ООО «АМИКОН»

УТВЕРЖДЕН

ПЕРС.26.20.40.140.004РА 01-ЛУ

Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» 4.0.2Q

Руководство администратора

ПЕРС.26.20.40.140.004РА 01

Листов 704

2025

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением программных и программно-аппаратных комплексов «Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4» (версия программного обеспечения 4.0.2Q, далее - ФПСУ). В документе содержатся общие сведения о ФПСУ, 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 ФПСУ и требуемый уровень безопасности, является отсутствие ошибок при конфигурировании комплекса. Поэтому конфигурирование ФПСУ 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 ФПСУ для различных сетевых топологий, представленные в разделе «Примеры настройки ФПСУ».

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», 1994-2025. 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 10

2. Общие сведения 13

2.1. Применимость руководства 17
2.2. Принцип действия 19
2.3. Разграничение доступа и пользователи 25
2.4. Ограничения функционала ФПСУ в зависимости от оперативной памяти 28
2.5. ПАК FPSUIP-ORD4-KRK 29
2.5.1. Общая конструкция и назначение органов управления 30
2.5.2. Технические характеристики изделия 32
2.5.3. Указания для правильной и безопасной эксплуатации 33
2.5.4. Способы оценки технического состояния 34
2.5.4.1 Перечень возможных неисправностей и их решение 34
2.5.5. Сведения об утилизации изделия 35
2.6. ПАК FPSUIP-EXT3-KRK-SX-V 35

3. Процедуры приемки и безопасной установки 37

3.1. Общий порядок поставки и комплектность 37
3.2. Правила пользования 37
3.3. Указания для полного или частичного устранения идентифицированных скрытых каналов 49
3.3.1. ISN Evaluation 50
3.3.2. TCP URG Pointer 50
3.3.3. IP ToS Evaluation 51
3.4. Технические условия эксплуатации и хранения 55
3.5. Гарантийные обязательства 57
3.6. Настройки платформ виртуализации 58
3.6.1. Настройка виртуальной машины QEMU/KVM 58
3.6.2. Настройка виртуальной машины VMware 69
3.6.2.1 Настройка порта резервного ФПСУ в VMware 73
3.7. Консольное подключение к ФПСУ 76
3.7.1. Настройки BIOS для консольного подключения 77
3.7.2. Установка драйверов консольного кабеля 79
3.7.3. Подключение к ФПСУ с помощью «Терминала» 86
3.7.4. Авторизация пользователя на ФПСУ 92
3.8. Установка ПО ФПСУ с дистрибутива 95
3.8.1. Установка ПО ФПСУ с установочного носителя 95

3.8.2. Установка ФПСУ с готового образа диска на USB-носителе в QEMU/KVM ... 99
3.9. Технологический режим ФПСУ ... 103
3.9.1. Переход в рабочий режим, перерегистрация основного ТМ, регистрация запасного ТМ ... 108
3.9.2. Инициализация HW аппаратного устройства автозапуска ... 116

4. Запуск и режим фильтрации ФПСУ ... 122

4.1. Запуск ФПСУ в режим фильтрации пакетов ... 125
4.2. Мониторинг аппаратного состояния и суточная статистика ... 127
4.3. Окно справки ... 133
4.4. Меню управления ключами УА ... 136
4.5. Окно состояния рабочих LAN портов ... 138
4.6. Окно состояния ARP-кэша ... 145
4.7. Окно состояния работы пользователей ... 147
4.8. Окно состояния VPN-туннелей с другими ФПСУ ... 153
4.9. Окно состояния связи с удаленными администраторами ... 155
4.10. Окно мониторинга подключенных ФПСУ-IP/Клиентов ... 157
4.11. КРК. Общая статистика ... 159
4.12. Окно состояния подсистемы «горячего» резервирования ... 160
4.13. Информационные окна жидкокристаллического экрана ... 163

5. Контроль целостности программного обеспечения ... 166

5.1. Проверка целостности программных модулей ФПСУ ... 168
5.2. Самотестирование функций межсетевого экрана ФПСУ ... 169

6. Конфигурация ФПСУ ... 171

6.1. Общие параметры конфигурации ФПСУ ... 174
6.2. Установка ключей ... 187
6.3. Использование ключей ... 191
6.4. Конфигурация драйверов сетевых адаптеров ... 192
6.4.1. Агрегированный сетевой адаптер ... 198

7. Настройка системы ... 202

7.1. Окно регистрации ТМ ... 202
7.1.1. Установка пароля Главного администратора ... 206
7.1.2. Повторная регистрация ТМ-идентификатора ... 208
7.1.3. Удаление ТМ ... 212
7.2. Включение автозапуска ФПСУ ... 214
7.3. Установка дополнений/изменений ... 216
7.4. Установка лицензии из USB-ТМ-токена ... 221

7.5. Установка пароля администратора 225
7.6. Установка даты и времени 227
7.7. Регистрация Удаленных Администраторов 229
7.7.1. Регистрация удаленного администратора на ФПСУ 232
7.7.2. Ключи ФПСУ для связи с УА 237
7.8. Параметры «Горячего резерва» 239
7.8.1. Настройка ФПСУ на работу с партнером по резервированию 242
7.8.1.1 Замена ключа горячего резерва 243
7.8.2. Принудительная синхронизация данных 249
7.8.3. Параметры проверки линий связи для портов ФПСУ 250
7.8.3.1 Интерфейс настройки проверки линий связи 251
7.8.3.2 Пример работы системы проверки связи 254
7.9. Настройки СКЗИ 258
7.9.1. Отключение автозапуска 259
7.9.2. Переинициализация ключа ПДСЧ 261
7.9.3. Переинициализация дополнительного ключа ПДСЧ для КРК 263
7.9.4. Загрузка ключа ПДСЧ из файла 266
7.9.5. Установка срока действия ключей 269

8. Порты ФПСУ 273

8.1. Описание основных настроек порта 275
8.2. Описание VLAN и IP-адресов порта 277
8.3. Описание маршрутизации порта 280
8.3.1. Описание параметров используемых маршрутизаторов 282
8.3.2. Описание параметров туннелей с другими ФПСУ 285
8.3.2.1 Дополнительные параметры соединения ФПСУ-ФПСУ 289
8.3.2.2 Потоки данных в туннеле между ФПСУ 292
8.3.2.3 Режим «Мост» между ФПСУ (L2-шифрование) 302
8.3.2.4 Динамические ФПСУ 305
8.3.2.5 Описание туннеля типа IPIP 307
8.3.3. Описание параметров абонентов 308
8.3.3.1 Описание абонента «Хост» 310
8.3.3.2 Описание абонента «Подсеть» 316
8.3.3.3 Описание абонента «Любой Хост» 319
8.3.3.4 Работа со списком абонентов 321
8.4. Динамическая маршрутизация 325
8.4.1. Динамическая маршрутизация OSPF 326
8.4.1.1 Настройки 328
8.4.1.2 Области 330

8.4.1.3 Интерфейсы и туннели 333
8.4.1.4 Отладка 339
8.4.2. Динамическая маршрутизация BGP 341
8.4.2.1 General 343
8.4.2.2 Networks 345
8.4.2.3 Peers 346
8.4.2.4 Prefix-list 349
8.4.2.5 Route Map-list 351
8.4.2.6 AS Path-list 356
8.4.2.7 Community-list 357

9. Параметры доступа, правила трафика межсетевого экрана 361

9.1. Правила трафика 363
9.1.1. Общие настройки правил трафика 366
9.1.2. Вкладки «Источник» и «Назначение» правил трафика 369
9.1.3. Службы в правилах трафика 373
9.2. Службы 376
9.2.1. Протокол ICMP в службах 379
9.2.2. Служба для запрета фрагментированных пакетов 381
9.2.3. Протокол REGEXP в службах 382
9.2.4. Признак VLAN в службах 389
9.3. Управление полосой пропускания 390
9.4. Фильтрация трафика по содержимому (DPI) 394
9.4.1. Создание правила фильтрации по содержимому и его общие настройки 396
9.4.2. Исследуемый правилом фильтрации трафика по содержимому протокол 398
9.4.3. Дополнительные фильтры для протокола http 401
9.4.4. Службы в правилах фильтрации трафика по содержимому 405
9.5. Маршрутизация на основе политик 406
9.6. Интервалы времени 411
9.7. Группы IP-адресов 413
9.8. Дополнительные параметры и защита от flood-атак 416

10. Подсистемы и дополнения ФПСУ 424

10.1. Дополнения 426
10.1.1. Дополнение frr 427
10.1.2. Дополнение rkl 429

11. Квантовое распределение ключей 432

11.1. Общая схема построения квантовой сети 435
11.2. Установка дополнений для работы с СВКРК 437
11.2.1. Установка дополнения option_krk_pdu 438
11.3. Взаимодействие СВКРК и ФПСУ 442
11.3.1. Стандартные сетевые параметры СВКРК 442
11.3.2. Настройка СВКРК на сетевых адаптерах ФПСУ 443
11.4. Настройка квантовых туннелей 446
11.4.1. Настройка квантового распределения ключей на ФПСУ 446
11.4.2. Настройка служебного туннеля 455
11.4.3. Настройка квантово-сервисного туннеля 457
11.4.4. Настройка комбинированного туннеля 459
11.4.5. Настройка квантово-защищенного туннеля 462
11.4.6. Установка предраспределенных ключей для участников квантовой сети 464
11.4.7. Управление Модулем КРК 466

12. Клиенты ФПСУ 468

12.1. Клиент для ФПСУ 468
12.1.1. Установка и удаление общесистемных ключей 471
12.1.2. Описание логической группы клиентов 472
12.1.3. Установка правил работы клиентов 475
12.1.4. RKL для обновления ключевых данных клиентов 485
12.1.4.1 Настройка диапазона клиентов на работу с RKL 488
12.1.4.2 Настройка диапазона клиентов на работу с Сервером лицензирования 491
12.1.4.3 Серверы ЦРМК и Сервер лицензирования 494
12.1.5. Настройка правил работы отдельного клиента 495
12.2. Настройка диапазона клиентов на работу с Radius 499
12.3. Балансировка нагрузки Клиентов 502
12.4. Балансировка нагрузки Клиентов на основе единого IP-адреса 504

13. Сетевые сервисы 508

13.1. Общие правила разделения потоков 508
13.2. Учет трафика IPFIX 512
13.2.1. Отвергнутый трафик 515
13.2.2. Разрешенный трафик 516
13.2.3. Трафик с NAT 521
13.3. SNMP-клиент на ФПСУ 527
13.4. Syslog-клиент на ФПСУ 532
13.4.1. Настройка SysLog событий ФПСУ 533

13.4.2. Опции работы с SysLog сервером 543
13.4.3. Формат отправляемых SysLog сообщений 546
13.5. DNS-серверы 553
13.6. DHCP-сервер и DNS-Relay 555
13.7. DHCP-Relay 559
13.7.1. Создание списка DHCP-серверов 559
13.7.2. Настройка DHCP-Relay на портах ФПСУ 562
13.8. Http-proxy ФПСУ 564
13.8.1. Авторизация на http-proxy 566
13.9. Взаимодействие со средствами обнаружения вторжений 570
13.10. NTP-клиент ФПСУ 573
13.11. Особенности реализации ICMP протокола 575
13.12. RADIUS 577
13.12.1. Настройка RADIUS-серверов на ФПСУ 579
13.12.2. Спецификация реализации RADIUS на ФПСУ 583
13.13. Поддержка Wake-on-Lan 588
13.14. Служебные протоколы и порты на ФПСУ 589

14. Статистика ФПСУ 591

14.1. Просмотр статистики 591
14.2. Выдача системного журнала 594
14.3. Выдача журнала изменений конфигурации межсетевого экрана 596
14.4. Ограничение сбора статистики 599

15. Восстановление работы ФПСУ после сбоев 603

16. Примеры настройки ФПСУ 605

16.1. Базовая настройка ФПСУ для ретрансляции пакетов локальной сети 606
16.2. Защита локальной сети, состоящей из двух IP-подсетей 608
16.3. Разделение подсети на два фрагмента ФПСУ на уровне маршрутизации 611
16.4. Использование ФПСУ для создания VPN-туннелей 614
16.4.1. Использование раздельных VPN-туннелей 616
16.4.2. Использование совмещенных VPN-туннелей 621
16.5. Использование ФПСУ в режиме моста (L2 шифрование) 625
16.6. Каскадная схема установки ФПСУ в локальной сети 627
16.7. Использование ФПСУ для контроля доступа в интернет с NAT 636
16.8. Использование ФПСУ для контроля доступа ФПСУ-IP/Клиентов 639
16.9. Использование ФПСУ для объединения офисов с одинаковой внутренней адресацией 644

16.10. Использование ФПСУ для смены порта назначения трафика, направляемого в адрес абонента 650
16.11. Использование ФПСУ для балансировки нагрузки на порты внутреннего сервера 653
16.12. Использование ФПСУ на медленных каналах. Спутник, spoofing 657
16.13. Применение prefix-list в протоколе BGP 662

17. Способы разрешения возможных проблем при работе ФПСУ 665

17.1. Первый запуск ФПСУ 665
17.2. Устранение неполадок, связанных с работой сетевого оборудования 666

18. Диагностика ошибок ФПСУ 668

18.1. Выдача файла Kmsg 679
18.2. Выдача файла отладки OSPF 681
18.3. Диагностика ошибок с помощью mlog 682
18.4. Дампы 686

19. Удаление программного обеспечения ФПСУ 688

19.1. Удаление СКЗИ 688
19.2. Удаление ПО с помощью USB-носителя со средством восстановления 691
19.3. Удаление экземпляра СКЗИ с USB-носителя в ОС Windows 693
19.4. Удаление экземпляра СКЗИ с USB-носителя в ОС Ubuntu 700

1. Список используемых сокращений и определений

АРМ УА ФПСУ, АРМ УА	автоматизированное рабочее место удаленного администратора ФПСУ, программный комплекс «Удаленный администратор "ФПСУ-IP"»
АПМДЗ	Аппаратный модуль доверенной загрузки
БиоДСЧ	Биологический датчик случайных чисел
Клиент PKI	программный комплекс «ФПСУ Клиент PKI»
МЭ	межсетевой экран
НСД	несанкционированный доступ к информации
ПДСЧ	программный датчик случайных чисел
ПЗУ	постоянное запоминающее устройство ФПСУ, твердотельный накопитель SSD (solid-state drive)
ПО	программное обеспечение
СВКРК, ККС ВРК	система выработки квантового распределения ключей (квантовая криптографическая система выработки и распределения ключей), реализующая использующий квантовые явления метод распределения симметричных ключей между узлами сети связи
СВКРК-А	устройство квантовой криптографической системы выработки и распределения ключей разработки ООО «СМАРТС-Кванттелеком», модуль-отправитель фотонов (подробнее см. https://quanttelecom.ru)
СВКРК-Б	устройство квантовой криптографической системы выработки и распределения ключей разработки ООО «СМАРТС-Кванттелеком», модуль-получатель фотонов (подробнее см. https://quanttelecom.ru)
Сервер лицензирования	программный комплекс «Сервер лицензирования комплексов «ФПСУ-IP/Клиент» разработки ООО «АМИКОН», реализующий сетевой сервис выдачи и учета лицензий Клиентам ФПСУ
Сертификат	Сертификат открытого ключа – электронный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу
СЗИ НСД	система защиты информации от несанкционированного доступа

СКЗИ	средство криптографической защиты информации
ТМ, ТМ-идентификатор	электронный идентификатор «touch-memory»: микроэлектронное USB-устройство «TM-Key» производства ООО «АМИКОН» (ПЕРС.466226.004, ПЕРС.466226.005, ПЕРС.466226.008, ПЕРС.466226.009) или iButton DS1993 – DS1996
УЦ	Удостоверяющий центр – доверенная третья сторона, ответственная за выдачу и отзыв сертификатов, издает сертификат открытого ключа пользователя на определенный срок и подтверждает, что конкретному пользователю принадлежит открытый ключ и соответствующий ему закрытый ключ
ФПСУ (ФПСУ-IP)	Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4, программный или программно-аппаратный комплекс, программная компонента которого является средством криптографической защиты информации «ФПСУ-IP Amigo» (модификацией 4.0.2Q варианта исполнения «ФПСУ-IP Q КС1», «ФПСУ-IP Q КС2» или «ФПСУ-IP Q КС3»).
ФПСУ-IP ULT 10G	программно-аппаратный комплекс ФПСУ на основе аппаратной платформы семейства ULT, обеспечивающий скорость шифрования не менее 10 Гбит/сек.
ФПСУ-IP STD3	программно-аппаратный комплекс ФПСУ на основе аппаратной платформы FPSUIP-STD3, обеспечивающий скорость шифрования не менее 150 Мбит/сек.
ЦВК	программно-аппаратный комплекс «Центр выработки ключей»
ЦГКК	программное обеспечение «Центр генерации ключей клиентов»
ЦПУ	центральное процессорное устройство, процессор
Хост	узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую
ARP	«Address Resolution Protocol», протокол для отображения IP-адреса рабочей станции сети по ее аппаратному адресу
DC	«Domain Controller», контроллер домена
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
OCSP	«Online Certificate Status Protocol», протокол состояния сетевого сертификата
PKI	«Public Key Infrastructure», инфраструктура открытых ключей
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

2. Общие сведения

Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4 (ФПСУ - сокращенное название от «фильтр пакетов сетевого уровня») является средством защиты от несанкционированного доступа к информации.

ФПСУ выпускается в программном и программно-аппаратном исполнениях.

ФПСУ позволяет выделять в открытой сети защищаемые области с ограниченным доступом, а также обеспечивать защищенную передачу данных между такими областями.

ФПСУ обеспечивает шифрование и имитозащиту IP-трафика, проходящего через общедоступные сети передачи данных, в соответствии с:

- ГОСТ 28147–89 «Системы обработки информации. Защита криптографическая»;
- ГОСТ 34.12–2018 «Информационная технология. Криптографическая защита информации. Блочные шифры»;
- ГОСТ 34.13–2018 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров»;
- Р 1323565.1.026–2019 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров, реализующие аутентифицированное шифрование»;
- ГОСТ Р 34.11–2012 «Информационная технология. Криптографическая защита информации. Функция хэширования».

ФПСУ обеспечивает организацию служебного канала для квантовых криптографических систем выработки и распределения ключей, получение квантовых ключей от квантовых криптографических систем выработки и распределения ключей и распределение квантово-защищенных ключей в соответствии с:

- Р 1323565.1.029–2019. «Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем»;
- Р 1323565.1.046–2023. «Информационная технология. Криптографическая защита информации. Защищенный протокол взаимодействия квантово-криптографической аппаратуры выработки и распределения ключей и средства криптографической защиты информации»;
- РОФ.ПЕРС.00113-01 91 01. «Профиль протокола ProtoQa, применяемый при взаимодействии вариантов исполнений «ФПСУ-IP Q КС1», «ФПСУ-IP Q КС2», «ФПСУ-IP Q КС3» СКЗИ «ФПСУ Amigo» с СКЗИ-распределителями и/или СКЗИ-потребителями в рамках передачи квантово-защищенных ключей» (далее «Профиль № 1»).

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

ФПСУ подключается в сеть передачи данных таким образом, чтобы входящие и исходящие из защищаемой сети межсетевые потоки данных проходили через ФПСУ. Подключение может быть физическое (в случае программно-аппаратного исполнения) или логическое (в случае программного исполнения для виртуальных машин).

Основными функциями ФПСУ являются ***фильтрация*** передаваемых данных, заключающаяся в анализе их по совокупности критериев и принятии решения о возможности их дальнейшей передачи (с ***регистрацией*** результатов фильтрации), и ***установка VPN-туннелей с другими ФПСУ*** для организации защищенной передачи данных.

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

VPN-туннели также могут быть образованы между ФПСУ и рабочими станциями, оснащенными комплексами «ФПСУ-IP/Клиент». Решение предназначено для защиты межсетевого взаимодействия удаленных рабочих станций и защищаемой IP-сети. Для формирования туннелей на ФПСУ 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 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 реализован ряд дополнительных возможностей, в частности:

- возможность безопасного дистанционного контроля и управления работой из любого фрагмента IP-сетей, которая может быть предоставлена нескольким (максимально 128) зарегистрированным на ФПСУ удаленным администраторам;
- использование технологии DPI (Deep Packet Inspection) для анализа содержимого передаваемых данных;
- встроенный HTTP- и SOCKS-proxy;
- возможность разделения общего потока отправляемых через VPN-туннель данных по заданным администратором критериям. 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 могут работать в режиме горячего резервирования. В режиме горячего резервирования оба ФПСУ 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 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 или при возникновении аппаратных неполадок на активном, резервный ФПСУ в течение 3 секунд берет управление на себя. Передача функций резервному ФПСУ может также осуществляться вручную, по команде локального или удаленного администратора.

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

Программное обеспечение ФПСУ 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. на деятельность по разработке и(или) производству средств защиты конфиденциальной информации и №0536 от 21 ноября 2006 г. на деятельность по технической защите конфиденциальной информации).

ФПСУ поставляется в соответствии с формуляром на модификацию 4.0.2Q вариантов исполнений «ФПСУ-IP Q КС1», «ФПСУ-IP Q КС2», «ФПСУ-IP Q КС3» средства криптографической защиты информации «ФПСУ-IP Amigo».

ФПСУ следует использовать в соответствии с правилами пользования модификациями 4.0.2Q вариантов исполнений «ФПСУ-IP Q КС1», «ФПСУ-IP Q КС2», «ФПСУ-IP Q КС3» средства криптографической защиты информации «ФПСУ-IP Amigo».

СКЗИ«ФПСУ-IP Amigo» разработано ООО «АМИКОН».

СКЗИ «ФПСУ-IP Amigo» удовлетворяет:

- «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» для классов КС1, КС2 и КС3 в соответствии со следующей таблицей:

Класс	**Вариант исполнения**
КС1	«ФПСУ-IP Q КС1»
КС2	«ФПСУ-IP Q КС2»
КС3	«ФПСУ-IP Q КС3»

- «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации (СТ-Р)» по уровню $КС_{Б}$;
- «Требованиям по защите линейной передачи средств криптографической защиты информации, не содержащей сведений, составляющих государственную тайну» по уровню защищенности $КС_{Б}$. имеет сертификат соответствия требованиям ФСБ России к шифровальным (криптографическим) средствам класса КС1, КС2 и КС3.

2. 1. Применимость руководства

Руководство предназначено для работы с версией 4.0.2Q программного обеспечения ФПСУ и распространяется на следующие указанные в таблице варианты поставки изделия и дополнительные программные модули.

Таблица 1. Варианты поставки изделия

Код варианта изделия	**Наименование варианта изделия/дополнительного программного модуля**
FPSUIP-ORD3-KRK	«Программно-аппаратный комплекс "ФПСУ-IP" в компактном корпусе, подготовленный для работы с устройствами Квантового Распределения Ключей»
FPSUIP-ORD4-KPK	«Программно-аппаратный комплекс "ФПСУ-IP" на базе российской аппаратной платформы в компактном корпусе, подготовленный для работы с устройствами Квантового Распределения Ключей»
FPSUIP-STD3-KRK	«Программно-аппаратный комплекс "ФПСУ-IP" на базе аппаратной платформы типоразмера 1U, подготовленный для работы с устройствами Квантового Распределения Ключей»
FPSUIP-EXT3-KRK-SX	«Программно-аппаратный комплекс "ФПСУ-IP" 1G повышенной производительности с 7 активированными дополнительными вычислительными потоками, с 4 дополнительными оптическими интерфейсами 1000BASE-SX, подготовленный для работы с устройствами Квантового Распределения Ключей»
FPSUIP-ULT-1U-10G-KRK-SR	«Программно-аппаратный комплекс "ФПСУ-IP" 10G на базе многопроцессорной аппаратной платформы типоразмера 1U с 2 дополнительными оптическими портами 10GBASE-SR, подготовленный для работы с устройствами Квантового Распределения Ключей»

Код варианта изделия	**Наименование варианта изделия/дополнительного программного модуля**
FPSUIP-ULT5-2U-10G-KRK	«Программно-аппаратный комплекс "ФПСУ-IP" 10G на базе многопроцессорной аппаратной платформы типоразмера 2U с 16 оптическими сетевыми интерфейсами 1/10 Gb SR и 6 интерфейсами 1Gb UTP, подготовленный для работы с устройствами Квантового Распределения Ключей»
FPSUIP-ULT6-10G-KRK	«Программно-аппаратный комплекс "ФПСУ-IP" максимальной производительности на базе аппаратной платформы ULT6-10G, подготовленный для работы с устройствами Квантового Распределения Ключей»
FPSUIP-SUB3-KRK-PDU	Модуль-агент поддержки взаимодействия с устройствами КРК шифрования в качестве сервера промежуточного доверенного узла (ПДУ)

Таблица 2. Варианты поставки изделия. Модуль-агенты

Код варианта изделия	**Наименование варианта изделия/дополнительного программного модуля**
FPSUIP-SUB4-CLIENT	«Встраиваемый в комплекс "ФПСУ-IP" версии 4 (Amigo) категорий STD и EXT модуль-агент подсистемы поддержки клиентов»
FPSUIP-SUB4-CLIENT-ULT	«Встраиваемый в комплекс "ФПСУ-IP" версии 4 (Amigo) категории ULT модуль-агент подсистемы поддержки клиентов»
FPSUIP-SUB4-CLIENT-ULT10G	«Встраиваемый в комплекс "ФПСУ-IP" версии 4 (Amigo) категории ULT10G модуль-агент подсистемы поддержки клиентов»
FPSUIP-SUB4-PUNIT1	«Встраиваемый в комплекс "ФПСУ-IP" версии 4 (Amigo) категорий ORD, STD, EXT, ULT модуль-агент активации дополнительного вычислительного потока»

Код варианта изделия	**Наименование варианта изделия/дополнительного программного модуля**
FPSUIP-SUB4-CLIENT-SOFT-ADD	«Встраиваемый в комплекс "ФПСУ-IP" версии 4 (Amigo) модуль-агент активации программных клиентов "ФПСУ-IP/Клиент"»

2. 2. Принцип действия

ФПСУ подключается в сеть передачи данных между защищаемой областью и остальной частью сети таким образом, чтобы все входящие и исходящие из области потоки данных проходили через ФПСУ. Если защищаемая область связана с остальной сетью передачи данных более чем в одной точке (транзитная область), ФПСУ следует устанавливать на каждом выходе из неё.

Вследствие поддержки программным обеспечением ФПСУ режима «ARP-proxy» включение его в сеть не требует изменения её топологии или изменения конфигурационной информации уже существующей в сети аппаратуры, и не имеет ограничений на размер защищаемой области.

Основные функции ФПСУ:

- VPN-построитель: установка защищенных туннелей с другими ФПСУ для организации безопасной передачи данных через сети, которым нет доверия;
- межсетевой экран - в соответствии с установленными администратором правилами ФПСУ анализирует входящие и исходящие пакеты данных IP-протокола по совокупности критериев, осуществляет контроль доступа к ресурсам сети и определяет возможность передачи данных.

При этом в таких туннелях обеспечиваются:

- начальные идентификация и аутентификация взаимодействующих ФПСУ;
- сеансовые идентификация и аутентификация взаимодействующих ФПСУ;
- идентификация, аутентификация и контроль целостности принимаемых по туннелю данных;
- шифрование и инкапсуляция IP-в-IP отфильтрованных пакетов, обеспечивающее сокрытие сетевых адресов отправителя и получателя, номеров IP-протоколов и других полей IP-пакетов, а также защиту передаваемых данных от прочтения, искажения и подмены.

На начальном этапе анализа все пакеты, поступающие на каждый из интерфейсов ФПСУ, контролируются на предмет корректности их формата и соответствия стандартам стека IP-протоколов. Если начальная обработка пакета осуществлена успешно, пакет будет передан для анализа в подсистему фильтрации ФПСУ.

Фильтрация пакетов IP-протокола, производимая ФПСУ, заключается в сопоставлении полей IP-пакета установленным администратором правилам. На основании произведенного анализа принимается решение о допустимости дальнейшей передачи пакета абоненту-получателю, о необходимости дальнейшей идентификации и аутентификации пакета, а также о методах передачи данных и способах контроля за процессом приёма/передачи данных.

Применяемый ФПСУ механизм контроля передачи пакетов на сетевом уровне позволяет задавать в качестве критериев фильтрации:

- регистрационные данные комплексов ФПСУ-IP/Клиент;
- IP-адреса и MAC-адреса отправителя и получателя;
- день недели и время соединения;
- используемые протоколы транспортного уровня;
- используемые порты TCP и UDP соединений;
- разрешённые режимы работы абонентов (см. ниже);
- разрешённые парные связи абонентов и ФПСУ-IP/Клиентов.

В зависимости от топологии сети и от требований политики безопасности организации возможны варианты применения ФПСУ (функциональные схемы основных вариантов приведены ниже) и различные режимы его работы.

В простейшем случае обмен IP-пакетами абонентов сегмента ЛВС с другими абонентами может осуществляться через один ФПСУ. Для защищаемой области достаточно установить один ФПСУ на выходе из неё.

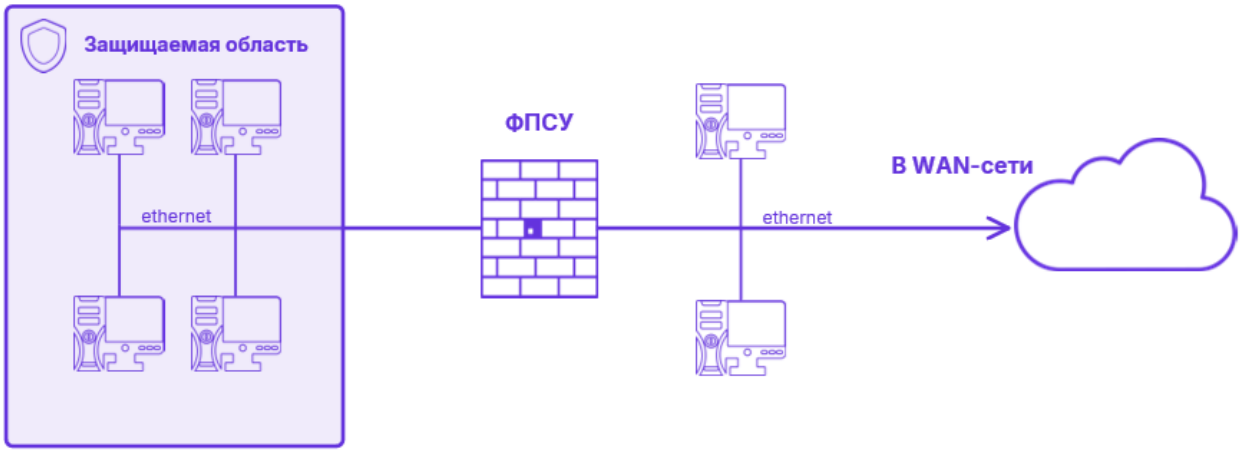


Рисунок 1 - Функциональная схема использования одного ФПСУ для защиты области

Таким образом, из локальной сети выделяется группа абонентов (защищаемая область), для которых обмен IP-пакетами с остальными абонентами сети может быть специальным образом регламентирован и проконтролирован. Применяя ФПСУ по этой схеме, можно разделить локальную сеть на две части (не меняя при этом IP-адресов и установок сетевого программного обеспечения хостов), одна из которых защищена, а абонентам другой будет разрешён обычный обмен пакетами. По этой же схеме можно установить ФПСУ на выходе из локальной сети в удаленные сети и защитить работу всей локальной сети.

Если обмен пакетами абонентов будет производиться через один ФПСУ, может быть реализован только самый слабый уровень защиты, так называемый режим ретрансляции, при котором будут задействованы только механизмы фильтрации пакетов по различным критериям.

Более высокий уровень защиты возможен при обмене пакетами через два аналогичных ФПСУ, работающих в паре. В этом режиме включаются механизмы аутентификации абонентов защищённых сегментов ЛВС и трансляции их сетевых адресов, скрывающей внутренние адреса субъектов и объектов передачи, а также используемых ими сетевых протоколов и прикладных функций защищаемой сети. Кроме того, в таком режиме могут быть использованы механизмы сжатия и шифрования.

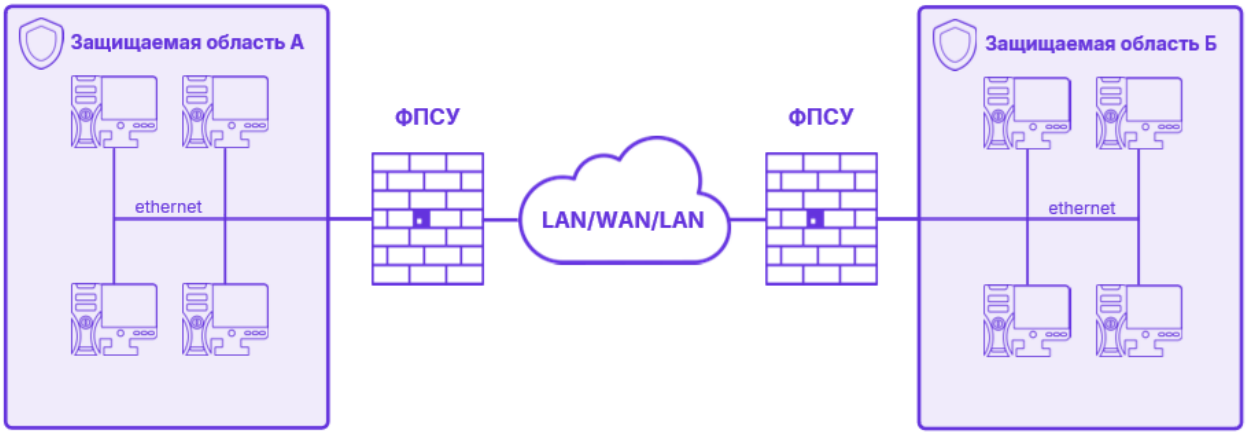


Рисунок 2 - Функциональная схема использования двух ФПСУ, работающих в паре

Данная схема применения позволяет задействовать весь предоставляемый комплексом набор средств защиты от НСД. Однако она не может обеспечить полную безопасность обмена пакетами в случае, если для некоторых абонентов защищаемых областей разрешены открытые соединения (через один ФПСУ в режиме ретрансляции без аутентификации) с абонентами или сетевыми службами через глобальную сеть.

Если открытые соединения всё же необходимы для доступа к разнообразным утилитам и сервисам Интернет, обеспечить безопасность защищаемой области можно следующими способами:

- вынести за границы защищаемой области специально выделенный хост (хосты), с которого (которых) будет осуществляться обычная работа по Интернет, а остальным абонентам в конфигурации комплекса установить режим работы через удаленный ФПСУ;
- на ФПСУ, разрешающем некоторым абонентам открытые соединения, создать логическую группу, к которой будут приписаны абоненты с указанными явно адресами, а на компьютерах этих абонентов принять меры по предотвращению запуска программ или фрагментов кода, принятых из сети;
- отделить особо важные хосты в защищаемой оконечной области ещё одним ФПСУ, работающим в «каскадном» режиме с первым, причём на втором ФПСУ должны быть запрещены все открытые соединения. Таким образом, локальная сеть будет разделена на две части, имеющие различный уровень защиты (см. рисунок ниже).

Каскадная установка нескольких ФПСУ и запрет открытых соединений на последнем комплексе создают максимальный уровень защиты для оконечной области (область А, рисунок ниже), предоставляя доступ к ней только аутентифицированным абонентам. При этом подсистема фильтрации создаёт достаточно высокий уровень защиты от НСД и для абонентов транзитной защищаемой области В, позволяя им осуществлять соединения с

абонентами других сетей (не защищённых) через глобальную сеть. Обратите внимание, что для абонентов оконечной области фильтрация пакетов по всем заданным критериям будет производиться только ближайшим комплексом, а транзитный ФПСУ будет фильтровать пакеты только по IP-адресам.

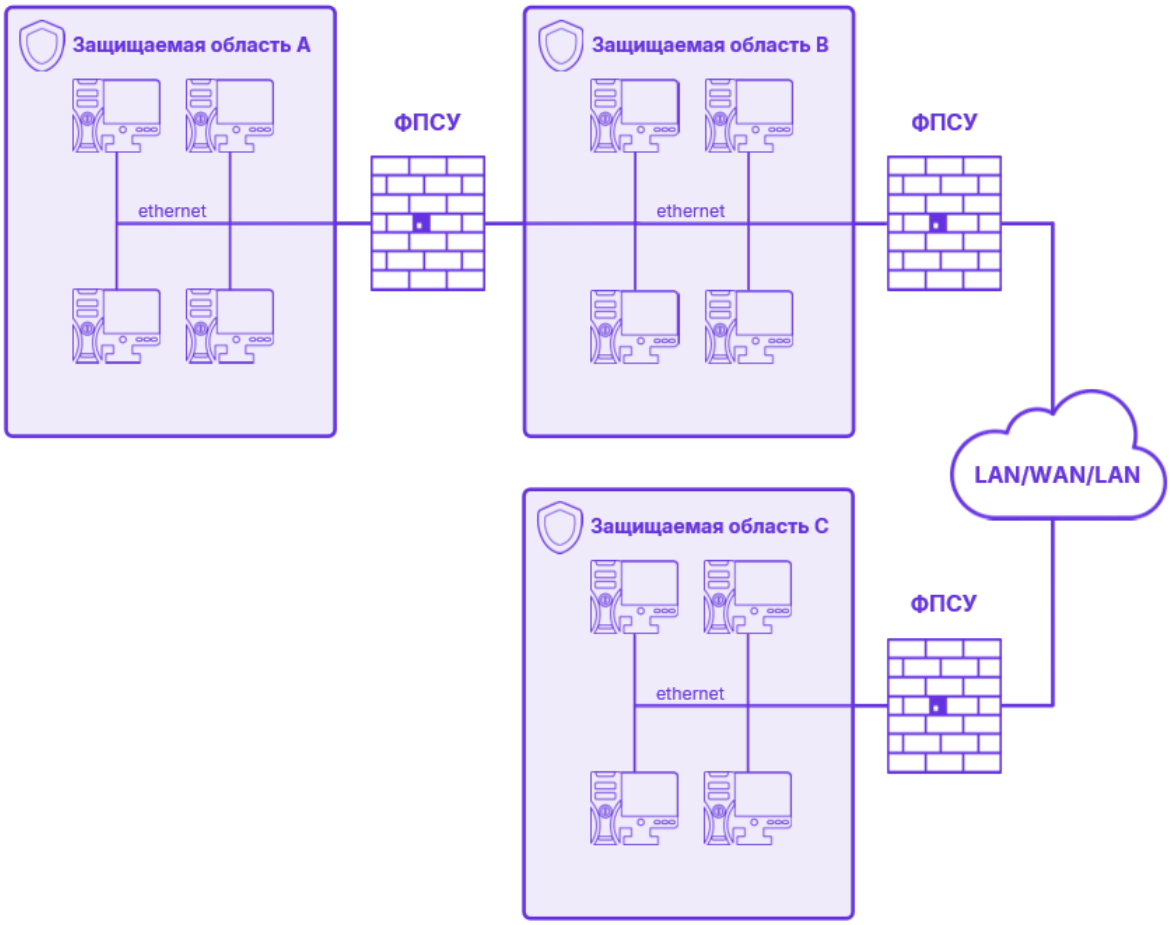


Рисунок 3 - Каскадная установка двух ФПСУ в защищаемой области

ФПСУ может применяться не только для организации безопасного взаимодействия IP-подсетей, но и для защиты межсетевого обмена отдельных рабочих станций и устройств, на которых установлен программный или программно-аппаратный комплекс ФПСУ-IP/Клиент. При этом ФПСУ может использоваться как для безопасного доступа пользователей ФПСУ-IP/Клиентов из открытых сетей в защищаемую им подсеть, так и для организации VPN-соединений ФПСУ-IP/Клиентов друг с другом.

Каждый из ФПСУ-IP/Клиентов работает с ФПСУ в режиме «клиент/сервер», посылая запрос на доступ, который производится ФПСУ только после идентификации и аутентификации. Для передачи данных между ФПСУ-IP/Клиентом и ФПСУ организуется защищённый межсетевой VPN-туннель, в котором производится шифрование информации и

(опционально) сжатие.

На схеме (см. рисунок ниже), ФПСУ обеспечивает пользователям ФПСУ-IP/Клиентов A и B безопасный доступ к абонентам защищаемой им подсети. Взаимодействуя через ФПСУ друг с другом, ФПСУ-IP/Клиенты A и B образуют VPN-подсеть в открытых сетях, а ФПСУ-IP/Клиенты C и D - VPN-подсеть внутри защищённого фрагмента. Каждый из ФПСУ-IP/Клиентов A и B может также образовывать VPN-соединения через ФПСУ с ФПСУ-IP/Клиентами C и D.

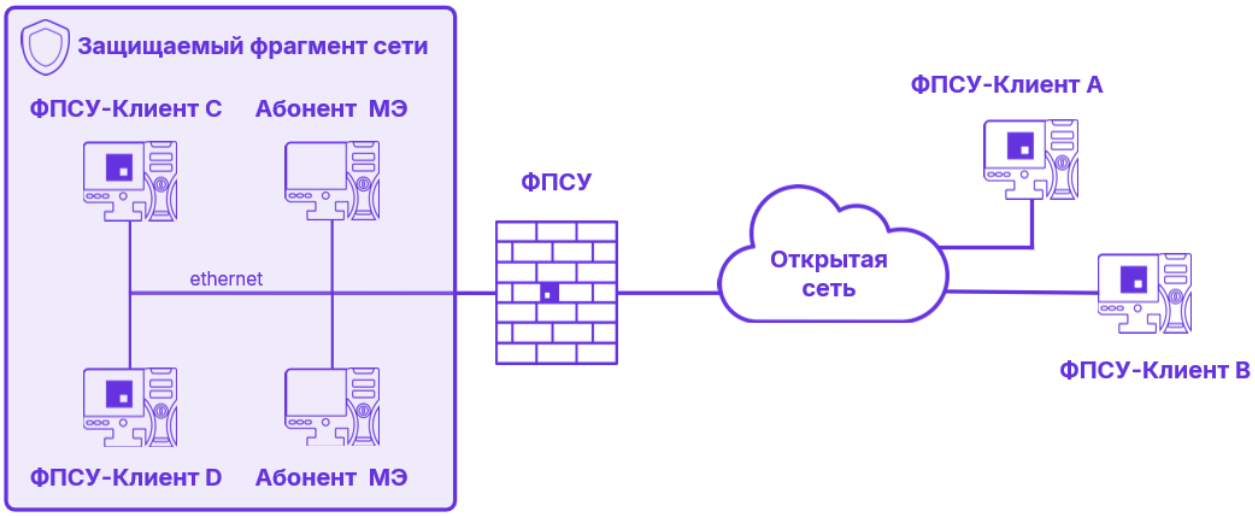


Рисунок 4 - Схема некоторых вариантов применения ФПСУ для организации безопасного взаимодействия рабочих станций, оборудованных ФПСУ IP/Клиентами

В процессах идентификации, аутентификации и фильтрации запросов ФПСУ-IP/Клиентов участвуют не их IP-адреса, а ключевые данные пользователя ФПСУ-IP/Клиента, которые выдаются пользователям с помощью программы ЦГКК. Поэтому доступ ФПСУ-IP/Клиентов к защищаемым ФПСУ рабочим станциям может быть реализован с произвольной рабочей станции, оборудованной ФПСУ-IP/Клиентом (более подробную информацию см. в руководстве пользователя ФПСУ-IP/Клиента).

ФПСУ имеет средства защиты от вмешательства в логику его работы, а также защиты его информационной и программной частей от несанкционированного доступа. Программно-аппаратный комплекс ФПСУ не может содержать постороннего программного обеспечения.

Специальная подсистема ФПСУ реализует в изолированную и функционально замкнутую программную среду, предоставляя администраторам возможность управлять его работой - конфигурировать его (устанавливать и редактировать правила фильтрации, настраивать на ФПСУ параметры сетевого оборудования, подключать желаемое

оборудование и специальное программное обеспечение и т.д.), а также просматривать и записывать на съемные носители регистрационную информацию.

ФПСУ осуществляет и разграничивает доступ к своим модулям и подсистемам администраторов по правам (см. пункт «Разграничение доступа и пользователи»).

При работе ФПСУ информация о его работе и происходящих событиях регистрируется - накапливается в специальном хранилище для последующего просмотра и обработки администраторами, а также отображается на экране монитора (в частности, результат фильтрации и попытки нарушения правил фильтрации).

Хранилище регистрационной информации защищается от НСД посредством доступа к нему по предъявлению ТМ-идентификатора соответствующего класса и невозможности изъятия данных (за исключением автоматического вытеснения начальных записей при переполнении). Во избежание потерь регистрационной информации её можно снимать на внешние носители или выгружать в АРМ УА ФПСУ для последующего хранения или анализа.

ФПСУ укомплектован подсистемой автозапуска, предназначенной для автоматического возобновления работы подсистемы фильтрации после сбоев электропитания в отсутствие оператора. Подсистема автозапуска настраивается и разрешается к применению пользователем ФПСУ с полномочиями «Администратор» или «Главный администратор».

В ФПСУ реализована возможность дистанционного контроля и управления работой группы ФПСУ удаленным администратором, который работает с ними по принципу «Клиент-Сервер». Дистанционное управление работой ФПСУ производится через специализированные защищённые межсетевые туннели и осуществляется посредством:

- настройки на ФПСУ подсистемы удаленного управления и контроля;
- использования программного комплекса «Удаленный администратор ФПСУ».

Доступ к ФПСУ могут получить до ста двадцати восьми (128) различных удаленных администраторов, зарегистрированных на этом ФПСУ локальным администратором с фиксированным набором прав на контроль и управление данным ФПСУ.

2. 3. Разграничение доступа и пользователи

Программное обеспечение ФПСУ функционирует в собственной изолированной и функционально замкнутой операционной среде. Среда осуществляет разграничение доступа к операционной системе ФПСУ, защиту программных и информационных модулей на ПЗУ комплекса.

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

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

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

Кроме того, вход может быть защищен паролем подключаемого ТМ. В этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Таблица 3. Роли и классы пользователей ФПСУ

Роль/Класс	Разрешенные действия
Пользователь/ Оператор	• запуск ФПСУ; • просмотр экранов мониторинга рабочего режима ФПСУ; • остановка рабочего режима ФПСУ; • 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 по кнопке «Power».
Администратор/ Инженер	Все права класса *Оператор* и дополнительно: • переинициализация ПДСЧ; • загрузка ключа ПДСЧ из файла; • конфигурирование сетевых адаптеров;

Роль/Класс	Разрешенные действия
	• конфигурирование IP-адресов портов ФПСУ; • установка даты и времени; • контроль целостности исполняемых программных модулей ФПСУ (только по хранящимся на ФПСУ контрольным суммам с выводом результата на экран); • запуск процесса функционального самотестирования межсетевого экрана ФПСУ; • сохранение текущей конфигурации ФПСУ на USB-flash; • настройка общих параметров работы ФПСУ (watchdog, аварийный перезапуск, переход на резервный, гашение экрана, запрет работы при сбоях жесткого диска, не сообщать об устаревших ключах, контроль сети); • просмотр регистрационной информации (статистики).
Администратор/ Администратор	Все права класса *Инженер* и дополнительно: • отключение автозапуска; • восстановление с USB-носителя и редактирование конфигурации ФПСУ; • включение режима «Запрет открытых соединений» в общих параметрах работы ФПСУ; • регистрация и предоставление полномочий на определенные действия удаленным администраторам; • регистрация, проверка и удаление ТМ-идентификаторов; • установка пароля ТМ Главного администратора; • настройка подсистемы автозапуска; • 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 срока действия ключей; • контроль целостности исполняемых программных модулей ФПСУ (без ограничений на варианты проверки); • установка изменений и дополнений к программным модулям

Роль/Класс	Разрешенные действия
	ФПСУ; • контроль целостности конфигурации ФПСУ.
Администратор/ Главный администратор	Все права класса *Администратор* и дополнительно: • выдача на USB-носитель системного журнала статистики; • переустановка программного обеспечения ФПСУ со специального средства восстановления (USB-носителя).
Администратор/УА	В зависимости от назначенных Администратором или Главным Администратором полномочий, УА (удаленному администратору) могут быть разрешены следующие действия: • опрос текущего состояния; • получение данных о работе абонентов; • получение данных о работе локальных администраторов; • получение данных о работе удаленных администраторов и передача управления партнеру по горячему резервированию; • чтение конфигурации; • изменение конфигурации и загрузка/установка файлов на ФПСУ; • согласование времени и получение дампа; • установка дополнений, изменений; • управление ключами и правами удаленных администраторов.

2. 4. Ограничения функционала ФПСУ в зависимости от оперативной памяти

Программное обеспечение ФПСУ версии 4.0.2Q на базе аппаратных платформ и виртуальных сред позволяет достигать следующих максимальных значений в зависимости от количества доступной оперативной памяти, приведенных в таблице ниже:

Таблица4. Показатели ФПСУ

Показатель	Объем памяти				
	2 Gb	**4 Gb**	**8 Gb**	**16 Gb**	**32+ Gb**

Максимальное количество IP-интерфейсов (data-портов)	4	10	16	16	32
Максимальное количество зарегистрированных удаленных администраторов	128				
Максимальное количество одновременно работающих удаленных администраторов	4		8	16	
Максимальное количество абонентов	8 000	32 000		64 000	
Максимальное количество туннелей с другими ФПСУ	128	1024		10 240	
Максимальное количество групп ФПСУ-IP/Клиентов	4			128	
Макс. количество правил встроенного средства обнаружения вторжений	1 500	10 000	30 000	100 000	
Модуль DPI	Нет	Да			

2. 5. ПАК FPSUIP-ORD4-KRK

FPSUIP-ORD4-KRK является программно-аппаратным комплексом на базе российской аппаратной платформы в компактном корпусе, подготовленным для работы с устройствами системы выработки квантового распределения ключей.

FPSUIP-ORD4-KRK применяется при построении квантовых сетей. Для построения VPN-туннелей с использованием квантовых и квантово-защищенных ключей аппаратная платформа подключается к устройствам системы выработки квантового распределения ключей (устройства СВКРК).

В составе FPSUIP-ORD4-KRK находится программное средство, выполняющее функции СКЗИ с использованием аппаратных возможностей платформы.

FPSUIP-ORD4-KRK предназначен для защиты каналов связи до 50 Мбит/с, может

обеспечивать фильтрацию данных и их передачу через криптографические туннели на скорости до 80 Мбит/с при размере пакета около 1400 байт (при активации второго вычислительного потока).

При упоминании ФПСУ в этом разделе следует учитывать, что речь идет о Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4, программно-аппаратный вариант исполнения FPSUIP-ORD4-KRK.

2. 5. 1. Общая конструкция и назначение органов управления

Внешний вид аппаратной платформы представлен на рисунках ниже.

На аппаратной платформе FPSUIP-ORD4-KRK расположены следующие индикаторы и разъёмы:

1) индикаторы работы платформы:
   - «PWR» - светодиодный индикатор подачи питания. Не горит - питание отключено, горит зеленым светом - питание подаётся;
   - «RUN» - светодиодный индикатор состояния платформы. Горит зеленым светом при работе процессора, платформа включена (запущена);
   - «USR» - светодиодный индикатор USER GPIO. Назначение индикатора конфигурируется пользователем в соответствии поставленными задачами;

2) «  » - кнопка включения электропитания устройства;

3) «RESET» - кнопка аппаратной перезагрузки устройства;

4) 2 USB-порта:
   - интерфейс для подключения устройств по стыку USB 2.0;
   - интерфейс для подключения устройств по стыку USB 3.0;

5) «CONSOLE» - интерфейс для подключения к стыку RS-232C, порт для подключения консольного кабеля с разъёмом RJ45;

6) 3 сетевых порта «LAN1» … «LAN3» - интерфейсы для подключения устройств по стыкам Ethernet 1G/100M;

7) «HDMI» - интерфейс HDMI для подключения к устройству дисплея;

8) «  » - клемма защитного заземления. Клемма заземления для подключения корпуса аппаратной платформы к контуру защитного заземления при помощи медножильного провода сечением не менее 0,75 мм^2;

9) «12VDC» - разъём для подключения блока питания постоянного тока напряжением 12 В.

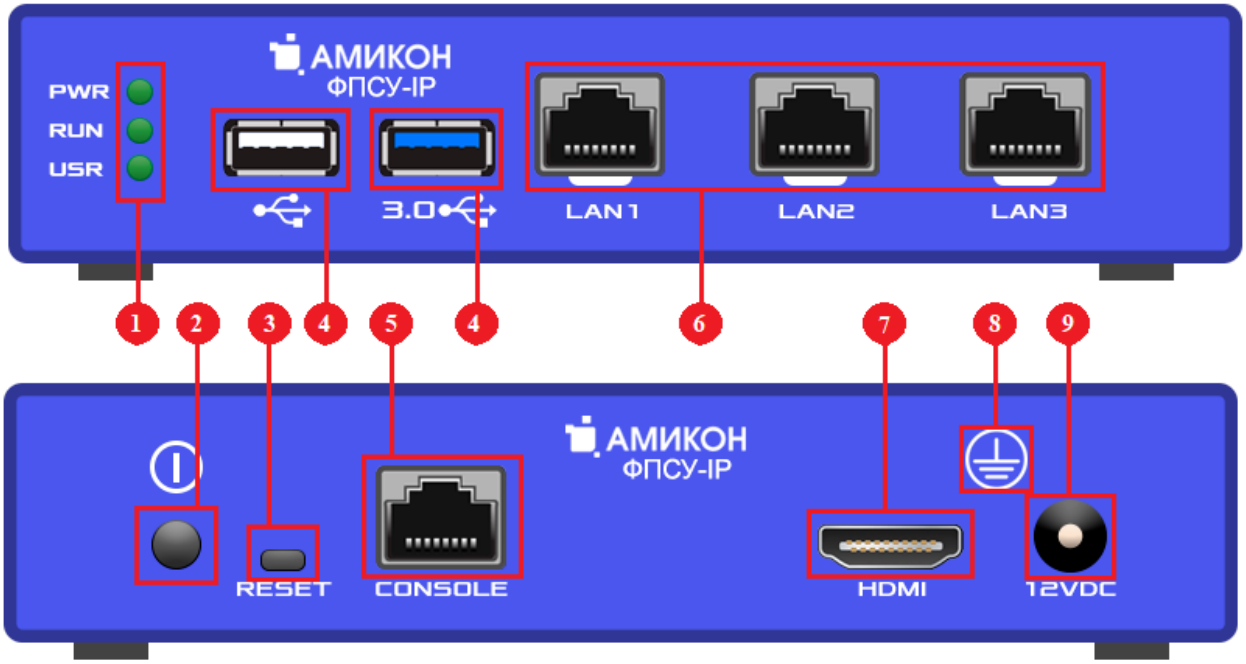


Рисунок 5 - Аппаратная платформа FPSU-ORD4, вверху – главный вид, внизу – вид сзади

Разъём консольного порта (X9) представлен на рисунке ниже.

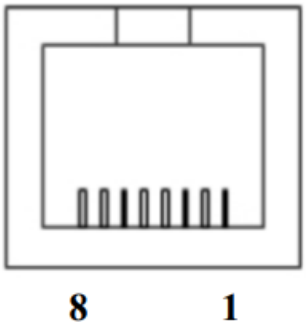


Рисунок 6 - Разъем консольного порта (X9)

Назначение контактов разъёма консольного порта (X9) представлено в таблице.

Таблица 5. Сигналы разъёма X9

Разъём X9	Сигнал
3	TX Debug Port (выход)

6	RX Debug Port (вход)
1	TX SIO Port (выход)
8	RX SIO Port (вход)
4,5	GND

2. 5. 2. Технические характеристики изделия

Технические характеристики платформы FPSUIP-ORD4-KRK приведены в таблице ниже.

Таблица 6. Технические характеристики

Базовые характеристики	Значения
Процессор Integrated Intel Atom*	АТБ-АТОМ-1.1 - E3815 - 1 ядро, 1 Мб кэш, 1.3ГГц
Оперативная память DDR3L 1067 MHz non-ECC*	2 Гб
Жесткий диск SSD mSATA mini (half board)*	8 Гб
Сетевой интерфейс	3 x Ethernet 1G/100M (Intel i210 или i211, RJ-45)
Консольный порт	1 x RS-232C (RJ-45)
Интерфейс USB	2 x (USB 2.0, USB 3.0, внутренний на miniPCIe)
Видеоадаптер	Integrated Intel® HD Graphics, 1 x HDMI port
Слоты расширения	1 x mini-PCIe
Специализированные аппаратные средства	датчик вскрытия корпуса; аппаратная и программная защита BIOS; аппаратный Watchdog Timer с программным управлением; программно-доступный серийный номер платформы.

Базовые характеристики	Значения
Электропитание	+12В ±10%, 40Вт (внешний источник питания);
Охлаждение	Пассивное (кондуктивное, без вентиляторов);
Конструктивное исполнение, габариты	Исполнение: настольное; ДхШхВ:150х150х30мм; Крепление: VESA; Масса, не более: 1 кг
Программное обеспечение*	BIOS, ФПСУ.
Надежность	Срок службы 5 лет; Наработка на отказ не менее 40000 ч.
Стойкость к климатическим воздействиям	Диапазон рабочих температур: от 0 °С до +50 °С; Диапазон температур хранения: от -40 °С до +70 °С; Класс защиты: IP30 по ГОСТ 14254-2015; Исполнение: УХЛ категории 4.2 по ГОСТ 15150.

Примечание* - по требованию заказчика предусмотрено изменение конфигурации ФПСУ: установка оперативной памяти объемом до 8 Гб, установка жесткого диска объемом до 32 Гб.

2. 5. 3. Указания для правильной и безопасной эксплуатации

ФПСУ предназначен для круглосуточной непрерывной эксплуатации без постоянного присутствия обслуживающего персонала.

Эксплуатация ФПСУ должна осуществляться в соответствии с правилами и требованиями, приведенными в руководстве по эксплуатации ФПСУ.

При эксплуатации ФПСУ не требуются работы по настройке и регулировке аппаратной платформы.

Ремонт ФПСУ должен проводиться на предприятии-изготовителе.

Монтаж и эксплуатация ФПСУ должны производиться лицами, изучившими данное руководство по эксплуатации.

Меры безопасности

Запрещается работать с ФПСУ лицам, не изучившим данное руководство по эксплуатации.

При работе с ФПСУ соблюдайте правила безопасности, изложенные в «Правилах по охране труда при эксплуатации электроустановок», утвержденных Приказом Минтруда России от 15.12.2020 N 903н (Зарегистрировано в Минюсте России 30.12.2020 N 61957).

2. 5. 4. Способы оценки технического состояния

При неисправности ФПСУ система автоматического контроля обеспечивает обнаружение и индикацию на соответствующих светодиодных индикаторах состояний на передней панели. Описание индикаторов на передней панели указано в таблице.

Таблица 7. Состояние индикаторов

Индикатор	Состояние	Описание
RUN	Светит постоянно	Подано электропитание на процессор
	Не светит	Не поступает электропитание на процессор
PWR	Светит постоянно	Внешнее напряжение питания подано
	Не светит	Внешнее напряжение питания отсутствует

2. 5. 4. 1. Перечень возможных неисправностей и их решение

Перечень возможных неисправностей в процессе использования ФПСУ и методы их устранения приведены в таблице.

Таблица 8. Перечень возможных неисправностей и их решения

Состояние индикатора	Возможная неисправность	Решение
RUN не светит	Сбой в работе программного обеспечения	Выключите и включите ФПСУ

Состояние индикатора	Возможная неисправность	Решение
	Отсутствует электропитание ФПСУ	Проверьте правильность подсоединения блока питания, убедитесь в его исправности (по индикатору PWR)
	Неисправность ФПСУ	Обратитесь к изготовителю ФПСУ
PWR не светит	Не выполнено подключение блока питания к источнику постоянного тока напряжением 12 В	Подключите ФПСУ к источнику питания постоянного тока напряжением 12 В
	Неисправность источника питания	Замените источник питания на исправный
	Внешнее напряжение питания отсутствует	Примите меры для восстановления электроснабжения

2. 5. 5. Сведения об утилизации изделия

Решение о прекращении эксплуатации и утилизации ФПСУ принимает заказчик с учетом установленного срока службы.

Утилизация ФПСУ производится без принятия специальных мер по защите окружающей среды. При утилизации ФПСУ необходимо руководствоваться действующим экологическим законодательством в месте эксплуатации.

Материалы, примененные при изготовлении ФПСУ, комплектующие изделия не содержат вредных и опасных для жизни, здоровья людей и окружающей среды веществ.

2. 6. ПАК FPSUIP-EXT3-KRK-SX-V

Вариант исполнения FPSUIP-EXT3-KRK-SX-V является программно-аппаратным комплексом, поставляется на базе аппаратной платформы FPSUIP-EXT3-KRK-SX-V без корпуса, подготовленным для работы с устройствами системы выработки квантового распределения ключей.

FPSUIP-EXT3-KRK-SX-V применяется при построении квантовых сетей. Для

построения VPN-туннелей с использованием квантовых и квантово-защищенных ключей аппаратная платформа подключается к устройствам системы выработки квантового распределения ключей (устройства СВКРК).

В составе FPSUIP-EXT3-KRK-SX-V находится программное средство, выполняющее функции СКЗИ с использованием аппаратных возможностей платформы.

FPSUIP-EXT3-KRK-SX-V предназначен для защиты скоростных каналов связи с пропускной способностью от 100 Мбит/с до 1 Гбит/с, может обеспечивать фильтрацию данных и их передачу через криптографические туннели на скорости до 1 Гбит/с при размере пакета около 1400 байт (при активации всех восьми вычислительных потоков).

При упоминании ФПСУ в этом разделе следует учитывать, что речь идет о комплексе Криптомаршрутизатор и межсетевой экран «ФПСУ Amigo» версии 4, программно-аппаратном варианте исполнения FPSUIP-EXT3-KRK-SX-V.

3. Процедуры приемки и безопасной установки

3. 1. Общий порядок поставки и комплектность

В общем случае комплектность поставки ФПСУ указана в таблице ниже. Комплектность поставки может быть изменена по согласованию с заказчиком. Точную комплектность поставки конкретного экземпляра ФПСУ следует смотреть в паспорте на изделие.

Наименование	**Кол-во**
Комплект ПО средств автоматизированного восстановления ПАК «ФПСУ-IP» на USB-носителе	1 шт.
Главный ТМ-идентификатор	1 шт.
Запасной ТМ-идентификатор	1 шт.
Картонная коробка для хранения USB-носителя и ТМ-идентификаторов	1 шт.
Аппаратная платформа ПАК «ФПСУ-IP» с предустановленным программным обеспечением, подготовленная для работы в режиме «основной» системы горячего резервирования	1 шт.
Аппаратная платформа ПАК «ФПСУ-IP» с предустановленным программным обеспечением, подготовленная для работы в режиме «резервный» системы горячего резервирования (опционально)	1 шт.

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

3. 2. Правила пользования

Средствами ФПСУ НЕ ДОПУСКАЕТСЯ защищать информацию, составляющую государственную тайну.

ФПСУ предназначен для эксплуатации на территории Российской Федерации.

Допускается локальное администрирование ФПСУ с использованием программы терминального доступа Putty (далее Терминал), входящей в состав изделия (поставляется

отдельно от остального программного обеспечения изделия по запросу), при этом подключение Терминала к ФПСУ должно производиться в пределах контролируемой территории.

Сроки действия используемой в средствах системы защиты информации семейства ФПСУ ключевой информации не должны превышать 1 год и 3 месяца.

В настройках должен быть включен режим информирования об использовании ключа при превышении срока его действия (см. пункт «Общие параметры конфигурации ФПСУ»).

Отчуждаемые ключевые носители должны храниться в сейфе. Пользователь несет персональную ответственность за сохранность отчуждаемых ключевых носителей. Отчуждаемыми ключевыми носителями являются:

- TM-идентификатор (устройство «Touch Memory» DS1993 – DS1996 или устройство «TM-Key»);
- устройство USB Flash Drive, если на нём находятся полученные от Центра выработки ключей ключевые данные или ключи для связи с АРМ УА;
- оптический компакт диск (при транспортировке ключевых данных Центра выработки ключей).

Транспортировка носителей с ключевой информацией на рабочее место ФПСУ или АРМ УА должна осуществляться доверенным образом.

При эксплуатации ФПСУ с активированной подсистемой автозапуска:

- в политике безопасности, принятой в организации в области неявной компрометации, должны быть предусмотрены организационно-технические меры, исключающие возможность использования изделия посторонними лицами в отсутствие пользователей изделия;
- на системный блок ФПСУ распространяются требования к отчуждаемым ключевым носителям;
- не допускается передача в ремонт внутреннего накопителя информации ФПСУ, если с внутреннего накопителя не была удалена штатными средствами ФПСУ копия ключа запуска (см. пункт «Отключение автозапуска»).

Уничтожение ключей на ключевых носителях:

Ключевая информация на ключевых носителях, срок действия которой истек, уничтожается путем очистки средствами изделия ЦВК с повторной записью на них новых ключей. Уничтожение ключевых носителей типа «Touch Memory», «TM-Key», «Flash Memory» в том числе вышедших из строя, и дистрибутивного носителя «Flash Memory» осуществляется путем расплющивания молотком на наковальне. Уничтожение ключевых носителей типа

«компакт диск» осуществляется путем оплавления до бесформенной массы. Использование внутренних накопителей информации ФПСУ допускается после проведения очистки внутреннего накопителя информации в соответствии с пунктом «Удаление программного обеспечения ФПСУ». При невозможности очистки, внутренние накопители следует уничтожить путем оплавления до бесформенной массы.

Компрометация ключей:

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

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

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

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

Запрещается устанавливать ключевую информацию, скомпрометированную в процессе транспортировки.

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

Компрометация ключа запуска:

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

администратора необходимо переустановить ПО ФПСУ.

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

Компрометация парно-выборочных ключей:

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

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

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

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

Компрометация общесистемного ключа:

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

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

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

Компрометация ключей для связи с АРМ УА:

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

1. Прекратить использование на ФПСУ скомпрометированных ключей (создать новые ключи для связи с АРМ УА, и текущие и следующие, см. пункт «Регистрация Удаленных Администраторов»);

2. Считать скомпрометированными все переданные по каналу связи, защищенном скомпрометированным ключом, долговременные ключи и выполнить соответствующие требования по действиям при компрометации;

3. Проверить конфигурацию ФПСУ, были ли несанкционированные изменения;

4. Передать сформированный в п. 1 открытый ключ на АРМ УА и заново установить открытый ключ АРМ УА.

Компрометация ключей горячего резерва:

Компрометация ключей горячего резерва возможна при хранении их на отчуждаемых носителях, если после установки их на внутренний носитель ФПСУ, они были оставлены для аварийного восстановления (см. пункт «Настройка ФПСУ на работу с партнером по резервированию»). В этом случае, а также если стало известно о компрометации в ходе транспортировки, предусматривается следующий порядок действий:

1. Прекратить использование на основном и резервном ФПСУ скомпрометированных ключей (см. пункт «Замена ключа горячего резерва»);

2. Создать на основном ФПСУ и установить на резервный новый ключ горячего резерва (см. пункт «Замена ключа горячего резерва»).

Компрометация ключей горячего резерва возможна при несанкционированном доступе к внутреннему накопителю ФПСУ при эксплуатации ФПСУ с активированной подсистемой автозапуска, в этом случае после переустановки ПО ФПСУ следует создать на основном ФПСУ и установить на резервный новый ключ горячего резерва.

Требования по размещению технических средств ФПСУ:

При размещении технических средств ФПСУ, необходимо выполнять следующие

требования.

Должны быть приняты меры по исключению несанкционированного доступа в помещения, в которых установлены технические средства ФПСУ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях.

Должны выполняться требования политики безопасности, принятой в организации в области размещения технических средств, обрабатывающих конфиденциальную информацию.

Для обеспечения специальной защиты ФПСУ должны выполняться следующие требования:

1. В целях защиты ключевой и цифровой открытой информации используемой в системе средств защиты информации ФПСУ по уровню КСБ от утечки по каналу связи при подключении объектов информатизации (ПЭВМ, аппаратно-программные комплексы и др.), в которые устанавливаются компоненты системы средств защиты ФПСУ, к каналам связи, выходящим за пределы контролируемой территории, необходимо, чтобы канал связи был реализован в виде:

- радиоканалов GSM. GPRS, 3G/4G, WiFi, а также других современных каналов мобильной или беспроводной связи с цифровой модуляцией штатного информационного сигнала;
- волоконно-оптических линий связи, уходящих за пределы контролируемой территории.

2. Использование средств защиты информации семейства ФПСУ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, без проведения специальных исследований и специальной проверки аппаратных средств ФПСУ и среды функционирования ФПСУ запрещается.

Требования к эксплуатации:

1. Не допускается непрерывное функционирование ФПСУ более суток (24 часов) без перезагрузки ФПСУ;

2. Действия в нештатных ситуациях, связанных с использованием ФПСУ: при отображении на экране изображений, не соответствующих приведенным в эксплуатационной документации на ФПСУ, следует обратиться в службу технической поддержки организации-производителя ФПСУ;

3. Должен производиться контроль основных характеристик при эксплуатации и

после хранения изделий путем проверки целостности ПО ФПСУ (см. пункт «Контроль целостности программного обеспечения»);

4. Запрещается подключение Терминала к каналам и линиям связи, за исключением консольного порта.

Требования к программному обеспечению:

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

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

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

1. Проверить наличие и статус сервиса DiagTrack (Панель управления -> Система и безопасность -> Администрирование -> Службы);

2. Если сервис запущен, остановить его;

3. Удалить запись регистрации сервиса DiagTrack из реестра (Пуск -> выполнить -> regedit, раздел HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services. Здесь необходимо найти и удалить папку DiagTrack);

4. Удалить подготовленные к отправке данные, которые сохраняются в четырех файлах с расширением *.rbs, хранящихся в директории %ProgramData%\Microsoft\Diagnosis. Имена файлов для production сборок ОС – event00.rbs, event01.rbs, event10.rbs и event11.rbs. Для insider сборок ОС имена могут отличаться, поэтому необходимо удалить все файлы с расширением *.rbs. При возникновении проблем с удалением данных файлов необходимо в свойствах на вкладке «Безопасность» разрешить полный доступ к файлу, а затем удалить;

5. Остановить автоматическую (AutoLogger) ETW сессию AutoLogger-DiagTrack-Listener, которую DiagTrack активирует в процессе своей остановки;

6. Удалить файл, в который автоматическая (AutoLogger) ETW сессия AutoLogger-DiagTrack-Listener сохраняла собранные данные;

7. Путь к файлу хранится в реестровой записи AutoLogger-DiagTrack-Listener в значении FileName. Конфигурации автоматических (AutoLogger) ETW сессий находятся в ключе реестра HKLM\SYSTEM\CurrentControlSet\Control\WMI\AutoLogger. Конфигурация целевой сессии хранится в данном ключе под записью AutoLogger-DiagTrack-Listener;

8. В настоящее время данные сохраняются в файл %ProgramData% \Microsoft\Diagnosis\ETLLogs\AutoLogger\AutoLogger-DiagTrack-Listener.etl;

9. Удалить запись регистрации конфигурации автоматической (AutoLogger) ETW сессии AutoLogger-DiagTrack-Listener из реестра;

Данные действия необходимо выполнять после каждого кумулятивного обновления ОС.

Требования по защите от несанкционированного доступа:

Организационные меры защиты информации от НСД:

При использовании средств защиты семейства ФПСУ следует принять следующие организационные меры:

1. Право доступа к рабочим местам с установленным ПО средств защиты семейства ФПСУ, в том числе через Терминал, должно предоставляться только лицам, ознакомленным с изложенными в данном пункте правилами пользования изучившим эксплуатационную документацию на ФПСУ;

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

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

4. Запретить запись на ключевые носители посторонней информации;

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

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

Организационно-технические меры защиты от НСД:

1. В Терминале и хостовой ОС (при эксплуатации ФПСУ в гостевой ОС) для класса КС1 перед началом работы ФПСУ, пользователь должен осуществлять контроль целостности ПО программой контроля целостности, входящей в состав ФПСУ. В состав модулей программного обеспечения, подлежащих проверке, должны быть включены исполняемые модули операционной системы, Терминала и гипервизора, а также его

конфигурационные файлы. Перед первым запуском ПО Терминала необходимо сверить контрольные суммы, находящиеся в файле с эталонными контрольными суммами. Перед первым использованием гипервизора, необходимо рассчитать эталонные контрольные суммы на ПО гипервизора и настройки гипервизора (конфигурационные файлы) программой контроля целостности fpsuhash, входящей в состав средства защиты семейства ФПСУ. Если в процессе работы программы будет обнаружено несовпадение контрольных сумм, то работа с Терминалом или хостовой ОС запрещается до прохождения процедуры восстановления целостности ПО.

2. В Терминале для классов КС2/КС3 перед началом работы с ФПСУ, пользователь должен осуществлять контроль целостности с помощью сертифицированного по требованиям ФСБ России АПМДЗ с действующим сертификатом соответствия. В состав модулей программного обеспечения, подлежащих проверке, должны быть включены исполняемые модули операционной системы, ПО Терминала и драйвера ПО АПМДЗ. Если в процессе работы будет обнаружено несовпадение контрольных сумм, то работа с Терминалом запрещается, до прохождения процедуры восстановления целостности ПО. Перед первым запуском Терминала необходимо сверить контрольные суммы, находящиеся в файле с эталонными контрольными суммами. Если в процессе работы программы будет обнаружено несовпадение контрольных сумм, работа с Терминалом запрещается до прохождения процедуры восстановления целостности ПО.

3. На ФПСУ контроль целостности обеспечивается автоматически при инсталляции ПО и перед каждым его запуском, дополнительно возможна регламентная проверка в соответствии с эксплуатационной документацией.

4. На технических средствах должны быть реализованы следующие меры:

- в BIOS ПЭВМ следует определить установки, исключающие возможность загрузки операционной системы, отличной от заданной администратором, отключить возможность загрузки с гибкого магнитного диска, привода CD-ROM, USB-носителей, сетевой загрузки; не должны применяться ПЭВМ с ПО BIOS исключающим возможность отключения сетевой загрузки ОС и загрузки с USB носителей;
- вход в BIOS ПЭВМ должен быть защищен паролем с длиной не менее 6 символов, при этом он должен содержать буквы в верхнем и нижнем регистрах, цифры и специальные символы (знаки пунктуации, скобки, знаки арифметических действий), пароль должен меняться не реже одного раза в 6 месяцев;
- средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты;
- ПО BIOS ПЭВМ должно соответствовать документу «Временные методические

рекомендации к проведению исследований программного обеспечения BIOS по документированным возможностям». Если средство вычислительной техники, на котором установлено программное обеспечение средств защиты семейства ФПСУ, используется для хранения обработки и (или) передачи данных, не подлежащих обязательной защите в соответствии с законодательством Российской Федерации, требования данного пункта носят рекомендательный характер;

- должен быть запрещен информационный обмен между виртуальными машинами с использованием общих ресурсов хостовой машины за исключением сетевого обмена между ФПСУ, запущенными в рамках одного гипервизора;
- должно быть проведено опечатывание системного блока с установленным программным обеспечением средств защиты семейства ФПСУ, в том числе Терминала, исключающее возможность бесконтрольного изменения аппаратной части рабочей станции (для классов КС2/КС3);

На технических средствах, оснащенных Терминалом для классов КС2/КС3 дополнительно должен быть установлен сертифицированный по требованиям ФСБ России АПМДЗ с действующим сертификатом соответствия и реализован следующий комплекс мероприятий по его установке и наладке:

- установка и настройка АПМДЗ должна производиться в соответствии с эксплуатационной документацией на АПМДЗ. Перед эксплуатацией АПМДЗ необходимо ознакомиться с комплектом документации на данный комплекс и принять рекомендуемые в документации защитные организационные меры;
- должно быть установлено ограничение времени (минимальное время) на инициализацию АПМДЗ, для обеспечения невозможности отключить АПМДЗ средствами BIOS;
- должно быть установлено ограничение на максимальное количество неудачных попыток аутентификации – не более 10;
- средствами АПМДЗ должна блокироваться загрузка операционных систем со съёмных носителей и по сети;
- средствами АПМДЗ должен быть обеспечен контроль целостности системных файлов операционной системы и программных модулей средств защиты семейства ФПСУ, установленных на ПЭВМ;
- в случае обнаружения не зарегистрированных программ или нарушения целостности программного обеспечения, работа должна быть прекращена; для восстановления целостности программного обеспечения, установленного на ПЭВМ, необходимо его переустановить.

Требования по аутентификации пользователей:

Пользователи ФПСУ: разграничение доступа допущенных лиц и контроль их полномочий при запуске ФПСУ и управлении его работой осуществляется по символьному паролю и предъявляемым допущенными лицами ТМ-идентификаторам в соответствии с логическим разделением пользователей ФПСУ на две роли и шесть условных классов. Перечень ролей и классов приведен в пункте 2, «Общие сведения».

1. Аутентификация пользователя ФПСУ с использованием аутентификационных ключей.

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

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

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

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

2. Аутентификация пользователя ФПСУ с использованием символьного пароля.

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

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

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

Удаленные администраторы не могут устанавливать или изменять символьный пароль.

3. Аутентификация средствами АПМДЗ.

Обеспечивается с помощью АПМДЗ в соответствии с его эксплуатационной документацией.

3. 3. 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. 3. 1. ISN Evaluation

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

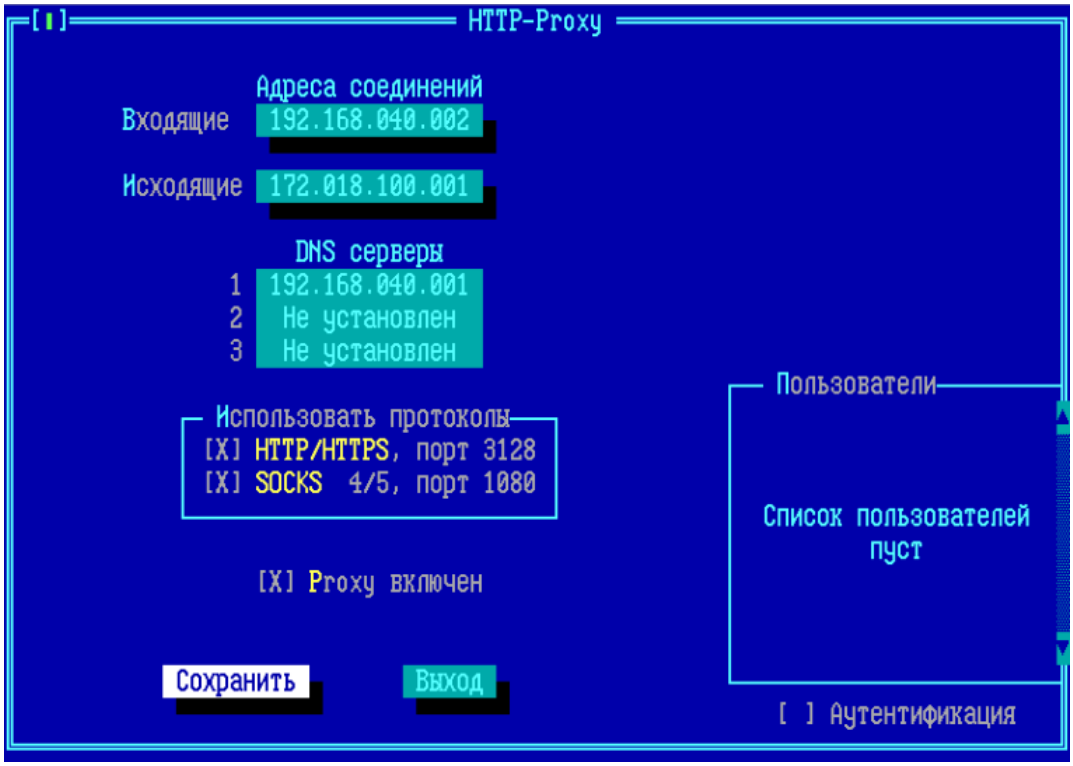


Рисунок 7 - Настройки Proxy

3. 3. 2. TCP URG Pointer

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

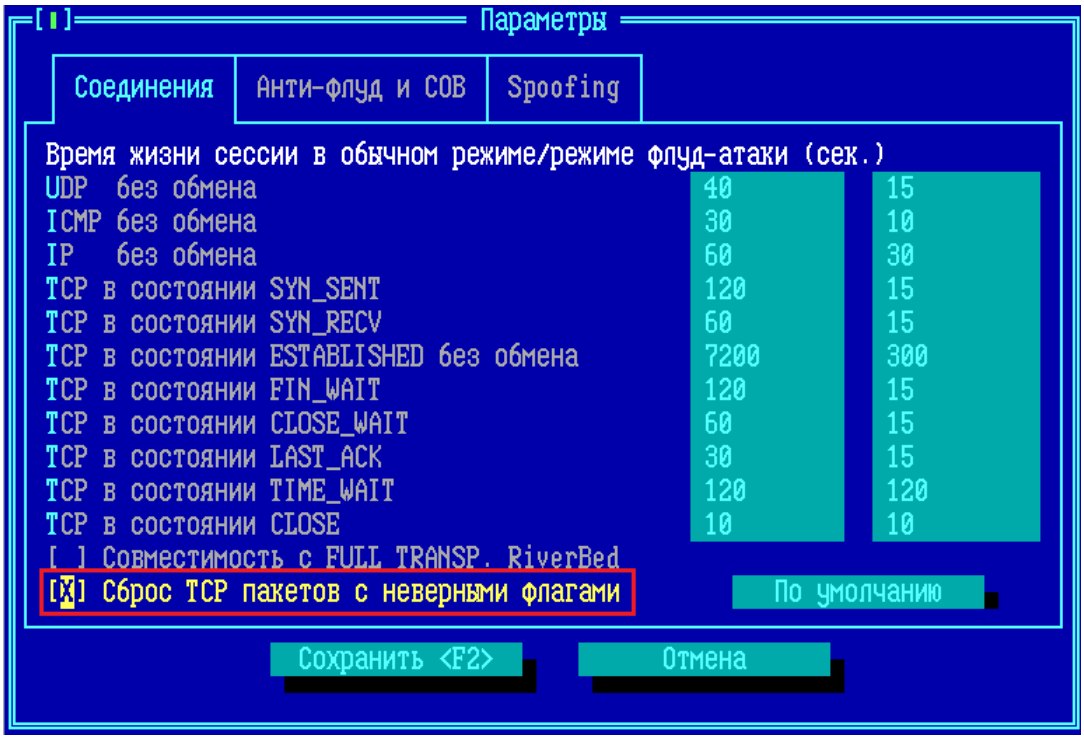


Рисунок 8 - Настройки правил соединения и фильтрации

3. 3. 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». На ФПСУ необходимо настроить соответствующий способ обслуживания. Также следует разрешить главные типы ICMP протокола (0, 3, 4, 11, 12).

Типы ICMP-сообщений:
0 – echo reply (echo-ответ, пинг);
3 – destination unreachable (адресат недосягаем);
4 – source quench (подавление источника, просьба посылать пакеты медленнее);
11 – time-to-live exceeded (истечение срока жизни пакета);
12 – IP header bad (неправильный заголовок IP-пакета).

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

Для включения запрещающего правила в ФПСУ необходимо:

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

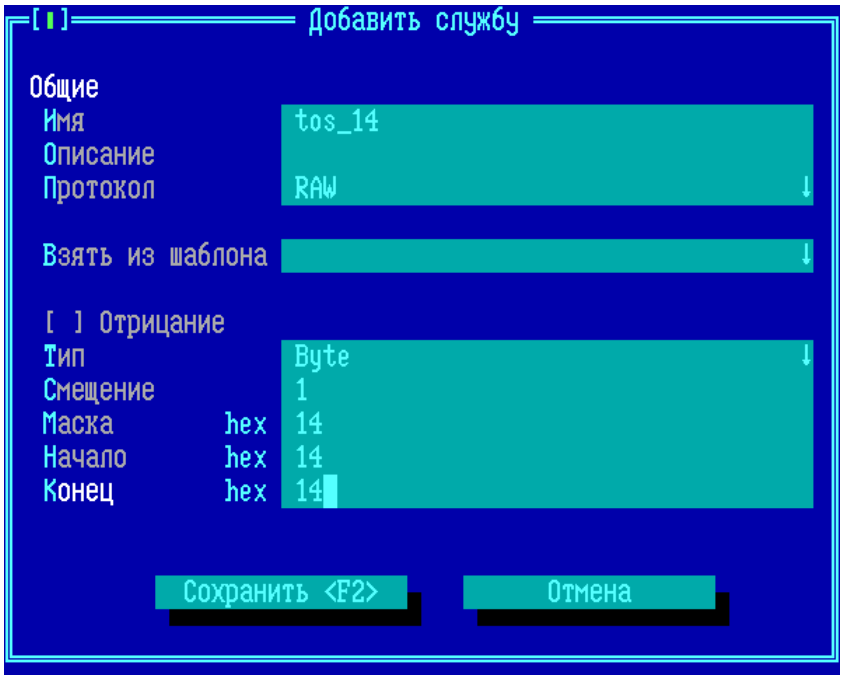


Рисунок 9 - Добавление службы RAW

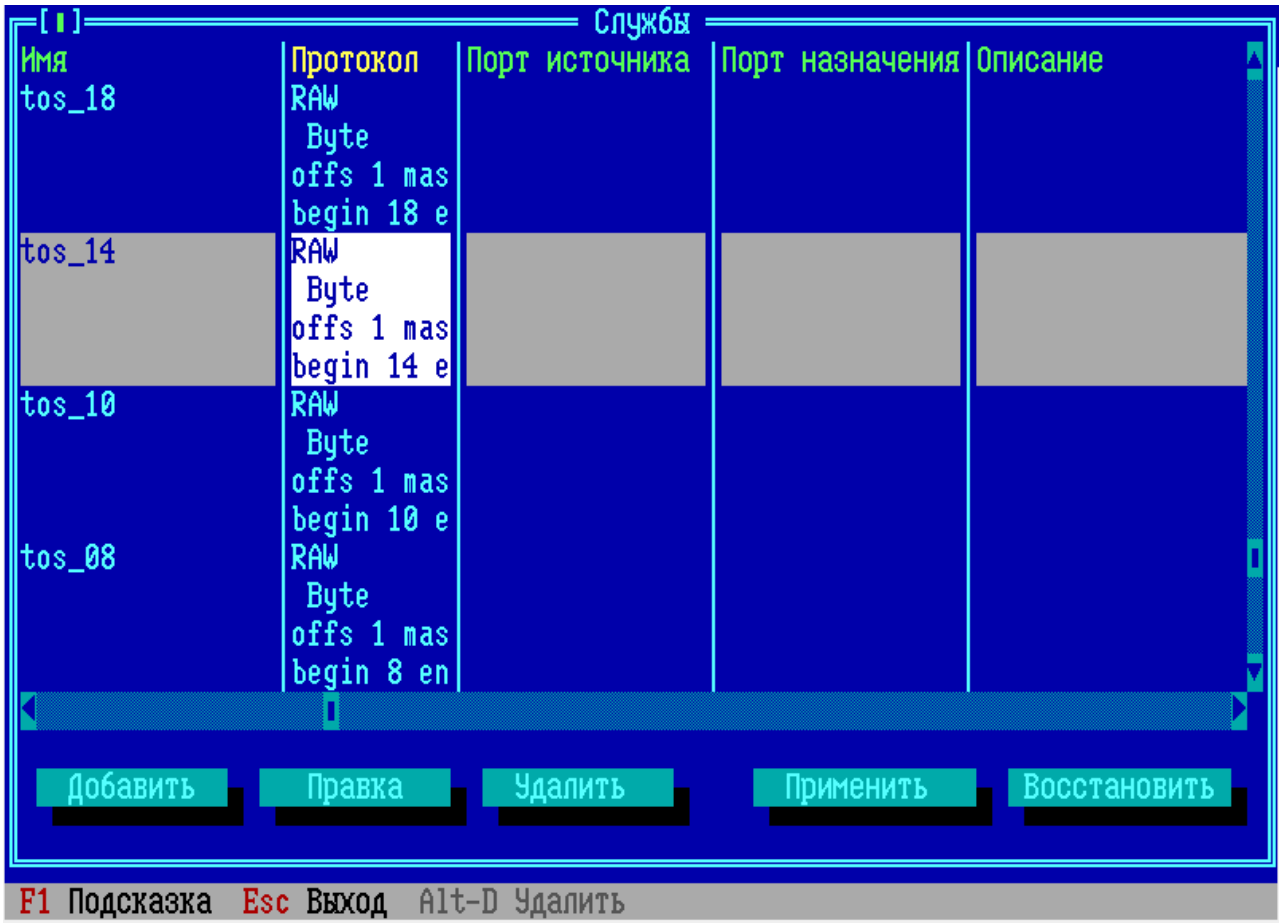


Рисунок 10 - Служба добавлена

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

При необходимости изменить правило трафика:

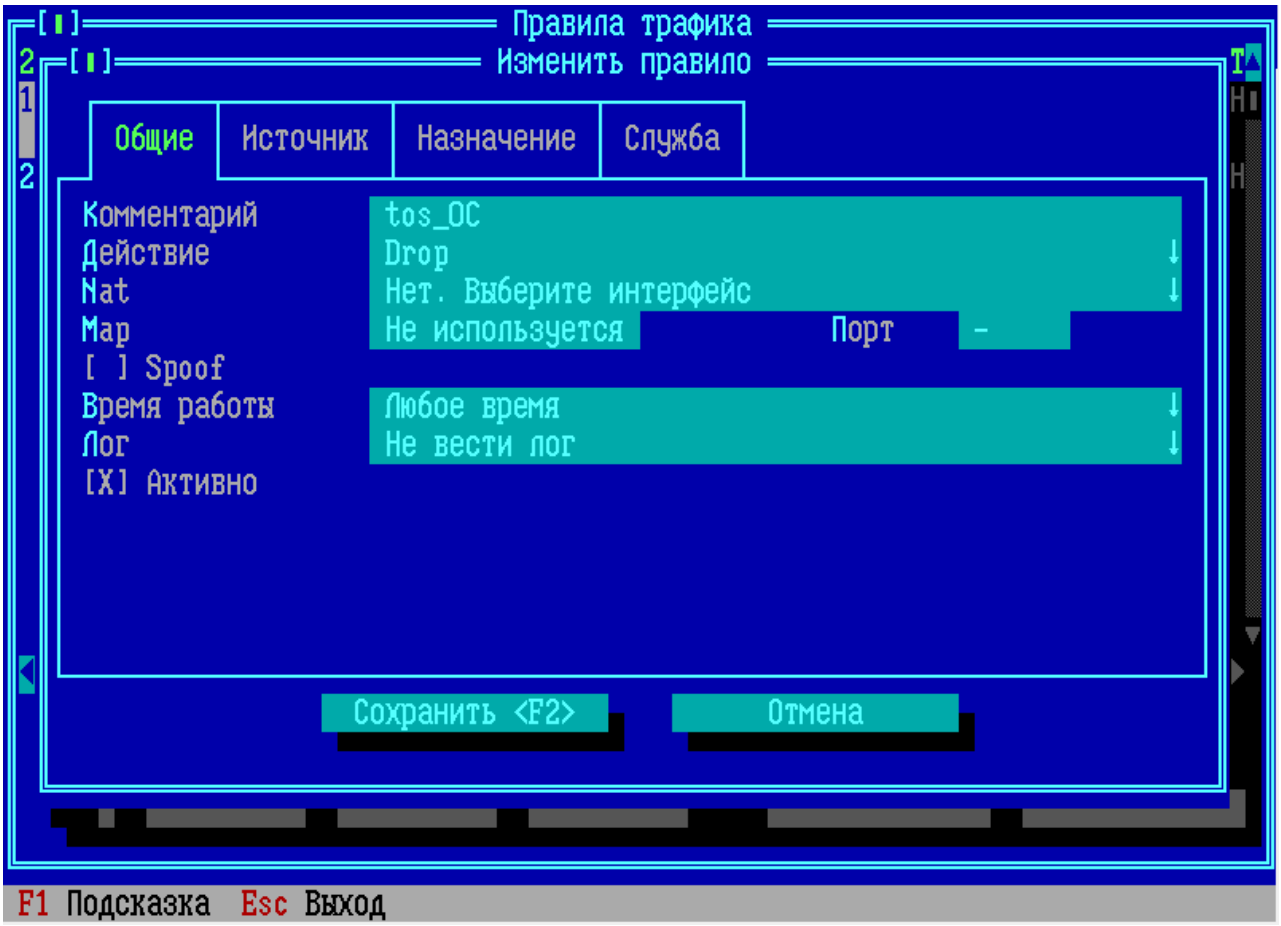


Рисунок 11 - Изменение общих свойств правила

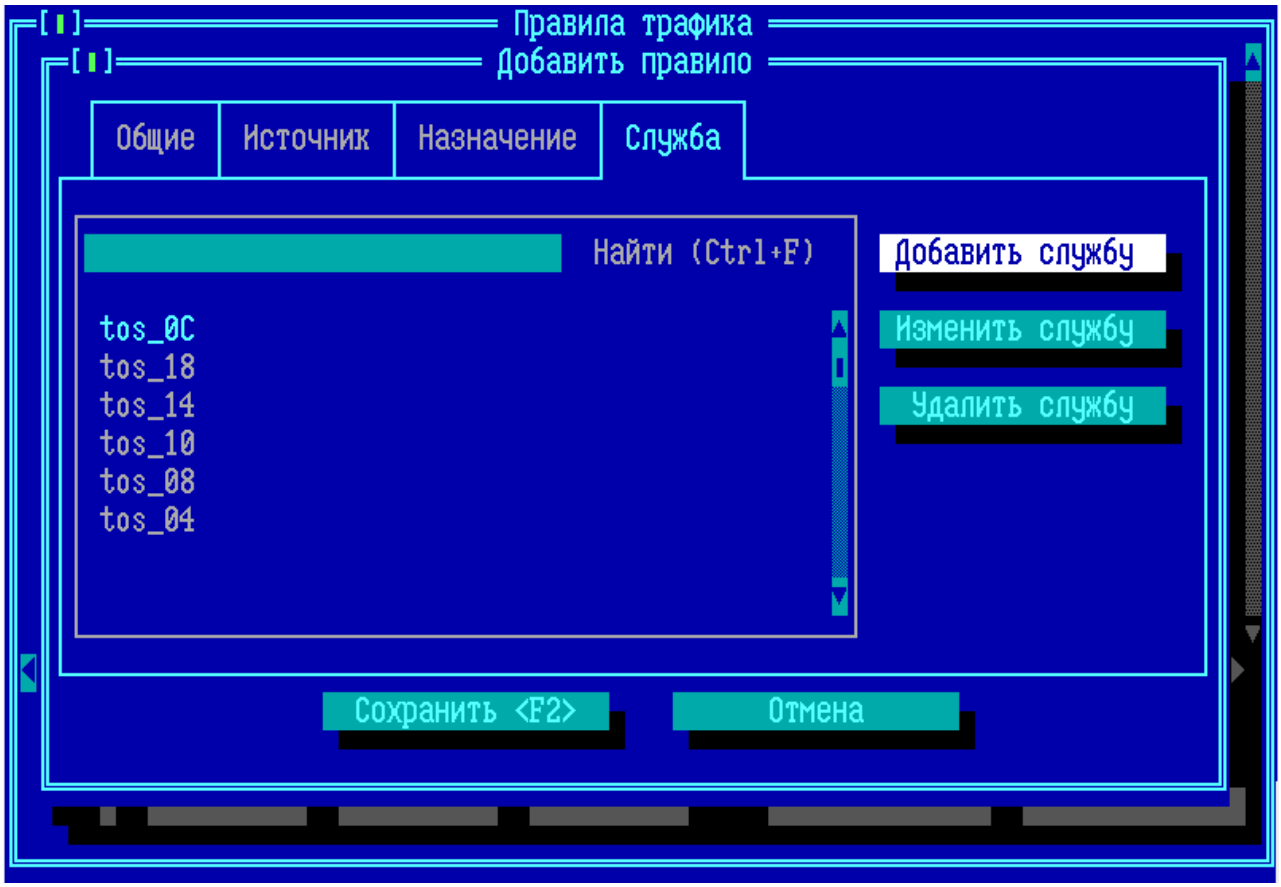


Рисунок 12 - Работа со службами

3. 4. Технические условия эксплуатации и хранения

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

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

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

Аппаратная часть программно-аппаратного комплекса ФПСУ 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°(±5°) С;
- относительная влажность окружающего воздуха - 60 (±15)%;
- атмосферное давление - от 84 до 107 кПа (630–800 мм рт. ст.);
- запыленность воздуха - не более 0,75 мг/м³;
- в воздухе не должно быть агрессивных примесей (паров кислот и щелочей), вызывающих коррозию.

Допускается эксплуатация ФПСУ на базе аппаратных платформ FPSUIP-STD3, FPSUIP-EXT3 при следующих изменениях нормальных климатических условий:

- температура окружающего воздуха – от 10°С до 35°С;
- относительная влажность окружающего воздуха – от 5% до 90% (без конденсата).

Допускается эксплуатация ФПСУ на базе аппаратной платформы FPSUIP-ORD3 при следующих изменениях нормальных климатических условий:

- температура окружающего воздуха – от 0°С до 40°С;
- относительная влажность окружающего воздуха – от 0% до 90% (без конденсата).

Допускается эксплуатация ФПСУ на базе аппаратной платформы FPSUIP-ORD4 при следующих изменениях нормальных климатических условий:

- температура окружающего воздуха – от 0°С до 50°С;
- относительная влажность окружающего воздуха – от 0% до 90% (без конденсата).

Допускается эксплуатация ФПСУ на базе аппаратных платформ FPSUIP-ULT-1U, FPSUIP-ULT5, FPSUIP-ULT5-2U, FPSUIP-ULT6 при следующих изменениях нормальных климатических условий:

- температура окружающего воздуха – от 10°С до 35°С;
- относительная влажность окружающего воздуха – от 8% до 80% (без конденсата).

Условия хранения

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

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

3. 5. Гарантийные обязательства

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

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

При обнаружении дефекта в ФПСУ 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 прекращается, если потребителем внесены изменения в ФПСУ без согласования с производителем. Гарантийные обязательства не распространяются на копии ФПСУ, изготовленные по инициативе потребителя.

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

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.

Обратите внимание! Производитель не гарантирует совместимость ФПСУ с SFP-модулями сетевых карт, отличных от поставленных производителем в комплекте с аппаратной платформой.

3. 6. Настройки платформ виртуализации

3. 6. 1. Настройка виртуальной машины QEMU/KVM

В данном разделе описывается подготовка виртуальной машины QEMU/KVM для развертывания ФПСУ.

Виртуальные машины могут эксплуатироваться под управлением следующих хостовых ОС: Windows 7 x64, Windows 8.1 x64, Windows 10 x64, Windows 11 x64, Windows Server 2019 x64, ubuntu 22.04 LTS x86-64, ubuntu 24.04 LTS x86-64, Debian 12 x86-64, Debian 13 x86-64, Astra Linux SE 1.7.4 x86-64, REDOS 8 x86-64.

Поддерживаемые версии QEMU: 6.2.0, 7.0.0, 7.1.0, 8.0.0, 8.1.0, 8.2.0.

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;
- настроить сетевые интерфейсы и другие устройства.

Далее приводится пример установки ФПСУ в QEMU/KVM 6.2.0 на Ubuntu 22.04.4 LTS.

QEMU/KVM 6.2.0 предварительно установлена.

Предварительно установлены пакеты libvirt-clients версии 8.0.0-1ubuntu7.10 amd64, libvirt-daemon-system версии 8.0.0-1ubuntu7.10 amd64, bridge-utils версии 1.7-1ubuntu3 amd64.

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

```
kvm-ok
```

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

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

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

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

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

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

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

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

Проверить членство в группе можно командой:

```
groups <имя пользователя>
```

Включите поддержку встроенного ПО UEFI для виртуальной машины QEMU/KVM, установив пакет ovmf, если не установлен:

```
sudo apt install ovmf
sudo cp /usr/share/OVMF/OVMF_CODE.fd /var/lib/libfirt/
```

Версия устанавливаемого пакета ovmf 2022.02-3ubuntu0.22.04.3.

Для автоматизации процесса установки ОС используется утилита virt-install, могут быть использованы preseeds, kickstart и пр. Утилита virt-install является частью пакета virtinst. Данный пакет был установлен ранее. Версия установленного пакета virtinst 4.0.0-1.

Запустите гостевую операционную систему ФПСУ в виртуальной машине QEMU/KVM, vfpsu, выполнив команду в терминале:

```
sudo virt-install --name vfpsu --memory 2048 --disk vfpsu.qcow2,size=1 --osinfo
detect=off,require=off  --import --boot
loader=$(pwd)/OVMF_CODE.fd,bootmenu.enable=on,bios.useserial=on --network none
```

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

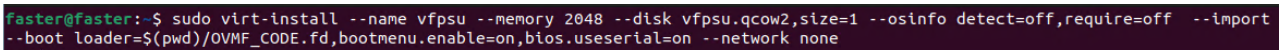


Рисунок 13 - Создание виртуальной машины

Закройте окно виртуальной машины.

В некоторых случаях необходимо отключить безопасную загрузку UEFI. Для этого при загрузке виртуальной машины, нажать *<F2>*, зайти в настройки BIOS, выбрать в меню «Device Manager → Secure Boot Configuration», выбрать опцию «Attempt Secure Boot» и снять флаг, выйти из BIOS с сохранением изменений по *<F10>*.

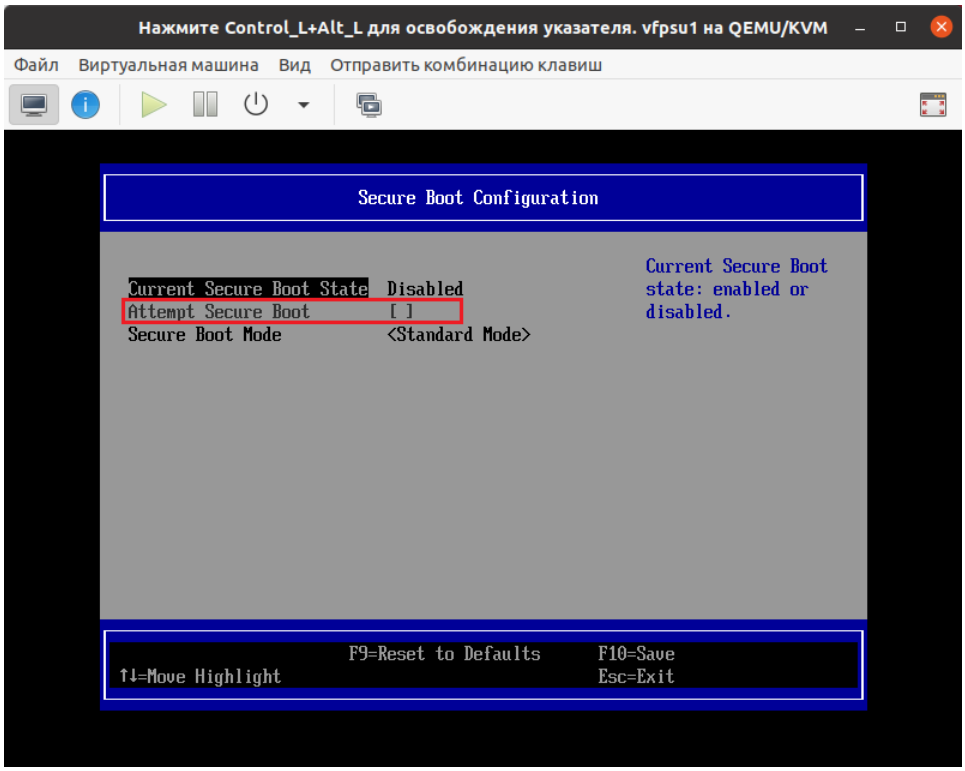


Рисунок 14 - Настройки BIOS виртуальной машины

Перед запуском виртуальной машины необходимо настроить второй сетевой интерфейс, проверить или настроить процессоры, загрузочный диск для ФПСУ, добавить в список оборудования USB Disk 2.0 и TM-Key, изменить порядок загрузки, задав загрузку с USB-носителя на время установки ФПСУ.

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

Настройка QEMU/KVM для установки ФПСУ с готового образа диска приведена в пунктах 1 - 9.

Настройка QEMU/KVM для установки ФПСУ с установочного носителя приведена в пунктах 1 - 7, 10.

1. Запустите графический интерфейс виртуальной машины QEMU/KVM.

Для управления виртуальной машиной могут быть использованы различные утилиты. В примере используется рекомендуемый пакет virt-manager, который содержит утилиту с графическим интерфейсом для управления локальными и удаленными виртуальными машинами. Утилита virt-manager является частью пакета virtinst. Данный пакет был ранее установлен. Версия установленного пакета virtinst 4.0.0-1.

Запустите virt-manager командой:

```
sudo virt-manager
```

(Если менеджер виртуальных машин не установлен, установите пакет virt-manager командой: `sudo apt-get install virt-manager`).

Откроется окно управления виртуальными машинами:

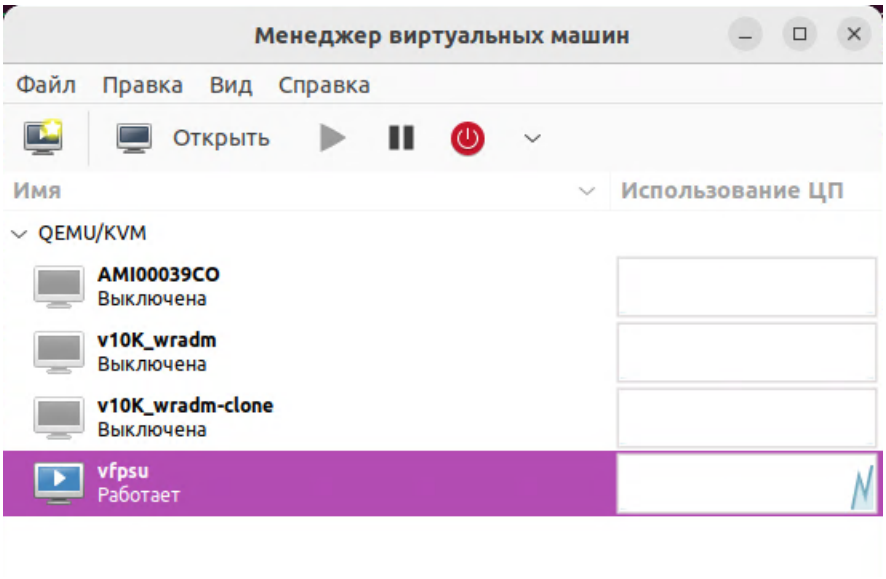


Рисунок 15 - Окно менеджера виртуальных машин

ВНИМАНИЕ! Для изменения настроек виртуальная машина должна быть выключена.

Выключите виртуальную машину vfpsu, выбрав соответствующую команду в контекстном меню.

Откройте виртуальную машину vfpsu, откройте настройки виртуального оборудования, нажав на кнопку  .

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

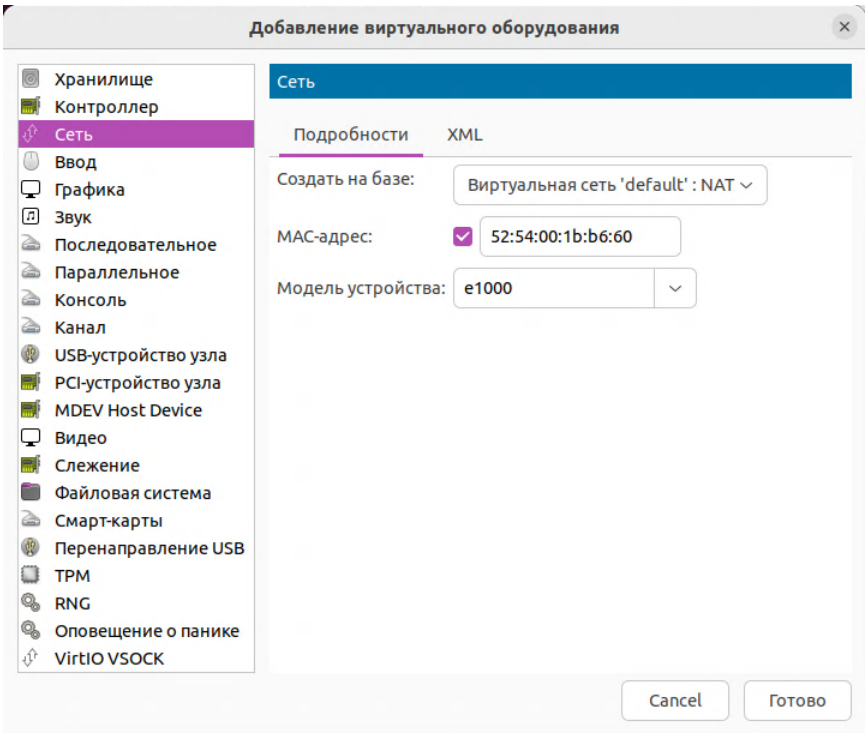


Рисунок 16 - Добавление сетевого интерфейса

Для сетевого интерфейса необходимо выбрать модель устройства «e1000».

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

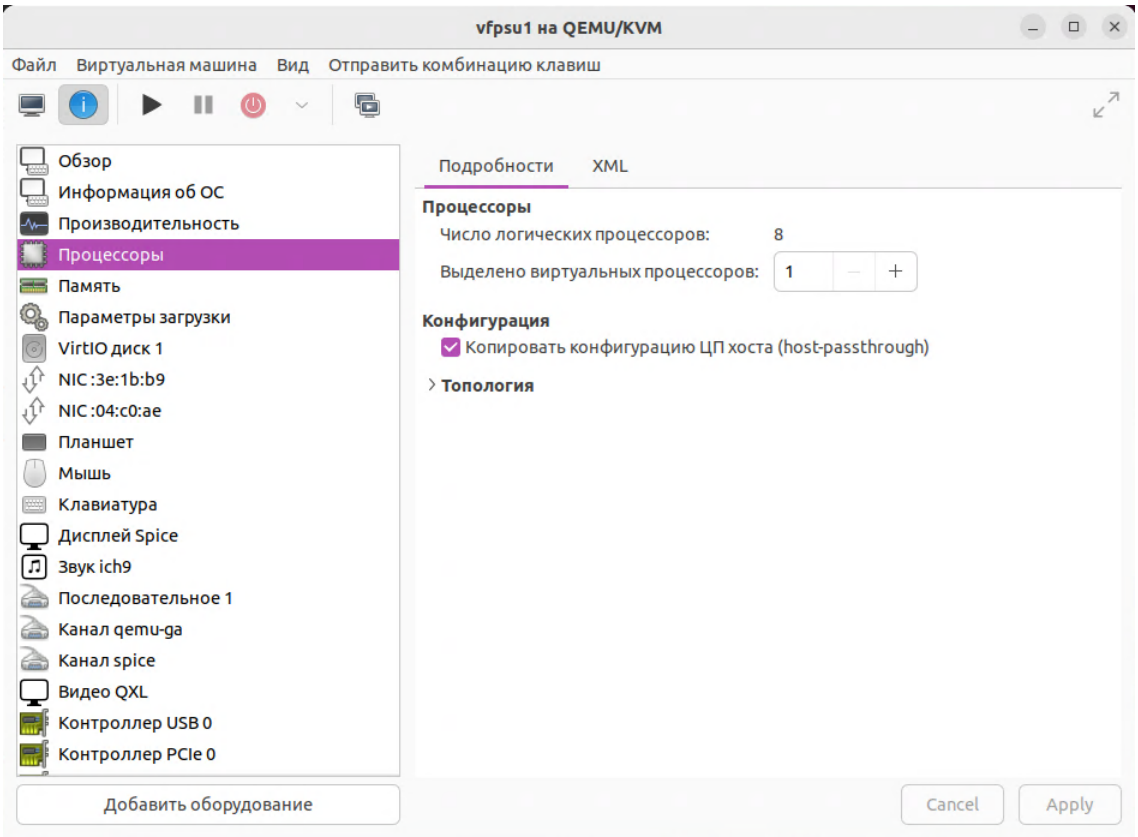


Рисунок 17 - Процессоры

4. Проверьте настройки диска виртуальной машины. Тип шины диска выбирается «IDE», размер диска установите 1 ГБ.

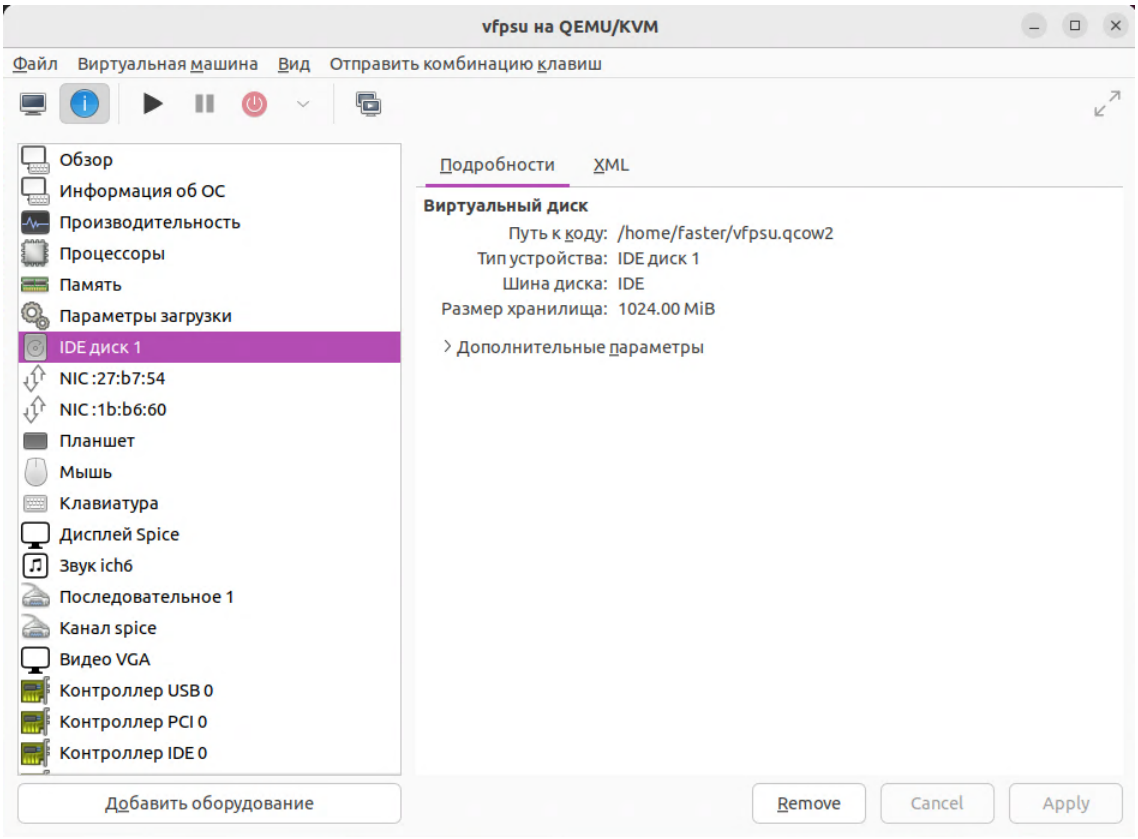


Рисунок 18 - Диск

5. Проверьте настройки видео виртуальной машины. Выберите модель «VGA».

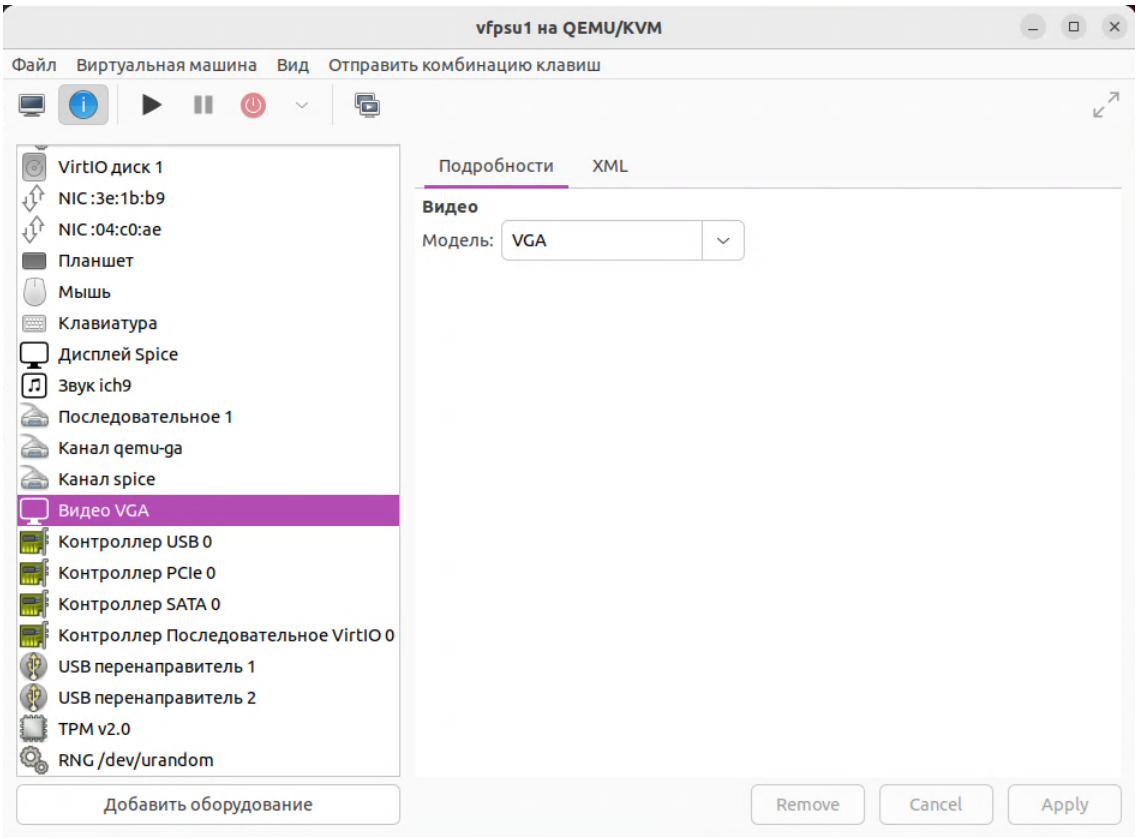


Рисунок 19 - Видео

6. При создании виртуальной машины необходимо добавить в список оборудования USB Disk 2.0 и USB-устройство ТМ (ТМ-считыватель или ТМ-Key):

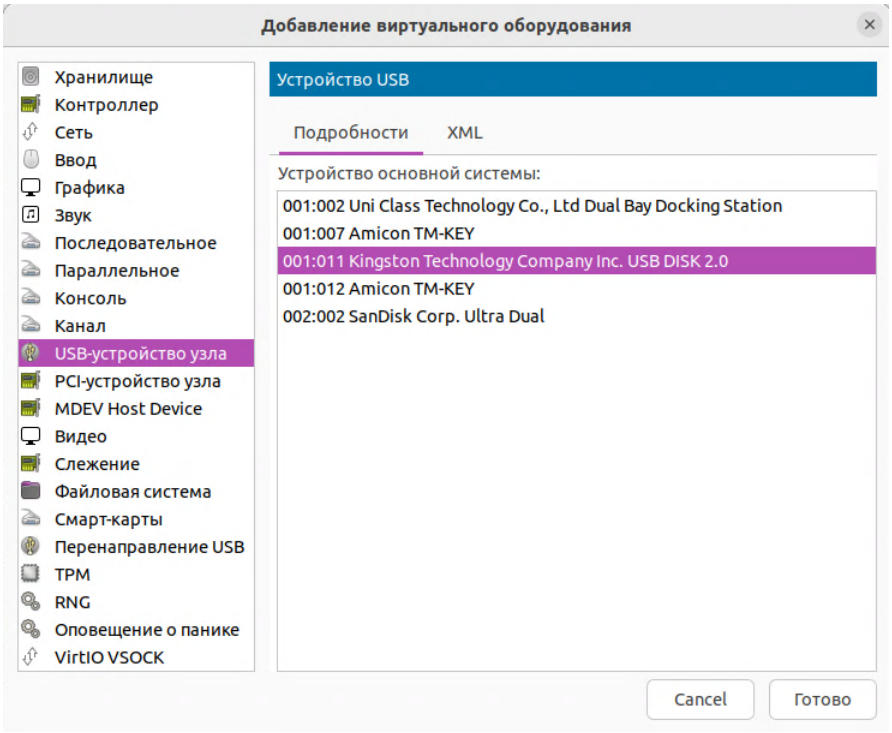


Рисунок 20 - Добавление оборудования

Подключите установочный USB-носитель к рабочей станции, нажмите кнопку «Добавить оборудование», в открывшемся окне выберите «USB-устройства узла», в списке найденного оборудования отметьте «USB Disk 2.0» и подтвердите выбор по кнопке «Готово».

Подключите TM-Key к рабочей станции, нажмите кнопку «Добавить оборудование», в открывшемся окне выберите «USB-устройства узла», в списке найденного оборудования отметьте «Amicon TM-KEY» и подтвердите выбор по кнопке «Готово».

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

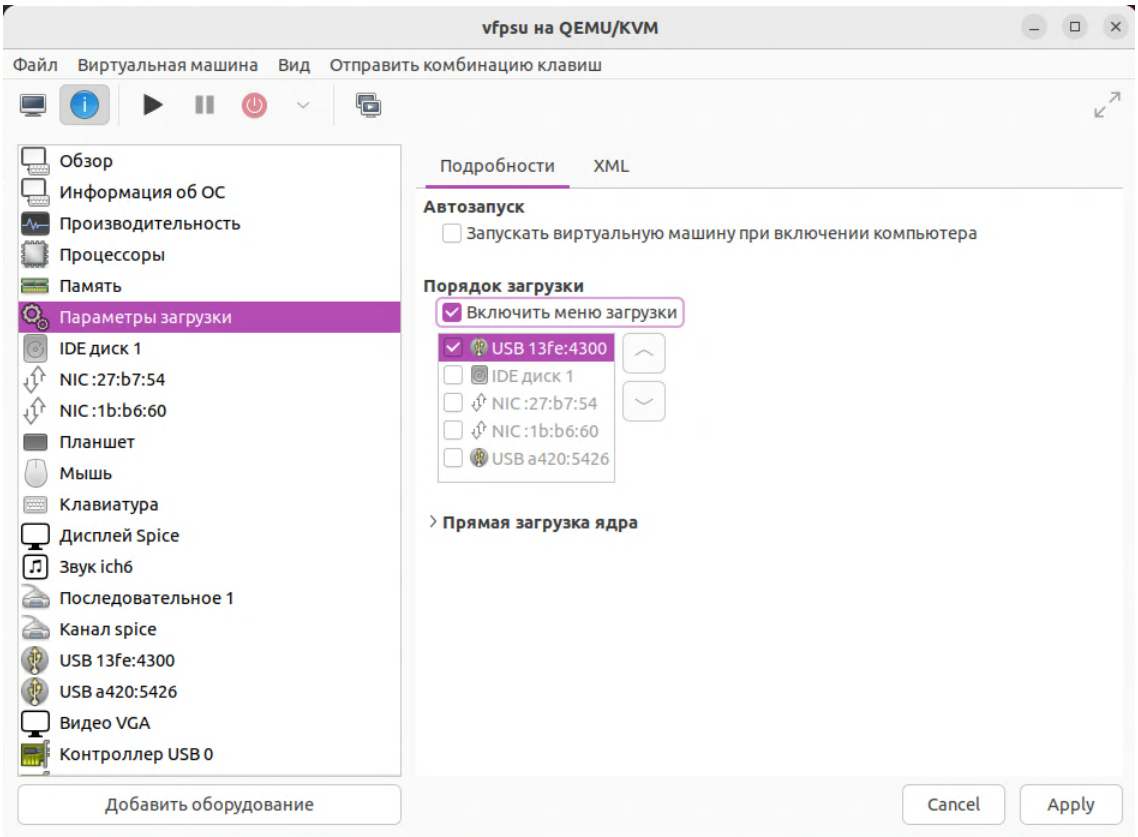


Рисунок 21 - Изменение порядка загрузки дисков

Настройка QEMU/KVM для установки ФПСУ с готового образа диска

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

9. В параметрах загрузки виртуальной машины необходимо вернуть первоначальный порядок загрузки дисков (был изменен в пункте 7).

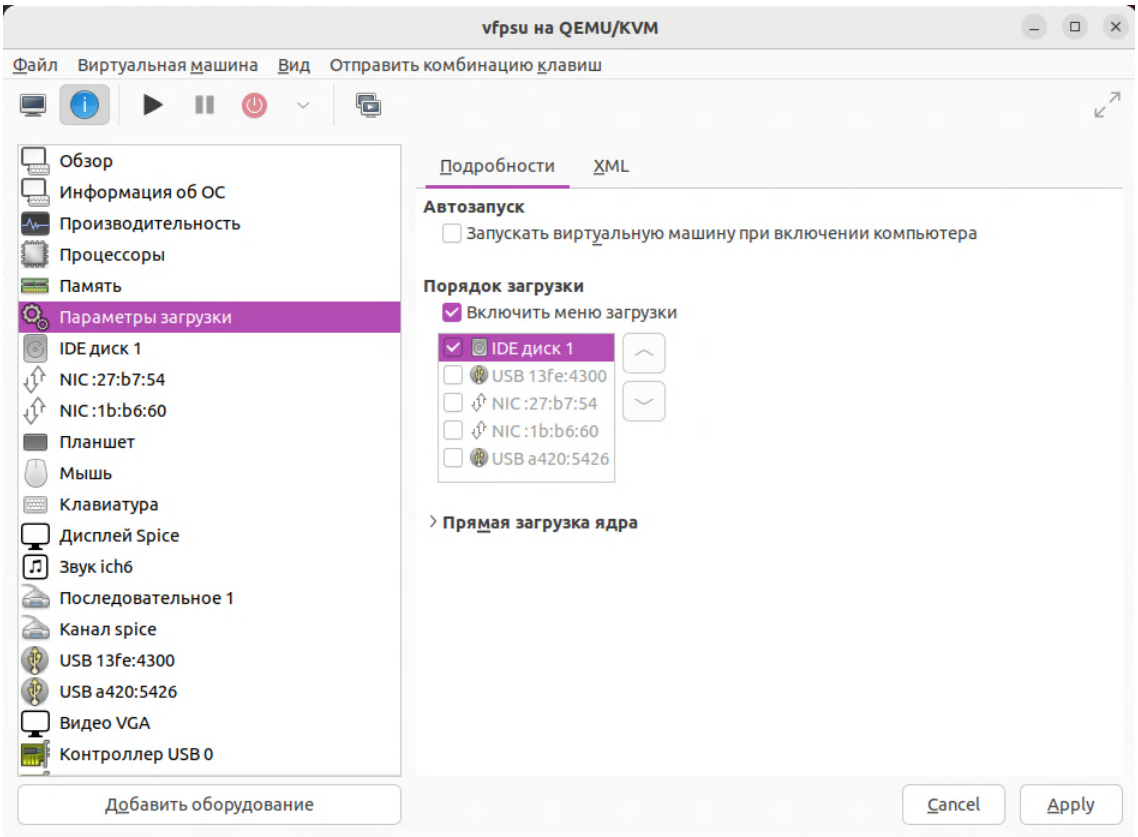


Рисунок 22 - Изменение порядка загрузки дисков

Настройка QEMU/KVM для установки ФПСУ с установочного носителя

10. После добавления в конфигурационный файл виртуальной машины USB-носителя с инсталляционным комплектом ФПСУ поменяйте порядок загрузки, установив загрузку с USB-носителя (действие аналогичное п. 7), и проведите установку ПО. Описание процедуры установки ПО ФПСУ находится в разделе «Установка ПО ФПСУ с установочного носителя». После процедуры установки и первоначальной настройки (см. пункт «Технологический режим ФПСУ») поменяйте обратно порядок загрузки, установив загрузку с диска (действие аналогичное п. 9).

Создание виртуальной машины закончено.

Для запуска ФПСУ в QEMU/KVM запустите vfpsu по кнопке  или введите команду в терминале:

```
virsh start vfpsu
```

На экране отобразится главное меню ФПСУ.

3. 6. 2. Настройка виртуальной машины VMware

В данном разделе описывается подготовка виртуальной машины VMware Workstation Pro/VMware Workstation/VMware EsXi для развертывания ФПСУ.

Виртуальные машины могут эксплуатироваться под управлением следующих хостовых ОС: Windows 7 x64, Windows 8.1 x64, Windows 10 x64, Windows 11 x64, Windows Server 2019 x64, ubuntu 22.04 LTS x86-64, ubuntu 24.04 LTS x86-64, Debian 12 x86-64, Debian 13 x86-64, Astra Linux SE 1.7.4 x86-64, REDOS 8 x86-64.

Поддерживаемые виртуальные машины:

- VMware ESXi версий 6.7.0 (8169922), 6.7.0 U1 (10302608), 6.7.0 U2 (13006603), 6.7.0 U3 (14320388), 6.7.0 P04 (17167734), 7.0.0 (15843807), 7.0.0b (16324942), 7.0.1 (16850804), 7.0.2 (18538813), 7.0.3 (20036589), 8.0.0 (20513097), 8.0.1 (21203435);
- VMware Workstation/Workstation Pro версий 16.0.0 (16894299), 16.1.0 (17198959), 16.1.1 (17801498), 16.1.2 (17966106), 16.2.0 (18760230), 16.2.1 (18811642), 16.2.2 (19200509), 16.2.3 (19376536), 16.2.4 (20089737), 17.0.0 (20800274), 17.0.1 (21139696), 17.0.2 (21581411), 17.5.0 (22583795), 17.5.1 (23185310).

Для создания в интерфейсе VMware виртуальной машины с поддерживаемыми характеристиками выполните следующее:

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

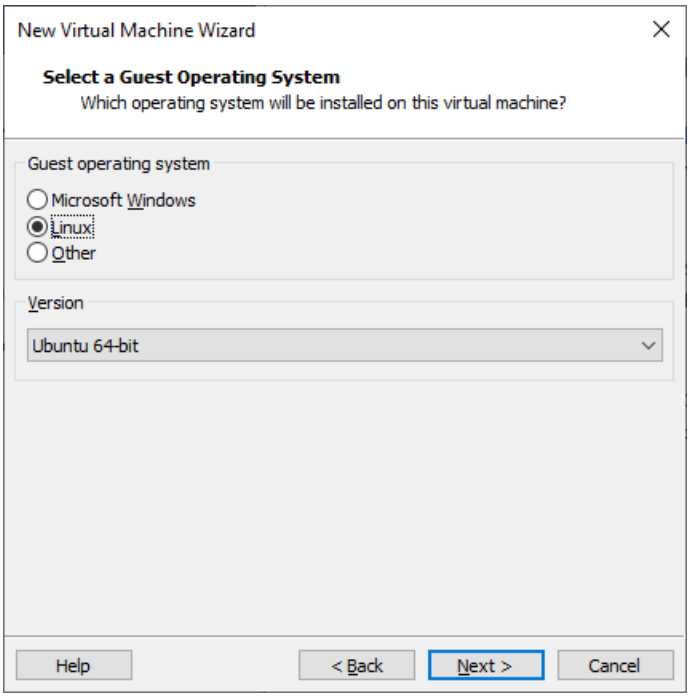


Рисунок 23 - Выбор ОС

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). Рекомендуется выбирать 4°GB и больше.

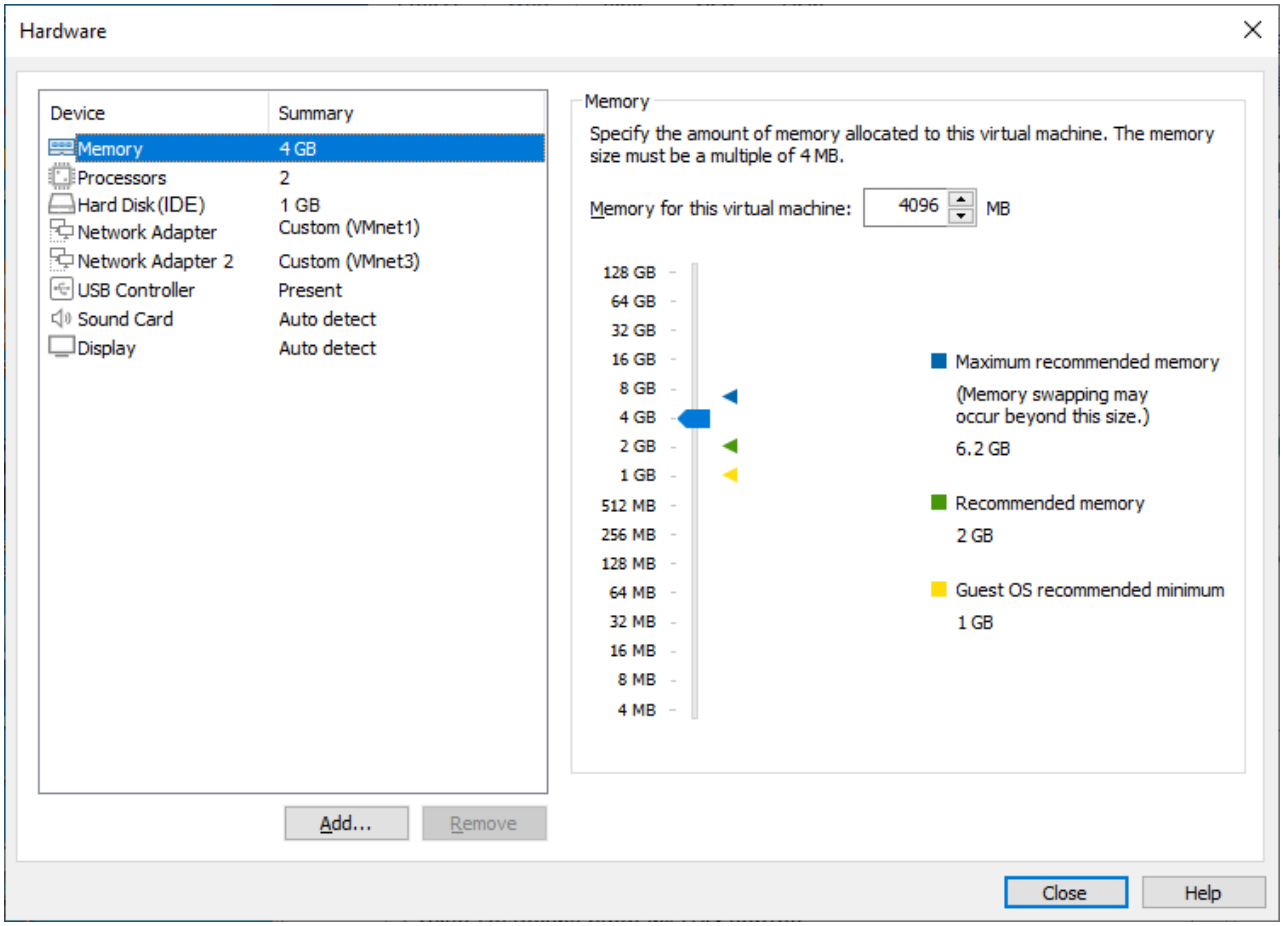


Рисунок 24 - Оперативная память виртуальной машины

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

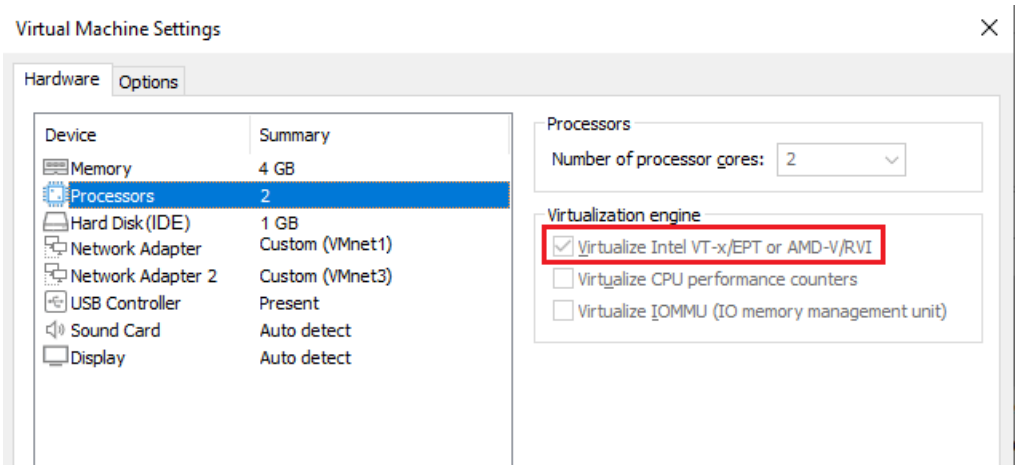


Рисунок 25 - Настройки процессора

5. Добавьте виртуальный жесткий диск объемом 1°GB, выберите контроллер виртуального жесткого диска – «IDE». В ОС ФПСУ 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».

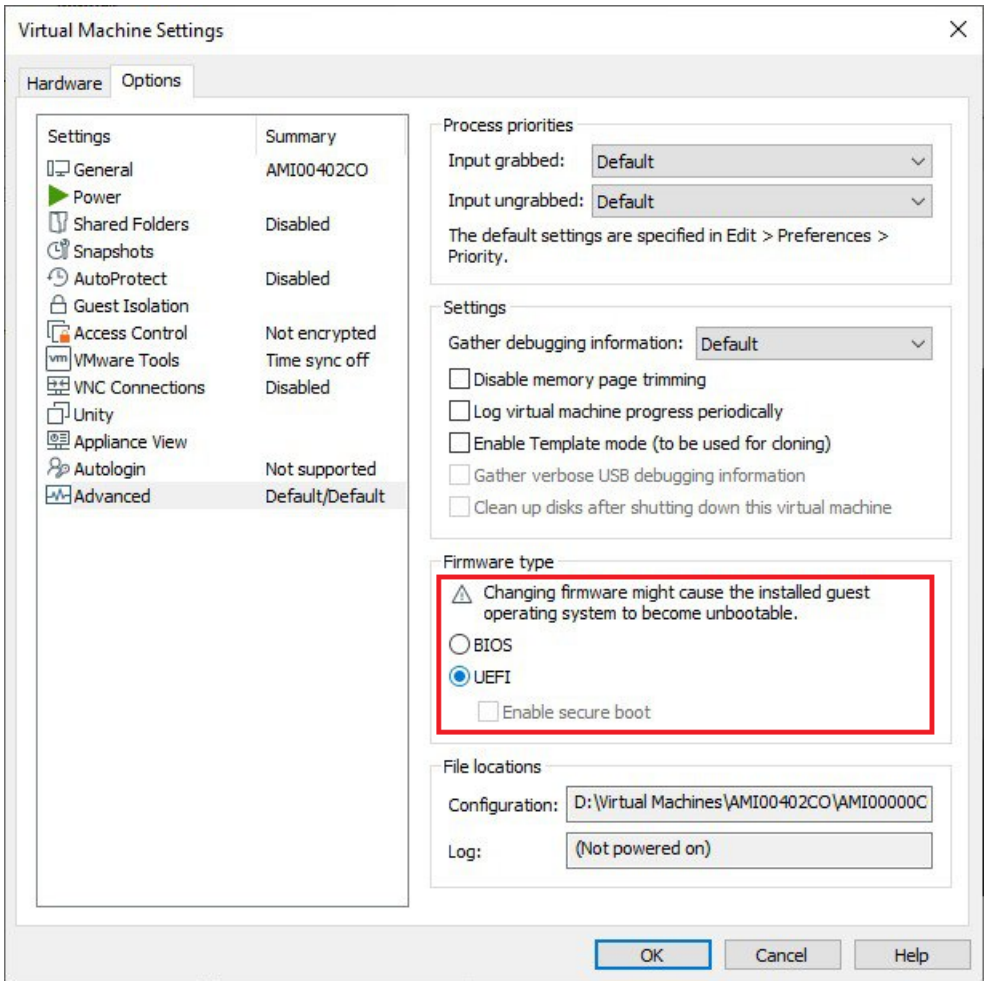


Рисунок 26 - Настройки интерфейса прошивки

Для VMware Workstation после завершения процесса создания виртуальной машины внесите изменения в файл с расширением .vmx из каталога виртуальной машины, как указано в пункте 11.

Закройте окно настроек и завершите создание виртуальной машины.

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

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

Сохраните файл.

11. Для VMware Workstation измените в конфигурации виртуальной машины тип встроенного ПО «UEFI». Откройте для редактирования файл с расширением .vmx

из каталога виртуальной машины, добавьте в середину файла (например, после параметра mem.hotadd) строку:

```
firmware = "efi"
```

Сохраните файл.

Внести изменения в конфигурацию виртуальной машины можно с помощью утилиты VM_Tweaker.exe. Откройте для редактирования файл с расширением .vmx из каталога виртуальной машины, на вкладке «EFI BIOS Tweaks» включите флаг «Enable "efi" BIOS boot type» и сохраните изменения, нажав на кнопку «Apply Changes».

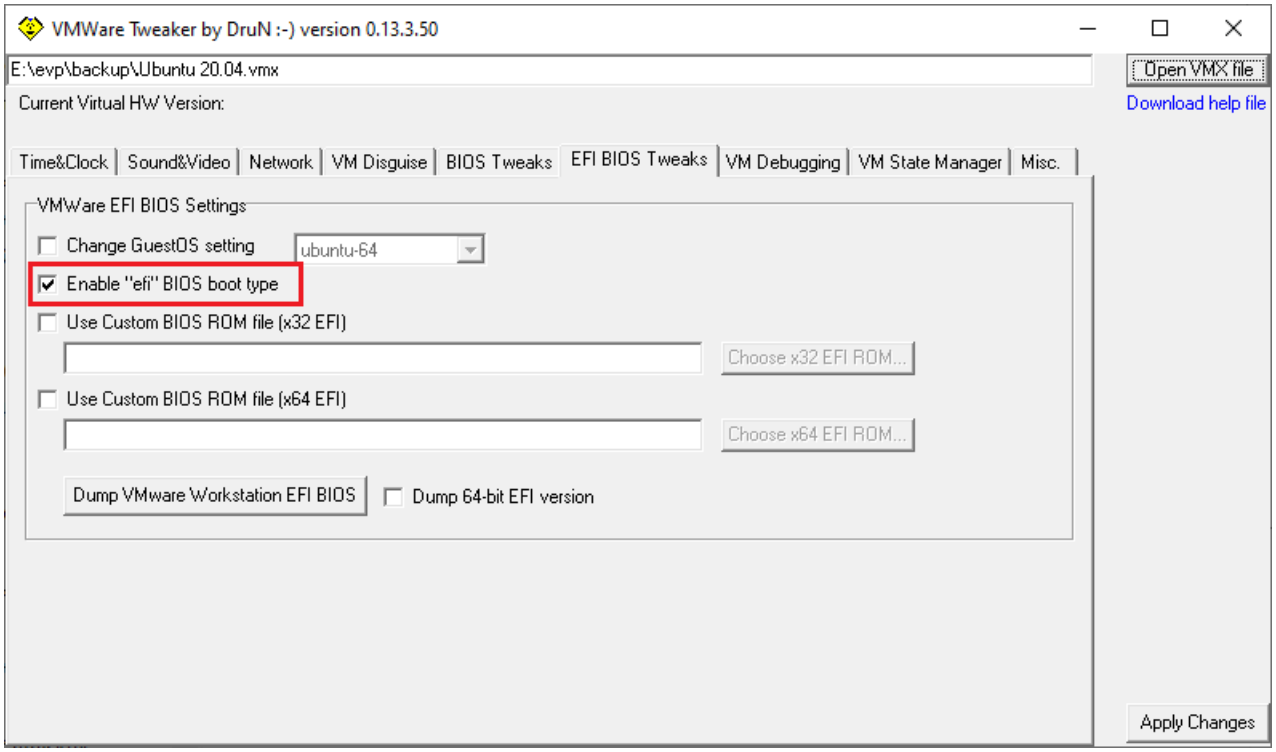


Рисунок 27 - Настройка BIOS

Создание виртуальной машины закончено.

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

3. 6. 2. 1. Настройка порта резервного ФПСУ в VMware

Особенностью работы ФПСУ с сетевым оборудованием является добавление виртуального MAC-адреса к физическому MAC-адресу сетевого адаптера.

Для обхода ограничения VMware, которое не позволяет изменить MAC-адрес сетевого адаптера, необходимо вручную прописать требуемый MAC-адрес в настройках виртуальной машины (в интерфейсе VMware) для данного сетевого адаптера.

Для работы резервного ФПСУ на VMware в настройках порта горячего резерва нужно установить отличающийся от основного ФПСУ MAC-адрес.

Для изменения конфигурации виртуальной машины с резервным ФПСУ требуется остановить виртуальную машину, открыть окно настроек виртуальной машины.

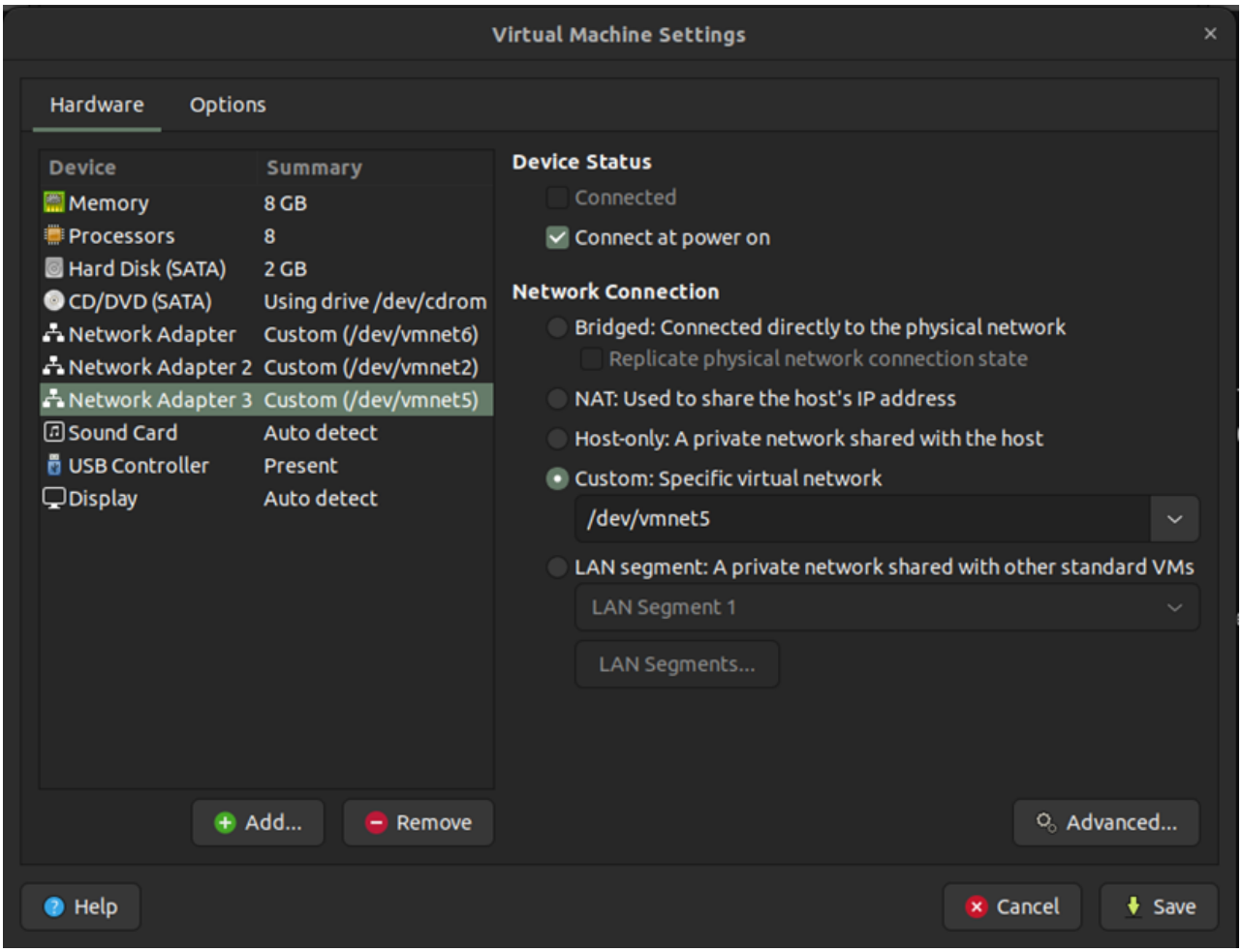


Рисунок 28 - Окно настроек виртуальной машины

Далее перейти в расширенные настройки сетевого адаптера, который подключен к порту горячего резерва ФПСУ и сгенерировать новый MAC-адрес, отличающийся от основного ФПСУ.

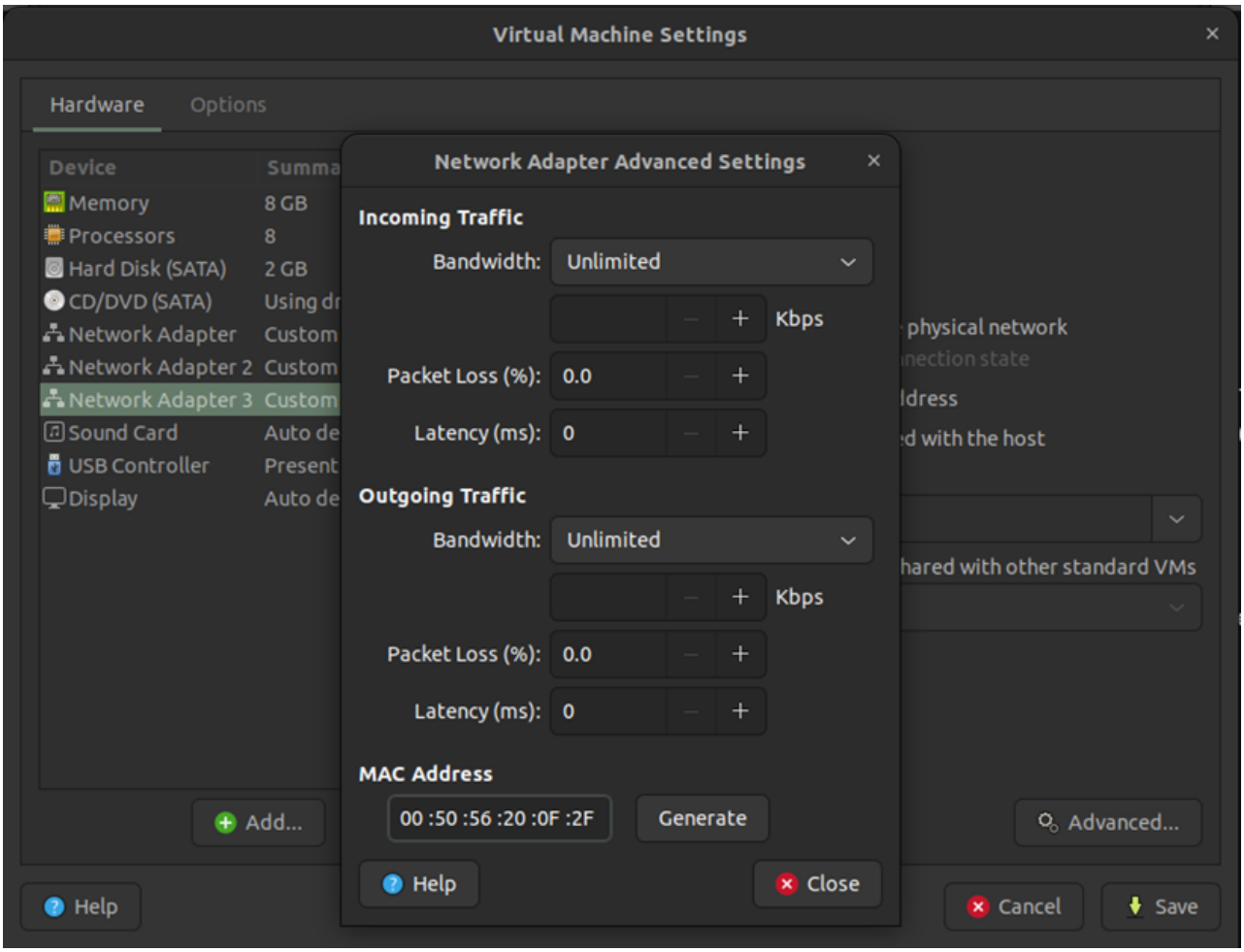


Рисунок 29 - Расширенные настройки сетевого адаптера

С разными MAC-адресами резервный ФПСУ синхронизируется и работает.

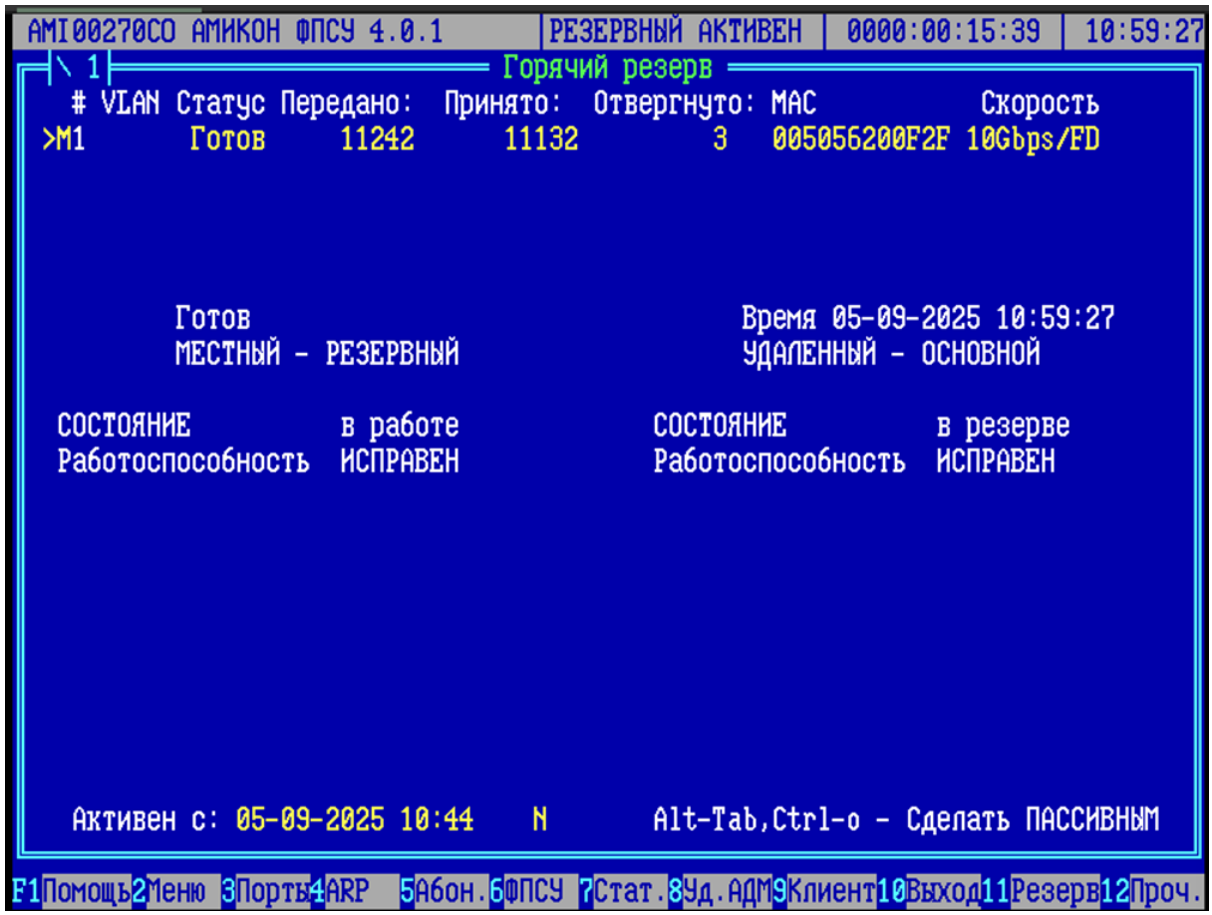


Рисунок 30 - Окно состояния подсистемы резервирования на резервном ФПСУ

3. 7. Консольное подключение к ФПСУ

Локальное управление ФПСУ, 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 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 потребуется поставляемый в комплекте с комплексом консольный кабель для RJ45 интерфейса.

Возможности работы с интерфейсом ФПСУ 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. 7. 1. Настройки BIOS для консольного подключения

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

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

- Console Redirection — установить значение Serial Port A;
- Build Rate — выбрать скорость передачи данных 115.2k;
- Terminal type — тип терминала установить значение VT100;
- Terminal Resolution — установить значение 80x24.

Примечание. Параметр Terminal Resolution в некоторых BIOS может отсутствовать.

Сохраните внесенные в BIOS изменения и перезапустите ФПСУ.

В примере рассматривается утилита настройки BIOS - Apatio Setup Utility, используемой на аппаратных платформах семейств FPSUIP-STD3, FPSUIP-EXT3, FPSUIP-ORD3. Название значимых параметров может отличаться от приведенных выше. Откройте утилиту Apatio, перейдите на вкладку Advanced, выберите пункт Serial Port Console Redirection.

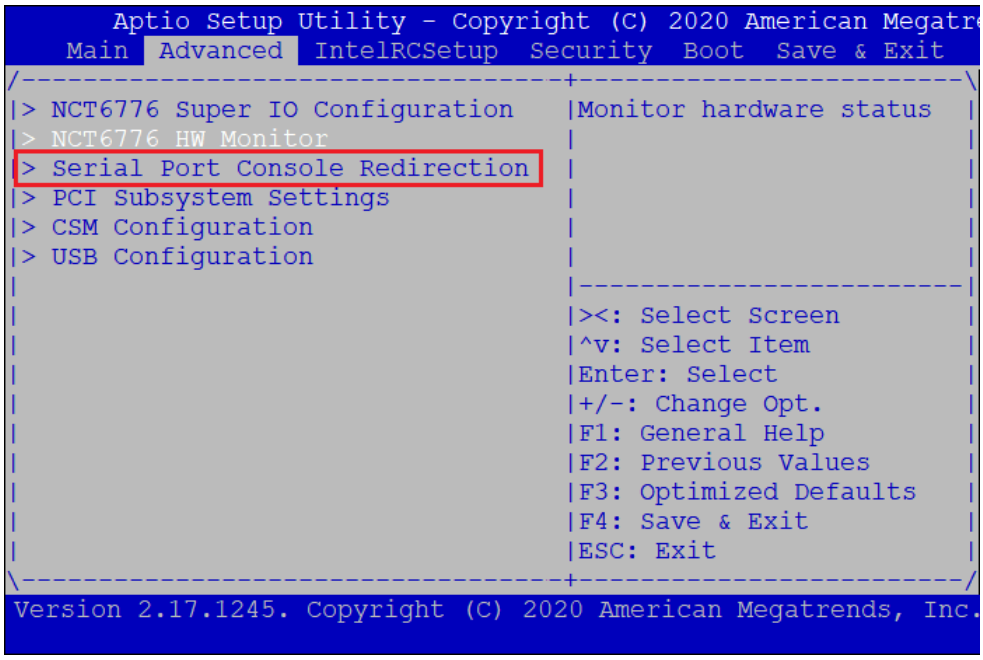


Рисунок 31 - Настройки BIOS

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

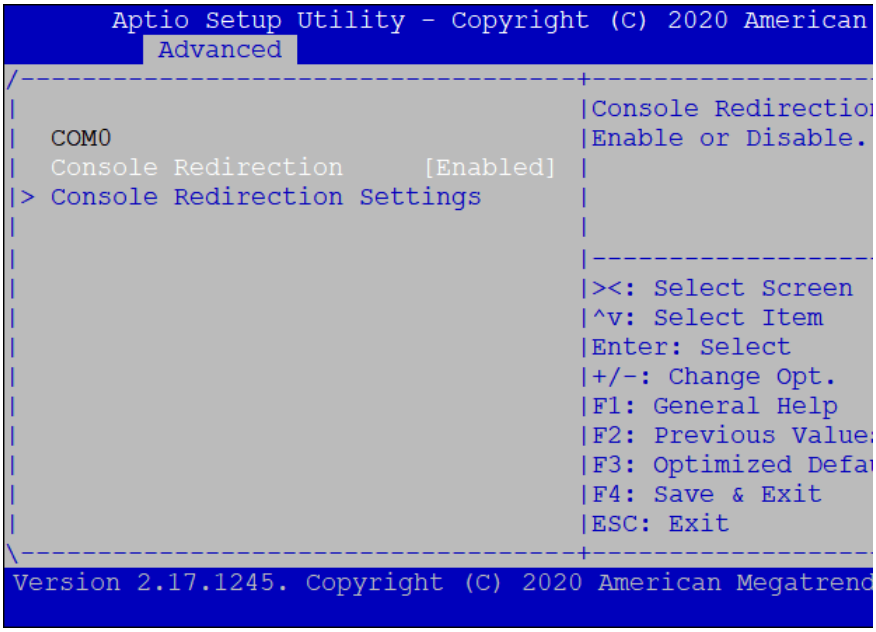


Рисунок 32 - Настройка Console Redirection

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.

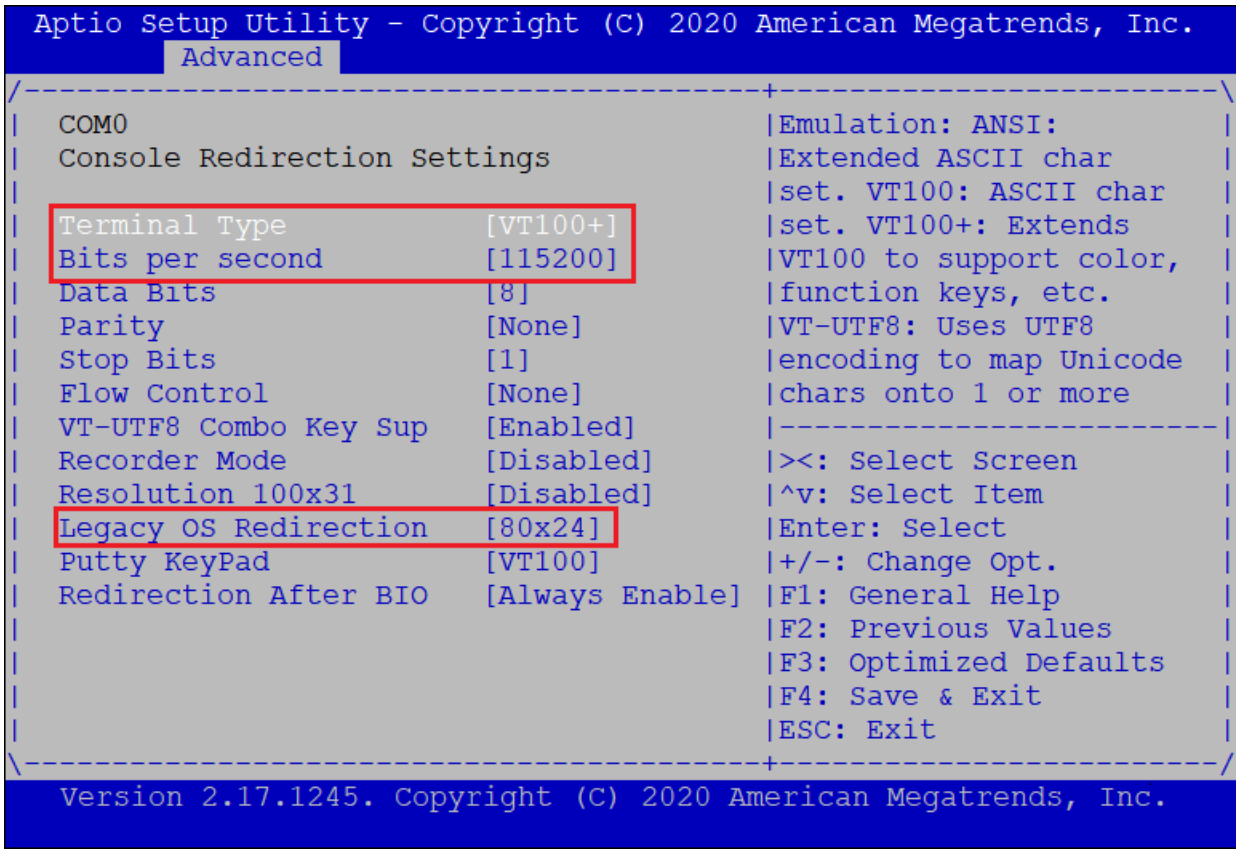


Рисунок 33 - Установка параметров

Сохраните внесенные в BIOS изменения и перезапустите ФПСУ.

3. 7. 2. Установка драйверов консольного кабеля

Для использования консольного подключения к ФПСУ 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 ООО «АМИКОН» https://amicon.ru/download.php драйвер для подключения консоли к ФПСУ для Windows.



Рисунок 34 - 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.

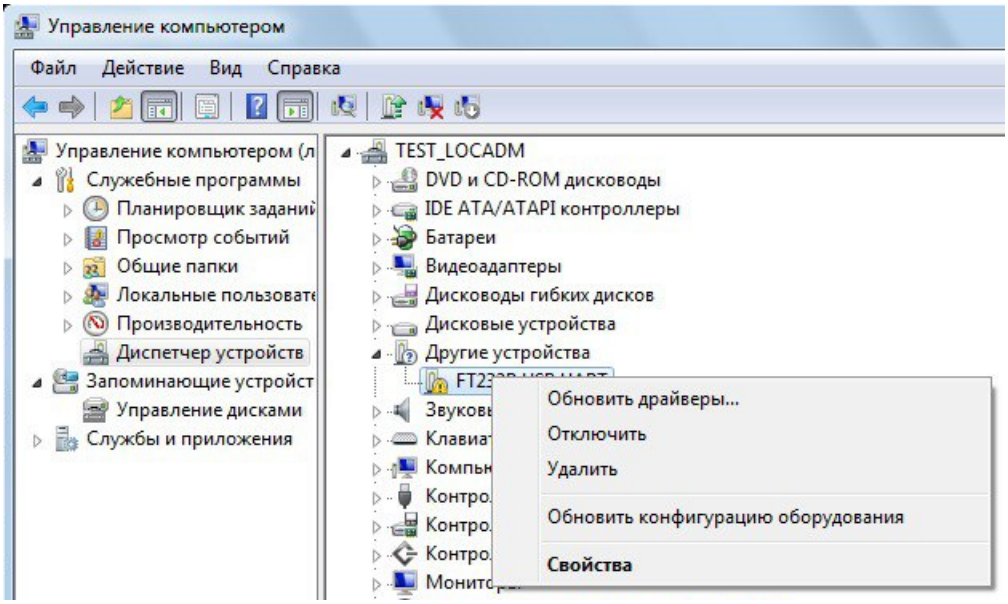


Рисунок 35 - Отображение консольного кабеля в диспетчере устройств

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

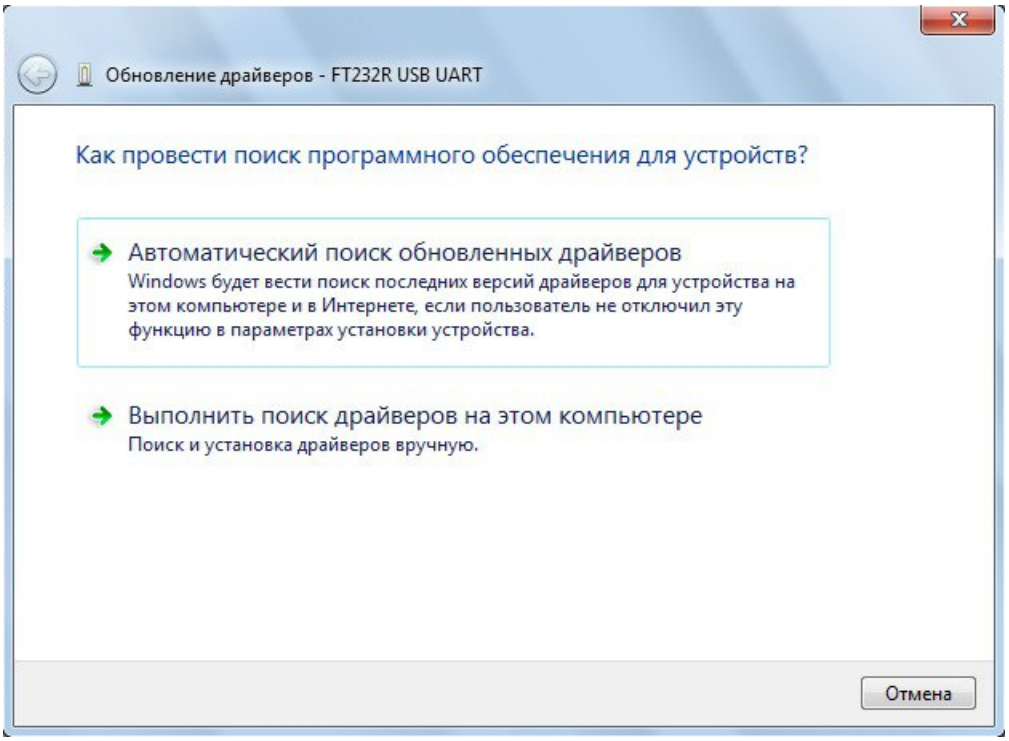


Рисунок 36 - Мастер установки драйвера

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

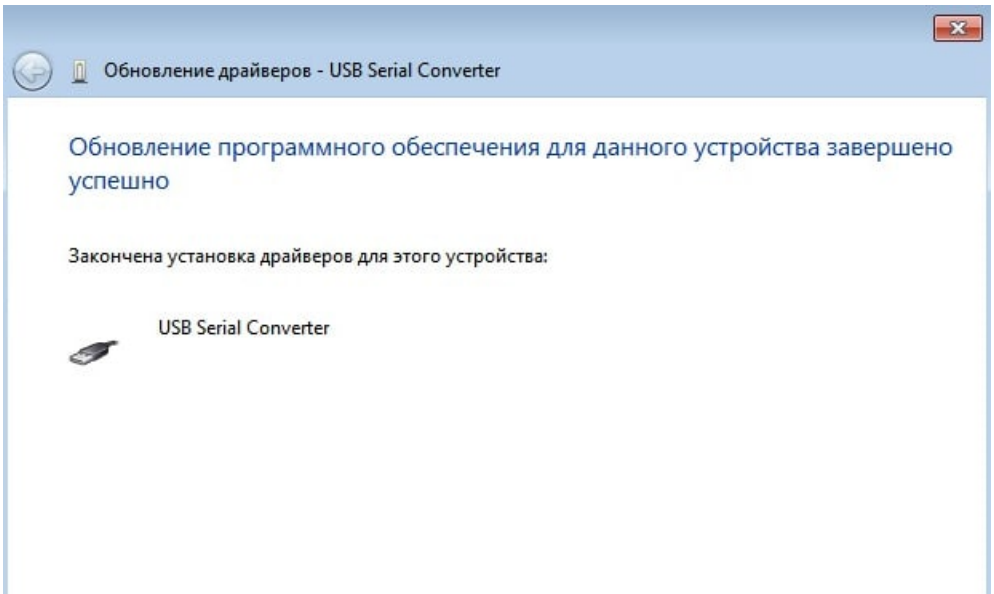


Рисунок 37 - Обновление драйвера консольного кабеля

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.

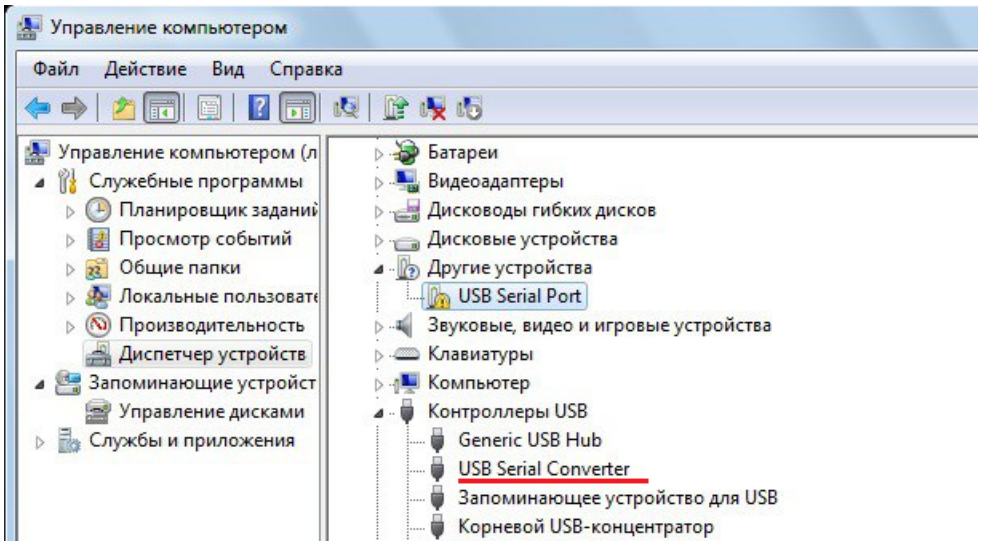


Рисунок 38 - Отображение консольного кабеля после установки драйвера

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

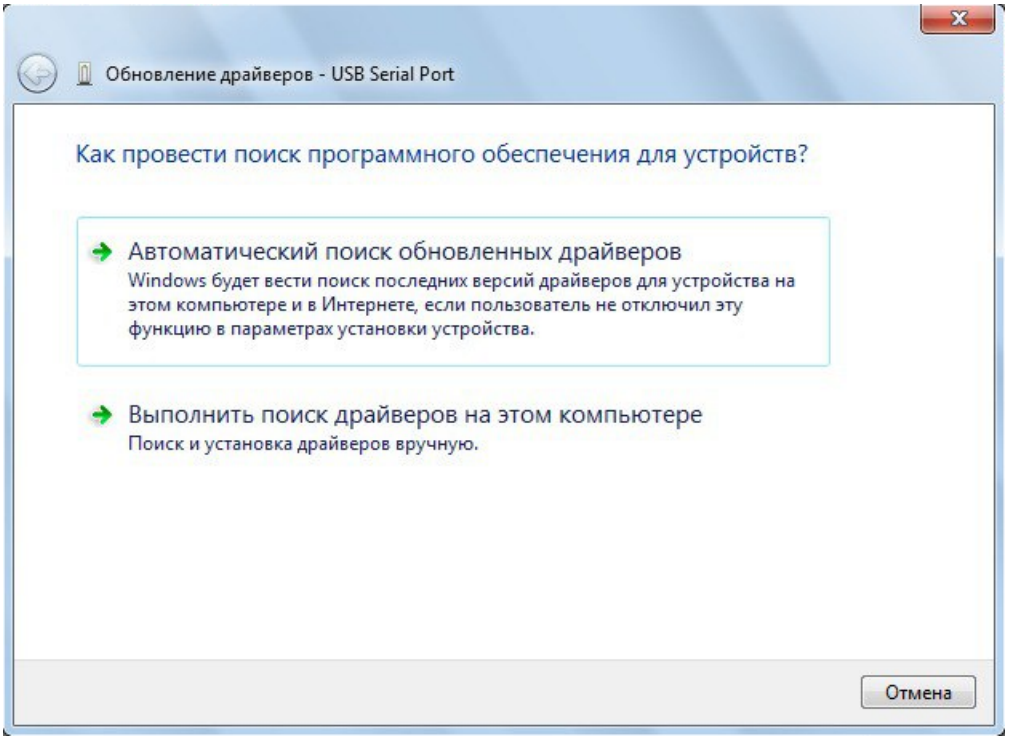


Рисунок 39 - Мастер установки драйвера

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

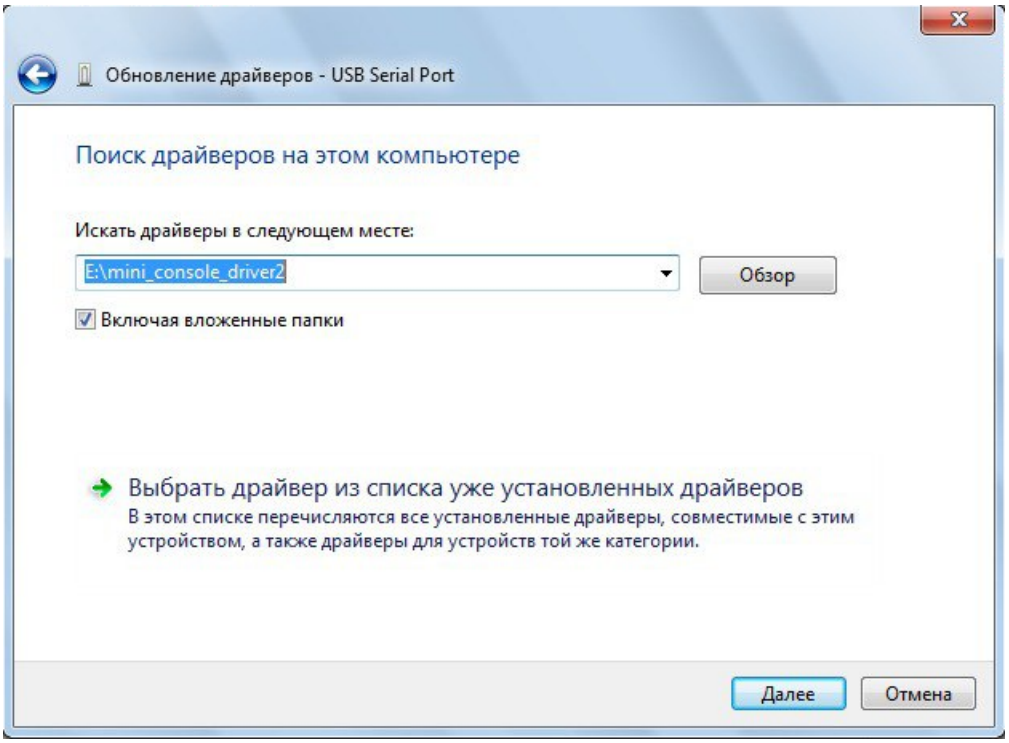


Рисунок 40 - Выбор каталога с драйвером

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

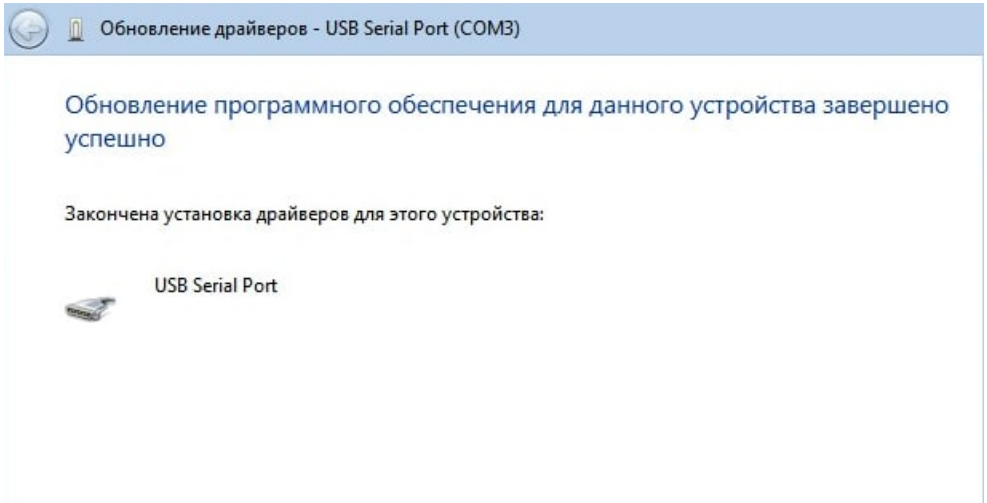


Рисунок 41 - Обновление драйвера консольного кабеля

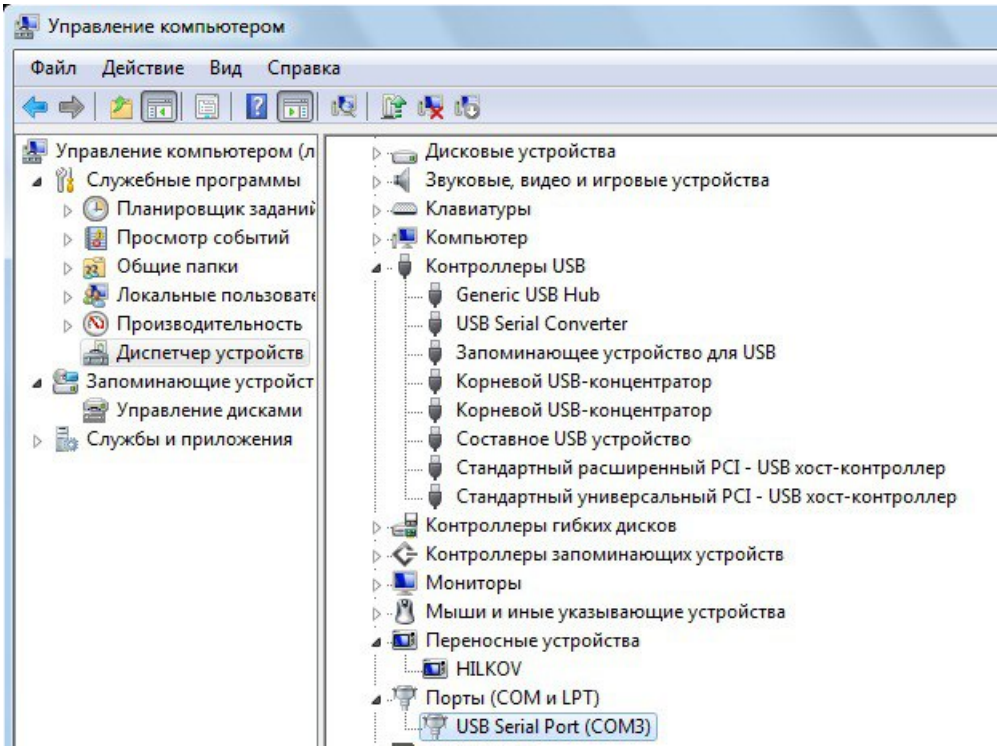


Рисунок 42 - Отображение консольного кабеля после повторной установки драйвера

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 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.

