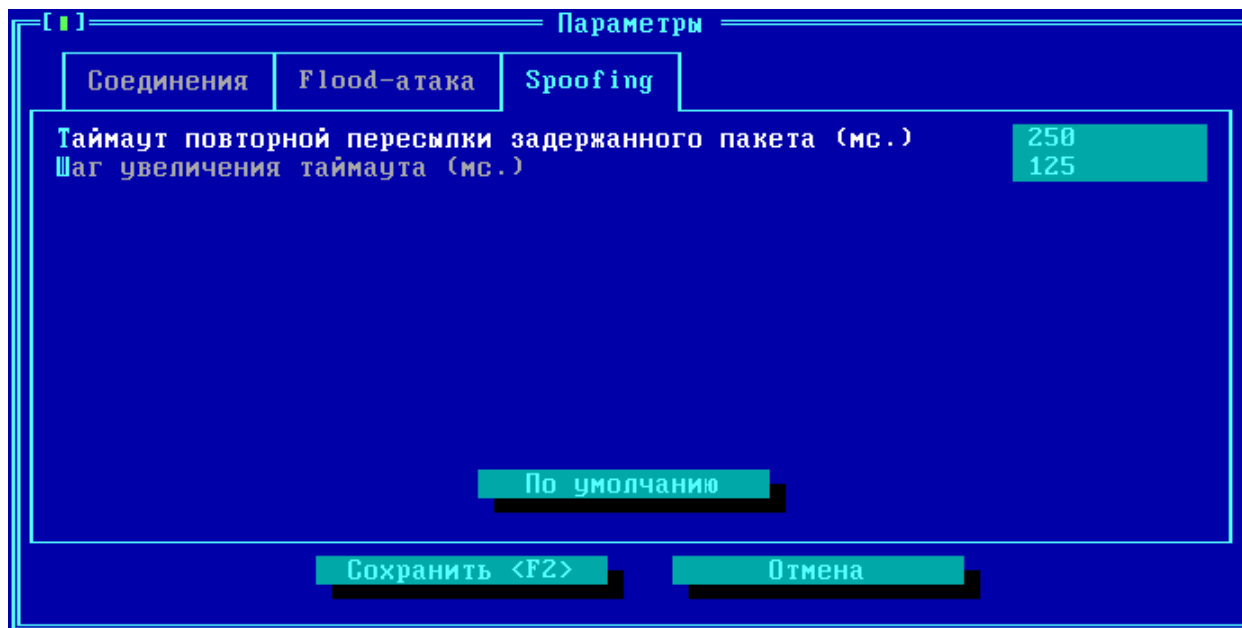


Рисунок 230 - Параметры передачи подтверждений в режиме Spoofing

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, номер группы в Криптосети, номер клиента в группе).

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 МЭ ФПСУ-IP, который должен работать шлюзом для подключений клиентов.

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, принадлежащим одной или нескольким Криптосетям Клиентов, в одной группе может быть зарегистрировано не более 1024 Клиентов.

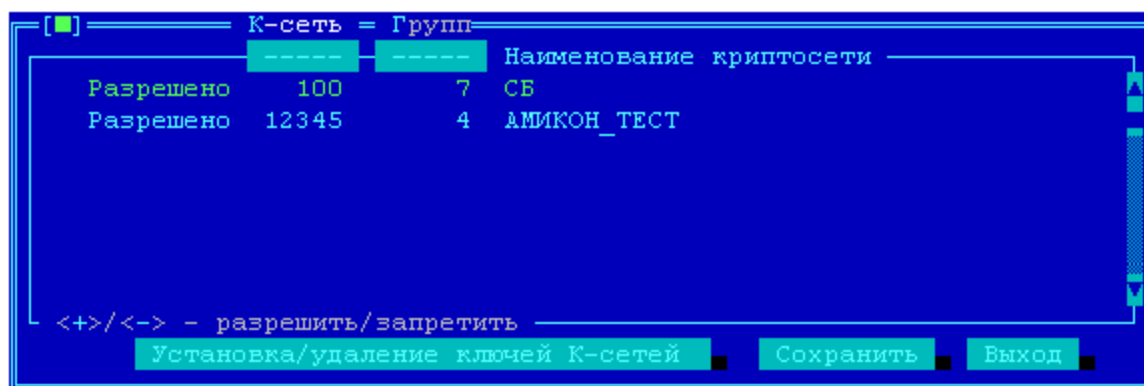


Рисунок 231 - Список групп Клиентов на ФПСУ-IP

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 . 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 поле "Установка/удаление ключей ЦГКК" – см. раздел "[Установка и удаление общесистемных ключей](#)".

11. 1. Установка и удаление общесистемных ключей

Для установки нового общесистемного ключа на ФПСУ-IP выполните следующие действия:

В окне списка групп криптосетей нажмите кнопку "Установка/удаление ключей Крипосетей", после чего на экран монитора будет выдан список Крипосетей клиентов, ключи которых были установлены на ФПСУ-IP.

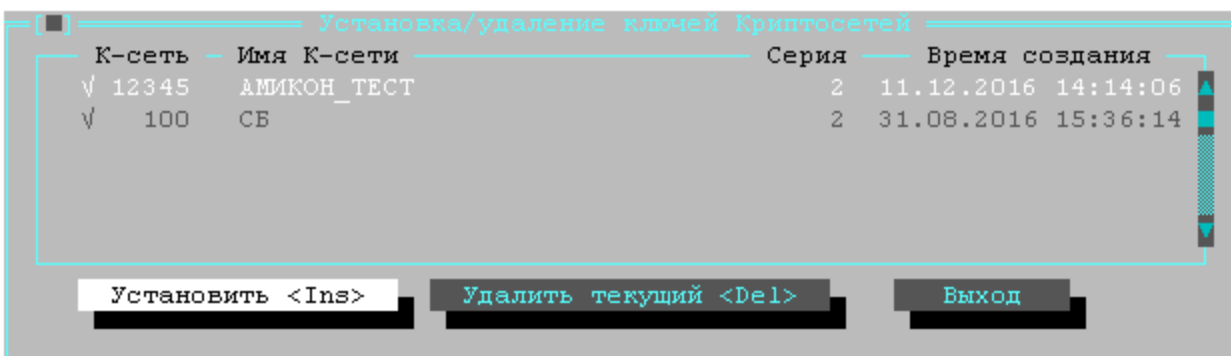


Рисунок 232 - Установленные на ФПСУ-IP ключи Крипосетей клиентов

Если строка слева помечена символом "v" – это означает, что ключи уже зарегистрированы на ФПСУ-IP, то есть для Крипосети 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 Крипосети клиентов. Если ключи не используются в конфигурации ФПСУ-IP, их можно удалить с помощью клавиши или выбора соответствующей кнопки.

Чтобы установить новые ключи, активизируйте поле "Установить <Ins>", после чего на экран будут последовательно выдаваться приглашения на прижатие к контактному устройству всех ТМ-идентификаторов с первичными ключами, которые были выработаны ЦГКК.

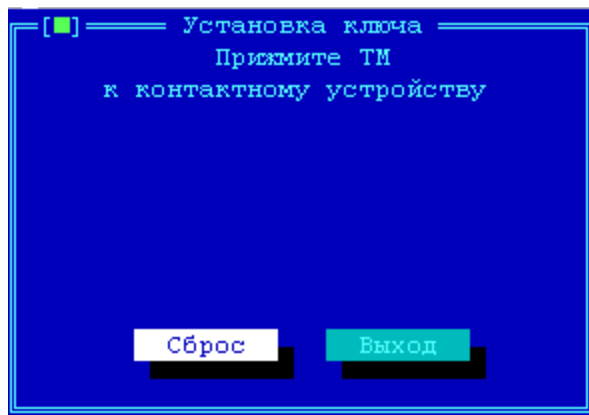


Рисунок 233 - Ожидание ТМ-идентификатора

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.

11. 2. Описание логической группы клиентов

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

В окне "Группы ЦГКК" нажмите клавишу <Ins>, после чего на экран будет выдан список Криптосетей, общесистемные ключи которых были ранее установлены на ФПСУ-IP.

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.
- VPNMOBIL – пользователи программного комплекса "ФПСУ-IP/Клиент", не использующие USB-устройство VPN-Key. **ВНИМАНИЕ!** для поддержки пользовательских подключений VPNMOBIL на ФПСУ-IP необходимо

установить специальное обновление активации мобильных клиентов ФПСУ-IP!

После введения номера и указания типа группы клиентов нажмите кнопку "Добавить". В результате выполнения команды пустая запись группы появится в окне "Группы ЦГКК".

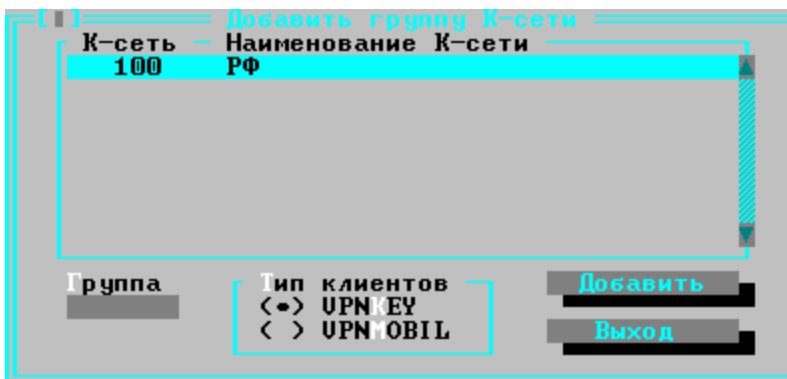


Рисунок 234 - Добавление группы клиентов

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 мобильных клиентов типа VPNMOBIL, то она будет дополнительно отмечена буквой "М".

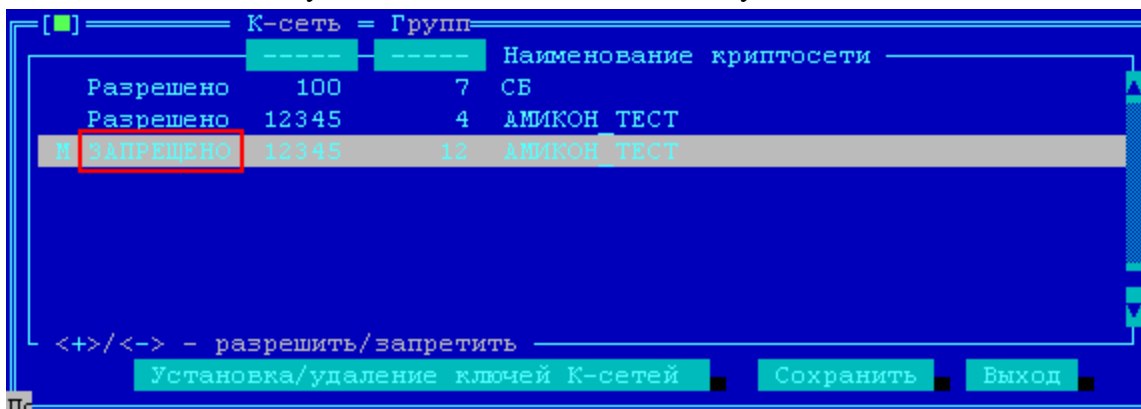


Рисунок 235 - Создана новая группа клиентов

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.

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.

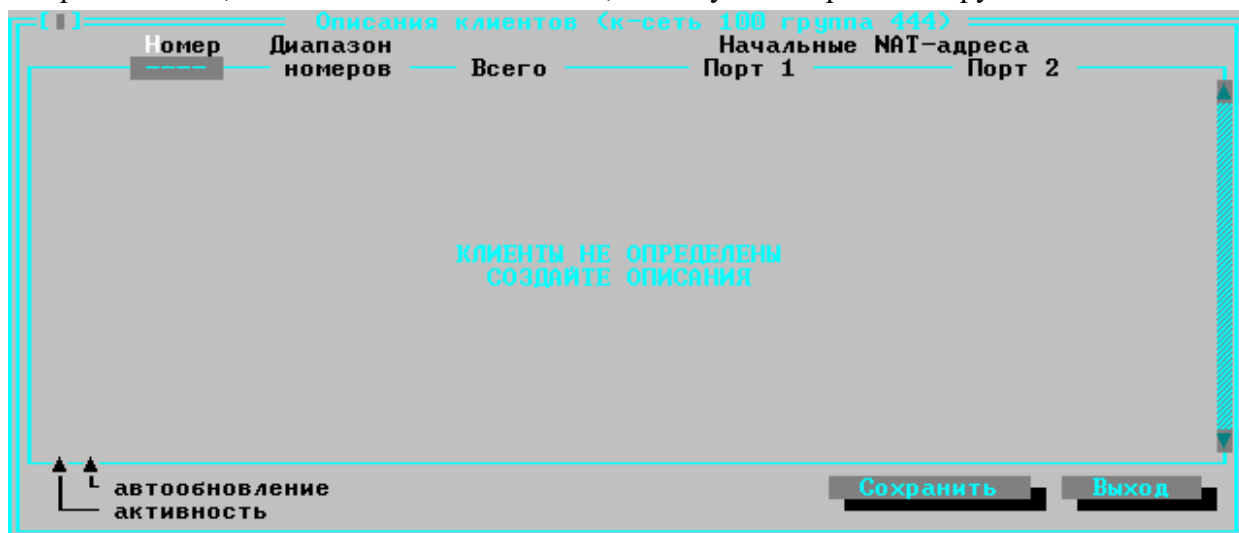


Рисунок 236 - Пустой список описаний новой группы

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>*. Появится окно указания параметров взаимодействия клиентов и ФПСУ-IP.

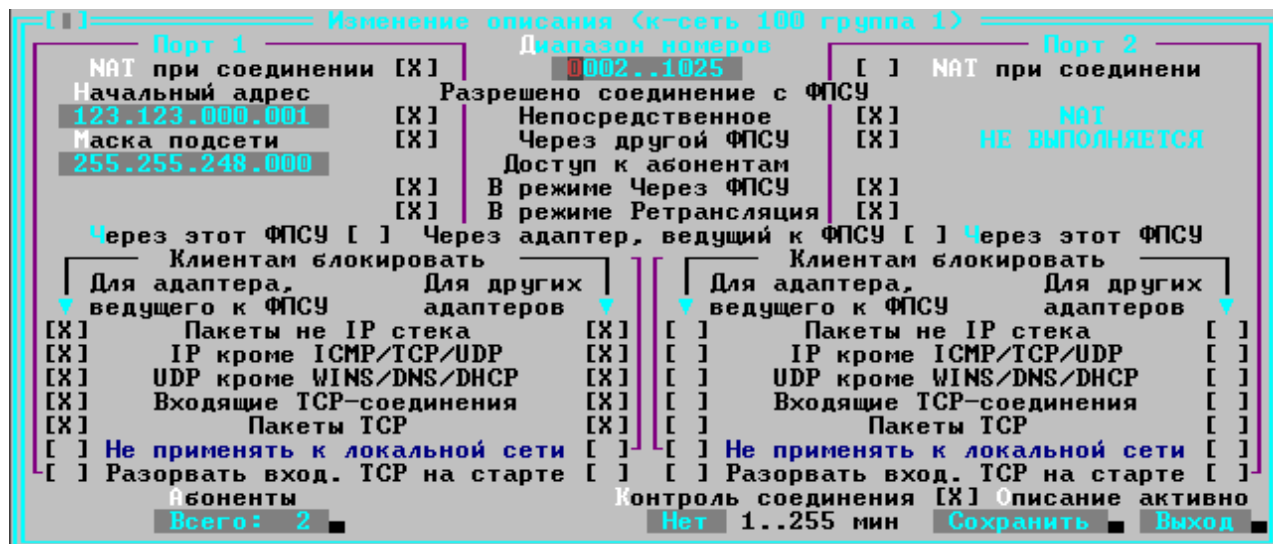


Рисунок 237 - Описание параметров работы диапазона Клиентов

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

Обратите внимание, что 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
<i>Диапазон номеров</i>	- диапазон уникальных номеров клиентов, для которых устанавливаются правила. Диапазоны номеров различных описаний не могут пересекаться;
<i>NAT при соединении</i>	- указание ФПСУ-IP производить трансляцию реальных IP адресов клиентов описываемого диапазона во внутренние (виртуальные) адреса защищаемой подсети при соединениях со стороны данного порта;
<i>Начальный адрес</i>	- в случае применения NAT-трансляции первый из IP адресов внутренней подсети, в который будет транслироваться реальный IP-адрес первого клиента описываемого диапазона;

Параметр	Описание параметра
Маска подсети	<p>- в случае применения NAT-трансляции используется маска внутренней подсети, рассчитанная на количество клиентов описываемого диапазона.</p> <p>ВНИМАНИЕ! В диапазон адресов, образованный начальным адресом и маской, не должен попадать ни один реально существующий IP-адрес, указанный в конфигурации ФПСУ-IP;</p>
Разрешено соединение через ФПСУ	<p>- 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, отметьте при помощи клавиши <Пробел> оба переключателя. Если ни один переключатель не выставлен – доступ клиентам со стороны данного порта ФПСУ-IP предоставляться не будет;</p>
Разрешен доступ к абонентам	<p>- 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, отметьте при помощи клавиши <Пробел> оба переключателя. Если ни один переключатель не выставлен, доступ клиентам со стороны данного порта ФПСУ-IP к другим рабочим станциям предоставляться не будет;</p>
Через адаптер, ведущий к ФПСУ	<p>- 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. <u>Обратите внимание</u>, что при включении опции открытые соединения рабочей станции Клиента через ведущий к ФПСУ-IP сетевой адаптер будут невозможны;</p>
Клиентам	<p>- указание клиентам при работе со стороны данного порта ФПСУ-IP</p>

Параметр	Описание параметра
блокировать	блокировать соответствующие соединения. Установленные администратором ФПСУ-IP ограничения будут выполняться на всех указанных сетевых адаптерах рабочих станций клиентов принудительно, независимо от собственных установок клиентов. (Примечание: для клиентов типа VPNMOBIL такой вид <u>дополнительной настройки недоступен</u>);
Не применять к локальной сети	- переключатель, позволяющий 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.
Контроль соединения	- временной интервал (от 1 до 255 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. Если контроль не требуется, оставьте поле пустым и нажмите <Enter>. 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. <u>Если переключатель не выставлен в положение "X", работа клиентов данного диапазона будет блокирована.</u> Переключатель включается и выключается при помощи клавиши <Пробел>.
Группы доступа	- переход к интерфейсу настройки параметров доступа абонентов и

Параметр	Описание параметра
	клиентов ФПСУ-IP (см. раздел " Правила трафика межсетевого экрана ").
<i>VLAN</i>	Номер виртуальной частной сети, в которой участвует клиент.
<i>Абоненты</i>	- 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.

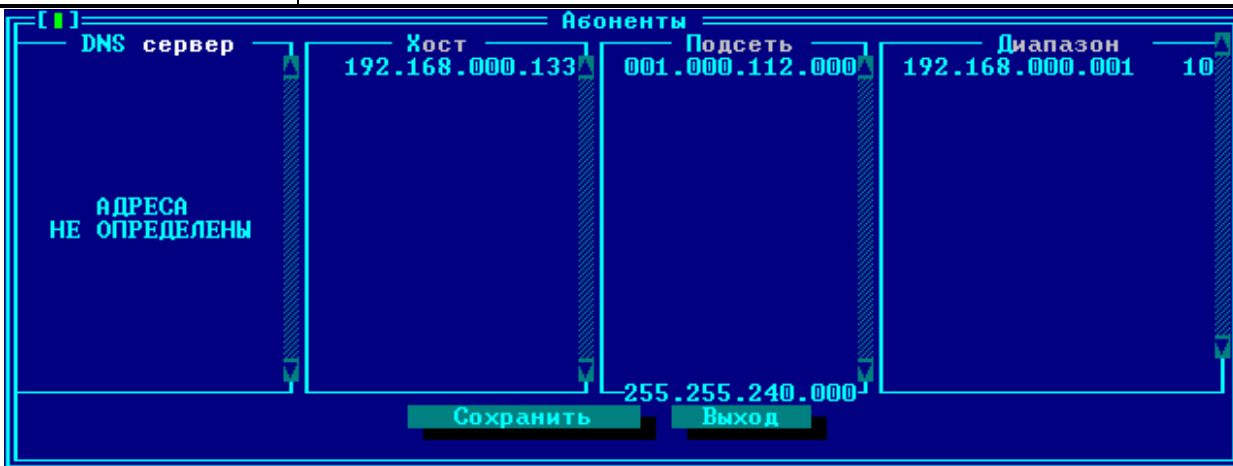


Рисунок 238 - Абоненты ФПСУ-IP, доступные ФПСУ-IP/Клиенту

Для создания или корректировки списка абонентов, нажмите кнопку "Абоненты", после чего откроется окно списка передаваемых клиенту IP-адресов.

Абонентами могут выступать описатели отдельного IP-адреса (столбец "Хост"), подсети, диапазон последовательно идущих IP-адресов (столбец "Диапазон") и специальный абонент "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), ** (для удаления), *<Enter>* или *<Пробел>* (для редактирования).

Нажатие кнопки "Сохранить" возвращает в окно описания параметров работы группы клиентов.

После установки всех параметров активизируйте поле "Сохранить", после чего будет произведен выход в окно списка описаний со списком клиентов в группе.

Номер	Время работы		NAT-адреса	
	От	До	Порт 1	Порт 2
2	Не задано	Всегда	123.123.000.001	NAT отключена
3	Не задано	Всегда	123.123.000.002	NAT отключена
4	Не задано	Всегда	123.123.000.003	NAT отключена
5	Не задано	Всегда	123.123.000.004	NAT отключена
6	Не задано	Всегда	123.123.000.005	NAT отключена
7	Не задано	Всегда	123.123.000.006	NAT отключена
8	Не задано	Всегда	123.123.000.007	NAT отключена
9	Не задано	Всегда	123.123.000.008	NAT отключена
10	Не задано	Всегда	123.123.000.009	NAT отключена
11	Не задано	Всегда	123.123.000.010	NAT отключена
12	Не задано	Всегда	123.123.000.011	NAT отключена
13	Не задано	Всегда	123.123.000.012	NAT отключена
14	Не задано	Всегда	123.123.000.013	NAT отключена
15	Не задано	Всегда	123.123.000.014	NAT отключена
16	Не задано	Всегда	123.123.000.015	NAT отключена
17	Не задано	Всегда	123.123.000.016	NAT отключена

Подключение → IP: Любой Host
 разрешение активности: Любой
 Buttons: Сохранить, Выход

Рисунок 239 - Список зарегистрированных в группе Клиентов

Для перехода к форме списка описаний правил работы нажмите клавишу <Пробел>.

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

Номер	Диапазон номеров	Всего	Начальные NAT-адреса	
			Порт 1	Порт 2
v	2.. 6	5	192.168.005.001	NAT отключена
-	52.. 62	11	NAT отключена	NAT отключена

Buttons: Сохранить, Выход

Рисунок 240 - Список описаний диапазонов Клиентов

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 изменить правила работы какого-либо клиента, отметьте его описатель и нажмите <Пробел>.