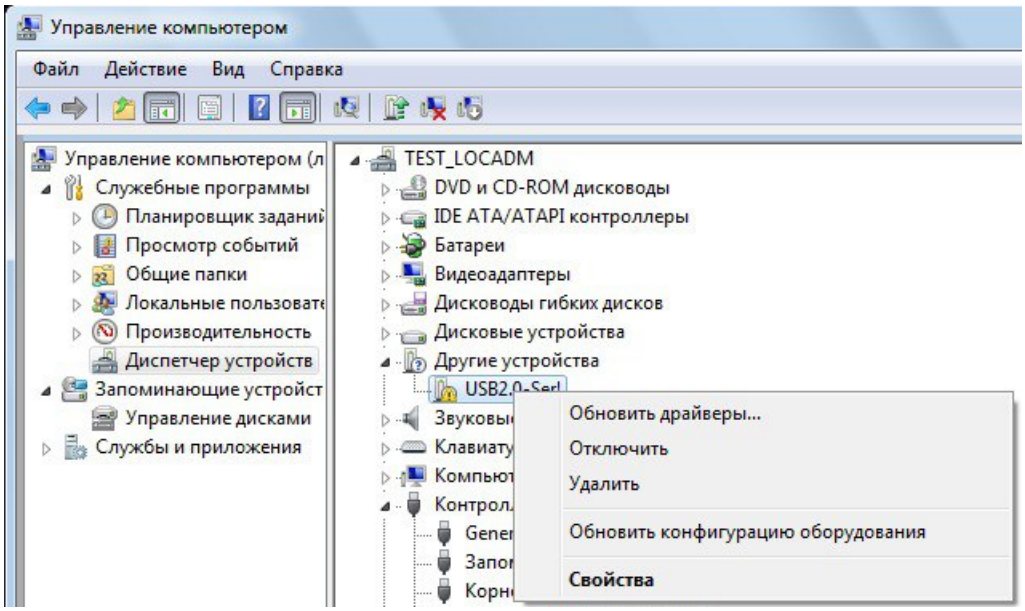


Рисунок 43 - Отображение консольного кабеля в диспетчере устройств

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.

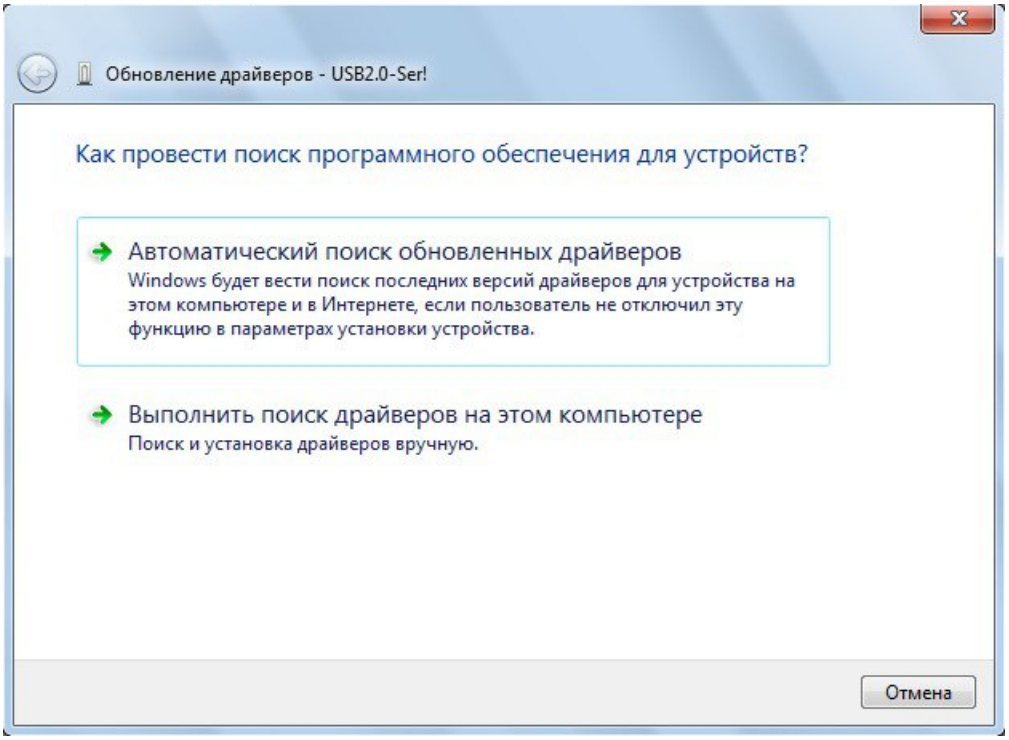


Рисунок 44 - Мастер установки драйвера

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

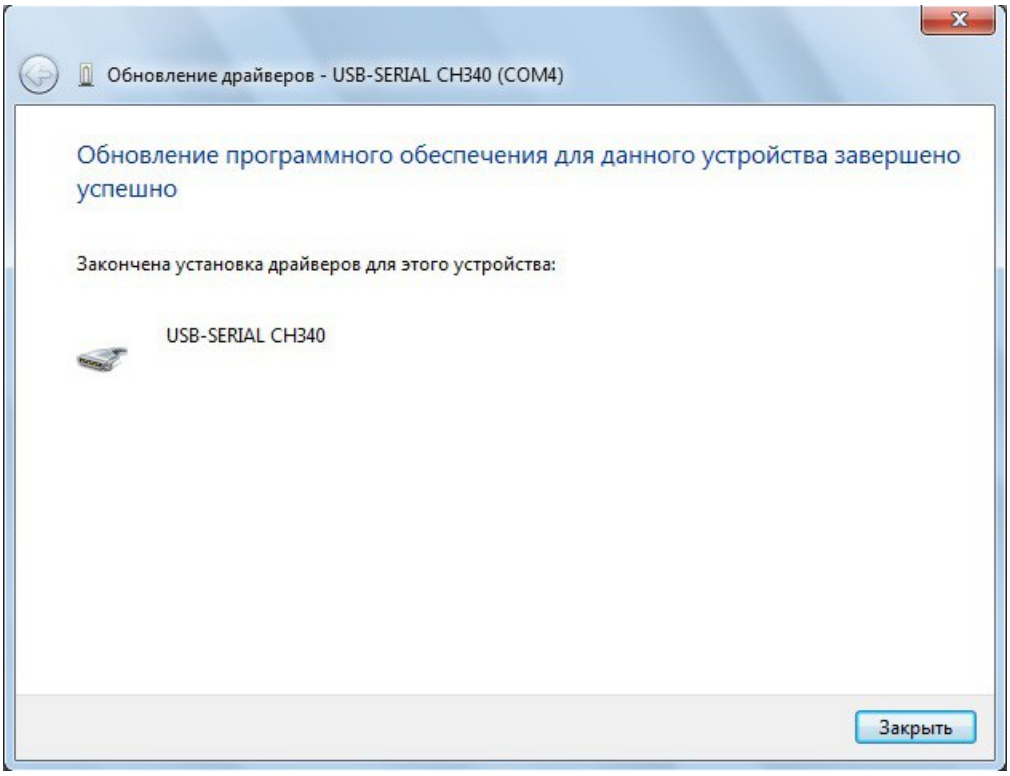


Рисунок 45 - Обновление драйвера консольного кабеля

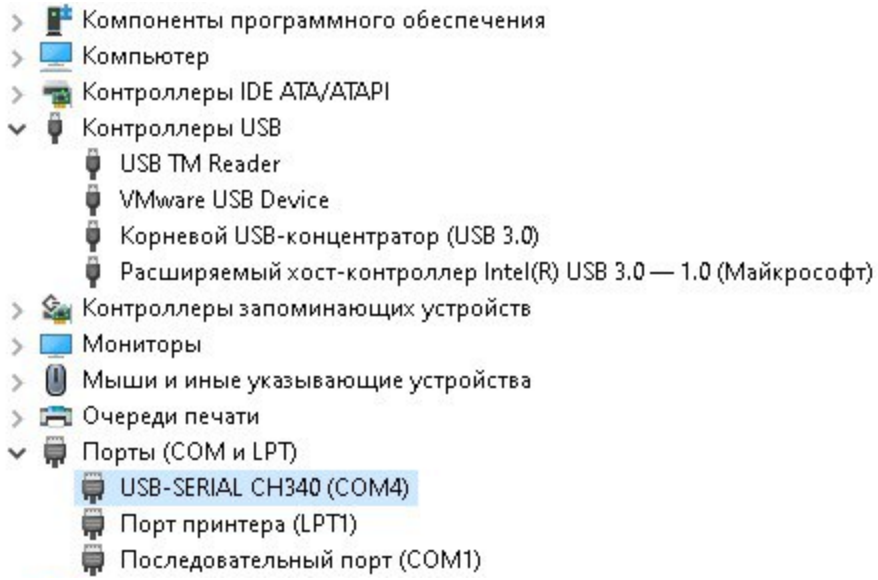


Рисунок 46 - Отображение консольного кабеля после установки драйвера

3. 7. 3. Подключение к ФПСУ с помощью «Терминала»

Для консольного подключения к ФПСУ, осуществляемого с Windows станций, следует использовать программу «Терминал».

«Терминал» доступен для загрузки с официального сайта ООО «АМИКОН»

https://amicon.ru/download.php, ссылка с архивом «Терминала» имеет название «ФПСУ-терминал для Windows».

Перед запуском «Терминала» соедините консольным кабелем рабочую станцию с ФПСУ. 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 «Терминале» при настройке подключения.

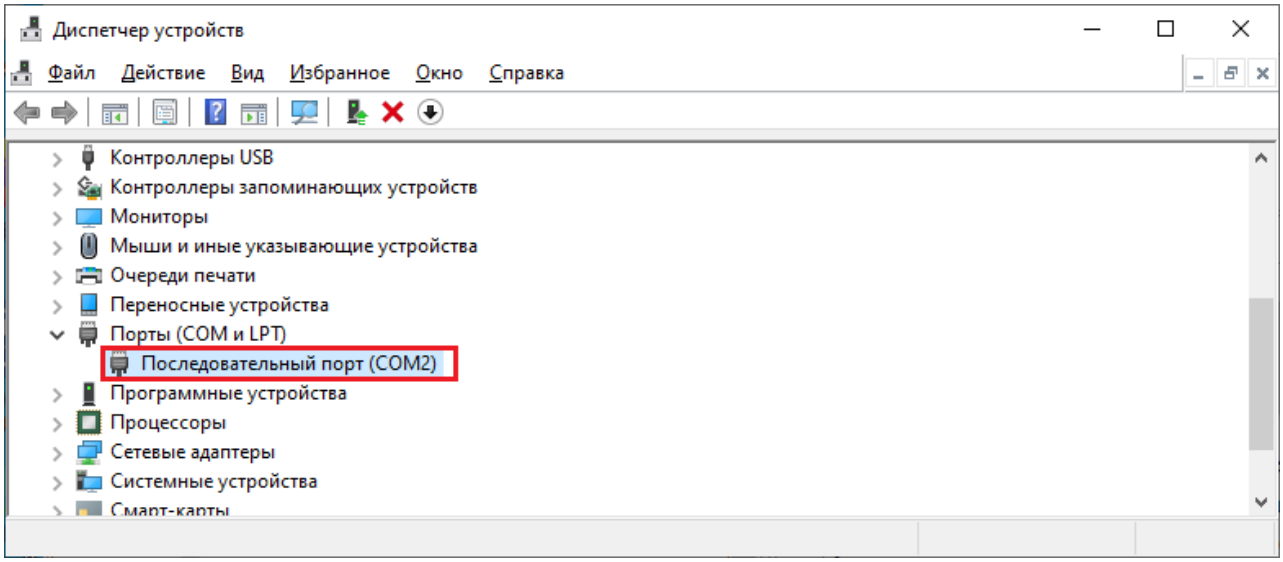


Рисунок 47 - COM порт консольного соединения в диспетчере устройств

Запустите исполняемый файл «Терминала», 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».

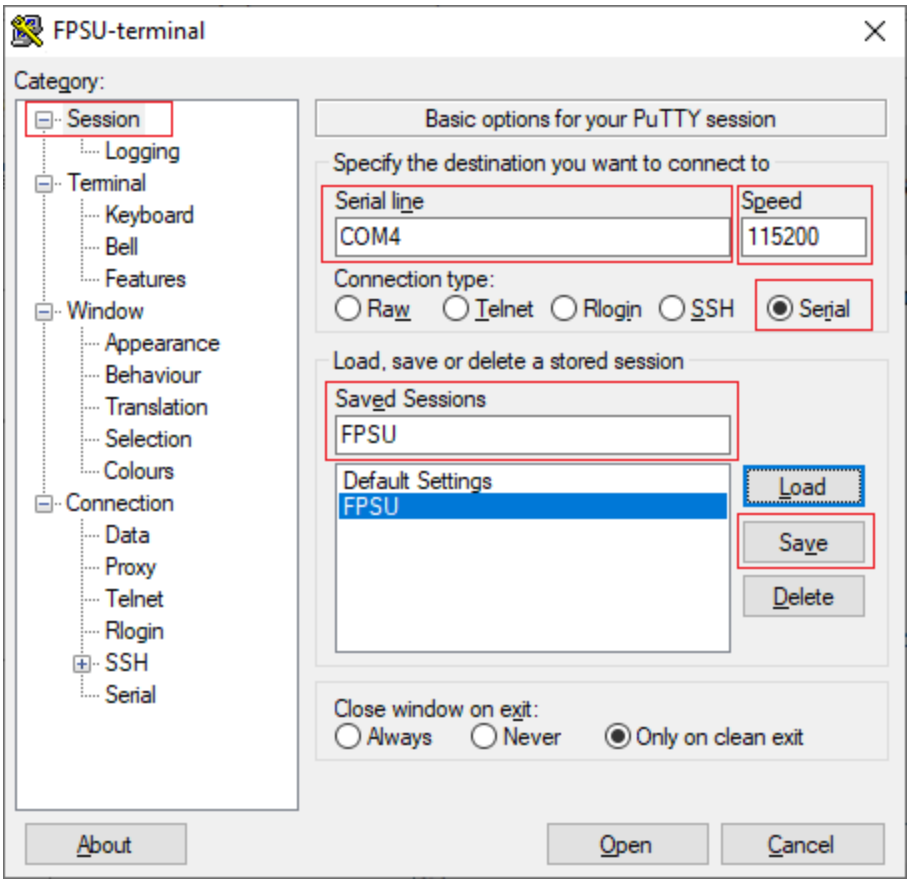


Рисунок 48 - Настройка подключения

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

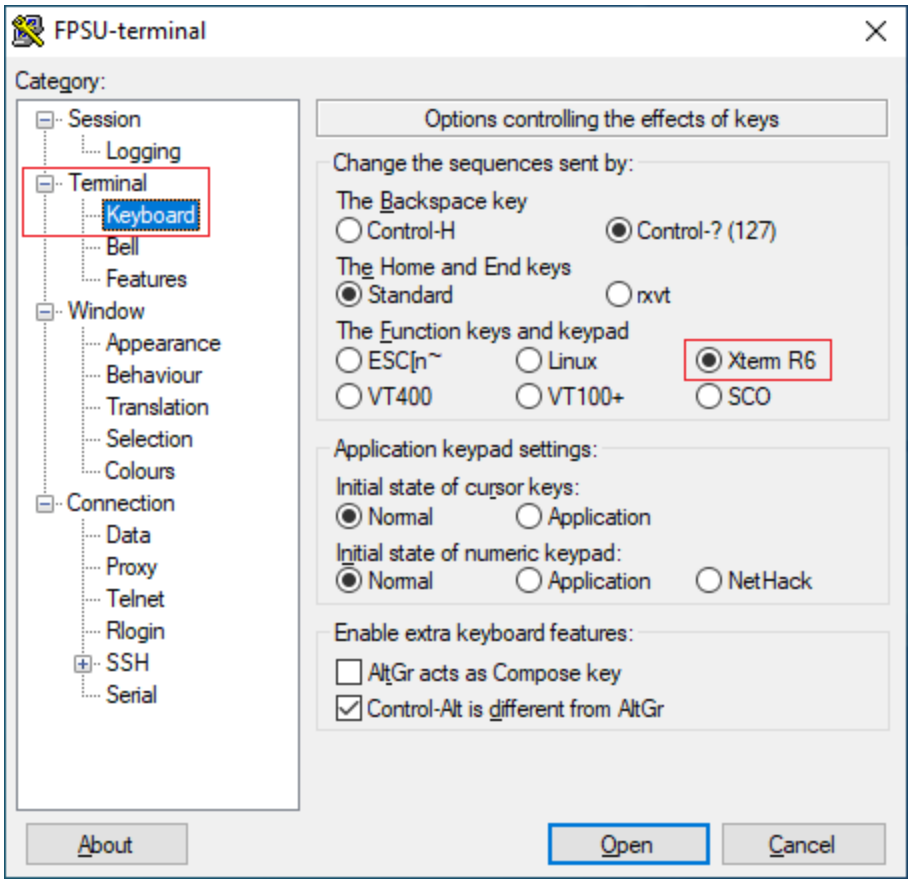


Рисунок 49 - Выбор типа клавиатуры

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

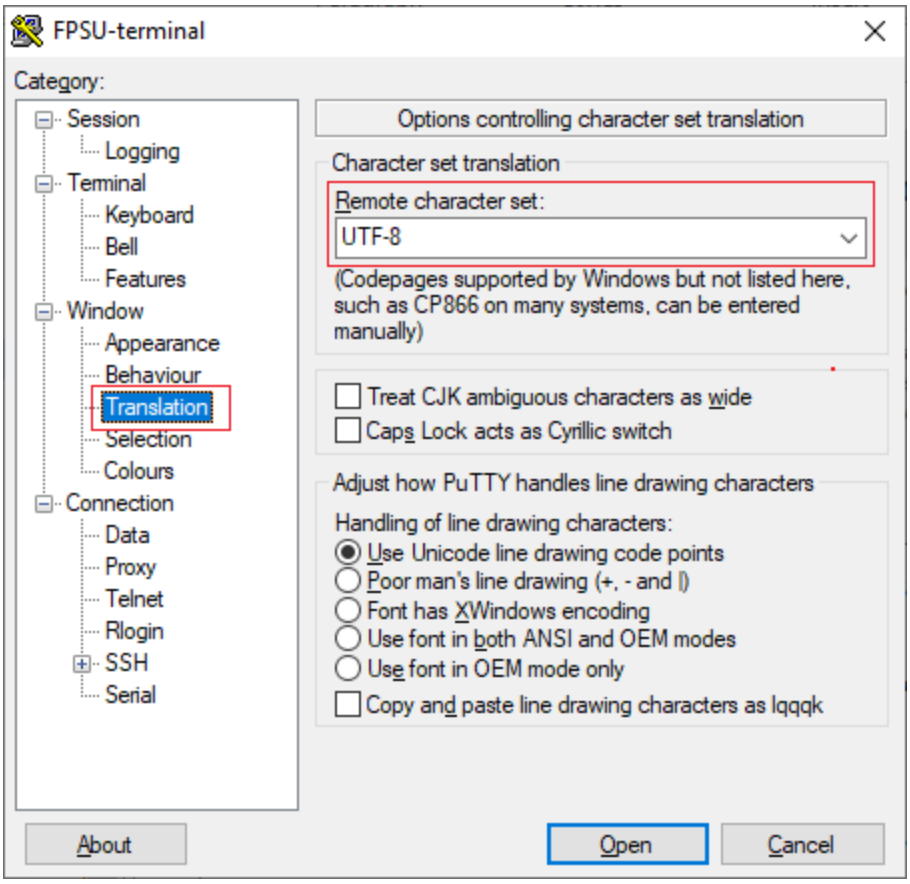


Рисунок 50 - Выбор кодировки

Задайте количество строк – 25 (устанавливается в интерфейсе «Терминала»: Window–Rows).

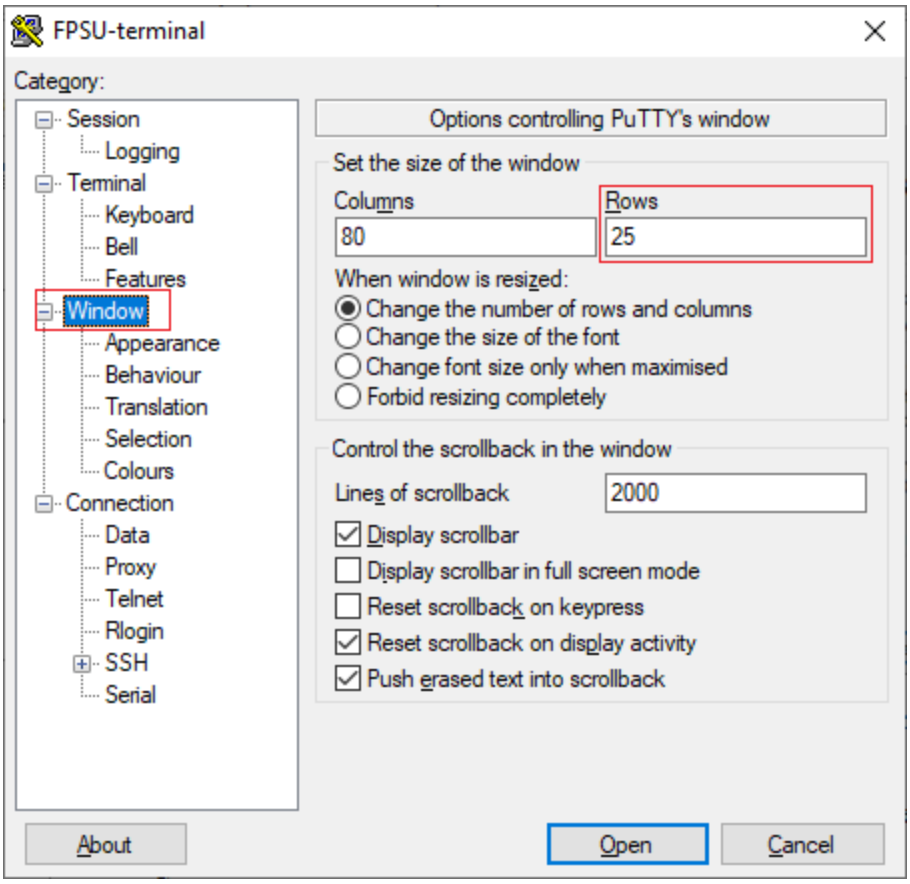


Рисунок 51 - Выбор количества строк

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

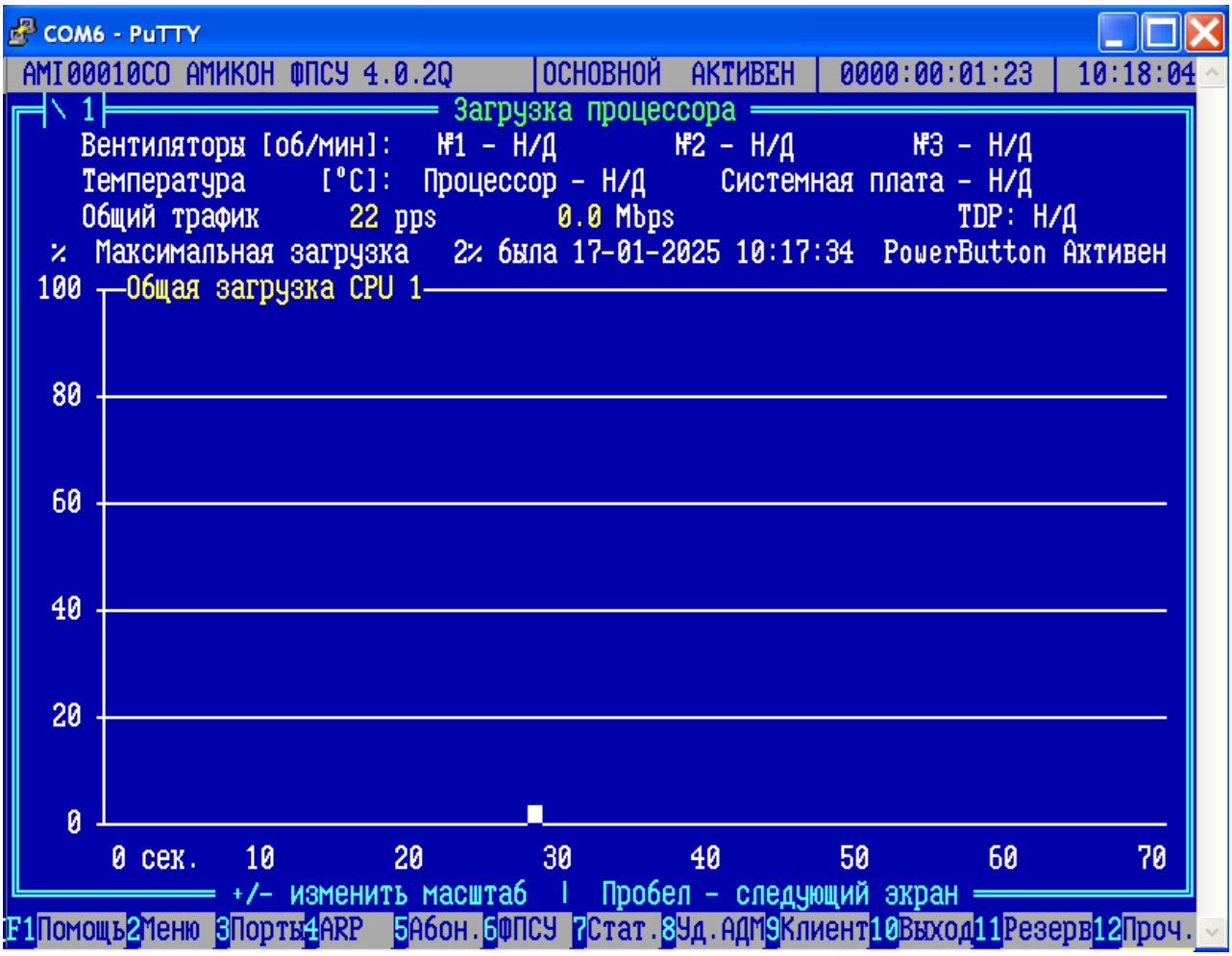


Рисунок 52 - Консольное подключение установлено

3. 7. 4. Авторизация пользователя на ФПСУ

Разграничение доступа допущенных лиц и контроль их полномочий при запуске ФПСУ и управлении его работой осуществляется по предъявляемым допущенными лицами электронным идентификаторам «touch-memory» (в качестве которых могут выступать микроэлектронные USB-устройства «TM-Key» производства ООО «АМИКОН» или устройства iButton DS1993 – DS1996) и символьным паролям (подробнее см. пункт «Разграничение доступа и пользователи»).

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

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

В процессе идентификации пользователя запрашиваются полномочия допущенного лица, на экран ФПСУ выдается следующее сообщение для предъявления ТМ-идентификатора :

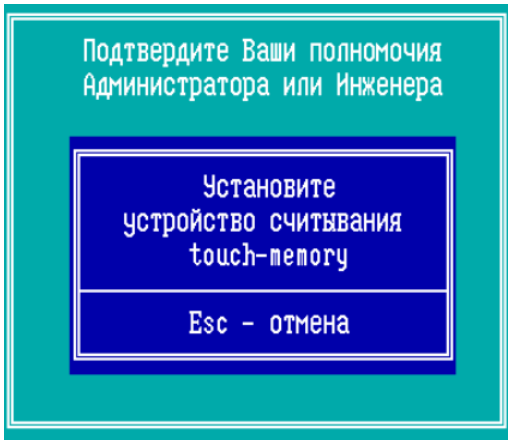


Рисунок 53 - Подтверждение полномочий

В случае предъявления неверного ТМ-идентификатора на экран выводится сообщение о незарегистрированном на данном ФПСУ ТМ-идентификаторе:

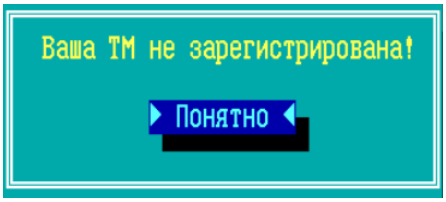


Рисунок 54 - Незарегистрированный ТМ-идентификатор

Если пользователь в течение 10 попыток не предъявил корректный ТМ-идентификатор потребуется перезагрузка ФПСУ, на экран будет выдано сообщение:

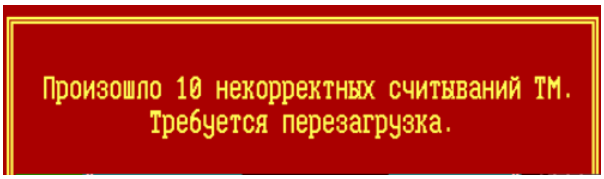


Рисунок 55 - Требование перезагрузки ФПСУ

Кроме того, вход может быть защищен паролем подключаемого ТМ. В этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе (подробнее см. пункты «Установка пароля Главного администратора», «Повторная регистрация ТМ-идентификатора»). Для ввода пароля ТМ на экран выводится следующее сообщение:

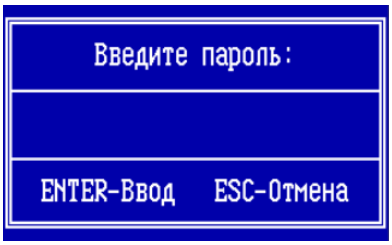


Рисунок 56 - Ввод пароля ТМ

При вводе неправильного пароля на экран выводится сообщение с количеством оставшихся попыток ввода пароля:

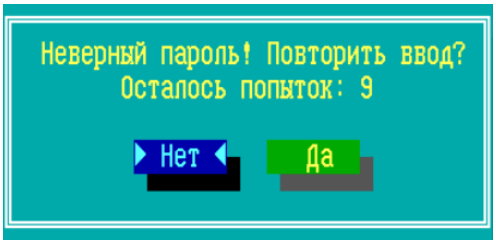


Рисунок 57 - Ввод неверного пароля ТМ

В случае исчерпания 10 попыток ввода пароля ТМ доступ на ФПСУ будет заблокирован на 5 минут и будет выдано сообщение:

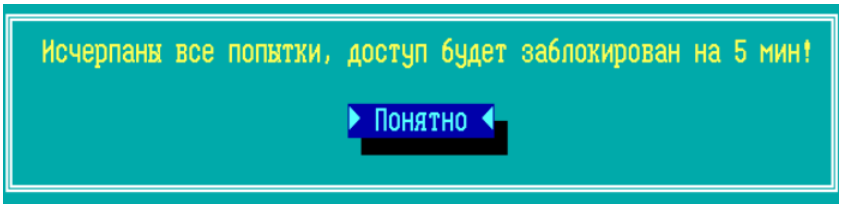


Рисунок 58 - Исчерпание попыток ввода пароля ТМ

Во время блокировки ФПСУ в случае запуска или выполнения команды меню на экран выдается сообщение с датой и временем блокировки:

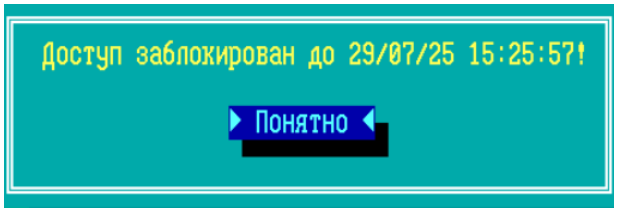


Рисунок 59 - Дата и время блокировки ФПСУ

После истечения времени блокировки доступ на ФПСУ восстанавливается.

3. 8. Установка ПО ФПСУ с дистрибутива

Программно-аппаратный комплекс ФПСУ поставляется с предустановленным на аппаратную платформу программным обеспечением. Описанные ниже процедуры установки программного обеспечения ФПСУ используются в случае необходимости выполнения повторной установки программного обеспечения ФПСУ. Для повторной установки программного обеспечения ФПСУ в виртуальную среду см. пункт Установка ПО ФПСУ с установочного носителя.

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

- установочный USB-flash накопитель;
- ТМ-идентификатор Главного Администратора ФПСУ;
- Аппаратная платформа ФПСУ, на которую будет установлено ПО ФПСУ.

3. 8. 1. Установка ПО ФПСУ с установочного носителя

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

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



Рисунок 60 - 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 серийный номер (значение поля «Serial#») **обязан** быть «XXX00000.XX»:

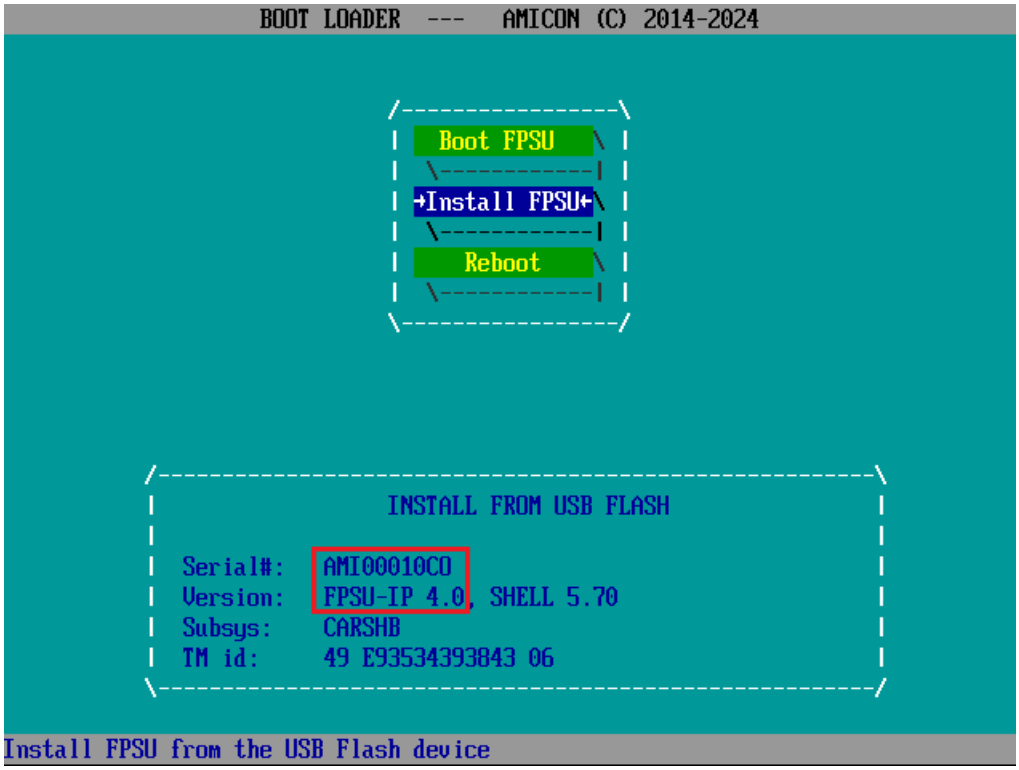


Рисунок 61 - Экран установки ФПСУ

Если серийный номер не совпадает с ожидаемым, следует прекратить установку и обратиться к поставщику программного обеспечения.

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. Подтвердите продолжение установки выбором команды «Да»:

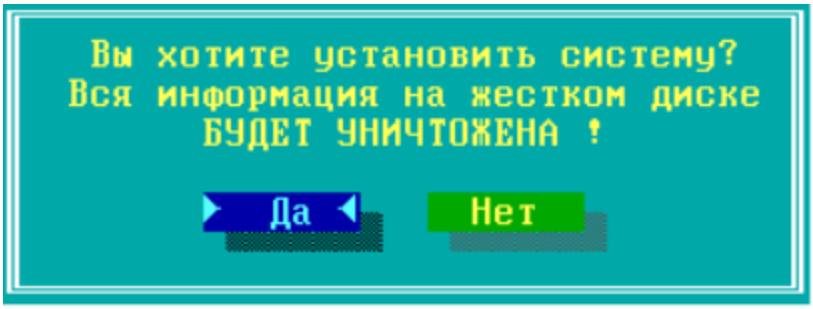


Рисунок 62 - Очистка ПЗУ ФПСУ

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

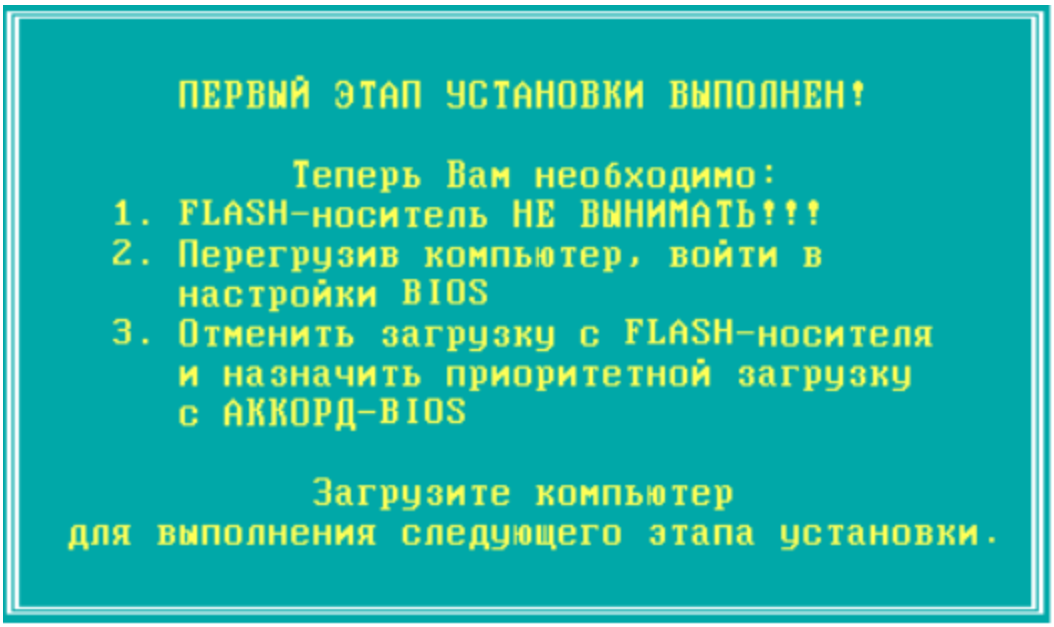


Рисунок 63 - Завершение первого этапа установки

5. После перезагрузки и запуска операционной системы ФПСУ, начнется второй этап установки программного обеспечения. Для продолжения потребуется подтвердить полномочия Главного администратора (права роли «Администратор» класса «Главный администратор», см. пункт «Разграничение доступа и пользователи», Таблица 3):

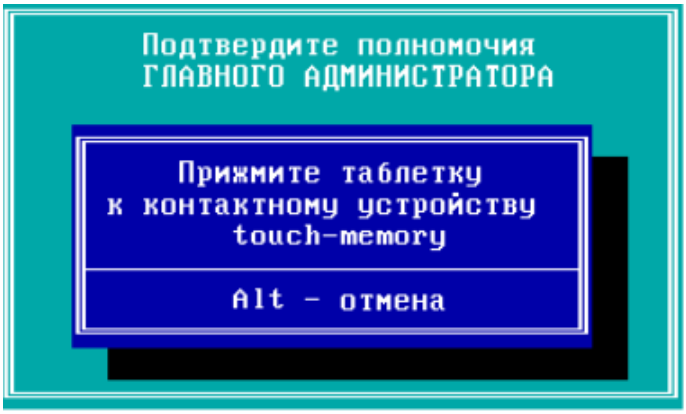


Рисунок 64 - Проверка полномочий Главного администратора

6. Если инсталляционный комплект выдан для ФПСУ с установленной подсистемой «горячего» резервирования, то после проверки полномочий Главного администратора программа установки предложит указать режим функционирования данного ФПСУ в комплексе «горячего» резерва. Выберите

требуемый режим — «Основной/Единственный» или «Горячий резерв» и нажмите клавишу <*Enter*>.

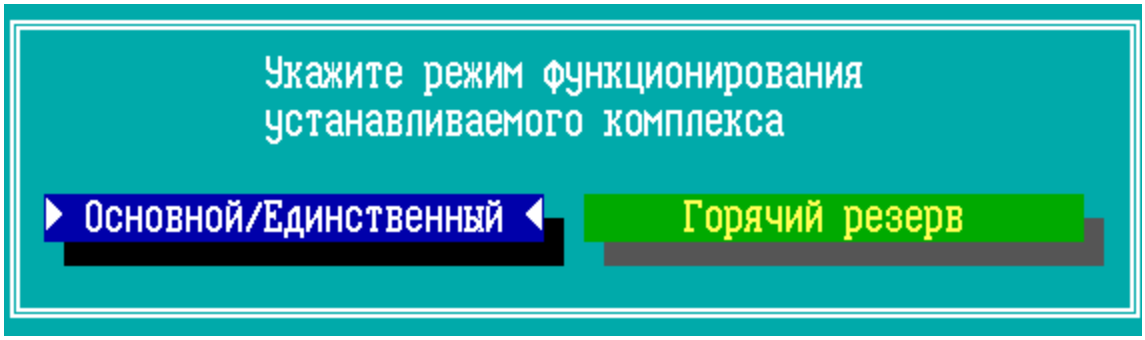


Рисунок 65 - Выбор режима функционирования ФПСУ

7. После выбора режима функционирования ФПСУ в подсистеме «горячего» резервирования, начнется формирование разделов на жестком диске и затем копирование файлов ФПСУ на ПЗУ:

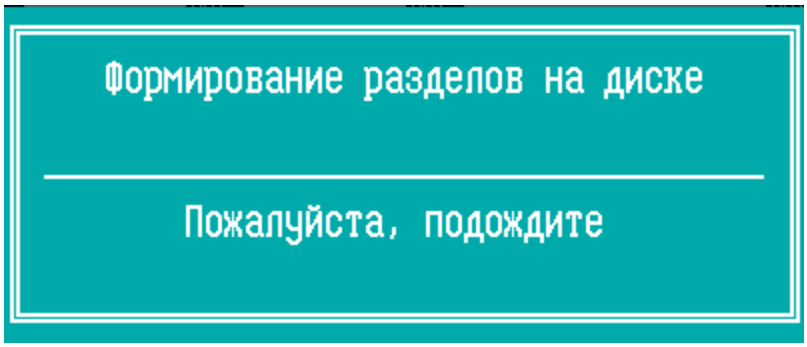


Рисунок 66 - Формирование разделов

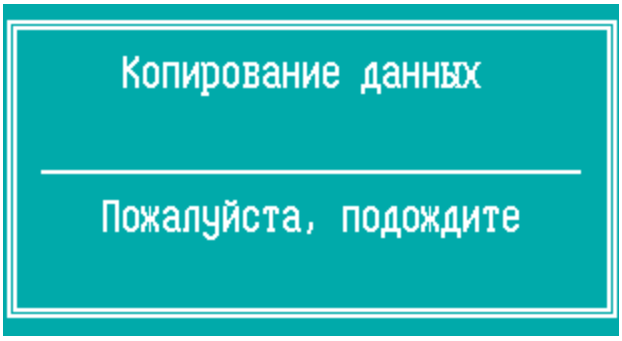


Рисунок 67 - Копирование системных файлов

После завершения копирования системных файлов на ПЗУ комплекса, ***установка программного обеспечения комплекса завершается***. На экран будет выдано сообщение об успешной установке комплекса.

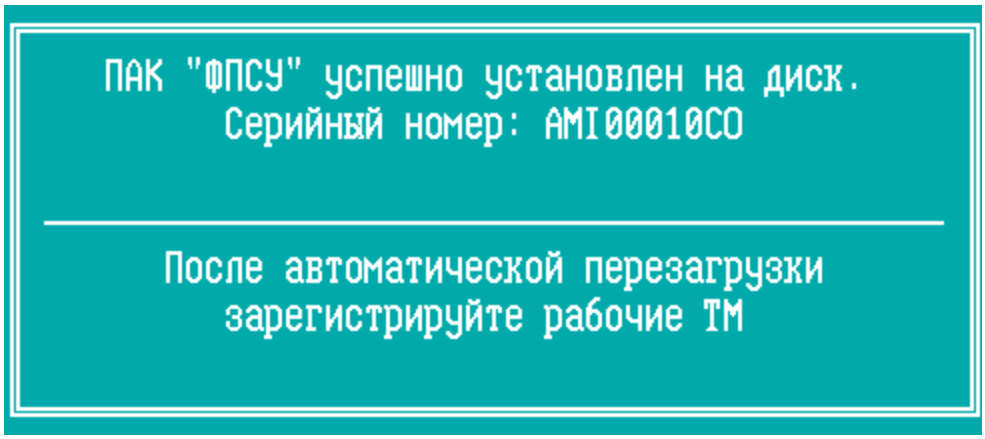


Рисунок 68 - Сообщение об успешной установке

ФПСУ будет перезагружен, и после перезагрузки начнет работать в технологическом режиме (см. пункт. «Технологический режим ФПСУ»).

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

3. 8. 2. Установка ФПСУ с готового образа диска на USB-носителе в QEMU/KVM

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

Запустите виртуальную машину, нажав на черный треугольник (на рисунке QEMU/KVM 6.2.0 на Ubuntu 22.04.4 LTS).

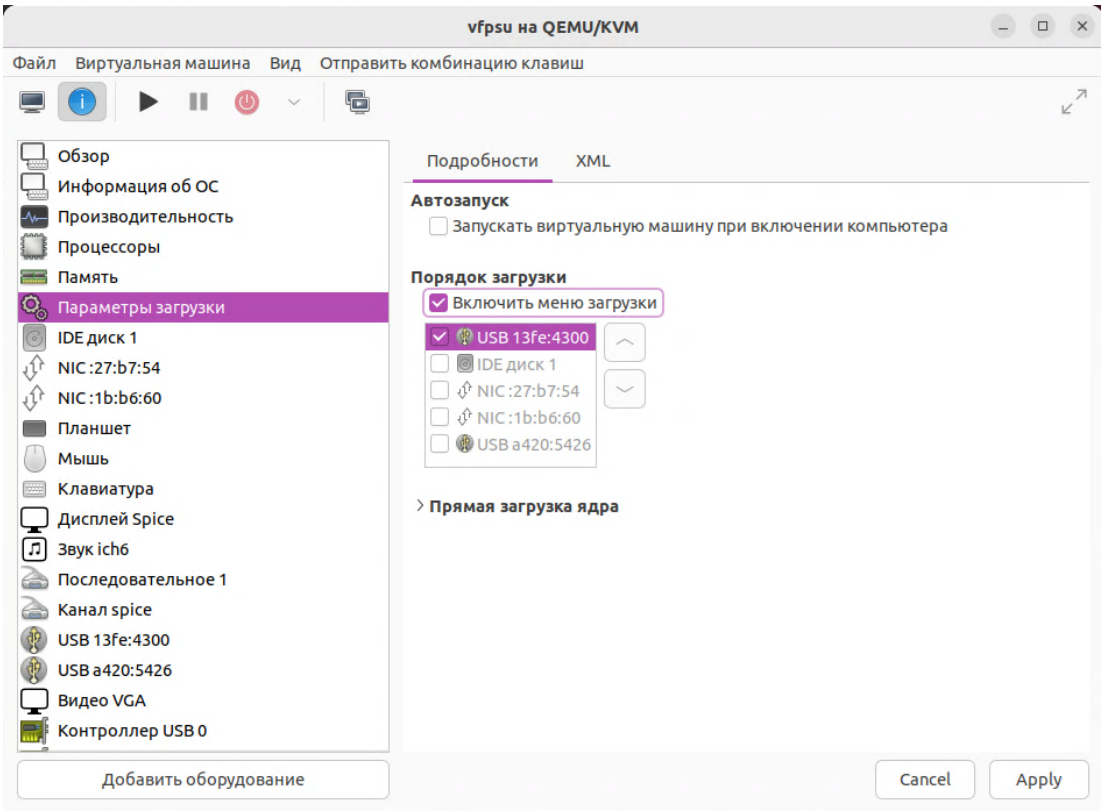


Рисунок 69 - Запуск виртуальной машины

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

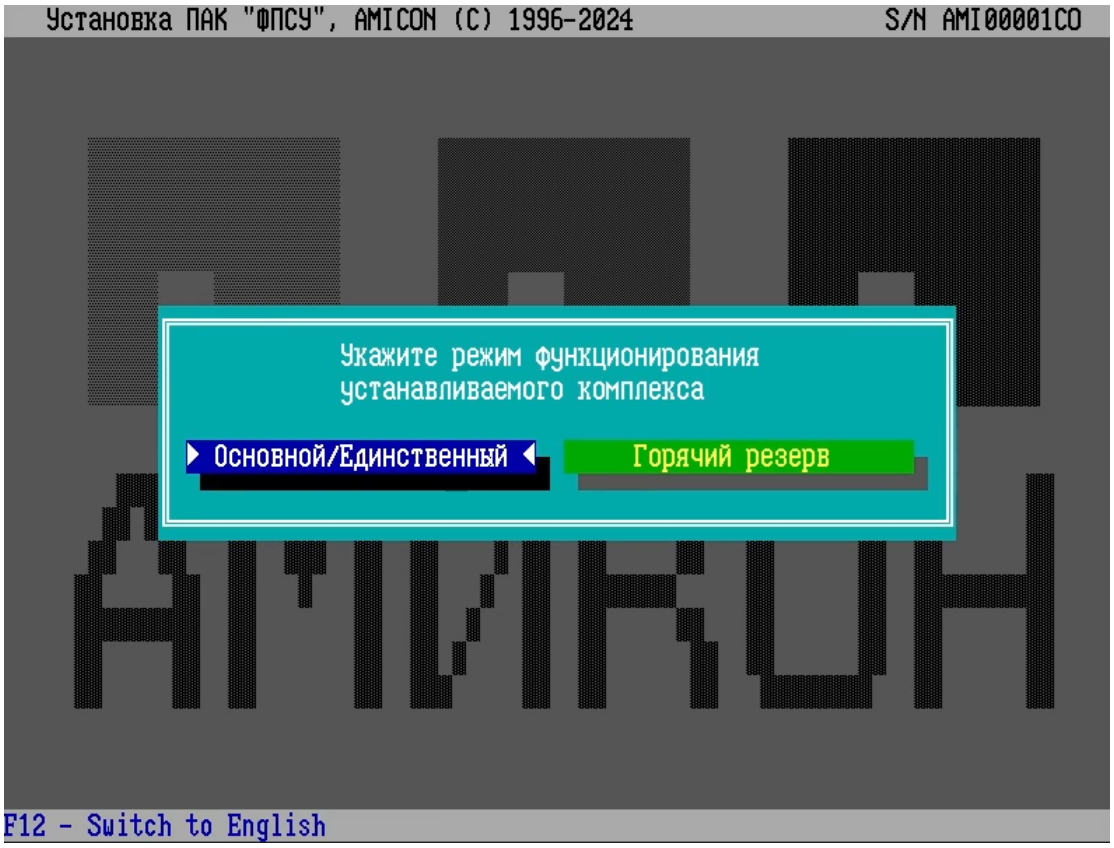


Рисунок 70 - Выбор режима функционирования ФПСУ

После выбора режима функционирования ФПСУ в подсистеме «горячего» резервирования будет запрашиваться ТМ Главного администратора для регистрации (при записи ТМ на него записывается ключ запуска).



Рисунок 71 - Регистрация ТМ Главного администратора

Затем начнется формирование разделов на диске:

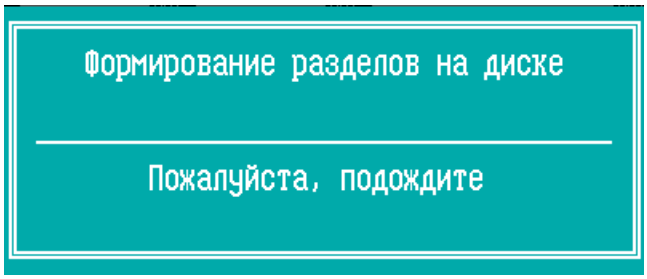


Рисунок 72 - Формирование разделов

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

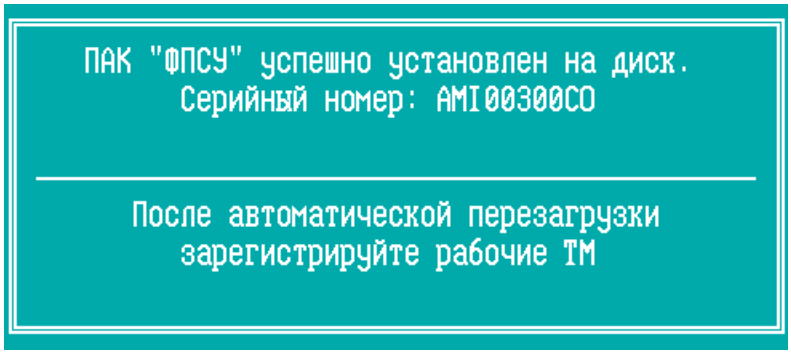


Рисунок 73 - ФПСУ установлен на диск

Отключите USB-носитель с инсталляционным комплектом ФПСУ.

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

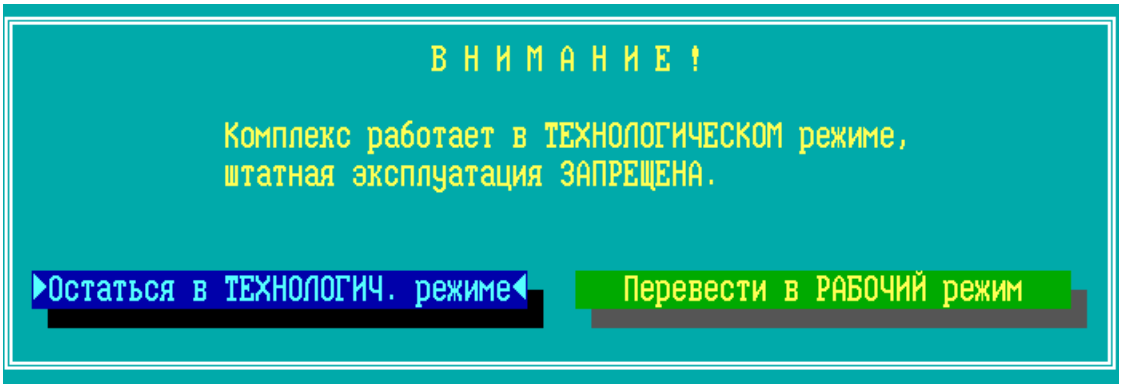


Рисунок 74 - Оповещение о работе в технологическом режиме

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

Необходимо произвести начальные настройки ФПСУ, зарегистрировать ТМ (см. пункт «Окно регистрации ТМ»).

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

3. 9. Технологический режим ФПСУ

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

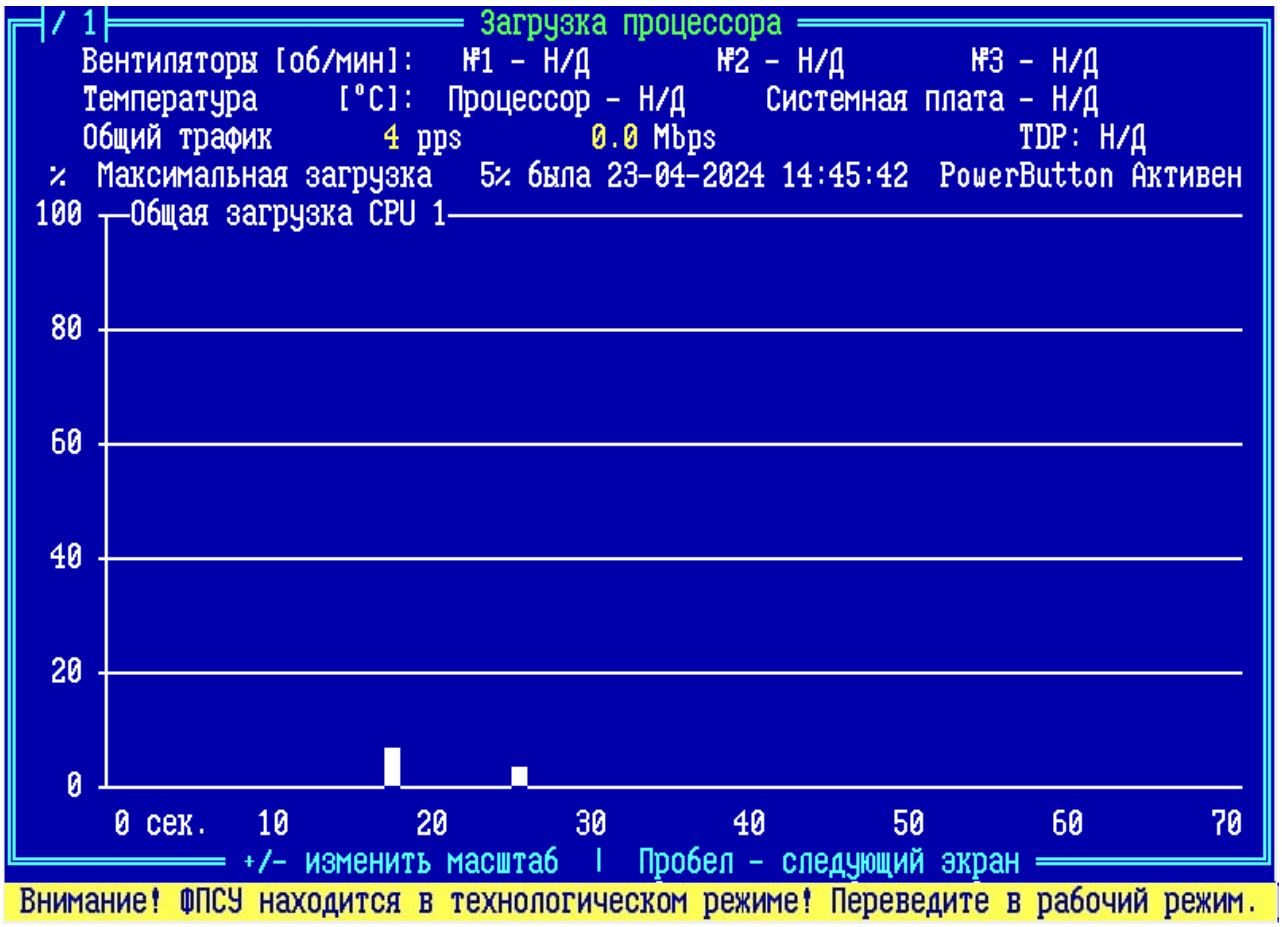


Рисунок 75 - Предупреждение о работе в технологическом режиме

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

- невозможность работы с подсистемой Клиентов (см. пункт «Клиент для ФПСУ»);
- невозможность работы с подсистемой регистрации ТМ-идентификаторов ФПСУ (см. пункт «Окно регистрации ТМ»);
- ограничение работы с ФПСУ горячего резерва (см. пункт «Параметры «Горячего резерва»»). После перевода ФПСУ 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 удаленными ФПСУ в режиме криптозащиты. Возможна работа туннелей только на тестовых, не рабочих ключах.

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

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

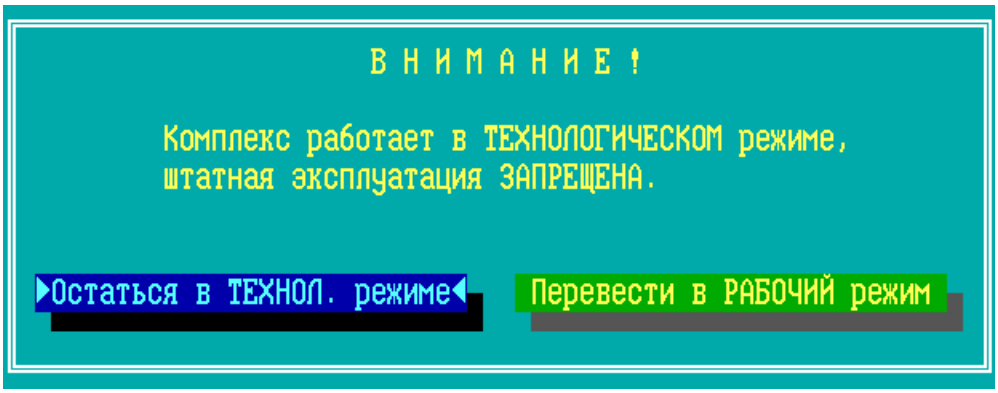


Рисунок 76 - Оповещение о работе в технологическом режиме

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

ВНИМАНИЕ! Программным комплексам ФПСУ, функционирующим под управлением виртуальных машин запрещается проводить инициализацию ПДСЧ средствами БиоДСЧ. Ключ ПДСЧ в таком случае следует получать с ЦВК.

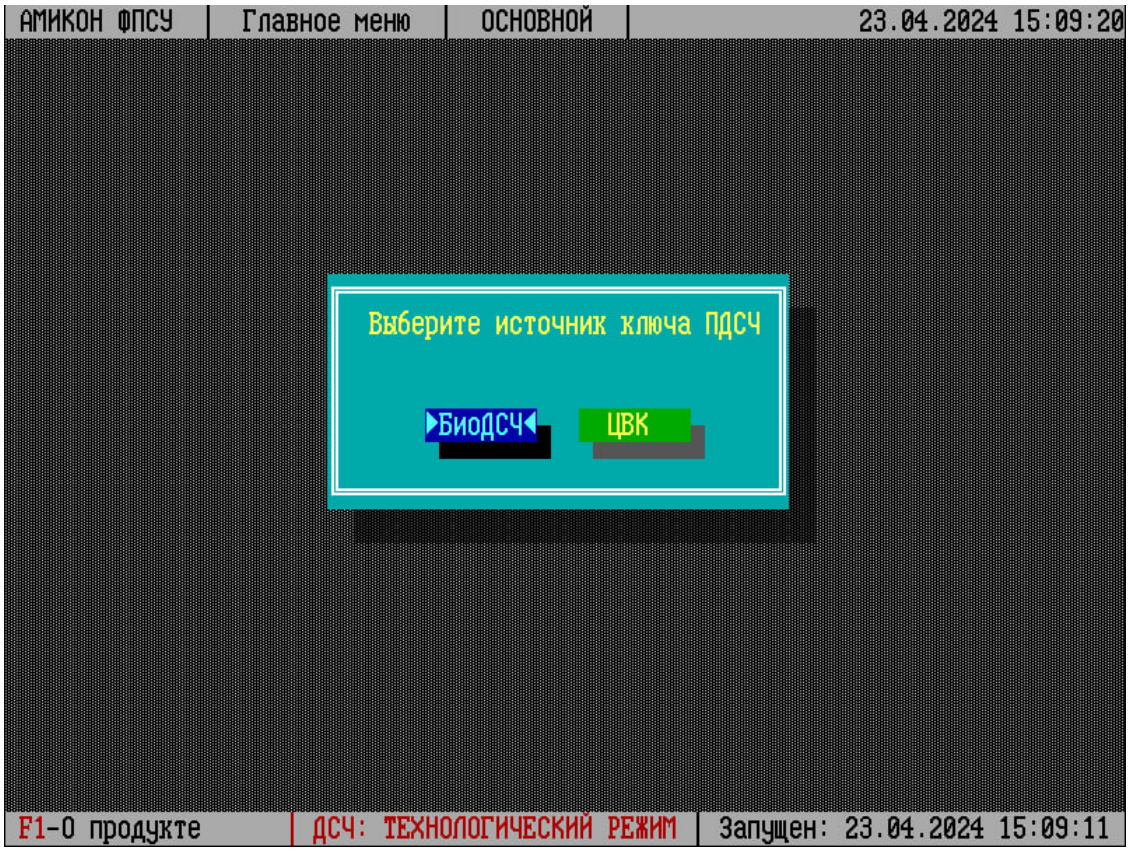


Рисунок 77 - Инициализация программного датчика случайных чисел

Для продолжения потребуется подтвердить полномочия Главного администратора (права роли *«Администратор»* класса *«Главный администратор»*, см. пункт «Разграничение доступа и пользователи», Таблица 3), подключив USB TM-идентификатор к USB-порту ФПСУ:

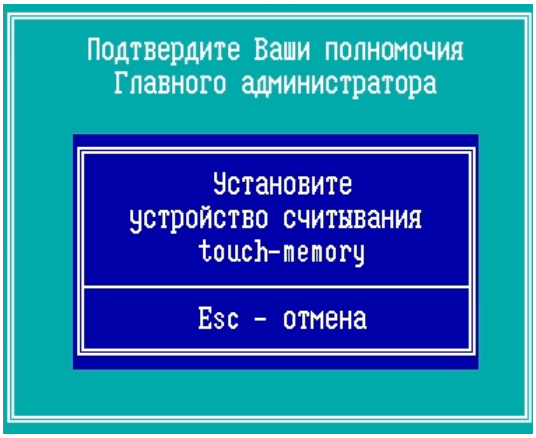


Рисунок 78 - Подтверждение полномочий Главного администратора

Затем откроется окно выбора источника ключа ПДСЧ. Инициализация ПДСЧ может быть проведена средствами БиоДСЧ, или путем загрузки файла с ключом ПДСЧ, выданного ЦВК.

При использовании БиоДСЧ от администратора требуется передвигать мышь в пределах экрана. Дальнейшая работа будет возможна, как только будет осуществлён набор достаточного числа случайных значений.



Рисунок 79 - Биологический датчик случайных чисел

Инициализацию ПДСЧ можно также провести с использованием файла с ключом ПДСЧ, полученного от ЦВК.

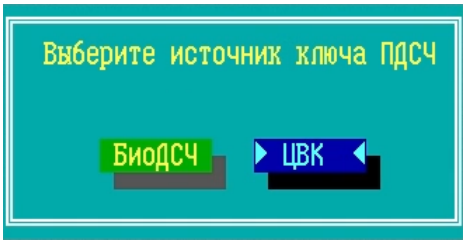


Рисунок 80 - Выбор источника ключа ПДСЧ

Для продолжения инициализации ПДСЧ с помощью полученного от ЦВК ключа, потребуется подтвердить полномочия Главного администратора (права роли *«Администратор»* класса *«Главный администратор»*, см. пункт «Разграничение доступа и пользователи», Таблица 3), подключив USB ТМ-идентификатор к USB-порту ФПСУ.

При выборе опции «ЦВК» требуется подключить к ФПСУ USB-носитель со сформированным средствами ЦВК файлом ключа ПДСЧ, и загрузить на ФПСУ файл с ключом ПДСЧ.

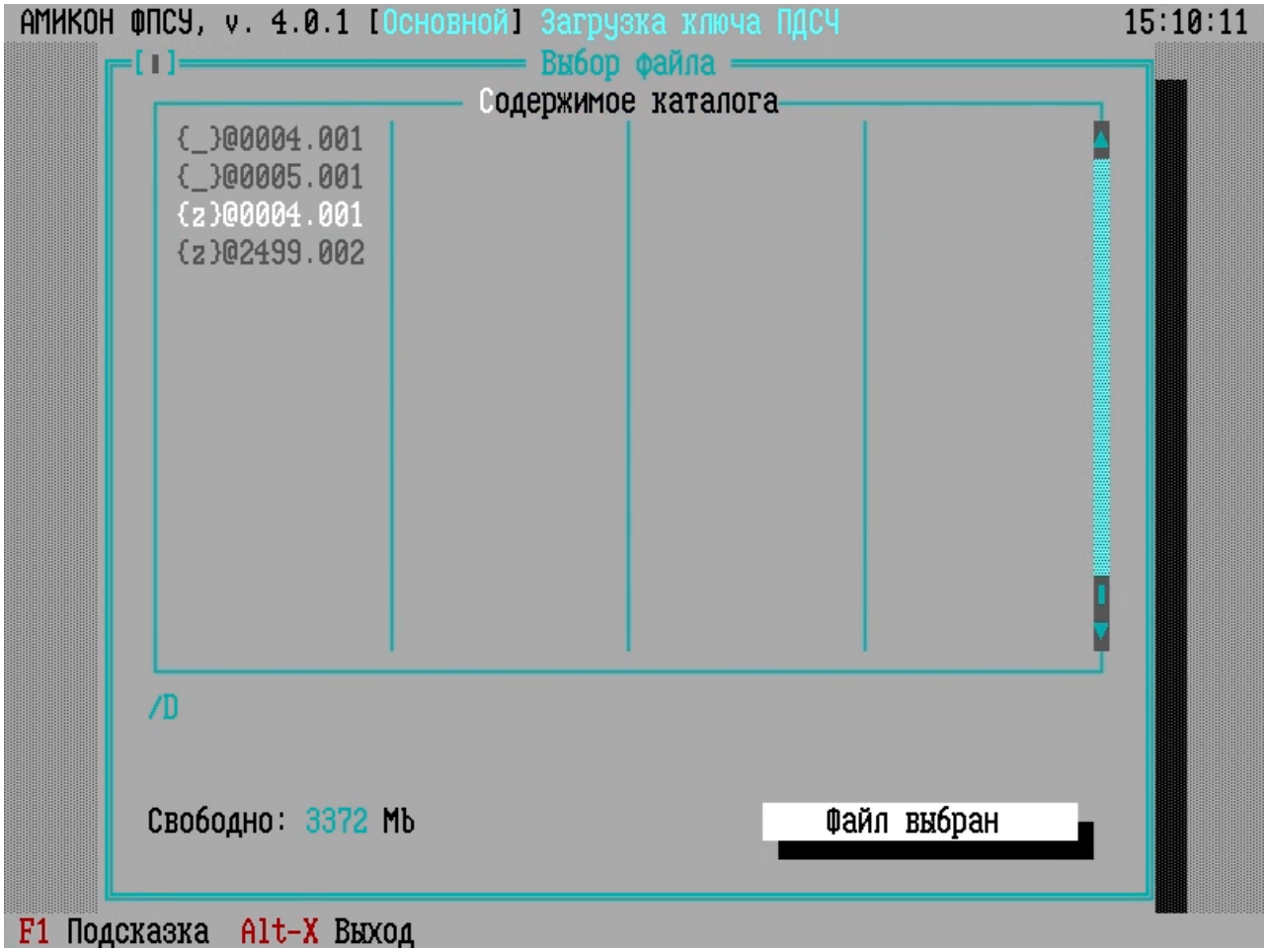


Рисунок 81 - Загрузка ключа ПДСЧ из файла

Переместите курсор на выбранный файл. Переход на кнопку «Файл выбран» осуществляется клавишей <*Tab*>. Подтвердите выбор файла, нажав на клавишу <*Enter*>. В открывшемся окне отобразится информация о ЦВК, выдавшем файл с ключом ПДСЧ, и предложением загрузить этот файл.

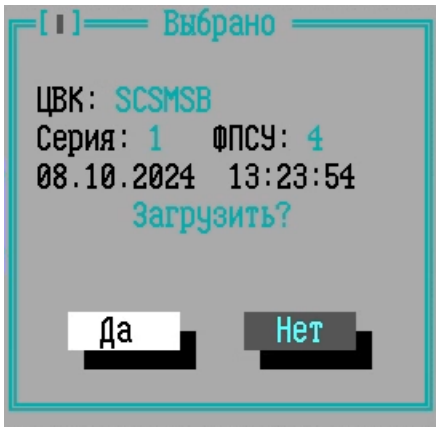


Рисунок 82 - Информация о загружаемом файле

После загрузки файла ФПСУ выдаст системное оповещение об успешном завершении процедуры инициализации ПДСЧ:

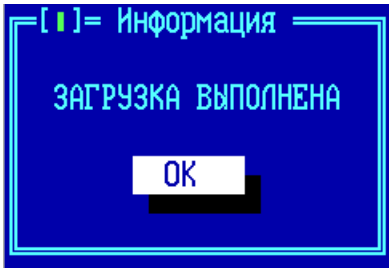


Рисунок 83 - Файл загружен

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 в режиме фильтрации и криптозащиты следует удалить установленные тестовые ключи парно-выборочной связи и установить рабочие наборы ключевых данных (подробнее см. пункты «Установка ключей» и «Использование ключей»).

3. 9. 1. Переход в рабочий режим, перерегистрация основного ТМ, регистрация запасного ТМ

После инициализации программного датчика случайных чисел для завершения перехода в рабочий режим будет предложено перерегистрировать основной ТМ Главного администратора и зарегистрировать ещё один ТМ-идентификатор, например, выбрать запасной ТМ администратора.

На экран будет выведено окно, показывающее наличие зарегистрированных

администраторов ФПСУ (ТМ-идентификаторов). Основной ТМ администратора может быть проверен на исправность и корректность хранимой идентификационной информации, и перерегистрирован.

ВНИМАНИЕ! Основной ТМ администратора зарегистрирован быть не может, он перерегистрируется только на этапах инсталляции или перехода из технологического в рабочий режим на ТМ, поставляемый вместе с ФПСУ.

Подтвердите переход из технологического режима в рабочий, нажав кнопку «Понятно». При переходе будет перерегистрирован основной ТМ-идентификатор.

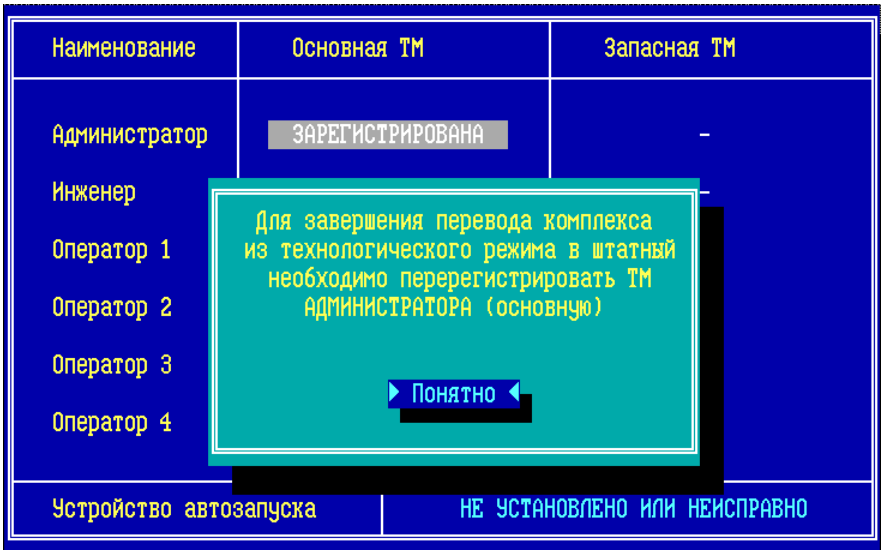


Рисунок 84 - Переход в рабочий режим

При выполнении операции требуется подключить основной ТМ-идентификатора учетной записи «Администратор», ТМ Главного администратора, к USB-порту ФПСУ для перерегистрации.

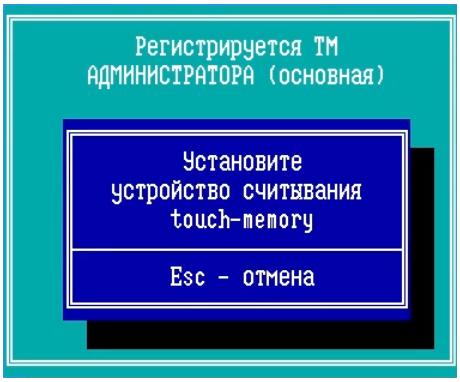


Рисунок 85 - Регистрация ТМ Главного администратора

Затем на экране отобразится запрос на установление пароля ТМ Главного

администратора.

ВНИМАНИЕ! Требование установки пароля для каждого ТМ-идентификатора является обязательным для ФПСУ классов КС2 и КС3, и опциональным для ФПСУ класса КС1.

Нажмите «Да» для задания пароля:

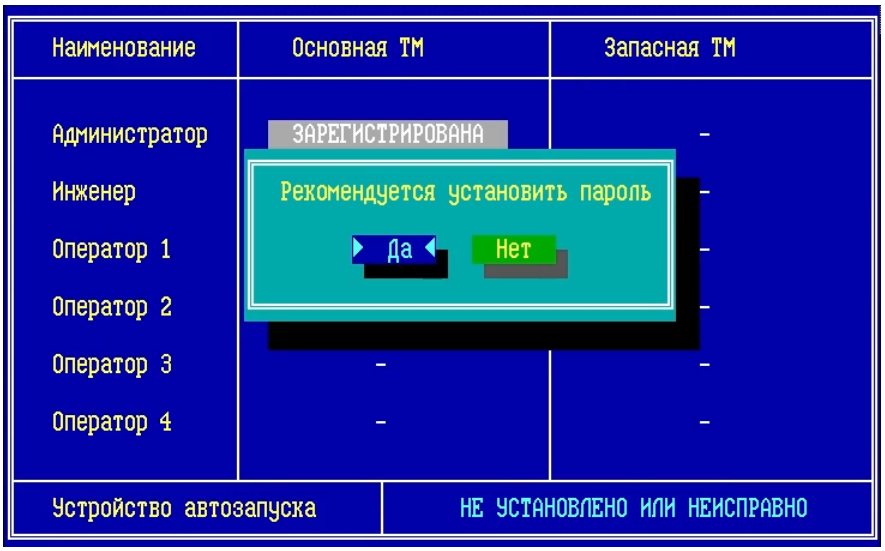


Рисунок 86 - Запрос на установление пароля ТМ Главного администратора

При подтверждении запроса откроется окно ввода пароля.

Длина пароля от 6 до 16 символов. Диапазон разрешённых символов заглавные и строчные латинские буквы, цифры, спецсимволы - коды 33-126 по таблице ASCII (! # $ % & ' ( ) * + , - . / 0-9 : ; < = > ? @ A-Z [\ ] ^ _ ` a-z { | } ~).

Поскольку вводимые символы не отображаются на экране, будет предложено ввести пароль еще раз с целью исключения возможной ошибки. Установка пароля 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.

ВНИМАНИЕ! Если администратор забыл пароль своего ТМ-идентификатора, то для восстановления доступа потребуется предъявить полномочия Главного Администратора, чтобы задать новый пароль. Если забыт пароль ТМ-идентификатора Главного Администратора, для восстановления доступа Главного Администратора к ФПСУ потребуется повторная установка ФПСУ с дистрибутива.

Необходимо ввести пароль и подтвердить ввод по нажатию клавиши <Enter>. В открывшемся окне повторно ввести пароль и нажать клавишу <Enter>.



Рисунок 87 - Ввод пароля ТМ

Администратор может отменить установку пароля. Для этого он должен выбрать ту же команду, оставить поле пустым (не вводить символы) и нажать <Enter>.

После установки пароля ТМ Главного администратора перезаписывается.

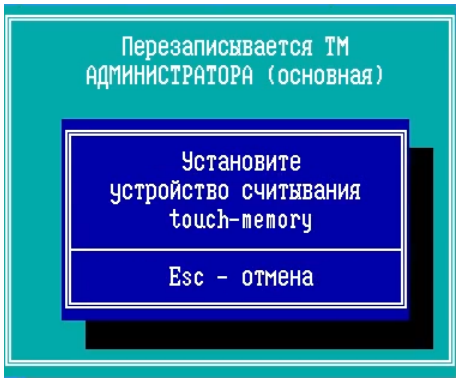


Рисунок 88 - Регистрация ТМ Главного администратора

Комплекс будет переведен в рабочий режим и перезагружен, для продолжения нажмите кнопку «Понятно».

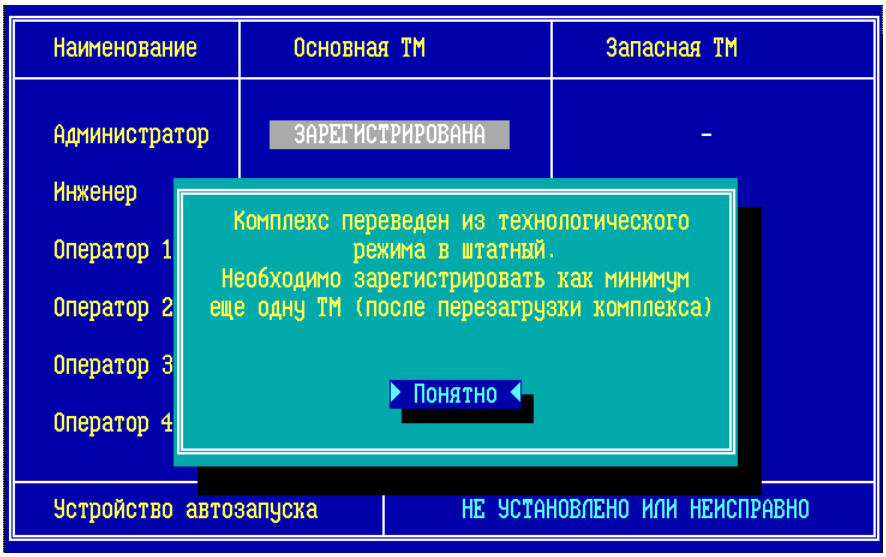


Рисунок 89 - Переход в рабочий режим

После перезагрузки комплекса потребуется авторизация для запуска, необходимо подтвердить полномочия с помощью вновь зарегистрированного ТМ-идентификатора Главного администратора.



Рисунок 90 - Авторизация на запуск ФПСУ

После перезагрузки отобразится таблица с уже зарегистрированным ТМ-идентификатором Главного администратора.

Далее потребуется регистрация ещё одного ТМ-идентификатора, например, запасного ТМ-идентификатора администратора.

ВНИМАНИЕ! На ФПСУ должны быть зарегистрированы минимум два ТМ-идентификатора, один из которых ТМ Главного администратора, иначе при закрытии окна регистрации ТМ-идентификаторов оно будет открываться снова, блокируя дальнейшую работу.

При регистрации второго ТМ-идентификатора требуется ТМ администратора для подтверждения права регистрации и другой ТМ для регистрации выбранного класса.

Уточнение: при регистрации запасного ТМ-идентификатора администратора требуется ТМ Главного администратора для подтверждения права регистрации и запасной ТМ для регистрации.

Окно регистрации ТМ содержит таблицу, показывающую наличие зарегистрированных ТМ-идентификаторов. Новый ТМ-идентификатор может быть только зарегистрирован как запасной для администратора, либо основной/запасной для любой другой учетной записи.

Для регистрации запасного ТМ-идентификатора администратора переведите курсор в ячейку «Запасная ТМ», и нажмите клавишу <*Ins*>.

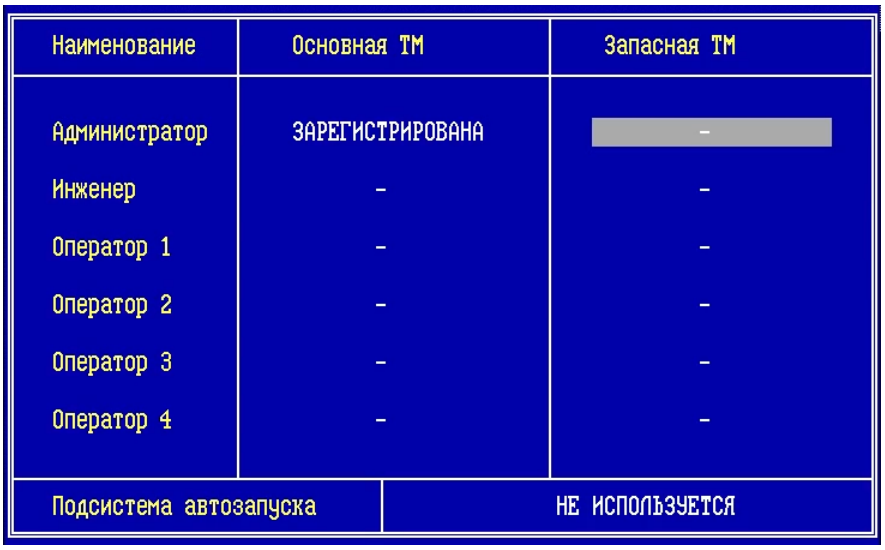


Рисунок 91 - Основной ТМ перерегистрирован

При выполнении операции по регистрации система будет требовать подтверждения полномочий Главного администратора.

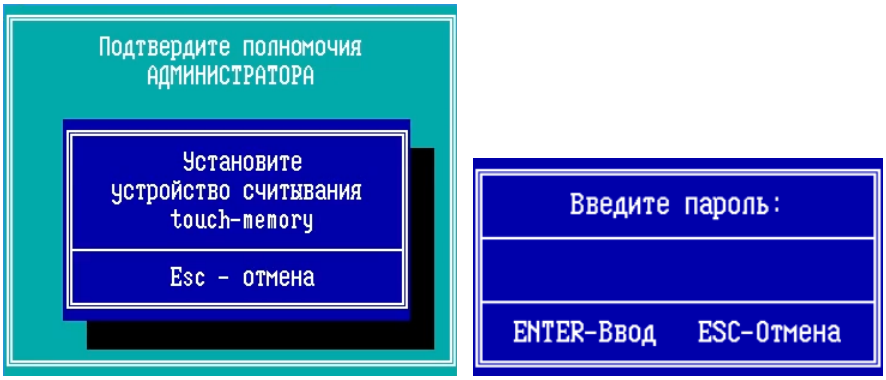


Рисунок 92 - Подтверждение прав администратора и ввод пароля ТМ

Затем необходимо убрать ТМ-идентификатор Главного администратора и предъявить запасной ТМ-идентификатор для его регистрации.

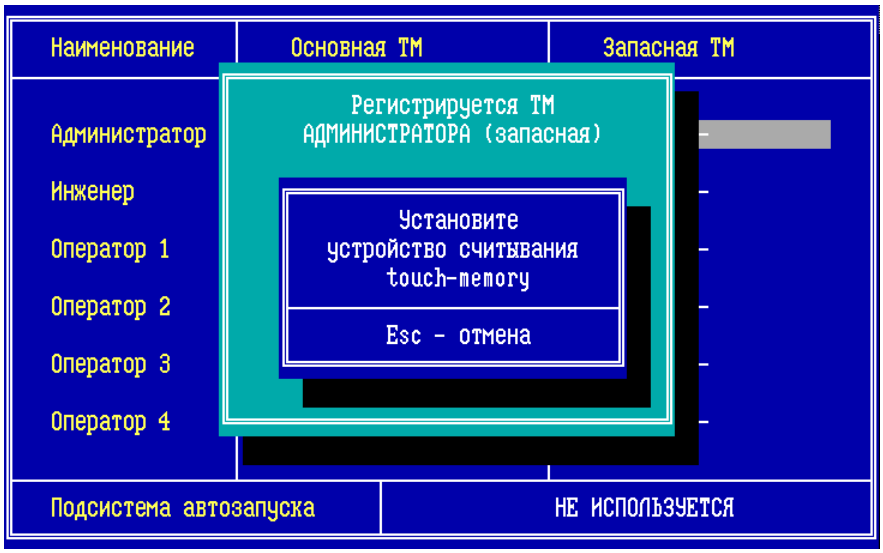


Рисунок 93 - Запись запасного ТМ администратора

Рекомендуется установить пароль зарегистрированного ТМ-идентификатора, на экране отобразится запрос на установление пароля ТМ.



Рисунок 94 - Запрос на установление пароля запасного ТМ администратора

При подтверждении запроса откроется окно ввода пароля. Все требования к паролю изложены выше (см. установка пароля ТМ Главного администратора).

Необходимо ввести пароль и подтвердить ввод по нажатию клавиши <*Enter*>. В открывшемся окне повторно ввести пароль и нажать клавишу <*Enter*>.



Рисунок 95 - Ввод пароля ТМ

В случае если запасной ТМ-идентификатор в процессе ввода пароля был отключен, необходимо повторно предъявить его для добавления пароля.



Рисунок 96 - Предъявление запасного ТМ

Запасной ТМ-идентификатор администратора зарегистрирован с установлением пароля.

После того, как запасной ТМ-идентификатор администратора зарегистрирован, отключите USB-носитель с дистрибутивом.

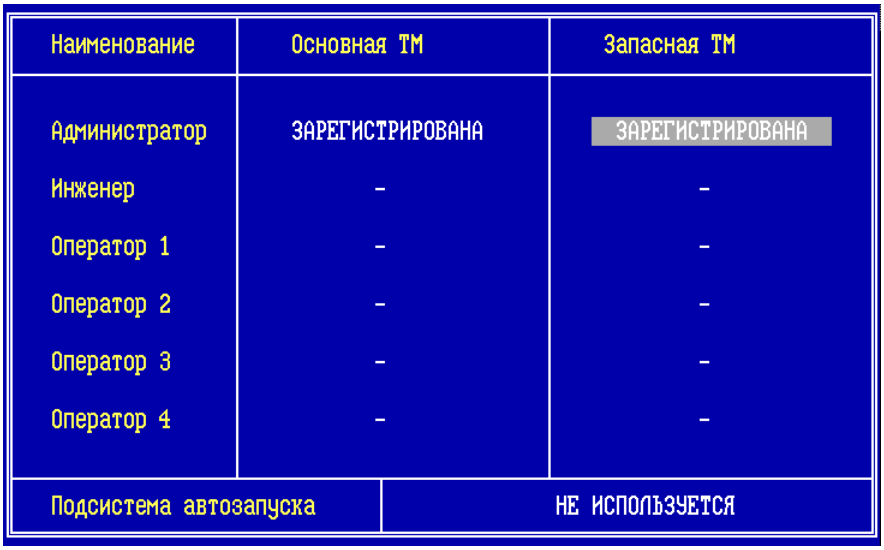


Рисунок 97 - Запасной ТМ администратора создан

После регистрации запасного ТМ необходимо сконфигурировать LAN-адаптеры, автоматически будет отображаться окно поиска драйверов и затем осуществлен переход в окно настройки сетевых адаптеров ФПСУ.

При переходе в окно настроек сетевых адаптеров ФПСУ потребуется подтвердить права администратора класса *Инженер* или выше.

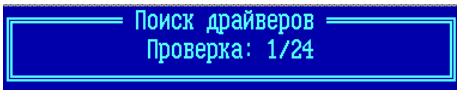


Рисунок 98 - Окно проверки LAN-адаптеров

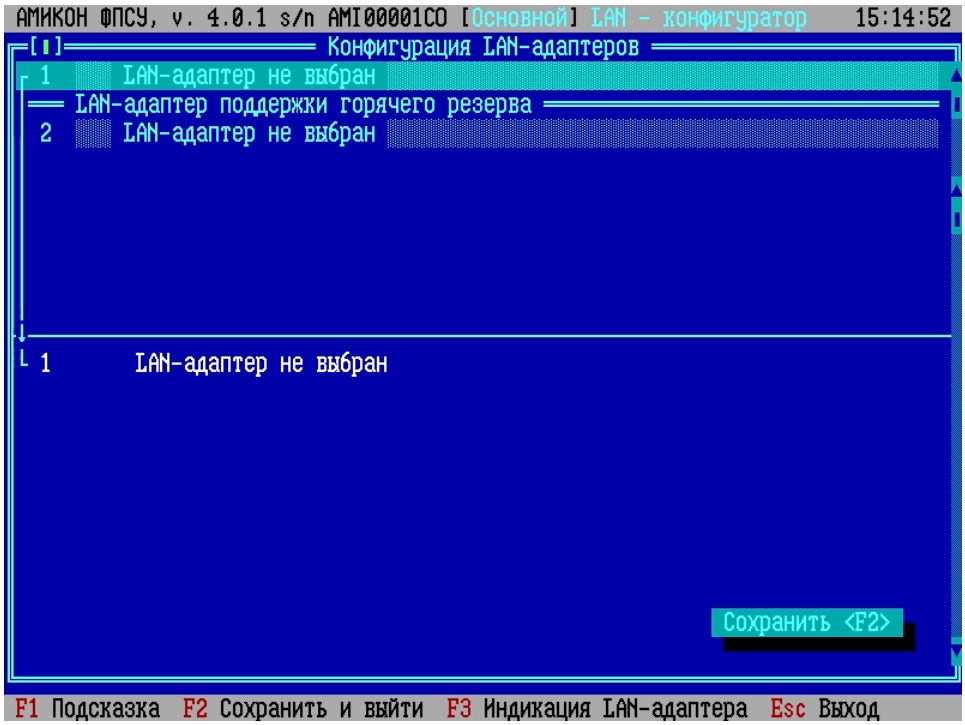


Рисунок 99 - LAN-адаптеры не настроены

Подробное описание настройки сетевых адаптеров ФПСУ приведено в пункте «Конфигурация драйверов сетевых адаптеров».

В некоторых случаях LAN-адаптеры предустановлены.

Переход в рабочий режим завершен.

Что можно сделать далее:

- инициализировать аппаратное устройство автозапуска HW, если оно входит в комплектацию аппаратной платформы (подробнее см. пункт «Инициализация HW аппаратного устройства автозапуска»);
- включить подсистему автозапуска, если не планируется использовать аппаратное устройство автозапуска HW (подробнее см. пункт «Включение автозапуска ФПСУ»);
- для возможности перевода ФПСУ в режим фильтрации пакетов настроить конфигурацию портов ФПСУ, назначить его сетевым портам IP-адреса (подробнее см. раздел «Порты ФПСУ»).

3. 9. 2. Инициализация HW аппаратного устройства автозапуска

Устройство автозапуска HW (hw - сокращение от «hard ware», «аппаратное решение») - аппаратное решение, предназначенное для авторизации запуска ФПСУ без участия администратора после штатной или нештатной перезагрузки ФПСУ. ФПСУ с

установленным и инициализированным устройством автозапуска HW после перезагрузки запускается в режим фильтрации пакетов, дополнительных действий администратора для разрешения запуска ФПСУ в данном случае не требуется.

Устройство автозапуска HW располагается внутри корпуса аппаратной платформы.

Виртуальная машина ФПСУ может взаимодействовать с USB-вариантом устройства автозапуска HW, если устройство подключено к USB-порту аппаратной платформы гипервизора.

Внимание! Для первоначальной инициализации устройства автозапуска HW необходимо, чтобы перед установкой программного обеспечения ФПСУ устройство было подключено к ФПСУ.

Внимание! Информация, содержащаяся в устройстве автозапуска HW для запуска ФПСУ, стирается при отключении электропитания ФПСУ или при отключении устройства автозапуска HW от ФПСУ. В случаях перебоев электропитания для дальнейшего запуска ФПСУ с помощью устройства автозапуска HW потребуется присутствие администратора и разовое предъявление ТМ-идентификатора администратора. После запуска ФПСУ потребуется заново инициализировать устройство автозапуска HW.

После установки ПО ФПСУ, при переходе из технологического в рабочий режим (см. пункт «Технологический режим ФПСУ») в окне регистрации ТМ устройство автозапуска HW будет отображаться как «НЕ УСТАНОВЛЕНО ИЛИ НЕИСПРАВНО», даже когда устройство автозапуска HW подключено к ФПСУ:

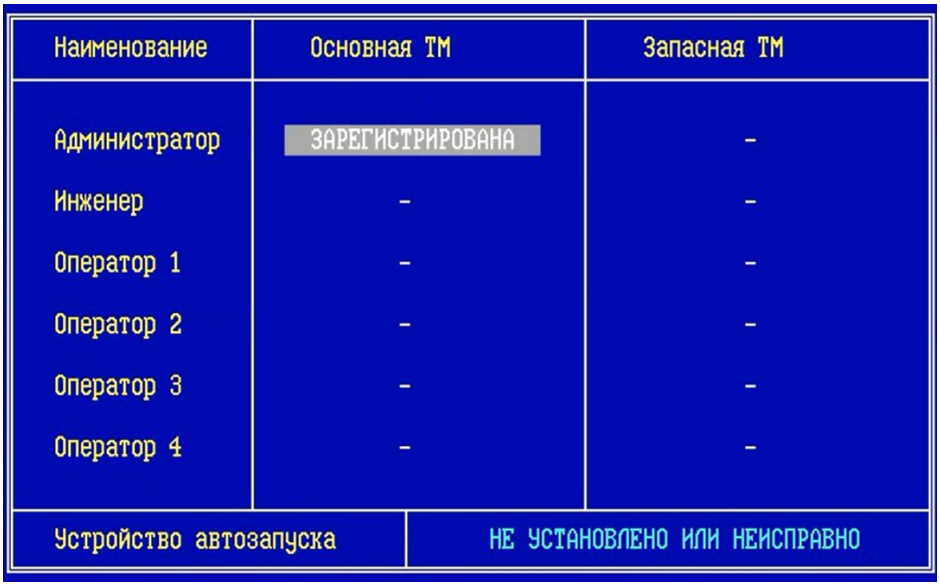


Рисунок 100 - Переход в рабочий режим

После ещё одной перезагрузки ФПСУ, статус устройства автозапуска HW изменится на «УСТАНОВЛЕНО И НЕ ИСПОЛЬЗУЕТСЯ»:

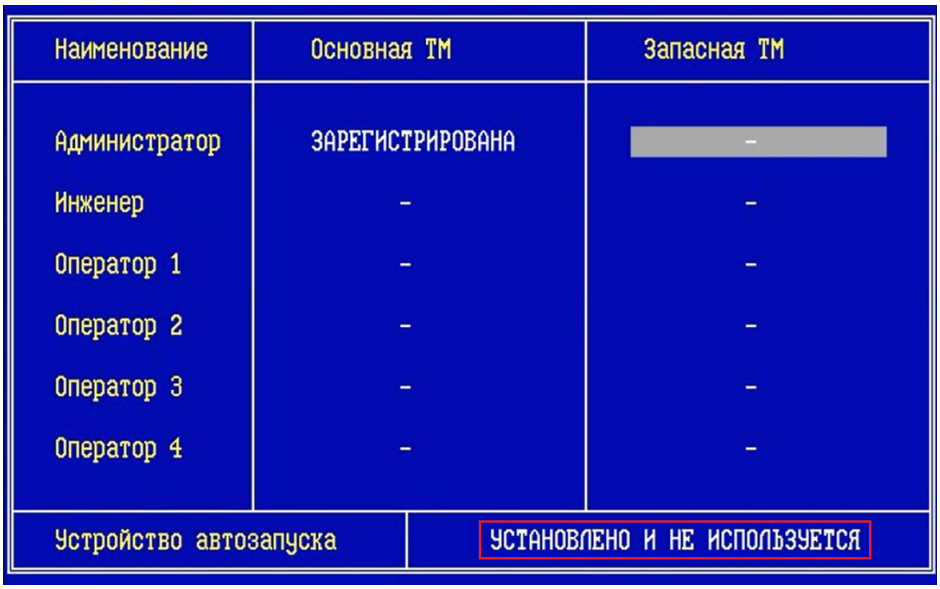


Рисунок 101 - Переход в рабочий режим

Внимание! Если включена подсистема автозапуска (см. пункт «Включение автозапуска ФПСУ»), запрещено использовать устройство автозапуска HW. После включения программной подсистемы автозапуска инициализировать устройство автозапуска HW можно только после переустановки программного обеспечения ФПСУ.

Инициализация устройства автозапуска HW

Для инициализации устройства автозапуска HW, в окне управления ТМ-идентификаторами ФПСУ перейдите в поле «Устройство автозапуска» и нажмите клавишу <Insert>:



Рисунок 102 - Запрос на инициализацию устройства автозапуска HW

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 103 - Подтверждение полномочий и ввод пароля ТМ

После подтверждения полномочий устройство автозапуска HW будет инициализировано. Если используется устройство автозапуска HW в виде USB-устройства, то его потребуется подключить к ФПСУ, на экран будет выдано следующее сообщение:

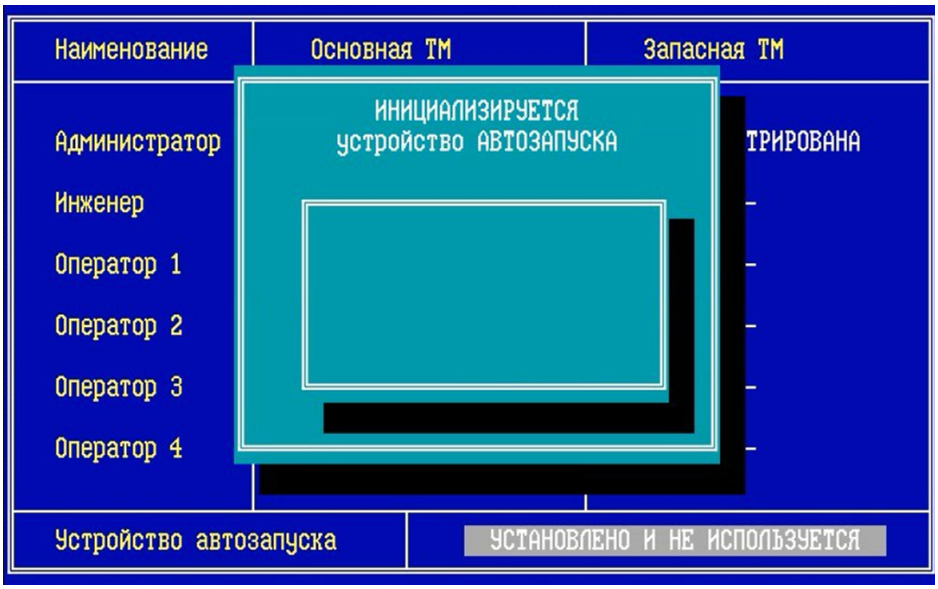


Рисунок 104 - Инициализация устройства автозапуска HW

После инициализации устройство автозапуска HW будет включено, его статус изменится на состояние «ИСПОЛЬЗУЕТСЯ».

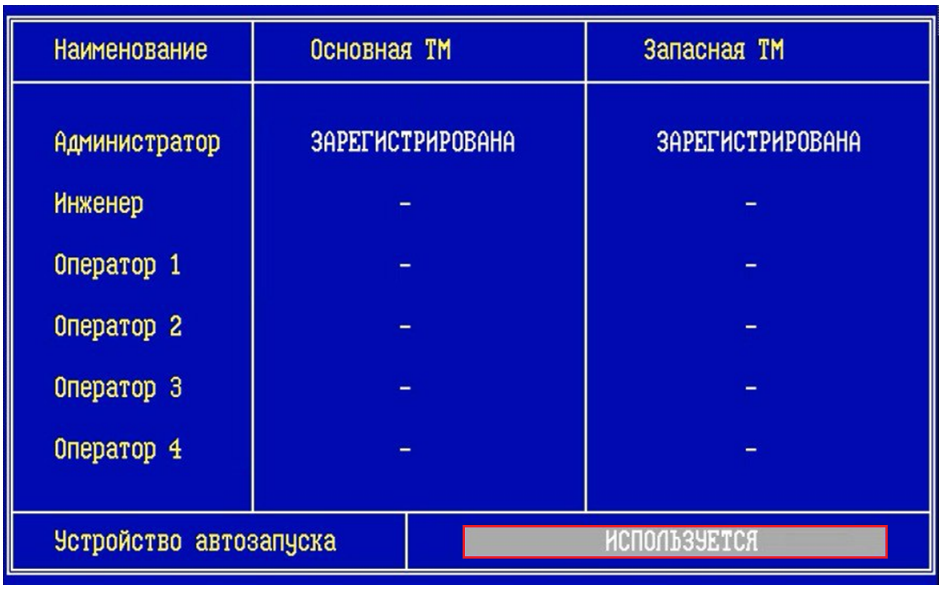


Рисунок 105 - Устройство автозапуска включено

Внимание! Если после инициализации устройства HW администратор активирует программную подсистему автозапуска, данное действие будет необратимым. Для возврата к разрешению запуска ФПСУ с помощью устройства HW потребуется переустановка программного обеспечения ФПСУ и последующая инициализация устройства автозапуска HW.

При активации программной подсистемы автозапуска на ФПСУ с

инициализированным устройством автозапуска HW на экран будет выдано предупреждение:

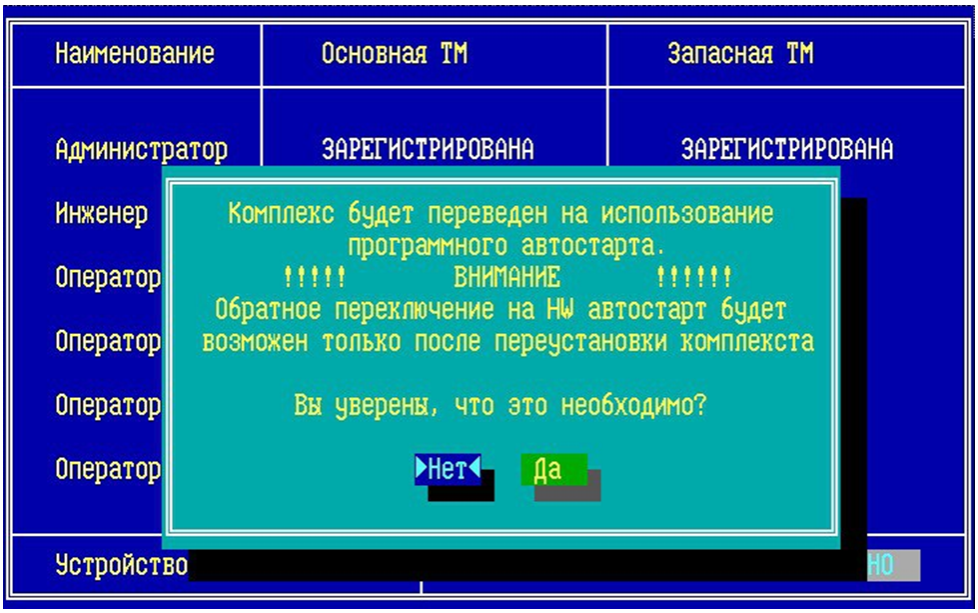


Рисунок 106 - Включение подсистемы автозапуска при включенном устройстве автозапуска HW

Если устройство автозапуска HW отключали и подключили обратно, или в случаях перебоев электропитания, для запуска ФПСУ и восстановления возможности последующих перезапусков ФПСУ с помощью устройства автозапуска HW потребуется разовое предъявление ТМ-идентификатора администратора и повторная инициализация устройства автозапуска HW. На экран при запуске ФПСУ в таком случае будет выдано сообщение «Touch a TM to the touch-memory reader»:

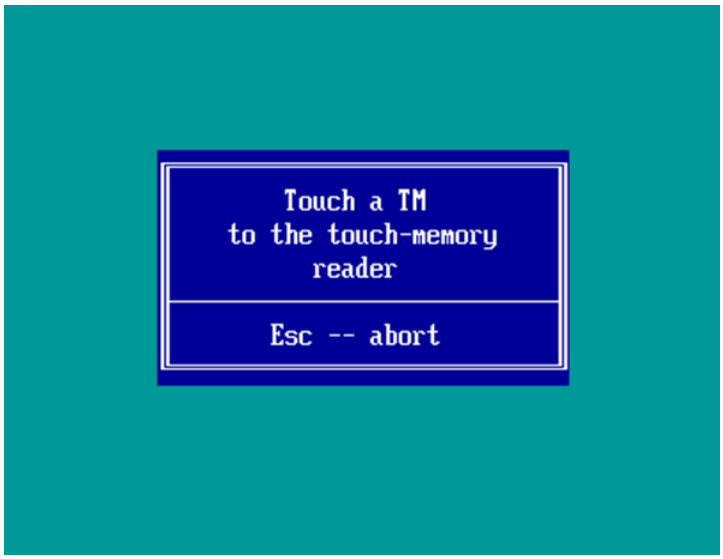


Рисунок 107 - Запрос на предъявление прав администратора при загрузке ФПСУ

4. Запуск и режим фильтрации ФПСУ

После включения питания и проведения диагностических тестов BIOS, на экран будет выдан запрос на подтверждение права доступа пользователя к работе с ФПСУ, сопровождаемый звуковым сигналом, замещающим экранную выдачу запроса в случае отсутствия монитора.



Рисунок 108 - Авторизация на запуск ФПСУ

Подключите USB TM-идентификатор к USB-порту зарегистрированный на ФПСУ TM-идентификатор (или прижмите к контактному устройству) с правами *«Оператор»* или выше. В случае успешной идентификации будет выдан звуковой сигнал, BIOS продолжит работу и ПО ФПСУ будет загружено.

Если ФПСУ уже сконфигурирован и параметры его работы установлены, система через несколько секунд автоматически осуществит перевод ФПСУ 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.

Выход в главное меню будет осуществлен также и при выходе из режима отображения работы подсистемы фильтрации.

Главное меню имеет вид, представленный на рисунке ниже, и содержит команды для настройки системы, конфигурирования оборудования, установки режимов работы и настройки параметров фильтрации. Выбор каждой команды повлечет за собой запрос на идентификацию допущенного лица и проверку его прав доступа (с предъявлением ТМ-идентификатора) на запрашиваемые действия (права допущенных лиц различных классов, см. пункт «Разграничение доступа и пользователи», Таблица 3).

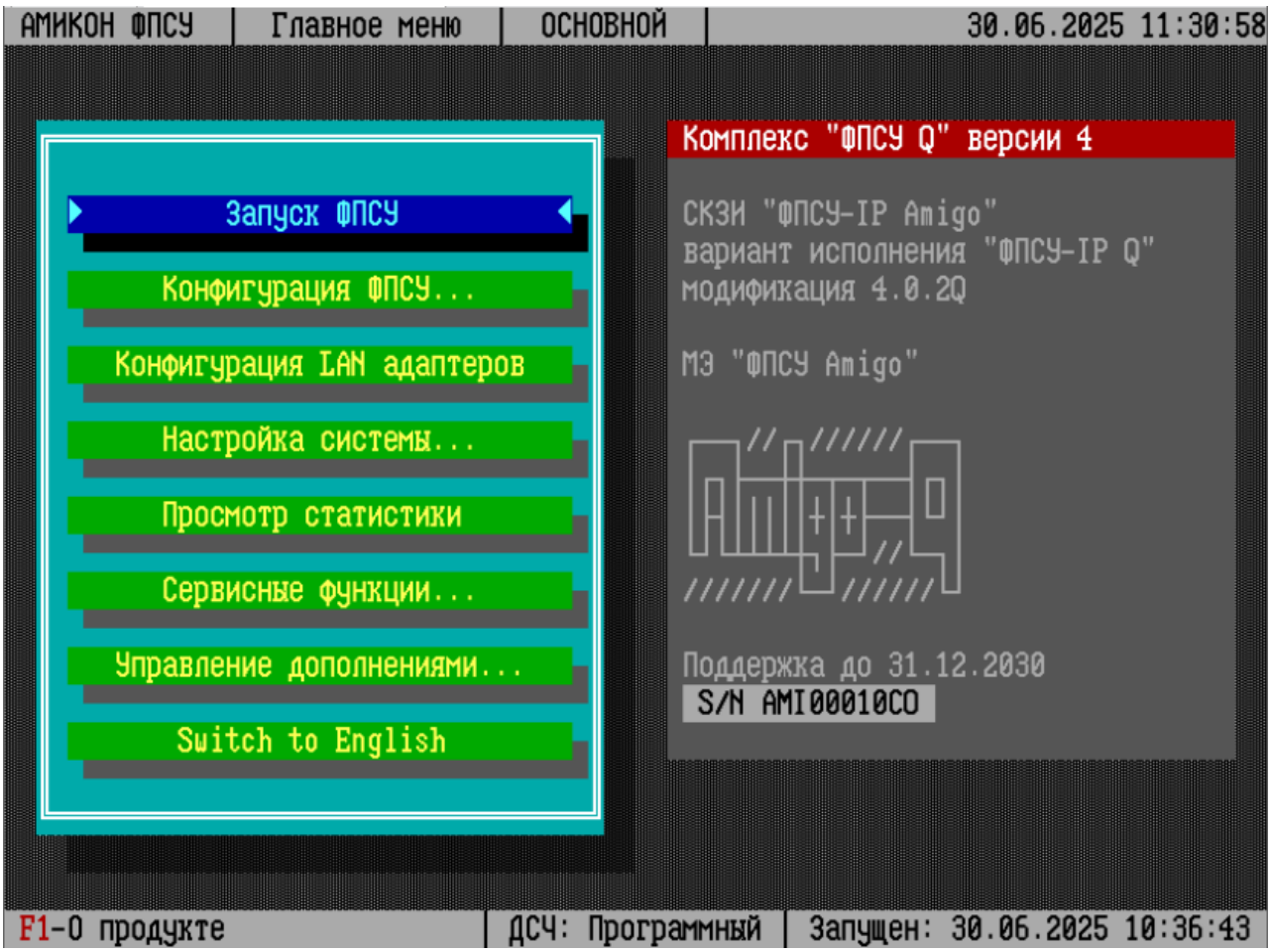


Рисунок 109 - Главное меню ФПСУ

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

При нажатии клавиши F1 выводится дополнительное окно со справочной информацией об изготовителе изделия.

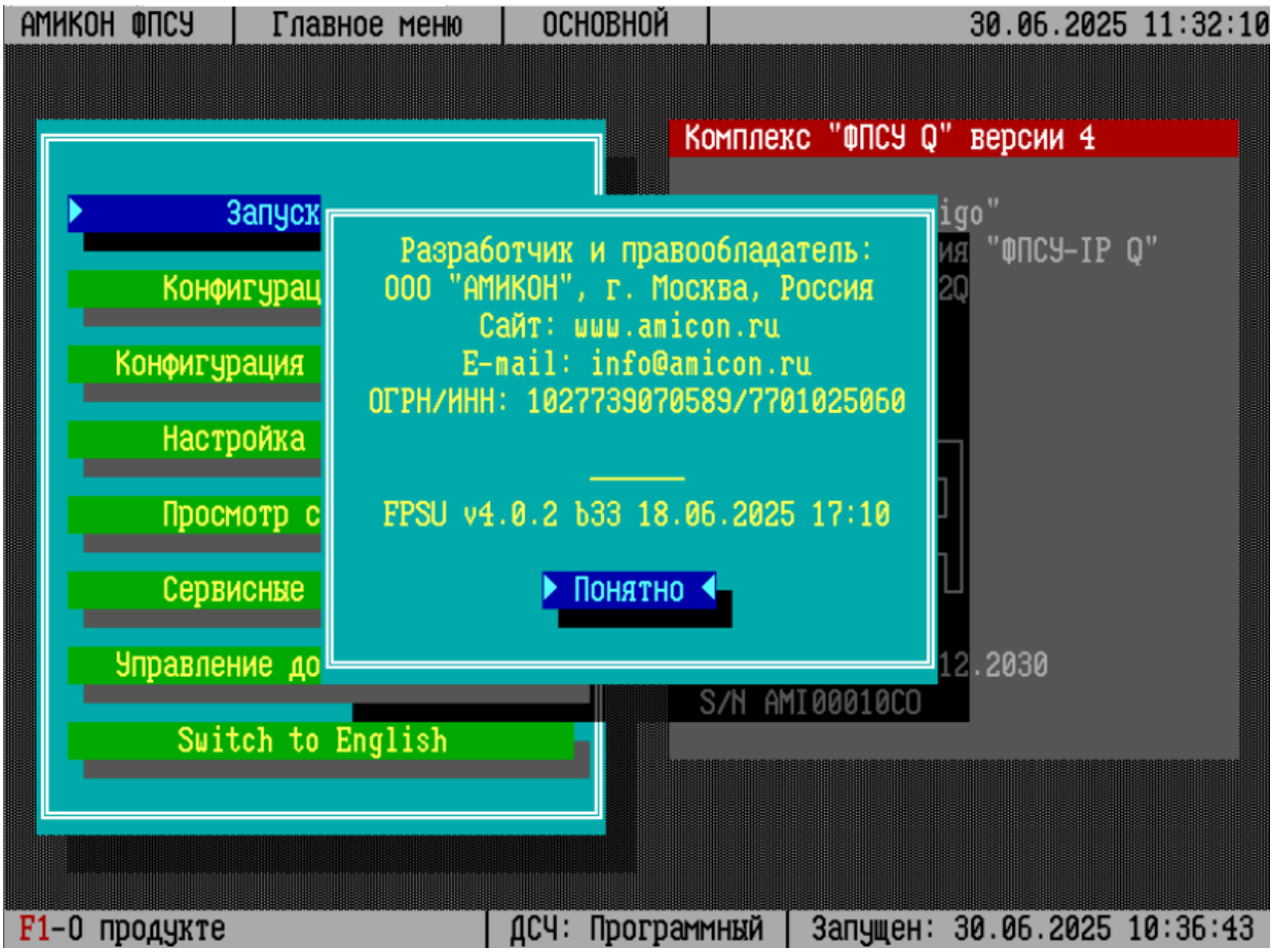


Рисунок 110 - Главное меню ФПСУ

Все команды главного меню описаны подробно в разделах далее.

Команда «Настройка дополнений» предназначена для перехода в меню управления установленными на ФПСУ дополнениями. Содержимое подменю «Настройка дополнений» определяется установленными дополнениями.

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

Перезагрузка ФПСУ

Перезагрузка ФПСУ осуществляется из главного меню с помощью сочетания клавиш *<Ctrl+Alt+Del>*.

4. 1. Запуск ФПСУ в режим фильтрации пакетов

Команда «Запуск ФПСУ» предназначена для перевода ФПСУ 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 выдаст сообщение об ошибке с диагностикой неисправности. После устранения причины ошибки может быть произведен повторный запуск режима фильтрации.



Рисунок 111 - Запуск ФПСУ из главного меню

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

Без подсистемы автозапуска команда «Запуск ФПСУ» из главного меню доступна администраторам класса *Оператор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3). При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора администратора к USB-порту ФПСУ, кроме того, вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации.

Если к ФПСУ 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 и др.

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

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

F2 – вывод на экран меню управления ключами удаленных администраторов;

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

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

F5 – переход на экран отображения подсистемы фильтрации пакетов абонентов;

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

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

F8 – переход на экран отображения взаимодействия с удаленными администраторами;

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

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

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

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

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, текущий статус ФПСУ в процессе «горячего» резервирования, время с момента последнего запуска подсистемы фильтрации и текущее время на ФПСУ.

Для завершения работы режима фильтрации и перехода в режим конфигурирования к главному меню ФПСУ (например, с целью проведения конфигурационных работ или просмотра статистики) нажмите клавишу *<F10>*, сочетание клавиш *<Alt+X>* или *<Ctrl+Alt+Del>*. При попытке выполнении команды потребуется подтвердить полномочия оператора или администратора:

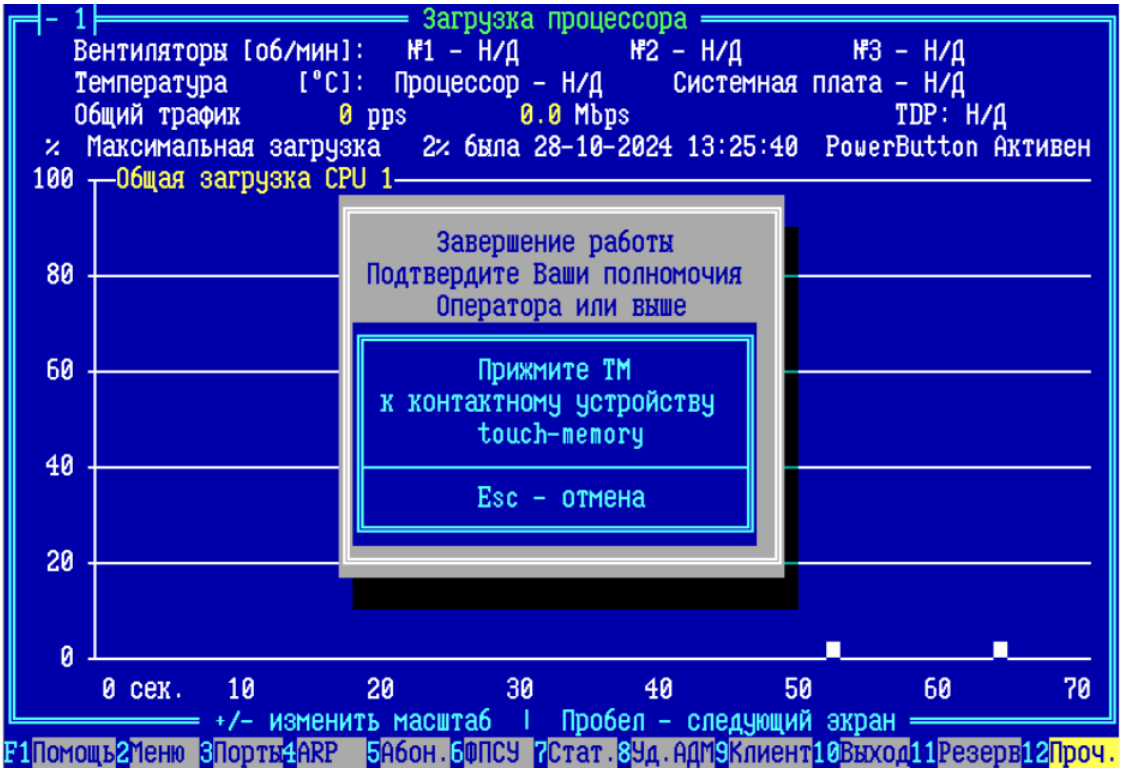


Рисунок 112 - Выход из режима фильтрации пакетов

После успешной авторизации с помощью ТМ-идентификатора, также потребуется ввести пароль подключенного ТМ, если он установлен, работа режима фильтрации ФПСУ будет завершена и ФПСУ перейдет в режим конфигурирования.

4. 2. Мониторинг аппаратного состояния и суточная статистика

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

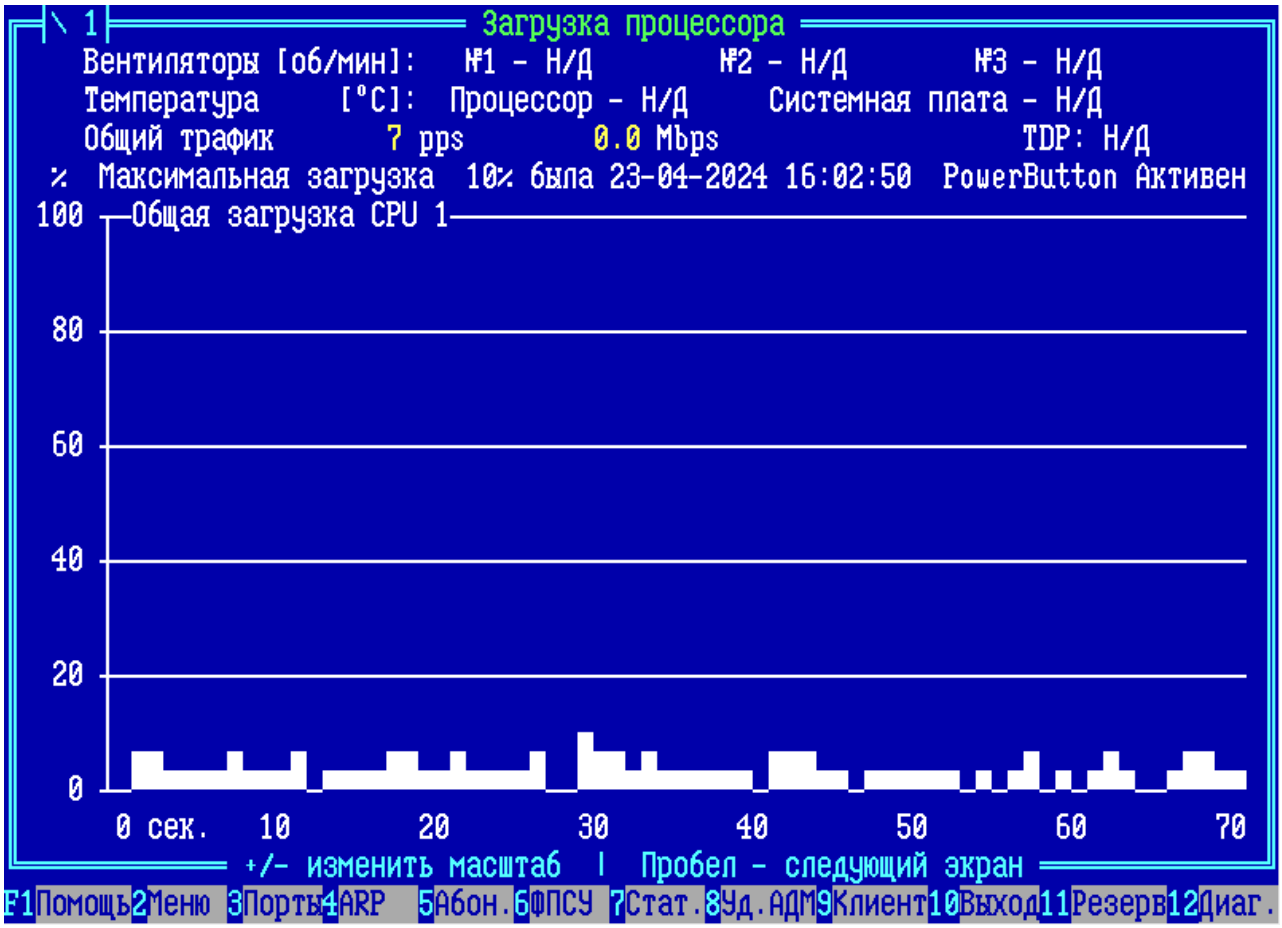


Рисунок 113 - Параметры аппаратного состояния ФПСУ

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

Вентиляторы - текущая частота вращения вентиляторов в оборотах в минуту.

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

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

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

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

PowerButton - индикация активности режима управления кнопкой питания. Значение «Активен» означает, что ФПСУ поддерживает функцию управления кнопкой

питания. В этом случае, при нажатии кнопки «Power» на корпусе ФПСУ, программное обеспечение корректно завершит свою работу, передаст управление резервному комплексу (если он доступен), запишет соответствующие сообщения в статистику и отключит электропитание ФПСУ.

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

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

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

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

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

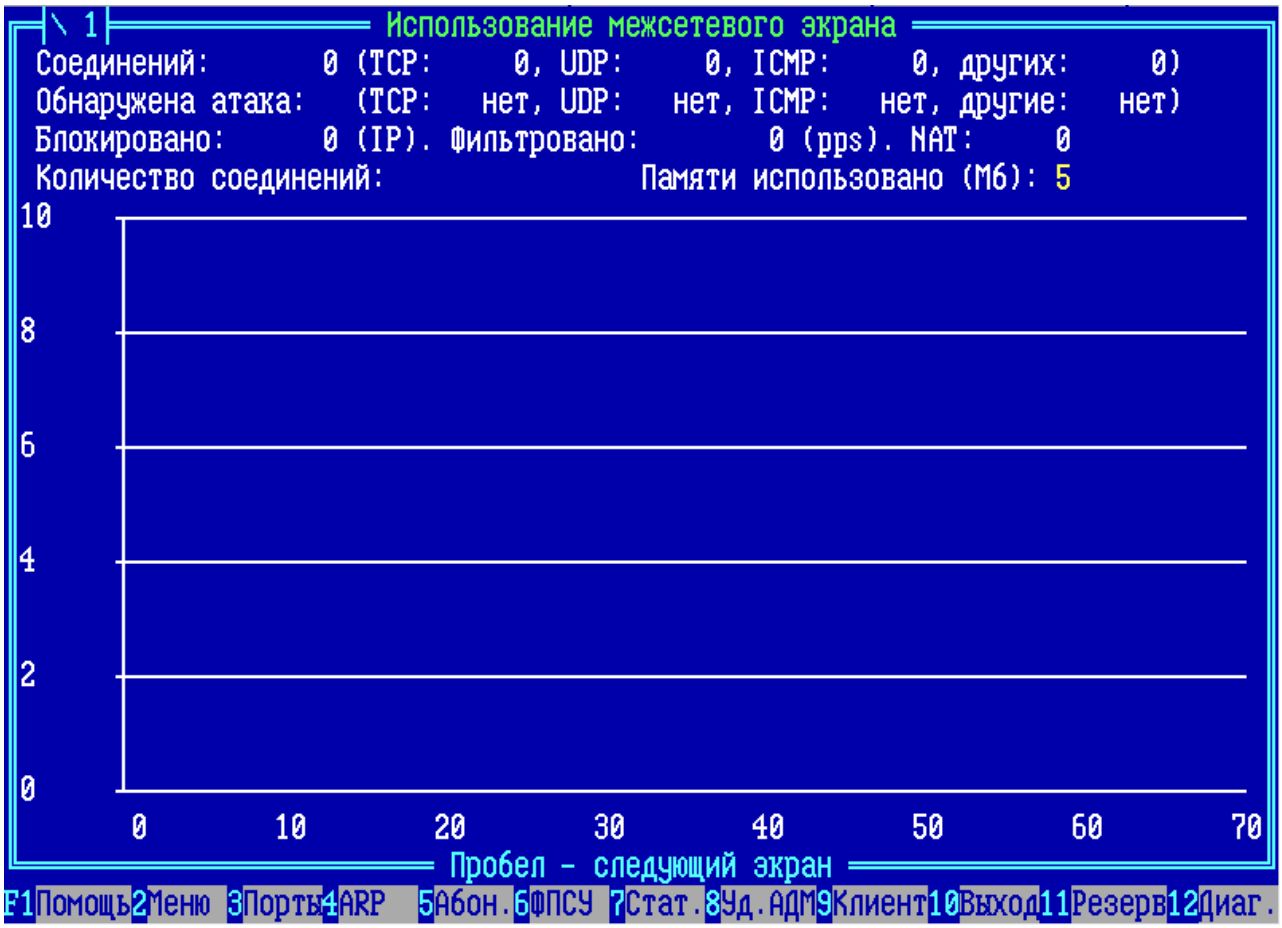


Рисунок 114 - Окно просмотра состояния ФПСУ

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

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

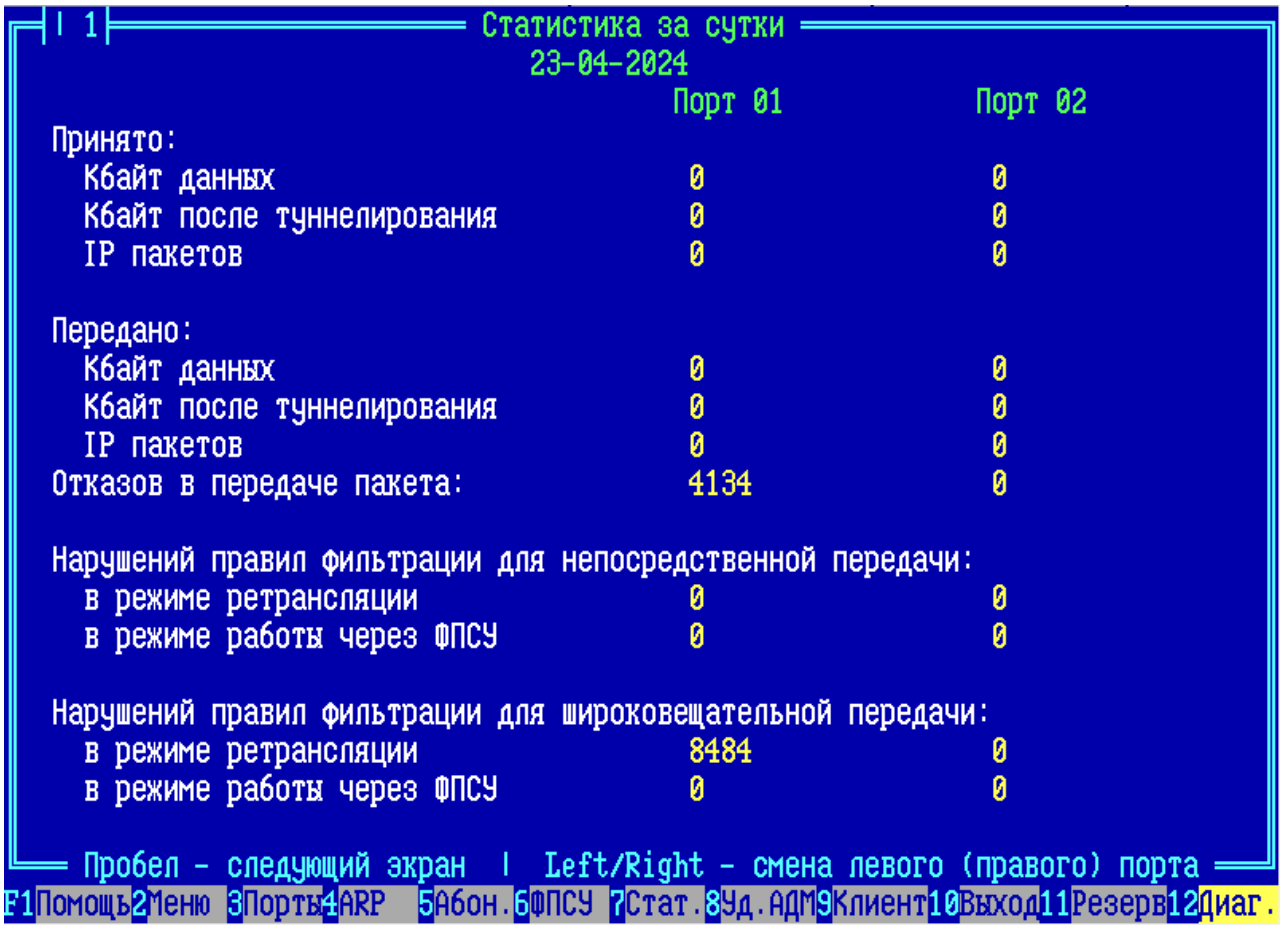


Рисунок 115 - Окно просмотра ежедневной статистки

Для каждого рабочего порта ФПСУ (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: 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 («Ретрансляция» и «Через ФПСУ»);
- количество нарушений правил фильтрации при широковещательных передачах для каждого режима работы ФПСУ.

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

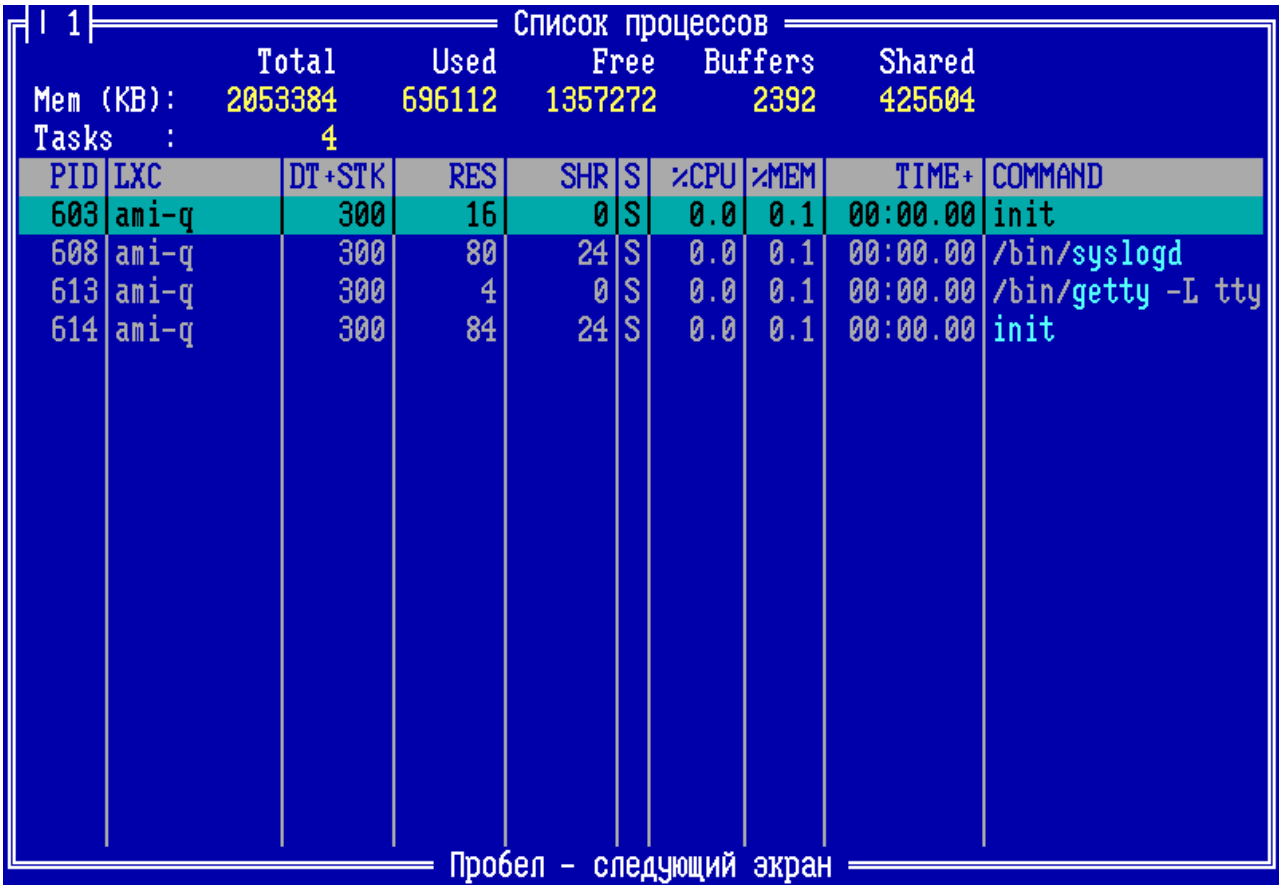


Рисунок 116 - Окно просмотра списка процессов

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

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

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

4. 3. Окно справки

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



Рисунок 117 - Справочное меню

Меню «Справка» содержит следующие команды:

- «Клавиши управления» - вывод на экран справки о функциональных клавишах и их назначении (см. пункт «Запуск ФПСУ в режим фильтрации пакетов»);
- «Информация о версиях» - вывод на экран справки о версии и номере и дате сборке ПО ФПСУ, модели материнской платы, аппаратной платформе, архитектуре ЦПУ;
- «Информация об установленных подсистемах» - вывод на экран информации об установленных подсистемах (горячий резерв, поддержка IP-клиентов и др.), серийном номере ФПСУ, а также количестве лицензированных ядер процессора ФПСУ;
- «Информация об аддонах» - вывод на экран справки об установленных дополнениях и их состоянии (dhcp, http-proxy, ids и т.д.);
- «Информация о системе» - вывод на экран справки о системе аппаратной платформы;
- «Ограничения» - вывод на экран справки о верхних границах ряда параметров (подробная таблица приводится в пункте «Ограничения функционала ФПСУ в зависимости от оперативной памяти»);
- «Информация о продукте» - вывод на экран информации данные о Разработчике.

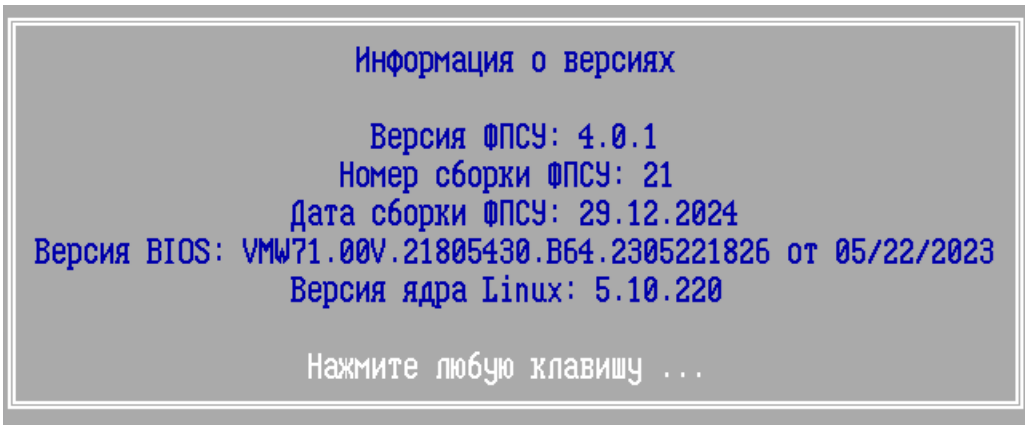


Рисунок 118 - Информация о версиях

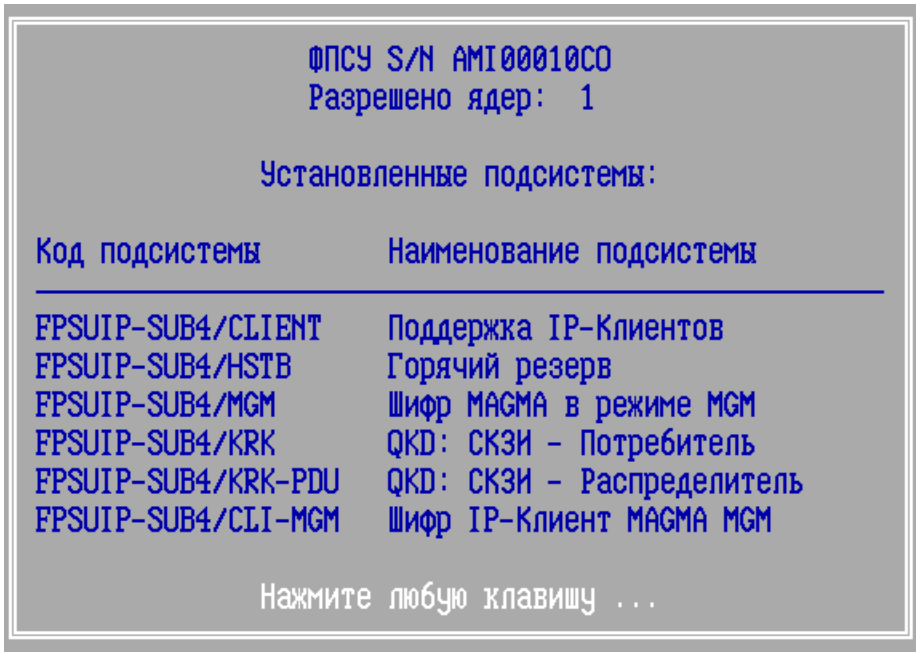


Рисунок 119 - Установленные подсистемы

Наименование модуля	№ сборки	Состояние	Выделение памяти (Mb) мин.	макс.	факт.	потр.
dhcp	19	отключен	16	32	0	0
http-proxy	94	отключен	32	512	0	0
rkl	51	отключен	20	30	0	0
frr	19	отключен	160	300	0	0
ami-q	73	используется	150	3000	321	159
ИТОГО:			378	3874	321	159

Нажмите любую клавишу ...

Рисунок 120 - Информация об установленных дополнениях

Информация о системе

Модель материнской платы: 440BX Desktop Reference Platform
Аппаратная платформа: VMware7,1
Архитектура ЦПУ: x86-64
Частота ЦПУ: 3149 MHz
Количество сокетов: 64
Количество потоков: 64
Объем памяти: 4 GB
Размер диска: 1 GB
Свободное место на диске: 797 MB

Нажмите любую клавишу ...

Рисунок 121 - Информация о системе

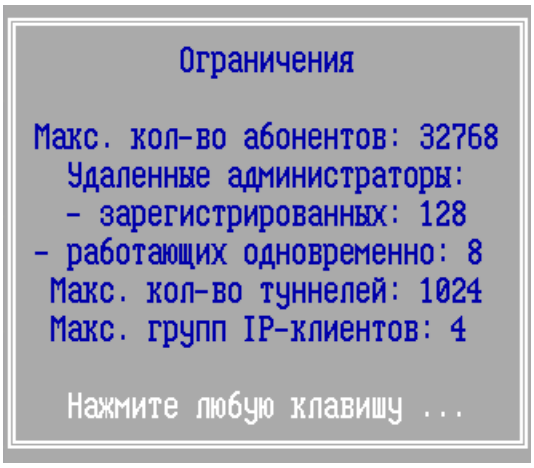


Рисунок 122 - Информация об ограничениях

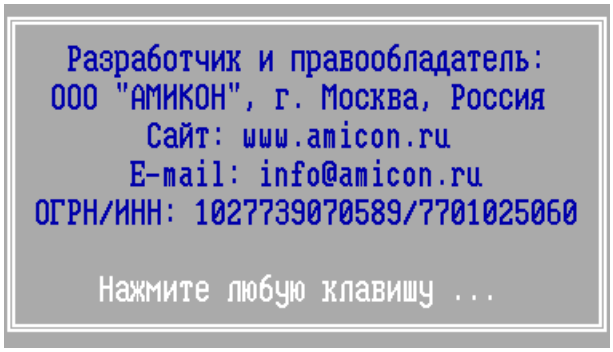


Рисунок 123 - Информация о разработчике продукта

4. 4. Меню управления ключами УА

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

Выполнение команд меню, кроме команд переключения языка и палитры, требуют авторизации.

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

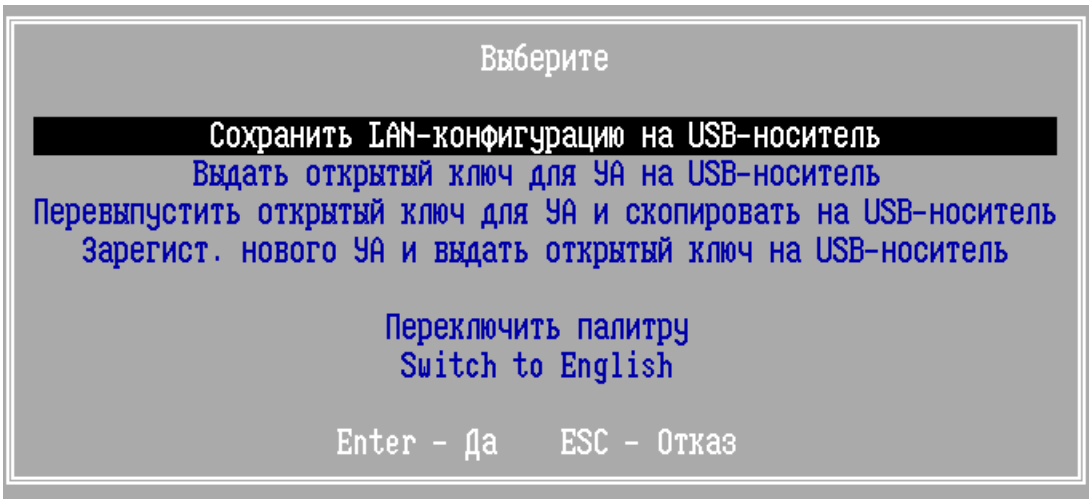


Рисунок 124 - Параметры экрана

При выполнении операции необходимо подтверждение полномочий посредством подключения ТМ-идентификатора, кроме того, вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

Меню УА содержит следующие команды:

«**Сохранить LAN-конфигурацию на USB-носитель**» – команда записи текущей конфигурации ФПСУ в специальном формате на съемный носитель без остановки рабочего режима ФПСУ, без перехода в режим конфигурирования. Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3). Подключите USB-носитель и выполните команду, будет выдано сообщение об успешном выполнении команды. На внешнем носителе создается каталог с серийным номером ФПСУ с файлом конфигурации с расширением .cfb в разжатом виде. Файл конфигурации с расширением .cfb может быть загружен удаленным администратором в программу «Удаленный администратор ФПСУ» для просмотра, изменения и дальнейшей установки на ФПСУ.

«**Выдать открытый ключ для УА на USB-носитель**» – команда записи текущего открытого ключа ФПСУ на внешний носитель, с целью регистрации его удаленным администратором. Операция доступна администраторам класса *Администратор* и выше. Выполняется без остановки рабочего режима ФПСУ, без перехода в режим конфигурирования. Подключите USB-носитель и выполните команду, будет выдано сообщение об успешном выполнении команды. На внешнем носителе создается каталог с серийным номером ФПСУ с файлом с расширением .CO1 - признак основного ФПСУ, .CO2 - горячего резерва. Команда доступна также в режиме изменения параметров конфигурации и настройки системы, более подробно см. пункт «Ключи ФПСУ для связи с УА».

«Перевыпустить открытый ключ для УА и скопировать на USB-носитель» – команда выработки нового открытого ключа ФПСУ и его записи на внешний носитель, с целью регистрации его удаленным администратором. Выполняется без остановки рабочего режима ФПСУ, без перехода в режим конфигурирования. Операция доступна администраторам класса *Администратор* и выше. На внешнем носителе создается каталог с серийным номером ФПСУ с файлом с расширением .CO1 - признак основного ФПСУ, .CO2 - горячего резерва. Данная команда доступна также в режиме изменения параметров конфигурации и настройки системы, более подробно см. пункт «Ключи ФПСУ для связи с УА», команда «*Создать новые ключи»*.

«**Зарегистрировать нового УА и выдать открытый ключ на USB-носитель**» – команда регистрирует на ФПСУ учетную запись удаленного администратора ФПСУ и записывает текущий открытый ключ ФПСУ на внешний носитель для дальнейшей регистрации данного ФПСУ в программе «Удаленный администратор ФПСУ». Операция доступна администраторам класса *Администратор* и выше. На USB-носителе может быть не более одного описателя удаленного администратора, иначе новый удаленный администратор не будет зарегистрирован. Выполняется без остановки рабочего режима ФПСУ, без перехода в режим конфигурирования. При выполнении команды система выполняет поиск на подключенном внешнем USB-носителе открытого ключа удаленного администратора. Если открытый ключ удаленного администратора найден, он будет зарегистрирован на ФПСУ как разрешенный к работе с правами «Опрос текущего состояния» и «Получение данных о работе Абонентов». При записи текущего открытого ключа ФПСУ на внешнем носителе создается каталог с серийным номером ФПСУ с файлом с расширением .CO1 - признак основного ФПСУ, .CO2 - горячего резерва. Данная команда доступна также в режиме изменения параметров конфигурации и настройки системы, более подробно см. пункты «Регистрация Удаленных Администраторов», «Регистрация удаленного администратора на ФПСУ», «Ключи ФПСУ для связи с УА».

«Переключить палитру» – переключение между темами интерфейса (синей, черной, серой, белой).

«Switch to English» – смена языка интерфейса на английский.

4. 5. Окно состояния рабочих LAN портов

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

Окно разделено на две половины, в каждой из которых отображается состояние

одного из портов ФПСУ, используемых для связи локальных подсетей и передачи пакетов абонентов. По умолчанию выводится информация по первым двум портам, зарезервированным в ОС ФПСУ под номерами 1 и 2. Для переключения и отображения информации по другому порту следует воспользоваться стрелками <→> и <←>. Выводимые параметры разбиты на три группы.

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

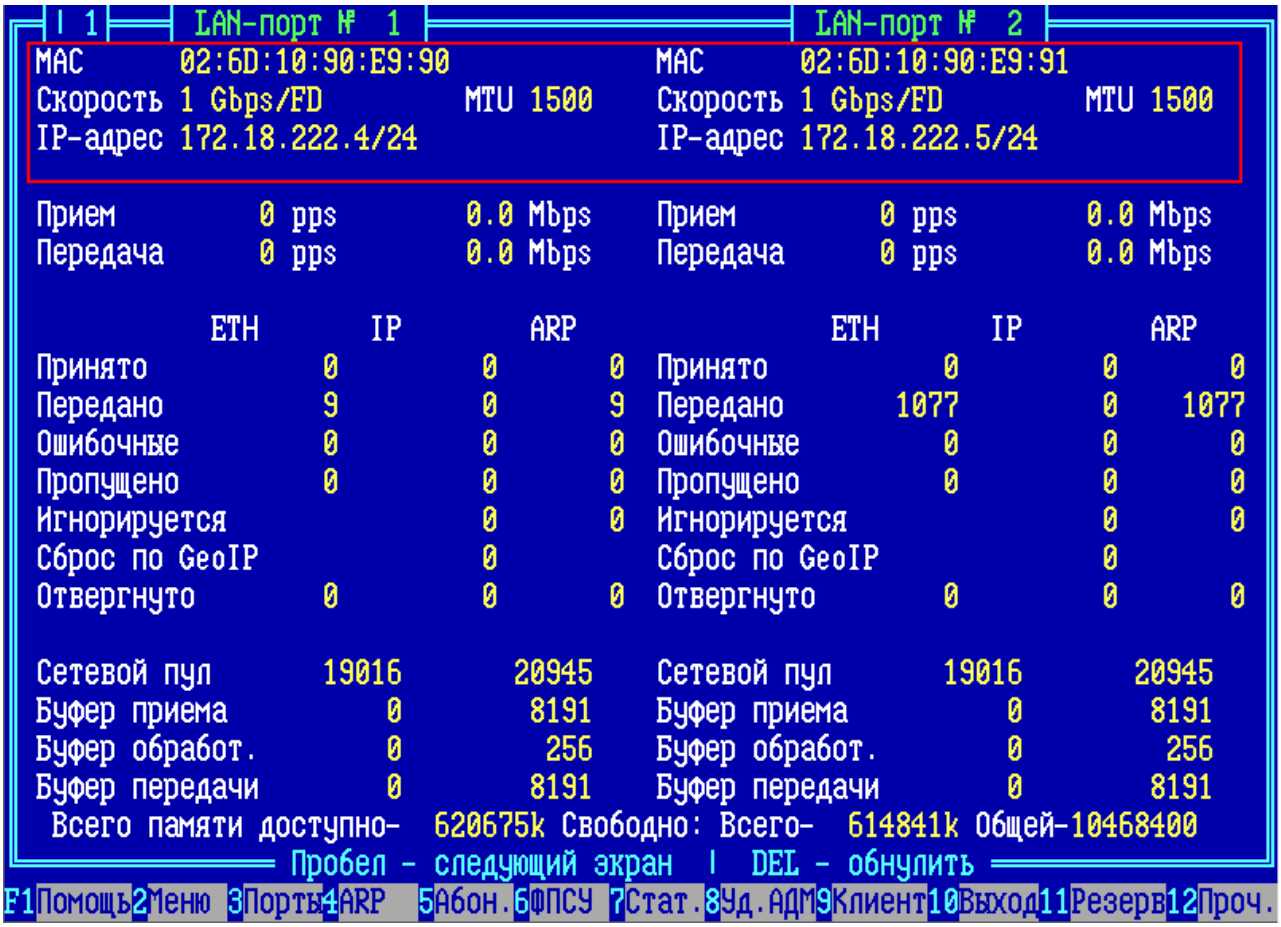


Рисунок 125 - Состояние рабочих портов ФПСУ

Вторая группа отображает статистику событий на сетевом адаптере с момента запуска подсистемы фильтрации (см. рисунок ниже):

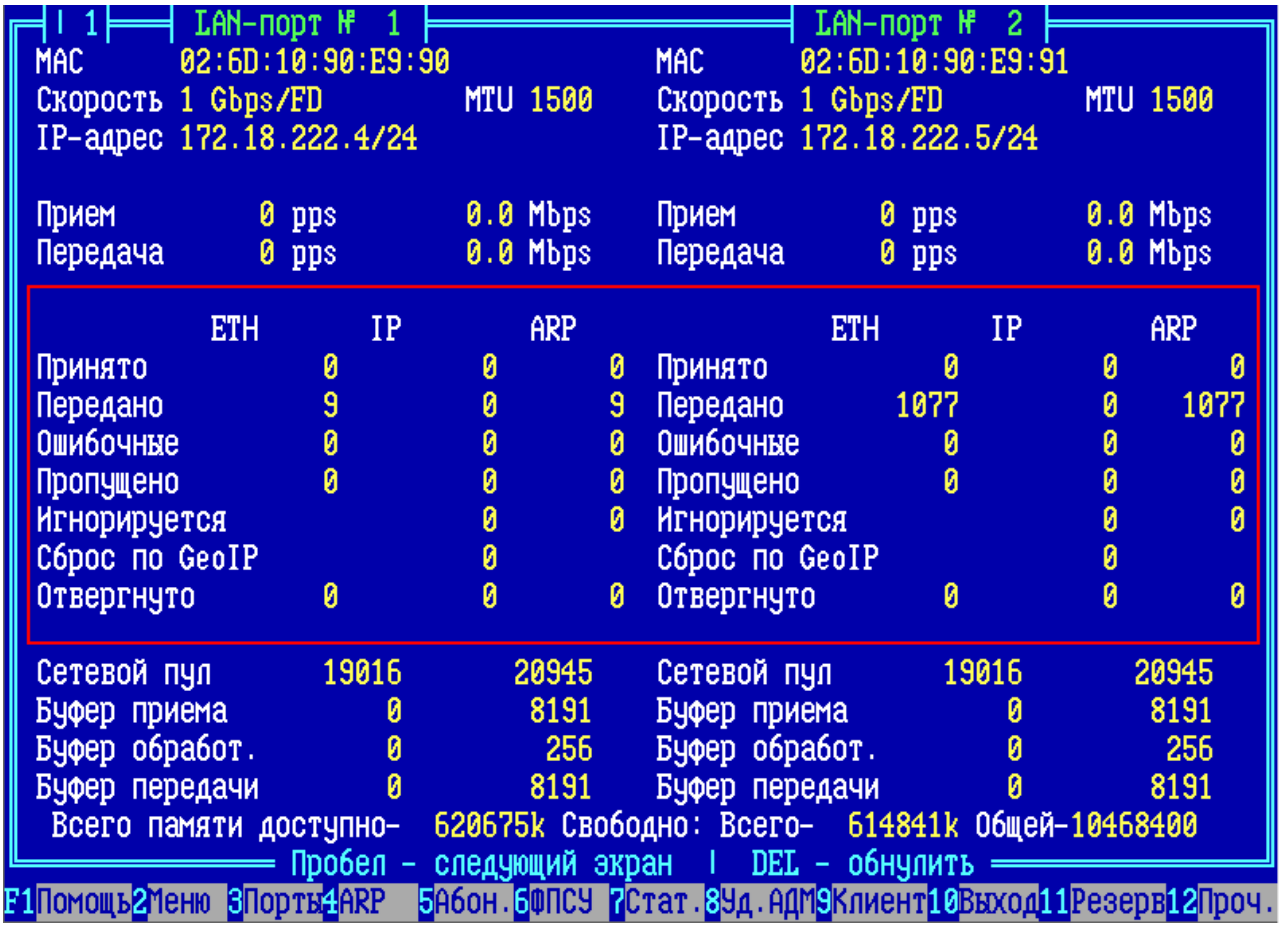


Рисунок 126 - Статистика полученных пакетов на LAN-адаптерах

Она содержит сведения о количестве поступивших на сетевой адаптер по сети пакетов различных протоколов (до фильтрации), переданных с этого адаптера в сеть пакетах различных протоколов, отвергнутых пакетах (не прошедших фильтрацию или по причине неполадок сетевого уровня) и пакетах, содержащих ошибки кадрового уровня. Если перед каким-либо значением стоит символ «*» - соответствующий счетчик превысил значение 4294967296 и начал отсчет с нуля.

В строках указываются количество фреймов или пакетов, подпадающих под события. Разные типы сетевых данных отмечены столбцами ETH, IP, ARP (соответственно фреймы Ethernet, IP-пакеты и ARP-пакеты):

Принято - успешно принятые сетевым адаптером фреймы или пакеты;

Передано - успешно переданные сетевым адаптеров фреймы или пакеты;

Ошибочные - не принятые фреймы или пакеты по причине ошибки приёма на сетевом адаптере, или когда размер полученного пакета больше разрешенного MTU;

Пропущено - фреймы или пакеты, которые сетевой адаптер не успел обработать (событие возникает по причине отсутствия свободной памяти на сетевом адаптере для приема фрейма);

Игнорируется - общий счетчик для всех сетевых пакетов, которые были сброшены ФПСУ по одной из следующих следующим причин:

- запрет межсетевого экрана ФПСУ, пакет не попал в разрешительные правила доступа;
- адрес отправителя не был указан в маршрутизации на портах ФПСУ;
- ошибка в одном из IP-адресов в заголовке IP-пакета (см. ошибку «Неверен IP адрес» в разделе «Диагностика ошибок ФПСУ»);
- пакет должен быть отправлен в туннель, но туннель не установлен (см. ошибку «ФПСУ не работает» в разделе «Диагностика ошибок ФПСУ»);
- Не сошлась имитовставка у полученного из туннеля пакета.

Сброс по GeoIP - пакеты, которые не прошли фильтр GeoIP и были сброшены ;

Отвергнуто - пакеты, которые не удалось успешно передать через этот сетевой адаптер (счетчик сброса растер по такими причинам, как переполнения буфера передачи, поврежденный кабель, плохой контакт в разъеме, Ethernet коллизия, неисправность самого сетевого адаптера).

Нажатие клавиши <*Del*> сбрасывает накопленную с момента запуска статистику в нулевые значения.

Третья группа значений демонстрирует состояние динамической памяти протокольного стека и носит справочный характер (см. рисунок ниже):

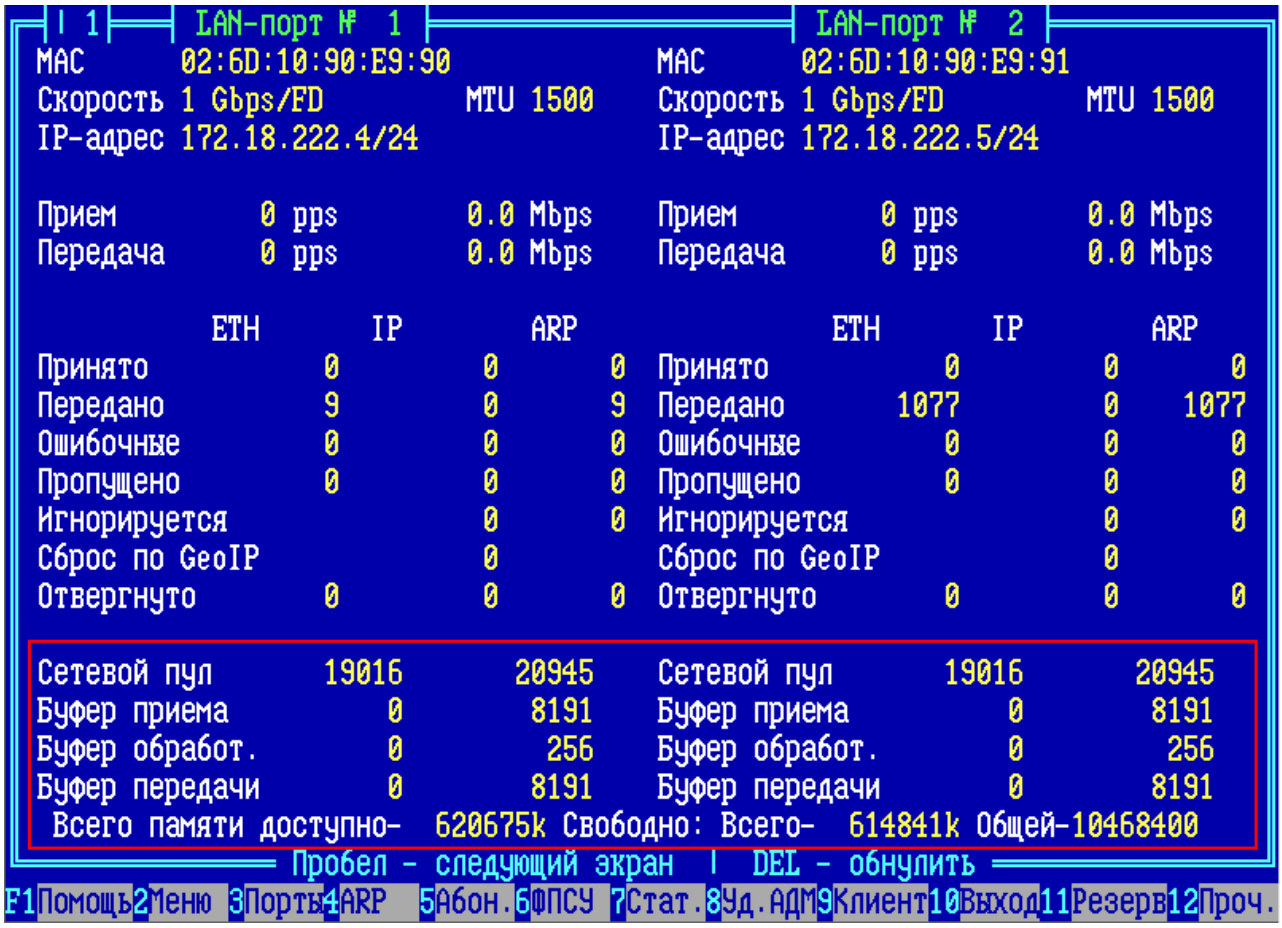


Рисунок 127 - Справочная информация состояния динамической памяти LAN-адаптеров

Сетевой пул — количество памяти в ethernet пакетах (фреймах), область выделенная в оперативной памяти ФПСУ, в которую сетевая карта помещает полученные фреймы. Размер пула указан в строке «Сетевой пул». Первое значение - сколько свободных частей памяти для фреймов есть в пуле, второе значение - размер пула. Как правило, один фрейм занимает одно значение в пуле. В зависимости от версии ФПСУ и конфигурации аппаратуры пулов может быть несколько. ФПСУ назначает пул каждому порту. Двум разным портам может быть назначен один и тот же общий пул, а могут быть назначены и разные пулы.

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

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

данной стадии.

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

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

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

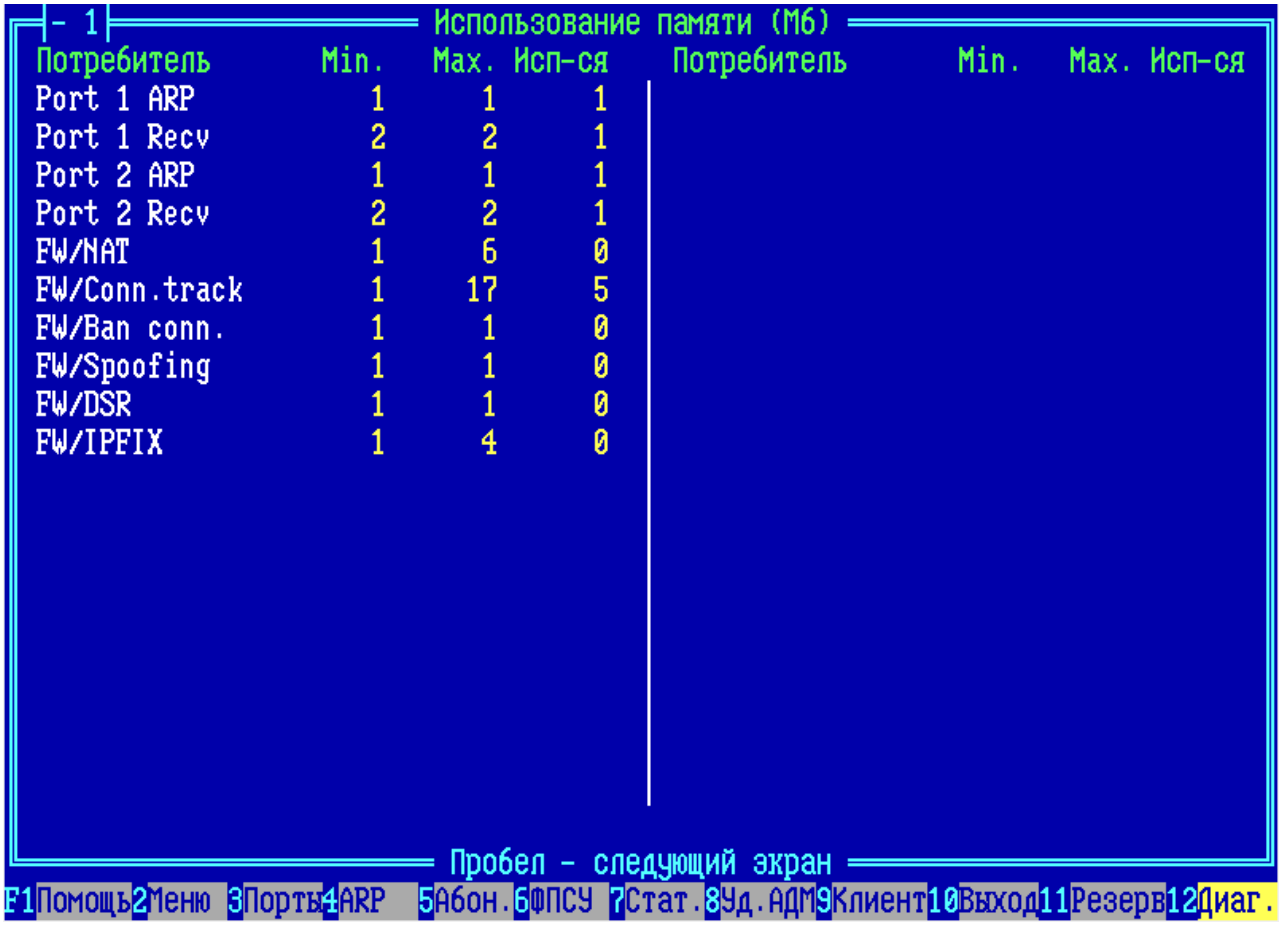


Рисунок 128 - Использование памяти ФПСУ

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

По нажатию клавиши *<Пробел>* осуществляется переход в окно «Мониторинг

сетевых портов»:

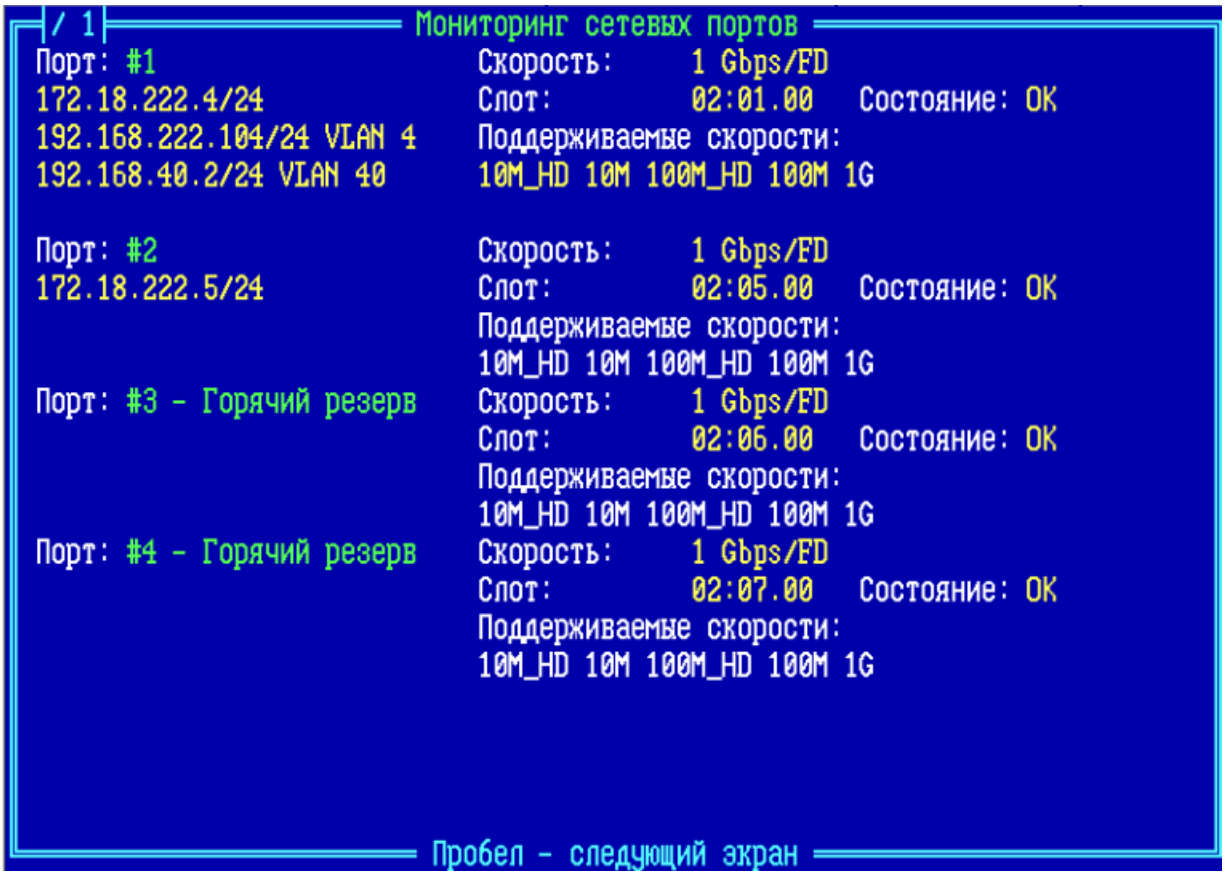


Рисунок 129 - Мониторинг сетевых портов ФПСУ

В окне выводится список портов, перемещение по списку осуществляется клавишами *<PgUp>*, *<PgDn>*.

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

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

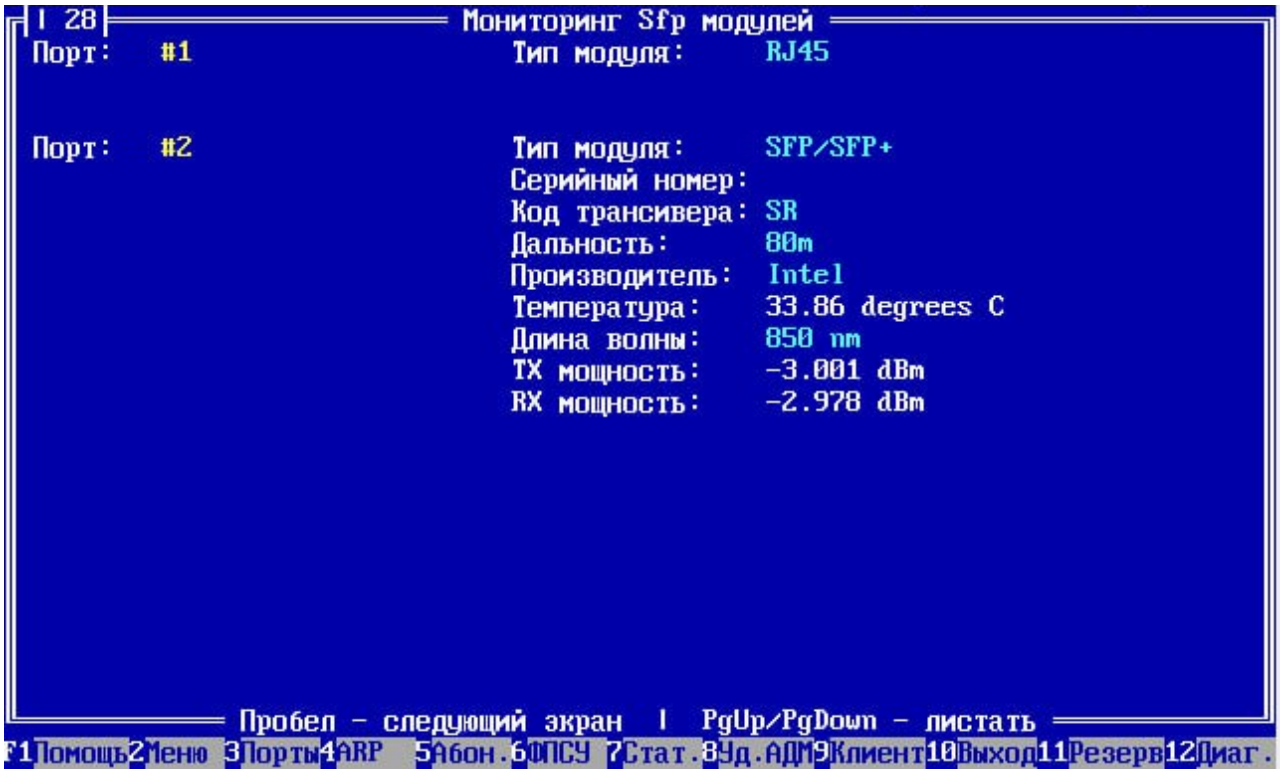


Рисунок 130 - SFP мониторинг ФПСУ

В окне выводится список портов, перемещение по списку осуществляется клавишами *<PgUp>*, *<PgDn>*.

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

4. 6. Окно состояния ARP-кэша

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

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

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

Запись может находиться в следующих состояниях (последнее поле):

***F** (Find)* - начата процедура определения MAC-адреса IP-абонента;

***D** (Dyn)* - MAC-адрес для соответствующего IP-адреса определен и запись будет вытеснена по истечении указанного времени, указанный IP-адрес является IP адресом явно описанного в конфигурации ФПСУ маршрутизатора или другого ФПСУ;

***A** (Auto)* - MAC-адрес для соответствующего IP-адреса определен и запись будет вытеснена по истечении указанного времени;

***C** (Check)* — начата процедура проверки соответствия IP адреса и MAC адреса данной записи ввиду истечения времени состояний Dyn или Auto;

***B** (BadFind)* - процедура поиска закончилась отрицательно, запись будет вытеснена по истечении указанного времени;

***S** (Static)* - для IP адреса задан статический MAC адрес, указанный в строке.

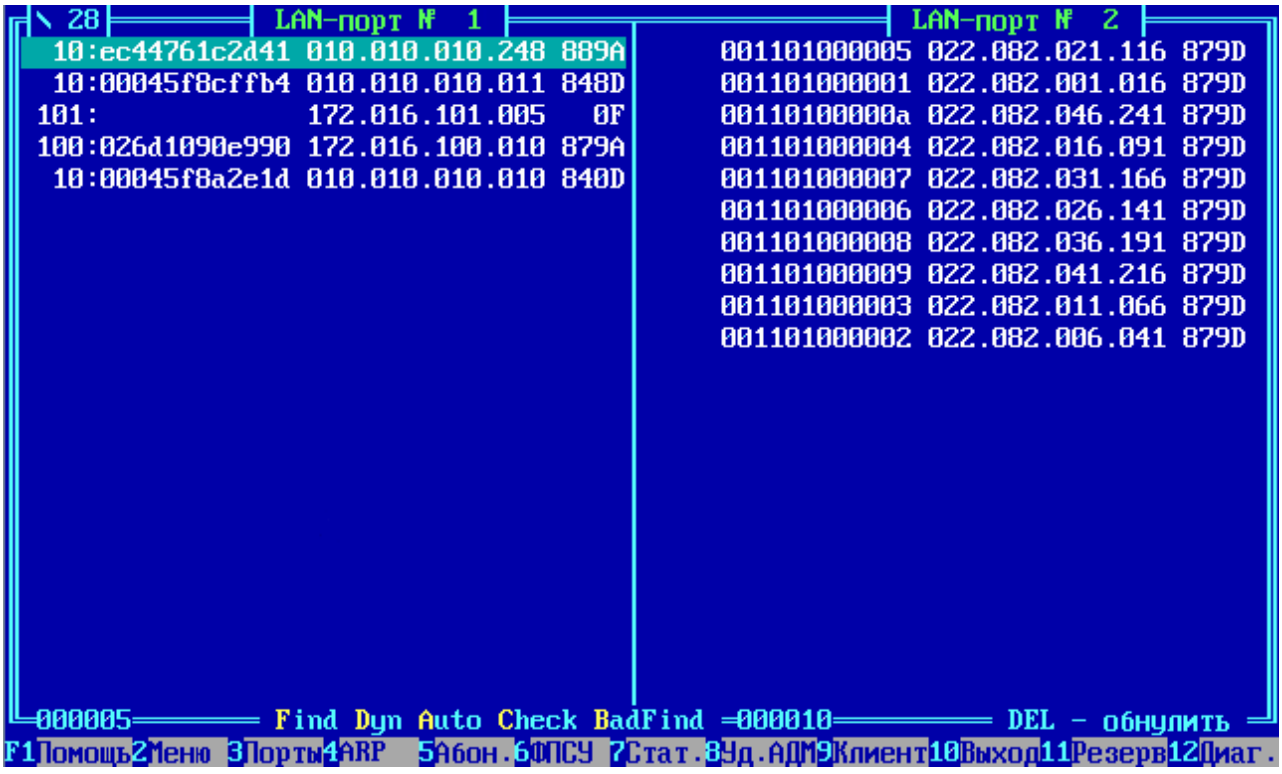


Рисунок 131 - Состояние ARP-кэша

Цифры внизу («000005» и «000010» на рисунке) означают общее количество записей в ARP-кэше для каждого порта.

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

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

4. 7. Окно состояния работы пользователей

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

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

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

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

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

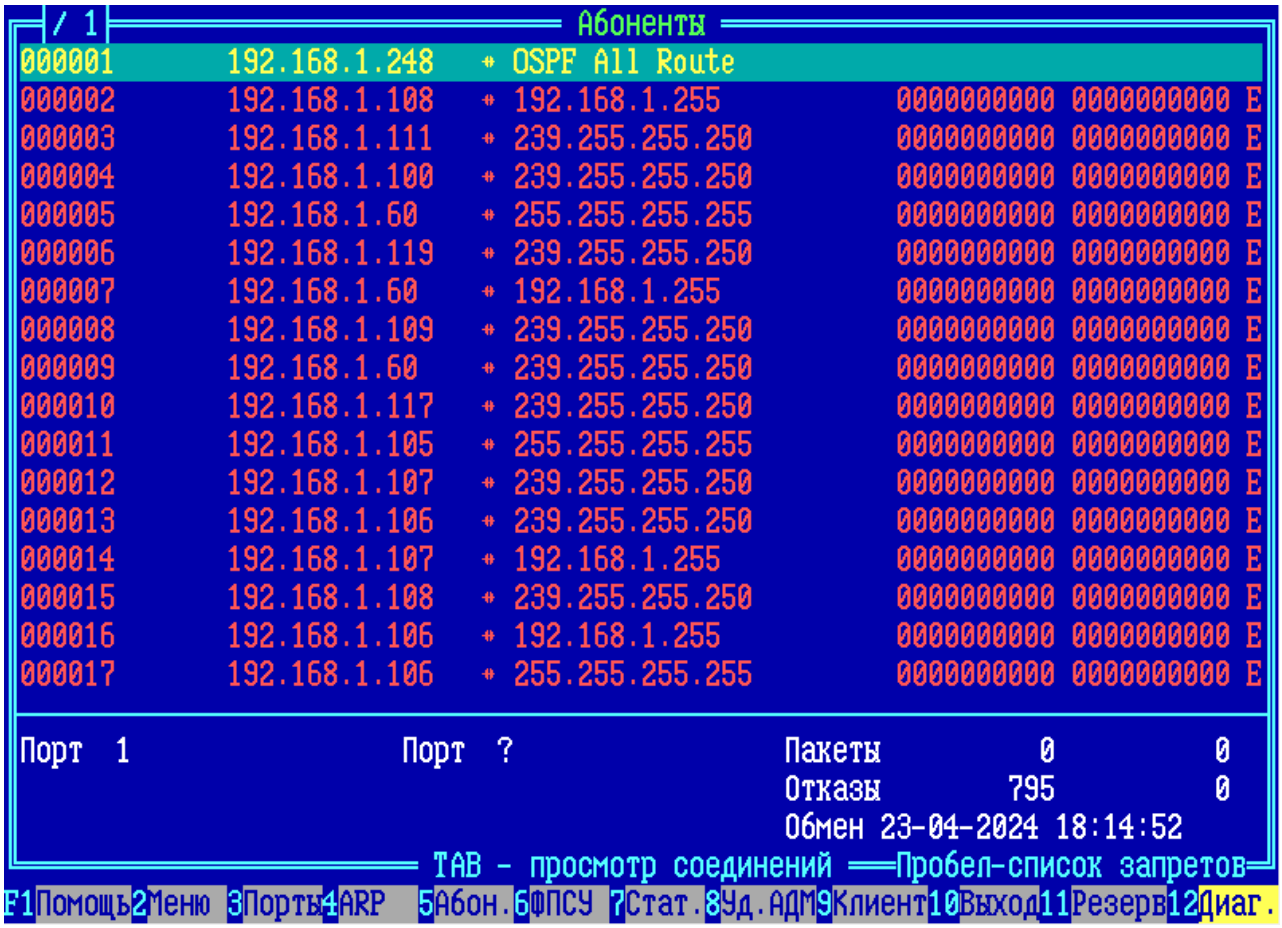


Рисунок 132 - Статистика переданных IP-пакетов

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

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

Рисунок 133 - Информация об ошибке

В окне отображаются количество отказов для данной пары абонентов, дата и время первого и последнего отказов, протокол, которому принадлежат пакеты, и причина отказа. Могут быть указаны следующие причины:

Ошибка МЭ	- запрет работы правилами межсетевого экрана (см. пункт «Параметры доступа, правила трафика межсетевого экрана»);
Мало памяти	- недостаточно оперативной памяти для обработки пакета;
Неверен IP адрес	- неверен IP адрес отправителя (широковещательный);
Короткий пакет	- ошибка формата пакета;
Дублирование адресов	- MAC-адрес отправителя равен MAC-адресу LAN-адаптеров ФПСУ;
Входящий не описан	- отправитель пакета не прописан в конфигурации портов ФПСУ (маршрутизации);
Получатель не описан	- получатель пакета не описан в конфигурации портов ФПСУ (маршрутизации);
Запрет работы	- отказ в доступе по причине «запрет работы» в конфигурации портов ФПСУ для одного или обоих абонентов-участников обмена;
Абонент миновал ФПСУ	- абонент в конфигурации портов ФПСУ указан как работающий через VPN-туннель с другим ФПСУ, но его пакеты приходят не из VPN-туннеля;
ФПСУ не работает	- ФПСУ 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 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 указан как работающий в режиме ретрансляция, но пакеты от него приходят из VPN-туннеля от другого ФПСУ;
Запрет SourceRoute	- было сброшен пакет с опцией SourceRoute: в общих параметрах конфигурации ФПСУ стоит запрет передачи пакетов с опцией SourceRoute;
Ошибочный фрагмент	- ошибка фрагментации удаленной станции;
Неверен список опций	- неверен список опций IP заголовка;
Нет ФПСУ-туннеля	- невозможно передать пакет в VPN-туннель, т.к. VPN-туннель между двумя ФПСУ не согласован;
Ошибочный ФПСУ-пакет	- ошибочный пакет от ФПСУ-IP, отправитель присылает пакет, обозначенный как пакет протокола взаимодействия между ФПСУ-IP, но структура пакета содержит ошибки.

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

В строке соединения предоставляются следующие сведения о соединении:

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

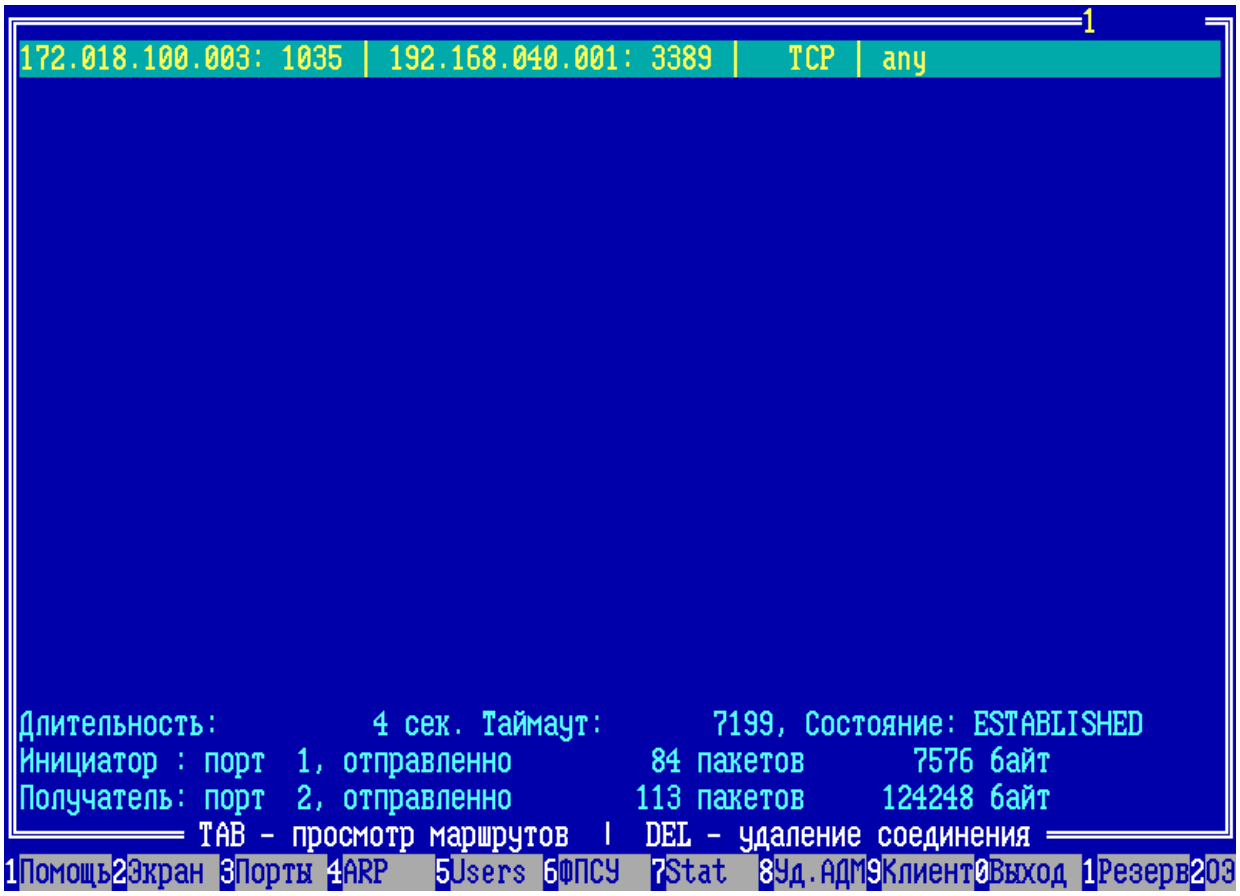


Рисунок 134 - Таблица состояния соединений ФПСУ

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;
- текущее состояние сессии;
- порт инициатора и получателя соединения;
- объем переданных в рамках соединения данных, в пакетах и байтах.

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

В окне текущих соединений по клавише *<Tab>* осуществляется переход в окно просмотра маршрутов.

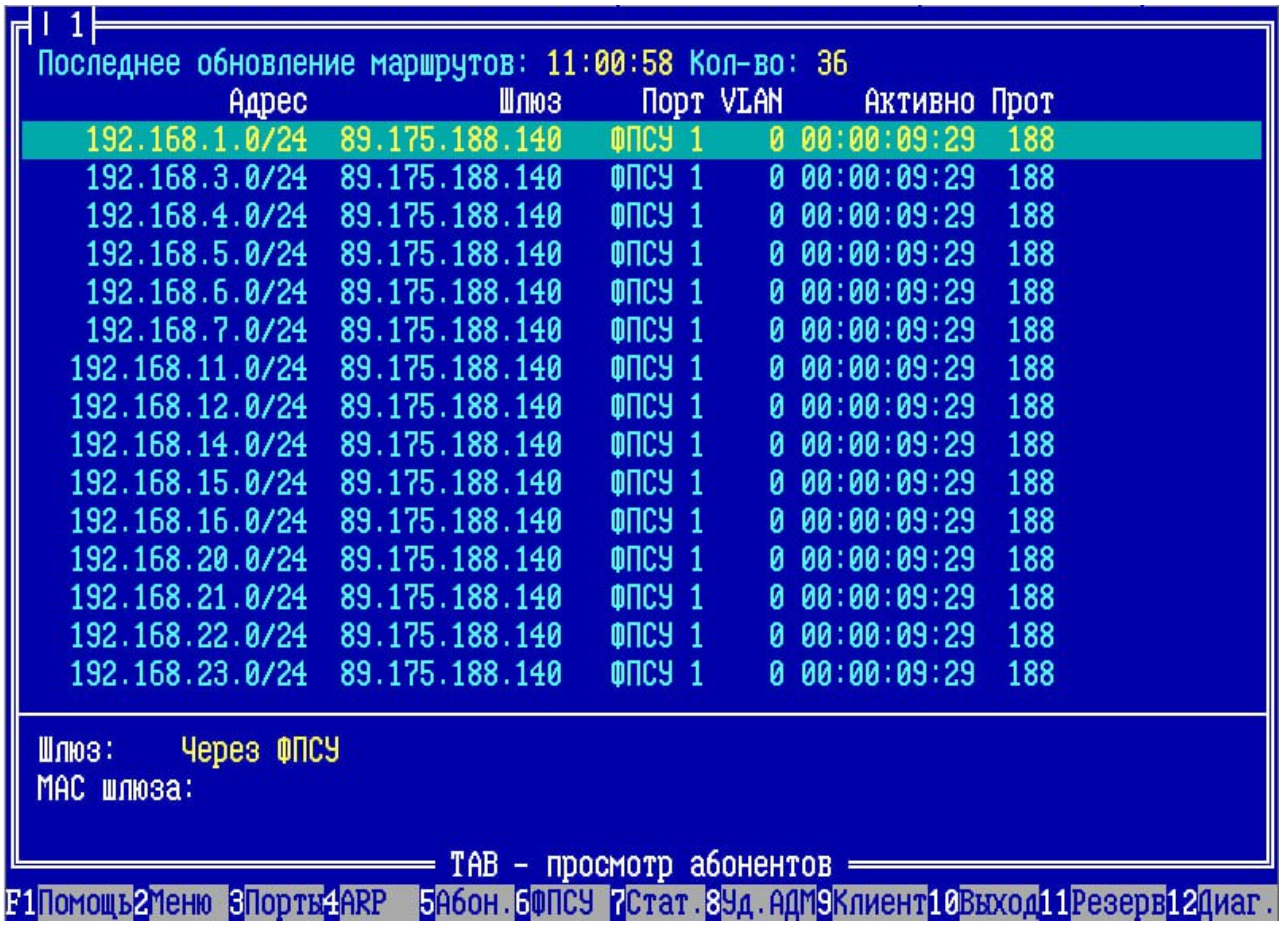


Рисунок 135 - Таблица динамических маршрутов на ФПСУ

В строке маршрута выводятся сведения:

- адрес сети или узла назначения, маска сети назначения;
- шлюз, обозначающий IP-адрес порта ФПСУ или маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения;
- номер порта ФПСУ, являющийся шлюзом;
- описатель VLAN;
- текущее время маршрута;
- протокол маршрутизации:

  2 - статический маршрут;

  3 - маршрут, установленный во время загрузки;

  186 - BGP;

  188 - OSPF.

4. 8. Окно состояния VPN-туннелей с другими ФПСУ

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

В окне отображаются сведения о VPN-туннелях с другими ФПСУ или IP-in-IP маршрутизаторами. Для каждого туннеля указывается ряд справочной информации: номер порта и VLAN (если настроен), указанное в конфигурации наименование и IP-адрес удаленного ФПСУ и сведения о состоянии внутреннего протокола обмена между ними.

Записи о VPN-туннеле в таблице маркируются разным цветом в зависимости от состояния VPN-туннеля. Запись желтым цветом свидетельствует об успешном установлении VPN-туннеля. Запись красным цветом свидетельствует об ошибке установления VPN-туннеля.

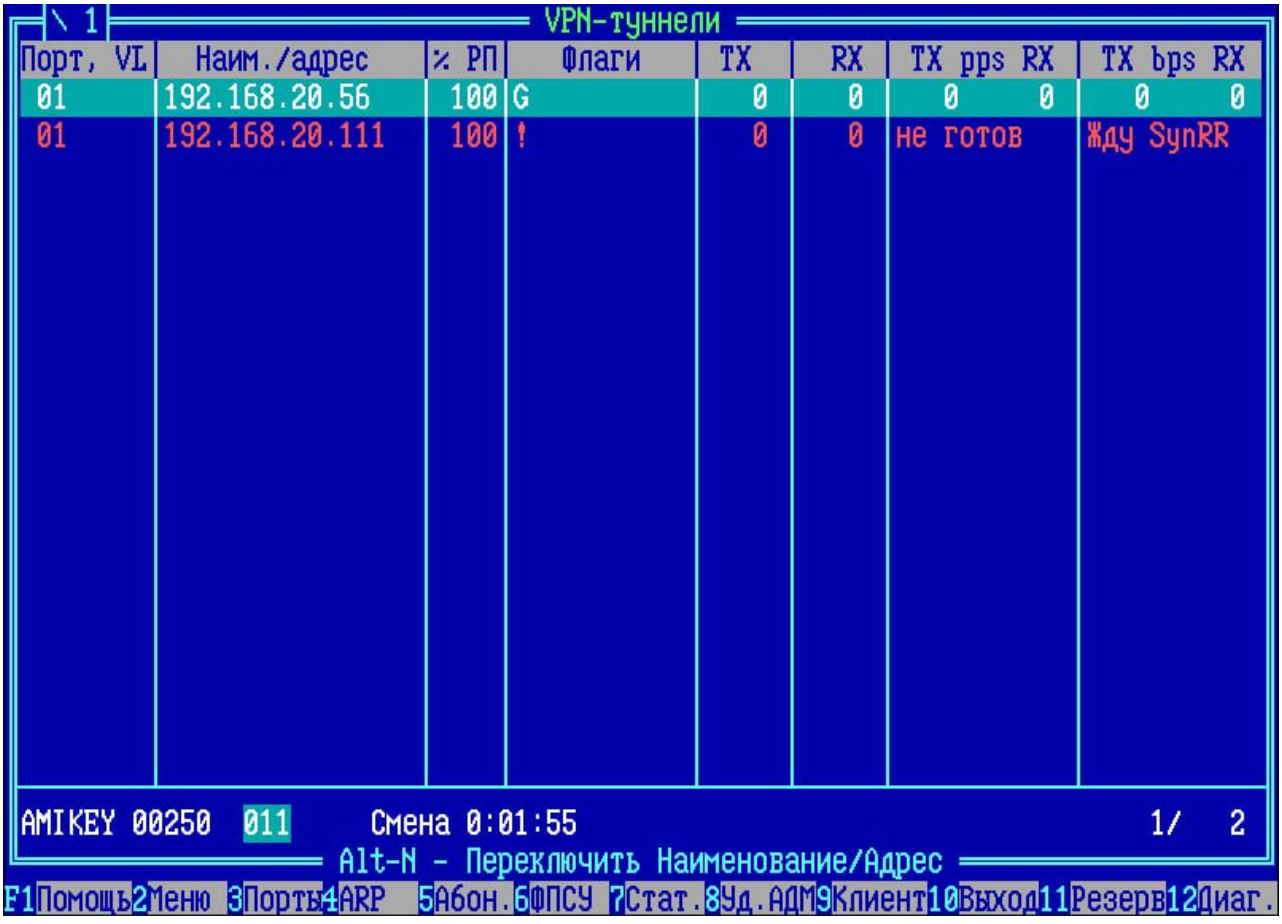


Рисунок 136 - Состояние туннелей с другими ФПСУ

В столбцах **TX** (**RX**) указывается количество переданных (принятых) пакетов через выбранный туннель.

В столбце **TX pps RX** указывается текущая скорость передачи данных в туннеле, в пакетах в секунду.

В столбце **TX bps RX** указывается текущая скорость передачи данных в туннеле, в байтах в секунду.

Состояния туннеля могут быть следующими:

- *RecvOk SendOk* - туннель работоспособен, состояние показывает, что соединение с другим ФПСУ прошло успешно и туннель готов принимать и передавать данные абонентов;
- *RecvOk* - прием возможен и разрешен;
- *NoRecv* - прием данных от другого ФПСУ невозможен;
- *SendOk* - передача возможна и разрешена;
- *NoSend* - передача данных другому ФПСУ невозможна;
- *WaitARP* - прием и передача данных абонентов невозможны, маршрут до удаленного ФПСУ 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. Отображается в случаях ошибок с парно-выборочными ключами на текущем или удаленном ФПСУ (например, не согласованность конфигураций ФПСУ в используемых номерах ключевых данных, серии или криптосети; ошибки чтения файла с ключевыми данными). Также отображается, когда по указанному IP-адресу находится не ФПСУ, а другое устройство, с которым невозможно установить VPN-туннель;
- *WaitSynOk* - прием и передача данных абонентов невозможна, ожидается синхронизация с удаленным ФПСУ;
- *Ошибка сериализации* - удаленный и локальный ФПСУ имеют одинаковые серийные номера, установление соединения невозможно.

После разрешения синхронизации возможны следующие дополнительные флаги, указывающее на те или иные параметры соединения:

! - для данного туннеля не задействовано шифрование передаваемых данных;

A - для данного туннеля включен режим контроля туннеля (задан интервал контроля туннеля, подробнее см. пункт «Дополнительные параметры соединения ФПСУ-ФПСУ»);

a - для данного туннеля включен режим контроля туннеля и доминирует настройка соседнего ФПСУ;

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 (L2-шифрование);
Aut - ожидается подтверждение на выданный удаленному ФПСУ сеансовый аутентификатор;
C - согласован режим потокового сжатия данных абонентов в VPN-туннеле между двумя ФПСУ;
T - согласован режим криптозащиты данных абонентов в VPN-туннеле между двумя ФПСУ;
P - согласован режим пакетного шифрования данных абонентов. Этот маркер появляется только тогда, когда хотя бы на одном из двух участвующих в построении туннеля ФПСУ 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 с версиями программного обеспечения 3.0 и выше.

В нижней части экрана для текущего удаленного ФПСУ отображаются согласованные им для использования ключи и время, оставшееся до смены сеансовых ключей.

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

4. 9. Окно состояния связи с удаленными администраторами

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

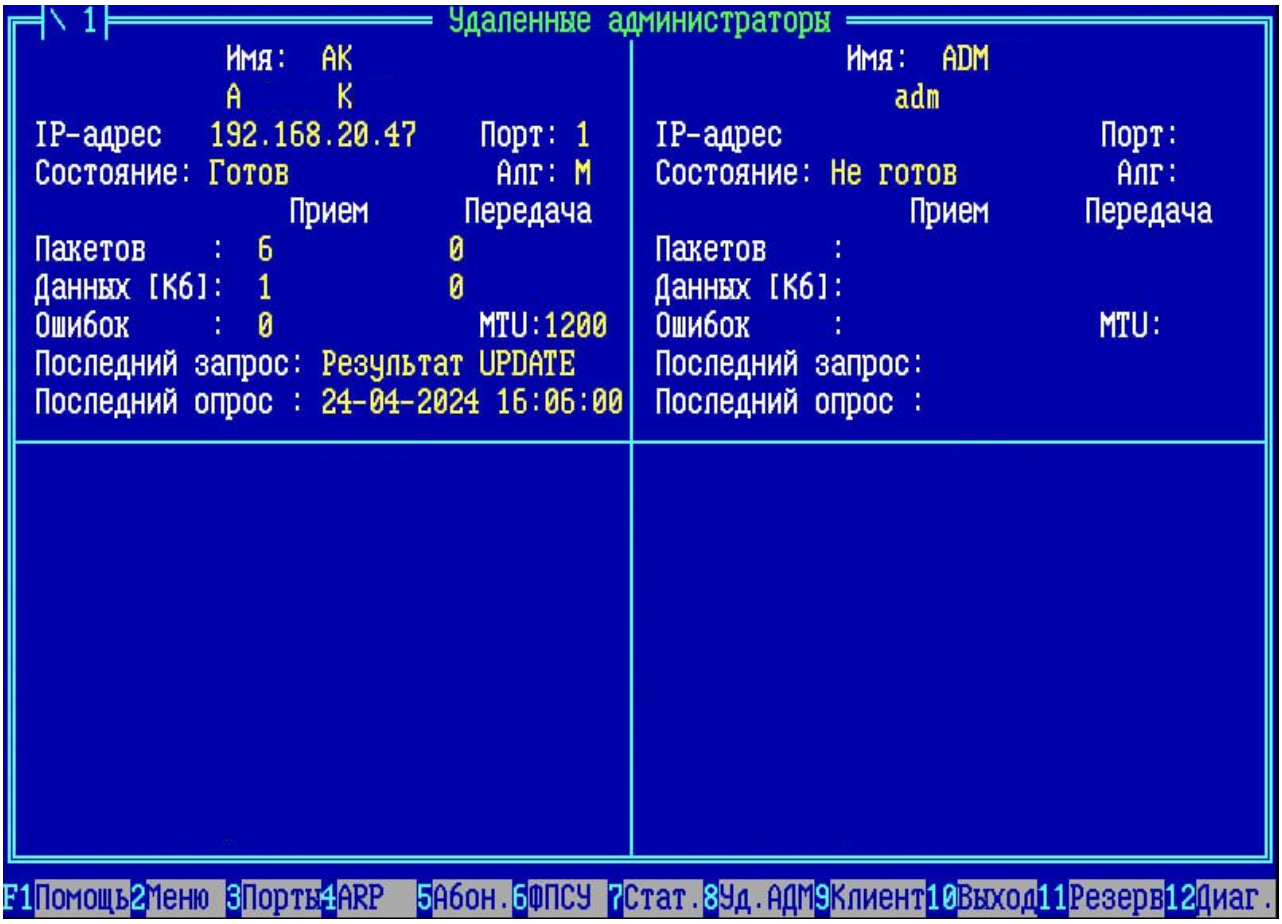


Рисунок 137 - Просмотр состояния удаленных администраторов

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

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

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

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

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

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

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

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

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

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

  C – при передаче данных используется сжатие.

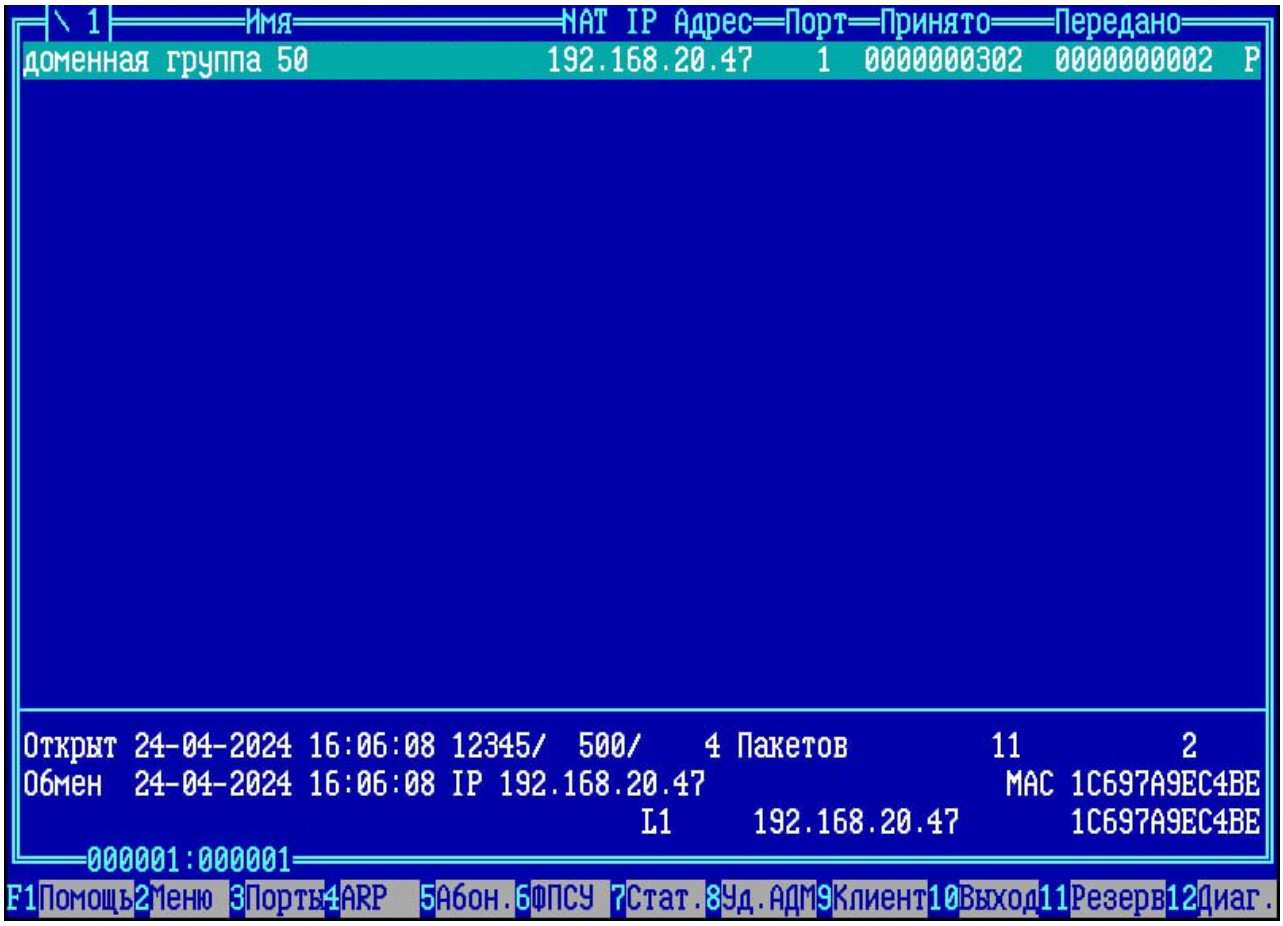


Рисунок 138 - Отображение состояния работы Клиентов

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

- дата и время открытия туннеля - соединения ФПСУ-IP/Клиента с ФПСУ;
- 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;
- дата и время последнего обмена данными между ФПСУ и ФПСУ-IP/Клиентом;
- IP-адрес рабочей станции, с которой подключился ФПСУ-IP/Клиент;
- MAC-адрес ФПСУ-IP/Клиента в ARP-таблице ФПСУ.

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. 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 пакетов (см. пункт «Окно состояния работы пользователей»).

4. 11. КРК. Общая статистика

Для просмотра информации с подключенных к ФПСУ устройств СВКРК нажмите <*F12*>. В окнах общей диагностики следует, нажимая клавишу <*Пробел*>, перейти к экрану «КРК: Общая статистика».

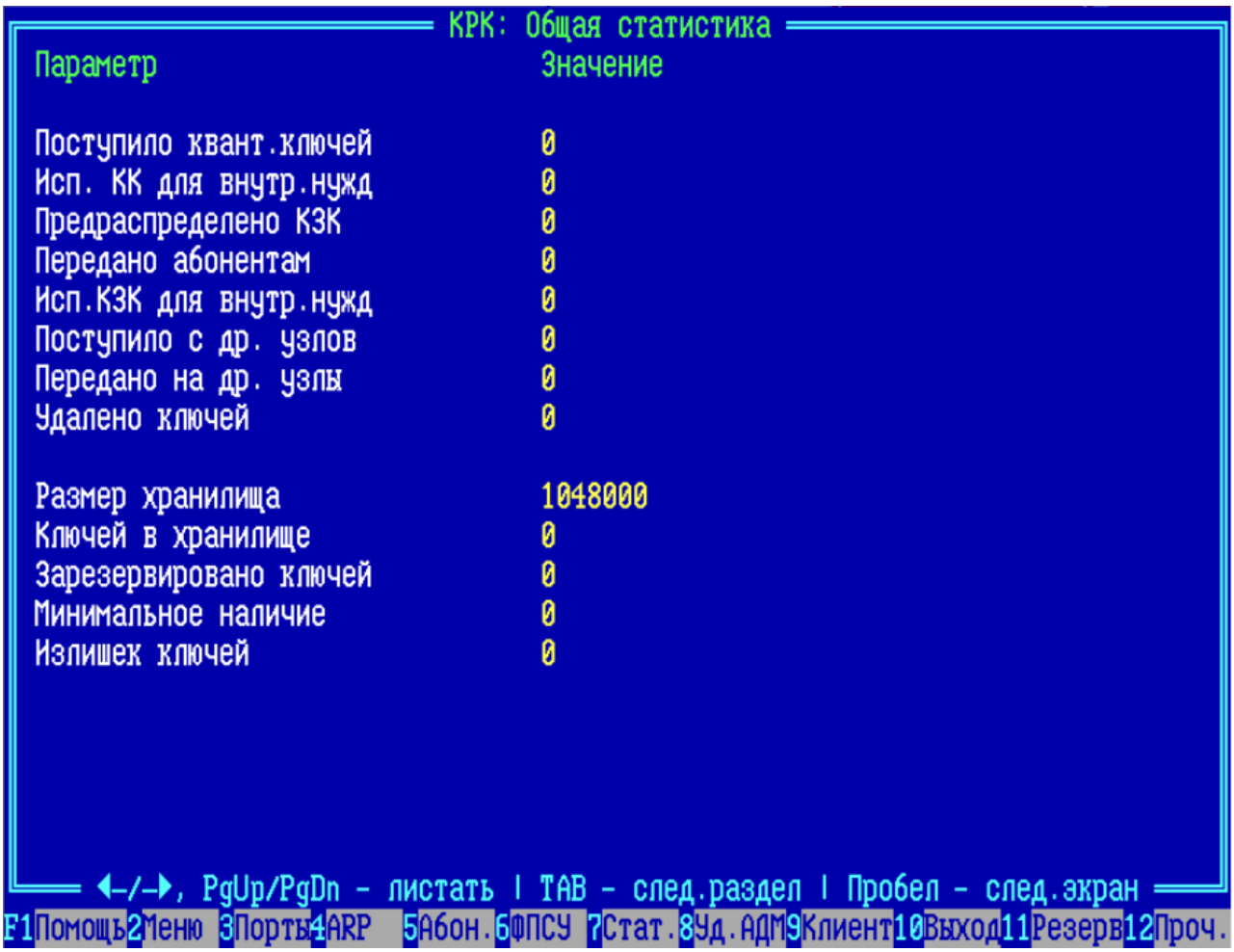


Рисунок 139 - Отображение состояния работы Клиентов

На экран выдается информация о количестве квантовых ключей с детализацией о поступивших на ФПСУ КК, об использованных КК и КЗК для внутренних нужд; о предраспределенных квантово-защищенных ключах, о ключах переданных абонентам, о ключах поступивших с других узлов, о ключах переданных на другие узлы, об удаленных ключах, о ключах в хранилище, о зарезервированных ключах, о минимальном наличии и об излишке ключей в хранилище, а также о размере хранилища ключей. В таблице ниже

приведено описание выводимых параметров:

4. 12. Окно состояния подсистемы «горячего» резервирования

Вызов окна отображения состояния текущей работы ФПСУ 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 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 и его партнером по резервированию), через которые происходит взаимодействие между участвующими в системе «горячего» резервирования ФПСУ. Для ФПСУ, начиная с релиза программного обеспечения 2.65, может быть установлено до четырех таких туннелей, до двух через сетевые адаптеры подсистемы горячего резервирования, и до двух через сетевые адаптеры рабочих портов.

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

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

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

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

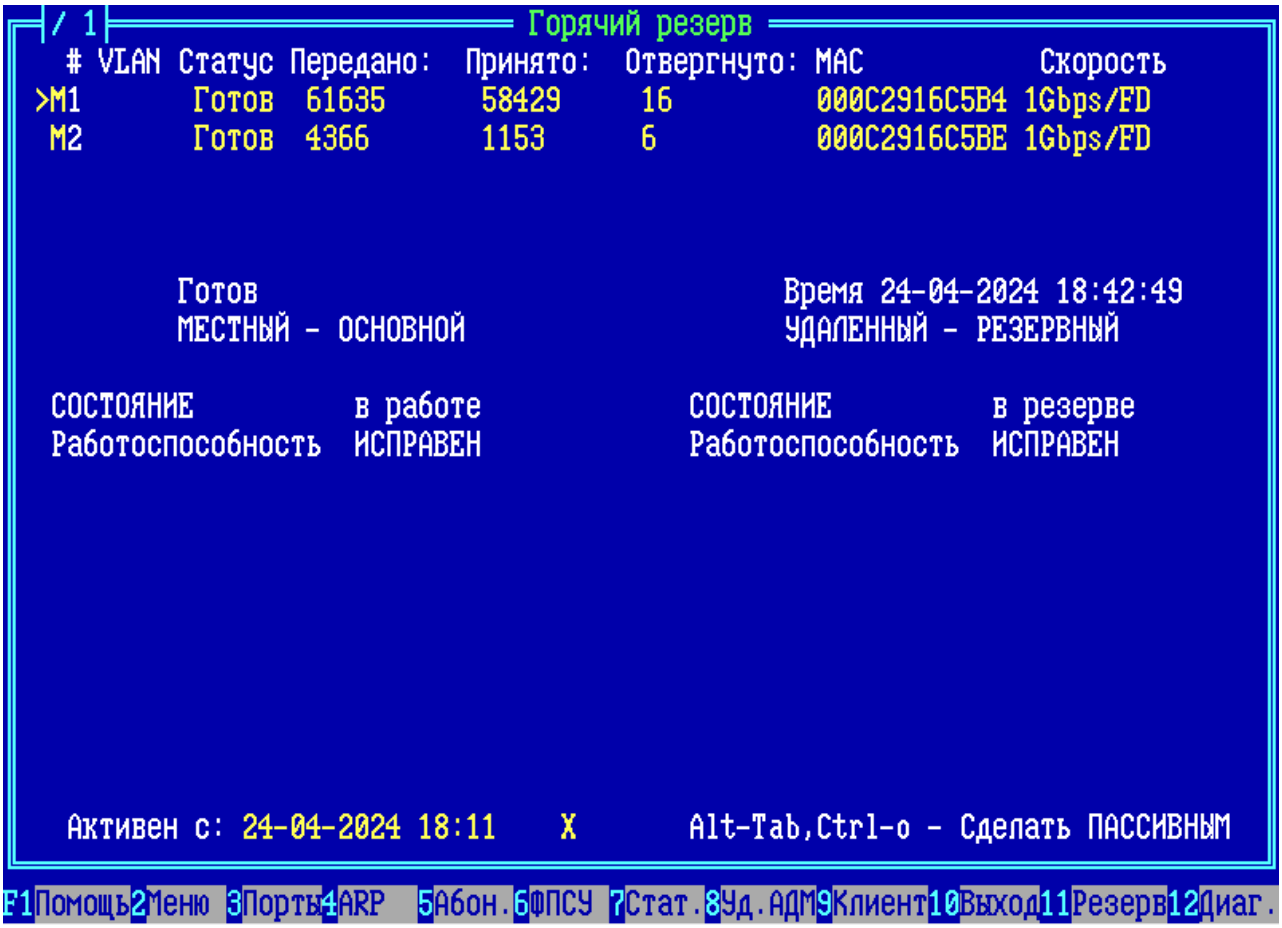


Рисунок 140 - Отображение состояния «горячего» резервирования

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

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

- *«Передано»* - количество переданных пакетов от этого ФПСУ в данный VPN-туннель «горячего резерва»;
- *«Принято»* - количество корректно принятых пакетов от удаленного ФПСУ через данный VPN-туннель «горячего резерва»;
- *«Ошибочных»* - количество принятых пакетов от удаленного ФПСУ через данный VPN-туннель «горячего резерва», которые были сброшены на этом ФПСУ. 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 по резервированию.

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

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

Исключение: при включении питания и запуске ФПСУ 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 принимает решение, что отсутствие подключения к сети передачи данных на этом сетевом адаптере является штатным режимом взаимодействия ФПСУ с сетью передачи данных и устанавливает локальную оценку состояния ФПСУ в значение «Работоспособность: ИСПРАВЕН» (такое исключение требуется при подключении ФПСУ к сетевому оборудованию не в разрыв сети, а только одним рабочим портом).

Если на ФПСУ 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»).

В левом нижнем углу указывается информация о длительности текущего функционального статуса ФПСУ, 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 через консольное соединение), о чем сообщает подсказка в нижней части экрана. Операция доступна администраторам класса *Оператор* и выше, кроме того, вход может быть защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации в системе.

4. 13. Информационные окна жидкокристаллического экрана

Программно-аппаратный комплекс ФПСУ 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 141 - Жидкокристаллический дисплей ФПСУ

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

Основное информационное окно

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

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

Схематичный пример основного информационного окна:

A	**M**	**I**	**0**	**0**	**0**	**0**	**1**	**C**	**O**			**О**	**С**	**Н**	**О**	**В**	**Н**	**О**	**Й**
/		**В**		**Р**	**А**	**Б**	**О**	**Т**	**Е**			**А**	**К**	**Т**	**И**	**В**	**Е**	**Н**	

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

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

Окно версий компонентов ФПСУ

В информационном окне версий компонентов ФПСУ отображаются:

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

Пример окна версий компонентов ФПСУ:

П	**О**		**Ф**	**П**	**С**	**У**	**-**	**I**	**Р**					**v**	**4**	**.**	**0**	**1**	
H	**W**		**F**	**P**	**S**	**U**	**I**	**P**	**-**	**S**	**T**	**D**	**3**	**-**	**1**	**U**			

Окно продолжительности работы и текущей загрузки

В информационном окне продолжительности работы и текущей загрузки отображаются:

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

Пример продолжительности работы и текущей загрузки ФПСУ:

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**	**%**		

5. Контроль целостности программного обеспечения

ФПСУ содержит ряд механизмов, обеспечивающих защиту программных модулей от НСД, в частности, автоматический контроль целостности программных модулей, находящихся на внутреннем носителе информации.

В случае локального управления ФПСУ с помощью консольного подключения через COM-порт, необходимо выполнять контроль целостности программного обеспечения рабочей станции, с которой осуществляется подключение, в соответствии с правилами пользования на СКЗИ.

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

Дополнительная проверка целостности внутренних программных модулей ФПСУ проводится при попытке запуска файла. Действие запуска файла перехватывается при попытке выполнения, файл сравнивается по списку разрешенных к выполнению файлов. Если запускаемый файл присутствует в списке, то выполняется подсчёт контрольной суммы файла и сравнение рассчитанной контрольной суммы с эталонной. Только при совпадении рассчитанной контрольной суммы с эталонной файл разрешается к запуску. Результаты проверки записываются в статистику (подраздел статистики 6.4).

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

Дополнительная проверка целостности ПО и запуск тестов осуществляется из пункта «Сервисные функции → Проверка целостности» главного меню ФПСУ.

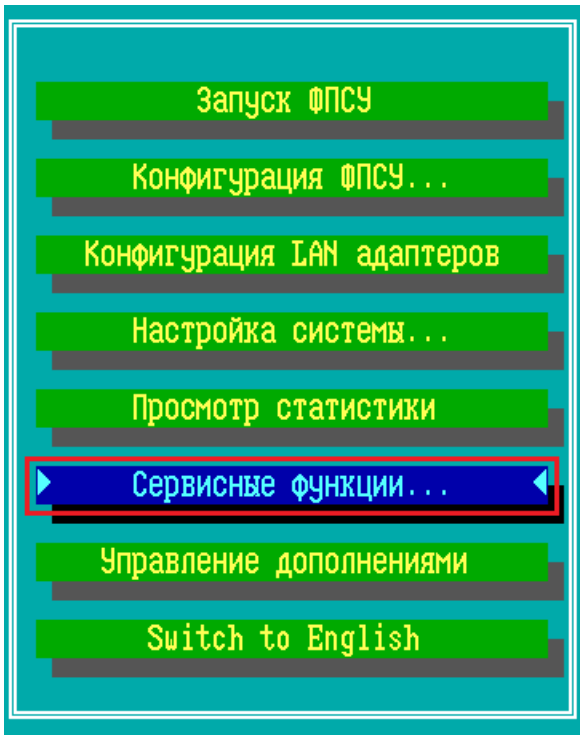


Рисунок 142 - Главное меню ФПСУ

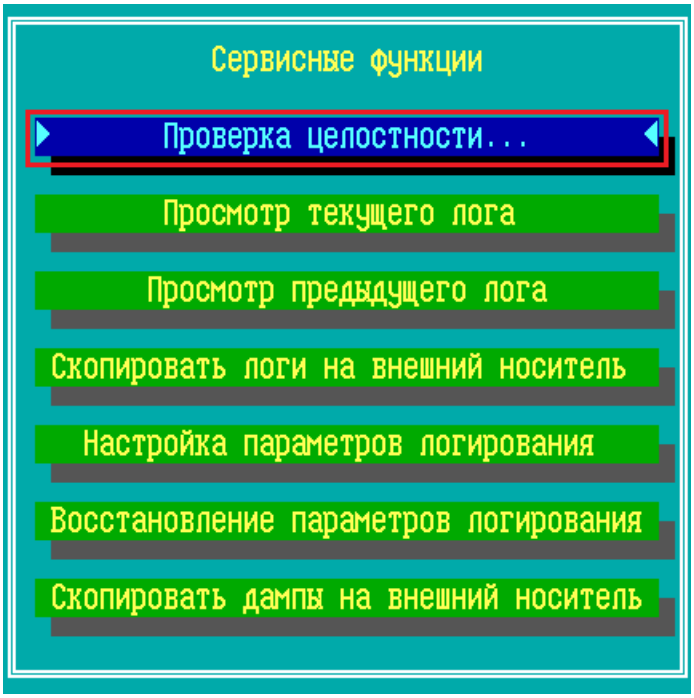


Рисунок 143 - Меню «Сервисные функции»

5. 1. Проверка целостности программных модулей ФПСУ

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

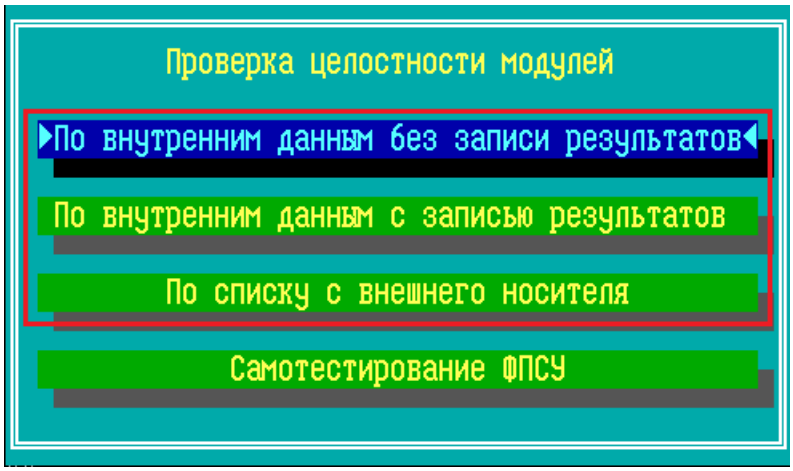


Рисунок 144 - Меню проверки целостности ПО

«По внутренним данным без записи результатов» - проверка целостности ПО ФПСУ происходит по хранящимся на внутреннем накопителе эталонным контрольным суммам, с выводом результата проверки (успешно или обнаружена ошибка) на экран. Операция доступна администраторам класса Администратор или Инженер.

«По внутренним данным с записью результатов» - проверка целостности ПО ФПСУ происходит по хранящимся на внутреннем накопителе эталонным контрольным суммам, с выводом результата проверки (успешно или обнаружена ошибка) на экран и в файл с расширением .LST на внешний носитель. Операция доступна администраторам класса Администратор.

«По списку с внешнего носителя» - проверка целостности ПО ФПСУ 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. Операция доступна администраторам класса Администратор.

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

После отработки программы результаты проверки будут выданы на экран монитора и в файл FPSUHASH.LST на тот же носитель, с которого был считан файл-задание. Файл

FPSUHASH.LST может быть прочитан и обработан на другом компьютере средствами текстового редактора, поддерживающим кодировку OEM/DOS.

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

5. 2. Самотестирование функций межсетевого экрана ФПСУ

Из пункта меню «Проверка целостности» администратор может выполнить ручную проверку функционала межсетевого экрана ФПСУ, «Самотестирование ФПСУ»:

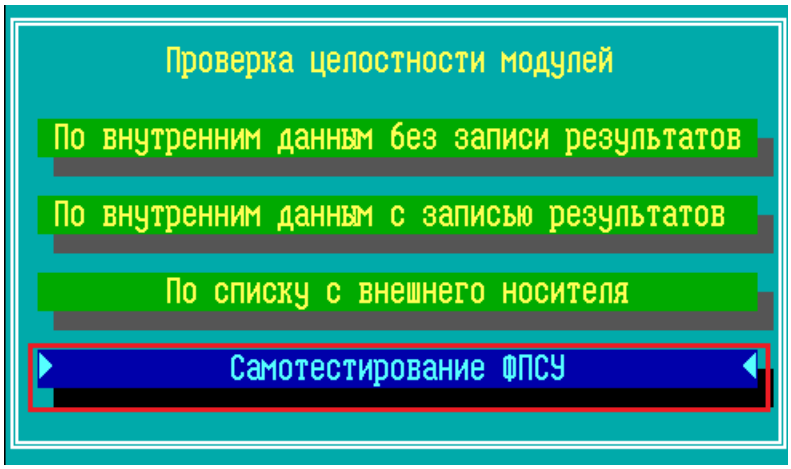


Рисунок 145 - Команда запуска внутреннего теста межсетевого экрана ФПСУ

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).

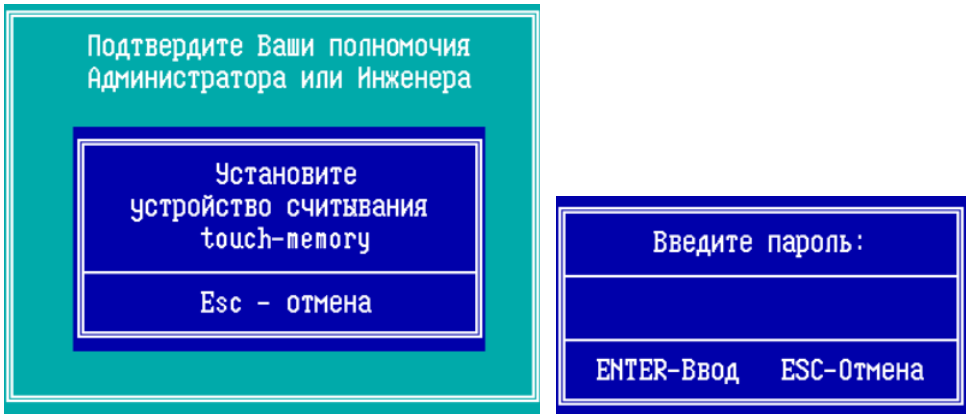


Рисунок 146 - Подтверждение полномочий и ввод пароля ТМ

При выполнении этой команды ФПСУ 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 и выведено окно с процессом выполнения самотестирования:

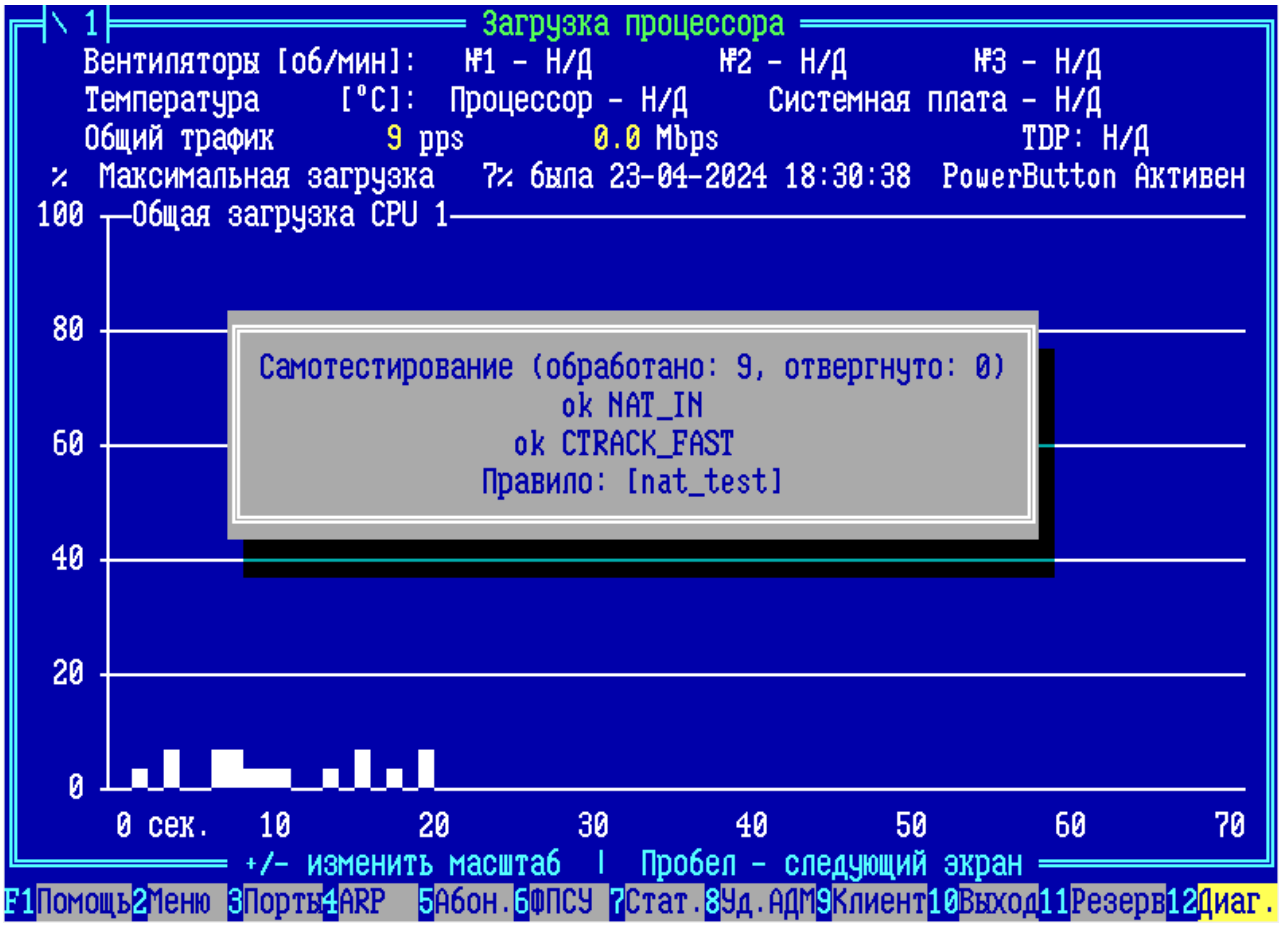


Рисунок 147 - Выполняется самотестирование ФПСУ

В случае успешной проверки, будет выдано оповещение:



Рисунок 148 - Сообщение об успешно пройденном самотестировании

В случаях, если самотестирование ФПСУ завершилось с ошибкой, требуется переустановить ФПСУ с дистрибутива.

Результат прохождения самотестирования записывается в статистику ФПСУ.

6. Конфигурация ФПСУ

Конфигурирование ФПСУ 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:

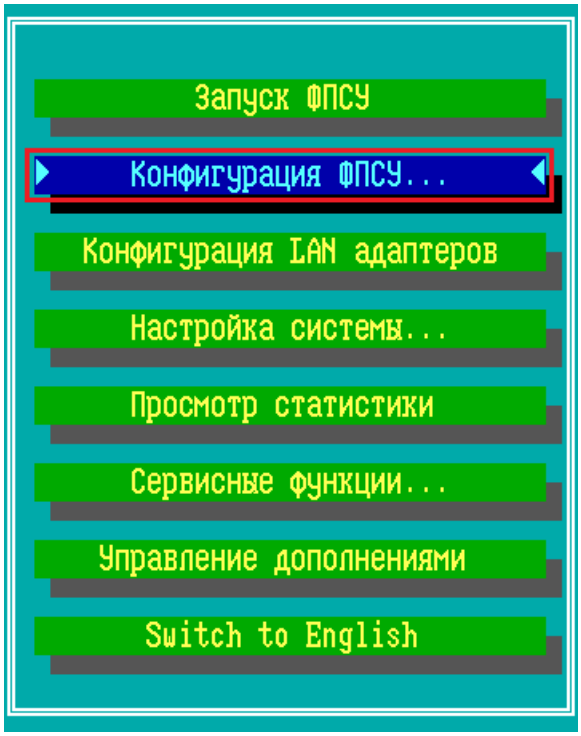


Рисунок 149 - Главное меню ФПСУ

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



Рисунок 150 - Команды работы с конфигурацией

Опции меню «Конфигурация ФПСУ»:

- «Отредактировать» – команда входа в подсистему конфигурирования для внесения изменений в параметры работы ФПСУ.
- «Сохранить на носитель» – команда записи текущей конфигурации ФПСУ в специальном формате на съемный носитель для хранения или переноса на рабочее место удаленного администратора. Опция доступна администраторам классов *«Инженер»* и *«Администратор»* (см. пункт «Разграничение доступа и пользователи», Таблица 3).
- «Восстановить с носителя» – команда восстановления конфигурации ФПСУ из ранее сохраненной. Опция доступна администратору класса *«Администратор»*.
- «Контроль целостности» – команда проверки внутреннего файла конфигурации ФПСУ по хранящейся на внутреннем накопителе ФПСУ контрольной сумме. Контрольная сумма конфигурации ФПСУ не является неизменной, она пересчитывается каждый раз, когда администратор ФПСУ сохраняет выполненные изменения в конфигурации. Для выполнения команды требуются права роли *«Администратор»*. Результат ручной проверки целостности конфигурации пишется в статистику ФПСУ.

При попытке войти в подсистему конфигурирования (команда «Отредактировать»), ФПСУ потребует прижать к контактному устройству электронный ТМ-идентификатор (или подключить USB ТМ-идентификатор к USB-порту ФПСУ), 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 подключаемого ТМ (см. раздел «Окно регистрации ТМ»).



Рисунок 151 - Подтверждение полномочий и ввод пароля ТМ

Установленные параметры конфигурации ФПСУ могут впоследствии редактироваться администратором, имеющим полномочия *Администратора* или *Инженера*.

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

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

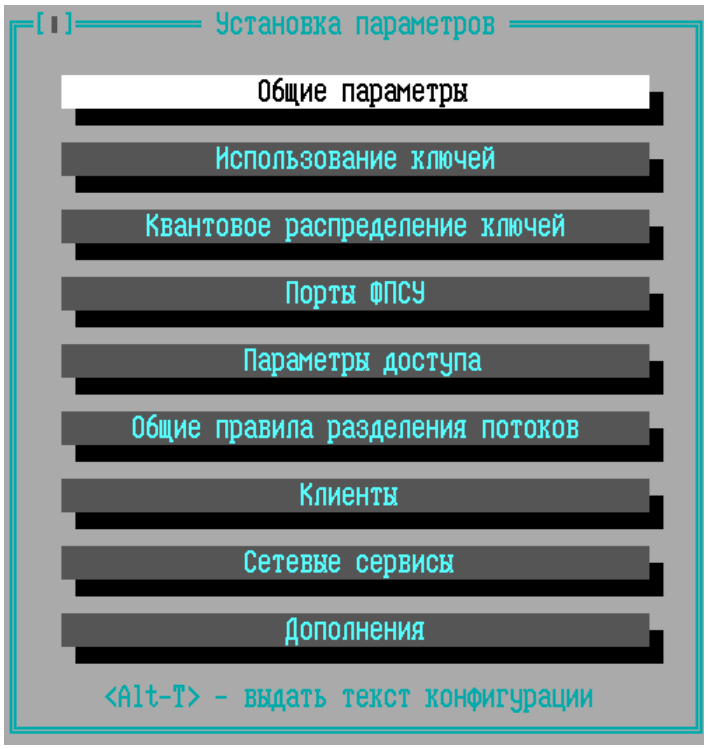


Рисунок 152 - Меню подсистемы конфигурирования ФПСУ

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

6. 1. Общие параметры конфигурации ФПСУ

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

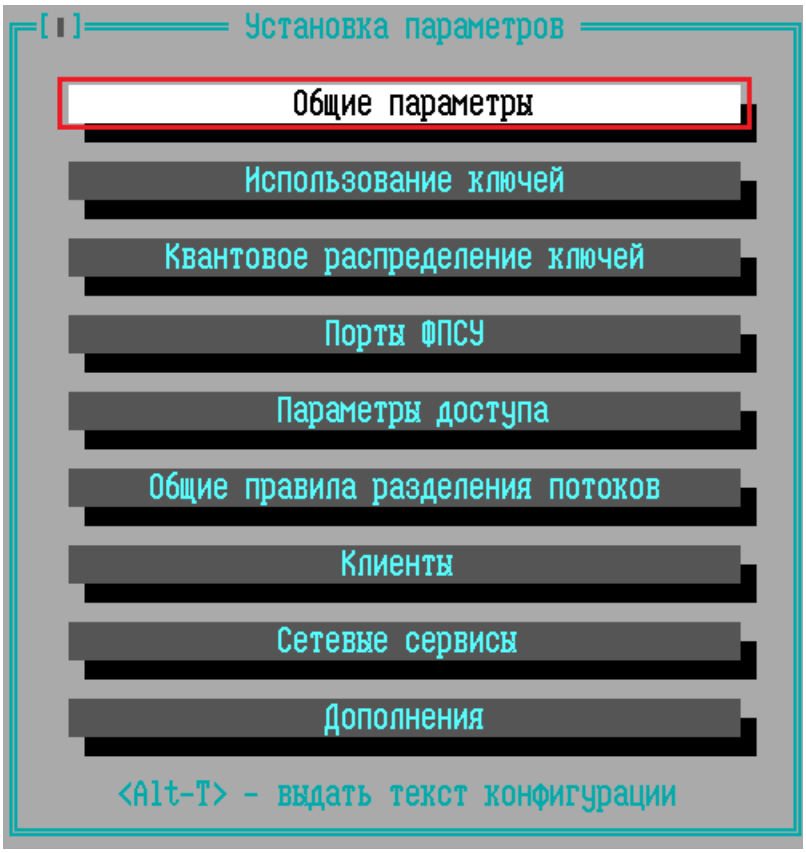


Рисунок 153 - Вход в общие настройки из основного меню конфигурации ФПСУ

Окно установки содержит следующие настраиваемые общие параметры:

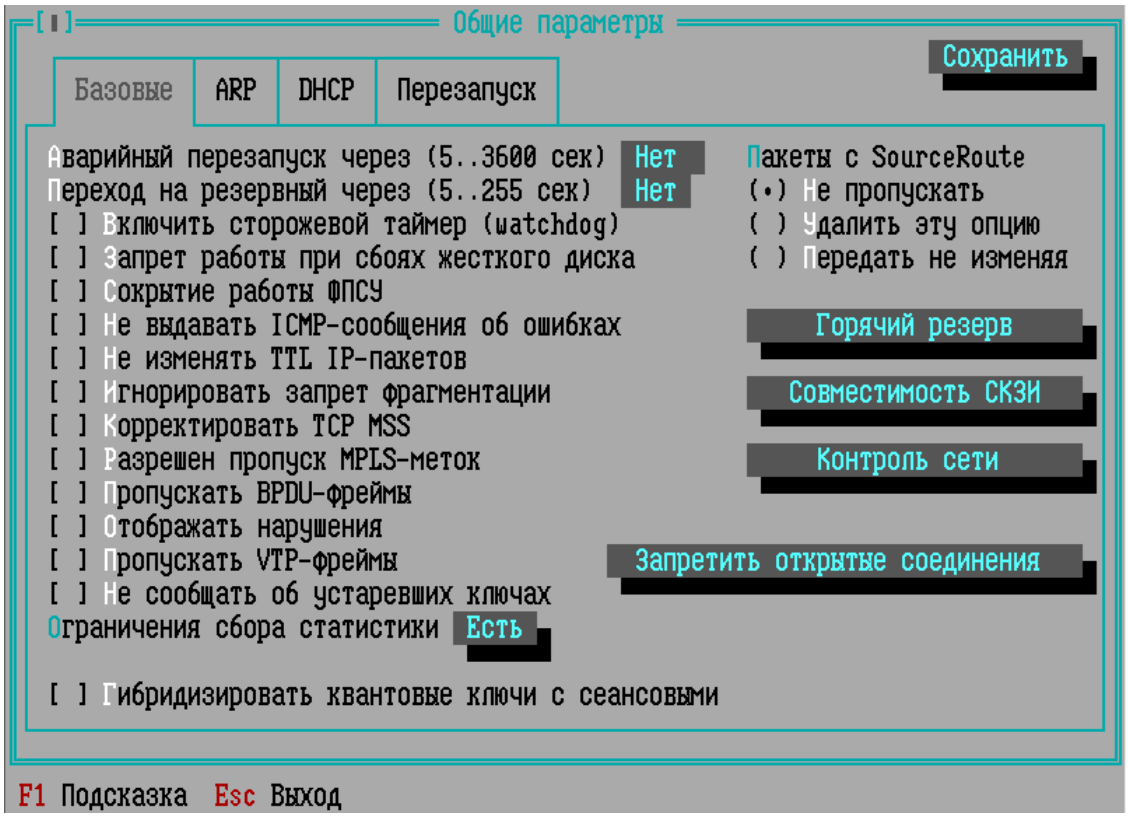


Рисунок 154 - Настройка общих параметров ФПСУ

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

Настройки на вкладке «Базовые» окна «Общие параметры»:

Аварийный перезапуск. Если при работе ФПСУ происходит аппаратный сбой сетевых адаптеров, ФПСУ 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 автоматически перегрузятся, после чего ФПСУ 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 получает сигнал от сетевой аппаратуры об отсутствии физического соединения на каком-либо из рабочих портов, ФПСУ может передать управление партнеру по системе горячего резервирования. В диалоговом

поле строки укажите время, по истечении которого будет задействован резервный ФПСУ (в диапазоне от 5 до 255 секунд), или оставьте поле пустым, если такая операция не требуется.

Включить сторожевой таймер (watchdog). Этот флаг позволяет активировать автоматическую перезагрузку ФПСУ при аппаратном или программном «зависании» комплекса. При включении таймера активируется 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 должен сработать программный датчик, перегрузив ФПСУ, 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 внутреннего носителя информации, ФПСУ 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 при сбоях внутреннего накопителя информации должен прекращать свою работу – задействуйте этот флаг.

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

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

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

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

Игнорировать запрет фрагментации – флаг, работающий в VPN-туннелях между ФПСУ, и в VPN-туннелях между ФПСУ 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 при включении опции будет снижена. Если опция выключена – слишком длинный для соединения или туннеля пакет с флагом DF будет сброшен, а отправитель получит ICMP-сообщение о необходимости смены MTU.

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

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

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

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

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

Не сообщать об устаревших ключах – если данный флаг не установлен, то ФПСУ при старте выдает информационное оповещение об истечении срока действия ключей. Для отмены выдачи такого информационного оповещения следует установить флаг «Не сообщать об устаревших ключах». По умолчанию, флаг снят.

ВНИМАНИЕ! При использовании варианта исполнения «ФПСУ-IP КС3» в настройках в обязательном порядке должен быть включен режим информирования об использовании ключа при превышении срока его действия (флаг «Не сообщать об устаревших ключах» должен быть снят).

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

Гибридизировать квантовые ключи с сеансовыми – При включенном флаге квантово-защищенные ключи, получаемые от СКЗИ-Распределителя, будут смешиваться с сеансовыми ключами. Эта процедура позволяет сохранить безопасность канала в случае компрометации поступающих ключей.

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 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 будет обрабатывать эту опцию и указать это в описываемом поле.

ФПСУ предоставляет три возможных способа обработки опции SourceRoute:

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

- *передать не изменяя* пакет, оставить опцию SourceRoute без изменения.

Включение или выключение флага, отображающего выбираемый способ обработки, осуществляется клавишей <*Пробел*>.

Горячий резерв – кнопка перехода в окно настроек работы ФПСУ в подсистеме горячего резерва:

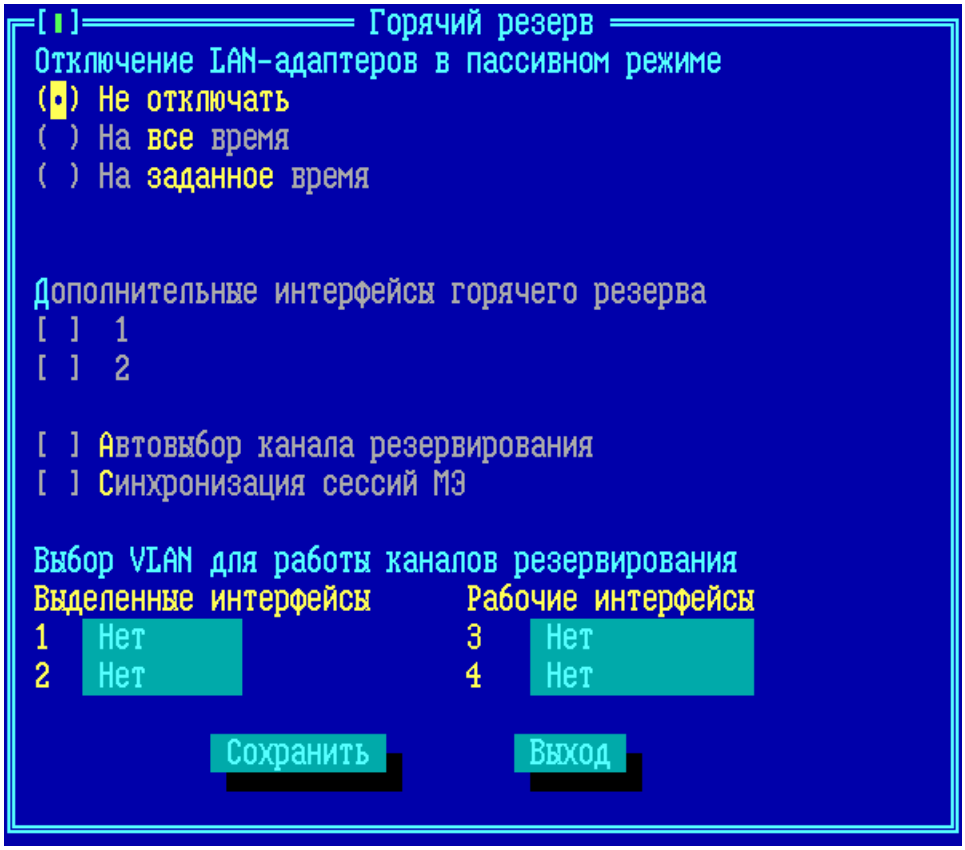


Рисунок 155 - Настройка горячего резерва

- ***Отключение LAN-адаптеров в пассивном режиме*** – опция, относящаяся к схеме горячего резервирования. Включите эту опцию, если хотите, чтобы ФПСУ 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 физическому порту коммутатора при переключении управления между основным и резервным комплексами.

- ***Дополнительные интерфейсы горячего резерва –*** флаги «[ ] 1» и «[ ] 2». Позволяют комплексу устанавливать через сетевые адаптеры, настроенные как рабочие порты, туннель с партнером горячего резерва. Без включения данной опции туннель между комплексами ФПСУ, работающими в режиме горячего резервирования, устанавливается через специально выделенные для этой цели дополнительные LAN-адаптеры. Опция не работает с включенной опцией ***Отключение LAN-адаптеров в пассивном режиме.*** Опция не работает, если для рабочего порта ФПСУ настроен работающий в режиме моста туннель (см. пункт «Описание параметров туннелей с другими ФПСУ»).

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

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

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

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

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

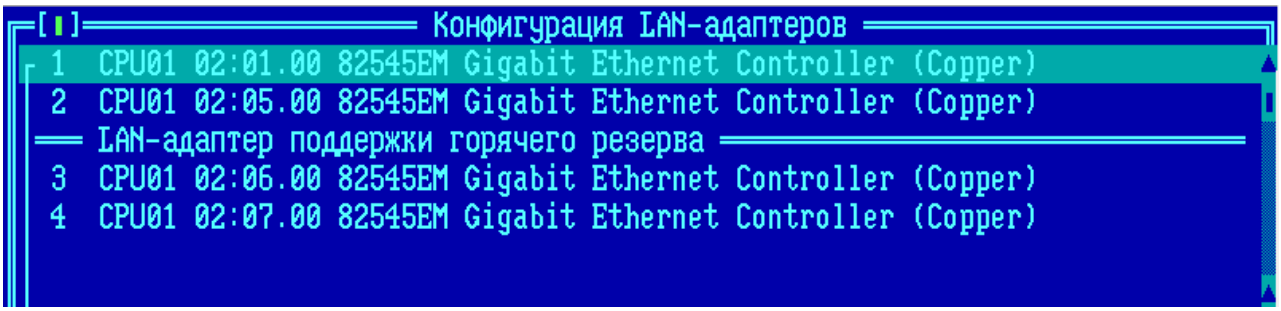


Рисунок 156 - Окно «Конфигурация LAN-адаптеров»



Рисунок 157 - Окно «Горячий резерв»

Совместимость СКЗИ – кнопка перехода в окно настроек алгоритмов шифрования СКЗИ.

ВНИМАНИЕ! Взаимодействие с совместимыми, но не сертифицированными СКЗИ равносильно отсутствию шифрования!

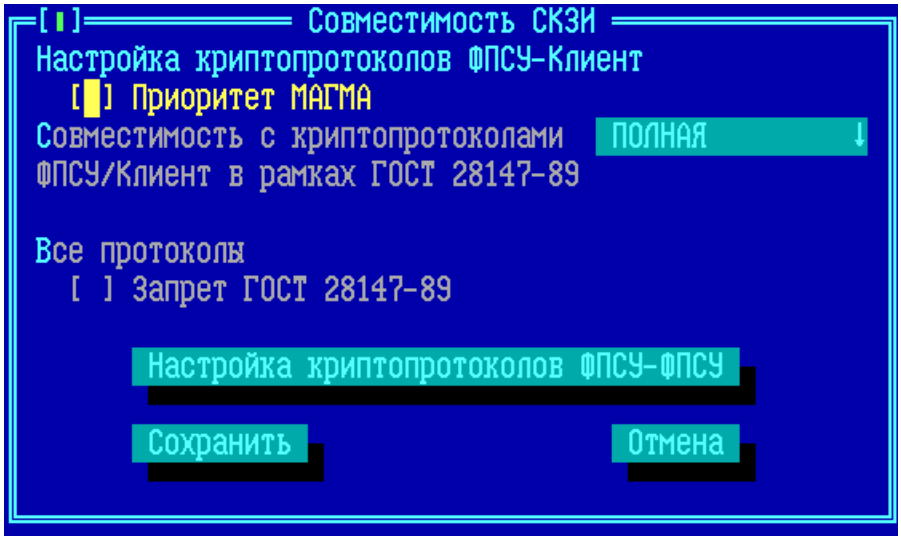


Рисунок 158 - Совместимость СКЗИ

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

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

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

КРОМЕ Тун 1 – создаются защищенные соединения с ФПСУ-IP/Клиентами, использующих СКЗИ, отличное от «Туннель/Клиент».

КРОМЕ Тун 2 – создаются защищенные соединения с ФПСУ-IP/Клиентами, использующих СКЗИ, отличное от «Туннель 2.0».

Полная – принимаются пользовательские подключения от ФПСУ-IP/Клиентов с любой версией СКЗИ.

Отключена – принимаются пользовательские подключения только от ФПСУ-IP/Клиентов, начиная с версии ПО 6.0.38 (и устройства VPN-Key с версией микрокода 7-й или выше, поддерживающей алгоритм МАГМА).

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

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

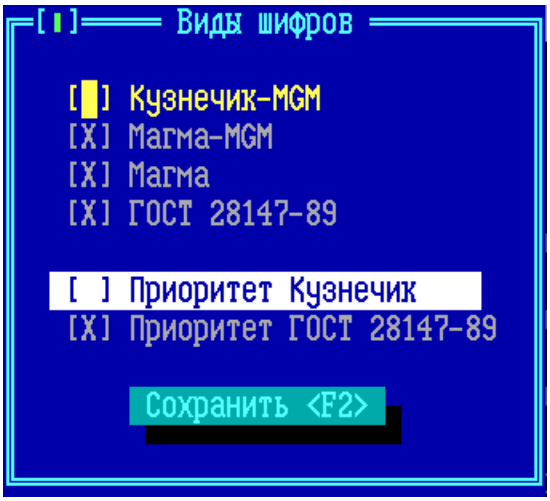


Рисунок 159 - Настройка криптопротоколов ФПСУ-ФПСУ

- ***Кузнечик-MGM*** – опция, разрешающая шифрование данных блочным шифром «Кузнечик» в режиме MGM (Multilinear Galois Mode), активируется лицензией. Если лицензия отсутствует, данная опция недоступна (отмечена белым фоном);
- ***Магма-MGM*** – опция, разрешающая шифрование данных блочным шифром «Магма» в режиме MGM, активируется лицензией. Если опция «Приоритет Кузнечик» не установлена, то работа ФПСУ будет происходить по алгоритму шифрования «Магма MGM», в случае если партнер поддерживает этот алгоритм. Если лицензия отсутствует, данная опция недоступна (отмечена белым фоном);

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

По умолчанию опции «Магма», «ГОСТ 28147-89» и «Приоритет ГОСТ» установлены. В случае, когда не установлена ни одна опция, при передаче данных применяется алгоритм шифрования ГОСТ 28147-89.

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

Запретить открытые соединения **–** кнопка, включающая режим *«Запрет открытых соединений»*, в котором вся информация, передаваемая из внутреннего порта ФПСУ на внешний порт ФПСУ (подробнее про внутренние и внешние порты см. пункт «Порты ФПСУ»), и в обратную сторону, в принудительном порядке шифруется, либо передача блокируется. После включения режима он может быть снят только повторной инсталляцией программного обеспечения ФПСУ. Для активации кнопки необходимо открыть общие параметры конфигурации ФПСУ («Конфигурация ФПСУ → Отредактировать → Общие параметры») с правами классов «*Администратор»* и «*Главный Администратор»* (см. пункт «Разграничение доступа и пользователи», Таблица 3).

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 туннелей с другими ФПСУ», или режима абонента «Ретрансляция», п.

«Описание абонента «Хост»), должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации или с объектов информатизации в защищаемой ЛВС.

Настройки на вкладке «ARP» окна «Общие параметры»:

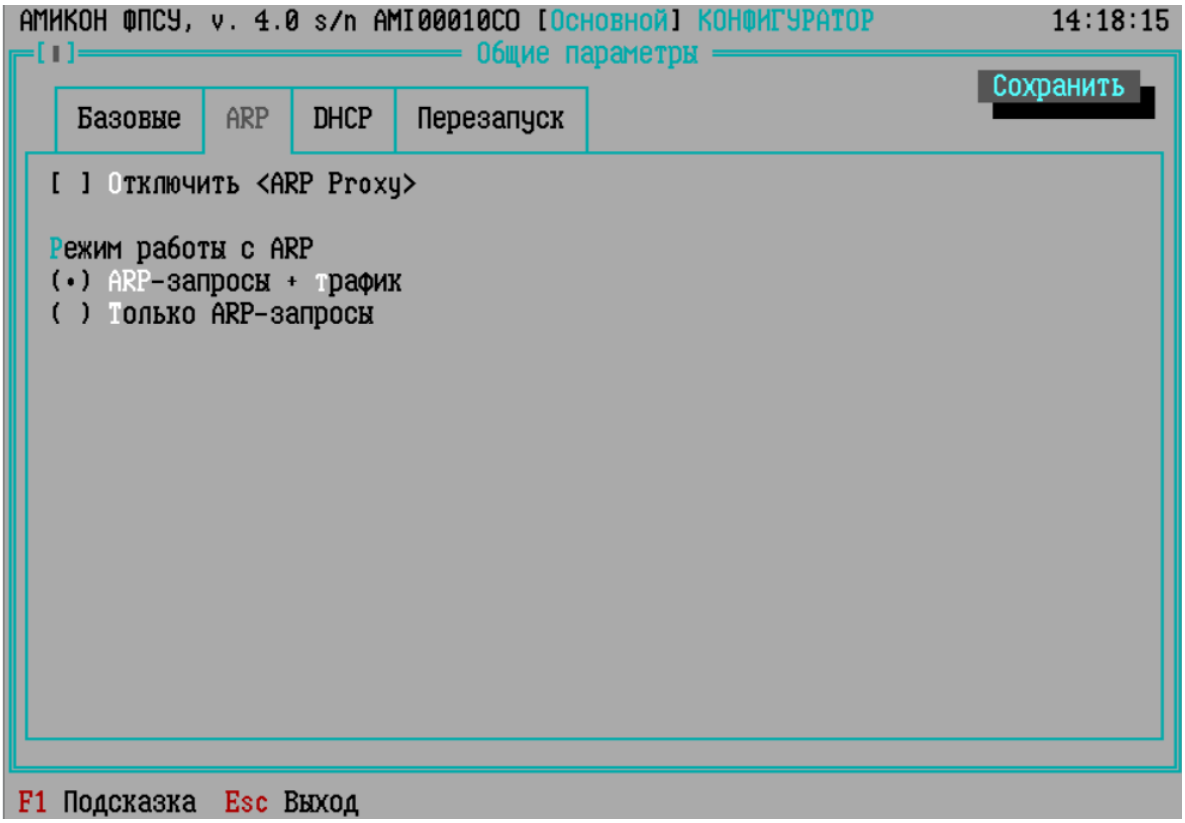


Рисунок 160 - Вкладка «ARP» окна общих параметров ФПСУ

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

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

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

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

Настройки на вкладке «DHCP» окна «Общие параметры»:

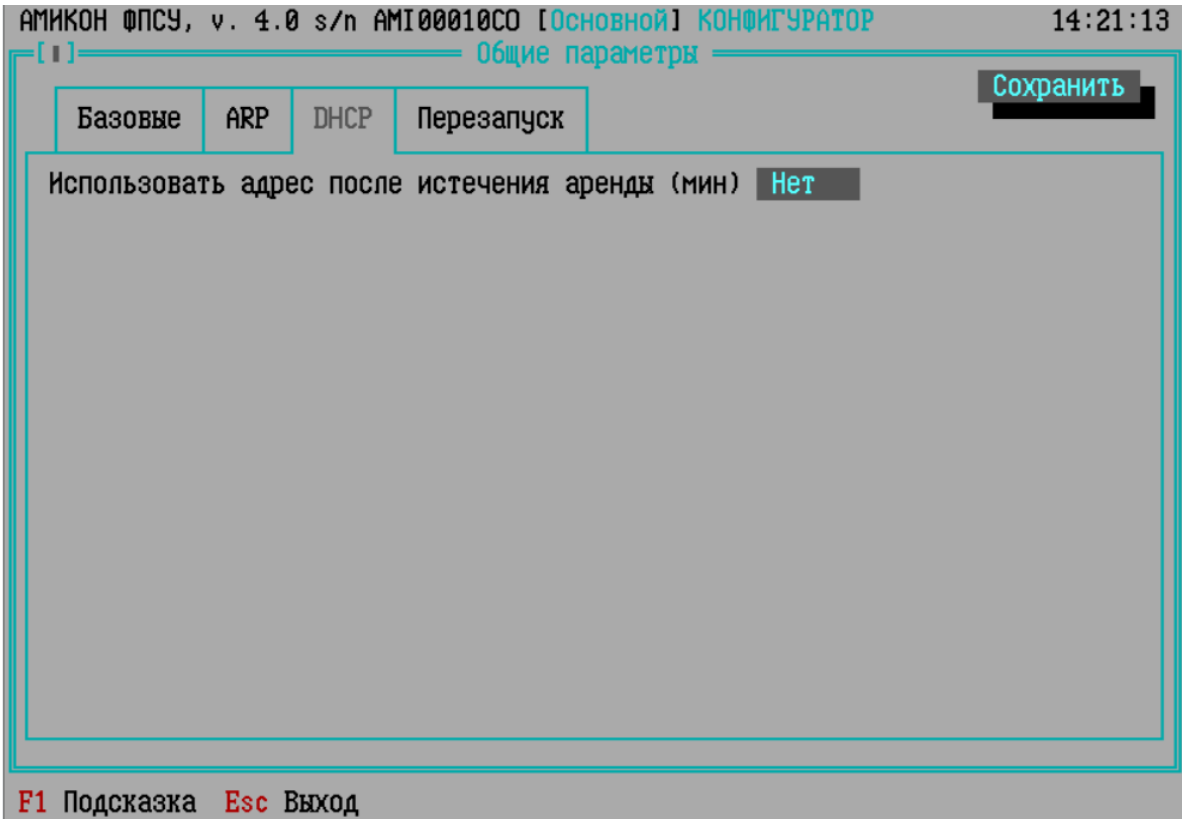


Рисунок 161 - Вкладка «DHCP» окна общих параметров ФПСУ

Использовать адрес после истечения аренды – ФПСУ может выступать в роли DHCP-клиента, в этом случае ФПСУ может запрашивать у DHCP-сервера IP-адреса для своих портов. IP-адрес для порта ФПСУ арендуется на определенное время, установленное на DHCP-сервере. По истечении срока аренды ФПСУ должен либо продлить аренду, либо перестать использовать IP-адрес. После истечения срока аренды сетевая активность на порту

прекращается (ФПСУ отправляет сообщение DHCPDISCOVER), чтобы предотвратить обрыв соединений в случае недоступности DHCP-сервера, можно установить время в минутах, в течении которого порт будет доступен по старому IP-адресу (ФПСУ продолжает отсылать сообщение DHCPREQUEST в течении этого времени для продления аренды). После истечения и этого времени ФПСУ перестанет использовать IP-адрес. Настраивая данную опцию, администратор должен быть уверен, что понимает последствия данного решения.

Настройки на вкладке «Перезапуск» окна «Общие параметры»:

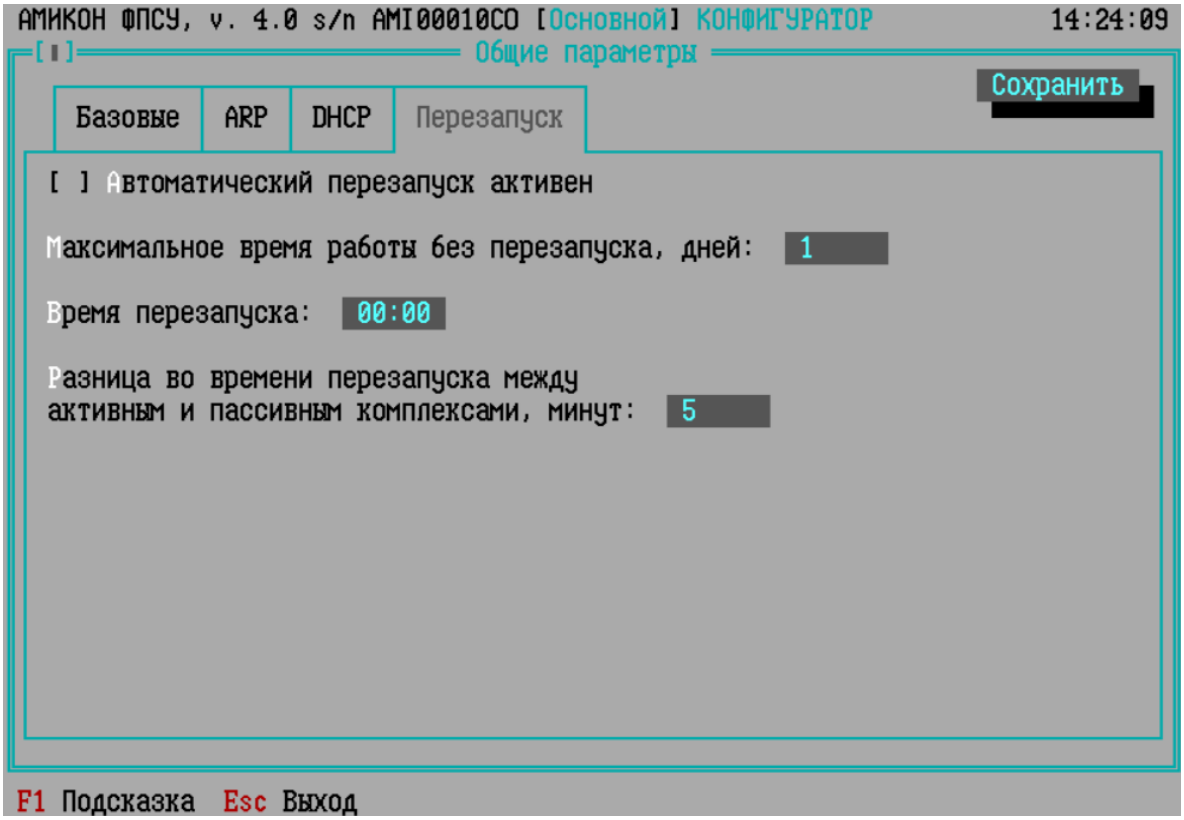


Рисунок 162 - Вкладка «Перезапуск» окна общих параметров ФПСУ

Автоматический перезапуск может быть активирован, если включен режим автозапуска на ФПСУ (подробнее о включении автозапуска см. пункт «Включение автозапуска ФПСУ»), либо при использовании специального токена, хранящего основной ключ ФПСУ на время перезапуска.

Автоматический перезапуск активен – установленный флаг включает настройки автоматического перезапуска.

Максимальное время работы без перезапуска, дней – через установленное количество дней активный ФПСУ будет автоматически перезапущен.

Время перезапуска – время перезапуска активного ФПСУ.

Разница во времени перезапуска между активным и пассивным комплексами, минут – в случае успешного перезапуска активного ФПСУ через указанный период времени будет автоматически перезапущен пассивный ФПСУ.

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

6. 2. Установка ключей

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

Команда вызывается из окна «Использование ключей» (с пустым по умолчанию списком установленных ключей парно-выборочной связи):

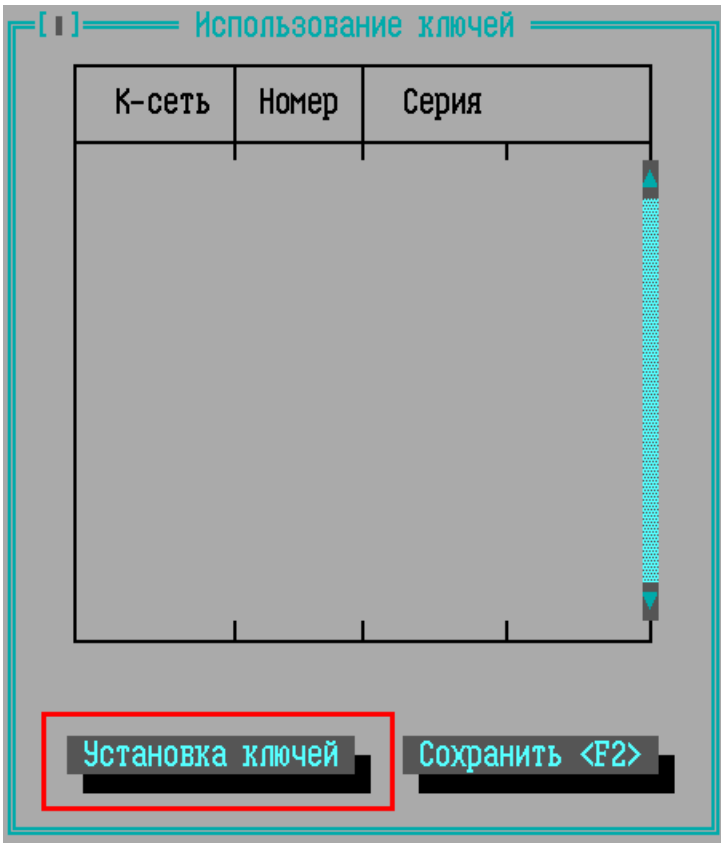


Рисунок 163 - Установка ключей из меню использования ключей

Если при выдаче данных на внешний носитель «Центром выработки ключей» транспортная копия была защищена специальным символьным паролем, при установке на ФПСУ 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).

Для выполнение процедуры установки необходимо открыть конфигурацию ФПСУ («Конфигурация ФПСУ → Отредактировать → Установка ключей»/«...→ Использование ключей») с правами классов «*Администратор*» и «*Главный Администратор*» (см. пункт «Разграничение доступа и пользователи», Таблица 3).

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

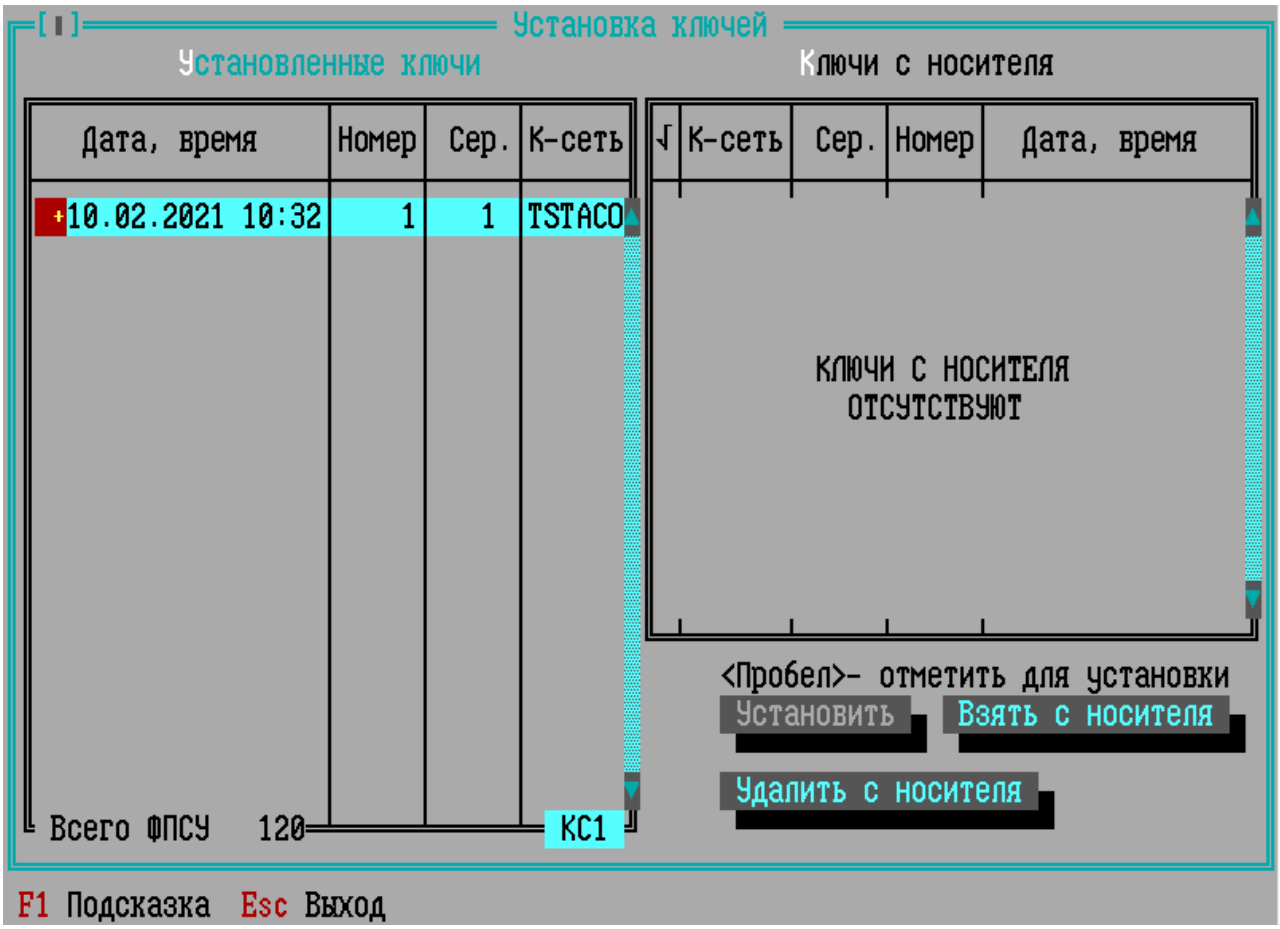


Рисунок 164 - Установка ключей

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, а К=1÷4 - номер комплекта данных с в рамках серии и номера;
- *«К-сеть»* – имя криптосети ключевых данных.
- строка *«Всего ФПСУ №№№№»* – при выборе курсором ключевых данных, внизу таблицы указывается общее количество ключей, сгенерированных ЦВК в рамках текущей серии;
- поле «*КС№»* – при выборе курсором ключевых данных, внизу таблицы указывается класс защиты согласно требованиям ФСБ к шифровальным (криптографическим) средствам, КС2 или КС3.

- состояние ключевых данных в конфигурации, перед названием криптосети:
  - «+ » – ключевые данные разрешено использовать в конфигурации ФПСУ;
  - « +» – ключевые данные разрешено использовать в конфигурации ФПСУ, и они используются для организации соединений с другими ФПСУ (см. пункт «Описание параметров туннелей с другими ФПСУ»);
  - « - » – лишние ключевые данные, которые **необходимо** удалить, прежде чем ФПСУ будет запущен в рабочий режим;
  - если никаких обозначений нет, то ключевые данные только установлены на ФПСУ, 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 носитель (USB-flash), на который записан ключ, выработанный «Центром выработки ключей», и выполните команду «*Взять с носителя»* в правой нижней части экрана. При этом в окне «Данные с носителя» появится список всех найденных на нем ключевых данных.

Выделите нужные данные курсором, отметьте их клавишей *<Пробел>* (слева от строки появится метка «√») и выполните команду «*Установить отмеченные»*. Отметить и установить на ФПСУ можно только комплекты ключевых данных одного номера для каждой криптосети. На ФПСУ можно отметить и установить два комплекта ключевых данных одной криптосети, только если у них совпадает номер, и они отличаются только серией и/или номером комплекта ключевых данных в рамках серии. Например, если на ФПСУ 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 можно поставить комплект ключевых данных «AMITST:10:5.2» (запасной комплект ключевых данных этой же серии) или «AMITST:10:6.1» (новый комплект ключевых данных новой серии), но нельзя поставить комплект ключевых данных «AMITST:9:5.1» (комплект ключевых данных с другим номером в этой же криптосети) без предварительного удаления комплекта «AMITST:10:5.1».

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

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

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

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

6. 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. Ключи парно-выборочной связи вырабатываются «Центром 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 перейдет в режим отображения установленных на ФПСУ ключевых данных и выдаст на экран монитора следующее окно:

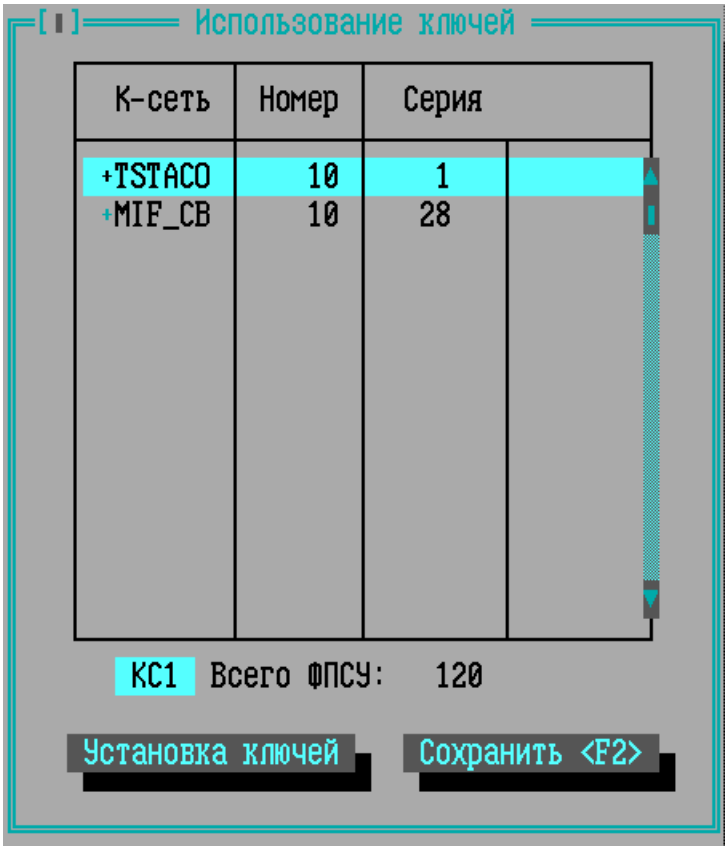


Рисунок 165 - Выбор используемых ключей

Окно содержит список криптосетей, ключи из которых установлены на ФПСУ. Каждая строка содержит информацию о ключевых данных определенной криптосети: её

символьное имя, номер установленных ключевых данных в рамках этой криптосети, серия ключевых данных и номер комплекта ключевых данных. На ФПСУ могут быть установлены не более двух комплектов ключевых данных одной криптосети, при этом номер этих комплектов должен совпадать.

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

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

Для разрешения/запрета использования ключевых данных, установите курсор на строке и нажмите клавишу <*Пробел*>. Строка будет отмечена знаком «√». Далее, при выполнении команды «*Сохранить <F2>*», состояние каждой помеченной строки будет изменено на противоположное – неразрешенные станут разрешенными и наоборот.

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

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

6. 4. Конфигурация драйверов сетевых адаптеров

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

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

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

Выбор команды «Конфигурация LAN адаптеров» главного меню открывает окно настройки сетевых адаптеров ФПСУ.

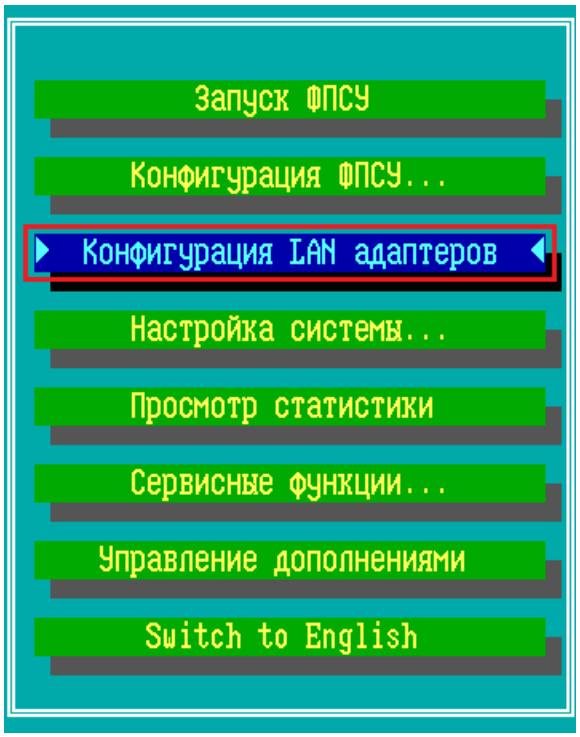


Рисунок 166 - Главное меню ФПСУ

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).

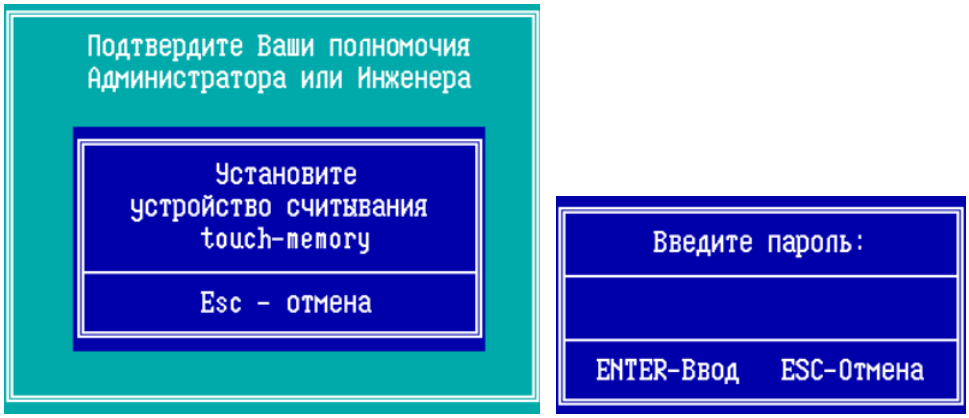


Рисунок 167 - Подтверждение полномочий и ввод пароля ТМ

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

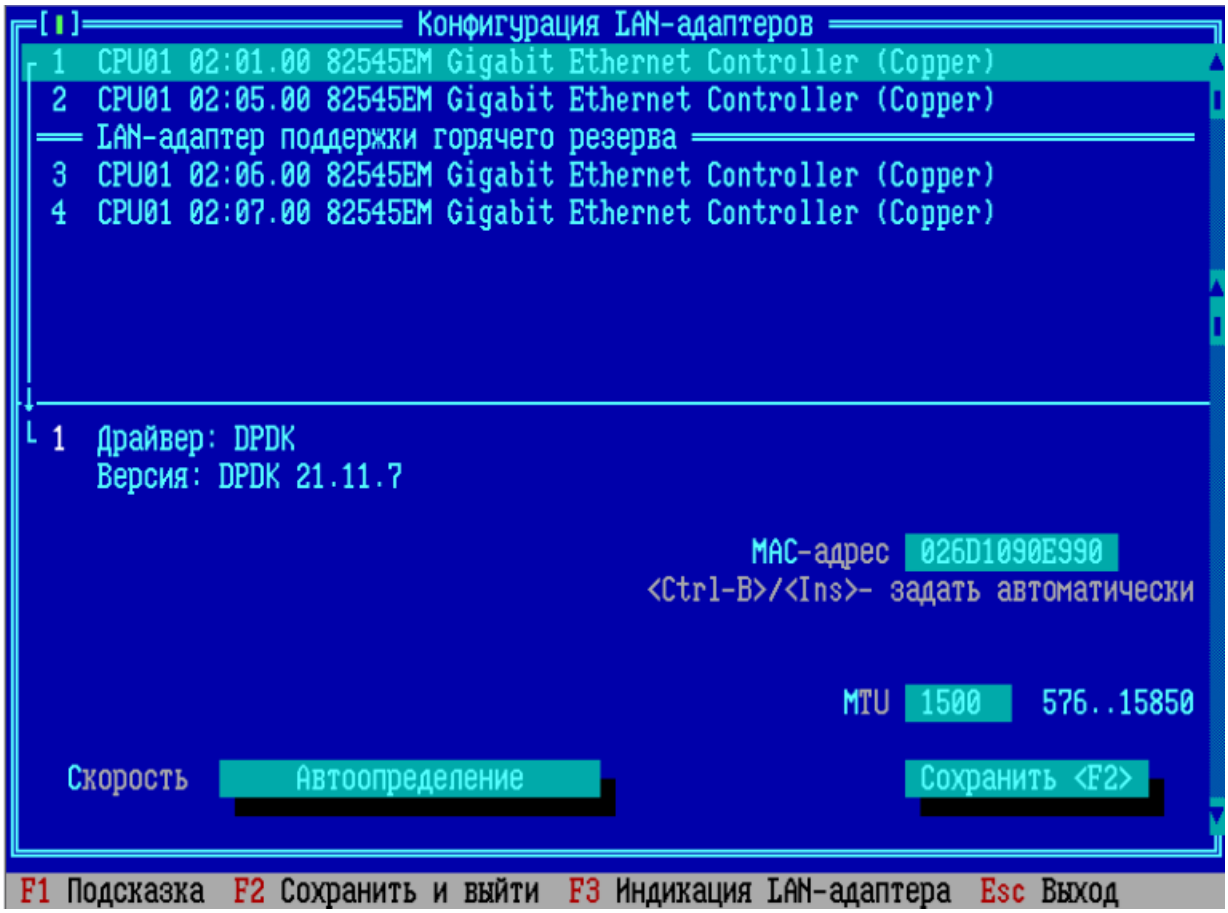


Рисунок 168 - Окно установки параметров конфигурации LAN-адаптеров

Для функционирования ФПСУ требуется установленная конфигурация сетевых адаптеров, используемых для организации рабочих портов (верхние строки после надписи «Конфигурация LAN-адаптеров»). При этом номер адаптера (номер строки) будет соответствовать номеру порта, установленному для описания локальной сети, подключаемой к ФПСУ через этот сетевой адаптер (см. раздел «Порты ФПСУ»).

В строке LAN-адаптера указан номер строки - соответствует номеру порта, приводится стандартная адресация PCI устройства - [domain:]bus:device.function, где domain - процессор материнской платы, к которому подключен LAN-адаптер, bus и device - номер шины и номер слота на материнской плате, к которым подключен LAN-адаптер, function «00» означает все функции устройства.

Строки после надписи «LAN-адаптер поддержки горячего резерва», 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 на рисунке). Чтобы настроить запасной LAN-адаптер поддержки горячего резерва, следует установить курсор на строку №3 и нажать клавишу <*Ins*>.

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

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



Рисунок 169 - 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.

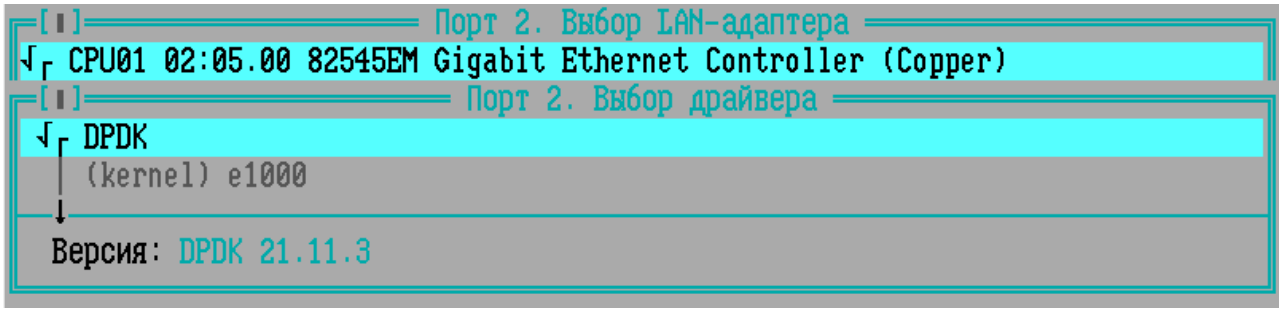


Рисунок 170 - Выбор драйвера для сетевого адаптера

ВНИМАНИЕ! Подсистема http-прокси (см. пункт «Http-proxy ФПСУ») и подсистема поддержки квантового распределения ключей (см. пункт «Квантовое распределение ключей») 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 подтвердить или изменить предустановленные значения двух параметров: «Скорость» и «MAC-адрес».

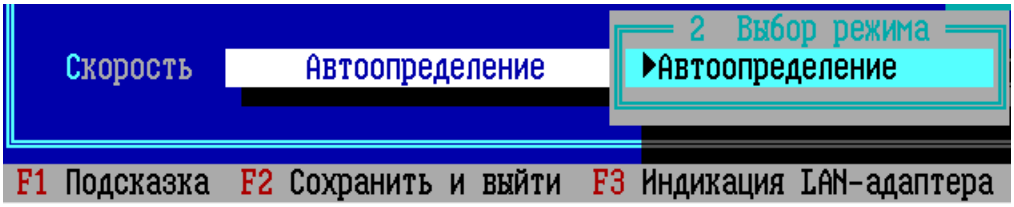


Рисунок 171 - Выбор режима работы адаптера

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

Для установки MAC-адреса выделите его поле курсором и наберите с клавиатуры желаемое значение. Если драйвер адаптера позволяет, ФПСУ 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.

ВНИМАНИЕ! Выполнение команды «**задать автоматически**» MAC-адреса обязательно для организации работы горячего резерва: это обеспечивает идентичность аппаратных адресов для основного и резервного ФПСУ.

ВНИМАНИЕ! Выполнение команды «**задать автоматически»** для MAC-адреса следует выполнять ПОСЛЕ установления на ФПСУ обновления с серийным номером!

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

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

ВНИМАНИЕ! Если на выбранном сетевом адаптере будет организован туннель типа «мост» к другому ФПСУ (подробнее см. Режим «Мост» между ФПСУ (L2-шифрование)), то рекомендуется изменить MTU, установив его в значение на 100 меньше чем MTU для остальных сетевых адаптеров данного ФПСУ. Это позволит избежать потерей в производительности ФПСУ по причине дефрагментации/фрагментации пакетов.

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

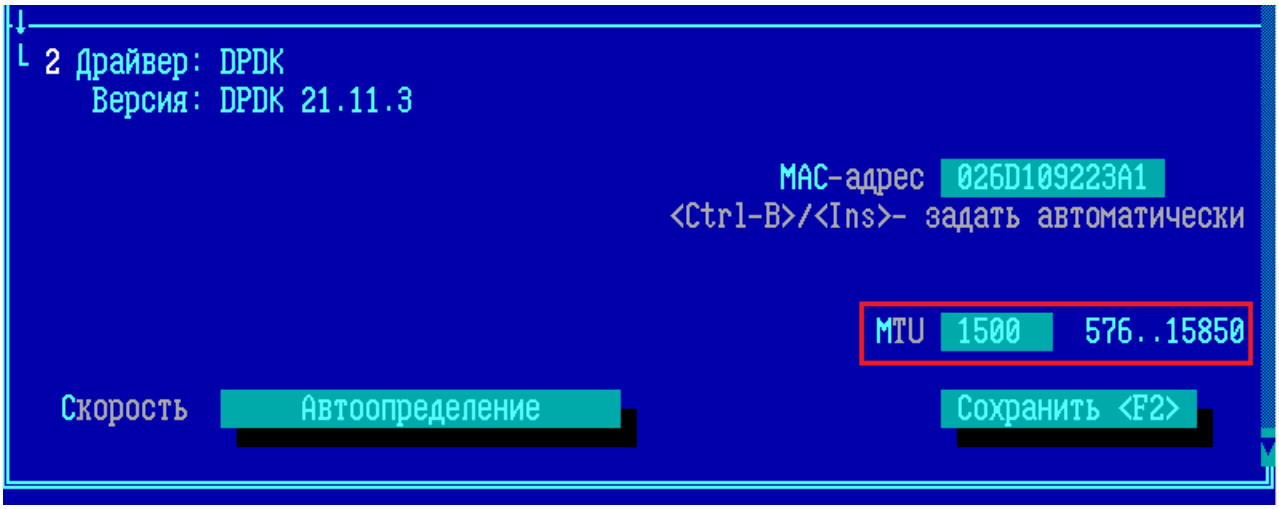


Рисунок 172 - Изменение параметра MTU сетевого адаптера с DPDK драйвером

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

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

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

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

6. 4. 1. Агрегированный сетевой адаптер

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

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

Выберите LAN-адаптер в состоянии «LAN-адаптер не выбран», по нажатию клавиши <*Enter*> или <*Пробел*> на экран будет выдано окно выбора сетевых адаптеров. Выделите курсором строку с типом сетевого адаптера «Виртуальный Link Aggregation», назначаемого для агрегированного сетевого адаптера ФПСУ и нажмите <*Enter*>.

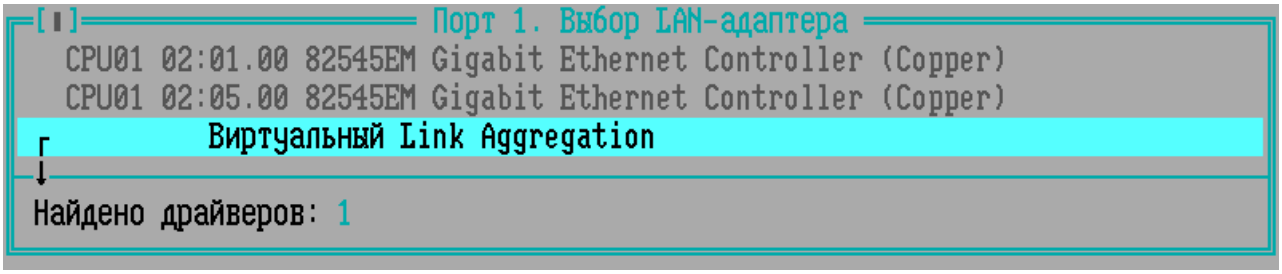


Рисунок 173 - Выбор сетевого адаптера для порта

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

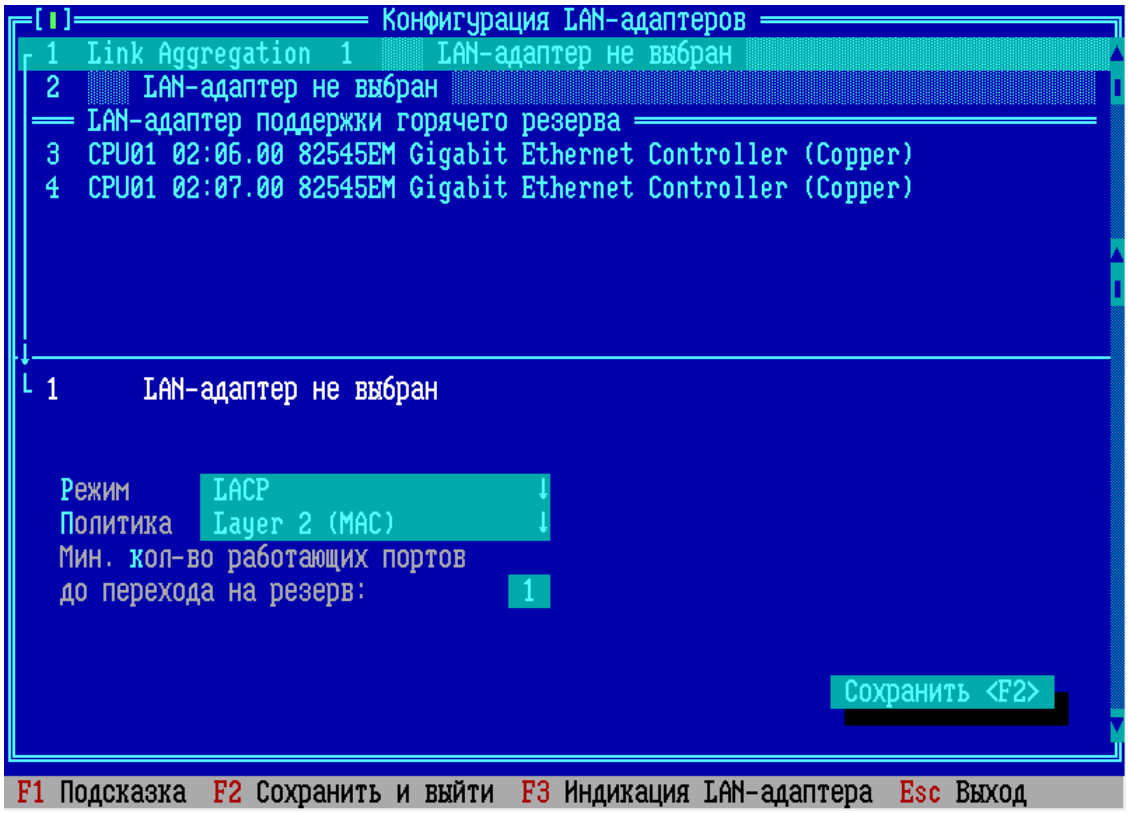


Рисунок 174 - Агрегированный сетевой адаптер

Агрегированный сетевой адаптер может быть задан только для рабочих сетевых адаптеров, не используется для сетевых адаптеров «горячего» резерва. Агрегированный сетевой адаптер конфигурируется минимум двумя LAN-адаптерами, может объединять до 4 LAN-адаптеров.

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

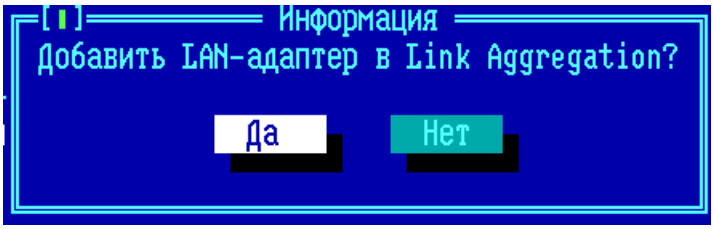


Рисунок 175 - Добавление LAN-адаптера

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

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

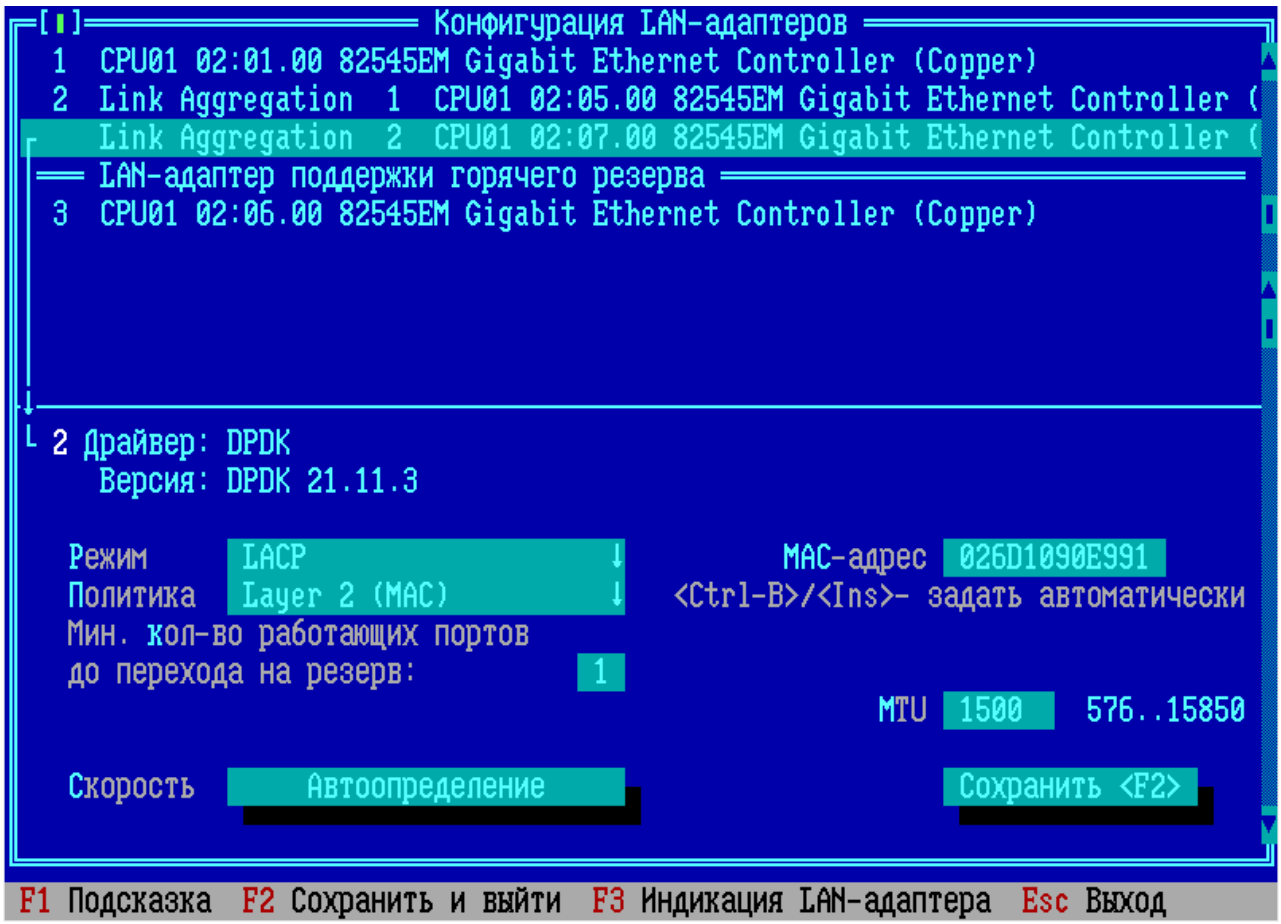


Рисунок 176 - Агрегированный сетевой адаптер, второй LAN-адаптер

Для агрегированного сетевого адаптера рекомендуется использовать LAN-адаптеры:

- одинаковых моделей и типов;
- расположенные на одном ЦПУ;
- с идентичными настройками скорости, дуплекса, VLAN, типа порта.

Для сетевого адаптера необходимо задать следующие параметры:

Режим - режимы работы агрегированного сетевого адаптера:
Active Backup - режим, при котором активен только один порт, если он выходит из

строя, оборудование переключается на другой работающий. Обеспечивается отказоустойчивость без увеличения скорости.

Balance XOR - режим, при котором активны несколько портов, исходящие пакеты распределяются по нескольким линиям исходя из Политики (см. ниже). Обеспечивается балансировка нагрузки при передаче пакетов и отказоустойчивость.

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

Политика определяет способ распределения пакетов по линиям для режимов «Balance XOR» и «LACP»:

L2 - балансировка на основе MAC-адреса отправителя;

L2-L3 - балансировка на основе MAC-адреса и IP адреса отправителя или получателя;

L3-L4 - балансировка на основе IP-адреса и TCP/UDP порта отправителя или получателя.

Минимальное количество работающих портов до перехода на резерв - значение ограничено от 1 до числа LAN-адаптеров, объединенных в агрегированный адаптер, с учетом ограничений аппаратной платформы. Управление ФПСУ передается «горячему» резерву, в случае если количество работающих портов меньше указанного.

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

7. Настройка системы

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

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

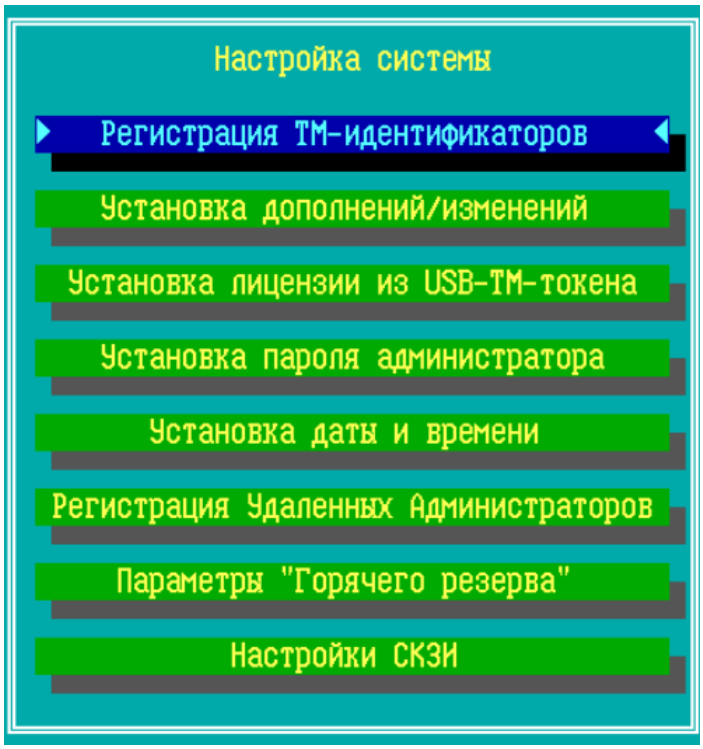


Рисунок 177 - Меню «Настройка системы»

7. 1. Окно регистрации ТМ

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

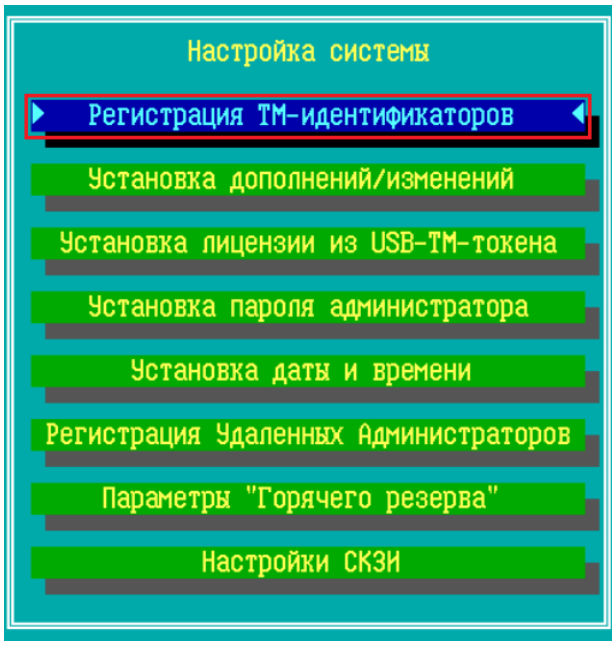


Рисунок 178 - Выбор пункта «Регистрация ТМ-идентификаторов»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 179 - Подтверждение полномочий и ввод пароля ТМ

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

- регистрация ТМ-идентификаторов новых локальных администраторов ФПСУ;
- управление паролями для учетных записей локальных администраторов ФПСУ;
- 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 (см. пункты

«Включение автозапуска ФПСУ» и «Отключение автозапуска»).

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

ВНИМАНИЕ! Ячейке таблицы [пусто] «Администратор» - «Основная ТМ» соответствует пользователь класса «*Главный администратор*». Ячейке таблицы [пусто] «Администратор» - «Запасная ТМ» соответствует пользователь класса «*Администратор*». Ячейкам таблицы строки «Инженер» соответствуют пользователи класса «*Инженер*». Ячейкам таблицы строк «Оператор 1», «Оператор 2», «Оператор 3» и «Оператор 4» соответствуют пользователи класса «*Оператор*».

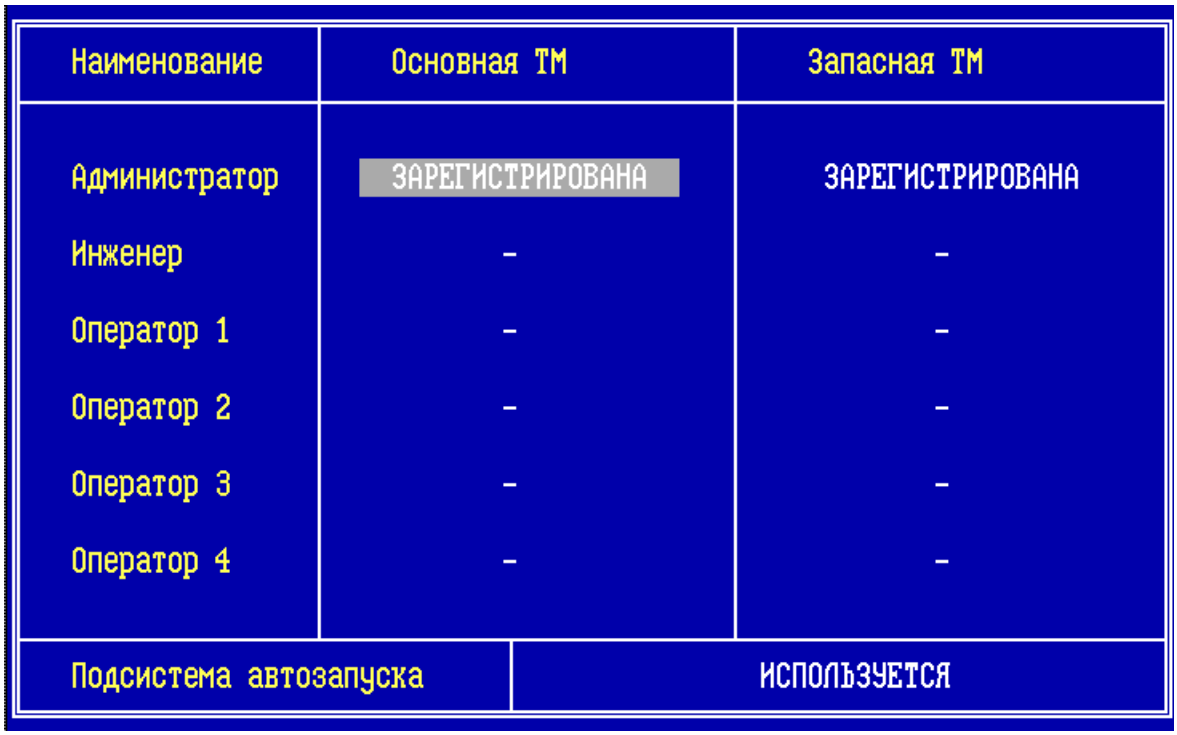


Рисунок 180 - Окно управления ТМ-идентификаторами ФПСУ

Для зарегистрированных ТМ-идентификаторов могут быть осуществлены следующие операции:

- «Основной» ТМ-идентификатор строки «Администратор» закреплен за администратором класса «Главный администратор», может быть только проверен;
- остальные ТМ-идентификаторы могут быть проверены, очищены или повторно зарегистрированы с новой ключевой информацией;
- для каждого ТМ-идентификатора может быть задан пароль.

Новый ТМ-идентификатор может быть только зарегистрирован как «запасная ТМ» для строки «Администратор», или «основная ТМ»/«запасная ТМ» для любого другого

наименования пользователей. ***Основной ТМ-идентификатор администратора зарегистрирован быть не может, он перерегистрируется только при повторной инсталляции или переходе ФПСУ из технологического в рабочий режим, и только на ТМ-идентификатор, поставляемый вместе с дистрибутивом ФПСУ и маркированный как ТМ-идентификатор Главного администратора.***

ВНИМАНИЕ! На ФПСУ должны быть зарегистрированы минимум два ТМ-идентификатора, один из которых ТМ Главного администратора, иначе при закрытии окна регистрации ТМ-идентификаторов оно будет открываться снова, блокируя дальнейшую работу.

ВНИМАНИЕ! Требование установки пароля для каждого ТМ-идентификатора является обязательным для ФПСУ классов КС2 и КС3, и опциональным для ФПСУ класса КС1.

Пароль Главного администратора задается в окне регистрации ТМ (подробнее см. пункт «Установка пароля Главного администратора»), пароль для других классов администраторов задается при первоначальной или повторной регистрации их ТМ-идентификаторов.

Примечание. Не используемый ТМ-идентификатор любого класса пользователей ФПСУ, кроме ТМ Главного администратора, может быть перерегистрирован с тем же классом пользователей или с любым другим классом пользователей, кроме Главного администратора. В любом случае ключевая информация удаляется и записываются новые ключевые данные на ТМ.

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

Внесенные в настройки изменения сохраняются автоматически.

При выполнении операций по регистрации, проверке или очистке ТМ система будет требовать подтверждения полномочий администратора посредством подключения ТМ-идентификатора к USB-порту ФПСУ с целью предотвращения несанкционированных действий.

При выборе зарегистрированного ТМ-идентификатора и нажатии клавиши <*Enter*>, подключенный ТМ-идентификатор отображается в меню регистрации ТМ-идентификаторов как «Правильный». На рисунке ниже слева выбран основной ТМ-идентификатор администратора, по нажатию клавиши <*Enter*> отображается результат проверки - «Правильный», этот ТМ-идентификатор подключен к ФПСУ. На рисунке ниже справа

выбран запасной ТМ-идентификатор администратора, по нажатию клавиши *<Enter>* отображается результат проверки - «Неправильный», этот ТМ-идентификатор не подключен к ФПСУ.

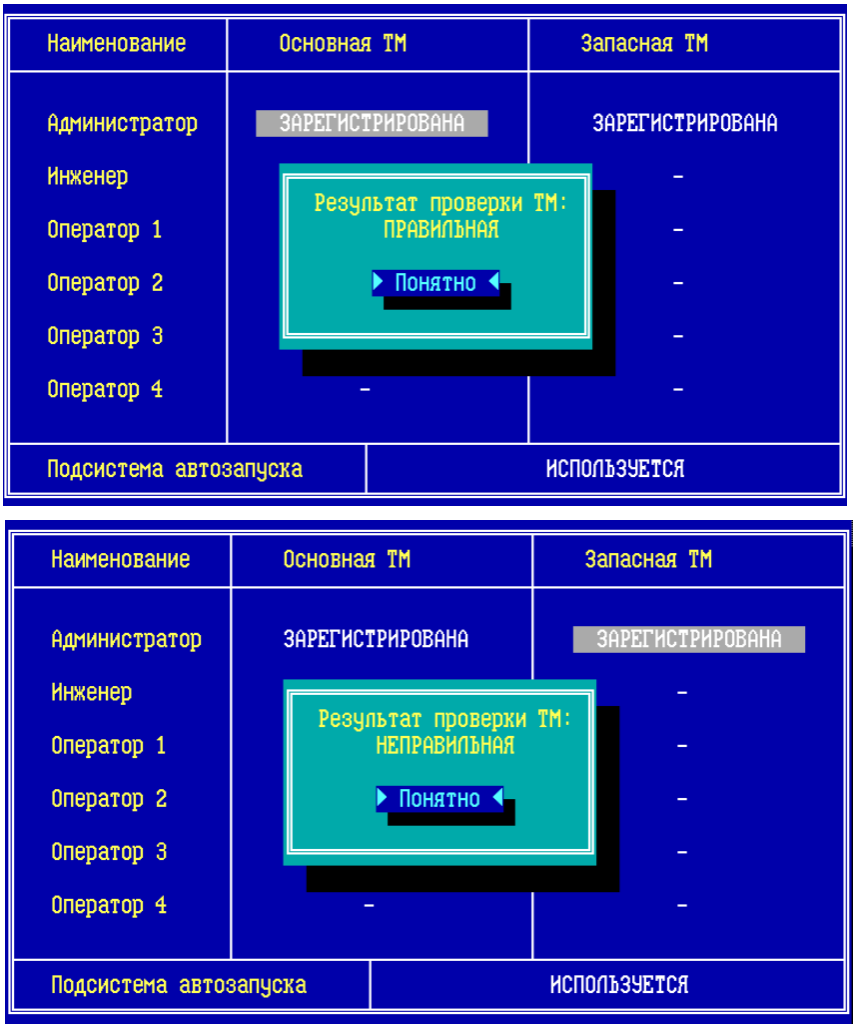


Рисунок 181 - Проверка подключенного ТМ-идентификатора администратора

Выход из окна регистрации ТМ с возвратом в меню «Настройки системы» ФПСУ осуществляется по сочетанию клавиш *<ALT>+<X>*.

7. 1. 1. Установка пароля Главного администратора

Пароли администраторов ФПСУ всех классов (см. пункт Разграничение доступа и пользователи) устанавливаются/изменяются в окне регистрации ТМ. Операция доступна администраторам класса *Администратор* и выше.

Для установки пароля Главного администратора: выделите ячейку *Администратор-Основная ТМ* и нажмите клавишу *<Ins>*, на экране отобразится запрос на задание/изменение

пароля основного ТМ. Нажмите «Да» для задания пароля:

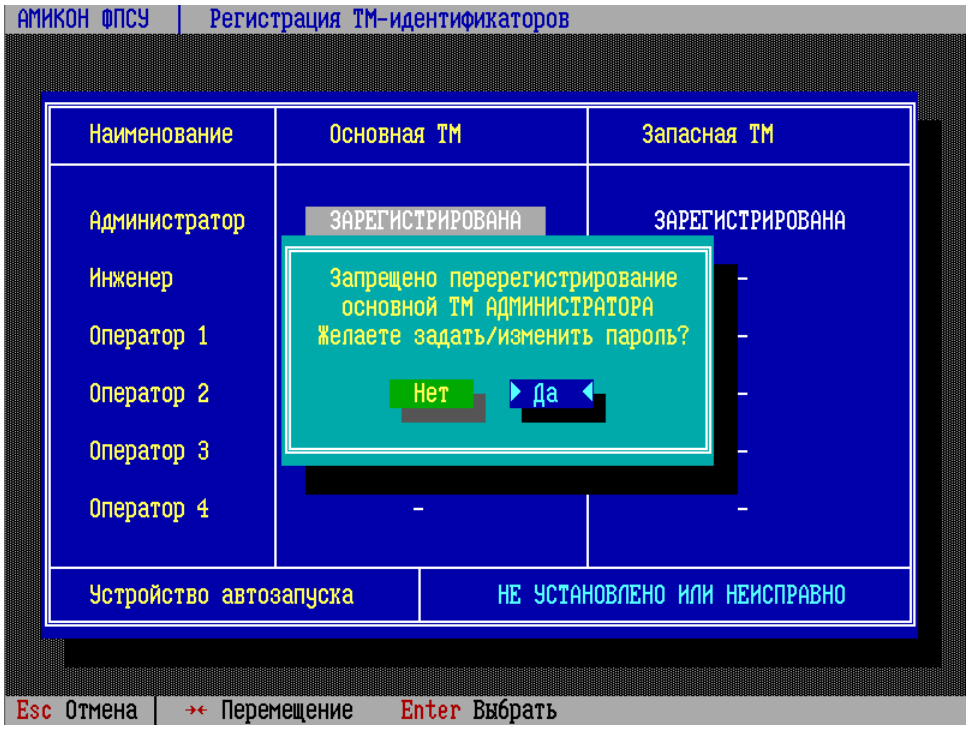


Рисунок 182 - Установка/изменение пароля ТМ

При подтверждении запроса откроется окно ввода пароля.

Длина пароля от 6 до 16 символов. Диапазон разрешённых символов заглавные и строчные латинские буквы, цифры, спецсимволы - коды 33-126 по таблице ASCII (! # $ % & ' ( ) * + , - . / 0-9 : ; < = > ? @ A-Z [\ ] ^ _ ` a-z { | } ~).

Поскольку вводимые символы не отображаются на экране, будет предложено ввести пароль еще раз с целью исключения возможной ошибки. Установка пароля 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.

ВНИМАНИЕ! Если администратор забыл пароль своего ТМ-идентификатора, то для восстановления доступа потребуется предъявить полномочия Главного Администратора, чтобы задать новый пароль. Если забыт пароль ТМ-идентификатора Главного Администратора, для восстановления доступа Главного Администратора к ФПСУ потребуется повторная установка ФПСУ с дистрибутива.

Необходимо ввести пароль и подтвердить ввод по нажатию клавиши <Enter>. В

открывшемся окне повторно ввести пароль и нажать клавишу <Enter>.



Рисунок 183 - Ввод пароля ТМ

Администратор может отменить установку пароля. Для этого он должен выбрать ту же команду, оставить поле пустым (не вводить символы) и нажать <Enter>.

Пароль Главного администратора (основного ТМ класса администратор) установлен.

7. 1. 2. Повторная регистрация ТМ-идентификатора

Повторная регистрация ТМ-идентификатора любого пользователя, кроме Главного администратора, проводится в окне Регистрации ТМ. Процедура повторной регистрации выполняется в случаях плановой замены ключевой информации ТМ-идентификатора или при компрометации ТМ-идентификатора.

Для выполнения необходимо предъявить ТМ-идентификатор класса Администратор, а также регистрируемый ТМ-идентификатор выбранного класса.

Уточнение: при регистрации запасного ТМ-идентификатора администратора требуется ТМ Главного администратора для подтверждения права регистрации и запасной ТМ для регистрации.

Для повторной регистрации ТМ-идентификатора выделите ячейку таблицы администраторов ФПСУ, соответствующую учетной записи администратора, чей ТМ-идентификатор повторно регистрируется. Нажмите клавишу <*Ins*> для старта процедуры повторной регистрации. На экране отобразится запрос с подтверждением необходимости повторной регистрации ТМ-идентификатора:

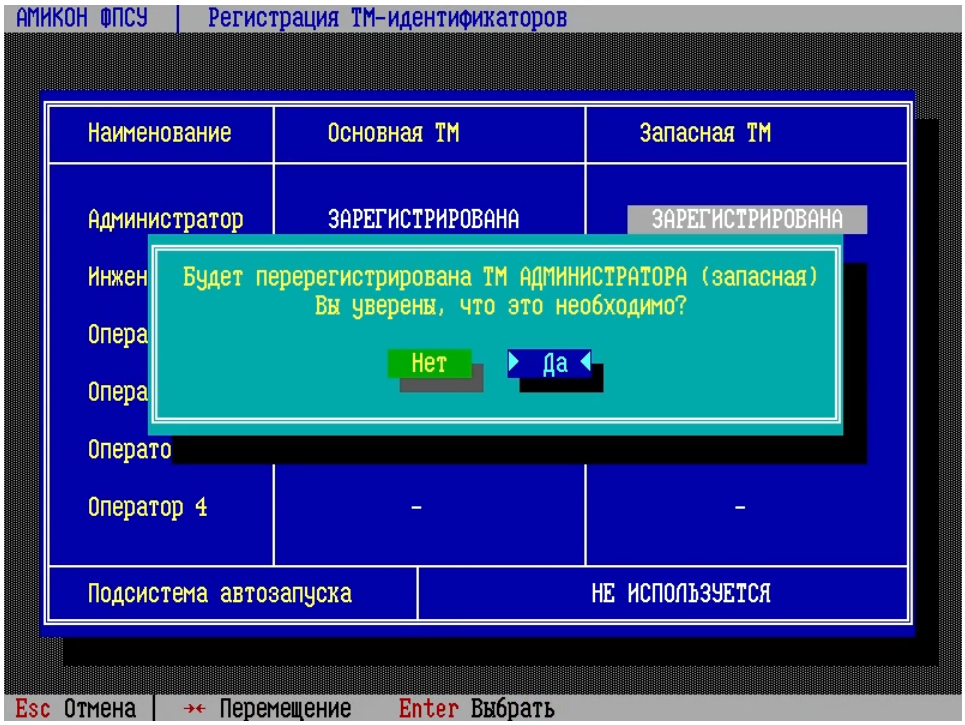


Рисунок 184 - Перерегистрация ТМ

Нажмите «Да» для продолжения или «Нет» для отказа от процедуры.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 185 - Подтверждение полномочий и ввод пароля ТМ

Затем необходимо убрать ТМ-идентификатор подтвердившего операцию администратора и предъявить повторно регистрируемый ТМ-идентификатор.

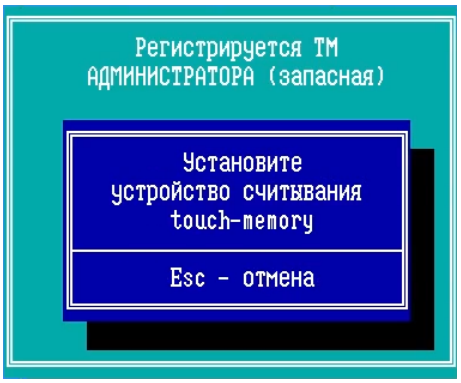


Рисунок 186 - Предъявление ТМ для регистрации

После того, как система обнаружит подлежащий повторной регистрации ТМ-идентификатор, будет предложено установить пароль для соответствующей обнаруженному ТМ-идентификатору учетной записи выбранного класса.

ВНИМАНИЕ! Требование установки пароля для каждого ТМ-идентификатора является обязательным для ФПСУ классов КС2 и КС3, и опциональным для ФПСУ класса КС1.

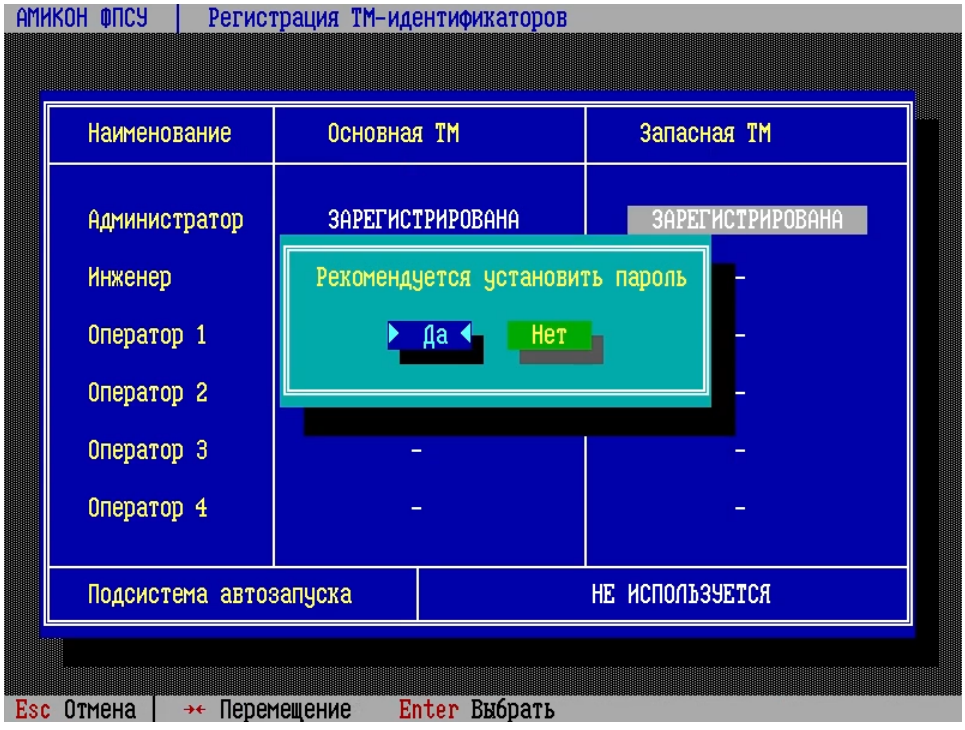


Рисунок 187 - ТМ перерегистрирован

При подтверждении запроса откроется окно ввода пароля.

Длина пароля от 6 до 16 символов. Диапазон разрешённых символов заглавные и строчные латинские буквы, цифры, спецсимволы - коды 33-126 по таблице ASCII (! # $ % & ' ( ) * + , - . / 0-9 : ; < = > ? @ A-Z [\ ] ^ _ ` a-z { | } ~).

Поскольку вводимые символы не отображаются на экране, будет предложено ввести пароль еще раз с целью исключения возможной ошибки. Установка пароля 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.

ВНИМАНИЕ! Если администратор забыл пароль своего ТМ-идентификатора, то для восстановления доступа потребуется предъявить полномочия Главного Администратора, чтобы задать новый пароль. Если забыт пароль ТМ-идентификатора Главного Администратора, для восстановления доступа Главного Администратора к ФПСУ потребуется повторная установка ФПСУ с дистрибутива.

Необходимо ввести пароль и подтвердить ввод по нажатию клавиши <Enter>. В открывшемся окне повторно ввести пароль и нажать клавишу <Enter>.



Рисунок 188 - Ввод пароля ТМ

Администратор может отменить установку пароля. Для этого он должен выбрать ту же команду, оставить поле пустым (не вводить символы) и нажать <Enter>.

В случае если ТМ-идентификатор в процессе ввода пароля был отключен, необходимо повторно предъявить его для добавления пароля к учетной записи.



Рисунок 189 - Предъявление запасного ТМ

После подключения запасной ТМ-идентификатор зарегистрирован с установлением пароля.

7. 1. 3. Удаление ТМ

При удалении записанной на потерявшем актуальность или скомпрометированном ТМ-идентификаторе ключевой информации, требуется предъявить ТМ администратора и ТМ-идентификатор, который очищается, чтобы провести удаление ключевых данных. При выполнении операции по очистке ключевых данных ТМ-идентификатора система будет требовать подтверждения полномочий администратора с целью предотвращения несанкционированных действий.

Отказаться от операции удаления ТМ можно, нажав клавишу <Esc>.

Для удаления перейдите в соответствующее ТМ-идентификатору поле таблицы, например ТМ инженера, и нажмите клавишу <*Delete*>. На экране отобразится запрос:

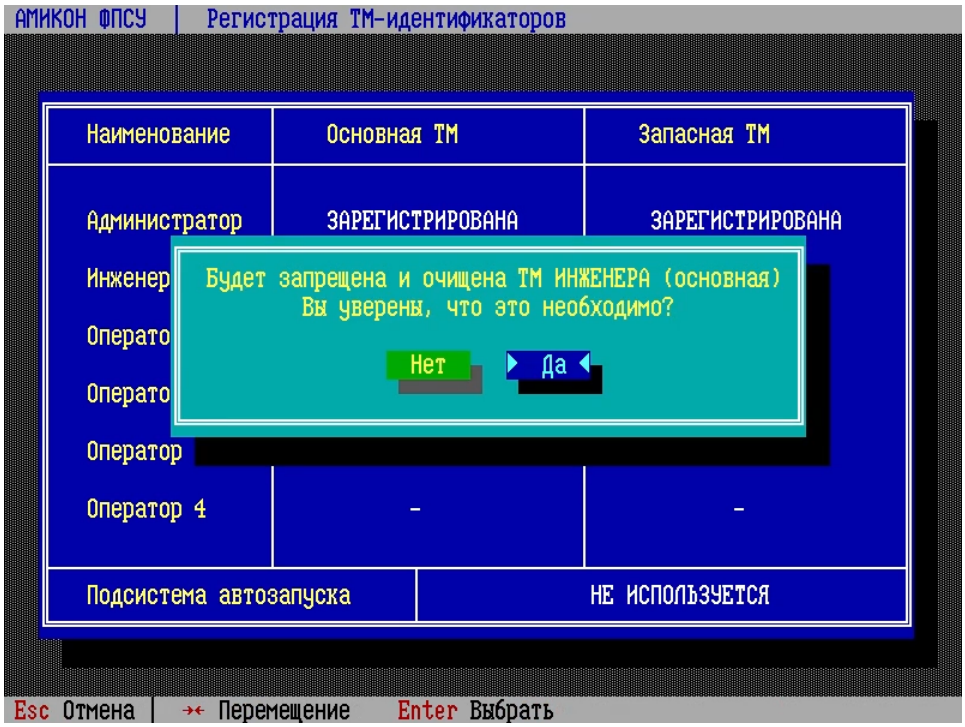


Рисунок 190 - Удаление ТМ

По нажатию кнопки «Да» будет запущен процесс удаления ТМ.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 191 - Подтверждение полномочий и ввод пароля ТМ

Затем необходимо убрать ТМ-идентификатор администратора и предъявить ТМ-идентификатор инженера для его удаления. При этом соответствующий ТМ-идентификатору ключ запуска будет удален с ФПСУ.

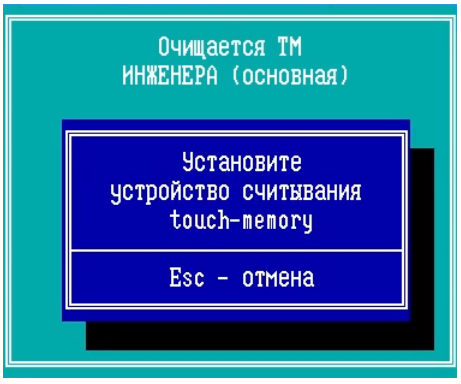


Рисунок 192 - Предъявление ТМ инженера для удаления

ТМ-идентификатор инженера удален.

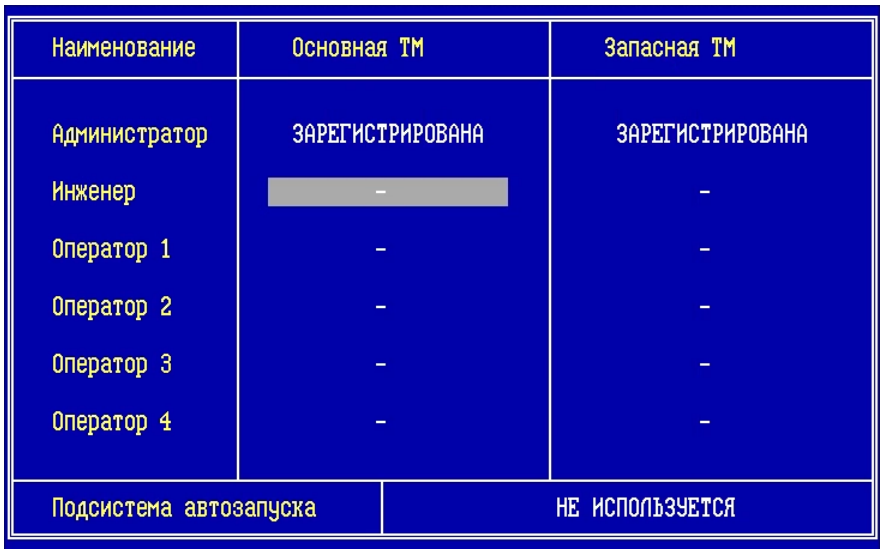


Рисунок 193 - Окно регистрации ТМ

7. 2. Включение автозапуска ФПСУ

Включение автозапуска доступно из окна, открываемого по команде «Регистрация ТМ-идентификаторов» меню «Настройки системы» ФПСУ.

Подсистема автозапуска на ФПСУ по умолчанию выключена.

При включении электропитания ФПСУ с активированной подсистемой автозапуска, ФПСУ после загрузки операционной системы будет переведен в режим фильтрации пакетов так, как если бы эту команду выполнил пользователь с правами учетной записи «*Оператор*».

При работе ФПСУ с активированной подсистемой автозапуска, команда «Запуск ФПСУ» выполняется без предъявления ТМ-идентификатора и пароля, с использованием ключа запуска, хранящего на внутреннем носителе ФПСУ (подробнее см. пункт «Запуск ФПСУ»).

Если подсистема автозапуска не включена, её статус в строке состояния отображается как «НЕ ИСПОЛЬЗУЕТСЯ».

ВНИМАНИЕ! В случае, когда на ФПСУ установлено аппаратное устройство автозапуска (см. пункт «Инициализация HW аппаратного устройства автозапуска»), включение программной подсистемы автозапуска отменит автозапуск с аппаратного устройства. Вернуть автозапуск с аппаратного устройства станет возможным только после переустановки программного обеспечения ФПСУ!

Для включения подсистемы автозапуска, в окне управления ТМ-идентификаторами ФПСУ перейдите в поле «Подсистема автозапуска» и нажмите клавишу <*Insert*>:

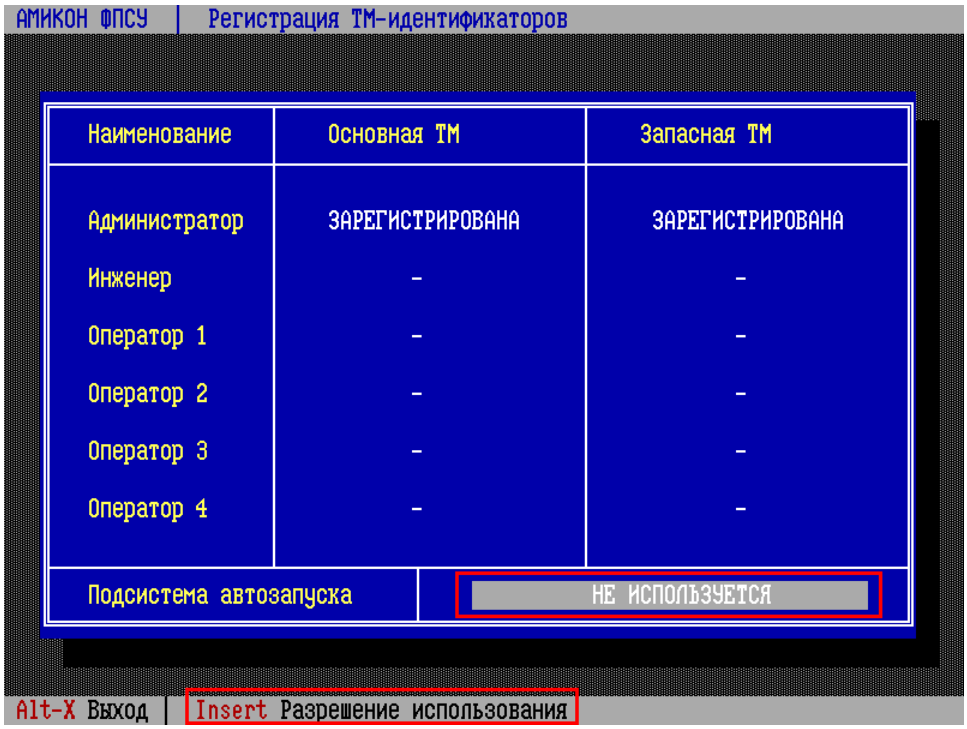


Рисунок 194 - Окно управления ТМ-идентификаторами ФПСУ

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 195 - Подтверждение полномочий и ввод пароля ТМ

Подтвердите в появившемся окне выполнение включения режима автозапуска.

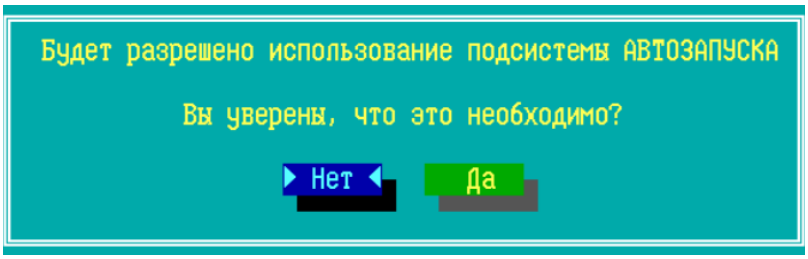


Рисунок 196 - Запрос на включение автозапуска

В случае подтверждения выполнения команды, подсистема автозапуска будет включена, её статус изменится на состояние «ИСПОЛЬЗУЕТСЯ».

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

Внесенные в настройки изменения сохраняются автоматически.

Выход из окна регистрации ТМ с возвратом в меню «Настройки системы» ФПСУ осуществляется по сочетанию клавиш *<ALT>+<X>*.

7. 3. Установка дополнений/изменений

Опция «Установка дополнений/изменений» меню «Настройка системы» предназначена для установки новых программных модулей, опциональных подсистем, или обновлений существующих модулей ФПСУ.

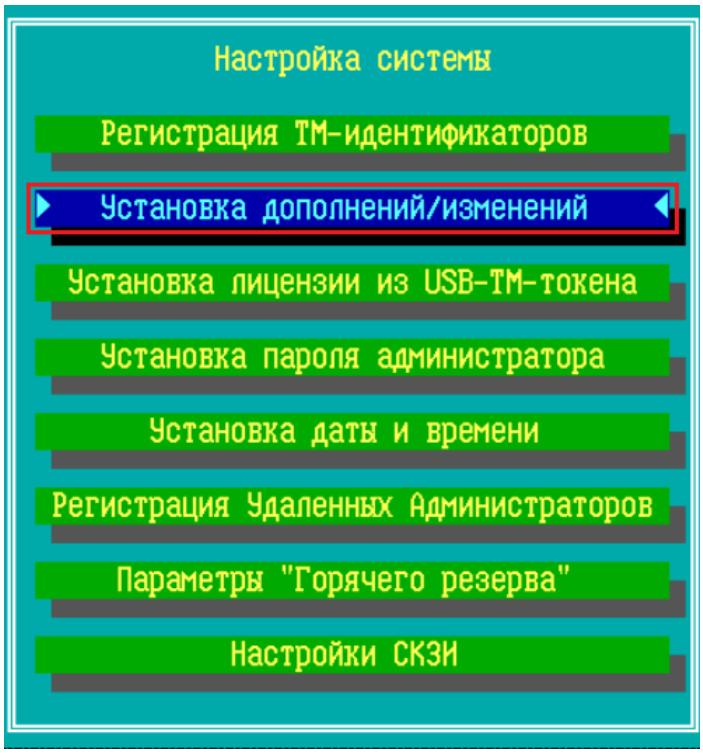


Рисунок 197 - Выбор пункта «Установка дополнений/изменений»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 198 - Подтверждение полномочий и ввод пароля ТМ

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

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

серийного номера ФПСУ (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.
2. Подключите USB-носитель к АП ФПСУ или к виртуальной машине.

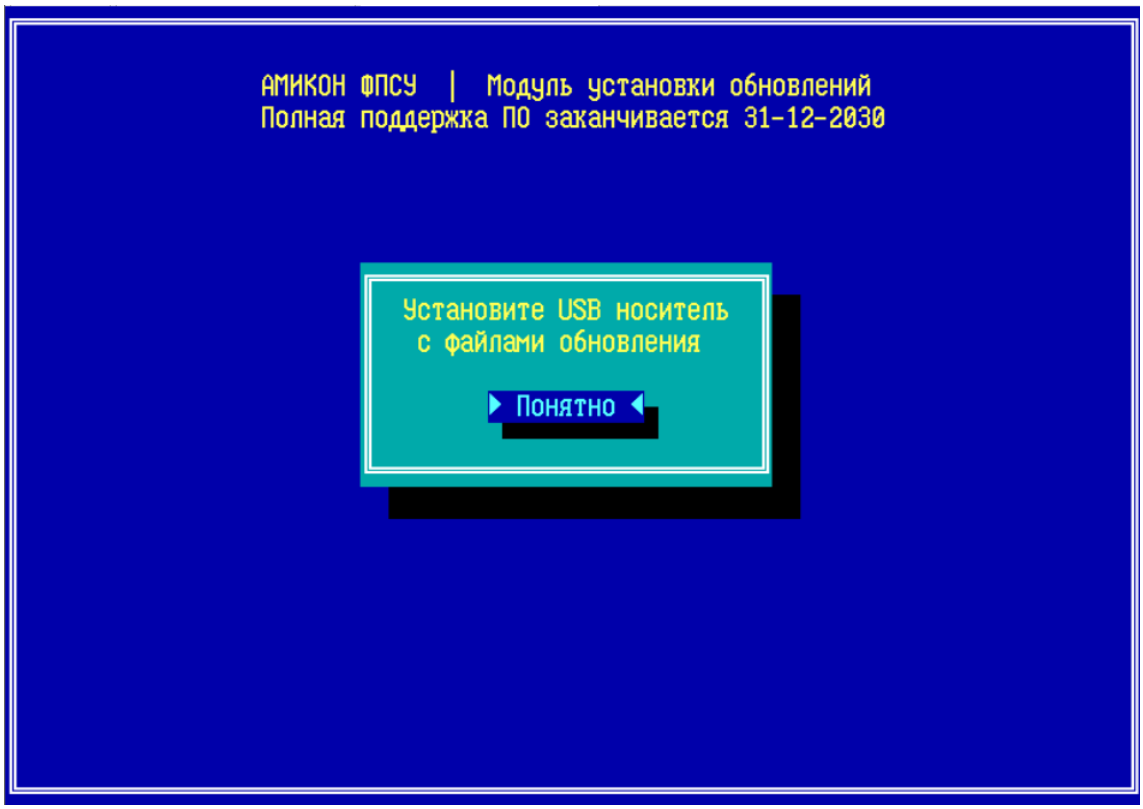


Рисунок 199 - Подключение USB-носителя

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

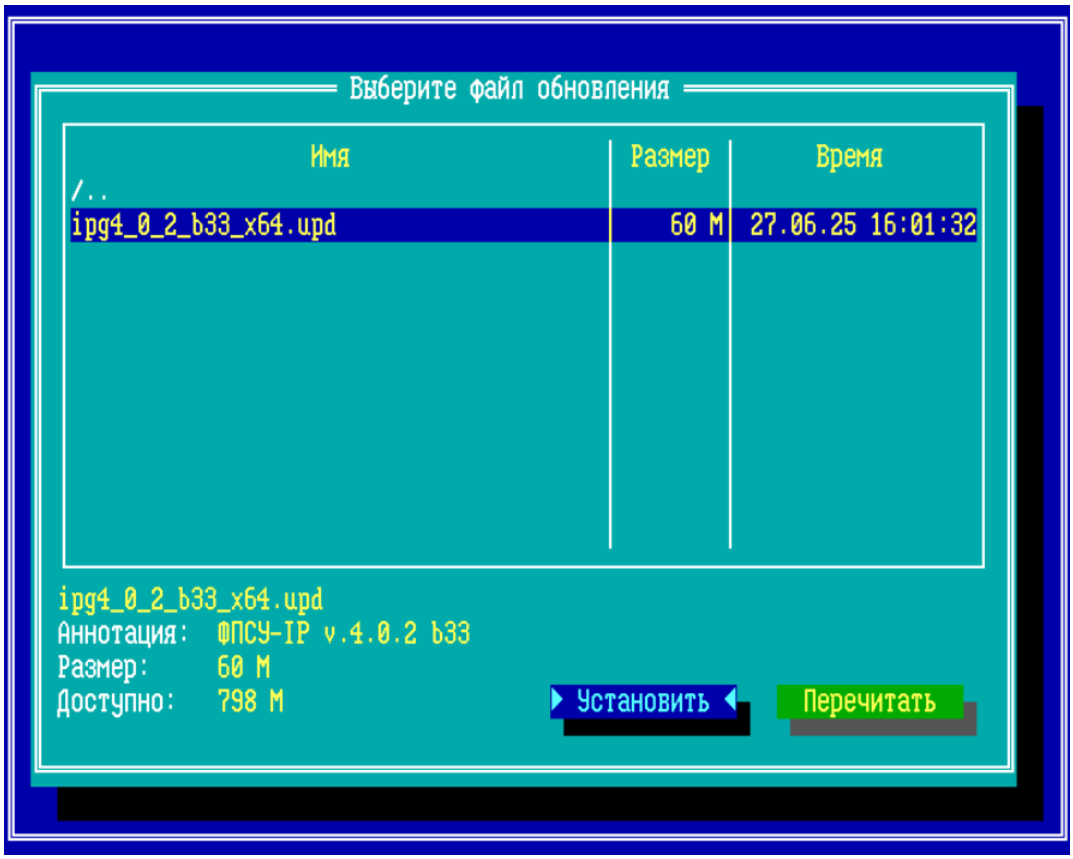


Рисунок 200 - Выбор файла обновления

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

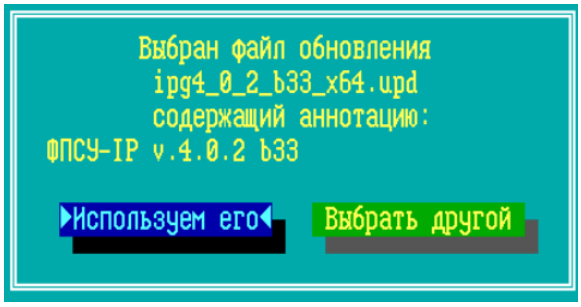


Рисунок 201 - Подтверждение обновления

Начнется процесс установки обновления, необходимо подтверждать этапы установки.

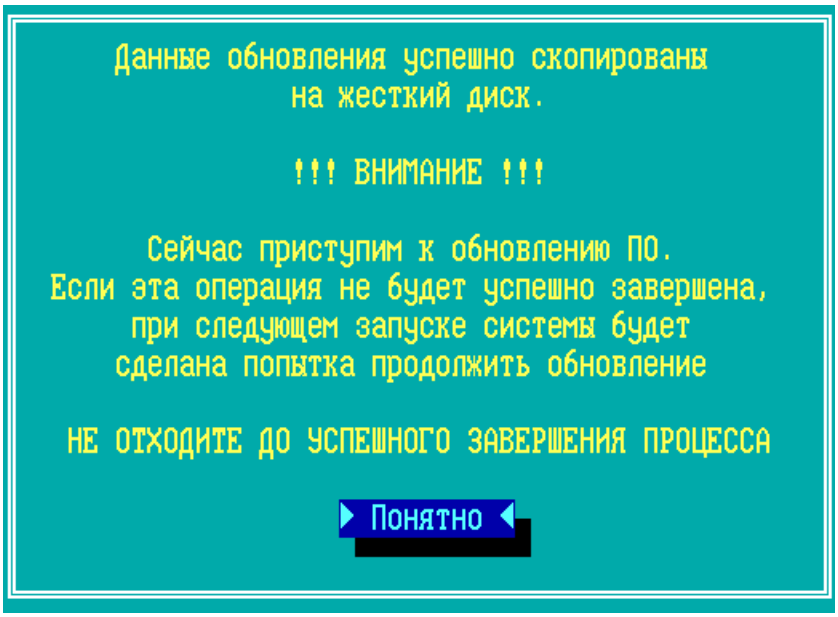


Рисунок 202 - Процесс установки обновления

После установки обновления система будет перезагружена автоматически.

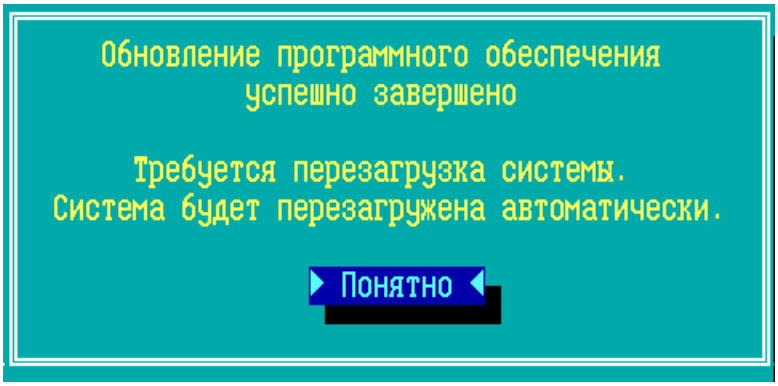


Рисунок 203 - Завершение процесса установки

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



Рисунок 204 - Авто включение фильтрации

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



Рисунок 205 - Главное меню

7. 4. Установка лицензии из USB-TM-токена

Установка лицензии на право использования ФПСУ с присвоением серийного номера комплексу доступна при подключении устройства TM-Key. Для активации лицензии необходимо выполнить обновление ПО по команде меню «Настройка системы → Установка лицензии из USB-TM-токена».

Настройка ФПСУ без лицензии и серийного номера ограничена до его установки.

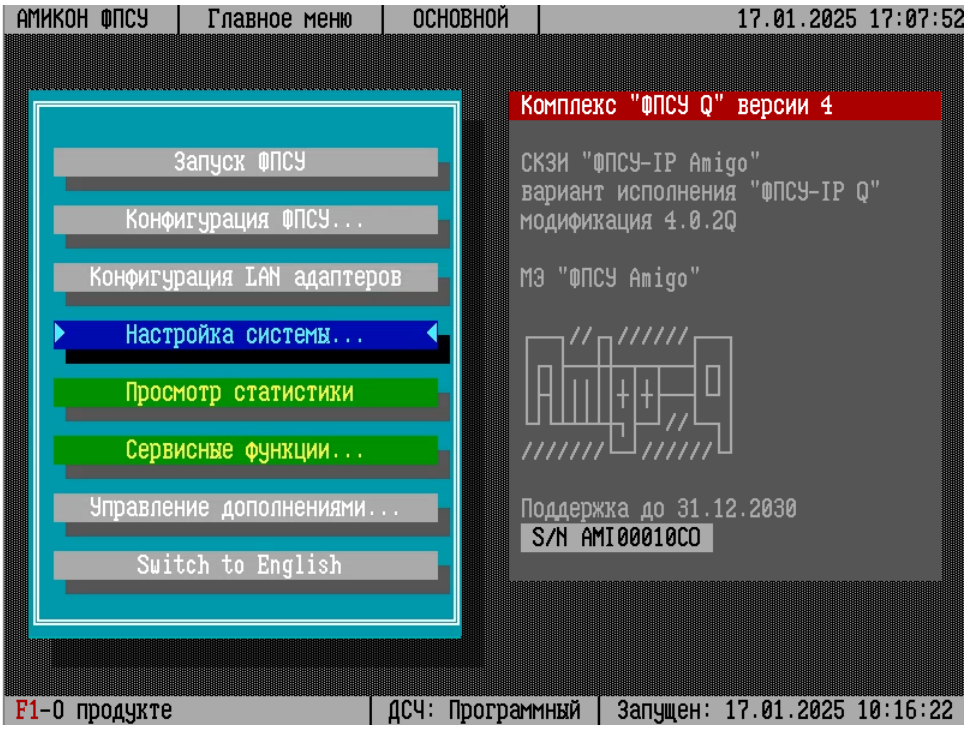


Рисунок 206 - ФПСУ без серийного номера

Лицензия устанавливается на ФПСУ без серийного номера.



Рисунок 207 - Выбор пункта «Установка лицензии из USB-ТМ-токена»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 208 - Подтверждение полномочий и ввод пароля ТМ

Для установки лицензии выполните следующие действия:

Выберите пункт меню «Установка лицензии из USB-TM-токена». Для продолжения потребуется подтвердить полномочия администратора.

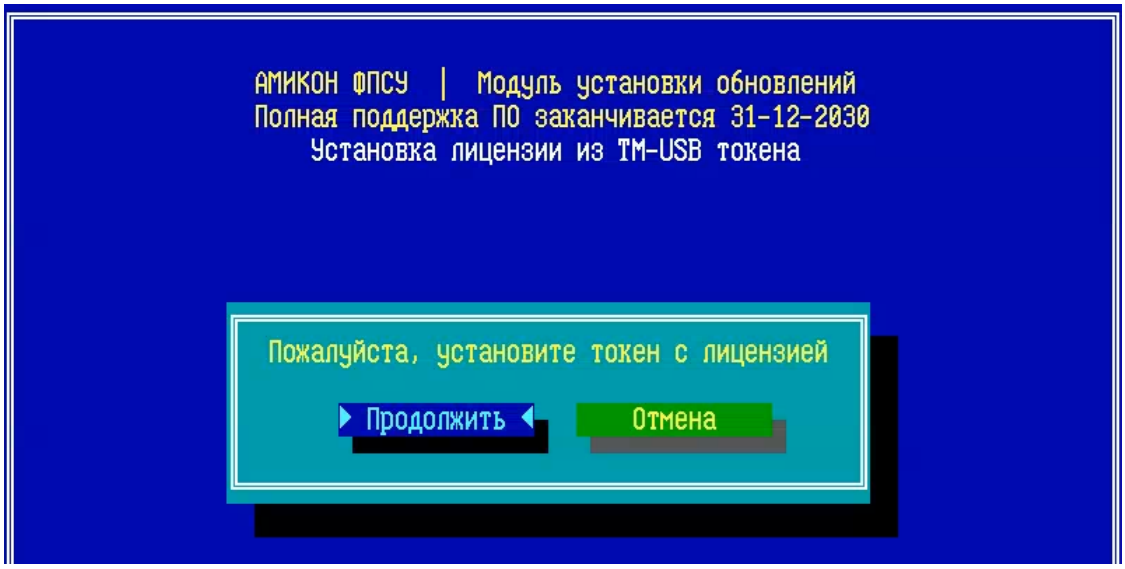


Рисунок 209 - Подключение USB-носителя

Подключите USB-носитель к АП ФПСУ или к виртуальной машине. Требуется подтвердить запуск процесса обновления, выбрав команду «Используем его».

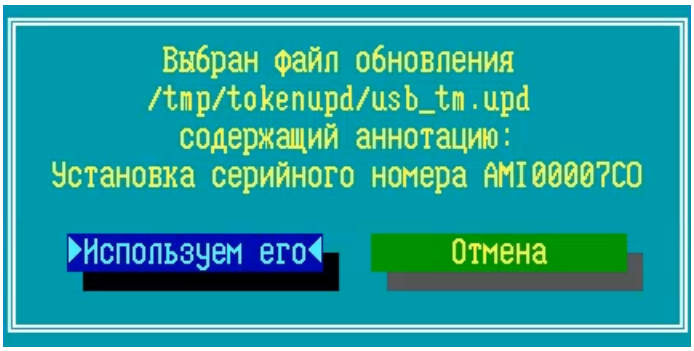


Рисунок 210 - Выбор файла обновления

Начнется процесс установки обновления, необходимо подтвердить этапы установки.

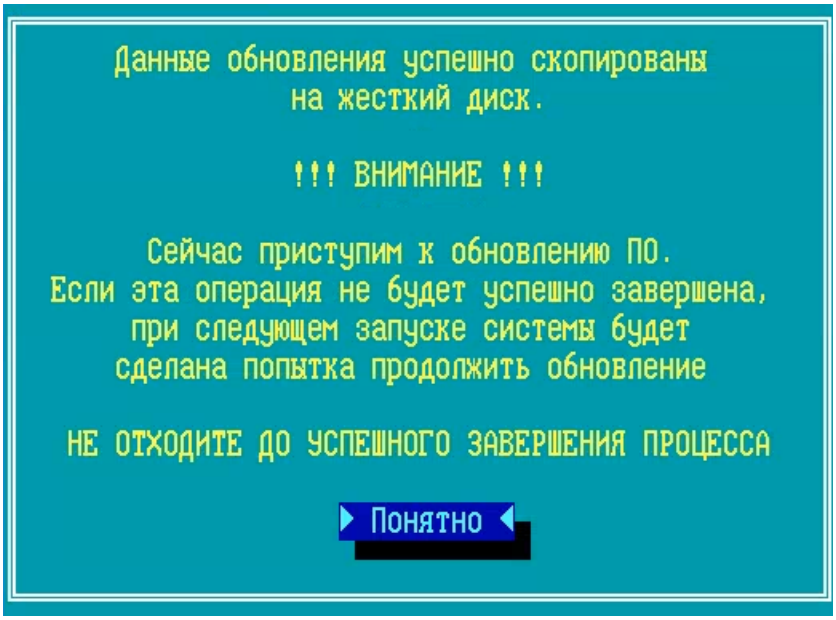


Рисунок 211 - Процесс установки обновления

После установки обновления система будет перезагружена автоматически.

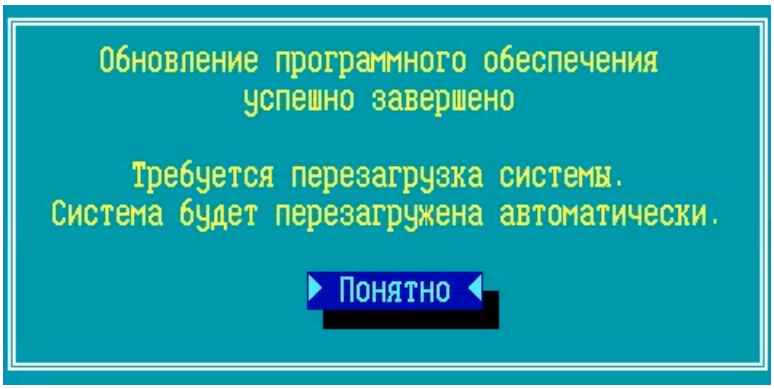


Рисунок 212 - Завершение процесса установки

После перезагрузки откроется главное меню ФПСУ, при успешной установке

лицензии комплексу присваивается серийный номер, информация о серийном номере выводится в открывшемся окне (справа внизу). После присвоения серийного номера ФПСУ станут доступны все команды главного меню.

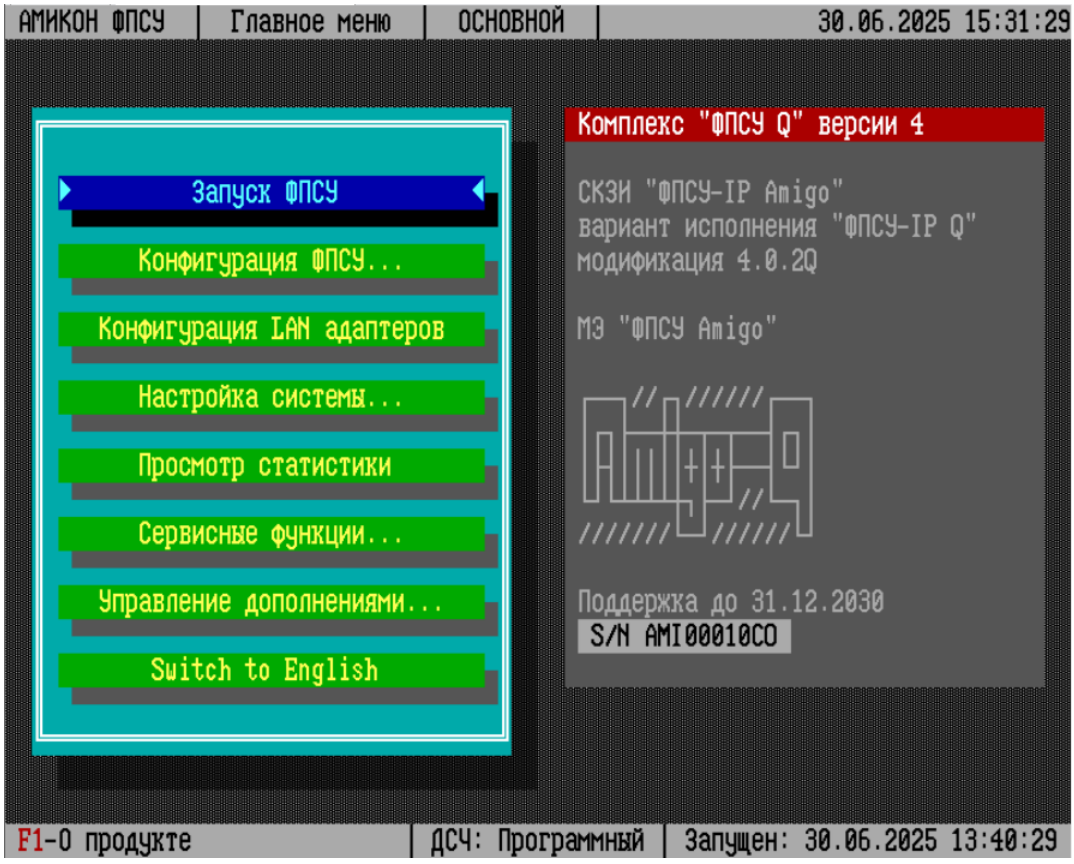


Рисунок 213 - ФПСУ с серийным номером

7. 5. Установка пароля администратора

Команда «Установка пароля администратора» меню «Настройка системы» предназначена для задействования, изменения или отмены пароля на вход в подсистемы конфигурирования ФПСУ и сетевых адаптеров.

ВНИМАНИЕ! Установка пароля условно-постоянного действия на администрирование не рекомендуется для версий ФПСУ 4.0.1 и выше. Данный пункт меню оставлен для обратной совместимости с предыдущими версиями ФПСУ. Для дополнительной авторизации пользователей по паролю используйте пароли ТМ-идентификаторов (см. пункт «Окно регистрации ТМ»).

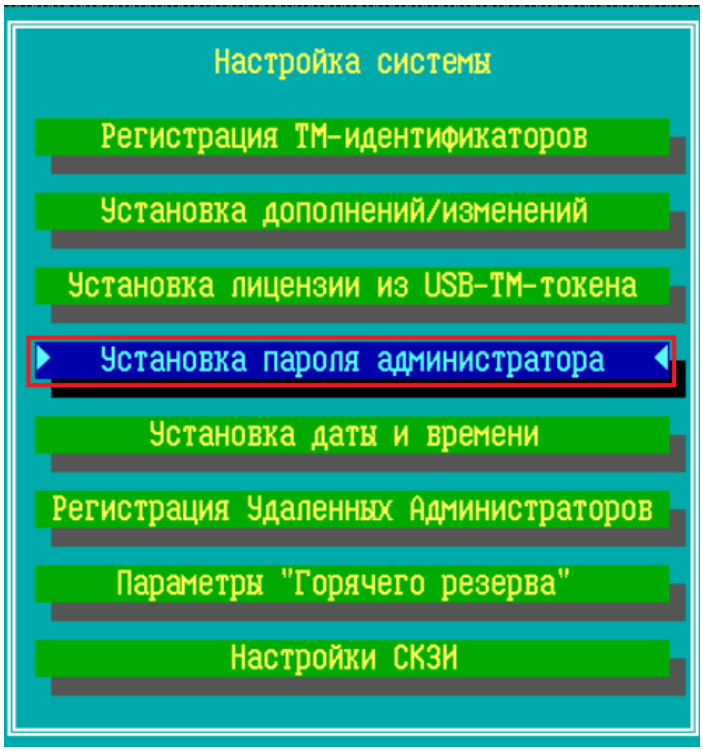


Рисунок 214 - Команда «Установка пароля администратора»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 215 - Подтверждение полномочий и ввод пароля ТМ

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

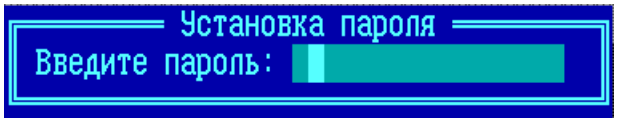


Рисунок 216 - Установка пароля администратора

Вводимые символы не отображаются на экране, требуется повторно ввести пароль с целью исключения возможной ошибки. Установка пароля производится только после повторного ввода 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 (выборе соответствующей команды) будут блокироваться 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 изменения пароля администратора необходимо активировать команду «*Установка пароля администратора»*, 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 потребуется повторная установка ФПСУ с дистрибутива.