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

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

11. 4. 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:

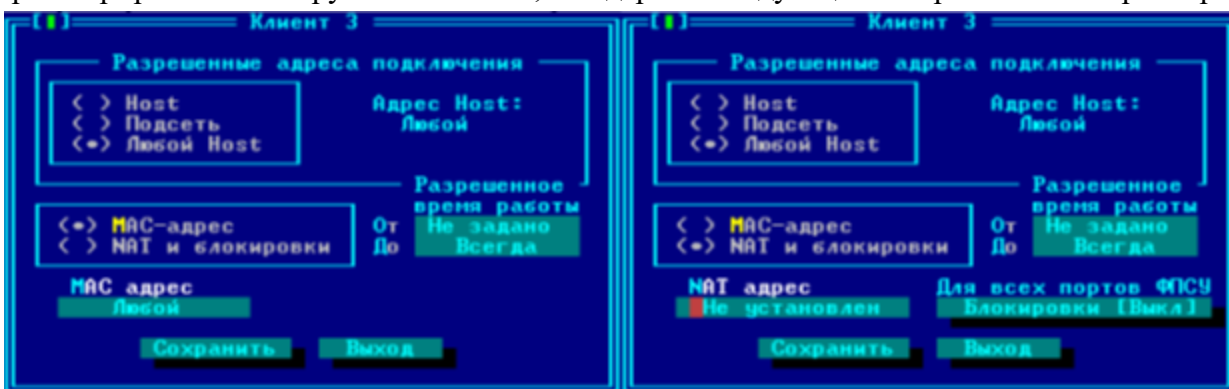


Рисунок 241 - Параметры работы отдельного Клиента

Разрешенные адреса подключения, выбор диапазона IP-адресов, с которого данному Клиенту разрешено подключение к ФПСУ-IP:

- *Host* – 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.

MAC-адрес – значение переключателя, при выставлении 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 выставленном переключателе *MAC-адрес не работают* настройки, ранее выполненные в полях "*NAT и блокировки*" (см. далее).

NAT и блокировки – значение переключателя, при выставлении которого можно указать исключения в работе данного Клиента из общих настроек, сделанных в описании диапазона Клиентов (см. пункт "[Установка правил работы клиентов](#)").

При выставлении переключателя "*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 выставленном переключателе "*NAT и блокировки*" так же могут быть указаны отличные от выставленных в описании всего диапазона Клиентов блокировки. Для этого выполните переход в окно индивидуальных блокировок, нажав кнопку "*Для всех портов ФПСУ- Блокировки*".

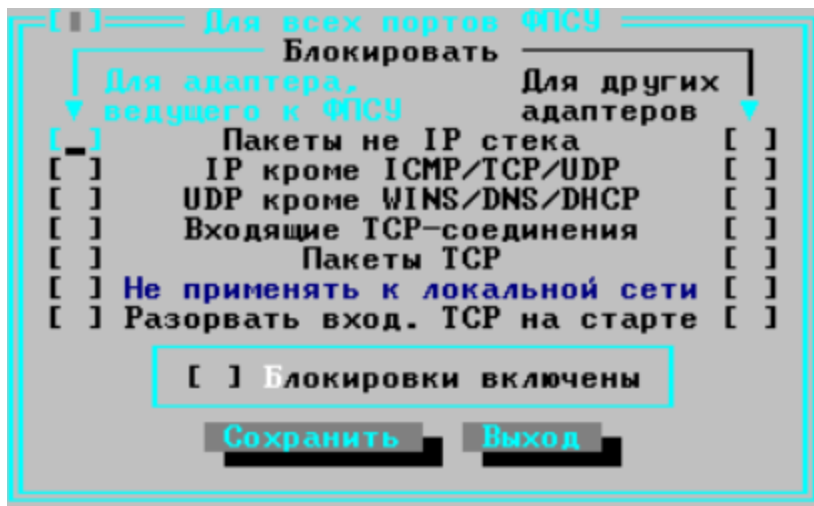


Рисунок 242 - Индивидуальные блокировки Клиента

В окне индивидуальных блокировок отдельного Клиента, при выставлении переключателя "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 выставленном переключателе "*NAT и блокировки*" не работают ранее

выполненные настройки, указанные в поле "MAC адрес".

Примечание: для клиентов типа VPNMOBILE 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, сконфигурированный на формирование нескольких различных потоков с различными маршрутами следования или ограничения полосы их пропускания (функция "shaping"), этот маршрутизатор не сможет вычленив 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 сконфигурирован на разделение потоков, а один из пограничных маршрутизаторов (или даже все) - не сконфигурирован, 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.

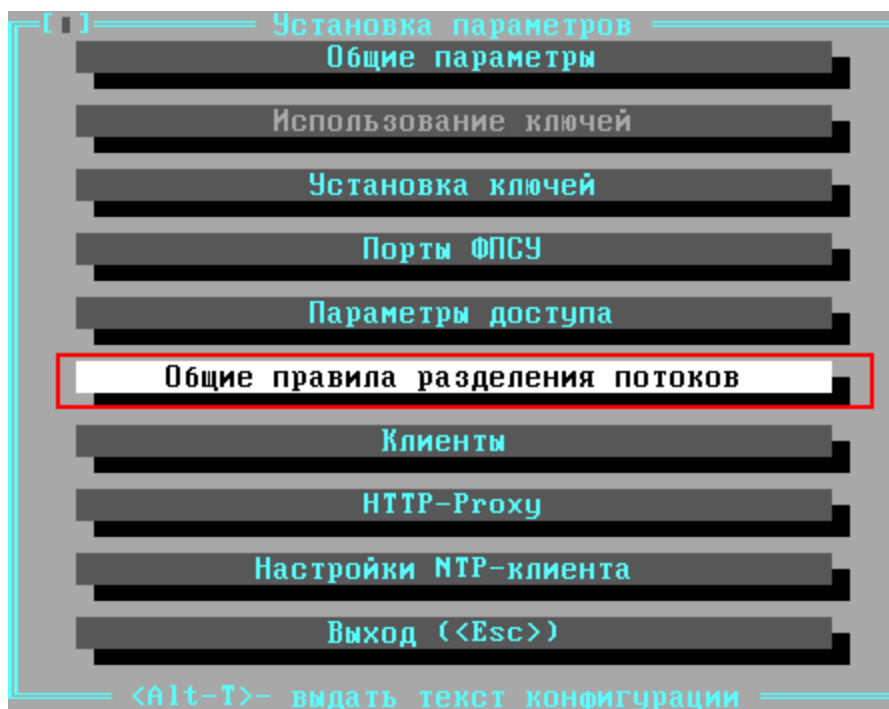


Рисунок 243 - Меню подсистемы конфигурирования ФПСУ-IP

По активизации команды "Общие правила разделения потоков" на экране появляется окно, содержащее список установленных общих правил или пустое, если правила еще не описывались.

Чтобы добавить новое общее правило, следует нажать клавишу <Ins>, после чего открывается окно "Установка нового общего правила".

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).

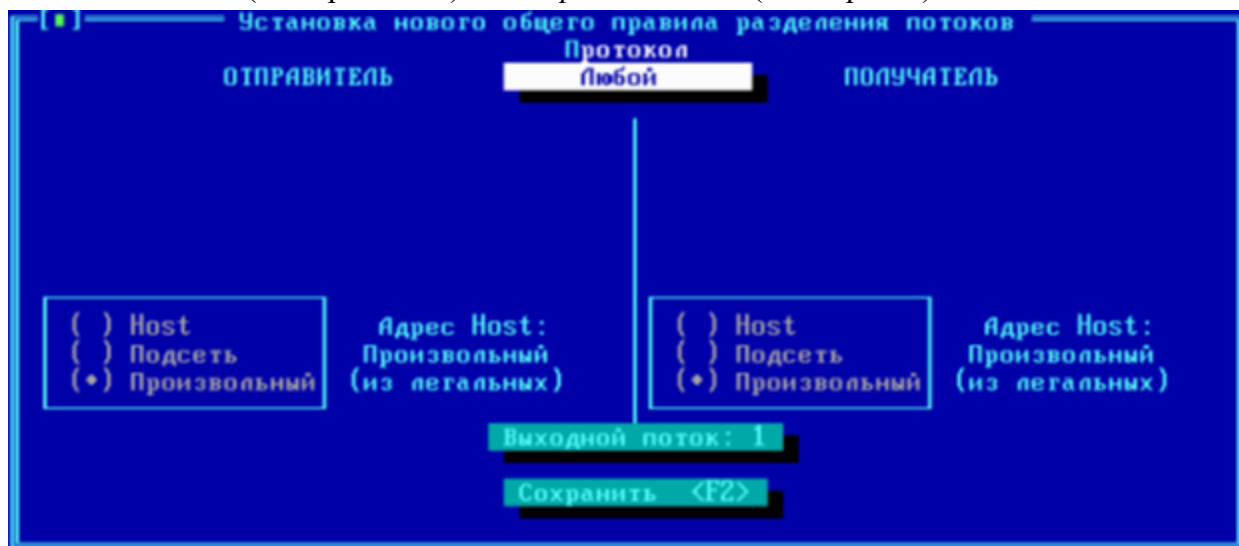


Рисунок 244 - Создание нового общего правила разделения потоков

Чтобы установить для выходного потока какой-либо конкретный протокол, нужно "встать" 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).

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 умолчанию 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.

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)».

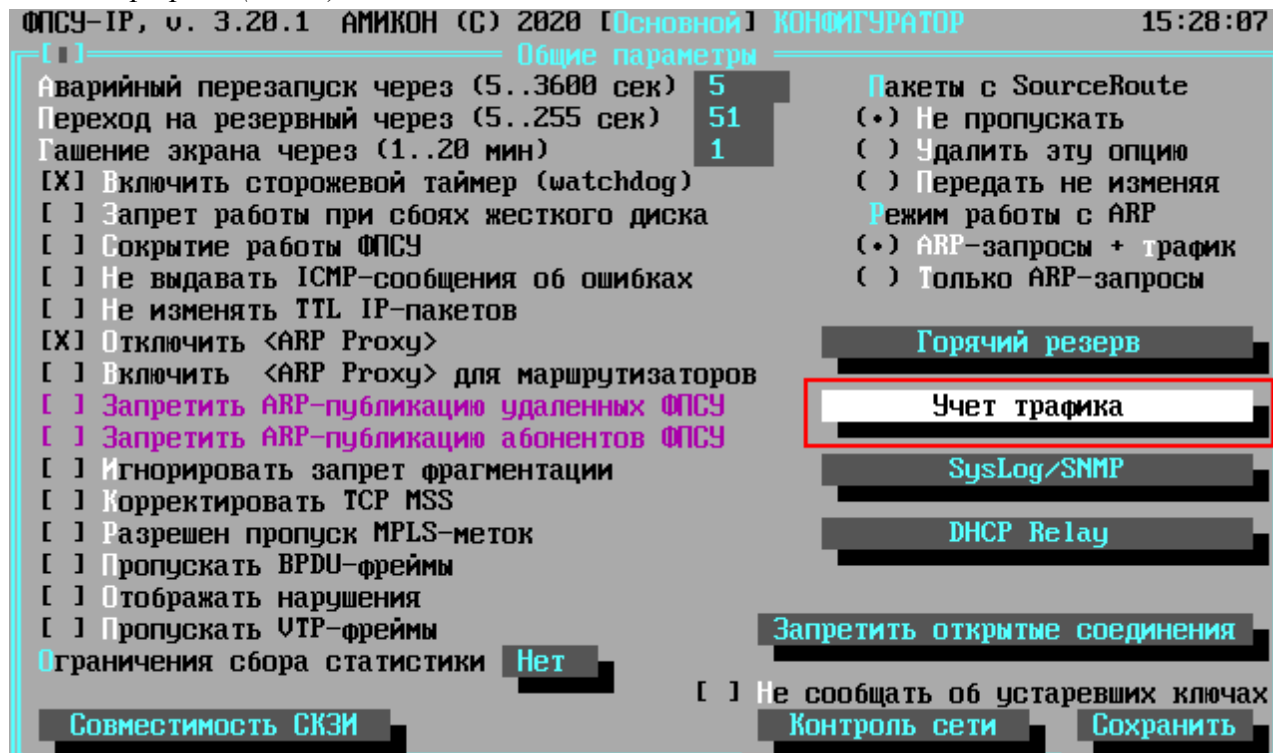


Рисунок 245 - Общие параметры, вызов окна настроек учета трафика IPFIX

По команде меню открывается окно со списком коллекторов IPFIX, по умолчанию список пустой.

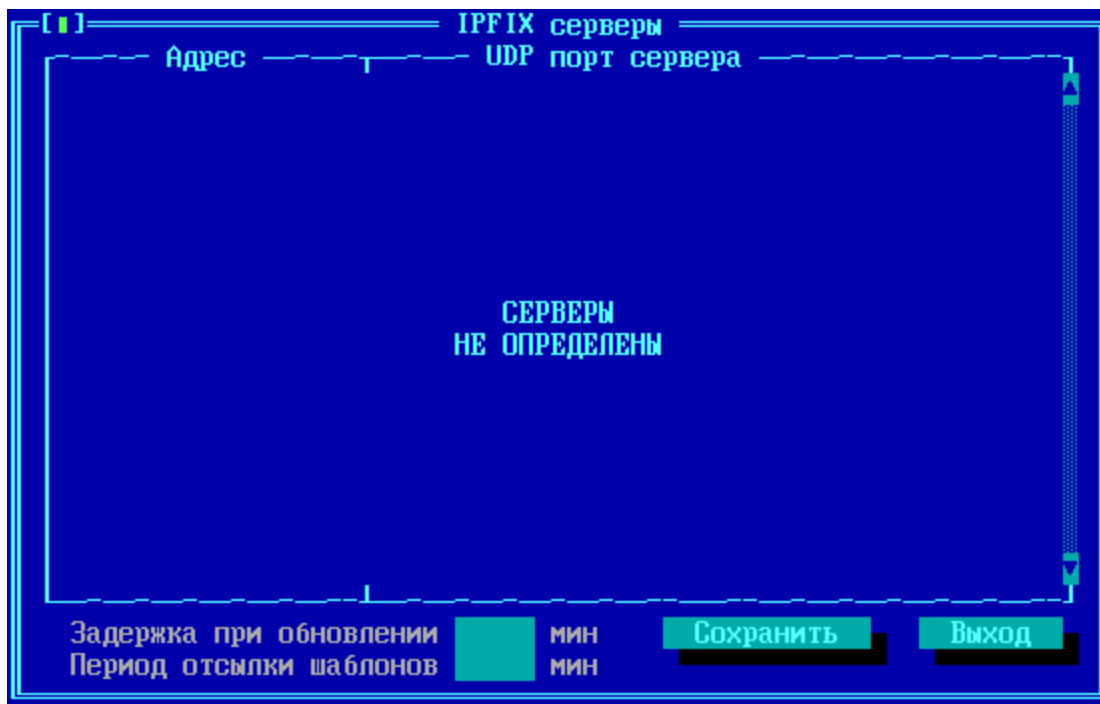


Рисунок 246 - Общие параметры, вызов окна настроек учета трафика IPFIX

Включение поддержки IPFIX может замедлять работу межсетевого экрана ФПСУ-IP.

Отправляемые данные распределяются по нескольким шаблонам в зависимости от типа трафика:

- Шаблон 260 - передача обычного трафика;
- Шаблон 258 - передача трафика с NAT-адреса;
- Шаблон 259 - отвергнутый (сброшенный) 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.

Отправка шаблонов о сброшенном трафике в версии 3.20.1 не поддерживается.

12. 3. Syslog-клиент на ФПСУ-IP

ФПСУ-IP поддерживает возможность отправки сообщений о происходящих на ФПСУ-IP событиях по протоколам SysLog и SNMP. Для это реализована подсистема, которая отслеживает происходящие на ФПСУ-IP события и отправляет их по протоколам SysLog и/или SNMP на внешний сервер.

Сообщения отправляются в кодировке OEM/DOS (866) по умолчанию.

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 "Общие параметры" конфигурации ФПСУ-IP при нажатии на кнопку "SysLog/SNMP".

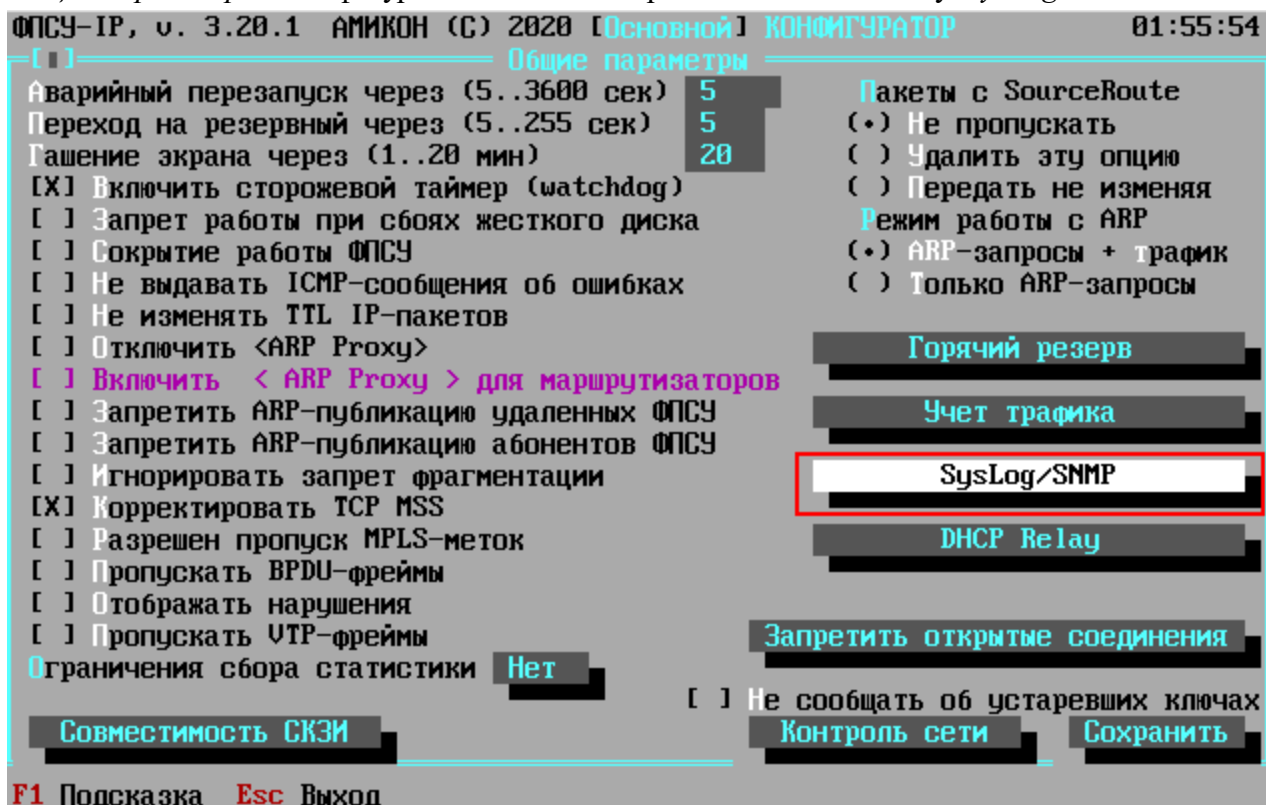


Рисунок 247 - Общие параметры, вызов окна настроек SysLog

12.3.1. Настройка SysLog событий ФПСУ-IP

После выполнения команды "SysLog/SNMP", из окна общих параметров, появится интерфейс управления SysLog подсистемой на ФПСУ-IP. В левой части появившегося окна расположен список событий, при наступлении которых следует выдать сообщение серверу.

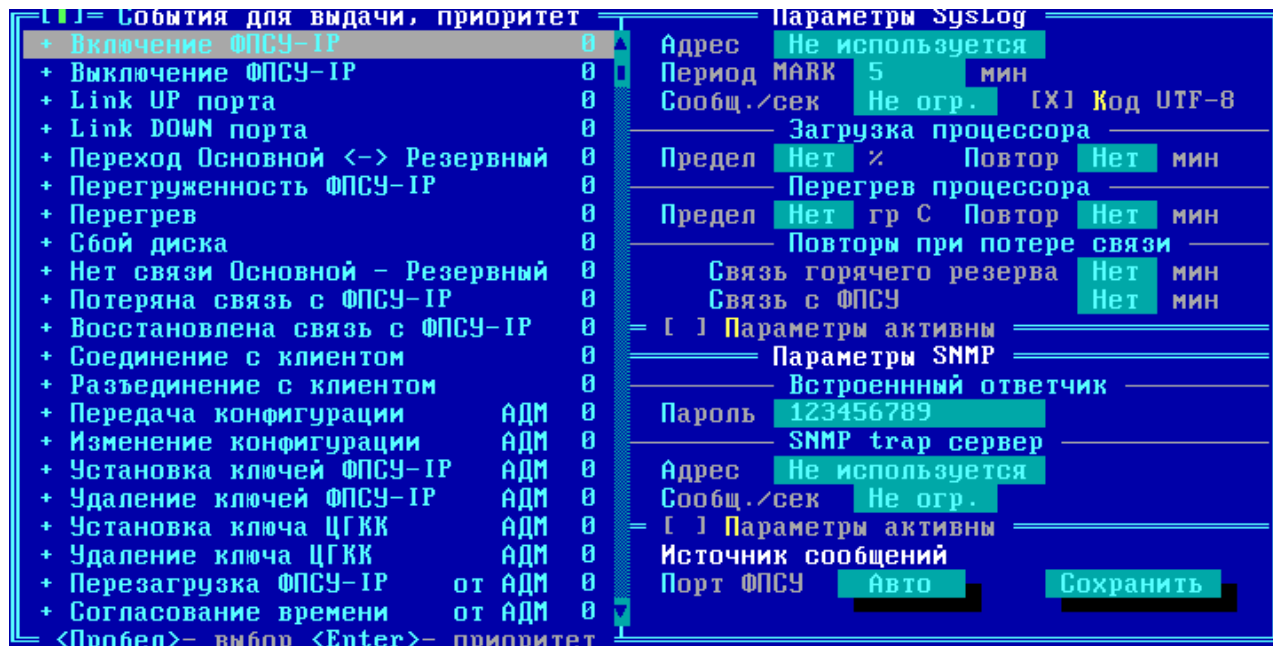


Рисунок 248 - Настройка параметров SysLog

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

Таблица 4. SysLog сообщения

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;
MARK сообщения	200007	Служебное периодическое оповещение ФПСУ-IP о работоспособности комплекса;

Название события	Код события в тексте SysLog сообщения	Причина
Link UP порта	500001	Включение сетевого адаптера в сеть передачи данных;
Link DOWN порта	500002	Прекращение работы сетевого адаптера с сетью передачи данных;
Переход Основной - Резервный	400001	Произошла передача управления партнёру по горячему резервированию;
Перегруженность ФПСУ	200005	Загрузка ЦПУ ФПСУ-IP достигла порогового значения, указанного в параметре "Загрузка процессора, Предел";
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, обычно при попытке записи статистической информации;
Нет связи Основной - Резервный	400002	Партнер по горячему резерву не ответил на запрос;
Потеряна связь с ФПСУ	200001	Произошло разъединение защищенного соединения (туннеля) с удаленным ФПСУ;
Восстановлена связь с ФПСУ	200002	Установлен туннель с удалённым ФПСУ;

Название события	Код события в тексте SysLog сообщения	Причина
Соединение с клиентом	300001	Установлено защищенное соединение (туннель) с комплексом ФПСУ-IP/Клиент;
Разъединение с клиентом	300002	Произошло разъединение защищенного соединения (туннеля) с комплексом ФПСУ-IP/Клиент;
Передача конфигурации АДМ	100001	Удаленный администратор ФПСУ-IP отправил запрос на получение конфигурации с ФПСУ-IP;
Изменение конфигурации АДМ	100003	Удаленный администратор ФПСУ-IP передал на ФПСУ-IP и активизировал изменённую конфигурацию;
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;

Название события	Код события в тексте SysLog сообщения	Причина
Перезагрузка ФПСУ-IP АДМ	100008	Удаленным администратором произведена перезагрузка Комплекса ФПСУ;
Согласование времени с АДМ	100009	Время на ФПСУ-IP было синхронизировано со временем на АРМ УА ФПСУ-IP;
Текущая температура	500005	Периодическое отправление сообщения с текущим уровнем нагрева ЦПУ ФПСУ-IP, периодичность отправки указывается в параметре "Перегрев процессора, Повтор";
Нет канала Основной - Резервный	400003	Отсутствует физический канал связи между партнерами по горячему резерву;
Окончание поддержки	500006	Заканчивается срок поддержки комплекса;
Блокировка ресурсов	700007	Блокировка абонента межсетевым экраном;
	700008	Разблокировка абонента межсетевым экраном.