7. 6. Установка даты и времени

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

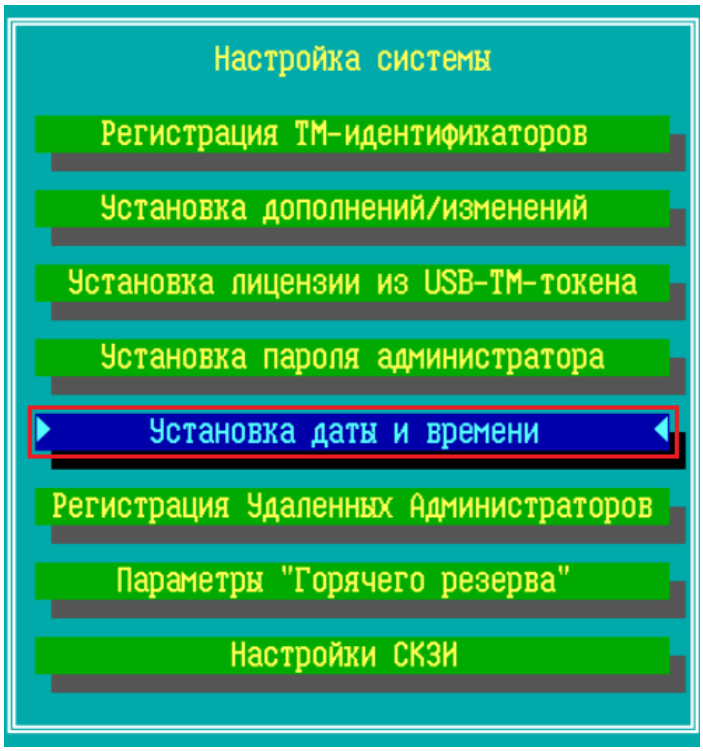


Рисунок 217 - Команда «Установка даты и времени»

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 218 - Подтверждение полномочий и ввод пароля ТМ

Затем на экран будет выдано диалоговое окно:

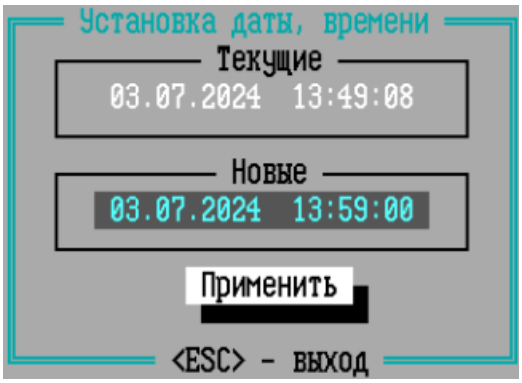


Рисунок 219 - Установка даты и времени на ФПСУ

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

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

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

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

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

7. 7. Регистрация Удаленных Администраторов

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

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

- удаления ранее зарегистрированных удаленных администраторов;
- выдачи открытого ключа ФПСУ для удаленного администратора;
- повторной генерации пары открытый/закрытый ключ ФПСУ, используемых в подсистеме удаленного управления.

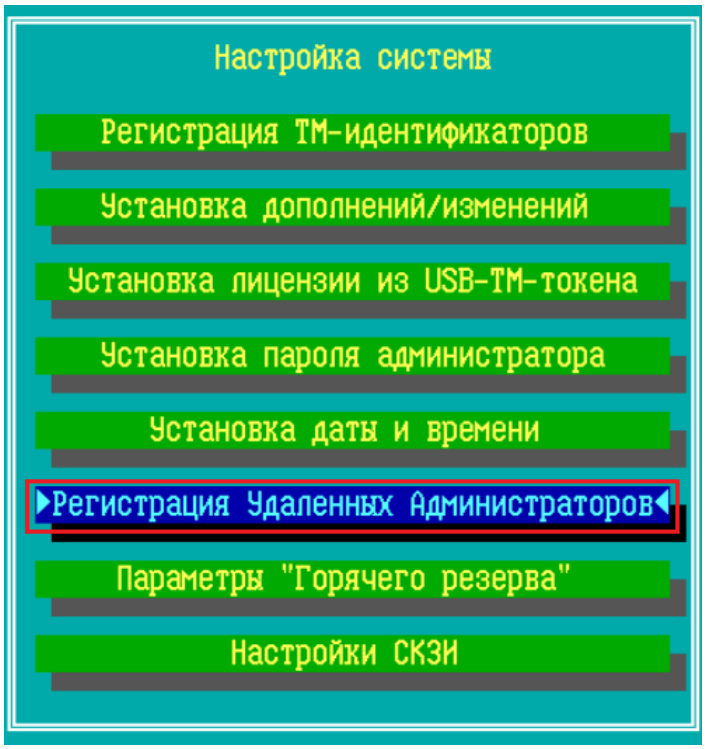


Рисунок 220 - Команда «Регистрация Удаленных Администраторов»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 221 - Подтверждение полномочий и ввод пароля ТМ

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 и удаленного администратора производится следующим образом:

1. локальным администратором ФПСУ выдается на внешний USB-flash носитель файл с открытым ключом ФПСУ;
2. файл с открытым ключом ФПСУ отправляется удаленному администратору (передача файла по незащищенной сети передачи данных запрещается);
3. получив файл с открытым ключом ФПСУ, администратор регистрирует у себя данный ФПСУ в программе «Удаленный администратор ФПСУ»;
4. удаленный администратор с помощью программы «Удаленный администратор ФПСУ» выдает на внешний носитель файл с открытым ключом удаленного администратора;
5. файл с открытым ключом удаленного администратора отправляется локальному администратору ФПСУ (передача файла по незащищенной сети передачи данных запрещается);
6. получив файл с открытым ключом удаленного администратора, локальный администратор ФПСУ регистрирует удаленного администратора и предоставляет ему права на доступ к подсистемам ФПСУ.

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

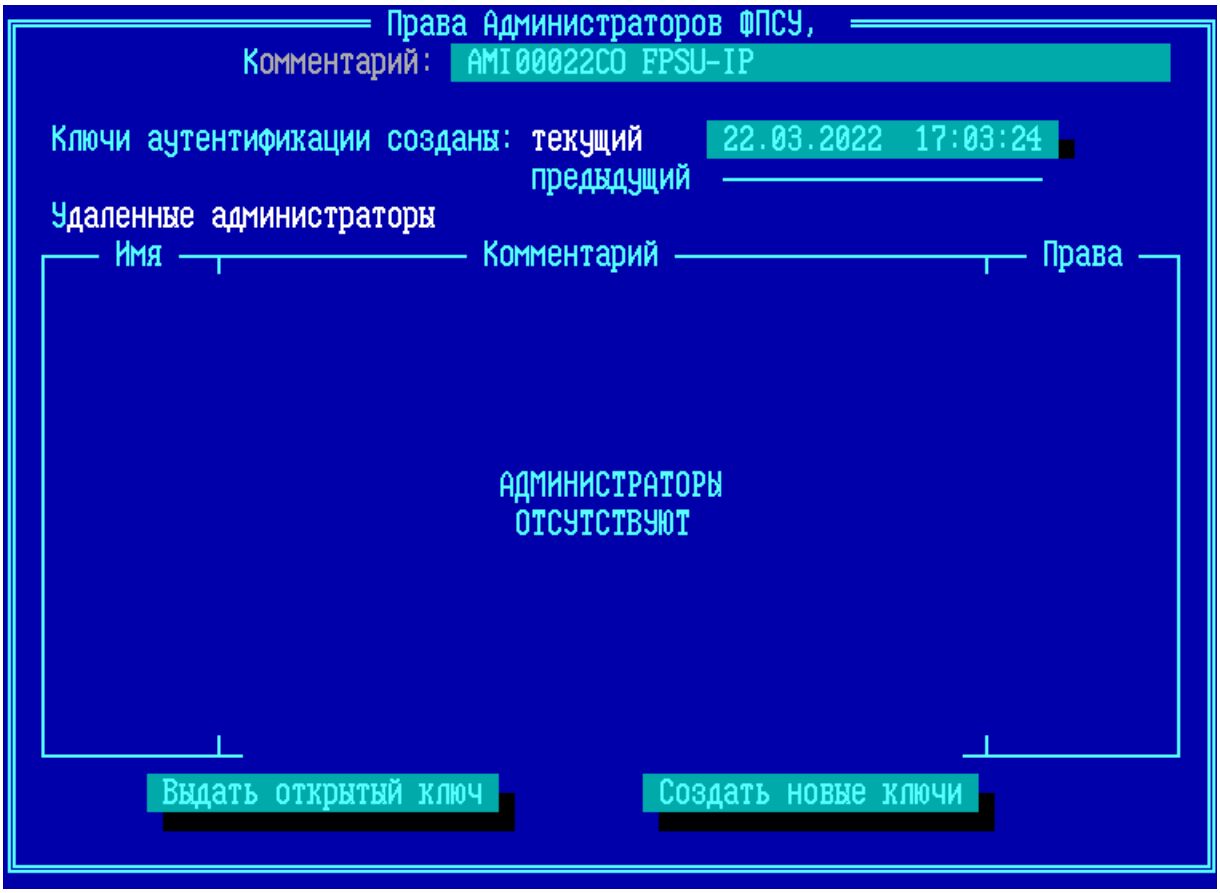


Рисунок 222 - Список удаленных администраторов

Количество удаленных администраторов, зарегистрированных на ФПСУ, не может превышать сто двадцать восемь.

Выход из подсистемы регистрации удаленных администраторов осуществляется клавишами <*Alt+X*> или <*Esc*>.

7. 7. 1. Регистрация удаленного администратора на ФПСУ

Для регистрации первой учетной записи удаленного администратора на ФПСУ необходимо нажать клавишу <*Ins*>, установив курсор на текст «Администраторы отсутствуют». Подсистема запросит установить носитель с открытыми ключами удаленных администраторов, которые должны быть предварительно получены от удаленного администратора. Подключив USB-flash с открытыми ключами удаленных администраторов, требуется нажать кнопку «*ОК*» или клавишу <*Enter*>.

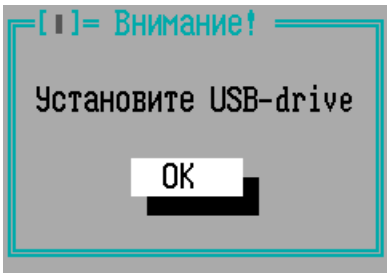


Рисунок 223 - Ожидание подключения USB-носителя с ключами

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

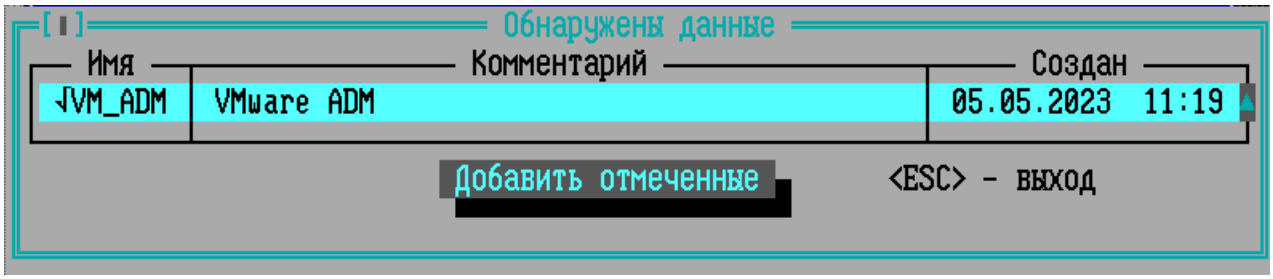


Рисунок 224 - Найденные открытые ключи удаленного администратора

После выполнения команды строки с зарегистрированными удаленными администраторами будут выведены в списке окна «Права администраторов».

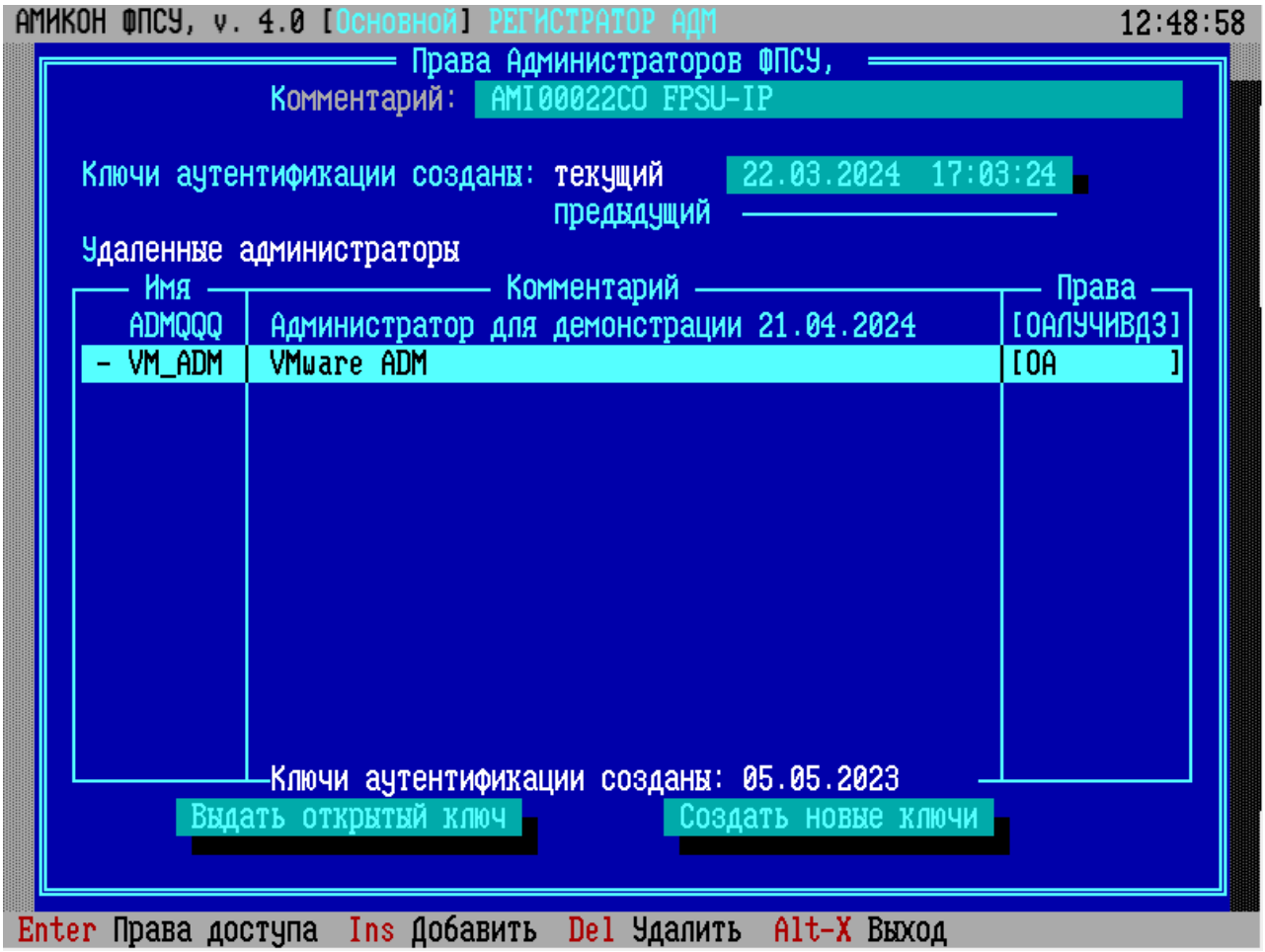


Рисунок 225 - Зарегистрирован удаленный администратор

В верхней части окна отображаются даты создания пар открытый/закрытый ключ ФПСУ для связи с АРМ УА - текущей и предыдущей.

В таблице ниже для каждого зарегистрированного удаленного администратора отображается имя, комментарий к имени, права на доступ к подсистемам ФПСУ и дата создания открытого ключа удаленного администратора для связи с ФПСУ.

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

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

Для присвоения удаленному администратору прав на доступ к подсистемам ФПСУ или изменения существующих, необходимо отметить его в списке и нажать *<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.

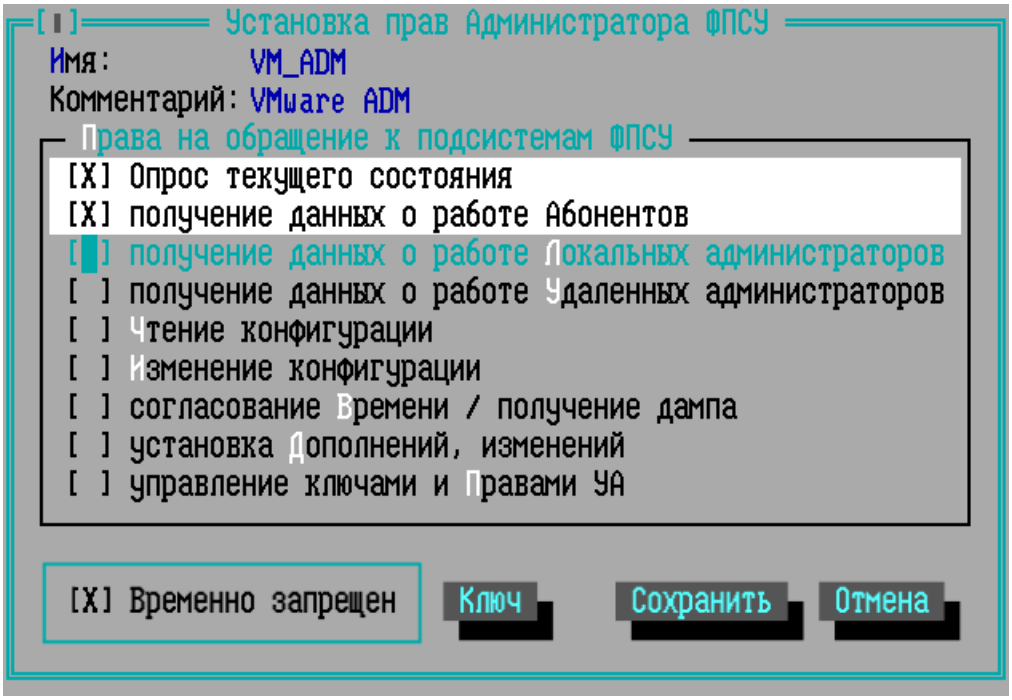


Рисунок 226 - Назначение прав удаленному администратору

Права на обращение к подсистемам ФПСУ:

Опрос текущего состояния – удаленному администратору доступна информация об изменениях конфигурации ФПСУ: изменения, внесенные локальным администратором, удаленным администратором, по резерву; количество запусков ФПСУ; события установки ключей; события согласования времени вручную и автоматически; изменения программного обеспечения. Удаленному администратору также доступна информация о состояние аппаратной части – скорости вращения вентиляторов, температуре и напряжении.

Получение данных о работе абонентов – удаленному администратору доступно получение информации о состоянии работы абонентов и клиентов ФПСУ-IP – статистическая информация о передаче данных в открытом виде и через VPN-туннель, об ошибках при передаче, отказе доступа, отсутствии связи, о передаче данных за сутки.

Получение данных о работе локальных администраторов – удаленному администратору доступно получение статистики ФПСУ о работе локальных администраторов – запуске ФПСУ, начале и окончании работы ФПСУ, регистрации ТМ-

идентификаторов и их удалении, изменении параметров конфигурации ФПСУ, установке изменений или дополнений программного обеспечения ФПСУ, регистрации администраторов УА ФПСУ и т.д.

Получение данных о работе удаленных администраторов – удаленному администратору доступно получение статистики ФПСУ о работе удаленных администраторов – получении статистических данных и правил фильтрации ФПСУ, изменении текущего времени ФПСУ, дистанционной установке изменений или дополнений к программному обеспечению и т.д. Удаленному администратору также доступно передавать управление партнеру по горячему резервированию.

Чтение конфигурации – удаленному администратору доступно получать конфигурацию с ФПСУ.

Изменение конфигурации – удаленному администратору доступно устанавливать конфигурацию на ФПСУ. Удаленному администратору также доступно загружать и устанавливать файлы на ФПСУ.

Согласование времени/получение дампа – удаленному администратору доступно устанавливать время на ФПСУ, устанавливать автокоррекцию времени на ФПСУ, что позволит автоматически синхронизировать текущее время на ФПСУ с текущим временем УА ФПСУ. 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. Удаленному администратору также доступно получение дампа.

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

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

Установка дополнений, изменений – удаленному администратору доступно передавать изменения/дополнения на ФПСУ, рассылать обновления ПО на множество ФПСУ в фоновом режиме, массовая загрузка обновлений ПО на ФПСУ по списку.

Управление ключами и правами УА – удаленному администратору доступна установка и удаление парно-выборочных ключей ФПСУ, выработанных ЦВК; установка и удаление ключевые данные клиентов ФПСУ, сгенерированных ЦГКК. Удаленному администратору также доступно редактировать список удаленных администраторов

выбранного ФПСУ.

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

Данные об открытом ключе удаленного администратора отображаются по кнопке *«Ключ»*. В открывшемся окне отображается период действия открытого ключа удаленного администратора, а также когда будет активировано оповещение об окончании срока действия ключа с установленной периодичностью.

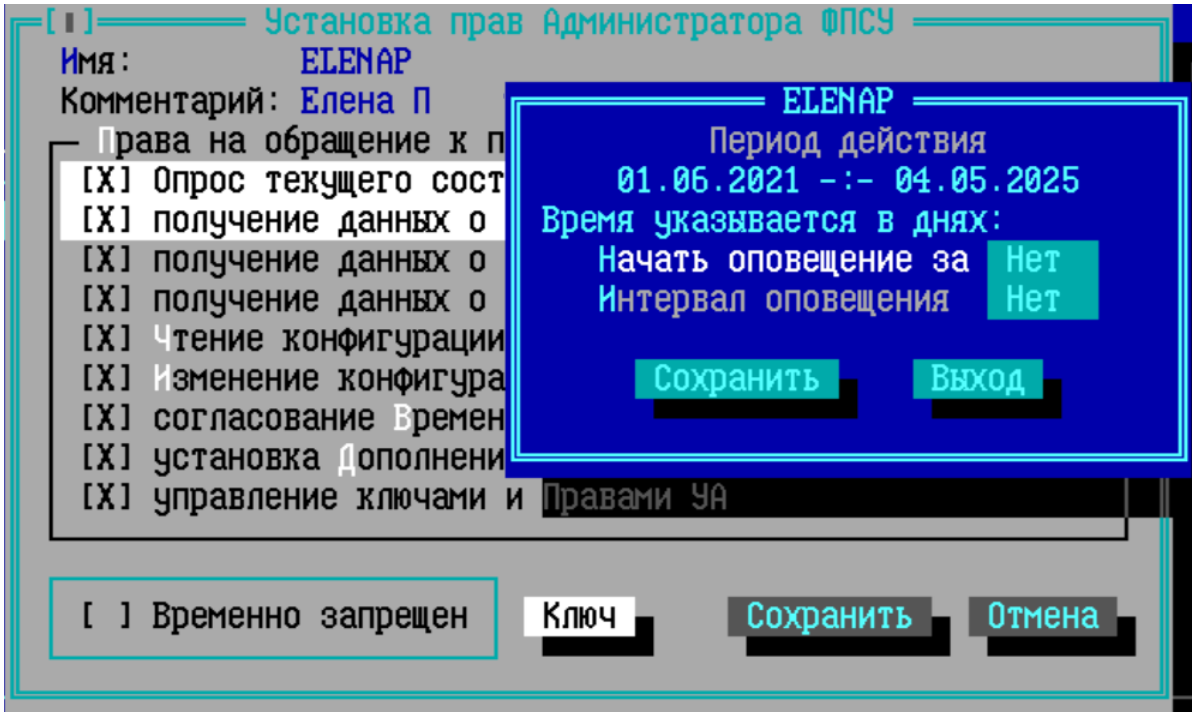


Рисунок 227 - Данные об открытом ключе удаленного администратора

7. 7. 2. Ключи ФПСУ для связи с УА

Ключи ФПСУ для связи с УА представляют собой пару открытый/закрытый ключ и требуются для регистрации ФПСУ удаленным администратором в программе «Удаленный администратор ФПСУ-IP».

Ключи ФПСУ для связи с УА подлежат замене в ряде случаев: завершение установленного срока действия ключа, утеря или компрометация носителя с ключом.

Ключи ФПСУ для связи с УА могут иметь статус «текущие» и «предыдущие». И «текущие» и «предыдущие» ключи являются действительными для установления соединения с удаленным администратором. При создании новой пары открытый/закрытый ключ ФПСУ,

«текущие» ключи становятся «предыдущими», а «предыдущие» становятся недействительными.

Открытый ключ ФПСУ выдается на внешний носитель с целью регистрации его удаленным администратором. Для записи текущего открытого ключа ФПСУ на внешний носитель нажмите кнопку «*Выдать открытый ключ*». Выдать предыдущий открытый ключ ФПСУ нельзя.

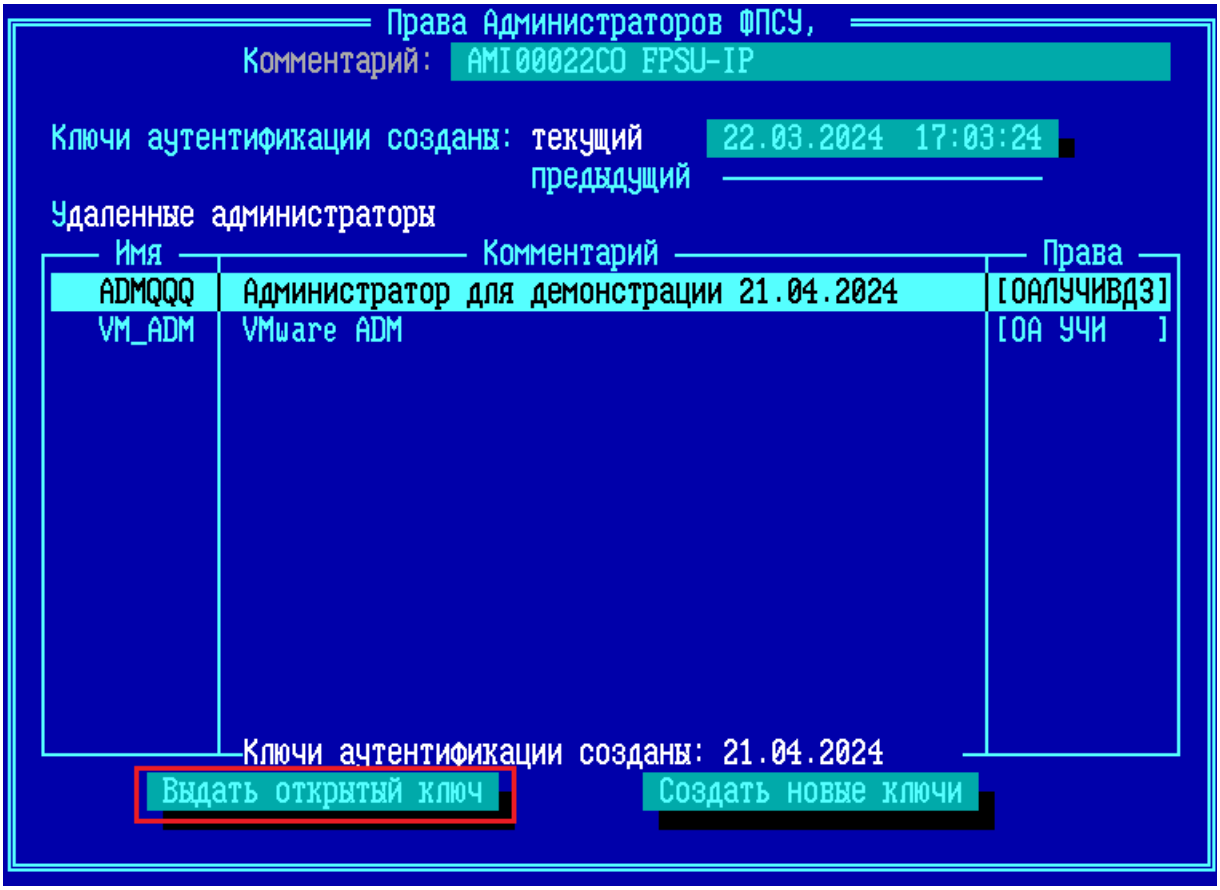


Рисунок 228 - Команда выдачи открытого ключа ФПСУ

Для выработки новой пары открытый/закрытый ключ ФПСУ, выполните команду «*Создать новые ключи*». В случае компрометации «текущих» ключей этой командой придется воспользоваться два раза (сначала сделать «текущие» ключи «предыдущими», а затем недействительными).

После генерации новых ключей ФПСУ для связи с УА, доступ всех удаленных администраторов к ФПСУ будет заблокирован. Удаленным администраторам потребуется выполнить повторную регистрацию ФПСУ с новым открытым ключом ФПСУ.

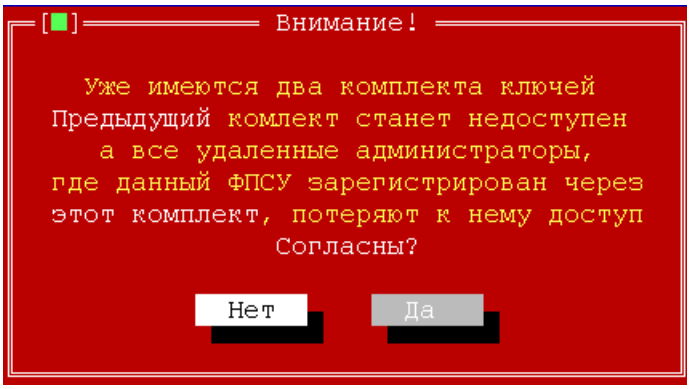


Рисунок 229 - Предупреждение при создании новой пары открытый/закрытый ключ ФПСУ

7. 8. Параметры «Горячего резерва»

Команда «Параметры «Горячего резерва» меню «Настройка системы» предназначена для конфигурации подсистемы резервирования и включает следующие действия:

- активацию режима горячего резервирования работы ФПСУ;
- разовую принудительную синхронизацию данных основного и резервного ФПСУ системы резервирования;
- взаимную регистрацию ФПСУ и его партнера по резервированию.



Рисунок 230 - Команда «Параметры «Горячего резерва»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 231 - Подтверждение полномочий и ввод пароля ТМ

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

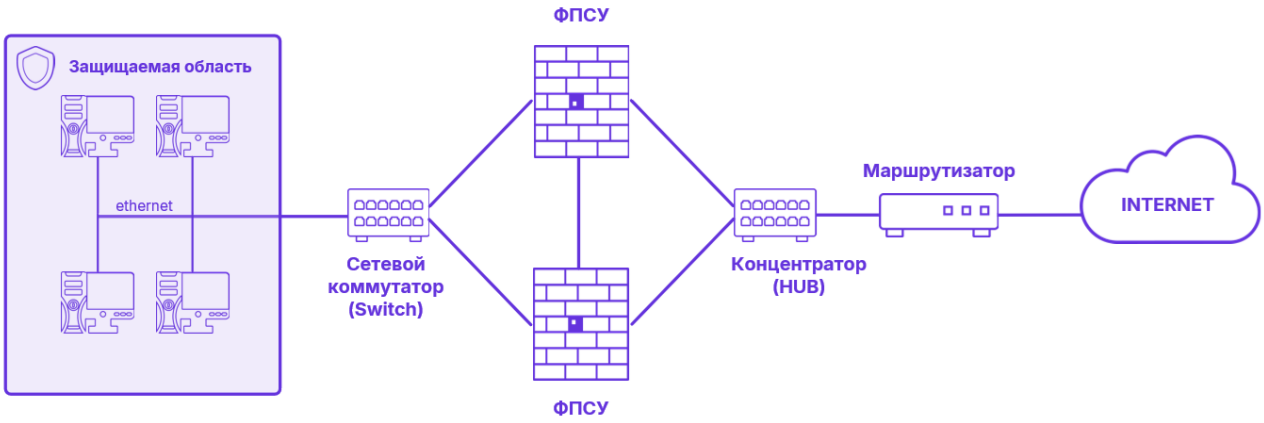


Рисунок 232 - Пример схемы подключения горячего резерва ФПСУ

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

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

Маркер каждого из ФПСУ («основной» или «резервный» в схеме горячего резервирования) устанавливается один раз при инсталляции ПО ФПСУ, а функциональный статус может меняться в процессе работы: каждый из ФПСУ 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 производят периодический опрос работоспособности друг друга. При отсутствии ответа от активного ФПСУ или при получении сообщения об аппаратных неполадках на активном, пассивный ФПСУ забирает управление, становится активным, и начинает работу по обработке и передаче данных. При необходимости, допущенное лицо с правами класса *«Оператор»* и выше может поменять текущий функциональный статус ФПСУ вручную (см. раздел «Окно состояния подсистемы «горячего» резервирования»).

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

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

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

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

Часть рабочих данных каждого из ФПСУ остается автономной:

- настройки LAN-адаптеров;
- информация подсистемы регистрации и статистики;
- пароль администратора;
- данные о зарегистрированных на ФПСУ ТМ-идентификаторах (кроме Главного администратора, его ТМ-идентификатор общий для обоих ФПСУ).

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

7. 8. 1. Настройка ФПСУ на работу с партнером по резервированию

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

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

Для настройки работы ФПСУ в режиме «горячего» резервирования:

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

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

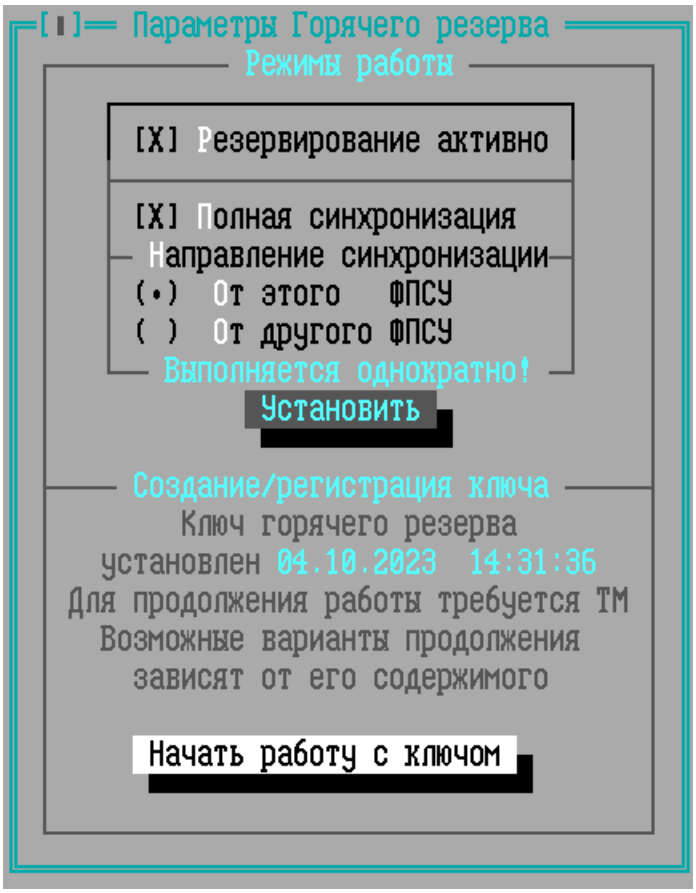


Рисунок 233 - Окно настроек работы горячего резерва

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

7. 8. 1. 1. Замена ключа горячего резерва

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

В случае истечения срока действия ключа горячего резерва на экран ФПСУ выдается следующее предупреждение:

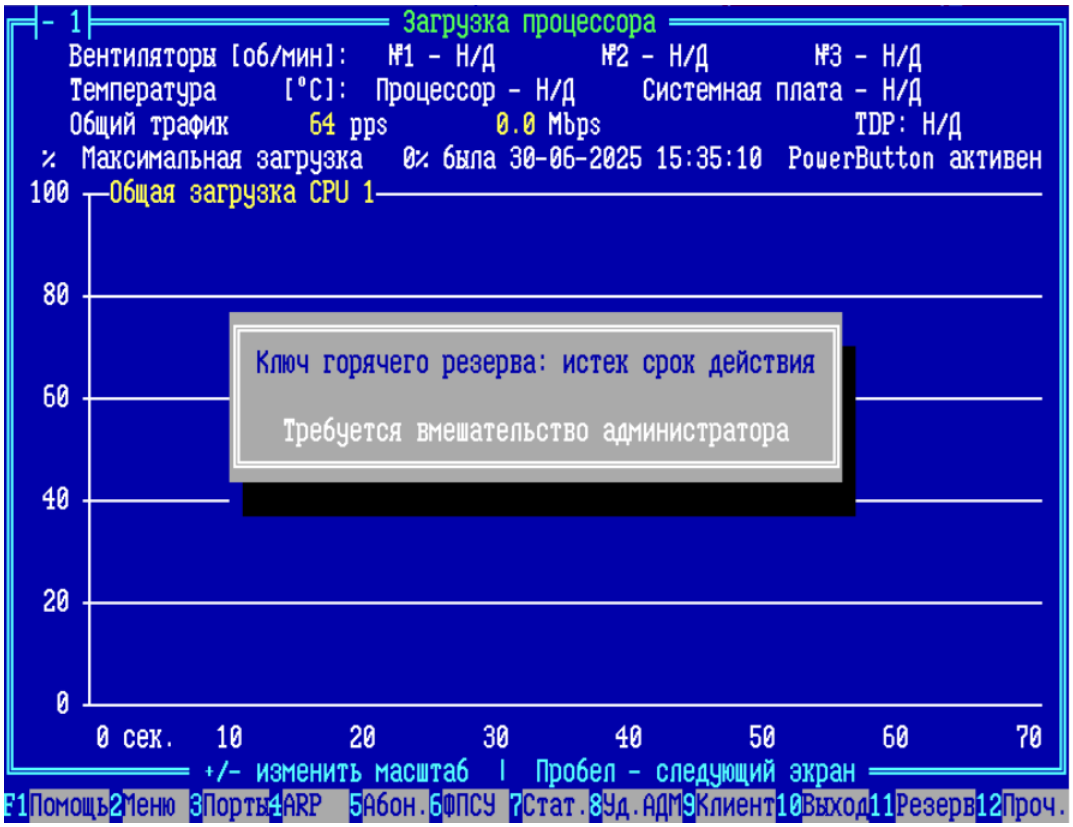


Рисунок 234 - Предупреждение об истечении срока действия ключа горячего резерва

Для замены ключа горячего резерва следует выполнить следующие действия, **начиная с основного ФПСУ** системы резервирования:

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

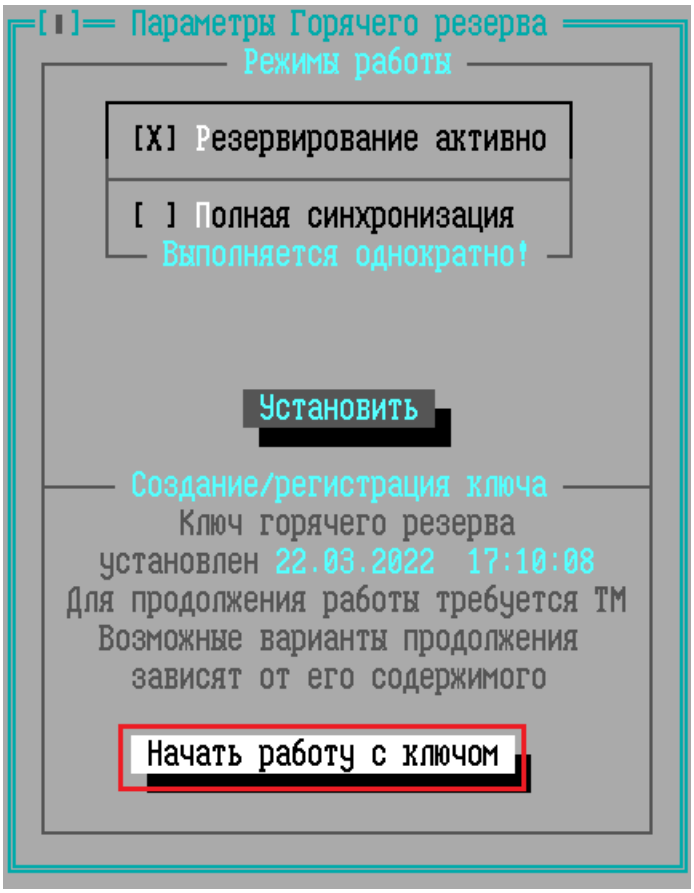


Рисунок 235 - Окно настроек горячего резерва

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

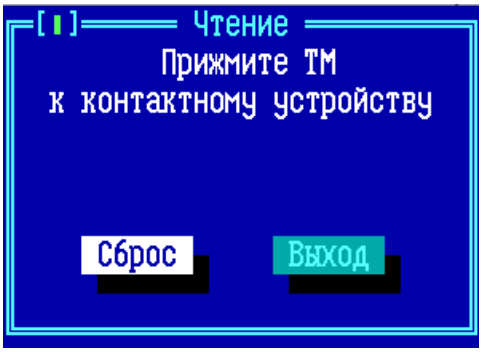


Рисунок 236 - Требование предъявить ТМ-идентификатор для ключа горячего резерва

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

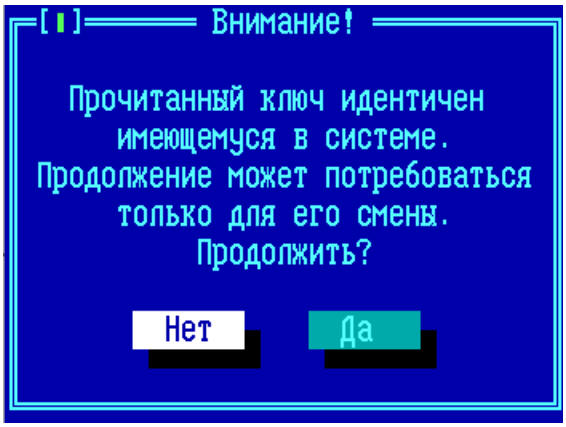


Рисунок 237 - Сообщение об имеющемся ключе горячего резерва

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

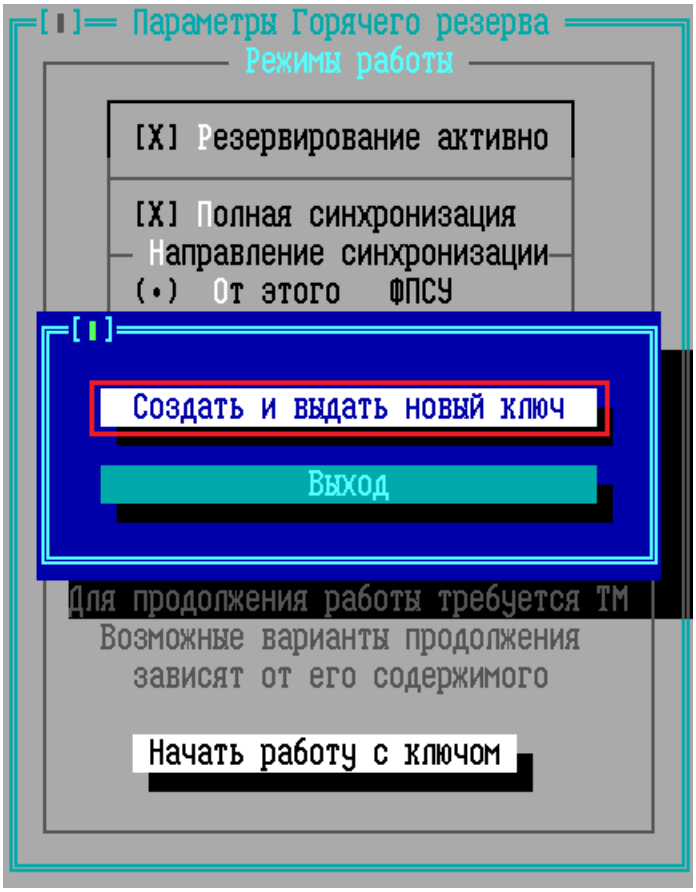


Рисунок 238 - Команда создания нового ключа горячего резерва

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

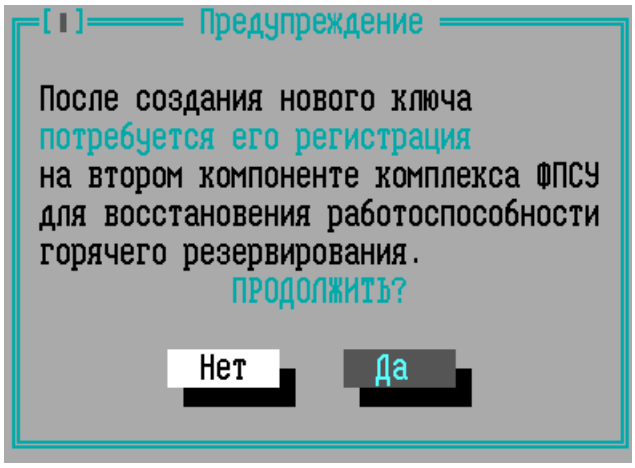


Рисунок 239 - Подтверждение выполнения команды

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

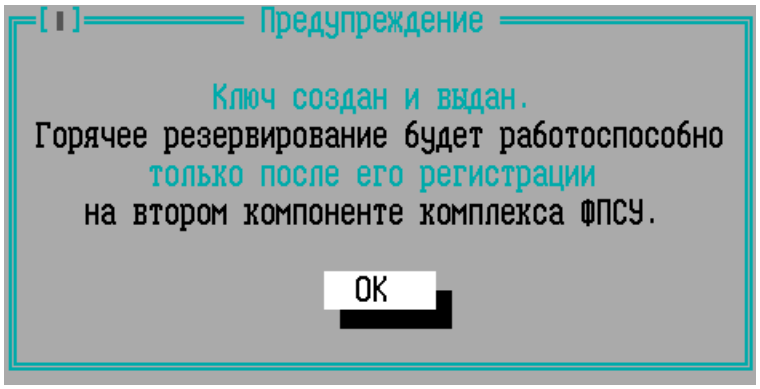


Рисунок 240 - Новый ключ горячего резерва создан и выдан на ТМ

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

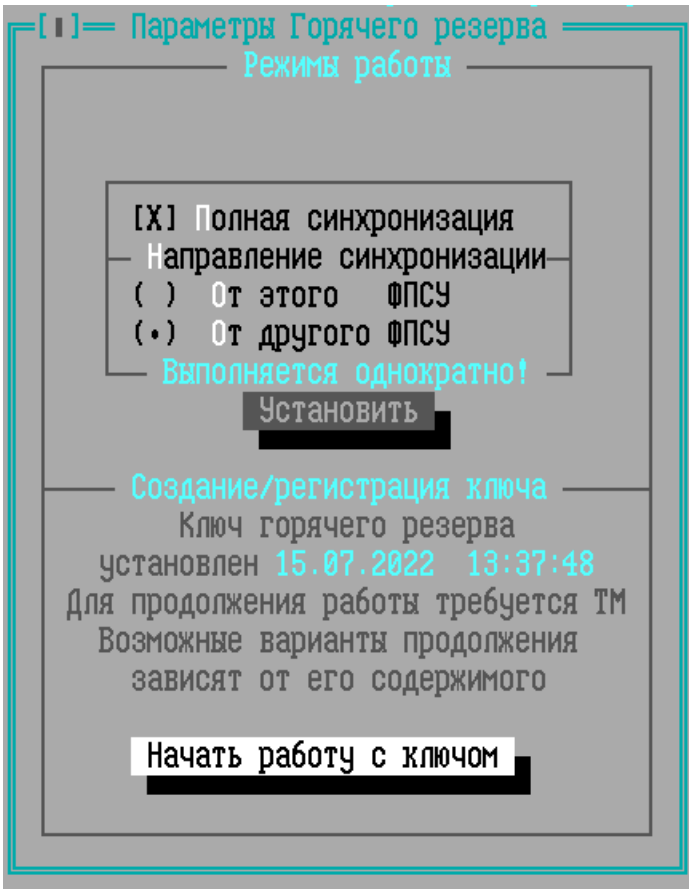


Рисунок 241 - Окно настроек горячего резерва на резервном ФПСУ

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

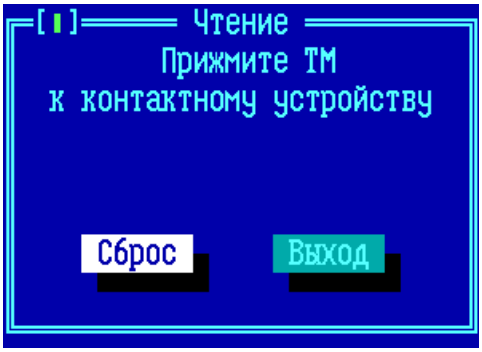


Рисунок 242 - Требование предъявить ТМ-идентификатор с новым ключом горячего резерва

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

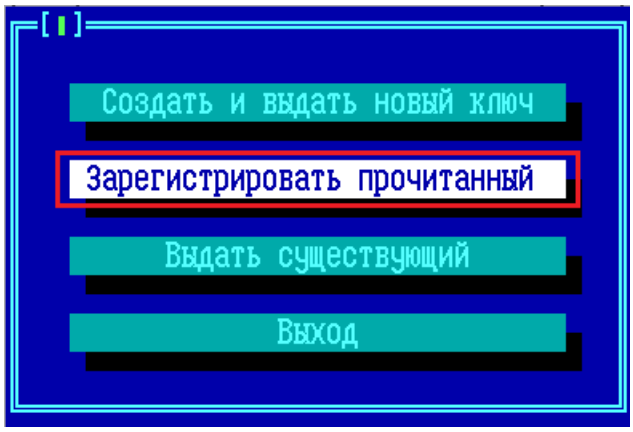


Рисунок 243 - Команда регистрации нового ключа горячего резерва на резервном ФПСУ

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

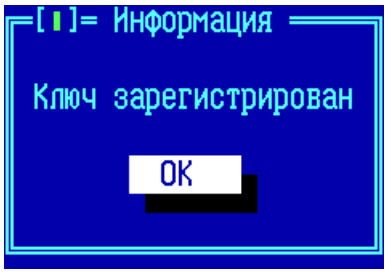


Рисунок 244 - Окончание регистрации нового ключа горячего резерва на резервном ФПСУ

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

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

7. 8. 2. Принудительная синхронизация данных

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

1. При установке и настройке ПО одного из ФПСУ с целью сокращения времени работы и исключения ошибок конфигурирования;
2. При восстановлении работы одного из ФПСУ после аварий и сбоев оборудования;

3. Если при внесении изменений на один из ФПСУ администратор не был уверен, что за время его работы никто не редактировал рабочие данные активного комплекса.

В двух первых перечисленных случаях на настраиваемый ФПСУ достаточно инсталлировать ПО ФПСУ, содержащее подсистему резервирования, установить параметры резервирования (см. предыдущий раздел, «Настройка ФПСУ 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.

В третьем случае рекомендуется сделать принудительную синхронизацию от работающего ФПСУ, на котором были внесены изменения в конфигурацию, что обеспечит немедленное применение всех изменений конфигурации на резервном ФПСУ.

Для выполнения однократной синхронизации:

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

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

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

7. 8. 3. Параметры проверки линий связи для портов ФПСУ

Одним из параметров работоспособности ФПСУ в системе горячего резервирования является успешная проверка указанных администратором ФПСУ линий связи (по умолчанию отключена). Если проверка включена, то она начинает выполняться через 15

секунд после запуска ФПСУ в рабочий режим или перехода из пассивного в активный.

Проверка линий связи выполняется для каждого порта ФПСУ независимо. Если хотя бы для одного порта ФПСУ 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, 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). После передачи управления, ставший пассивным комплекс ФПСУ 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 в системе горячего резервирования устанавливается как «*Работоспособность: частичная»* с дополнительной строкой сообщения «*нет канала связи»*. Если передача управления по причине неуспешной проверки линии связи происходит не в первый раз, длительность запрета и состояния частичной работоспособности умножаться на первоначальный коэффициент 5 не будет.

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

7. 8. 3. 1. Интерфейс настройки проверки линий связи

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

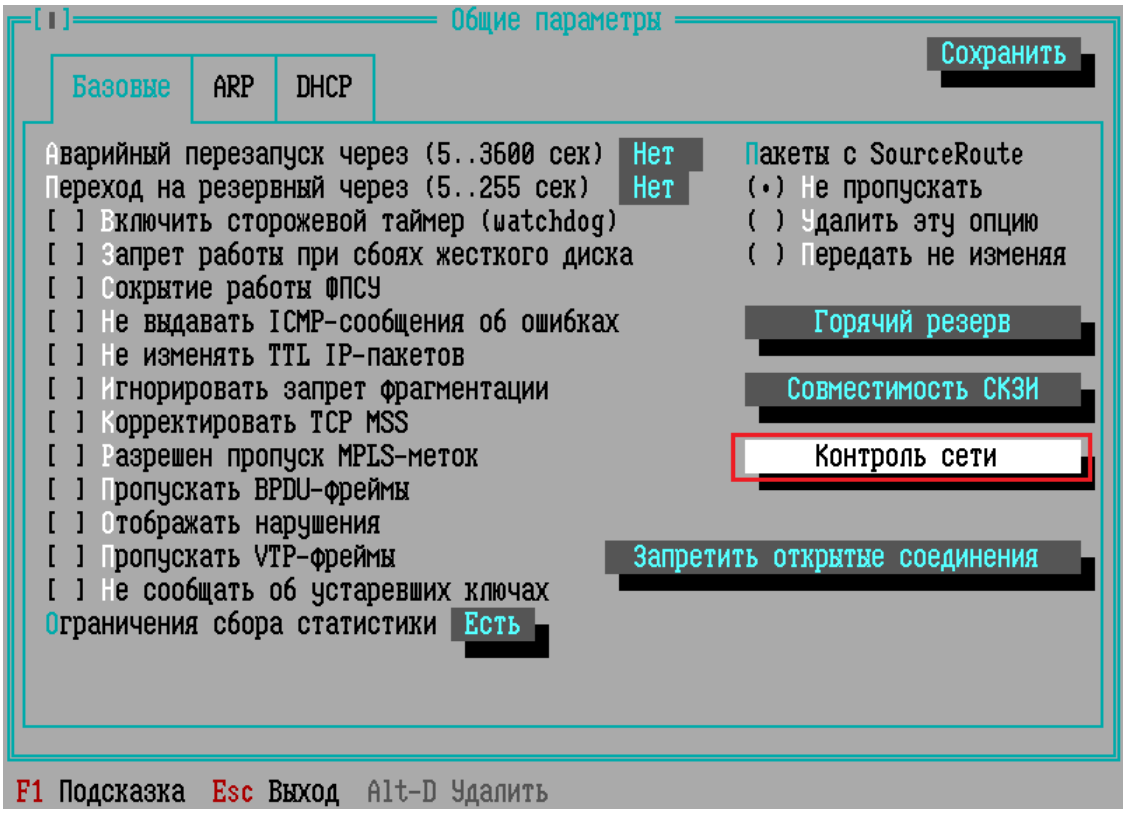


Рисунок 245 - Общие параметры ФПСУ

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

В окне будет отображен список параметров контроля сети и список абонентов, описанных как «хост» для выбранного порта (см. пункт «Описание абонента «Хост»). Если на выбранном порту ФПСУ 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».

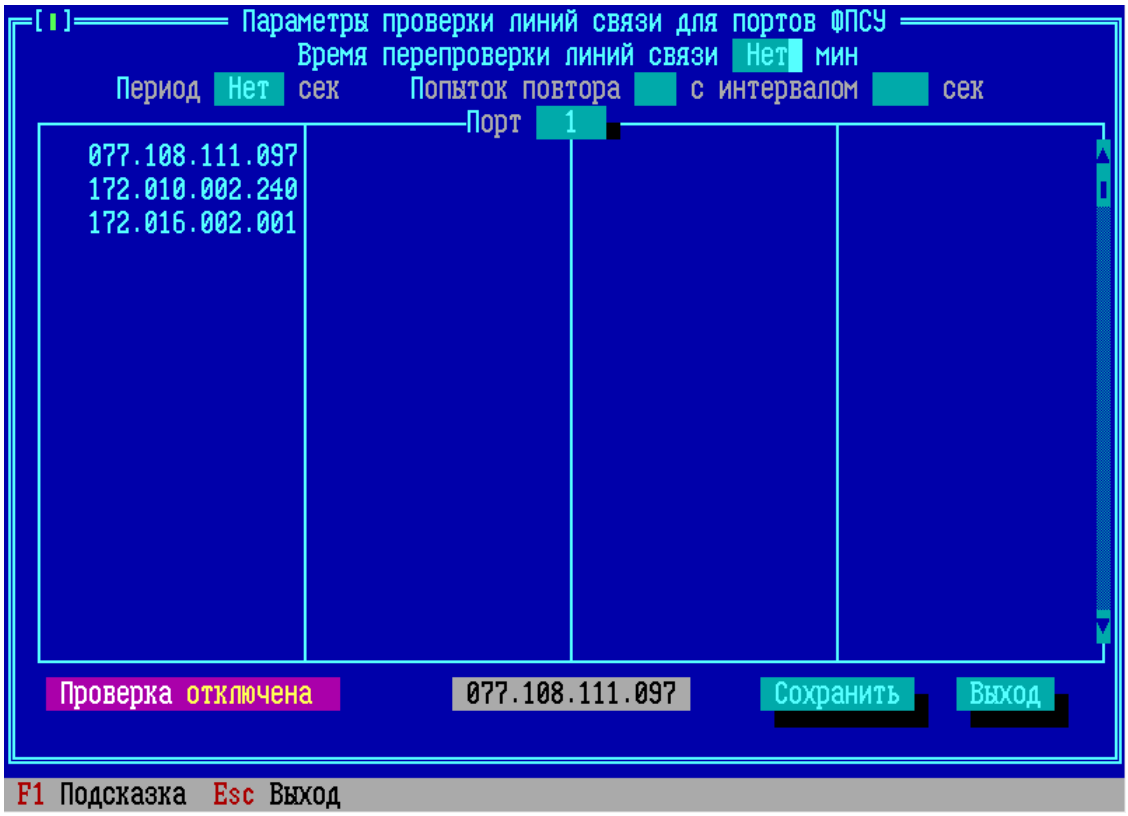


Рисунок 246 - Окно настройки параметров контроля связи

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 может быть выбрано до 8 абонентов для контроля сети.

Параметры, которые необходимо установить:

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

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

Период – временной интервал отправки эхо-запросов в заданные администратором IP-адреса. Устанавливается в пределах от 3-х до 255-и секунд. ФПСУ 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, в случае если ни от одного из IP-адресов контролируемого списка не пришел ответ. Только после исчерпания попыток повтора активный ФПСУ 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 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 следует выполнить команду «Сохранить» или нажать клавишу <F2>. Выход без внесения настроек в конфигурацию осуществляется по клавише <Esc> или команде «Выход».

7. 8. 3. 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 с двумя рабочими портами, работающий в режиме «горячего» резервирования, будет проводить отдельную проверку для каждого рабочего порта следующим образом:

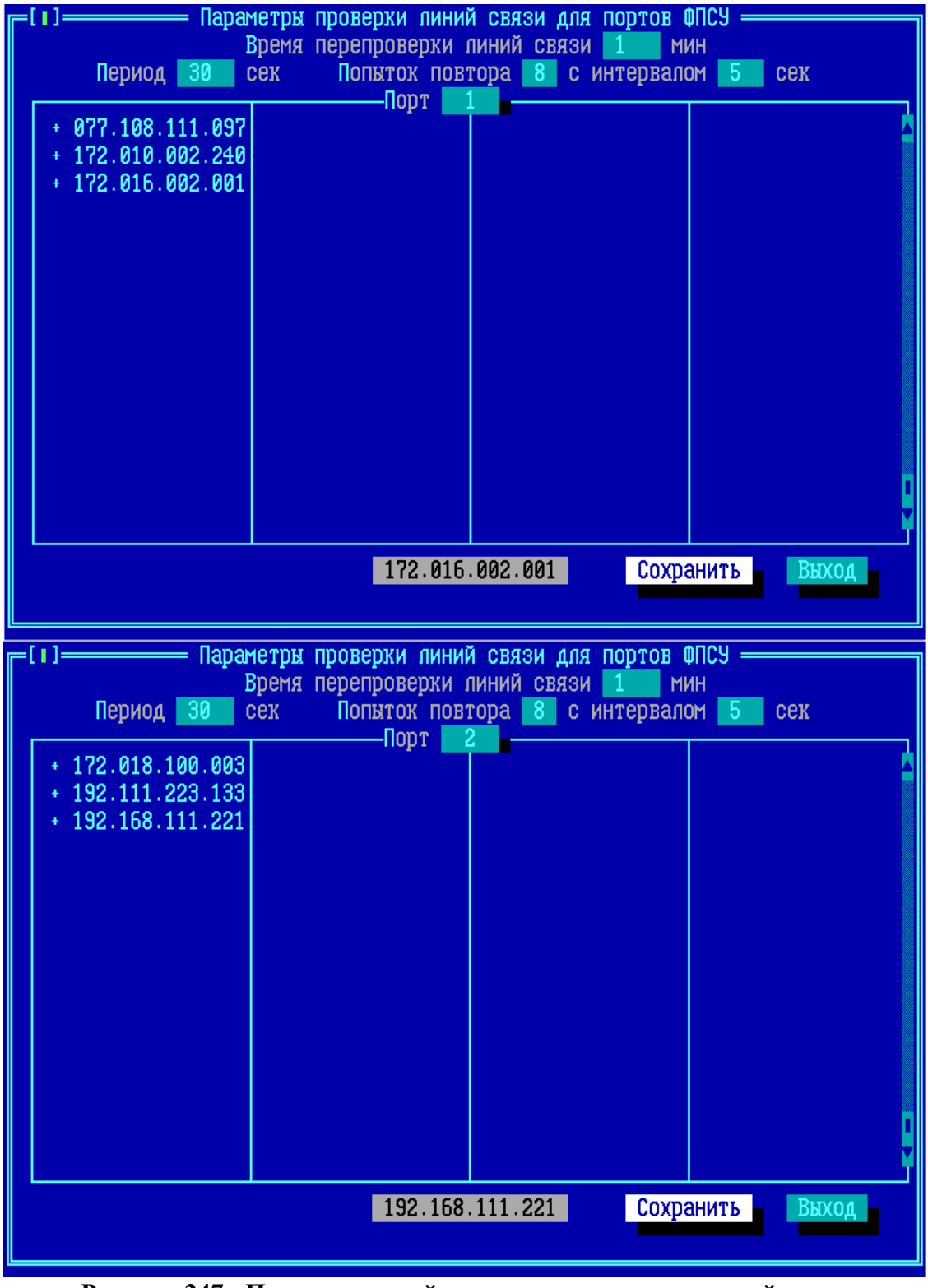


Рисунок 247 - Пример настройки системы проверки линий связи

Активный комплекс ФПСУ системы горячего резерва (далее **ФПСУ№1**) каждые **30**

секунд будет направлять эхо-запросы в адрес хостов первого порта **077.108.111.097**, **172.010.002.240**, **172.016.002.001**, и эхо-запросы в адрес хостов второго порта **172.018.100.003**, **198.111.223.133**, **192.168.111.211**. Проверки доступности хостов каждого порта проводятся независимо друг от друга.

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

Если в результате **8 повторных рассылок** не был получен эхо-ответ от хотя бы одного хоста «замолчавшего» порта, **ФПСУ№1** отдает управление другому комплексу горячего резерва (далее **ФПСУ№2**), становясь пассивным и устанавливая **5-минутный** (1 минута параметра **время перепроверки линий связи** умножается на 5, поскольку это первая передача управления по причине неуспешной проверки линии связи) таймер, запрещающий принимать активное управление обратно. В течении работы таймера состояние **ФПСУ№1** в системе горячего резервирования устанавливается как «*Работоспособность: частичная»* с дополнительной строкой сообщения «*нет канала связи»*, что можно отследить на экране отображения состояния горячего резерва.

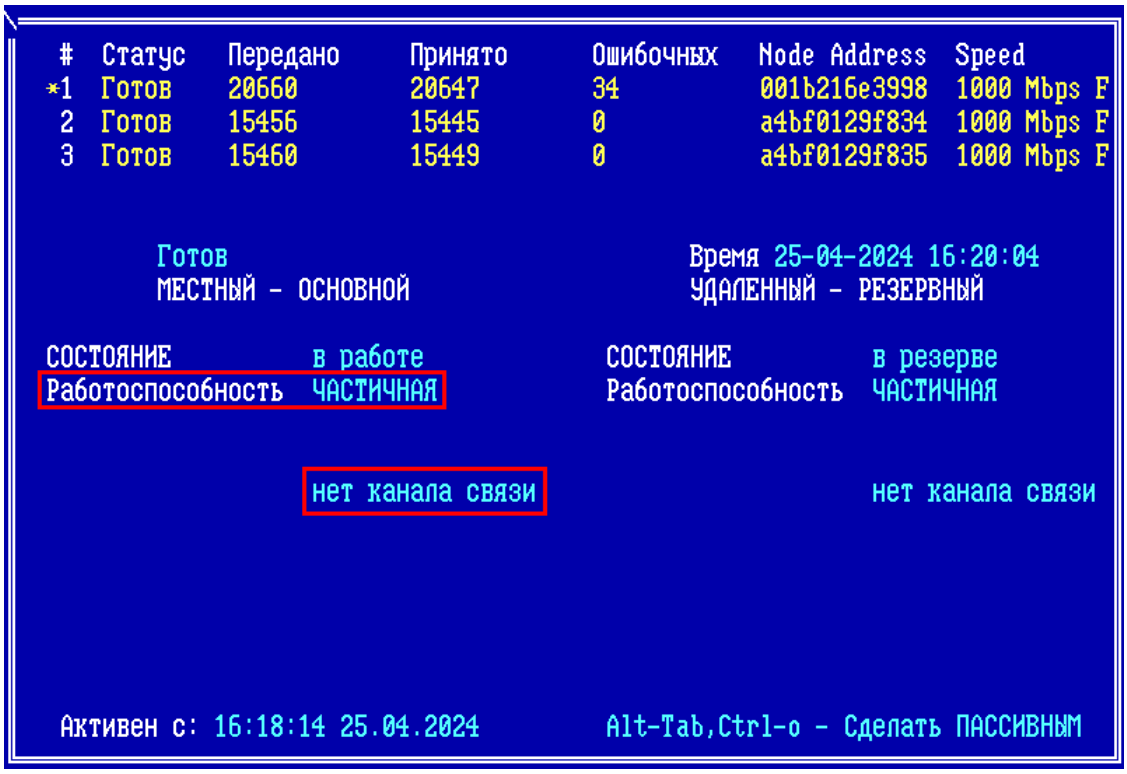


Рисунок 248 - Проверка линии связи неуспешна

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

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

После каждой неуспешной серии проверок **ФПСУ№2** запрашивает **ФПСУ№1** о возможности передать управление комплексом. Если во время такого запроса таймер запрета передачи управления на **ФПСУ№1** уже закончился, то **ФПСУ№2** передает управление на **ФПСУ№1** и устанавливает собственный таймер запрета передачи управления, равный **5 минутам** (1 минута параметра **время перепроверки линий связи** умножается на 5, поскольку это первая передача управления по причине неуспешной проверки линии связи).

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

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

7. 9. Настройки СКЗИ

Команда «Настройки СКЗИ» меню «Настройка системы» предназначена для перехода в интерфейс отключения подсистемы автозапуска, повторной инициализации программного датчика случайных чисел, управления сроками действия ключевых данных ФПСУ, удаления СКЗИ с внутреннего носителя ФПСУ.

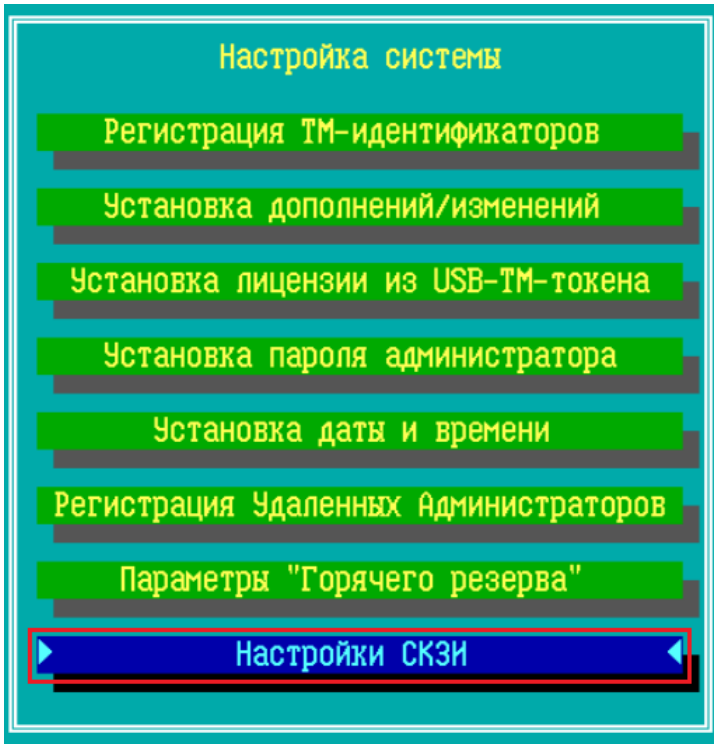


Рисунок 249 - Меню настройки системы ФПСУ

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



Рисунок 250 - Меню настройки СКЗИ ФПСУ

- «Отключение автозапуска» – переход в окно регистрации ТМ-идентификаторов для отключения подсистемы автозапуска ФПСУ (см. пункт «Отключение автозапуска»);
- «Переинициализация ключа ПДСЧ» – команда запуска процедуры повторной инициализации программного датчика случайных чисел (см. пункт «Переинициализация ключа ПДСЧ»);
- «Переинициализация доп. ключа ПДСЧ» – команда запуска процедуры дополнительной повторной инициализации программного датчика случайных чисел;
- «Загрузка ключа ПДСЧ из файла» – команда позволяет загрузить из файла ключ ПДСЧ, изготовленный средствами ЦВК («Загрузка ключа ПДСЧ из файла»);
- «Установка срока действия ключей» – переход в окно управления сроками действия ключевых данных ФПСУ (см. пункт «Установка срока действия ключей»);
- «Удаление СКЗИ» – запуск процедуры удаления программных модулей ФПСУ и форматирования внутреннего носителя (см. пункт «Удаление СКЗИ»).

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

7. 9. 1. Отключение автозапуска

Команда «Отключение Автозапуска» предназначена для отключения подсистемы автозапуска, если она была ранее задействована локальным администратором. Команда «Отключение Автозапуска» выполняется из пункта «Настройки СКЗИ».

Операция доступна администраторам класса *Администратор* и выше (см. пункт

«Разграничение доступа и пользователи», Таблица 3).



Рисунок 251 - Подтверждение полномочий и ввод пароля ТМ

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

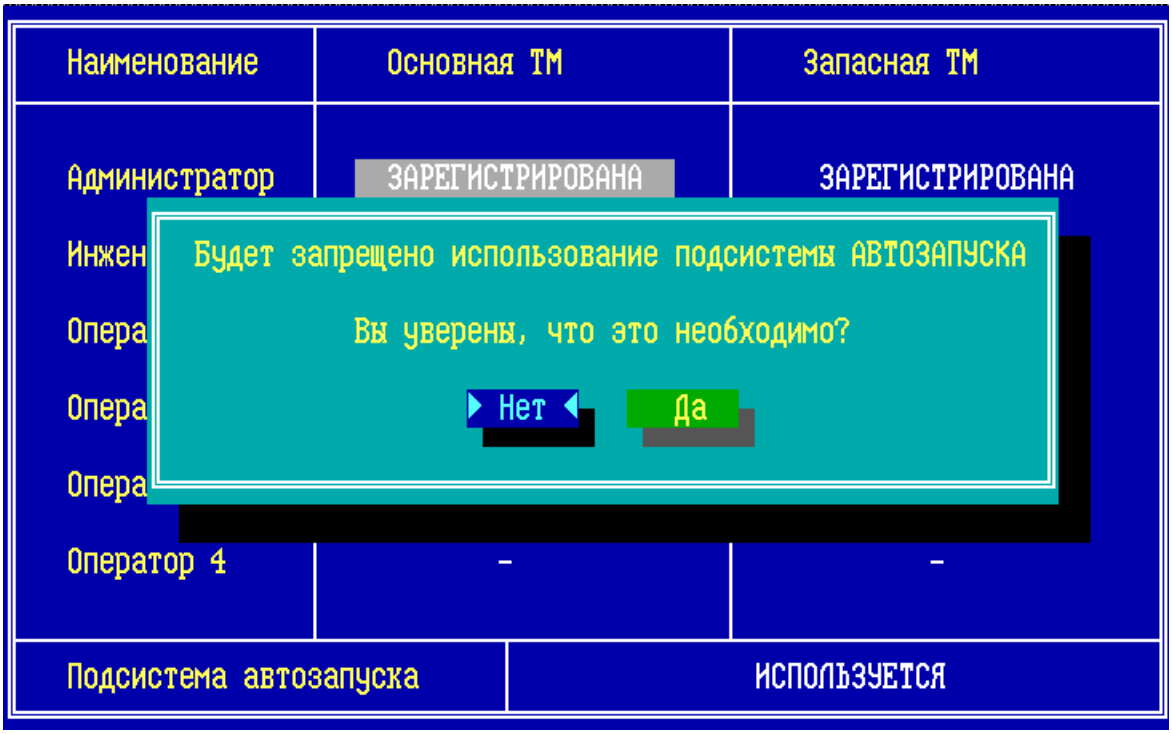


Рисунок 252 - Подтверждение отключения подсистемы автозапуска

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

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

7. 9. 2. Переинициализация ключа ПДСЧ

Команда «Переинициализация ключа ПДСЧ» подменю «Настройки СКЗИ» предназначена для повторной инициализации программного датчика случайных чисел ФПСУ средствами биологического датчика случайных чисел. Для успешного выполнения команды, к ФПСУ должен быть подключен манипулятор типа «мышь». Частота повторной инициализации программного датчика случайных чисел ФПСУ регулируется правилами пользования СКЗИ.

ВНИМАНИЕ! Программным комплексам ФПСУ, функционирующим под управлением виртуальных машин, запрещается проводить повторную инициализацию ПДСЧ средствами БиоДСЧ. Новый ключ ПДСЧ в таком случае следует загружать из файла, выданного ЦВК.



Рисунок 253 - Команда повторной инициализации ДСЧ

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 254 - Подтверждение полномочий и ввод пароля ТМ

После подтверждения полномочий запустится интерфейс биологического датчика случайных чисел. От администратора требуется двигать мышью в пределах экрана:



Рисунок 255 - Биологический датчик случайных чисел

Переинициализация ключа ПДСЧ завершится успешно, как только датчик считает достаточное для генерации ключа количество движений указателя мыши. В любой момент

до успешного завершения процесс можно отменить, вернувшись по клавише <*Esc*> обратно в подменю «Настройки СКЗИ».

7. 9. 3. Переинициализация дополнительного ключа ПДСЧ для КРК

Команда «Переинициализация доп. ключа ПДСЧ» подменю «Настройки СКЗИ» предназначена для повторной инициализации программного датчика случайных чисел ФПСУ для КРК. Дополнительный ключ ПДСЧ используется в ККС ВРК. Переинициализация дополнительного ключа ПДСЧ выполняется средствами биологического датчика случайных чисел. Для успешного выполнения команды, к ФПСУ должен быть подключен манипулятор типа «мышь». Инициализация может быть запущена несколько раз для формирования нескольких дополнительных ключей ПДСЧ для КРК. Частота повторной инициализации программного датчика случайных чисел ФПСУ для КРК регулируется правилами пользования СКЗИ.

ВНИМАНИЕ! Программным комплексам ФПСУ, функционирующим под управлением виртуальных машин, запрещается проводить инициализацию дополнительного ключа ПДСЧ для КРК средствами БиоДСЧ.



Рисунок 256 - Команда повторной инициализации ДСЧ

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 257 - Подтверждение полномочий и ввод пароля ТМ

После подтверждения полномочий в отдельном окне необходимо задать срок действия дополнительного ключа ПДСЧ для КРК, значение от 1 до 1825 дней.



Рисунок 258 - Срок действия ключа ПДСЧ

Затем запустится интерфейс биологического датчика случайных чисел. От администратора требуется двигать мышью в пределах экрана:



Рисунок 259 - Биологический датчик случайных чисел

Переинициализация дополнительного ключа ПДСЧ для КРК завершится успешно, как только датчик считает достаточное для генерации ключа количество движений указателя мыши.

В любой момент до успешного завершения процесс можно отменить, вернувшись по клавише <*Esc*> обратно в подменю «Настройки СКЗИ», в этом случае на экран будет выдано сообщение о том, что инициализация не выполнена.



Рисунок 260 - Инициализация дополнительного ключа ПДСЧ для КРК не выполнена

После успешной инициализации дополнительного ключа ПДСЧ на экран будет выдано сообщение о сгенерированном дополнительном ключе ПДСЧ для КРК (затравке) и запросе на инициализацию следующего дополнительном ключе ПДСЧ:

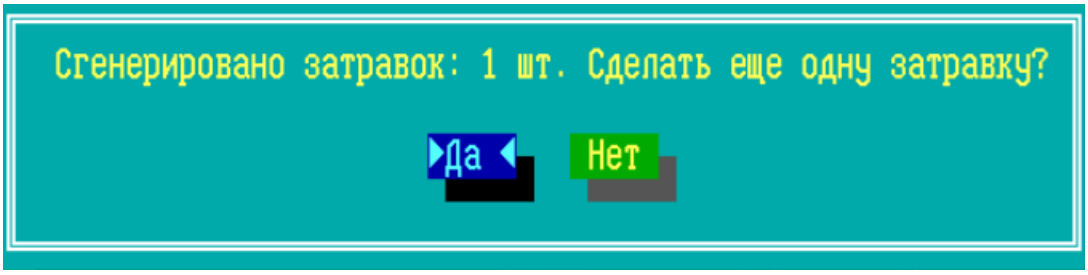


Рисунок 261 - Инициализация дополнительного ключа ПДСЧ для КРК выполнена

При завершении процедуры инициализации дополнительного ключа ПДСЧ, по нажатию кнопка *«Да»* запустится процесс инициализации следующего дополнительного ключа ПДСЧ. При нажатии кнопки *«Нет»* в сообщении о запросе на инициализацию будет осуществлен выход обратно в подменю «Настройки СКЗИ».

При активации команды меню «Переинициализация доп. ключа ПДСЧ» в случае, если дополнительные ключи ПДСЧ сгенерированы, на экран будет выдано сообщение с возможностью их удалить:



Рисунок 262 - Возможность удаления дополнительных ключей ПДСЧ для КРК

По нажатию кнопка *«Да»* дополнительные ключи ПДСЧ будут удалены. При нажатии кнопки *«Нет»* или клавиши *<Esc>* запустится процесс инициализации следующего дополнительного ключа ПДСЧ.

7. 9. 4. Загрузка ключа ПДСЧ из файла

Загрузка ключа ПДСЧ из файла, изготовленного средствами ЦВК, производится для программных комплексов ФПСУ, функционирующих под управлением виртуальных машин и программно-аппаратных комплексов ФПСУ, где не используется БиоДСЧ. Частота загрузки ключа ПДСЧ из файла на ФПСУ регулируется правилами пользования СКЗИ.

Подключите к ФПСУ USB-носитель с файлом ключа ПДСЧ и выберите команду меню «Загрузка ключа ПДСЧ из файла» подменю «Настройки СКЗИ»:

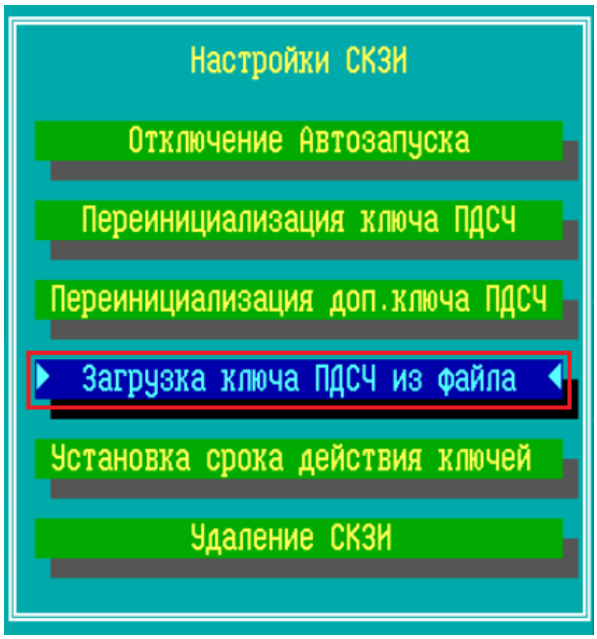


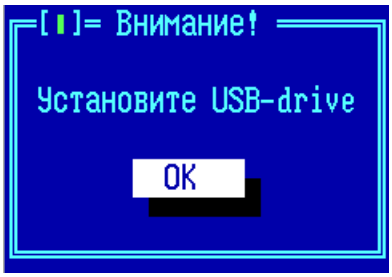
Рисунок 263 - Команда «Загрузка ПДСЧ из файла»

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 264 - Подтверждение полномочий и ввод пароля ТМ

После подтверждения полномочий и ввода пароля ТМ, если USB-носитель предварительно не подключен, то система предложит подключить к ФПСУ USB-носитель с файлом ключа ПДСЧ. Подключите носитель к ФПСУ и подтвердите выполнение команды, нажав клавишу Enter.



Если USB-носитель будет обнаружен ФПСУ, то откроется окно диалога, в котором следует выбрать файл на носителе.

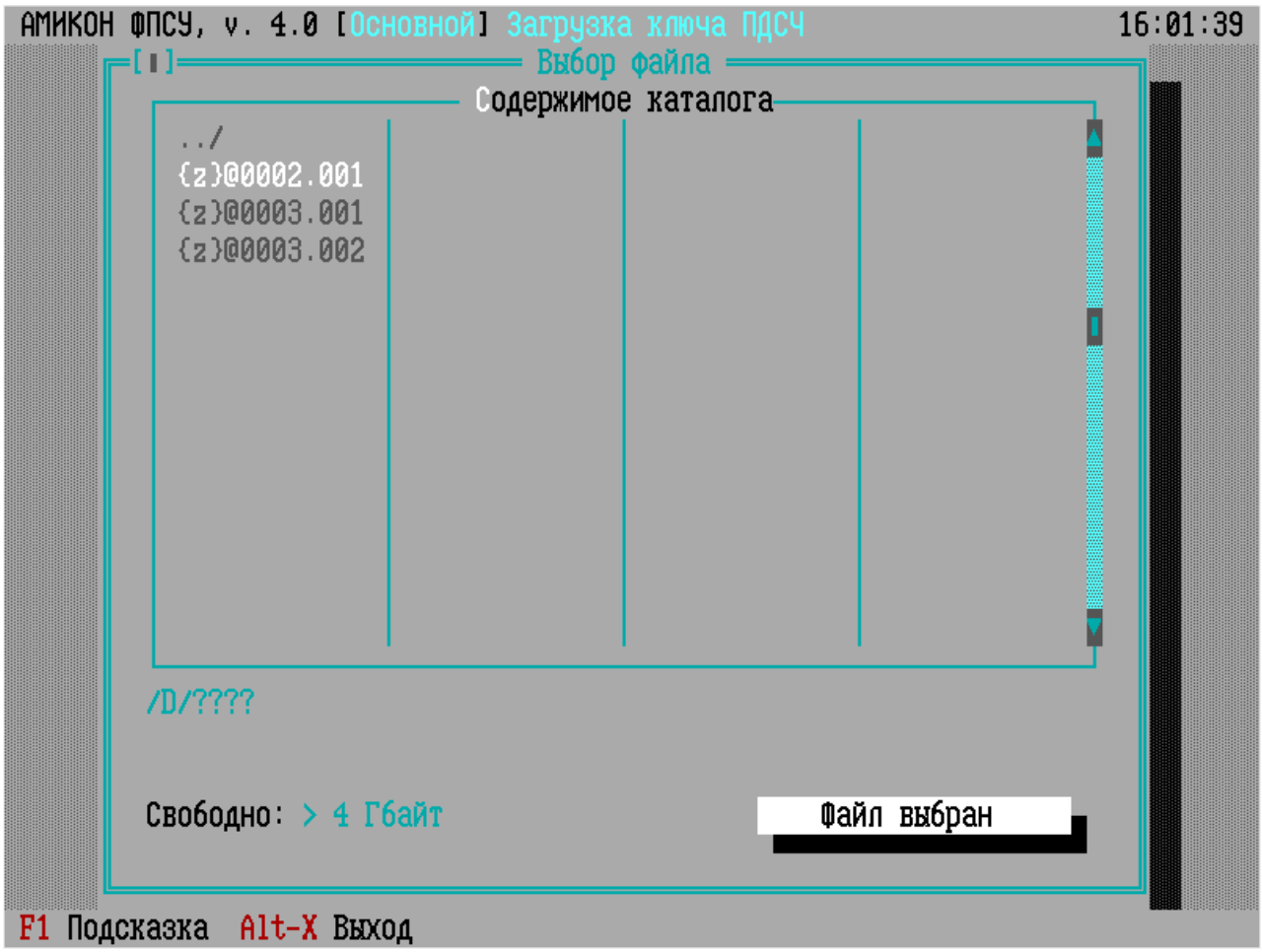


Рисунок 265 - Выбор файла для загрузки

Переместите курсор на выбранный файл. Переход на кнопку «Файл выбран» осуществляется клавишей <*Tab*>. Подтвердите выбор файла, нажав на клавишу <*Enter*>. В открывшемся окне отобразятся информация о файле с ключом ПДСЧ, изготовленным средствами ЦВК, и предложение загрузить этот файл.

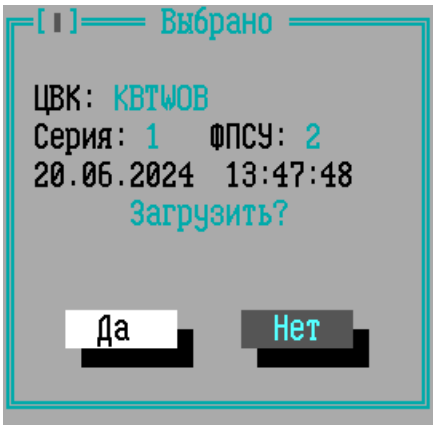


Рисунок 266 - Информация о загружаемом файле

После загрузки файла, ФПСУ выдаст системное оповещение о завершении процедуры:

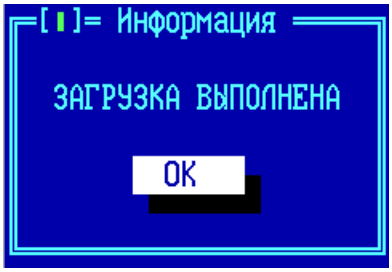


Рисунок 267 - Файл загружен

7. 9. 5. Установка срока действия ключей

Команда «Установка срока действия ключей» меню «Настройки СКЗИ» позволяет администратору ФПСУ устанавливать временное ограничение на использование ключа запуска, ключа ПДСЧ и ключа горячего резерва ФПСУ. Эта команда обеспечивает возможность настройки программного обеспечения в соответствии с требованиями правил пользования СКЗИ.

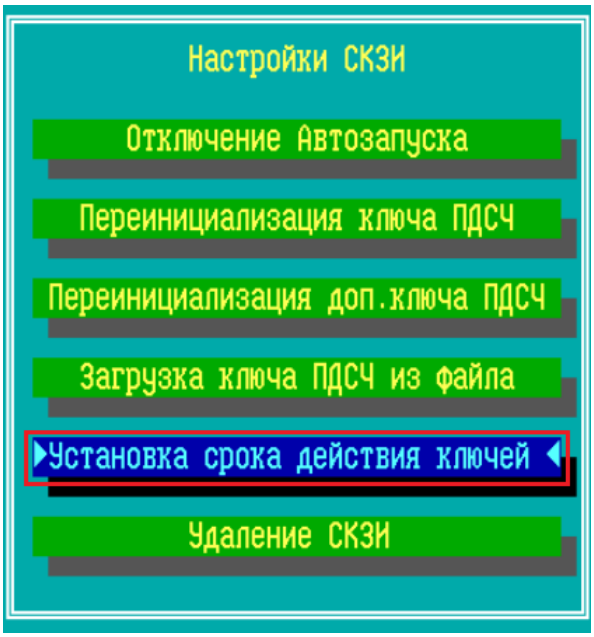


Рисунок 268 - Команда «Установка срока действия ключей»

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 269 - Подтверждение полномочий и ввод пароля ТМ

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

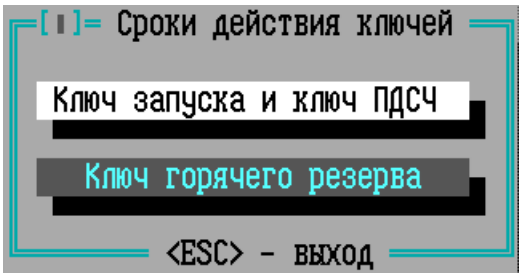


Рисунок 270 - Выбор типа ключа

При выборе пункта меню «Ключ запуска и ключ ПДСЧ» или «Ключ горячего резерва» открывается окно настроек сроков действия выбранных ключей, в котором указывается дата создания ключа и текущие настройки.

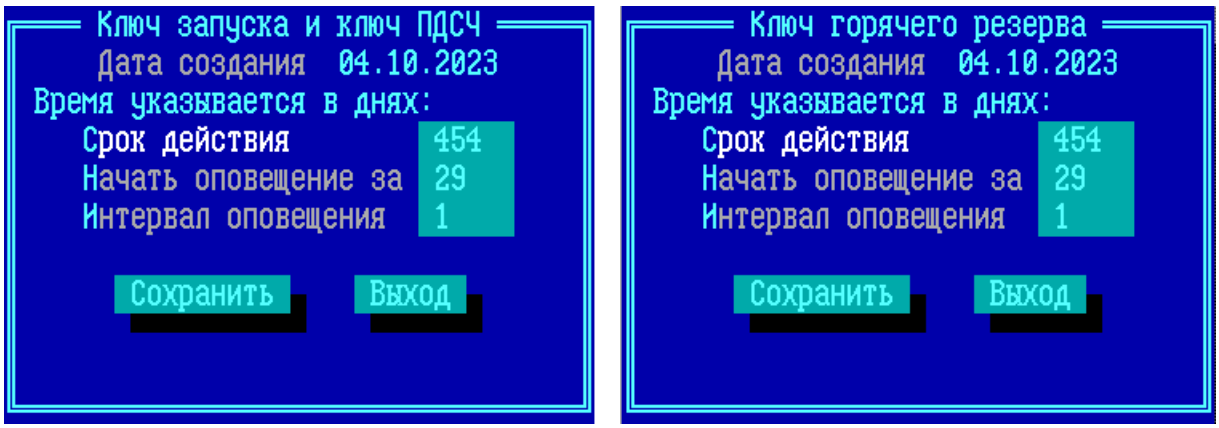


Рисунок 271 - Настройка сроков действия выбранного ключа

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 будет при запуске ФПСУ выводится сообщение о приближающемся окончании срока действия ключа;

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

Сохранение параметров выполняется по нажатию кнопки «Сохранить».

После определения сроков действия ключей начинается обратный отсчет дней, начиная с даты создания ключей. При наступлении срока оповещения администратору будет выдаваться сообщение об истечении срока действия ключа с заданным интервалом.

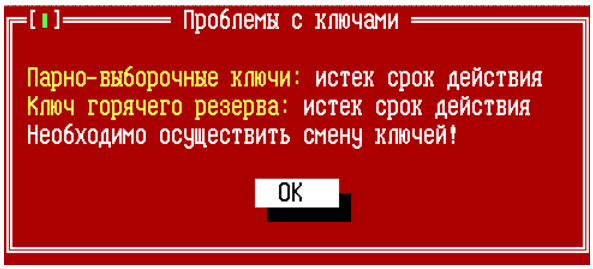


Рисунок 272 - Настройка сроков действия выбранного ключа

В случае получения оповещения необходимо сменить ключи (см. пункты «Переинициализация ключа ПДСЧ» и «Замена ключа горячего резерва»).

8. 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.

Маршрутизация на портах может задаваться статически в конфигурации, а может быть получена с помощью протоколов динамической маршрутизации. Далее описываются настройки для статической маршрутизации. Описание работы с динамической маршрутизацией находится в разделе «Динамическая маршрутизация OSPF».

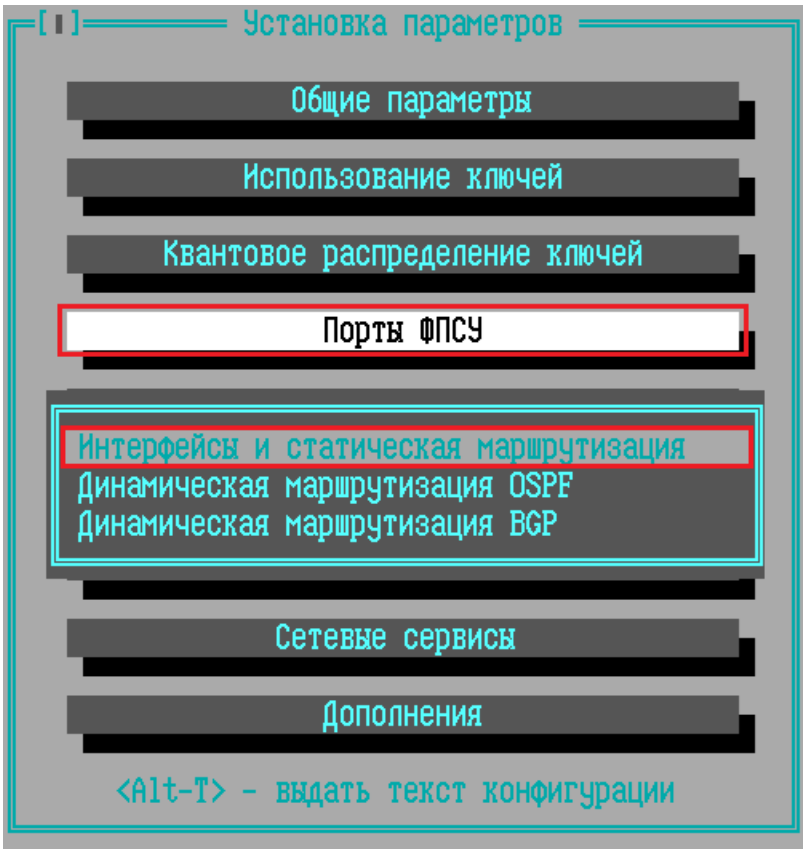


Рисунок 273 - Меню конфигурации ФПСУ

Основной блок настроек выполняется в пункте **Интерфейсы и статическая маршрутизация**.

При использовании статической маршрутизации для каждого рабочего порта ФПСУ необходимо:

- создать список абонентов, которым разрешается подключаться к ФПСУ со стороны этого порта;
- указать ФПСУ, с которыми будут устанавливаться VPN-туннели;

- указать маршрутизаторы, через которые абоненты будут доступны;
- установить правила работы абонентов, маршрутизаторов, VPN-туннелей.

ФПСУ 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 производиться не будет.

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



Рисунок 274 - Порты ФПСУ

По умолчанию выводится две строки для двух рабочих портов. Для добавления описателя порта нажмите клавишу <Ins>. Для удаления описателя порта нажмите клавишу <Del>.

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, какой адаптер связан с каким сегментом IP-сети.

Для каждого рабочего порта необходимо указать:

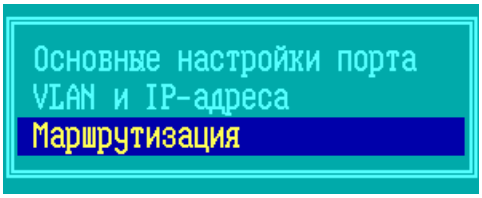


Рисунок 275 - Настройки порта ФПСУ

- Описание основных настроек порта;
- Описание VLAN и IP-адресов порта;
- Описание маршрутизации порта.

8. 1. Описание основных настроек порта

Для основной настройки порта необходимо определить будет ли являться данный порт внутренним, со стороны которого будет подключена защищаемая локальная сеть, или внешним, со стороны которого будет подключена открытая (не защищённая) сеть передачи данных, каким будет IP-адрес порта – задан статически или получен динамически по протоколу DHCP.

Передвижение по полям окна осуществляется клавишами <↓>, <↑>, <*Enter*> (движение вперед).

Окно содержит следующие параметры порта ФПСУ:

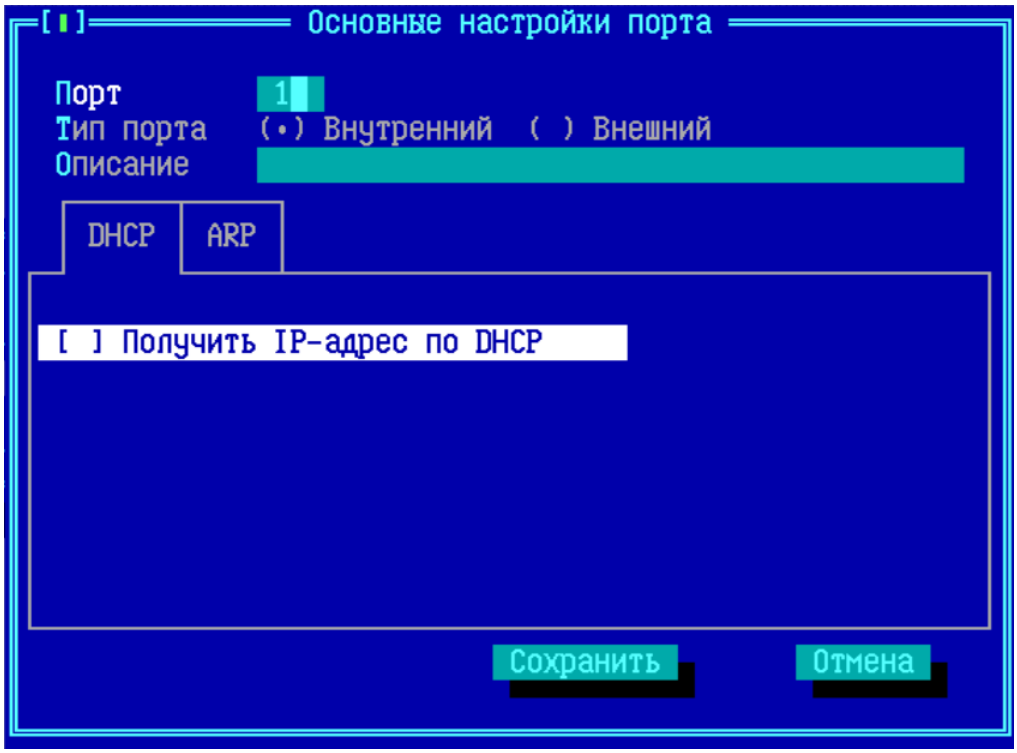


Рисунок 276 - Основные настройки порта ФПСУ

Порт **–** справочный параметр, номер порта, соответствующий номеру LAN-адаптера (присвоенному LAN-адаптеру при конфигурировании), который осуществляет взаимодействие с сетью передачи данных со стороны описываемого порта.

Описание **–** имя порта, текстовое описание.

Тип порта **–** указатель на значимость порта по отношению к режиму работы *«Запрет открытых соединений»* (см. пункт «Общие параметры конфигурации ФПСУ»). Внутренний порт логически обозначает сетевой интерфейс, к которому подключается защищаемая

локальная сеть, к внешнему порту подключается открытая (не защищённая) сеть передачи данных, например, Internet/Intranet. При включенном режиме *«Запрет открытых соединений»* автоматически не допускаются открытые (без шифрования) соединения абонентов внутреннего порта с абонентами внешнего порта ФПСУ. Если оба порта ФПСУ помечены как «Внутренние», то открытые соединения абонентов через ФПСУ 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 следует:

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

Получить IP-адрес по DHCP – установленный флаг разрешает автоматическое получение IP-адреса по протоколу DHCP.

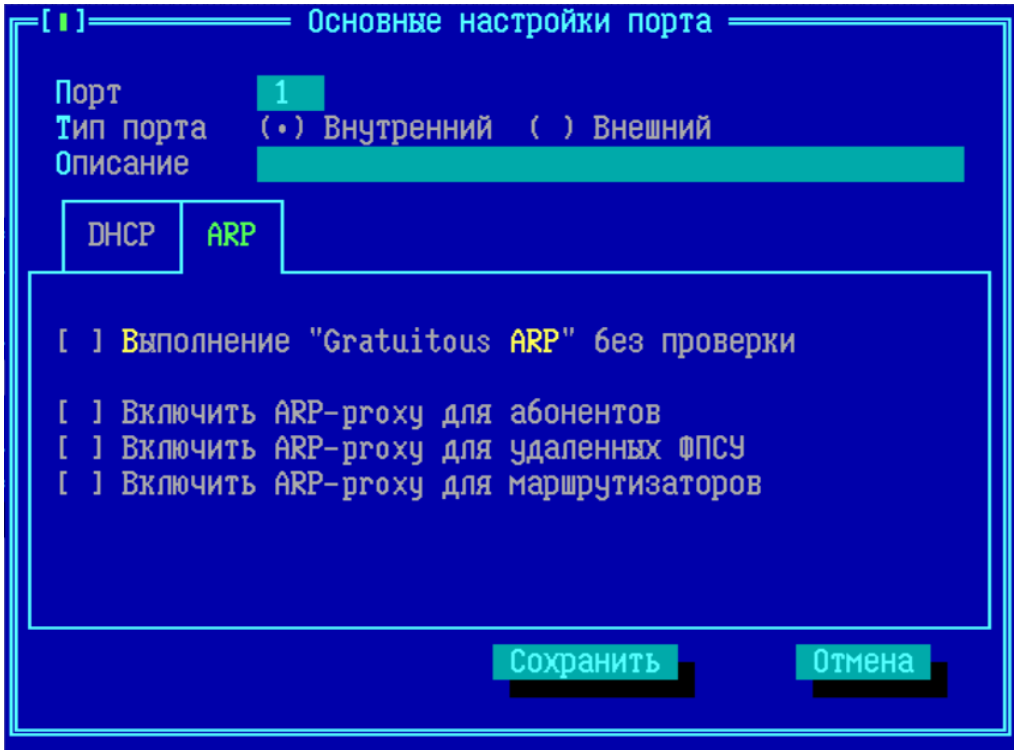


Рисунок 277 - Основные настройки порта ФПСУ на вкладке ARP

Выполнение «Gratuitous ARP» без проверки – способ обработки принятого «Gratuitous ARP» запроса/ответа. При снятом флаге ФПСУ 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 разрешено сразу изменить значение MAC-адреса в таблице ARP.

Флаги ***Включить ARP-proxy ...*** задействуются только в случае, если флаг ***Отключить <ARP-proxy>*** в общих параметрах конфигурации выключен (см. пункт «Общие параметры конфигурации ФПСУ», вкладка ARP, флаг ***Отключить <ARP-proxy>***).

Включить ARP-proxy для абонентов – флаг, разрешающий ARP-публикацию аппаратных адресов абонентов, описанных со стороны данного порта ФПСУ, в локальную сеть со стороны других портов.

Включить ARP-proxy для удаленных ФПСУ – флаг, разрешающий ARP-публикацию аппаратных адресов удаленных ФПСУ, описанных со стороны данного порта ФПСУ, в локальную сеть со стороны других портов.

Включить ARP-proxy для маршрутизаторов – флаг, разрешающий ARP-публикацию аппаратных адресов маршрутизаторов, описанных со стороны данного порта ФПСУ, в локальную сеть со стороны других портов.

8. 2. Описание VLAN и IP-адресов порта

В открывшемся окне находится список VLAN, в которых участвует данный порт ФПСУ.

По умолчанию подсистема VLAN на ФПСУ не сконфигурирована и указанный в списке «Без VLAN» IP-адрес порта не участвует в VLAN.

В одном описателе VLAN допустимо описать не более 8 IP-адресов, на порту - не более 128 IP-адресов всего, на порту - не более 128 VLAN.

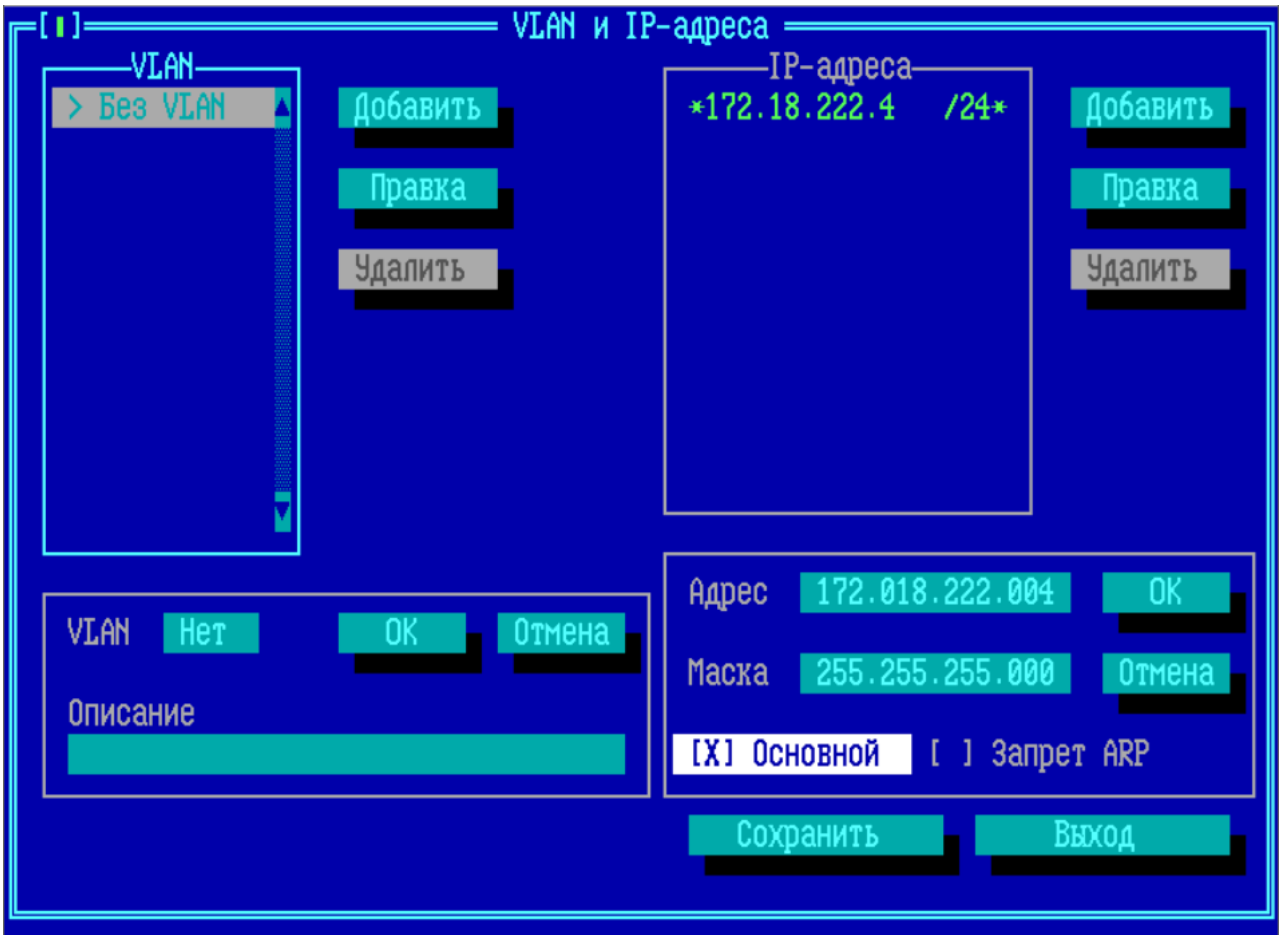


Рисунок 278 - Настройки VLAN и IP-адресов порта ФПСУ

Для добавления описателя VLAN следует нажать кнопку *«Добавить»* рядом со списком VLAN или клавишу <*Ins*> в списке и указать требуемые параметры:

VLAN – идентификатор описываемого VLAN. Указывает, какому VLAN принадлежит фрейм, допустимые значения идентификатора от 2 до 4090.

Описание – имя порта, текстовое описание.

Для сохранения в список VLAN порта нового описателя нажмите кнопку *«ОК»* или клавишу <*F2*>. Для отмены действия нажмите клавишу <*Esc*> или кнопку *«Отмена»*.

Для добавления IP-адреса к описателю VLAN следует нажать кнопку *«Добавить»* рядом со списком IP-адресов или клавишу <*Ins*> в списке, и указать требуемые параметры:

Адрес – IP-адрес порта ФПСУ в описываемом VLAN.

Маска – маска IP-адреса порта ФПСУ в описываемом VLAN, IP-маска в представлении «dotted-decimal» подсети. Введите значение рассчитанной маски

непосредственно или выделите поле ввода и нажмите <*Пробел*>, после чего введите в появившемся окне число необходимых значащих разрядов (от 1 до 30), в таком случае ФПСУ рассчитает значение маски автоматически.



Рисунок 279 - Ввод числа необходимых разрядов

***Основной адрес* —** адрес используемый по умолчанию для данного VLAN.

***Запрет ARP* –** установленный флаг активирует запрет публикации и ответа ARP при старте, и каждые 10 минут анонс ARP при работе.

Для сохранения IP-адреса в список нажмите кнопку *«ОК»* или клавишу <*F2*>. Для отмены действия нажмите клавишу <*Esc*> или кнопку *«Отмена»*.

Для выбранного описателя VLAN отображается список IP-адресов, выбранный описатель дополнительно выделен цветом и отмечен знаком «<>» в списке.

В списке IP-адресов адрес, используемый по умолчанию для данного VLAN, отмечен знаком «*».

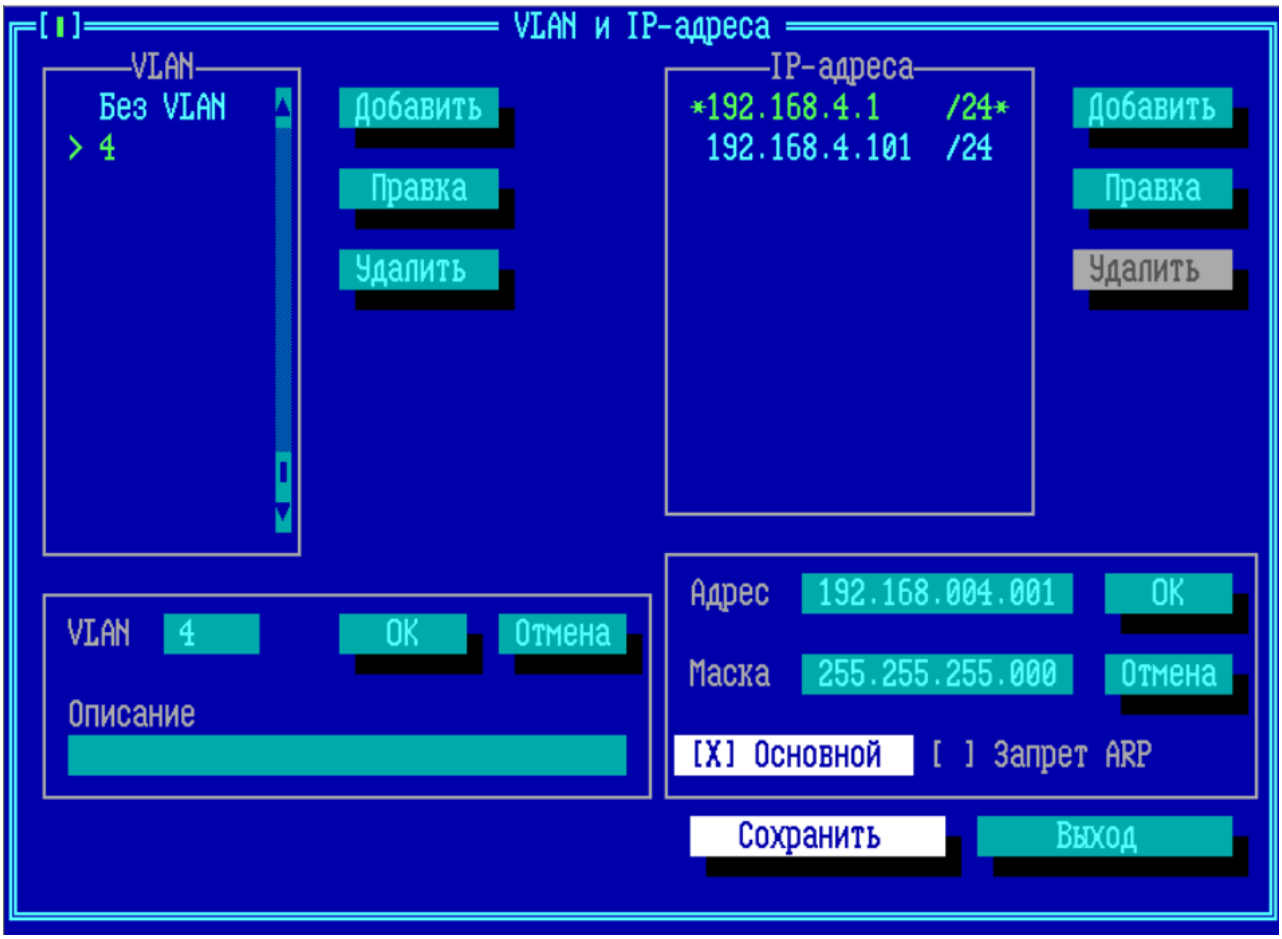


Рисунок 280 - Настройки VLAN и IP-адресов порта ФПСУ

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

8. 3. Описание маршрутизации порта

При первом запуске подсистемы конфигурирования порта таблица параметров будет пустой. В диалоговом окне настроек порта указываются сетевые параметры соседних маршрутизаторов, соседних ФПСУ и абонентов.

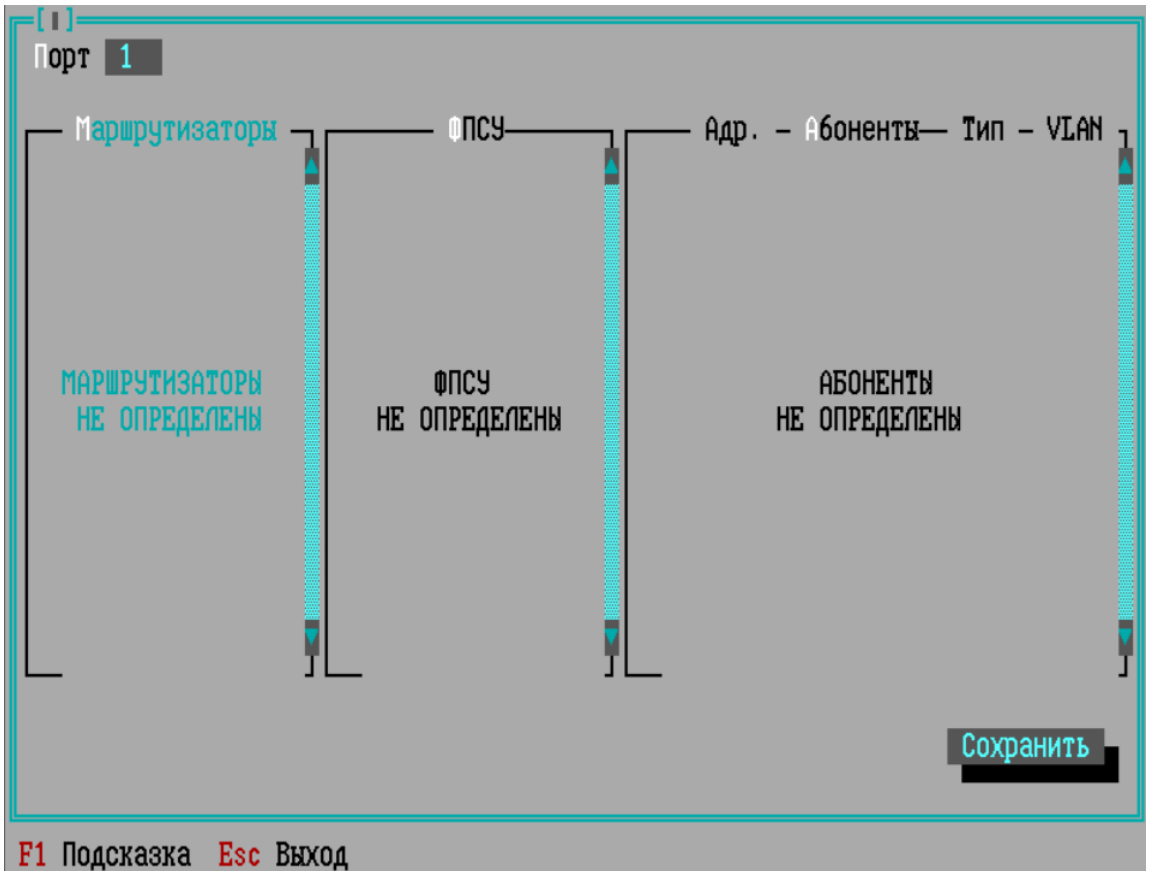


Рисунок 281 - Настройки маршрутизации порта ФПСУ

Передвижение по полю со списком параметров осуществляется по нажатию клавиш <Tab> или <→> и обратно по нажатию клавиши <←>.

Окно содержит следующие параметры порта ФПСУ:

Порт – информационное поле с номером порта, соответствующего номеру LAN-адаптера (присвоенному LAN-адаптеру при конфигурировании), который осуществляет взаимодействие с сетью передачи данных со стороны описываемого порта.

Маршрутизаторы – список описателей маршрутизаторов, через которые будут доступны абоненты или другие ФПСУ со стороны данного порта, подробно о настройке в пункте «Описание параметров используемых маршрутизаторов».

ФПСУ – список описателей ФПСУ, которые будут участвовать в создании VPN-туннелей передачи данных между защищаемыми ими абонентами (сетями) и абонентами настраиваемого ФПСУ, подробно о настройке в пункте «Описание параметров туннелей с другими ФПСУ».

Абоненты – список описателей абонентов со стороны данного порта ФПСУ, для которых будет разрешен обмен пакетами с другими абонентами ФПСУ, подробно о настройке в пункте «Описание параметров абонентов».

8. 3. 1. Описание параметров используемых маршрутизаторов

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

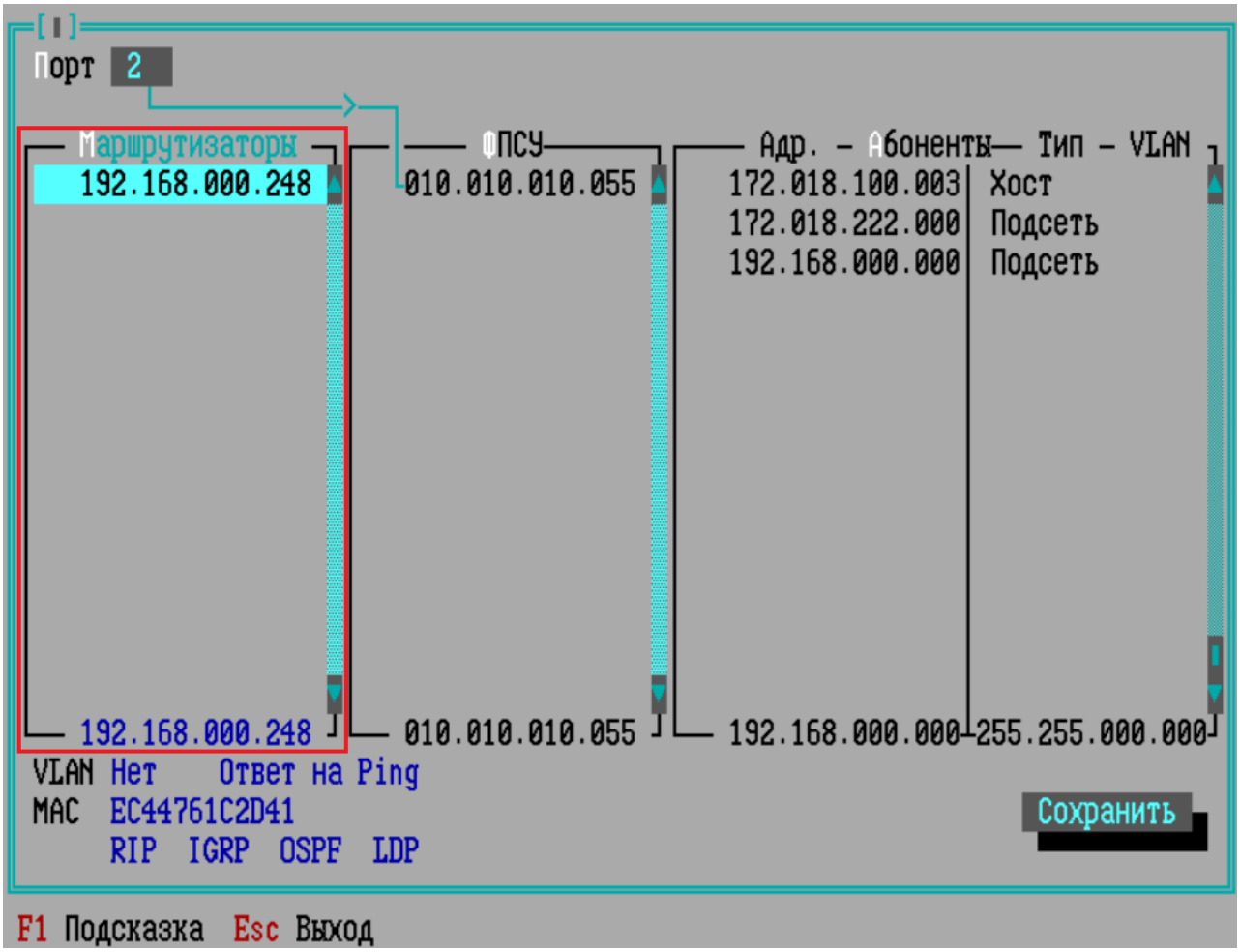


Рисунок 282 - Маршрутизаторы порта ФПСУ

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

- если они являются пограничными (то есть расположены между описываемым портом ФПСУ 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);

- если необходимо пропускать через сообщения протоколов маршрутизации, исходящих от маршрутизаторов, находящихся со стороны разных портов ФПСУ;
- если ФПСУ 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 ICMP-сообщений переадресации (Redirect) от уполномоченных маршрутизаторов;
- если рабочие станции защищаемых областей будут осуществлять управление этими маршрутизаторами (только для ФПСУ с более ранними версиями программного обеспечения, чем 3.0, см. раздел «DHCP-Relay»).

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

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:

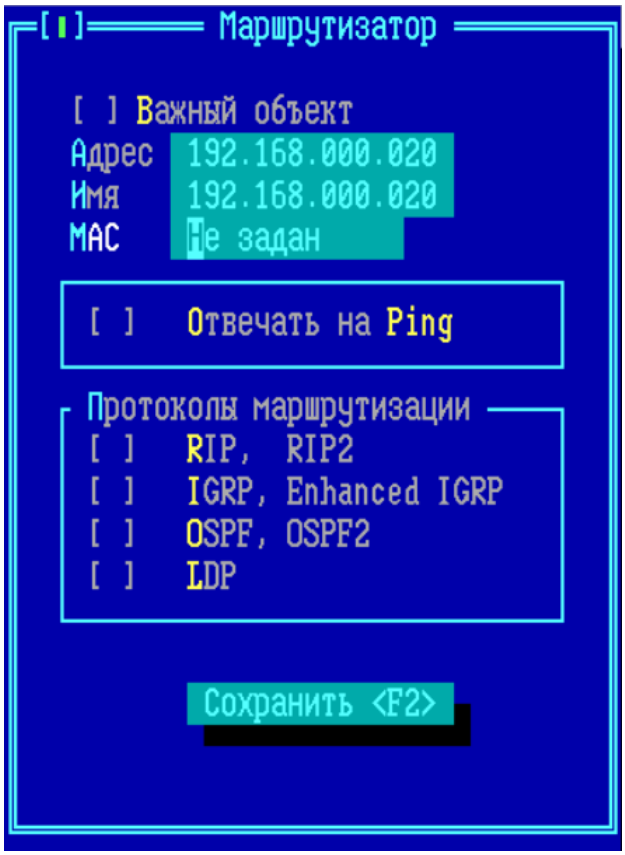


Рисунок 283 - Параметры маршрутизатора

Важный объект – флаг в положении «включено» запрещает удалять описание маршрутизатора из интерфейса портов ФПСУ. 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;

Имя – название маршрутизатора, которое будет отображаться в списке;

MAC – аппаратный адрес порта маршрутизатора, связанного с ФПСУ.

Отвечать на Ping - указание для ФПСУ: отвечать на ICMP (ECHO) запросы, направленные от описываемого маршрутизатора в IP-адреса портов конфигурируемого ФПСУ. Отметка (разрешение отвечать на запросы) производится по нажатию клавиши <*Пробел*>. ВНИМАНИЕ! ФПСУ 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.

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! При включении на ФПСУ протокола динамической маршрутизации OSPF необходимо отключить флаги «Протоколы маршрутизации» в описываемых на портах маршрутизаторах.

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

В случае, когда на ФПСУ задействовано два рабочих порта (см. пункт «Порты ФПСУ»), можно использовать блок настроек в окне описателя «Маршрутизатор» для фильтрации и пересылки протоколов маршрутизации RIP, RIP2, IGRP, EIGRP, OSPF, OSPF2, LDP. Динамическая маршрутизация протокола OSPF должна быть выключена (см. пункт «Динамическая маршрутизация OSPF»).

Если на ФПСУ задействовано более двух рабочих портов, данный блок настроек не используется и пакеты протоколов маршрутизации не пересылаются согласно указанным в блоке флагам. Для фильтрации и пересылки протоколов маршрутизации в таком случае следует использовать правила межсетевого экрана (см. пункт «Параметры доступа, правила трафика межсетевого экрана»).

Для пересылки пакетов протоколов маршрутизации RIP, RIP2, IGRP, EIGRP, OSPF, OSPF2, LDP в маршрутизаторе с одного порта на другой существует ещё один способ - описать маршрутизатор на порту ФПСУ в качестве абонента, в этом случае флаги протоколы маршрутизации для данного маршрутизатора должны быть сняты, правила межсетевого экрана не используются (см. пункт «Описание абонента «Хост»»).

В случае, когда необходимо обеспечить работу с указанным маршрутизатором по другим протоколам (отличным от указанных в области «Протоколы маршрутизации»), потребуется дополнительно описать маршрутизатор абонентом записью типа «Хост» (подробнее см. пункт «Описание абонента «Хост»»).

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

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

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

8. 3. 2. Описание параметров туннелей с другими ФПСУ

В поле ***ФПСУ*** окна параметров порта необходимо описать все другие ФПСУ, которые будут участвовать в создании VPN-туннелей передачи данных между защищаемыми ими абонентами (сетями) и абонентами настраиваемого ФПСУ.

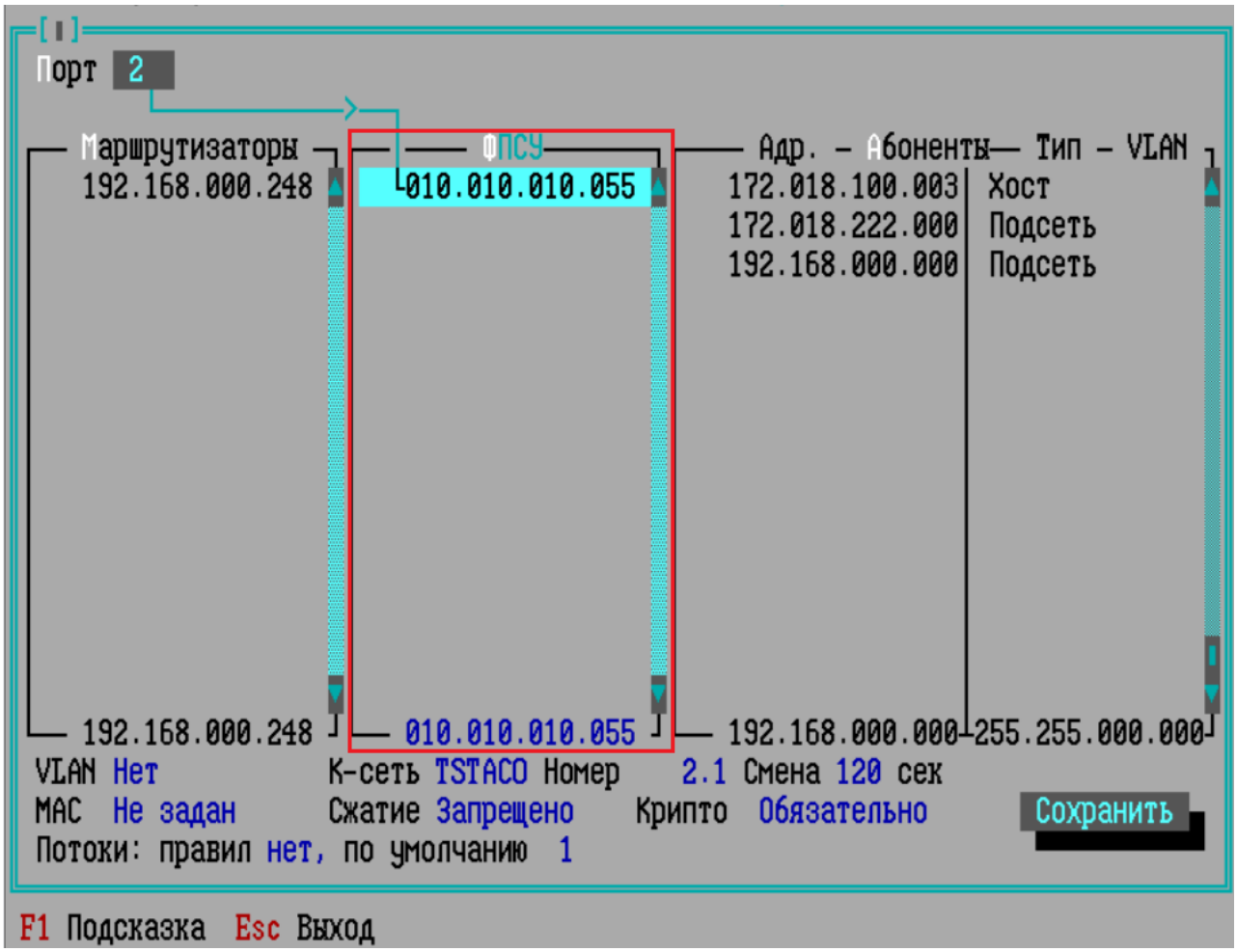


Рисунок 284 - Описатели удаленных ФПСУ порта

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

Максимальное количество ФПСУ, которое может быть описано на порту, – 1024.

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

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

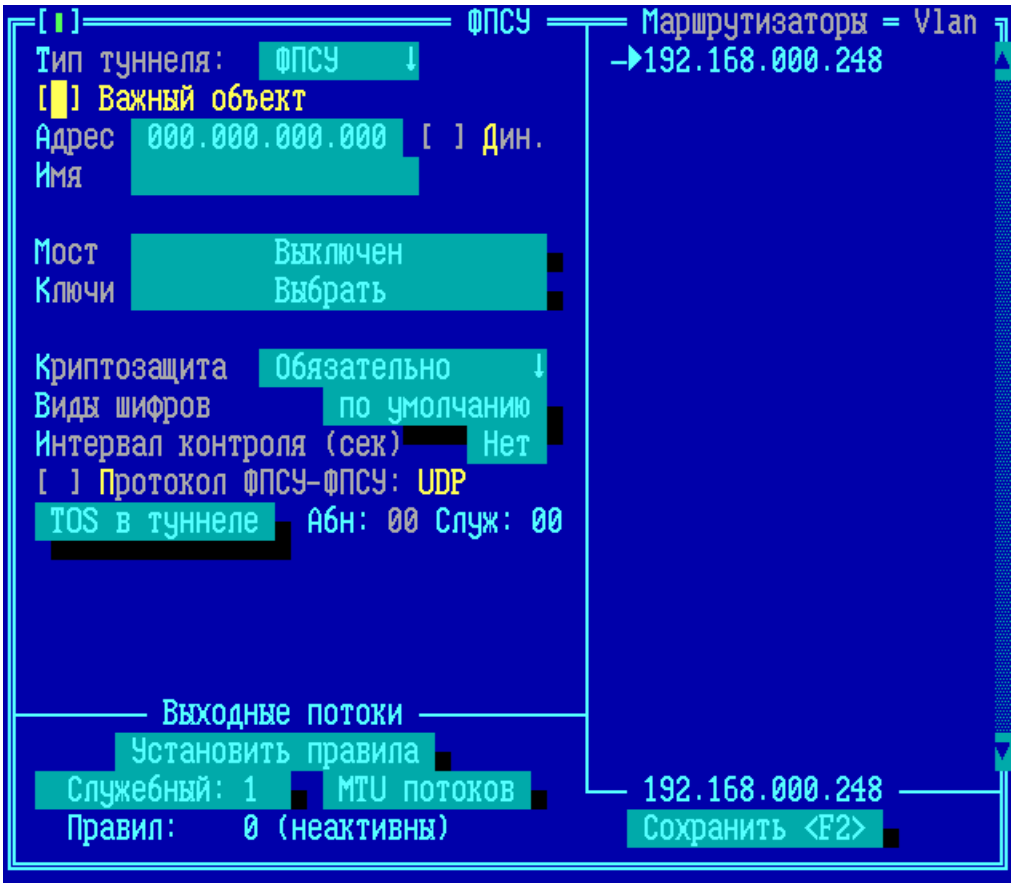


Рисунок 285 - Настройка удаленного ФПСУ

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

Имя **–** символьное имя этого ФПСУ, оно будет отображаться в списке ФПСУ 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, будут применяться в процессе шифрования.

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

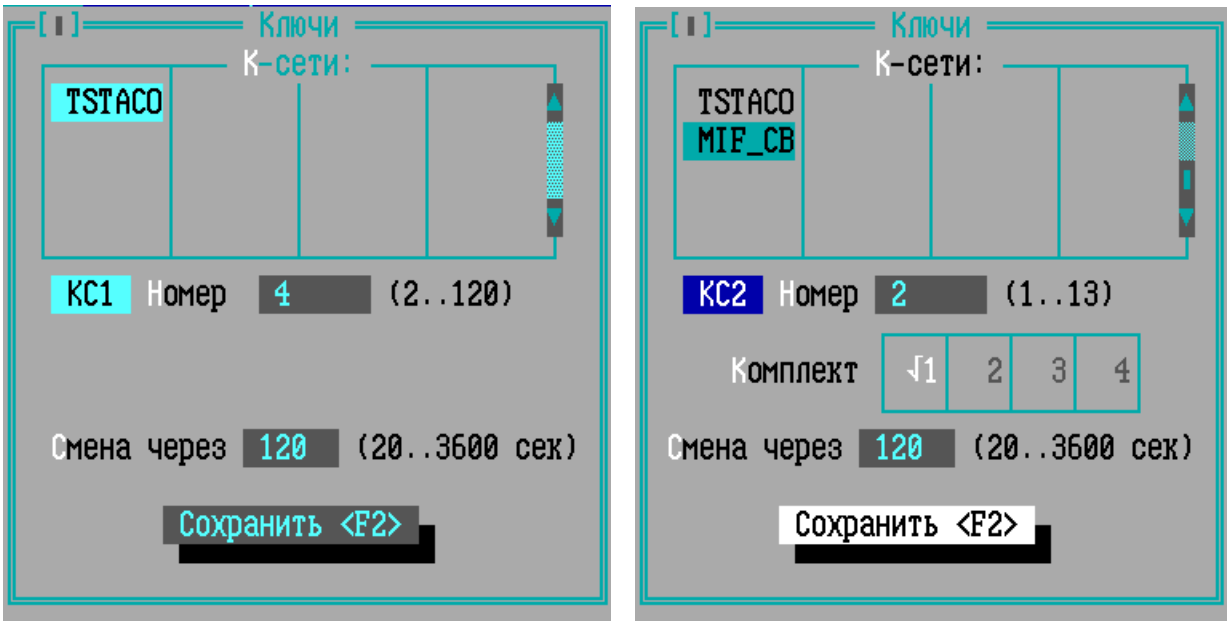


Рисунок 286 - Указание ключевых данных партнера

Определите время, по истечении которого при взаимодействии другого ФПСУ с конфигурируемым на основе выделенных ключей парно-выборочной связи будут вырабатываться новые сеансовые ключи (от 20 до 3600 секунд). Фактически, это время является временем проверки работоспособности VPN-соединения между двумя ФПСУ, 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).

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

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

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

ФПСУ из списка можно приписывать к различным маршрутизаторам, регламентируя тем самым нагрузку на маршрутизаторы. Следует особо отметить ситуацию, когда конфигурируемый ФПСУ имеет несколько смежных маршрутизаторов, которые могут

направлять ему ICMP-сообщения переадресации (Redirect) на другой маршрутизатор. Эти сообщения будут учитываться ФПСУ следующим образом:

- если в поле «Маршрутизаторы» при описании параметров работы конфигурируемого порта с удаленным ФПСУ ни один маршрутизатор не отмечен (символом «→»), сообщение переадресации принимается ФПСУ 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 (символом «→») 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 должно быть указано как минимум два маршрутизатора).

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

Отметить маршрутизатор символом «→» можно по нажатию клавиши <*Пробел*> на строке с выбранным маршрутизатором.

VLAN **–** справочный параметр, номер виртуальной локальной сети, в которой участвует маршрутизатор.

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

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

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

8. 3. 2. 1. Дополнительные параметры соединения ФПСУ-ФПСУ

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

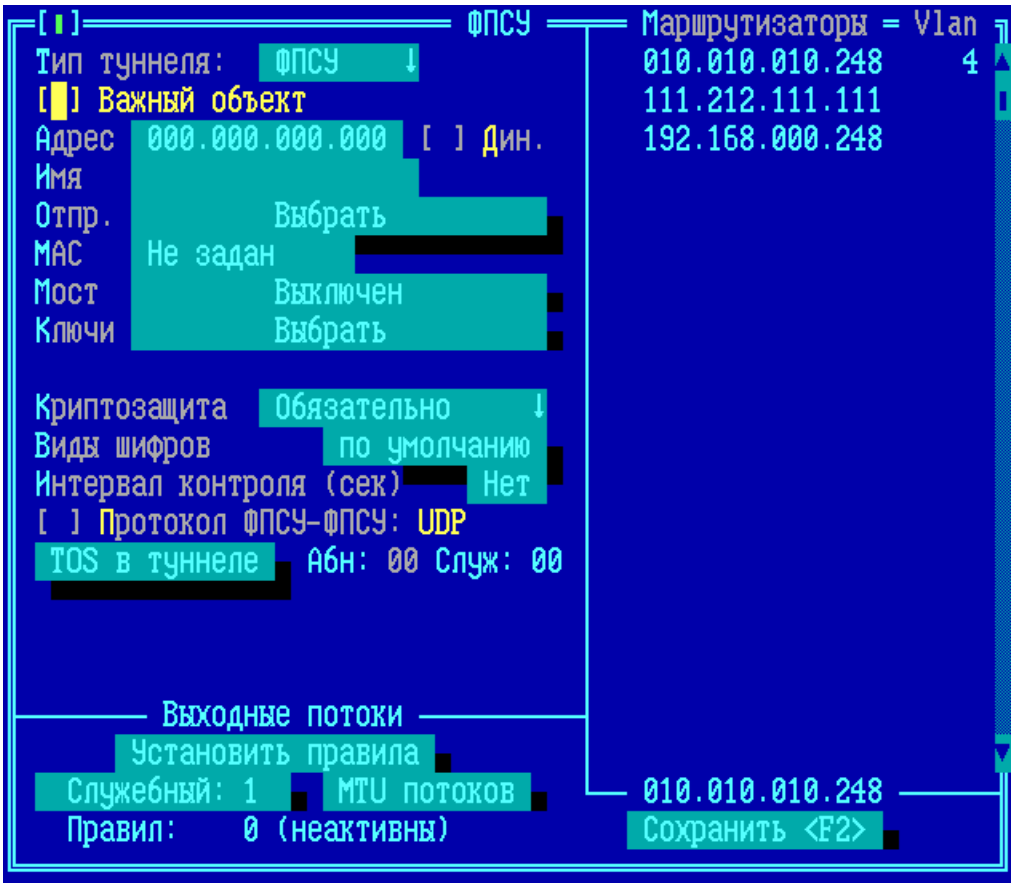


Рисунок 287 - Настройка удаленного ФПСУ

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

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

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

Отправитель – один из вторичных адресов порта, который подставляется в поле source при отправке пакета в сеть.

MAC – аппаратный адрес порта ФПСУ.

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

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

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

Интервал контроля (сек) – период контроля туннеля, параметр задается для поддержания соединения между двумя соседними ФПСУ, когда в туннеле нет трафика. С заданной периодичностью оба ФПСУ отправляют служебные сообщения навстречу друг другу; отправка контрольных пакетов осуществляется, если в течении четверти времени от заданного интервала контроля не было отправлено каких-либо пакетов; количество контрольных пакетов составляет «интервал контроля/4». Если ни одно сообщение не получено в течении интервала контроля, туннель сбрасывается в состояние пересоединения. Разрывает соединение тот ФПСУ, на котором истек таймер, инициирует пересоединение не получивший пакеты ФПСУ. Если оба ФПСУ не получили пакеты, то оба ФПСУ одновременно будут инициировать пересоединение. Период контроля туннеля можно настраивать только на одном ФПСУ, соседний ФПСУ, с которым установлен туннель, начнет отправлять сообщения автоматически. Если на соседних ФПСУ указан разный период контроля туннеля, то сообщения будут отправляться с минимальным периодом из двух. Контроль туннеля поддерживается только тогда, когда на обоих соседних ФПСУ установлена версия программного обеспечения 4 или выше.

Пример: Задан интервал контроля 20 секунд. Если в туннеле нет трафика в течении 5 секунд, то будет отправлено 5 пакетов. Если за 20 секунд ни один пакет не дошел до соседнего ФПСУ, то туннель сбрасывается в состояние пересоединения.

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

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

Абн (абоненты) – настройки типа обслуживания для пользовательского трафика (весь

трафик, кроме служебных соединений между ФПСУ);
Служ (службы) – настройки типа обслуживания для служебного трафика (служебные соединения между ФПСУ).

В пакетах абонентов – настройки для пользовательского трафика:

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

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

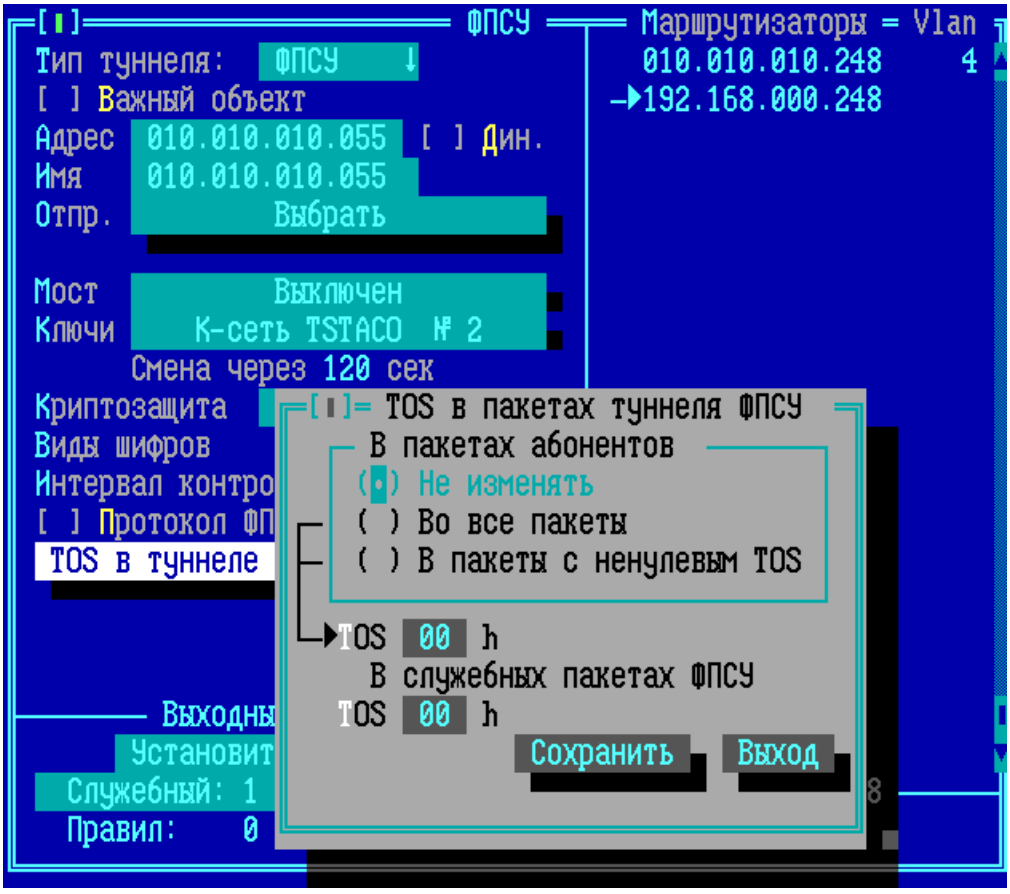


Рисунок 288 - Настройка типа обслуживания в туннеле

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

Дополнительно устанавливаются параметры для потоков данных в туннеле между ФПСУ:

Выходные потоки - правила разделения поступающих в VPN-туннель между ФПСУ 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 с удаленным партнером.

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

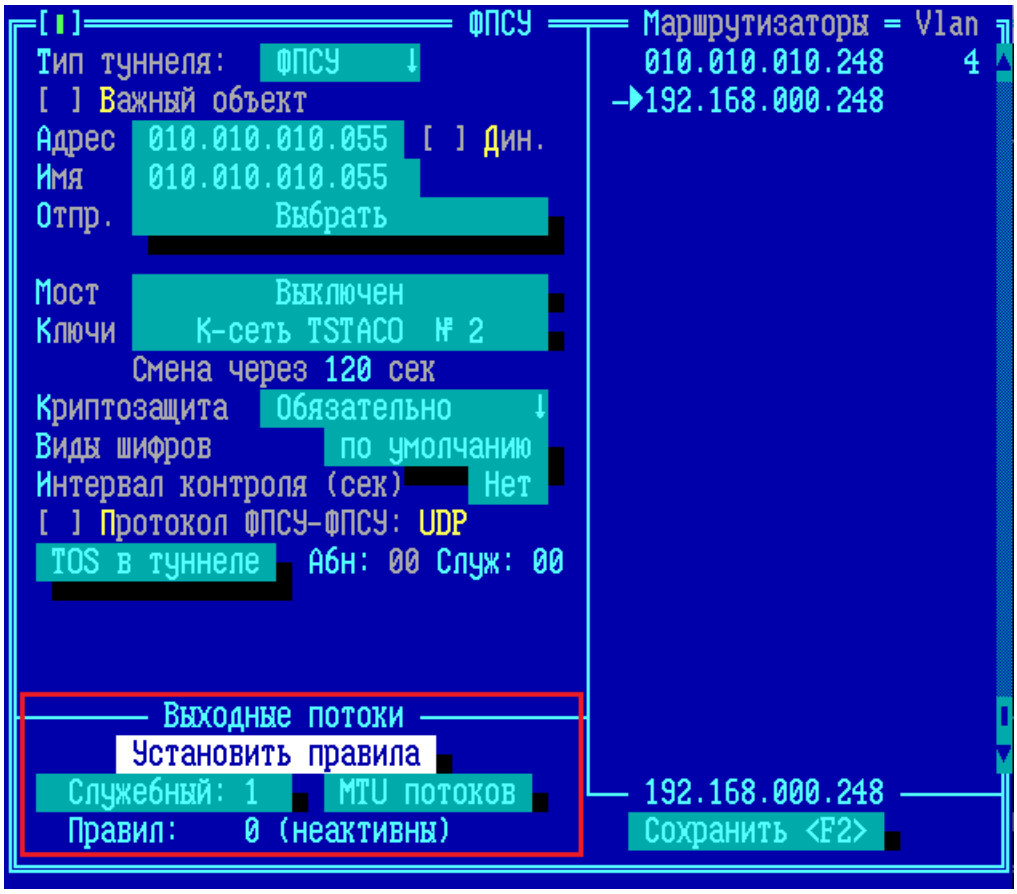


Рисунок 289 - Поле настроек выходных потоков в туннеле между ФПСУ

На экран будет выдано окно, содержащее список правил разделения потоков для VPN туннеля между конфигурируемым ФПСУ 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*»:

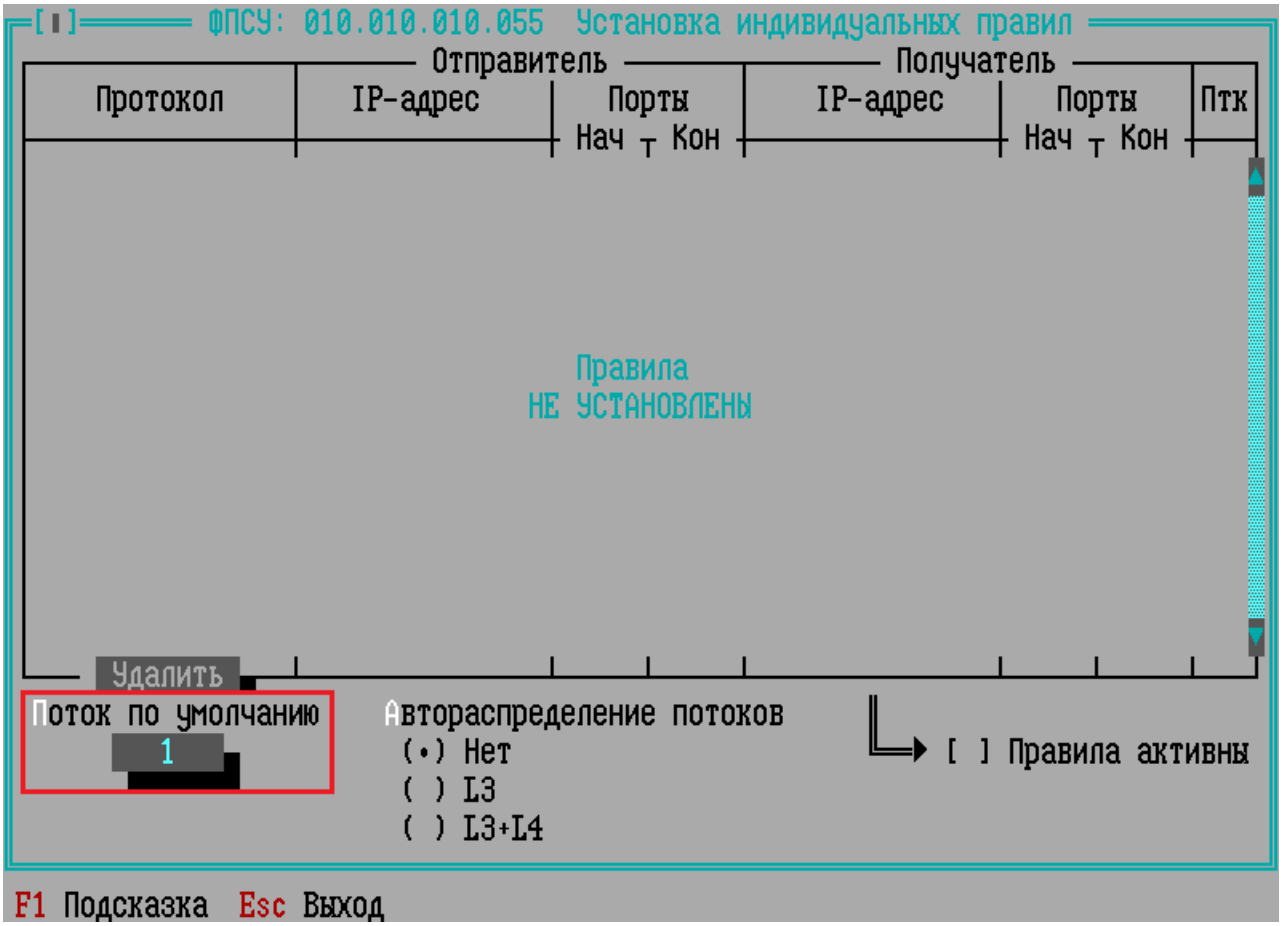


Рисунок 290 - Окно установки правил потоков для удаленного ФПСУ

Потоки могут распределятся вручную администратором, исходя из индивидуальных устанавливаемых правил. Альтернативный вариант: автоматическое случайное распределение пакетов по потокам, которое включает опция «*Авторасределение*

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. В связи с тем, что туннелированный трафик между двумя ФПСУ 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).

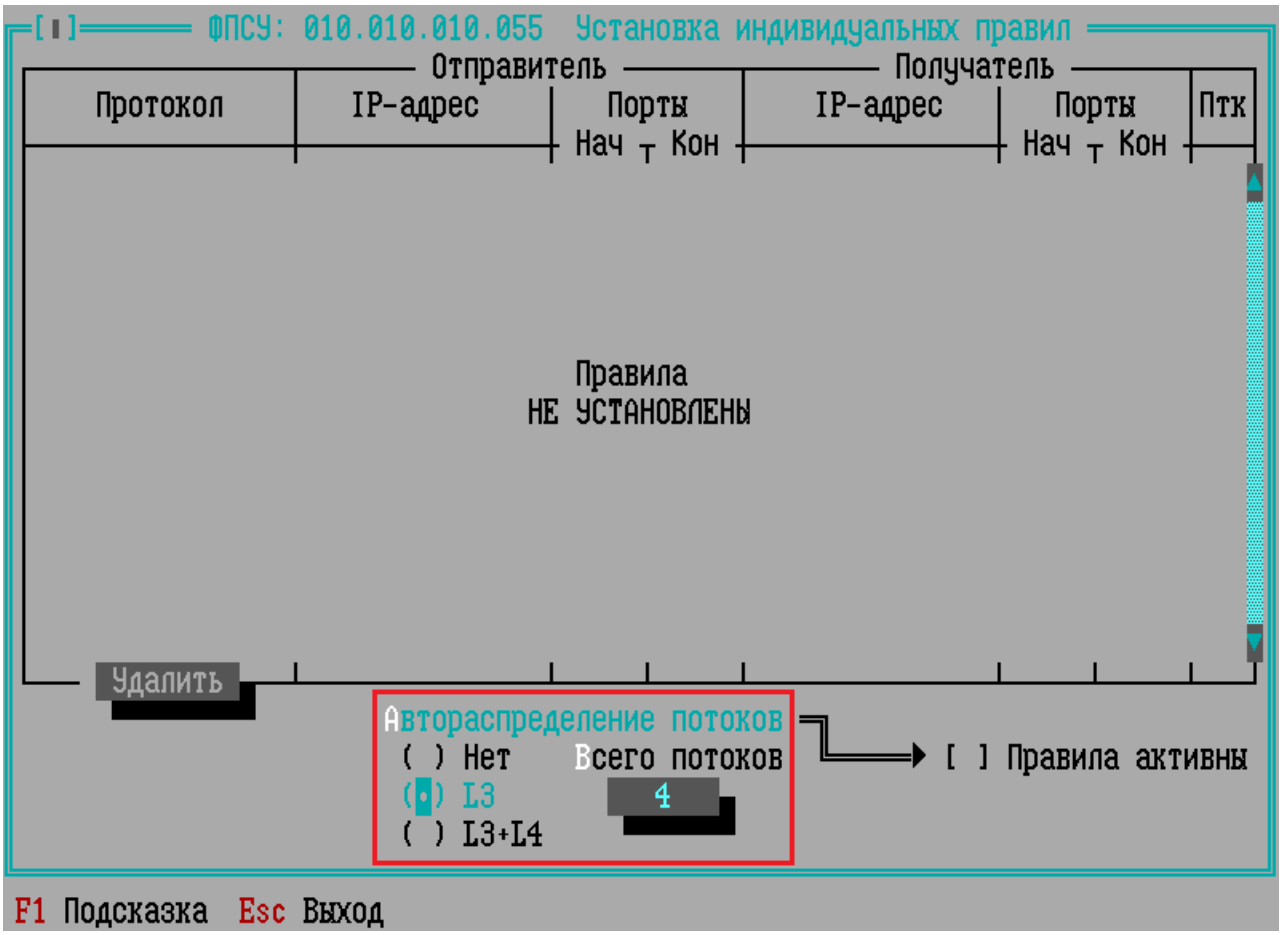


Рисунок 291 - Окно установки правил потоков для удаленного ФПСУ

Если администратор поставил опцию «*Авторапределение 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.

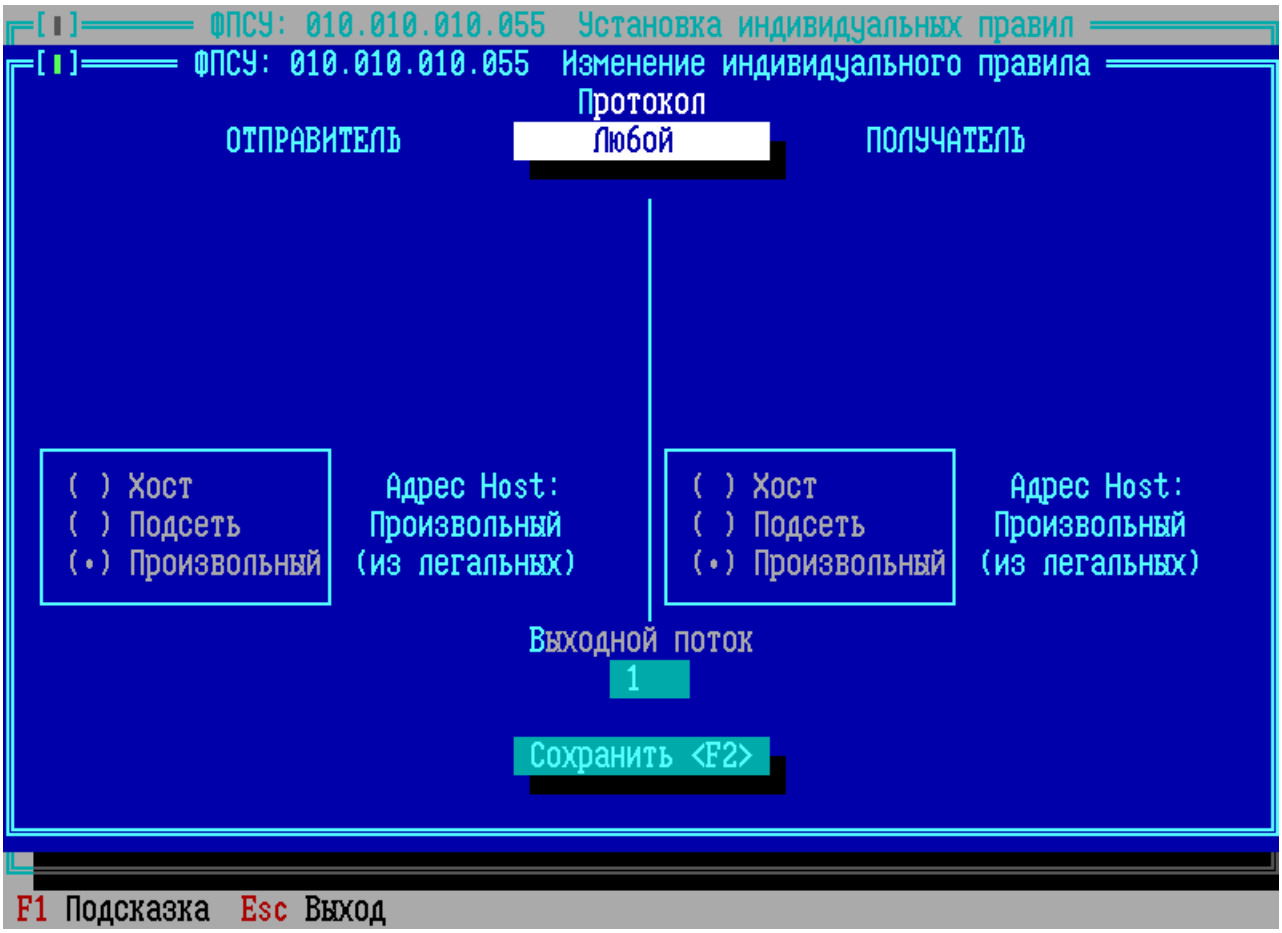


Рисунок 292 - Окно задания правила для нового потока

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

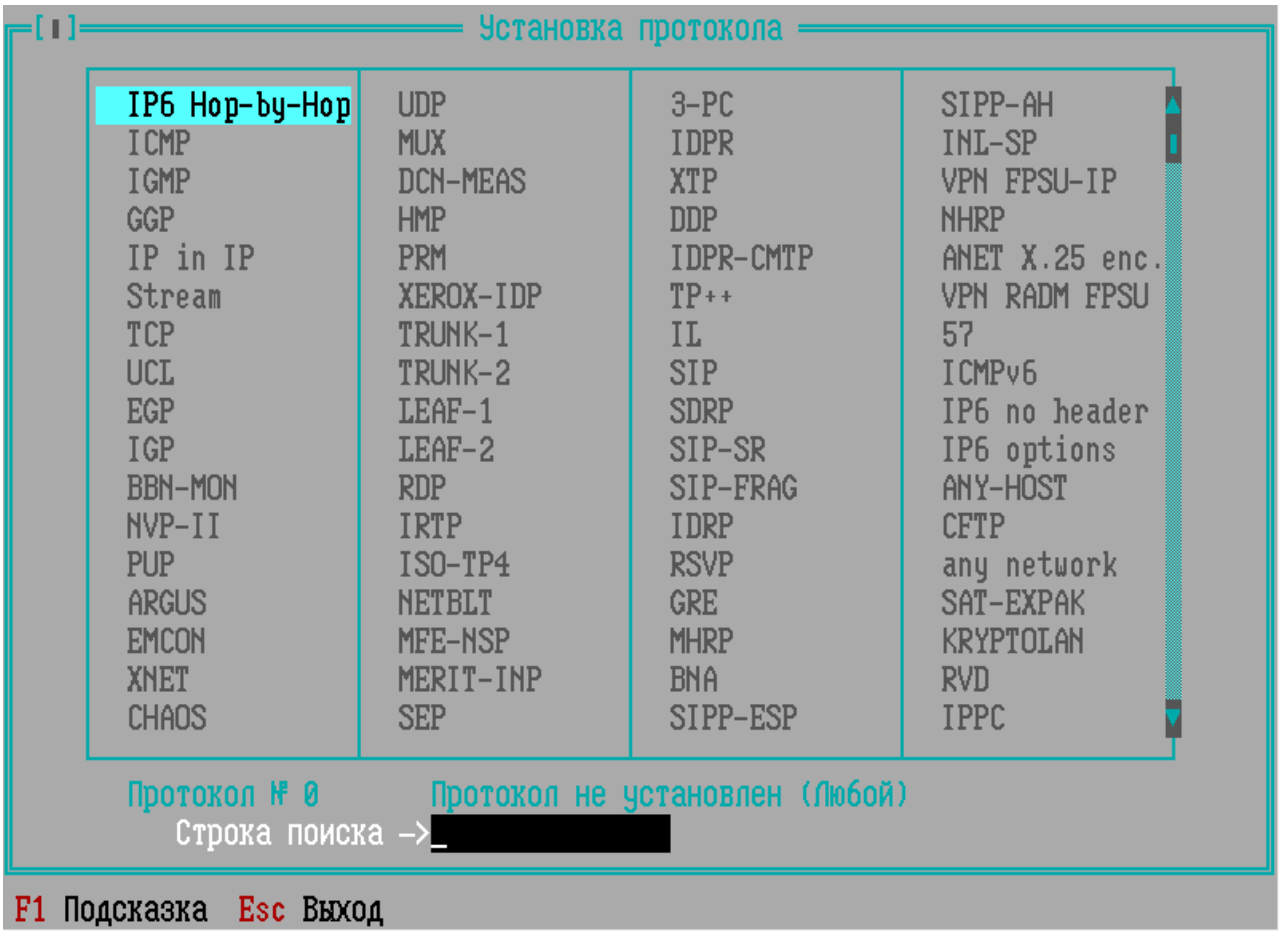


Рисунок 293 - Окно установления протокола для нового потока

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

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

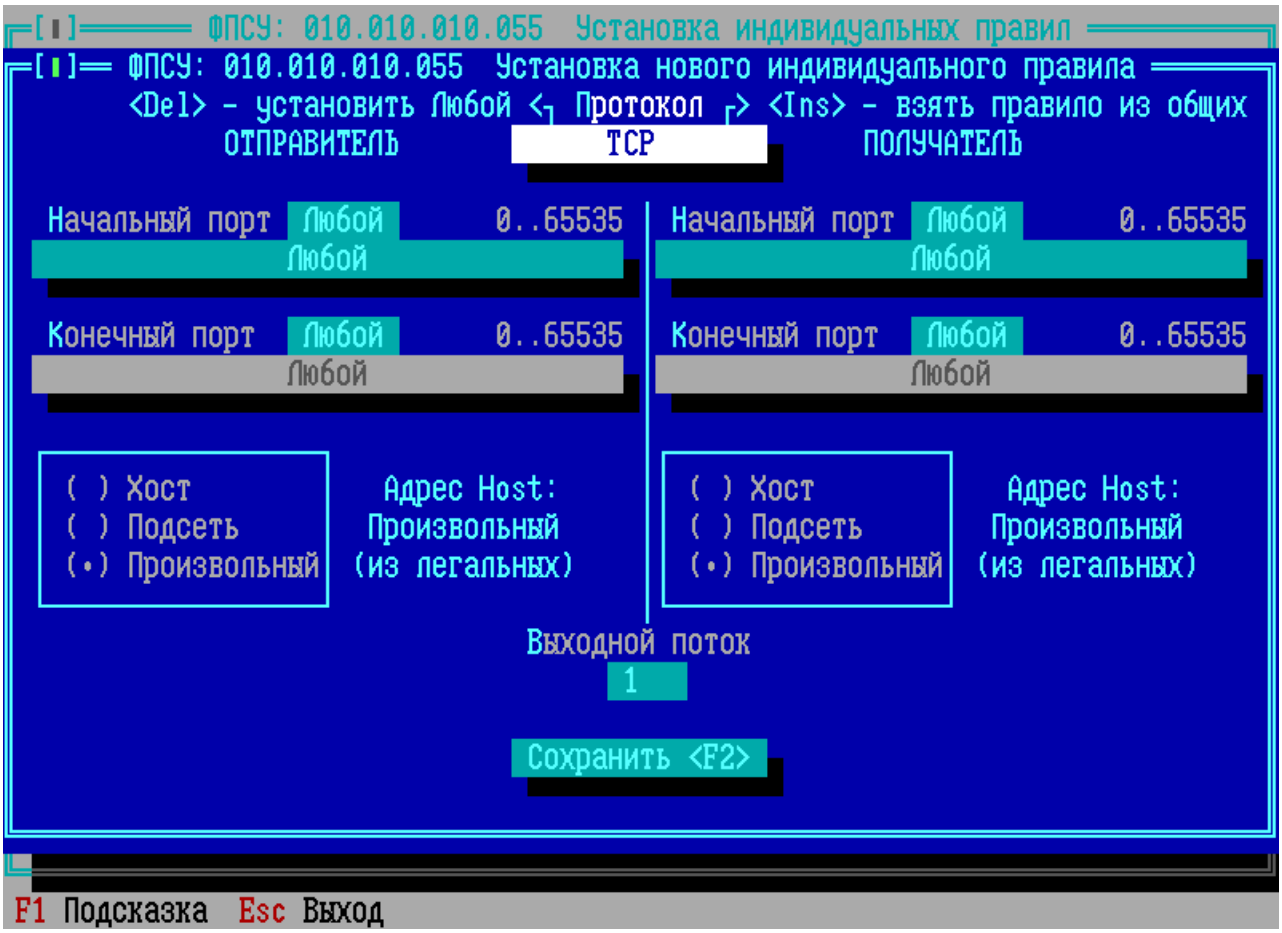


Рисунок 294 - Дополнительные поля для протокола TCP

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

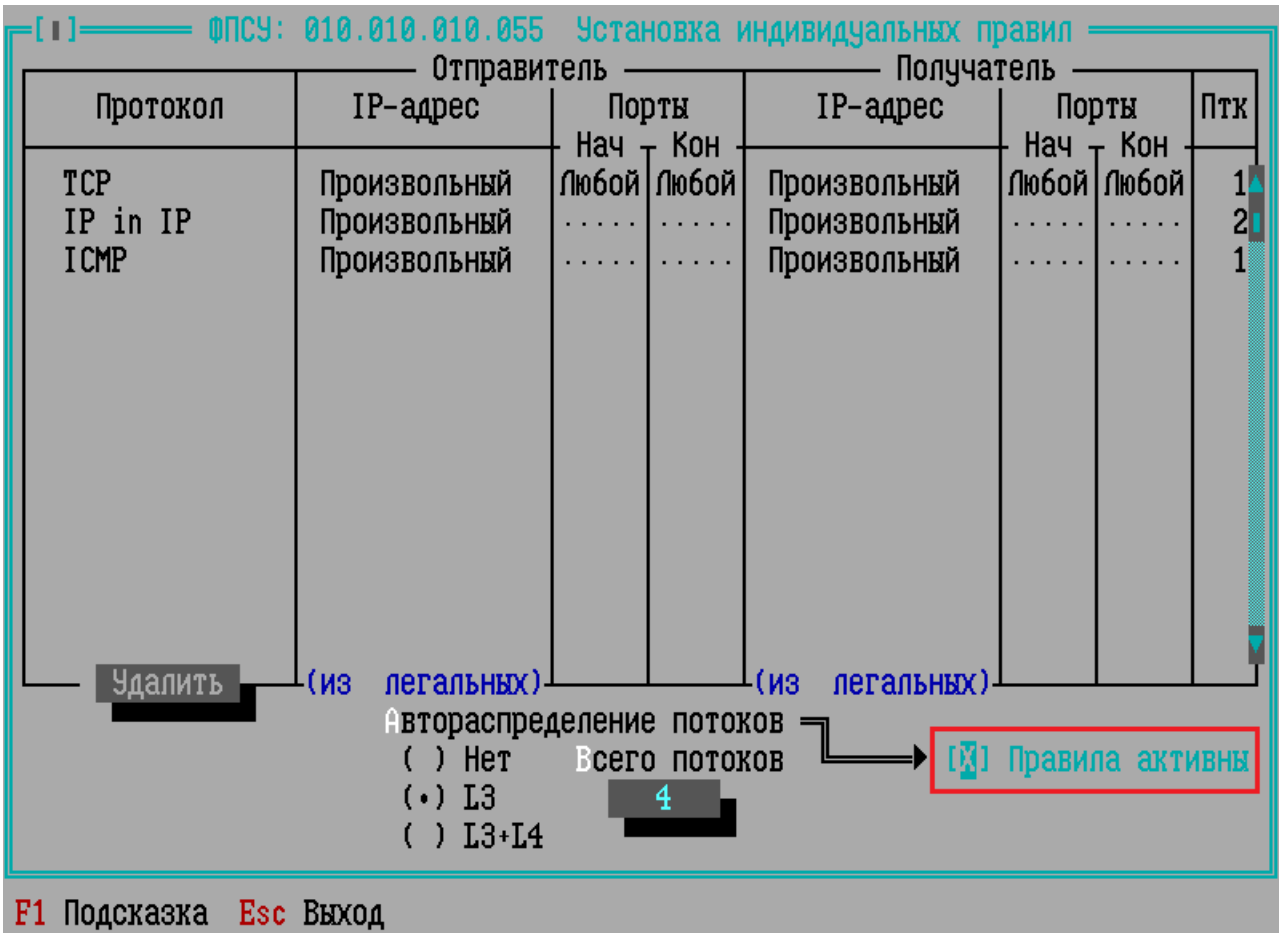


Рисунок 295 - Установка флага «Правила активны»

Для выхода из окна «Установка индивидуальных правил» в окно параметров туннеля между ФПСУ 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.

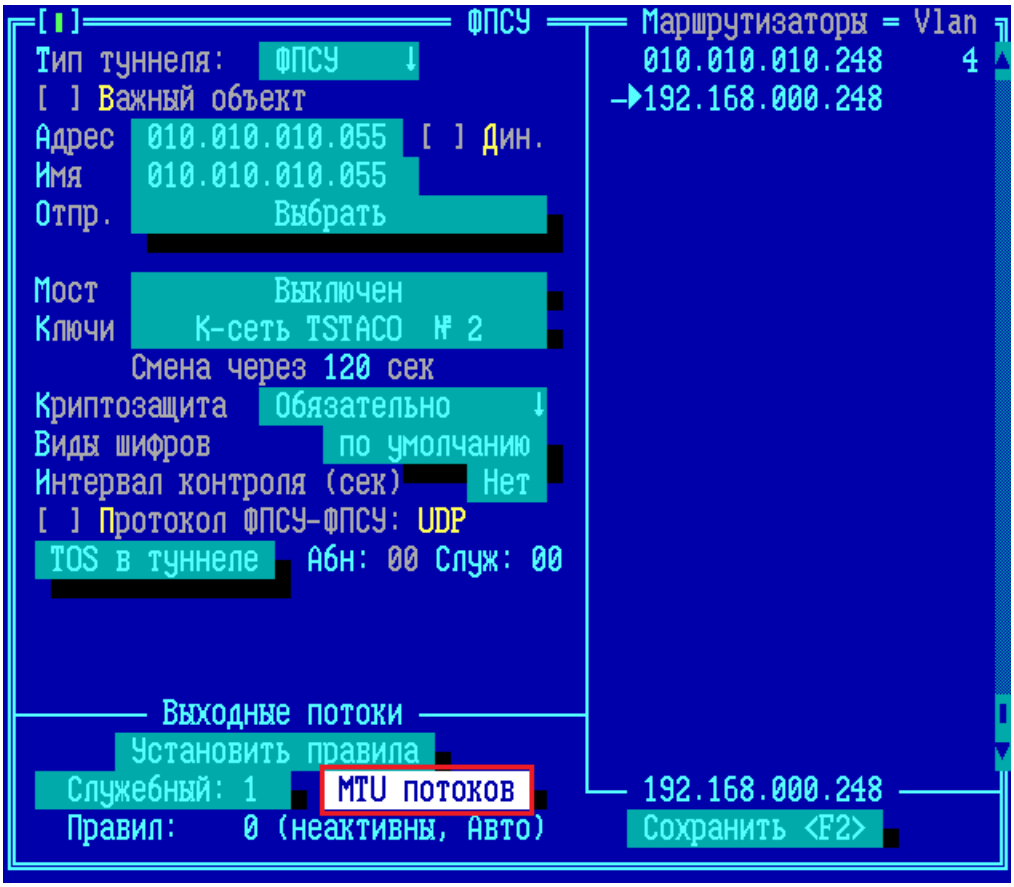


Рисунок 296 - Настройка удаленного ФПСУ

MTU **-** максимальный размер IP-пакетов (в байтах), которые будут передаваться с конфигурируемого порта ФПСУ удаленному ФПСУ через VPN-туннель. Значение этого поля возможно установить в диапазоне от 576 до размера 65535 байт (ВНИМАНИЕ! Фактический MTU будет не выше значения, установленного в настройках сетевого адаптера, см. пункт «Конфигурация драйверов сетевых адаптеров»). По умолчанию («От LAN-платы») будет использоваться значение MTU, которое конфигурируемый ФПСУ 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 на загруженных «медленных» магистральных линиях связи. Обычно характерным проявлением такой ситуации является появление на удаленном ФПСУ сообщений (в рабочем окне абонентов, см. Раздел «Окно состояния работы пользователей») об истечении времени жизни пакета от адреса конфигурируемого ФПСУ в собственный адрес удаленного ФПСУ. Необходимо также учитывать, что при уменьшении значения MTU производительность магистральной линии связи между двумя ФПСУ МОЖЕТ СНИЖАТЬСЯ ввиду фрагментирования/дефрагментирования пакетов средствами ФПСУ.

8. 3. 2. 3. Режим «Мост» между ФПСУ (L2-шифрование)

Режим моста предназначен для передачи **всех** входящих сетевых фреймов (L2) с одного порта ФПСУ в туннель к другому ФПСУ **без дополнительной проверки и фильтрации**. Режим моста может быть включен только для одного туннеля между ФПСУ версии ниже 4.

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

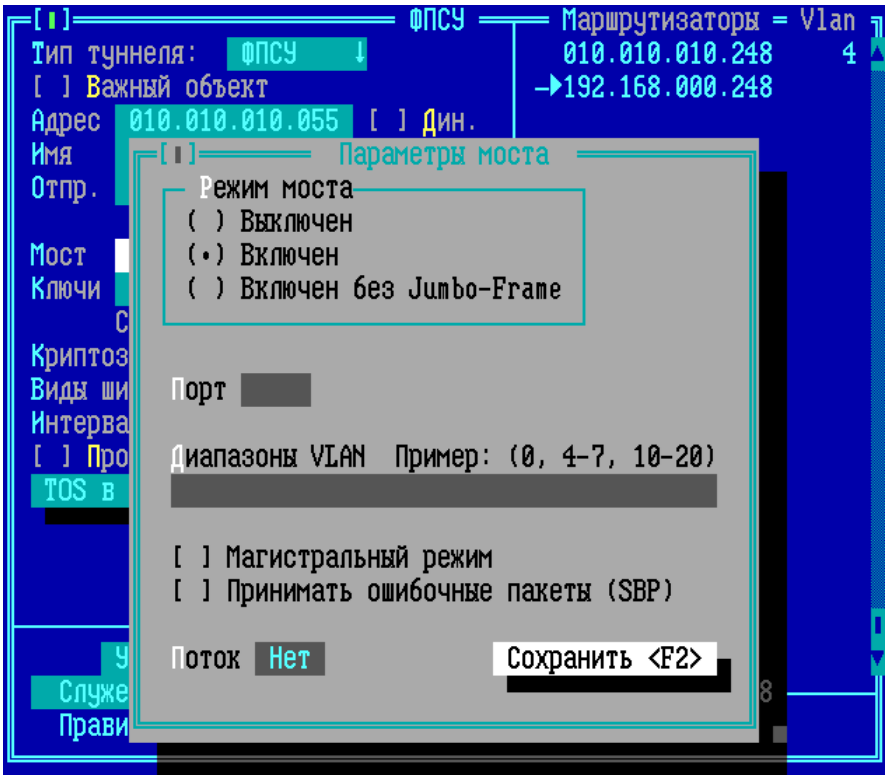


Рисунок 297 - Режим моста ФПСУ-ФПСУ

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

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

Включен — в туннеле используется режим моста; ФПСУ 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. 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 и задействованных Ethernet сервисов) после инкапсуляции превысят 1500 байт и будут разбиты на два пакета, что и может вызвать ухудшение скоростных характеристик.

Порт — обязательный параметр, в туннель в режиме моста будут передаваться пакеты только от указанного порта ФПСУ.

VLAN — опциональный параметр, в туннель в режиме моста будут передаваться пакеты только с интерфейсов с указанным VLAN или диапазоном VLAN.

Магистральный режим — используется, когда размер MTU на порту увеличен по сравнению со стандартным, при включении флага последовательность полученных фреймов объединяется в один, пока не получится фрейм с указанным размером MTU. Объединенный «большой» фрейм отсылается с указанного для моста туннельного порта. Например, если на порту установлен MTU 9000 байт, фреймы будут объединяться в один фрейм размером 9000 байт.

Принимать ошибочные пакеты (SBP) — установленный флаг включает приём непринятых пакетов (Store Broken Packets), поврежденных пакетов по причине неверной длины, либо испорченных пакетов. Режим будет включён, если сетевая карта его поддерживает. (Поддерживается в ФПСУ версии 4, начиная с билда 1683.)

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

ВНИМАНИЕ! Во избежание потерь в производительности ФПСУ по причине дефрагментации/фрагментации пакетов, MTU на сетевом адаптере, на котором добавлен описатель другого ФПСУ в режиме мост, рекомендуется установить на 100 меньше, чем установленный MTU для остальных сетевых адаптеров (см. пункт «Конфигурация драйверов сетевых адаптеров»).

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

- кадров, отправленные в MAC-адрес портов ФПСУ;

- пакетов от абонентов, описанных на портах ФПСУ.

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 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 выполняется в обычном порядке.

ВНИМАНИЕ! ФПСУ, 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-proxy 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 версии ниже 4 только один туннель может быть настроен на работу в режиме моста.

В конфигурации ФПСУ версии 4 на работу в режиме моста может быть настроено 1024 туннеля.

Примечание. При дополнительном лицензировании максимальное количество туннелей, описанных в конфигурации, может быть увеличено до 10 000.

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.

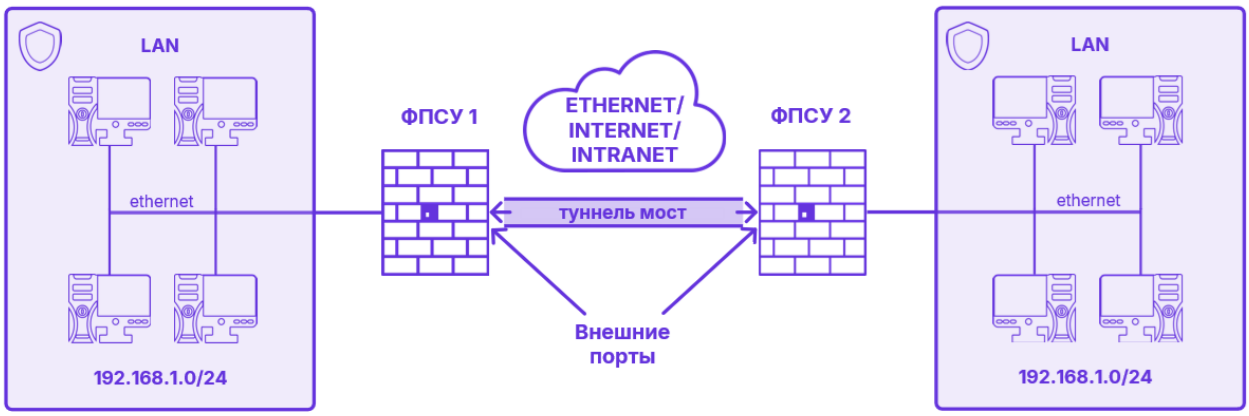


Рисунок 298 - Режим моста в туннеле ФПСУ-ФПСУ

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

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

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

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

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

8. 3. 2. 4. Динамические ФПСУ

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

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

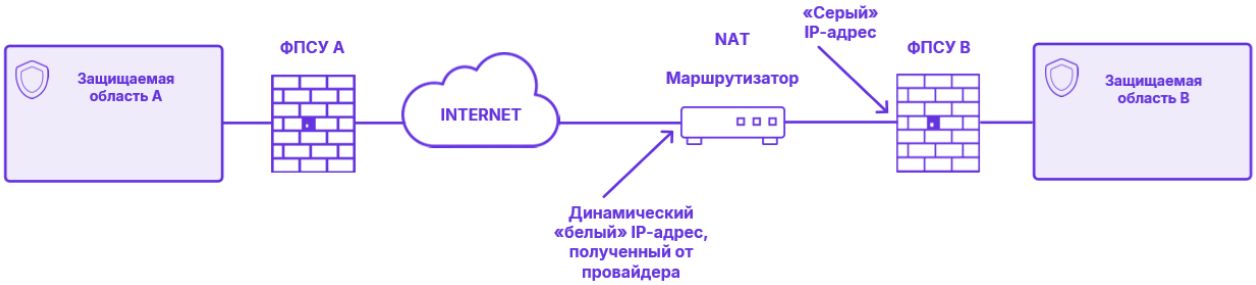


Рисунок 299 - Схема при установлении динамического туннеля с другим ФПСУ

Флаг «Дин. (Динамический)» для ФПСУ может быть задействован только в случае использования ключей класса КС1 или КС3. Если на ФПСУ используются только ключи класса КС2, не получится указать ФПСУ как «Дин. (Динамический)».

Признак динамического удаленного ФПСУ устанавливается в описателе ФПСУ:

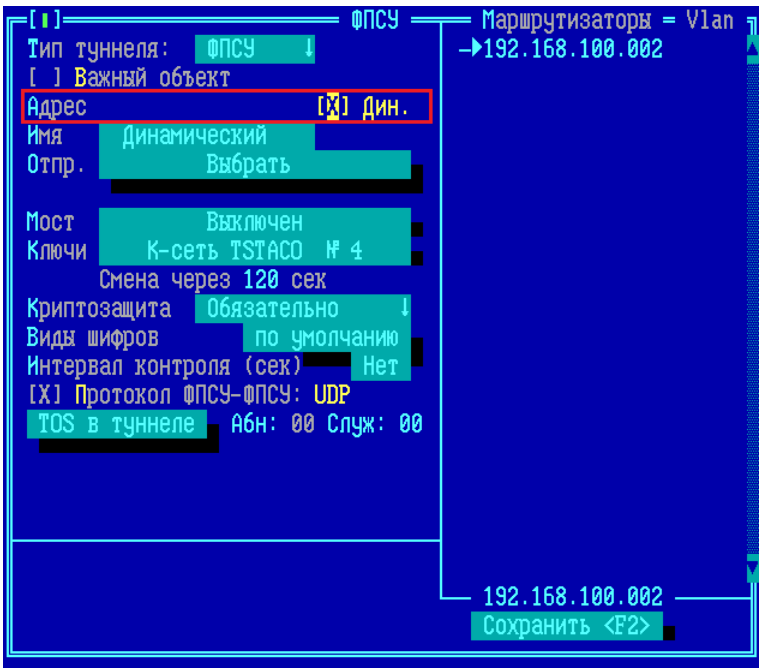


Рисунок 300 - Динамический туннель с другим ФПСУ

При использовании флага описателя ФПСУ - «Дин. (Динамический)», следует учитывать следующие отличия такого VPN-туннеля от стандартного:

- динамический ФПСУ может быть указан только как доступный через

маршрутизатор;

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

ВНИМАНИЕ! Если администраторы обоих ФПСУ указали партнера по VPN-туннелю как «Дин. (Динамический)», VPN-туннель не будет установлен.

8. 3. 2. 5. Описание туннеля типа IPIP

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

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

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

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

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

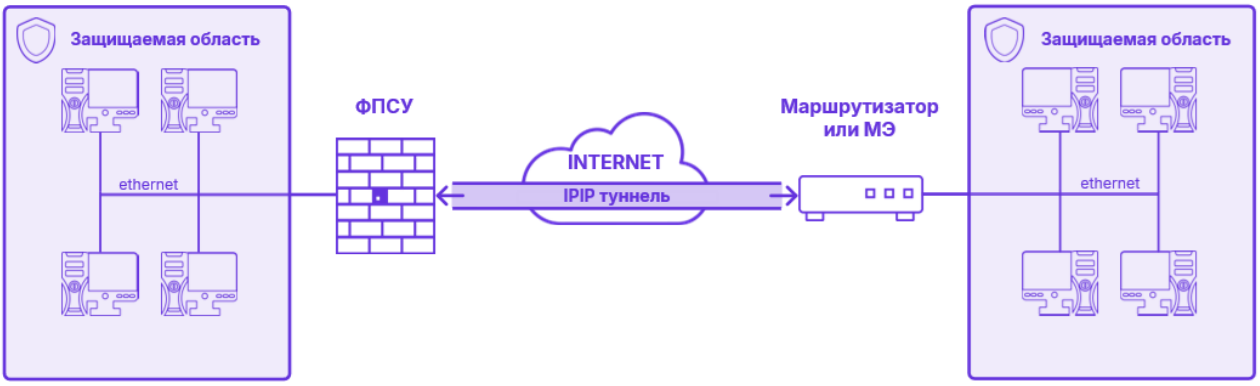


Рисунок 301 - Режим IPIP-туннеля ФПСУ-ФПСУ

8. 3. 3. Описание параметров абонентов

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

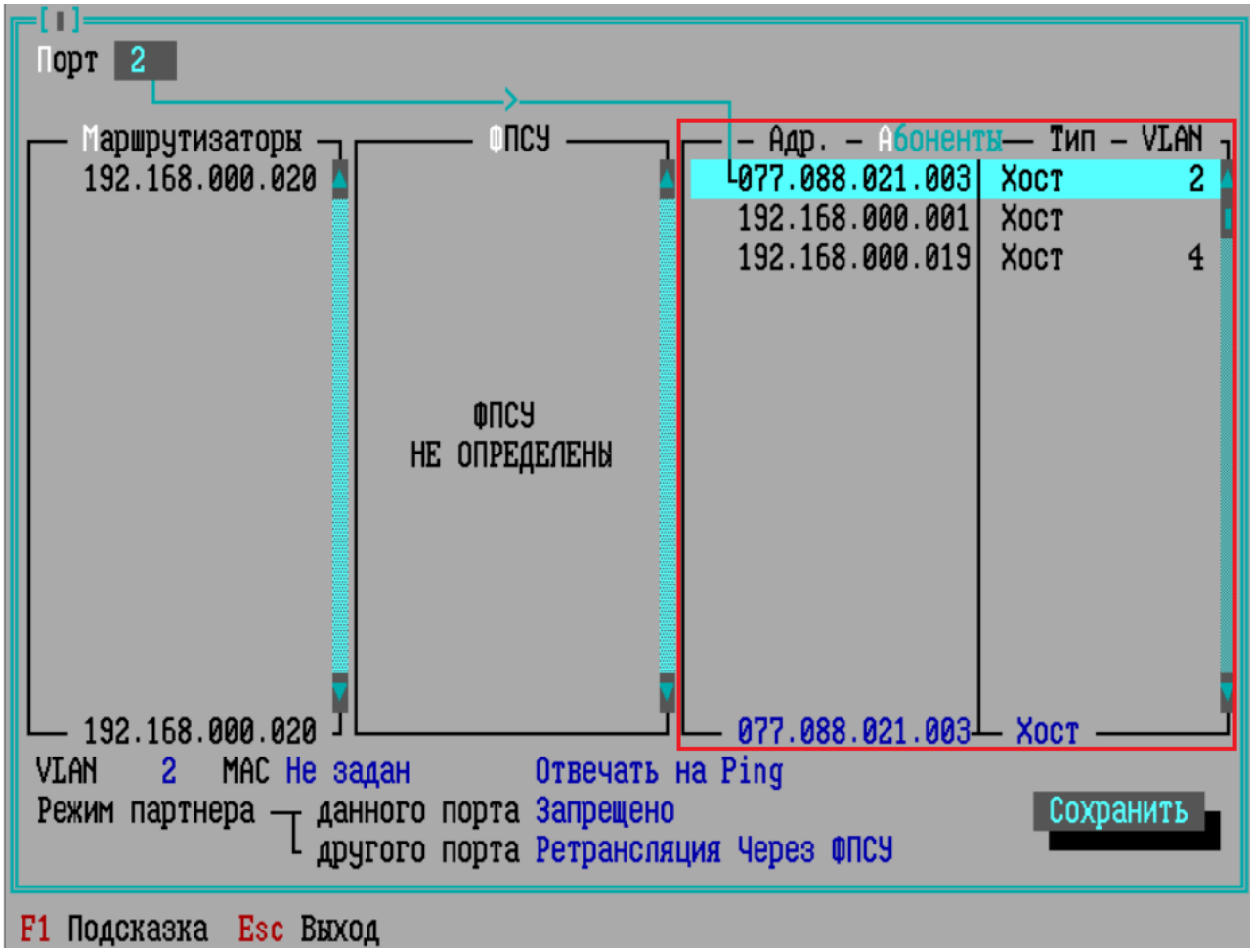


Рисунок 302 - Абоненты порта ФПСУ

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

В списке абонентов порта используются три типа записей:

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

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

При проверке проходящего через ФПСУ пакета, поиск адреса в таблице (и соответствующая фильтрация для этого адреса) производится по принципу «наибольшего совпадения», то есть в описателях конфигурации данного порта ищется «самый определенный» адрес. Сначала проверяется, не входит ли искомый адрес в список адресов индивидуальных хостов, если такой адрес в таблице обнаружен - поиск прекращается и для абонента производится фильтрация по правилам, установленным для данного конкретного адреса.

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

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

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

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

Во всех случаях откроется окно «*Абонент*», содержащее несколько полей, позволяющих определить тип адресной записи, ввести численные значения адресов, определить режим работы для описываемого адреса и определить другие необходимые

параметры. Все установки осуществляются посредством выбора соответствующей строки и нажатия клавиши <*Пробел*>.

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

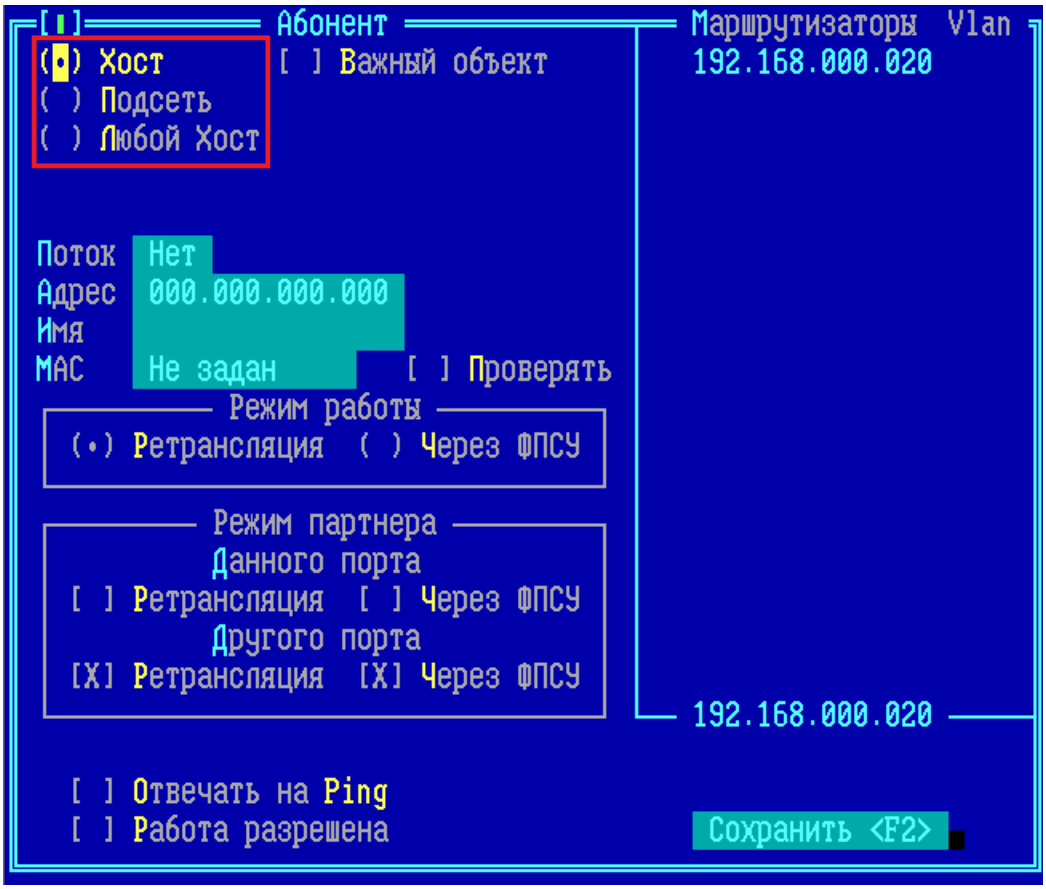


Рисунок 303 - Окно «Абонент»

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

8. 3. 3. 1. Описание абонента «Хост»

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

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

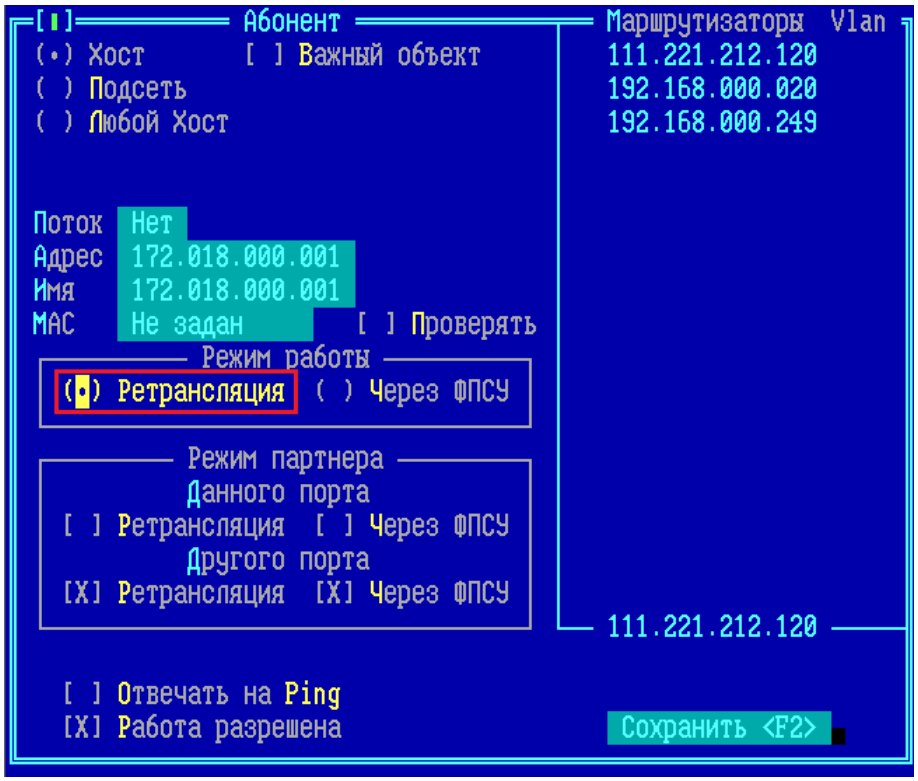


Рисунок 304 - Параметры абонента типа хост, режим «Ретрансляция»

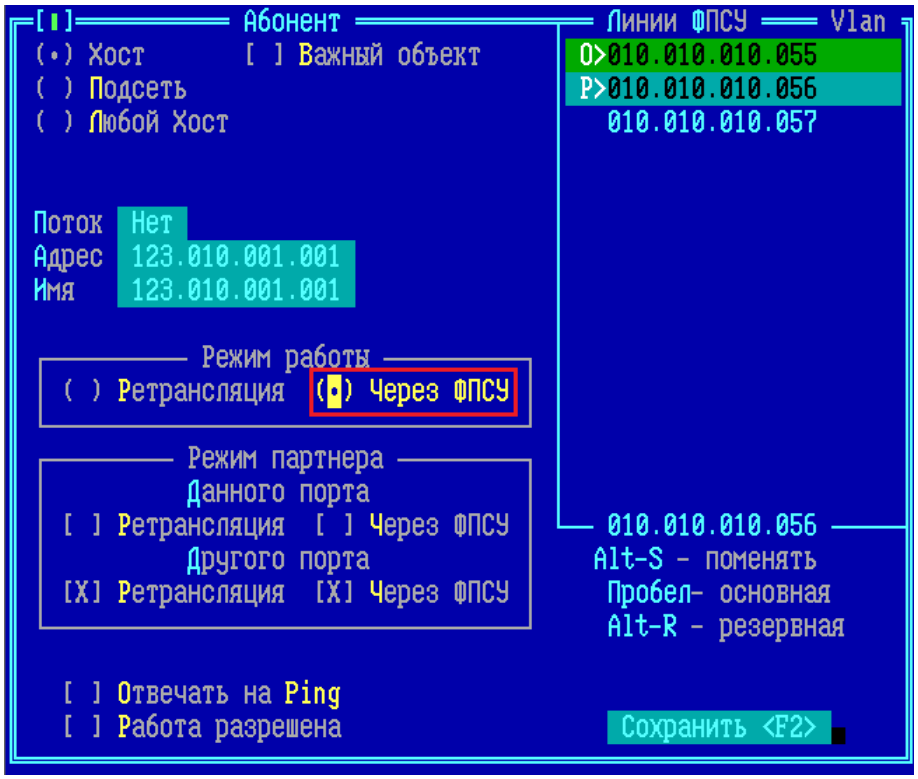


Рисунок 305 - Параметры абонента типа хост, режим «Через ФПСУ»

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

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

Адрес – IP-адрес рабочей станции.

Имя – имя абонента, которое будет отображаться в списке.

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

Проверять MAC – Только для абонентов типа «Хост», работающих в режиме «Ретрансляция». Требует заполненного поля «MAC». При включении опции ФПСУ 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.

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

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

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

При выборе режима «Ретрансляция» в правой части окна будет отображаться список маршрутизаторов, описанных со стороны данного порта. Если абонент доступен через какой-либо маршрутизатор, то такой маршрутизатор следует отметить нажатием клавиши <*Пробел*> (если в списке нет маршрутизаторов, необходимо сначала описать их). Заметим,

что администратор может регламентировать нагрузку на маршрутизаторы, приписывая различных абонентов к определенным маршрутизаторам. При передаче IP-пакетов описываемому абоненту ФПСУ будет учитывать ICMP сообщения переадресации (см. пункт «Описание параметров туннелей с другими ФПСУ»).

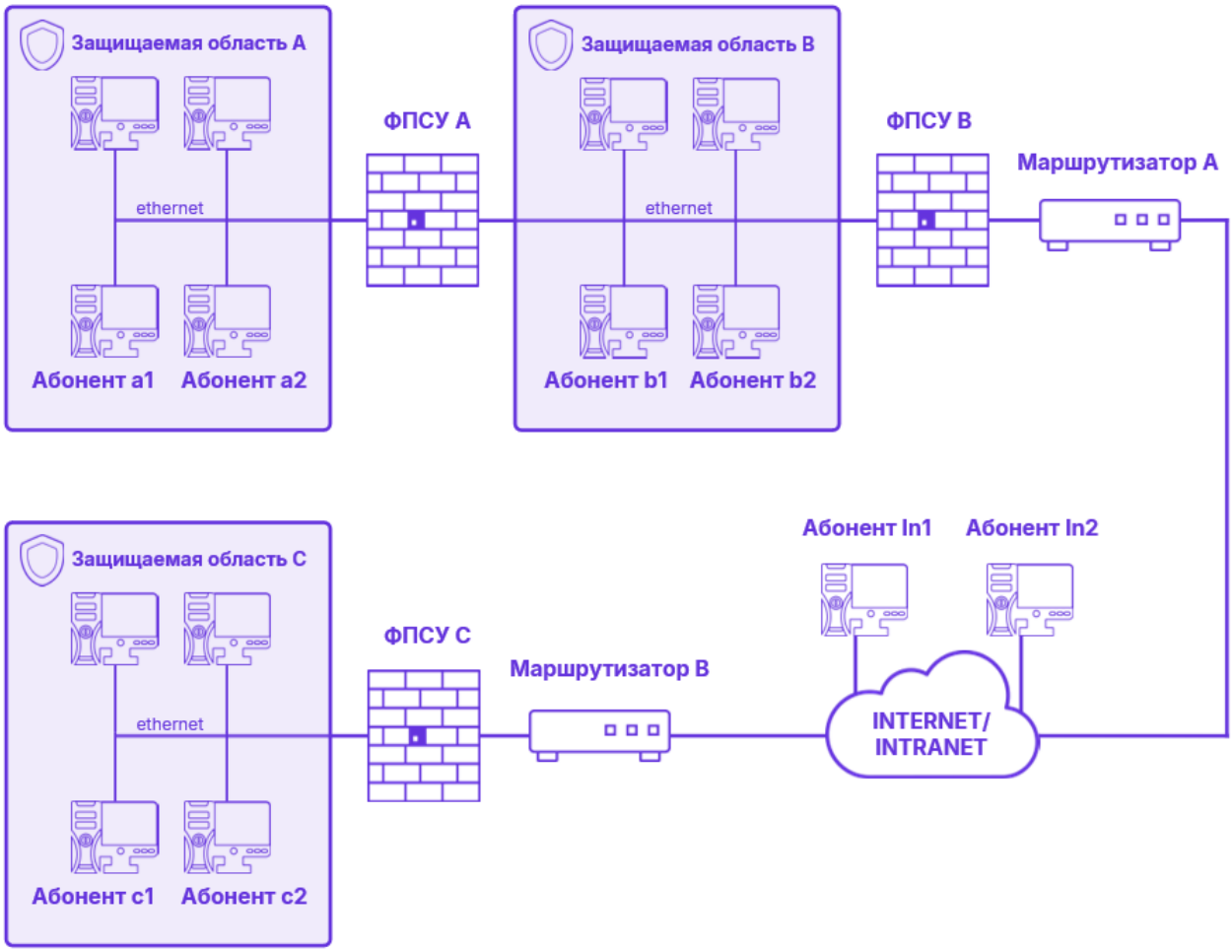


Рисунок 306 - Режим работы партнеров абонента

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

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

В случае указания режима работы «*Через ФПСУ*» в правой части окна будет отображен список линий смежных ФПСУ (если список пуст, вернитесь к процедурам, описанным ранее). При помощи клавиши <*Пробел*> отметьте имя удаленного ФПСУ, через который будет доступен абонент (слева от строки появится отметка). Для абонента требуется выбрать основную линию ФПСУ, через туннель с которым будут передаваться данные. Если абонент может передавать данные через внешнюю сеть по нескольким маршрутам, то в настройках ФПСУ есть возможность указать резервный (запасной) ФПСУ, через туннель с которым будут передаваться данные в случае невозможности организовать туннель с основным ФПСУ. Выберите описатель ФПСУ, который требуется назначить запасным, и нажмите <*Alt+R*>. Нажмите <*Alt+C*> чтобы поменять для данного абонента основной ФПСУ и запасной.

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

- Абонент a → ФПСУ A → туннель A-B → ФПСУ B → Абонент b;
- Абонент a → ФПСУ A → туннель A-C → ФПСУ C → Абонент b.

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

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

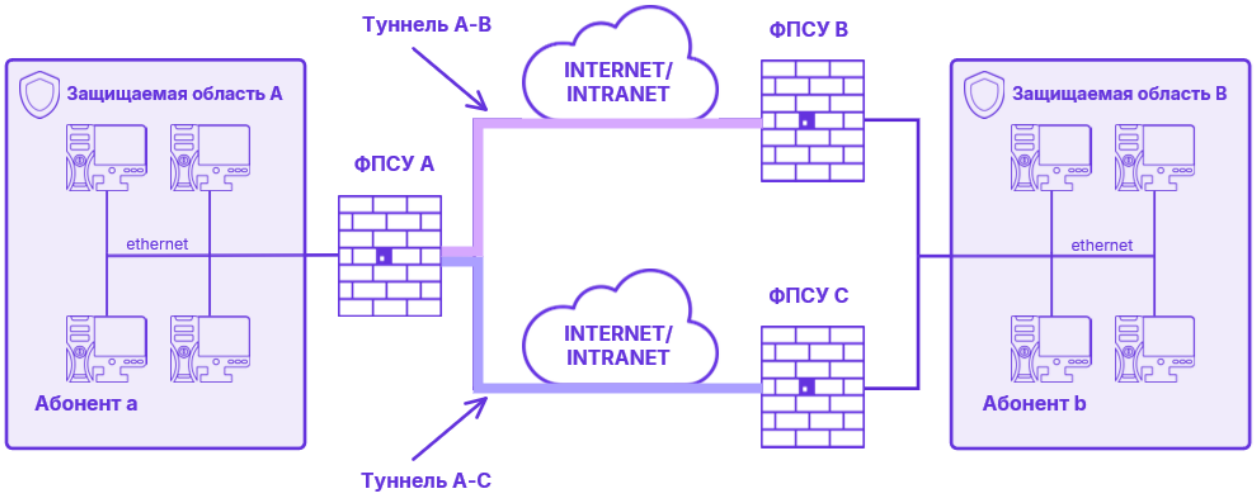


Рисунок 307 - Использование основной и резервной (запасной) линий ФПСУ

Для каждого описываемого абонента может быть установлено дополнительное правило фильтрации по режиму работы с другими зарегистрированными на настраиваемом ФПСУ 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 напрямую. Например, на рис. «Режим работы партнеров абонента» для ФПСУ C и описываемого на нем «Абонента a1» партнером данного порта в режиме ретрансляция является «Абонент In1» или «Абонент In2»; для ФПСУ B и описываемого «Абонента a2» таким партнером является «Абонент b2».

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

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

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

Партнер другого порта в режиме «Через ФПСУ» — это абонент, зарегистрированный на другом логическом порту ФПСУ относительно описываемого абонента, который подключен к настраиваемому ФПСУ через установленный VPN-туннель с другим ФПСУ. Например, для ФПСУ A и описываемого «Абонента a1» партнерами другого порта в режиме «Через ФПСУ» являются «Абонент c1» или «Абонент in1»; для ФПСУ C и описываемого «Абонента c2» такими партнерами являются «Абонент a2» или «Абонент b2».

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

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

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

8. 3. 3. 2. Описание абонента «Подсеть»

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

трафика межсетевого экрана (см. раздел «Параметры доступа, правила трафика межсетевого экрана»).

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

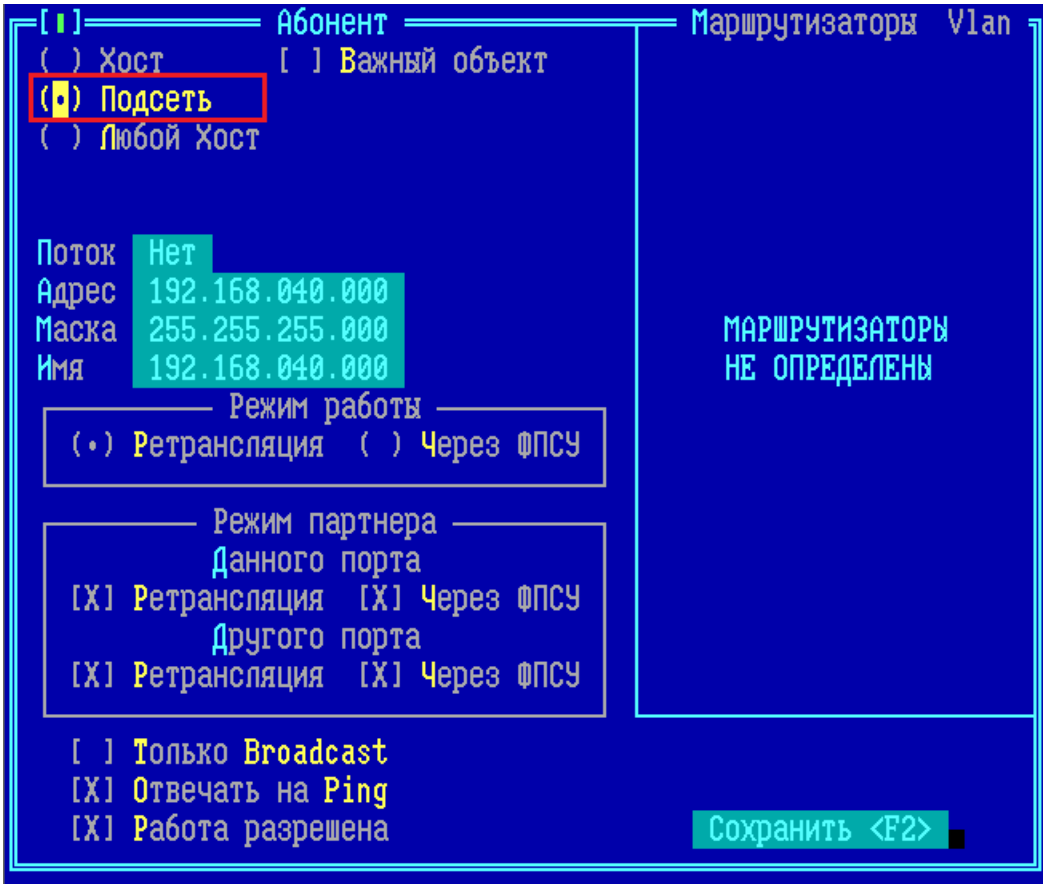


Рисунок 308 - Описание абонента ФПСУ типа «Подсеть»

Для описания **подсети** заполните следующие поля:

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

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

Адрес подсети — IP-адрес подсети.

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

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

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

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

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

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

Отвечать на Ping — указание ФПСУ отвечать на ICMP (ECHO) пакеты, направленные от IP-адреса абонентов описываемой подсети в IP-адреса портов настраиваемого ФПСУ. Отметка (разрешение отвечать на запросы) производится по нажатию клавиши <*Пробел*>. ФПСУ 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 настраиваются особым образом. Предположим, что со стороны одного порта ФПСУ 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. Для обработки подобной ситуации предусмотрена следующая последовательность установок:

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

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

8. 3. 3. 3. Описание абонента «Любой Хост»

Специальный адрес «Любой Хост» может быть описан только один раз со стороны любого порта и предназначен для реализации возможности обмена пакетами через ФПСУ с абонентами произвольных IP-адресов, принадлежащими всей сети Internet/Intranet.

Использование или неиспользование адреса этого типа определяется политикой безопасности организации.

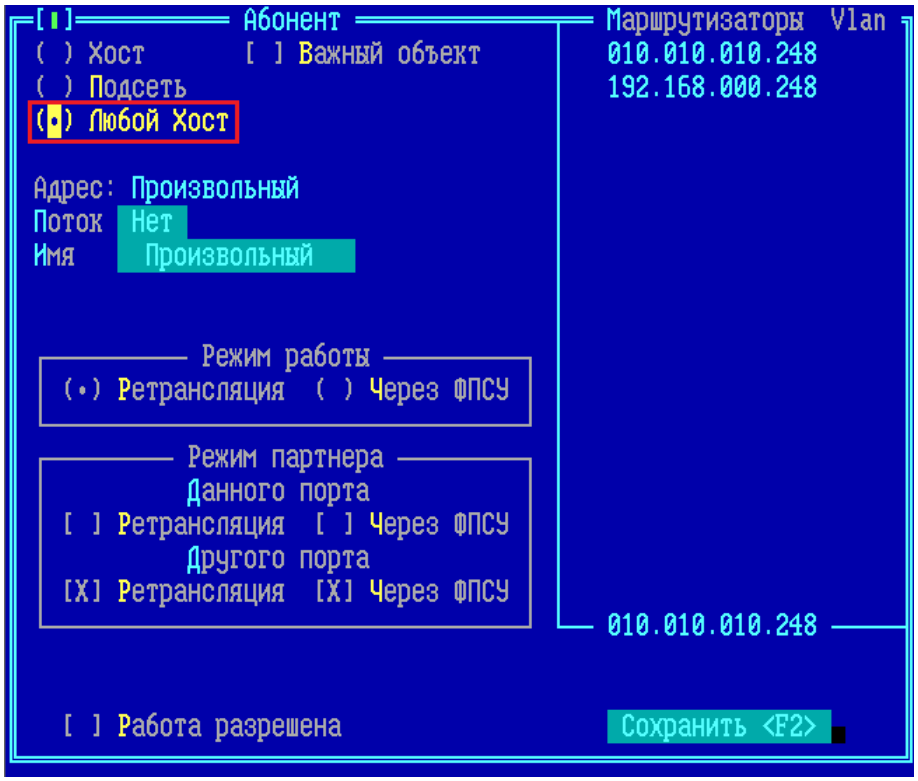


Рисунок 309 - Абонент «Любой Хост», режим «Ретрансляция»

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

8. 3. 3. 4. Работа со списком абонентов

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

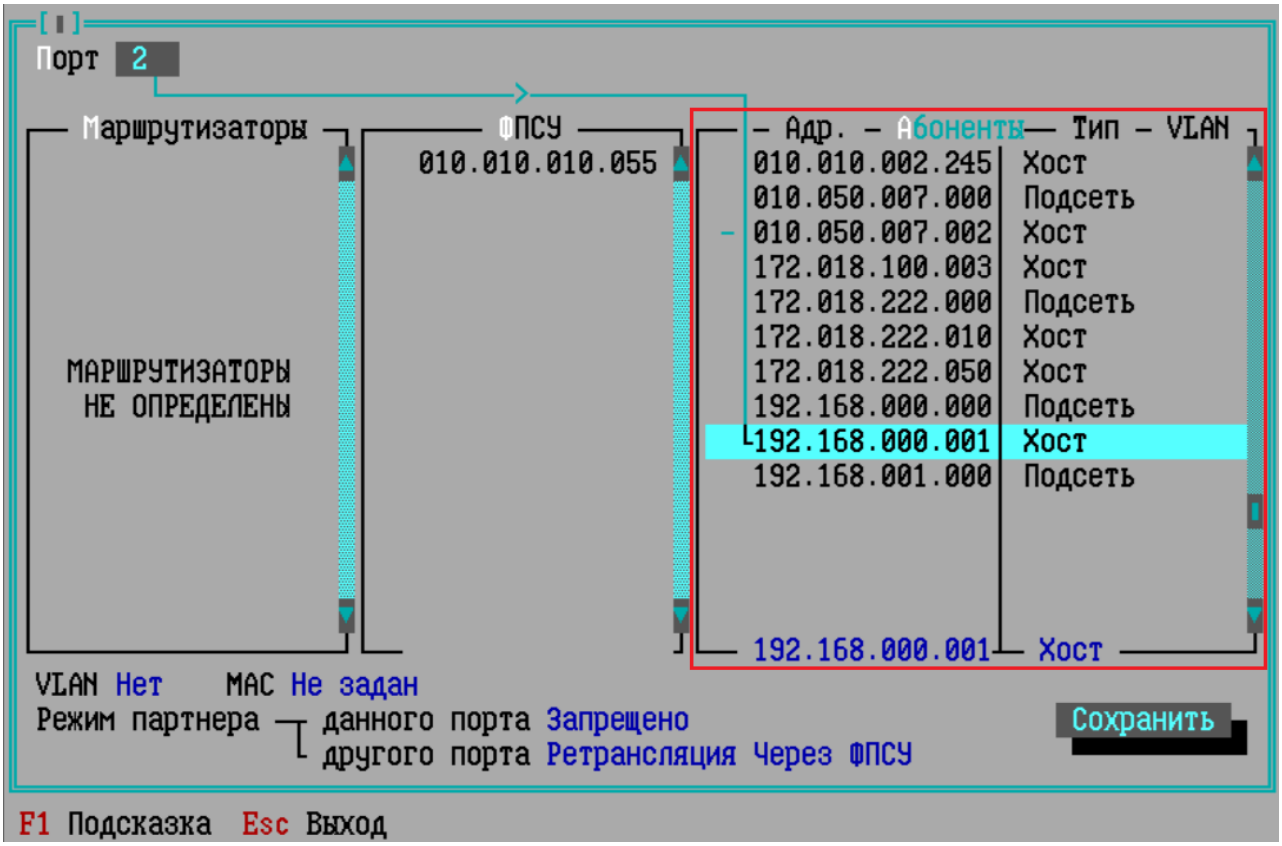


Рисунок 310 - Абоненты порта ФПСУ

Переход к списку туннелей ФПСУ 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 311 - 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*>.

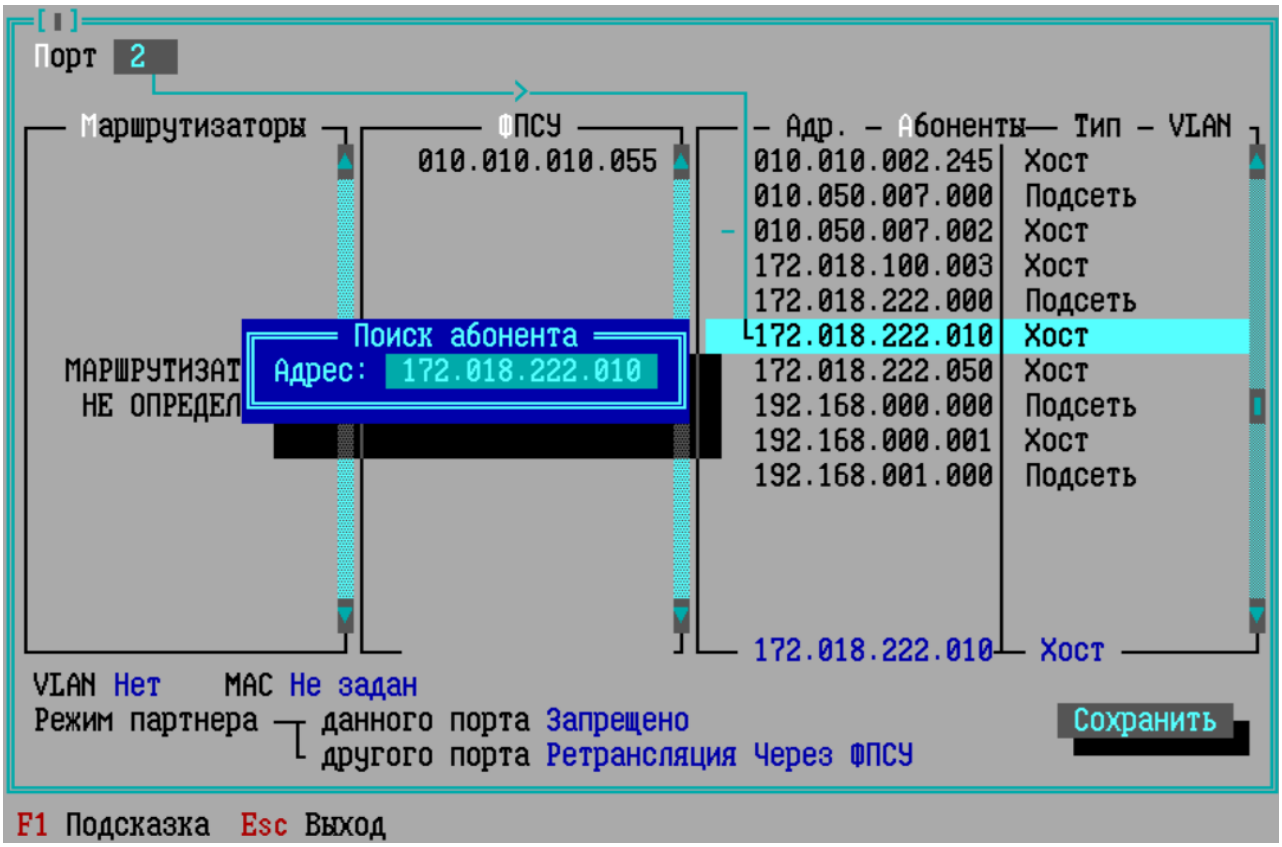


Рисунок 312 - Поиск абонента в списке

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

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

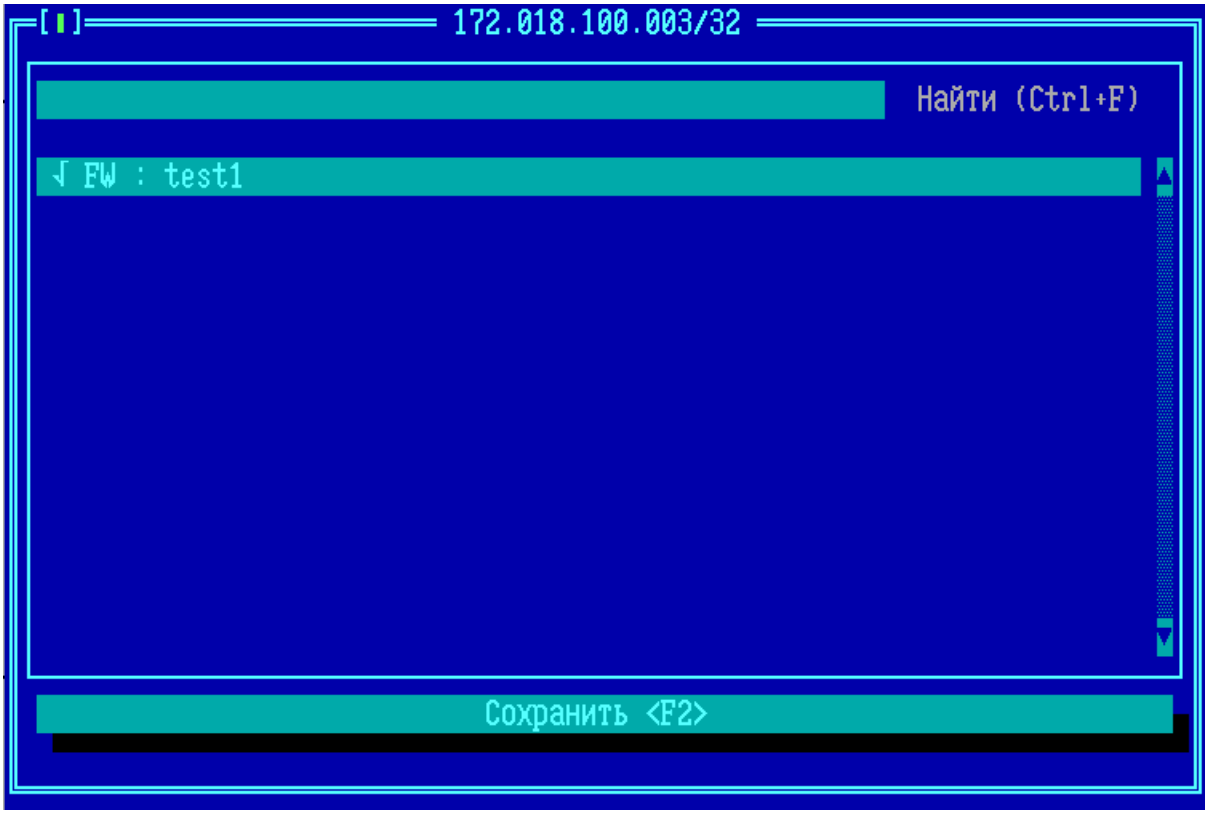


Рисунок 313 - Поиск абонента в правилах МЭ

Добавление группы абонентов

Находясь курсором в списке абонентов окна параметров порта ФПСУ (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.

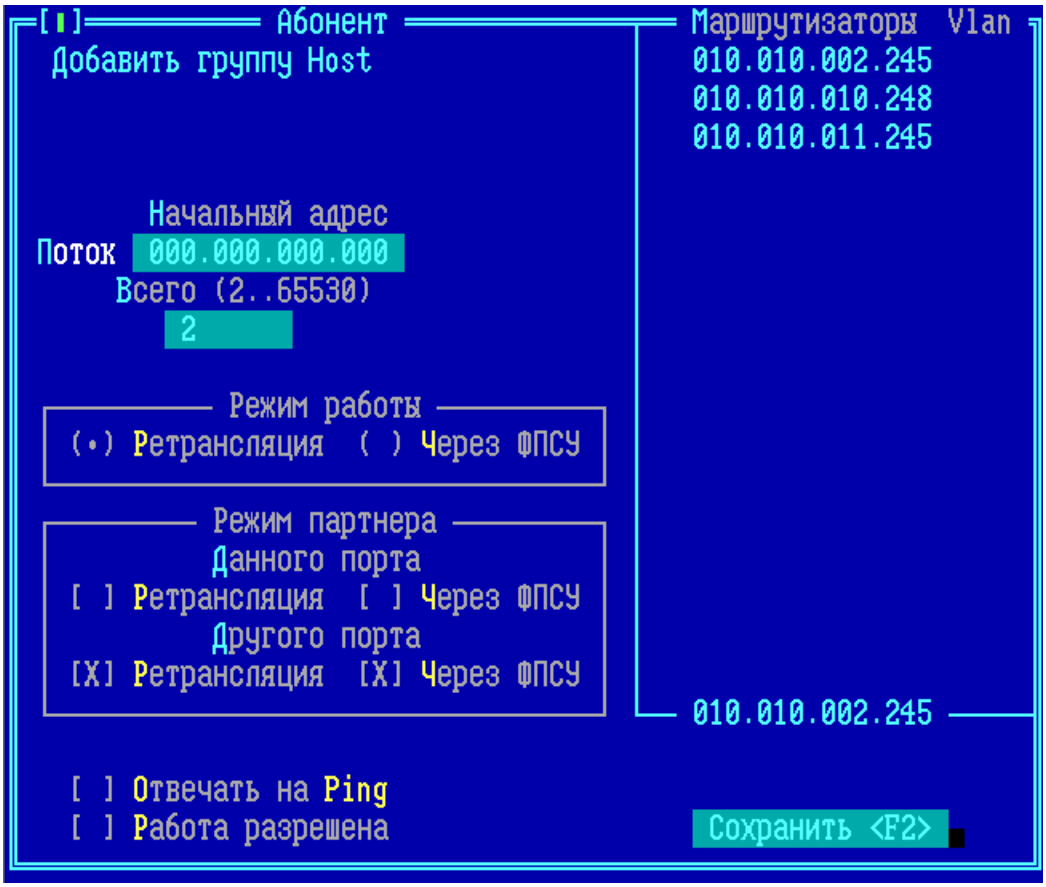


Рисунок 314 - Окно добавления группы описателей типа «хост»

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

Удаление абонентов

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

Для удаления нескольких абонентов одновременно, находясь курсором в списке абонентов, нажмите сочетание клавиш <*Ctrl+Del*> или <*Ctrl+D*>. Появится окно со списком абонентов порта.

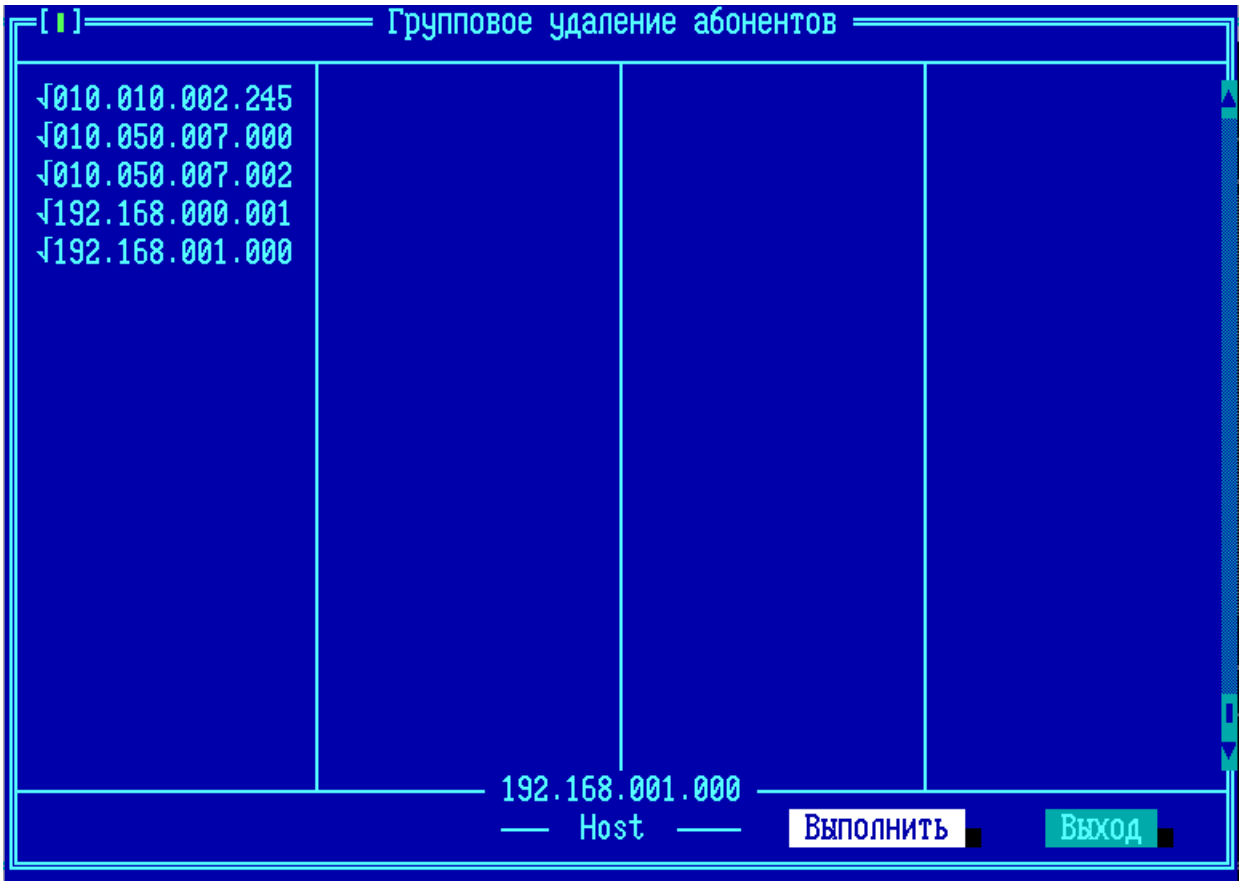


Рисунок 315 - Групповое удаление абонентов

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.

8. 4. Динамическая маршрутизация

На ФПСУ применяется статическая и динамическая маршрутизация.

Статическая маршрутизация настраивается в конфигурации на портах. Статические маршруты заносятся в таблицу маршрутизации вручную администратором. В случае конфликта маршрутов статическая маршрутизация является приоритетной.

Динамическая маршрутизация позволяет ФПСУ получать маршруты от других устройств в сети, маршрутизаторов и ФПСУ. Протоколы динамической маршрутизации позволяют ФПСУ автоматически получать информацию о новых сетях, выбирать

оптимальный путь к месту назначения, обновлять данные маршрутизации о состоянии сети, а также находить альтернативные пути в случае, если ранее определенный маршрут недоступен. Динамические маршруты добавляются в таблицу маршрутизации автоматически.

Внимание! Динамическая маршрутизация поддерживается на ФПСУ версии 4.0 с установленным дополнением frr. Без установленного дополнения frr динамическая маршрутизация на ФПСУ работать не будет!

Для задействования динамической маршрутизации необходимо настроить протоколы на каждом ФПСУ и маршрутизаторе, которые будут участвовать в динамической маршрутизации.

Динамическая маршрутизация на ФПСУ использует протокол внутридоменной маршрутизации OSPF и протокол междоменной маршрутизации BGP.

8. 4. 1. Динамическая маршрутизация OSPF

Динамическая маршрутизация может быть настроена с помощью протокола OSPF (Open Shortest Path First).

OSPF – протокол динамической маршрутизации, отслеживает состояния канала и использует алгоритм поиска кратчайшего пути (алгоритм Дейкстры) для расчета оптимальных маршрутов в сети. OSPF представляет собой протокол внутренней маршрутизации, регламентированный стандартом RFC 2328.

ФПСУ получает и распространяет информацию о доступных маршрутах между маршрутизаторами и другими ФПСУ с помощью протокола OSPF в домене маршрутизации, выступает в качестве OSPF-маршрутизатора.

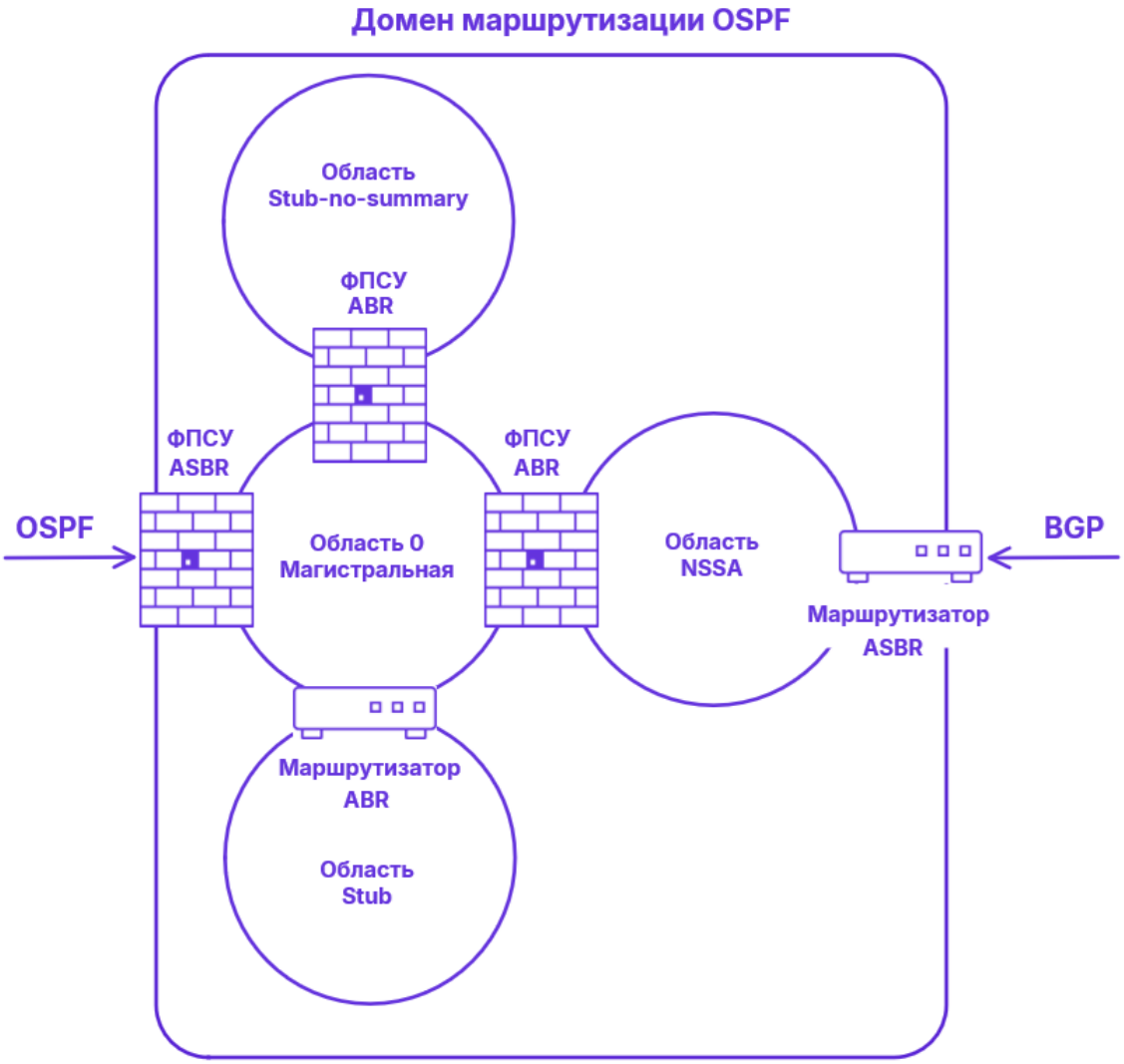


Рисунок 316 - Схема сети с маршрутизацией на основе OSPF

По умолчанию, динамическая маршрутизация отключена на ФПСУ.

Настройки динамической маршрутизации открываются из пункта меню «Порты ФПСУ → Динамическая маршрутизация OSPF».

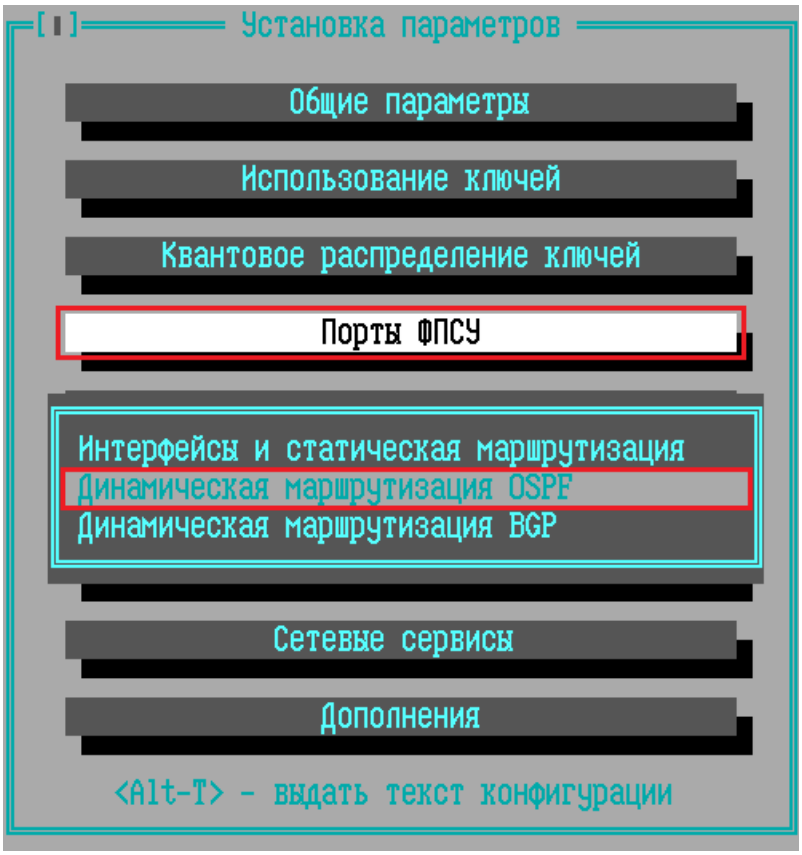


Рисунок 317 - Подменю команды «Порты ФПСУ»

В окне «Настройки динамической маршрутизации OSPF» находятся вкладки с настраиваемыми параметрами протокола. Переход с активной вкладки на соседнюю осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

На каждой вкладке необходимо указать обязательные для настройки протокола OSPF параметры:

- Настройки
- Области
- Интерфейсы и туннели
- Отладка

Для выхода в меню с сохранением настроек протокола OSPF, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

8. 4. 1. 1. Настройки

На вкладке **Настройки** включается протокол OSPF и добавляются маршруты из

других источников.

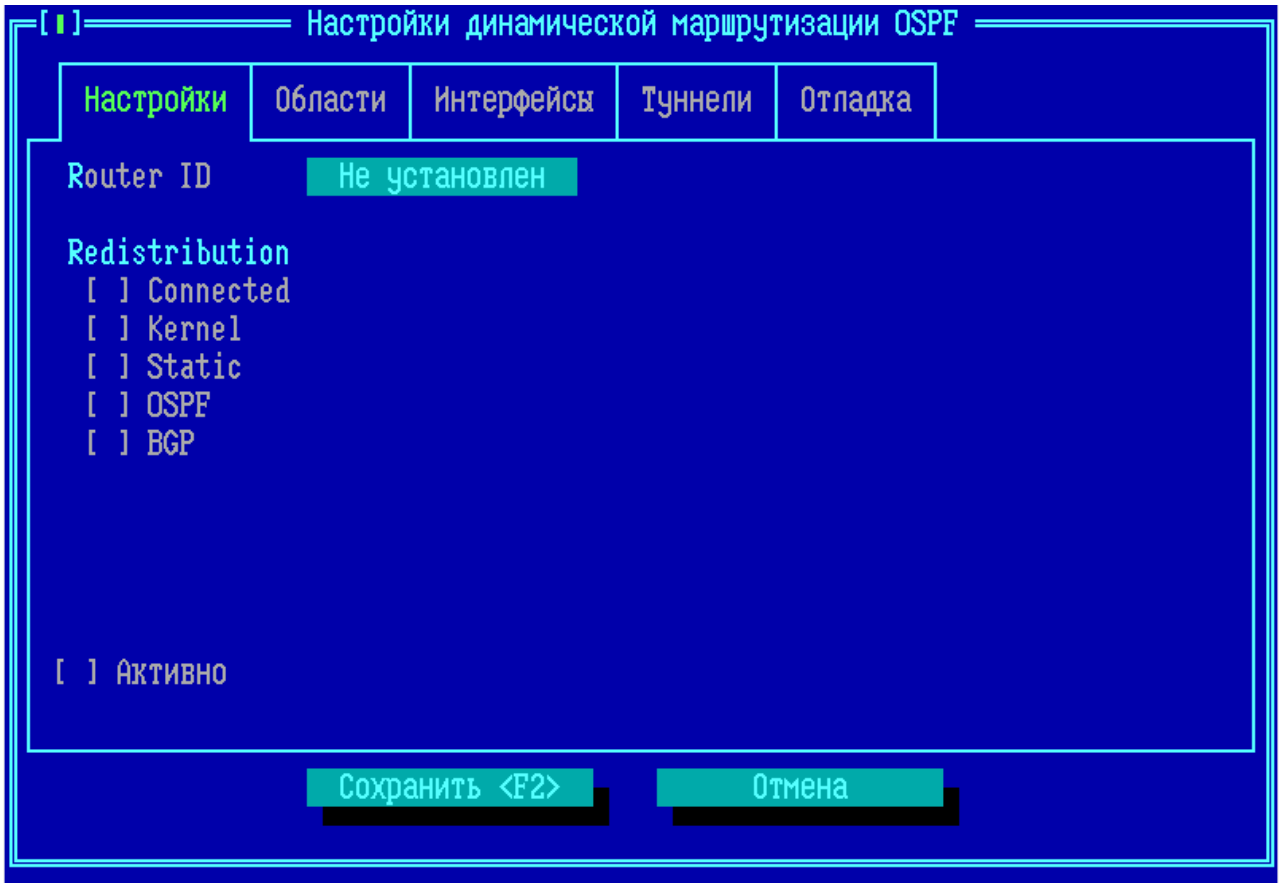


Рисунок 318 - Вкладка «Настройки»

Для включения ФПСУ в домен маршрутизации требуется идентификатор, на вкладке **Настройки** задайте «Router ID».

Router ID - идентификатор маршрутизатора OSPF, 32-разрядное значение в формате адреса IPv4. Идентификатор маршрутизатора служит уникальным обозначением маршрутизатора OSPF, может совпадать с IP-адресом интерфейса ФПСУ . Если «Router ID» дублируется для какого-то маршрутизатора или ФПСУ в домене маршрутизации, отношения смежности с этим устройством не будут установлены. Для работы протокола OSPF необходимо, чтобы данный ФПСУ сформировал отношения смежности с соседними устройствами, иначе ФПСУ не сможет обмениваться информацией о состоянии каналов с соседними устройствами, маршруты соседних устройств не будут добавлены в таблицу маршрутизации этого ФПСУ.

Информация о статических маршрутах, маршрутах с прямым подключением, маршрутах из другого протокола динамической маршрутизации может быть перераспределена в протокол OSPF с помощью перераспределения маршрутов.

Перераспределение маршрутов позволяет избегать конфликтов маршрутов на ФПСУ при использовании протоколов динамической маршрутизации.

Флаги Redistribution - перераспределение маршрутов из указанных источников в OSPF. В таблице маршрутов ФПСУ объявляются маршруты, которые будут добавлены из других источников.

Connected – напрямую подключенные маршруты;
Kernel – маршруты, установленные во время загрузки из настроек абонентов ФПСУ;
Static – статические маршруты из настроек портов ФПСУ;
OSPF – динамические маршруты протокола OSPF;
BGP – динамические маршруты протокола BGP.

Установленный флаг *«Активно»* включает протокол OSPF.

Для дальнейшей настройки протокола OSPF необходимо перейти на следующую вкладку.

Для выхода в меню с сохранением настроек протокола OSPF, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

8. 4. 1. 2. Области

На вкладке **Области** задаются области OSPF, включается аутентификация пакетов в области.

Домен маршрутизации может быть определен в одной области - магистральной области, также может быть расположен в нескольких областях, обеспечивая иерархическую маршрутизацию. В случае, если домен объединяет несколько областей:

- сеть сегментируется, уменьшаются или исключаются потоки трафика маршрутизации между областями;
- в таблицах маршрутизации сокращается количество записей, сетевые адреса могут быть суммированы на границах областей;
- уменьшается размер областей и сокращается потребление ресурсов ЦП и памяти ФПСУ;
- при изменении топологии сети в пределах области ФПСУ выполнит алгоритм поиска кратчайшего пути (алгоритм SPF) в пределах этой области, в остальных областях перерасчет алгоритма SPF не производится, а только обновляются таблицы маршрутизации;
- сокращается количество объявлений LSA о состоянии канала в домене маршрутизации, рассылка LSA ограничена пределами области.

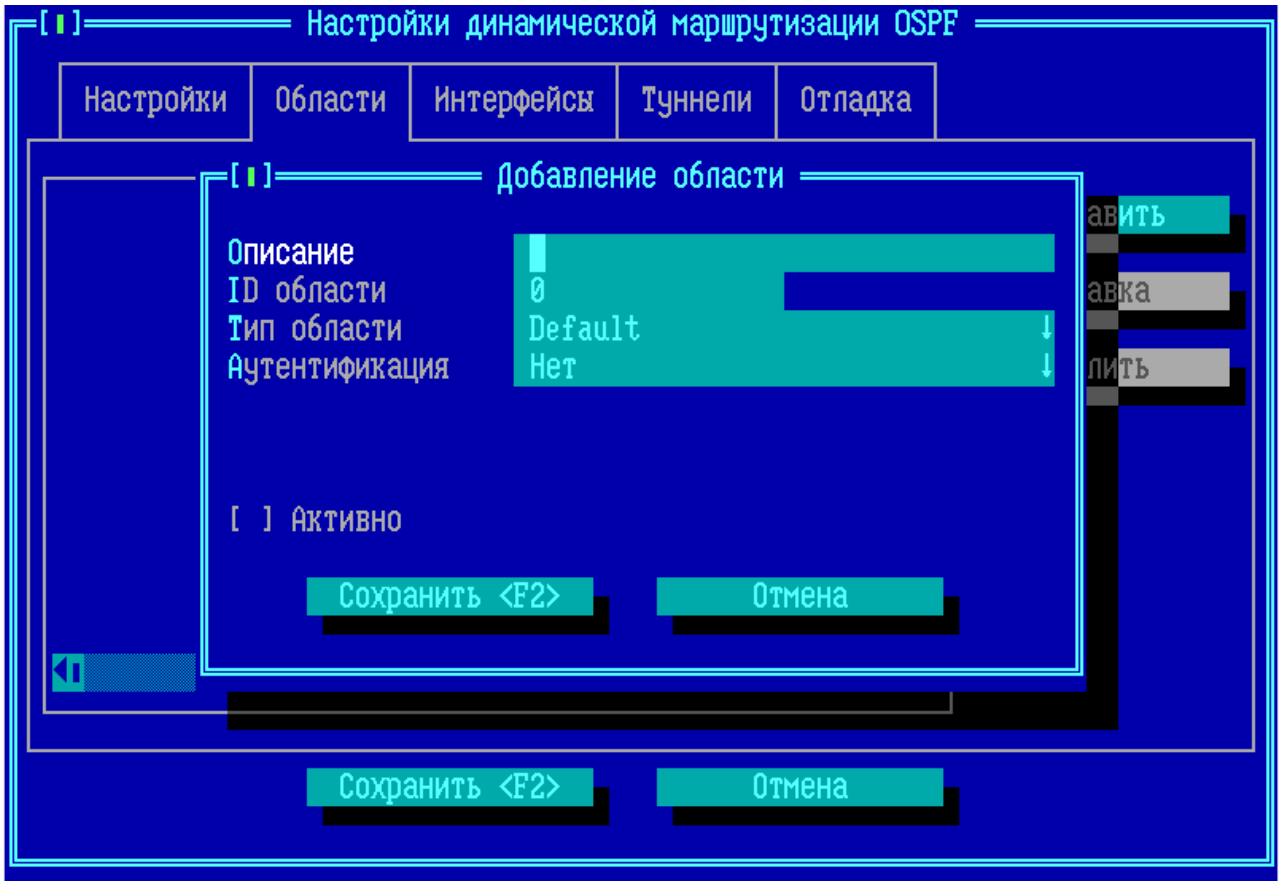


Рисунок 319 - Вкладка «Области»

По умолчанию, области OSPF на ФПСУ не заданы. Для указания области, в которую входит ФПСУ, обязательно указываются идентификатор и тип.

Для описания области укажите следующие параметры:

Описание – текстовое наименование области.

ID области – идентификатор области OSPF, в которую ФПСУ передает пакет; обязательный параметр. ID области должен быть уникальным в пределах домена маршрутизации.

Тип области – области OSPF подразделяются на типы, в зависимости от того какие типы LSA сообщений в них пересылаются; обязательный параметр.

- *Default* – магистральная область (Backbone area, область 0) является ядром сети OSPF. Присутствует всегда, через неё проходит весь сетевой трафик. Должна быть смежной с другими областями, распространяет маршруты между другими областями. Разрешены LSA1 (объявления о состоянии интерфейса от маршрутизатора), LSA2 (объявления о сети от выделенного маршрутизатора DR), LSA3 (объявления о маршрутах в другую область от ABR), LSA4 (объявления о

присутствии ASBR в других областях от ABR), LSA5 (объявления о маршрутах других доменов маршрутизации от ASBR).

- *Stub* – область не принимает информацию о внешних маршрутах для домена маршрутизации, но принимает маршруты из других областей. Для передачи информации за границу домена используется маршрут по умолчанию. Разрешены LSA1, LSA2, LSA3. LSA5 из сторонних областей при попадании в область Stub преобразовывается в LSA3 с информацией о маршруте по умолчанию. В области нет ASBR (граничного маршрутизатора домена маршрутизации).
- *Stub no-summary* – область не принимает информацию о внешних маршрутах для домена маршрутизации и маршруты из других областей. Если маршрутизаторам необходимо передавать информацию за пределы области, то они используют маршрут по умолчанию. Разрешены LSA1, LSA2. LSA3 и LSA5 из соседних областей заменяются на один LSA3 с маршрутом по умолчанию.
- *NSSA (Not-So-Stubby Area)* – область отправляет внешние маршруты в другие области, принимает маршруты из других областей. Для передачи информации за границу домена используется маршрут по умолчанию. Разрешены LSA1, LSA2, LSA3, LSA4, LSA7 (объявления о маршрутах других доменов маршрутизации в NSSA). Маршрутизатор ABR (граничный маршрутизатор области) в области NSSA преобразует LSA7 в LSA5 и распространяет сведения о внешних маршрутах в соседние области. В области есть ASBR.

Аутентификация – способ аутентификации пакетов в области OSPF, позволяет защитить паролем пересылаемые в области пакеты. При задании аутентификации ФПСУ проверяет источник каждого принятого пакета обновления путем обмена ключами аутентификации, которые известны отправителю и получателю пакета. ФПСУ принимает маршрутную информацию только от устройств, сконфигурированных с теми же параметрами аутентификации. Возможные значения:

- *нет* – при передаче пакетов не используется аутентификация;
- *простая* – аутентификация пакетов на основе пароля;
- *MD5* – аутентификация пакетов на основе алгоритма хэширования MD5.

Простая аутентификация на основе пароля позволяет настраивать для каждой области свой пароль. Пароль передается в открытом виде. Необходимо задать ***Пароль***, комбинацию символов от 1 до 16. Все интерфейсы маршрутизаторов из одной и той же области должны иметь одинаковый пароль.

При аутентификации на основе алгоритма хэширования MD5 для области задается ***Пароль***, комбинация символов от 1 до 16, и ***ID пароля***, число от 1 до 255, по умолчанию 1. Алгоритм MD5 используется для вычисления хэш-значения из содержимого пакета OSPF и

пароля. Значение хэша передается в пакете вместе с идентификатором пароля и неубывающим порядковым номером. Для корректной работы аутентификации MD5 необходимо, чтобы на всех интерфейсах маршрутизаторов из одной и той же области, были заданы одинаковый пароль аутентификации и одинаковый идентификатор ID пароля.

На ФПСУ может быть задана аутентификация пакетов в области OSPF и аутентификация пакетов отдельного интерфейса, приоритетной является аутентификация пакетов интерфейса.

Активно – при включении флага активируются настройки области OSPF.

Для дальнейшей настройки протокола OSPF необходимо перейти на следующую вкладку.

Для выхода в меню с сохранением настроек протокола OSPF, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

8. 4. 1. 3. Интерфейсы и туннели

На вкладке **Интерфейсы** выводятся сведения о настроенных интерфейсах статической маршрутизации.

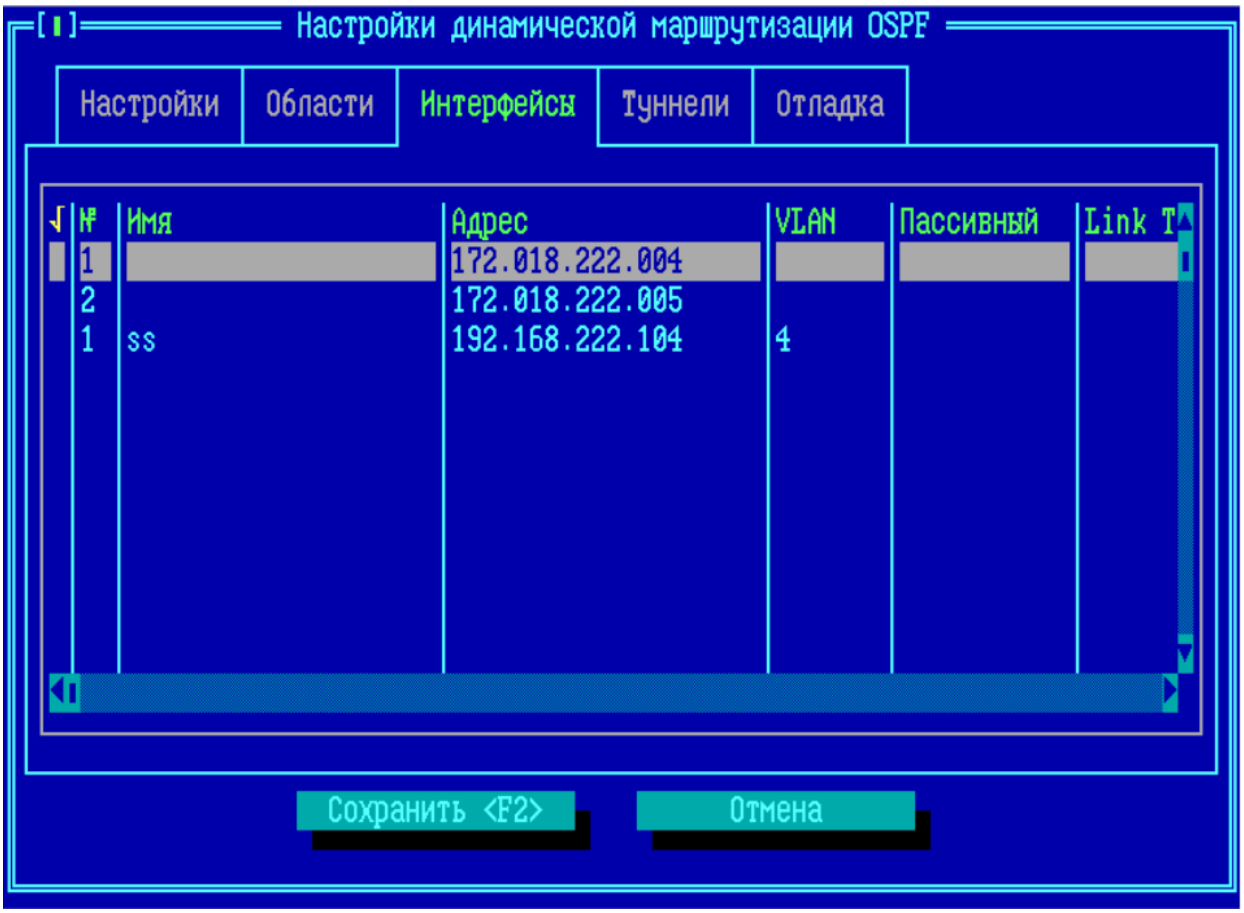


Рисунок 320 - Вкладка «Интерфейсы»

В списке отображаются интерфейсы, описанные на портах ФПСУ. Для каждого интерфейса выводятся: IP-адрес, имя, идентификатор VLAN, признак пассивного интерфейса, тип соединения, идентификатор области OSPF, стоимость, приоритет. Описание указываемых параметров приведено далее по тексту.

На вкладке **Туннели** отображаются сведения о туннелях с другими ФПСУ, работающими в паре с данным ФПСУ.

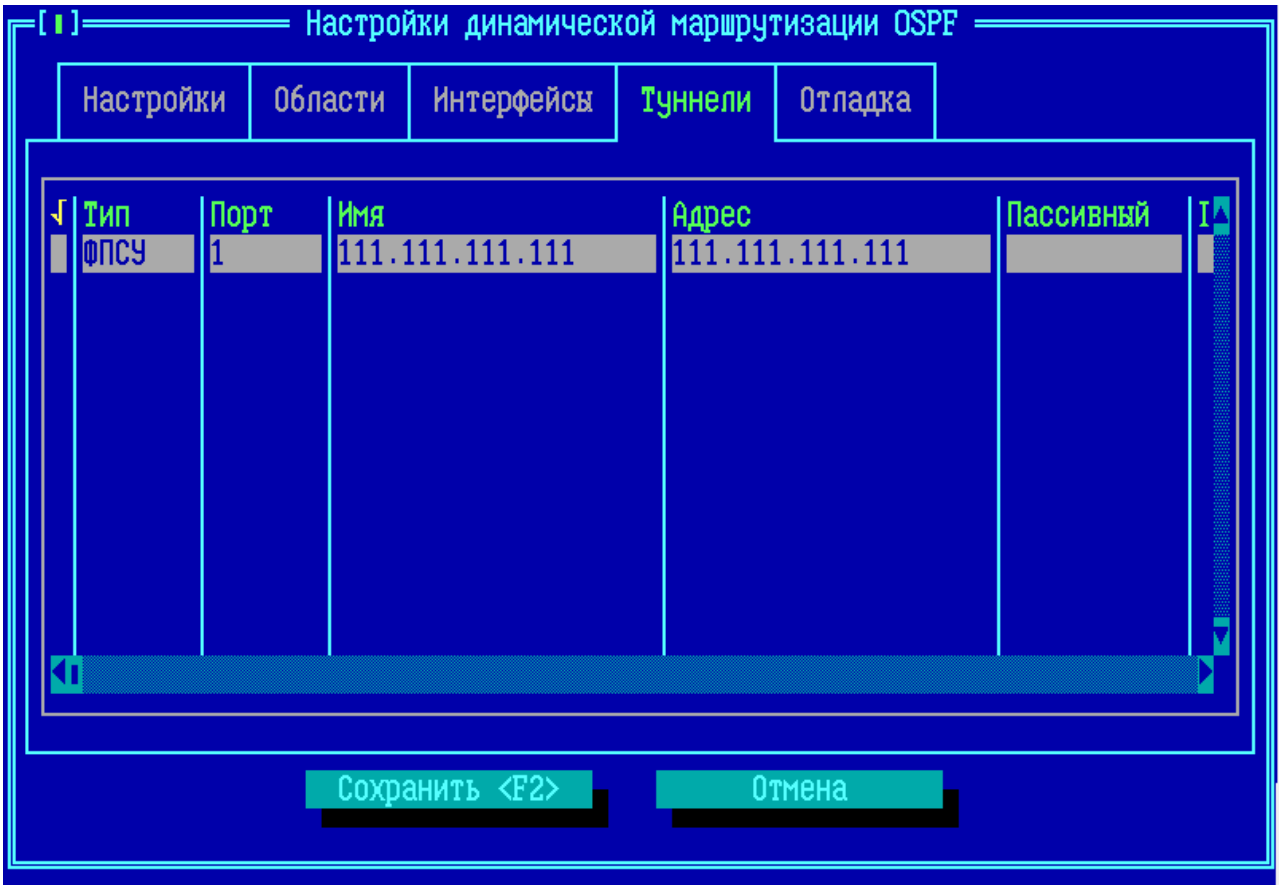
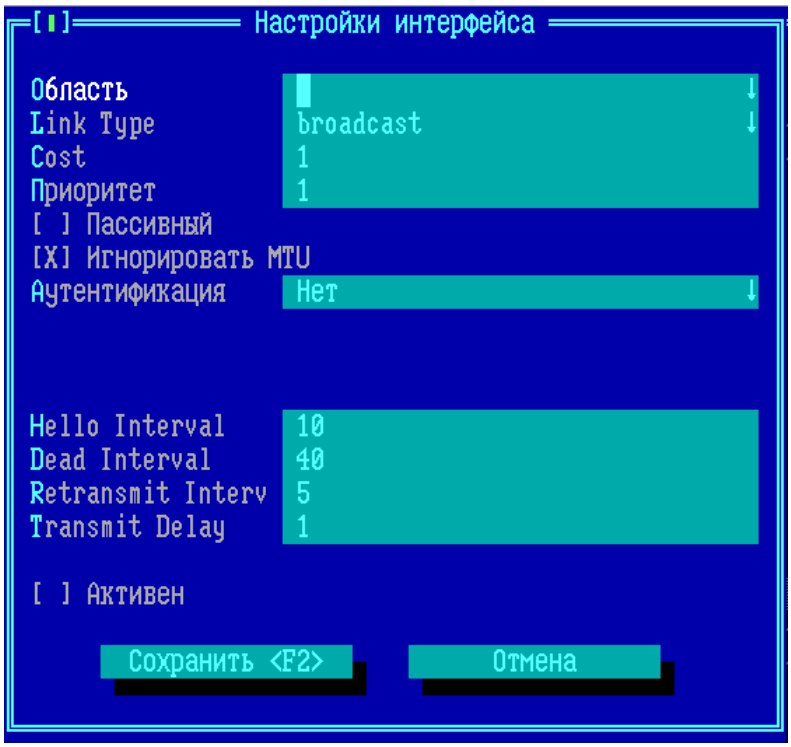


Рисунок 321 - Вкладка «Туннели»

В списке отображаются туннели с ФПСУ, описанные на портах. Для каждого туннеля выводится следующая информация: порт, имя, IP-адрес порта к которому привязан туннель, идентификатор VLAN, признак пассивного интерфейса, идентификатор области OSPF, стоимость интерфейса, приоритет. Описание указываемых параметров приведено далее по тексту.

Окно изменения настроек интерфейса или туннеля с ФПСУ открывается по нажатию клавиши *«Enter»* на выделенной строке.



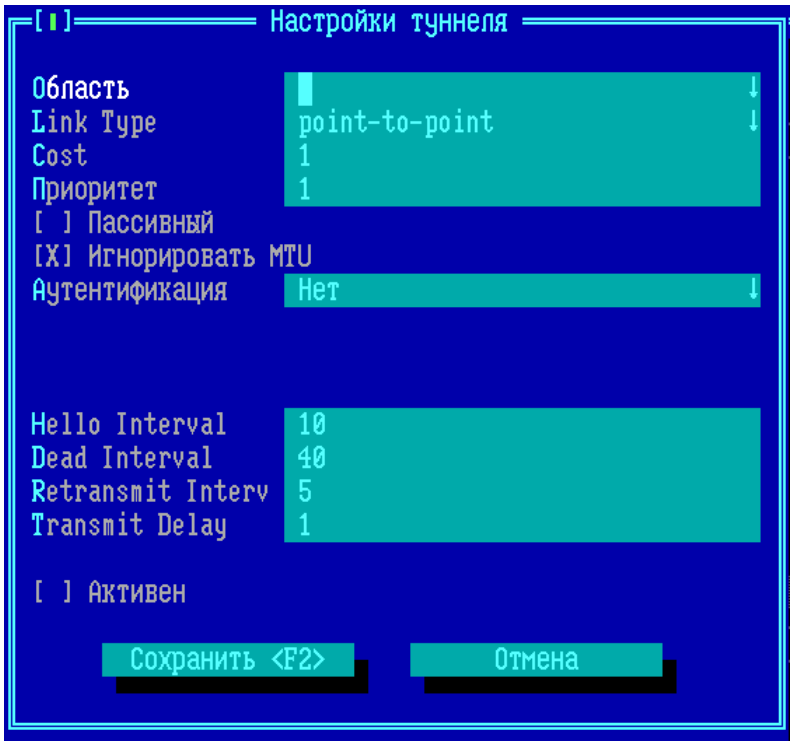


Рисунок 322 - Настройки интерфейса или туннеля

Редактируются следующие параметры:

Область – необходимо выбрать идентификатор области OSPF для включения интерфейса или туннеля в маршрутизацию OSPF. По умолчанию область не задана, интерфейс в маршрутизации OSPF не участвует.

Link type – тип сети OSPF. Задаются следующие значения:

Broadcast – широковещательная сеть с множественным доступом, состоит из нескольких маршрутизаторов, подключенных между собой по сети Ethernet. Все маршрутизаторы в сети принимают все широковещательные кадры и кадры групповой рассылки. Используется групповая рассылка Hello пакетов для автоматического определения соседей. IP-адреса соседей выдаются из одной подсети. В сети broadcast выбирается выделенный маршрутизатор DR и резервный выделенный маршрутизатор BDR, выделенный маршрутизатор управляет количеством смежностей и переполнением объявлений состояния канала в сети. Необходимо, чтобы сеть поддерживала полно-связную топологию. По умолчанию для интерфейса установлен тип сети broadcast.

Non-broadcast – не широковещательная сеть OSPF. Соседние маршрутизаторы настраиваются вручную. В сети производятся выборы DR и BDR маршрутизаторов, DR и BDR могут быть выбраны администратором. DR и BDR должны быть связаны со всеми остальными маршрутизаторами сети. Допускается сеть с частично-связной топологией. IP-адреса соседей выдаются из одной подсети.

Point-to-multipoint – сеть рассматривается как совокупность каналов «Point-to-point». Используется групповая рассылка для автоматического определения соседей, но не производятся выборы DR и BDR маршрутизаторов. Сеть с частично-связной топологией и топологией «звезда». Каждый маршрутизатор соединяется с другим набором виртуальных каналов, которые конфигурируются вручную. IP-адреса соседей выдаются из одной подсети.

Point-to-point – сеть состоит из единственной пары маршрутизаторов, один канал соединяет два маршрутизатора (например, по протоколам HDLC или PPP). Для каждого логического канала используется своя подсеть. Установка отношений смежности осуществляется автоматически с помощью периодической рассылки hello пакетов. В такой сети отключен процесс выбора DR/BDR. По умолчанию для туннеля установлен тип сети point-to-point.

Cost – Стоимость интерфейса обратно пропорциональна его пропускной способности. Маршрут с более низкой стоимостью является оптимальным по сравнению с маршрутом с более высокой стоимостью. Значение по умолчанию 1.

Приоритет – число от 0 до 255, по умолчанию 1. Приоритет определяет выбор маршрутизатора в качестве выделенного маршрутизатора DR или резервного выделенного

маршрутизатора BDR в широковещательных сетях. Маршрутизатор с наибольшим приоритетом в сегменте сети станет DR для этого сегмента, процесс выбора повторяется для BDR. Если у интерфейсов одинаковый приоритет, то в качестве DR/BDR будет выбран маршрутизатор с большим значением Router ID. Маршрутизатор с нулевым значением приоритета не может быть выбран DR/BDR и становится DROTHER. Если отношения смежности установлены, при изменении приоритета у одного из маршрутизаторов перевыборы DR и BDR не происходят. Процесс перевыборов DR/BDR запускается в случае недоступности DR или BDR в сети.

Флаг «Пассивный» – при включении флага запрещается рассылка сообщений об обновлении маршрутизации через интерфейс, но разрешается объявление этой сети для других маршрутизаторов.

Флаг «Игнорировать MTU» – при включении флага будет игнорироваться значение MTU интерфейсов при установлении смежности между соседними маршрутизаторами.

Аутентификация – способ аутентификации пакетов интерфейса, позволяет защитить пересылаемые между интерфейсами пакеты паролем. При задании аутентификации ФПСУ проверяет источник каждого принятого пакета обновления путем обмена ключами аутентификации, которые известны отправителю и получателю пакета. ФПСУ принимает маршрутную информацию только от устройств, сконфигурированных с теми же параметрами аутентификации. Возможные значения:

- *нет* – при передаче пакетов не используется аутентификация;
- *простая* – аутентификация пакетов на основе пароля;
- *MD5* – аутентификация пакетов на основе алгоритма хэширования MD5.

Простая аутентификация на основе пароля позволяет настраивать для каждого интерфейса свой пароль. Пароль передается в открытом виде. Необходимо задать ***Пароль***, комбинацию символов от 1 до 16. Соседние маршрутизаторы должны иметь одинаковый пароль.

При аутентификации на основе алгоритма хэширования MD5 для интерфейса задается ***Пароль***, комбинация символов от 1 до 16, и ***ID пароля***, число от 1 до 255, по умолчанию 1. Алгоритм MD5 используется для вычисления хэш-значения из содержимого пакета OSPF и пароля. Для корректной работы аутентификации MD5 необходимо, чтобы на соседних маршрутизаторах были заданы одинаковый пароль аутентификации и одинаковый идентификатор ID пароля.

Hello interval – интервал приветствия; целое, не отрицательное число, по умолчанию 10 секунд. Период времени между отправкой пакетов приветствия маршрутизатором.

Dead interval – интервал простоя; по умолчанию в 4 раза превышает интервал приветствия. Период времени, по истечении которого соседний маршрутизатор считается неисправным, если от него не приходит hello-пакет.

Интервалы OSPF должны быть одинаковыми на соседних маршрутизаторах, иначе отношения смежности не установятся.

Retransmit Interv – интервал повторной передачи информации о потерянных соединениях; по умолчанию равен 5 секундам. Период времени, по истечении которого маршрутизатор повторно отправит пакет, на который не получил подтверждения о получении. Маршрутизатор посылает объявления о состоянии соединения (LSA) своим соседям, он содержит в себе предыдущий LSA до тех пор пока не получит ответ. Если маршрутизатор не получит ответа вовремя, он будет продолжать раздавать старый LSA.

Transmit Delay – задержка передачи информации о состоянии соединения; по умолчанию равен 1 секунде. Период времени, необходимый для отправки пакета обновления о состоянии интерфейса.

Активен - при включении флага активируются настройки интерфейса или туннеля. Если интерфейс или туннель не активен, он не участвует в маршрутизации OSPF.

В списке активированный интерфейс или туннель отмечен знаком «√».

Для выхода в меню с сохранением настроек протокола OSPF, нажмите кнопку «Сохранить» или клавишу *<F2>*. Для выхода без сохранения настроек нажмите клавишу *<Esc>*.

8. 4. 1. 4. Отладка

На вкладке **Отладка** настраивается вывод отладочной информации протокола. Данная информация записывается в файл, который можно скопировать из меню ФПСУ «Настройка дополнений → FRR → Скопировать логи» на USB-носитель (см. пункт «Выдача файла отладки OSPF»).

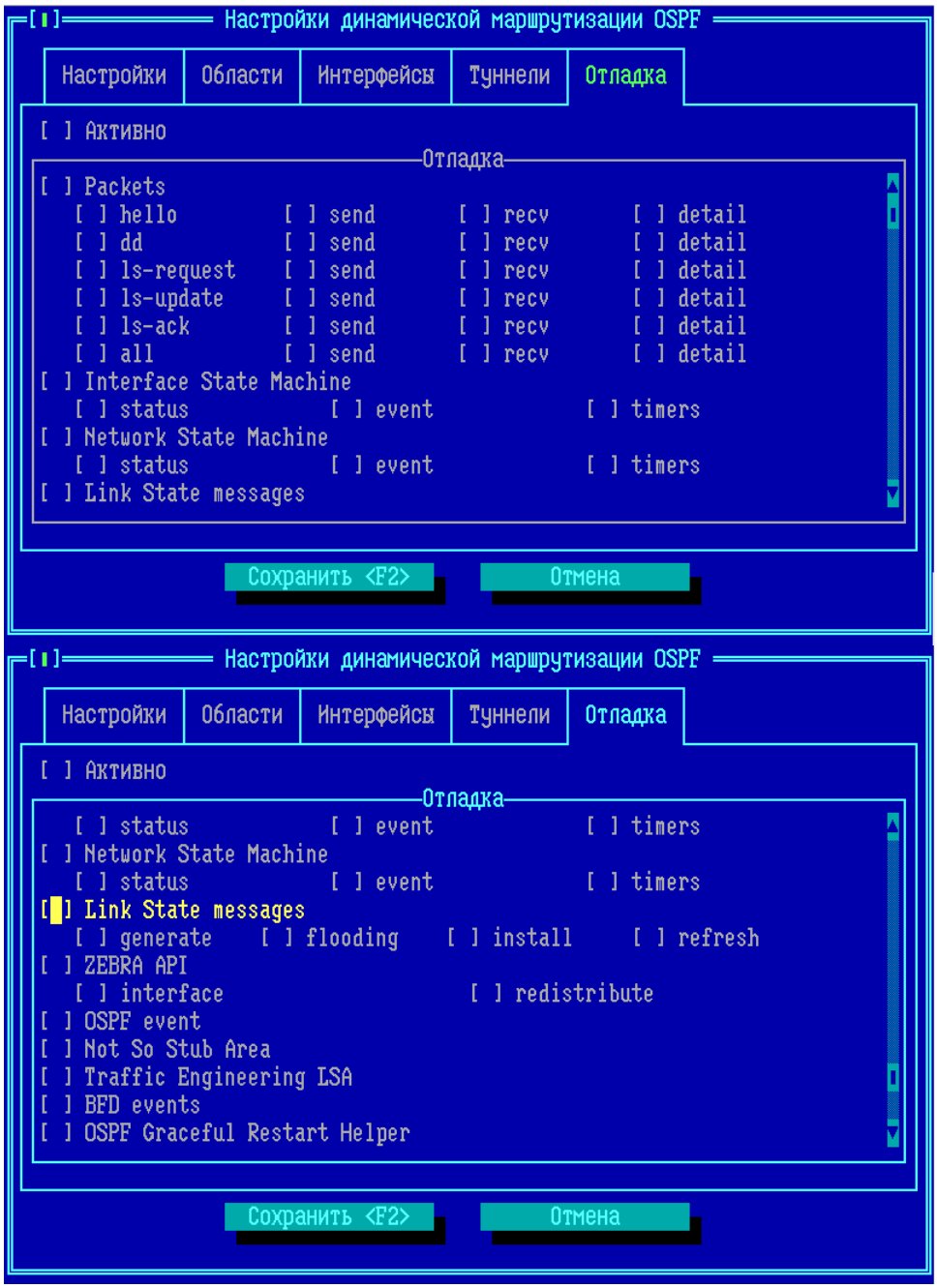


Рисунок 323 - Вкладка «Отладка»

Для выхода в меню с сохранением настроек протокола OSPF, нажмите кнопку «Сохранить» или клавишу *<F2>*. Для выхода без сохранения настроек нажмите клавишу *<Esc>*.

8. 4. 2. Динамическая маршрутизация BGP

Динамическая маршрутизация может быть настроена с помощью протокола BGP (Border Gateway Protocol).

BGP – протокол динамической маршрутизации, обеспечивает междоменную маршрутизацию. BGP предназначен для обмена маршрутной информацией между автономными системами. Автономные системы BGP являются отдельными доменами маршрутизации с локальными политиками, на которые разделены глобальные внешние сети. Информация о достижимости сетей между автономными системами передается вместе с атрибутами пути, с помощью которых выбирается наилучший маршрут. Соединение между взаимодействующими ФПСУ и маршрутизаторами, принадлежащими различным автономным системам, организуется посредством внешнего протокола eBGP.



Рисунок 324 - Схема сети с маршрутизацией на основе BGP

Внутренний протокол iBGP внутри автономных систем не поддерживается.

По умолчанию, динамическая маршрутизация отключена на ФПСУ.

Настройки динамической маршрутизации открываются из пункта меню «Порты ФПСУ → Динамическая маршрутизация BGP».

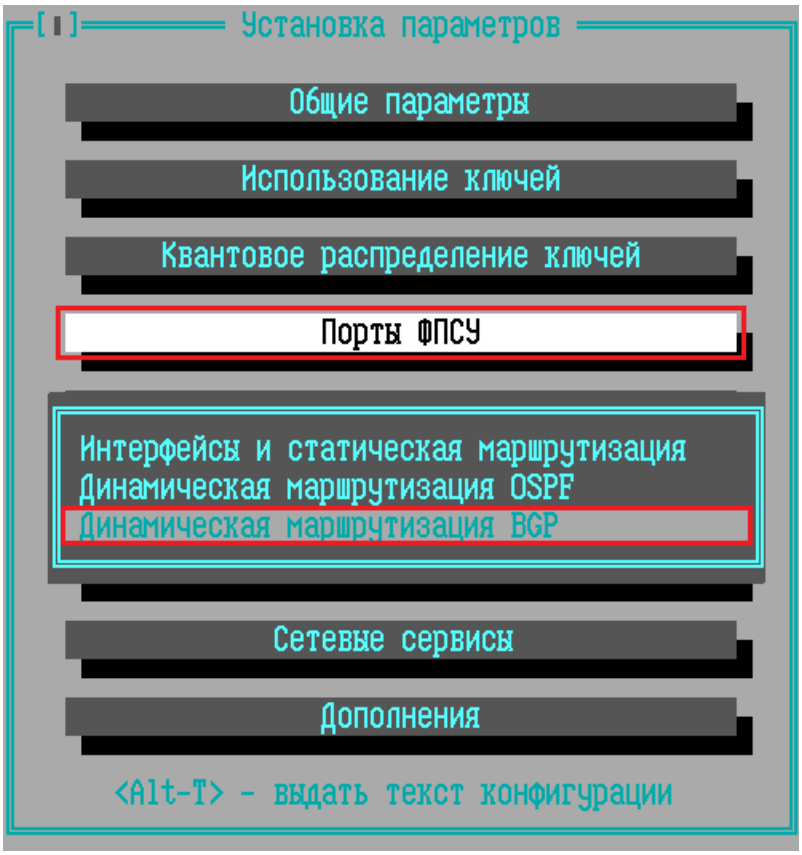


Рисунок 325 - Подменю команды «Порты ФПСУ»

В окне «Настройки динамической маршрутизации BGP» находятся вкладки с настраиваемыми параметрами протокола. Переход с активной вкладки на соседнюю осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

Для включения ФПСУ в протокол BGP требуется указать номер автономной системы Local AS и идентификатор Router ID, включить протокол на вкладке «General», задать соседей на вкладке «Peers».

Конфигурация протокола BGP записывается в файл bgpd.conf после запуска ФПСУ (см. пункт «Дополнения»).

На каждой вкладке необходимо указать обязательные для настройки протокола BGP параметры:

- General
- Networks
- Peers
- Prefix-list
- Route Map-list

- AS Path-list
- Community-list

Для выхода в меню с сохранением настроек протокола BGP, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

8. 4. 2. 1. General

На вкладке **General** включается протокол BGP и добавляются маршруты из других источников.

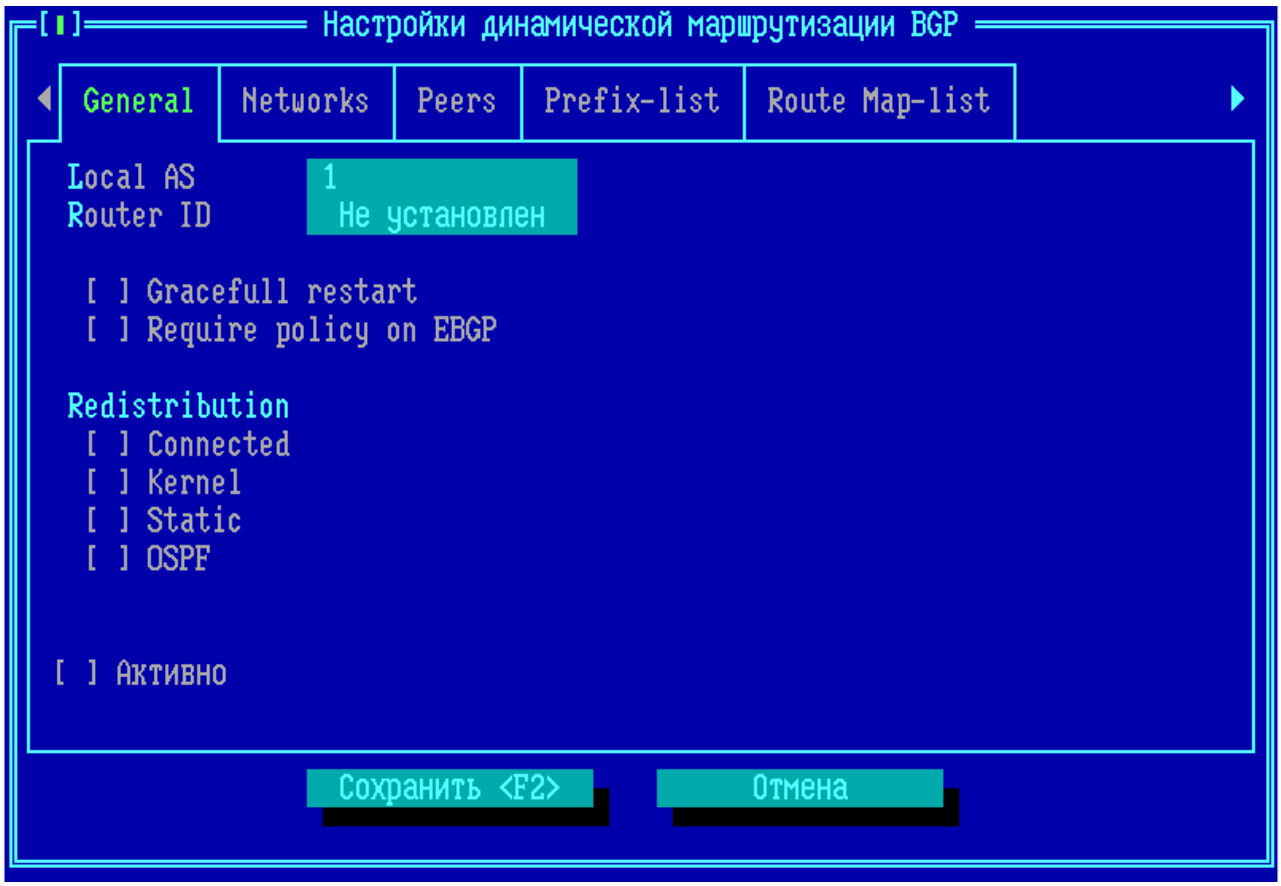


Рисунок 326 - Вкладка «General»

Local AS – идентификатор локальной автономной системы; 32-битное число указывается в формате asplain - простое число, либо в формате asdot - два 16-битных числа, разделенных точкой.

Router ID – идентификатор маршрутизатора BGP, 32-разрядное значение в формате адреса IPv4. Идентификатор маршрутизатора служит уникальным обозначением однорангового узла BGP в сети, может совпадать с IP-адресом интерфейса ФПСУ. Если

«Router ID» дублируется для какого-то маршрутизатора или ФПСУ, BGP-сессия с этим устройством не будет установлена. Для работы протокола BGP необходимо, чтобы данный ФПСУ сформировал отношения соседства с соседними устройствами, иначе BGP-соседи не смогут обмениваться информацией о маршрутах через сообщения обновления, маршруты соседних устройств не будут добавлены в таблицу маршрутизации этого ФПСУ.

Одноранговым узлом, BGP-узлом, называется устройство (ФПСУ или маршрутизатор), поддерживающее протокол BGP, которое имеет активное TCP-соединение с другим устройством, поддерживающим BGP.

BGP-спикер - устройство (ФПСУ или маршрутизатор), которое обменивается маршрутами с другим устройством (BGP-спикером) по протоколу BGP.

Graceful restart – установленный флаг включает глобальный режим плавного перезапуска ФПСУ, возможность сохранения маршрутов в плоскости пересылки во время перезапуска плоскости управления данного ФПСУ. ФПСУ, являясь BGP-спикером, сохраняет состояние пересылки во время перезапуска BGP. Информация о маршрутах временно сохраняется при завершении и повторном установлении TCP-сессии с BGP-узлом до завершения первоначального обновления маршрутизации на перезапускаемом ФПСУ. В этот период BGP-узел помечает любые маршруты, связанные с перезапускаемым ФПСУ, как «устаревшие», но продолжает использовать эти маршруты для пересылки пакетов. BGP-узел не передает какие-либо изменения состояния перезапускаемого ФПСУ ни одному из своих соседей. BGP-узел отправляет обновления BGP, чтобы перезапускающийся ФПСУ мог повторно получить свою информационную базу маршрутизации BGP - RIB.

Graceful restart может быть включен на уровне протокола и на уровне внешнего BGP-узла. Глобальный режим Graceful restart включается для всех внешних BGP-узлов.

Require policy on EBGP – установленный флаг включает обмен маршрутами с внешними BGP-узлами на основе политик. Отправка и получение маршрутов внешним BGP-узлам разрешены только при наличии политик на основе карт входящих и исходящих маршрутов, согласно RFC 8212. Никакие маршруты не будут отправлены внешним BGP-узлам или получены от них при отсутствии политик. Политики настраиваются с помощью route-map на вкладке «Route Map-list».

Информация о статических маршрутах, маршрутах с прямым подключением, маршрутах из другого протокола динамической маршрутизации может быть добавлена в протокол BGP с помощью перераспределения маршрутов. Перераспределение маршрутов позволяет избегать конфликтов маршрутов на ФПСУ при использовании протоколов динамической маршрутизации.

Флаги Redistribution – перераспределение маршрутов из указанных источников в BGP. В таблице маршрутов ФПСУ объявляются маршруты, которые будут добавлены из других источников.

Connected – напрямую подключенные маршруты;
Kernel – маршруты, установленные во время загрузки из настроек абонентов ФПСУ;
Static – статические маршруты из настроек портов ФПСУ;
OSPF – динамические маршруты протокола OSPF.

Активно – установленный флаг включает протокол BGP.

Для дальнейшей настройки протокола BGP необходимо перейти на следующую вкладку.

Для выхода в меню с сохранением настроек протокола BGP, нажмите кнопку «Сохранить» или клавишу *<F2>*. Для выхода без сохранения настроек нажмите клавишу *<Esc>*.

8. 4. 2. 2. Networks

На вкладке **Networks** указываются входящие в данную автономную систему подсети, ФПСУ анонсирует эти подсети по протоколу BGP внешним BGP-узлам.

Для создания подсети необходимо во вкладке нажать кнопку «Добавить».



Рисунок 327 - Добавление подсети на вкладке «Networks»

Описание – текстовое описание подсети.

Адрес – IP-адрес подсети. Объявляемая подсеть должна присутствовать в таблице маршрутизации ФПСУ, описана как абонент на одном из портов ФПСУ, либо перераспределена из протокола OSPF.

Маска – маска подсети; можно ввести значение маски непосредственно, а можно в

поле ввода нажать <*Пробел*>, после чего в появившемся окне ввести число значащих разрядов (от 1 до 30) и нажать <*Пробел*>, в таком случае ФПСУ рассчитает значение маски автоматически.

Активно – при включении флага подсеть будет анонсирована протоколом BGP. Если подсеть не отмечена флагом, она не отображается в маршрутизации BGP.

В списке запись активированной подсети отмечена знаком «√».

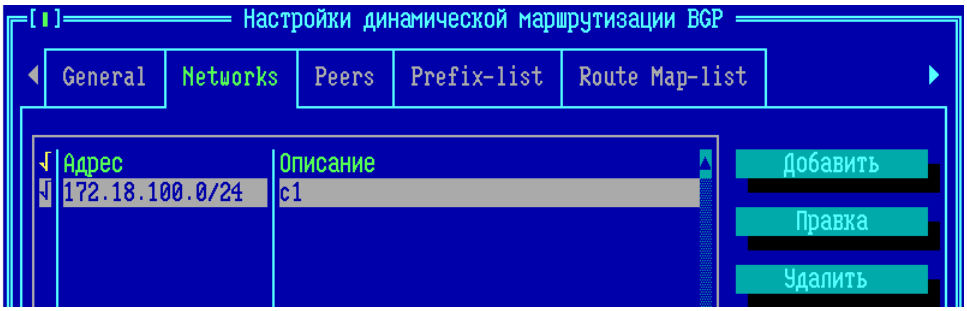


Рисунок 328 - Активированная подсеть

Для дальнейшей настройки протокола BGP необходимо перейти на следующую вкладку.

Для выхода в меню с сохранением настроек протокола BGP, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

8. 4. 2. 3. Peers

На вкладке **Peers** добавляются BGP-соседи, с которыми ФПСУ будет обмениваться маршрутной информацией.

Для создания BGP-узла необходимо во вкладке нажать кнопку «Добавить».

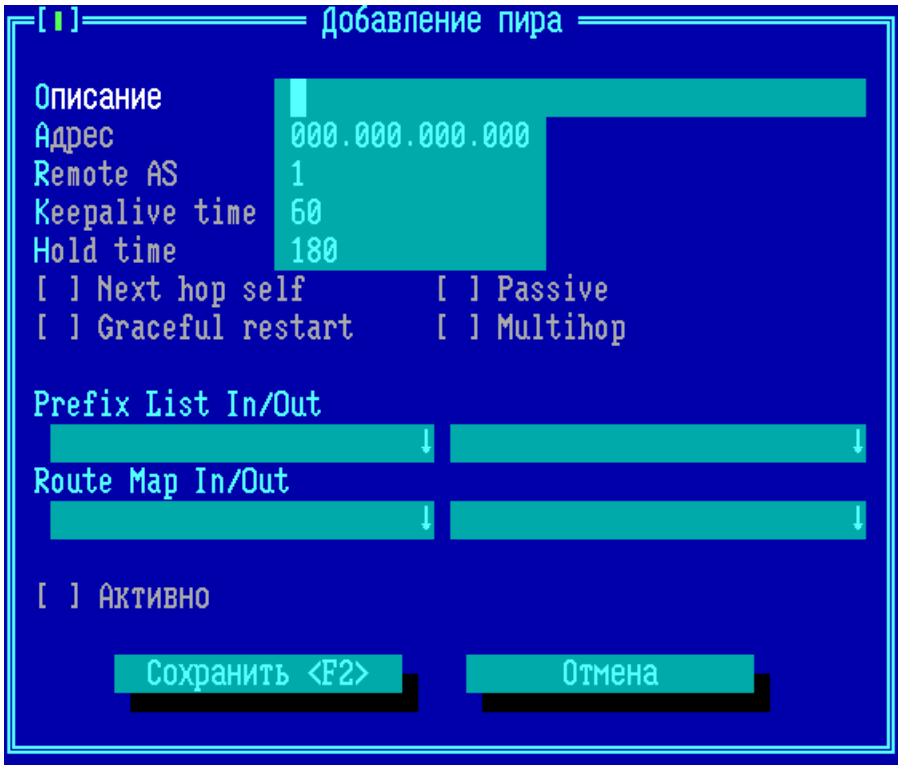


Рисунок 329 - Добавление BGP-узла на вкладке «Peers»

Описание – текстовое описание внешнего BGP-узла.

Адрес – IP-адрес внешнего BGP-узла.

Remote AS – номер автономной системы, в которой находится внешний BGP-узел.

Keepalive time – Интервал времени между отправкой сообщений Keepalive. По умолчанию 60 секунд. Сообщение Keepalive периодически отправляется между BGP-узлами, чтобы поддерживать активность TCP-соединения.

Hold time – Интервал времени, по истечении которого сосед будет считаться недоступным. По умолчанию 180 секунд. Если интервал Hold time истекает и сообщение Keepalive не получено, то BGP-узел считается недоступным.

Next hop self – при включении флага ФПСУ объявляет себя следующим узлом на маршрутах, о которых он оповещает BGP-узел.

Graceful restart – установленный флаг включает поддержку плавного перезапуска ФПСУ на внешнем BGP-узле, возможность сохранения маршрутов в плоскости пересылки во время перезапуска плоскости управления данного ФПСУ. ФПСУ, являясь BGP-спикером, сохраняет состояние пересылки во время перезапуска BGP. Информация о маршрутах временно сохраняется при завершении и повторном установлении TCP-сессии с BGP-узлом до завершения первоначального обновления маршрутизации на перезапускаемом ФПСУ. В этот период BGP-узел помечает любые маршруты, связанные с перезапускаемым ФПСУ, как «устаревшие», но продолжает использовать эти маршруты для пересылки пакетов. BGP-узел не передает какие-либо изменения состояния перезапускаемого ФПСУ ни одному из своих BGP-соседей. BGP-узел отправляет обновления BGP, чтобы перезапускающийся ФПСУ мог повторно получить свою информационную базу маршрутизации BGP - RIB (Routing Information Base).

Graceful restart может быть включен на уровне протокола и на уровне внешнего BGP-узла. Если глобальный режим Graceful restart выключен, а для внешнего BGP-узла включен, то плавный перезапуск ФПСУ будет поддерживаться только с этим BGP-узлом.

Для ограничения количества получаемых и отправляемых маршрутов BGP-узлом используются фильтры Prefix-list и Route-map.

Passive – при установлении флага BGP-узел переходит в пассивный режим и не пытается установить соединение с ФПСУ, а ожидает управляющих пакетов от ФПСУ, прежде чем начать отвечать. По умолчанию флаг отключен и BGP-узел в активном режиме пытается установить соединение с ФПСУ.

Multihop – установленный флаг позволяет устанавливать сеансы с соседями eBGP, когда они находятся на расстоянии нескольких переходов. Если сосед не подключен напрямую и флаг выключен, соединение не установится.

Prefix-list – списки префиксов используются для фильтрации маршрутов. В поле «IN» указывается список префиксов, ограничивающий маршруты, получаемые от внешнего BGP-узла. В поле «OUT» выбирается список префиксов, ограничивающий маршруты, объявляемые внешнему BGP-узлу. Списки префиксов предварительно должны быть созданы на вкладке «Prefix-list».Пример использования prefix-list при настройке исходящих и входящих маршрутов приведен в пункте «Применение prefix-list в протоколе BGP».

Route Map-list – карты маршрутов используются для настройки политик с изменением атрибутов маршрута, применяются к обновлениям маршрутов получаемым или отправляемым внешнему BGP-узлу, используются для управления таблицами маршрутов и указания условий, при выполнении которых маршруты передаются между BGP-узлами. В поле «IN» выбирается карта маршрутов, применяемая к маршрутам, получаемым от внешнего

BGP-узла. В поле «OUT» выбирается карта маршрутов, применяемая к маршрутам, отправляемым внешнему BGP-узлу. Карты маршрутов предварительно должны быть созданы на вкладке «Route Map-list».

Активно – при включении флага BGP-узел добавляется в протокол BGP, ФПСУ устанавливает BGP-сессию с данным BGP-узлом. В списке активированный BGP-узел отмечен знаком «√».

Для дальнейшей настройки протокола BGP необходимо перейти на следующую вкладку.

Для выхода в меню с сохранением настроек протокола BGP, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

8. 4. 2. 4. Prefix-list

На вкладке **Prefix-list** описываются списки префиксов. Применяется при описании BGP-узла и в карте маршрутов.

Для создания prefix-list необходимо во вкладке нажать кнопку «Добавить».

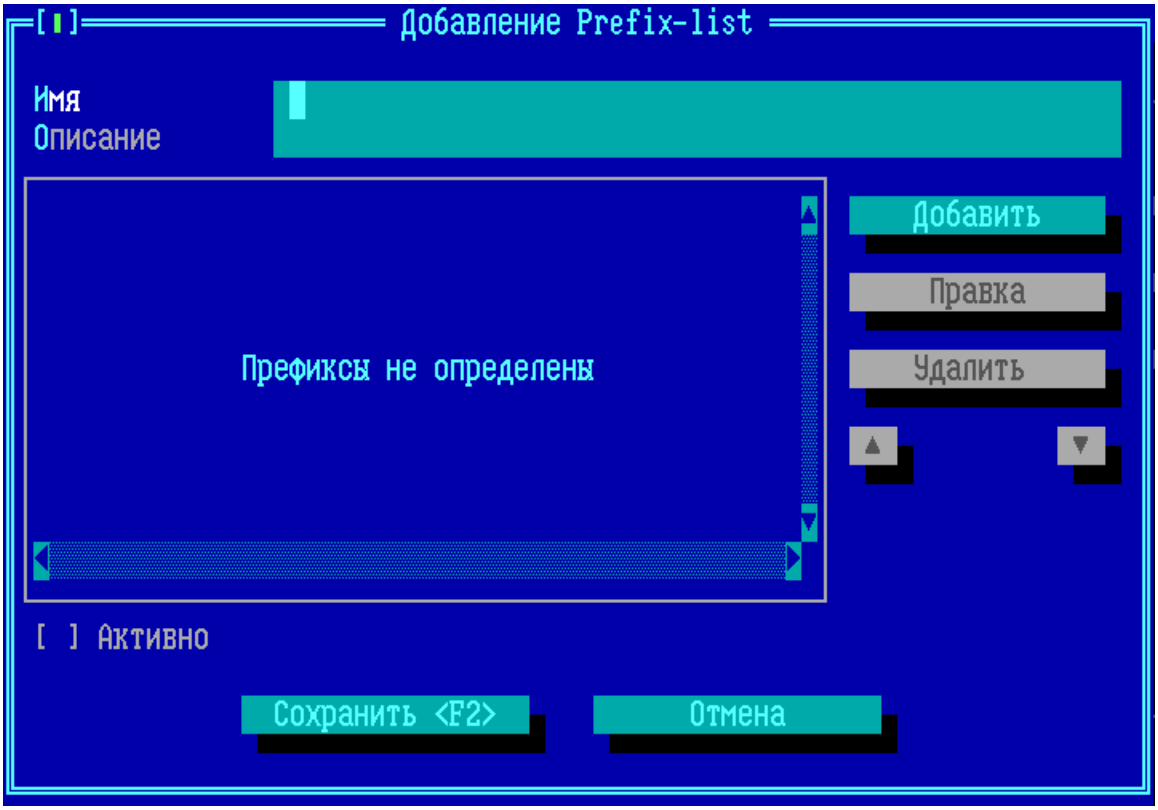


Рисунок 330 - Добавление списка префиксов на вкладке «Prefix-list»

Имя – наименование списка префиксов.

Описание – текстовое описание, уточнение применения списка для входящих или исходящих маршрутов (in/out).

Активно – при включении флага активируется список префиксов. При выключенном флаге маршруты не будут фильтроваться по списку префиксов. В списке активированный Prefix-list отмечен знаком «√».

Prefix-list состоит из правил, нумерованных записей. Правило содержит порядковый номер, разрешающее или запрещающее действие, префикс сети. Проверка соответствия маршрута префиксу производится по списку, начиная с записи префикса с наименьшим порядковым номером, до тех пор пока не будет найдено соответствие. Как только соответствие найдено, применяется указанное в правиле действие. Если соответствие не найдено, применяется неявная политика запрета по умолчанию «deny any». Важен порядок следования правил в списке.

Для добавления prefix нажмите кнопку «Добавить».

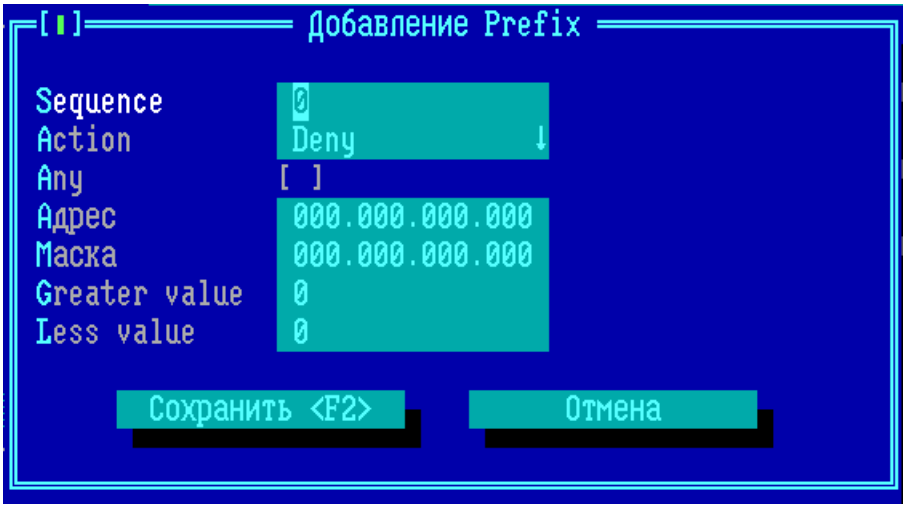


Рисунок 331 - Добавление префикса в список

Sequence – порядковый номер правила в списке префиксов, определяет порядок сканирования правил при проверке соответствия маршрута префиксу.

Action – действие правила, разрешающее или запрещающее префикс. Если префикс разрешен, то маршрут используется.

Any – любой IP-адрес, не требует задания IP-адреса и маски подсети. Действие «Action» будет распространяться на все маршруты.

Для задания префикса необходимо указать адрес и маску подсети.

Адрес – IP-адрес подсети.

Маска – можно ввести значение маски подсети непосредственно, а можно в поле ввода нажать <*Пробел*>, после чего в появившемся окне ввести число значащих разрядов (от 1 до 32) и нажать <*Пробел*>, в таком случае ФПСУ рассчитает значение маски автоматически.

Для задания диапазона префиксов необходимо указать значения маски подсети «от» и «до» с помощью параметров «Greater value» и «Less value». При указании параметров должно выполняться условие:

Маска <= Greater value <= Less value <= 32

Greater value – наименьшее значение диапазона длины (в битах) сетевой маски («от» диапазона длин).

Less value – наибольшее значение диапазона длины (в битах) сетевой маски («до» диапазона длин).

Для дальнейшей настройки протокола BGP необходимо перейти на следующую вкладку.

Для выхода в меню с сохранением настроек протокола BGP, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

8. 4. 2. 5. Route Map-list

На вкладке **Route Map-list** описываются карты маршрутов. Применяются при описании BGP-узла. С помощью карты маршрутов настраивается политика с изменением атрибута маршрута.

Для создания списка карт маршрутов необходимо во вкладке нажать кнопку «Добавить».

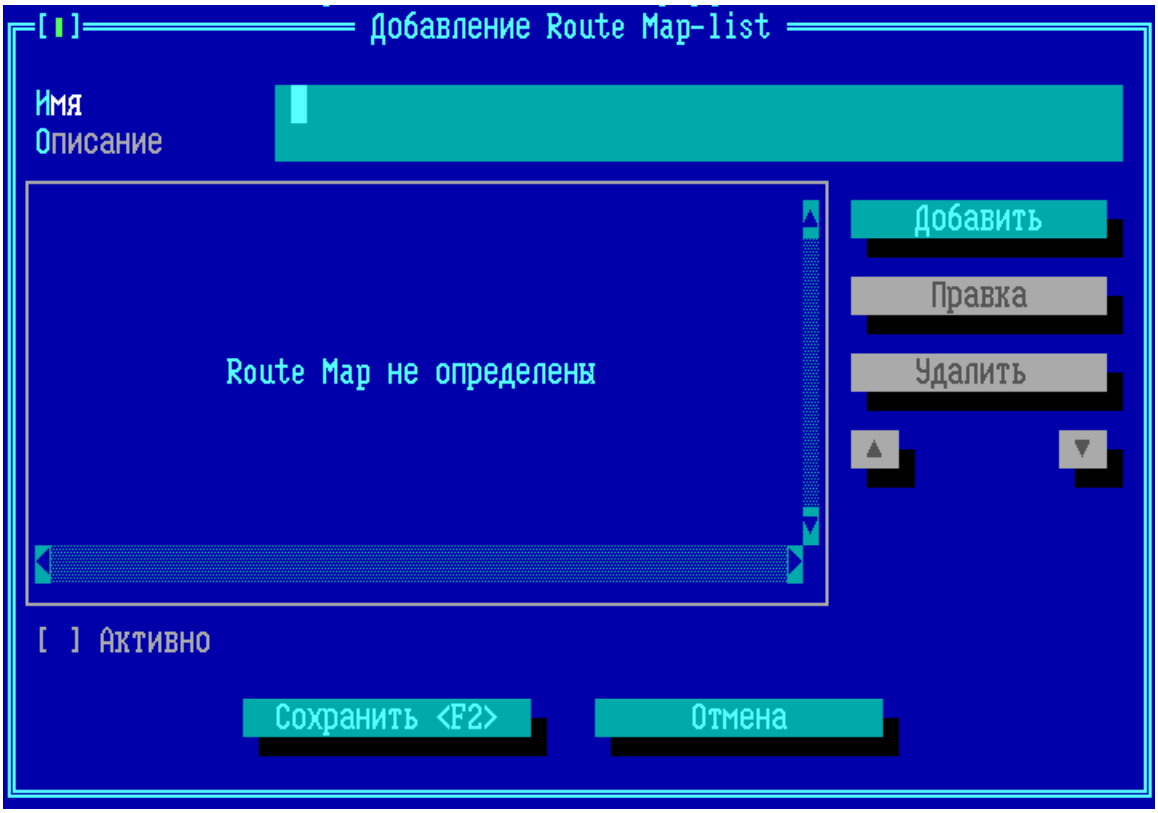


Рисунок 332 - Добавление карты маршрутов на вкладке «Route Map-list»

Имя – наименование карты маршрутов.

Описание – текстовое описание, уточнение применения карты для входящих или исходящих маршрутов (in/out).

Активно – при включении флага активируется карта маршрутов. При выключенном флаге условия карты маршрутов не будут применяться при фильтрации маршрутов. В списке активированная карта маршрутов отмечена знаком «√».

Карта маршрутов содержит список правил, нумерованные записи. Правило включает порядковый номер, разрешающее или запрещающее действие при выполнении условий фильтрации (Prefix-list, AS-Path, Community), атрибут BGP, устанавливаемый маршруту командой SET. Карта маршрутов срабатывает, если маршрут попадает под условие фильтра, для срабатывания должны быть выполнены все условия фильтра. Проверка правил производится по списку, начиная с правила с наименьшим порядковым номером, обработка карты маршрутов прекращается при обнаружении соответствия. При срабатывании применяется указанное действие и изменяется указанный атрибут маршрута.

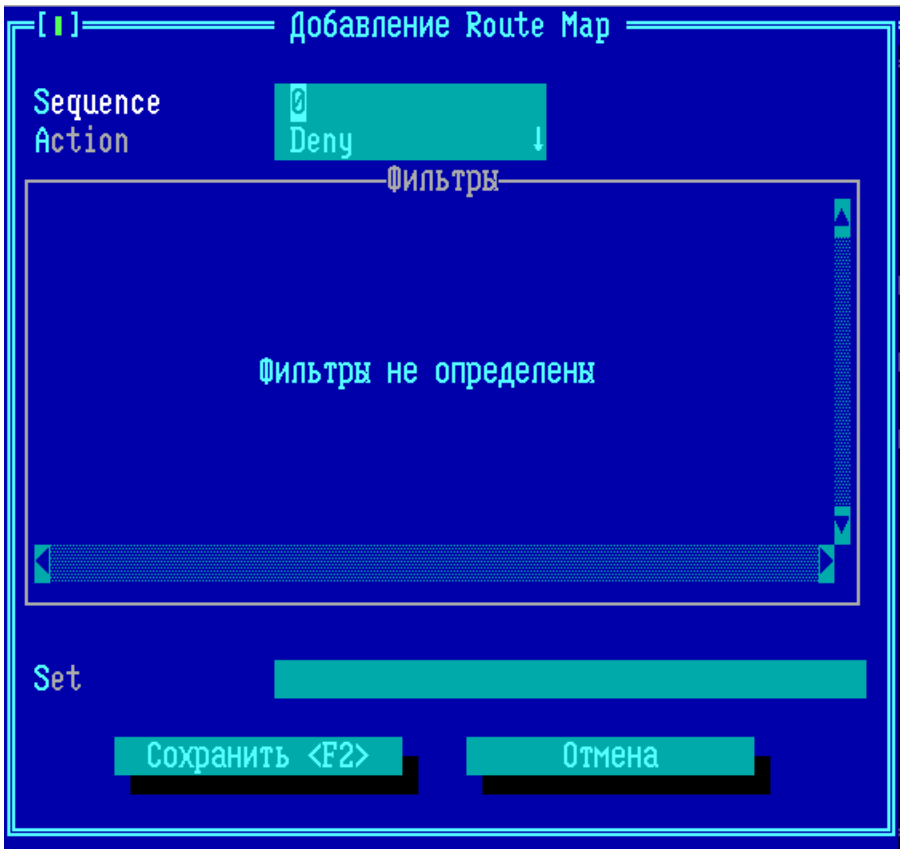


Рисунок 333 - Добавление правила карты маршрутов

Sequence – порядковый номер правила в карте маршрутов, определяет порядок сканирования правил при проверке соответствия маршрута условиям карты маршрута.

Action – действие правила, разрешающее или запрещающее.

- Permit – если маршрут совпадает с условием фильтра, выполняется действие SET (устанавливается или изменяется атрибут маршрута). Маршрут разрешается с изменением указанного атрибута маршрута.
- Deny – если маршрут совпадает с условием фильтра, обработка карты маршрута завершается отклонением маршрута.

Действие карты маршрутов по умолчанию, если маршрут не попадает ни под одно условие, он отклоняется. Чтобы изменить это поведение, необходимо задать в качестве последнего правила разрешение любых маршрутов.

Фильтры – условие попадания маршрута под данное правило. В качестве фильтра может выступать Prefix-list, AS-Path, Community. Для выбора фильтра в списке выделите строку и нажмите <*Пробел*>, в крайнем левом столбце фильтр будет отмечен знаком «√».

Set – команда SET устанавливает новое значение атрибута маршрута, если

обновление маршрута соответствует условию карты маршрутов. Список атрибутов BGP, устанавливаемых командой SET, приведен в таблице.

Таблица 9. Атрибуты BGP, изменяемые командой SET

Команда set	Описание
as-path prepend *AS_PATH*	Увеличение длины пути, добавляются лишние переходы в AS-Path при анонсировании маршрутов. Строка номеров автономных систем добавляется к AS_PATH. Может быть добавлен свой номер автономной системы
community *COMMUNITY*	Атрибут Community. устанавливает значение Community в обновлениях BGP
distance *DISTANCE*	Административное расстояние, которое будет использоваться для маршрута. Применяется локально, не распространяется среди BGP-соседей
ip next-hop *IPV4_ADDRESS*	Атрибуту следующего перехода присваивается значение IPv4. Как для входящих, так и для исходящих route map
ip next-hop *peer-address*	Атрибуту следующего перехода присваивается адрес BGP-узла. Для входящей маршрутной карты это означает, что используется IP-адрес BGP-узла. Для исходящей маршрутной карты это означает, что собственный IP-адрес ФПСУ используется для установления соединения с BGP-соседом
ip next-hop unchanged	Атрибут следующего перехода не изменяется. Изменение поведения по умолчанию атрибута NEXT-HOP для eBGP-соседа — все обновления для BGP-узла отправляются без изменения атрибута NEXT-HOP (по умолчанию, когда маршрут анонсируется eBGP-соседу, атрибут next-hop меняется на IP-адрес маршрутизатора, который анонсирует маршрут)
local-preference *LOCAL_PREF*	Атрибут LOCAL_PREF. Маршрут будет анонсироваться с новым значением атрибута. Действует внутри автономной системы, не передается в другие автономные системы

Команда set	Описание
local-preference *+LOCAL_PREF*	Добавление значения к существующему LOCAL_PREF
local-preference *-LOCAL_PREF*	Вычитание значения из существующего LOCAL_PREF
metric *METRIC*	Метрика. Атрибут используется для информирования eBGP-соседей о том, какой путь в автономную систему более предпочтительный, передается в другие автономные системы. Распространяется внутри автономной системы. Значение по умолчанию 0, чем больше значение, тем ниже приоритет. Атрибут будет влиять на выбор маршрута, в случае если атрибуты сравниваемых маршрутов WEIGHT, LOCAL_PREF, AS_PATH и ORIGIN имеют одинаковое значение
metric *<[+|-](1-4294967295)| rtt|+rtt|-rtt>*	Для атрибута метрика может быть установлено определенное значение. Значение может быть добавлено или вычтено. Значение может быть установлено временно, период временного значения метрики может быть увеличен и уменьшен
origin *ORIGIN <egp|igp| incomplete>*	Атрибут ORIGIN
tag *TAG*	Метка на выбранном маршруте. Значение этого тега изменяется от 1 до 4294967295. Значение тега преобразуется в значение области (если включена поддержка Linux Realms), затем области может быть назначена политика маршрутизации
weight *WEIGHT*	Вес маршрута. Не распространяется за пределы маршрутизатора. Чем больше значение BGP-веса, тем приоритетней данный маршрут. По умолчанию BGP-вес равен 32768 для всех маршрутов, сгенерированных данным маршрутизатором, и 0 - для всех маршрутов, полученных от соседей. Диапазон допустимых значений: 0 - 65535

Для дальнейшей настройки протокола BGP необходимо перейти на следующую

вкладку.

Для выхода в меню с сохранением настроек протокола BGP, нажмите кнопку «Сохранить» или клавишу *<F2>*. Для выхода без сохранения настроек нажмите клавишу *<Esc>*.

8. 4. 2. 6. AS Path-list

На вкладке **AS Path-list** описываются списки AS-Path. Применяется в карте маршрутов для фильтрации по пути.

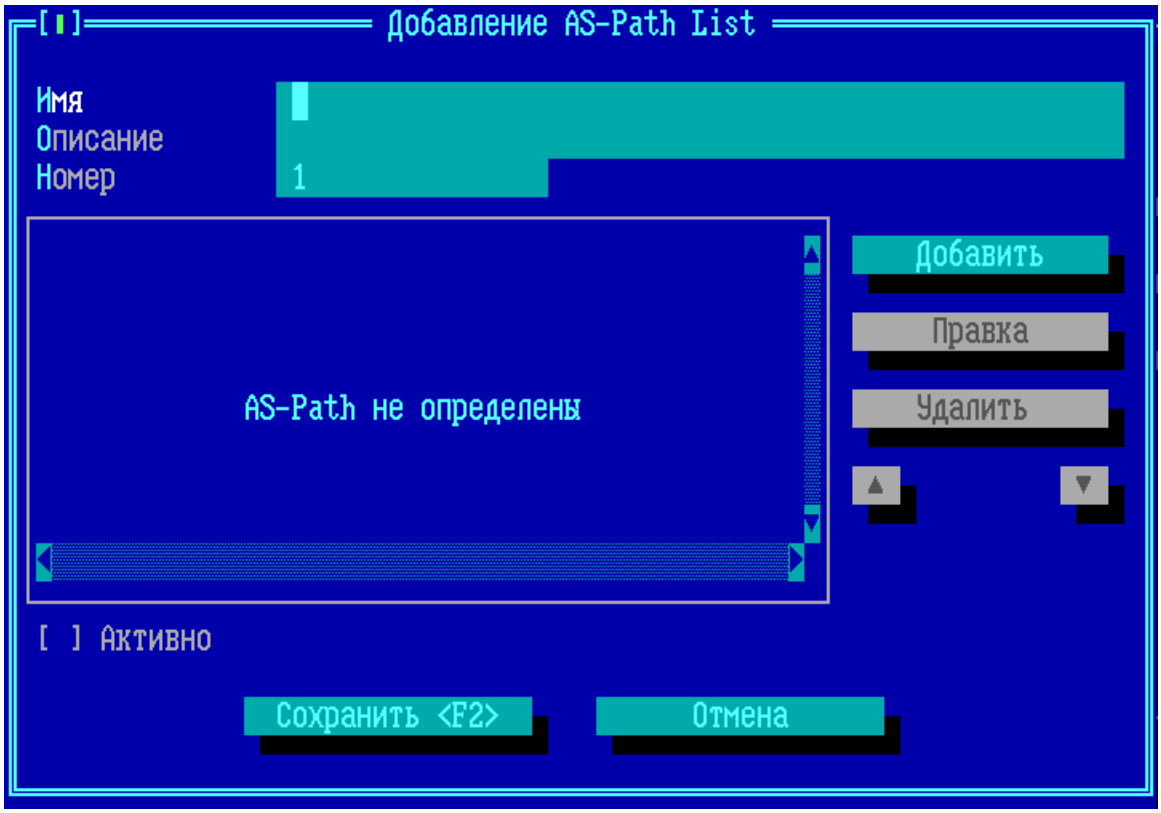


Рисунок 334 - Добавление AS Path-list на вкладке «AS Path-list»

Имя – наименование списка AS-Path.

Описание – текстовое описание, уточнение применения списка AS-Path для входящих или исходящих маршрутов.

Номер – номер списка AS-Path.

Активно – при включении флага активируется список AS-Path. При выключенном флаге условие AS-Path не будут применяться при фильтрации маршрутов. Активный список AS-Path отмечен знаком «√» на вкладке «AS Path-list».

Список AS-Path состоит из правил, нумерованных записей. Правило содержит порядковый номер, разрешающее или запрещающее действие, условие, записанное в виде регулярного выражения. Проверка соответствия маршрута условиям списка AS-Path производится по списку, начиная с записи с наименьшим порядковым номером, до первого соответствия. Если соответствие не найдено, применяется неявная политика запрета по умолчанию «deny any».

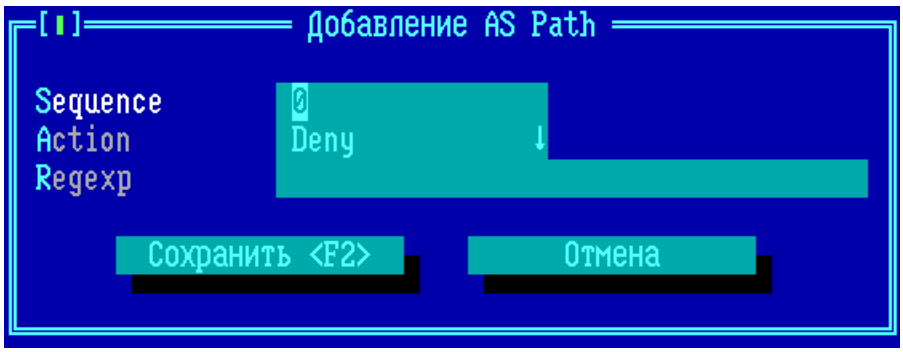


Рисунок 335 - Добавление правила AS Path

Sequence – порядковый номер правила в списке AS-Path, определяет порядок сканирования правил при проверке соответствия маршрута условиям списка AS-Path.

Action – разрешающее или запрещающее действие правила, удовлетворяющего условиям regexp.

Regexp – регулярное выражение, которому должен соответствовать AS-Path. AS-Path представляет собой список чисел - номеров автономных систем. Регулярное выражение строится по правилам регулярных выражений Unix, но пробелу соответствует символ подчеркивания «_».

Для дальнейшей настройки протокола BGP необходимо перейти на следующую вкладку.

Для выхода в меню с сохранением настроек протокола BGP, нажмите кнопку «Сохранить» или клавишу *<F2>*. Для выхода без сохранения настроек нажмите клавишу *<Esc>*.

8. 4. 2. 7. Community-list

На вкладке **Community-list** описываются списки Community. Применяется в карте маршрутов для фильтрации входящих и исходящих маршрутов на основе тега Community.

Community – группа маршрутов, которые имеют общее свойство, используется для тегирования маршрутов.

Список Community состоит из правил, нумерованных записей. Правило содержит порядковый номер, разрешающее или запрещающее действие, набор атрибутов и значение Community. Действие списка как в AS Path-list.

Поддерживаются стандартные нумерованные списки Community (номер списка в диапазоне от 1 до 99).

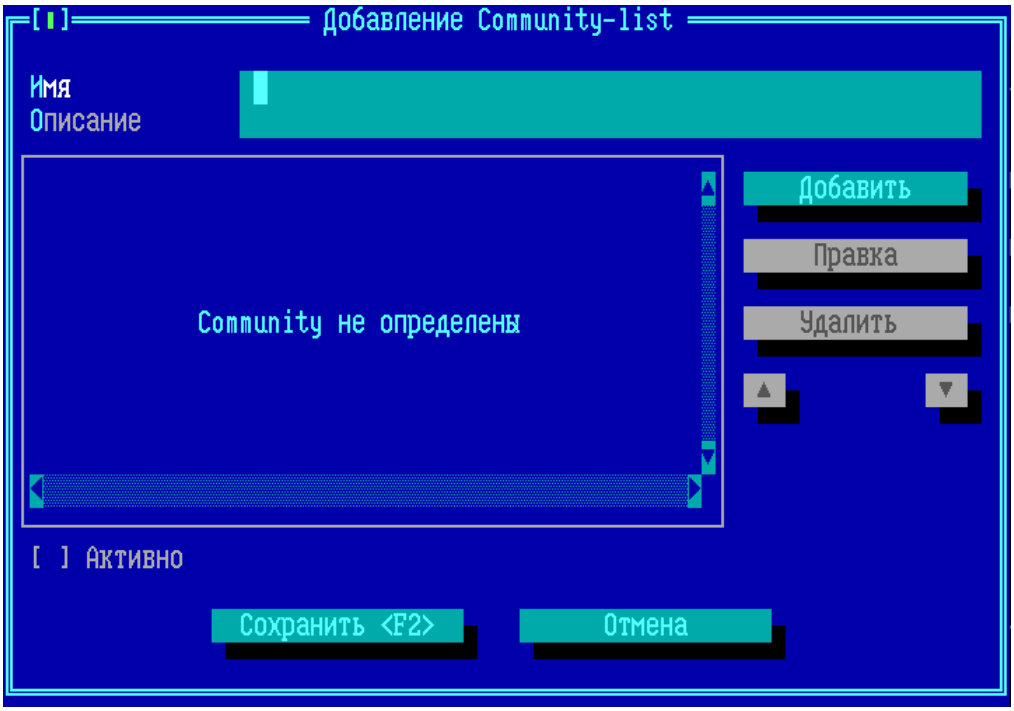


Рисунок 336 - Добавление Community-list на вкладке «Community-list»

Имя – наименование Community.

Описание – текстовое описание, уточнение применения Community для входящих или исходящих маршрутов.

Активно – при включении флага активируется список Community. При выключенном флаге Community не будет применяться при фильтрации маршрутов. Активный список Community отмечен знаком «√» на вкладке «Community-list».

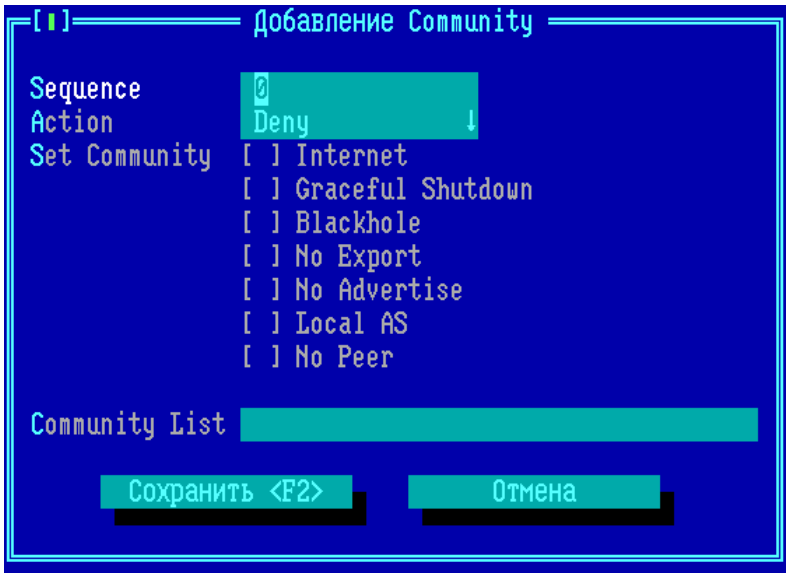


Рисунок 337 - Добавление Community

Sequence – порядковый номер Community в списке, определяет порядок сканирования правил при проверке соответствия маршрута условиям списка Community.

Action – действие правила, разрешающее или запрещающее.

Set Community – Один маршрут может обладать несколькими атрибутами Community одновременно.

- *Internet* – разрешает анонсирование префикса всем соседям BGP. При фильтрации по нескольким значениям Community требуется совпадение со всеми указанными значениями. Если в правиле перечислено несколько значений, все они должны присутствовать в атрибутах маршрута для выполнения условия. По умолчанию все маршруты принадлежат общему Internet Community.
- *Gracefull Shutdown* – Community, используемое с функцией плавное завершение сеанса BGP, позволяет уменьшить количество потерянного трафика при отключении сеансов BGP для обслуживания, в соответствии с RFC 8326.
- *Blackhole* – отправка префиксов одноранговым узлам eBGP и восходящему потоку с целью блокировки нежелательного трафика, в соответствии с RFC 7999. Префиксы, отмеченные этим сообществом, обычно не должны повторно объявляться за пределы соседней сети, получившей анонс. При получении сообщения BLACKHOLE community от BGP-спикера сообщество NO ADVERTISE или NO_EXPORT добавляется автоматически.
- *No Export* – при объявлении маршрута eBGP-соседу не объявляет маршрут внешним BGP-узлам за пределы конфедерации. Если соседний узел BGP является частью конфедерации, узел считается находящимся внутри конфедерации, поэтому

маршрут будет объявлен узлу.

- *No Advertise* – при добавлении Community, принимающий маршрутизатор BGP будет использовать и сохранять префикс в своей таблице BGP, но он не будет объявлять префикс никаким BGP-соседям.
- *Local AS* – все маршруты с таким значением, не должны объявляться внешним BGP-узлам. Если BGP-сосед является частью конфедерации, он считается внешним одноранговым узлом, поэтому маршрут не будет объявлен одноранговому узлу.
- *No Peer* – используется для передачи в другую сеть информации о том, как исходная сеть хочет распространить префикс, в соответствии с RFC 3765.

Community List – значения Community; Значение указывается в виде числа или в формате ASN:VALUE, где ASN - идентификатор автономной системы, VALUE - значение Community. Значения разделяются запятой.

Для дальнейшей настройки протокола BGP необходимо перейти на следующую вкладку.

Для выхода в меню с сохранением настроек протокола BGP, нажмите кнопку «Сохранить» или клавишу <*F2*>. Для выхода без сохранения настроек нажмите клавишу <*Esc*>.

9. Параметры доступа, правила трафика межсетевого экрана

В разделе «Параметры доступа» меню конфигурации ФПСУ находятся опциональные настройки межсетевого экрана, позволяющие администратору вести фильтрацию передаваемого трафика по ряду критериев.

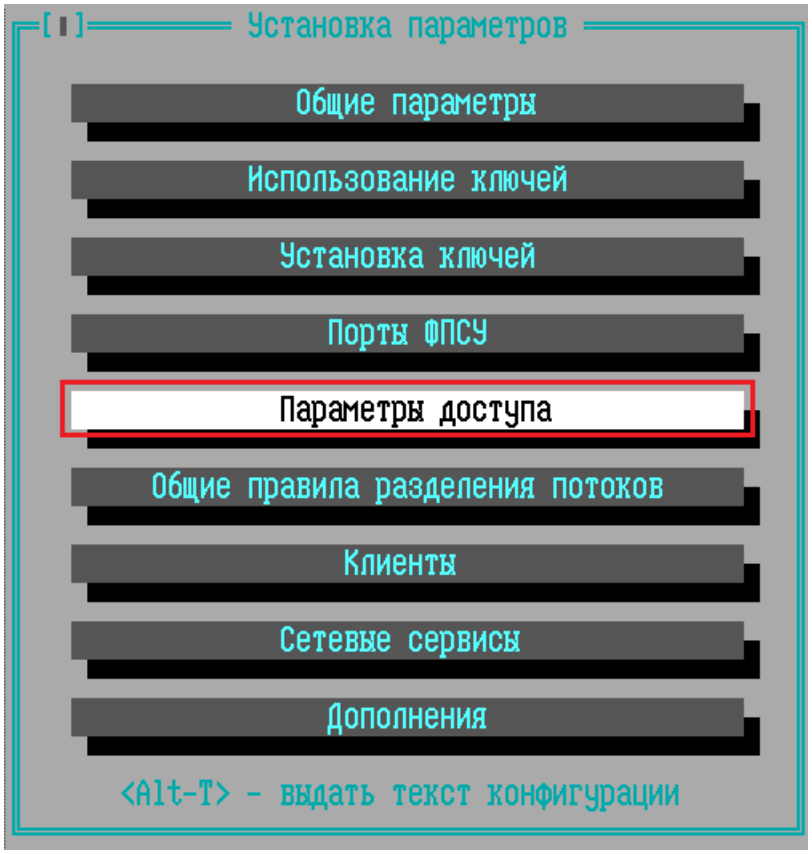


Рисунок 338 - Меню конфигурации ФПСУ

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 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, ФПСУ Клиенты

PKI). Для правила могут быть указаны диапазоны времени разрешенной работы объектов, к которым это правило применяется, а также разрешенные протоколы передачи данных. Правило может быть разрешительным (Accept) или запретительным (Reject, Drop).

Межсетевым экраном отслеживается инициатор установления соединения, возвратный трафик разрешается.

Правила располагаются в списке правил трафика по приоритету, и в случае возникновения взаимоисключающих настроек, будет работать правило, находящееся выше по списку.

ВНИМАНИЕ! По умолчанию, правила дополнительной фильтрации выключены, и трафик абонентов передается без дополнительных проверок. После создания администратором ФПСУ как минимум одного правила трафика (см. пункт «Правила трафика»), активируется также правило по умолчанию «**Block other traffic»**, запрещающее передачу пакетов, не разрешенных хотя бы одним из правил дополнительной фильтрации. Правило по умолчанию «**Block other traffic»** всегда имеет самый низкий приоритет.

После нажатия кнопки главного меню «Параметры доступа» происходит переход в подменю «Настройки» правил дополнительной фильтрации.

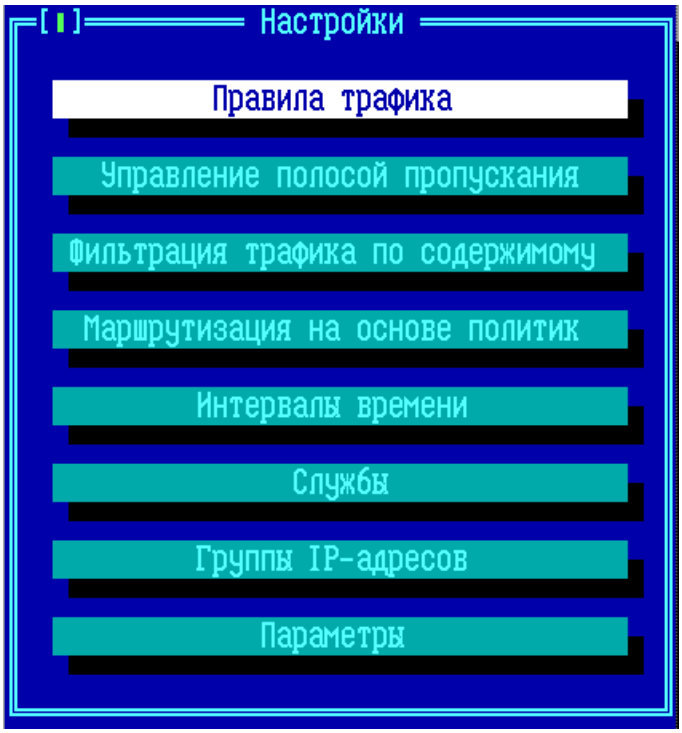


Рисунок 339 - Команды меню «Параметры доступа»

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)»;
- «Маршрутизация на основе политик» — переход в окно управления правилами на основе политик, трафик перенаправляется с выбранного порта ФПСУ или в выбранный туннель, подробнее см. пункт «Маршрутизация на основе политик»;
- «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 осуществляется нажатием клавиши <*Esc*> или <*F2*>.

9. 1. Правила трафика

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

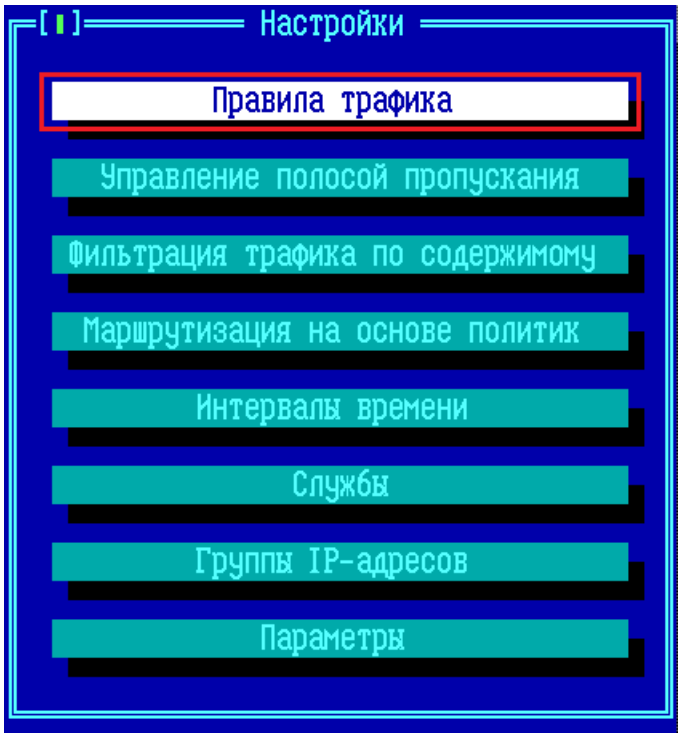


Рисунок 340 - Меню «Параметры доступа» → «Правила трафика»

После выполнения команды «Правила трафика», происходит переход в окно, где отображен список используемых на ФПСУ 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 не добавлял в список ни одного правила, то есть список правил пуст, то ограничений на передачу трафика нет, в том числе выключено и правило по умолчанию **Block other traffic**. В этом случае все пакеты передаются в соответствии с маршрутизацией, заданной в пункте «Порты ФПСУ».

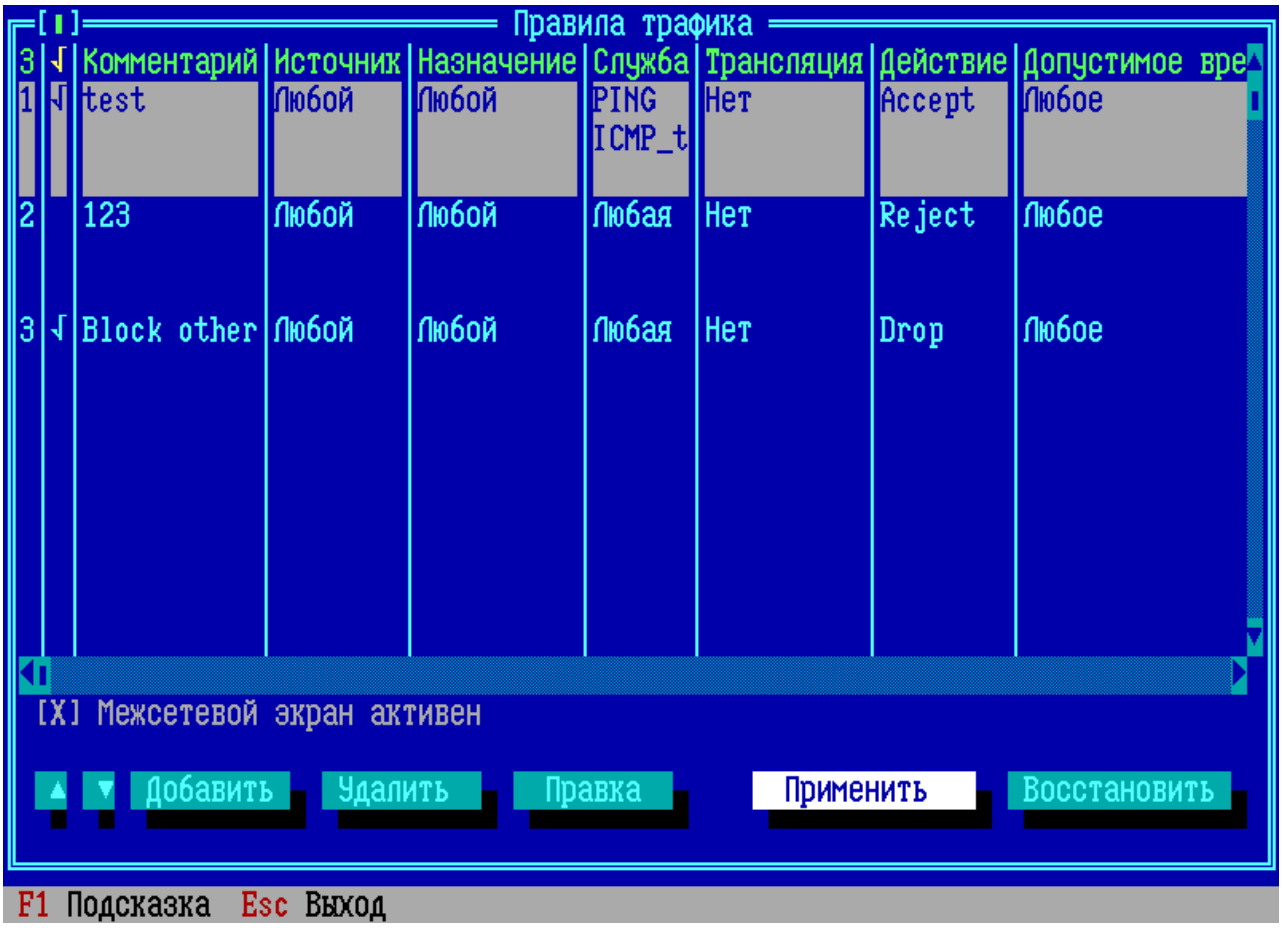


Рисунок 341 - Список правил трафика на ФПСУ

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), диапазон разрешенного времени работы, и основное действие с пакетом: разрешить передачу (Accept) или запретить (Drop или Reject).

Флаг «*Межсетевой экран активен*» включает работу дополнительных правил фильтрации. Без установленного флага работают только основные правила маршрутизации списка абонентов, заданные администратором в пункте главного меню «Порты ФПСУ».

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

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

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

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

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

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

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

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

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

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

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

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

9. 1. 1. Общие настройки правил трафика

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

Вкладка **Общие** предназначена для выбора обязательного основного действия с передаваемым пакетом (сбросить или пропустить), и опциональных дополнительных действий. Символ «↓» в конце настраиваемого поля обозначает наличие выпадающего списка, вызываемого нажатием клавиши *<Пробел>* при установленном на поле курсоре.

Вкладка **Общие** содержит следующие настраиваемые опции:

Комментарий — обязательное произвольное текстовое поле для пояснения правила.

Действие — обязательное правило, определяющее, как поступить с передаваемым пакетом. В выпадающем меню могут быть выбраны следующие варианты основного действия:

- *Drop* — действие по умолчанию, пакет данных будет сброшен, ICMP-оповещение об отказе передачи пакета не будет передано отправителю;
- *Reject* — пакет данных будет сброшен, отправителю будет передано ICMP-оповещение об отказе передачи пакета;
- *Accept* — пакет данных будет передан по назначению.

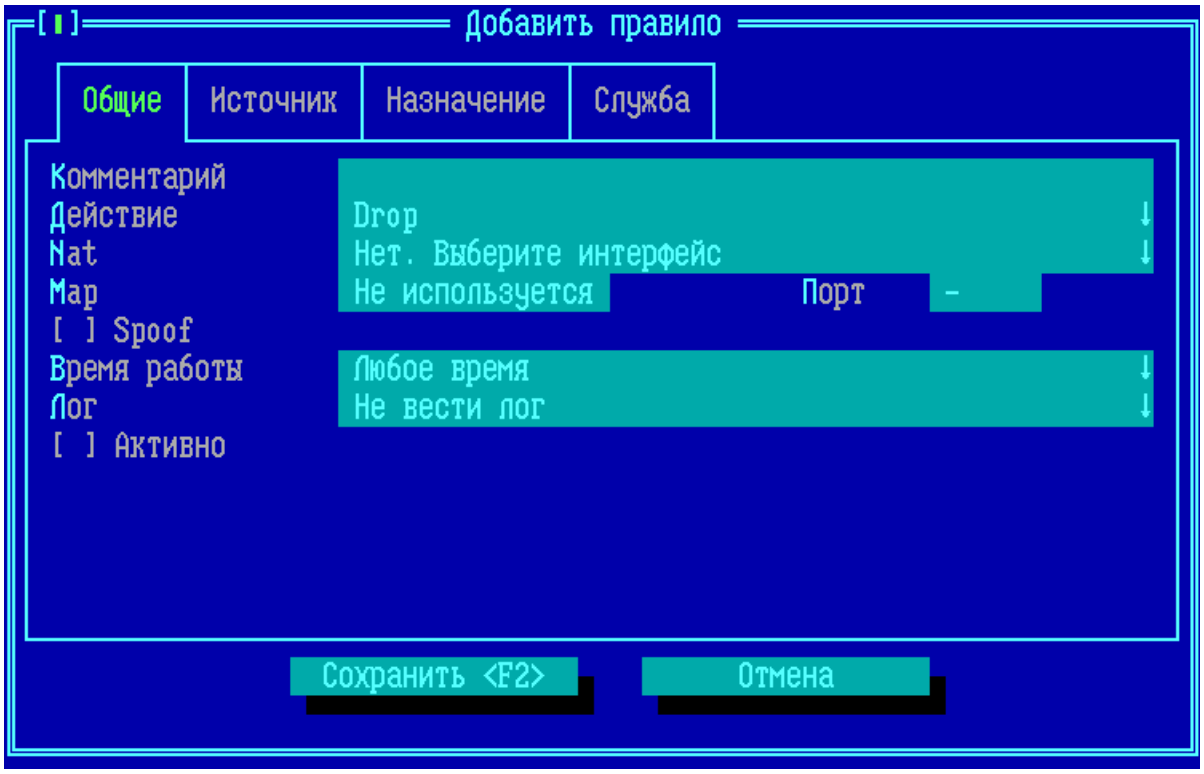


Рисунок 342 - Добавление нового правила трафика

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 будет использован для трансляции адреса источника при передаче пакета получателю.

MAP, Порт. Правило, включающее в себя дополнительную опцию MAP, позволяет перенаправить полученные ФПСУ пакеты, где получателем пакета являются собственные IP-адреса ФПСУ (при этом во вкладке «Назначение» IP-адрес порта ФПСУ должен быть добавлен как объект «Интерфейс»), на другой, указанный в поле этой опции, IP-адрес. В поле ***Порт*** указывается номер порта протоколов TCP/UDP. Если в поле ***Порт*** установлено отличное от нуля значение, то трафик будет перенаправляться, изменяя порт назначения транспортного протокола на указанный номер. Если в поле ***Порт*** опции ***MAP*** стоит значение 0, то трафик на указанный в поле ***MAP*** IP-адрес будет перенаправлен без изменения порта назначения.

Примеры применения правил NAT и MAP можно посмотреть в пунктах «Использование ФПСУ для контроля доступа в интернет с NAT», «Использование ФПСУ для объединения офисов с одинаковой внутренней адресацией», «Использование ФПСУ для смены порта назначения трафика, направляемого в адрес абонента», «Использование ФПСУ для балансировки нагрузки на порты внутреннего сервера».

Spoof – опция для сетевых соединений на медленных каналах передачи данных с большими задержками (например, спутниковые каналы связи). Если задействована опция подтверждения получения данных ACK, то ФПСУ отвечает отправителю самостоятельно, не дожидаясь подтверждения от получателя сегмента.

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

Лог — если требуется вести журнал, содержащий разрешенные и запрещенные в рамках данного правила передачи данных, то следует выбрать из выпадающего списка опцию *Вести лог* или *Вести лог, писать заголовки пакетов*. Значение по умолчанию - *Не вести лог.*

Для того, чтобы все указанные в правиле настройки после сохранения были задействованы, следует перед выходом установить флаг *«Активно»*.

Помимо общих настроек, можно указать параметры на других вкладках создаваемого правила. Перемещение между вкладками осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

9. 1. 2. Вкладки «Источник» и «Назначение» правил трафика

Правило трафика применяется только к тем пакетам, IP-адреса источника и назначения которых указаны в соответствующих вкладках. Исключение: если во вкладках **Источник** и **Назначение** нет ни одной записи (список пуст), то правило трафика применяется ко всем пакетам.

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

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

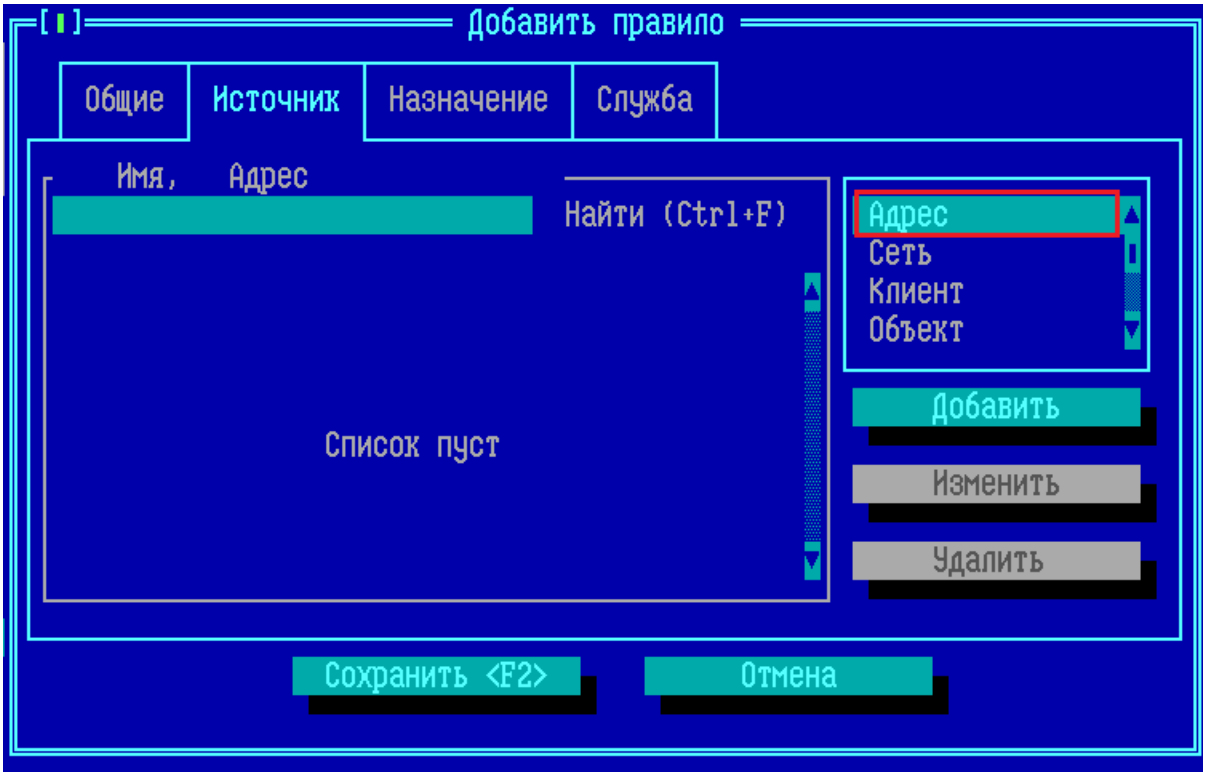


Рисунок 343 - Назначение источников для правила трафика

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

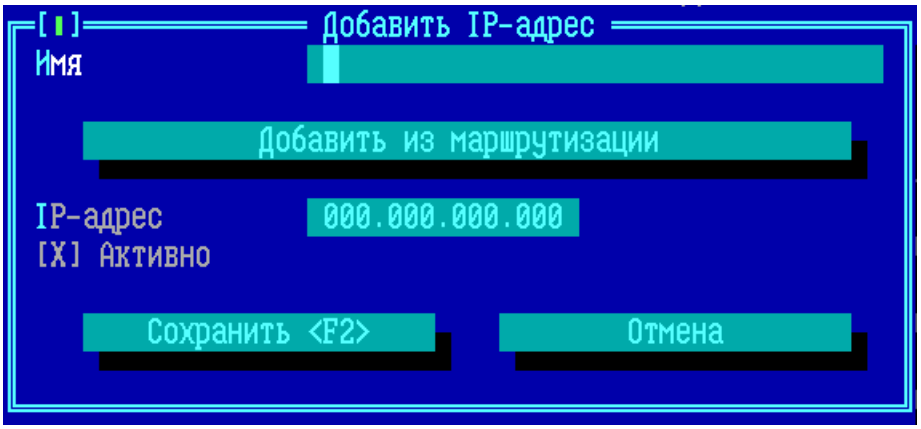


Рисунок 344 - Команда «Добавить» для отдельного IP-адреса

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

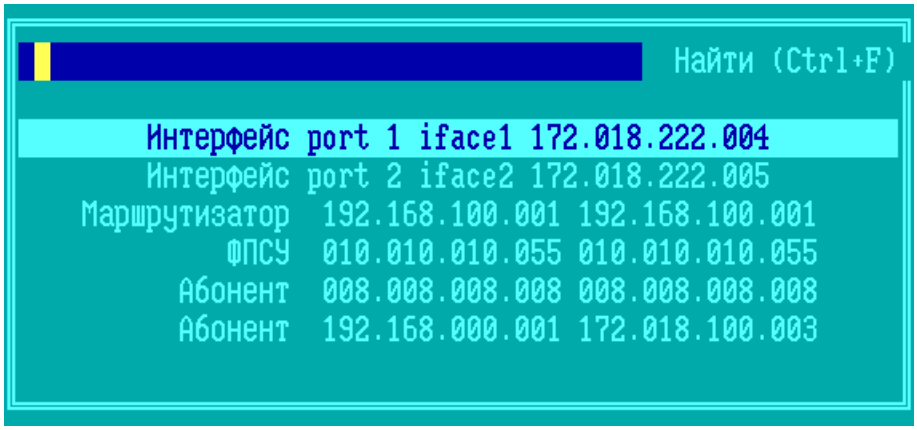


Рисунок 345 - Список найденных объектов в маршрутизации (Портах ФПСУ)

Перемещение по списку осуществляется клавишами <↑> и <↓>, выбор осуществляется нажатием клавиши <*Enter*> или <*Пробел*>. Например, при выборе объекта «Абонент 010.010.010.248 010.010.010.248», интерфейс добавления IP-адреса автоматически заполнится данными, взятыми из списка маршрутизации:

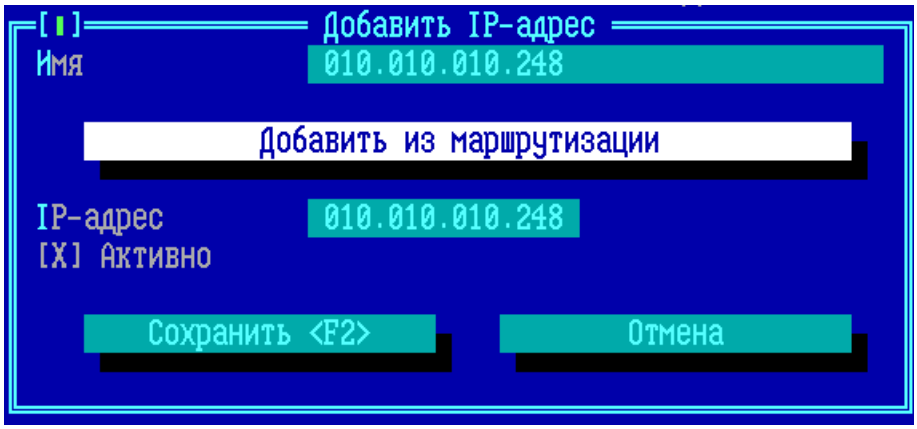


Рисунок 346 - Данные взяты из списка маршрутизации

ВНИМАНИЕ! Если флаг *«Активно»* выключен, то IP-адрес будет добавлен в список, но правило трафика по нему отрабатывать не будет.

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

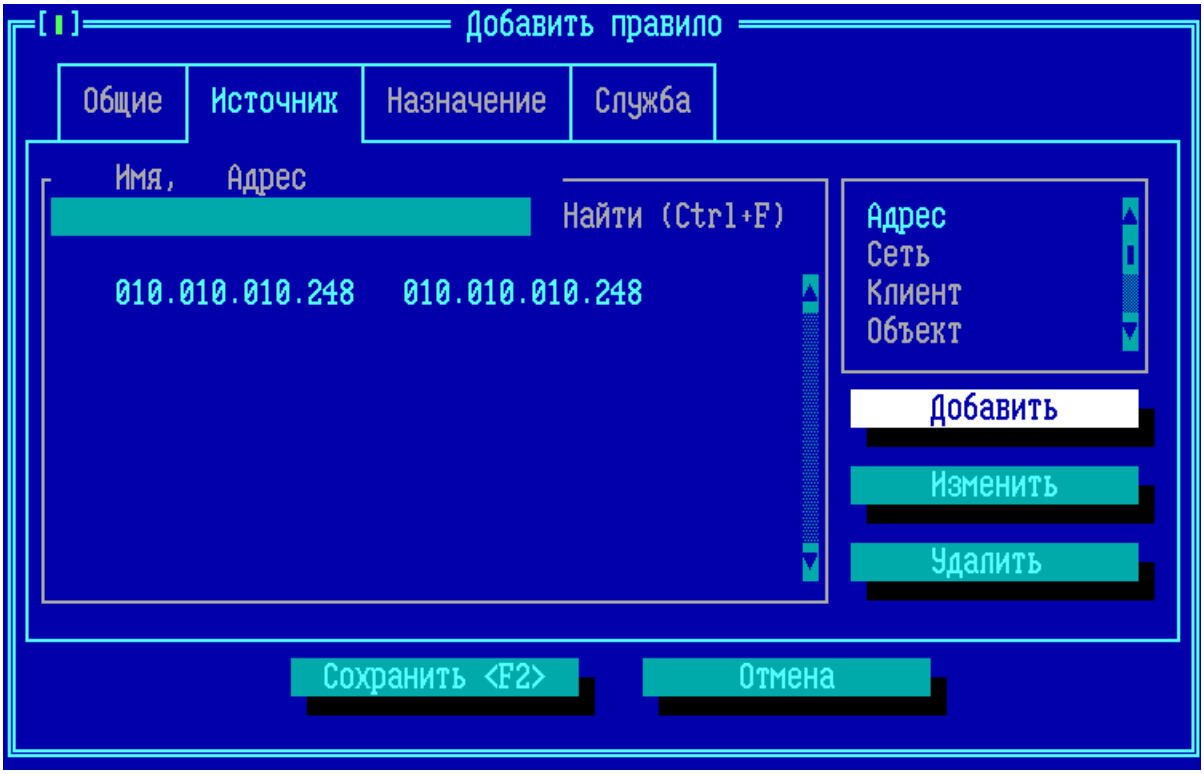


Рисунок 347 - В список «Источник» правила трафика добавлена новая запись

Сеть — для добавления в список обрабатываемых правилом источников подсети IP-адресов, следует установить курсор на строке «Сеть», затем по нажатию клавиши *<Tab>* перейти на кнопку *«Добавить»* и нажать *<Enter>*. Подсеть должна быть выбрана из

диапазона подсетей, прописанных в маршрутизации на портах ФПСУ, либо входить в такую.

Клиент — для добавления в список обрабатываемых правилом источников трафика данных, поступающих от ФПСУ-IP/Клиентов, следует установить курсор на строке «Клиент», затем по нажатию клавиши <*Tab*> перейти на кнопку «*Добавить*» и нажать <*Enter*>. Описатель клиента должен быть выбран из заранее сконфигурированной на ФПСУ группы клиентов зарегистрированной Криптосети или соответствовать значению "Все клиенты PKI".

Для группы клиентов PKI может быть задано условное правило, применяемое в зависимости от текущего уровня доступа клиента. Уровень доступа клиент получает по протоколу RADIUS от сервера авторизации (см. пункты RADIUS и Настройка диапазона клиентов на работу с Radius). В правиле трафика в *Источнике* или *Назначении* выбирается тип *Клиент* и задается условие для сравнения уровня доступа (>, <, ==, != <=, >=) и уровень доступа для группы клиентов. Правило срабатывает, если выполняется заданное условие для уровня конкретного клиента.

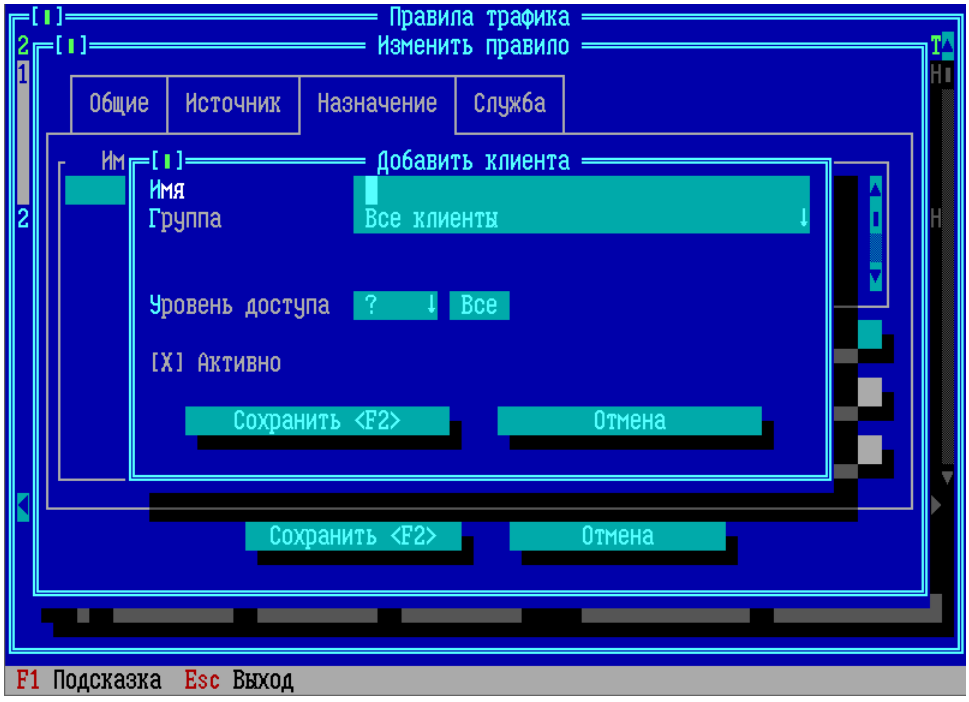


Рисунок 348 - В список «Источник» правила трафика добавляются клиенты

Объект — в список может быть добавлена заранее созданная логическая группа IP-адресов и подсетей (подробнее см. пункт «Группы IP-адресов»). Для добавления в список обрабатываемых правилом источников трафика от ФПСУ-IP/Клиента, следует установить курсор на строке «Объект», затем по нажатию клавиши <*Tab*> перейти на кнопку «*Добавить*» и нажать <*Enter*>.

Интерфейс — в список обрабатываемых правилом источников передаваемых пакетов может быть выбран один из логических интерфейсов ФПСУ (IP-адрес «Порта ФПСУ» №1 и №2, а также IP-адреса портов ФПСУ, назначенные VLAN). Для добавления в список IP-адреса интерфейса ФПСУ, следует установить курсор на строке «Интерфейс», затем по нажатию клавиши <*Tab*> перейти на кнопку «*Добавить*» и нажать <*Enter*>.

ВНИМАНИЕ! Суммарно в правилах МЭ может быть описано не более 1024*1024 записей в источнике.

Каждая запись списка вкладок **Источник** или **Назначение** может быть временно исключена из проверяемых фильтров, при снятии включенного по умолчанию флага «*Активно*».

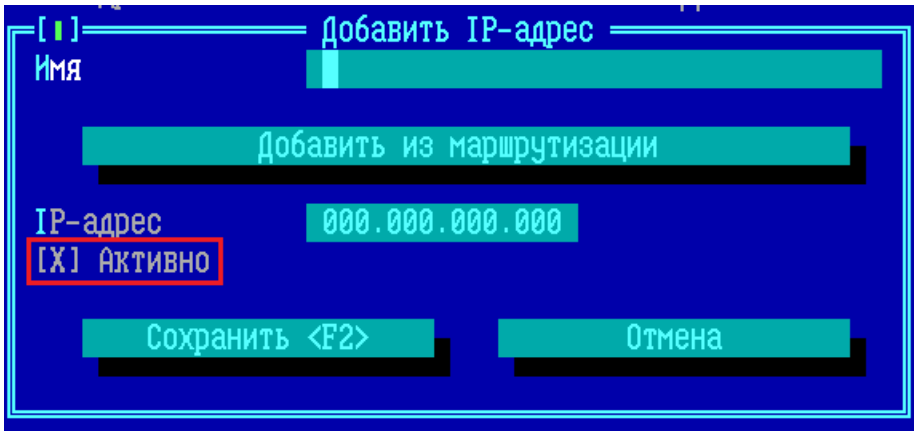


Рисунок 349 - Активация добавленного адреса

9. 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 на все пакеты, а только на те, которые используют указанные в списке этой вкладки протоколы (службы). Служба идентифицируется комбинацией транспортного протокола и номера порта для фильтрации трафика в правилах. Шаблоны служб создаются администратором ФПСУ в окне правил дополнительной фильтрации (см. пункт «Службы»).