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 5. 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:

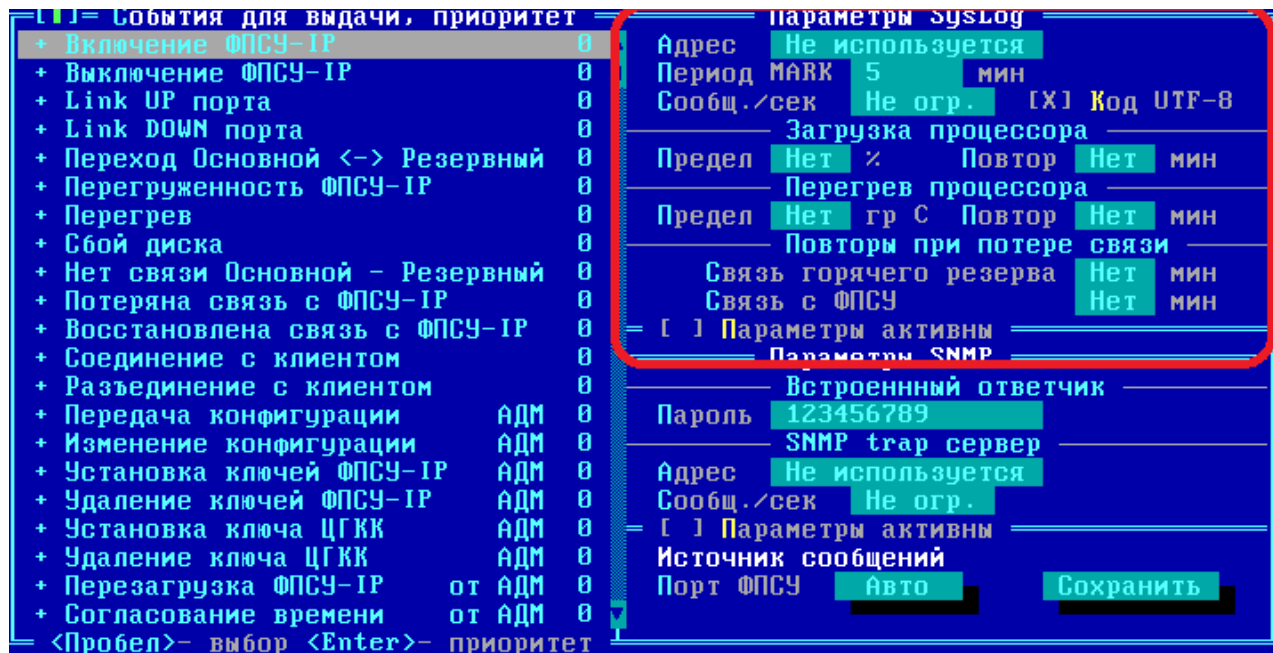


Рисунок 249 - Параметры SysLog

- *Адрес* — IP-адрес SysLog сервера, на него будут отправляться SysLog-сообщения;
- *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* — переключатель, указывающий изменение кодировки отправляемых сообщений на UTF-8 (по умолчанию выставлена 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;

- *Источник сообщений* — 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.

- *Параметры активны* — переключатель, включающий/выключающий работу с указанным в поле "*Адрес*" SysLog сервером. При выключенном переключателе 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 6. Формат SysLog сообщения

Службное число	Дата отправления сообщения с ФПСУ-IP	Серийный номер ФПСУ	ФПСУ	Код события	Имя события	Детали события	Номер ФПСУ в системе "горячего" резерва
Службное число	Дата 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:

Включение ФПСУ – дополнительные поля отсутствуют;

Выключение ФПСУ – дополнительные поля отсутствуют;

Link UP порта – логический номер LAN-порта, а также его IP-адрес;

Link DOWN порта – логический номер LAN-порта, а также его IP-адрес;

Переход Основной - Резервный – режим функционирования ФПСУ-IP горячего резерва, на который произошло переключение (основной или резервный);

Перегруженность ФПСУ – загрузка ЦПУ, в процентах;

Перегрев – температура ЦПУ по шкале Цельсия;

Сбой диска – дополнительные поля отсутствуют;

Нет связи Основной - Резервный – режим функционирования ФПСУ-IP горячего резерва, с которым не удаётся установить связь (основной или резервный);

Потеряна связь с ФПСУ – серийный номер и IP-адрес ФПСУ-IP, с которым потеряно защищенное соединение;

Восстановлена связь с ФПСУ – серийный номер и IP-адрес ФПСУ-IP, с которым восстановлено защищенное соединение;

Соединение с клиентом – IP-адрес и номер порта ФПСУ-IP, к которому произошло подключение, имя подключившегося Клиента, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, IP-адрес подключившегося Клиента;

Разъединение с клиентом – IP-адрес и номер порта ФПСУ-IP, от которого произошло отключение, имя разъединившегося Клиента, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, IP-адрес разъединившегося Клиента;

Передача конфигурации АДМ – служебный текст "Администратор", имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора;

Изменение конфигурации АДМ – служебный текст "Администратор", имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора;

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;

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;

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 установленный Криптосети Клиентов;

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 "Крипtosеть номер, номер удалённой Крипtosети Клиентов;

Перезагрузка ФПСУ АДМ – служебный текст "Администратор", имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора;

Согласование времени с АДМ – служебный текст "Администратор", имя удаленного администратора, номер порта ФПСУ-IP, к которому подключился удаленный администратор, IP адрес удалённого администратора;

Период <MARK> – дополнительные поля отсутствуют.

12. 4. SNMP-клиент на ФПСУ-IP

Доступ к окну настроек параметров SNMP-клиента на ФПСУ-IP предоставляется из меню "Общие параметры" конфигурации ФПСУ-IP при нажатии на кнопку "SysLog/SNMP".

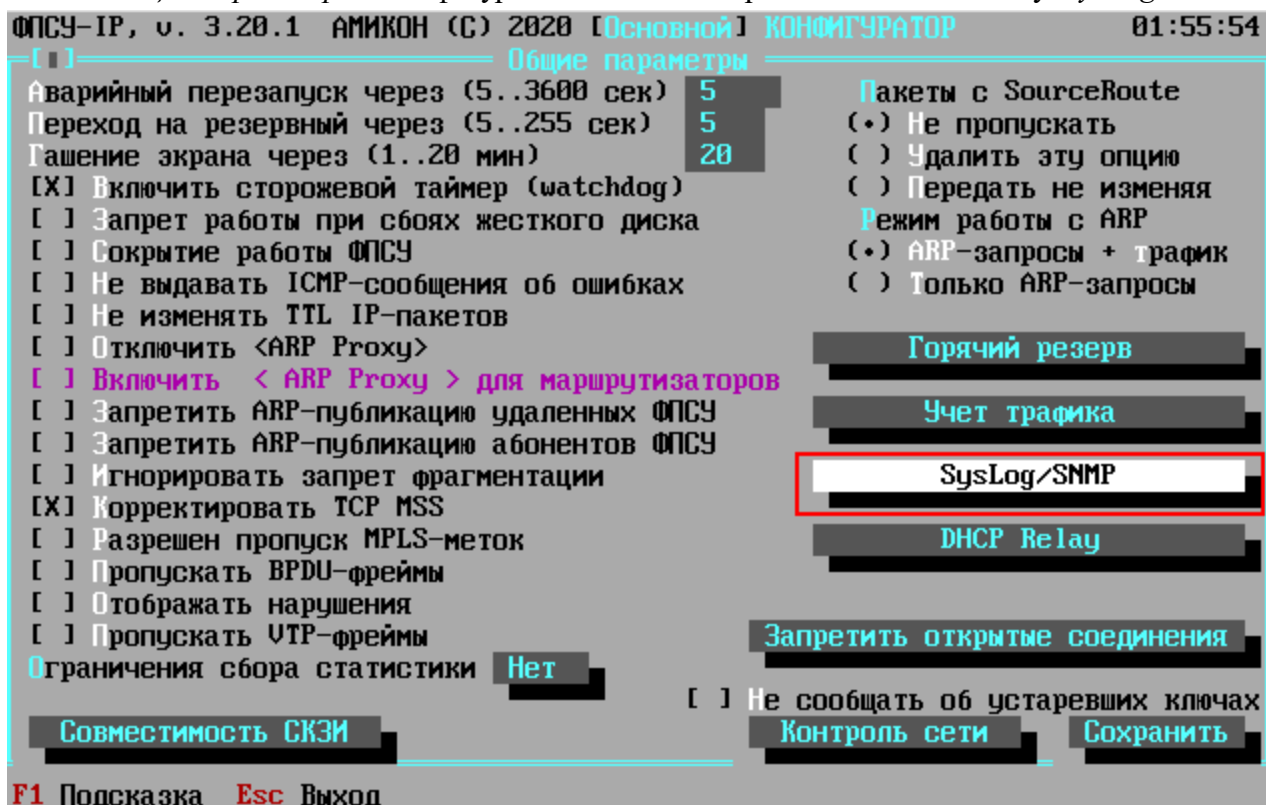


Рисунок 250 - Общие параметры, переход к настройкам SNMP

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.

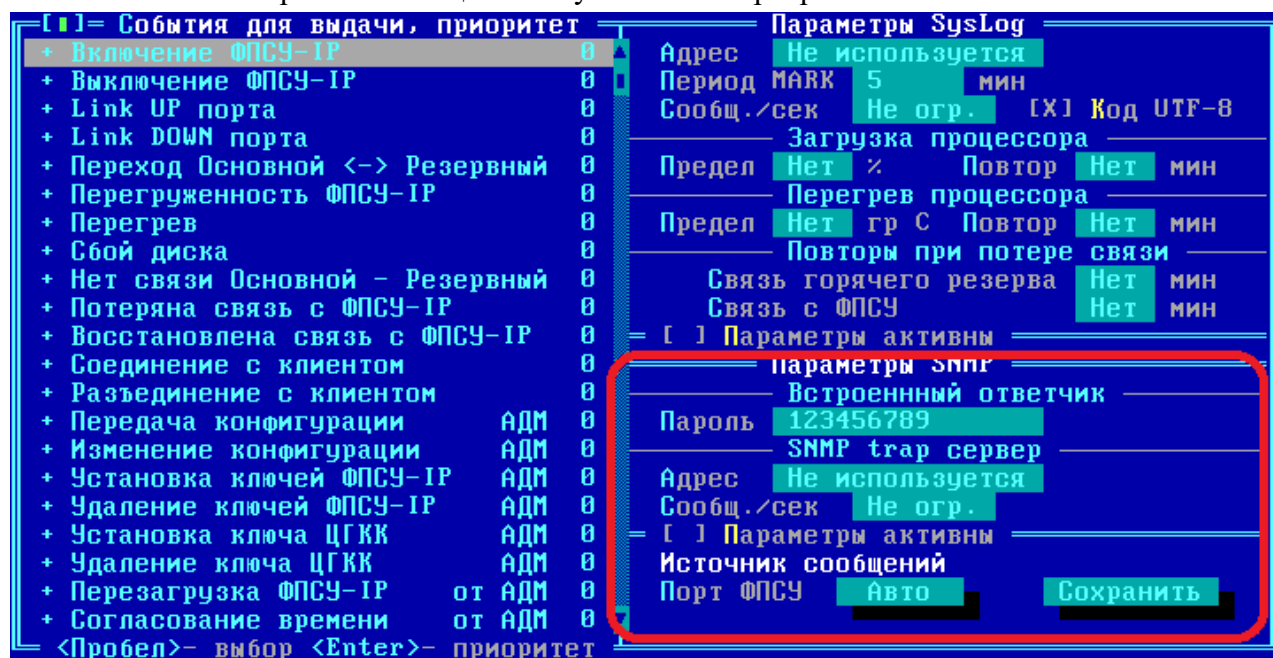


Рисунок 251 - Интерфейс настройки SNMP

Настраиваемые параметры SNMP-клиента:

Встроенный 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 trap server, Адрес — IP-адрес SNMP-менеджера, на него будут отправляться SNMP TRAP сообщения;

SNMP trap server, 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;

Источники сообщений — 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.

Параметры активны — переключатель, включающий/выключающий работу с указанным в поле "Адрес" SNMP-менеджером. При выключенном переключателе 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:

Advanced Properties of SNMP Agent

Address: 192.168.0.222

Port: 161

Read Community:

Write Community:

SNMP Version: 3

SNMPv3

USM User: authOnlyUser

Security Level: auth, no priv

Auth Algorithm: MD5

Auth Password: *****

Privacy Algorithm: DES

Privacy Password:

Context Name:

Engine ID: 0x 80 00 91 81 80 00 8C B1 4F 32 80 5D

Localized Auth Key: 0x E8 E4 E7 E0 25 40 4F 24 3B B3 5B 4F EC 53 A4 59

Localized Priv Key:

Рисунок 252 - Настройки SNMP-агента ФПСУ-IP в iReasoning MIB Browser

12. 5. 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 две настройки:

- завести в общих параметрах 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.

12.5.1. Создание списка DHCP-серверов

Для создания и/или редактирования списка DHCP-серверов, которым ретранслируются DHCP-запросы, следует зайти в конфигурацию общих параметров ФПСУ-IP и нажать кнопку "DHCP-Relay":

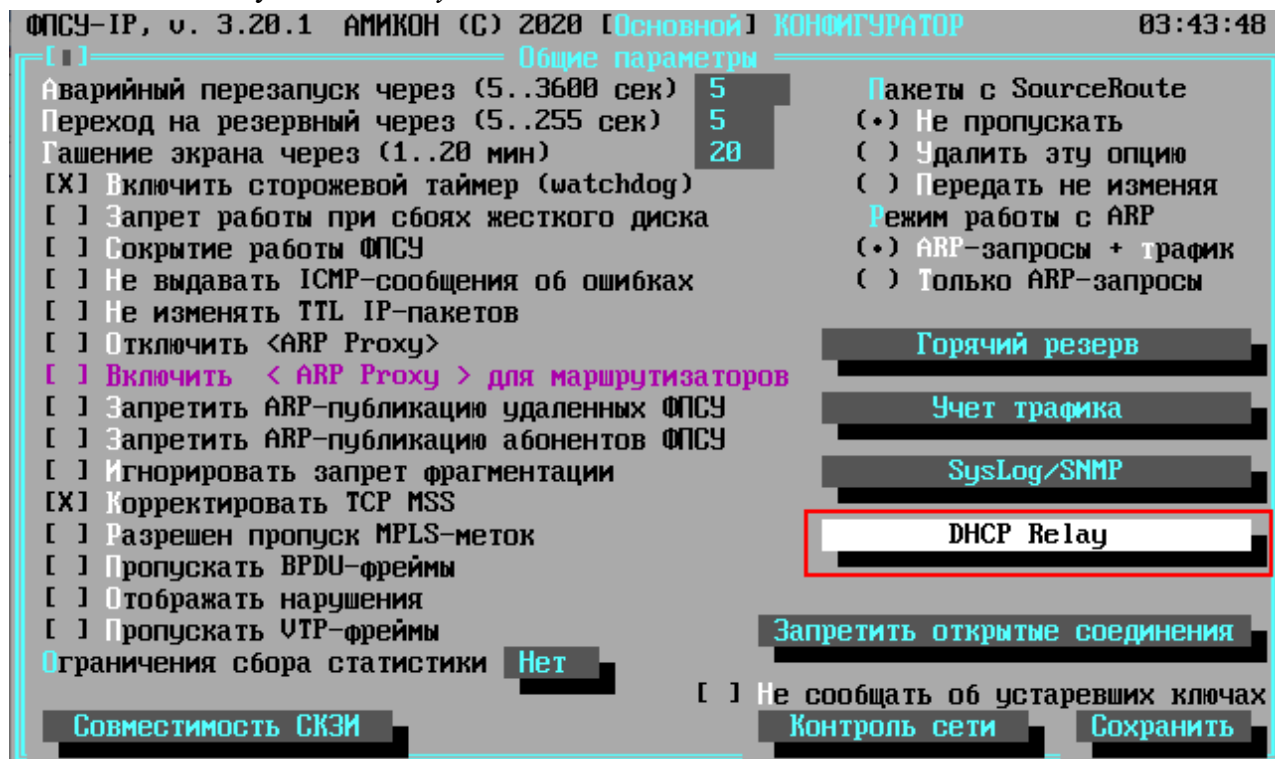


Рисунок 253 - Общие параметры ФПСУ-IP

Список DHCP-серверов 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, должны быть предварительно добавлены в этот список.



Рисунок 254 - Список DHCP-серверов

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

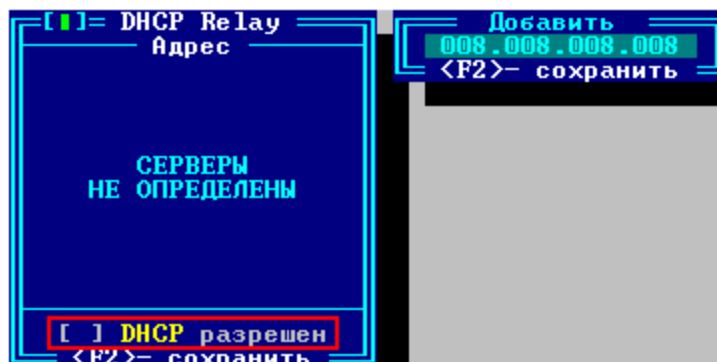


Рисунок 255 - Добавление DHCP-сервера

IP-адрес сервера 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 DHCP-серверов, установите курсор на строке и нажмите клавишу . Редактирование существующей записи выполняется по нажатию клавиши <Enter>.

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

После сохранения, IP-адреса из списка можно использовать в конфигурации портов ФПСУ-IP в качестве получателя ретранслируемых DHCP-запросов (см. пункт ["Настройка DHCP-Relay на портах ФПСУ"](#)).

12. 5. 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. ["Создание списка DHCP-серверов"](#)). Таким образом, администратор определяет, куда ретранслировать пришедший DHCP-запрос, в зависимости от того, на какой порт (и в какой VLAN) он пришёл.

Обратите внимание, что 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.

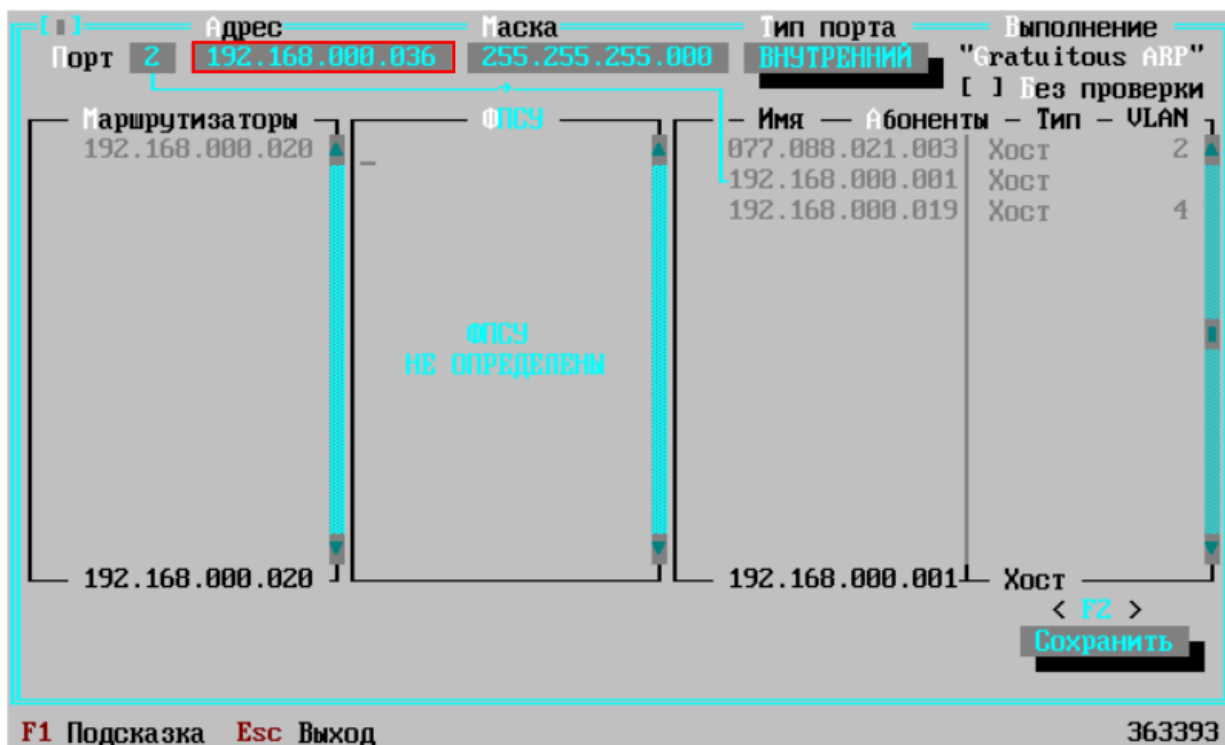


Рисунок 256 - Параметры порта ФПСУ-IP

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.

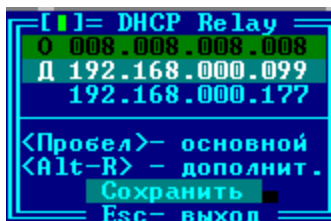


Рисунок 257 - Настройка DHCP на порту без VLAN

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.

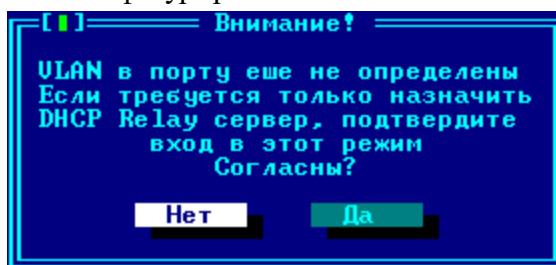


Рисунок 258 - Служебное оповещение

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.

Адрес	Маска	VLAN	Основной DHCP	Дополнительный
077.108.111.100	255.255.255.000		Не установлен	Не установлен
192.168.101.123	255.255.255.000	2	008.008.008.008	192.168.000.123
192.168.000.122	255.255.255.000	3	Не установлен	Не установлен
010.010.000.010	255.255.000.000	19	Не установлен	Не установлен

Рисунок 259 - Настройка DHCP на порту с определенными VLAN

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

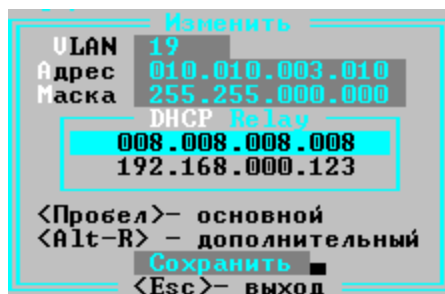


Рисунок 260 - Настройка DHCP-сервера для отдельного VLAN порта

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. Так же, отменить выбор основного DHCP-сервера можно только тогда, когда не выбран или предварительно отменен выбор дополнительного сервера.

12. 6. 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:

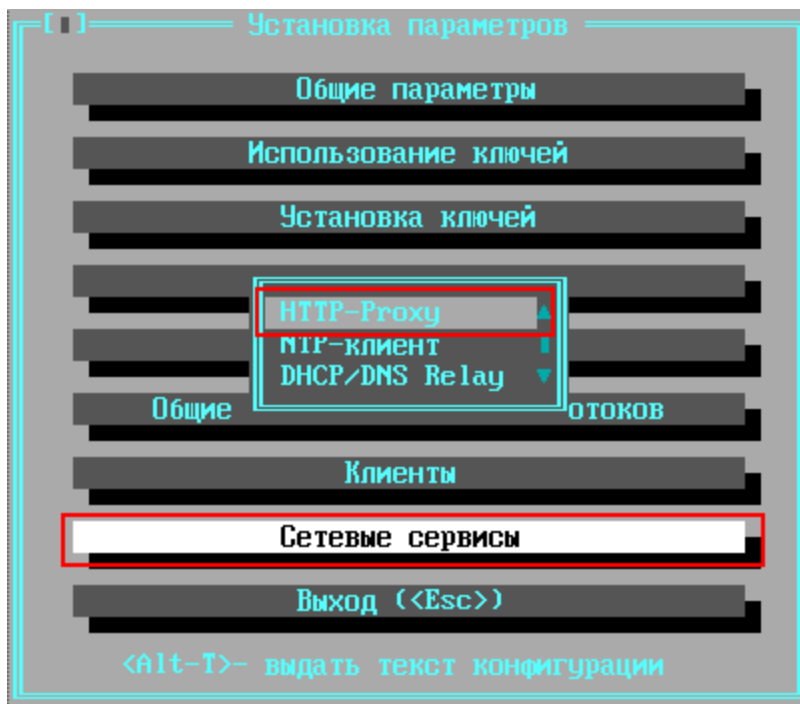


Рисунок 261 - Команда перехода в конфигурацию проху на ФПСУ-IP

ВНИМАНИЕ! Подсистема http-прокси работает только при 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:

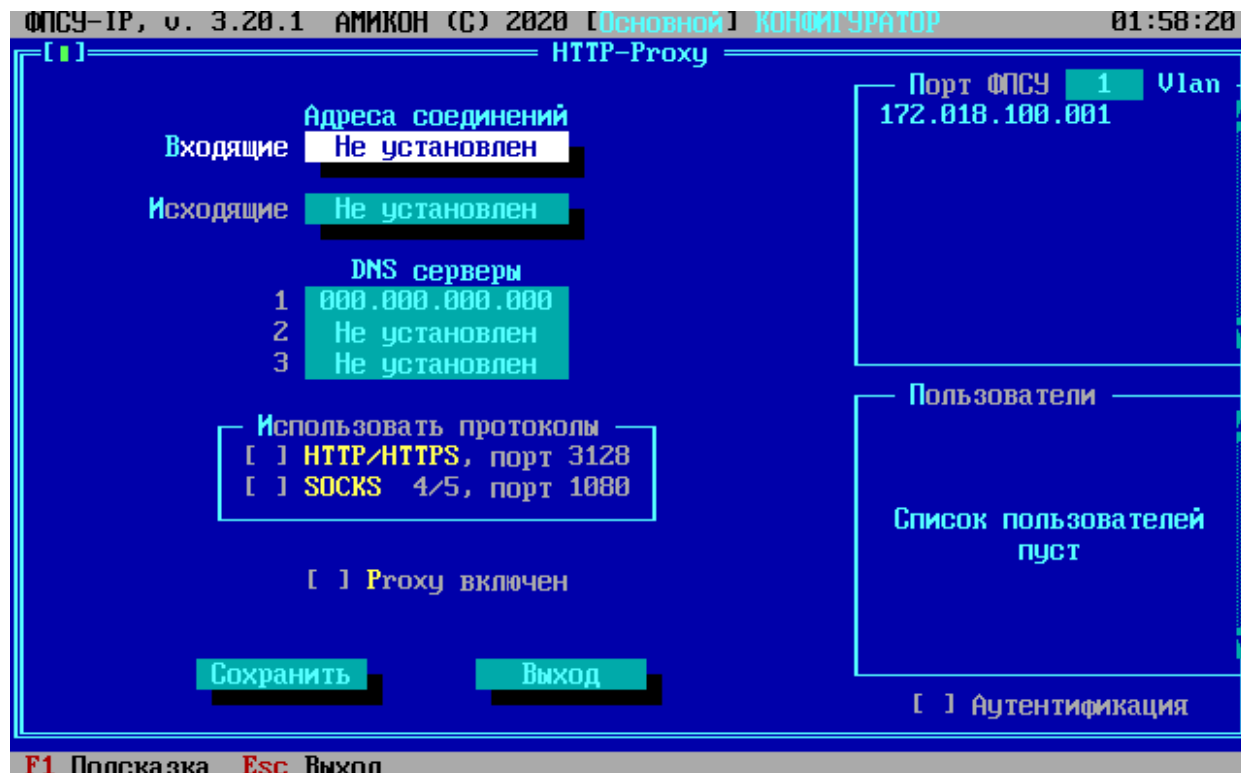


Рисунок 262 - Окно настроек HTTP-proxy

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.

Прoxy включен – переключатель, запускающий прокси на ФПСУ-IP с указанными настройками. Если метка переключателя снята, прокси не будет запущен.

Пользователи, Аутентификация - блок настроек, отвечающий за режим доступа пользователей к проху 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 "[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. 6. 1. Авторизация на http-proxy

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

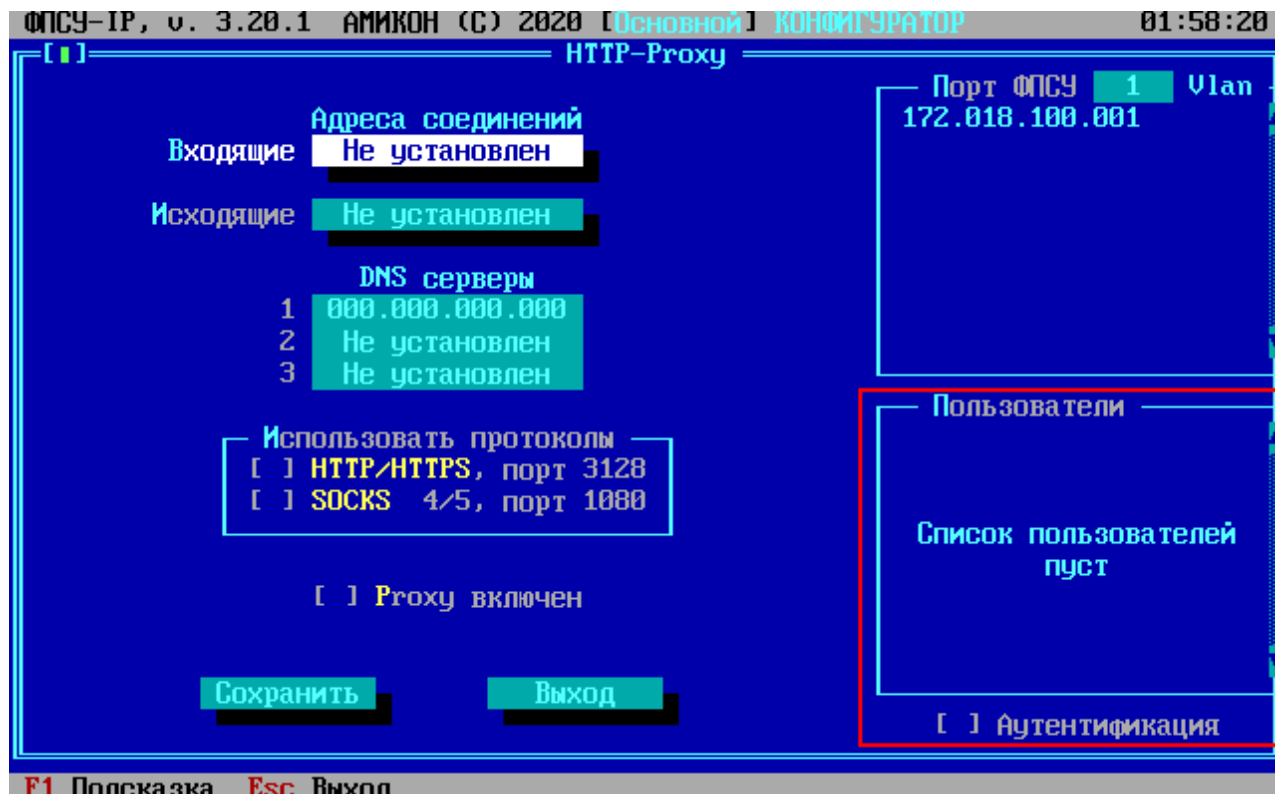


Рисунок 263 - Блок настройки пользователей проxy ФПСУ-IP

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:

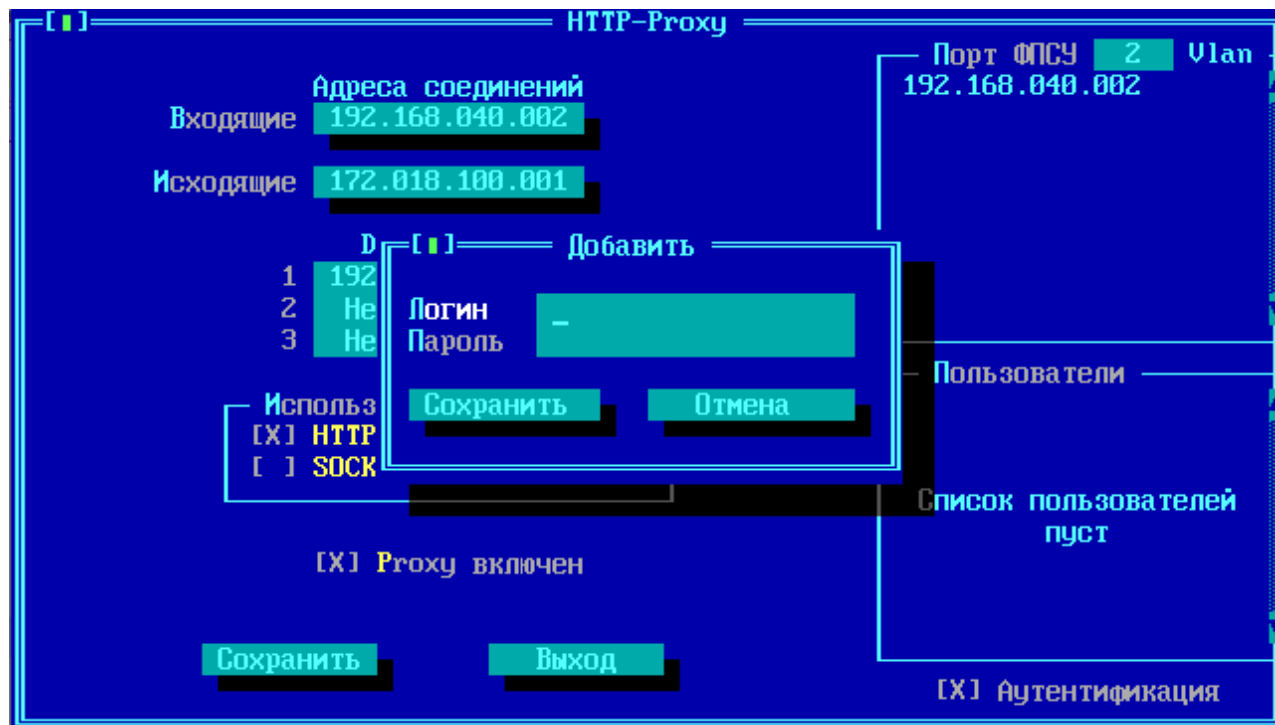


Рисунок 264 - Добавление учетной записи нового пользователя прокси ФПСУ-IP

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:

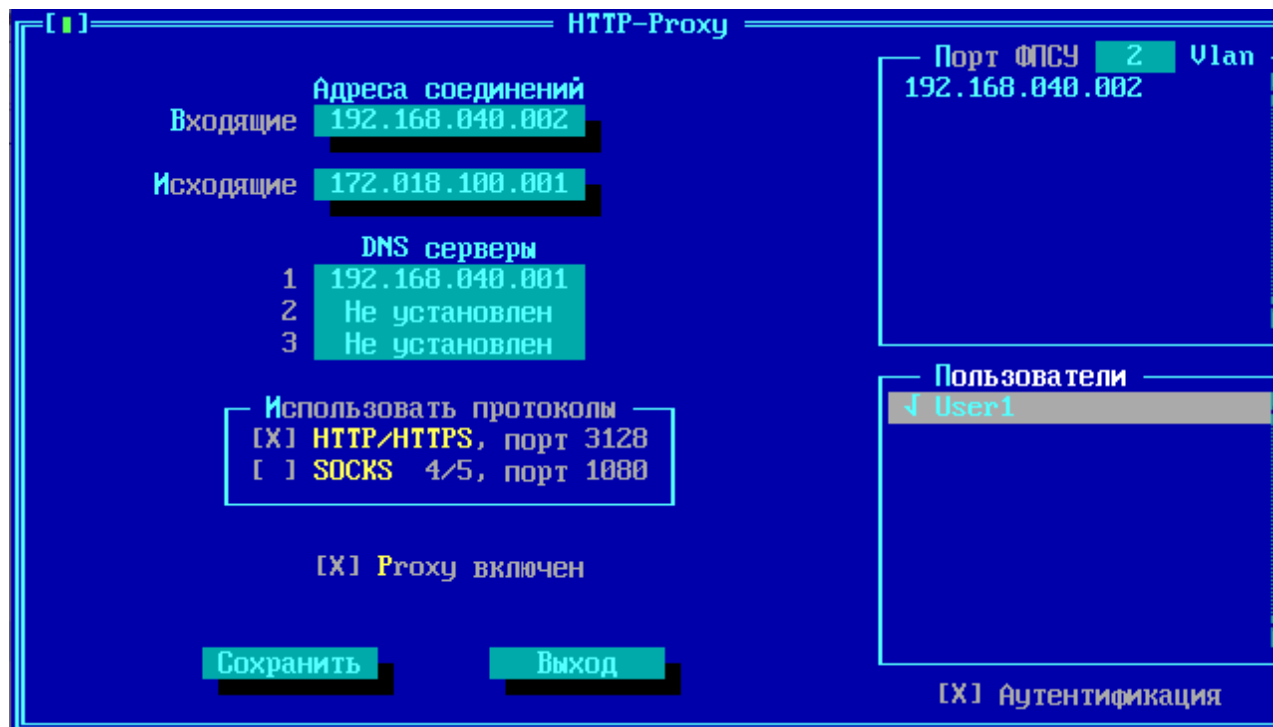


Рисунок 265 - Новый пользователь прокси ФПСУ-IP добавлен

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 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. 7. 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, указанного администратором ФПСУ-IP, IP-адреса СОВ. 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 межсетевое экрана ФПСУ-IP на заданное администратором ФПСУ-IP время.

Интерфейс настройки взаимодействия с СОВ вызывается по нажатию кнопки <СОВ> вкладки *Flood-атака* параметров трафика межсетевое экрана. Переключатель "Flood control" должен быть задействован для работы с СОВ.

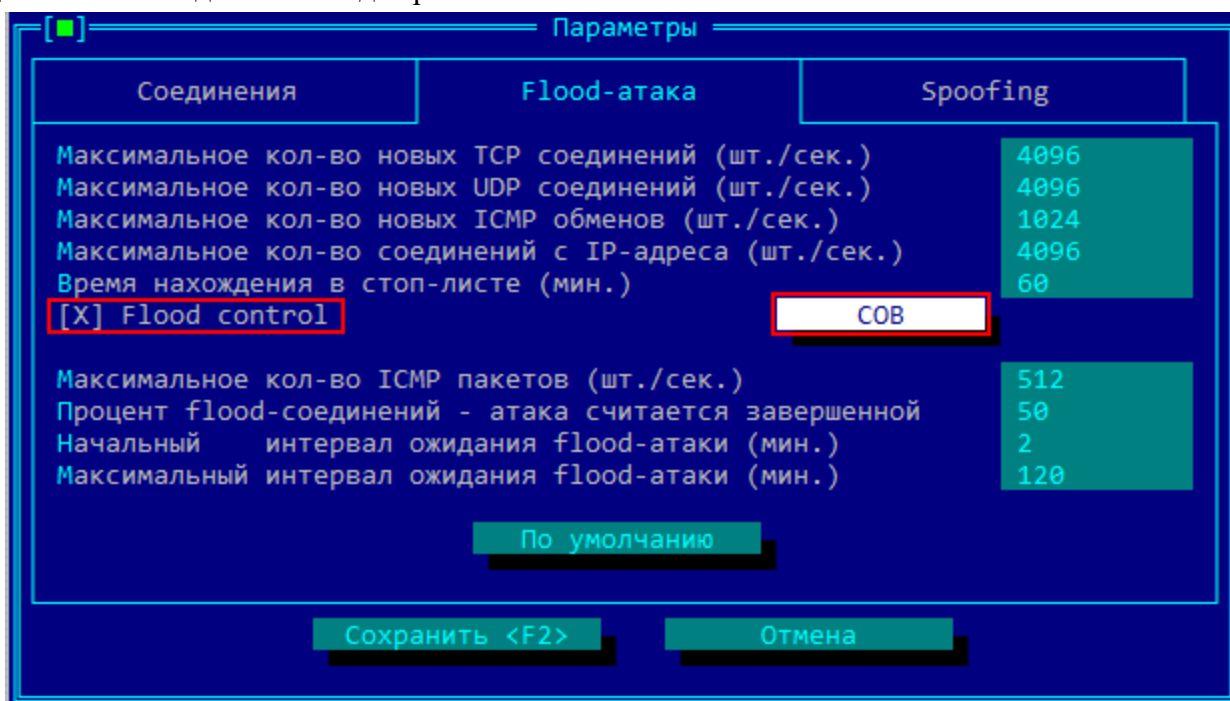


Рисунок 266 - Вызов интерфейса настройки взаимодействия с СОВ

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

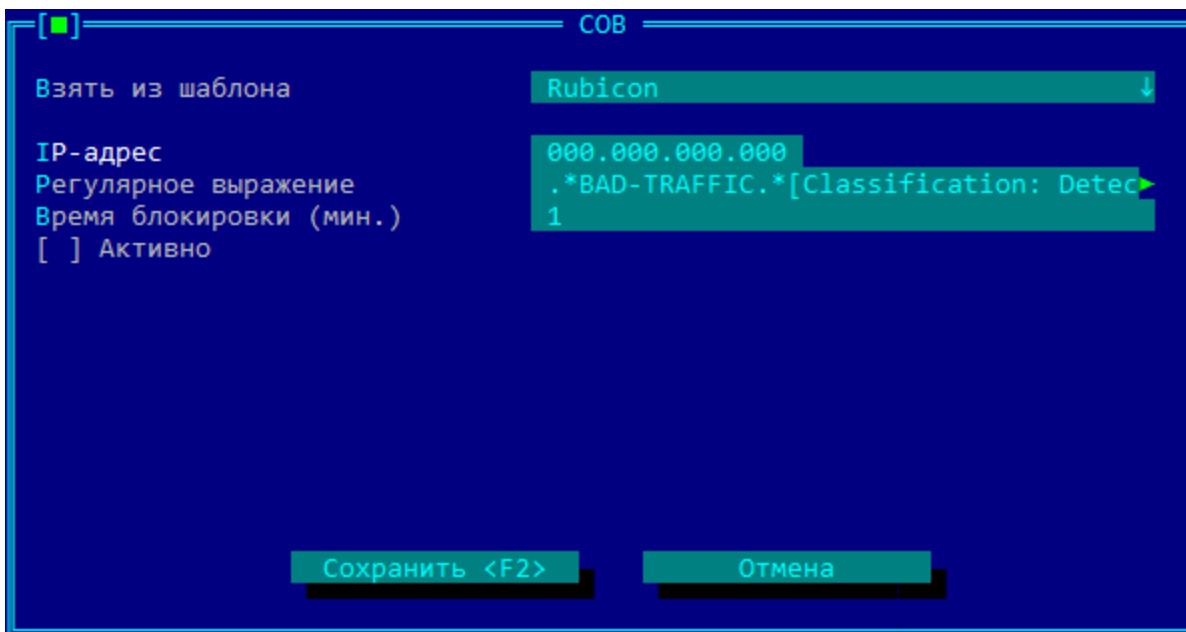


Рисунок 267 - Параметры взаимодействия с СОВ

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, наличие которого будет искаться 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, на которое будет помещен в стоп-лист IP-адрес, вызвавший событие СОВ. Устанавливается в пределах от 1 до 65535.

Активно – обязательная настройка; переключатель, указывающий на включенный режим взаимодействия с СОВ. Если переключатель 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).

Время	Тип	19(20)
06.11.19 12:40:02	Журнал ARP: Host зарегистрирован (найден при поиске)	
06.11.19 12:40:02	Журнал ARP: Host зарегистрирован (найден при поиске)	
06.11.19 12:40:02	Журнал ARP: Host зарегистрирован (найден при поиске)	
06.11.19 12:40:02	Журнал ARP: Host зарегистрирован (найден при поиске)	
06.11.19 12:40:02	ОТКАЗ 192.168.100.025 → 192.168.016.025	
06.11.19 12:40:04	ОТКАЗ 192.168.100.025 ← 192.168.016.025	
06.11.19 12:40:18	Обмен 192.168.100.024 → 192.168.016.024	
06.11.19 12:40:26	Журнал ARP: Host зарегистрирован (найден при поиске)	
06.11.19 12:40:30	Статистика IPS В черном списке до 06.11.2019 12:41:28	
06.11.19 12:40:30	Обмен 192.168.016.055 ← 192.168.016.020	
06.11.19 12:40:32	Журнал ARP: Host зарегистрирован (найден при поиске)	
06.11.19 12:40:40	ОТКАЗ 192.168.100.024 → 192.168.016.024	
06.11.19 12:40:52	ОТКАЗ 192.168.100.026 → 192.168.016.026	
06.11.19 12:40:54	ОТКАЗ 192.168.100.026 ← 192.168.016.026	
06.11.19 12:41:34	Статистика IPS Исключен из списка блокировки	
06.11.19 12:42:08	Конец работы: По запросу оператора	

Alt-W Вывод на носитель

Рисунок 268 - 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 (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. 8. NTP-клиент ФПСУ-IP

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

ВНИМАНИЕ! НЕ СЛЕДУЕТ одновременно задействовать NTP-клиента и синхронизацию времени на ФПСУ с удаленным администратором (см. пункт ["Регистрация](#)

[удаленного администратора на ФПСУ-IP](#)!)