Список примененных к правилу служб по умолчанию пуст:

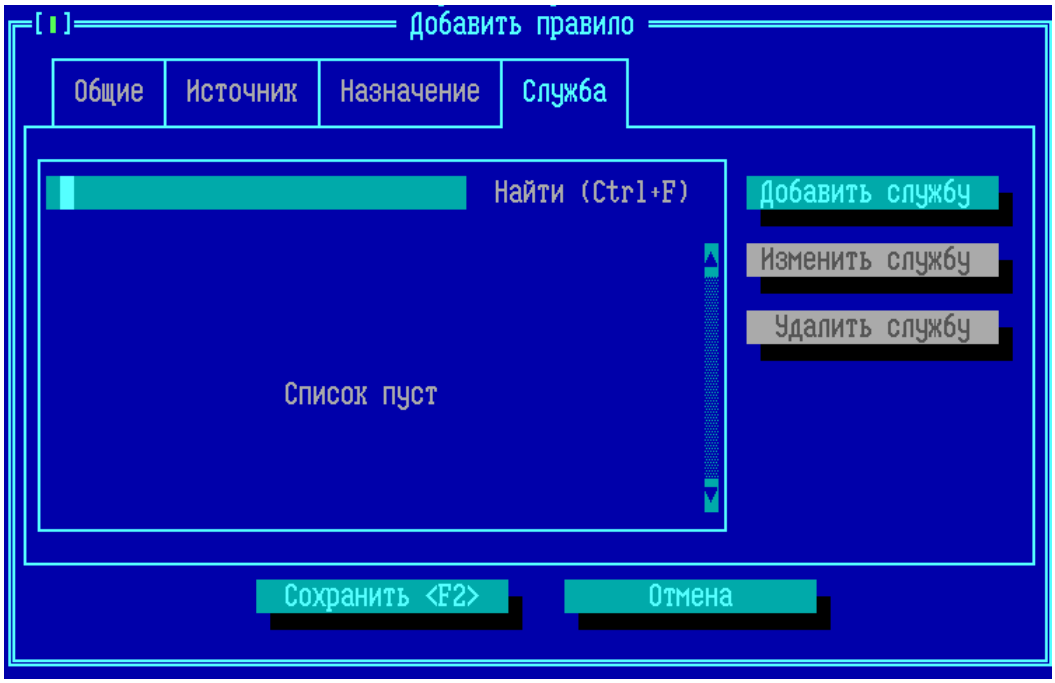


Рисунок 350 - Пустой список служб у нового добавляемого правила

Для внесения новой службы в список, нажмите кнопку *«Добавить службу»* и выберите из появившегося перечня заранее созданных служб (на примере в конфигурации ФПСУ заранее создана служба с именем «TCP 80»):

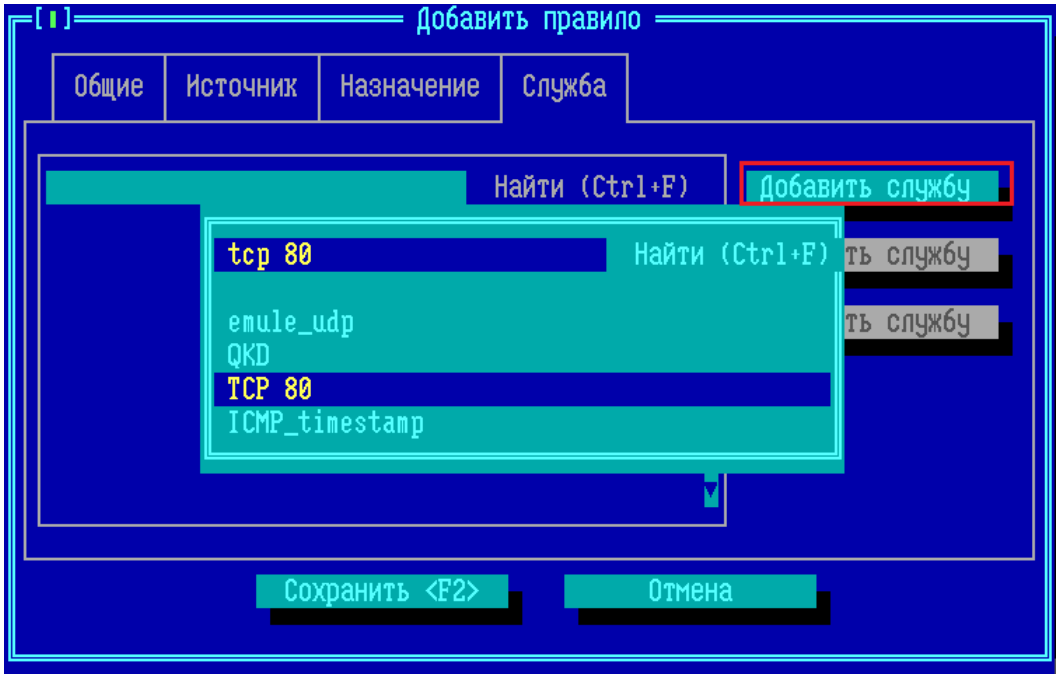


Рисунок 351 - Добавление службы в правило трафика

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

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

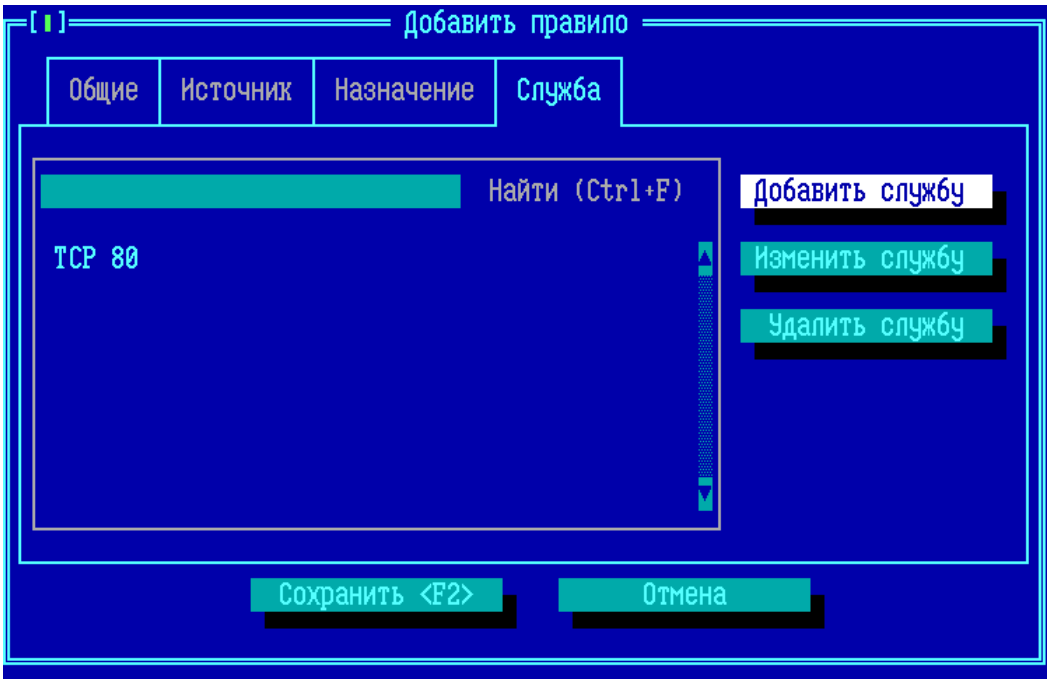


Рисунок 352 - Вкладка со списком служб правила трафика

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

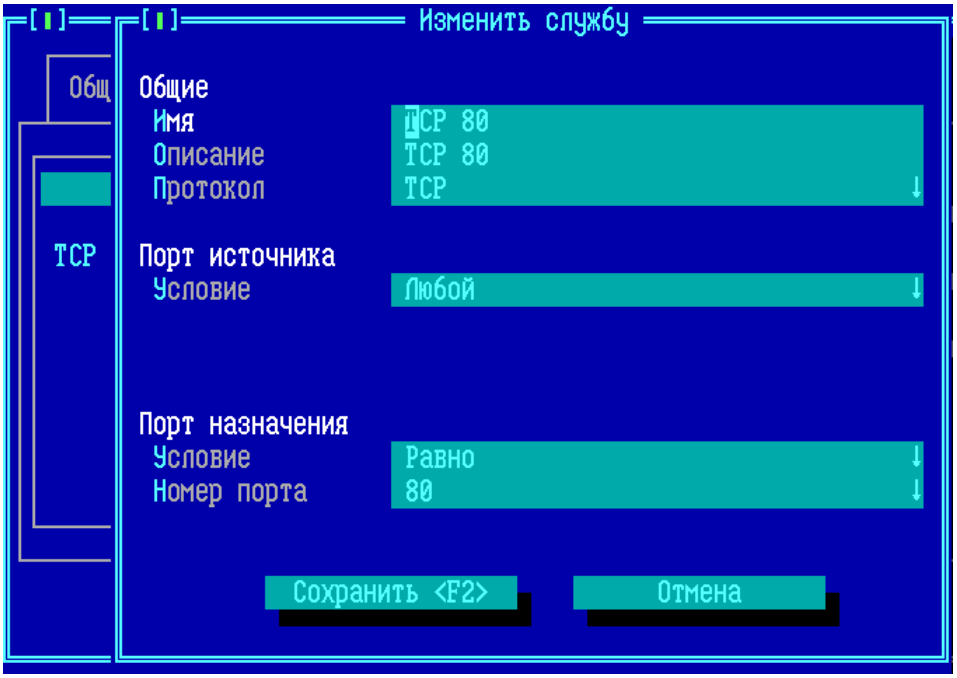


Рисунок 353 - Изменение службы из окна настроек правила доступа

9. 2. Службы

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

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

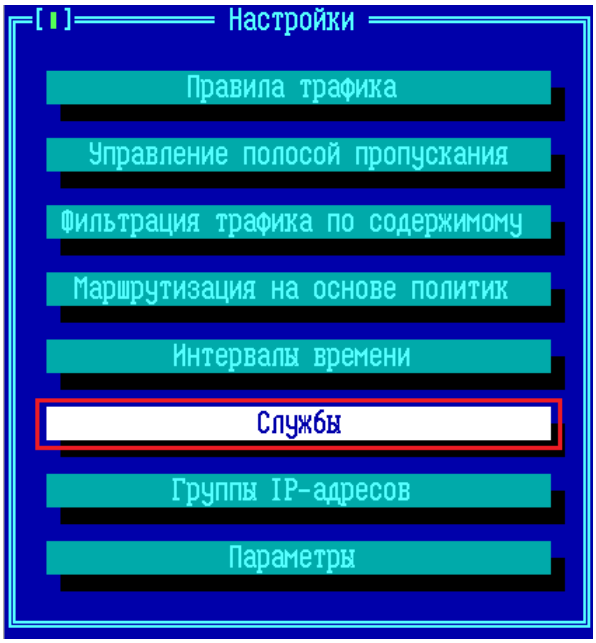


Рисунок 354 - Команда «Службы» настроек правил доступа

В списке служб по умолчанию отображаются шаблоны популярных служб.

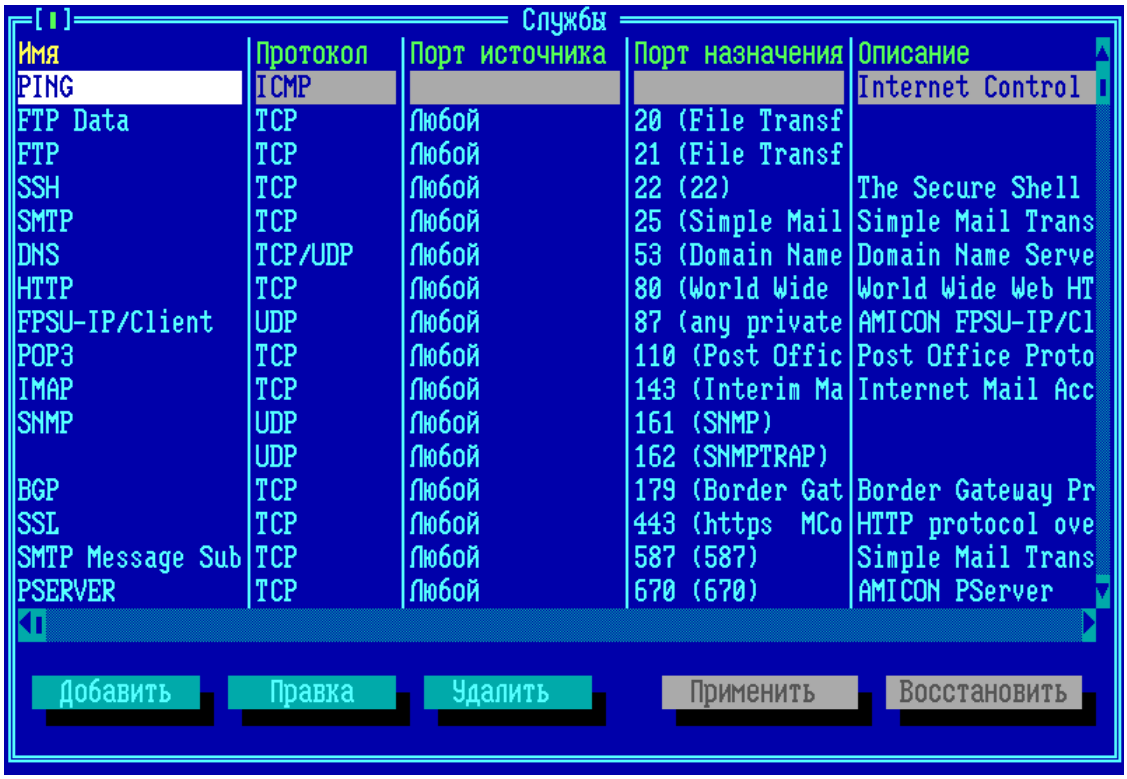


Рисунок 355 - Список служб

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.

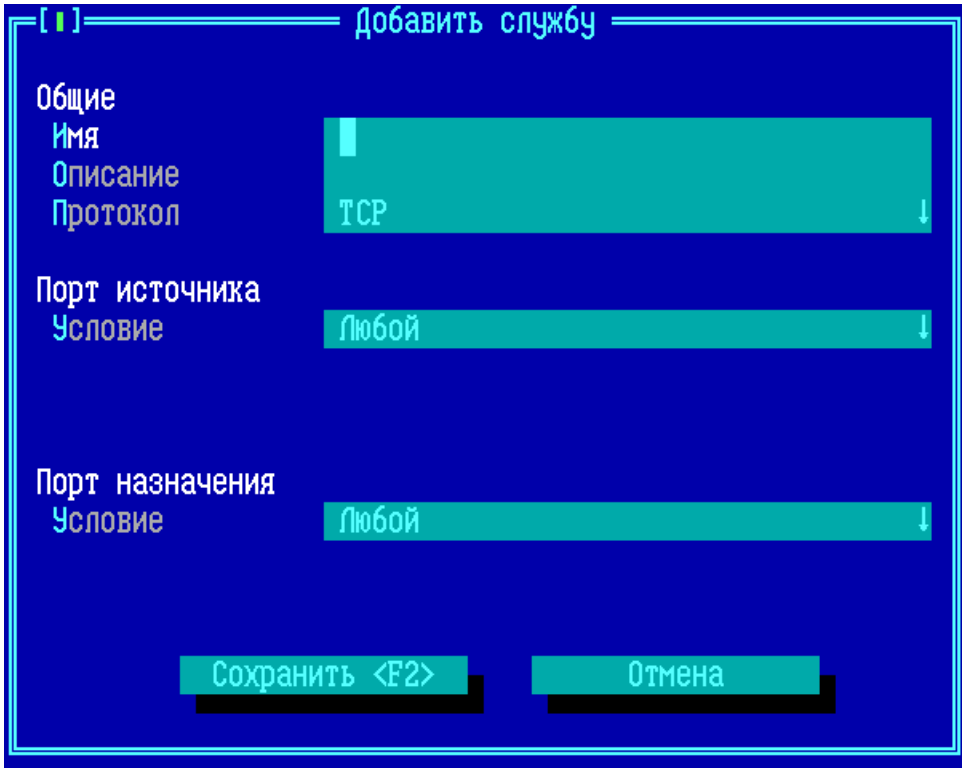


Рисунок 356 - Добавление службы в список

В открывшемся окне указываются следующие параметры службы:

Имя — обязательный параметр, символьное название службы. Это имя будет потом использоваться администратором для прикрепления службы к правилу трафика, поэтому стоит выдавать как можно более точное название (например «TCP:80», если правило будет распространяться на протокол TCP, обращающийся к назначению по 80-му порту протокола TCP);

Описание — произвольное текстовое описание службы, опционально;

Протокол — поле выбора из выпадающего списка протокола передачи данных создаваемой службы. В качестве протокола могут быть выбраны следующие:

- *TCP* – служба ограничивает правило трафиком, передаваемым с помощью протокола Transmission Control Protocol;
- *UDP* – служба ограничивает правило трафиком, передаваемым с помощью протокола User Datagram Protocol;
- *TCP/UDP* – служба ограничивает правило трафиком, передаваемым с помощью протоколов TCP или UDP;
- *ICMP* – служба ограничивает правило трафиком, передаваемым с помощью протокола ICMP (см. пункт «Протокол ICMP в службах»);
- *Другие (IP)* – служба ограничивает правило трафиком, передаваемым с помощью протокола IP;
- *DSCP* – служба ограничивает правило трафиком, указанным в поле приоритета согласно RFC 2474 (значение от 0 до 63);
- *RAW* – служба, предназначенная для установки произвольных фильтров на основе значений битов заголовков сетевого уровня (пример использования протокола RAW см. пункт «Служба для запрета фрагментированных пакетов»);
- *REGEXP* – служба, предназначенная для установки произвольных фильтров на основе символьных строк и регулярных выражений (подробнее см. пункт «Протокол REGEXP в службах»);
- *VLAN* – служба, предназначенная для установки фильтра на основе признака VLAN трафика, обрабатываемого ФПСУ (подробнее см. пункт «Признак VLAN 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*>.

9. 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.

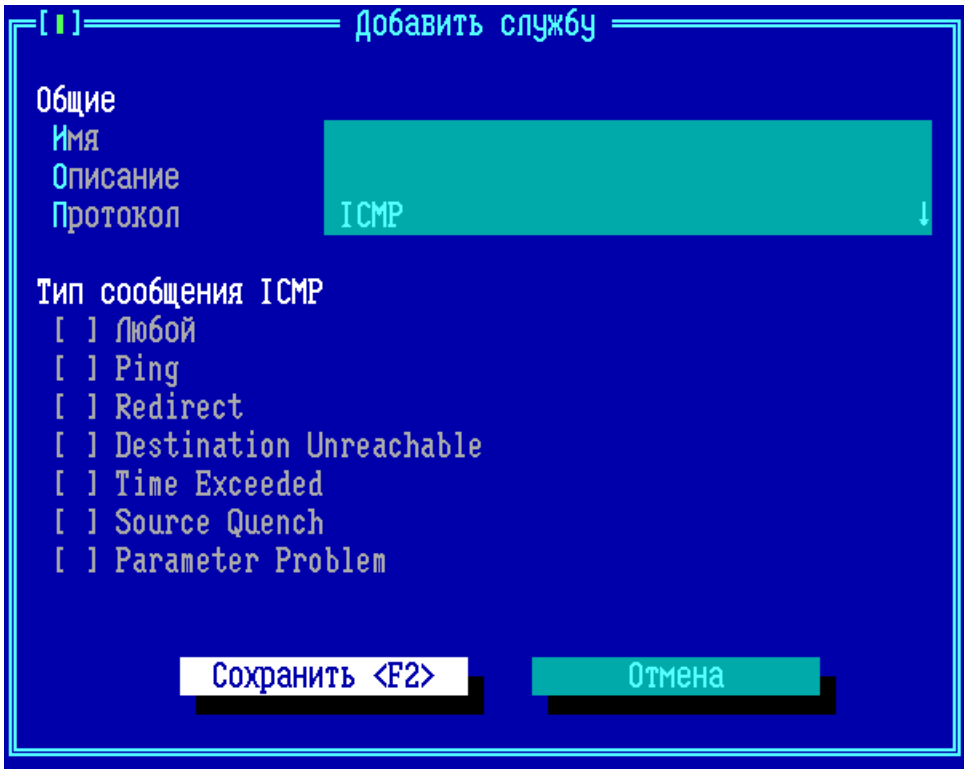


Рисунок 357 - Выбор сообщений ICMP в службе

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

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

9. 2. 2. Служба для запрета фрагментированных пакетов

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

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

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

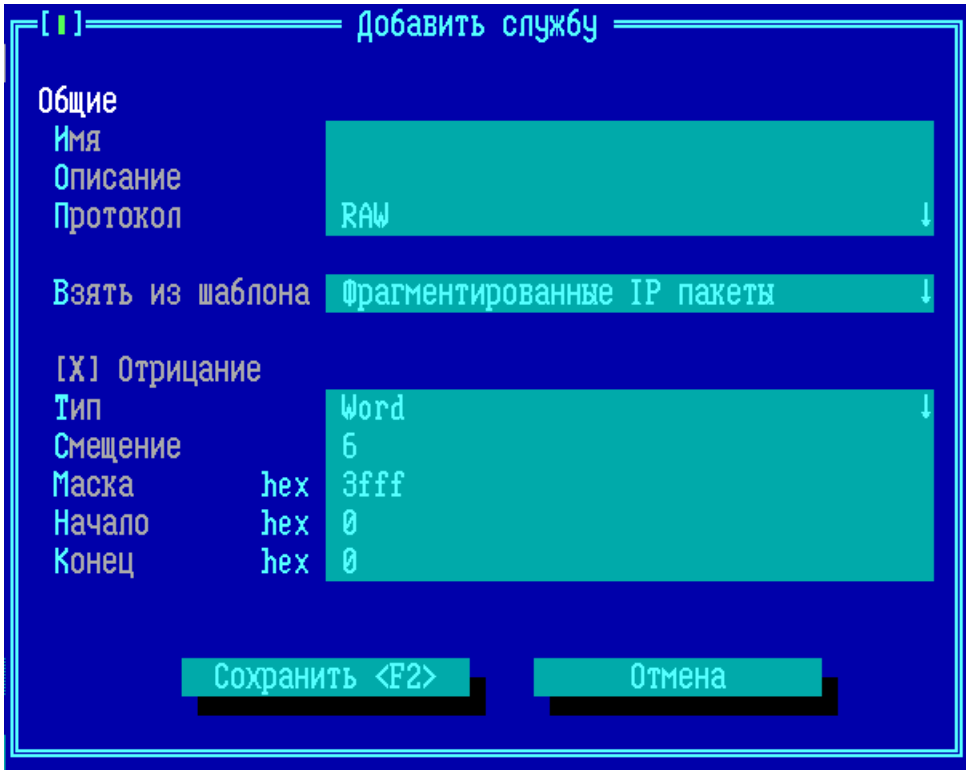


Рисунок 358 - Шаблон для фильтра фрагментированных IP-пакетов

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

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

9. 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 добавлении/изменении службы выбор протокола REGEXP в настройках службы активирует блок со списком регулярных выражений, по умолчанию пустой:

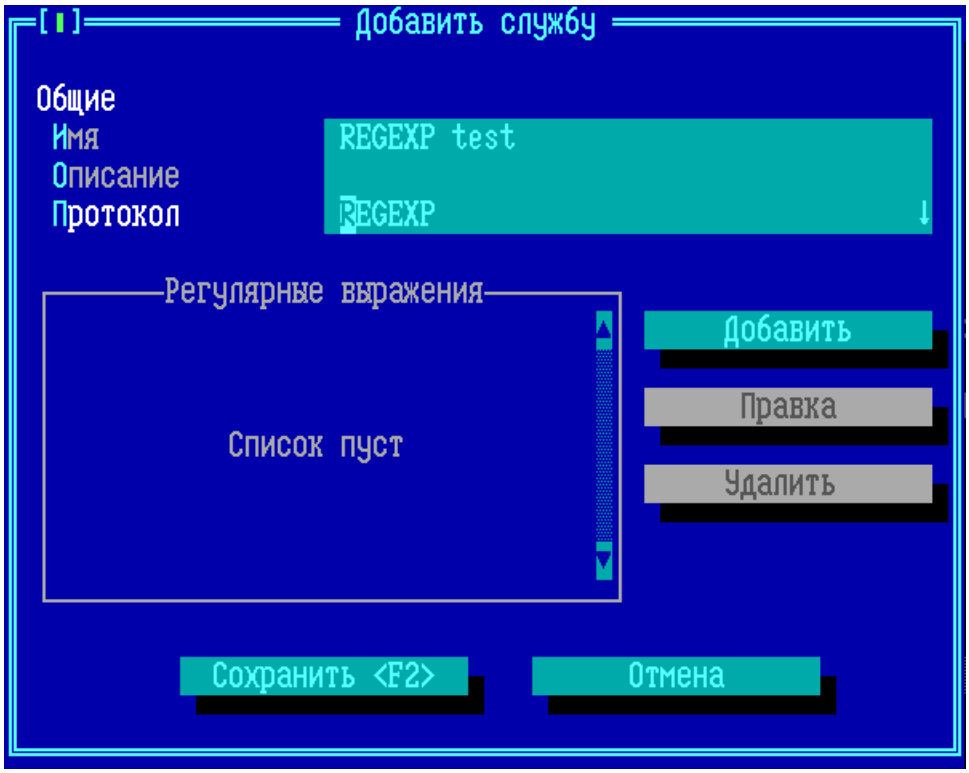


Рисунок 359 - Добавление службы REGEXP

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:

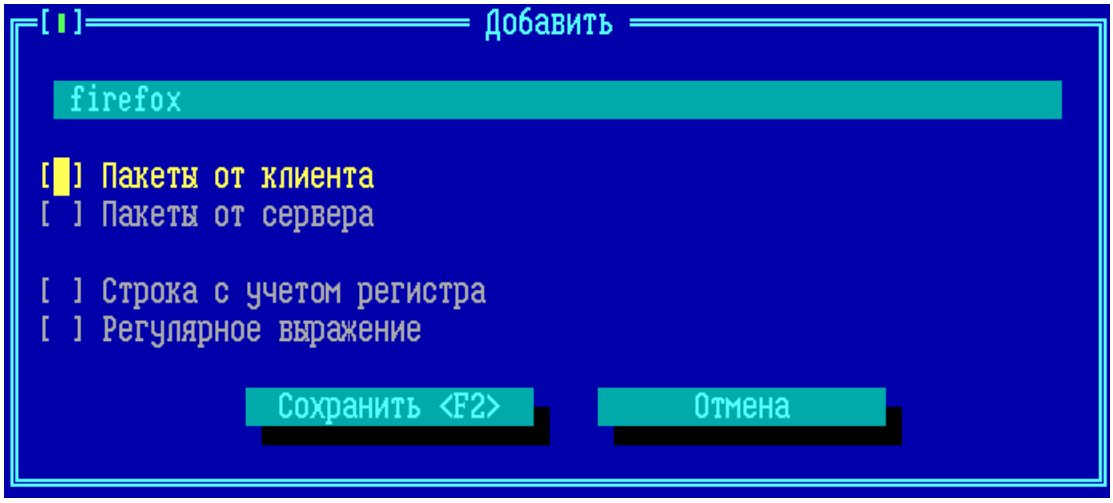


Рисунок 360 - Добавление службы REGEXP

Поле ввода окна «Добавить» - символьная строка или регулярное выражение, не должно быть пустым, количество символов ограничено 1024, обязательная опция. Межсетевой экран исследует передаваемые пакеты на наличие в IP-пакете символьной строки/регулярного выражения, указанных в поле ввода. Символьная строка ищется в кодировке cp866, если требуется искать символьную строку в другой кодировке, то следует использовать запись в кодах Unicode через символ «\u» с включенной опцией ***Регулярное выражение***. Например, для поиска сочетания латинской буквы A с латинской буквой B (символьной строки AB) следует написать в поле значение «\u0041\u0042».

Пакеты от клиента - опция, указывает на то, что символьную строку/регулярное выражение следует искать только в пакетах, передающихся от инициатора соединения (клиента) к принимающей соединение стороне (серверу).

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

ВНИМАНИЕ! Должна быть задействована хотя бы одна из опций «Пакеты от клиента» или «Пакеты от сервера» (могут быть задействованы обе)!

Строка с учетом регистра - необязательная опция. Указывает на то, что в анализируемой символьной строке важен регистр (прописные или ЗАГЛАВНЫЕ символы).

Регулярное выражение - необязательная опция. Указывает на то, что в поле ввода

указана не символьная строка, а регулярное выражение. Используются регулярные выражения библиотеки glibc (подробнее можно посмотреть в официальной документации на регулярные выражения glibc, https://www.gnu.org/software/libc/manual/html_node/Regular-Expressions.html). Включение опции «Регулярное выражение» отключает опцию «Строка с учетом регистра».

Для сохранения настроек окна «Добавить» и возврата в окно «Добавить службу», нажмите кнопку «*Сохранить (F2)*» или клавишу <*F2*>. Для выхода из окна «Добавить» без сохранения изменений используйте кнопку «*Отмена*» или клавишу <*Esc*>. После сохранения новая запись появится в списке «*Регулярные выражения*» окна «Добавить службу».

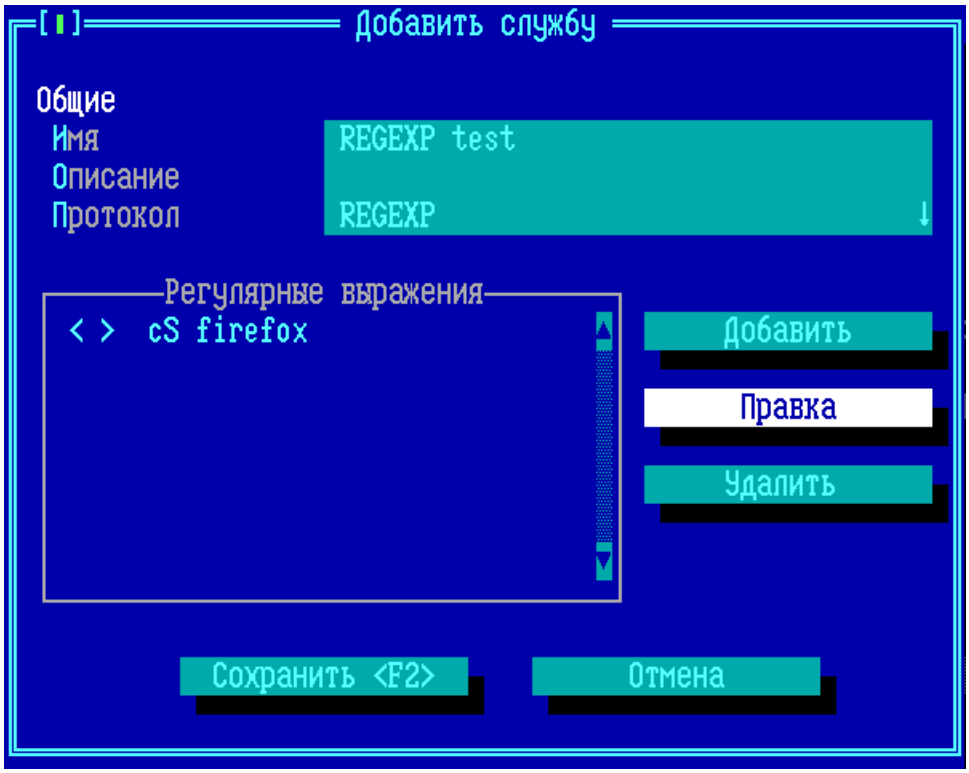


Рисунок 361 - Добавление службы REGEXP

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 до 255 записей символьных строк или регулярных выражений. В этом случае будет анализироваться IP-пакет на совпадение с любым из перечисленных символьных строк/регулярных выражений. Для удаления выбранной курсором записи нажмите клавишу <Del>.

Применение протокола REGEXP для частичной или полной блокировки приложений

Фильтр на основе протокола REGEXP может быть использован для частичной или полной блокировки сетевого трафика 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:

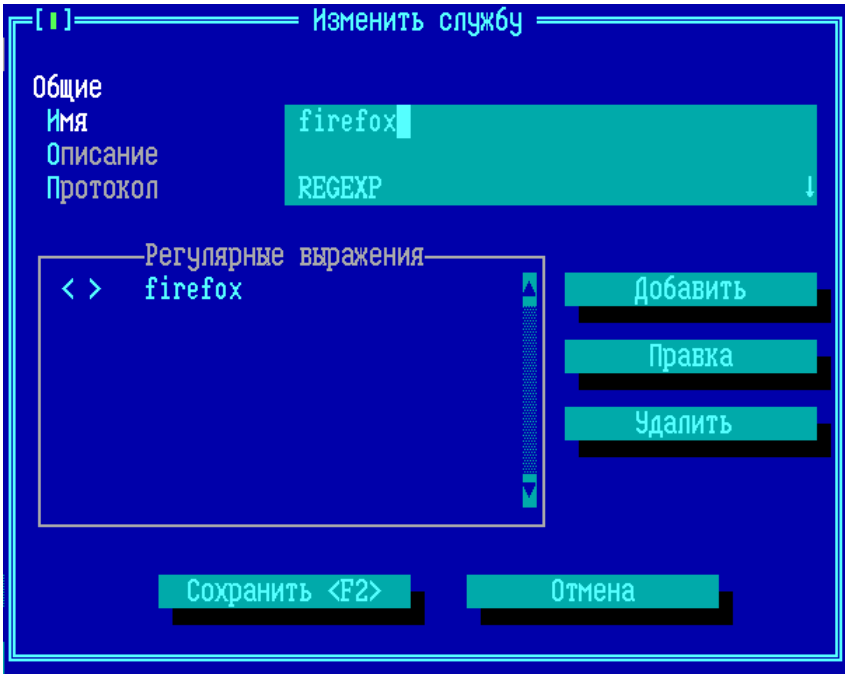


Рисунок 362 - Блокировка браузера Mozilla Firefox, правило 1

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

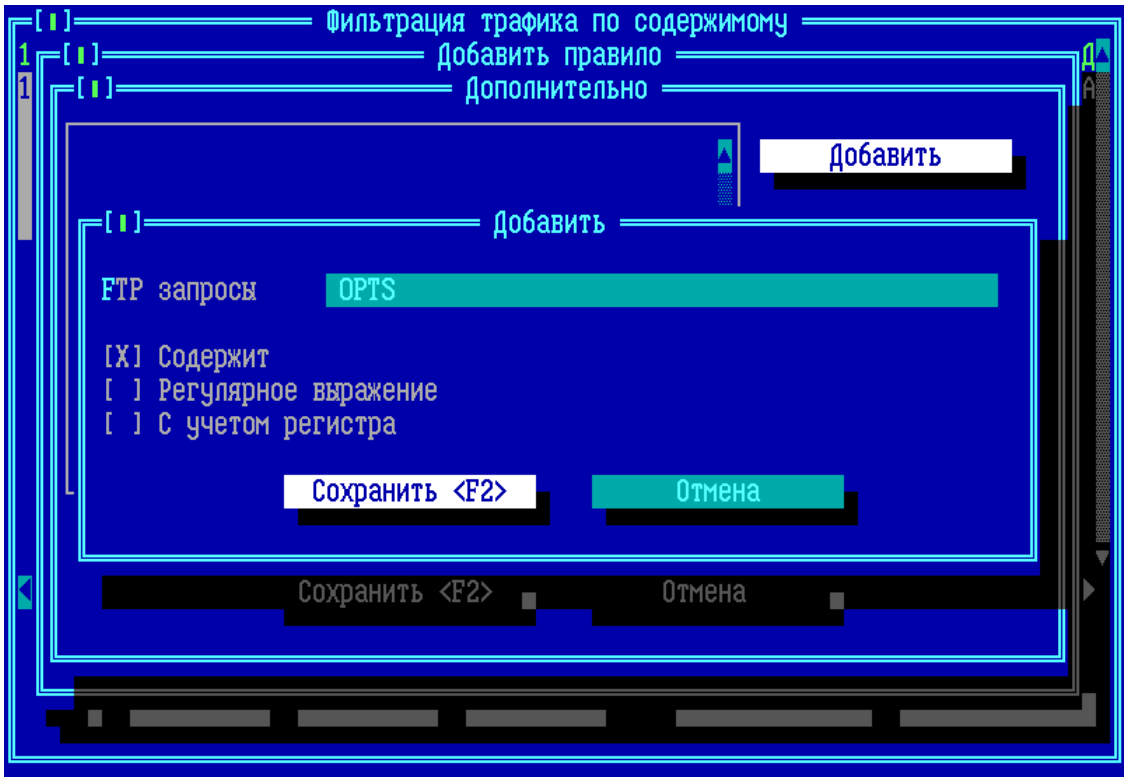


Рисунок 363 - Блокировка браузера Mozilla Firefox, правило 2

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

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



Рисунок 364 - Блокировка браузера Google Chrome, правило 1

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

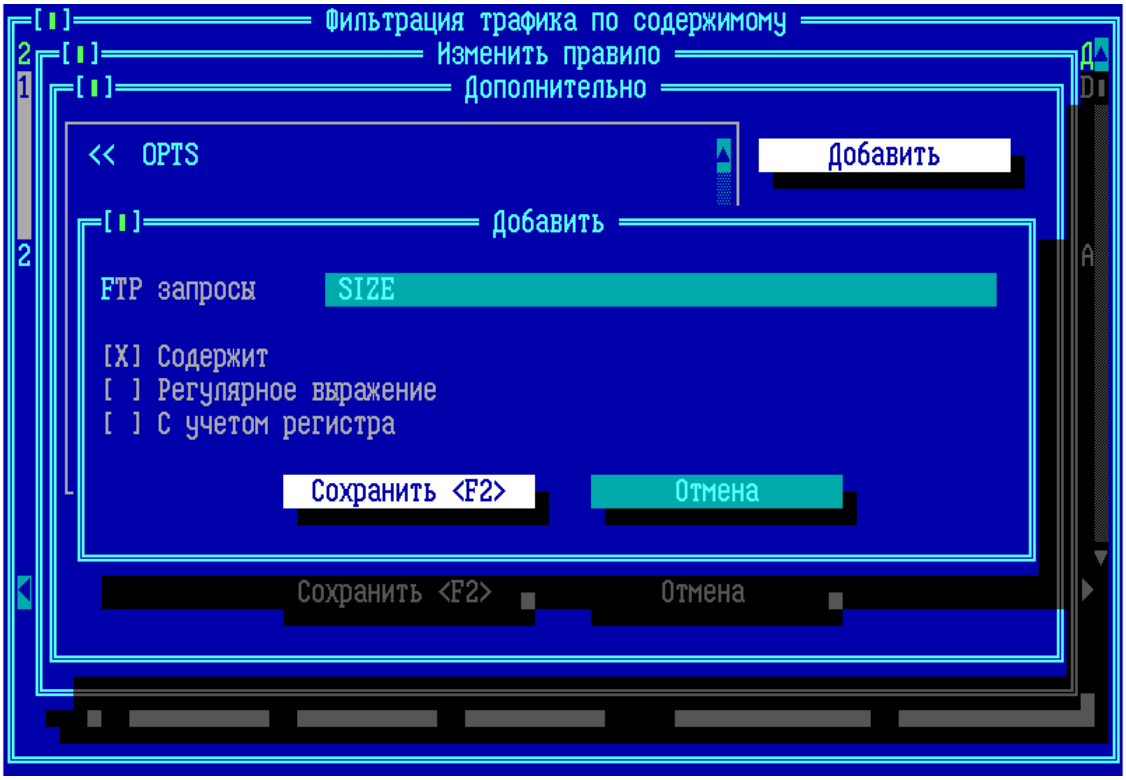


Рисунок 365 - Блокировка браузера Google Chrome, правило 2

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:

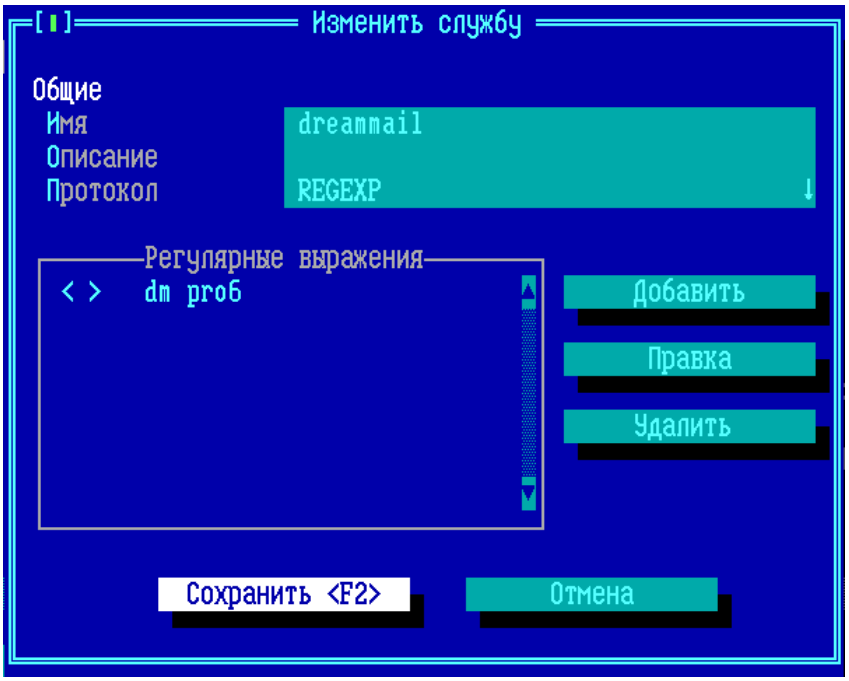


Рисунок 366 - Блокировка работы почтового клиента Dreammail по протоколу SMTP

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:

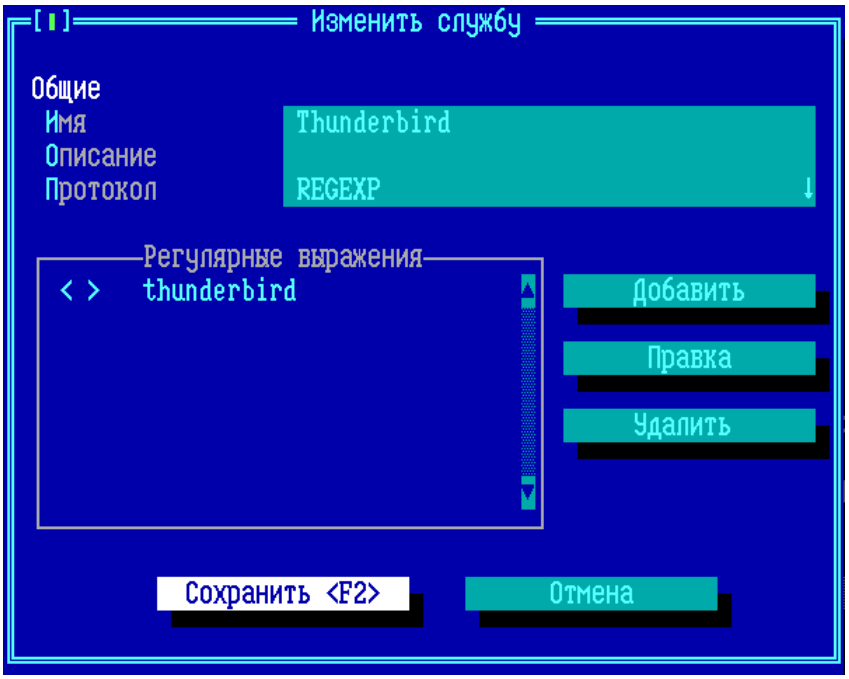


Рисунок 367 - Блокировка работы почтового клиента Thunderbird по протоколу SMTP

9. 2. 4. Признак VLAN в службах

Протокол VLAN в службах предназначен для установки фильтра на основе признака VLAN трафика, обрабатываемого ФПСУ. В дальнейшем следует создать правило МЭ, фильтруя трафик заданной службой VLAN, что позволит перенаправлять, ограничивать или разрешать трафик с данным признаком.

При выборе в добавлении/изменении службы типа протокола VLAN отображается поле для выбора идентификатора описываемого VLAN, выбираемый идентификатор VLAN предварительно должен быть задан в настройках одного из портов.

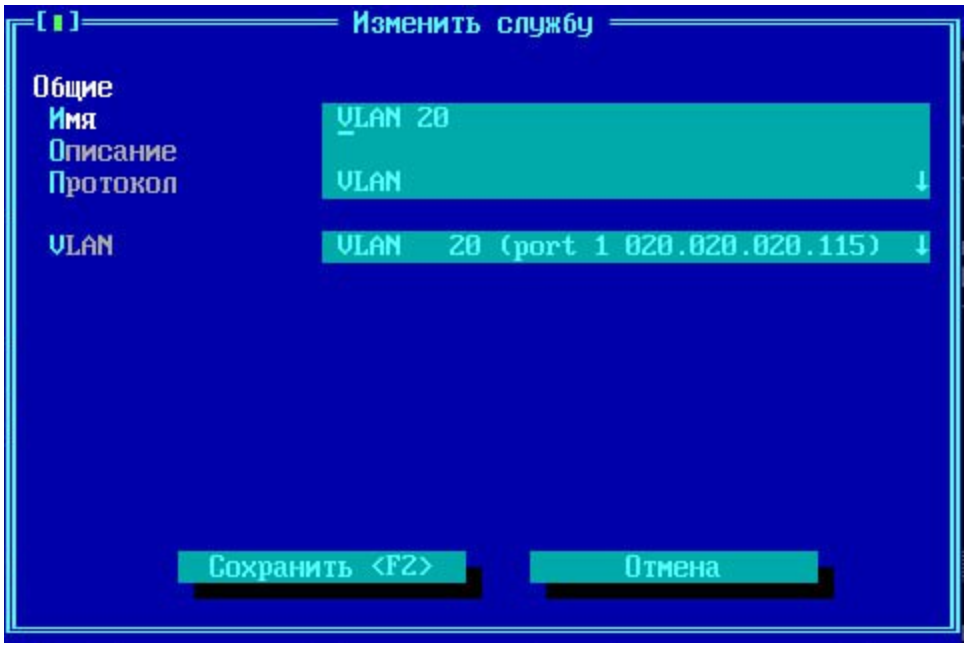
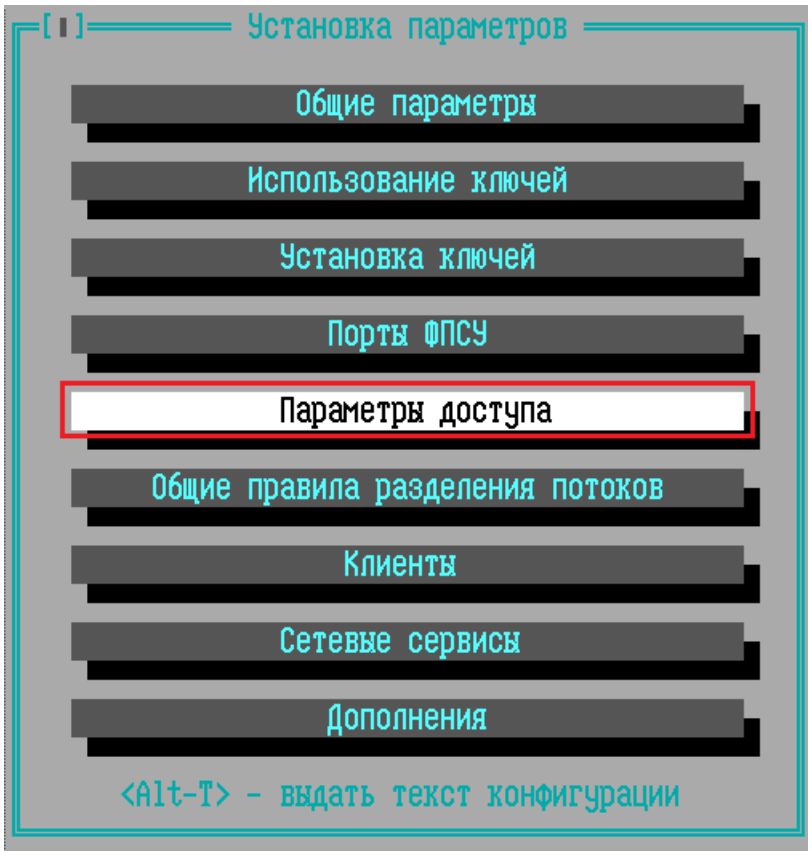


Рисунок 368 - Добавление службы VLAN

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

9. 3. Управление полосой пропускания

Скорость передачи абонентских данных через ФПСУ может контролироваться межсетевым экраном. Для этого в конфигурации параметров доступа ФПСУ создаются специальные правила управления полосой пропускания:



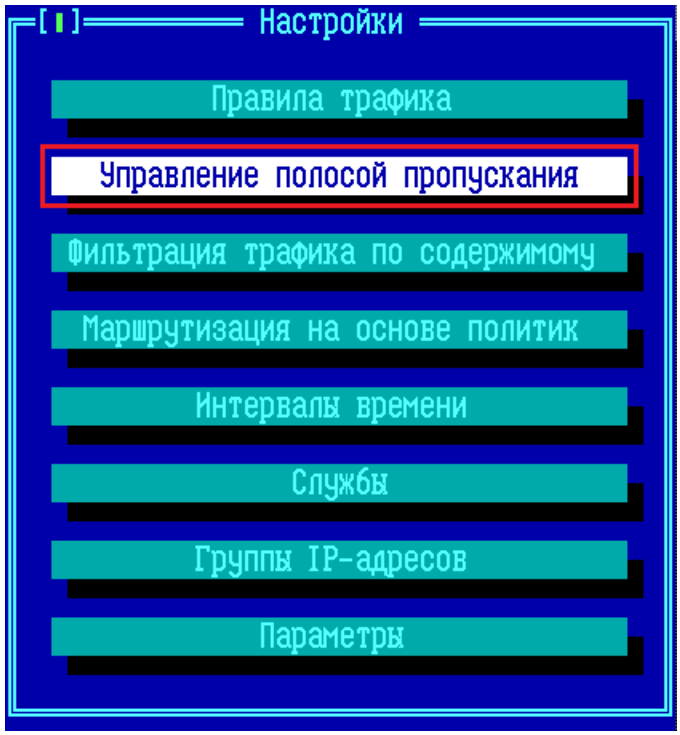


Рисунок 369 - Команды «Параметры доступа» и «Управление полосой пропускания»

Управление ограничением скорости передаваемых через ФПСУ пользовательских данных реализовано следующим образом: администратор ФПСУ 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 правил ограничения скорости передачи данных. Правило по умолчанию одно — **Other —** не устанавливает никаких ограничений на скорость передачи трафика через ФПСУ.

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

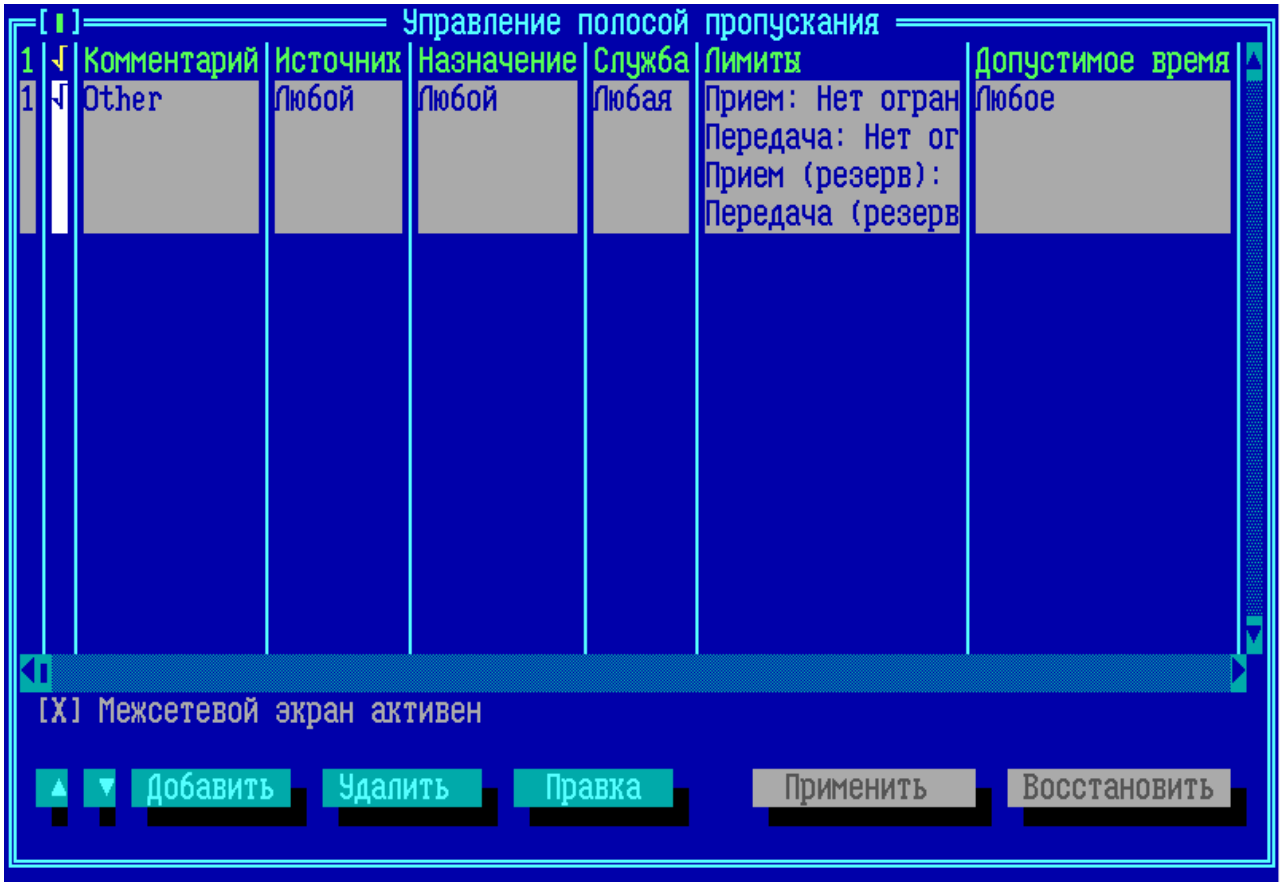


Рисунок 370 - Окно списка правил управления полосой пропускания

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

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

Для создания нового правила управления полосой пропускания, следует нажать клавишу <*Ins*> или кнопку «*Добавить*». В появившемся окне «Добавить правило» находятся четыре вкладки с настраиваемыми опциями. Переход с активной вкладки на соседнюю осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

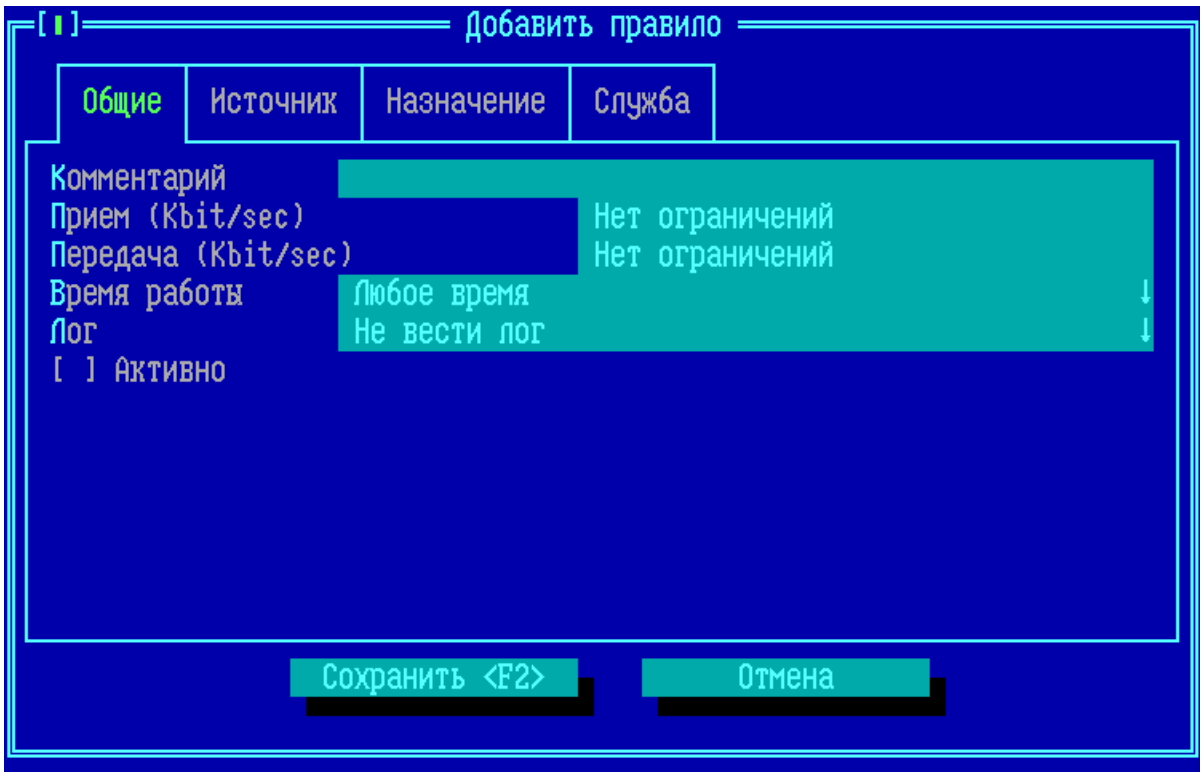


Рисунок 371 - Создание нового правила ограничения скорости передачи данных

Для каждого создаваемого правила требуется указать:

- ограничение скорости приема и передачи данных;
- источник и назначение передачи;
- тип ограничиваемого трафика.

Вкладка **Общие** предназначена для выбора разрешенной скорости передачи данных и опциональных дополнительных настроек. Символом «↓» в конце настраиваемого поля обозначается наличие выпадающего списка, вызываемого нажатием клавиши <*Пробел*> при установленном на поле курсоре.

Вкладка **Общие** содержит следующие настраиваемые опции:

Комментарий — обязательное произвольное текстовое поле для пояснения правила.

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

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

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

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

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

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

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

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

9. 4. Фильтрация трафика по содержимому (DPI)

В дополнение к фильтрации по правилам маршрутизации и правилам трафика межсетевого экрана, на ФПСУ реализована фильтрация и принятие решения о блокировке пакета на основе передаваемого содержимого. Анализируются передаваемые данные

различных протоколов, в том числе методы, контент и адрес http-запросов.

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

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

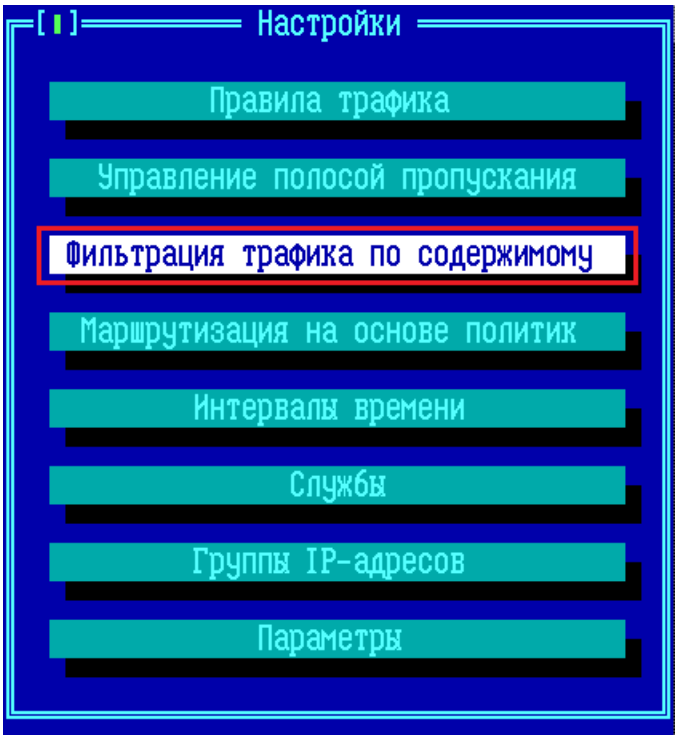


Рисунок 372 - Меню настройки межсетевого экрана ФПСУ

В открывшемся окне будет выведен список используемых на ФПСУ 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 пакетам.

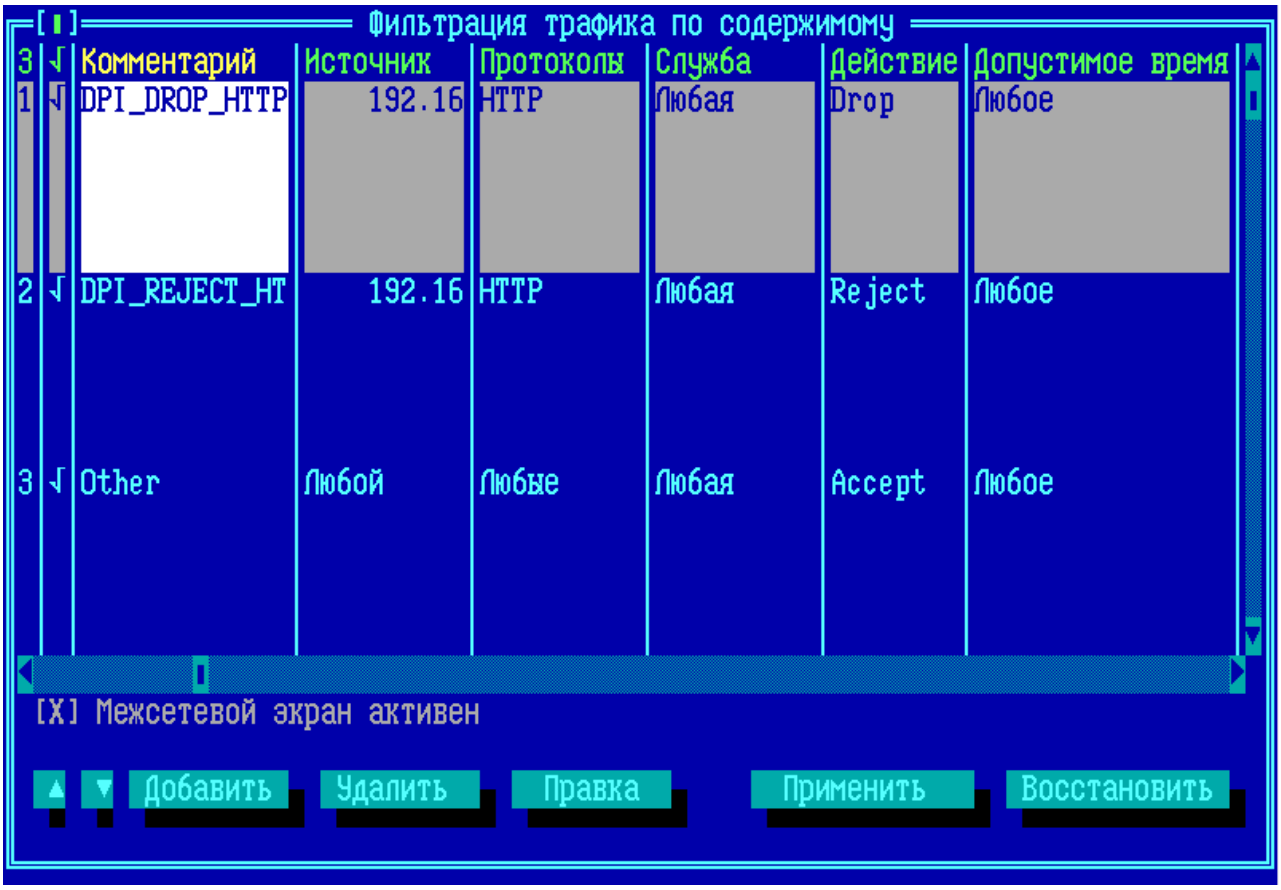


Рисунок 373 - Окно списка правил фильтрации трафика по содержимому

Фильтрация трафика по содержимому осуществляется только при активном межсетевом экране ФПСУ. Флаг «*Межсетевой экран активен*» указывает на работу дополнительных правил фильтрации, в том числе правил фильтрации трафика по содержимому.

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

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

9. 4. 1. Создание правила фильтрации по содержимому и его общие настройки

Для создания нового правила фильтрации по содержимому следует нажать клавишу <*Ins*> или кнопку «*Добавить*» в окне списка правил фильтрации по содержимому.

В появившемся окне «Добавить правило» находятся вкладки с настраиваемыми параметрами правила, которые определяют, как и какой тип трафика будет исследоваться. Переход с активной вкладки на соседнюю осуществляется установлением курсора на вкладку и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

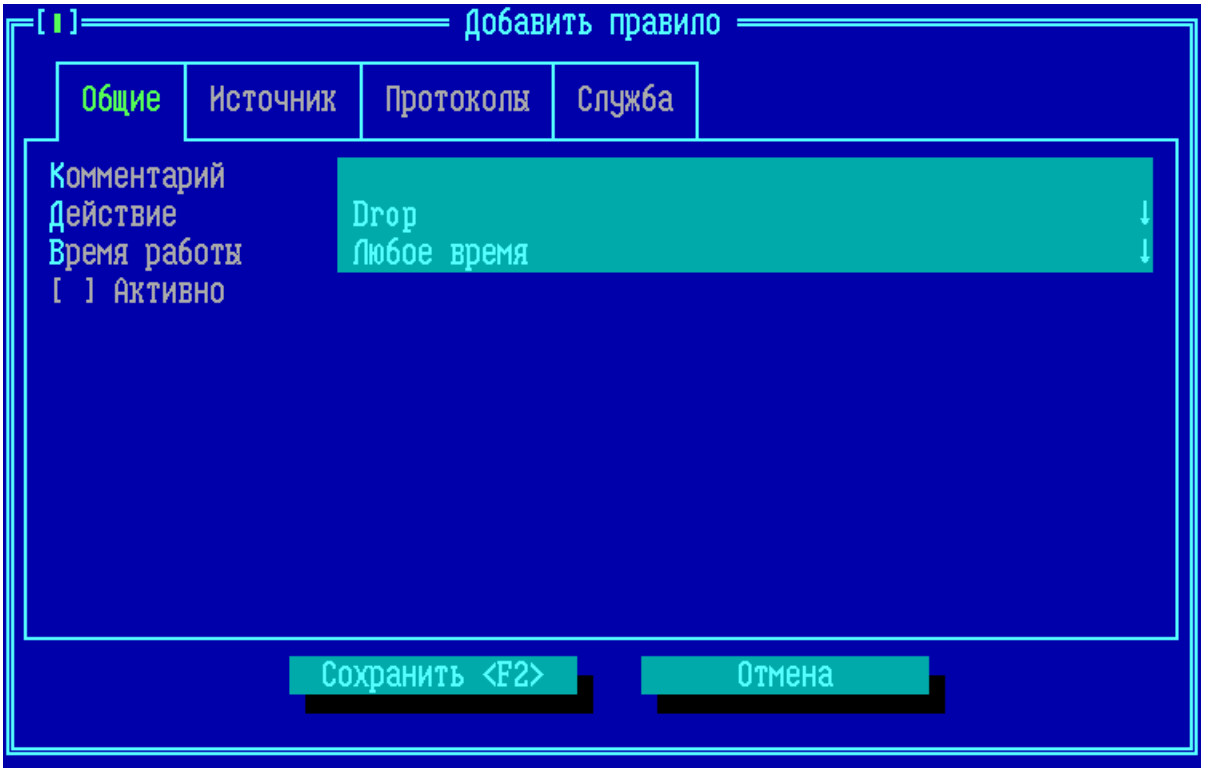


Рисунок 374 - Добавление нового правила фильтрации по содержимому

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; она определяет, как поступить с передаваемым пакетом. В выпадающем меню могут быть выбраны следующие варианты действий:

- *Drop* — действие по умолчанию, пакет данных будет сброшен, оповещение об отказе передачи пакета не будет передано отправителю;
- *Reject* — пакет данных будет сброшен, отправителю будет передано ICMP-оповещение об отказе передачи пакета.

Символом «↓» в конце настраиваемого поля обозначается наличие выпадающего списка, вызываемого нажатием клавиши <*Пробел*> при установленном на поле курсоре.

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

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

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

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

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

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

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

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

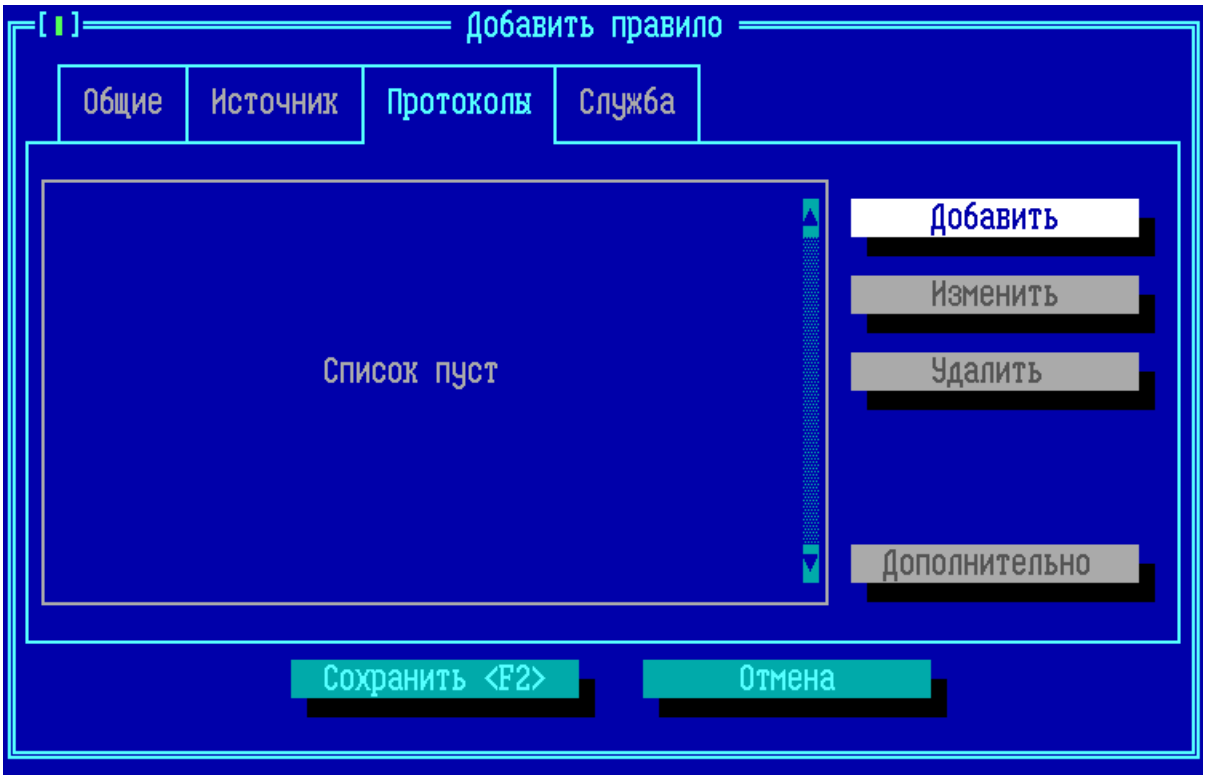


Рисунок 375 - Вкладка «Протоколы»

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 376 - Окно выбора исследуемого протокола

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

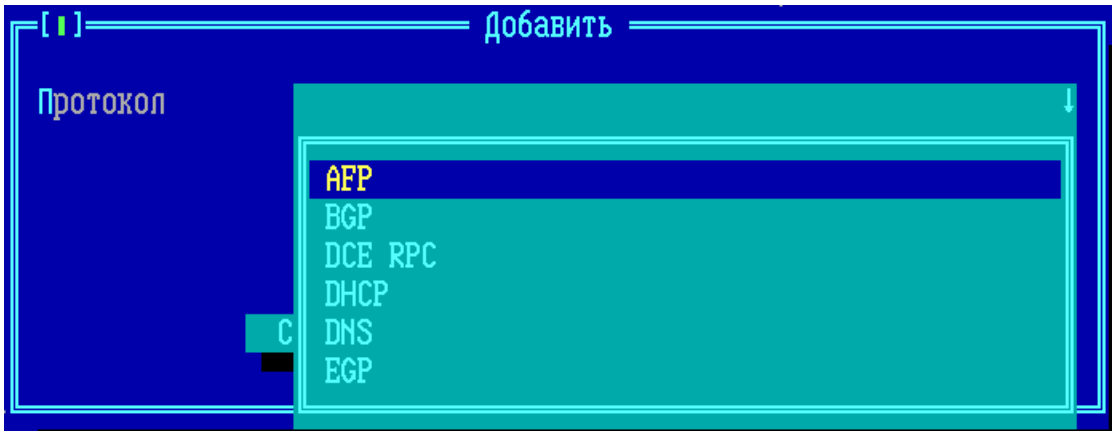


Рисунок 377 - Выбор исследуемого протокола

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

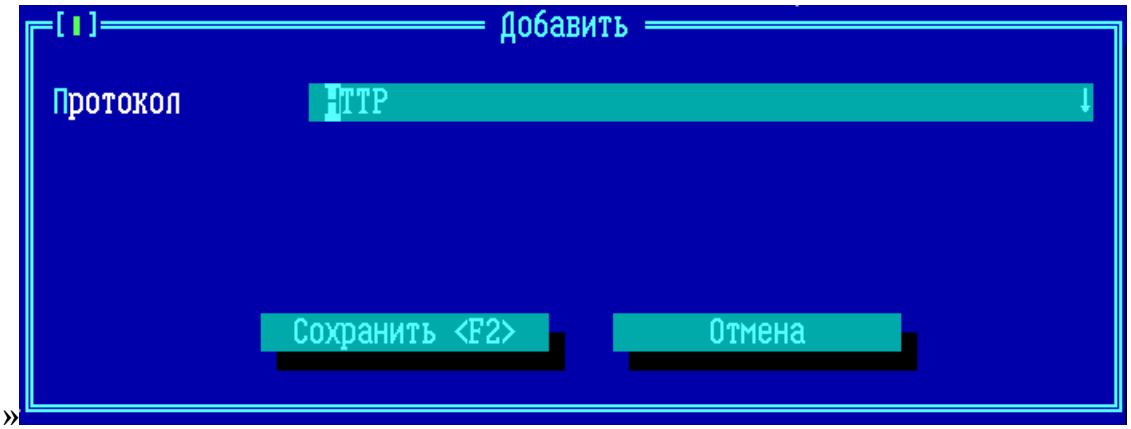


Рисунок 378 - Выбран протокол для исследования

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

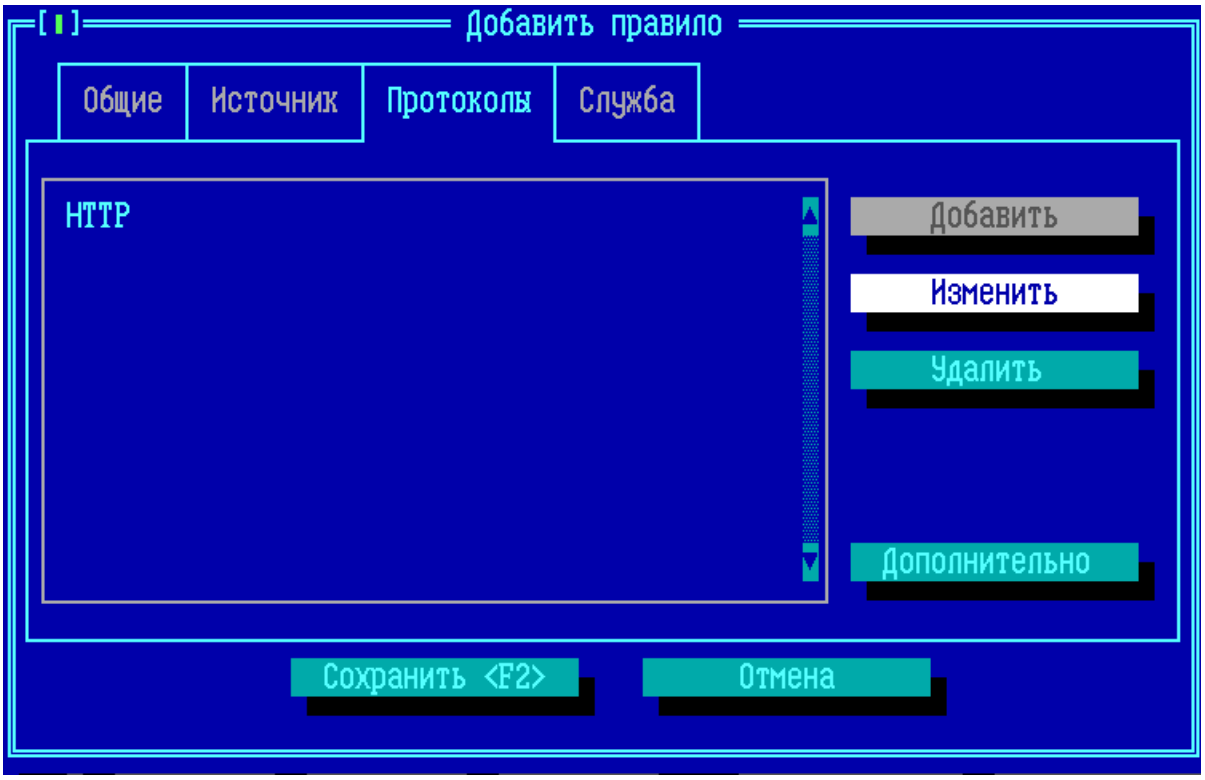


Рисунок 379 - Протокол, исследуемый правилом

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.

9. 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:

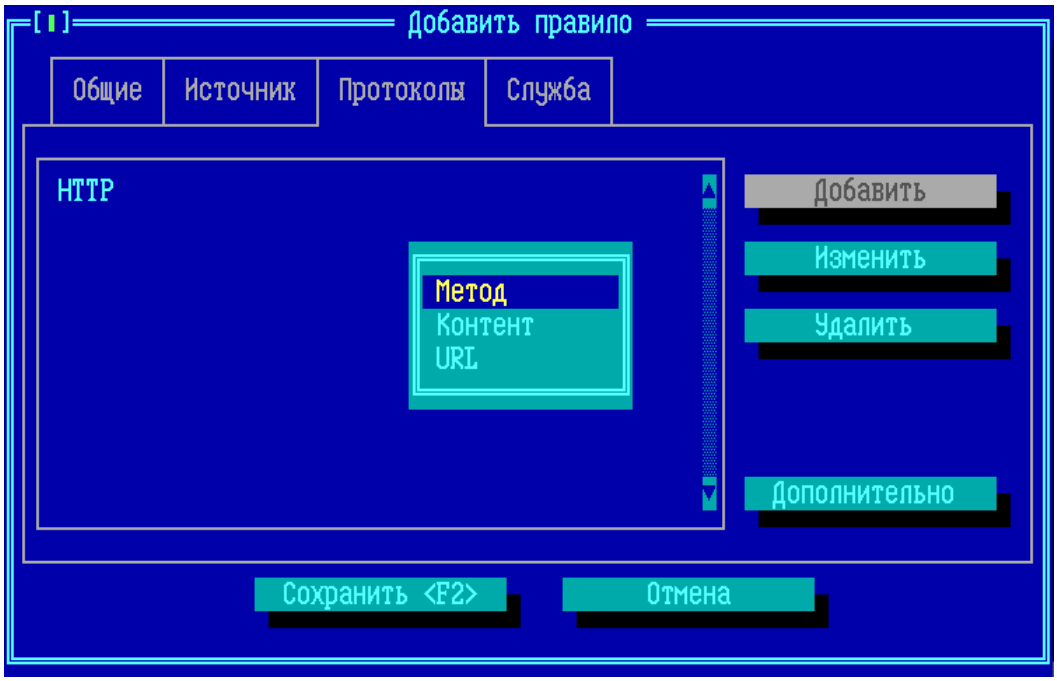


Рисунок 380 - Доступные опции исследования протокола HTTP

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

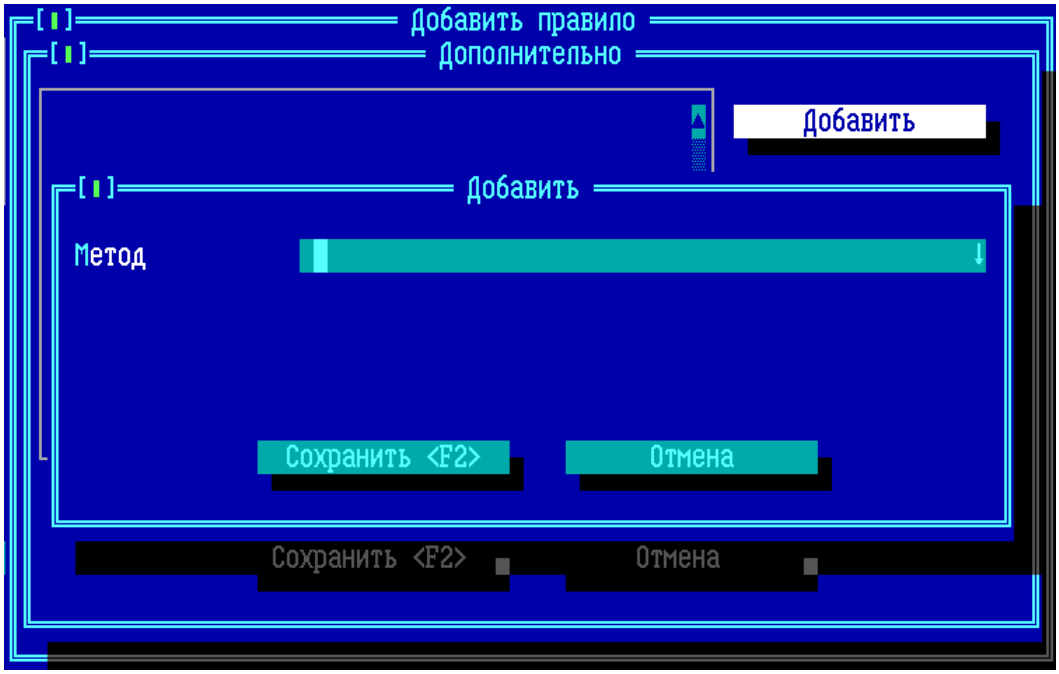


Рисунок 381 - Добавление фильтруемого метода протокола http

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):

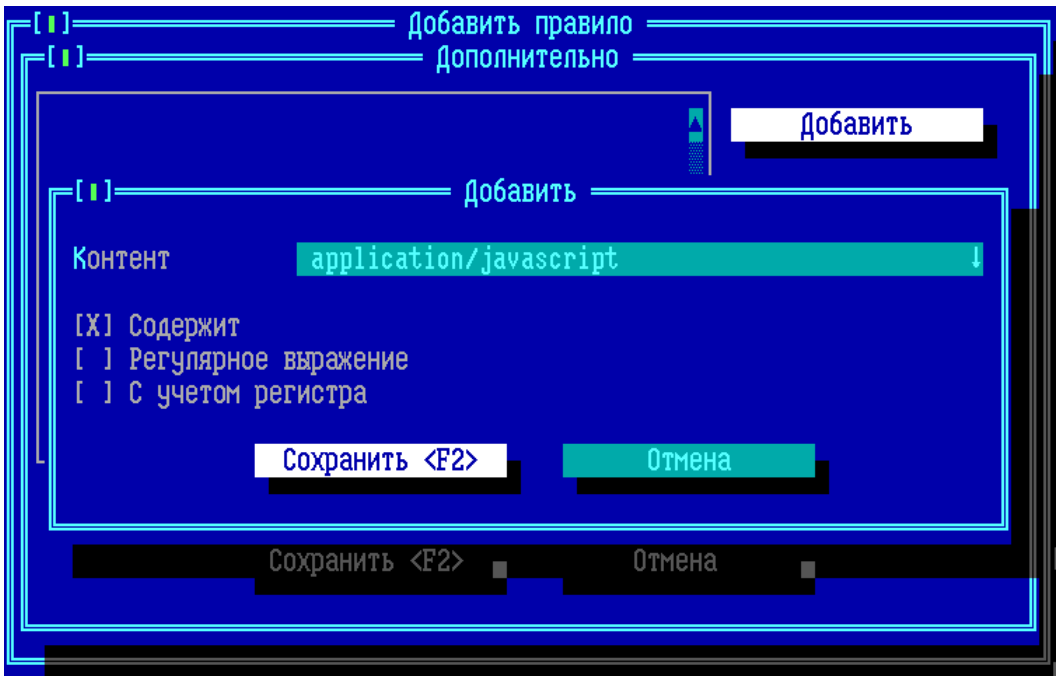


Рисунок 382 - Добавление фильтруемого контента протокола http

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

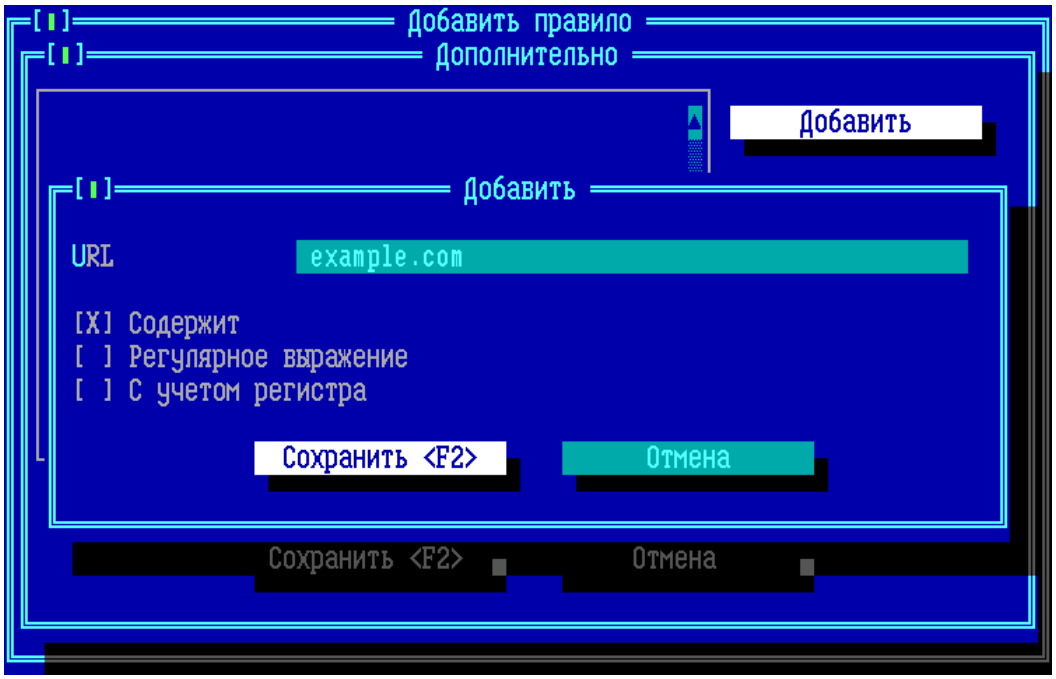


Рисунок 383 - Добавление фильтруемого URL-адреса протокола http

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

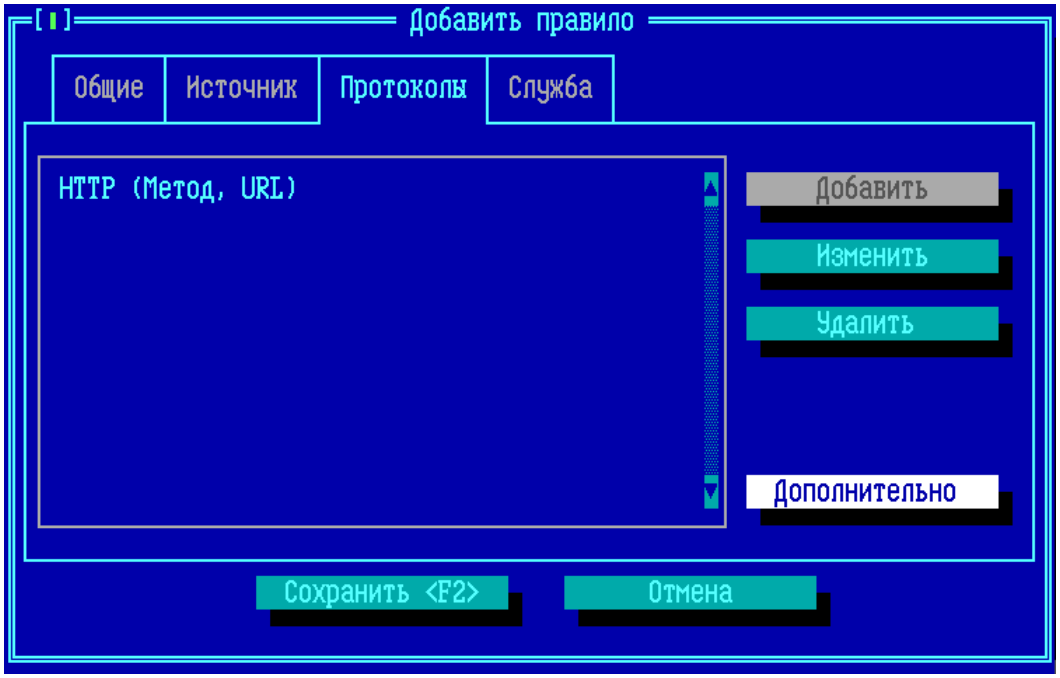


Рисунок 384 - Правило с дополнительными фильтрами протокола http

9. 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»).

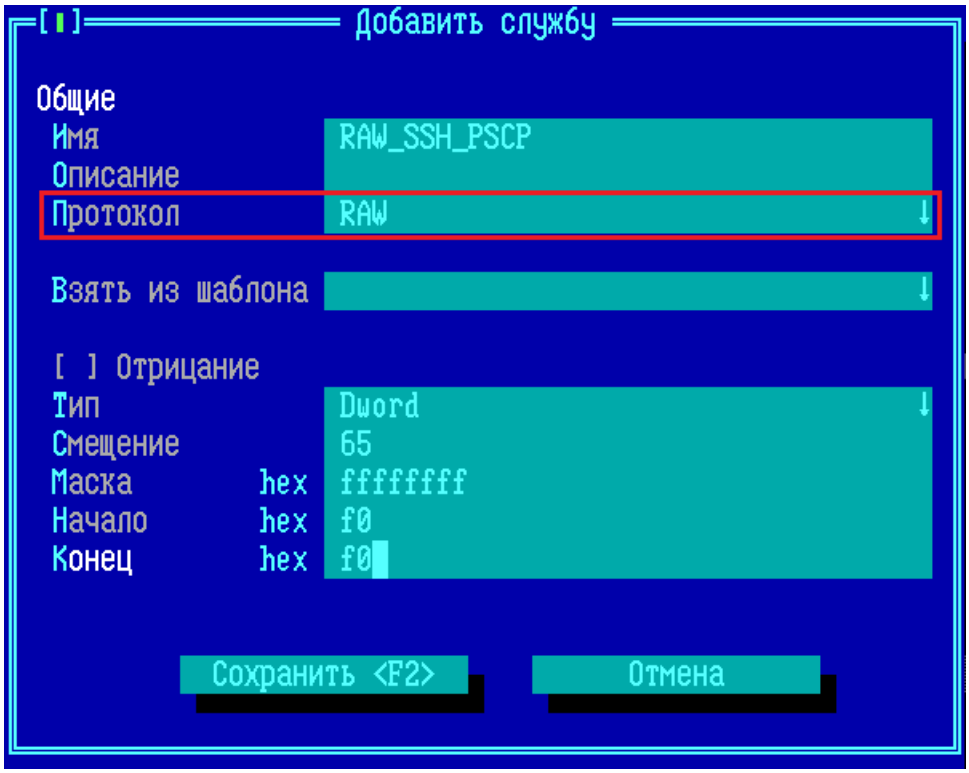


Рисунок 385 - Служба для протокола RAW

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

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

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

Приоритет этих двух правил относительно друг друга не важен.

9. 5. Маршрутизация на основе политик

На ФПСУ реализована маршрутизация на основе политик, трафик можно перенаправлять с выбранного порта ФПСУ или в выбранный туннель. Пакет при этом не меняется, как и адрес получателя.

Маршрутизация на основе политик применяется в случае наличия нескольких сетевых интерфейсов и необходимости отправлять определенные пакеты через выбранный интерфейс. Маршрут пакета определяется не только на основе адреса назначения, есть возможность задать маршрут на основе источника или назначения пакета, а также по типу протокола.

Маршрутизация на основе политик выполняется после статической или динамической маршрутизации, изменяет маршрут и отправляет пакеты по настроенным правилам. Если для группы пакетов в маршрутизации на основе политик не указано как их маршрутизировать, то они будут отправлены по правилам статической или динамической маршрутизации.

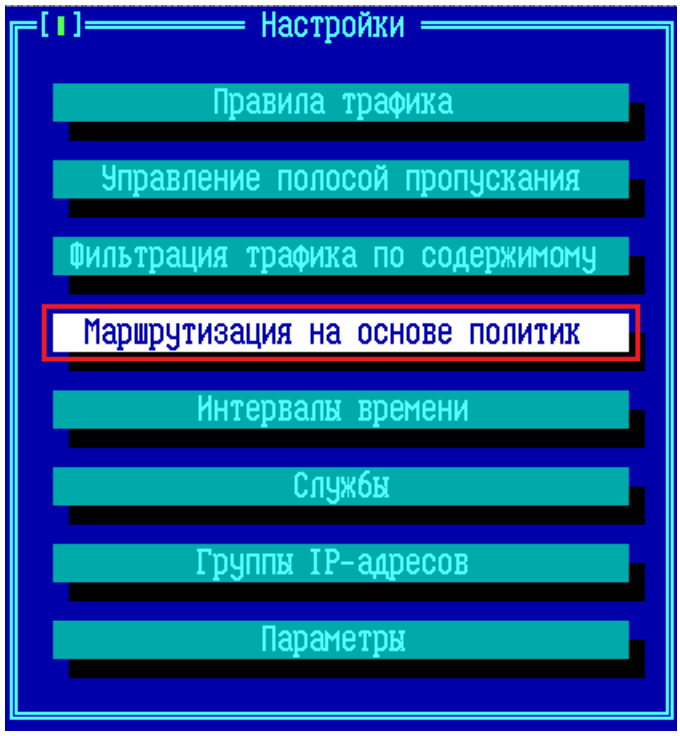


Рисунок 386 - Меню настройки межсетевого экрана ФПСУ

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

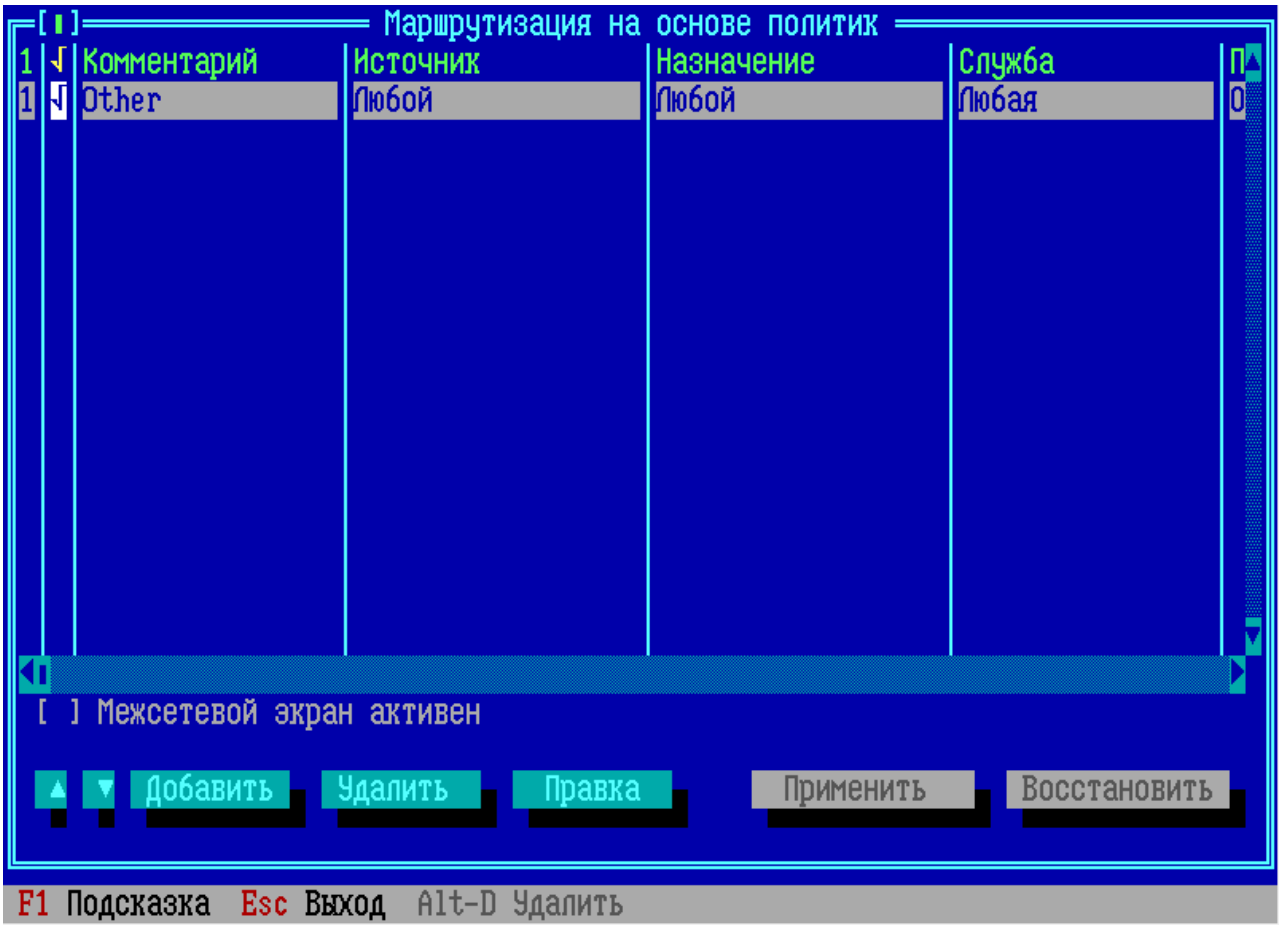


Рисунок 387 - Окно списка правил фильтрации трафика на основе политик

Фильтрация трафика по содержимому осуществляется только при активном межсетевом экране ФПСУ. Флаг «*Межсетевой экран активен*» указывает на работу дополнительных правил фильтрации, в том числе правил фильтрации трафика на основе политик.

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

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

Для создания нового правила фильтрации на основе политик, следует нажать клавишу <*Ins*> или кнопку «*Добавить*» в окне списка правил фильтрации по содержимому.

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

Символ «↓» в конце настраиваемого поля обозначает наличие выпадающего списка, вызываемого нажатием клавиши <*Пробел*> при установленном на поле курсоре.

Вкладка **Общие** содержит следующие настраиваемые опции:

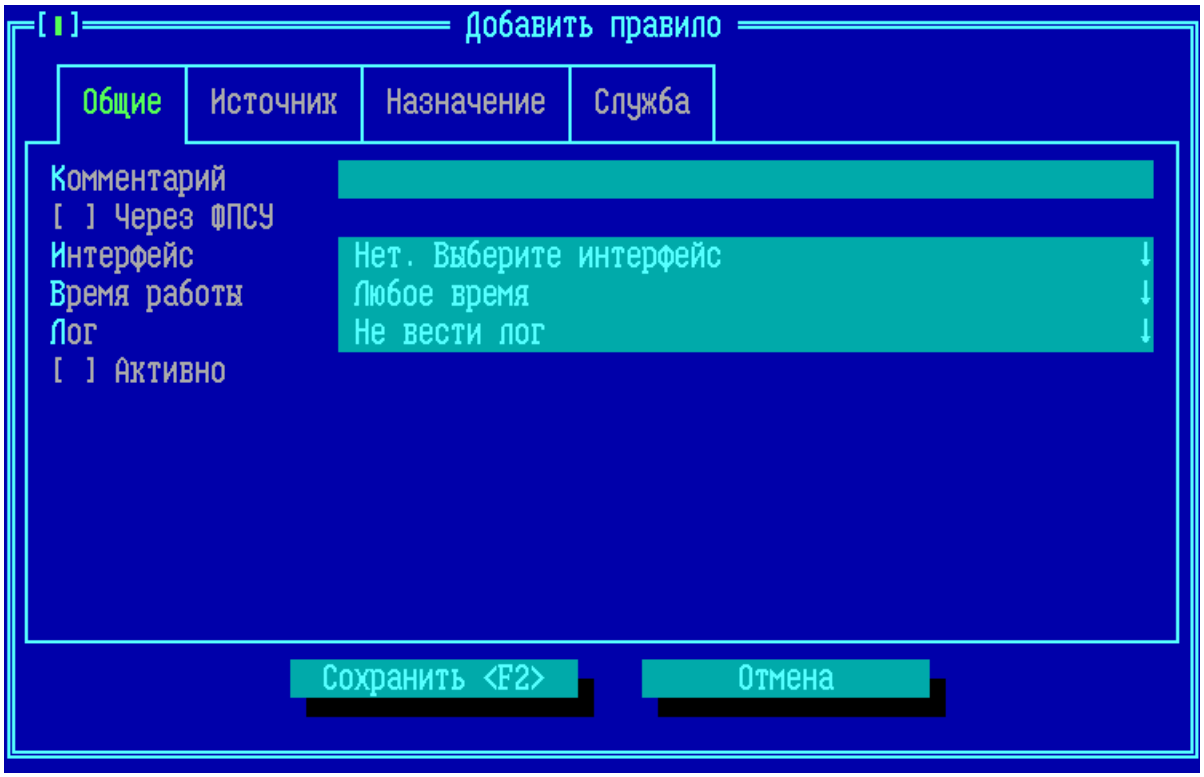


Рисунок 388 - Добавление нового правила трафика

Комментарий – обязательное текстовое поле для пояснения правила.

Через ФПСУ – при установлении флага пакеты, подпадающие под данное правило трафика, будут отправляться в туннель между ФПСУ. Название поля ниже поменяется на «ФПСУ», в этом поле следует выбрать ФПСУ из списка, описанных на портах ФПСУ.

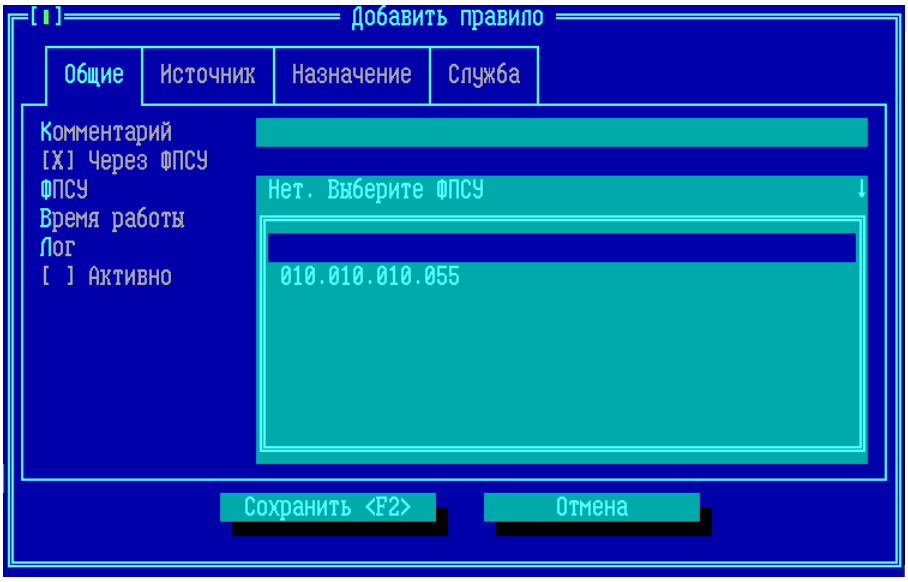


Рисунок 389 - Флаг «Через ФПСУ» установлен

Интерфейс – выбор порта ФПСУ, с которого пакеты отправляются получателю.

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

Лог — если требуется вести журнал, содержащий разрешенные и запрещенные в рамках данного правила передачи данных, то следует выбрать из выпадающего списка опцию *Вести лог* или *Вести лог, писать заголовки пакетов*. Значение по умолчанию - *Не вести лог*.

Для того, чтобы все указанные в правиле настройки после сохранения были задействованы, следует перед выходом установить флаг *«Активно»*.

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

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

На вкладке **Служба** устанавливаются ограничения в скорости передачи данных не для всего трафика между указанными сетевыми объектами, а только для подпадающего под

дополнительные фильтры (подробнее про вкладку **Служба** см. пункт «Службы в правилах трафика»).

9. 6. Интервалы времени

Пункт «Интервалы времени» меню правил доступа предназначен для создания и управления используемых правилами трафика и правилами фильтрации по содержимому временных интервалов.

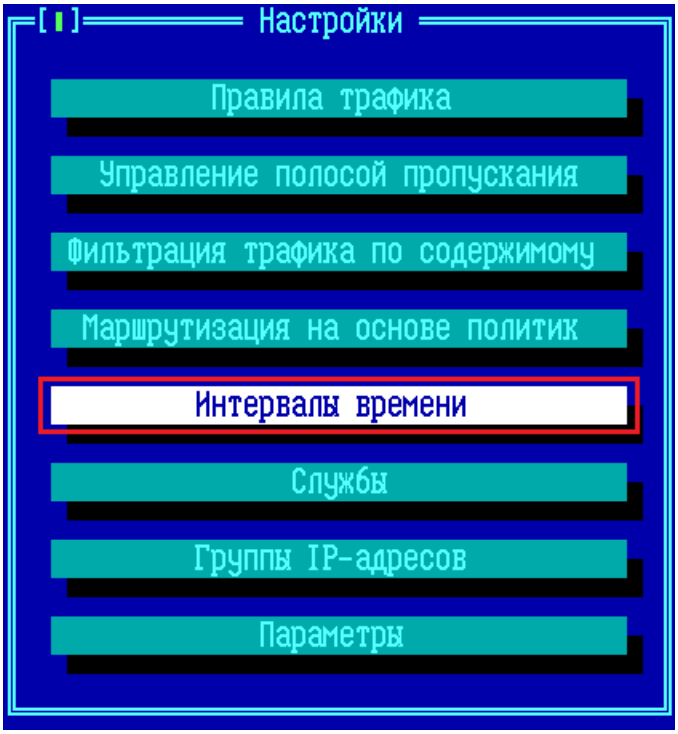


Рисунок 390 - Команда «Интервалы времени»

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):

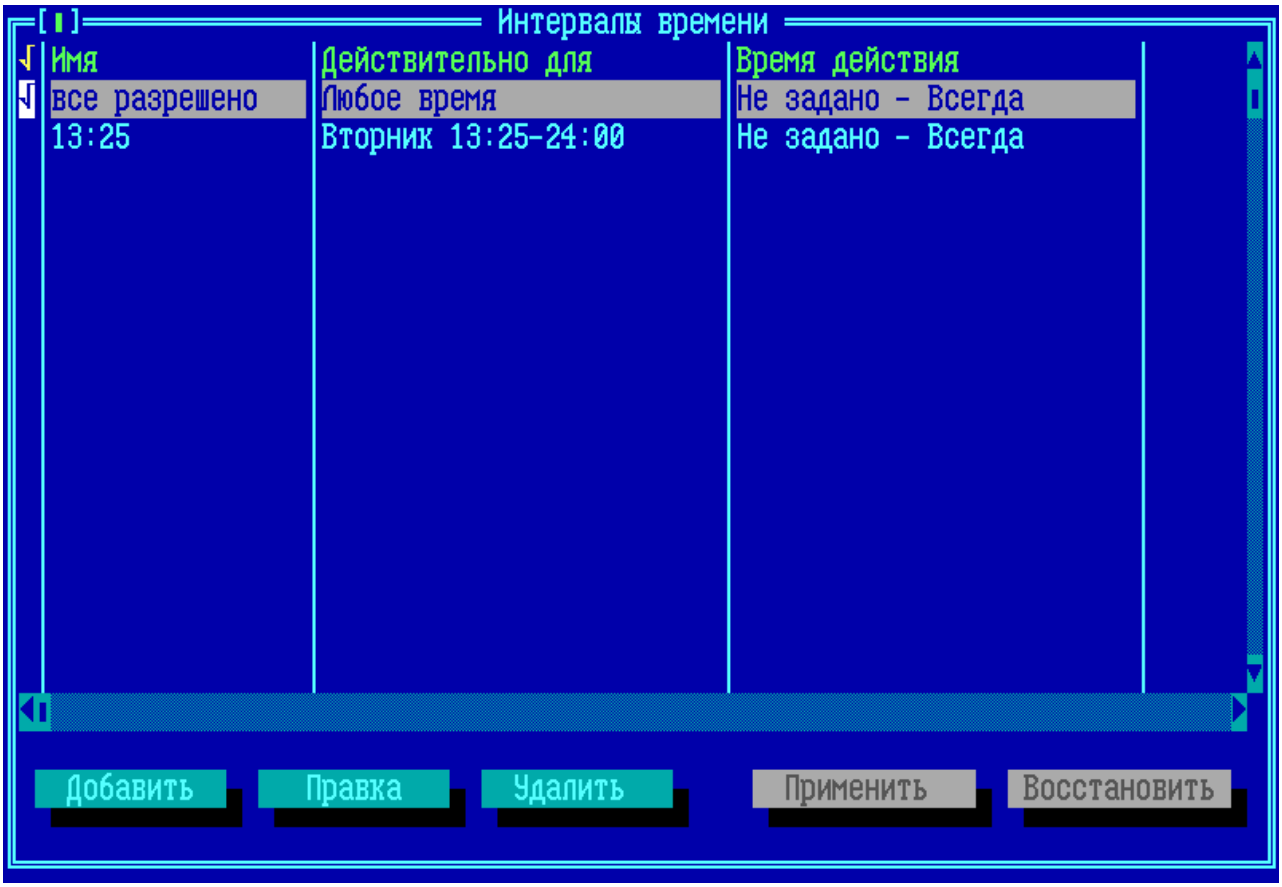


Рисунок 391 - Список определенных интервалов времени

Команды окна управления списком интервалов:

Добавить **—** кнопка, по нажатию который происходит вызов окна создания нового интервала времени.

Правка — кнопка, по нажатию которой (или клавиши <*Enter*>) происходит вызов окна параметров ранее созданного интервала времени.

Удалить — по нажатию кнопки происходит удаление интервала времени, отмеченного курсором.

Применить — при внесении изменений в существующие интервалы времени следует подтвердить изменения, нажав эту кнопку (или клавишу <*F2*>). ВНИМАНИЕ! При выходе из окна управления списком интервалов времени по клавише <*Esc*> или сочетанию клавиш <*Alt+X*>, изменения не сохраняются!

Восстановить — по нажатию этой кнопки будут отменены все выполненные в этот сеанс работы изменения в существующих интервалах времени.

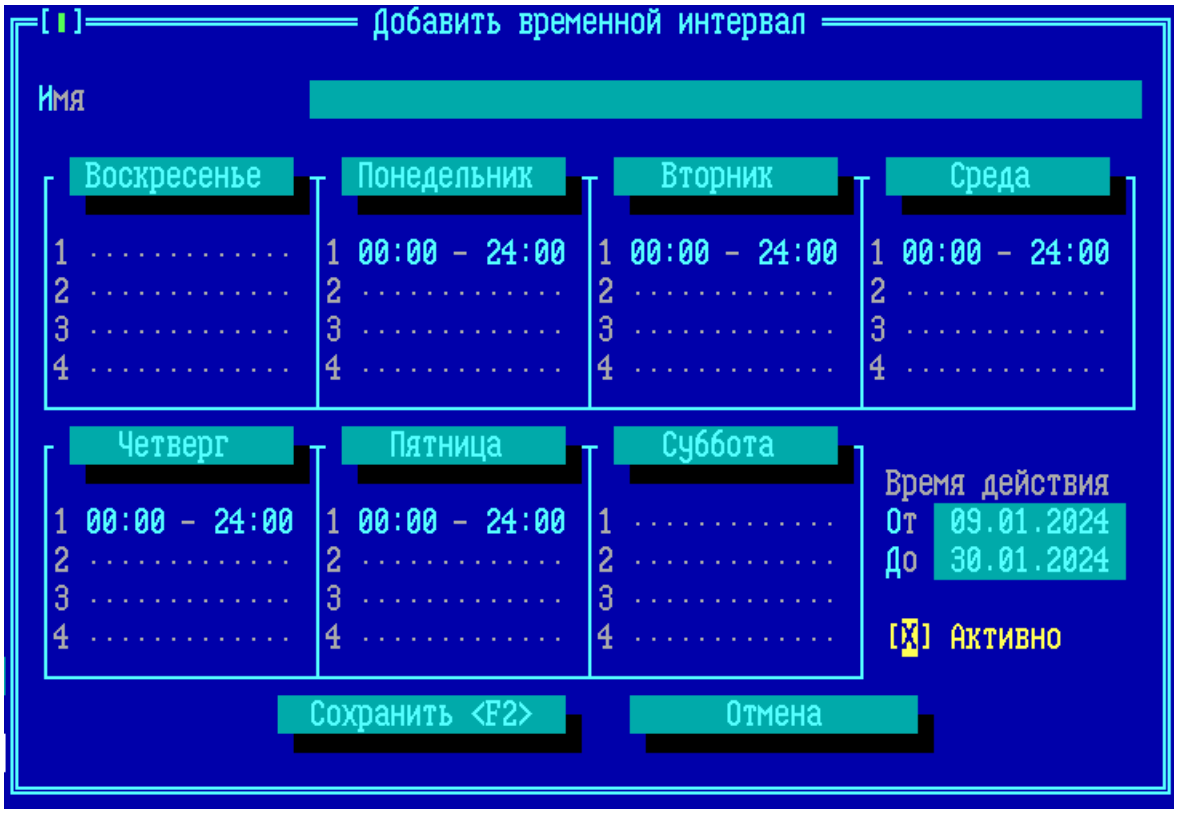


Рисунок 392 - Параметры временного интервала

Для каждого дня недели можно указать до четырех временных интервалов, в которые разрешен обмен пакетами. Если ограничений нет - устанавливается интервал 00:00 - 24:00, если работа не разрешена - временные интервалы должны быть пусты. Удаления значений в каждом из интервалов работы производится нажатием клавиши <*Del*>. После определения всех интервалов следует включить флаг «*Активно*» (при помощи клавиши <*Пробел*>) для активации сделанных ограничений.

Во временном интервале может быть опционально установлено время действия правила в масштабе временных дат. В графе «Время действия» в таком случае следует указать дату начала и дату завершения разрешенного периода действия временного интервала.

Сохраните сделанные установки нажатием клавиши <*F2*> (или выйдите без сохранения при помощи <*Esc*>).

9. 7. Группы IP-адресов

Действие создаваемого правила трафика (пункт «Правила трафика») можно ограничить, установив его действие не на все передаваемые данные между указанными отправителями и получателями, а только на те, которые дополнительно входят и в диапазон указанных во вкладке «Группы IP-адресов».

В окне, вызываемом по выполнению команды «Группы IP-адресов» меню настройки конфигурации «Параметры доступа» правил дополнительной фильтрации, находится список созданных администраторами ФПСУ групп IP-адресов (по умолчанию пустой).

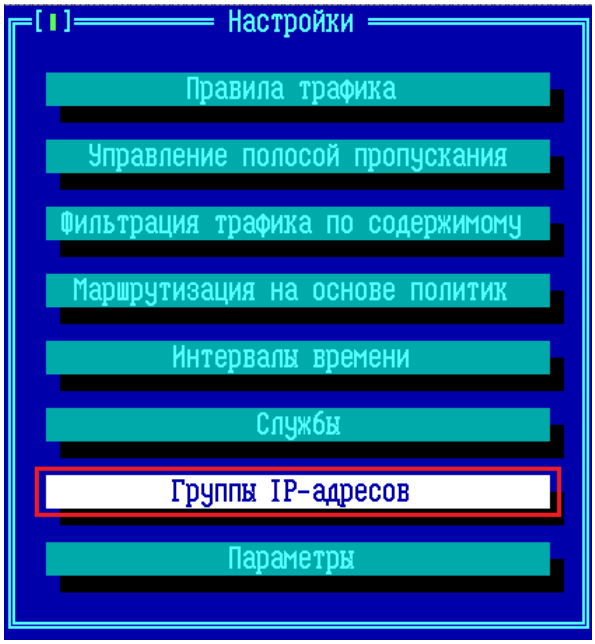


Рисунок 393 - Команда настройки групп IP-адресов параметров доступа

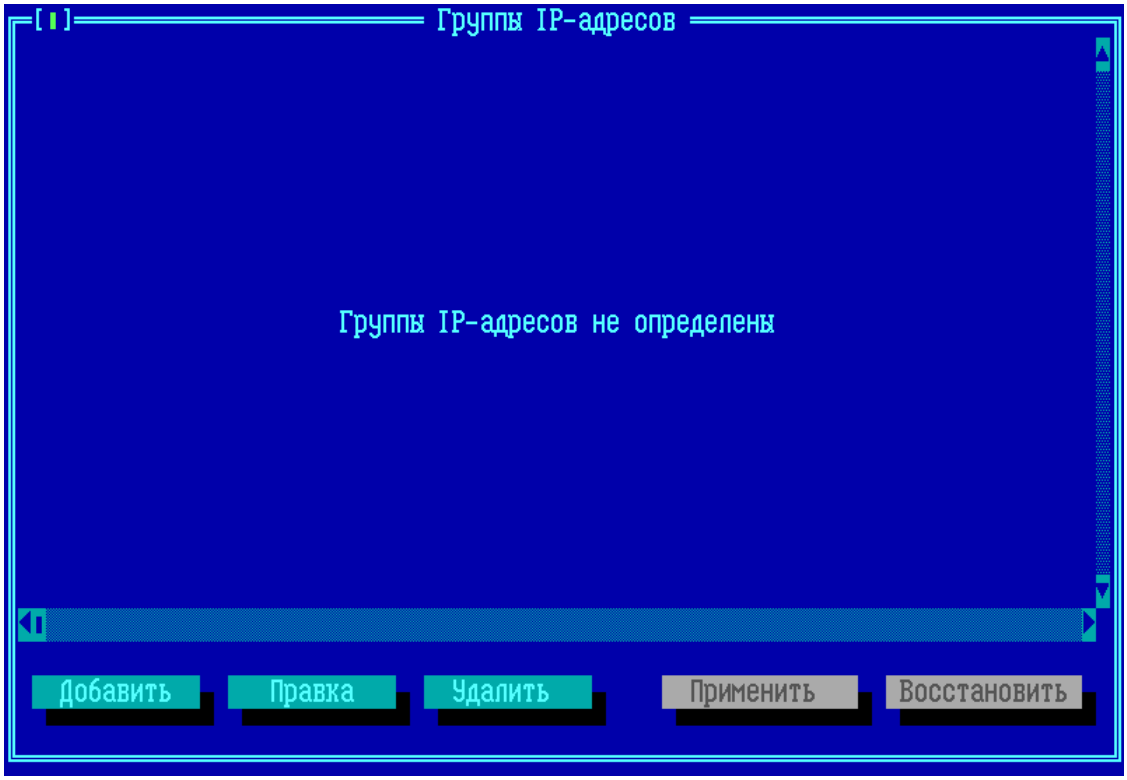


Рисунок 394 - Окно со списком групп IP-адресов

Находящиеся в списке группы IP-адресов используются при создании и изменении правил трафика (см. пункт «Вкладки «Источник» и «Назначение» правил трафика», описание последовательности действий «*Объект → Добавить*»).

Для добавления новой группы IP-адресов в список, нажмите в окне списка групп IP-адресов кнопку «*Добавить*» или клавишу <*Ins*>.

В открывшемся окне «Добавить группу» расположено несколько вкладок с параметрами создаваемой группы. Переход с активной вкладки на соседнюю осуществляется установлением курсора на вкладке и нажатием сочетаний клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

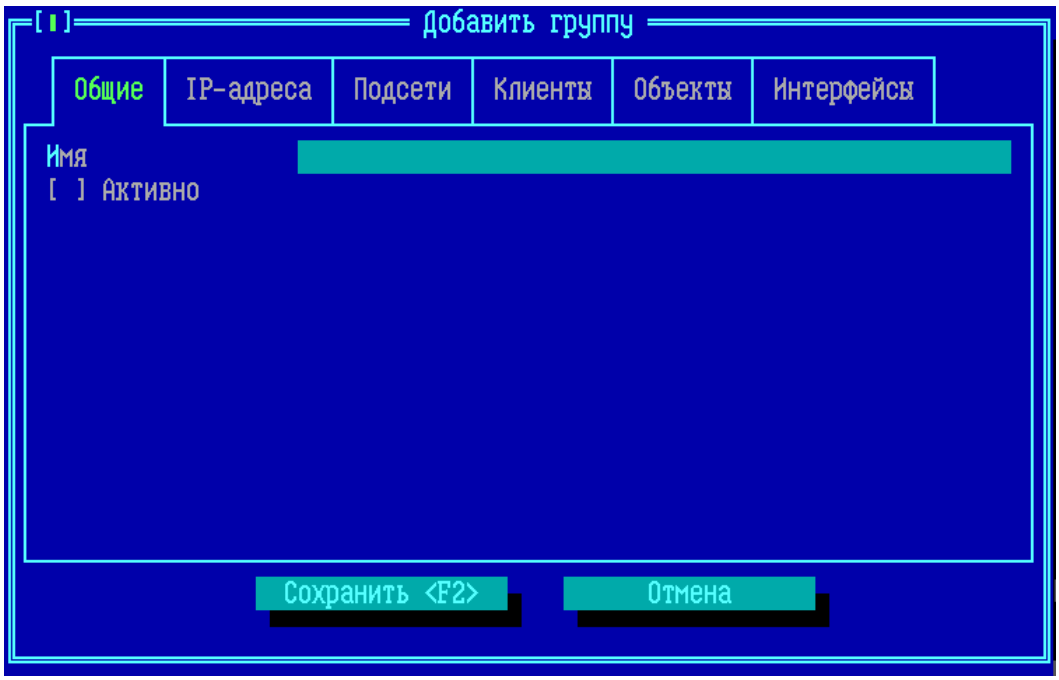


Рисунок 395 - Создание новой группы IP-адресов

Вкладка **Общие** содержит символьное название создаваемой группы, которое будет использоваться для привязки группы IP-адресов к тому или иному правилу трафика, и флаг «*Активно*», подтверждающий действие внесенных в группу изменений.

Вкладка **IP-адреса** содержит список входящих в группу отдельных IP-адресов (по умолчанию пустой). IP-адреса, вносимые в список, должны принадлежать диапазону описанных и разрешенных к маршрутизации IP-адресов (см. раздел «Порты ФПСУ»).

Вкладка **Подсети** содержит список входящих в группу подсетей, выбранных из маршрутизации (по умолчанию пустой). Подсети IP-адресов, вносимые в список, должны принадлежать диапазону описанных и разрешенных к маршрутизации IP-адресов (см. раздел «Порты ФПСУ»).

Вкладка **Клиенты** содержит список (по умолчанию пустой) входящих в группу описателей ФПСУ-IP/Клиентов, выбранных из списка зарегистрированных на данном ФПСУ криптосетей и групп клиентов (см. раздел «Клиент для ФПСУ»).

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 (по умолчанию пустой).

После сохранения группы, она помещается в окно списка:

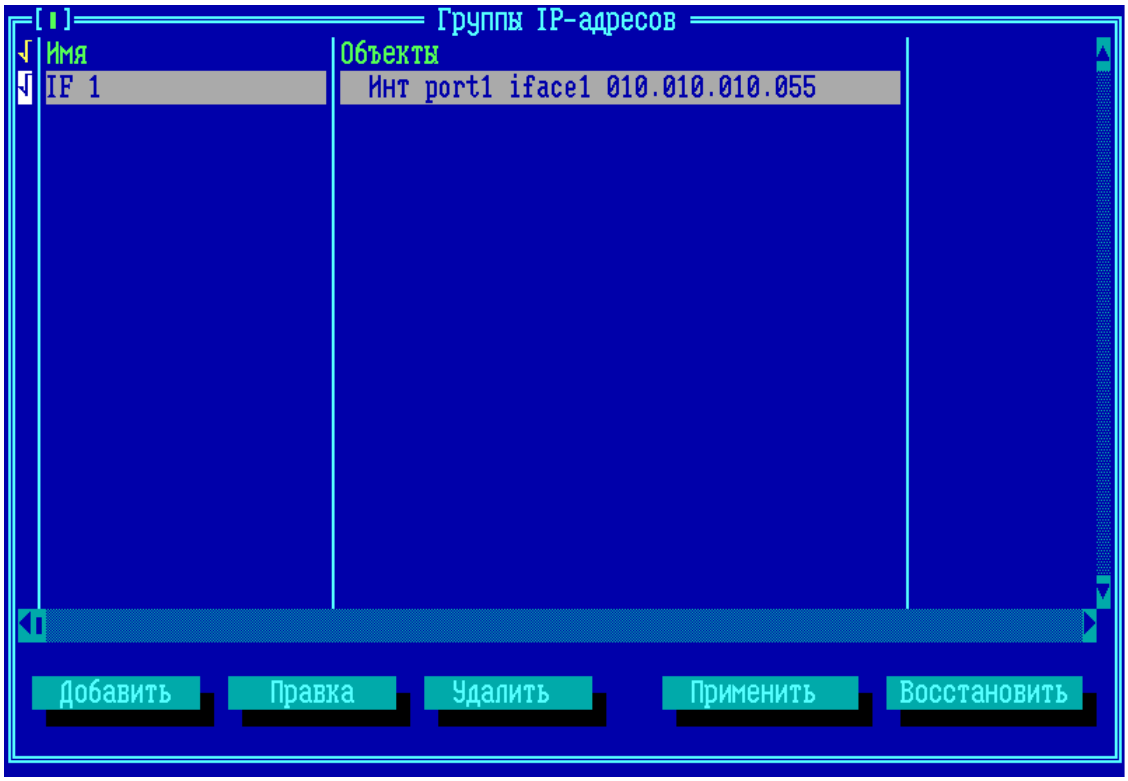


Рисунок 396 - В список групп IP-адресов добавлена новая запись

9. 8. Дополнительные параметры и защита от flood-атак

Команда «Параметры» меню «Параметры доступа» правил дополнительной фильтрации содержит список дополнительных опций межсетевого экрана.

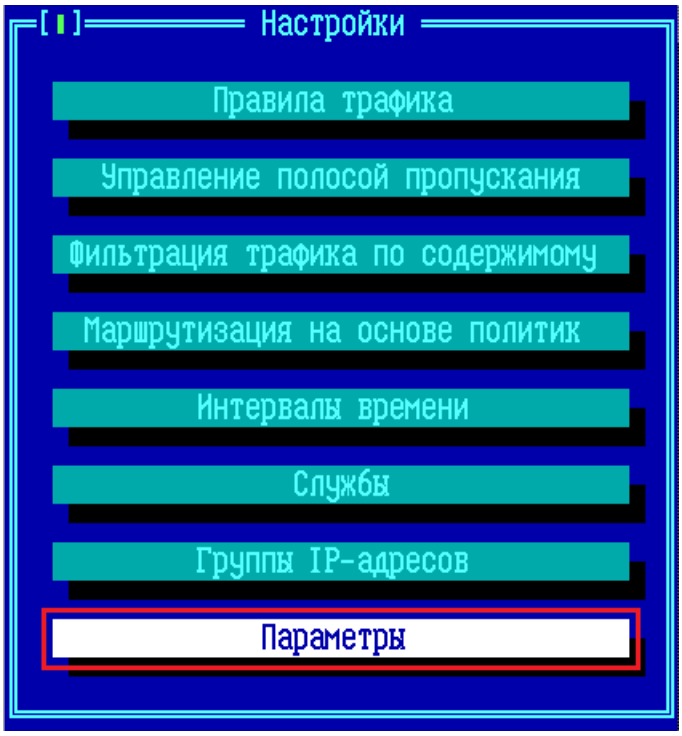


Рисунок 397 - Дополнительные параметры межсетевого экрана ФПСУ

Окно состоит из трех вкладок. Первые две, **Соединения** и **Анти-флуд и СОВ**, предназначены для настройки системы защиты ФПСУ от атак отказа в обслуживании (flood-атак). Переход между вкладками осуществляется установлением курсора на вкладке и нажатием сочетания клавиш <*Ctrl* →> и <*Ctrl* ←> или клавиш <→> и <←>.

Вкладка **Соединения** содержит установленные по умолчанию параметры работы межсетевого экрана ФПСУ 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 (первый столбец), и время обнаружения атаки отказа в обслуживании (второй столбец).

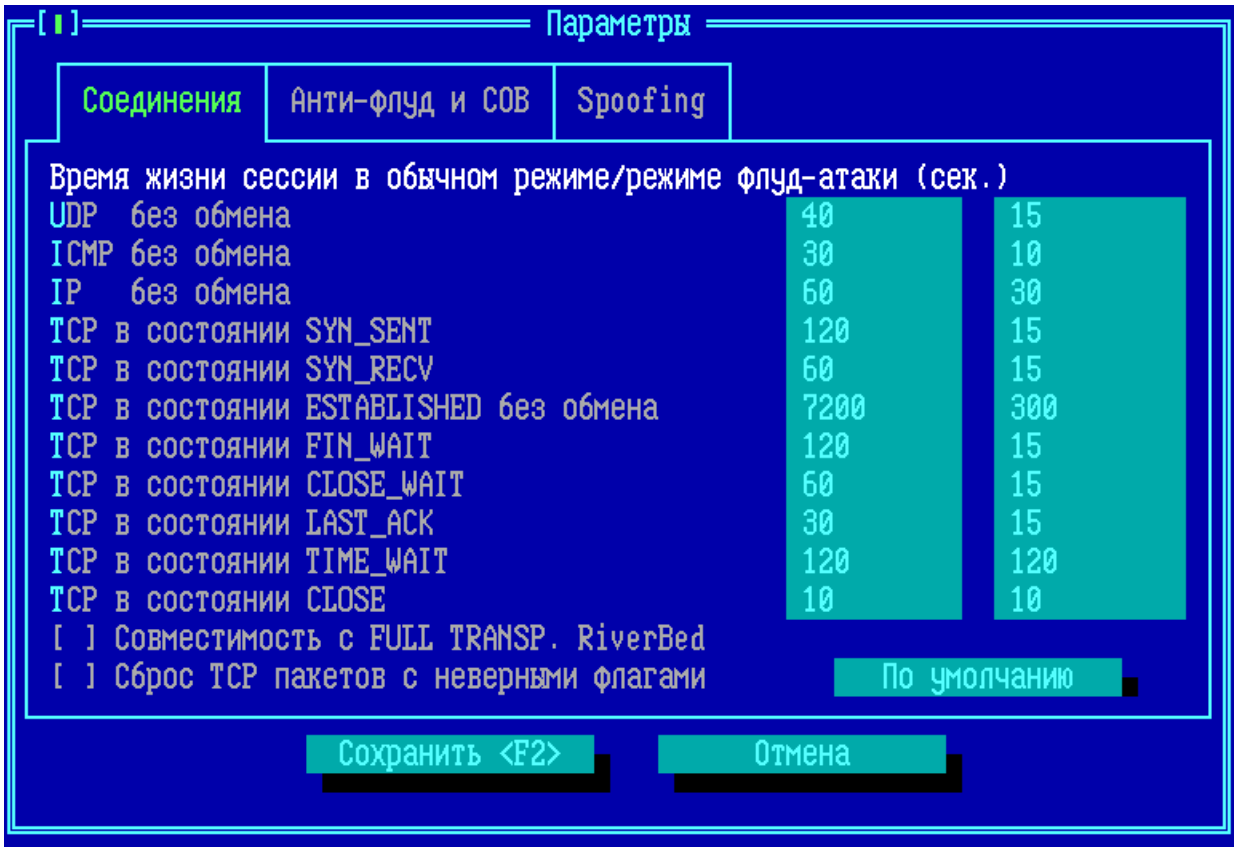


Рисунок 398 - Параметры ограничения соединений

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. 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. 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. По таймауту запись будет удалена из таблицы, и дальнейшее взаимодействие между этой парой абонентов должно будет начаться с повторного установления TCP-соединения. Новые пакеты, не относящиеся

к установлению TCP-соединения, после удаления записи из таблицы будут сброшены. Для каждого состояния TCP-соединения используется одна запись в таблице контроля соединений межсетевого экрана ФПСУ, но таймауты различаются.

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

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

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

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

В режиме защиты от flood-атаки ФПСУ 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.

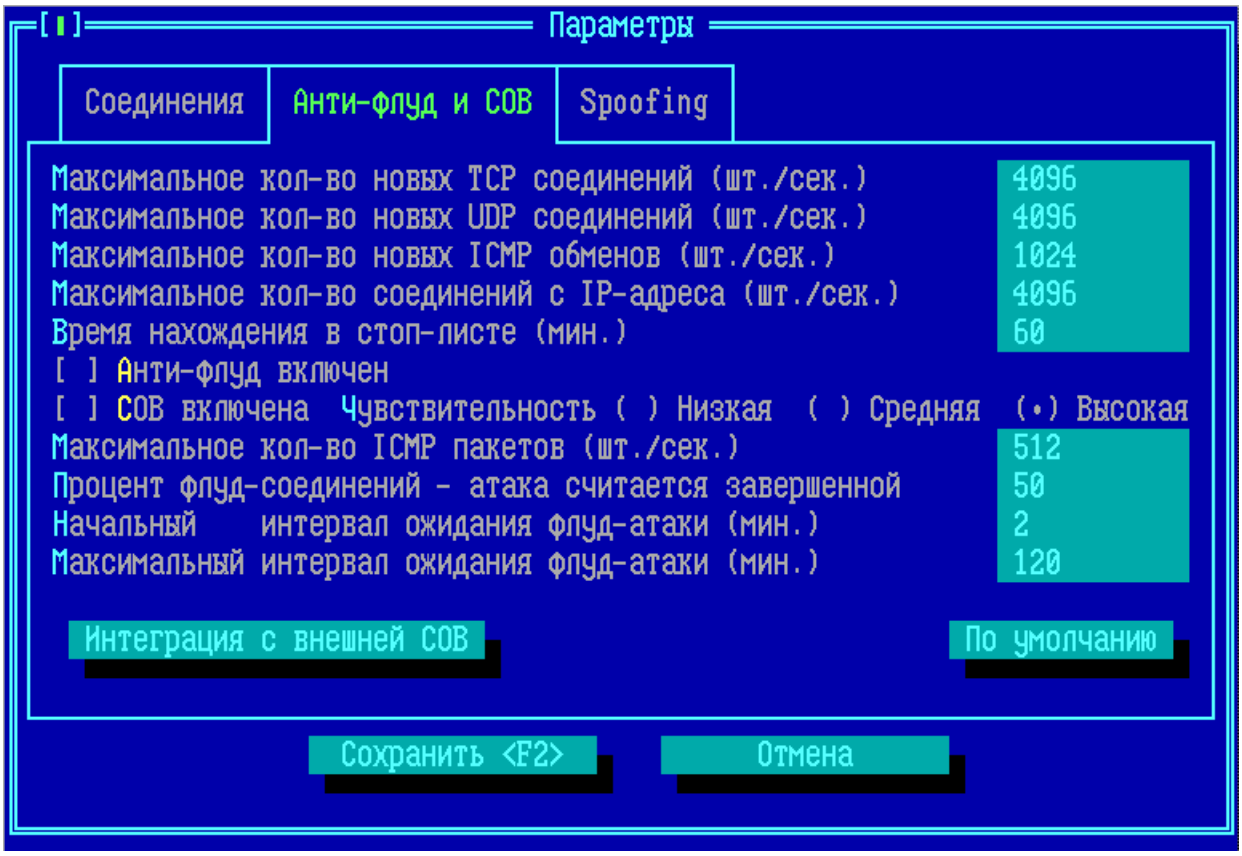


Рисунок 399 - Параметры работы ФПСУ во время flood атаки

ФПСУ 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 начинает считать количество пакетов в секунду, отправленных с IP-адресов абонентов. Если это число превышает параметр ***«Максимальное кол-во соединений с IP-адреса (шт./сек.)»***, то этот IP-адрес заносится в стоп-лист, то есть все исходящие от него пакеты будут блокироваться.

Анти-флуд включен. Если флаг *«Анти-флуд включен»* установлен, то IP-адрес будет находится в стоп-листе время, указанное в поле ***«Время нахождения в стоп-листе (мин.)»***. Если флаг *«Анти-флуд включен»* не установлен, то IP-адрес будет находится в стоп-листе до перезагрузки ФПСУ.

Флаг *«Анти-флуд включен»* влияет на действие/бездействие параметров ***«Максимальное кол-во новых TCP соединений (шт./сек.)»***, ***«Максимальное кол-во новых UDP соединений (шт./сек.)»***, ***«Максимальное кол-во новых ICMP обменов (шт./сек.)»***, ***«Максимальное кол-во соединений с IP-адреса (шт./сек.)»***. Если флаг снят, то ФПСУ будет переходить в режим защиты от flood-атаки только в случаях полной загрузки оперативной памяти и в случае превышения порога ICMP эхо-запросов.

СОВ включена. Опция не применима в данной версии программного обеспечения.

Интеграция с внешней СОВ – команда перехода в интерфейс настройки взаимодействия ФПСУ со сторонними средствами обнаружения вторжений (подробнее см. пункт «Взаимодействие со средствами обнаружения вторжений»).

На момент начала атаки ФПСУ запоминает общее количество всех типов соединений – это значение потребуется для определения времени завершения атаки. Для начала выхода ФПСУ 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 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 переходит в обычный режим работы.

Если общее количество соединений за указанное время превысило пороговое значение, то ФПСУ 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 с TCP-соединениями в режиме spoofing на медленных каналах связи.

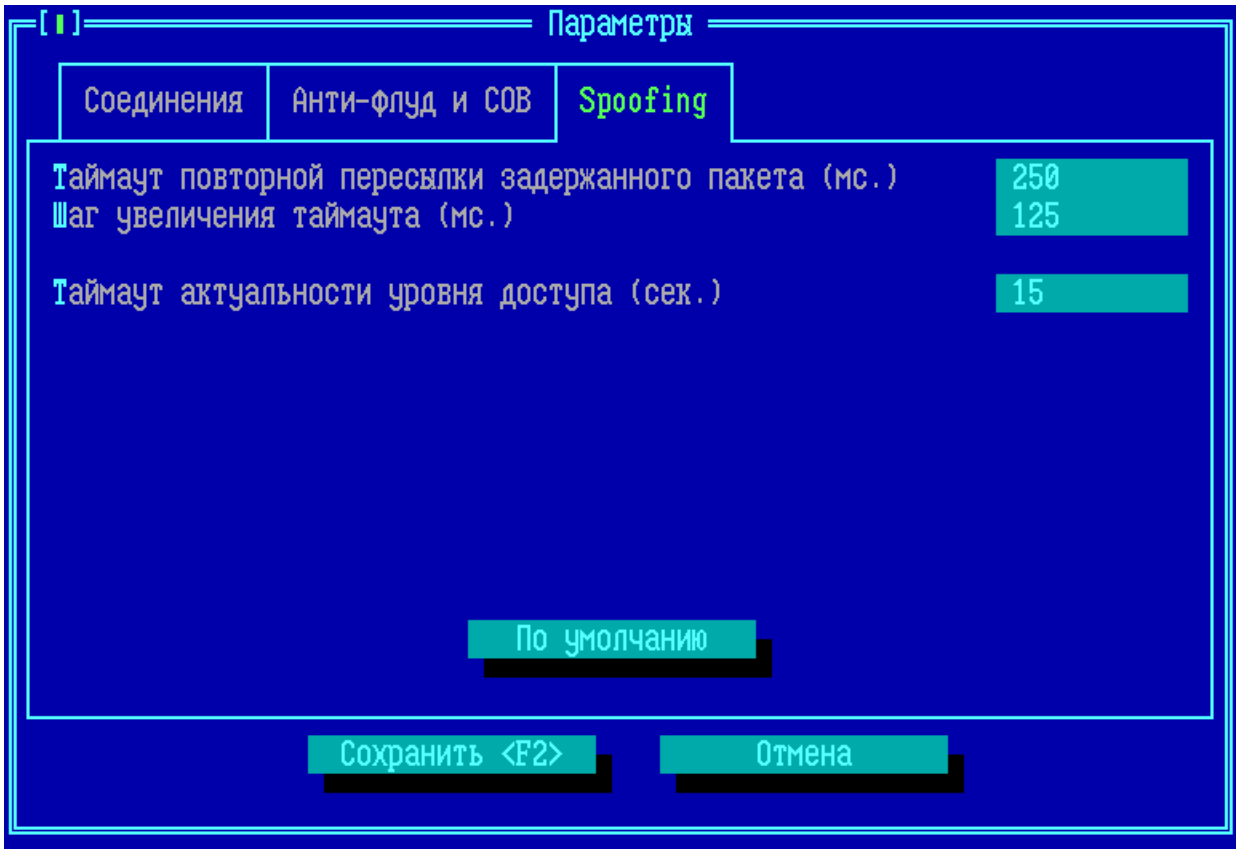


Рисунок 400 - Параметры передачи подтверждений в режиме Spoofing

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 отправляет подтверждение о передаче пакета получателем отправителю самостоятельно, не дожидаясь такого подтверждения от получателя. После этого ФПСУ 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 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.

Таймаут актуальности уровня доступа (сек.) – клиенты получают по протоколу RADIUS от сервера авторизации текущий уровень доступа. Уровень доступа клиента является одним из критериев, по которым МЭ ФПСУ осуществляет фильтрацию трафика. На ФПСУ для группы клиентов в правиле трафика может быть определено условие, по которому клиенты получают доступ в защищенную сеть на основе заданного уровня доступа. Сервер авторизации может присылать ФПСУ уведомления на изменение уровня доступа для конкретного клиента. Таймаут актуальности уровня доступа – это максимальный период времени реакции на смену уровня доступа клиентов при его изменении. Чем меньше таймаут, тем больше требуется ресурсов. Чем больше таймаут, тем больше задержка реакции на изменение доступа клиента.

10. Подсистемы и дополнения ФПСУ

Основные функции ФПСУ могут быть расширены дополнительными возможностями, подключаемыми подсистемами и дополнениями.

Подсистема – встроенный или дополнительно устанавливаемый функционал, расширяющий возможности ФПСУ, для активации требуется лицензия на подсистему.

Дополнение – внешнее дополнительное ПО или базовое ПО, устанавливается отдельно или включено в обновление, добавляет новые возможности, может быть удалено или отключено.

Подсистемы

Установленные и активированные подсистемы ФПСУ отображаются в режиме фильтрации по нажатию на функциональную клавишу *<F1>* и выбору пункта меню «Информация о установленных подсистемах».

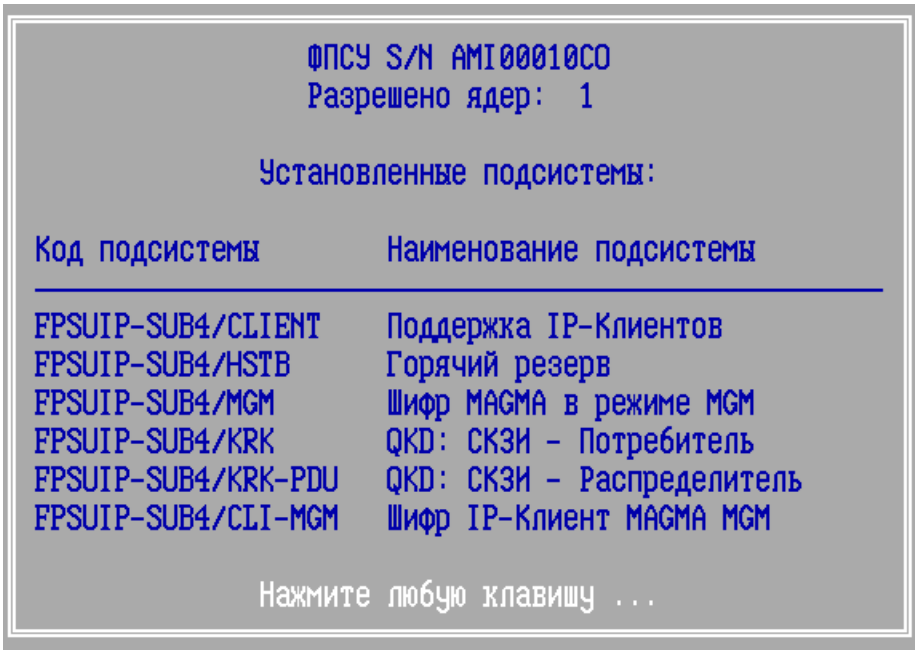


Рисунок 401 - Режим фильтрации. Меню «F1 → Информация об установленных подсистемах»

Могут быть задействованы следующие подсистемы:

CLIENT – подсистема поддержки IP-Клиентов, встраиваемый в ПО ФПСУ сервер доступа и обслуживания «ФПСУ-IP/Клиентов». Подробное описание настройки приведено в разделе «Клиент для ФПСУ».

HSTB – подсистема горячего резерва. Подробное описание настройки приведено в разделе «Параметры «Горячего резерва»».

KRK – подсистема поддержки технологий КРК, ***KRK-PDU*** – подсистема Сервер КЗК. Подсистемы позволяют ФПСУ работать в режимах потребителя квантовых ключей и распределителя квантовых ключей. Подробное описание настройки приведено в разделе «Квантовое распределение ключей».

MGM – подсистема, разрешающая шифрование данных блочным шифром «Магма» в режиме MGM. Для использования необходимо включение опции «Магма-MGM», описание приведено в пункте «Общие параметры конфигурации ФПСУ».

RKL – подсистема удаленной загрузки ключей. Подробное описание настройки приведено в пункте «Настройка диапазона клиентов на работу с RKL».

CLI-MGM – шифр IP-Клиент MAGMA.

CLI-MOB – подсистема активации мобильных ФПСУ-IP/Клиентов (с ограничением на количество одновременных подключений). Для использования необходимо создание логической группы клиентов с типом «VPNPROGRAM», описание приведено в пункте «Описание логической группы клиентов».

Дополнения

Установленные дополнения ФПСУ отображаются в режиме фильтрации по нажатию на функциональную клавишу <*F1*> и выбору пункта меню «Информация об аддонах».



Рисунок 402 - Режим фильтрации. Меню «F1 → Информация об аддонах»

На ФПСУ используются следующие дополнения:

dhcp – предустановленное дополнение позволяет разворачивать DHCP-сервер на

ФПСУ. DHCP-сервер раздает адреса ФПСУ-IP/Клиентам из заданного пула адресов. Подробное описание настройки приведено в пункте «DHCP-сервер и DNS-Relay».

http-proxy – предустановленное дополнение позволяет разворачивать прокси сервер на ФПСУ. Подробное описание настройки приведено в пункте «Http-proxy ФПСУ».

frr – дополнение включает работу протоколов динамической маршрутизации OSPF и BGP, протокола обнаружения двунаправленной переадресации BFD. Описание установки/удаления приведено в пункте «Дополнение frr». Подробное описание настройки приведено в пунктах «Динамическая маршрутизация OSPF», «Динамическая маршрутизация BGP».

rkl – при удаленной загрузке ключевых данных дополнение включает взаимодействие с ЦРМК и Сервером лицензирования. Должна быть установлена подсистема RKL. Подробное описание настройки приведено в пунктах «RKL для обновления ключевых данных клиентов», «Настройка диапазона клиентов на работу с RKL», «Настройка диапазона клиентов на работу с Сервером лицензирования», «Серверы ЦРМК и Сервер лицензирования».

iperf – в дополнение встроена утилита iperf3, позволяет тестировать производительность каналов. Iperf3 – консольная клиент-серверная программа — генератор TCP, UDP и SCTP трафика для тестирования пропускной способности сети.

10. 1. Дополнения

Дополнения на ФПСУ – это дополнительные программные модули, которые задействуют различные функциональные возможности.

Пункт меню конфигурации «Дополнения» отображается, если установлено одно из дополнений для ФПСУ, предназначен для настройки и использования дополнений.

Пункт меню «Дополнения»:

Пункт меню «Управление дополнениями»:

Параметры RKL-клиента – данный пункт меню отображается для установленного дополнения rkl, требуется установленная подсистема RKL, при удаленной загрузке ключевых данных дополнение включает взаимодействие с ЦРМК и Сервером лицензирования. Описание установки/удаления приведено в пункте «Дополнение rkl».

FRR – данный пункт меню отображается для установленного дополнения frr.

Дополнение frr требуется для работы протоколов динамической маршрутизации OSPF и BGP, протокола обнаружения двунаправленной переадресации BFD. Позволяет посмотреть конфигурационные файлы протоколов динамической маршрутизации OSPF и BGP, выдать файлы отладки на внешний носитель. Подробное описание установки/удаления приведено в пункте «Дополнение frr».

Управление Модулем КРК – данный пункт меню отображается для установленного дополнения ami-q. Дополнение ami-q встроено в версию 4.0.2Q, позволяет ФПСУ создавать VPN-туннели с использованием квантовых и/или квантово-защищенных ключей. Открывающееся меню содержит команды просмотра и выдачи отладочных журналов, а также сброса счетчиков при проведении пуско-наладочных работ.

Удаление дополнений – команда удаляет выбранное дополнение.

Управление ключами – команда управления предраспределенными ключами для участников квантовой сети. Подробное описание установки/удаления ключей приведено в пункте «Установка предраспределенных ключей для участников квантовой сети».

10. 1. 1. Дополнение frr

Дополнение frr включает динамическую маршрутизацию на ФПСУ. Подробное описание динамической маршрутизации приведено в разделе «Динамическая маршрутизация».

Для установки дополнения требуются файлы frr_installer_b14.up0, frr_installer_b14.upd. Установка дополнения производится в соответствии с пунктом «Установка дополнений/изменений».

Для удаления дополнения frr выполните команду «Настройка дополнений → Удаление дополнений → frr », после удаления дополнения ФПСУ будет перезагружен.

Проверить установленное дополнение ФПСУ можно в режиме фильтрации, нажав на функциональную клавишу <*F1*> и выбрав пункт «Информация об аддонах».

Наименование модуля	№ сборки	Состояние	Выделение памяти (Mb) мин.	макс.	факт.	потр.
ids	55	используется	580	4096	861	1
dhcp	19	отключен	16	32	0	0
http-proxy	94	отключен	32	512	0	0
frr	18	отключен	160	300	0	0
ИТОГО:			788	4940	861	1

Нажмите любую клавишу ...

Рисунок 403 - Режим фильтрации. Меню «F1 → Информация об аддонах»

В режиме конфигурации меню frr открывается из пункта меню «Настройка дополнений → configure frr».



Рисунок 404 - Меню «Настройка дополнений»

Меню конфигурационных файлов дополнения frr, содержит следующие команды:

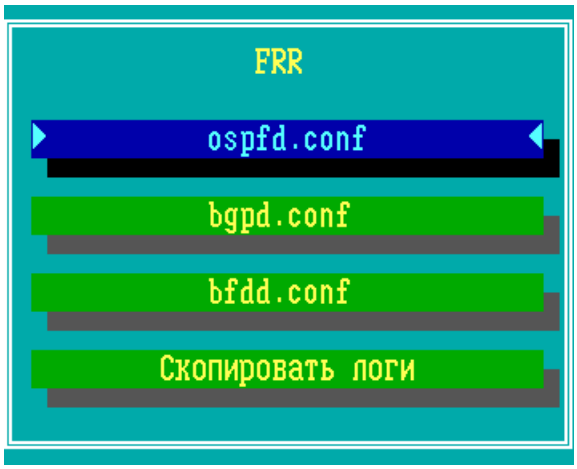


Рисунок 405 - Меню «Configure frr»

ospfd.conf – файл конфигурации протокола OSPF.

bgpd.conf – файл конфигурации протокола BGP.

bfdd.conf – файл конфигурации для быстрого обнаружения неисправностей сети.

Файлы конфигураций .conf открываются в текстовом редакторе, несмотря на то, что файлы могут быть отредактированы, внесенные изменения сбрасываются при запуске ФПСУ и в файл записывается новая конфигурация.

Скопировать логи – команда выдачи файла отладки OSPF на внешний носитель. Перед запуском команды необходимо к ФПСУ подключить USB-носитель. На внешнем носителе будет создан каталог frr.log с файлом лога OSPF.

10. 1. 2. Дополнение rkl

Дополнение rkl включает взаимодействие с ЦРМК и Сервером лицензирования на ФПСУ при удаленной загрузке ключевых данных. Подробное описание взаимодействий приведено в пунктах «RKL для обновления ключевых данных клиентов», «Настройка диапазона клиентов на работу с RKL», «Настройка диапазона клиентов на работу с Сервером лицензирования», «Серверы ЦРМК и Сервер лицензирования».

Для установки дополнения требуются файлы rkl_installer_b50.up0, rkl_installer_b50.upd. Установка дополнения производится в соответствии с пунктом «Установка дополнений/изменений».

Для удаления дополнения rkl выполните команду «Настройка дополнений → Удаление дополнений → RKL», после удаления дополнения ФПСУ будет перезагружен.

В режиме фильтрации, по нажатию на функциональную клавишу *<F1>* и выбору пункта «Информация об аддонах» отображается установленное дополнение rkl со статусом «используется».



Рисунок 406 - Режим фильтрации. Меню «F1 → Информация об аддонах»

В режиме конфигурации меню rkl открывается из пункта меню «Настройка дополнений → Параметры RKL-клиента».



Рисунок 407 - Меню «Настройка дополнений»

Меню дополнения rkl, содержит следующие команды:

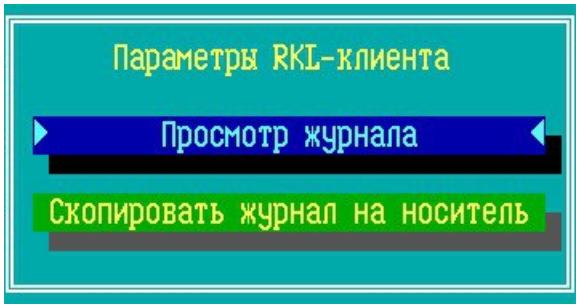


Рисунок 408 - Меню «Параметры RKL-клиента» ***Просмотр журнала*** – записи журнала rkl.log выдаются на экран с указанием события и времени регистрации.

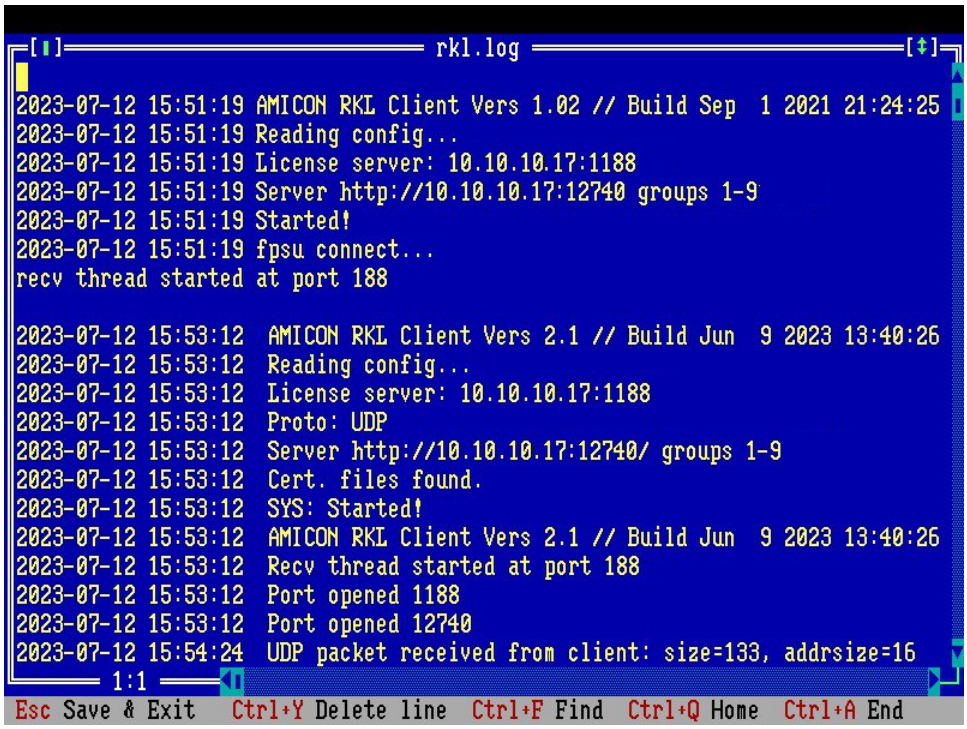


Рисунок 409 - Журнал rkl.log

Скопировать журнал на носитель – на внешний носитель выдается файл лога RKL-клиента. Перед выполнением команды необходимо подключить USB-носитель, на который будет выдан файл, к ФПСУ и запустить команду.

11. Квантовое распределение ключей

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

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

Для работы с устройствами квантового распределения ключей на ФПСУ должен быть установлен дополнительный программный модуль «Модуль-агент поддержки взаимодействия с устройствами КРК шифрования в качестве сервера промежуточного доверенного узла (ПДУ)», код продукта FPSUIP-SUB3-KRK-PDU.

Начиная с 4-й версии, ФПСУ поддерживает работу с устройствами СВКРК. Для работы с СВКРК на ФПСУ должны быть предварительно установлено дополнение «option_krk_pdu». Главное меню ФПСУ, подготовленного для работы с устройствами СВКРК, содержит надписи «Комплекс "ФПСУ Q" версии 4», «СКЗИ "ФПСУ-IP Amigo"», «вариант исполнения "ФПСУ-IP Q"» и «модификация 4.0.2Q».

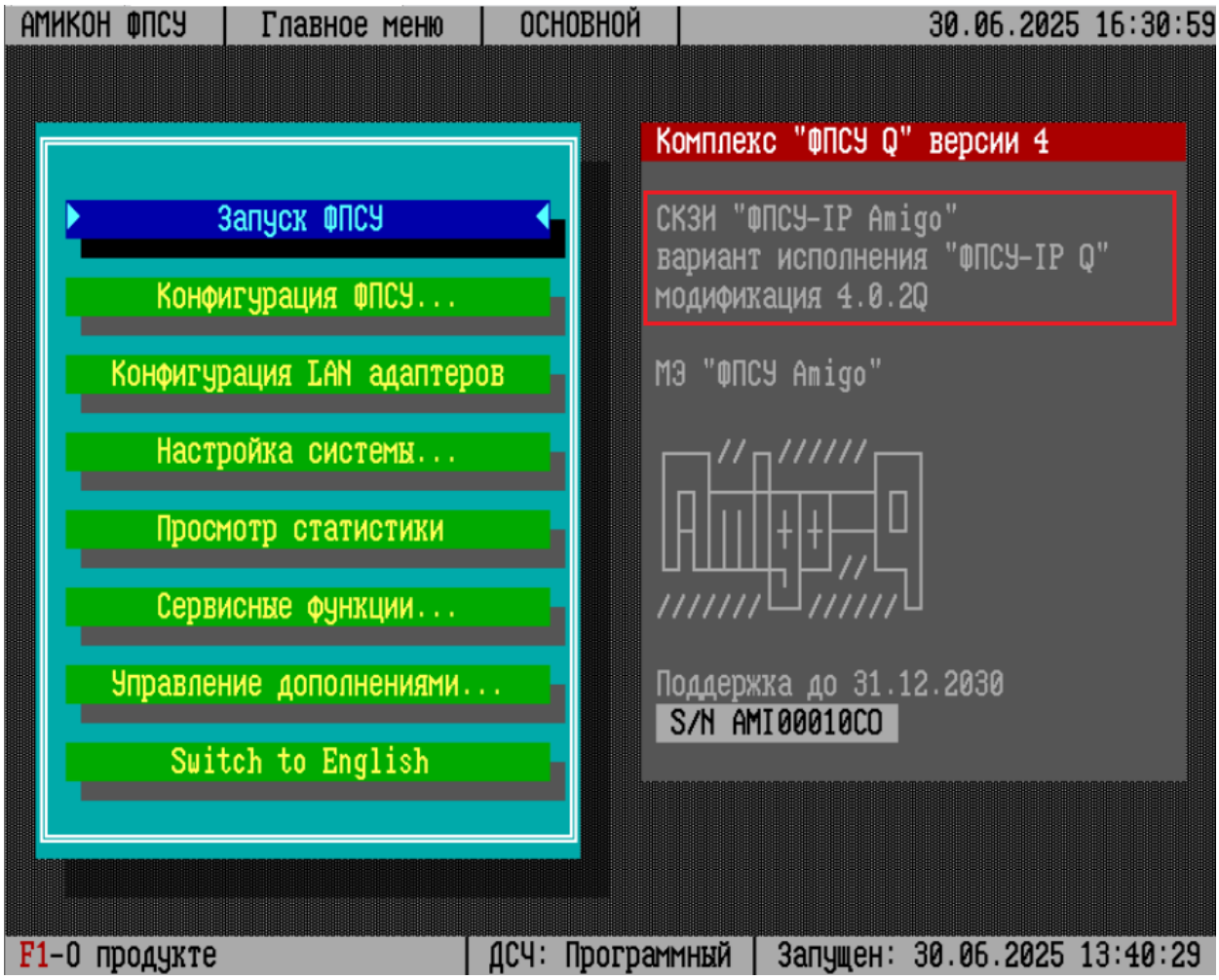


Рисунок 410 - Главное меню ФПСУ с поддержкой СВКРК

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

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

Принятая в данном разделе дополнительная терминология:

ФПСУ-IP ULT 10G – программно-аппаратный комплекс ФПСУ на основе аппаратной платформы семейства ULT, обеспечивающий скорость шифрования не менее 10 Гбит/сек.;

ФПСУ-IP 150M – программно-аппаратный комплекс ФПСУ на основе аппаратной платформы FPSUIP-STD3, обеспечивающий скорость шифрования не менее 150 Мбит/сек.;

СВКРК-А – устройство квантовой криптографической системы выработки и распределения ключей разработки ООО «СМАРТС-Кванттелеком», модуль-отправитель

фотонов (подробнее см. https://quanttelecom.ru);

СВКРК-Б – устройство квантовой криптографической системы выработки и распределения ключей разработки ООО «СМАРТС-Кванттелеком», модуль-получатель фотонов;

СВКРК – обобщенное обозначение модулей СВКРК-А и СВКРК-Б;

Квантовый ключ – секретный ключ, выработанный парой СВКРК в результате выполнения квантового криптографического протокола выработки и распределения ключей;

Квантовый туннель – защищенное имитовставкой и шифрованием виртуальное соединение (туннель), организованное между ФПСУ с использованием полученных от соседних устройств СВКРК квантовых ключей или с использованием полученных от промежуточного узла квантово-защищенных ключей;

Квантовая сеть – сеть передачи данных, состоящая из связанных квантовыми туннелями узлов;

Квантово-защищенный ключ (КЗК, КЗК-ключ) – это секретный ключ, используемый для построения квантового туннеля между несмежными ФПСУ квантовой сети, переданный на них при помощи каналов связи, защищенных квантовыми ключами (переданный через квантовые туннели);

ККС ВРК – квантовая криптографическая система выработки и распределения ключа;

Служебный туннель – криптографически защищенное соединение (туннель) между двумя смежными в рамках квантовой сети ФПСУ, в рамках которого осуществляется обмен служебными данными между соседними устройствами СВКРК в процессе выработки квантовых ключей. Служебные данные используются для синхронизации случайных последовательностей между соседними устройствами СВКРК.

Квантово-сервисный туннель – защищенное имитовставкой и шифрованием виртуальное соединение (туннель), организованное между ФПСУ с использованием полученных от соседних устройств СВКРК квантовых ключей. Квантово-сервисный туннель предназначен для передачи квантово-защищённых ключей (КЗК) между смежными ФПСУ в рамках квантовой сети;

Комбинированный туннель – криптографически защищенное соединение (туннель) между двумя ФПСУ, которому разрешено шифровать передаваемую информацию как на основе квантовых ключей (в случае их наличия), так и на основе полученных от ЦВК ключей. Квантовые ключи считаются более приоритетными, как только на ФПСУ

появляются квантовые ключи, шифрование в комбинированном туннеле переходит на них;

Администратор безопасности квантовой сети – лицо, ответственное за согласованность участвующих в построении квантовой сети конфигураций ФПСУ.

11. 1. Общая схема построения квантовой сети

Общая структура квантовой сети предполагает существование опорных узлов, между которыми строится квантовый туннель для передачи защищенного на квантовых или КЗК-ключах пользовательского трафика, и промежуточных узлов, необходимых для выработки квантового ключа. Расстояние между опорными узлами может быть любым. Расстояние между соседними промежуточными узлами ограничено физическими возможностями оптического канала выработки квантовых ключей и возможностей устройств СВКРК, составляет от 50 до 100 км (приблизительные данные, точные данные следует смотреть в руководствах эксплуатации СВКРК).

Порядок установления квантового туннеля между опорными узлами следующий:

- между всеми промежуточными узлами устанавливаются служебные туннели;
- каждая пара промежуточных узлов должна получить от устройств СВКРК квантовые ключи для организации квантово-сервисных туннелей между соседними узлами;
- между всеми промежуточными узлами устанавливаются квантово-сервисные туннели;
- опорные узлы через квантово-сервисные туннели получит КЗК-ключ для установления соединения с другим опорным узлом;
- опорные узлы строят квантовый туннель, защищенный полученным КЗК-ключом.

Пример линейной квантовой сети, состоящей из двух опорных узлов и произвольного количества промежуточных узлов, представлен на рисунке ниже:

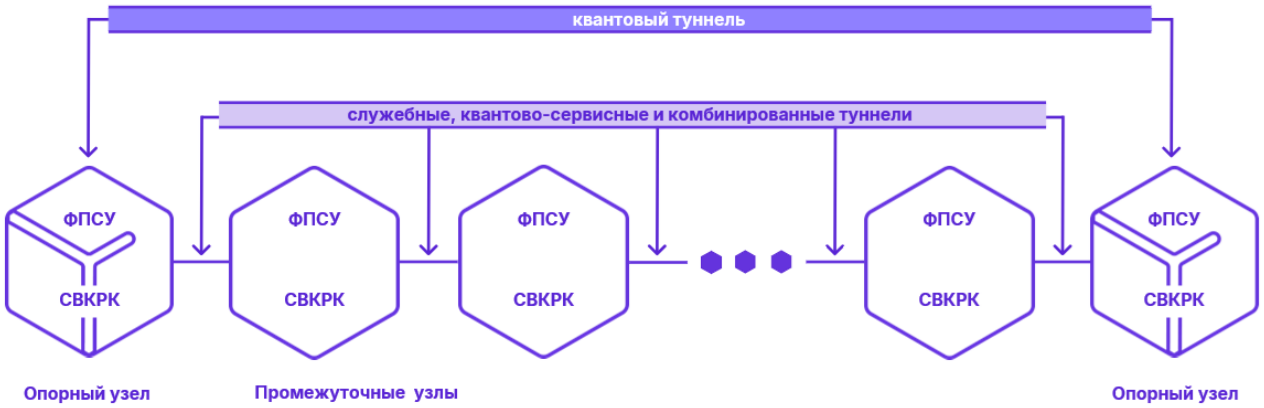


Рисунок 411 - Общая схема линейной квантовой сети

Краткое описание схемы туннелей между двумя ФПСУ в квантовой сети

Общая логическая схема соединения каждых двух промежуточных узлов или промежуточного и опорного узла предусматривает настройку от двух до четырех туннелей на интерфейсах ФПСУ. Туннели для соединения с соседним узлом могут быть организованы в рамках одного сетевого интерфейса промежуточного узла, в таких случаях для каждого туннеля на интерфейсе ФПСУ создается VLAN. Каждый VLAN предназначен для своего туннеля: служебного, комбинированного, квантово-сервисного и квантового.

Между опорными узлами линейной квантовой сети настраивается и используется только квантовый туннель.

Для промежуточных узлов обязательными для соединения друг с другом являются только два, служебный и квантово-сервисный туннель.

Если между промежуточными узлами передается и пользовательский трафик, к обязательным добавляется и квантовый туннель между ними.

Трафик управления ФПСУ (соединения с АРМ УА, Syslog и SNMP-серверами) можно передавать через служебный туннель, но рекомендуется под него выделить комбинированный туннель. Рекомендуется при возможности комбинированный туннель с трафиком управления подключать к специально выделенному RJ45 сетевому интерфейсу ФПСУ, физически разделяя каналы, по которым передается трафик управления и служебный/квантово-сервисный трафик.

Возможен вариант с разделением всех туннелей по отдельным интерфейсам ФПСУ, чтобы избежать возможного исчерпания полосы пропускания интерфейса и перерывов связи.

Количество подключаемых к ФПСУ устройств СВКРК зависит от схемы сети и расположения настраиваемого ФПСУ в ней. К промежуточному узлу линейной квантовой сети подключается два устройства СВКРК, каждое для связи с соседним узлом в своём направлении (предыдущий промежуточный узел и следующий промежуточный узел). Если ФПСУ является опорным узлом и при этом конечной точкой линейной квантовой сети, то достаточно одного устройства СВКРК, подключаемого к выделенному интерфейсу RJ45 ФПСУ.

Ниже приведена общая принципиальная схема туннелей для квантовой сети, состоящей из двух узлов.

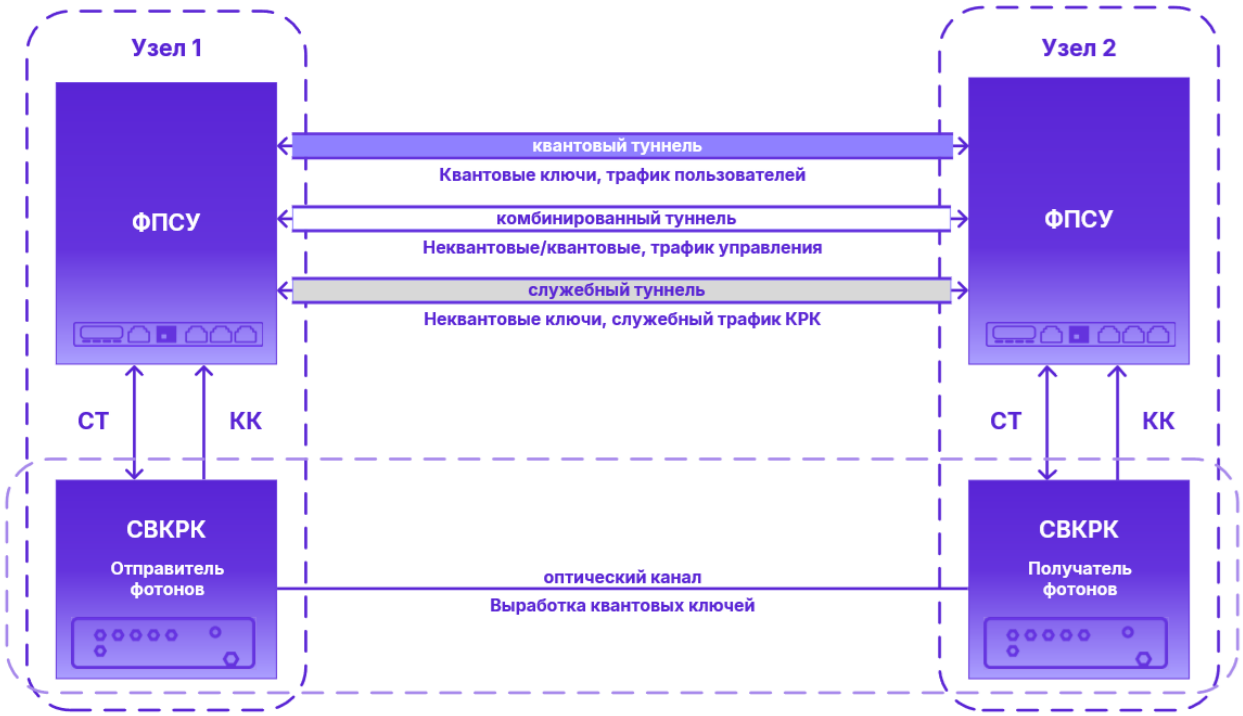


Рисунок 412 - Общая схема туннелей узлов квантовой сети

Обозначения на схеме:

КК – квантовый ключ, выработанный парой СВКРК и передаваемый от СВКРК к ФПСУ;

СТ – служебный трафик между СВКРК, защищаемый средствами ФПСУ при передаче на соседний узел квантовой сети в служебном туннеле.

Для сети, состоящей из двух узлов, обязательными туннелями являются два: квантовый и служебный.

Наличие комбинированного туннеля в таком случае опционально, так же как и в случае линейной квантовой сети. Квантово-сервисный в схеме из двух узлов не применяется.

11. 2. Установка дополнений для работы с СВКРК

В разделе содержатся сведения об установке обновлений ПО ФПСУ, необходимых для работы с устройствами квантового распределения ключей.

Для выполнения задачи требуется установить два дополнения программного обеспечения ФПСУ, обеспечивающих взаимодействие с устройствами квантового распределения ключей (далее – обновления).

Для установки обновлений ФПСУ, администратору потребуются следующие устройства и файлы:

- ФПСУ;
- USB-flash накопитель с поддержкой передачи данных в соответствии со стандартом USB 2.0;
- TM-идентификатор Администратора или Главного Администратора данного ФПСУ (в форм-факторе устройства iButton или USB TM-Key);
- полученные от поставщика программного обеспечения ФПСУ и записанные на USB-flash накопитель файлы обновлений:
  1. option_krk_pdu.up0;
  2. option_krk_pdu.upd.

Файлы «option_krk_pdu.up0» и «option_krk_pdu.upd» являются файлами дополнения, обеспечивающего поддержку опций FPSU-KRK и FPSU-KRK-PDU. Установка данного обновления приведена в пункте Установка дополнения option_krk_pdu.

11. 2. 1. Установка дополнения option_krk_pdu

Дополнение «option_krk_pdu» может быть установлено только на ФПСУ 4-й версии. Файлы дополнения: «option_krk_pdu.up0» и «option_krk_pdu.upd».

Дополнение позволяет ФПСУ работать в режимах потребителя квантовых ключей и распределителя квантовых ключей.

Рекомендуемый порядок установки дополнения:

1. Выполните стандартную процедуру установки обновления до появления таблицы со списком файлов с обновлениями (см. пункт Установка дополнений/изменений);

2. Выберите из списка найденных дополнений и обновлений запись «option_krk_pdu.upd» и подтвердите его установку командой «Установить»:

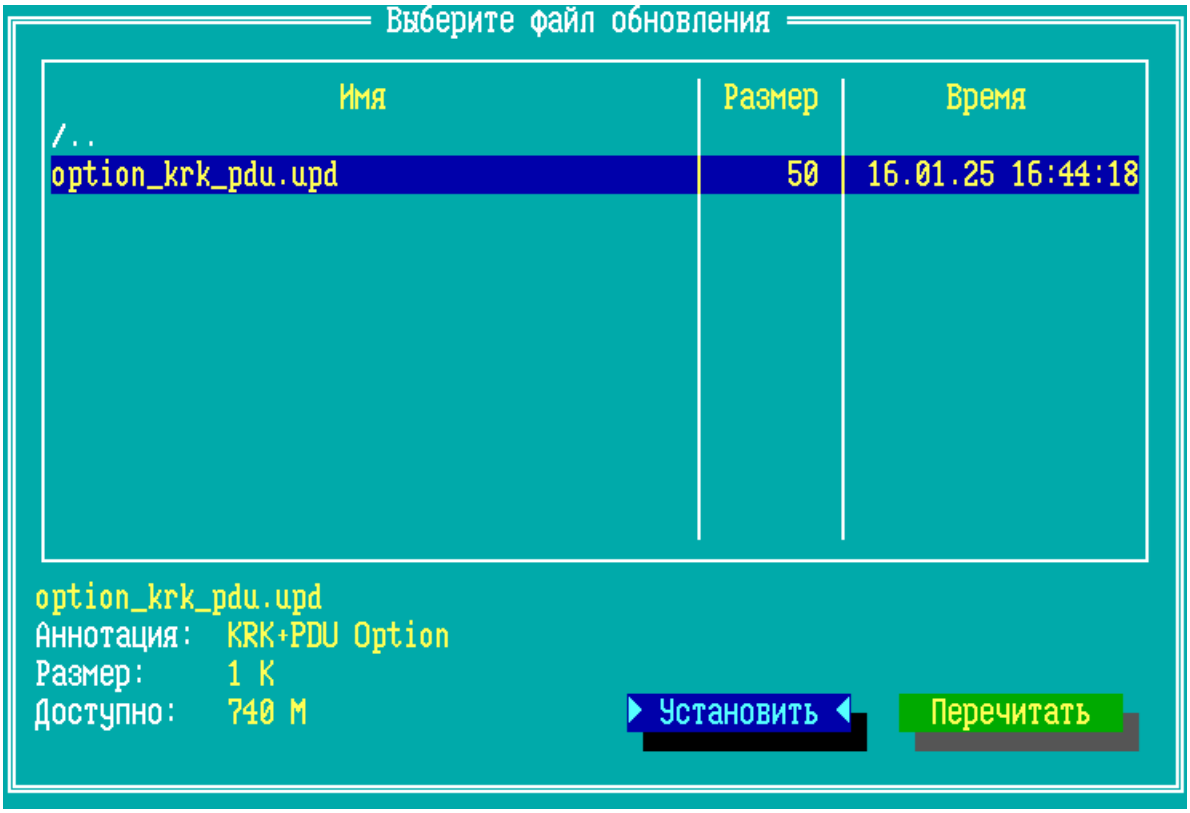


Рисунок 413 - Выбор дополнения

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

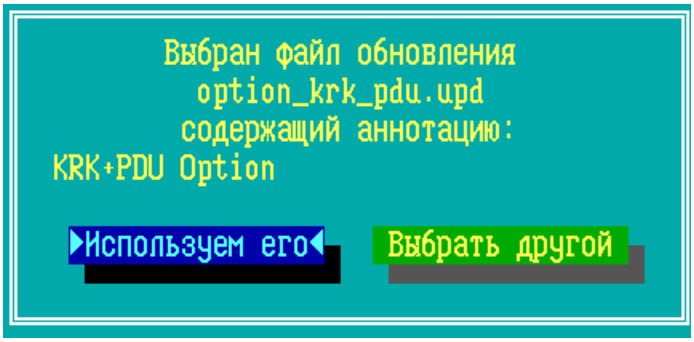


Рисунок 414 - Выбран файл с дополнением

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

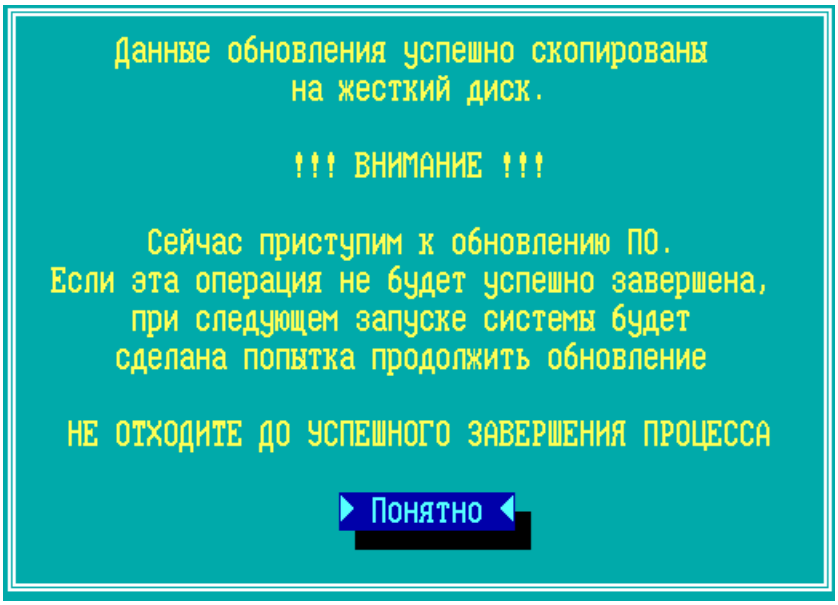


Рисунок 415 - Файлы дополнения скопированы

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

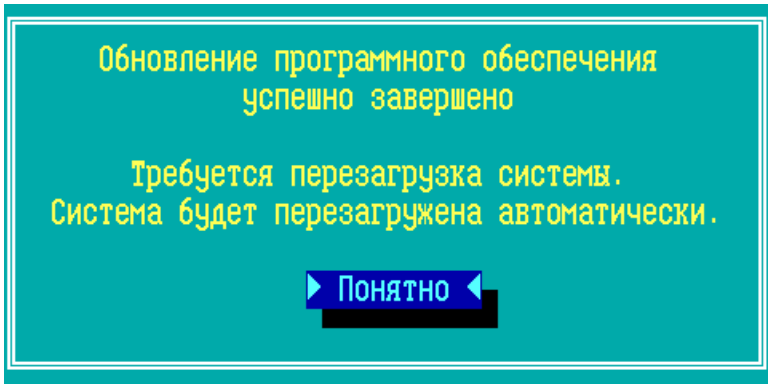


Рисунок 416 - Обновление установлено, требуется перезагрузка

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

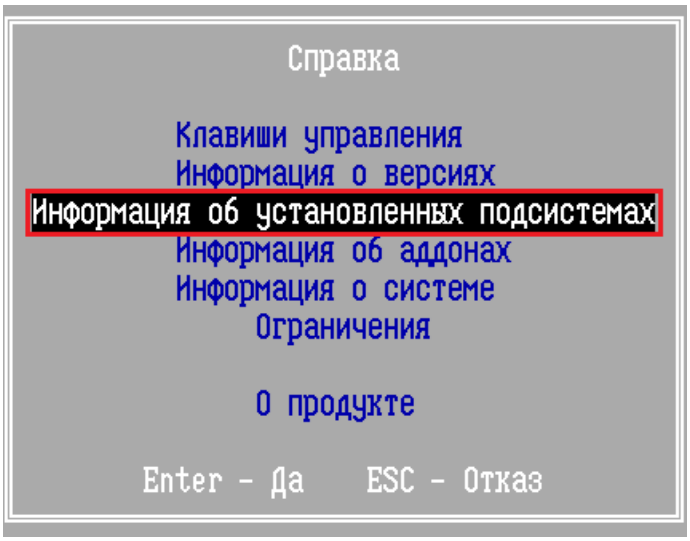


Рисунок 417 - Меню справки

Дополнение «option_krk_pdu» считается установленным успешно, если в окне информации будут присутствовать строки установленных опций «Поддержка технологии КРК» и «Сервер КЗК»:

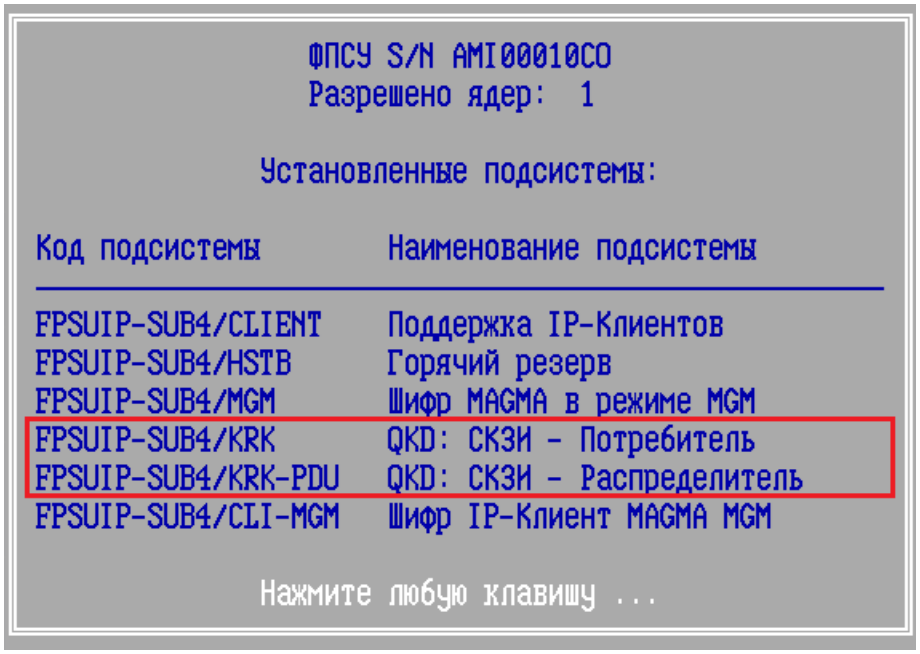


Рисунок 418 - Дополнение «option_krk_pdu» установлено

Процедура установки дополнения «option_krk_pdu» завершена.