Настройка синхронизации времени выполняется из пункта "Сетевые сервисы - NTP-клиент" конфигурации ФПСУ:

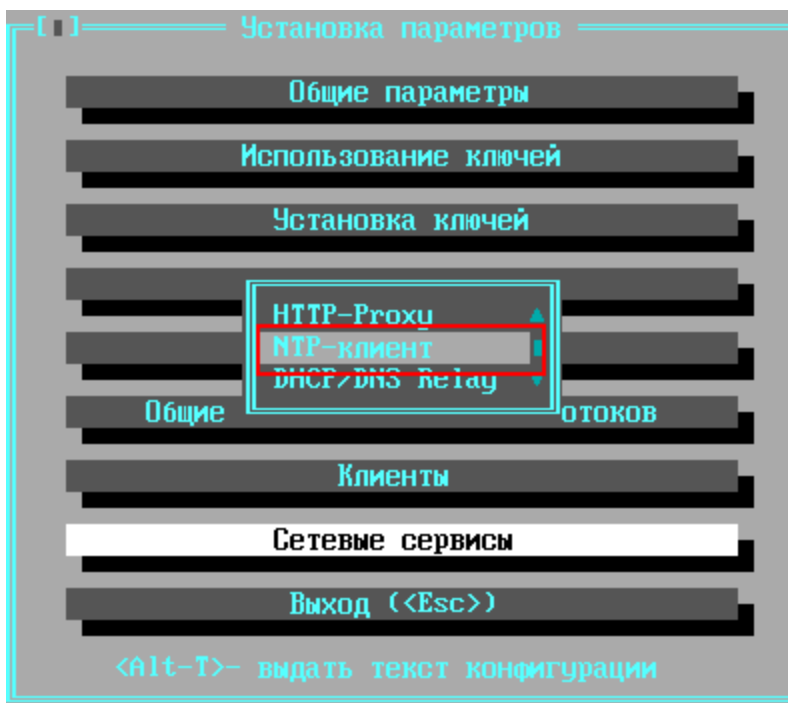


Рисунок 269 - Меню конфигурации ФПСУ

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

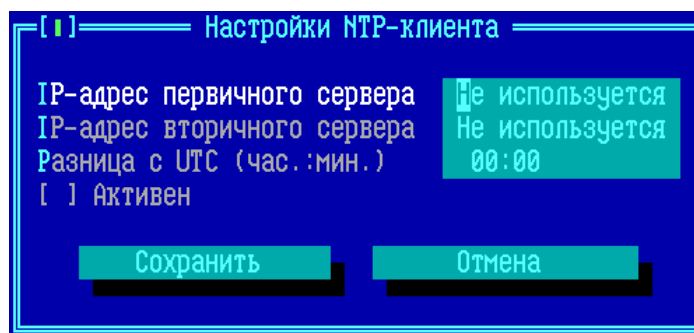


Рисунок 270 - Настройки NTP-клиента по умолчанию

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

- указать адрес первичного NTP-сервера;
- установить разницу временного пояса, в котором работает ФПСУ, с UTC временем;

- задействовать переключатель "Активен";
- нажать кнопку "Сохранить".

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

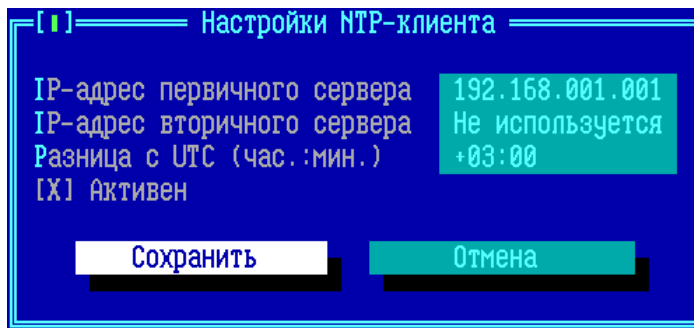


Рисунок 271 - Пример настроек NTP-клиента

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

12. 9. Служебные протоколы и порты на ФПСУ-IP

Таблица. Служебные протоколы и порты на ФПСУ-IP

Описание	Номер протокола или порта
Протокол VPN-туннеля между ФПСУ-IP сетевого уровня, основной поток	IP №53
Порт VPN-туннеля между ФПСУ-IP транспортного уровня, основной поток	UDP:30004
Протокол удаленного администрирования сетевого уровня	IP №56
Порт и протокол удаленного администрирования транспортного уровня	UDP:30003

Описание	Номер протокола или порта
Порт и транспортный протокол VPN-туннеля ФПСУ-IP/Клиента	UDP:87
Порт и транспортный протокол отправляемых Syslog-сообщений	UDP:514
Порт и транспортный протокол для ответчика SNMP на ФПСУ-IP	UDP:161
Порт и транспортный протокол для SNMP trap на ФПСУ-IP	UDP:162
Порт и транспортный протокол NTP-клиента ФПСУ-IP	UDP:123
Протоколы VPN-туннеля между ФПСУ-IP сетевого уровня, дополнительные потоки	IP №№110-226
Порты VPN-туннеля между ФПСУ-IP транспортного уровня, дополнительные потоки	UDP:№№ 55 000 - 55 126
Порты и транспортные протоколы VPN-туннеля между ФПСУ-IP для динамических ФПСУ-IP	UDP:№№ 40 000 - 50 000
Порты и транспортные протоколы VPN-туннеля между ФПСУ-IP для автораспределения 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. Так же статистика может быть отправлена удаленному администратору по запросу.

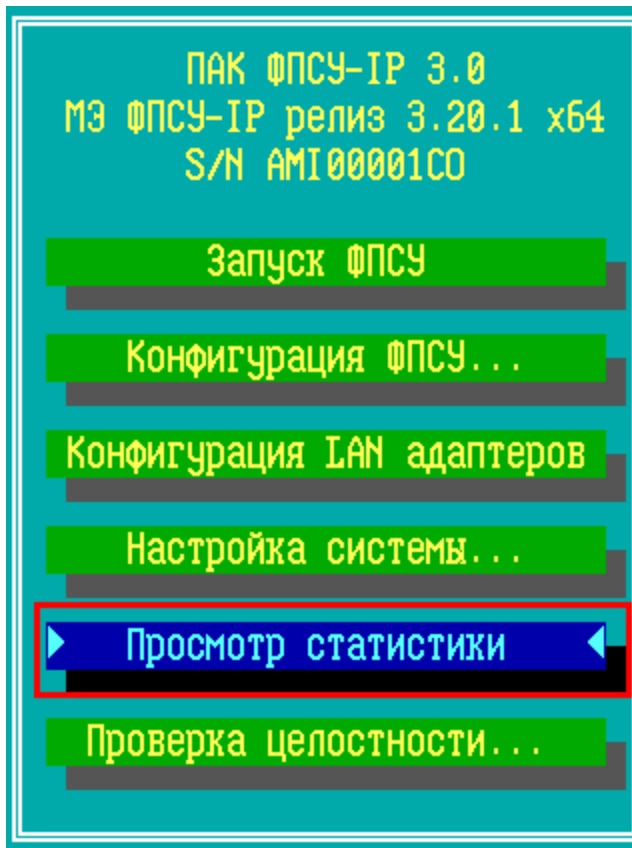


Рисунок 272 - Главное меню ФПСУ-IP

13. 1. Просмотр статистики

Команда "Просмотр статистики" главного меню ФПСУ-IP доступна администраторам класса "Инженер" и выше.

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

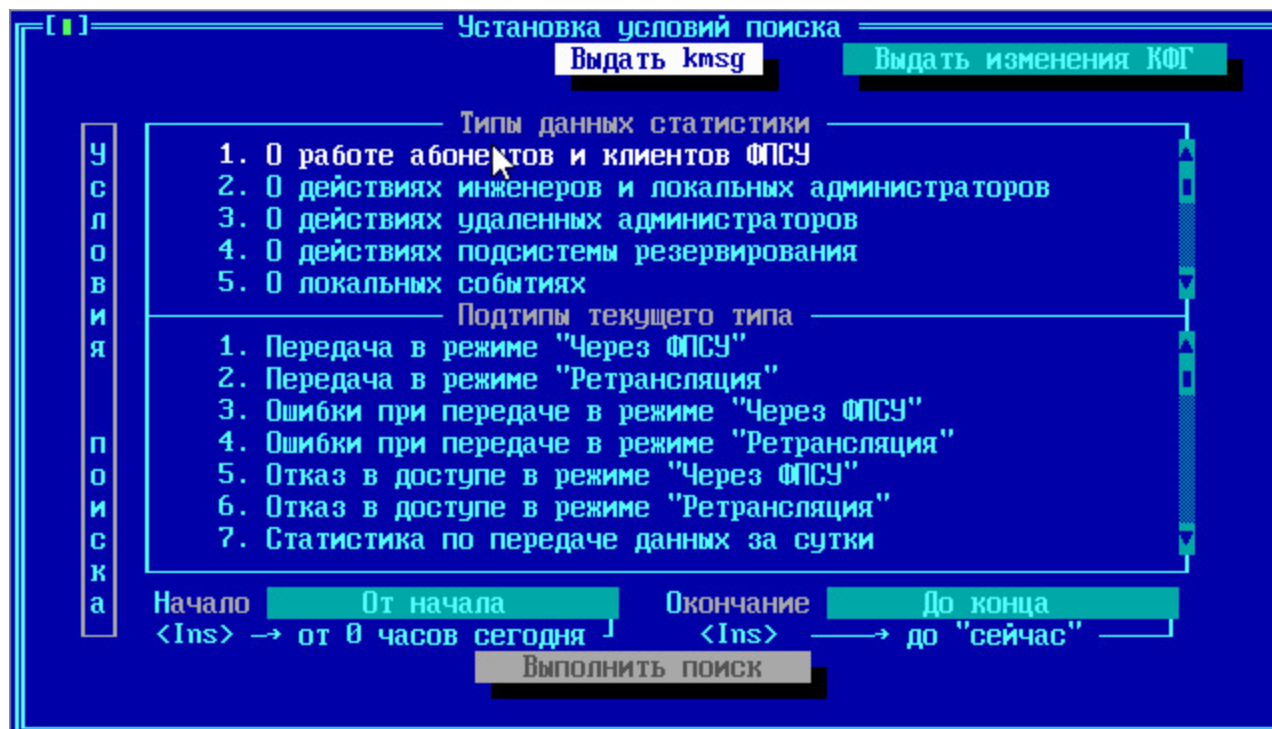


Рисунок 273 - Окно создания запроса на получение статистики

Для получения необходимых данных сначала отметьте нужный тип, для чего выделите соответствующую строку и нажмите *<Пробел>*. При этом строка отметится слева знаком "v", а в окне подтипов появится относящийся к данному типу список. Переход к подтипам осуществляется по нажатию *<Tab>* или *<>*. Подтипы отмечаются так же, как и типы.

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:

Время		Статистика		Тип		15(47)	
10.10.19	08:17:54	■	ЗАПУСК МАШИНЫ				
10.10.19	08:17:54		Контроль целостности файлов				
10.10.19	08:28:56		Идентификация с помощью ТМ				
10.10.19	08:29:06		Начало работы				
10.10.19	08:30:08		Самотестирование ФПСУ: ПРОЙДЕНО УСПЕШНО				
10.10.19	08:30:38		Конец работы: По запросу оператора				
10.10.19	08:36:32		Идентификация с помощью ТМ				
10.10.19	08:36:56		Контроль целостности файлов				
10.10.19	08:37:08		Идентификация с помощью ТМ				
10.10.19	08:37:28		Изменены общие параметры конфигурации				
10.10.19	09:19:58	■	ЗАПУСК МАШИНЫ				
10.10.19	09:19:58		Контроль целостности файлов				
10.10.19	09:19:58		Идентификация с помощью ТМ				
10.10.19	09:20:14		Начало работы				
10.10.19	09:27:26		Идентификация с помощью ТМ				
10.10.19	09:27:38		Конец работы: По запросу оператора				
Доступ разрешен: Завершение работы Требовались права: Оператора Предъявлена ТМ: АДМИНИСТРАТОРА (основная)							
Alt-W Вывод на носитель							

Рисунок 274 - Результат запроса статистики

Обратите внимание, что поиск будет выполняться лишь в том случае, если отмечен хотя бы один тип 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 $\langle Alt+W \rangle$. 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 журнала изменений конфигурации межсетевое экрана

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

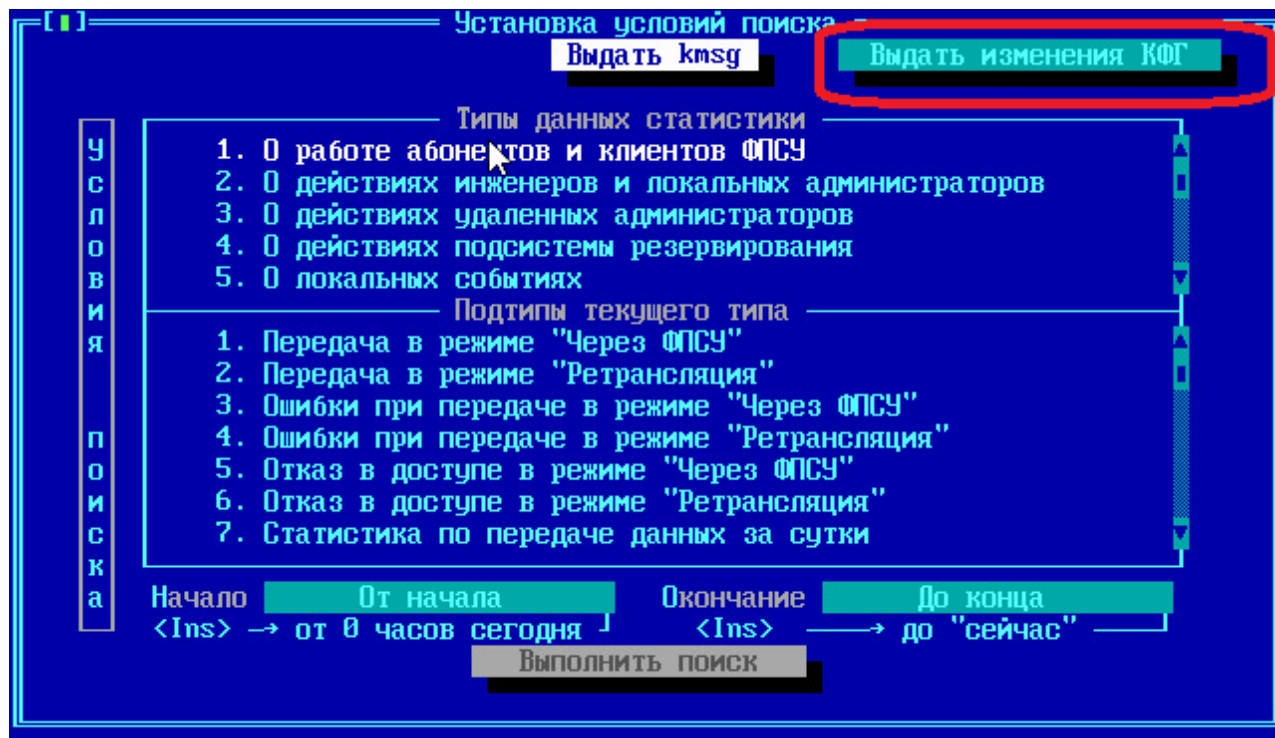


Рисунок 275 - Команда выдачи журнала изменений конфигурации межсетевого экрана

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

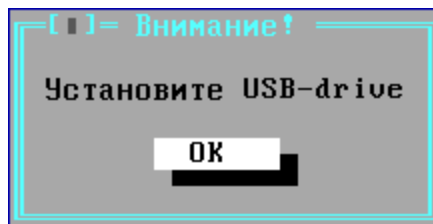


Рисунок 276 - Предложение подключить внешний носитель

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.

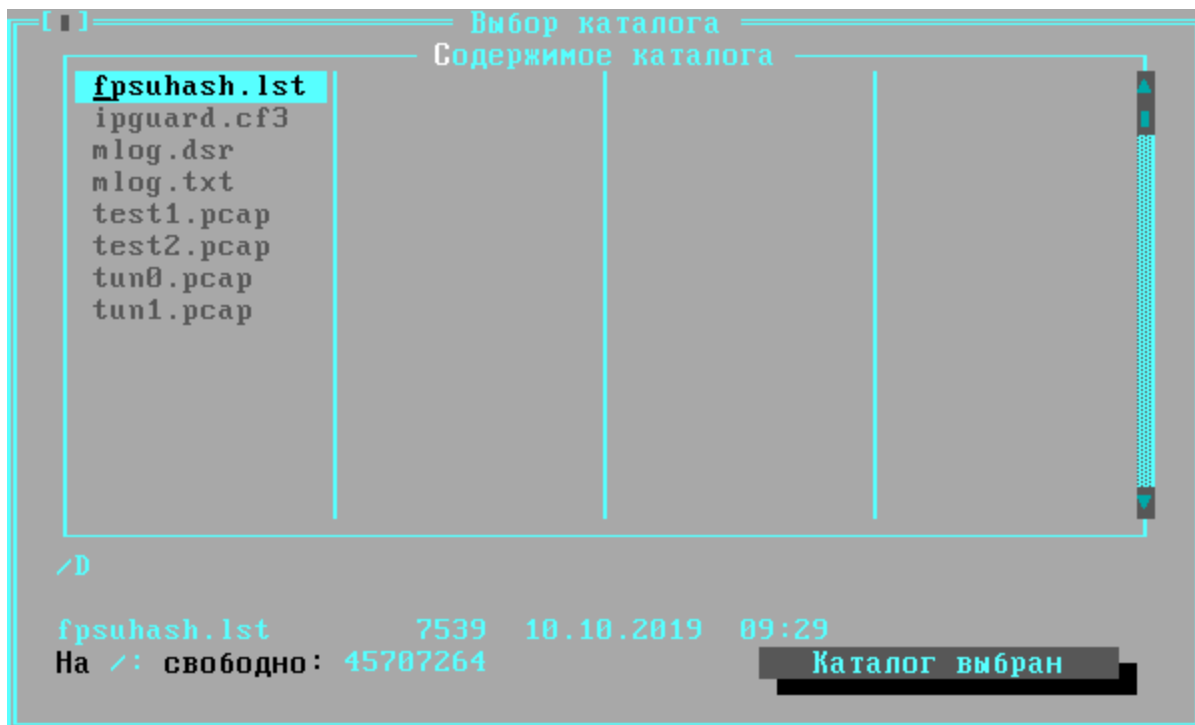


Рисунок 277 - Выбор каталога для выгрузки журнала

Подтвердите место выгрузки журнала, выполнив команду "Каталог выбран".

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

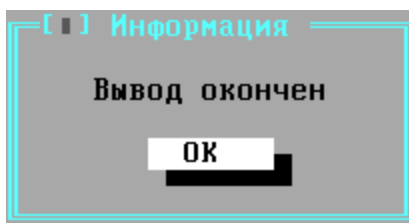


Рисунок 278 - Сообщение о завершении процедуры

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

13.3. Ограничение сбора статистики

Администратор может ввести ограничения на типы статистики, собираемой ФПСУ-IP. По умолчанию никаких ограничений не выставлено, 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.

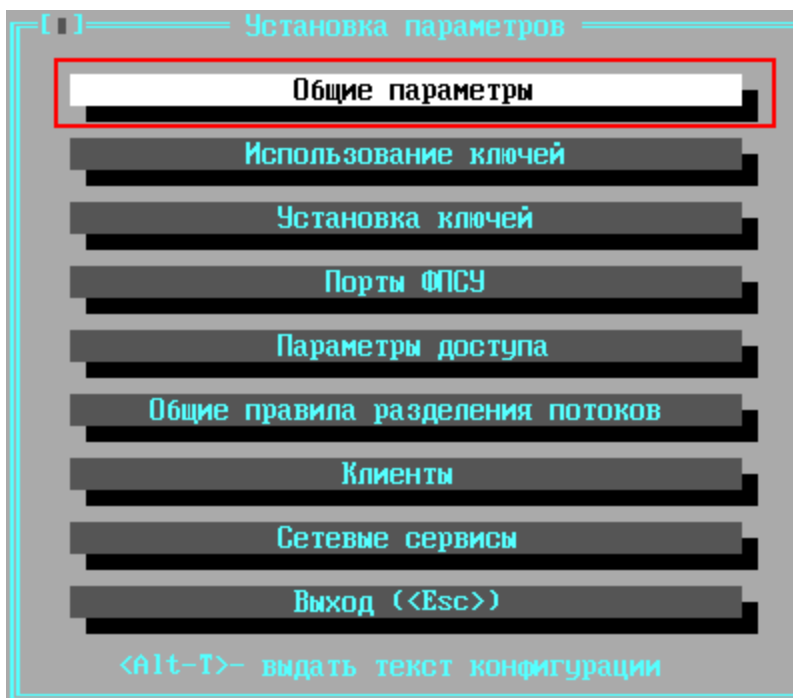


Рисунок 279 - Вход в общие настройки из основного меню конфигурации ФПСУ-IP

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

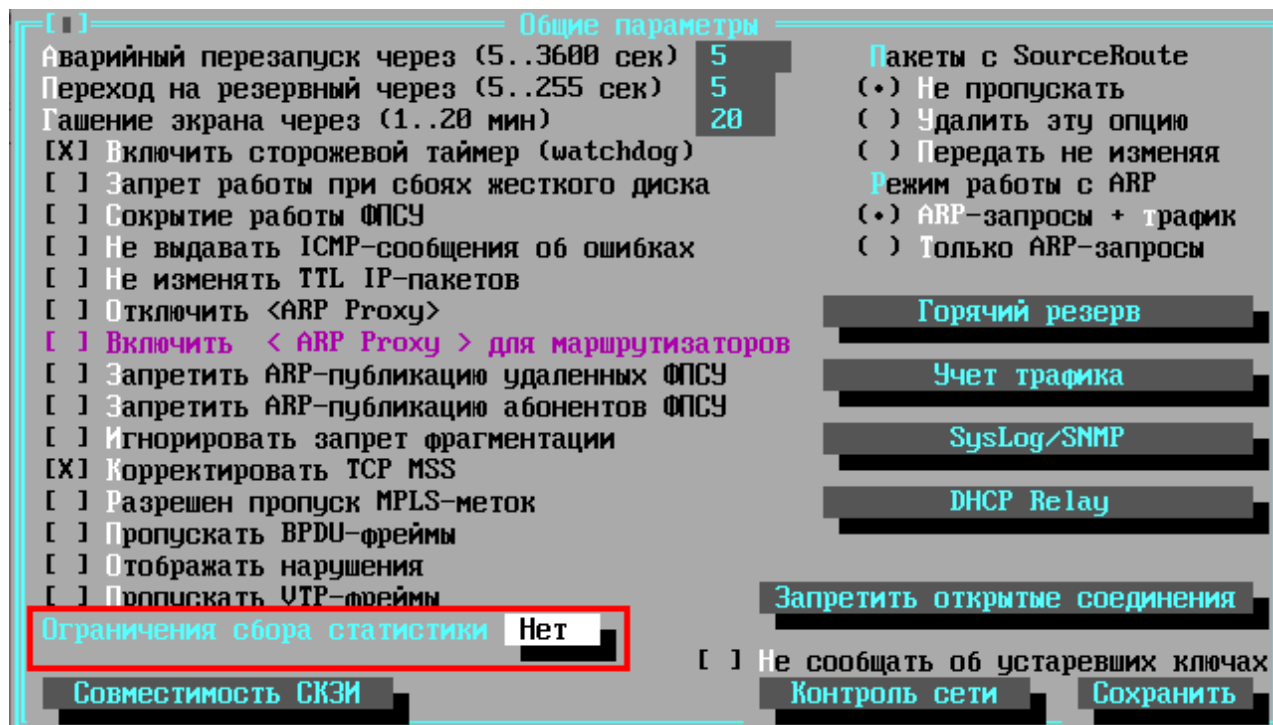


Рисунок 280 - Окно общих параметров ФПСУ-IP

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

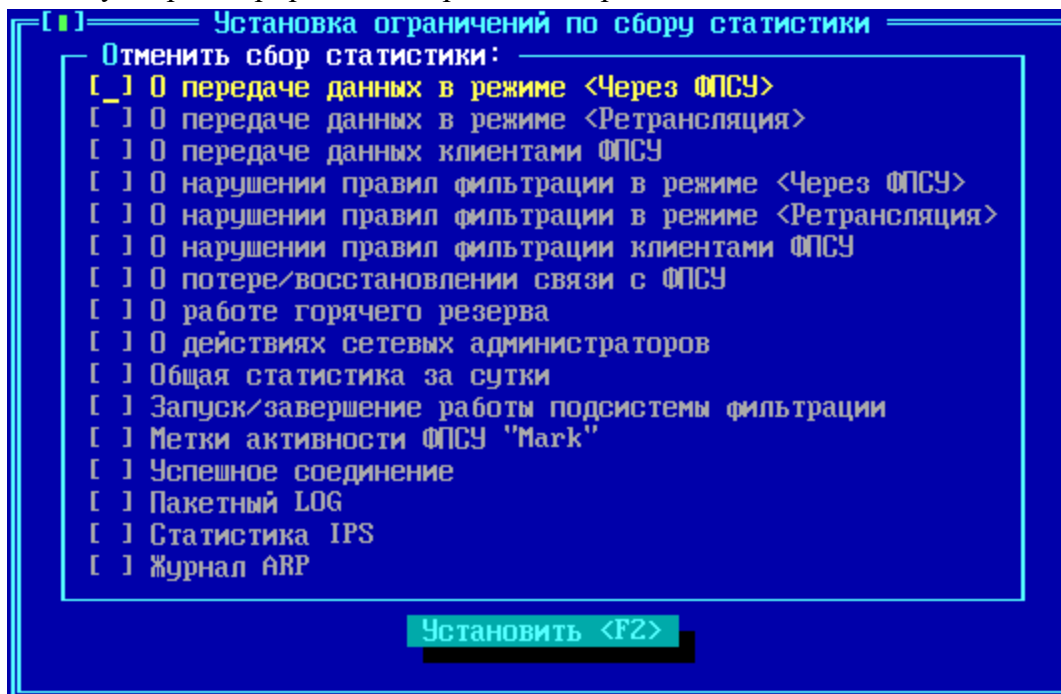


Рисунок 281 - Окно ограничения сбора статистики

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".

Пакетный LOG – ФПСУ-IP не будет вносить регистрировать для каждого обработанного межсетевым экраном пакета отдельную запись статистики (см. пункт "[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.

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 удастся, 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 администратора или главного администратора.

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 "Host" используются для регламентации передачи индивидуальных пакетов (unicast);
- описатели типа "Подсеть" и "Любой Host" используются для регламентации передачи как индивидуальных, так и широковещательных пакетов;
- индивидуальные IP-адреса абонентов (описатели типа "Host") 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 (переключатель "Только Broadcast" выключить нельзя).

15. 1. Использование одного ФПСУ-IP для защиты локальной сети

Предположим, что IP-сеть организации до установки ФПСУ-IP представляла из себя одну подсеть с IP-адресом 11.12.13.0 и маской 255.255.255.0 (24 разряда) и содержала маршрутизатор для выхода в другие IP-сети. 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.

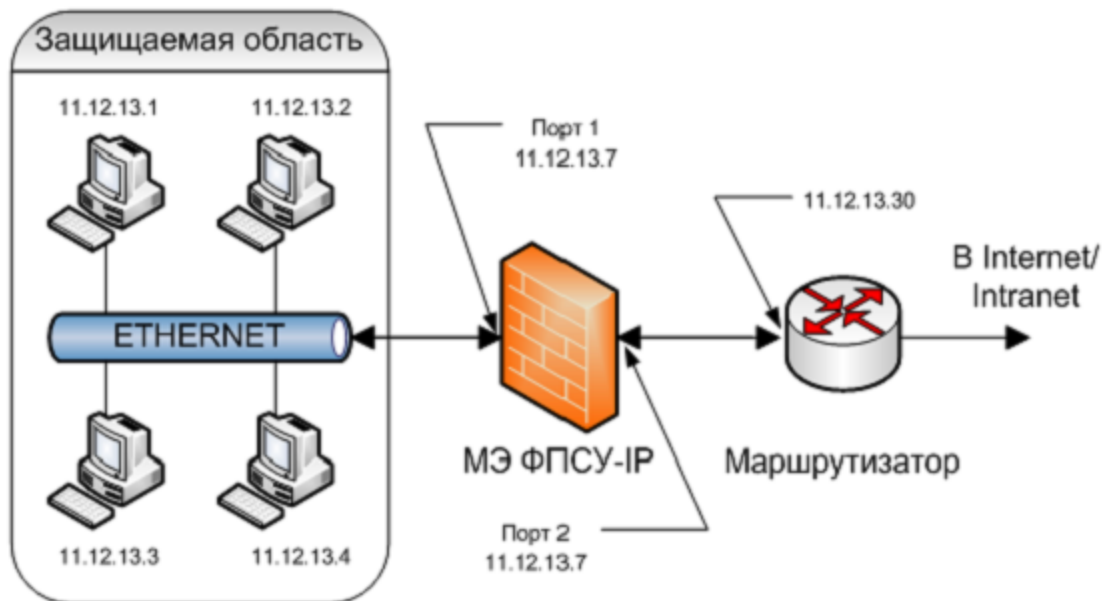


Рисунок 282 - Применение ФПСУ-IP для защиты оконечной области

Конфигурация МЭ должна содержать следующие установки:

=====

Порт 1:

Номер 1

Адрес 11.12.13.7

Маска 255.255.255.0 (24 разряда)

ФПСУ не определены

Маршрутизаторы не определены

Абоненты:

Подсеть; Адрес 11.12.13.0; Маска 255.255.255.0;

режим работы ретрансляция;

режим партнера этого порта – выключен;

режим партнера другого порта – включен только в ретрансляции;

переключатель "Только Broadcast" выключен; переключатель "Отвечать на Ping" – на усмотрение администратора; переключатель "Работа разрешена" включен.

Хост; 11.12.13.1;

режим работы ретрансляция;

режим партнера этого порта – выключен;

режим партнера другого порта – включен только в ретрансляции;

переключатель "Отвечать на Ping" – на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:

Номер 2;

Адрес 11.12.13.7;

Маска 255.255.255.0 (24 разряда);

ФПСУ не определены;

Маршрутизаторы 11.12.13.30;

протоколы маршрутизации выключены;

переключатель "Отвечать на Ping" – на усмотрение администратора.

Абоненты: Любой хост

режим работы ретрансляция;

через маршрутизатор 11.12.13.30;

переключатель "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 "[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).

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 11.12.13.30 или IP-адрес 1-го порта ФПСУ-IP.

На работу подсети наложены следующие ограничения:

- хост с IP-адресом 11.12.13.1 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.

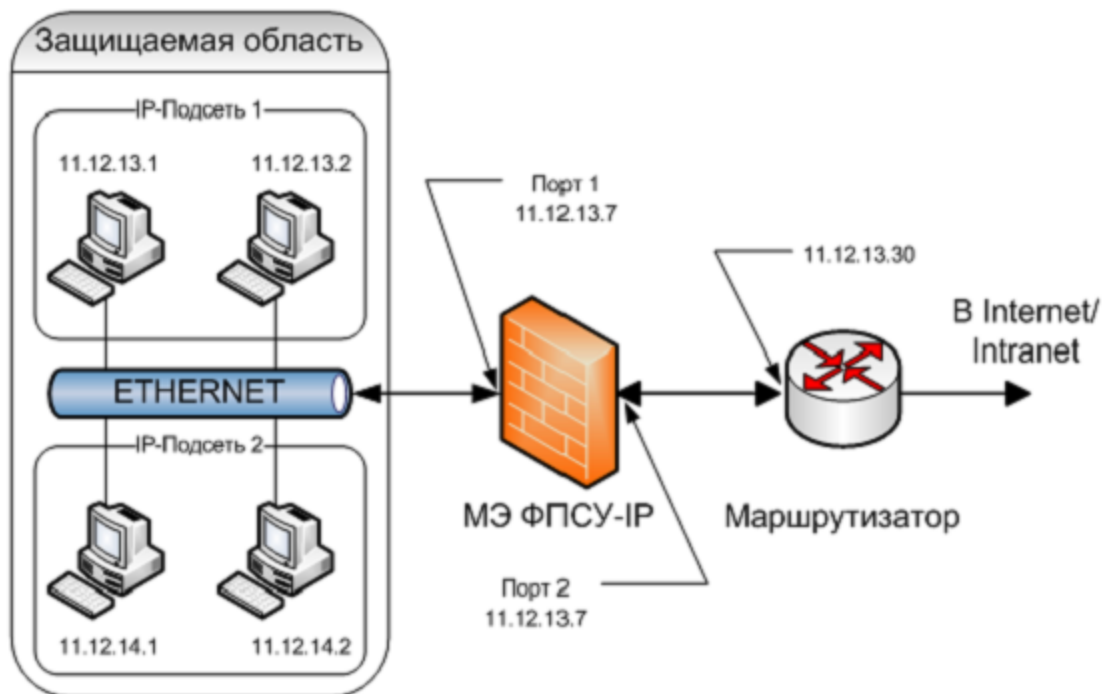


Рисунок 283 - Защита двух подсетей

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 11.12.13.1 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 11.12.13.7,

Маска 255.255.255.0 (24 разряда),

ФПСУ не определены,

Маршрутизаторы не определены,

Абоненты:

Подсеть; 11.12.13.0; 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;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Подсеть; 11.12.14.0; 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;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Хост; 11.12.13.1,

режим работы ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только в ретрансляции;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:

Номер 2;

Адрес 11.12.13.7;

Маска 255.255.255.0 (24 разряда);

ФПСУ не определены;

Маршрутизаторы

11.12.13.30,

протоколы маршрутизации выключены;

переключатель "Отвечать на Ping" - на усмотрение администратора.

Абоненты:**Любой хост;**

режим работы ретрансляция;
через маршрутизатор 11.12.13.30;
переключатель "Работа разрешена" включен.

Для выполнения дальнейших настроек рекомендуется ознакомиться с разделом ["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 11.12.13.1 (источник) с маршрутизатором 11.12.13.30 (назначение);
2. правило, разрешающее взаимодействие абонента 11.12.13.1 (источник), и абонента Любой хост 2 порта ФПСУ (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 11.12.13.1 (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 11.12.13.1 от IP-подсети 2 (запрещение обменов) производится двумя независимыми друг от друга ограничениями:

1. по настройке абонента 11.12.13.1 в разделе конфигурации "Порты ФПСУ", по признаку "Режим партнера – Данного порта" (режим "Ретрансляция" выключен);
2. Правил 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 в только в одно правило доступа, разрешающее взаимодействие лишь с абонентом 11.12.13.1.

15. 3. Разделение подсети на два фрагмента средствами ФПСУ-IP

Представим теперь, что до установки ФПСУ-IP существовала одна IP-подсеть с адресом 11.12.13.0 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 (["Защита локальной сети, состоящей из двух IP-подсетей"](#)) разделение абонентов на две подсети было логическим, то есть для его осуществления была необходима особая конфигурация ТСР/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.

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 11.12.13.1, и все хосты области 2 должны иметь полный доступ друг к другу, в том числе должна обеспечиваться возможность поиска и подключения сетевых дисков;
- хост 11.12.13.1 не должен иметь доступа в область 2.

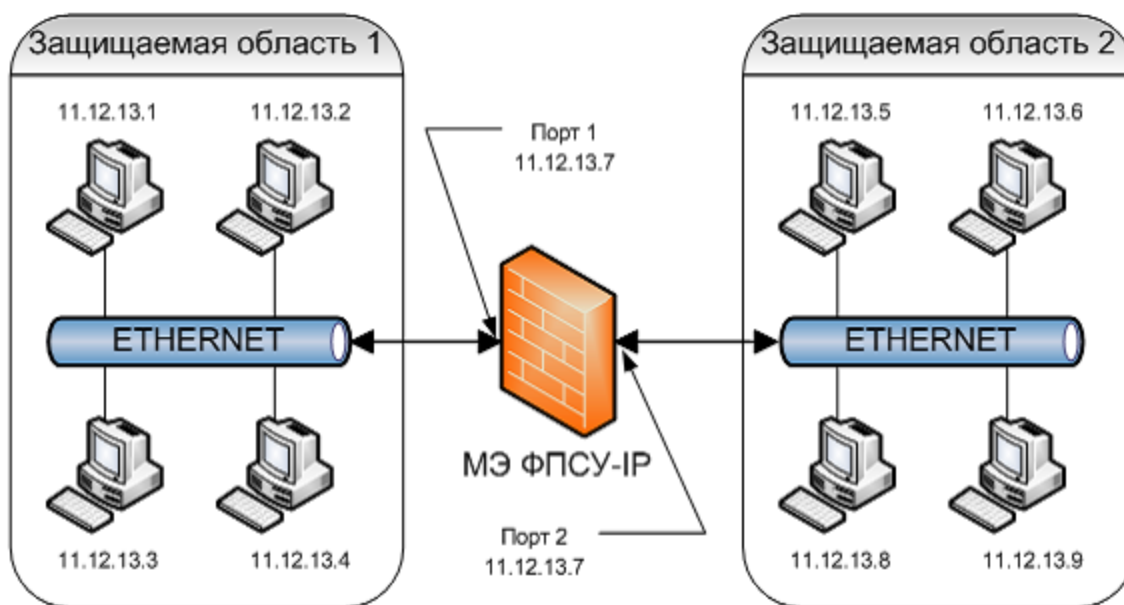


Рисунок 284 - Разбиение сети на фрагменты

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 невозможны;
- работа с ключевыми данными при такой топологии не производится;
- абоненту с IP-адресом 11.12.13.1 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 11.12.13.7,

Маска 255.255.255.0 (24 разряда),

ФПСУ не определены,

Маршрутизаторы не определены,

Абоненты:

Подсеть; 11.12.13.0; 255.255.255.0 (24 разряда),

режим работы ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только в ретрансляции;

переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Хост; 11.12.13.1;

режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - выключен;
переключатель "Работа разрешена" выключен.

Порт 2:

Номер 2,

Адрес 11.12.13.7,

Маска 255.255.255.0 (24 разряда),

ФПСУ не определены,

Маршрутизаторы не определены,

Абоненты:

Подсеть 11.12.13.0; 255.255.255.0 (24 разряда),

режим работы ретрансляция;
переключатель "Только Broadcast" включен;
переключатель "Работа разрешена" включен.

Хост; 11.12.13.5,

режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Хост; 11.12.13.6,

режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Хост; 11.12.13.8,

режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Хост; 11.12.13.9;

режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "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 11.12.13.1 запрещение работы с абонентами области 2 осуществляется через выключение переключателя "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 А - 11.12.1.0, маска 255.255.255.0 (24 бита);
- защищаемая область В - 11.12.2.0, маска 255.255.255.0 (24 бита);
- защищаемая область С - 11.12.3.0, маска 255.255.255.0 (24 бита);
- внутренний порт маршрутизатора А - 11.12.1.1;
- внутренний порт маршрутизатора В - 11.12.2.1;
- внутренний порт маршрутизатора С - 11.12.3.1.

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 (А, В, С) должно осуществляться только из защищаемой области С.

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

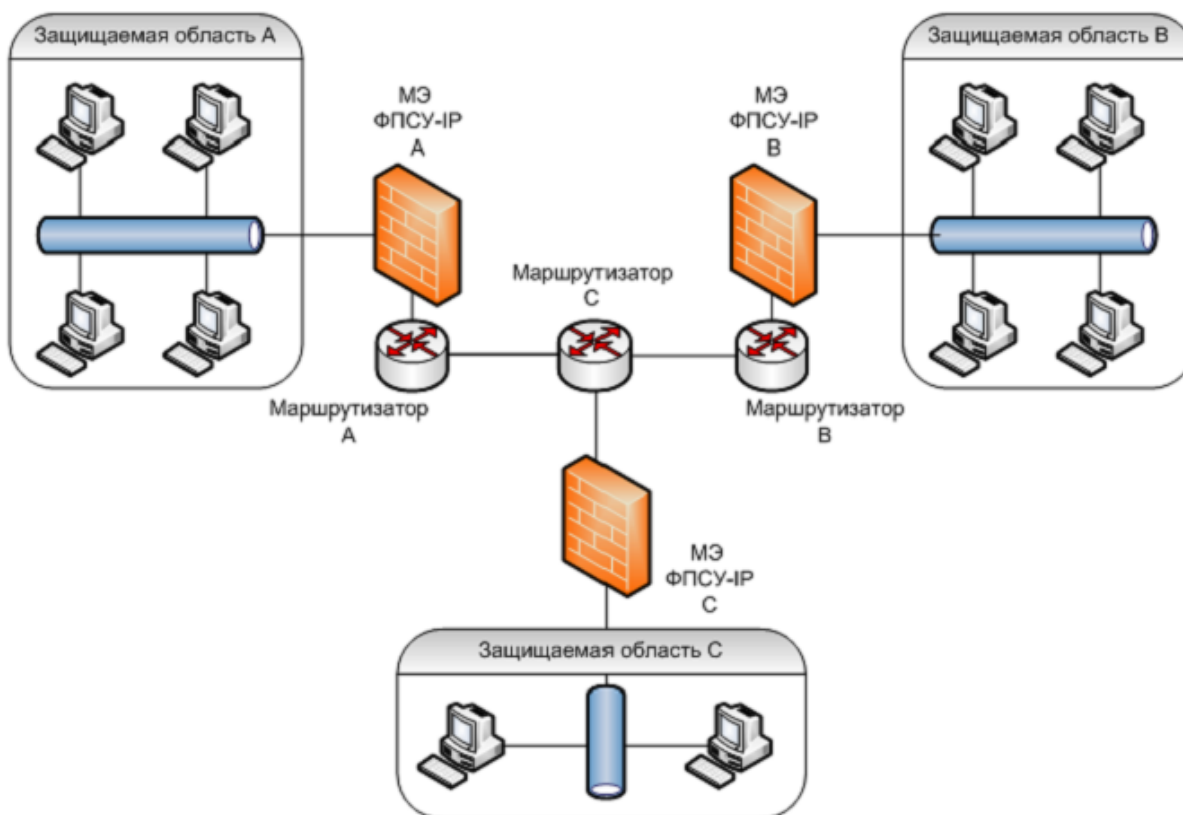


Рисунок 285 - Схема виртуальной частной сети на ФПСУ-IP

С точки зрения конфигурирования ФПСУ-IP А, В и С 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 А указан собственный номер ключа 1, на ФПСУ-IP В - номер 2 и на ФПСУ-IP С - номер 3;

- со стороны внешнего порта ФПСУ-IP установлены пограничные маршрутизаторы, управление которыми должно осуществляться только из защищаемой области С, 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 отдельных 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 А с областью С;
- VPN-2 - обмен области В с областью С;
- VPN-3 - обмен области А с областью В.

На рисунке ниже показаны организованные VPN-туннели.

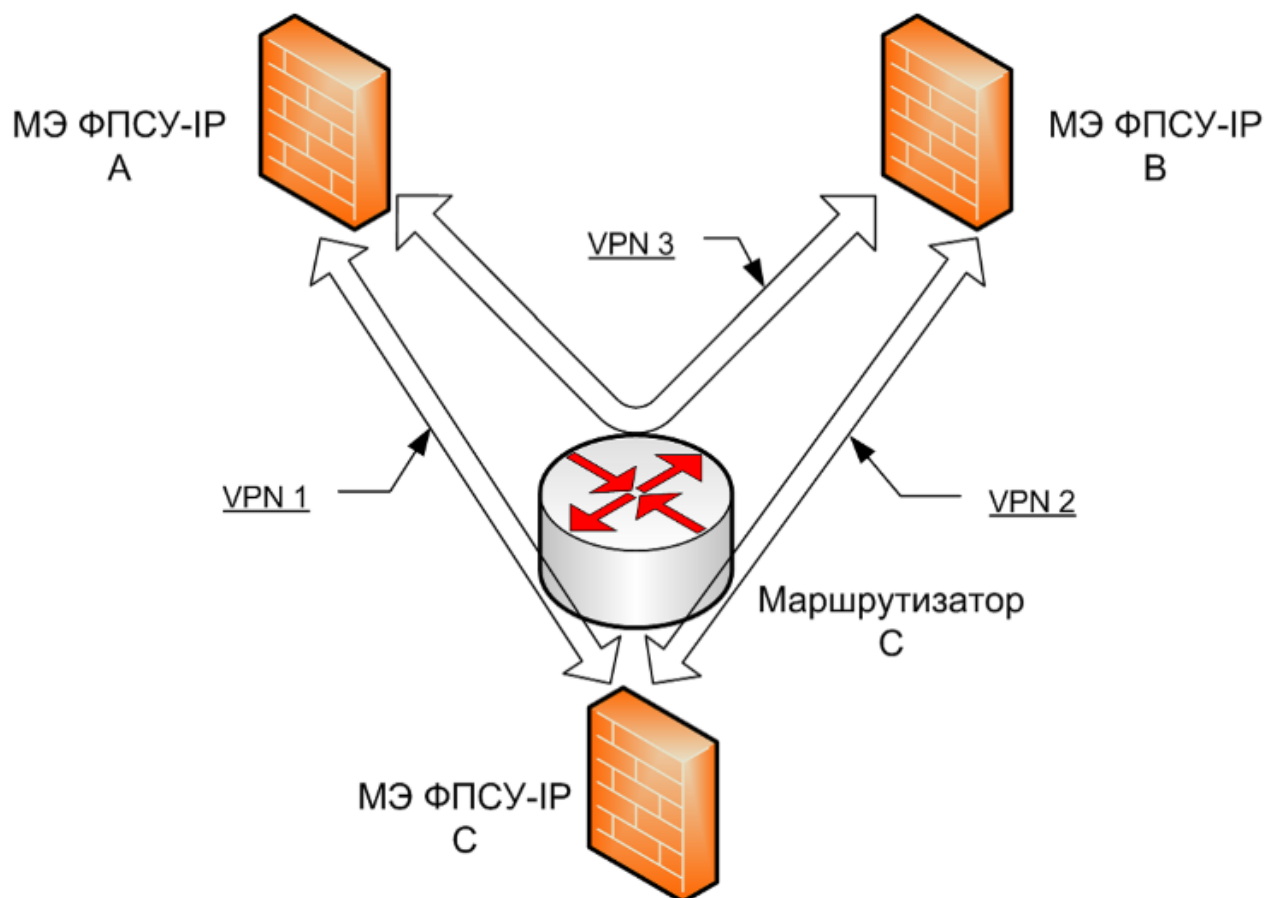


Рисунок 286 - Схема подключения с отдельными туннелями

Как видно из схемы, туннель 3 будет проходить через маршрутизатор С, минуя ФПСУ-IP С, т.е. маршрутизатор С будет осуществлять переброску (маршрутизацию) пакетов с одного из своих интерфейсов на другой для доставки их ФПСУ-IP А или ФПСУ-IP В.

Конфигурация ФПСУ-IP должна содержать следующие установки:

⇒

Для ФПСУ-IP А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1.1 (ключи с номерами 1.2, 1.3, 1.4 - на усмотрение администратора). Ключи номер 1.1 указаны как собственные.

Порт 1:

Номер 1;

Адрес 11.12.1.50;

Маска 255.255.255.0 (24 разряда);

ФПСУ не определены;

Маршрутизаторы не определены.