11. 3. Взаимодействие СВКРК и ФПСУ

Устройство СВКРК подключается к ФПСУ напрямую Ethernet кабелем через специально выделенный разъем RJ45. Если к ФПСУ требуется подключить более одного СВКРК, то для каждого СВКРК требуется выделить отдельный сетевой адаптер на ФПСУ.

Не допускается подключение СВКРК к ФПСУ через стороннее сетевое оборудование.

Взаимодействие между СВКРК и ФПСУ начинается после включения питания на обоих устройствах, причём ФПСУ должен быть переведен в режим фильтрации пакетов.

На порту ФПСУ, к которому подключен СВКРК, требуется выполнить настройки, указанные в пункте Настройка СВКРК на сетевых адаптерах ФПСУ с учетом сетевых параметров подключенного к ФПСУ СВКРК. Стандартные сетевые параметры СВКРК указаны ниже .

11. 3. 1. Стандартные сетевые параметры СВКРК

Модули СВКРК как сетевые устройства обычно имеют предустановленные сетевые адреса, указанные в таблице ниже:

Таблица. Стандартные сетевые адреса СВКРК

Модуль СВКРК	Стандартный MAC-адрес	Стандартный IP-адрес
СВКРК-А Тип 1	FA:CE:AA:CC:EE:AA	192.168.0.210
СВКРК-Б Тип 1	FA:CE:B0:BB:0B:BB	192.168.0.220

В узлах, где пересекаются 3 и более сегмента квантовой сети, должны использоваться КРК с нестандартными адресами, иначе в пределах одного узла будут функционировать несколько устройств с идентичными MAC- и IP-адресами, что приведет к проблемам в функционировании сети:

Таблица. Возможные нестандартные сетевые адреса СВКРК

Модуль и тип СВКРК	MAC-адрес	IP-адрес
СВКРК-А Тип 1	FA:CE:AA:CC:EE:AA	192.168.0.210
СВКРК-Б Тип 1	FA:CE:B0:BB:0B:BB	192.168.0.220
СВКРК-А Тип 3	FA:CE:AA:CC:EE:14	192.168.0.140
СВКРК-Б Тип 3	FA:CE:B0:BB:0B:15	192.168.0.150
СВКРК-А Тип 4	FA:CE:AA:CC:EE:17	192.168.0.170
СВКРК-Б Тип 4	FA:CE:B0:BB:0B:18	192.168.0.180

11. 3. 2. Настройка СВКРК на сетевых адаптерах ФПСУ

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

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

Таблица соответствия MAC-адресов для настройки на ФПСУ указана ниже:
Таблица. MAC-адреса СВКРК и ФПСУ

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

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

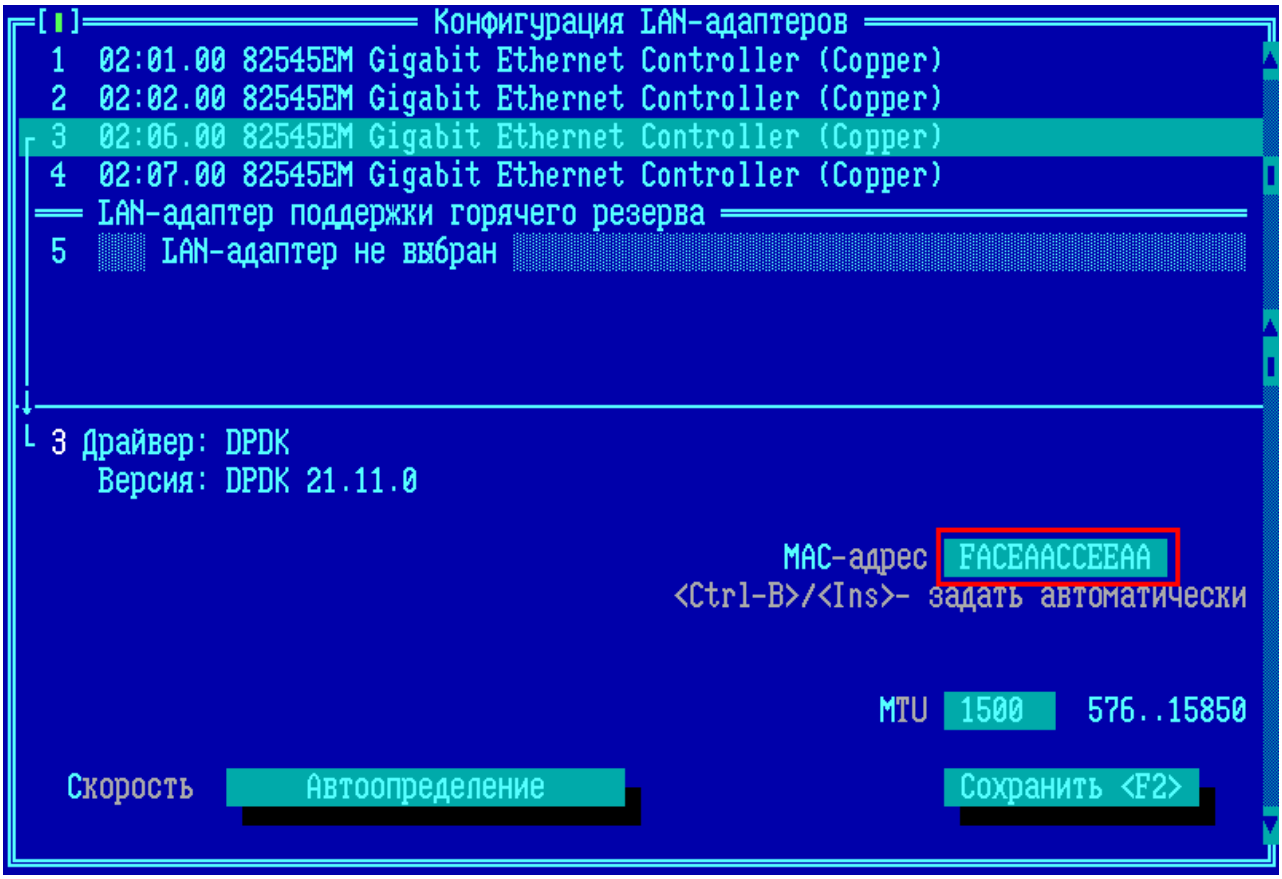


Рисунок 419 - MAC адрес сетевого адаптера, к которому подключен СВКРК-Б

Следующим шагом требуется назначить порту ФПСУ, к которому подключен локальный СВКРК, специальный IP-адрес.

Порт ФПСУ должен получить IP-адрес, производный от адреса соседнего СВКРК - четвертый октет адреса соседнего КРК, увеличенный на единицу.

Таблица соответствия IP-адресов для настройки на ФПСУ указана ниже:
Таблица. IP-адреса СВКРК и ФПСУ

Подключенный к ФПСУ модуль	**Стандартный IP-адрес СВКРК**	**IP-адрес порта ФПСУ**
СВКРК-А	192.168.0.210	192.168.0.221
СВКРК-Б	192.168.0.220	192.168.0.211

Например, если к порту ФПСУ локально подключен СВКРК-Б с адресом 192.168.0.210, взаимодействующий с соседним СВКРК-А с адресом 192.168.0.220, то IP-адрес порта ФПСУ должен быть установлен равным IP-адресу соседнего СВКРК А, увеличенным на единицу:«**192.168.000.221**»:



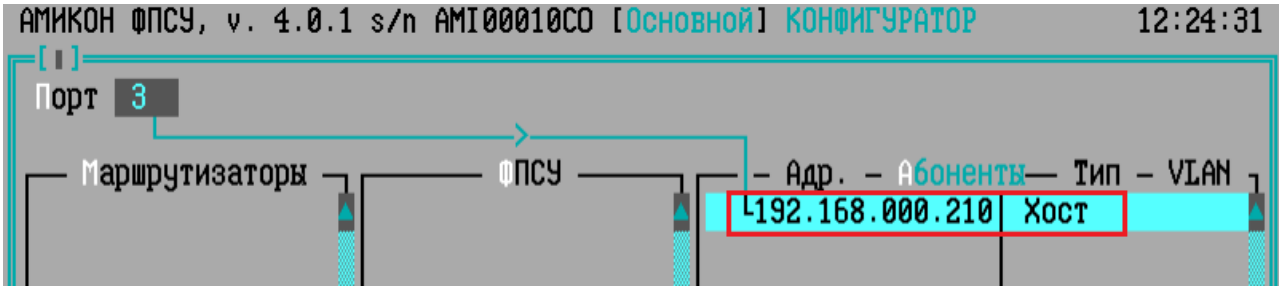


Рисунок 420 - IP-адрес порта ФПСУ и КРК в списке абонентов

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

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

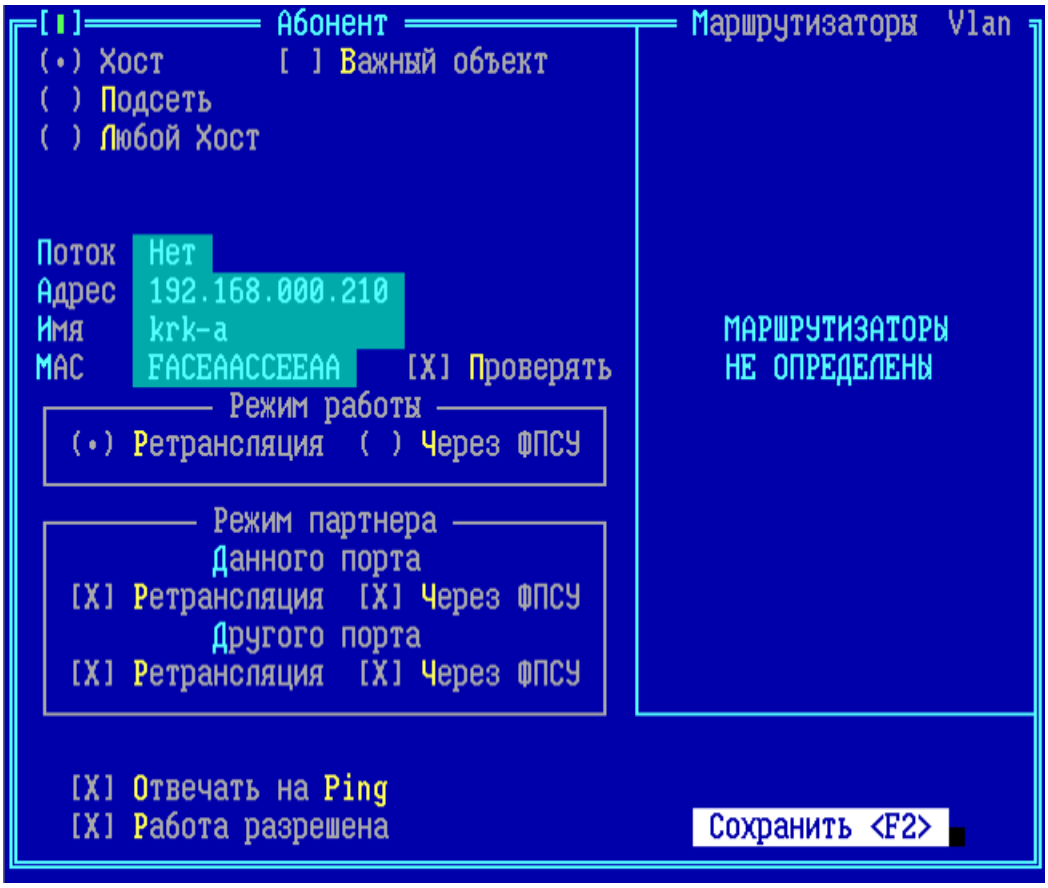


Рисунок 421 - Запись абонента для подключенного СВКРК

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

11. 4. Настройка квантовых туннелей

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

11. 4. 1. Настройка квантового распределения ключей на ФПСУ

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

Настройка доступна только при установленном дополнительном программном модуле «Модуль-агент поддержки взаимодействия с устройствами КРК шифрования в качестве сервера промежуточного доверенного узла (ПДУ)», код продукта FPSUIP-SUB3-KRK-PDU.

Доступ к настройке предоставляется из меню конфигурации по команде «Квантовое распределение ключей → Локальные настройки»:

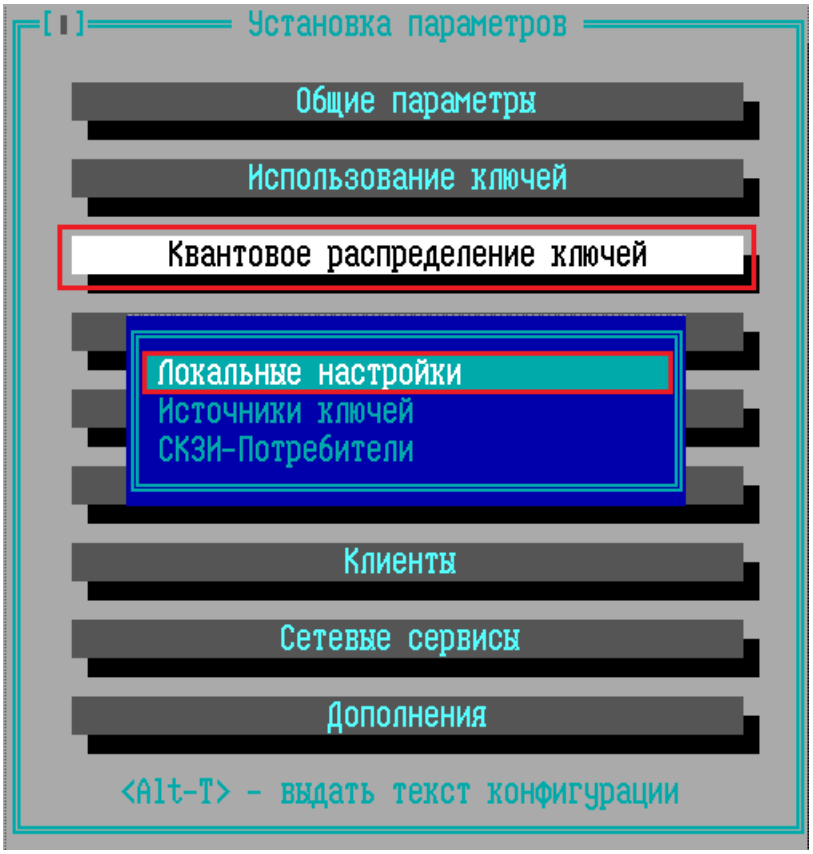


Рисунок 422 - Меню конфигурации ФПСУ - КРК

Для настройки квантового распределения ключей на ФПСУ устанавливаются локальные настройки СКЗИ-Распределителя, определяются источники ключей, задаются СКЗИ-Потребителей.

ФПСУ может являться как промежуточным доверенным узлом, обеспечивающим защищенную передачу данных между сегментами квантовой сети, так и опорным промежуточным доверенным узлом, обеспечивающим защищенную передачу данных между магистральной квантовой сетью и подключенными абонентами. При указании СКЗИ-Потребителей ФПСУ становится опорным промежуточным узлом.

ФПСУ, работая в режиме СКЗИ-Распределителя, накапливает ключи, полученные от ККС ВРК, либо от другого СКЗИ-Распределителя. Впоследствии ФПСУ эти ключи предоставляет СКЗИ-Потребителям (абонентам).

ФПСУ может выступать в режиме СКЗИ-Потребителя, в этом случае задается только источник ключей с типом СКЗИ-Распределителя.

В окне «Локальные настройки» находятся параметры ФПСУ, которые требуется установить администратору исходя из схемы квантовой сети. Локальные настройки устанавливаются, когда ФПСУ задействуется в качестве СКЗИ-Распределителя, в данном случае он будет являться сервером распределения ключей. Настройки по умолчанию не задействованы в большинстве параметров:

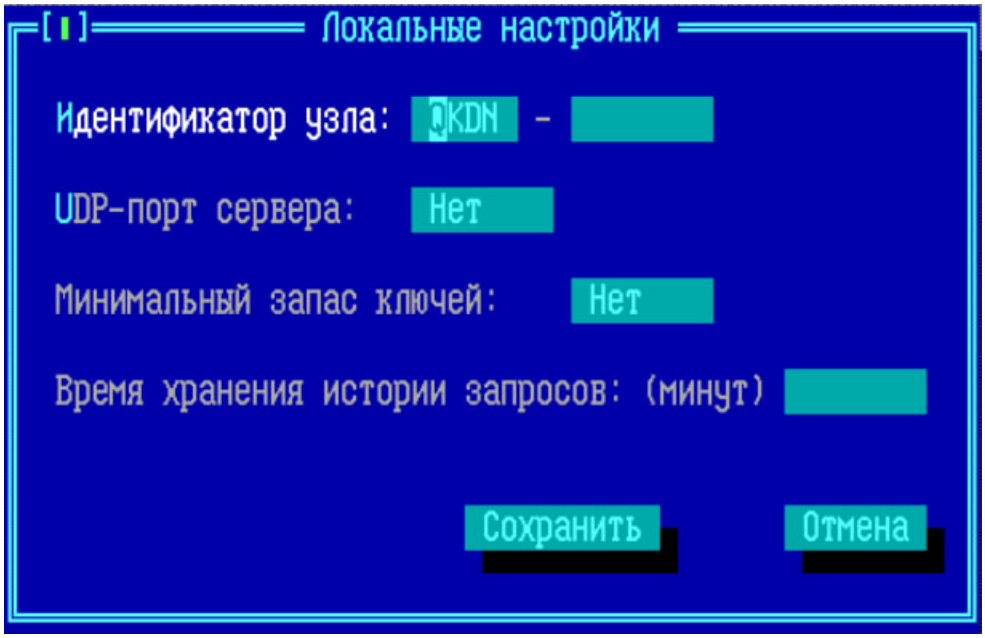


Рисунок 423 - Локальные настройки

В окне требуется установить следующие параметры:

Идентификатор узла – состоит из двух частей - идентификатора сети с названием квантовой сети и номера узла, присваиваемых данному ФПСУ.

Внутри одного идентификатора сети объединяются узлы с общим технологическим устройством, правилами подключения и тарификации. Это могут быть узлы внутри сегмента сети или всей сети одного оператора.

Идентификатор сети содержит четыре латинских символа, первые два символа - латинские буквы, последние два символа - латинские буквы или цифры. Параметр по умолчанию выставлен в значение «QKDN», изменять не требуется. Идентификатор сети

назначается администратором квантовой сети. Необходимость изменения Имени сети устанавливается администратором безопасности квантовой сети.

Номер узла – уникальный в пределах указанной сети номер, присваиваемый данному ФПСУ, число от 1 до 64999. Номер согласуется с администратором безопасности квантовой сети и не должен быть произвольным.

Например: Идентификатор узла MKS1-15, где название сети MKS1, номер узла 15.

UDP-порт сервера – указывается номер порта данного ФПСУ для подключения СКЗИ-Потребителей по протоколу ProtoQa. Значение «Нет» означает, что используется значение по умолчанию, UDP-порт 11577. Значение порта может быть изменено, интервал значений от 1 до 65535.

Минимальный запас ключей – настраивается администратором сети, исходя из количества подключенных на данном узле абонентов. Если количество ключей в накопителе ниже указанного, ФПСУ будет запрашивать дополнительный объём ключей у соседних узлов.

Время хранения истории запросов – настраивается для протокола ProtoQa, по умолчанию 1 сутки. Время хранения истории запросов это настраиваемый период, в течении которого накладывается требование на уникальность идентификаторов ключей.

Источники ключей можно задать из меню конфигурации по команде «Квантовое распределение ключей → Источники ключей»:

В окне «Источники ключей» задаются соседние узлы в топологии сети, которые будут являться источниками квантовых ключей для данного ФПСУ. Предопределены типы источников ключей - ККС ВРК, СКЗИ-Распределитель и стыковочный узел. Соседними узлами могут быть устройства ККС ВРК, описываются на вкладке «ККС ВРК», соседние узлы с типом СКЗИ-Распределитель и стыковочный узел описываются на вкладке «Прочие».

На вкладке «ККС ВРК» по кнопке «Добавить» открывается окно «Регистрация источника»:

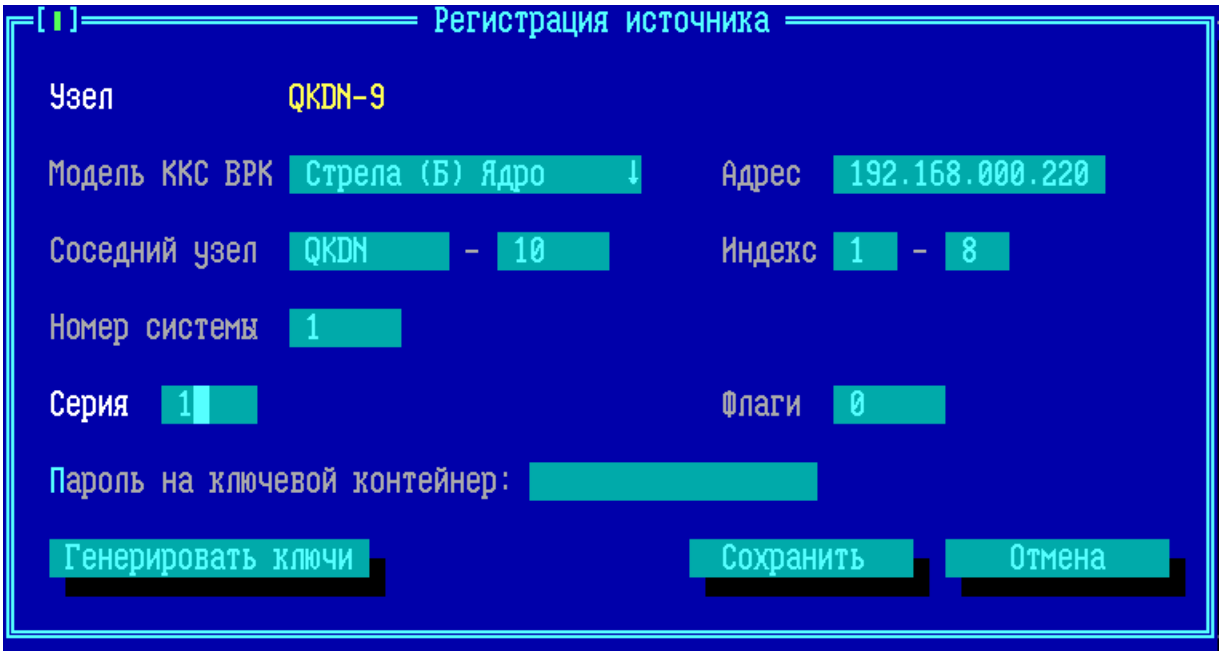


Рисунок 424 - Добавление источника ключей на вкладке «ККС ВРК»

Для источника в зависимости от модели устанавливаются следующие параметры:

Узел – идентификатор квантовой сети и номер узла данного ФПСУ, отображается как справочная информация.

Модель ККС ВРК – модель установленного на узле модуля КРК. Каждая модель может быть в двух исполнениях - (А) Отправитель фотонов и (Б) Получатель.

Адрес – указывается IP-адрес устройства СВКРК, подключенного к текущему ФПСУ. Типовой адрес проставляется автоматически, в зависимости от типа - (А) или (Б). Стандартные IP-адреса указаны в пункте «Стандартные сетевые параметры СВКРК». Указанный IP-адрес должен быть указан в списке абонентов у порта ФПСУ, к которому подключен СВКРК.

Соседний узел – идентификатор квантовой сети и номер узла, на котором находится ККС ВРК, с которой ККС ВРК ФПСУ вырабатывает ключи и будет строиться квантовый туннель. Номер узла согласовывается с администратором безопасности квантовой сети.

Индекс – заполняется для моделей «Звезда (А)» или «Стрела (А) Ядро». Это внутренний номер ККС ВРК внутри топологии «звезда».

Номер системы – заполняется для всех моделей «Звезда» или «Стрела Ядро», означает идентификационный номер выбранной топологии сети.

Серия – номер серии предраспределенных ключей для защиты обмена между ФПСУ и ККС ВРК по протоколу CRISP или ProtoQa.

Пароль на ключевой контейнер – пароль, задаваемый пользователем для защиты хранилища ключей. При генерации ключей пароль устанавливается на контейнер закрытого ключа при его формировании.

Предраспределенные ключи для участников квантовой сети генерируются на ЦВК. На ФПСУ ключ может быть доставлен в виде беспарольного контейнера - файла с расширением «.key». Другой стороне взаимодействия (на ККС ВРК) ключ доставляется в виде парольного контейнера, пароль на ключевой контейнер запрашивается при установке ключей с SD-карты или с USB-TM-токена. Описание установки ключей на ФПСУ приведено в пункте «Установка предраспределенных ключей для участников квантовой сети».

По нажатию кнопки «Генерировать ключи» происходит запись ключей на внешний USB-носитель.

На вкладке «Прочие» по кнопке «Добавить» открывается окно «Регистрация источника»:



Рисунок 425 - Добавление источника ключей на вкладке «Прочие»

Тип источника – СКЗИ-Распределитель или стыковочный узел.

Стыковочный узел взаимодействует с крайними доверенными узлами подсетей КРК, объединяет в сеть КРК разные подсети.

Узел – идентификатор квантовой сети и номер узла, на котором находится ККС ВРК, с которой ККС ВРК ФПСУ вырабатывает ключи и будет строиться квантовый туннель. Номер узла согласовывается с администратором безопасности квантовой сети.

Адрес – указывается IP-адрес устройства СВКРК, подключенного к текущему ФПСУ. Типовой адрес проставляется автоматически, в зависимости от типа - (А) или (Б). Стандартные IP-адреса указаны в пункте «Стандартные сетевые параметры СВКРК». Указанный IP-адрес должен быть указан в списке абонентов у порта ФПСУ, к которому подключен СВКРК.

Порт – указывается порт устройства СВКРК, подключенного к текущему ФПСУ. По умолчанию для обмена сообщениями между ФПСУ и устройством СВКРК используется UDP-порт 11577. Значение порта может быть изменено, интервал значений от 1 до 65535.

ID клиента – Идентификатор клиента, содержит четыре латинских символа, первые два символа - латинские буквы, последние два символа - латинские буквы или цифры.

Номер устройства – идентификатор клиентского устройства. Уникальный в пределах указанного узла номер, присваиваемый устройству, являющемуся потребителем ключей.

Серия – номер серии предраспределенных ключей для защиты обмена между ФПСУ и ККС ВРК по протоколу CRISP или ProtoQa.

Минимальный резерв ключей – настраивается администратором сети, исходя из потребности абонента.

Описание СКЗИ-Потребителей осуществляется из меню конфигурации по команде «Квантовое распределение ключей → СКЗИ-Потребители»:

В окне «СКЗИ-Потребители» задаются абоненты квантовой сети, которым ФПСУ распределяет квантовые ключи и с которыми ФПСУ строит квантовые туннели.

По кнопке «Добавить» открывается окно «СКЗИ-Потребителей»:

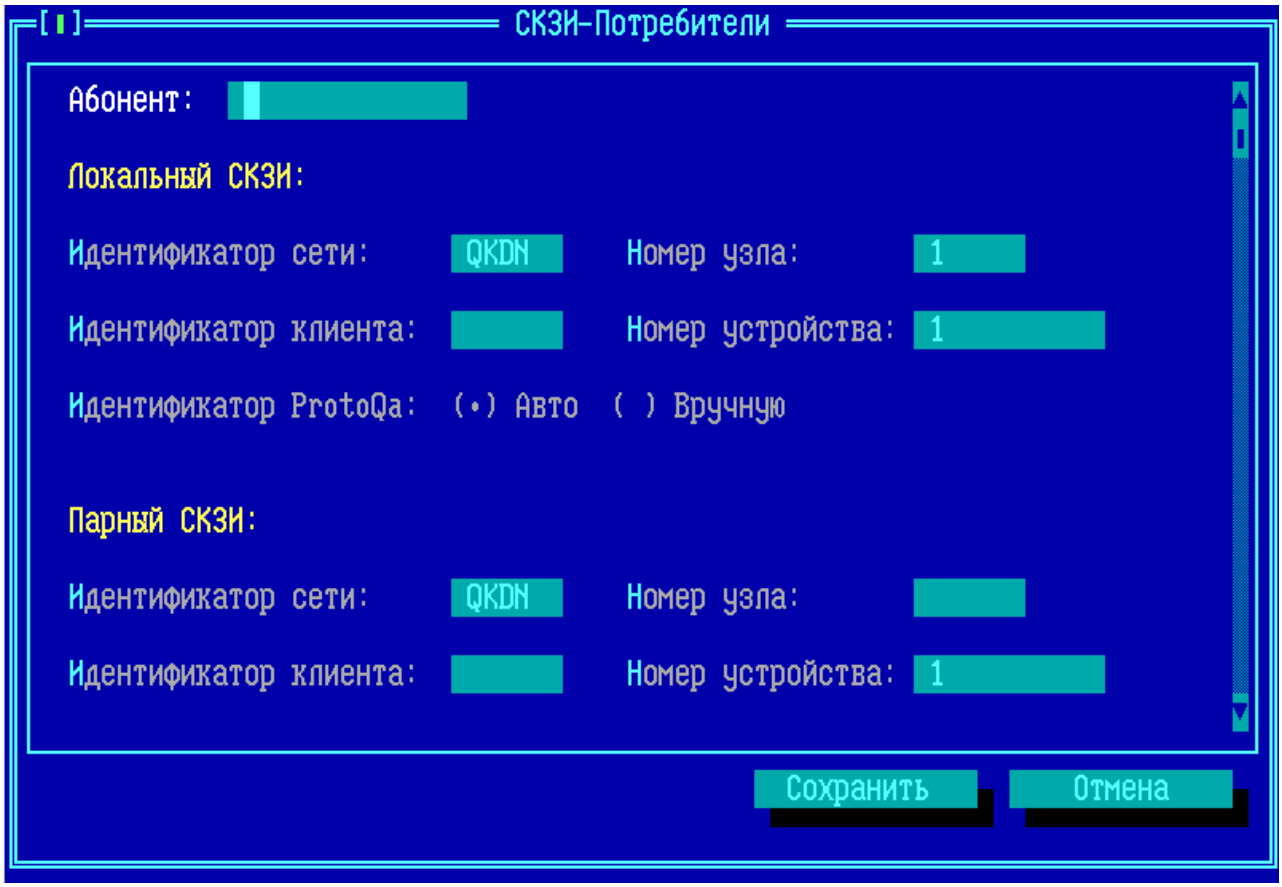


Рисунок 426 - Добавление абонента

Установите следующие параметры:

Абонент – текстовое описание СКЗИ-Потребителя.

Абонент получает пару ключей для обмена сообщениями между указанными узлами квантовой сети. Узел данного ФПСУ будет являться локальным СКЗИ для этого абонента, удаленный квантовый узел будет являться парным СКЗИ для этого абонента. На удаленном узле требуется выполнить зеркальные настройки для данного абонента, локальным СКЗИ будет являться парный СКЗИ.

Идентификатор сети – Идентификатор сети содержит четыре латинских символа, первые два символа - латинские буквы, последние два символа - латинские буквы или цифры. Параметр по умолчанию выставлен в значение «QKDN», изменять не требуется. Идентификатор сети назначается администратором квантовой сети. Внутри одного идентификатора сети объединяются узлы с общим технологическим устройством, правилами подключения и тарификации. Это могут быть узлы внутри сегмента сети или всей сети одного оператора. Необходимость изменения Имени сети устанавливается администратором безопасности квантовой сети.

Номер узла – уникальный в пределах указанной сети номер, присваиваемый данному ФПСУ, число от 1 до 64999. Номер согласуется с администратором безопасности квантовой сети и не должен быть произвольным.

Идентификатор клиента – Идентификатор клиента, содержит четыре латинских символа, первые два символа - латинские буквы, последние два символа - латинские буквы или цифры.

Номер устройства – идентификатор клиентского устройства. Уникальный в пределах указанного узла номер, присваиваемый устройству, являющемуся потребителем ключей.

Идентификатор ProtoQa – идентификатор формируется автоматически из атрибутов узла при установлении флага «Авто», либо вводится в отдельное поле при установлении флага «Вручную». Для СКЗИ-Потребителей производства ООО «АМИКОН», либо совместимых с ними в части адресации на квантовой сети, переключатель следует оставить в положении «Авто». В ином случае следует перевести переключатель в положение «вручную» и заполнить вручную идентификатор в виде 32-значного числа в hex-формате (используются цифры от «0» до «9» и латинские буквы от «a» до «f».

Лимит ключей в сутки – настраивается администратором сети, исходя из потребности абонента.

Номер серии – номер серии предраспределенных ключей для защиты обмена между ФПСУ и ККС ВРК по протоколу CRISP или ProtoQa.

Пароль на ключевой контейнер – пароль, задаваемый пользователем для защиты хранилища ключей. При генерации ключей пароль устанавливается на контейнер закрытого ключа при его формировании.

Предраспределенные ключи для участников квантовой сети генерируются на ЦВК. На ФПСУ ключ может быть доставлен в виде беспарольного контейнера - файла с расширением «.key». Другой стороне взаимодействия (на ККС ВРК) ключ доставляется в виде парольного контейнера, пароль на ключевой контейнер запрашивается при установке ключей с SD-карты или с USB-TM-токена. Описание установки ключей на ФПСУ приведено в пункте «Установка предраспределенных ключей для участников квантовой сети».

По нажатию кнопки «Генерировать ключи» происходит запись ключей на внешний USB-носитель.

11. 4. 2. Настройка служебного туннеля

Служебный туннель предназначен для защиты от подмены передаваемых между подключенными к смежным ФПСУ устройствами СВКРК служебных данных. Для каждой пары соединенных оптоволокном устройств СВКРК должен быть указан служебный туннель на ФПСУ.

По служебному туннелю передаются также служебные сообщения между ФПСУ, предназначенные для обслуживания туннеля. Идет ли обмен по служебному туннелю между СВКРК или нет можно сказать по интенсивности трафика в туннеле. В нормальном режиме при активном обмене между устройствами СВКРК передается служебный трафик порядка 200 pps и не менее 0,1 Mbps. Без трафика СВКРК в туннеле передаются только служебные данные между ФПСУ, несколько пакетов в секунду.

Служебный туннель описывается на порту интерфейса, подключенному к сети передачи данных.

Служебный туннель между двумя ФПСУ организуется на полученных от ЦВК ключах и описывается следующим образом (см. рисунок ниже):

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

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

Тип туннеля – ФПСУ;

Адрес – адрес соседнего ФПСУ в VLAN, предназначенном для передачи служебного трафика (на примере – 192.168.111.111 с указанием VLAN=2);

Имя – произвольное название, необязательный параметр. При выборе служебного типа КРК-туннеля будет предложено имя %идентификатор_сети%-%номер_соседнего_узла % в скобках добавится обозначение туннеля (QKDN-2 (SK) на примере), ;

Отправитель – один из вторичных адресов порта, который подставляется в поле source при отправке пакета в сеть;

MAC – не задается;

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

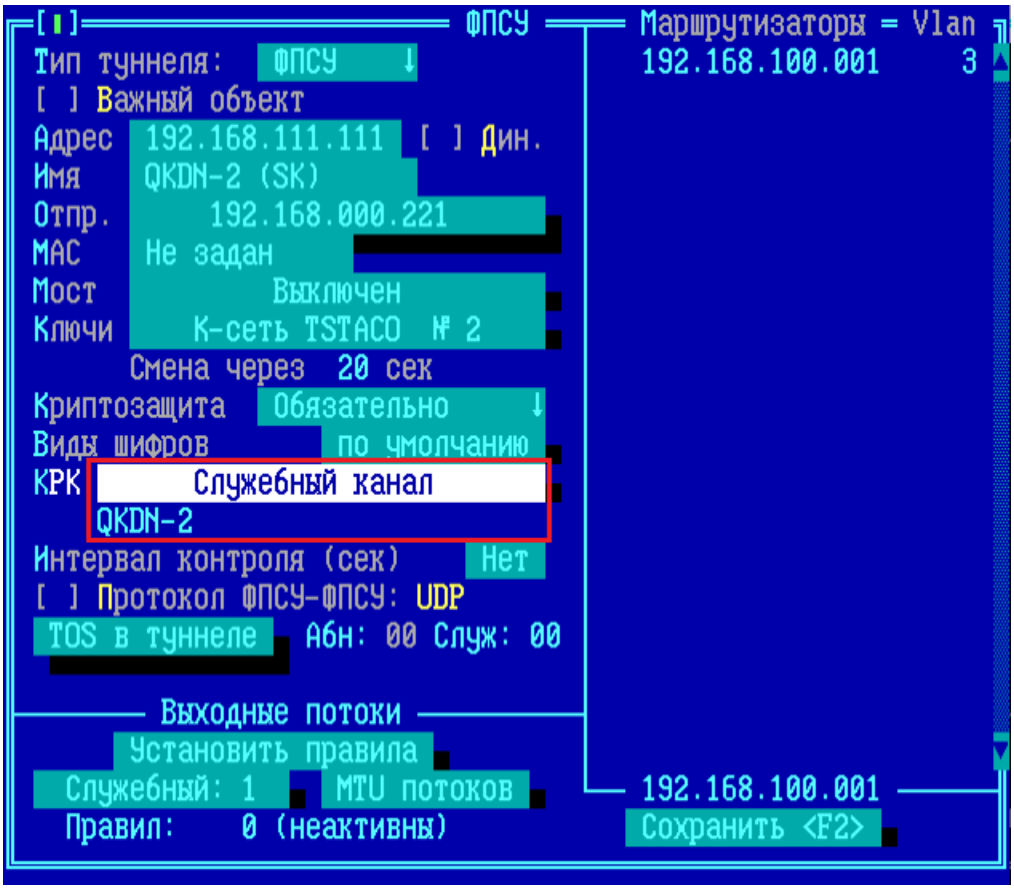


Рисунок 427 - Описание служебного туннеля

Криптозащита –следует установить «Обязательно»;

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

КРК – следует перейти в окно КРК и установить флаг «Служебный канал», с указанием идентификатора сети и полученного от администратора безопасности квантовой сети номера узла, зарегистрированного за соседним ФПСУ (см. рисунок ниже);

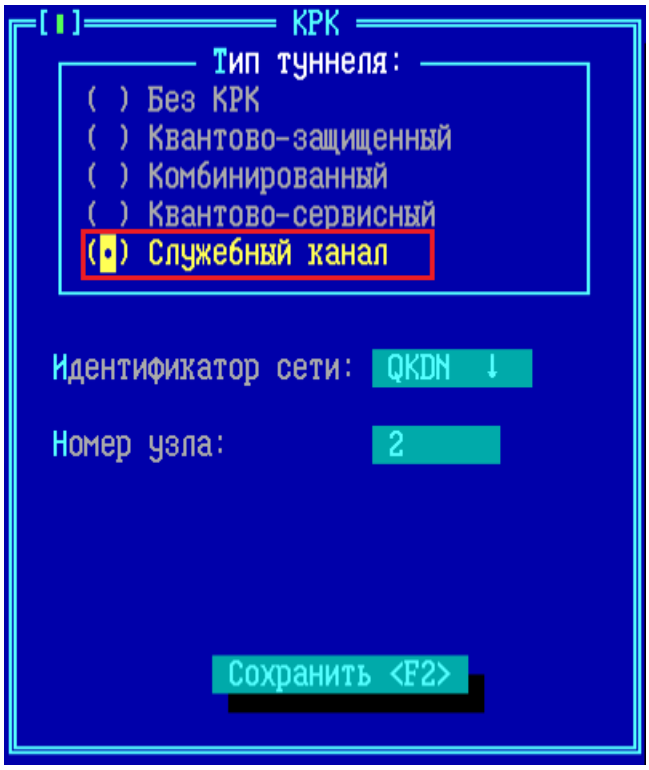


Рисунок 428 -Режим КРК для служебного туннеля

11. 4. 3. Настройка квантово-сервисного туннеля

Квантово-сервисный туннель предназначен для защищенной на квантовом ключе передачи КЗК-ключа соседним промежуточным узлом ФПСУ для последующей итоговой передачи на опорные узлы. Опорные узлы на основе полученных КЗК-ключей организуют квантовые туннели между опорными узлами. Для каждой пары соединенных оптоволокном устройств СВКРК должен быть указан квантово-сервисный туннель на ФПСУ.

Квантово-сервисный туннель описывается на порту интерфейсе, подключенному к сети передачи данных.

Квантово-сервисный туннель между двумя ФПСУ организуется на полученных от устройства СВКРК квантового ключа и описывается следующим образом (см. рисунок ниже):

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

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

Тип туннеля – ФПСУ;

Адрес – адрес соседнего ФПСУ в VLAN, предназначенном для передачи КЗК-ключей (на примере – 192.168.002.126);

Имя – произвольное название, необязательный параметр. При выборе квантово-сервисного типа КРК-туннеля будет предложено имя %идентификатор_сети%-% номер_соседнего_узла% в скобках добавится обозначение туннеля (QKDN-2 (QS) на примере);

Отправитель – один из вторичных адресов порта, который подставляется в поле source при отправке пакета в сеть;

MAC – не задается;

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

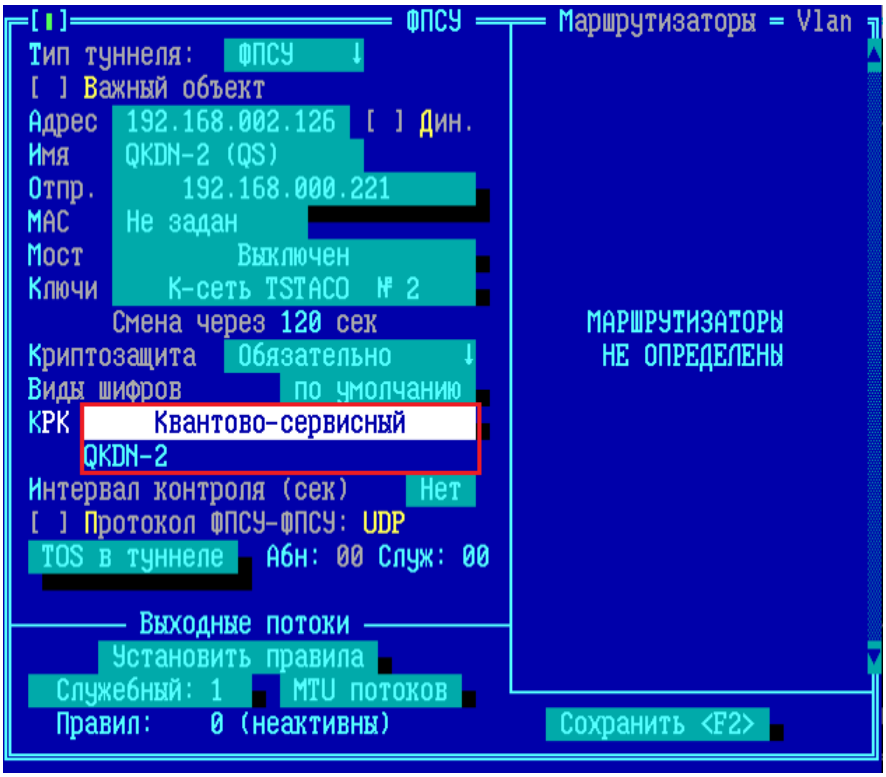


Рисунок 429 - Описание квантово-сервисного туннеля

Криптозащита –следует установить «Обязательно»;

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

КРК – следует перейти в окно КРК и установить флаг «Квантово-сервисный», с указанием идентификатора сети и полученного от администратора безопасности квантовой сети номера узла, зарегистрированного за соседним ФПСУ (см. рисунок ниже);

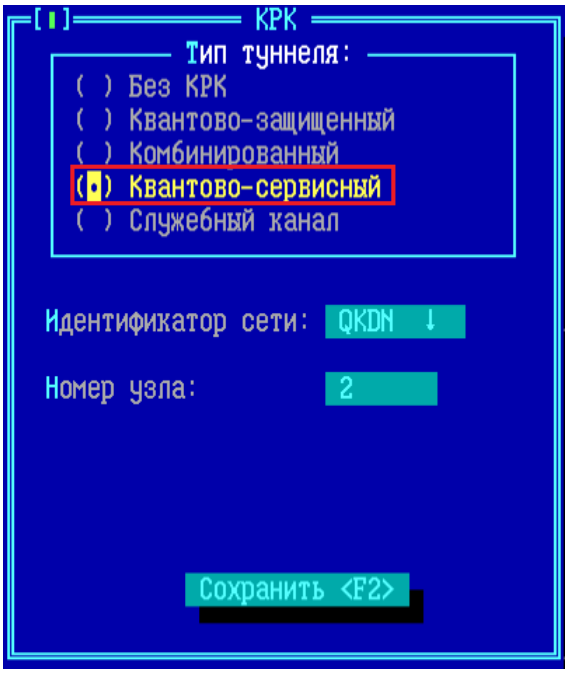


Рисунок 430 -Режим КРК для квантово-сервисного туннеля

11. 4. 4. Настройка комбинированного туннеля

Комбинированный туннель строится между промежуточными узлами, или между опорными узлами, или между промежуточным и опорным узлами. Комбинированный туннель предназначен в том числе для передачи через него трафика систем управления, таких как АРМ УА, сервера Syslog или SNMP. Передаваемый в комбинированном туннеле трафик защищается на квантовых или КЗК-ключах, если они присутствуют в накопительном буфере ФПСУ. Если по каким-либо причинам квантовых ключей или КЗК-ключей на ФПСУ ещё нет, трафик будет защищаться на полученных от ЦВК ключах.

Ситуация со временным отсутствием квантовых или КЗК-ключей на ФПСУ может возникнуть при старте или перезапуске ФПСУ и/или устройства СВКРК. В этом случае потребуется некоторое время, прежде чем устройства СВКРК выработают квантовый ключ и передадут его соседним ФПСУ. Для обеспечения возможности управления и мониторинга в этот период, для защиты трафика будут использоваться ключи ЦВК. Как только в буфере

ФПСУ появятся квантовые ключи, будет осуществлен переход защиты трафика с ключей ЦВК на квантовые ключи.

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

Комбинированный туннель между двумя ФПСУ описывается следующим образом (см. рисунок ниже):

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

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

Тип туннеля – ФПСУ;

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

Имя – произвольное название, необязательный параметр. При выборе комбинированного туннеля в окне КРК будет предложено имя %идентификатор_сети%-% номер_соседнего_узла% в скобках добавится обозначение туннеля (QKDN-2 (QC) на примере);

Отправитель – один из вторичных адресов порта, который подставляется в поле source при отправке пакета в сеть;

MAC – не задается;

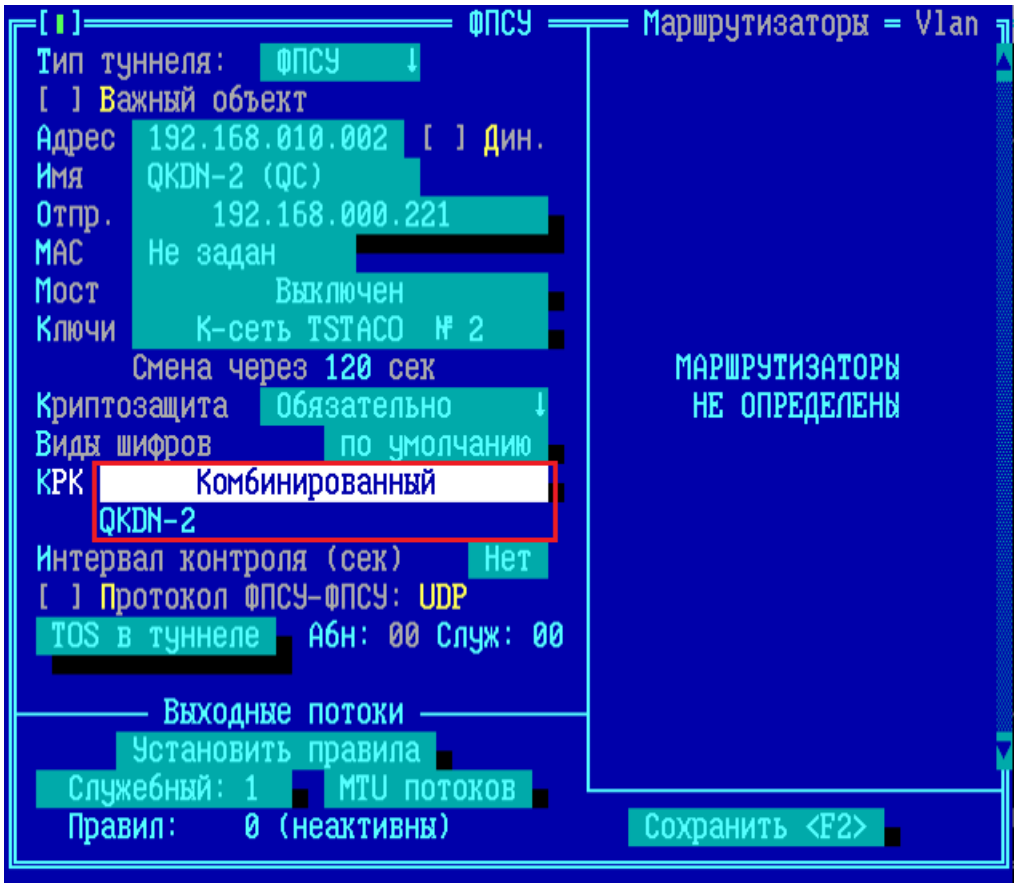


Рисунок 431 - Описание комбинированного туннеля

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

Криптозащита – следует установить «Обязательно»;

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

КРК – следует перейти в окно КРК и установить флаг «Комбинированный», с указанием идентификатора сети и полученного от администратора безопасности квантовой сети номера узла, зарегистрированного за соседним ФПСУ (см. рисунок ниже):

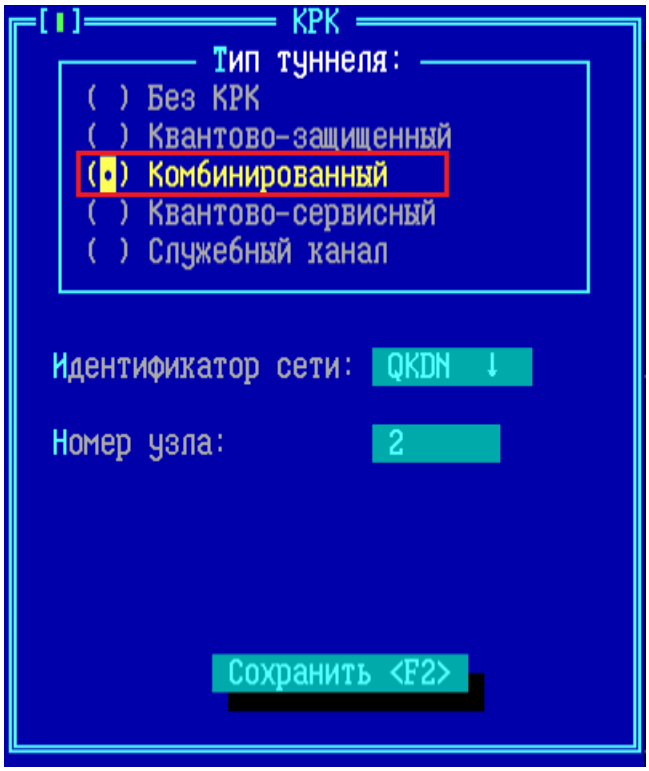


Рисунок 432 - Режим СВКРК для комбинированного туннеля

Настройка комбинированного туннеля завершена.

Сетевые сервисы, которые должны передавать защищенный трафик управления, описываются как абоненты в режиме «Через ФПСУ», где в качестве «Линии ФПСУ» выбран комбинированный туннель.

11. 4. 5. Настройка квантово-защищенного туннеля

Квантово-защищенный туннель строится между промежуточными узлами на квантовых ключах, получаемых строящими туннель ФПСУ от подключенных к ним соседних устройств СВКРК, после того как устройства СВКРК выработали квантовый ключ, или же между опорными узлами на КЗК-ключах, полученных через квантово-сервисный туннель от промежуточных узлов ФПСУ.

Квантово-защищенный туннель описывается на порту интерфейса, подключенному к сети передачи данных.

Квантово-защищенный туннель между двумя ФПСУ описывается следующим образом (см. рисунок ниже):

Включенные флаги «Важный объект», «Динамический», «Протокол ФПСУ-ФПСУ:UDP», параметры «Мост», «TOS в туннеле», «Выходные потоки» не являются

обязательными настройками для создания квантово-защищенного туннеля и должны устанавливаться по согласованию с администратором безопасности квантовой сети.

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

Тип туннеля – ФПСУ;

Адрес – адрес соседнего ФПСУ в VLAN, предназначенном для передачи пользовательского трафика, зашифрованного на квантовых ключах (на примере – 192.168.001.125);

Имя – произвольное название, необязательный параметр. При выборе квантового туннеля в окне КРК будет предложено имя %идентификатор_сети%-%номер_соседнего_узла % в скобках добавится обозначение туннеля (QKDN-2 (Q) на примере);

Отправитель – один из вторичных адресов порта, который подставляется в поле source при отправке пакета в сеть;

MAC – не задается;

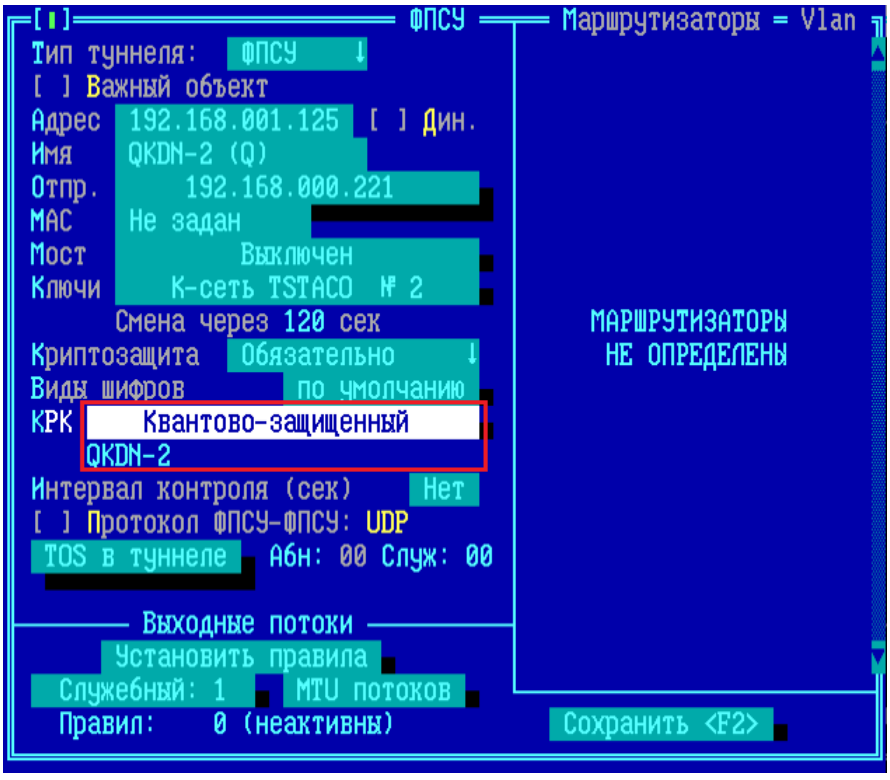


Рисунок 433 - Описание квантового туннеля

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

Криптозащита – следует установить «Обязательно»;

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

КРК – следует перейти в окно КРК и установить флаг «Квантово-защищенный», с указанием идентификатора сети и полученного от администратора безопасности квантовой сети номера узла, зарегистрированного за соседним ФПСУ (см. рисунок ниже):

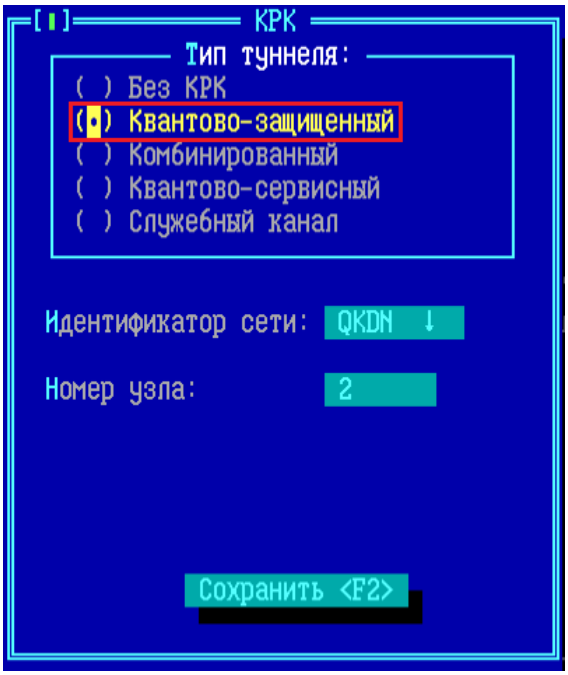


Рисунок 434 - Режим СВКРК для квантового туннеля

Настройка квантово-защищенного туннеля завершена.

Сетевые сервисы, которые должны передавать защищенный пользовательский трафик, описываются как абоненты в режиме «Через ФПСУ», где в качестве «Линии ФПСУ» выбран квантово-защищенный туннель.

11. 4. 6. Установка предраспределенных ключей для участников квантовой сети

Предраспределенные ключи для участников квантовой сети генерируются на ЦВК.

Установить ключи на ФПСУ следует по команде меню «Управление дополнениями → Управление ключами».

В открывшемся окне отображается список ключей аддонов, при первом открытии список пуст.

Для установки ключей на ФПСУ необходимо нажать кнопку «Добавить». После выполнения команды система предложит подключить USB-носитель с файлом с ключами, к ФПСУ:

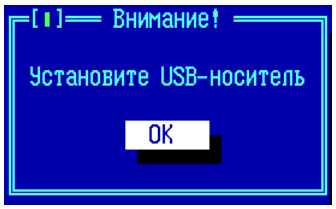


Рисунок 435 - Предложение подключить USB-носитель

Откроется окно выбора файла с ключами. Выделение строки с файлом и переход на кнопку «Файл выбран» осуществляется клавишей <*Tab*>.



Рисунок 436 - Выбор файла с ключами

На экран будет выдано сообщение о найденных ключевых данных:

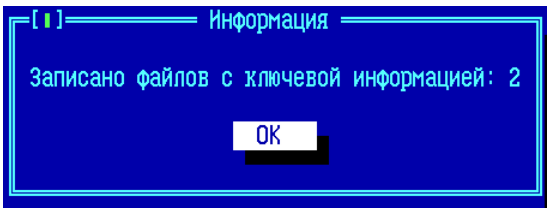


Рисунок 437 - Сообщение о найденных файлах с ключевой информацией

После подтверждения в списке ключей отобразятся установленные ключи.

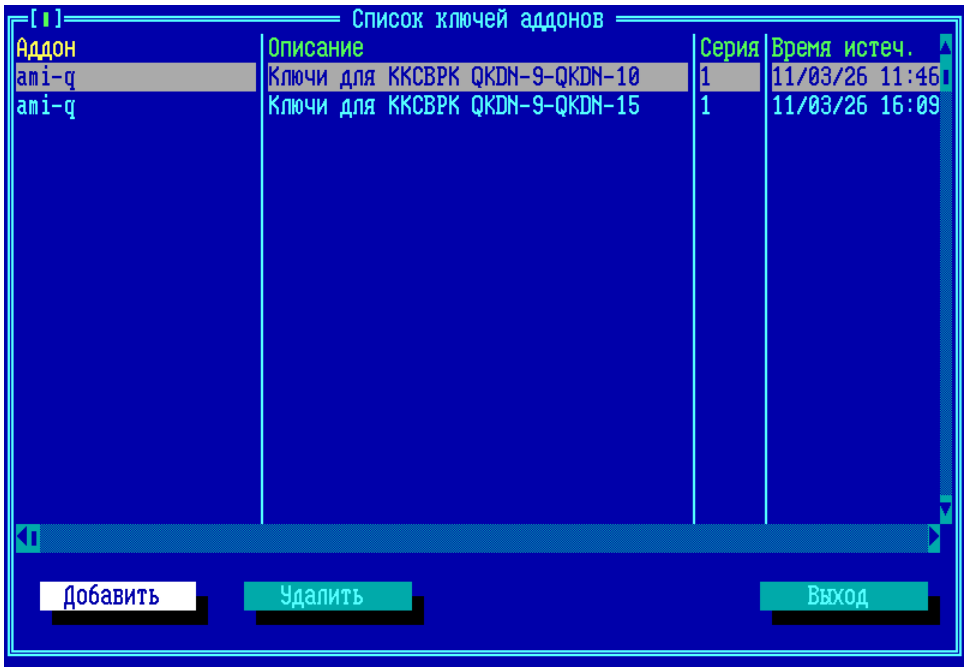


Рисунок 438 - Установленные ключи на ФПСУ

11. 4. 7. Управление Модулем КРК

В режиме конфигурации меню параметры модуля AMI-QKD открывается из пункта меню «Настройка дополнений → Управление модулем КРК»:



Рисунок 439 - Меню «Управление дополнениями»

Меню дополнения ami-q, содержит следующие команды для пуско-наладочных работ:

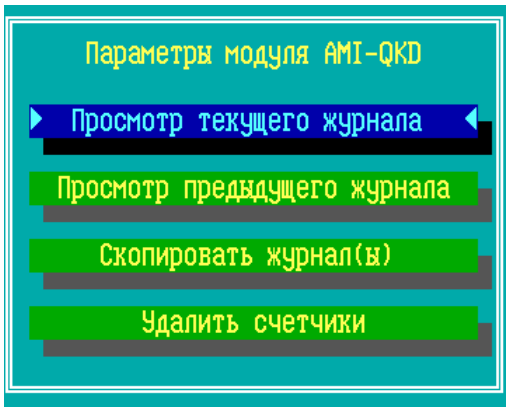


Рисунок 440 - Меню «Управление Модулем КРК»

Просмотр текущего журнала – записи отладочного журнала дополнения ami-q выдаются на экран с указанием события и времени регистрации.

Запись журнала ведется с момента запуска ФПСУ до следующего запуска ФПСУ, данная запись называется текущим журналом. После запуска ФПСУ начинается запись текущего журнала, существующий журнал становится предыдущим журналом и изменяет название, новый журнал становится текущим.

Просмотр предыдущего журнала – записи предыдущего отладочного журнала дополнения ami-q выдаются на экран с указанием события и времени регистрации.

Скопировать журнал – на внешний носитель выдается файл лога дополнения ami-q. Перед выполнением команды необходимо подключить USB-носитель, на который будет выдан файл, к ФПСУ и запустить команду.

Удалить счетчики – по команде обнуляются счетчики отправленных и полученных сообщений.

12. Клиенты ФПСУ

12. 1. Клиент для ФПСУ

Под «клиентом» ФПСУ в разделе подразумевается программный или программно-аппаратный комплекс «ФПСУ-IP/Клиент», предназначенный для защиты доступа отдельной рабочей станции к ресурсам сети передачи данных, защищенным ФПСУ.

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

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

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

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

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

- явно указывает системные идентификаторы клиентов (номер криптосети, номер группы, номер пользователя), которые смогут работать через ФПСУ;
- 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 и клиентом, администратор ФПСУ 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 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 может ограничить «миграцию» клиентов, указав IP- и MAC-адреса рабочих станций, с которых работа разрешена.

Для настройки ФПСУ в части работы с клиентами выберите команду меню конфигурации «*Клиенты → ФПСУ-Клиенты»*.

На экран будет выдано окно со списком зарегистрированных на ФПСУ групп Криптосетей, пустое (при первом запуске) или содержащее список пар Криптосеть /логическая группа клиентов, которые будут обслуживаться ФПСУ. На одном ФПСУ может быть описано не более 128 логических групп, принадлежащих одной или нескольким Криптосетям Клиентов, в одной группе может быть зарегистрировано не более 1024 Клиентов.

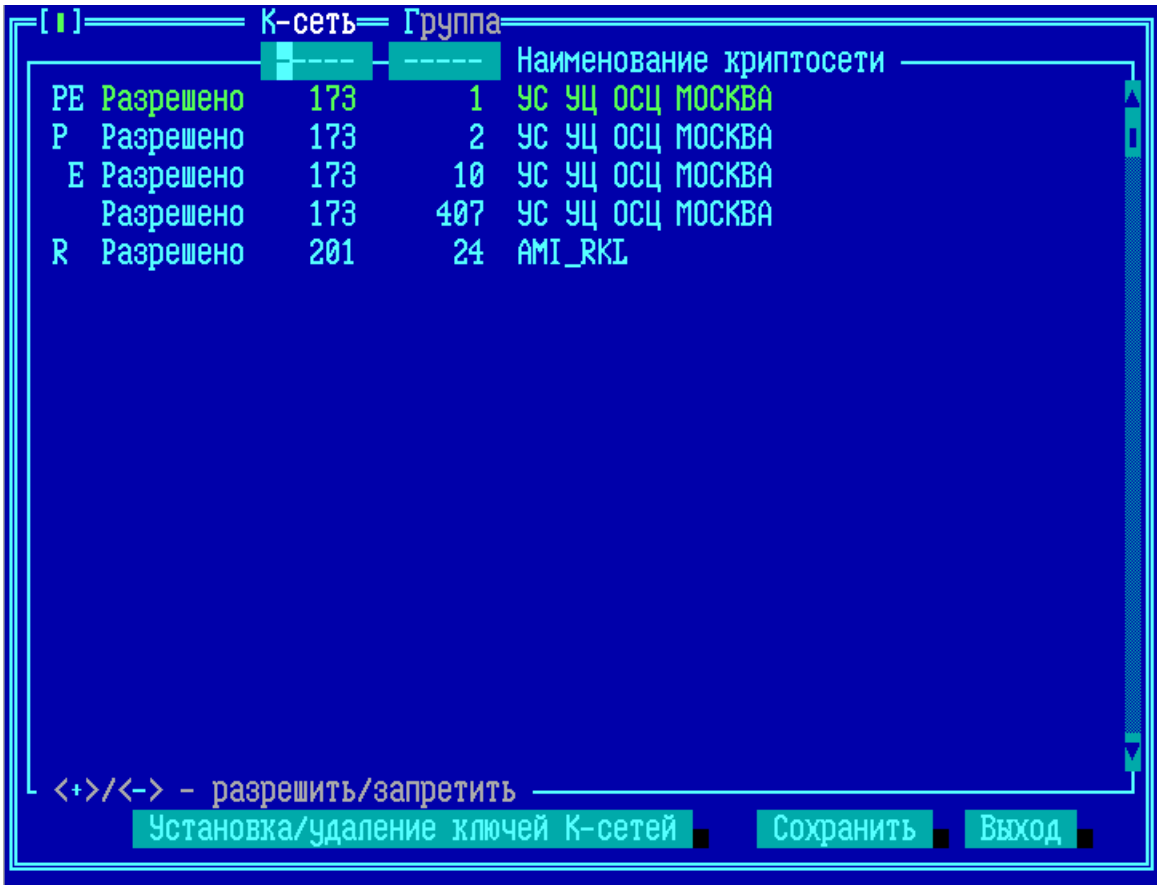


Рисунок 441 - Список групп Клиентов на ФПСУ

Для установки или изменения правил работы клиентов, входящих в одну из групп списка, отметьте ее строкой выбора и нажмите клавишу <*Enter*> - см. пункт «Установка правил работы клиентов».

Для удаления записи логической группы отметьте его и нажмите <*Del*>. Для того чтобы разрешить (запретить) работу через ФПСУ 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.

Для установки общесистемных ключей активируйте опцию «*Установка/удаление ключей К-сетей*» – см. раздел «Установка и удаление общесистемных ключей».

Переход курсора на опцию «*Установка/удаление ключей К-сетей*» осуществляется по клавише <→>, <*Tab*>.

Для перехода к полям поиска группы нажмите клавишу <←→>. В полях задайте номер Криптосети и номер искомой группы, нажмите <*Enter*>, в списке групп будет выделена строка с найденной группой.

12. 1. 1. Установка и удаление общесистемных ключей

По умолчанию, общесистемных ключей на ФПСУ не установлено. Без установленных общесистемных ключей ФПСУ не будет принимать соединения Клиентов.

Для установки нового общесистемного ключа на ФПСУ выполните следующие действия:

В окне списка групп Криптосетей нажмите кнопку «*Установка/удаление ключей К-сетей*», после чего на экран монитора будет выдан список Криптосетей Клиентов, ключи которых были установлены на ФПСУ.

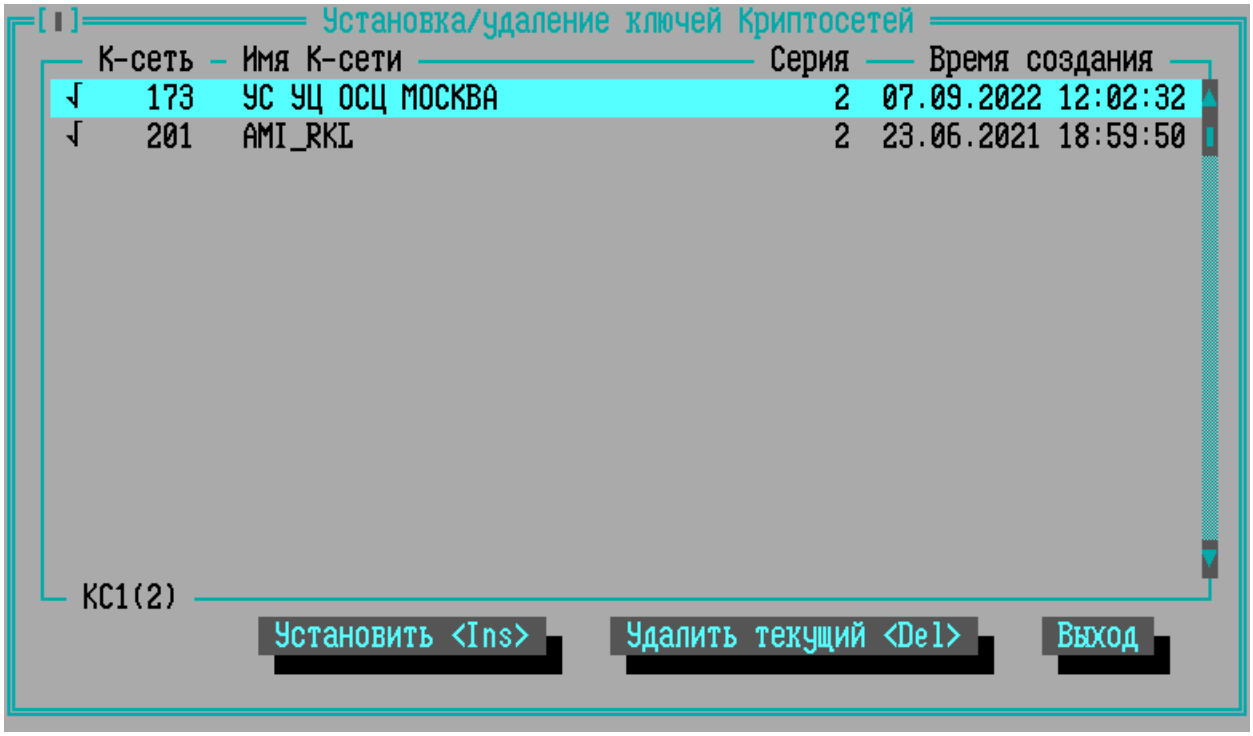


Рисунок 442 - Установленные на ФПСУ общесистемные ключи Криптосетей Клиентов

Если строка слева помечена символом «√» – это означает, что ключи уже зарегистрированы на ФПСУ, то есть для Криптосети создана хотя бы одна запись логической группы и определены правила работы клиентов. Такие ключи можно удалить только после того, как удалены записи всех логических групп, принадлежащих данной Криптосети Клиентов. Если ключи не используются в конфигурации ФПСУ, их можно удалить с помощью клавиши <*Del*> или нажатием кнопки «*Удалить текущий <DEL>*».

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

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

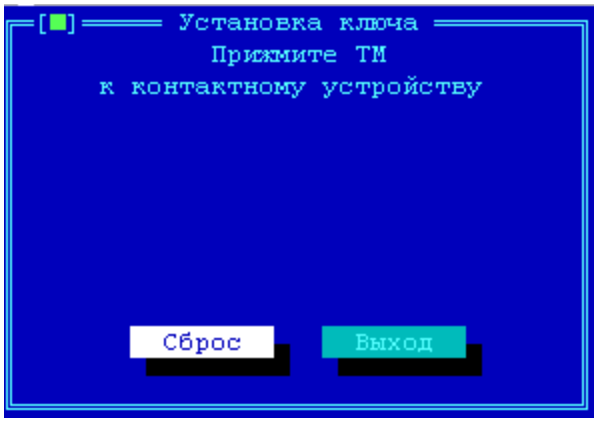


Рисунок 443 - Ожидание ТМ-идентификатора

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

12. 1. 2. Описание логической группы клиентов

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

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

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

В окне используемых на ФПСУ Криптосетей и Групп ЦГКК нажмите клавишу <*Ins*>, после чего на экран будет выдан список Криптосетей, общесистемные ключи которых были ранее установлены на ФПСУ.

В списке слева от Криптосети отметка «**R**» означает признак RKL-Криптосети, Клиенты такой Криптосети могут осуществлять удаленную загрузку ключевых данных Клиентов других Криптосетей. На ФПСУ может быть активна только одна RKL-Криптосеть.

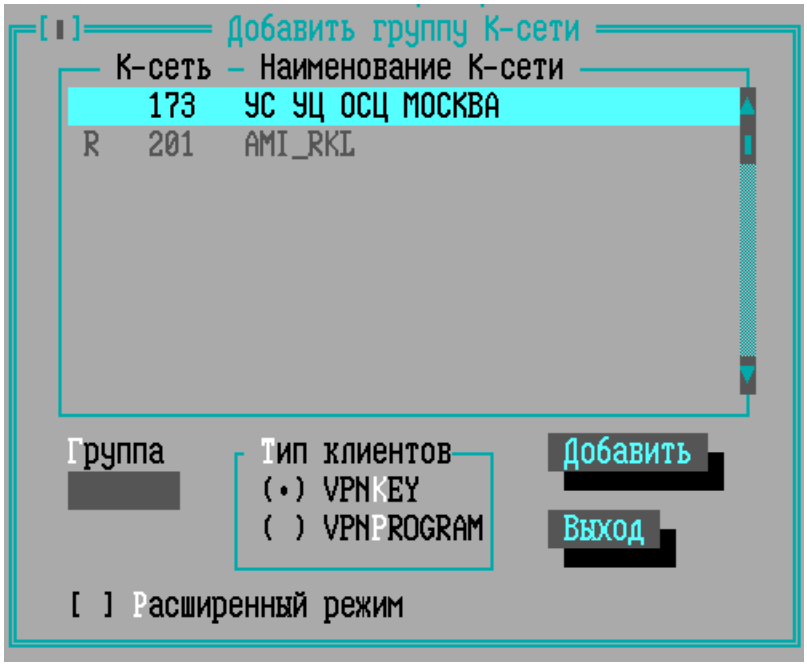


Рисунок 444 - Добавление группы клиентов

Выберите Криптосеть Клиентов, которой будет принадлежать описываемая группа, затем при помощи клавиши <→> или <*Tab*> переместитесь в поле «*Группа*», где следует ввести номер группы. Номер группы должен совпадать с логическим номером, присвоенным описываемой группе администратором программы ЦГКК.

Потом следует выбрать тип клиентов в создаваемой группе:

- VPNKEY – пользователи ПАК «ФПСУ-IP/Клиент», стандартный тип клиентов, ключевые данные которых хранятся в USB-устройстве VPN-Key. Далее по документу, если будет говориться о «клиенте» без уточнения, следует считать, что идет описание именно клиента типа VPN-Key.
- VPNPROGRAM – пользователи программного комплекса «ФПСУ-IP/Клиент», не использующие USB-устройство VPN-Key. Далее по документу, данный пользователь будут упоминаться как «программный клиент» или «мобильный клиент».

ВНИМАНИЕ! Для поддержки пользовательских подключений VPNPROGRAM на ФПСУ необходимо установить специальное обновление активации программных клиентов ФПСУ!

Для групп RKL-Криптосети тип клиентов предустановлен, всегда VPNKEY.

Расширенный режим - при установлении флага клиенты данной группы смогут осуществлять взаимодействие с ЦРМК, ЦРМК-RKL, внешней системой RKL. Расширенный режим позволяет вести учет ключевых данных для устройств с установленным ПО ФПСУ-IP/Клиент с помощью ЦРМК-RKL.

После введения номера и указания типа группы клиентов нажмите кнопку «*Добавить*». В открывшемся окне введите имя для описателя группы клиентов и нажмите кнопку *«Сохранить»*.

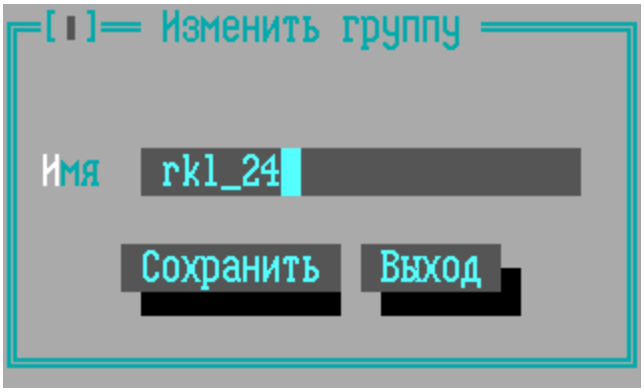


Рисунок 445 - Наименование группы клиентов

В результате выполнения команды пустая запись группы появится в окне групп ЦГКК.

На созданную группу будет по умолчанию выставлена метка «ЗАПРЕЩЕНО». Пока она выставлена, пользователям из указанной группы и криптосети будет запрещено выполнять соединение с ФПСУ.

Если группа содержит описатели программных клиентов типа VPNPROGRAM, то она будет отмечена буквой «**P**» (program).

Если при создании группы был активирован флаг «Расширенный режим», то она будет отмечена буквой «**E**» (extended).

Группа RKL-Криптосети отмечается в списке буквой «**R**».

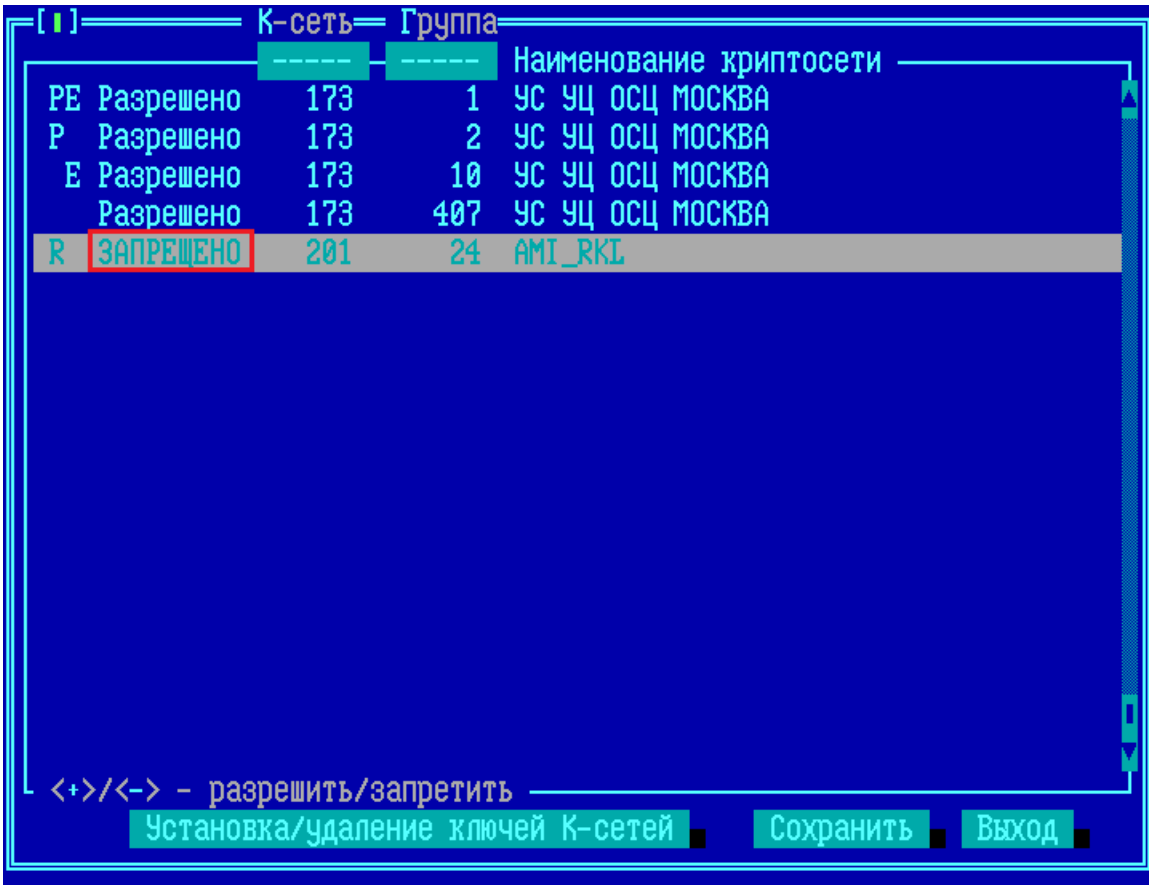


Рисунок 446 - Создана новая группа клиентов

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.

12. 1. 3. Установка правил работы клиентов

Параметры соединений клиентов группы с ФПСУ определяются специальными записями – описаниями. Для перехода к списку существующих в группе описаний, выберите группу в окне списка групп криптосетей и нажмите клавишу <*Enter*>. В открывшемся окне списка описаний клиентов, пустом по умолчанию, администратор может создавать, удалять и разделять описания правил работы клиентов.

В левой верхней части окна выводится символы признака группы: «**P**» (группа мобильных клиентов), «**E**» (группа клиентов с расширенным режимом RKL), «**R**» (группа RKL-клиентов), подробнее см. пункт «Описание логической группы клиентов».

Для каждой логической группы может быть создано от одного до 64 описаний правил работы, причем для каждого клиента правила работы устанавливаются однозначно, то есть номера клиентов, входящих в одно описание, не могут повторяться в других описаниях.

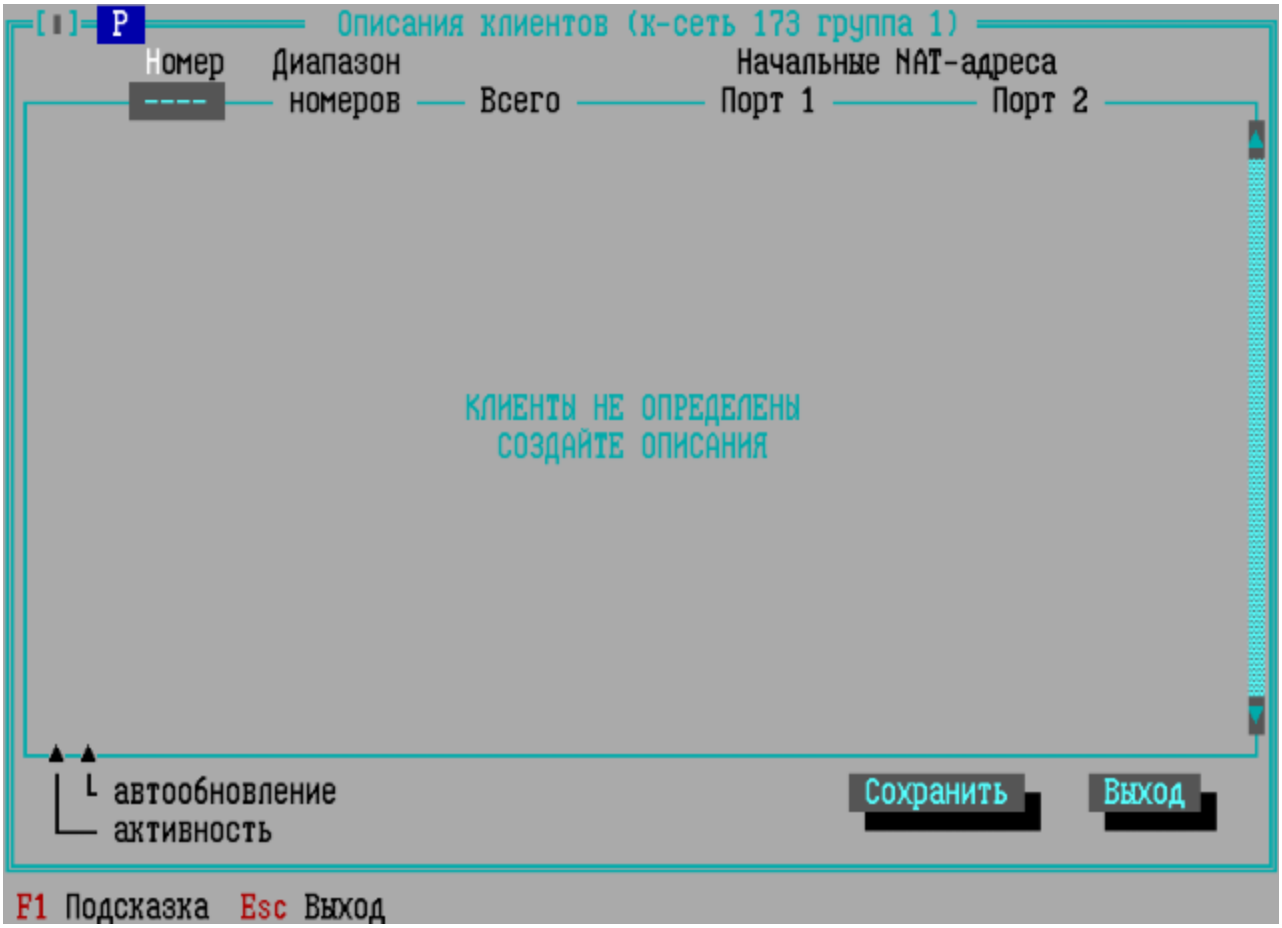


Рисунок 447 - Пустой список описаний новой группы

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

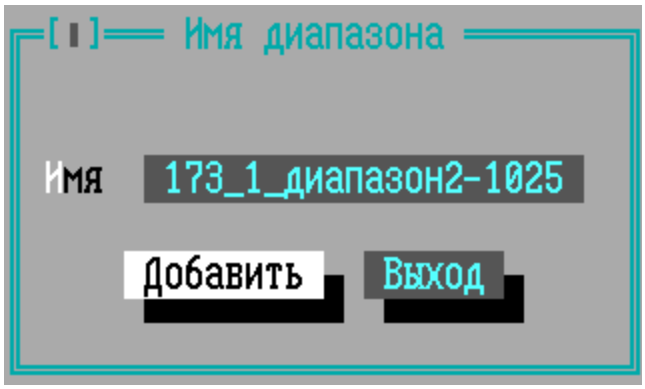


Рисунок 448 - Наименование диапазона номеров

Появится окно указания параметров взаимодействия клиентов и ФПСУ.

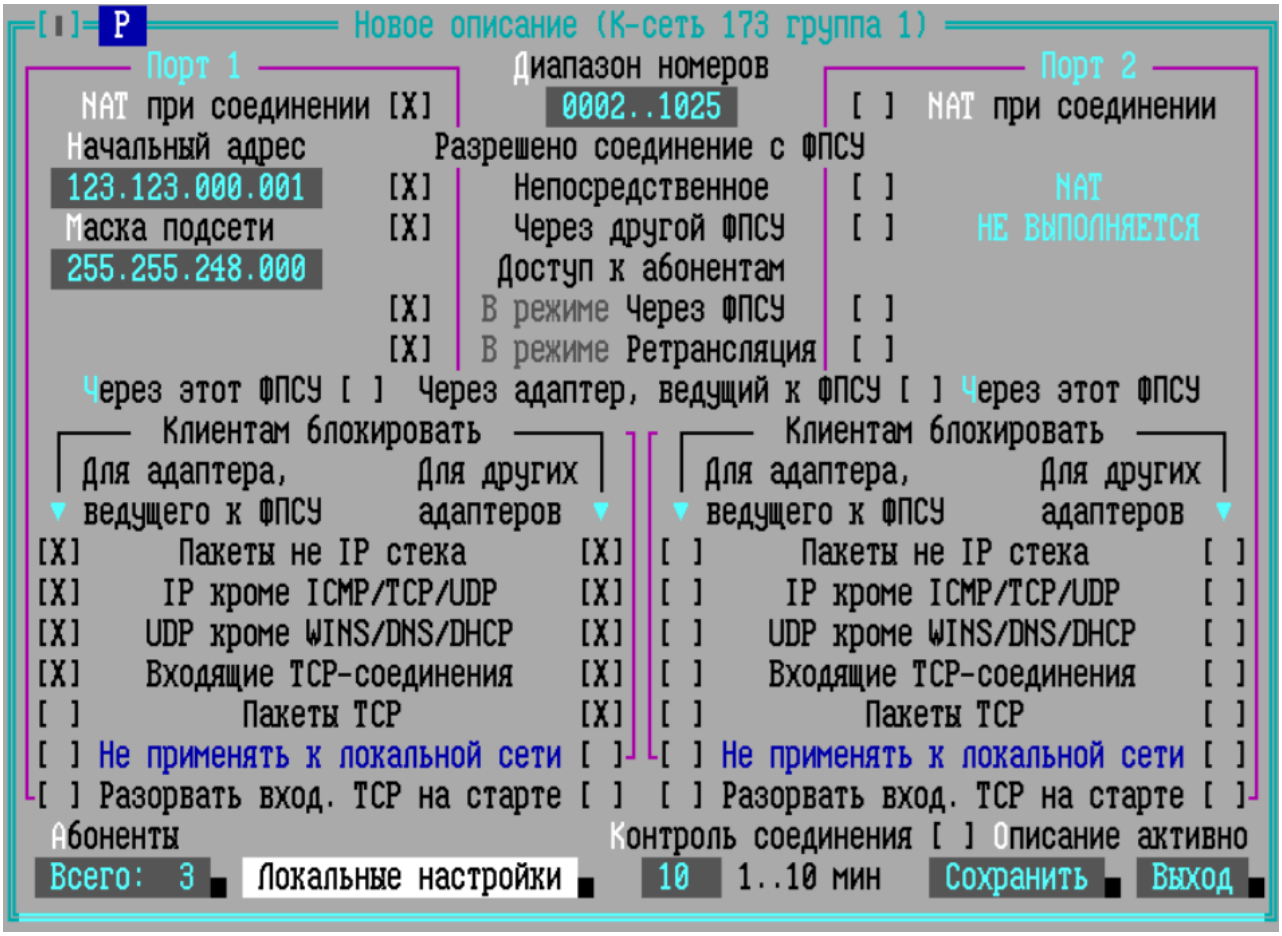


Рисунок 449 - Описание параметров работы диапазона Клиентов

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

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

В поля открывшегося окна описания введите:

Параметр	Описание параметра
Диапазон номеров	- диапазон уникальных номеров клиентов, для которых устанавливаются правила. Диапазоны номеров различных описаний не могут пересекаться;
NAT при соединении	- указание ФПСУ производить трансляцию реальных IP адресов клиентов описываемого диапазона во внутренние (виртуальные) адреса защищаемой подсети при соединениях со стороны данного порта;
Начальный адрес	- в случае применения NAT-трансляции первый из IP адресов внутренней подсети, в который будет транслироваться реальный IP-адрес первого клиента описываемого диапазона;
Маска подсети	- в случае применения NAT-трансляции используется маска внутренней подсети, рассчитанная на количество клиентов описываемого диапазона. ВНИМАНИЕ! В диапазон адресов, образованный начальным адресом и маской, не должен попадать ни один реально существующий IP-адрес, указанный в конфигурации ФПСУ;
Разрешено соединение через ФПСУ	- разрешение ФПСУ производить соединения с клиентами со стороны данного порта в задаваемом режиме (обмениваться данными с описываемыми клиентами непосредственно или через другой ФПСУ). Если режим соединений с клиентами не регламентируется, включите при помощи клавиши *<Пробел>* оба флага. Если ни один флаг не установлен – доступ клиентам со стороны данного порта ФПСУ предоставляться не будет;

Параметр	Описание параметра
Разрешен доступ к абонентам	- разрешение ФПСУ предоставлять клиентам, работающим со стороны данного порта, доступ к станциям назначения (со стороны любого порта) только в задаваемом режиме. Если режим соединений ФПСУ с рабочими станциями не регламентируется, включите при помощи клавиши *<Пробел>* оба флага. Если ни один флаг не установлен, доступ клиентам со стороны данного порта ФПСУ к другим рабочим станциям предоставляться не будет;
Через адаптер, ведущий к ФПСУ	- опция, изменяющая сетевые настройки на стороне рабочей станции Клиента. После её включения, все IP-пакеты, отправляемые рабочей станцией Клиента через сетевой адаптер, ведущий к ФПСУ, будут зашифрованы и отправлены в туннель к ФПСУ. ВНИМАНИЕ! При включении опции открытые соединения рабочей станции Клиента через ведущий к ФПСУ сетевой адаптер будут невозможны;
Клиентам блокировать	- указание клиентам при работе со стороны данного порта ФПСУ блокировать соответствующие соединения. Установленные администратором ФПСУ ограничения будут выполняться на всех указанных сетевых адаптерах рабочих станций клиентов принудительно, независимо от собственных установок клиентов. ВНИМАНИЕ! Для клиентов типа VPNPROGRAM такой вид дополнительной настройки недоступен;
Не применять к локальной сети	- флаг, разрешающий не применять указанные блокировки опции «Клиентам блокировать» для сетевых взаимодействий в пределах локальной сети рабочей станции Клиента.
Разорвать вход. TCP на старте	- указание принудительного разрыва всех входящих TCP сессий на рабочей станции Клиента, в момент установления соединения с ФПСУ.
Абоненты	- список IP-адресов абонентов, к которым клиенты могут запрашивать доступ при соединении с ФПСУ. Этот список будет передаваться клиентам при установке туннеля и дополнять их собственные списки абонентов.
Локальные настройки	- устанавливаемые для ФПСУ-IP/Клиентов локальные настройки, передаются с ФПСУ в момент соединения с ФПСУ-IP/Клиентом;

Параметр	Описание параметра
Контроль соединения	- временной интервал (от 1 до 10 минут), по истечении которого после получения последних данных от клиента ФПСУ будет производить контроль соединения с ним. В случае отсутствия связи соединение будет сброшено. Для клиентов RKL-Криптосети временной интервал (от 1 до 255 минут), поле может быть пустым, если контроль не требуется. Данная опция важна для тех каналов, в которых происходят частые обрывы связи (например, PPP). В сочетании с опциями ПАК ФПСУ-IP/Клиент «Помнить введенный Pin-код пока VPN-Key не отсоединен» и «Автосоединение при подключении VPN-Key» (подробнее см. руководство пользователя ФПСУ-IP/Клиента) позволяет при таких разрывах автоматически восстанавливать туннель между Клиентом и ФПСУ;
Описание активно	- указание ФПСУ на активность описания. Если флаг не установлен в положение «X», работа клиентов данного диапазона будет блокирована. Флаг включается и выключается при помощи клавиши *<Пробел>*.

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

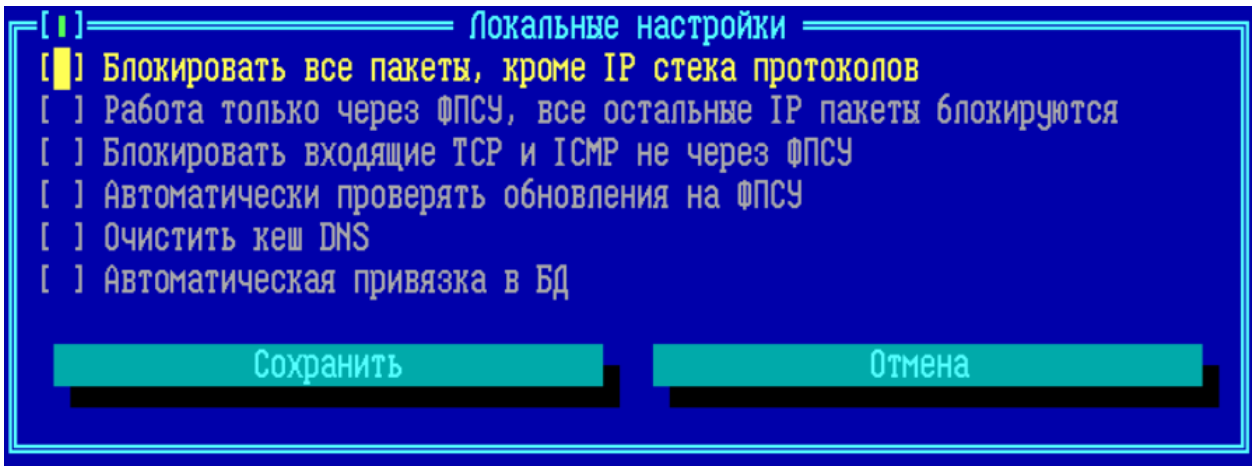


Рисунок 450 - Локальные настройки ФПСУ-IP/Клиента, устанавливаемые на ФПСУ

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

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

Блокировать входящие TCP и ICMP не через ФПСУ – установленный флаг означает, что ФПСУ-IP/Клиент после установления соединения с ФПСУ будет блокировать новые входящие TCP и ICMP-соединения, если они пришли не из туннеля к ФПСУ (исключение: входящие соединения FTP-data разрешаются).

Автоматически проверять обновления на ФПСУ – флаг, при установке которого при каждом соединении с ФПСУ (основным или дополнительным) ФПСУ-IP/Клиент будет запрашивать у него наличие новых версий программного обеспечения ФПСУ-IP/Клиента.

Очистить кэш DNS – флаг, при установке которого выполняется сброс кэша DNS на рабочей станции ФПСУ-IP/Клиента при установлении соединения с ФПСУ.

Автоматическая привязка в БД – установленный флаг позволяет привязать Клиента к рабочей станции или устройству с установленным программным обеспечением ФПСУ-IP/Клиент, чтобы пользователь мог работать с этим Клиентом только на одном АРМ. Привязка клиента хранит данные о серийных номерах ОС (только для Windows), материнской платы и системного диска устройства с установленным программным обеспечением ФПСУ-IP/Клиент в базе данных на ФПСУ. Каждый раз при подключении ФПСУ-IP/Клиента к ФПСУ эти данные сверяются, в случае подключения клиента с другого устройства работа данного клиента блокируется. База данных с привязками клиентов синхронизируется с дополнительным ФПСУ, заданным в настройках ФПСУ-IP/Клиента.

Нажатие кнопки *«Сохранить»* или клавиши *<F2>* сохраняет локальные настройки и возвращает в окно описания диапазона номеров группы клиентов.

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

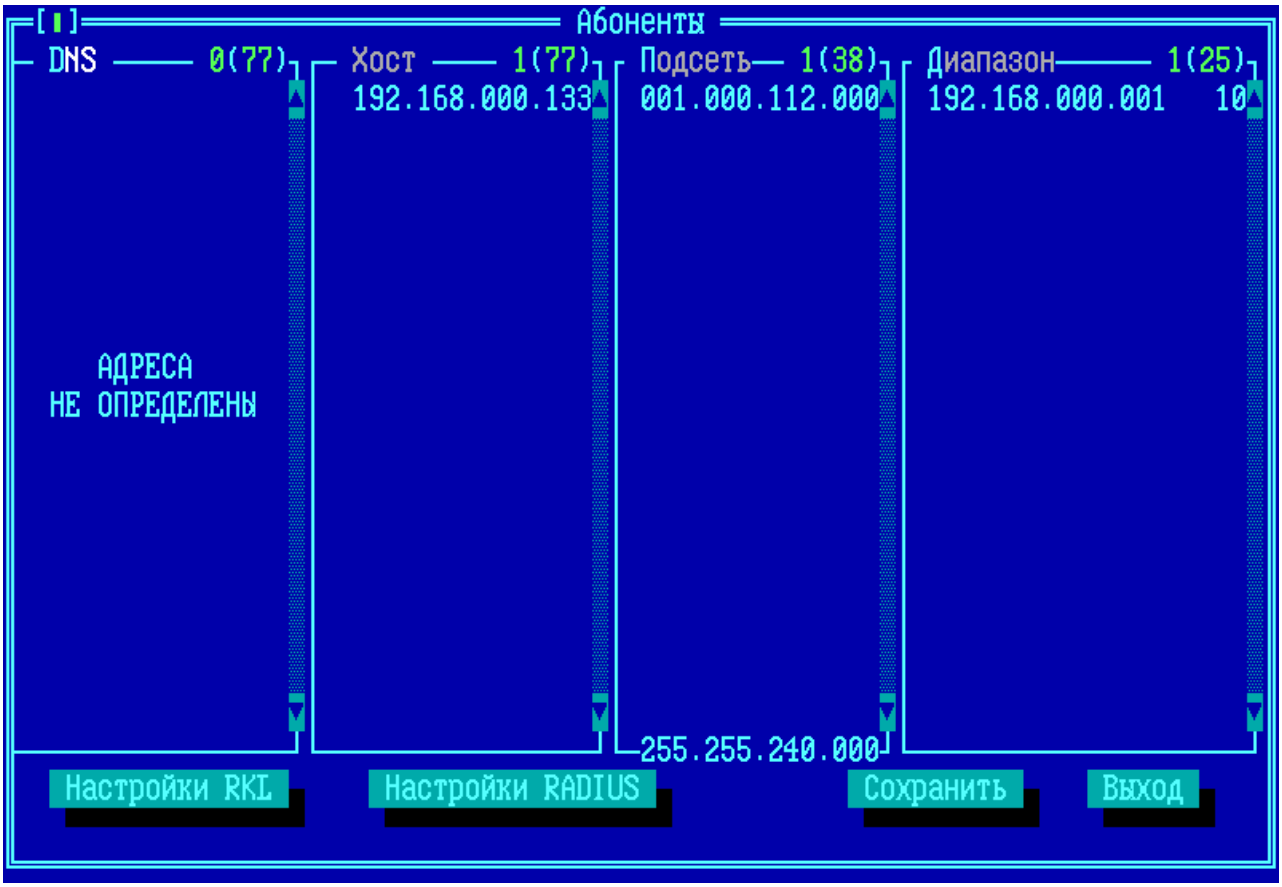


Рисунок 451 - Абоненты ФПСУ, доступные ФПСУ-IP/Клиенту

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

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

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

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

Сервер лицензирования доступен в сети (см. пункт «Настройка диапазона клиентов на работу с Сервером лицензирования»).

Настройки RADIUS – устанавливаются для аутентификации ФПСУ-IP/Клиентов в сети (см. пункт «Настройка диапазона клиентов на работу с Radius»).

После установки всех параметров в окне «Абоненты» нажмите кнопку «*Сохранить*», после чего будет произведен выход в окно списка описаний клиентов в группе.



Рисунок 452 - Список описаний диапазонов Клиентов

Для перехода к форме списка описаний отдельного клиента нажмите клавишу <*Пробел*>.

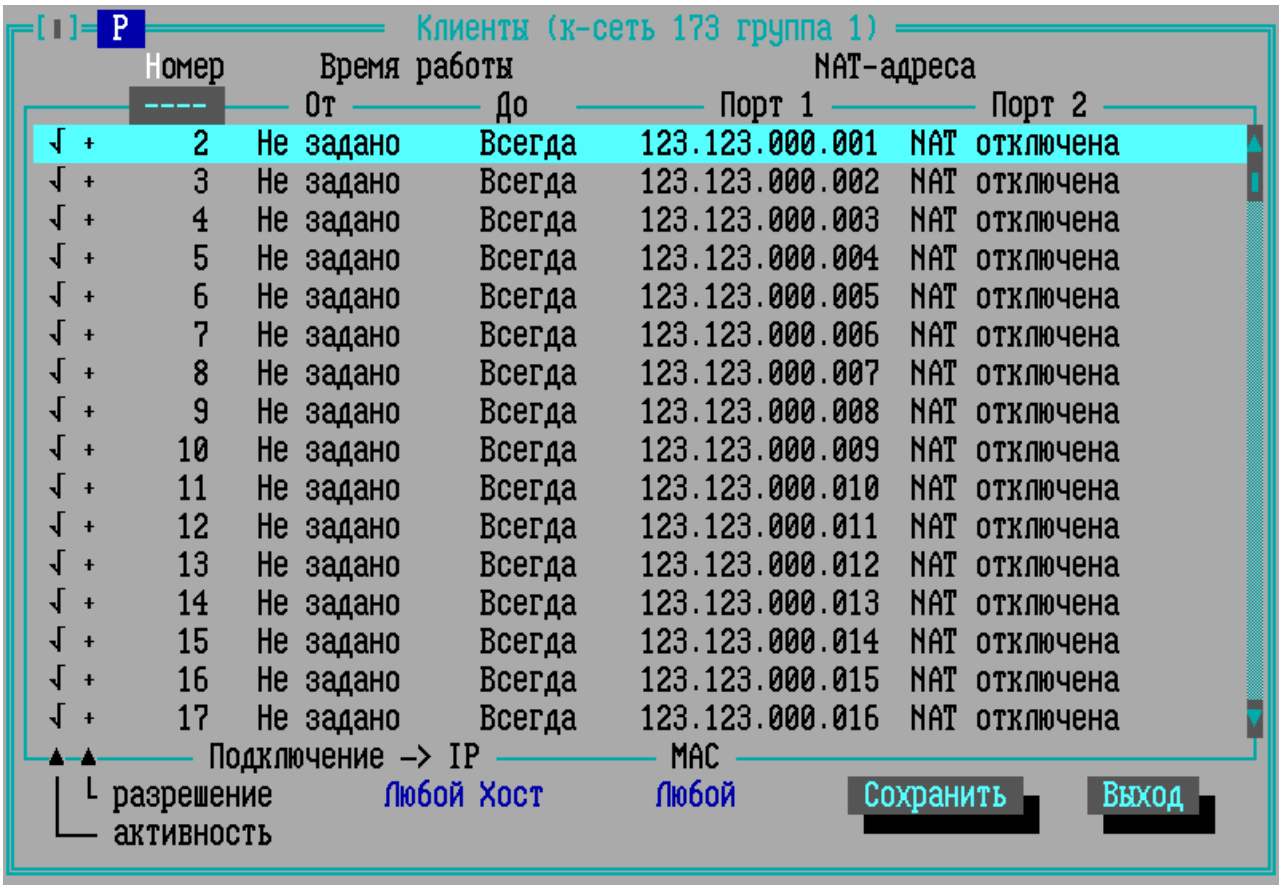


Рисунок 453 - Список зарегистрированных в группе Клиентов

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

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

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

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

12. 1. 4. RKL для обновления ключевых данных клиентов

Настройки RKL доступны на ФПСУ с установленной подсистемой RKL, позволяют проводить удаленную загрузку ключевых данных клиентов с ФПСУ на устройства с установленным ПО ФПСУ-IP/Клиент.

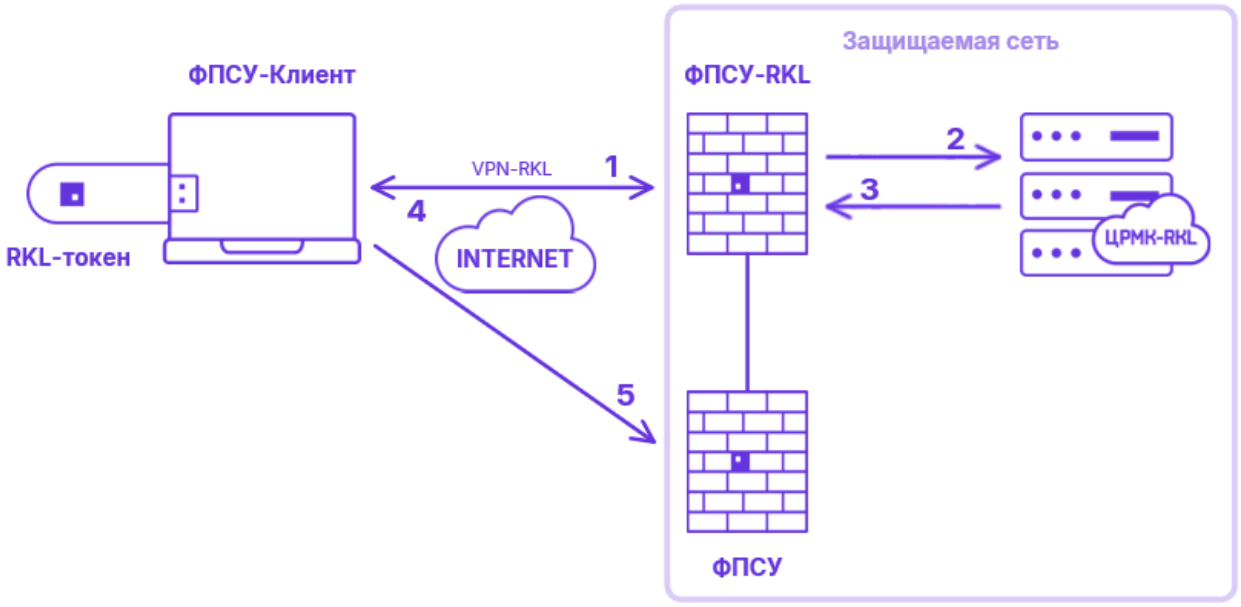
Удаленная загрузка ключевых данных проводится в двух режимах, получения/обновления ключевых данных по запросу с использованием RKL-токена и автоматического обновления ключевых данных целевого VPN-профиля при обнаружении новой серии ключевых данных на ФПСУ.

При получении/обновлении ключевых данных по запросу необходимо подключение RKL-токена в USB-порт рабочей станции или устройства с установленным программным обеспечением ФПСУ-IP/Клиент. ФПСУ-IP/Клиент осуществляет взаимодействие с ФПСУ-RKL, все другие соединения блокируются. Взаимодействие осуществляется по следующей схеме:

- ФПСУ-IP/Клиент с RKL-токеном запрашивает ключевые данные для целевого VPN-профиля у ФПСУ-RKL.
- В расширенном режиме ФПСУ-RKL запрашивает разрешение получения/обновления ключевых данных целевого VPN-профиля на ЦРМК-RKL.
- ЦРМК-RKL разрешает получение/обновление ключевых данных.
- ФПСУ-RKL выдает новый ключ ФПСУ-IP/Клиенту и ключ устанавливается на ФПСУ-IP/Клиенте.
- RKL-токен извлекается, ФПСУ-IP/Клиент устанавливает соединение с ФПСУ-IP на новой серии ключа целевого VPN-профиля.

В расширенном схеме взаимодействия ЦРМК-RKL позволяет вести учет ключевых данных для устройств с установленным ПО ФПСУ-IP/Клиент. ЦРМК-RKL хранит данные о ФПСУ-IP/Клиенте, его VPN-профиле, выданных ключевых данных.

В упрощенной схеме взаимодействия запрос ключевых данных не перенаправляется на ЦРМК-RKL, учет ключевых данных не ведётся (шаги 2,3 на схеме исключаются).

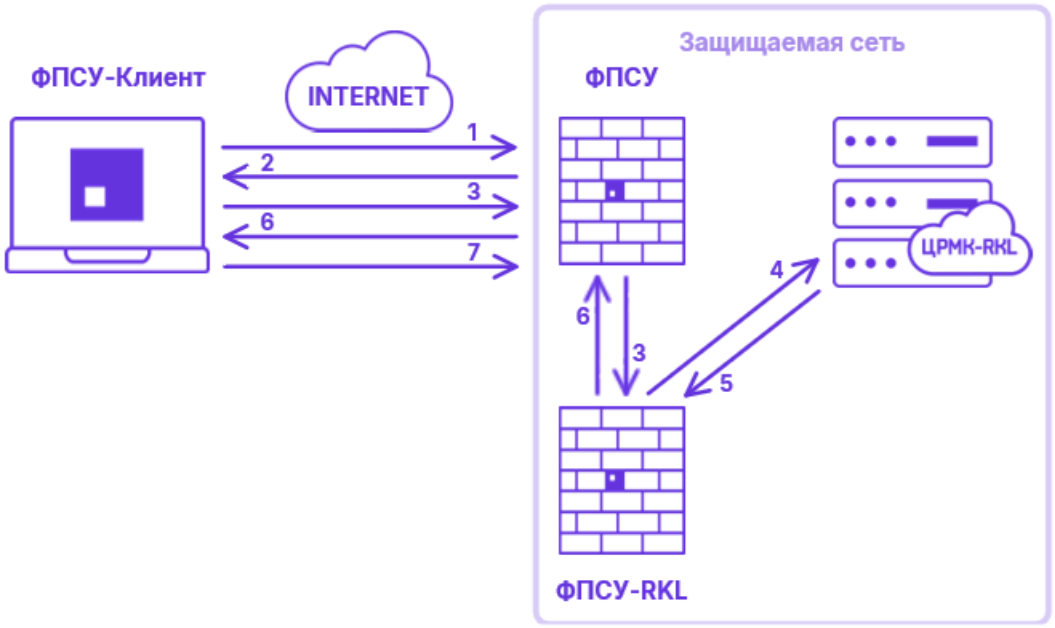


1 ФПСУ -Клиент с RKL-токеном запрашивает у ФПСУ-RKL получение или обновление ключа
2 ФПСУ-RKL запрашивает разрешение выдать ключ на ЦРМК-RKL
3 ЦРМК-RKL разрешает выдачу ключа
4 ФПСУ-RKL выдает ключ ФПСУ-Клиенту и ключ устанавливается на ФПСУ-Клиенте
5 После извлечения RKL-токена ФПСУ-Клиент устанавливает соединение с ФПСУ на новой серии ключа

Рисунок 454 - Схема получения/обновления ключа по запросу с RKL-токеном

При автоматическом обновлении ключевых данных ФПСУ-IP/Клиент запрашивает обновление ключа у ФПСУ-RKL при обнаружении новой серии ключевых данных на ФПСУ. ФПСУ-IP/Клиент осуществляет взаимодействие с ФПСУ-RKL через ФПСУ. Взаимодействие осуществляется по следующей схеме:

- ФПСУ-IP/Клиент устанавливает соединение с ФПСУ.
- ФПСУ сообщает о наличии новой серии ключа.
- ФПСУ-IP/Клиент запрашивает у ФПСУ-RKL смену ключевых данных, ФПСУ перенаправляет запрос ФПСУ-RKL.
- ФПСУ-RKL запрашивает разрешение выдать ключ на ЦРМК-RKL.
- ЦРМК-RKL разрешает обновление ключа.
- ФПСУ-RKL выдает ключ ФПСУ-IP/Клиенту через канал с ФПСУ и ключ устанавливается на ФПСУ-IP/Клиенте.
- ФПСУ-IP/Клиент устанавливает соединение с ФПСУ-IP на новой серии ключа.



1 ФПСУ-Клиент устанавливает соединение с ФПСУ
2 ФПСУ сообщает о наличии новой серии ключ
3 ФПСУ-Клиент запрашивает у ФПСУ-RKL смену ключа, ФПСУ перенаправляет запрос ФПСУ-RKL
4 ФПСУ-RKL запрашивает разрешение выдать ключ на ЦРМК-RKL
5 ЦРМК-RKL разрешает обновление ключа
6 ФПСУ-RKL выдает ключ ФПСУ-Клиенту через ФПСУ и ключ устанавливается на ФПСУ-Клиенте
7 ФПСУ-Клиент устанавливает соединение с ФПСУ на новой серии ключа

Рисунок 455 - Схема автоматического обновления ключа («зацепление»)

Рекомендуемый порядок действий при настройке:

Подсистема RKL для работы с ЦРМК и сервером лицензирования требует установки аддона rkl.

Настройка клиентов RKL-токенов требуется только при получении/обновлении ключевых данных с подключением RKL-токена.

1. Построить туннель между ФПСУ и ФПСУ-RKL (см. раздел «Описание параметров туннелей с другими ФПСУ»).

2. В упрощенном режиме на ЦГКК, в расширенном режиме на ЦРМК зарегистрировать две Криптосети Клиентов, одну с признаком RKL для клиентов RKL-токенов, другую для целевых клиентов с VPN-Key. Изготовить VPN-ключи для клиентов этих Криптосетей.

на ФПСУ-RKL:

3. Установить подсистему RKL, для расширенного режима установить дополнение rkl. Описание установки приведено в пункте «Установка дополнений/изменений». Должна быть предустановлена подсистема CLIENT.

4. Загрузить общесистемные ключевые данные RKL-Криптосети Клиентов и целевой Криптосети Клиентов (см. пункт «Установка и удаление общесистемных ключей»).

5. Создать группы клиентов этих Криптосетей (см. пункт «Описание логической группы клиентов»).

6. В группе RKL-Криптосети задать клиентов RKL-токенов и установить для них настройки RKL (см. пункты «Установка правил работы клиентов» и «Настройка диапазона клиентов на работу с RKL»).

7. В группе целевой Криптосети задать клиентов VPN-Key и установить для них настройки RKL.

8. Для расширенного режима настроить ЦРМК, Сервер лицензирования (опционально). В меню выбрать пункт «Сетевые сервисы → Серверы ЦРМК», задать URL ЦРМК для группы или диапазона групп целевой Криптосети, задать IP-адрес и порт Сервера лицензирования (опционально). Описание приведено в пункте «Серверы ЦРМК и Сервер лицензирования».

на ФПСУ целевом:

9. Должна быть предустановлена подсистема CLIENT.

10. Загрузить общесистемные ключевые данные целевой Криптосети Клиентов.

11. Создать группу клиентов целевой Криптосети.

12. В группе целевой Криптосети задать клиентов VPN-Key и установить для них настройки RKL.

12. 1. 4. 1. Настройка диапазона клиентов на работу с RKL

В зависимости от используемой схемы обновления ключевых данных на ФПСУ-IP/Клиентах (см. пункт «RKL для обновления ключевых данных клиентов») установите на целевом ФПСУ и на ФПСУ-RKL настройки RKL для клиентов VPN-Key и клиентов RKL-токенов.

В окне «Настройки RKL для диапазона» на вкладке «RKL» доступны следующие параметры:

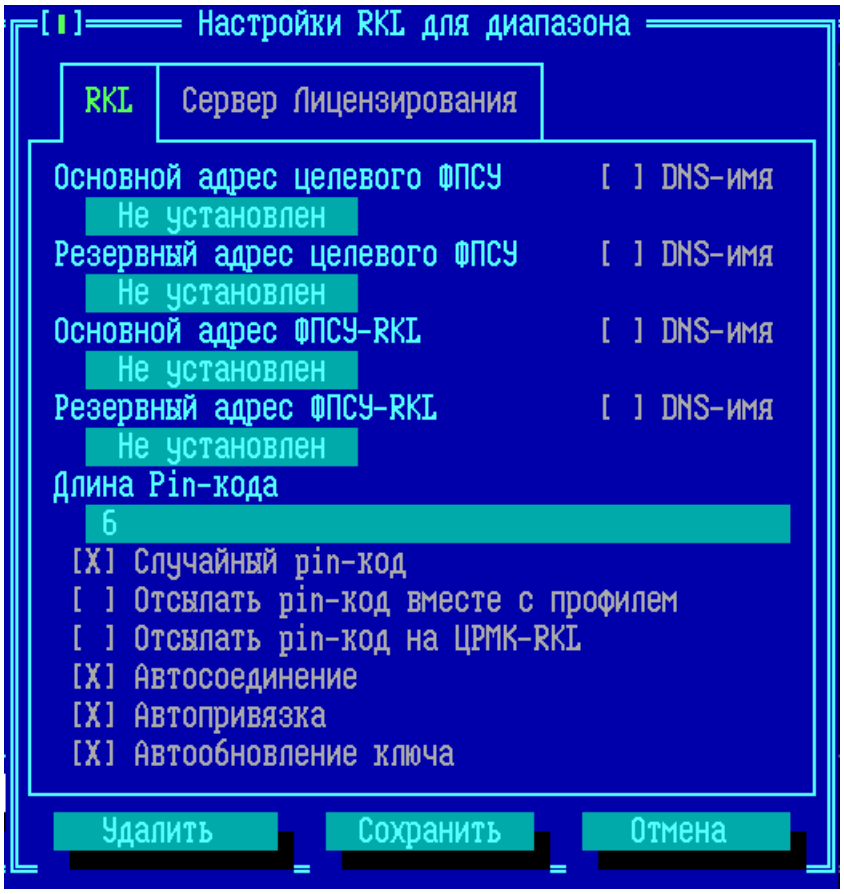


Рисунок 456 - Настройки RKL

Основной адрес целевого ФПСУ – в поле необходимо ввести IP-адрес ФПСУ, через который будет осуществляться доступ ФПСУ-IP/Клиента к защищенным хостам.

DNS-имя – флаг, позволяющий вместо указания IP-адреса ФПСУ сохранить в настройках DNS-имя. Служба DNS должна поддерживаться устройством с установленным ПО ФПСУ-IP/Клиент. В этом случае перед установлением соединения ФПСУ-IP/Клиента с ФПСУ будет каждый раз выполняться DNS-запрос на получение IP-адреса ФПСУ у обслуживающего данное устройство DNS-сервера.

Резервный адрес целевого ФПСУ – в поле необходимо ввести IP-адрес дополнительного ФПСУ, если в локальной сети имеется еще один ФПСУ, который может предоставить доступ ФПСУ-IP/Клиенту в случае отсутствия связи с основным.

Основной адрес ФПСУ-RKL – в поле необходимо ввести IP-адрес ФПСУ, через который будет осуществляться взаимодействие целевого ФПСУ с ЦРМК-RKL.

Резервный адрес ФПСУ-RKL – в поле необходимо ввести IP-адрес дополнительного ФПСУ, через который будет осуществляться взаимодействие целевого ФПСУ с ЦРМК-RKL в случае отсутствия связи с основным.

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

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

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

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

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

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

Автообновление ключа – флаг, позволяет планово (1 раз в год) удаленно обновлять общесистемные ключи на устройстве с установленным ПО ФПСУ-IP/Клиент. Для обновления ключей достаточно выпустить новую серию общесистемных ключей. К моменту наступления срока обновления ключа на ЦГКК должен быть создан общесистемный ключ новой серии, на целевом ФПСУ и ФПСУ-RKL должны быть установлены две серии ключей текущая и новая, выработанная на ЦГКК. Для ФПСУ-IP/Клиента при соединении с целевым ФПСУ проверяется наличие новой серии ключей на целевом ФПСУ. В случае если новая серия обнаружена, ФПСУ-IP/Клиент обращается к ФПСУ-RKL с запросом обновления ключей. При наличии на ФПСУ-RKL новой серии ключей для клиента запрос перенаправляется в ЦРМК-RKL. ЦРМК-RKL выдает разрешение на обновление ключей. На ФПСУ-IP/Клиенте обновляется серия общесистемных ключей без участия Администратора. Клиент пересоединяется с ФПСУ, используя новую серию ключа.

Нажатие кнопки *«Сохранить»* или клавиши *<F2>* сохраняет настройки вкладок RKL и Сервера лицензирования и возвращает в окно описания абонентов для диапазона номеров. Сбросить установленные настройки можно по нажатию кнопки *«Удалить»* или клавиши *<Del>*, отменить внесенные изменения – по нажатию кнопки *«Отмена».*

12. 1. 4. 2. Настройка диапазона клиентов на работу с Сервером лицензирования

Сервер лицензирования используется для учета и выдачи программных лицензий ФПСУ-IP/Клиентов.

Настройки Сервера лицензирования позволяют проводить автоматическую удаленную загрузку лицензий до истечения срока действия с Сервера лицензирования на устройства с установленным ПО ФПСУ-IP/Клиент.

Удаленная загрузка лицензий проводится в двух режимах, получения лицензии по запросу с использованием RKL-токена и автоматического обновления лицензии при истечении срока действия лицензии.

При получении лицензии по запросу необходимо подключение RKL-токена в USB-порт рабочей станции или устройства с установленным программным обеспечением ФПСУ-IP/Клиент. ФПСУ-IP/Клиент осуществляет взаимодействие с ФПСУ-RKL, все другие соединения блокируются. Взаимодействие осуществляется по следующей схеме:

- ФПСУ-IP/Клиент с RKL-токеном устанавливает защищенное соединение с ФПСУ-RKL.
- ФПСУ-IP/Клиент запрашивает лицензию у ФПСУ-RKL.
- ФПСУ-RKL отправляет запрос на получение лицензии на Сервер лицензирования.
- Сервер лицензирования выдает лицензию ФПСУ-IP/Клиенту.

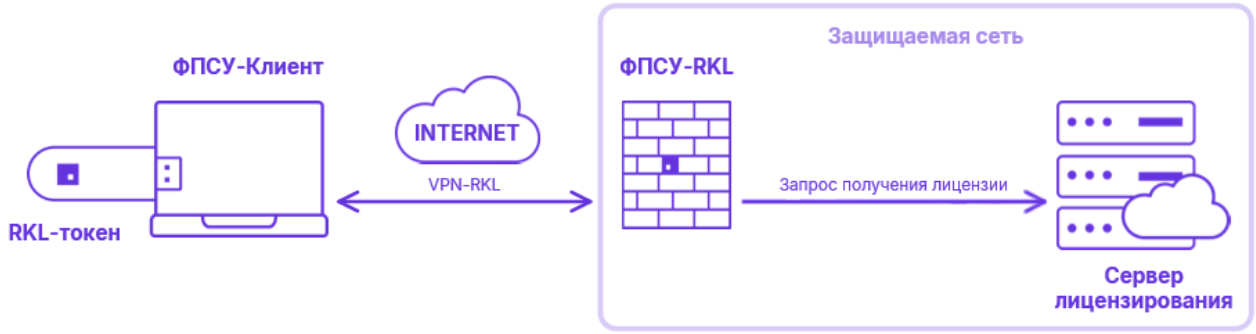


Рисунок 457 - Схема получения лицензии с Сервера лицензирования

При автоматическом обновлении лицензии ФПСУ-IP/Клиент в момент подключении к ФПСУ проверяется срок истечения лицензии, запрос обновления лицензии отправляется с ФПСУ за указанное количество дней до окончания поддержки на Сервер лицензирования. Сервер лицензирования выдает лицензию ФПСУ-IP/Клиенту. На ФПСУ-IP/Клиенте обновляется лицензия.

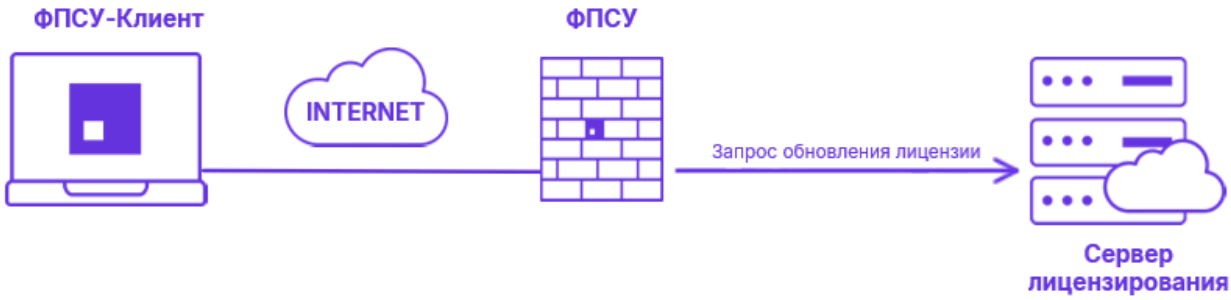


Рисунок 458 - Схема обновления лицензии с Сервера лицензирования

В зависимости от используемого режима получения или обновления лицензии на ФПСУ-IP/Клиентах установите на ФПСУ или/и на ФПСУ-RKL настройки Сервера лицензирования и в пункте меню «Сетевые сервисы → Серверы ЦРМК» (см. пункт «Серверы ЦРМК и Сервер лицензирования»)..

В окне «Настройки RKL для диапазона» на вкладке «Сервер лицензирования» доступны следующие параметры:

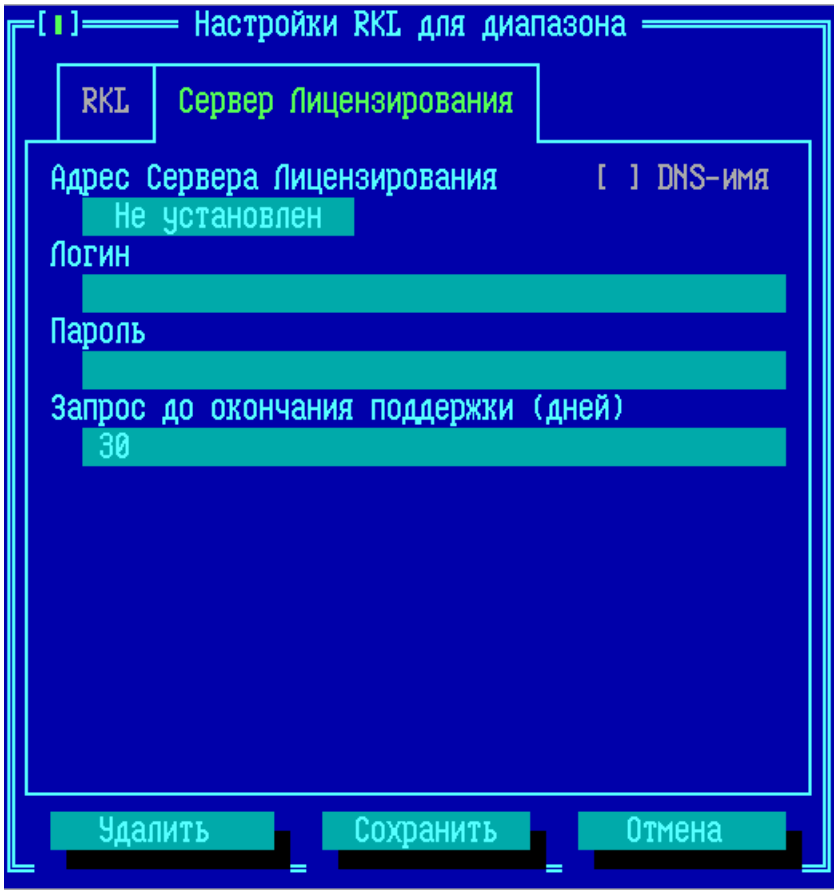


Рисунок 459 - Настройки RKL. Вкладка Сервер Лицензирования

Адрес Сервера лицензирования – в поле необходимо ввести IP-адрес Сервера лицензирования или ФПСУ-RKL при использовании ЦРМК-RKL.

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

На Сервере лицензирования может быть установлена аутентификация, заданы ***Логин*** и ***Пароль***, для получения Клиентом лицензии.

Запрос до окончания поддержки – При старте ФПСУ-IP/Клиент проверяет дату окончания поддержки лицензии. За указанный период до её окончания отправляется запрос на Сервер лицензирования для автоматического обновления лицензии, по умолчанию за 30 дней.

Нажатие кнопки *«Сохранить»* или клавиши *<F2>* сохраняет настройки вкладок RKL

и Сервера лицензирования и возвращает в окно описания абонентов для диапазона номеров. Сбросить установленные настройки можно по нажатию кнопки *«Удалить»* или клавиши <*Del*>, отменить внесенные изменения – по нажатию кнопки *«Отмена»*.

12. 1. 4. 3. Серверы ЦРМК и Сервер лицензирования

Для расширенного режима при получении/обновлении ключевых данных требуется организовать взаимодействие с ЦРМК, необходимо указать сервер ЦРМК на ФПСУ-RKL.

При автоматическом удаленном получении/обновлении лицензий лицензии загружаются с Сервера лицензирования, в зависимости от схемы взаимодействия с сервером необходимо указать Сервер лицензирования на ФПСУ и/или на ФПСУ-RKL. Схемы взаимодействия с сервером описаны в пункте «Настройка диапазона клиентов на работу с Сервером лицензирования».

Настройка сервера ЦРМК и Сервера лицензирования выполняется из пункта меню «Сетевые сервисы → Серверы ЦРМК».

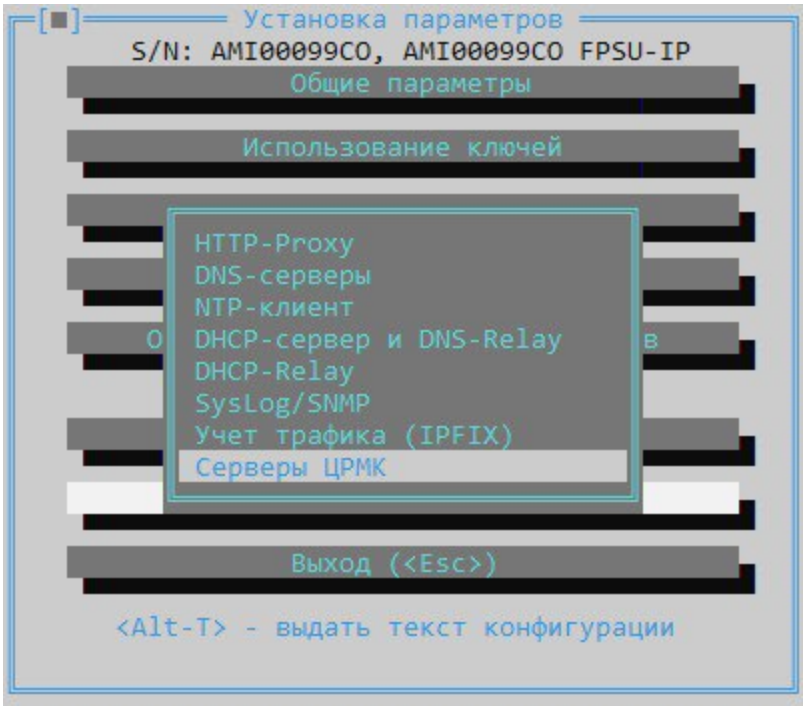


Рисунок 460 - Меню подсистемы конфигурирования ФПСУ

Для задания Сервера лицензирования в поле «Сервер лицензий» следует ввести IP-адрес сервера и порт подключения к серверу.

Для задания сервера ЦРМК необходимо задать диапазон групп целевой Криптосети и напротив ввести URL сервера ЦРМК.

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*».

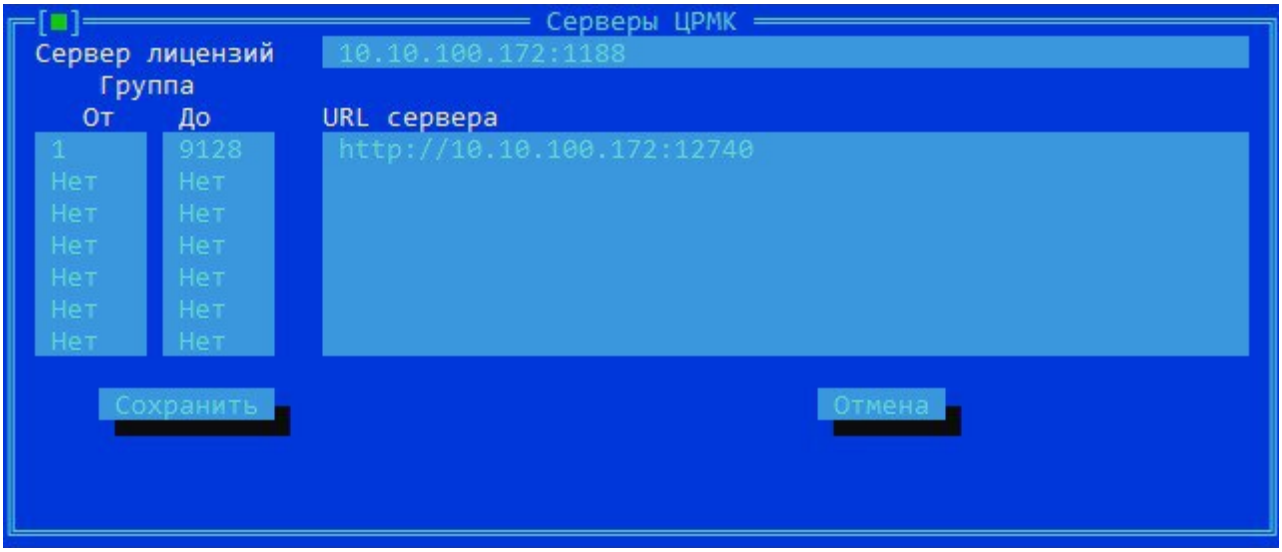


Рисунок 461 - Настройка ЦРМК и Сервера лицензирования

12. 1. 5. 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:

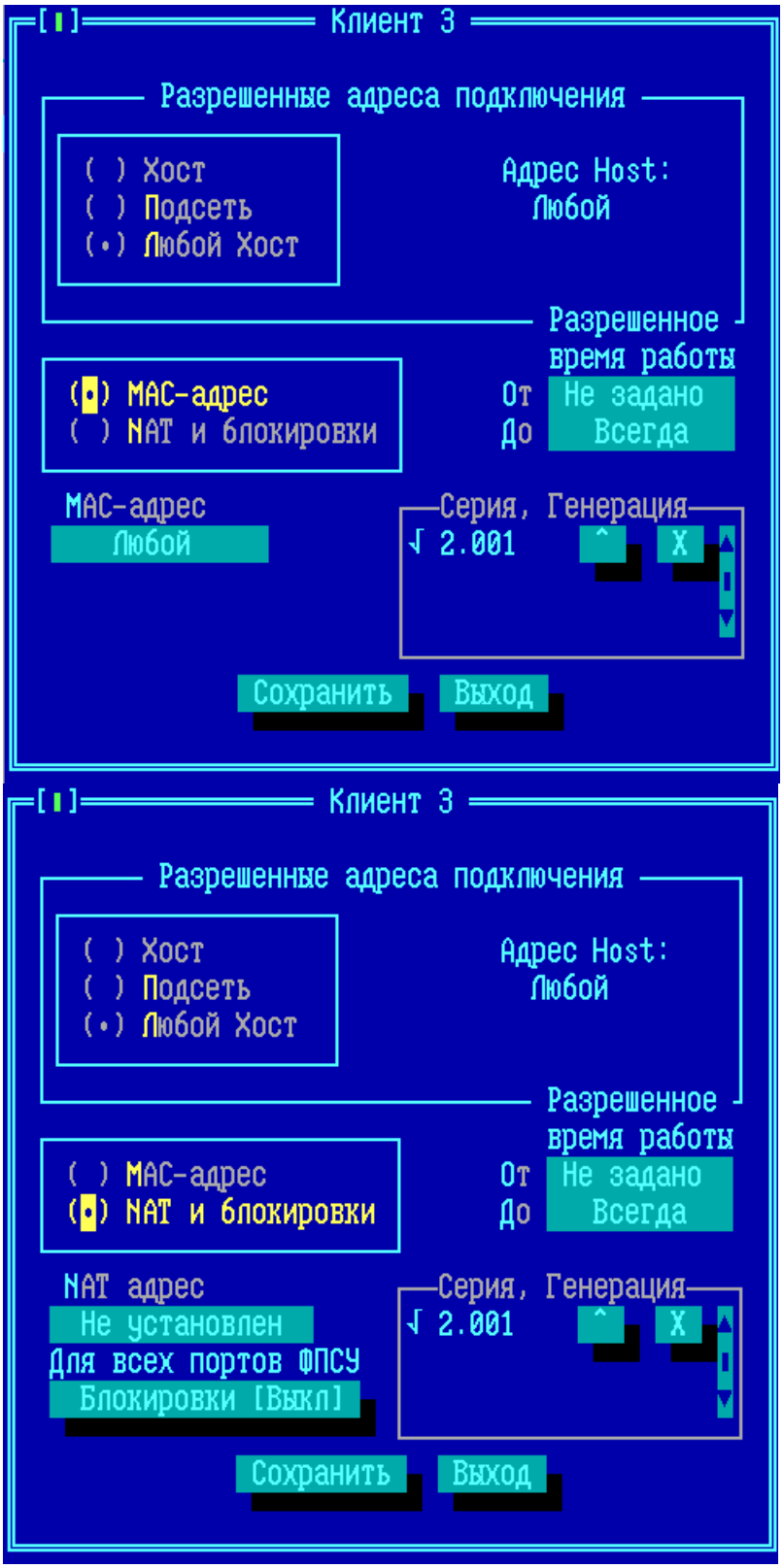


Рисунок 462 - Параметры работы отдельного Клиента

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

- *Хост* – Клиенту разрешено подключение только с одного указанного IP-адреса;
- *Подсеть* – Клиенту разрешено подключение только из указанной IP-подсети;
- *Любой хост* – настройка по умолчанию, Клиенту разрешено подключение к ФПСУ 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.

Серия – уникальный числовой идентификатор общесистемного ключа Криптосети.

Генерация – уникальный числовой идентификатор ключа Клиента, от 1 до 256.

Серия и генерация отображаются в виде X.YYY, где X - номер серии, YYY - номер генерации.

Знак «√» слева от серии ключа означает, что ключ Клиента Криптосети с данной серией и генерацией используется для установления соединения ФПСУ-IP/Клиента и ФПСУ.

В случае компрометации ключа Клиента необходимо сменить ключ Клиента, повысив номер генерации. Для увеличения номера генерации на единицу выделите кнопку «^» курсором и нажмите <*Enter*>. Данная операция необратима. Ключ Клиента со старым номером генерации блокируется.

В случае компрометации общесистемного ключа Криптосети необходимо сменить общесистемный ключ, для этого установить запрет на использование текущей серии и повысить номер серии. Для запрета серии ключа Криптосети выделите кнопку «***X***» курсором и нажмите <*Enter*>. Данная операция необратима. Смена серии общесистемного ключа производится на ЦГКК, подробно описана в руководстве «Центр генерации ключей клиентов» (процедуры установки полученного от администратора ЦГКК нового общесистемного ключа - см. пункт «Установка и удаление общесистемных ключей»).

MAC-адрес – флаг, при включении которого можно ограничить подключение клиента с только определенного MAC-адреса, указав ниже в поле «*MAC адрес*» ожидаемое значение физического адреса, с которого приходят IP-пакеты Клиента.

При установленном флаге «*MAC-адрес*» не работают настройки, ранее выполненные в полях «*NAT и блокировки*» (см. далее).

NAT и блокировки – флаг, при включении которого можно указать исключения в работе данного Клиента из общих настроек, сделанных в описании диапазона Клиентов (см. пункт «Установка правил работы клиентов»).

При установленном флаге «*NAT и блокировки*» в поле ***NAT адрес*** может быть указан транслируемый IP-адрес (NAT) для данного Клиента, если требуется для отдельного Клиента ФПСУ выдать отдельный NAT адрес, отличающийся от заданного в описании диапазона Клиентов.

При включенном флаге «*NAT и блокировки*» также могут быть указаны отличные от выставленных в описании всего диапазона Клиентов блокировки. Для этого выполните переход в окно индивидуальных блокировок, под надписью ***Для всех портов ФПСУ*** нажав кнопку «*Блокировки*».

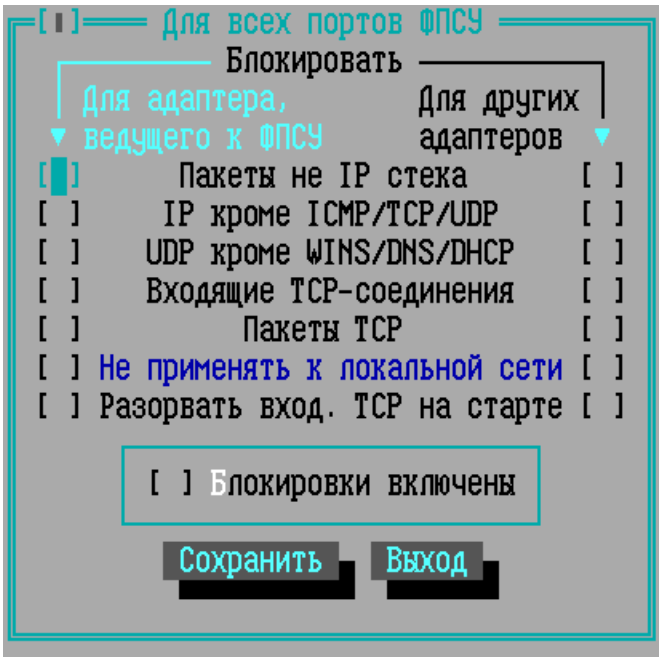


Рисунок 463 - Индивидуальные блокировки Клиента

В окне индивидуальных блокировок отдельного Клиента, при установлении флага «*Блокировки включены*», к данному клиенту будут применены указанные в этом окне параметры фильтрации трафика, полностью заменяя находящиеся в описании диапазона Клиентов (см. пункт «Установка правил работы клиентов») блокировки. Указанные блокировки будут действовать вне зависимости от того, с каким портом ФПСУ соединился Клиент.

При установленном флаге «*NAT и блокировки*» не работают ранее выполненные настройки, указанные в поле «*MAC адрес*».

Примечание. Для клиентов типа «VPNPROGRAM» такой вид дополнительной настройки блокировок недоступен.

12. 2. Настройка диапазона клиентов на работу с Radius

Настройки RADIUS позволяют установить дополнительные требования к аутентификации ФПСУ-IP/Клиентов при попытке соединения с ФПСУ для доступа в защищаемую сеть. Второй фактор аутентификации определяется настройками RADUIS-сервера, ФПСУ в данном случае выступает посредником между ФПСУ-IP/Клиентом и RADUIS-сервером.

Перед настройкой диапазона клиентов на работу с RADIUS, требуется предварительно на ФПСУ создать список используемых RADIUS-серверов (подробнее см. пункт «RADIUS»). Для быстрого перехода в окно задания списка RADIUS-серверов на ФПСУ воспользуйтесь кнопкой ***Редактор серверов***.

Далее, для настройки взаимодействия диапазона подключающихся к ФПСУ клиентов с сервером RADIUS, укажите следующие параметры:

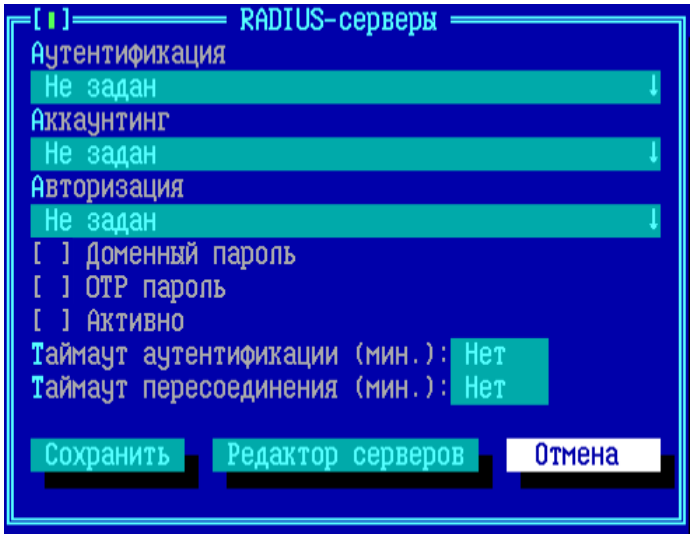


Рисунок 464 - Настройки RADIUS

Для каждого диапазона может быть указано до трех RADIUS-серверов, в зависимости от запрашиваемой у RADIUS-сервера информации. Указанный в настройках ФПСУ RADIUS сервер должен быть настроен на обработку данных от ФПСУ-IP/Клиентов и активен.

Аутентификация – укажите в этом поле RADIUS-сервер, настроенный для проверки учетных данных ФПСУ-IP/Клиентов (подробнее про возможности аутентификации см. дальше по тексту).

Аккаунтинг – укажите в этом поле RADIUS-сервер, настроенный для записи информации об использовании ресурсов ФПСУ-IP/Клиентов.

Авторизация – выбор RADIUS сервера для определения права доступа ФПСУ-IP/Клиентов к определенным сетевым ресурсам.

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

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

Активно – флаг при включении задействует настройки всех указанных в данном окне RADIUS-серверов на ФПСУ.

Возможности взаимодействия с RADUIS-сервером в режиме Аутентификация.

На ФПСУ может использоваться двухфакторная аутентификация ФПСУ-IP/Клиента с использованием доменного логина и пароля (первый фактор), временного OTP-пароля (второй фактор) или иного способа авторизации, в зависимости от настроек RADIUS сервера.

При указании на ФПСУ активного RADUIS-сервера в поле Аутентификация, с подключающихся ФПСУ-IP/Клиентов будет запрашиваться дополнительная информация, в общем случае указываемая пользователями ФПСУ-IP/Клиентов в полях Логин и Пароль (см. ниже).

Флаги ***Доменный пароль*** и ***OTP пароль*** влияют на отображение заголовка окна аутентификации ФПСУ-IP/Клиента, эти флаги не влияют на передаваемые по протоколу RADIUS данные.

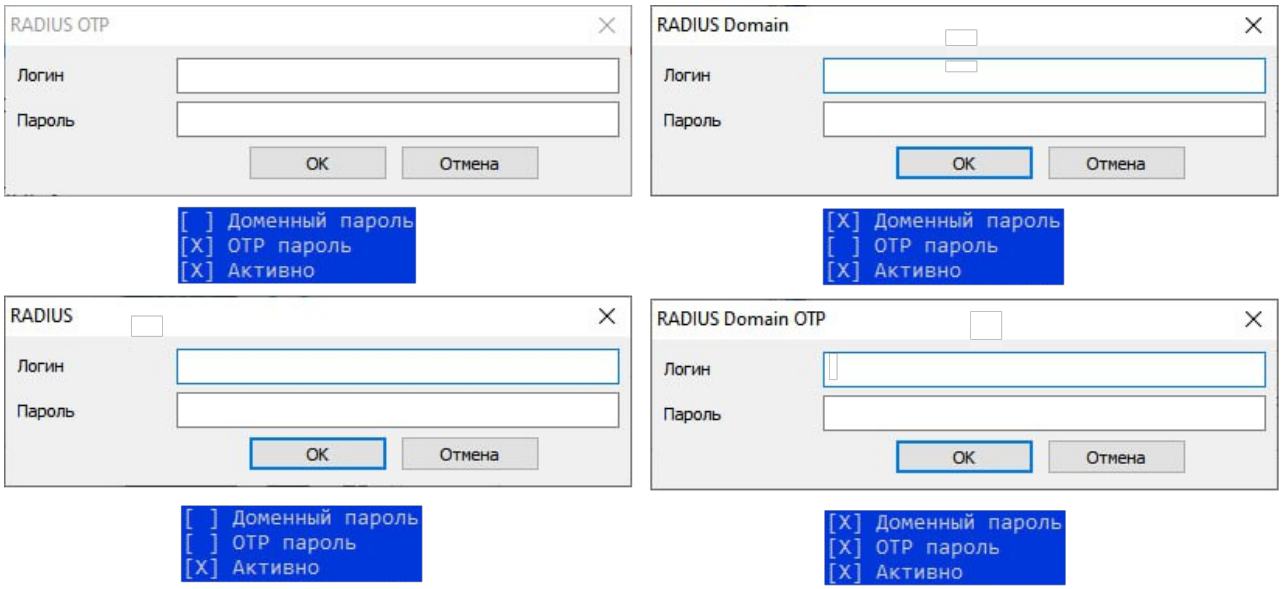


Рисунок 465 - Окно аутентификации ФПСУ-IP/Клиента в зависимости от настроек ФПСУ

Данные, вводимые в окне аутентификации ФПСУ-IP/Клиента, ФПСУ целиком ретранслирует на RADIUS-сервер вне зависимости от установленных флагов ***Доменный пароль*** и ***OTP пароль***. Процесс аутентификации зависит от того, как настроен RADIUS-сервер. Если RADIUS-сервер успешно проверяет и подтверждает данные ФПСУ-IP/Клиента, ФПСУ-IP/Клиент аутентифицируется на ФПСУ и получает доступ к защищаемой сети.

Дополнительные возможности работы с опцией OTP пароль.

При задействовании сервера аутентификации, сервера аккаунтинга и установки флага OTP пароля администратор ФПСУ может разрешить клиенту восстанавливать разорванное соединение без повторного предъявления OTP. В таком случае, клиент может восстановить разорванное соединение с ФПСУ без повторного ввода OTP в течение ***таймаута пересоединения***, если разрыв соединения произошел в течение действия ***таймаута аутентификации***, начинающегося после последнего ввода OTP.

Внимание! Таймаут аутентификации должен быть не меньше ***таймаута пересоединения***.

Таймаут пересоединения – время в минутах с момента разрыва соединения, в течение которого клиенту разрешено восстанавливать соединение с ФПСУ без повторного предъявления OTP.

Таймаут аутентификации – время в минутах с момента последнего ввода пароля и OTP клиентом, в течение которого клиенту разрешено восстанавливать соединение с ФПСУ

без повторного предъявления OTP.

Работа таймаутов на примере:

Установлены таймаут аутентификации - 3 часа (180 минут), таймаут пересоединения - 10 минут. OTP включен, авторизация по паролю включена.

Если клиент пытается восстановить соединение на 7-й минуте после рассоединения и в течение 3-х часов после последнего ввода OTP, то подключится без повторного запроса OTP, поскольку выполняет повторное соединение до истечения обоих таймаутов, и аутентификации и пересоединения.

Если клиент пытается восстановить соединение на 7-й минуте после 3-х часов после последнего ввода OTP, то будет повторно запрашиваться OTP, поскольку истек таймаут аутентификации.

Если клиент пытается восстановить соединение на 12-й минуте после рассоединения, то будет повторно запрашиваться OTP несмотря на состояние таймаута аутентификации, поскольку истек таймаут пересоединения.

Выход из окна настроек работы диапазона клиентов с RADIUS-серверами.

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

12. 3. Балансировка нагрузки Клиентов

Механизм горизонтального масштабирования (балансировка) позволяет распределить нагрузку подключений клиентов на несколько ФПСУ. Механизм балансировки нагрузки позволяет расширять и наращивать производительность системы, увеличивая количества ФПСУ в системе масштабирования и повышает надежность системы. При выходе из строя одного из ФПСУ система автоматически перераспределит нагрузку на работающие узлы. При горизонтальном масштабировании в инфраструктуру добавляется дополнительное отдельное программное или программно-аппаратное решение - балансировщик нагрузки, распределяющий трафик.

В случае с Клиентами (Клиент для ФПСУ или Клиент PKI), технология позволяет равномерно распределять подключающихся Клиентов между несколькими ФПСУ.

Настроенная для использования балансировки нагрузки система может масштабироваться для поддержки более 100 000 одновременных клиентских подключений.

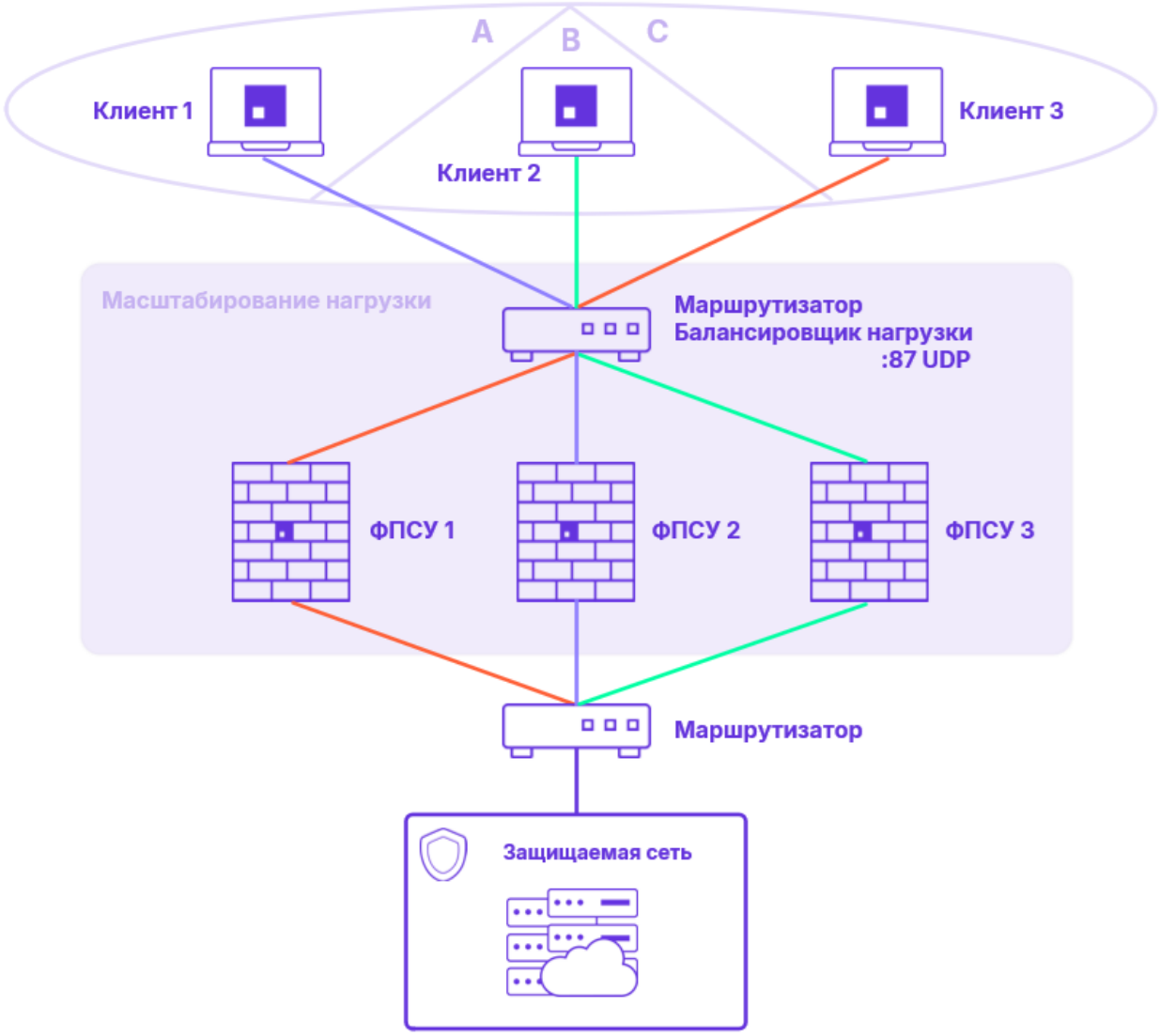


Рисунок 466 - Схема масштабирования нагрузки

В приведенной схеме горизонтального масштабирования (см. рисунок выше) используется балансировщик нагрузки, который является точкой входа для всех VPN-клиентов, ФПСУ-IP/Клиентов. Балансировщик принимает входящие запросы на подключение по UDP-порту 87. Далее балансировщик распределяет входящие запросы между доступными VPN-шлюзами ФПСУ, на основе заданного администратором балансировщика алгоритма (например, Round Robin, Least Connections и т.д.).

ФПСУ обрабатывают соединения от клиентов. Каждый ФПСУ системы масштабирования нагрузки должен быть настроен на работу с клиентами, ожидая входящих соединений клиентов на 87 порт UDP.

Клиент инициирует подключение, отправляя запрос на подключение к IP-адресу

балансировщика по UDP-порту 87. Балансировщик нагрузки получает запрос и, согласно заданному алгоритму распределения, выбирает один из доступных ФПСУ, затем перенаправляет запрос клиента на выбранный ФПСУ.

При установлении соединения ФПСУ принимает запрос на подключение, выполняет установленные администратором процедуры авторизации клиента. В случае успешных проверок идентификации и аутентификации клиента, ФПСУ устанавливает с ним VPN-туннель: клиент и ФПСУ обмениваются ключами шифрования и организуют безопасный канал связи.

После установления туннеля весь трафик клиента передается через выбранный ФПСУ. ФПСУ обеспечивает шифрование/расшифрование и пересылку данных между клиентом и корпоративной сетью или интернетом.

Для обеспечения отказоустойчивости, балансировщик должен быть настроен на выполнение постоянного мониторинга состояния соединений и доступности ФПСУ системы масштабирования. В случае обнаружения отсутствия связи с одним из ФПСУ, балансировщик должен перенаправить новые запросы клиентов на оставшиеся рабочие ФПСУ, обеспечивая отказоустойчивость.

Добавление новых ФПСУ в схему и конфигурацию балансировщика позволяет увеличить пропускную способность системы, что обеспечивает масштабируемость.

Равномерное распределение нагрузки между несколькими ФПСУ помогает предотвращать перегрузку отдельных серверов и обеспечивать более стабильную работу системы клиентских подключений к защищаемой сети.

12. 4. Балансировка нагрузки Клиентов на основе единого IP-адреса

Механизм горизонтального масштабирования (балансировка) позволяет распределить нагрузку подключений клиентов на несколько ФПСУ.

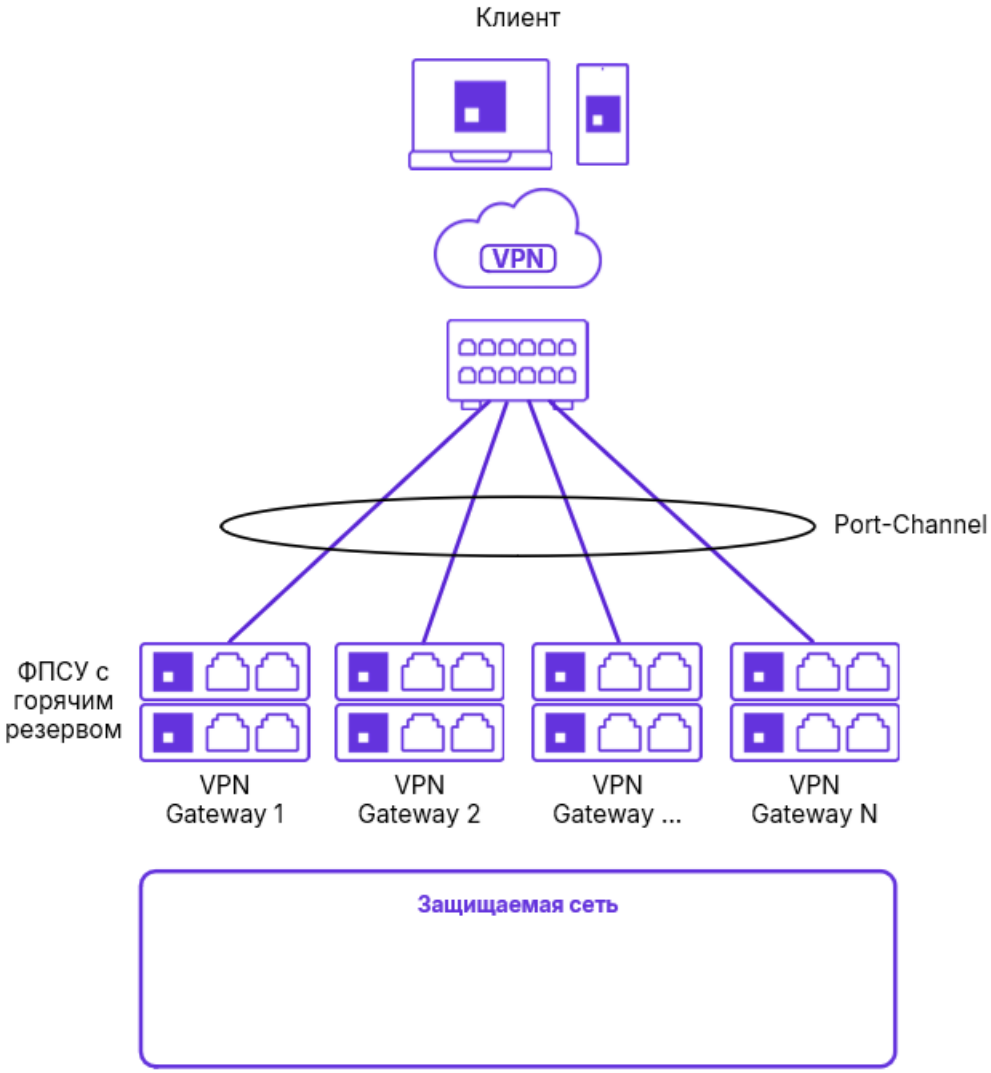


Рисунок 467 - Схема масштабирования нагрузки на основе единого IP-адреса

Рассмотрим схему, при которой VPN-клиенты, клиенты для ФПСУ или клиенты PKI, подключаются через один коммутатор к VPN-шлюзам, ФПСУ. В этой схеме требуется обеспечивать равномерное распределение нагрузки между пятью VPN-шлюзами, а также реализовать отказоустойчивость — если один из шлюзов выйдет из строя, оставшиеся должны автоматически взять на себя его нагрузку, продолжая беспрерывное обслуживание клиентов.

Данная схема позволяет равномерно распределять нагрузку, все VPN-шлюзы обрабатывают трафик в равной степени, что предотвращает перегрузку отдельных узлов и оптимизирует использование ресурсов. Обеспечивается высокая отказоустойчивость, в случае выхода из строя одного из шлюзов его трафик автоматически перераспределяется на другие работающие шлюзы, минимизируя влияние на клиентов. Добавляется гибкость и масштабируемость, схема легко расширяется за счет добавления новых VPN-шлюзов при необходимости увеличения пропускной способности или нагрузки. Данная конфигурация становится надежной, сбалансированной и отказоустойчивой VPN-инфраструктурой, гарантирует стабильную работу и высокую доступность сервиса для всех клиентов.

Для реализации схемы балансировки принципиальным является:

1. Агрегация каналов (Port-Channel)

Все физические интерфейсы на коммутаторе, соединяющие его с VPN-шлюзами, объединены в один логический интерфейс, называемый Port-Channel.

Port-Channel действует как единый высокоскоростной канал для передачи данных, обеспечивая увеличенную пропускную способность и повышенную отказоустойчивость за счет автоматического перераспределения трафика в случае сбоя одного из физических интерфейсов.

2. Единый IP-адрес для всех VPN-шлюзов

Все пять VPN-шлюзов настроены с одинаковым IP-адресом на интерфейсах, подключенных к коммутатору. Этот IP-адрес используется для обслуживания всех подключений клиентов. Данная схема, основанная на использовании единого IP-адреса (Anycast IP), позволяет коммутатору автоматически направлять трафик к любому доступному VPN-шлюзу, обеспечивая распределение нагрузки.

3. Балансировка нагрузки

Коммутатор использует алгоритмы хеширования для равномерного распределения трафика между физическими интерфейсами, входящими в Port-Channel. Хеширование может осуществляться на основе различных параметров пакетов, таких как IP-адреса источника и назначения. Это обеспечивает равномерное распределение нагрузки между всеми VPN-шлюзами, исключая возможность перегрузки одного из них.

4. Мониторинг состояния и отказоустойчивость

Коммутатор постоянно отслеживает доступность каждого VPN-шлюза. Мониторинг может быть реализован с помощью таких механизмов, как IP SLA, BFD или LACP. Если один

из шлюзов выходит из строя (например, перестает отвечать на запросы), коммутатор автоматически исключает его из Port-Channel. Это гарантирует, что трафик будет перенаправлен на оставшиеся работающие шлюзы, обеспечивая беспрерывное обслуживание клиентов.

13. Сетевые сервисы

13. 1. Общие правила разделения потоков

При обмене информацией между двумя ФПСУ, работающими в паре, данные передаются по сети в туннелированном виде, так что любая рабочая станция на пути следования IP пакетов от одного ФПСУ к другому, включая пограничные маршрутизаторы, может «видеть» в их IP-заголовках только IP-адреса отправляющего и получающего ФПСУ и номер IP-протокола, по которому осуществляется обмен между ФПСУ.

Таким образом, если на пути следования пакетов находится пограничный маршрутизатор, конфигурированный на формирование нескольких различных потоков с различными маршрутами следования или ограничения полосы их пропускания (функция «shaping»), этот маршрутизатор не сможет вычленить из пакетов данных необходимую информацию и выполнить указанные функции.

Для устранения этой проблемы и согласования работы ФПСУ 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, 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 выбран UDP). В потоке №1 передаются служебные и пользовательские данные между ФПСУ, если не включен режим разделения потоков.

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 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 конфигурирован на разделение потоков, а один из пограничных маршрутизаторов (или даже все) - не конфигурирован, удаленный ФПСУ получит посылаемые с конфигурируемого ФПСУ данные в IP-пакетах с номером протокола 53 в заголовке пакета (по маршруту,

который конфигурирован на пограничных маршрутизаторах для этого протокола). Установки удаленного ФПСУ по разделению потоков не влияют на выполнение описываемой функции конфигурируемым ФПСУ.

Правила разделения потоков устанавливаются индивидуально для каждого VPN-туннеля, образуемого конфигурируемым ФПСУ с соседними ФПСУ, при описании параметров порта (см. пункт «Описание параметров туннелей с другими ФПСУ»). 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. **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. Поэтому порядок следования общих правил в списке не имеет значения.

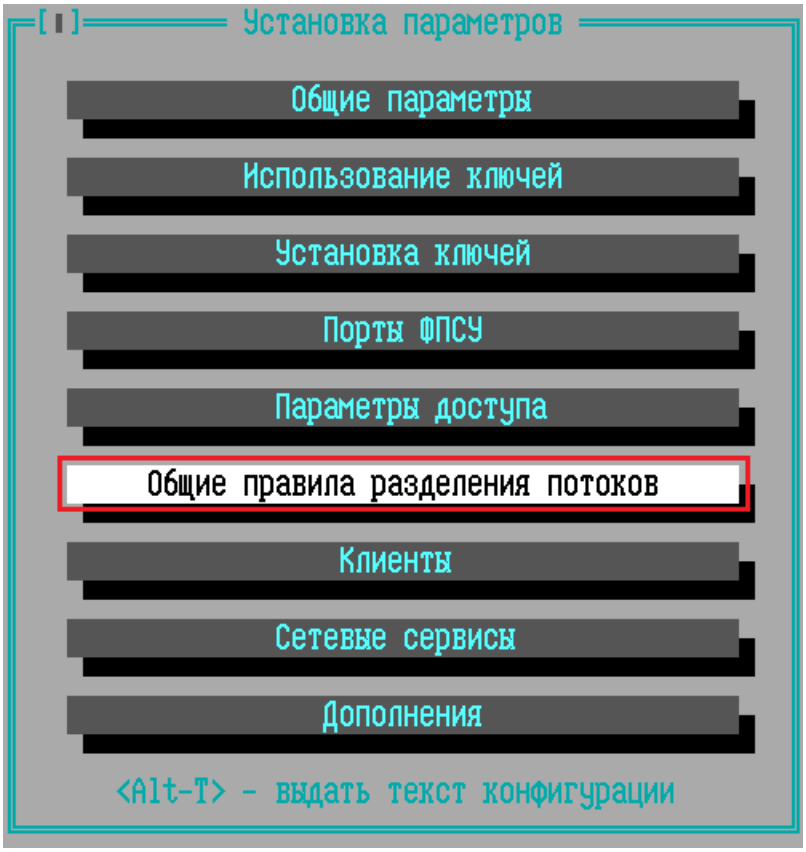


Рисунок 468 - Меню подсистемы конфигурирования ФПСУ

По команде «*Общие правила разделения потоков*» на экране отображается окно, содержащее список установленных общих правил или пустое, если правила еще не описывались.

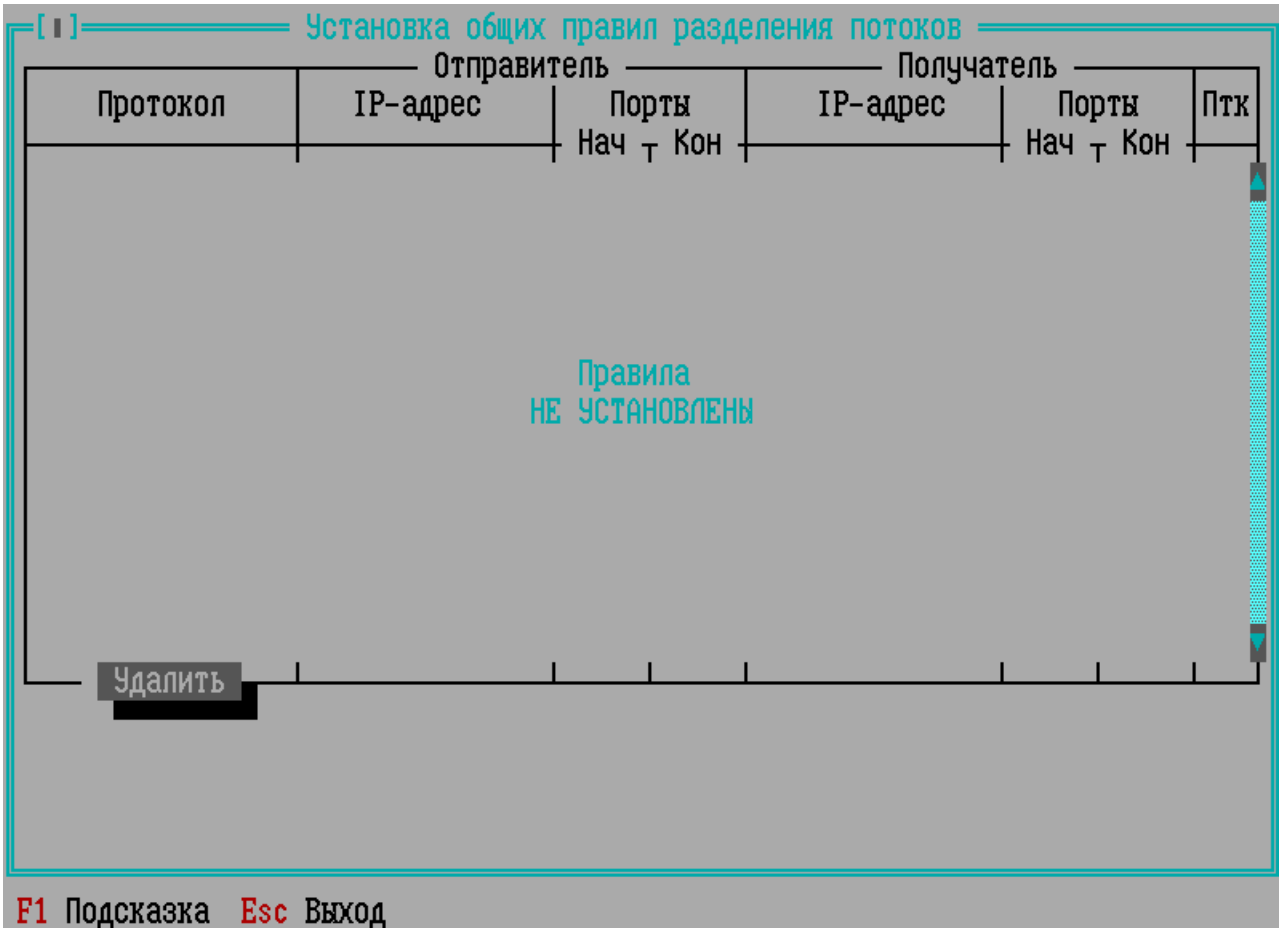


Рисунок 469 - Окно «Установка общих правил разделения потоков»

Чтобы добавить новое общее правило, следует нажать клавишу <*Ins*>, после чего открывается окно «*Установка нового общего правила разделения потоков*».

Чтобы установить правило, по которому поступающий в VPN-туннель со стороны конфигурируемого ФПСУ IP-пакет будет направлен в определенный выходной поток, следует указать ФПСУ номер IP-протокола, данные которого будут содержать пакет, IP-адрес (или диапазон адресов) отправителя (абонента, посылающего пакет со стороны конфигурируемого ФПСУ) 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).

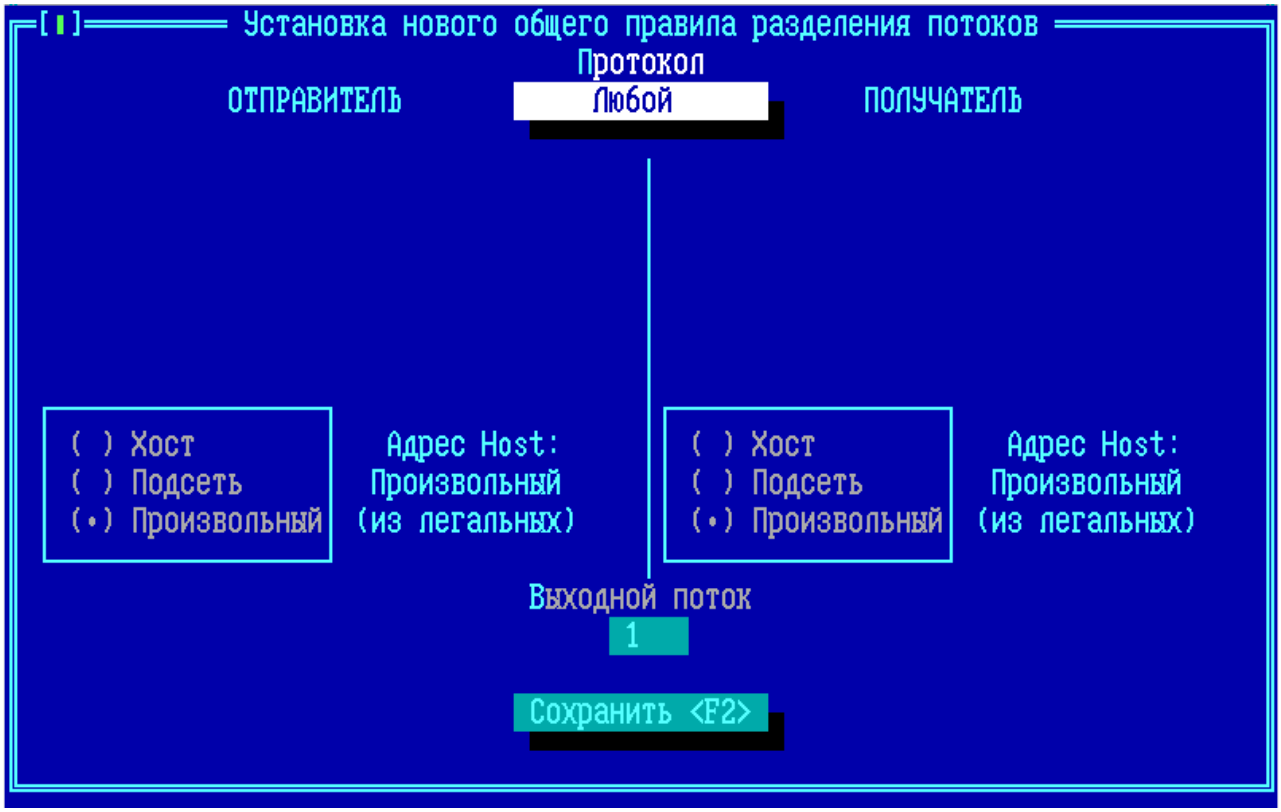


Рисунок 470 - Создание нового общего правила разделения потоков

Чтобы установить для выходного потока какой-либо конкретный протокол, нужно установить курсор на строку «Любой» под заголовком «Протокол» и нажать клавишу <*Пробел*>, затем в открывшемся списке протоколов установить курсор на нужный протокол и нажать <*Enter*> или <*Пробел*>, после чего будет осуществлен выход в окно установки описываемого правила. Если указанный протокол требует установки дополнительных параметров (например, номера начального и конечного портов для протоколов TCP или UDP), в окне появятся соответствующие поля ввода, в которые можно ввести либо номера портов (после чего в нижележащей строке будет отображено название «прикрепленного» к этому порту протокола, если оно есть), либо установить курсор на строку под полем ввода и нажать <*Пробел*>, после чего в появившемся списке отметить номер (или соответствующий протокол) нужного порта (в случае, если номер порта не превышает 1023).