Абоненты:

Подсеть; 11.12.1.0; 255.255.255.0 (24 разряда),

режим работы - ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:

Номер 2;

Адрес 11.12.1.50;

Маска 255.255.255.0 (24 разряда);

ФПСУ

11.12.2.50, ключевые данные - 2.1; смена через 30 мин,

сжатие и криптозащита - "желательно" или "обязательно",

через маршрутизатор 11.12.1.1;

11.12.3.50, ключевые данные - 3.1; смена через 30 мин,

сжатие и криптозащита - "желательно" или "обязательно",

через маршрутизатор 11.12.1.1;

Маршрутизаторы

11.12.1.1;

протоколы маршрутизации - на усмотрение администратора,

переключатель "Отвечать на Ping" - на усмотрение администратора;

Абоненты

Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда),

через ФПСУ 11.12.2.50,

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда),

через ФПСУ 11.12.3.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

⇒

Для ФПСУ-IP В:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2.1 (ключи с номерами 2.2, 2.3, 2.4 - на усмотрение администратора). Ключи номер 2.1 указаны как собственные.

Порт 1:**Номер** 1**Адрес** 11.12.2.50**Маска** 255.255.255.0 (24 разряда)**ФПСУ** не определены**Маршрутизаторы** не определены**Абоненты:****Подсеть**, 11.12.2.0; 255.255.255.0 (24 разряда), ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:**Номер** 2**Адрес** 11.12.2.50**Маска** 255.255.255.0 (24 разряда)**ФПСУ:****11.12.1.50**, ключевые данные - 1.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.2.1

11.12.3.50, ключевые данные - 3.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.2.1

Маршрутизаторы:**11.12.2.1**, протоколы маршрутизации - на усмотрение администратора;

переключатель "Отвечать на Ping" - на усмотрение администратора;

Абоненты:**Подсеть**, 11.12.1.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.1.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.
Подсеть; 11.12.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

⇒

Для ФПСУ-IP C:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3.1 (ключи с номерами 3.2, 3.3, 3.4 - на усмотрение администратора). Ключи номер 3.1 указаны как собственные.

Порт 1:

Номер 1,

Адрес 11.12.3.50,

Маска 255.255.255.0 (24 разряда),

ФПСУ не определены,

Маршрутизаторы не определены;

Абоненты:

Подсеть; 11.12.3.0; 255.255.255.0 (24 разряда); ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:

Номер 2,

Адрес 11.12.3.50,

Маска 255.255.255.0 (24 разряда);

ФПСУ:

11.12.1.50, ключевые данные - 1.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.3.1

11.12.2.50, ключевые данные - 2.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.3.1

Маршрутизаторы:

11.12.3.1, протоколы маршрутизации - на усмотрение администратора;
переключатель "Отвечать на Ping" - на усмотрение администратора;

Абоненты:

Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.1.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.2.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Только на ФПСУ-IP С для подсети 11.12.3.0 должно быть разрешено управление маршрутизаторами 11.12.1.1, 11.12.2.1, 11.12.3.1 (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

В данном варианте конфигурации будут созданы всего два VPN-туннеля, показанные на рисунке ниже:

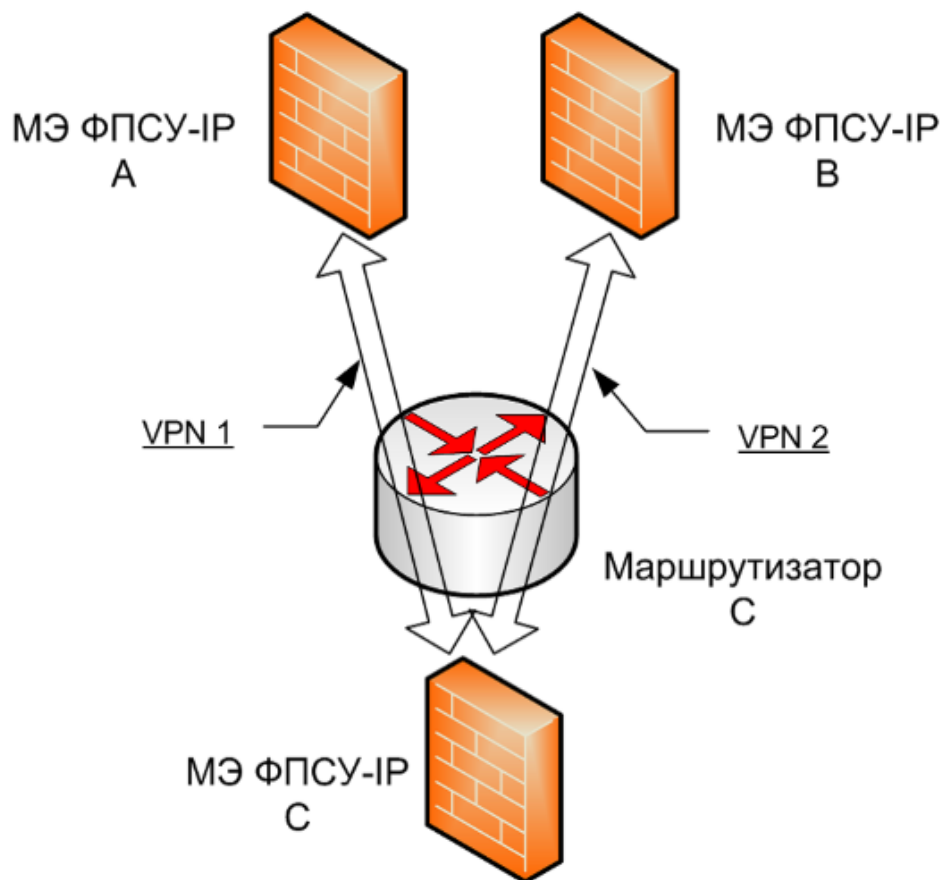


Рисунок 287 - Схема подключения с последовательными туннелями

При этом для обмена данными защищаемыми областями будут использоваться следующие туннели:

- VPN-1 - обмен области А с областью С;
- VPN-2 - обмен области В с областью С;
- VPN-1 и VPN-2 - обмен области А с областью В.

Конфигурация комплексов должна содержать следующие установки:

⇒

Для ФПСУ-IP А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1.1 (ключи с номерами 1.2, 1.3, 1.4 - на усмотрение администратора). Ключи номер 1.1 указаны как собственные.

Порт 1:**Номер** 1,**Адрес** 11.12.1.50,**Маска** 255.255.255.0 (24 разряда),**ФПСУ** не определены,**Маршрутизаторы** не определены,**Абоненты:****Подсеть**, 11.12.1.0; 255.255.255.0 (24 разряда); ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:**Номер** 2,**Адрес** 11.12.1.50,**Маска** 255.255.255.0 (24 разряда);**ФПСУ:****11.12.3.50**, ключевые данные - 3.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.1.1;

Маршрутизаторы**11.12.1.1**, протоколы маршрутизации - на усмотрение администратора;

переключатель "Отвечать на Ping" - на усмотрение администратора;

Абоненты:**Подсеть**, 11.12.2.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.3.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.3.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

⇒

Для ФПСУ-IP В:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2.1 (ключи с номерами 2.2, 2.3, 2.4 - на усмотрение администратора). Ключи номер 2.1 указаны как собственные.

Порт 1:**Номер** 1,**Адрес** 11.12.2.50,**Маска** 255.255.255.0 (24 разряда),**ФПСУ** не определены,**Маршрутизаторы** не определены;**Абоненты:****Подсеть**, 11.12.2.0; 255.255.255.0 (24 разряда); ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:**Номер** 2,**Адрес** 11.12.2.50,**Маска** 255.255.255.0 (24 разряда),**ФПСУ:****11.12.3.50**, ключевые данные - 3.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.2.1

Маршрутизаторы:**11.12.2.1**, протоколы маршрутизации - на усмотрение администратора;

переключатель "Отвечать на Ping" - на усмотрение администратора;

Абоненты:**Подсеть**, 11.12.1.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.3.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.3.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

⇒

Для ФПСУ-IP С:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3.1 (ключи с номерами 3.2, 3.3, 3.4 - на усмотрение администратора). Ключи номер 3.1 указаны как собственные.

Порт 1:

Номер 1,

Адрес 11.12.3.50,

Маска 255.255.255.0 (24 разряда),

ФПСУ не определены,

Маршрутизаторы не определены;

Абоненты:

Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда); ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:

Номер 2,

Адрес 11.12.3.50,

Маска 255.255.255.0 (24 разряда);

ФПСУ:

11.12.1.50, ключевые данные - 1.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.3.1

11.12.2.50, ключевые данные - 2.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.3.1

Маршрутизаторы:

11.12.3.1,

протоколы маршрутизации - на усмотрение администратора;

переключатель "Отвечать на Ping" - на усмотрение администратора;

Абоненты:

Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Только на ФПСУ-IP C для подсети 11.12.3.0 должно быть разрешено управление маршрутизаторами 11.12.1.1, 11.12.2.1, 11.12.3.1 (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-IP для создания в одной области двух защищаемых областей

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 А - 11.12.1.0, маска 255.255.255.0 (24 бита);
- защищаемая область В - 11.12.2.0, маска 255.255.255.0 (24 бита);
- защищаемая область С - 11.12.3.0, маска 255.255.255.0 (24 бита);
- внутренний порт маршрутизатора А - 11.12.2.1;

- внутренний порт маршрутизатора В -11.12.3.1.

На работу сети наложены следующие ограничения:

- хосты области А должны обмениваться пакетами только с хостами области С и не иметь доступа к другим абонентам;
- управление пограничными маршрутизаторами (А и В) должно осуществляться из защищаемой области В;
- хосты области В имеют доступ в мировую сеть Internet/Intranet и не имеют доступа к другим абонентам.

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

- со стороны внутреннего порта ФПСУ-IP (порта 1 со стороны области А) 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 В, доступ к которой необходимо запретить; IP-подсеть С, доступ в которую будет производиться через ФПСУ-IP В, а также мировая сеть, доступ в которую предоставлен не будет; существует также маршрутизатор А, находящийся с внешнего порта ФПСУ-IP В (поскольку он может являться маршрутизатором по умолчанию для хостов области А и является пограничным маршрутизатором);
- обмен между защищаемыми областями А и С должен производиться только внутри двух организованных ФПСУ-IP VPN-туннелей с проведением двусторонней аутентификации и использованием дополнительных процедур сжатия и криптозащиты;
- на ФПСУ-IP А должны быть установлены, и указаны как собственные, ранее выработанные ЦВК криптографические ключи номер 1;
- со стороны внешнего порта ФПСУ-IP (порта 2) присутствует пограничный маршрутизатор А, управление которым из защищаемой области А не должно осуществляться.

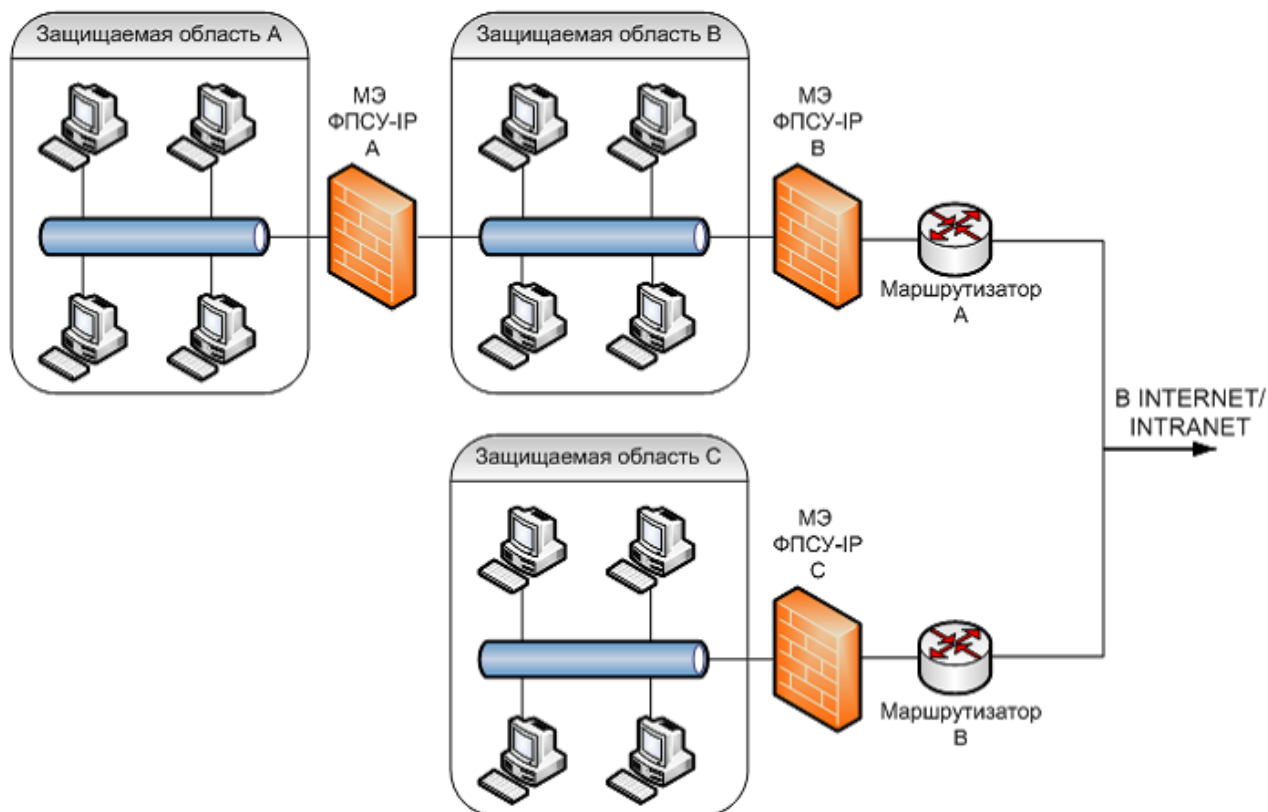


Рисунок 288 - Каскадное подключение ФПСУ-IP

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

- со стороны внутреннего порта (порта 1 со стороны области В) существуют две IP-подсети, доступ в область А должен быть запрещен абонентам В, к абонентам области В доступ будет производиться в режиме ретрансляции; маршрутизаторы отсутствуют; для организации туннеля через область В будет использован ФПСУ-IP А;
- со стороны порта 2 существуют IP-подсеть С, доступ к которой абонентам В должен быть запрещен, а также абоненты общедоступной сети передачи данных; доступ к общедоступной сети передачи данных производится через маршрутизатор А; ФПСУ-IP С существует и доступен через маршрутизатор А;
- на ФПСУ-IP В должны быть установлены, и указаны как собственные, ранее выработанные ЦВК криптографические ключи номер 2;
- со стороны внешнего порта ФПСУ-IP (порта 2) существует пограничный маршрутизатор А, управление которым должно осуществляться только из защищаемой области В, причем каналы управления маршрутизаторами В и С за

пределами их внешних портов должны быть защищены ФПСУ-IP В и С.

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

- со стороны внутреннего порта (порта 1 со стороны области С) 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 собственные ранее выработанные ключи номер 3;
- со стороны внешнего порта ФПСУ-IP существует пограничный маршрутизатор, управление которым должно осуществляться только из защищаемой области В, причем канал управления маршрутизатором за пределами его внешнего порта должен быть защищен ФПСУ-IP В и С.

Конфигурация ФПСУ-IP должна содержать следующие установки:

⇒

Для ФПСУ-IP А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1.1 (ключи с номерами 1.2, 1.3, 1.4 - на усмотрение администратора). Ключи номер 1.1 указаны как собственные.

Порт 1:

Номер 1,

Адрес 11.12.1.50,

Маска 255.255.255.0 (24 разряда),

ФПСУ не определены,

Маршрутизаторы не определены;

Абоненты:

Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда); ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Порт 2:

Номер 2,

Адрес 11.12.3.50,

Маска 255.255.255.0 (24 разряда);

ФПСУ:

11.12.2.50, ключевые данные - 2.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

Маршрутизаторы:

11.12.2.1, протоколы маршрутизации - все выключены;

переключатель "Отвечать на Ping" - выключен;

Абоненты:

Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.2.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Хост, 11.12.3.1, ретрансляция;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" выключен.

⇒

Для ФПСУ-IP В:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2.1 (ключи с номерами 2.2, 2.3, 2.4 - на усмотрение администратора). Ключи номер 2.1 указаны как собственные.

Заведена группа доступа, в которую включены подсети 11.12.1.0 и 11.12.3.0, переключатель "Контроль взаимосвязей Активен" - включен. Подсети 11.12.2.0 со стороны порта 1 разрешено управление маршрутизатором 11.12.2.1.

Порт 1:

Номер 1,

Адрес 11.12.2.50,

Маска 255.255.255.0 (24 разряда);

ФПСУ:

11.12.1.50, ключевые данные - 1.1; смена через 30 мин;
сжатие и криптозащита - "желательно" или "обязательно";

Маршрутизаторы не определены;

Абоненты:

Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.1.50;

режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Порт 2:

Номер 2,

Адрес 11.12.2.50,

Маска 255.255.255.0 (24 разряда),

ФПСУ:

11.12.3.50, ключевые данные - 3.1; смена через 30 мин;
сжатие и криптозащита - "желательно" или "обязательно";
через маршрутизатор 11.12.2.1.

Маршрутизаторы:

11.12.2.1, протоколы маршрутизации - все выключены;
переключатель "Отвечать на Ping" - на усмотрение администратора;

Абоненты:

Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.3.50;

режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Хост, 11.12.3.1; через ФПСУ 11.12.3.50;

режим партнера этого порта - включен только через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Любой хост;

переключатель "Работа разрешена" включен;
через маршрутизатор 11.12.13.30;

⇒

Для ФПСУ-IP С:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3.1 (ключи с номерами 3.2, 3.3, 3.4 - на усмотрение администратора). Ключи номер 3.1 указаны как собственные.

Заведена группа доступа, в которую включены подсети 11.12.1.0 и 11.12.3.0, переключатель "Контроль взаимосвязей Активен" - включен; Подсети 11.12.2.0 со стороны порта 2 разрешено управление маршрутизатором 11.12.3.1.

Порт 1:

Номер 1,

Адрес 11.12.3.50,

Маска 255.255.255.0 (24 разряда),

ФПСУ не определены,

Маршрутизаторы не определены;

Абоненты:

Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда); ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только режим через ФПСУ;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:

Номер 2,

Адрес 11.12.3.50,

Маска 255.255.255.0 (24 разряда);

ФПСУ:

11.12.2.50, ключевые данные - 2.1; смена через 30 мин;

сжатие и криптозащита - "желательно" или "обязательно";

через маршрутизатор 11.12.3.1.

Маршрутизаторы:

11.12.3.1, протоколы маршрутизации - все выключены;

переключатель "Отвечать на Ping" - выключен;

Абоненты:

Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.2.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда);

через ФПСУ 11.12.2.50;

режим партнера этого порта - включен только режим через ФПСУ;

режим партнера другого порта - включены все режимы;

переключатель "Только Broadcast" выключен;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

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 А:

- абоненты области А не получают доступа к области В, маршрутизатору А 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 А режим работы с абонентом противоположного порта (только через ФПСУ);
- отсутствие доступа абонентов области А к маршрутизатору А обеспечивается тем, что он описан (специально для этой цели) со стороны порта 2 с выключенным признаком "Работа разрешена" (все остальные установки в описателе, соответствующем маршрутизатору А, не имеют значения);
- Доступ от абонентов области А к абонентам области С осуществляется через ФПСУ-IP В.

В соответствии с установленной конфигурацией через ФПСУ-IP В:

- абоненты области В не имеют доступа к области А, поскольку в описателе А на порту 1 нет разрешения работы с абонентами данного порта; кроме того, доступу к А также препятствует то, что область В не входит в группу доступа, в которую входят А и С, а переключатель "Контроль взаимосвязей Активен" включен;
- абонентам области В разрешено управление маршрутизатором А и доступ в общедоступную сеть передачи данных;

- к абонентам области С (исключая маршрутизатор В, описанный отдельно) абоненты области В доступа не получают, поскольку область В не входит в группу доступа, в которую входят А и С, а переключатель "Контроль взаимосвязей Активен" включен;
- доступ к маршрутизатору В от абонентов области В обеспечивается тем, что он указан как абонент на порту 2 и будет осуществляться только через ФПСУ-IP С.

В соответствии с установленной конфигурацией через ФПСУ-IP С:

- отсутствие доступа абонентов области С к маршрутизатору А и области В обеспечивается тем, что область В не входит в группу доступа, в которую входят А и С, а переключатель "Контроль взаимосвязей Активен" включен;
- доступ абонентов области С к мировой сети невозможен - они не указаны на порту 2; кроме того, у абонентов С указан режим работы с абонентами противоположного порта только через ФПСУ-IP;
- доступ от абонентов области С к маршрутизатору В невозможен, поскольку, во-первых, управление маршрутизатором не разрешено, во-вторых, он не описан как абонент, в-третьих, у абонентов С указан режим работы с абонентами противоположного порта только через ФПСУ-IP.

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 "недоверенные" 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 "недоверенный" 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 7

Неполадки	Возможные причины неполадок	Методы определения и/или устранения
Отсутствие принимаемых пакетов на соответствующем порту ФПСУ-IP.	Несоответствующий тип соединительного кабеля между ФПСУ-IP и смежным оборудованием	Проверить тип применяемого кабеля и убедиться в его соответствии подключенному оборудованию
Отсутствие принимаемых пакетов на соответствующем порту ФПСУ-IP или появление большого количества ошибочных пакетов (см. пункт "Окно состояния рабочих LAN портов")	Дефект соединительного кабеля между ФПСУ-IP и смежным оборудованием	Проверить работоспособность применяемого кабеля и при обнаружении неисправности заменить кабель

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

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.

Ошибки формата принимаемых IP-пакетов:

Диагностика	Пояснение	Причина возникновения
<i>Короткий пакет</i>	Длина принятых данных короче, чем указано в IP заголовке принятого пакета.	Сбой или коллизии локальной сети; сбой у станции отправителя.
<i>Ошибка фрагментации</i>	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 ")
<i>Отмена фрагментации</i>	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.
<i>Ошибочный фрагмент</i>	Начало фрагментированного пакета не выровнено на 8 байтовую границу.	Некорректная работа программного обеспечения станции-отправителя.
<i>Неверен список опций</i>	Список IP-опций в заголовке IP пакета не отвечает принятым в сообществе Интернет правилам.	Некорректная работа программного обеспечения станции-отправителя.
<i>Мало памяти</i>	Недостаточно оперативной памяти для приема и/или обработки пакета.	Если такая ошибка указывается для разных IP адресов, причина возникновения - "штурм" 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.

Ошибки, связанные с обработкой принимаемых IP-пакетов:

Диагностика	Пояснение	Причина возникновения
<i>Маршрут неизвестен</i>	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

Диагностика	Пояснение	Причина возникновения
		ФПСУ-IP за непродолжительное время.
<i>Сбой LAN карты</i>	Сбой указанного сетевого адаптера при попытке передачи фрейма	Неустойчивая работа сбойного сетевого адаптера - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.
<i>Дублирование адресов</i>	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.
<i>Неверен IP адрес</i>	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.
<i>Истекло время</i>	Время жизни пакета истекло, или исчерпан лимит времени ожидания сборки пакета	У принятого пакета истекает время жизни. Если данная ошибка проявляется часто, причем получателем является данный ФПСУ-IP, а отправителем - другой ФПСУ-IP, рекомендуется в конфигурации обоих ФПСУ-IP изменить

Диагностика	Пояснение	Причина возникновения
		значение MTU (см. раздел "Описание параметров удаленных ФПСУ-IP")
<i>Протокол недоступен</i>	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.

Ошибки, связанные с попытками нарушения установленных правил фильтрации:

Диагностика	Пояснение	Причина возникновения
<i>Входящий не описан</i>	Отправитель пакета не описан в конфигурации	Отправитель пакета не описан в конфигурации портов ФПСУ-IP.
<i>Получатель не описан</i>	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.
<i>Запрет работы</i>	Отказ в доступе абоненту-отправителю пакета	Выключен переключатель " <i>Работа Разрешена</i> " у отправителя или получателя пакета. Попытка приема или передачи в индивидуальный адрес при включенном переключателе " <i>Только Broadcast</i> ". Попытка межмаршрутизаторного обмена по

Диагностика	Пояснение	Причина возникновения
		<p>неразрешенному протоколу маршрутизации для маршрутизатора-отправителя пакета.</p> <p>"Ping"- попытка ФПСУ-IP от прописанного абонента или маршрутизатора при выключенном переключателе "Отвечать на Ping".</p> <p>"Ping"- попытка ФПСУ-IP длинным пакетом.</p> <p>Не "Ping"-попытка обращения прописанного абонента к удаленному ФПСУ-IP или абонент не является удаленным администратором или ФПСУ-IP.</p>
<i>Запрет по доступу</i>	Запрет по режиму работы с партнером.	Запрет по режиму работы с партнером данного или противоположного порта.
<i>Групповой запрет</i>	Запрет по группам доступа.	Абоненты (отправитель и получатель) приписаны к разным группам доступа с непересекающимися условиями фильтрации.
<i>Запрет взаимосвязи</i>	Запрет по взаимосвязи соединений.	Абоненты отправитель и получатель не входят ни в одну из заведенных групп доступа с включенными переключателями "Контроль взаимосвязи активен".
<i>Запрет по портам</i>	Запрет доступа по TCP/UDP портам	В группе (группах) доступа, к которой приписаны абоненты отправитель и получатель пакета используемые TCP/UDP порты запрещены.
<i>Запрет SourceRoute</i>	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 переключатель "Пакеты с опцией SourceRoute" - "Не пропускать".
<i>Абонент</i>	Абонент должен	Принят пакет из VPN-туннеля от абонента, для

Диагностика	Пояснение	Причина возникновения
<i>через ФПСУ</i>	работать в режиме ретрансляции.	которого на данном ФПСУ-IP установлен режим работы "Ретрансляция".
<i>Абонент миновал ФПСУ</i>	Абонент должен работать через ФПСУ.	Принят пакет не из VPN-туннеля от абонента, для которого на данном ФПСУ-IP установлен режим работы "Через ФПСУ".
<i>ФПСУ не работает</i>	Удаленный ФПСУ-IP не работает.	<p>Не включен удаленный ФПСУ-IP или с ним нет связи.</p> <p>Не работает сетевой адаптер - адаптер необходимо заменить.</p> <p>Несовместимые режимы работы смежных сетевых адаптеров.</p>
<i>Нет ФПСУ-туннеля</i>	Отсутствие взаимодействия между ФПСУ-IP.	<p>VPN-туннель между двумя ФПСУ-IP не установлен к моменту попытки передачи через него пакетов от абонентов.</p> <p>Не включен удаленный ФПСУ-IP или с ним нет связи.</p> <p>Неустойчивая работа сбойного сетевого адаптера - адаптер необходимо заменить.</p> <p>Несовместимые режимы работы смежных сетевых адаптеров.</p>
<i>Ложный ФПСУ</i>	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.

Диагностика	Пояснение	Причина возникновения
<i>Ошибочный ФПСУ-пакет</i>	Ошибочный пакет от ФПСУ-IP.	<p>На местном или удаленном ФПСУ-IP указаны неверные значения номеров ключевых данных удаленных ФПСУ-IP.</p> <p>В процессе установки или поддержания VPN-туннеля произошел кратковременный сбой, что обычно очень редко проявляется в момент первичной установки VPN-туннеля.</p> <p>Попытка навязывания местному ФПСУ-IP VPN-данных или повторения ранее переданных удаленным ФПСУ-IP данных от "вредоносной" станции.</p>
<i>Ошибка клиент-пакет</i>	Искажены или повреждены находящиеся в полученном от ФПСУ-IP\Клиента пакете данные.	<p>Сообщение возникает на экране мониторинга подключенных ФПСУ-IP/Клиентов.</p> <p>Такие пакеты будут сброшены ФПСУ-IP.</p>

Ошибки, связанные с ключевыми данными:

Служебное сообщение	Пояснение	Действия администратора
<i>The TM does not contain the key</i>	Ошибка возникает при попытке запуска ФПСУ-IP с помощью ТМ-идентификатора, на котором находится искаженный ключ запуска.	<p>Если искажен ключ запуска Главного администратора - обратитесь к поставщику ФПСУ-IP для замены ТМ-идентификатора Главного администратора.</p> <p>Если искажен ключ запуска пользователя другого класса - повторно перезапишите ТМ-идентификатор пользователя средствами</p>

Служебное сообщение	Пояснение	Действия администратора
		ФПСУ-IP (Настройка системы - Регистрация ТМ-идентификаторов)
<p><i>Внимание!</i> <i>Повреждены критические компоненты комплекса. ВСЕ установленные ключевые данные и ТМ утрачены. Комплекс переведен в технологический режим. Возможно потребуется переустановка комплекса</i></p>	<p>ПО ФПСУ-IP обнаружило искажение ключа для хранения долговременных ключей.</p> <p>Требуется вмешательство администратора</p>	<p>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.</p> <p>В случае ошибки перевода ФПСУ-IP из технологического режима в рабочий режим, выполнить полную переустановку ПО ФПСУ-IP.</p>
<p><i>Внимание!</i> <i>Поврежден компонент комплекса. Необходима инициализация ДСЧ</i></p>	<p>ПО ФПСУ-IP обнаружило искажение ключа ПДСЧ.</p> <p>Требуется вмешательство администратора</p>	<p>Требуется выполнить повторный перевод ФПСУ-IP из технологического режима в рабочий режим.</p>
<p><i>Внимание! ФПСУ не работоспособен. Искажены данные конфигурации. Ожидание восстановления конфигурации с резервного комплекса или удаленного администратора</i></p>	<p>ПО ФПСУ-IP обнаружило искажение конфигурации ФПСУ-IP</p>	<p>Восстановить конфигурацию ФПСУ-IP любым из следующих способов:</p> <ul style="list-style-type: none"> • локально с помощью резервной копии конфигурации; • подключить к ФПСУ-IP комплекс горячего резерва; • установить на ФПСУ-IP новую конфигурацию средствами удаленного администратора.

Служебное сообщение	Пояснение	Действия администратора
<p><i>Ошибка инициализации! Служебный описатель искажен</i></p>	<p>Сообщение об ошибке выводится на экран просмотра состояний удаленных администраторов ФПСУ-IP.</p> <p>ПО ФПСУ-IP обнаружило искажение секретного ключа ФПСУ-IP подсистемы удаленного администрирования или открытых ключей удаленных администраторов.</p> <p>Удаленное управление ФПСУ-IP с такой ошибкой невозможно.</p>	<p>Заново зарегистрировать удаленных администраторов на ФПСУ-IP.</p> <p>Перерегистрировать ФПСУ-IP на всех удаленных администраторах.</p>
<p><i>Описатель удаленных администраторов испорчен или несовместимая версия!</i></p>	<p>Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ-IP.</p> <p>ПО ФПСУ-IP обнаружило искажение секретного ключа ФПСУ-IP подсистемы удаленного администрирования или открытых ключей удаленных администраторов</p> <p>Удаленное управление</p>	<p>Заново зарегистрировать удаленных администраторов на ФПСУ-IP.</p> <p>Перерегистрировать ФПСУ-IP на всех удаленных администраторах.</p>

Служебное сообщение	Пояснение	Действия администратора
	ФПСУ-IP с такой ошибкой невозможно.	
<i>*Имя_файла_с_открытым_ключом_удаленного_администратора*----> Поврежден</i>	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ-IP при попытке зарегистрировать нового удаленного администратора. Причина - искажен или поврежден предъявленный на внешнем USB-носителе открытый ключ удаленного администратора	Заново получить от администратора АРМ УА открытый ключ удаленного администратора и повторить процедуру регистрации удаленного администратора на ФПСУ-IP
<i>Состояние туннеля с другим ФПСУ-IP "WaitSynRR" с дополнительными сообщениями в журнале статистики "Аварийное состояние ключей/нештатные действия: Ошибка при зачитывании установленных ключей"</i>	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.
<i>Данные искажены, пропускаю!</i>	Сообщение об ошибке выводится на экране установки ключей меню	Заново получить от администратора ЦВК парно-выборочный ключ взамен

Служебное сообщение	Пояснение	Действия администратора
	<p>конфигурации ФПСУ-IP.</p> <p>Возникает при искажении предъявленного на внешнем USB-носителе парно-выборочного ключа</p>	искаженного.
<p><i>Испорчены служебные данные горячего резервирования</i></p>	<p>Сообщение об ошибке выводится на экране мониторинга состояния горячего резерва ФПСУ-IP (основной комплекс системы горячего резервирования).</p> <p>Ошибка возникает при искажении хранящегося на внутреннем накопителе ФПСУ-IP ключа горячего резерва</p>	<p>Считать на ТМ-идентификатор ключ горячего резерва с исправного комплекса (меню локального конфигурирования ФПСУ-IP "Настройка системы" - "Параметры горячего резерва").</p> <p>Если ключ горячего резерва не считывается с исправного комплекса, создать новый ключ горячего резерва.</p> <p>Повторно зарегистрировать ключ горячего резерва на сообщившем об ошибке ФПСУ-IP.</p>
<p><i>ФАТАЛЬНАЯ ОШИБКА. Резервный комплекс не может функционировать, так как испорчены служебные данные горячего резервирования. Возможно потребуется переустановка комплекса</i></p>	<p>Сообщение об ошибке выводится при запуске ФПСУ-IP (резервный комплекс системы горячего резервирования).</p> <p>Ошибка возникает при искажении хранящегося на внутреннем накопителе ФПСУ-IP ключа горячего резерва</p>	<p>Считать на ТМ-идентификатор ключ горячего резерва с исправного комплекса (меню локального конфигурирования ФПСУ-IP "Настройка системы" - "Параметры горячего резерва").</p> <p>Если ключ горячего резерва не считывается с исправного комплекса, создать новый ключ горячего резерва.</p> <p>Повторно зарегистрировать ключ горячего резерва</p>

Служебное сообщение	Пояснение	Действия администратора
		резерва на сообщившем об ошибке ФПСУ-IP.
<i>Испорчен или не установлен ключ центра</i>	Сообщение об ошибке выводится на экране мониторинга действий ФПСУ-IP\Клиентов. Искажен общесистемный ключ криптосети Клиентов. ФПСУ-IP\Клиенты не могут соединиться с ФПСУ-IP	Заново установить на ФПСУ-IP общесистемный ключ криптосети Клиентов вместо искаженного.
<i>ТМ испорчена</i>	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

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.

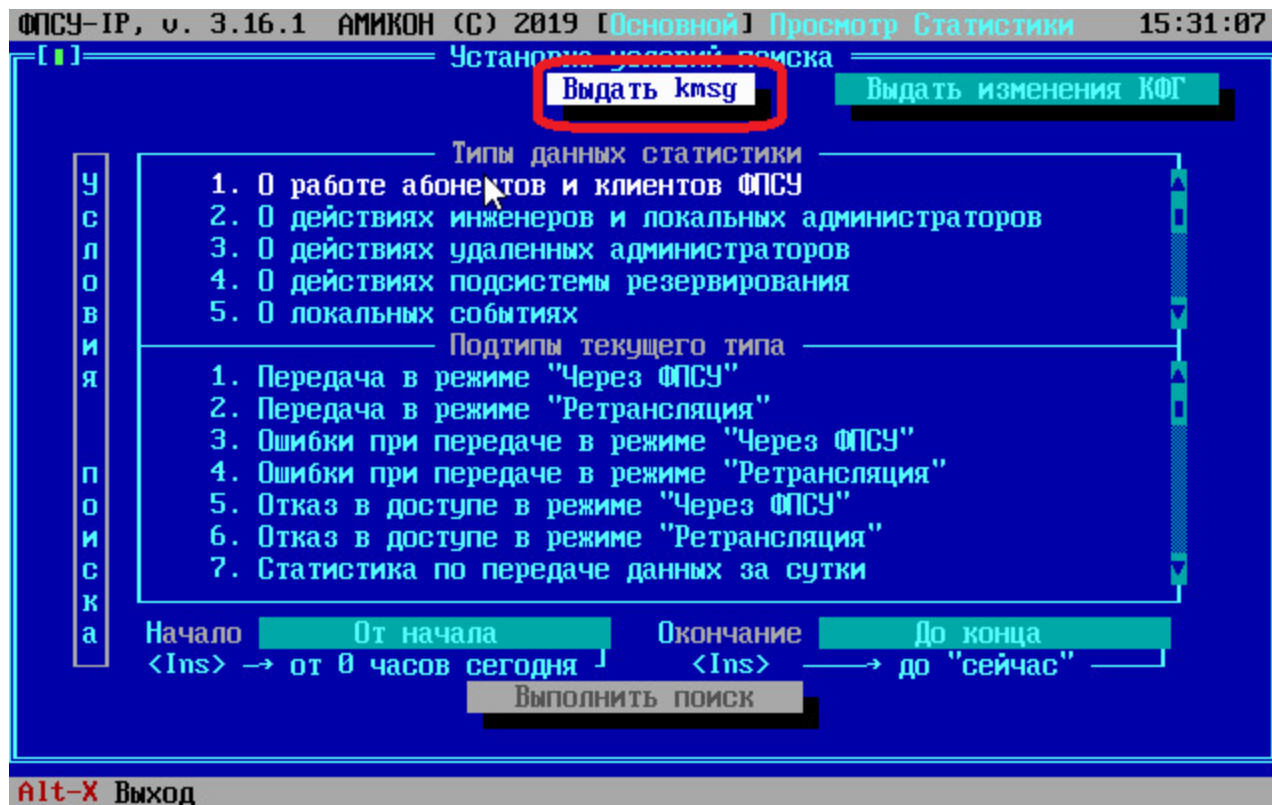


Рисунок 289 - Команда выдачи журнала изменений конфигурации межсетевого экрана

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

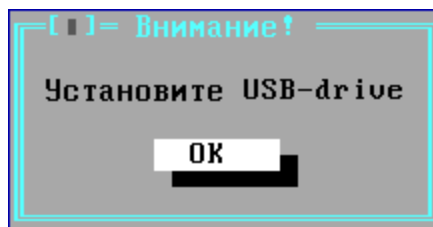


Рисунок 290 - Предложение подключить USB-носитель

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.

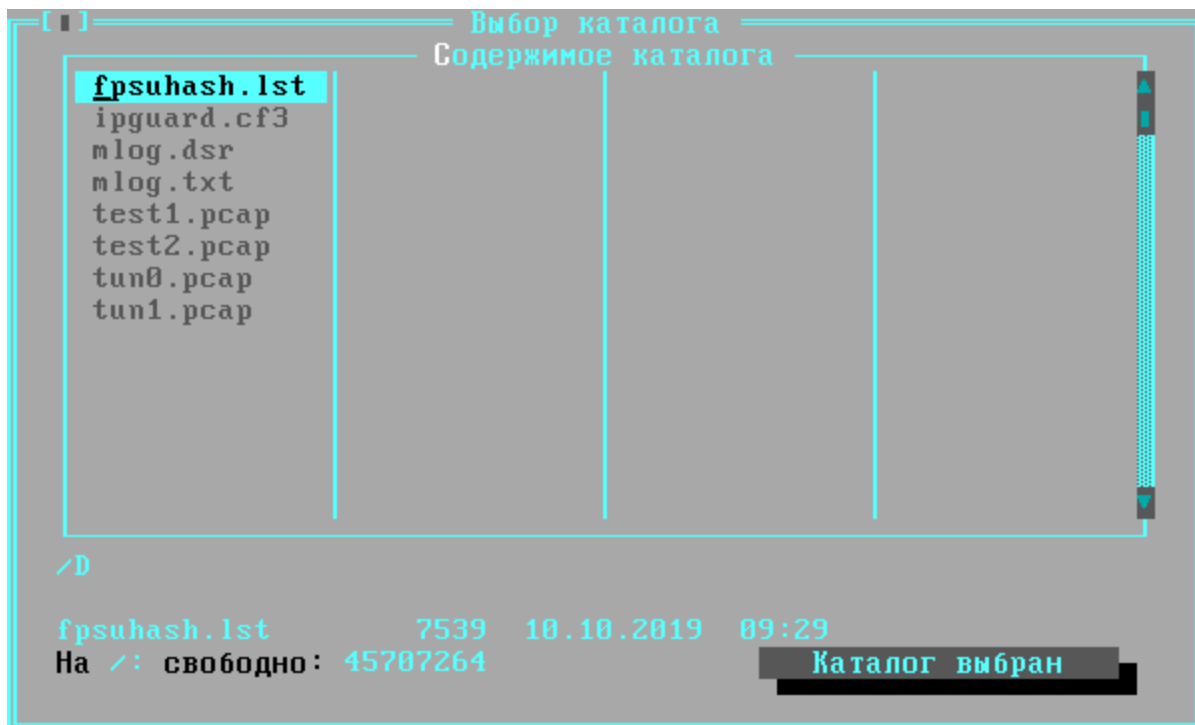


Рисунок 291 - Выбор каталога для выгрузки файла

Подтвердите место выгрузки файла, выполнив команду "Каталог выбран".

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

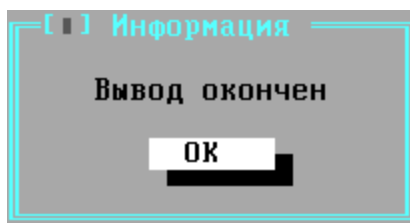


Рисунок 292 - Сообщение о завершении процедуры

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:

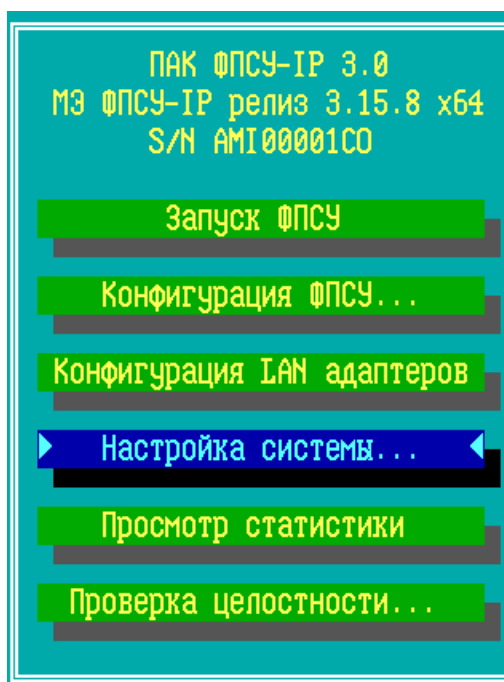


Рисунок 293 - Главное меню ФПСУ-IP

2. Команду "Настройки СКЗИ" меню настройки системы:



Рисунок 294 - Меню настройки системы ФПСУ-IP

3. Команду "Удаление СКЗИ" меню настройки СКЗИ.



Рисунок 295 - Запуск процедуры удаления СКЗИ

Появится окно с предложением подтвердить полномочия "Администратора" или "Главного администратора".

ВНИМАНИЕ! Сразу после приложения к ТМ-считывателю ФПСУ-IP ТМ-идентификатора, подтверждающего права "Администратора" или "Главного администратора", будет запущен необратимый процесс форматирования внутреннего накопителя!

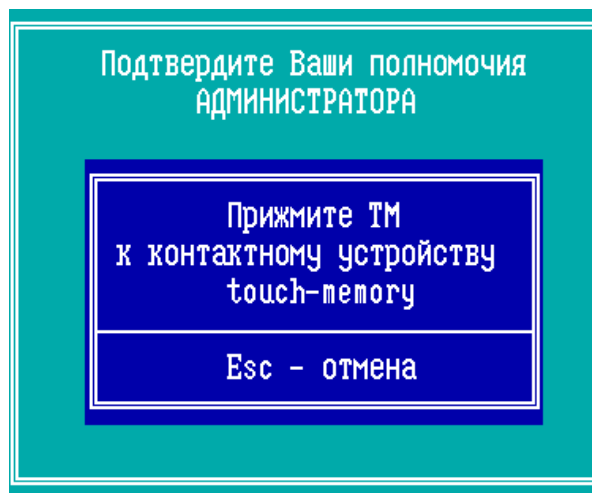


Рисунок 296 - Подтвердите полномочия для удаления СКЗИ

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 ACCESS-TM SHELL, 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/PnP**.

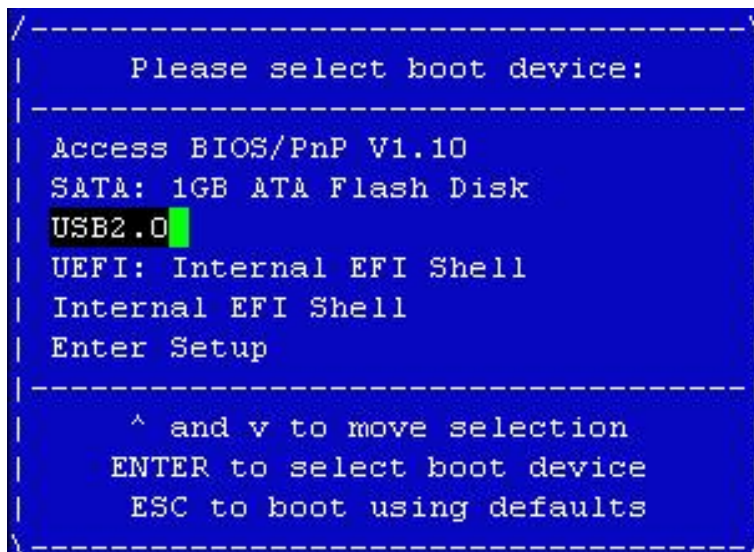


Рисунок 297 - Выбор загрузки с USB

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:

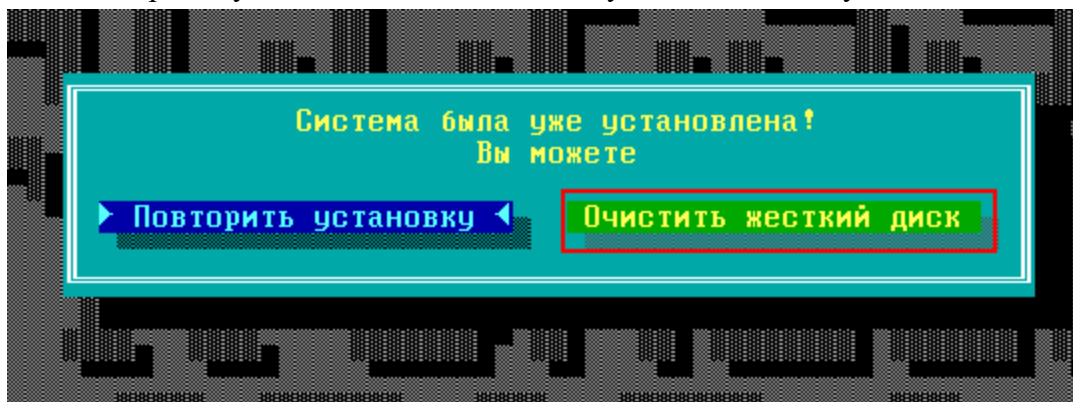


Рисунок 298 - Операционная система ФПСУ-IP уже установлена

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.