Для установки IP-адресов отправителей и получателей следует поместить курсор на нужную строку, нажать <*Пробел*> и набрать в появившихся полях ввода адрес и маску (если в качестве отправителя и/или получателя могут выступать подсети).

После описания всех критериев правила следует выбрать номер выходного потока, для чего требуется перейти в поле «*Выходной поток*», и указать номер (номер выходного потока должен соответствовать номеру протокола, который будет использован для формирования данного потока при конфигурировании пограничного маршрутизатора). По активизации поля «*Сохранить*» подсистема конфигурирования осуществит выход в окно списка установленных общих правил.

Над установленными общими правилами в списке можно осуществить следующие операции:

- редактировать текущее правило (по нажатию <*Enter*>);
- удалить текущее правило (по нажатию <*Del*>).

ВНИМАНИЕ! При выделении в отдельный поток данных протоколов, допускающих динамическое изменение номеров портов (например, FTP), правила направления IP-пакетов в этот поток могут работать некорректно (хотя пакеты в любом случае будут доставлены удаленному комплексу ФПСУ). Если администратору обязательно требуется сформировать отдельный FTP-поток, рекомендуется использовать с этой целью поток по умолчанию (см. раздел Описание параметров туннелей с другими ФПСУ). Для этого все прочие данные распределяются по каким-либо определенным потокам, а в качестве потока по умолчания устанавливается поток, соответствующий номеру протокола, конфигурированного на пограничном маршрутизаторе для требуемого маршрута передачи данных FTP-протокола.

13. 2. Учет трафика IPFIX

ФПСУ может выступать в качестве сенсора сетевой структуры IPFIX (выступать в качестве IPFIX Device согласно RFC 5470).

ФПСУ может собирать информацию о проходящем через него трафике, создавать на основе полученной информации шаблоны с данными IP-потоков, и периодически отправлять эти шаблоны на указанные IP-адреса коллекторов IPFIX.

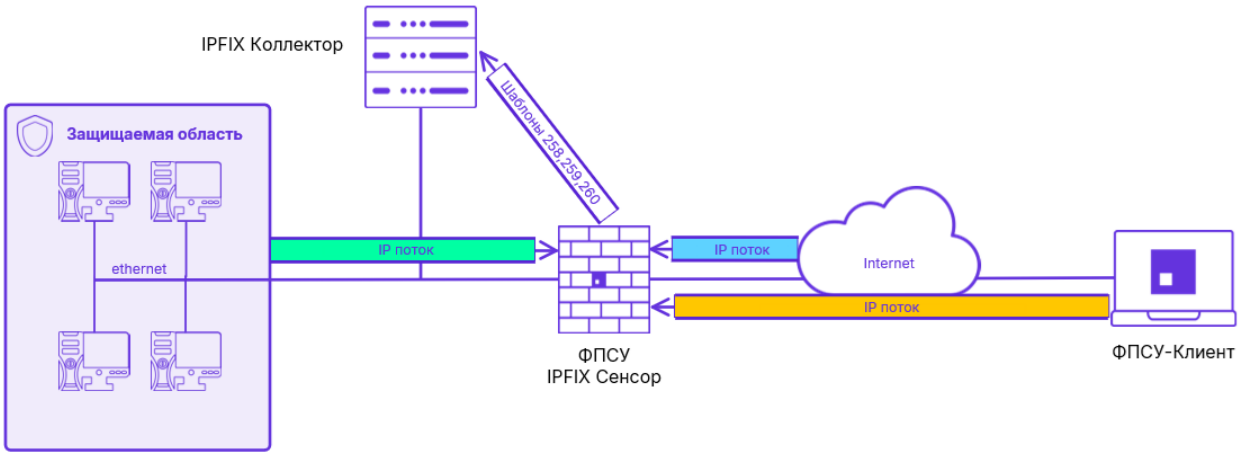


Рисунок 471 - ФПСУ в качестве сенсора IPFIX

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

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

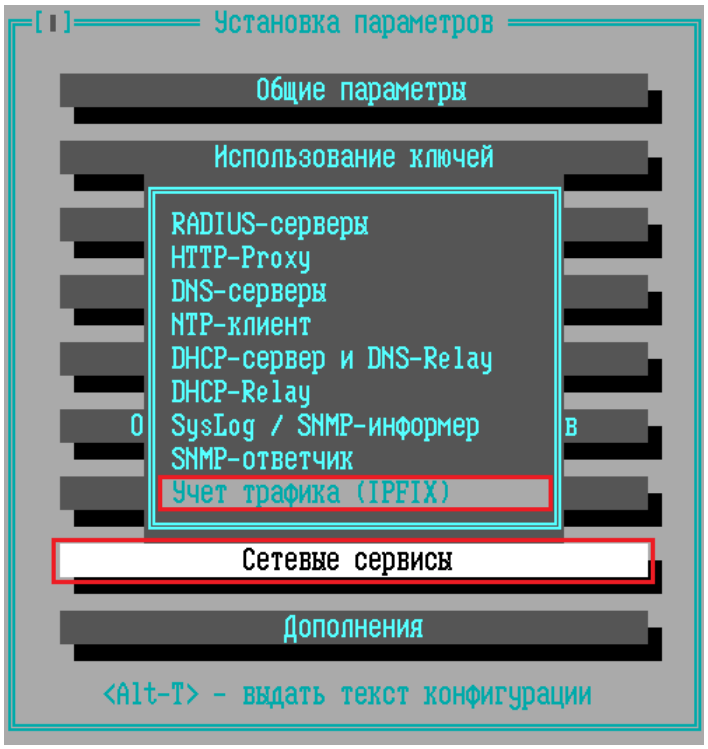


Рисунок 472 - Команда меню «Сетевые сервисы» → «Учет трафика (IPFIX)»

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

список пустой.

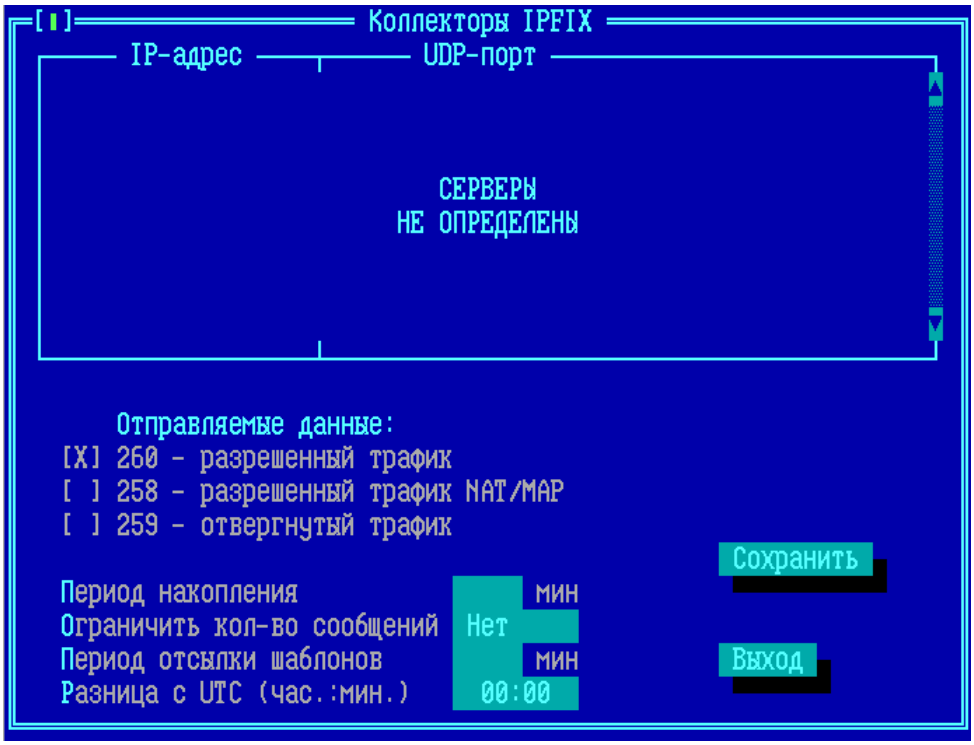


Рисунок 473 - Общие параметры, вызов окна настроек учета трафика IPFIX

Включение поддержки IPFIX может замедлять работу межсетевого экрана ФПСУ.

Для добавления нового коллектора IPFIX следует нажать клавишу <*Ins*>. Откроется окно, в котором задается IP-адрес коллектора и UDP-порт, по умолчанию 4739.

Флаг *«Работа запрещена»* при включении запрещает отправку шаблонов на указанный IP-адрес коллектора IPFIX.



Рисунок 474 - Добавление коллектора IPFIX

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

Шаблон 258 - трафик с NAT-адреса;

Шаблон 259 - отвергнутый трафик;

Шаблон 260 - разрешенный трафик.

Устанавливаются периоды накопления и отсылки шаблонов в минутах. Может быть задано ограничение на количество сообщений в шаблоне. Устанавливается разница временного пояса, в котором работает ФПСУ, с UTC временем.

13. 2. 1. Отвергнутый трафик

Таблица 10. Шаблон 259

№ п/п	Код	Наименование кода	Типоразмер	Описание
1	10	ingressInterface	unsigned8	Номер порта ФПСУ, на который были приняты пакеты
2	14	egressInterface	unsigned8	Номер порта ФПСУ, через который пакеты должны быть отправлены, либо 0, если это неизвестно
3	8	sourceIPv4Address	ipv4Address	IP-адрес отправителя
4	7	sourceTransportPort	unsigned16	TCP/UDP-порт отправителя
5	12	destinationIPv4Address	ipv4Address	IP-адрес получателя
6	11	destinationTransportPort	unsigned16	TCP/UDP-порт получателя
7	4	protocolIdentifier	unsigned8	Идентификатор протокола
8	150	flowStartSeconds	Milliseconds (64)	Время появления первого пакета в серии
9	151	flowEndSeconds	Milliseconds (64)	Время появления последнего пакета в серии
10	32	icmp_typecode	unsigned16	Тип/код сообщения для ICMP протокола см. пункт «Особенности реализации ICMP протокола» , таблица «Типы ICMP-ответов ФПСУ»
11	44	sourceIPv4Prefix	ipv4Address	Адрес ФПСУ, если абонент-отправитель прописан за ФПСУ (либо 0)
12	45	destinationIPv4Prefix	ipv4Address	Адрес ФПСУ, если абонент-получатель прописан через ФПСУ (либо 0)
13	233	firewallEvent	unsigned8	Код события: 3 - flow_denied

14	89	forwardingStatus	unsigned8	Способ обработки пакета. Проставляется: Dropped + код ошибки, см. таблица «Кодирование ошибок»
15	135	droppedPacketTotalCount	unsigned64	Общее количество пакетов в серии
16	133	droppedPacketDeltaCount	unsigned64	Количество пакетов с момента последнего отчета

13. 2. 2. Разрешенный трафик

Таблица 11. Шаблон 260

№ п/п	Код	Наименование кода	Типоразмер	Описание
1	1	octetDeltaCount	unsigned64	Количество октетов с момента предыдущего отчета (если есть) во входящих пакетах для этого потока в точке наблюдения. Количество октетов включает IP-заголовок(и) и полезную нагрузку IP
2	2	packetDeltaCount	unsigned64	Количество входящих пакетов с момента предыдущего отчета (если есть) для этого потока в точке наблюдения
3	4	protocolIdentifier	unsigned8	Идентификатор протокола
4	6	tcpControlBits	unsigned16	Наблюдаемые управляющие биты TCP для пакетов этого потока. Эта информация кодируется в виде битового поля; для каждого управляющего бита TCP в этом наборе есть бит. Бит устанавливается равным 1, если для любого наблюдаемого пакета этого потока установлен соответствующий бит управления TCP, равный 1. В противном случае бит будет очищен до 0. Значения каждого бита показаны ниже в соответствии с определением битов в заголовке TCP

				[RFC9293][RFC3168]: MSb LSb 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 +---+ | | | N | C | E | U | A | P | R | S | F / | Нулевой | Будущий | S | W | C | R | C | S | S / Y | I | | (Смещение данных) | Использовать | | R | E | G | K | H | T / N | N | +---+ битовый флаг значение имя описание ------+-----+---------- 0x8000 Ноль (см. tcpHeaderLength) 0x4000 Ноль (см. tcpHeaderLength) 0x2000 Ноль (см. tcpHeaderLength) 0x1000 Ноль (см. tcpHeaderLength) 0x0800 Будущее использование 0x0400 Будущее использование 0x0200 Будущее использование 0x0100 NS ECN одноразовая сумма Уменьшено окно перегрузки 0x0080 CWR

				0x0040 ECE ECN Echo 0x0020 URG Поле срочного указателя значимо 0x0010 Поле подтверждения значимо Функция Push 0x0008 PSH 0x0004 СНАЧАЛА сбросьте соединение 0x0002 SYN Синхронизирует порядковые номера 0x0001 FIN Больше нет данных от отправителя Поскольку наиболее значимые 4 бита октетов 12 и 13 (считая от нуля) заголовка TCP [RFC9293] используются для кодирования смещения данных TCP (длины заголовка), соответствующие биты в этой информации Элемент ДОЛЖЕН быть экспортирован как ноль и ДОЛЖЕН игнорироваться сборщиком. Используйте информационный элемент tcpHeaderLength для кодирования этого значения. Каждый из 3 битов (0x800, 0x400 и 0x200), которые зарезервированы для будущего использования в [RFC9293], СЛЕДУЕТ экспортировать, как указано в заголовках TCP пакетов этого потока. При экспорте в виде одного октета с кодировкой уменьшенного размера этот информационный элемент охватывает октет младшего порядка этого поля (т.е. биты от 0x80 до 0x01), исключая одноразовую сумму ECN и три бита будущего использования. Сборщик, получающий этот информационный элемент с кодировкой уменьшенного размера, не должен ничего предполагать о содержимом этих четырех битов.

				Экспортирующие процессы, экспортирующие этот информационный элемент от имени процесса учета, который не способен отслеживать какие-либо биты одноразового номера ECN или биты будущего использования, ДОЛЖНЫ использовать кодирование уменьшенного размера и экспортировать только 8 младших значащих битов этого информационного элемента. Обратите внимание, что в предыдущих версиях определения этого информационного элемента указывалось, что биты CWR и ECE должны экспортироваться как нулевые, даже если они соблюдены. Поэтому сборщики не должны предполагать, что нулевое значение для этих битов в этом информационном элементе указывает, что биты никогда не устанавливались в наблюдаемом трафике, особенно если эти биты равны нулю в каждой записи потока, отправленной данным экспортером.
5	7	sourceTransportPort	unsigned16	TCP/UDP-порт отправителя
6	8	sourceIPv4Address	ipv4Address	IP-адрес отправителя
7	10	ingressInterface	unsigned32	Номер порта ФПСУ, на который были приняты пакеты
8	11	destinationTransportPort	unsigned16	TCP/UDP-порт получателя
9	12	destinationIPv4Address	ipv4Address	IP-адрес получателя
10	14	egressInterface	unsigned32	Номер порта ФПСУ, через который пакеты должны быть отправлены, либо 0, если это неизвестно
11	32	icmpTypeCodeIPv4	unsigned16	Тип/код сообщения для ICMP протокола см. пункт «Особенности реализации ICMP протокола» , таблица «Типы ICMP-ответов ФПСУ»

12	44	sourceIPv4Prefix	ipv4Address	Адрес ФПСУ, если абонент-отправитель прописан за ФПСУ, либо 0
13	45	destinationIPv4Prefix	ipv4Address	Адрес ФПСУ, если абонент-получатель прописан через ФПСУ, либо 0
14	152	flowStartMilliseconds	dateTimeMilliseconds	Абсолютная временная метка первого пакета этого потока
15	153	flowEndMilliseconds	dateTimeMilliseconds	Абсолютная временная метка последнего пакета этого потока
16	231	initiatorOctets	unsigned64	Общее количество байтов полезной нагрузки уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и остается неизменным в течение срока действия сеанса
17	232	responderOctets	unsigned64	Общее количество байтов полезной нагрузки уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик – это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса
18	233	firewallEvent		Код события: 3 → flow_denied Указывает на событие брандмауэра. Допустимые значения перечислены в реестре firewallEvent: Значение Описание 0 Ignore (invalid) 1 Flow Created 2 Flow Deleted 3 Flow Denied 4 Flow Alert 5 Flow Update 6-255 Unassigned
19	298	initiatorPackets	unsigned64	Общее количество пакетов уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое

				инициировало создание сеанса, и остается неизменным в течение всего срока действия сеанса
20	299	responderPackets	unsigned64	Общее количество пакетов уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик – это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса

13. 2. 3. Трафик с NAT

Таблица 12. Шаблон 258

№ п/п	Код	Наименование кода	Типоразмер	Описание
1	1	octetDeltaCount	unsigned64	Количество октетов с момента предыдущего отчета (если есть) во входящих пакетах для этого потока в точке наблюдения. Количество октетов включает IP-заголовок(и) и полезную нагрузку IP
2	2	packetDeltaCount	unsigned64	Количество входящих пакетов с момента предыдущего отчета (если есть) для этого потока в точке наблюдения
3	4	protocolIdentifier	unsigned8	Идентификатор протокола
4	6	tcpControlBits	unsigned16	Наблюдаемые управляющие биты TCP для пакетов этого потока. Эта информация кодируется в виде битового поля; для каждого управляющего бита TCP в этом наборе есть бит. Бит устанавливается равным 1, если для любого наблюдаемого пакета этого потока установлен соответствующий бит управления TCP, равный 1. В противном случае бит будет очищен до 0.

				Значения каждого бита показаны ниже в соответствии с определением битов в заголовке TCP [RFC9293][RFC3168]: MSb LSb 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ | | | N | C | E | U | A | P | R | S | F | | Нулевой | Будущий | S | W | C | R | C | S | S | Y | I | | (Смещение данных) | Использовать | | R | E | G | K | H | T | N | N | +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+ битовый флаг значение имя описание ------+-----+---------- 0x8000 Ноль (см. tcpHeaderLength) 0x4000 Ноль (см. tcpHeaderLength) 0x2000 Ноль (см. tcpHeaderLength) 0x1000 Ноль (см. tcpHeaderLength) 0x0800 Будущее использование 0x0400 Будущее использование

				0x0200 Будущее использование 0x0100 NS ECN одноразовая сумма Уменьшено окно перегрузки 0x0080 CWR 0x0040 ECE ECN Echo 0x0020 URG Поле срочного указателя значимо 0x0010 Поле подтверждения значимо Функция Push 0x0008 PSH 0x0004 СНАЧАЛА сбросьте соединение 0x0002 SYN Синхронизирует порядковые номера 0x0001 FIN Больше нет данных от отправителя Поскольку наиболее значимые 4 бита октетов 12 и 13 (считая от нуля) заголовка TCP [RFC9293] используются для кодирования смещения данных TCP (длины заголовка), соответствующие биты в этой информации Элемент ДОЛЖЕН быть экспортирован как ноль и ДОЛЖЕН игнорироваться сборщиком. Используйте информационный элемент tcpHeaderLength для кодирования этого значения. Каждый из 3 битов (0x800, 0x400 и 0x200), которые зарезервированы для будущего использования в [RFC9293], СЛЕДУЕТ экспортировать, как указано в заголовках TCP пакетов этого потока. При экспорте в виде одного октета с

				кодировкой уменьшенного размера этот информационный элемент охватывает октет младшего порядка этого поля (т.е. биты от 0x80 до 0x01), исключая одноразовую сумму ECN и три бита будущего использования. Сборщик, получающий этот информационный элемент с кодировкой уменьшенного размера, не должен ничего предполагать о содержимом этих четырех битов. Экспортирующие процессы, экспортирующие этот информационный элемент от имени процесса учета, который не способен отслеживать какие-либо биты одноразового номера ECN или биты будущего использования, ДОЛЖНЫ использовать кодирование уменьшенного размера и экспортировать только 8 младших значащих битов этого информационного элемента. Обратите внимание, что в предыдущих версиях определения этого информационного элемента указывалось, что биты CWR и ECE должны экспортироваться как нулевые, даже если они соблюдены. Поэтому сборщики не должны предполагать, что нулевое значение для этих битов в этом информационном элементе указывает, что биты никогда не устанавливались в наблюдаемом трафике, особенно если эти биты равны нулю в каждой записи потока, отправленной данным экспортером.
5	7	sourceTransportPort	unsigned16	TCP/UDP-порт отправителя

6	8	sourceIPv4Address	ipv4Address	IP-адрес отправителя
78	10	ingressInterface	unsigned32	Номер порта ФПСУ, на который были приняты пакеты
9	11	destinationTransportPort	unsigned16	TCP/UDP-порт получателя
10	12	destinationIPv4Address	ipv4Address	IP-адрес получателя
11	14	egressInterface	unsigned32	Номер порта ФПСУ, через который пакеты должны быть отправлены, либо 0, если это неизвестно
12	32	icmpTypeCodeIPv4	unsigned16	Тип/код сообщения для ICMP протокола см. пункт «Особенности реализации ICMP протокола» , таблица «Типы ICMP-ответов ФПСУ»
13	44	sourceIPv4Prefix	ipv4Address	Адрес ФПСУ, если абонент-отправитель прописан за ФПСУ, либо 0
14	45	destinationIPv4Prefix	ipv4Address	Адрес ФПСУ, если абонент-получатель прописан через ФПСУ, либо 0
15	152	flowStartMilliseconds	dateTimeMilliseconds	Абсолютная временная метка первого пакета этого потока
16	153	flowEndMilliseconds	dateTimeMilliseconds	Абсолютная временная метка последнего пакета этого потока
17	225	postNATSourceIPv4Address	ipv4Address	Определение этого информационного элемента идентично определению информационного элемента 'sourceIPv4Address', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока NAT после того, как пакет прошел точку наблюдения

18	226	postNATDestinationIPv4Address	ipv4Address	Определение этого информационного элемента идентично определению информационного элемента 'destinationIPv4Address', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока NAT после того, как пакет прошел точку наблюдения
19	227	postNAPTSourceTransportPort	unsigned16	Определение этого информационного элемента идентично определению информационного элемента 'sourceTransportPort', за исключением того, что он сообщает измененное значение, вызванное функцией промежуточного блока преобразования сетевого адреса (NAPT) после того, как пакет прошел точку наблюдения
20	228	postNAPTDestinationTransportPort	unsigned16	Определение этого информационного элемента идентично определению информационного элемента 'destinationTransportPort', за исключением того, что он сообщает об измененном значении, вызванном функцией промежуточного блока преобразования сетевого адреса (NAPT) после того, как пакет прошел точку наблюдения.
21	231	initiatorOctets	unsigned64	Общее количество байтов полезной нагрузки уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и остается неизменным в течение срока действия сеанса.
22	232	responderOctets	unsigned64	Общее количество байтов полезной нагрузки уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик – это устройство, которое отвечает инициатору и остается неизменным в течение срока

				действия сеанса.
23	233	firewallEvent		Код события: 3 → flow_denied Указывает на событие брандмауэра. Допустимые значения перечислены в реестре firewallEvent: Значение Описание 0 Ignore (invalid) 1 Flow Created 2 Flow Deleted 3 Flow Denied 4 Flow Alert 5 Flow Update 6-255 Unassigned
24	298	initiatorPackets	unsigned64	Общее количество пакетов уровня 4 в потоке от инициатора с момента предыдущего отчета. Инициатором является устройство, которое инициировало создание сеанса, и остается неизменным в течение всего срока действия сеанса.
25	299	responderPackets	unsigned64	Общее количество пакетов уровня 4 в потоке от ответчика с момента предыдущего отчета. Ответчик – это устройство, которое отвечает инициатору и остается неизменным в течение срока действия сеанса.

13. 3. SNMP-клиент на ФПСУ

ФПСУ поддерживает возможность отправки сообщений о происходящих на ФПСУ событиях по протоколу SNMP. Для этого реализована подсистема, которая отслеживает происходящие на ФПСУ события и отправляет их в ответ на запросы SNMP-менеджера.

Доступ к окну настроек параметров SNMP-клиента на ФПСУ предоставляется меню «*Сетевые сервисы»* конфигурации ФПСУ при выборе в подменю команды «*SysLog/SNMP-информер»*.

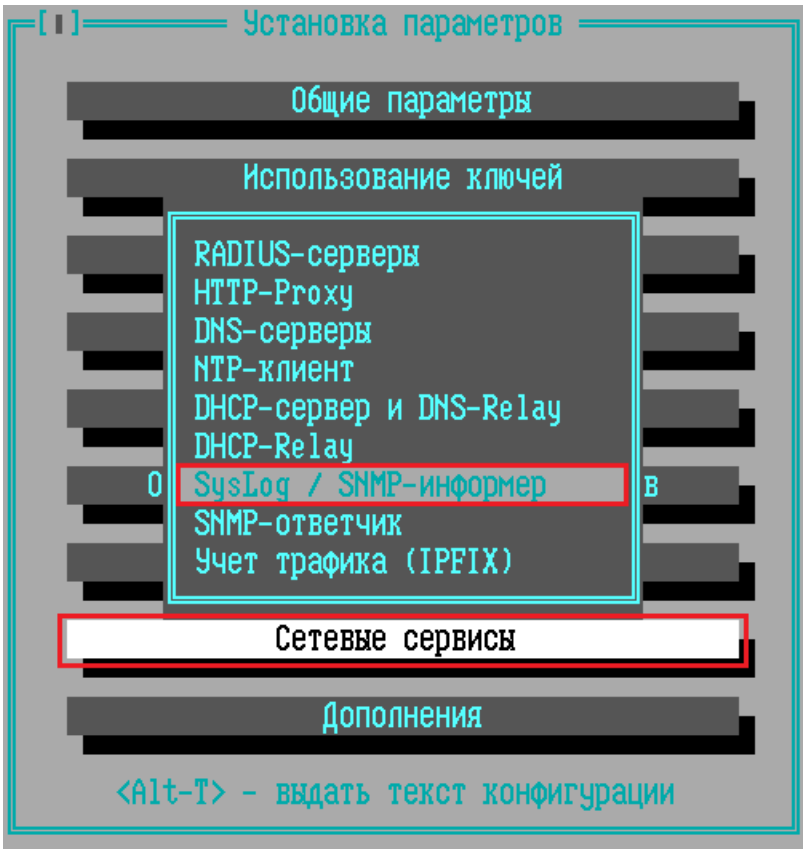


Рисунок 475 - Команда меню «Сетевые сервисы» → «SysLog/SNMP»

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

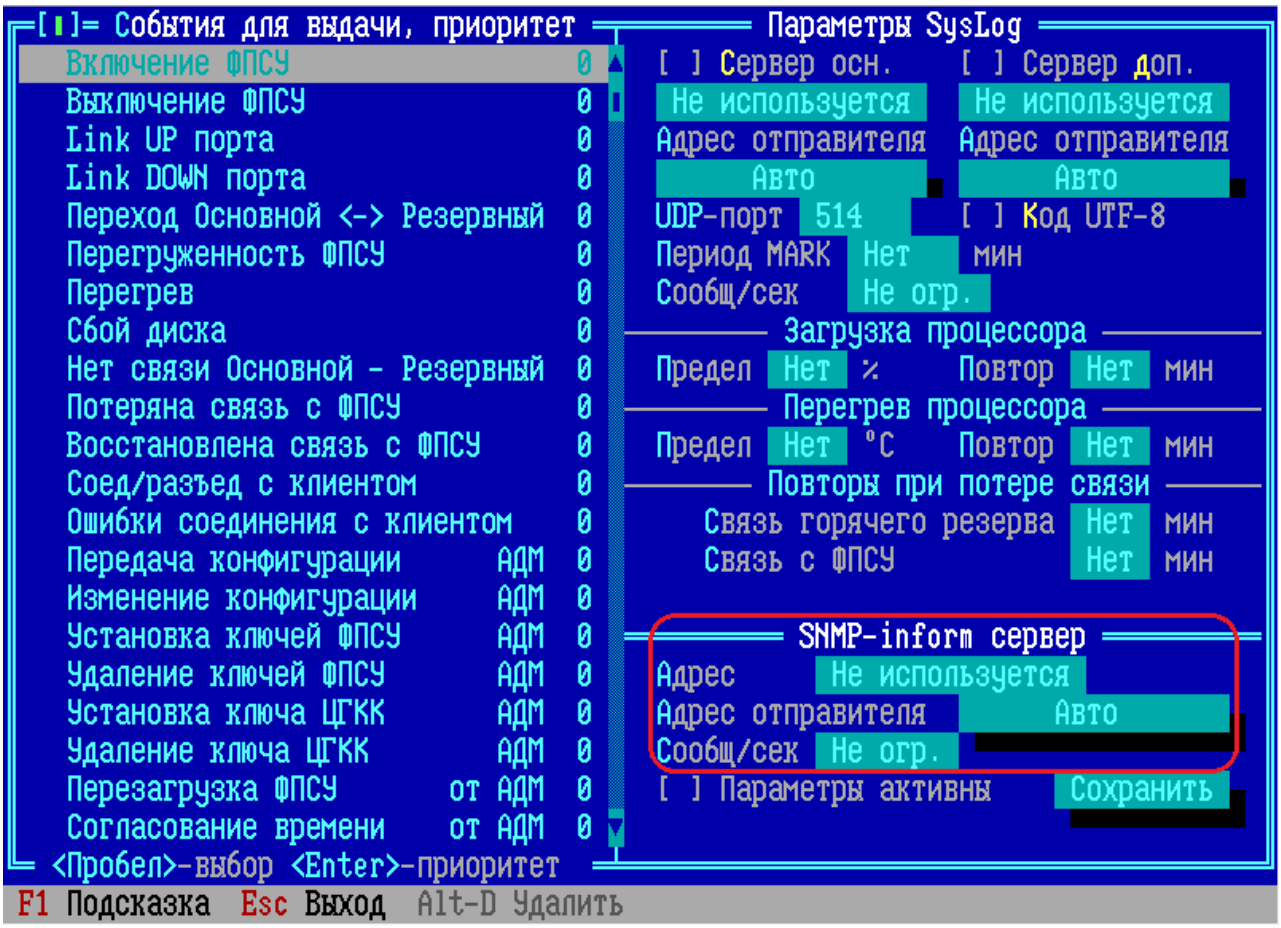


Рисунок 476 - Интерфейс настройки SNMP

Настраиваемые параметры SNMP-клиента:

SNMP-inform сервер, Адрес — IP-адрес SNMP-менеджера, на него будут отправляться SNMP-inform сообщения;

SNMP-inform сервер, Адрес отправителя — порт ФПСУ, 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-inform серверу IP-адрес. Администратор может безусловно указать, что сообщения следует отправлять от IP-адреса 1 или 2 порта ФПСУ;

SNMP-inform сервер, Сообщений/сек — максимальное количество SNMP-сообщений о событиях на настраиваемом ФПСУ, отправляемое в секунду. Рекомендуется устанавливать значение не более 100. По умолчанию не ограничено;

Параметры активны — флаг, при установлении которого включается выполнение SNMP TRAP, в поле «*Адрес*» должен быть задан IP-адрес SNMP-менеджера. При выключенном флаге выполнение SNMP TRAP не происходит. Включение или выключение осуществляется клавишей <*Пробел*>.

Дополнительно требуется установить пароль SNMP-ответчика, доступ к окну настроек параметров SNMP-ответчика на ФПСУ предоставляется меню «*Сетевые сервисы*» конфигурации ФПСУ при выборе в подменю команды «*SNMP-ответчик*».

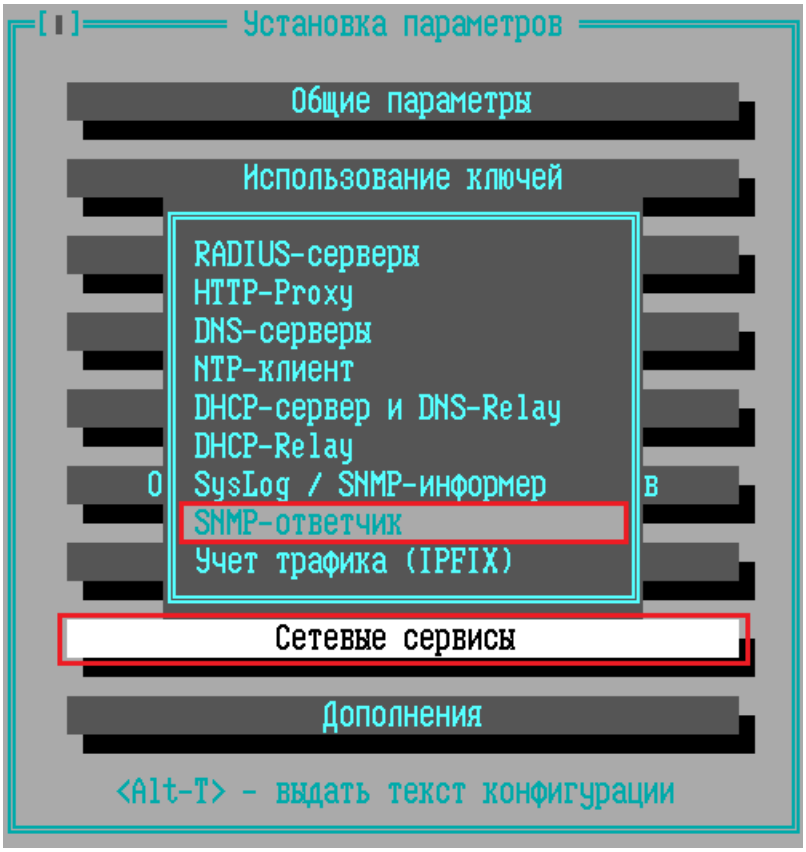


Рисунок 477 - Команда меню «Сетевые сервисы» → «SNMP-ответчик»

В открывшемся окне отображаются следующие настройки:

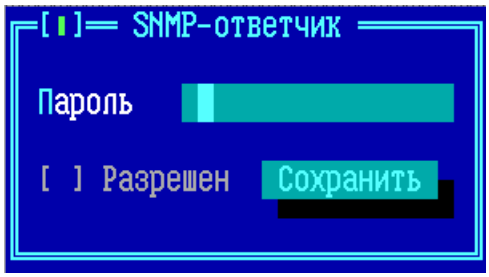


Рисунок 478 - Установление пароля SNMP

Встроенный SNMP(v3)-ответчик, Пароль — символьный пароль, указание которого требуется при направлении запроса к SNMP-агенту, работающему на ФПСУ, от SNMP-менеджера. Поле обязательно к заполнению, в случае если флаг Разрешен задействован (см. ниже).

Разрешен — установленный флаг включает SNMP-ответчик.

Помимо настроек на стороне ФПСУ, на стороне SNMP-менеджера требуется указать определенные параметры для подключения:

- MIB база ФПСУ 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 доступна в ветке OID - .1.3.6.1.4.1.37249.

Например, для SNMP-менеджера iReasoning MIB Browser параметры управляемого SNMP-агента выглядят следующим образом:

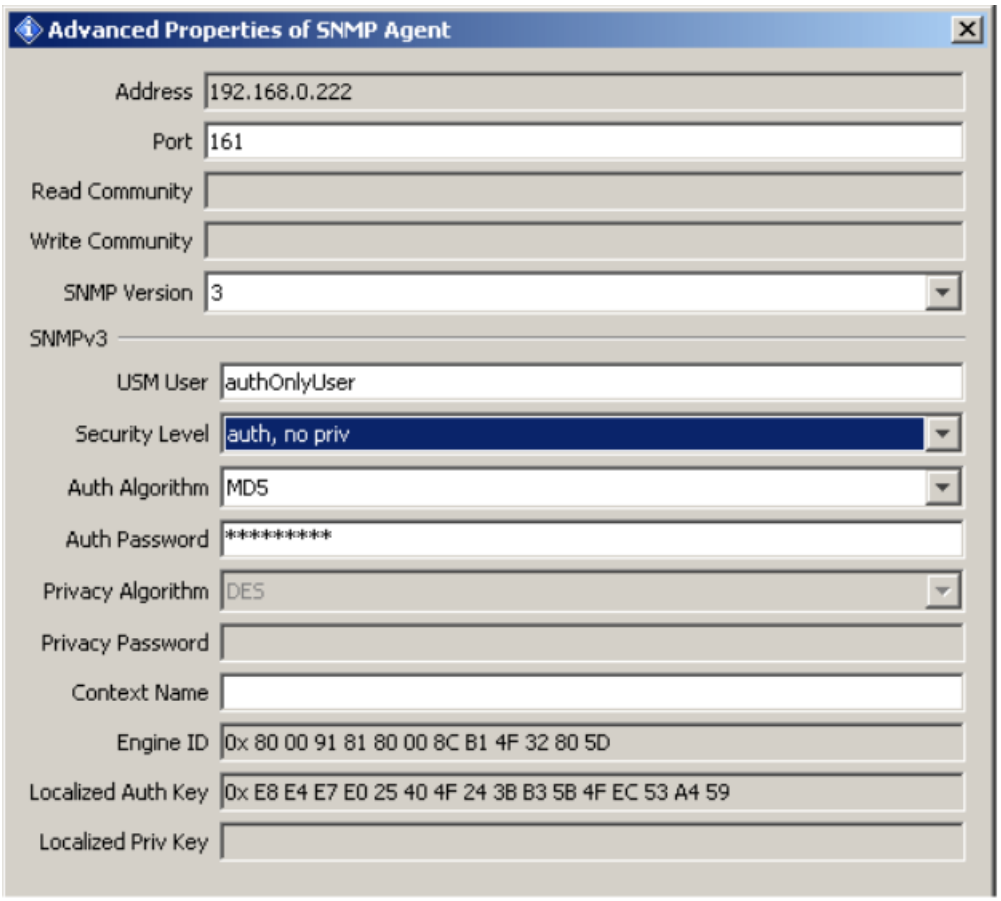


Рисунок 479 - Настройки SNMP-агента ФПСУ в iReasoning MIB Browser

13. 4. Syslog-клиент на ФПСУ

ФПСУ поддерживает возможность отправки сообщений о происходящих на ФПСУ событиях по протоколу SysLog. Для этого реализована подсистема, которая отслеживает происходящие на ФПСУ события и отправляет их на внешний SysLog-сервер.

Сообщения отправляются в кодировке OEM/DOS (866) по умолчанию (может быть переключена на UTF-8).

Для настройки SysLog-клиента на ФПСУ 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 предоставляется из меню *«Сетевые сервисы»* конфигурации ФПСУ при выборе в подменю команды *«SysLog/SNMP»*.

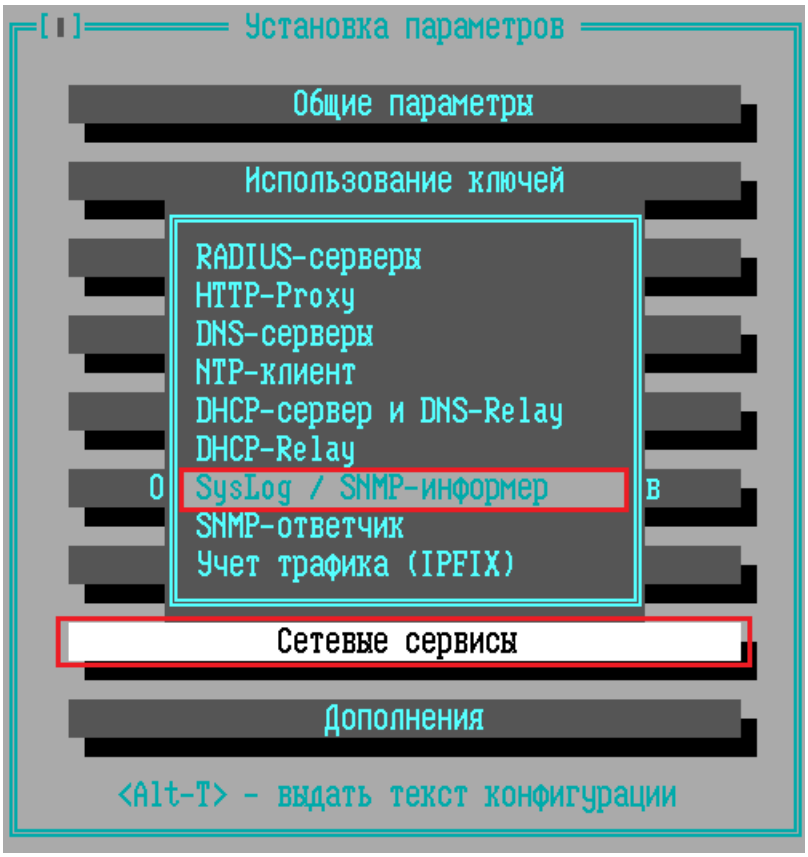


Рисунок 480 - Команда меню «Сетевые сервисы» → «SysLog/SNMP»

13. 4. 1. Настройка SysLog событий ФПСУ

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

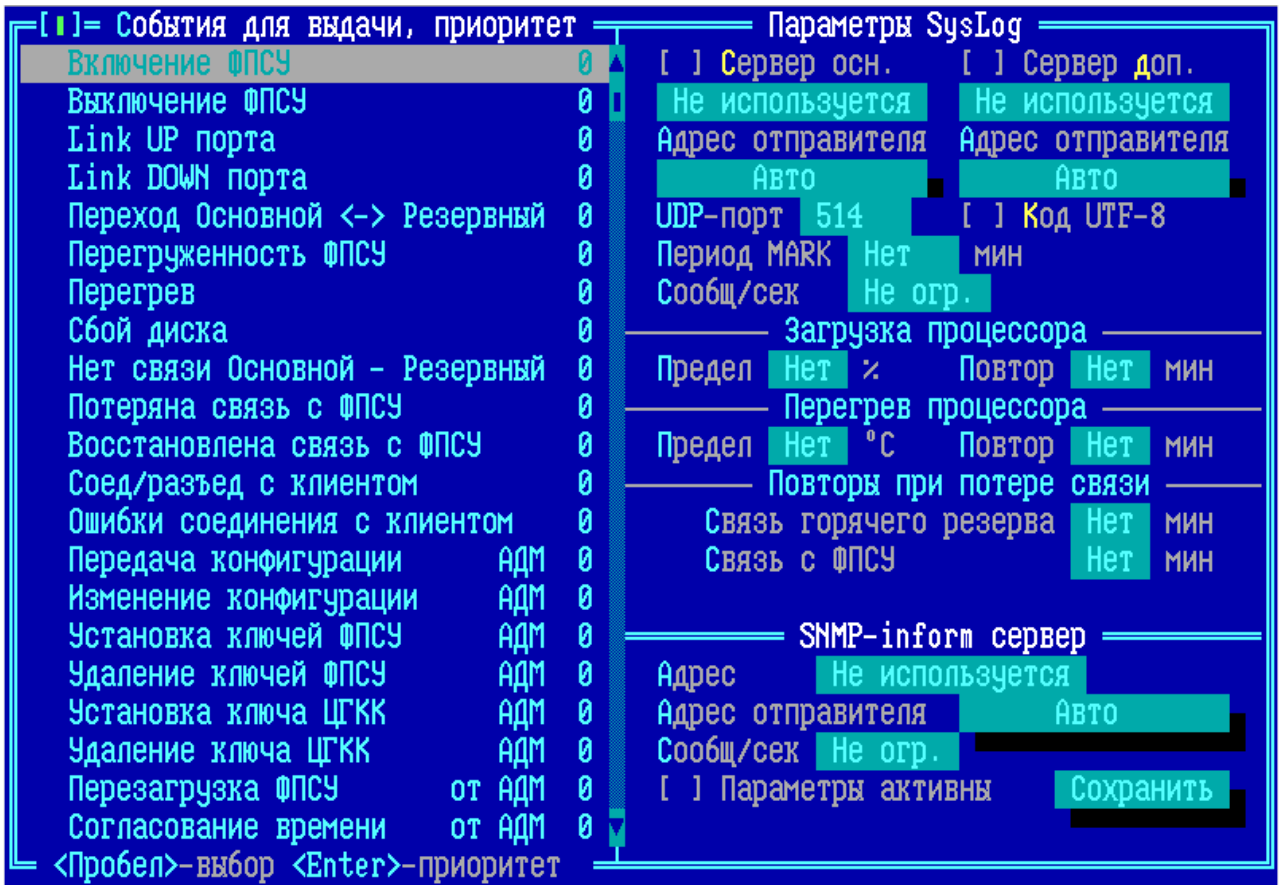


Рисунок 481 - Настройка параметров SysLog

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

Таблица 13. SysLog сообщения

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

Название события	**Код события в тексте SysLog сообщения**	**Причина**
Установка ключей ФПСУ АДМ	100004	Удаленный администратор ФПСУ выполнил установку на ФПСУ ключей парно-выборочной связи
Удаление ключей ФПСУ АДМ	100005	Удаленный администратор ФПСУ выполнил удаление с ФПСУ ключей парно-выборочной связи
Установка ключа ЦГКК АДМ	100006	Удаленный администратор ФПСУ выполнил установку на ФПСУ общесистемного ключа Криптосети Клиентов
Удаление ключа ЦГКК АДМ	100007	Удаленный администратор ФПСУ выполнил удаление с ФПСУ общесистемного ключа Криптосети Клиентов
Перезагрузка ФПСУ АДМ	100008	Удаленным администратором произведена перезагрузка комплекса ФПСУ
Согласование времени с АДМ	100009	Время на ФПСУ было синхронизировано со временем на АРМ УА ФПСУ
Подключение УА	100010	Удаленный администратор подключился к ФПСУ
Локальная установка ключей ФПСУ	110001	Локальный администратор ФПСУ выполнил установку на ФПСУ ключей парно-выборочной связи
Локальное удаление ключей ФПСУ АДМ	110002	Локальный администратор ФПСУ выполнил удаление с ФПСУ ключей парно-выборочной связи
Локальная установка ключа ЦГКК	110003	Локальный администратор ФПСУ выполнил установку на ФПСУ общесистемного ключа Криптосети Клиентов
Локальное удаление ключа ЦГКК	110004	Локальный администратор ФПСУ выполнил удаление с ФПСУ общесистемного ключа Криптосети Клиентов

Название события	**Код события в тексте SysLog сообщения**	**Причина**
Локальное изменение конфигурации	110005	Локальный администратор ФПСУ изменил конфигурацию
Изменение конфигурации LAN-адаптеров	110006	Локальный администратор ФПСУ изменил конфигурацию LAN-адаптеров
Локальные события	110007	Локальное изменение настроек дополнения
Потеряна связь с ФПСУ	200001	Произошло разъединение защищенного соединения (туннеля) с удаленным ФПСУ
Восстановлена связь с ФПСУ	200002	Установлен туннель с удаленным ФПСУ
Включение ФПСУ	200003	Включение работы ФПСУ в режим фильтрации
Выключение ФПСУ	200004	Выход ФПСУ из режима фильтрации пакетов
Перегруженность ФПСУ	200005	Загрузка ЦПУ ФПСУ достигла порогового значения, указанного в параметре «Загрузка процессора, Предел»
MARK сообщения	200007	Служебное периодическое оповещение ФПСУ о работоспособности комплекса
Локальные события	200011	Потеряна связь с ФПСУ в потоке
	200021	Восстановлена связь с ФПСУ в потоке
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

Название события	**Код события в тексте SysLog сообщения**	**Причина**
	300004	Ошибка авторизации ФПСУ-IP/Клиента на сервере RADIUS
События удаленной загрузки ключей	300010	Запрос получения ключа ФПСУ-IP/Клиентом
	300011	Запрос обновления ключа на ФПСУ-IP/Клиенте
	300012	Подтверждение получения ключа ФПСУ-IP/Клиентом
	300013	Не удалось установить соединение (отвергается доступ в криптосеть, неверная аппаратная привязка клиента)
Авторизация ФПСУ-IP/Клиента	300020	Произошла авторизация ФПСУ-IP/Клиента на сервере RADIUS
	300021	Accept от RADIUS
	300022	Reject от RADIUS
	300023	CoA от RADIUS
	300024	DM от RADIUS
ФПСУ Клиент PKI	310001	Соединение с ФПСУ Клиентом PKI
	310002	Разъединение с ФПСУ Клиентом PKI
Авторизация ФПСУ Клиента PKI	310020	Сообщения RADIUS
	310021	Accept от RADIUS

Название события	Код события в тексте SysLog сообщения	Причина
	310022	Reject от RADIUS
	310023	CoA от RADIUS
	310024	DM от RADIUS
Статистика ФПСУ Клиента PKI	310050	Текущая статистика
Переход Основной - Резервный	400001	Произошла передача управления партнёру по горячему резервированию
Нет связи Основной - Резервный	400002	Партнер по горячему резерву не ответил на запрос
Нет канала Основной - Резервный	400003	Отсутствует физический канал связи между партнерами по горячему резерву
Link UP порта	500001	Включение сетевого адаптера в сеть передачи данных
Link DOWN порта	500002	Прекращение работы сетевого адаптера с сетью передачи данных
Перегрев	500003	Температура ЦПУ ФПСУ 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

Название события	**Код события в тексте SysLog сообщения**	**Причина**
Текущая температура	500005	Периодическое отправление сообщения с текущим уровнем нагрева ЦПУ ФПСУ, периодичность отправки указывается в параметре «Перегрев процессора, Повтор»
Окончание поддержки	500006	Заканчивается текущий срок поддержки ФПСУ
Локальные события	500007	Sfp мониторинг
	500008	xstats портов
	500009	Появление нового дампа
Журнал ARP-записей	510001	MAC-адрес добавлен в ARP-таблицу
	510002	MAC-адрес исключен из ARP-таблицы
	600002	Обмен в режиме туннелирования
	600003	Обмен Клиент-Абонент
	600004	Отказ - отправитель не зарегистрирован
	600005	Отказ - получатель не зарегистрирован
	600006	Отказ - маршрут неизвестен
	600007	Ошибка- абонент не должен работать в режиме «через ФПСУ»
	600008	Ошибка- абонент должен работать в режиме «через ФПСУ»

Название события	**Код события в тексте SysLog сообщения**	**Причина**
	600009	Удаленный ФПСУ не работает
	600010	MAC-адрес станции совпадает с адресом ФПСУ
	600011	Запрет по режиму работы с партнером
События МЭ	700001	Соединение разрешено МЭ
	700002	Соединение запрещено МЭ
Блокировка абонента МЭ (flood)	700003	Абонент заблокирован МЭ (flood)
	700004	Абонент разблокирован МЭ (flood)
Блокировка абонента СОВ	700005	Абонент заблокирован СОВ
	700006	Абонент разблокирован СОВ
Блокировка ресурсов	700007	Блокировка абонента межсетевым экраном ФПСУ
	700008	Разблокировка абонента межсетевым экраном ФПСУ
	700009	Администратор заблокировал Port
	700010	Администратор разблокировал Port
	700011	Администратор заблокировал Proto
	700012	Администратор разблокировал Proto
Соединение запрещено МЭ (DPI)	700013	Соединение было сброшено межсетевым экраном ФПСУ по одному из правил DPI

Название события	**Код события в тексте SysLog сообщения**	**Причина**
FLOOD	700013	FLOOD включился
	700014	FLOOD выключился
Квантовые сообщения биллинга	820001	Начало отчетного периода
	820002	Выдан ключ абоненту
	820003	Ошибка выдачи ключа абоненту
События IDS (Intrusion detect system)	900099	IDS запускается
	900100	IDS запущена
	900101	IDS остановлена
	900103	База решающих правил обновлена
	900104	IDS: Переконфигурирование завершено успешно
	900200	Периодическое сообщение о статусе IDS
	900401	Сработала тревога уровня 1 (максимальная опасность)
	900402	Сработала тревога уровня 2
	900403	Сработала тревога уровня 3
	900404	Сработала тревога уровня 4 (и более, до 255, но код сообщения не меняется после 4х)
	900410	Эвристикой обнаружены потенциальные угрозы
	900420	Записи в локальной БД о сработавших тревогах были сжаты и перенесены в архив

Название события	Код события в тексте SysLog сообщения	Причина
	900430	Запрос на блокировку IP-адреса через МЭ ФПСУ
	900500	Ошибка — невозможно запустить систему
	900501	Критическая проблема при работе
	900502	IDS: Ошибка переконфигурации
	900503	IDS: Критическая ошибка при запуске
	900505	Ведение локальной БД сработавших тревог отключено - достигнут лимит

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 14. 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;

Приоритет	Описание
7	Отладка: сообщения диагностического уровня.

Приоритет каждому событию может быть назначен администратором ФПСУ 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.

13. 4. 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:

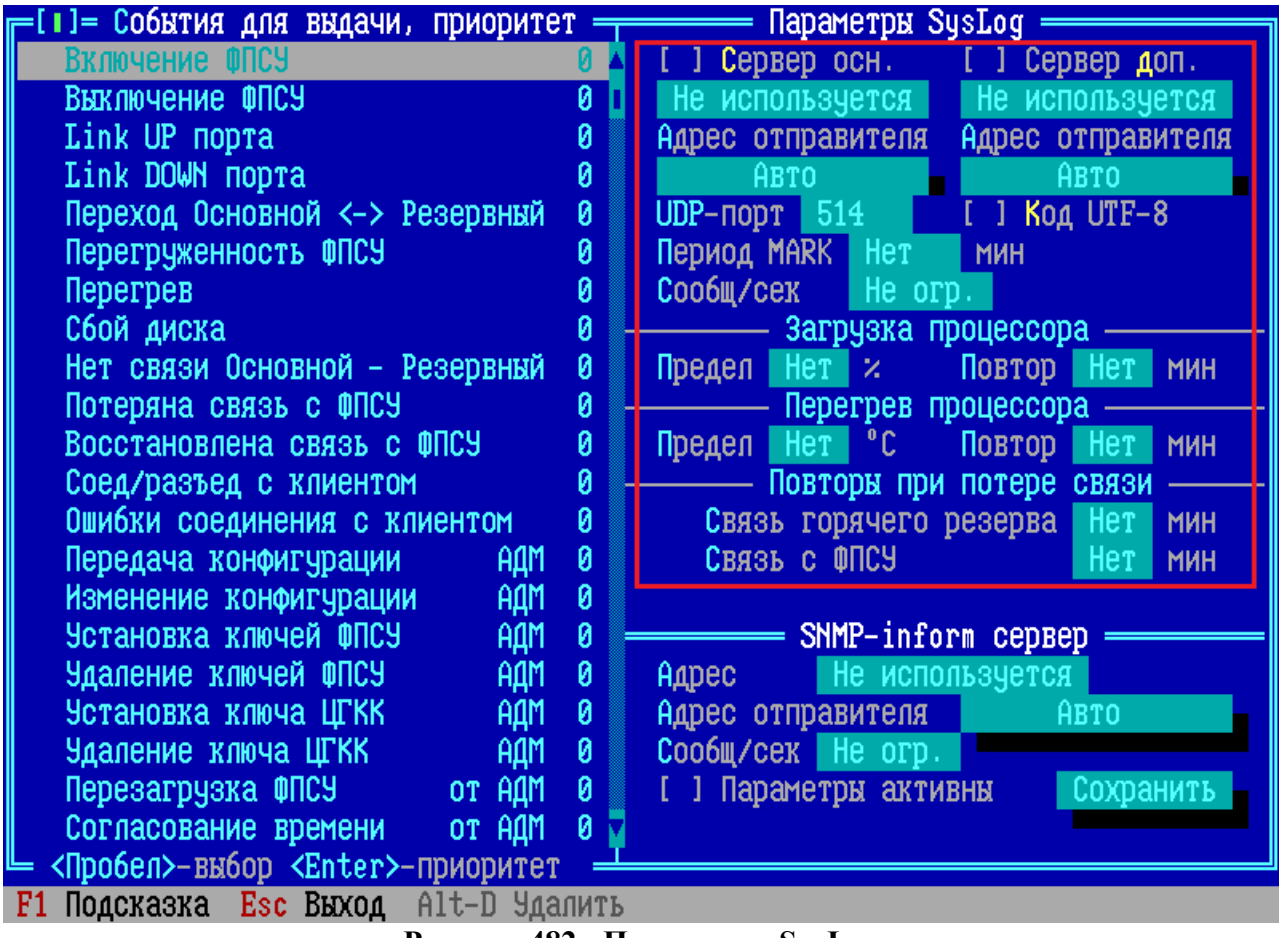


Рисунок 482 - Параметры SysLog

Сервер осн., Сервер доп. — при включении флага в поле ниже указывается IP-адрес SysLog сервера основного и дополнительного, на них будут отправляться SysLog-сообщения.

UDP порт — поле выбора UDP-порта принимающего сообщения SysLog сервера. По умолчанию - рекомендуемый UDP:514.

Код UTF-8 — если флаг задействован, сообщения отправляются в кодировке UTF-8 (кодировкой по умолчанию со снятым флагом является OEM/DOS (866).

Адрес отправителя — порт ФПСУ, чей IP-адрес будет указан в качестве отправителя SysLog-сообщений. По умолчанию режим «*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 указанного порта ФПСУ.

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

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

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

Загрузка процессора, Предел — отправка сообщения SysLog серверу о процентной загрузке центрального процессора ФПСУ. 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. 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. 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. 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 удаленного ФПСУ (см. пункт «Описание параметров туннелей с другими ФПСУ»). 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, через каждый указанный промежуток времени сообщение будет отправляться повторно.

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

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

13. 4. 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 заголовка, который состоит из следующих полей:

Таблица 15. Формат SysLog сообщения

Служебное число	Дата отправления сообщения с ФПСУ	Серийный номер ФПСУ	ФПСУ	Код события	Имя события	Детали события	Номер ФПСУ в системе «горячего» резерва
Служебное число	Дата и время в формате Мес ДД ЧЧ:ММ:СС	Серийный номер ФПСУ, отправившего сообщение	Текст [FPSU]:	Код события в соответствии с таблицей 4	Текст, содержащий название события	Дополнительные поля, в зависимости от события	1, если основной/ единственный ФПСУ; 2, резервный

Кроме полей заголовка, к сообщению прикрепляется дополнительная информация, в зависимости от произошедшего события:

100001 Передача конфигурации АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ, к которому подключился удаленный администратор, IP адрес удаленного администратора, текстовый комментарий удаленного администратора;

100003 Изменение конфигурации АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ, к которому подключился удаленный администратор, IP адрес удаленного администратора, текстовый комментарий удаленного администратора;

100004 Установка ключей ФПСУ АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ, к которому подключился удаленный администратор, IP адрес удаленного администратора, служебный текст «Ключ» имя группы ключей, номер серии ключей, номер комплекта ключей, текстовый комментарий удаленного администратора;

100005 Удаление ключей ФПСУ АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ, к которому подключился удаленный администратор, IP адрес удаленного администратора, служебный текст «Ключ» имя группы ключей, номер серии ключей, номер комплекта ключей, текстовый комментарий удаленного администратора;

100006 Установка ключа ЦГКК АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ, к которому подключился удаленный администратор, IP адрес удаленного администратора, служебный текст «Криптосеть номер» номер установленной Криптосети Клиентов, текстовый комментарий удаленного администратора;

100007 Удаление ключа ЦГКК АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ, к которому подключился удаленный администратор, IP адрес удаленного администратора, служебный текст «Криптосеть номер» номер удаленной Криптосети Клиентов, текстовый комментарий удаленного администратора;

100008 Перезагрузка ФПСУ АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ, к которому подключился удаленный администратор, IP адрес удаленного администратора;

100009 Согласование времени с АДМ – служебный текст «Администратор» имя удаленного администратора, номер порта ФПСУ, к которому подключился удаленный администратор, IP адрес удаленного администратора, текстовый комментарий удаленного администратора;

100010 Подключение УА – служебный текст «Удаленный администратор», имя удаленного администратора, служебный текст «подключился с IP-адреса» IP адрес удаленного администратора, «на порт» PORT;

110001 Локальная установка ключей ФПСУ – служебный текст «Локальная установка ключей ФПСУ, Ключ», имя группы ключей, номер ключа, служебный текст «Серия» номер серии ключей, служебный текст «предъявлен токен» имя(роль) локального администратора;

110002 Локальное удаление ключей ФПСУ АДМ – служебный текст «Локальное удаление ключей ФПСУ, Ключ», имя группы ключей, номер ключа, служебный текст «Серия» номер серии ключей, служебный текст «предъявлен токен» имя(роль) локального администратора;

110003 Локальная установка ключа ЦГКК – служебный текст «Локальная установка ключей клиентов, Криптосеть», имя Криптосети, служебный текст «Серия» номер серии ключей, служебный текст «предъявлен токен» имя(роль) локального администратора;

110004 Локальное удаление ключа ЦГКК – служебный текст «Локальное удаление ключей клиентов, Криптосеть», имя Криптосети, служебный текст «Серия» номер серии ключей, служебный текст «предъявлен токен» имя(роль) локального администратора;

110005 Локальное изменение конфигурации – служебный текст «Локальное изменение конфигурации», служебный текст «предъявлен токен» имя(роль) локального администратора;

110006 Изменение конфигурации LAN-адаптеров – служебный текст «Локальное изменение конфигурации LAN-адаптеров», служебный текст «предъявлен токен» имя локального администратора;

110007 Локальное изменение настроек дополнения – серийный номер ФПСУ, служебный текст «Локальное изменение настроек дополнения:», название дополнения, изменённые настройки, служебный текст «предъявлен токен» имя(роль) локального администратора;

200001 Потеряна связь с ФПСУ – серийный номер и IP-адрес ФПСУ, с которым потеряно защищенное соединение;

200002 Восстановлена связь с ФПСУ – серийный номер и IP-адрес ФПСУ, с которым восстановлено защищенное соединение;

200003 Включение ФПСУ – дополнительные поля отсутствуют;

200004 Выключение ФПСУ – дополнительные поля отсутствуют;

200005 Перегруженность ФПСУ – загрузка ЦПУ, в процентах;

200007 Период <MARK> – служебный текст «CPU(%)», загрузка ЦПУ, «Температура», температура ЦПУ по шкале Цельсия;

200011 Потеряна связь с ФПСУ в потоке – номер потока, номер UDP порта, имя туннеля, IP-адрес туннеля;

200021 Восстановлена связь с ФПСУ в потоке – номер потока, номер UDP порта, имя туннеля, IP-адрес туннеля;

300001 Соединение с клиентом – имя подключившегося Клиента, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, серийный номер устройства VPN-Key/Client, служебный текст «Порт», номер порта ФПСУ, к которому произошло подключение; служебный текст «IP», IP-адрес порта ФПСУ, к которому произошло подключение; служебный текст «IP-адрес NAT/Real», выданный от ФПСУ NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети, MAC-адрес подключившегося Клиента, служебный текст «HW vers:», версия микрокода устройства VPN-Key/Клиент, служебный текст «SW vers:» версия программного обеспечения ФПСУ-IP/Клиента, служебный текст «OS vers:» название и версия операционной системы рабочей станции подключившегося Клиента;

300002 Разъединение с клиентом – имя отключившегося Клиента, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, серийный номер устройства VPN-Key/Client, служебный текст «Port», номер порта ФПСУ, от которого произошло отключение; служебный текст «IP», IP-адрес порта ФПСУ, от которого произошло отключение; служебный текст «IP-адрес NAT/Real», полученный от ФПСУ NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети, MAC-адрес отключившегося Клиента;

300004 Ошибка авторизации – служебный текст «RADIUS: ошибка авторизации, клиент» имя Клиента, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, серийный номер устройства VPN-Key/Client;

300010 Запрос получения ключа – служебный текст «RKL: Запрос на получение ключа» имя группы ключей, номер ключа, служебный текст «токен» имя(роль) локального администратора, O/C, ID, ключ, лицензия, администратор;

300011 Запрос обновления ключа – служебный текст «RKL: Запрос на обновление ключа» имя группы ключей, номер ключа, служебный текст «токен» имя(роль) локального администратора, O/C, ID, ключ, лицензия, администратор;

300012 Подтверждение получения ключа – служебный текст «RKL: Подтверждение получения ключа» имя группы ключей, номер ключа, ID, терминал;

300013 Не удалось установить соединение – служебный текст «Не удалось установить соединение» имя Клиента, номер Криптосети Клиента - номер Группы Клиента - номер Клиента в группе, служебный текст «Port», номер порта ФПСУ, с которого не удалось соединиться; служебный текст «IP», IP-адрес порта ФПСУ, с которого не удалось соединиться, служебный текст «Отвергается доступ в криптосеть»;

300013 Не удалось установить соединение – служебный текст «Не удалось установить соединение» имя Клиента, номер Криптосети Клиента - номер Группы Клиента - номер Клиента в группе, служебный текст «Port», номер порта ФПСУ, с которого не удалось соединиться; служебный текст «IP», IP-адрес порта ФПСУ, с которого не удалось соединиться, служебный текст «Неверная аппаратная привязка клиента»;

300020 RADIUS: успешная авторизация – служебный текст «RADIUS: успешная авторизация» имя Клиента, логин на сервере RADIUS, номер Криптосети Клиента - номер Группы Клиента - номер Клиента в группе, служебный текст «s/n», серийный номер устройства VPN-Key/Client, служебный текст «Port», номер порта ФПСУ, с которого произошла авторизация; служебный текст «IP», IP-адрес порта ФПСУ, с которого произошла авторизация; служебный текст «IP-адрес NAT/Real», полученный от ФПСУ NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети;

300021 Accept от RADIUS – уровень доступа, имя Клиента, служебный текст «Порт»,

номер порта ФПСУ, с которого произошла авторизация; служебный текст «IP», IP-адрес порта ФПСУ, с которого произошла авторизация; служебный текст «IP-адрес NAT/Real», полученный от ФПСУ NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети; MAC-адрес;

300022 Reject от RADIUS – IP-адрес RADIUS сервера, имя Клиента, логин RADIUS, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, служебный текст «Порт», номер порта ФПСУ, с которого произошла авторизация; служебный текст «IP», IP-адрес порта ФПСУ, с которого произошла авторизация; служебный текст «IP-адрес NAT/Real», полученный от ФПСУ NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети; MAC-адрес;

300023 CoA от RADIUS – уровень доступа, IP-адрес RADIUS сервера, имя Клиента, логин RADIUS, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, служебный текст «Порт», номер порта ФПСУ, с которого произошла авторизация; служебный текст «IP», IP-адрес порта ФПСУ, с которого произошла авторизация; служебный текст «IP-адрес NAT/Real», полученный от ФПСУ NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети; MAC-адрес;

300024 DM от RADIUS – IP-адрес RADIUS-сервера, имя Клиента, логин RADIUS, номер Криптосети Клиента, номер Группы Клиента, номер Клиента в группе, служебный текст «Порт», номер порта ФПСУ, с которого произошла авторизация; служебный текст «IP», IP-адрес порта ФПСУ, с которого произошла авторизация; служебный текст «IP-адрес NAT/Real», полученный от ФПСУ NAT-IP-адрес Клиента, IP-адрес Клиента во внешней сети; MAC-адрес;

400001 Переход Основной - Резервный – режим функционирования ФПСУ горячего резерва, на который произошло переключение (основной или резервный);

400002 Нет связи Основной - Резервный – режим функционирования ФПСУ горячего резерва, с которым не удаётся установить связь (основной или резервный);

400003 Нет канала Основной - Резервный – служебный текст «Нет связи на порту», номер порта ФПСУ, служебный текст «горячего резерва»;

500001 Link UP порта – логический номер LAN-порта, а также его IP-адрес;

500002 Link DOWN порта – логический номер LAN-порта, а также его IP-адрес;

500003 Перегрев – температура ЦПУ по шкале Цельсия;

500004 Сбой диска – дополнительные поля отсутствуют;

500005 Текущая температура – служебный текст «Температура», температура ЦПУ по шкале Цельсия;

500006 Окончание поддержки – служебный текст «Поддержка комплекса истекает», дата;

500007 Sfp мониторинг – служебный текст «Порт» порт, «Sfp» (RX мощность, TX мощность, температура): значение параметра;

500008 xstats портов – порт, параметр значение параметра,...;
500009 Появление нового дампа – служебный текст «Сгенерирован новый дамп», имя файла дампа;
510001 MAC-адрес занесен в ARP-таблицу – служебный текст «MAC-адрес добавлен» MAC-адрес станции, IP-адрес станции, «Порт ФПСУ» порт, «VLAN ID» VLAN;
510002 MAC-адрес исключен из ARP-таблицы – служебный текст «MAC-адрес удален» MAC-адрес станции, IP-адрес станции, «Порт ФПСУ» порт, «VLAN ID» VLAN;
700001 Соединение разрешено МЭ – служебный текст «Соединение разрешено МЭ» , служебный текст «SRC IP:port» IP-адрес:порт «(SRC NAT/MAP [IP-адрес:порт])», служебный текст «DST IP:port» IP-адрес:порт «(DST NAT/MAP [IP-адрес:порт])», «Протокол» протокол, «Правило» правило, «SRC данные/пакеты» byte/pkt, «DST данные/пакеты» byte/pkt, «Входящий порт ФПСУ» порт, «Исходящий порт ФПСУ» порт, «Длительность» время «сек»;
700002 Соединение запрещено МЭ – служебный текст «Соединение запрещено МЭ» , служебный текст «SRC IP:port» IP-адрес:порт, служебный текст «DST IP:port» IP-адрес:порт, «Протокол» протокол, «Правило» правило (FLOOD/IPS/RADM), «Порт ФПСУ» порт, время;
700003 Абонент заблокирован МЭ (flood) – служебный текст «FLOOD заблокировал», IP-адрес, период блокировки «с до» в формате hh:mm:ss;
700004 Абонент разблокирован МЭ (flood) – служебный текст «FLOOD разблокировал», IP-адрес, время в формате hh:mm:ss;
700005 Абонент заблокирован СОВ – служебный текст «IPS заблокировал», IP-адрес, период блокировки «с до» в формате hh:mm:ss;
700006 Абонент разблокирован СОВ – служебный текст «IPS разблокировал», IP-адрес, время разблокировки в формате hh:mm:ss;
700007 Блокировка абонента МЭ ФПСУ – служебный текст «Администратор» имя администратора, «заблокировал IP» IP-адрес, период блокировки «с до» в формате mm-dd-yyyy hh:mm:ss;
700008 Разблокировка абонента МЭ ФПСУ – служебный текст «Администратор» имя администратора, «разблокировал IP» IP-адрес, период разблокировки «с» в формате mm-dd-yyyy hh:mm:ss;
700009 Администратор заблокировал Port – служебный текст «Администратор» имя администратора служебный текст «заблокировал Port» порт «с» время блокировки в формате mm-dd-yyyy hh:mm:ss;
700010 Администратор разблокировал Port – служебный текст «Администратор» имя администратора «разблокировал Port» порт «с» время разблокировки в формате

mm-dd-yyyy hh:mm:ss;

700011 Администратор заблокировал Proto – служебный текст «Администратор» имя администратора «заблокировал Proto» протокол «с» время блокировки в формате mm-dd-yyyy hh:mm:ss;

700012 Администратор разблокировал Proto – служебный текст «Администратор» имя администратора «разблокировал Proto» протокол «с» время разблокировки в формате mm-dd-yyyy hh:mm:ss;

700013 Соединение запрещено МЭ (DPI) – служебный текст «Соединение запрещено МЭ (DPI)», IP-адрес:порт источника, IP-адрес:порт назначения, служебный текст «Протокол» протокол, служебный текст «Правило» правило DPI, время;

700013 FLOOD включился – служебный текст «FLOOD включился», протокол {ICMP, UDP, TCP};

700014 FLOOD выключился – служебный текст «FLOOD выключился», протокол {ICMP, UDP, TCP};

820001 Начало отчетного периода – идентификатор узла, абонент, СКЗИ_локальный - СКЗИ_удаленный, длительность периода (сек), лимит ключей;

820002 Выдан ключ абоненту – идентификатор узла, абонент, СКЗИ_локальный - СКЗИ_удаленный, остаток лимита ключей;

820003 Ошибка выдачи ключа абоненту – идентификатор узла, абонент, СКЗИ_локальный - СКЗИ_удаленный, код ошибки;

900099 IDS: система запускается – дополнительные поля отсутствуют;

900100 IDS: система запущена – дополнительные поля отсутствуют;

900101 IDS: система остановлена – дополнительные поля отсутствуют;

900103 IDS: База решающих правил обновлена – служебный текст «IDS: База решающих правил обновлена», общее количество правил, количество включенных правил, количество добавленных правил, количество изменённых правил, количество удаленных правил;

900104 IDS: Переконфигурирование завершено успешно – дополнительные поля отсутствуют;

900200 IDS: Периодическое сообщение о статусе IDS – служебный текст «-- MARK --», служебный текст «detect.alert», количество срабатываний правил, служебный текст «capture.kernel_packets», количество обработанных пакетов с момента предыдущего сообщения MARK, служебный текст «capture.kernel_drops», количество сброшенных пакетов;

900401 IDS: Сработала тревога уровня 1 (максимальная опасность) – служебный текст «IDS: Тревога уровня 1», SID сработавшего правила, группа сработавшего правила, протокол сработавшего правила, IP-адрес источника тревоги, порт источника, IP-адрес назначения, порт назначения;

900402 IDS: Сработала тревога уровня 2 – служебный текст «IDS: Тревога уровня 2», SID сработавшего правила, группа сработавшего правила, протокол сработавшего правила, IP-адрес источника тревоги, порт источника, IP-адрес назначения, порт назначения;
900403 IDS: Сработала тревога уровня 3 – служебный текст «IDS: Тревога уровня 3», SID сработавшего правила, группа сработавшего правила, протокол сработавшего правила, IP-адрес источника тревоги, порт источника, IP-адрес назначения, порт назначения;
900404 IDS: Сработала тревога уровня 4 (и более, вплоть до 255, но код сообщения не меняется после 4х) – служебный текст «IDS: Тревога уровня 4», SID сработавшего правила, группа сработавшего правила, протокол сработавшего правила, IP-адрес источника тревоги, порт источника, IP-адрес назначения, порт назначения;
900410 IDS: Эвристикой обнаружены потенциальные угрозы – служебный текст «IDS: Эвристикой обнаружены потенциальные угрозы», идентификатор события, IP-адреса;
900420 IDS: Записи в локальной БД о сработавших тревогах были сжаты и перенесены в архив – дополнительные поля отсутствуют;
900430 IDS: Запрос на блокировку IP через МЭ ФПСУ – уровень серьёзности угрозы, сообщение, IP-адрес источника угрозы, IP-адрес назначения (при сообщении «Heuristic-C» IP-адрес назначения - 0).
900500 IDS: Ошибка — невозможно запустить систему – служебный текст «IDS: Невозможно запустить систему», внутренний код ошибки (для разработчиков), описание ошибки;
900501 IDS: Критическая проблема при работе – служебный текст «IDS: Критическая проблема при работе», внутренний код ошибки (для разработчиков), описание ошибки;
900502 IDS: Ошибка переконфигурации – служебный текст «IDS: Ошибка переконфигурации», внутренний код ошибки (для разработчиков), описание ошибки;
900503 IDS: Критическая ошибка при запуске – служебный текст «IDS: Критическая ошибка при запуске», внутренний код ошибки (для разработчиков), описание ошибки;
900505 IDS: Ведение локальной БД сработавших тревог отключено - достигнут лимит – дополнительные поля отсутствуют;

13. 5. DNS-серверы

ФПСУ поддерживает стандартный протокол DNS для некоторых установленных подсистем, используется для разрешения сетевых имён. При подключенной системе удаленной загрузки ключевых данных клиентов (RKL) на ФПСУ необходимо задать DNS-

сервер.

Для указания DNS-сервера выберите в меню «Сетевые сервисы» конфигурации ФПСУ команду *«DNS-серверы»*:

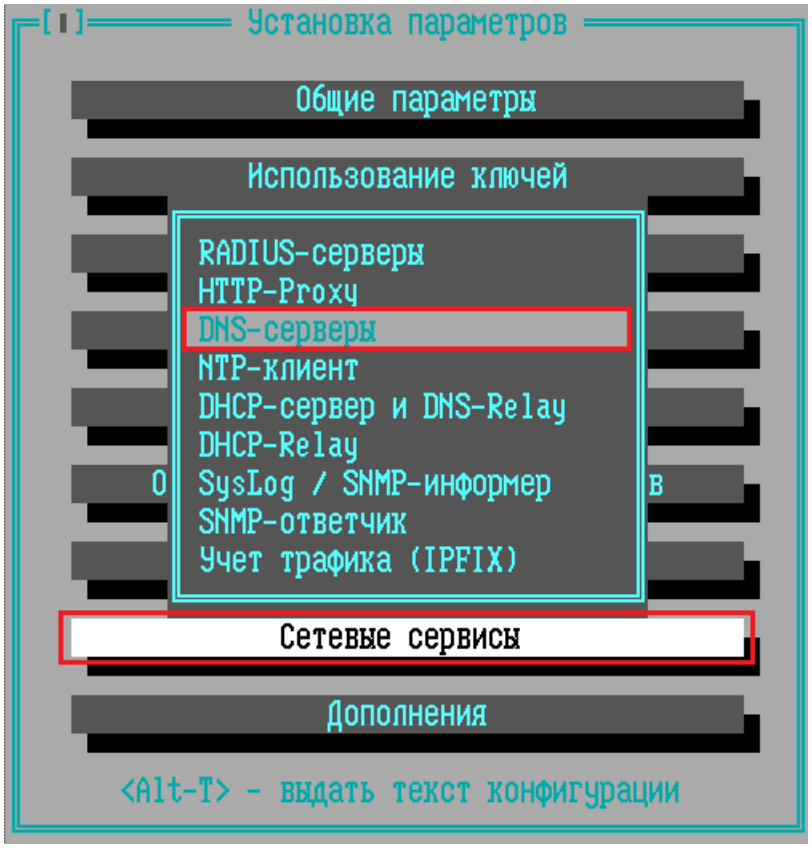


Рисунок 483 - Команда меню «Сетевые сервисы» → «DNS-серверы»

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

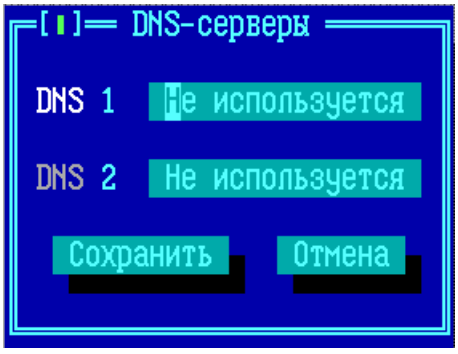


Рисунок 484 - Окно «DNS-серверы»

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

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

13. 6. DHCP-сервер и DNS-Relay

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

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

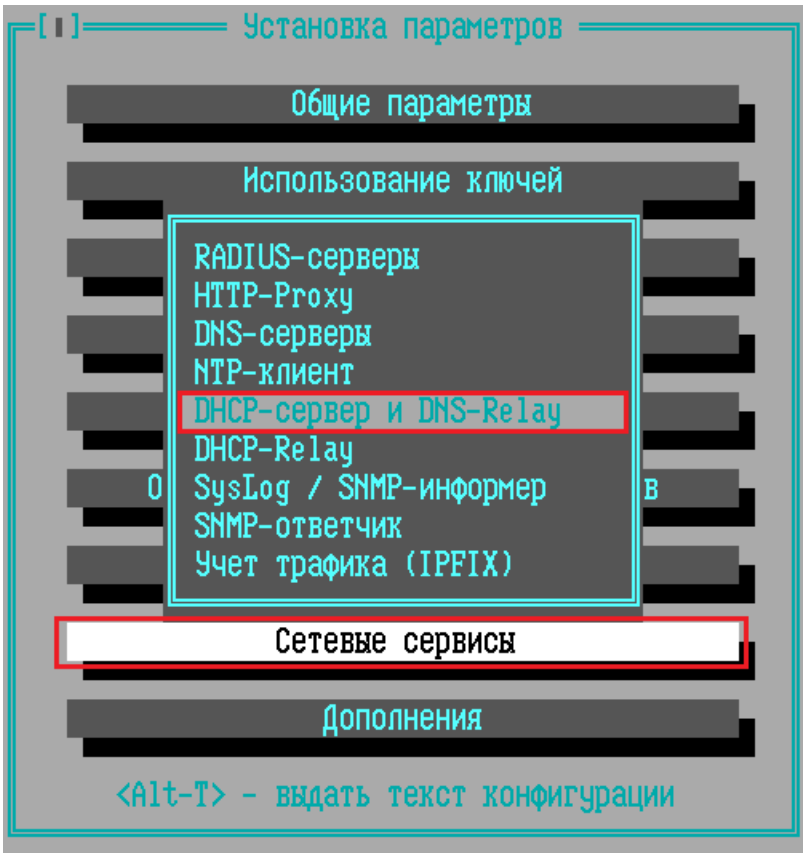


Рисунок 485 - Команда меню «Сетевые сервисы» → «DHCP-сервер и DNS-Relay»

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

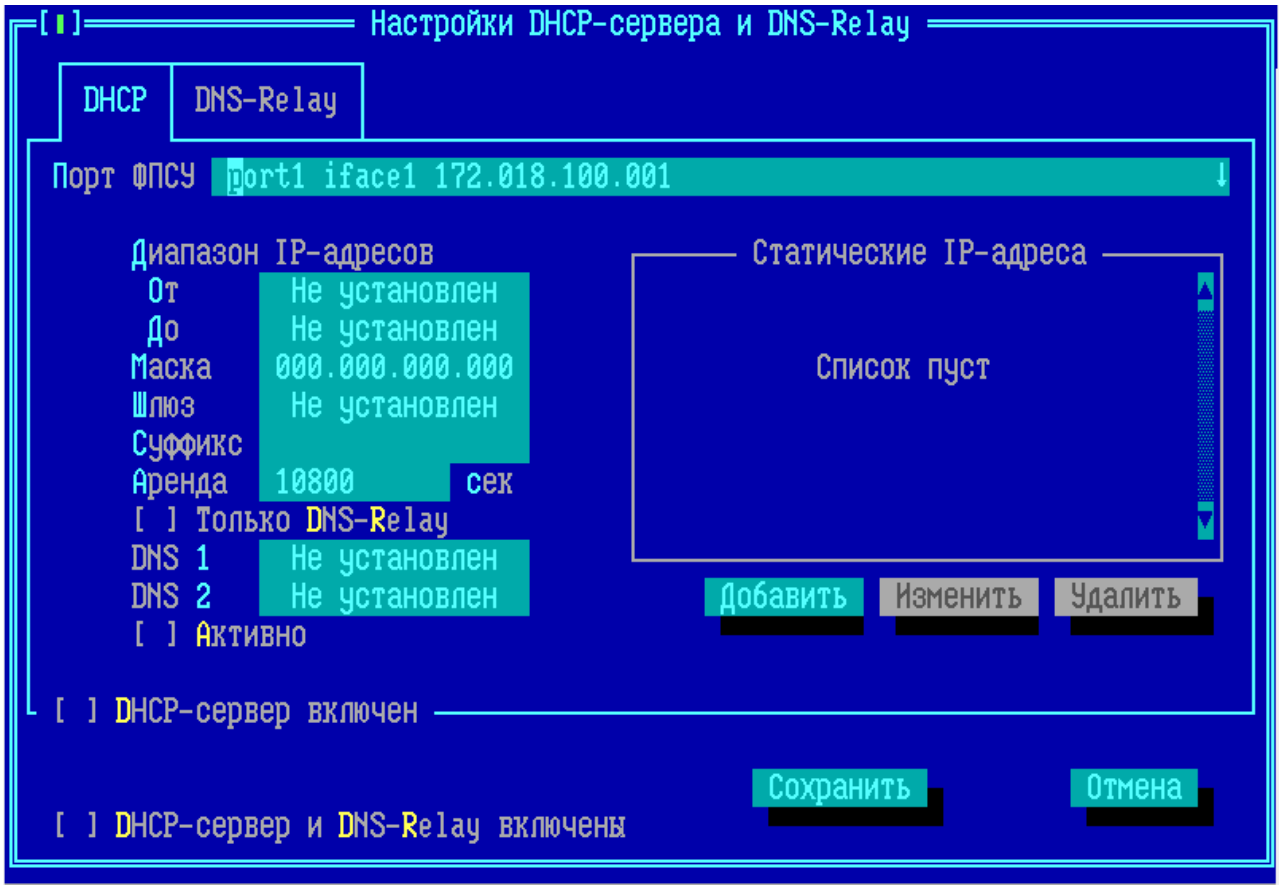


Рисунок 486 - Вкладка «DHCP»

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

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

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

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

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

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

Только DNS-Relay — флаг, устанавливающий работу ФПСУ в режиме ретрансляции DNS, клиенту не будут присылаться настройки внешних DNS-серверов. Если флаг снят, DHCP-клиенту будут отправлены IP-адреса из полей *DNS 1 и DNS 2* в качестве основного и дополнительного DNS-сервера.

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

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

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



Рисунок 487 - Добавление статического IP-адреса

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

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

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

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

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

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

ФПСУ поддерживает ретрансляцию запросов DNS. ФПСУ получает DNS-запросы от абонентов, перенаправляет эти запросы на указанные в списке DNS-серверы и пересылает обратно полученные ответы от DNS-серверов абонентам.

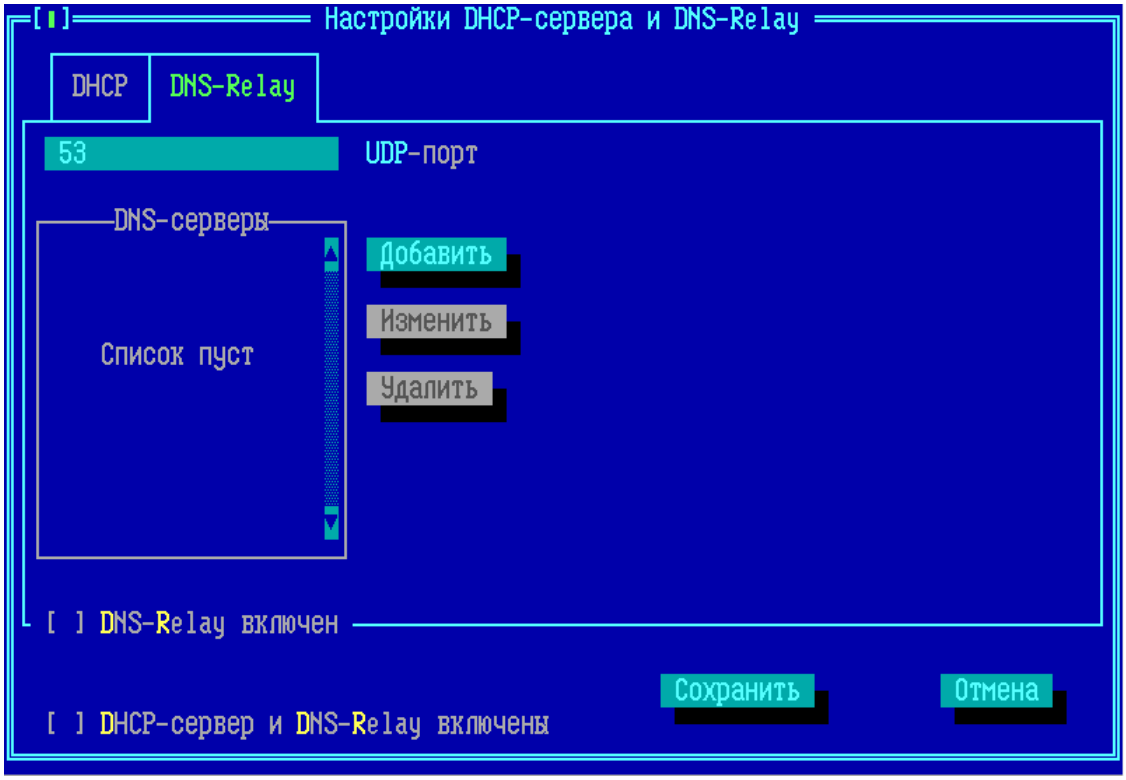


Рисунок 488 - Вкладка «DNS-Relay»

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

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

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

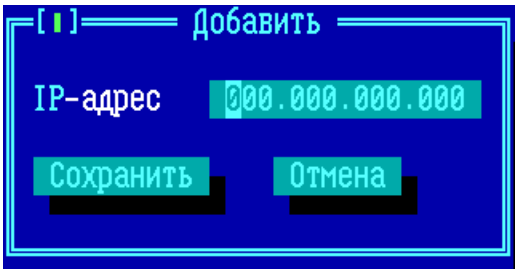


Рисунок 489 - Добавление DNS-сервера

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

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

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

13. 7. DHCP-Relay

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

Для включения службы в рабочий режим, требуется выполнить настройки:

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

13. 7. 1. Создание списка DHCP-серверов

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

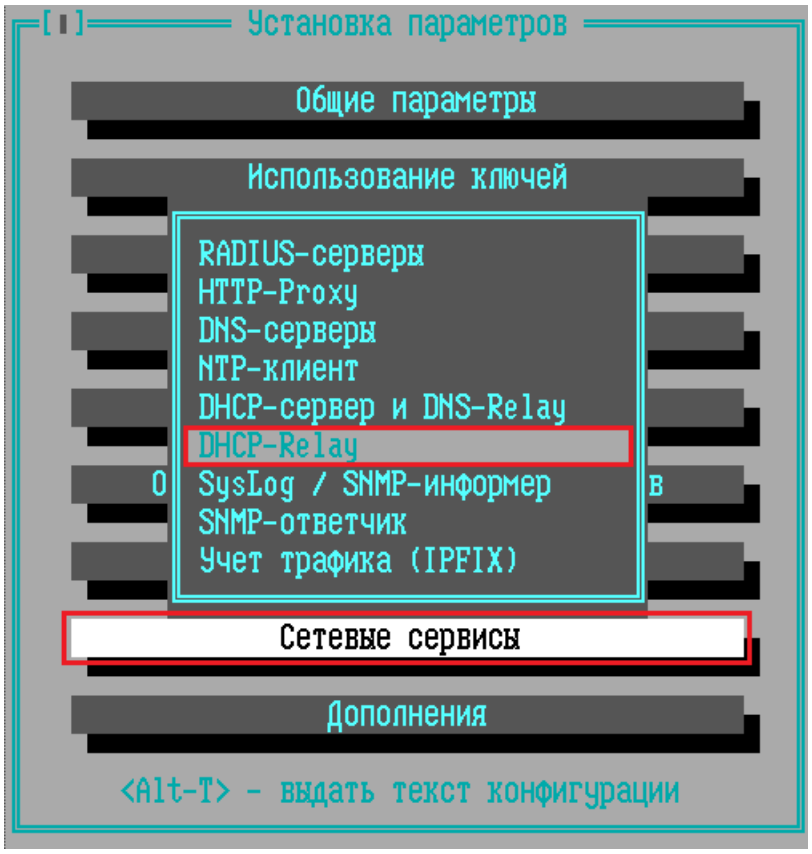


Рисунок 490 - Команда меню «Сетевые сервисы» → «DHCP-Relay»

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



Рисунок 491 - Список DHCP-серверов

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

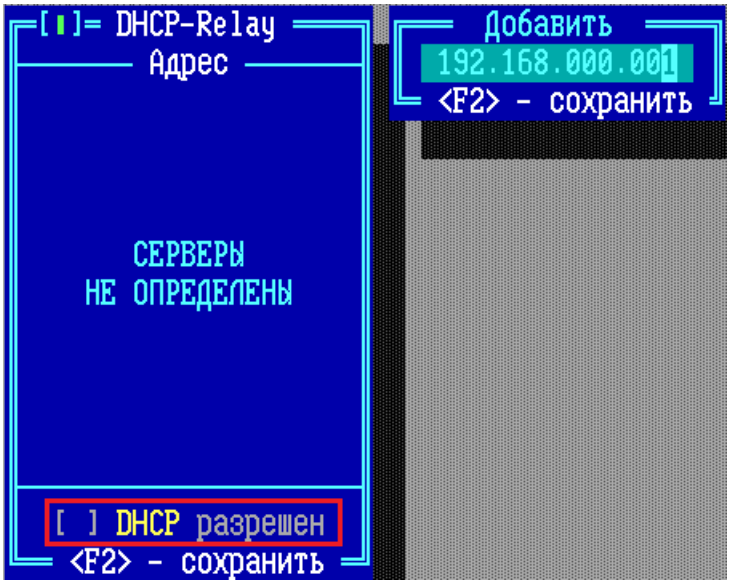


Рисунок 492 - Добавление DHCP-сервера

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

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

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

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

13. 7. 2. Настройка DHCP-Relay на портах ФПСУ

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

ВНИМАНИЕ! Назначить порту DHCP-сервер получится только в том случае, если IP-адреса портов 1 и 2 порта ФПСУ **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»***).

Вход в интерфейс назначения DHCP-серверов порту ФПСУ происходит из окна описания основных настроек порта.

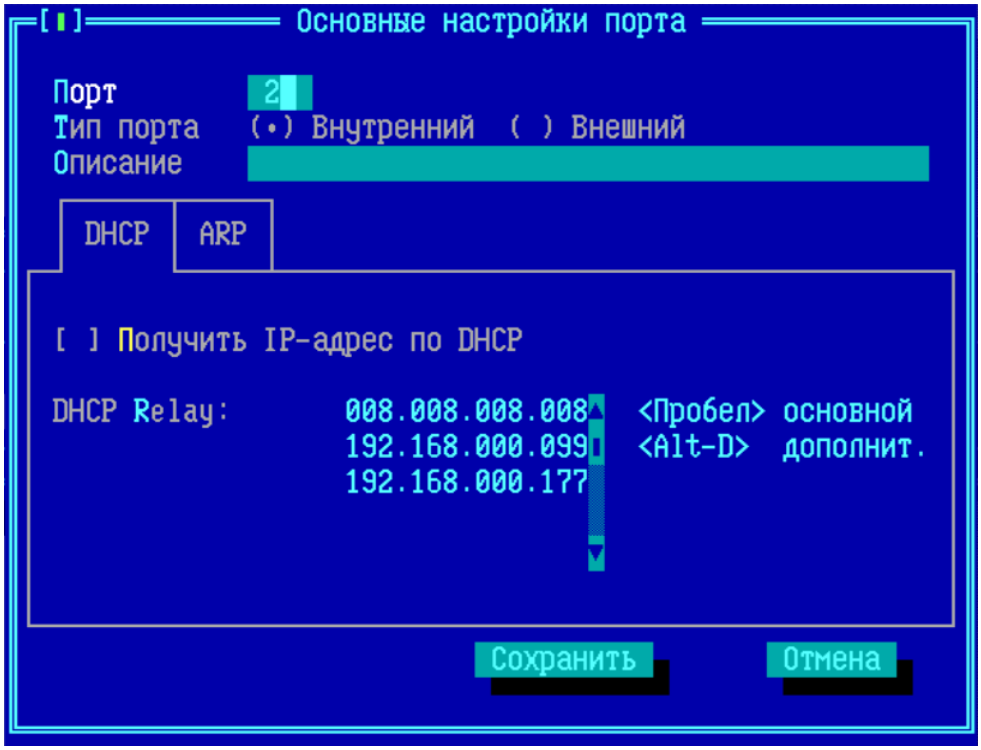


Рисунок 493 - Параметры порта ФПСУ

В списке DHCP-Relay можно выбрать основной и запасной DHCP-сервер для ретрансляции всех DHCP-запросов, поступающих на описываемый порт ФПСУ.

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

После установления адреса основного DHCP-сервера, можно выбрать 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+D>*. Запись адреса дополнительного DHCP-сервера будет выделена знаком «R√».

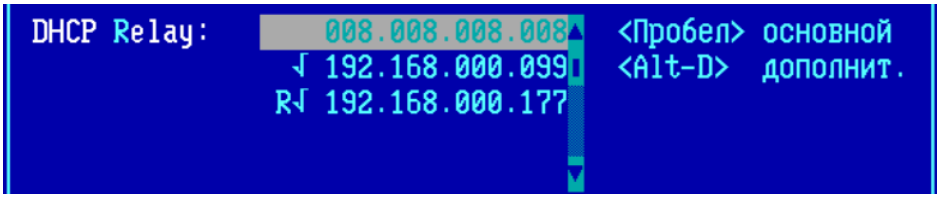


Рисунок 494 - Настройка DHCP на порту

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

13. 8. Http-proxy ФПСУ

На ФПСУ 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:

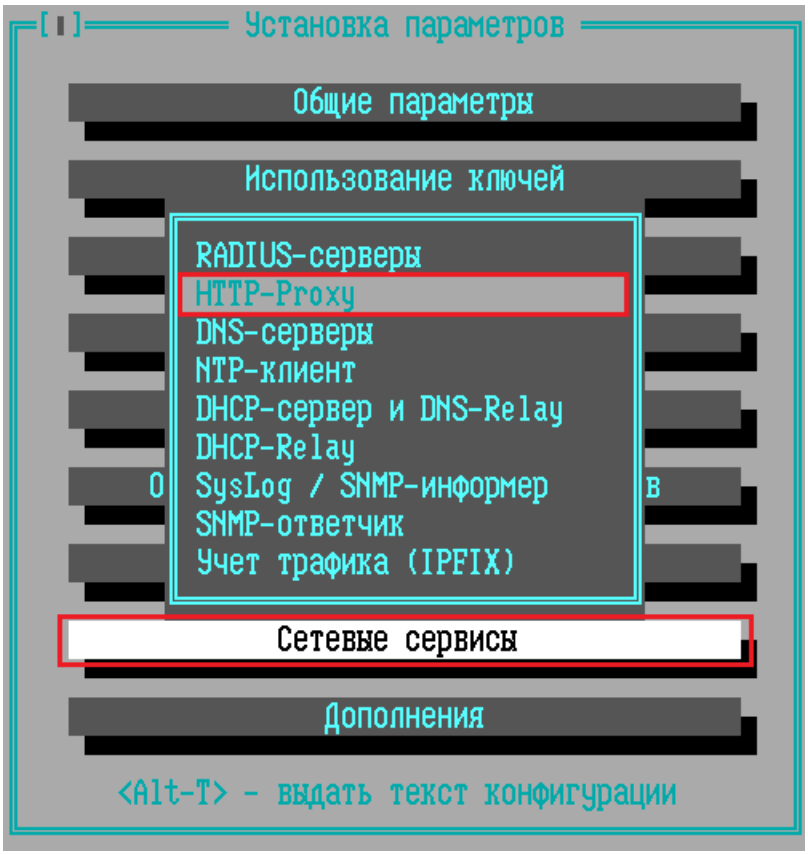


Рисунок 495 - Команда перехода в конфигурацию proxy на ФПСУ

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

ВНИМАНИЕ! В случае использования версии ФПСУ 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, в открывшемся окне настройки следует установить следующие параметры:

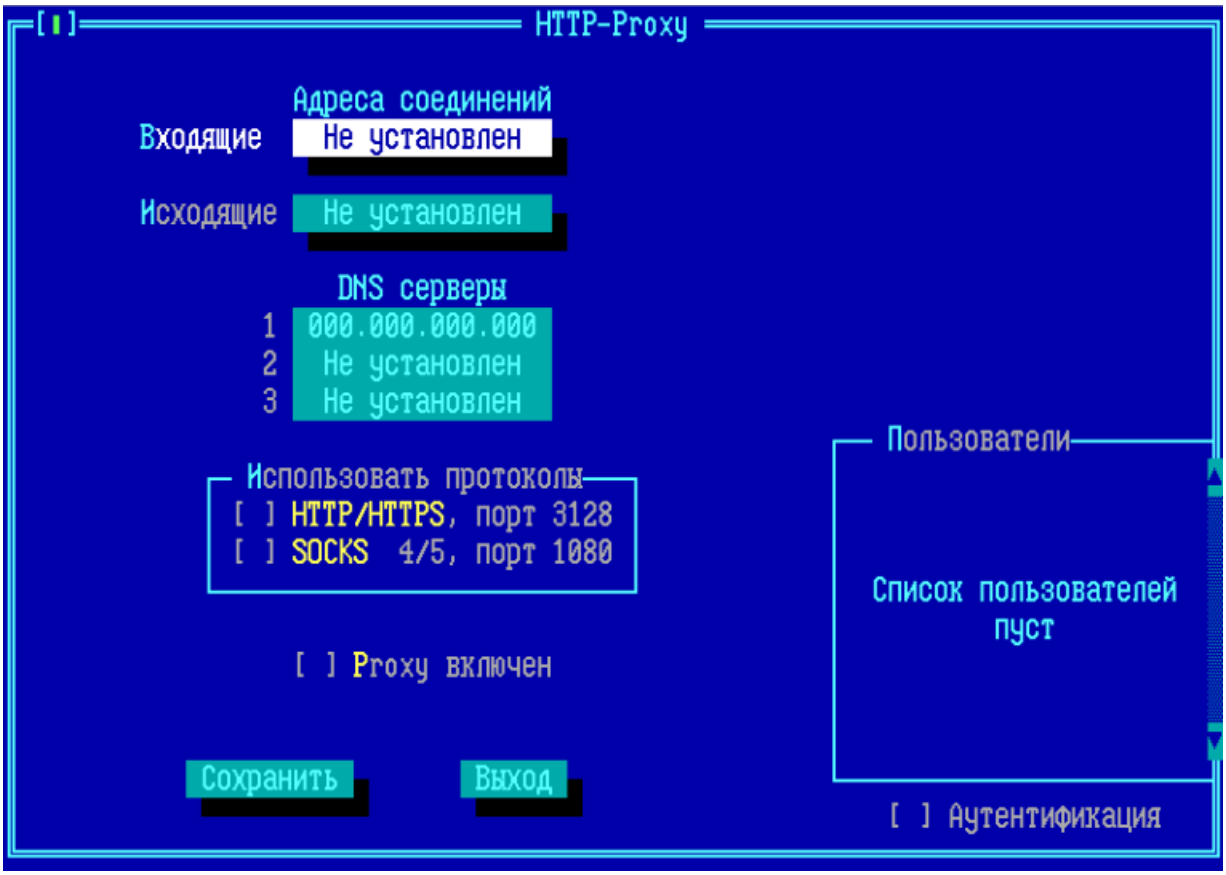


Рисунок 496 - Окно настроек HTTP-proxy

Адрес соединений, Входящие — здесь требуется указать IP-адрес логического порта ФПСУ, на котором будет запущена служба прокси для входящих соединений. Адрес выбирается из списка портов. 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, от которого будут переданы во внешнюю сеть пользовательские данные.

DNS серверы — для корректной работы http-прокси на ФПСУ, 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 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 будет принимать входящие соединения. Этот порт, вместе с IP-адресом входящих соединений, пользователи должны будут указать в браузере или операционной системе как порт прокси.

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

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

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

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

ВНИМАНИЕ! Если задействован межсетевой экран ФПСУ (см. пункт «Параметры доступа, правила трафика межсетевого экрана»), прокси на ФПСУ 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 в качестве прокси. Назначением устанавливается интерфейс ФПСУ, указанный в поле ***Адрес соединений, Входящие*** настроек прокси.
2. Правило, разрешающее передавать пакеты, источником которых является интерфейс ФПСУ, указанный в поле ***Адрес соединений, Исходящие***. Назначением устанавливаются IP-адреса, с которыми будут работать пользователи прокси.
3. Правило, разрешающее ФПСУ отправлять DNS-запросы на DNS-сервер. Источником пакетов является интерфейс ФПСУ, указанный в поле ***Адрес соединений, Входящие***, а назначением – IP-адреса DNS-серверов, заданных для прокси ФПСУ.

13. 8. 1. Авторизация на http-proxy

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

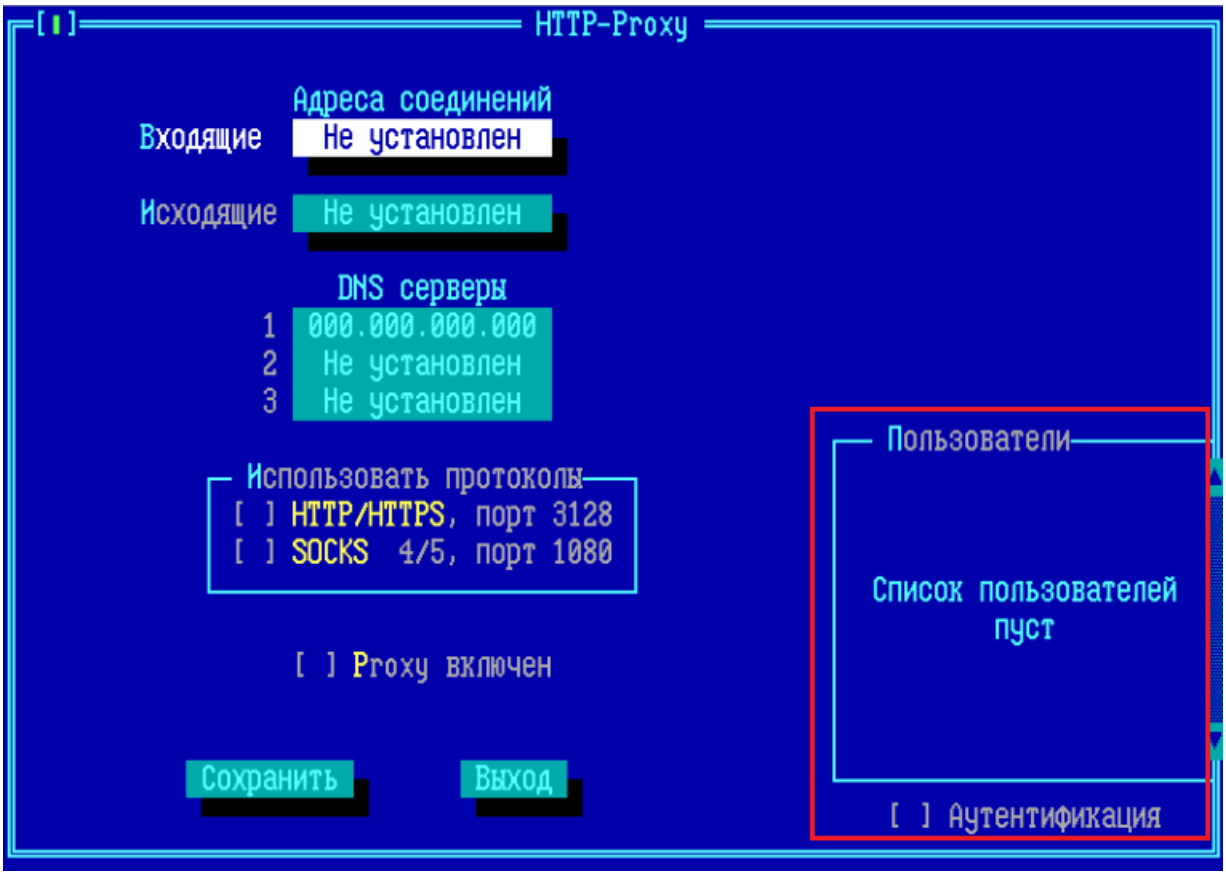


Рисунок 497 - Блок настройки пользователей proxy ФПСУ

При включении опции ***Аутентификация*** анонимный доступ пользователей к прокси запрещается. Обращение пользователя к прокси ФПСУ 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 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:

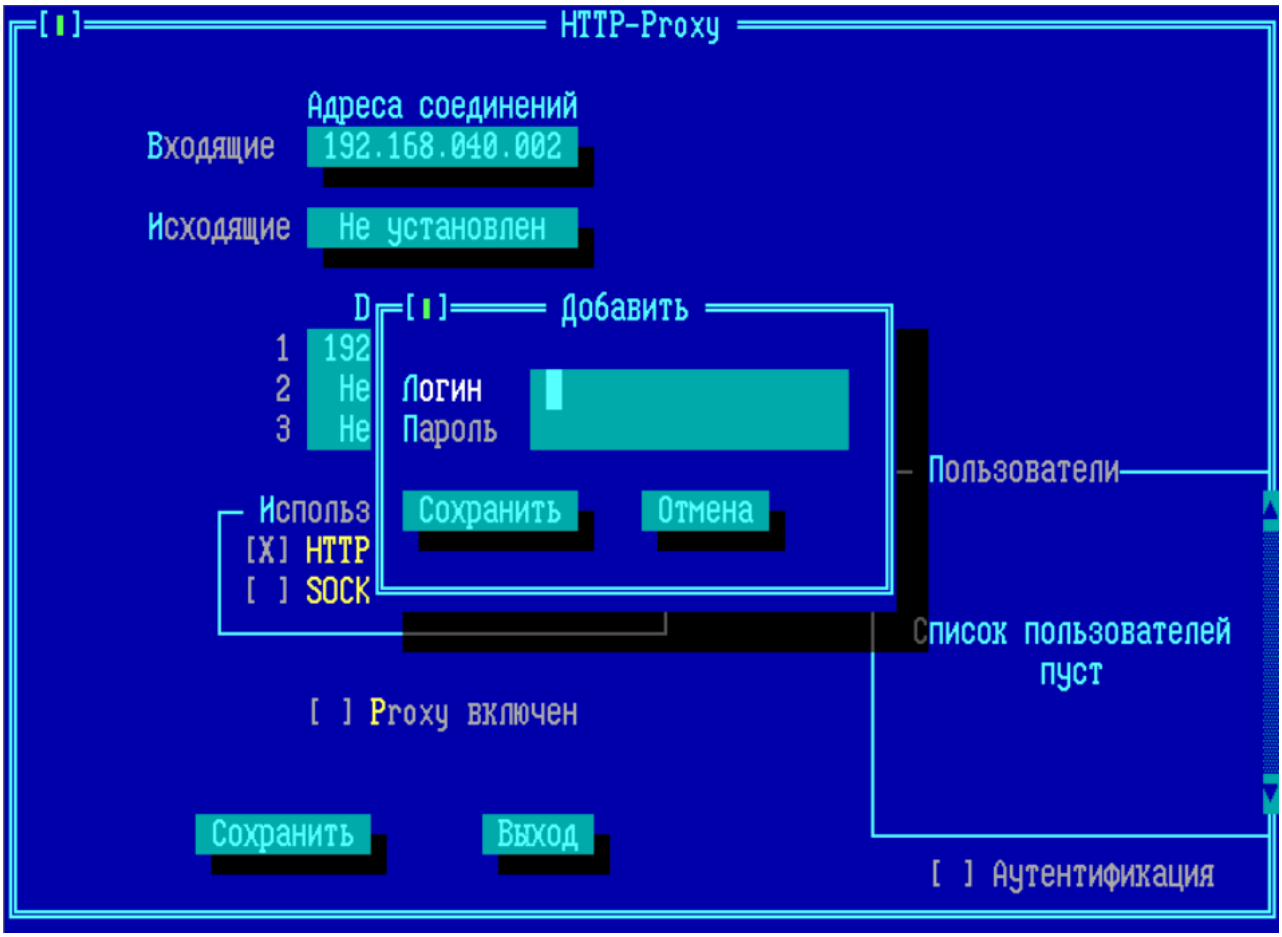


Рисунок 498 - Добавление учетной записи нового пользователя proxy ФПСУ

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

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

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

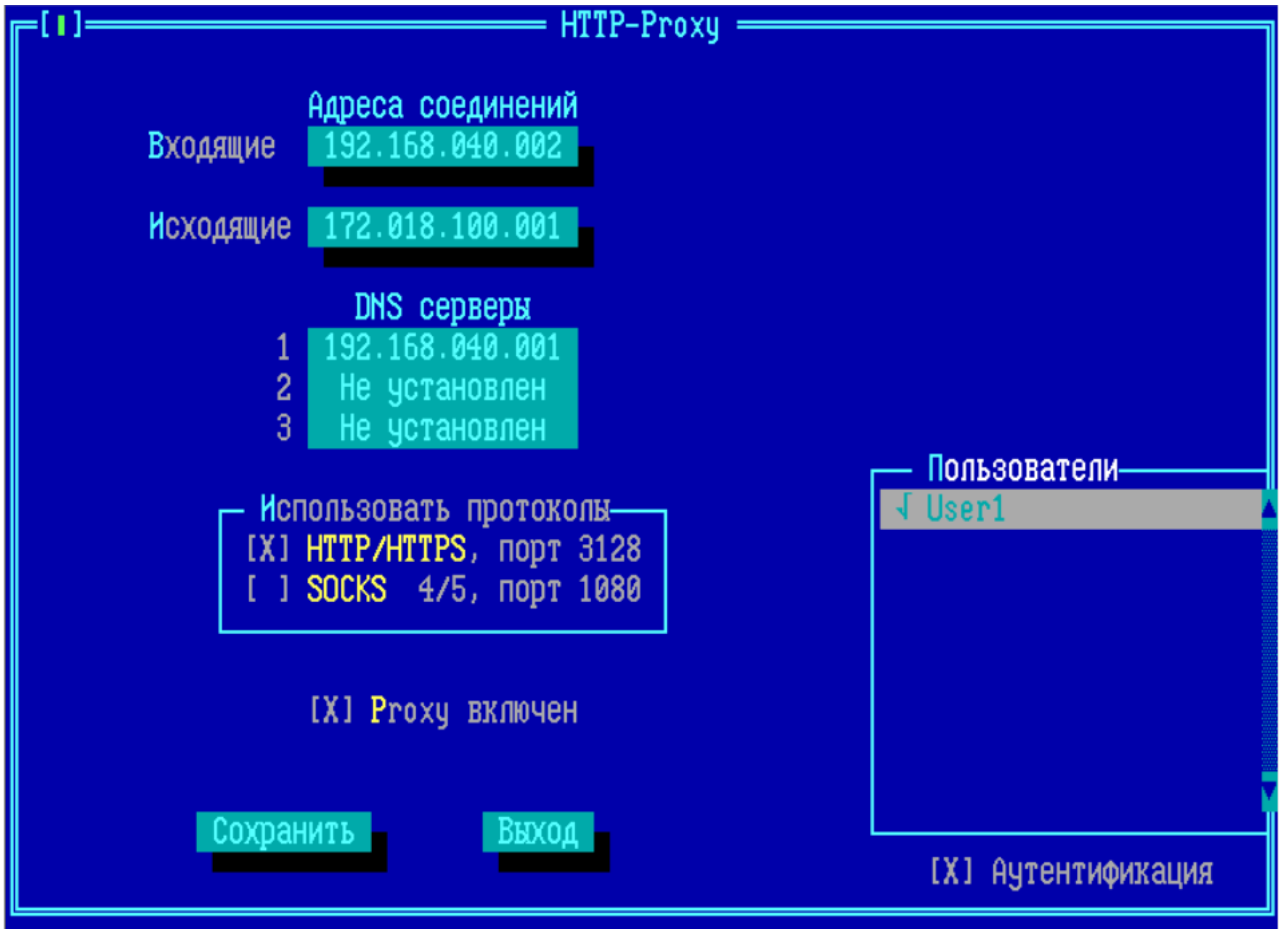


Рисунок 499 - Новый пользователь proxy ФПСУ добавлен

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

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

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

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

13. 9. Взаимодействие со средствами обнаружения вторжений

ФПСУ поддерживает взаимодействие со сторонними средствами обнаружения вторжений (далее СОВ). На ФПСУ реализован специальный SysLog сервер, принимающий сообщения по протоколу syslog, отправленные с одного IP-адреса СОВ, указанного администратором ФПСУ. Полученные с одобренного СОВ syslog-сообщения анализируются, и, если в них содержится текст заранее определенного администратором ФПСУ шаблона, то указанный в syslog сообщении IP-адрес заносится в стоп-лист межсетевого экрана ФПСУ на заданное администратором ФПСУ время.

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

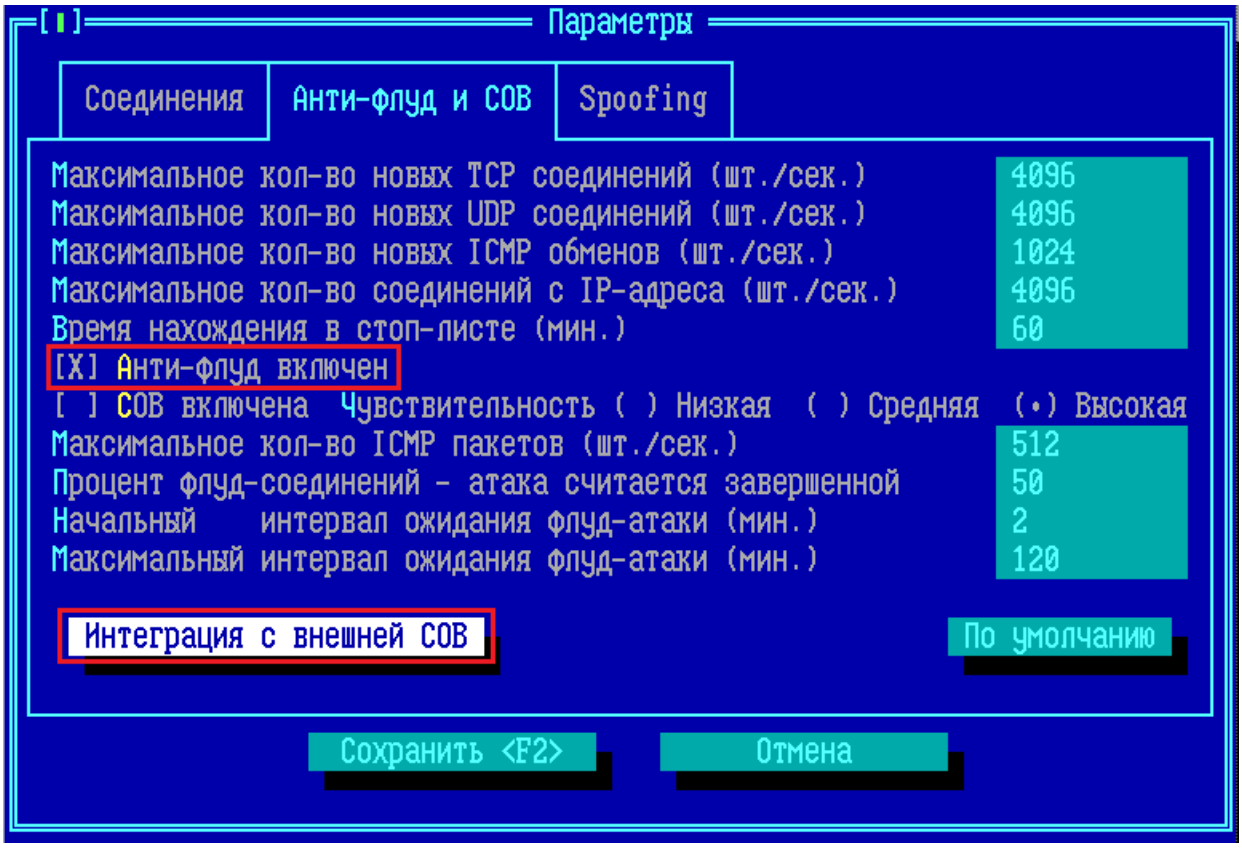


Рисунок 500 - Вызов интерфейса настройки взаимодействия с СОВ

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

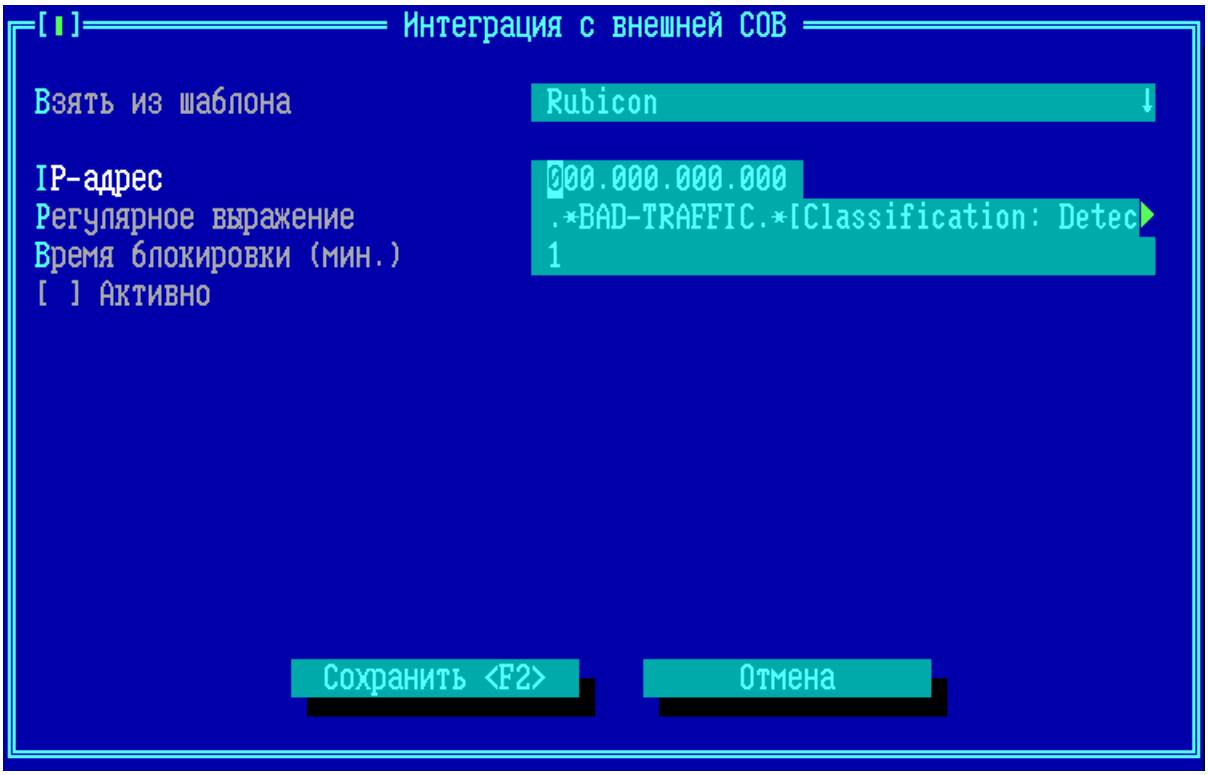


Рисунок 501 - Параметры взаимодействия с СОВ

Взять из шаблона – выбрать один из предложенных шаблонов взаимодействия с известными ФПСУ 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 будет принимать и анализировать syslog-сообщения. Syslog-сообщения с других IP-адресов будут сброшены.

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

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

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

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

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

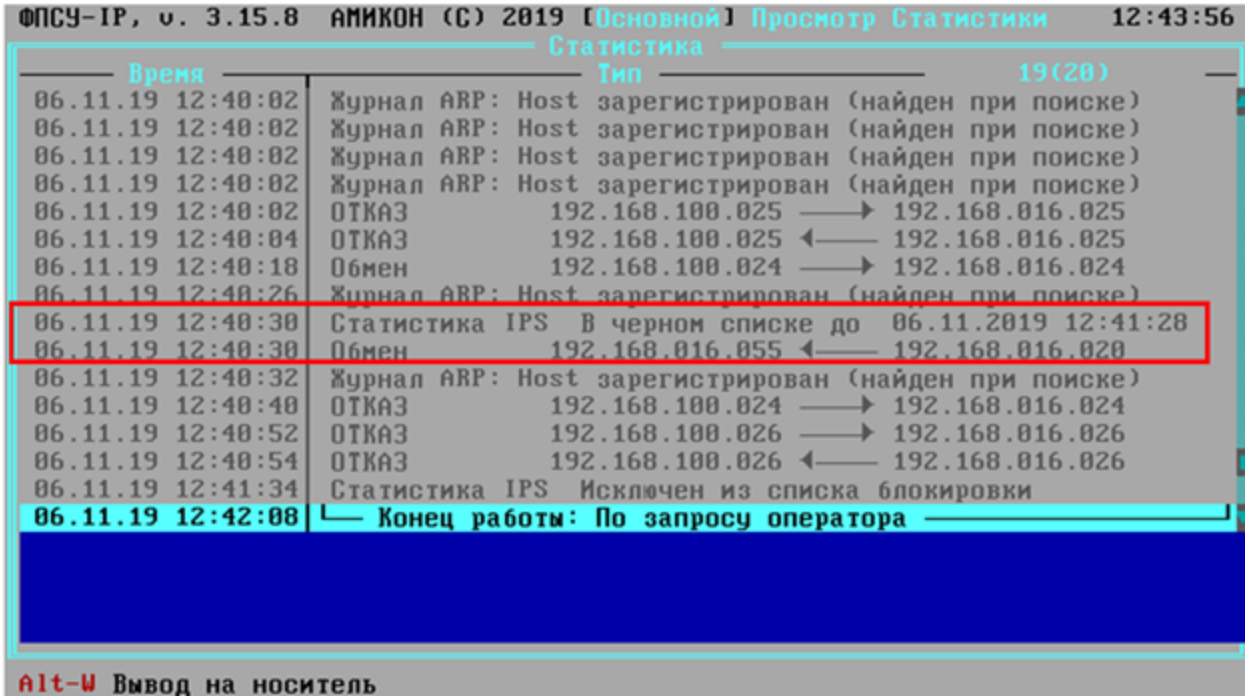


Рисунок 502 - Получено управляющее сообщение от СОВ

События блокировки передач абонентов по причине получения управляющего сообщения от СОВ (в случае совпадения полученного сообщения с заданным администратором ФПСУ 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 %».

13. 10. NTP-клиент ФПСУ

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»)!

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

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

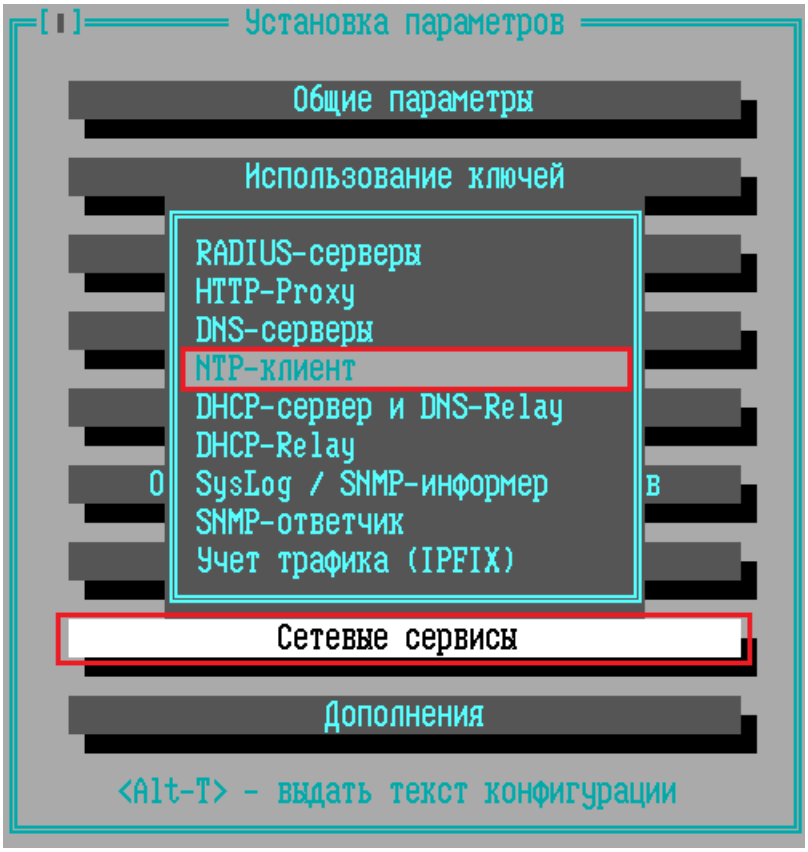


Рисунок 503 - Команда меню «Сетевые сервисы» → «NTP-клиент»

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

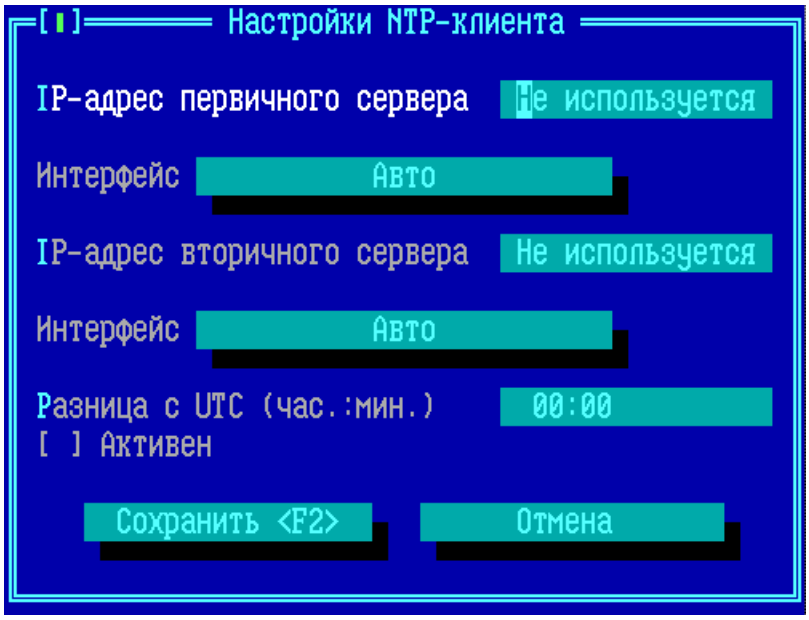


Рисунок 504 - Настройки NTP-клиента по умолчанию

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

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

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

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*».

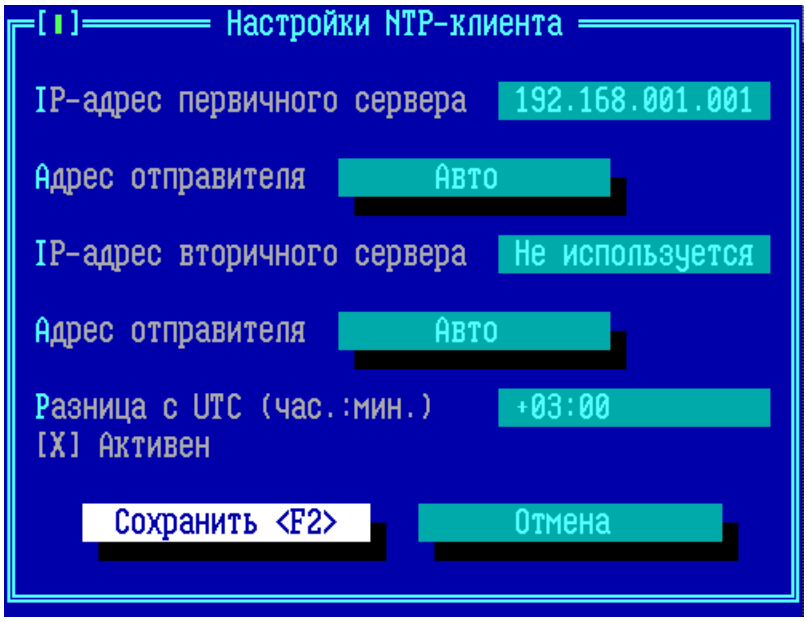


Рисунок 505 - Пример настроек NTP-клиента

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.

13. 11. Особенности реализации ICMP протокола

При работе ФПСУ с ICMP-сообщениями реализован ряд ограничений.

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

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

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

ФПСУ отправляет только следующие ICMP-сообщения об ошибках:

Таблица 16. Типы ICMP-ответов ФПСУ

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

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

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

13. 12. RADIUS

ФПСУ как клиент поддерживает сетевой протокол RADIUS (Remote Authentication Dial In User Service), для обеспечения возможности централизованных аутентификации, авторизации и аккаунтинга.

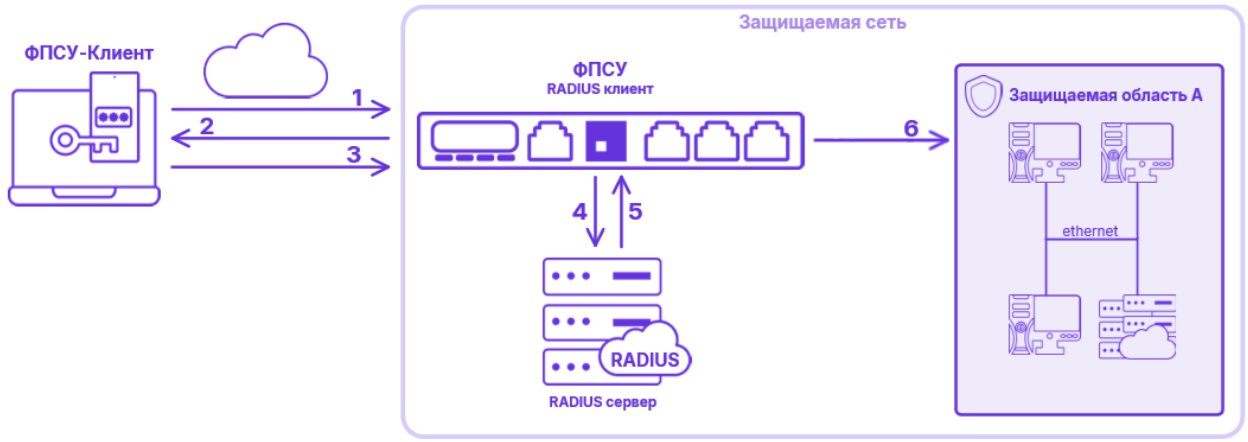
ФПСУ поддерживает протокол RADIUS для реализации двухфакторной аутентификации ФПСУ-IP/Клиентов при удаленном доступе к защищенной сети. После прохождения аутентификации ФПСУ-IP/Клиенты авторизуются для доступа к определенным сетевым ресурсам.

Схема аутентификации и последующей авторизации

Аутентификация ФПСУ на сервере RADIUS проводится согласно RFC 2865 с применением протокола PAP.

ФПСУ-IP/Клиент удаленно подключается к сетевым ресурсам защищенной области. На схеме ниже приведен пример аутентификации ФПСУ-IP/Клиента по доменному паролю на сервере RADIUS и дальнейшей его авторизации:

- ФПСУ-IP/Клиент отправляет запрос ФПСУ, который является сервером сетевого доступа, чтобы получить доступ к защищенной области, используя имя пользователя и пароль.
- ФПСУ отправляет сообщение с данными ФПСУ-IP/Клиента на сервер RADIUS, запрашивая его авторизацию для предоставления доступа.
- Сервером RADIUS подтверждается личность пользователя, а также права доступа к сетевым службам. Сервер RADIUS разрешает или запрещает доступ, отвечая ФПСУ на запрос.
- В случае получения разрешения от сервера RADIUS, ФПСУ-IP/Клиент получает доступ к запрошенному сетевому ресурсу, защищенной области A.
- При получении доступа к запрошенному сетевому ресурсу в случае настроенного аккаутинга информация об активности ФПСУ-IP/Клиента в сети может отправляться на сервер RADIUS для ведения учета действий ФПСУ-IP/Клиента и дальнейшего анализа.



1 ФПСУ-Клиент инициирует сессию работы с ФПСУ
2 ФПСУ в параметрах сессии присылает требование парольной аутентификации ФПСУ-Клиента на RADIUS сервере
3 ФПСУ-Клиент посылает ФПСУ логин и пароль аутентификации на RADIUS в составе шифрованных атрибутов сессии
4 ФПСУ отправляет логин и зашифрованный пароль на сервер RADIUS
5 Сервер RADIUS отвечает на запрос
6 ФПСУ получает ответ от RADIUS сервера, в случае успешной аутентификации ФПСУ-Клиент авторизуется в домене и получает доступ в защищенную область А

Рисунок 506 - Схема взаимодействия ФПСУ с сервером RADIUS

Двухфакторная аутентификация

Первым фактором аутентификации ФПСУ-IP/Клиента на ФПСУ является PIN-код VPN-Key или VPN-профиля, который известен только пользователю VPN-Key или VPN-профиля.

Вторым фактором является внешняя проверка подлинности пользователя ФПСУ-IP/Клиента, где задействуется внешний сервис удаленной аутентификации пользователей, RADIUS-сервер. При двухфакторной аутентификации в случае успешной аутентификации ФПСУ запрашивает у пользователя подтверждение доступа вторым фактором. Вторым фактором на ФПСУ служит пароль, доменный пароль или OTP-пароль. Настройки клиентов на работу с RADIUS описаны в пункте «Настройка диапазона клиентов на работу с Radius».

OTP-пароль пользователь ФПСУ-IP/Клиента получает по дополнительному каналу связи. Таким каналом связи может быть персональное мобильное устройство, доступ к которому имеет только пользователь VPN-Key или VPN-профиля.

ФПСУ становится транспортом пароля между ФПСУ-IP/Клиентом и внешним сервером RADIUS. ФПСУ передает пароль по протоколу RADIUS на сервер и возвращает ответ с разрешением или запретом, в случае разрешения пользователь авторизуется в защищенной сети.

В случае с установленным доменным паролем RADIUS сервер отправляет данные авторизации контроллеру домена для проверки.

Авторизация

Авторизация обеспечивает безопасность сети посредством предоставления доступа ФПСУ-IP/Клиентам только к тем ресурсам, на которые у них есть права. ФПСУ-IP/Клиенты, прошедшие аутентификацию, авторизуются в сети на основе данных, полученных от сервера RADIUS.

Динамическая авторизация

Динамическая авторизация ФПСУ-IP/Клиентов в сети проводится согласно RFC 5176. Динамическая авторизация позволяет быстро изменять права доступа пользователей в зависимости от их уровня доступа или принадлежности к доменной группе.

ФПСУ может предоставлять доступ клиентов в защищенную сеть на основе установленного уровня доступа клиента, присылаемого сервером RADIUS.

Аккаунтинг

Аккаунтинг включает сбор, хранение и анализ данных о действиях ФПСУ-IP/Клиентов в сети. Позволяет проводить мониторинг активности ФПСУ-IP/Клиентов, управлять сетевыми ресурсами, генерировать отчеты. С настройкой аккаутинга фиксируются факты доступа к системе: клиент получил доступ, доступ клиента прекращен, обновление статуса активности клиента, продолжительность соединения, объем данных, отправленных и полученных клиентом во время сеанса и другие факты.

13. 12. 1. Настройка RADIUS-серверов на ФПСУ

Доступ к окну настроек RADIUS-серверов на ФПСУ предоставляется из меню «*Сетевые сервисы»* конфигурации ФПСУ при выборе в подменю команды «*RADIUS-серверы»*.

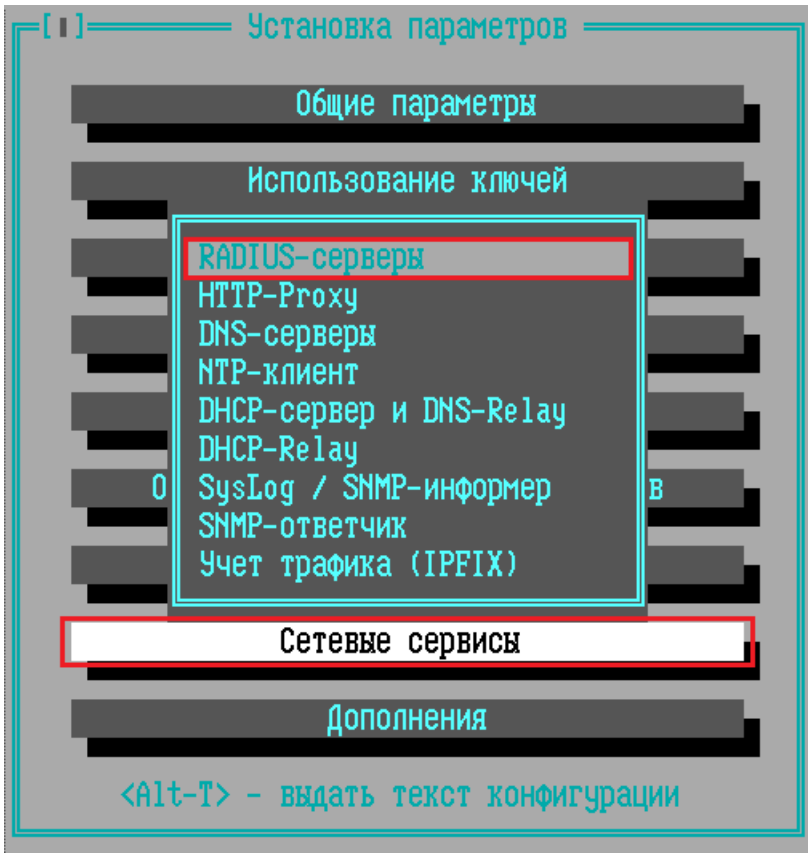


Рисунок 507 - Команда меню «Сетевые сервисы» → «RADIUS-серверы»

Для указания RADIUS-сервера необходимо в открывшемся окне нажать кнопку *«Добавить»*.

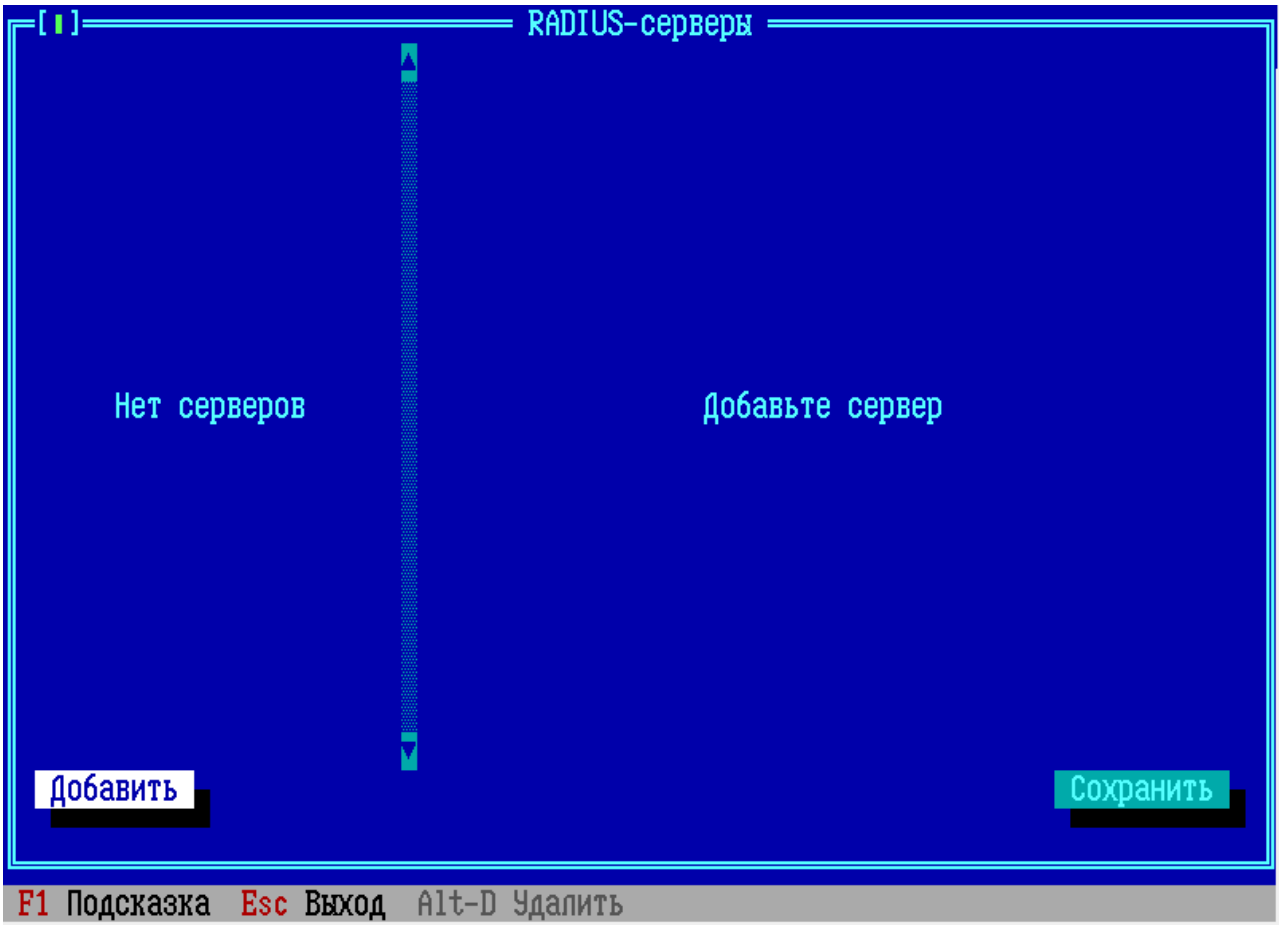


Рисунок 508 - Окно «RADIUS-серверы»

Установите следующие настройки RADIUS сервера:

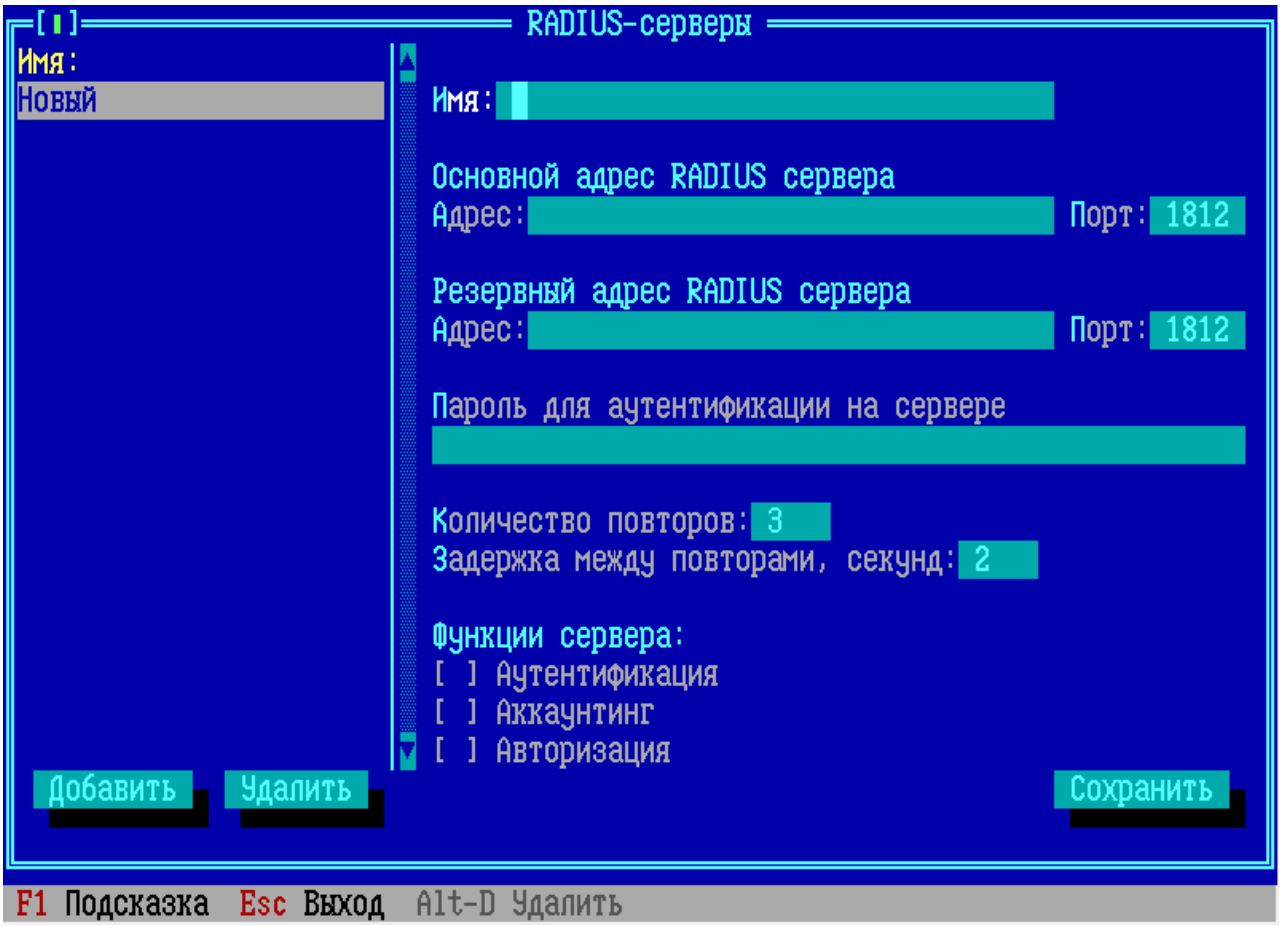


Рисунок 509 - Добавление RADIUS-сервера

Имя – текстовое произвольное описание RADIUS сервера.

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

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

Пароль для аутентификации на сервере – ФПСУ является RADIUS-клиентом и проходит аутентификацию на RADIUS-сервере с данным паролем. Требования к паролю определяются RADIUS-сервером. Аутентификация ФПСУ на RADIUS-сервере выполняется по протоколу PAP.

В случае отсутствия ответа RADIUS сервера могут быть заданы ***Количество повторов*** и ***Задержка между повторами***.

Аутентификация – RADIUS сервер проверяет подлинность учетных данных ФПСУ-IP/Клиентов.

Аккаунтинг – RADIUS сервер записывает информацию об использовании ресурсов ФПСУ-IP/Клиентов для аудита и мониторинга.

Авторизация – RADIUS сервер определяет права доступа ФПСУ-IP/Клиентов к определенным сетевым ресурсам.

13. 12. 2. Спецификация реализации RADIUS на ФПСУ

В данном пункте приводятся поддерживаемые ФПСУ типы сообщений и опциональные атрибуты реализации протокола удаленной аутентификации, аккаунтинга и авторизации RAIDUS. Протокол используется для управления доступом VPN-клиентов ФПСУ, использующими для подключения программное обеспечение «ФПСУ-IP/Клиент».

Выделенные курсивом *Поля* соответствуют одноименным полям описанным в этом пункте, жирный курсивом ***Поля*** соответствуют одноименным в приведенных ниже стандартах. Выделенные синим цветом поля доступны только для клиентов, использующих программное обеспечение «ФПСУ-IP/Клиент» там, где ограничение не указано явно.

Стандарты

Реализованы с выборочной поддержкой опциональных атрибутов следующие стандарты:

RFC **2865** – авторизация
RFC **2866** – аккаунтинг
RFC **2869** – дополнительные атрибуты
RFC **5176** – динамическая авторизация

Проприетарные атрибуты

Проприетарные атрибуты реализованы как атрибут ***Vendor-Specific*** (26) с ***Vendor-id*** равным **37249** (IANA Amicon ID) с ***Vendor type*** атрибутами, приведенными в таблице ниже:

Таблица 17. Проприетарные атрибуты

Номер	Имя	Тип	Описание
1	Amicon-SysID	integer	Номер криптосети клиента

Номер	Имя	Тип	Описание
2	Amicon-GroupID	integer	Номер группы клиента
3	Amicon-UserID	integer	Номер клиента в группе
4	Amicon-KeySerie	integer	Серия ключа клиента
5	Amicon-KeyGen	integer	Генерация ключа клиента
6	Amicon-Flags	integer	Флаги соединения
7	Amicon-ClientMAC	string	MAC АРМ клиента
8	Amicon-ClientIP	string	IPv4 АРМ клиента
9	Amicon-FWVer	string	Версия ПО USB токена клиента (при наличии)
10	Amicon-SWVer	string	Версия ПО «Клиент-IP»
11	Amicon-OSVer	string	Тип и версия ОС АРМ клиента
12	Amicon-ClientLic	string	Номер лицензии ПО «Клиент-IP»
13	Amicon-ClientLicExp	string	Срок действия лицензии ПО «Клиент-IP»
14	Amicon-ClientDCN	string	Доменное имя клиента при логине в ОС
15	Amicon-ClientDGUID	string	GUID ОС клиента в домене (при наличии)
16	Amicon-Certificate-ID	octet	Идентификатор

Номер	Имя	Тип	Описание
17	Amicon-Certificate-CN	string	Короткое наименование владельца сертификата
18	Amicon-Certificate-IssuerKID	octet	Идентификато ключа издателя сертификата
19	Amicon-Certificate-Serial	octet	Серийный номер сертификата
20	Amicon-Certificate-Issuer	string	Издатель сертификата
21	Amicon-Certificate-Alg	string	Алгоритм сертификата (RSA/GOST)

Аутентификация клиента

Поддерживается простая аутентификация по ***User-Password*** (RSA Message Digest Algorithm MD5 based method) запросом ***Access-Request*** и получением по результатам аутентификации сообщения ***Access-Accept*** в случае успеха и ***Access-Reject*** в случае отказа в доступе.

В ***Access-Request*** ФПСУ передает атрибуты: ***User-Name, User-Password, NAS-IP-Address, NAS-Port, Framed-IP-Address, Called-Station-Id, Calling-Station-Id, Message-Authenticator***, *Amicon-ClientMAC, Amicon-ClientIP, Amicon-SWVer, Amicon-OSVer, Amicon-ClientDCN, Amicon-ClientDGUID*.

Для подключений ФПСУ-IP/Клиент дополнительно: *Amicon-SysID, Amicon-GroupID, Amicon-UserID, Amicon-KeySerie, Amicon-KeyGen, Amicon-Flags, Amicon-ClientLic, Amicon-ClientLicExp, Amicon-FWVer*.

В ***Access-Access*** ФПСУ использует следующие атрибуты: ***Message-Authenticator, Session-Timeout, Idle-Timeout, Filter-ID, Class***.

Аккаунтинг клиента

При соединении (***Acct-Status-Type=Start***), отключение клиента (***Acct-Status-Type=Stop***), а также с заданной периодичностью во время сессии работы клиент (***Acct-Status-Type=Interrim-Update***), ФПСУ передает сообщения ***Accounting-Request*** на RADIUS сервер.

В ***Accounting-Request*** ФПСУ передает атрибуты: ***User-Name, Acct-Status-Type, Acct-Authentic, Acct-Session-Id, Acct-Input-Octets, Acct-Output-Octets, Acct-Session-Time, Acct-Input-Packets, Acct-Output-Packets, Acct-Terminate-Cause, Service-Type, Framed-Protocol, Class, NAS-IP-Address, NAS-Port, Framed-IP-Address, Called-Station-Id, Calling-Station-Id, Message-Authenticator***, *Amicon-ClientMAC, Amicon-ClientIP, Amicon-SWVer, Amicon-OSVer, Amicon-ClientDCN, Amicon-ClientDGUID.*

Для подключений ФПСУ-IP/Клиент дополнительно: *Amicon-SysID, Amicon-GroupID, Amicon-UserID, Amicon-KeySerie, Amicon-KeyGen, Amicon-Flags, Amicon-ClientLic, Amicon-ClientLicExp, Amicon-FWVer.*

Смена авторизации клиента

ФПСУ принимает сообщения ***CoA-Request*** на UDP порт 3799, изменяющие уровень доступа соединенного клиента на заданный атрибутом ***Filter-ID*** (типа string, строка содержит заданное UTF-8 текстом числовое значения уровня). Вновь соединившийся пользователь имеет уровень доступа "1". Пользователи, проходящие аутентификацию RADIUS, после успешной аутентификации имеют уровень доступа "2".

Клиент задается одним из 3 вариантов набора атрибутов:

- ***Acct-Session-Id*** – идентификатор сессии аккаунтинга RADIUS;
- ***Framed-IP-Address*** - внутренний IPv4 адрес клиента (NAT на ФПСУ либо реальный);
- *Amicon-SysID, Amicon-GroupID, Amicon-UserID* – учетные номера клиента. Только для подключений ФПСУ-IP/Клиент.

В ***CoA-Request*** ФПСУ использует следующие атрибуты: ***Acct-Session-Id, Framed-IP-Address, Message-Authenticator, Filter-ID, Avent-Timestamp, NAS-IP-Address***, *Amicon-SysID, Amicon-GroupID, Amicon-UserID.*

Следующие атрибуты являются обязательными и участвуют в дополнительных проверках:

Avent-Timestamp – отметка времени должна отличаться от времени ФПСУ не более чем на ±10с;

NAS-IP-Address – IP адрес должен совпадать с адресом назначения заголовка IP пакета;

Filter-ID – значения атрибута должно быть текстовым представлением числа от "1" до "99";

Одним из перечисленных выше вариантов быть задан клиент.

В случае успешной смены авторизации, ФПСУ отвечает сообщением ***CoA-ACK***. При ошибке — ***CoA-NAK*** с аттрибутами: ***Error-Cause***.

Возможные значения атрибута ***Missing Attribute*** (402), ***Error-Cause: Invalid Request*** (404), ***Session Context Not Found*** (503).

Отключение клиента

ФПСУ принимает сообщения ***Disconnect-Request*** на UDP порт 3799. Задание клиента для идентификации аналогично сообщению ***CoA-Request***.

В ***Disconnect-Request*** ФПСУ использует следующие атрибуты: ***Acct-Session-Id, Framed-IP?Address, Avent-Timestamp, NAS-IP-Address, Message-Authenticator***, *Amicon-SysID, Amicon-GroupID, Amicon-UserID.*

Следующие атрибуты являются обязательными у участвуют в дополнительных проверках:

Avent-Timestamp – отметка времени должна отличаться от времени ФПСУ не более чем на ±10с;

NAS-IP-Address – IP адрес должен совпадать с адресом назначения заголовка IP пакета;

Одним из перечисленных выше вариантов быть задан клиент.

В случае успешного отключения, ФПСУ отвечает сообщением ***Disconnect-ACK***. При ошибке — ***Disconnect-NAK*** с аттрибутами: ***Error-Cause***.

Возможные значения атрибута ***Missing Attribute*** (402), ***Error-Cause: Invalid Request*** (404), ***Session Context Not Found*** (503)

Приложение — словарь RADIUS

VENDOR	Amicon 37249		
BEGIN-VENDOR	Amicon		
ATTRIBUTE	Amicon-SysID	1	integer
ATTRIBUTE	Amicon-GroupID	2	integer
ATTRIBUTE	Amicon-UserID	3	integer
ATTRIBUTE	Amicon-KeySerie	4	integer
ATTRIBUTE	Amicon-KeyGen	5	integer
ATTRIBUTE	Amicon-Flags	6	integer
ATTRIBUTE	Amicon-ClientMAC	7	string
ATTRIBUTE	Amicon-ClientIP	8	string
ATTRIBUTE	Amicon-FWVer	9	string
ATTRIBUTE	Amicon-SWVer	10	string
ATTRIBUTE	Amicon-OSVer	11	string
ATTRIBUTE	Amicon-ClientLic	12	string
ATTRIBUTE	Amicon-ClientLicExp	13	string
ATTRIBUTE	Amicon-ClientDCN	14	string
ATTRIBUTE	Amicon-ClientDGUID	15	string
ATTRIBUTE	Amicon-Certificate-ID	16	octets
ATTRIBUTE	Amicon-Certificate-CN	17	string
ATTRIBUTE	Amicon-Certificate-IssuerKID	18	octets
ATTRIBUTE	Amicon-Certificate-Serial	19	octets
ATTRIBUTE	Amicon-Certificate-Issuer	20	string
ATTRIBUTE	Amicon-Certificate-Alg	21	string
END-VENDOR	Amicon		

13. 13. Поддержка Wake-on-Lan

На ФПСУ поддерживается технология удаленного включения Wake-on-LAN, позволяющая удаленно управлять включением рабочих станций.

Команда на отправление Wake-on-LAN в адрес рабочей станции осуществляется только удаленным администратором. Локальное управление ФПСУ с помощью консоли или клавиатуры не предполагает возможности отправить команду Wake-on-LAN.

Удаленный администратор в программе «Удаленный администратор ФПСУ-IP» устанавливает параметры работы Wake-on-LAN на ФПСУ. ФПСУ от себя передаёт на указанные в параметрах рабочие станции специальные сетевые фреймы, так называемые magic packet. Подробно о включении данной функции на ФПСУ изложено в руководстве «Удаленный администратор ФПСУ-IP».

13. 14. Служебные протоколы и порты на ФПСУ

Таблица 18. Служебные протоколы и порты на ФПСУ

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

Описание	Номер протокола или порта
Служебные протоколы VPN-туннеля между ФПСУ сетевого уровня, дополнительные потоки (если задействовано распределение потоков)	IP №№110-226
Служебные порты VPN-туннеля между ФПСУ транспортного уровня, дополнительные потоки (если задействовано распределение потоков)	UDP:№№ 55 000 - 55 126
Служебные порты VPN-туннеля между ФПСУ для динамических ФПСУ	UDP:№№ 40 000 - 50 000
Служебные порты VPN-туннеля между ФПСУ, для авторaспределения потоков	UDP:№№ 55 000 - 55 126
Служебный порт по умолчанию для исходящих соединений к RADUIS-серверам (может быть изменен администратором ФПСУ)	UDP:1812
Служебный порт для входящих соединений от RADUIS-серверов	UDP: 3799

14. Статистика ФПСУ

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

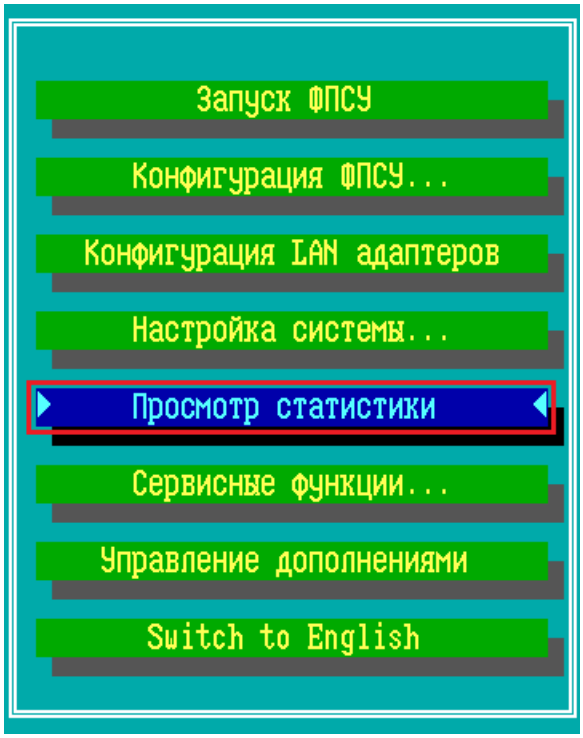


Рисунок 510 - Главное меню ФПСУ

14. 1. Просмотр статистики

Команда «Просмотр статистики» активируется из главного меню ФПСУ.

Операция доступна администраторам класса *Инженер* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 511 - Подтверждение полномочий и ввод пароля ТМ

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

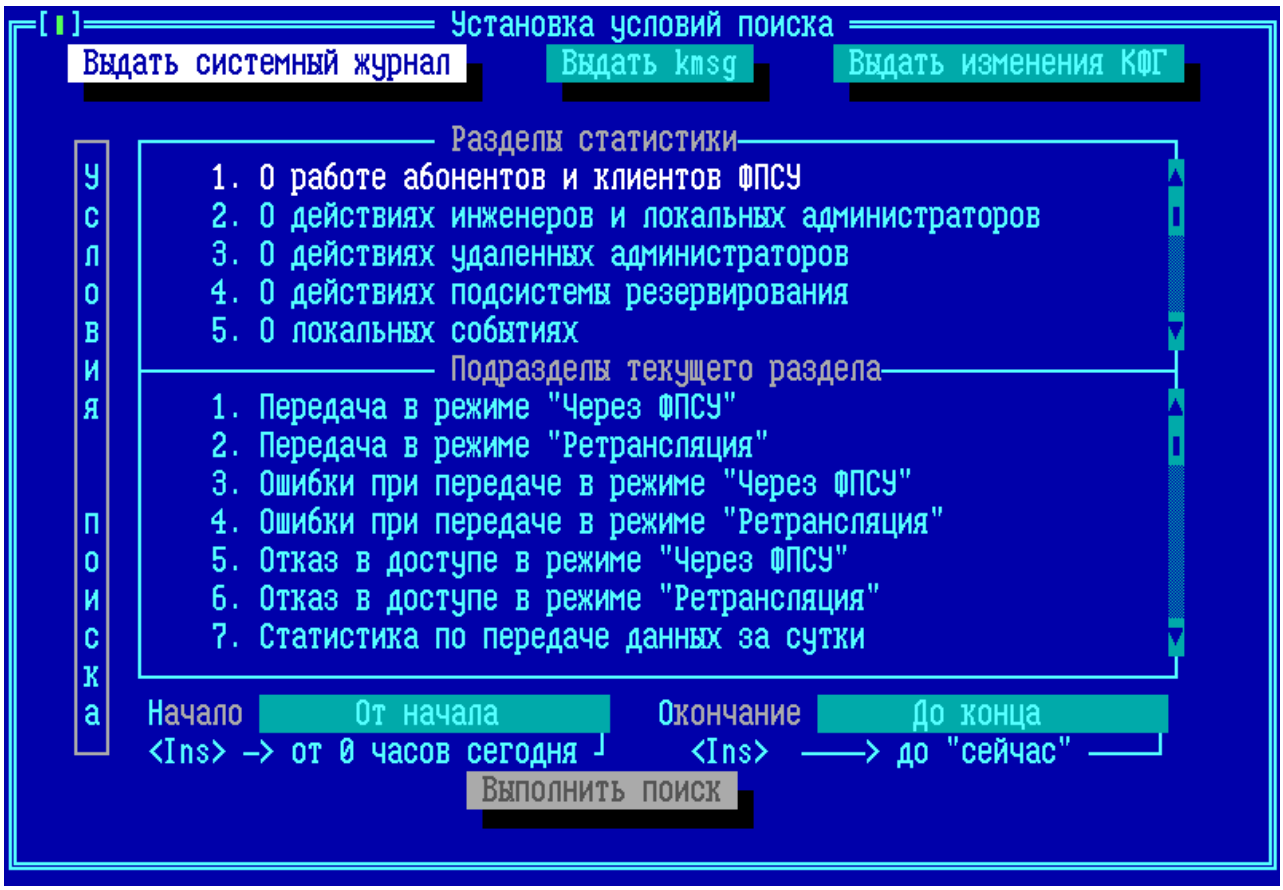


Рисунок 512 - Окно создания запроса на получение статистики

Для получения необходимых данных сначала отметьте нужный раздел, для чего выделите соответствующую строку и нажмите <*Пробел*>. При этом строка будет выделена слева знаком «√», а в окне подразделов отобразится относящийся к данному разделу список.

Переход к подразделам осуществляется по нажатию <*Tab*> или <→>. Подразделы отмечаются так же, как и разделы. Возврат от подразделов к разделу осуществляется по нажатию клавиши <←>.

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

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

После задания всех требуемых установок для поиска следует при помощи клавиши <*Tab*> отметить команду «*Выполнить поиск*» и нажать клавишу <*Enter*>. Подсистема регистрации осуществит поиск и выдаст результат на экран:

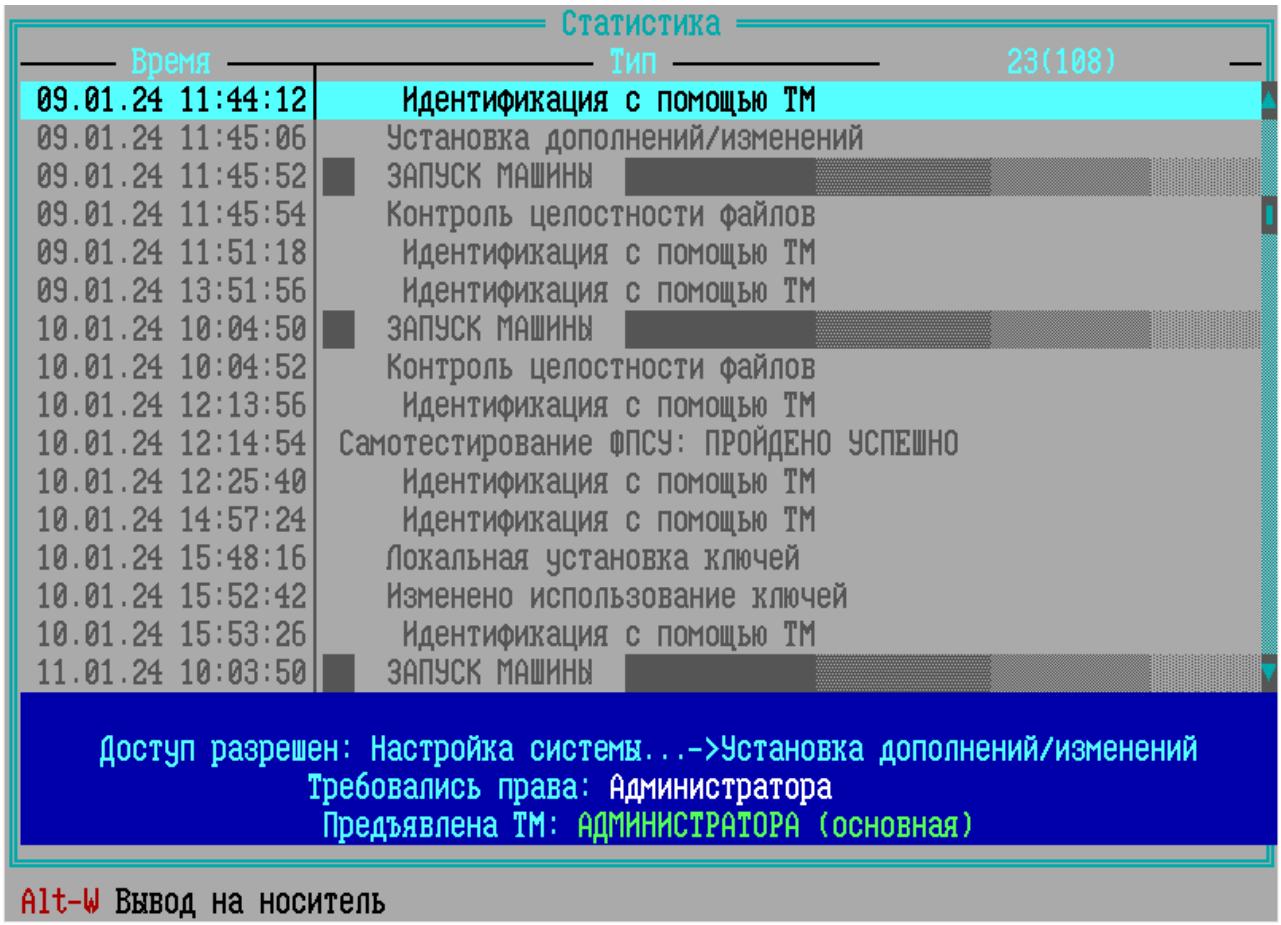


Рисунок 513 - Результат запроса статистики

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

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

Выданные данные могут быть записаны на внешний носитель по нажатию комбинации клавиш <*Alt+W*>. Данные будут записаны на носитель в специальном формате и могут быть прочитаны средствами программного 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.

14. 2. Выдача системного журнала

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

Операция разрешена администраторам ФПСУ класса *Главный администратор* (чтобы кнопка «Выдать системный журнал» была доступна, необходимо активировать команду главного меню «Просмотр статистики» с правами класса *Главный администратор*).

Вход в окно «Просмотр статистики» может быть дополнительно защищен паролем подключаемого ТМ, в этом случае будет запрашиваться пароль подключенного ТМ-идентификатора для авторизации.

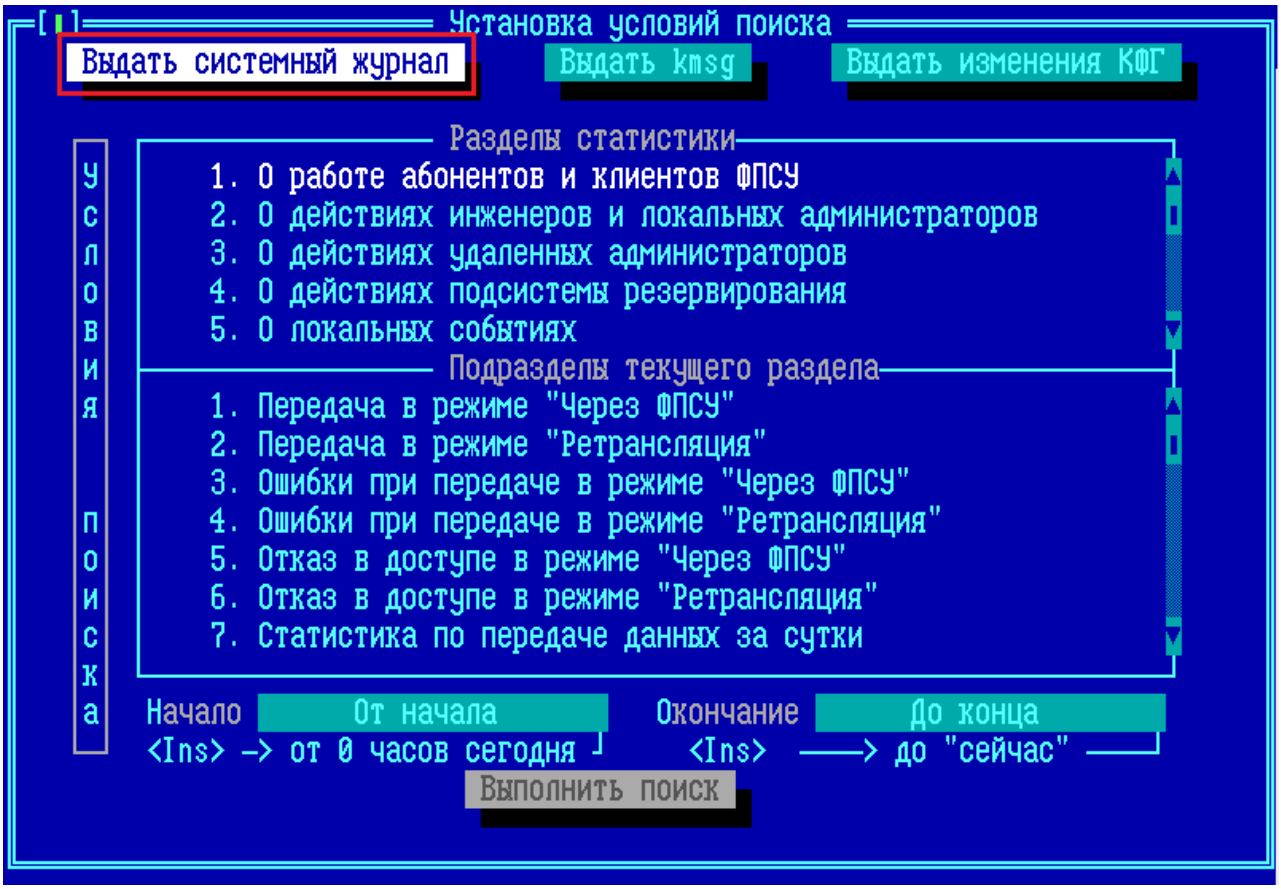


Рисунок 514 - Команда выдачи журнала изменений конфигурации межсетевого экрана

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

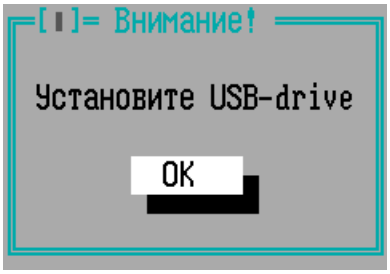


Рисунок 515 - Предложение подключить USB-носитель

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

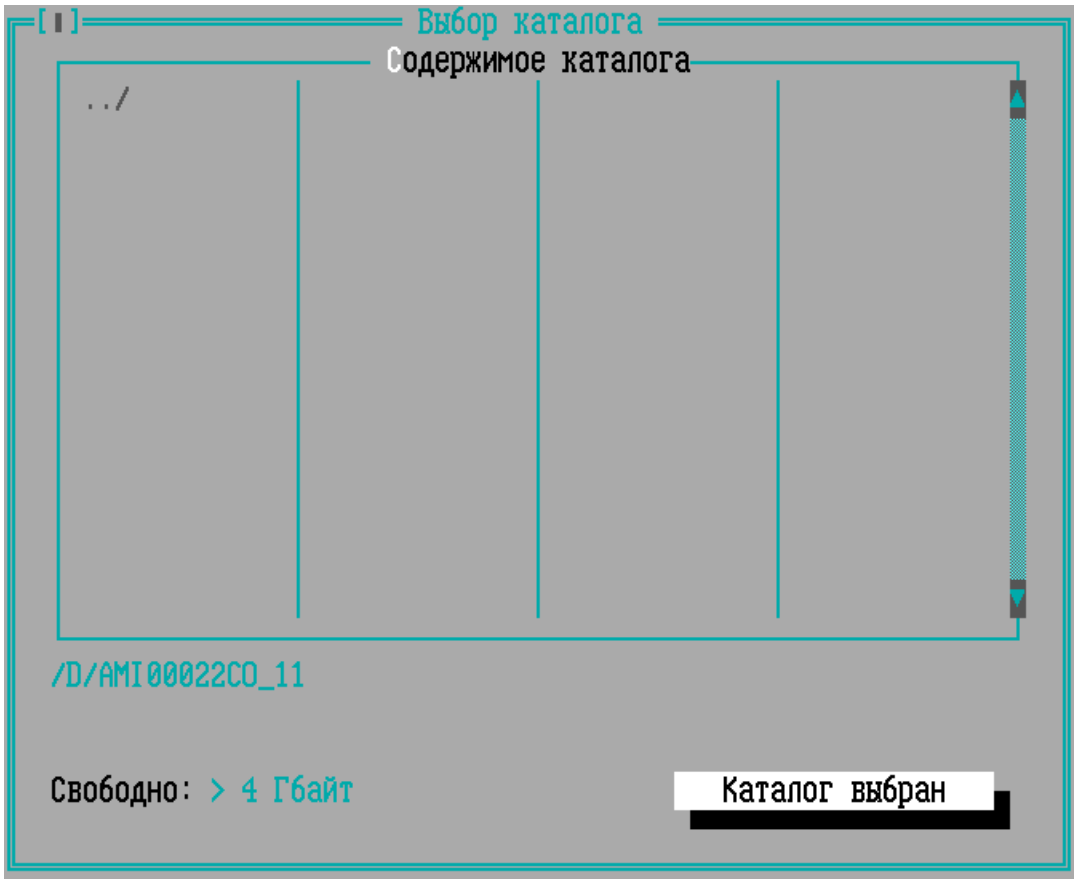


Рисунок 516 - Выбор каталога для выгрузки файла

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

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

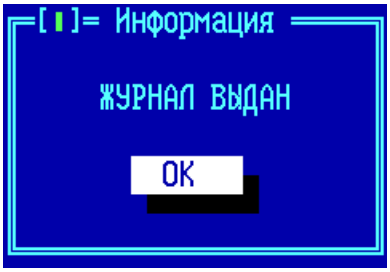


Рисунок 517 - Сообщение о завершении процедуры

14. 3. Выдача журнала изменений конфигурации межсетевого экрана

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

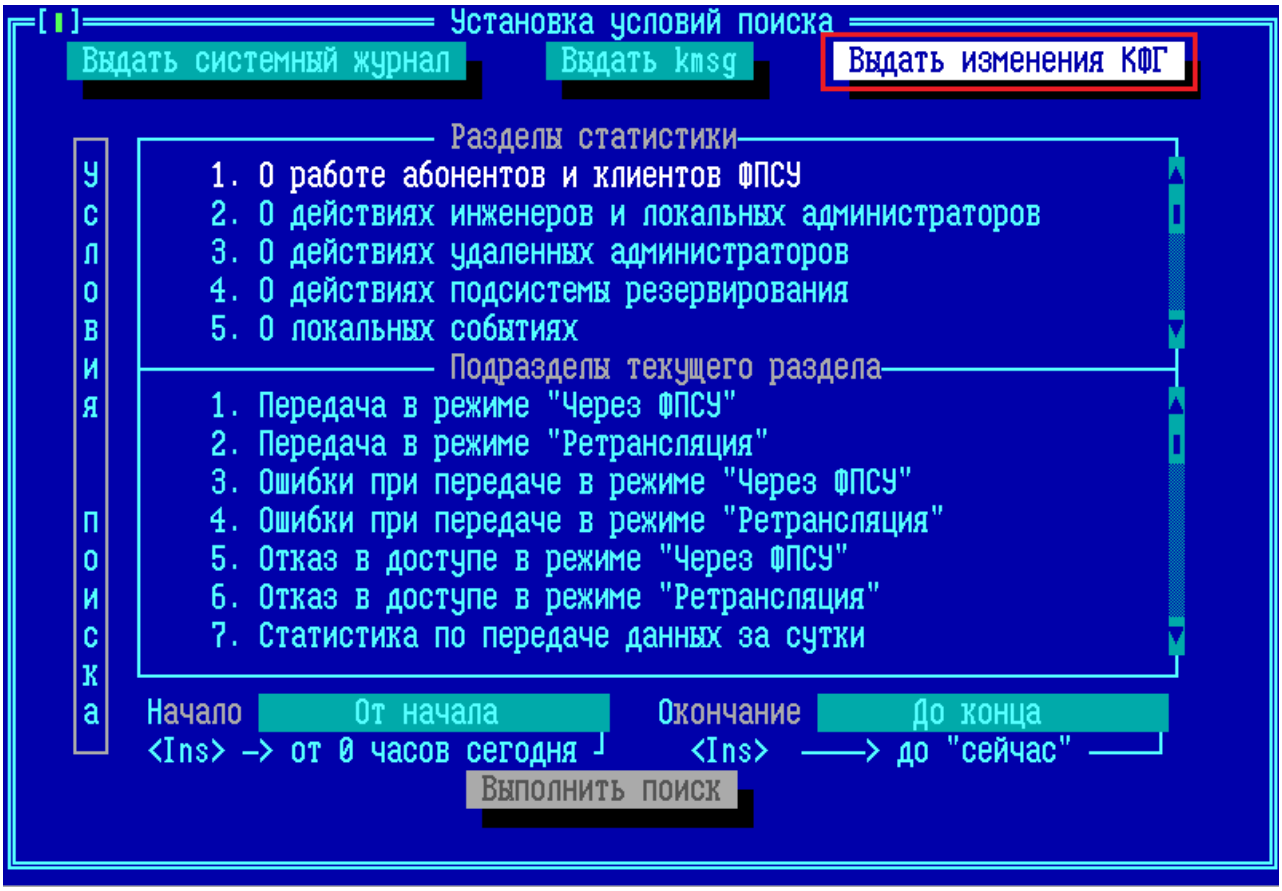


Рисунок 518 - Команда выдачи журнала изменений конфигурации межсетевого экрана

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

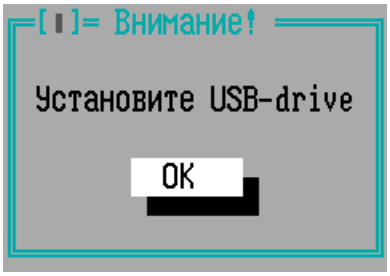


Рисунок 519 - Предложение подключить внешний носитель

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

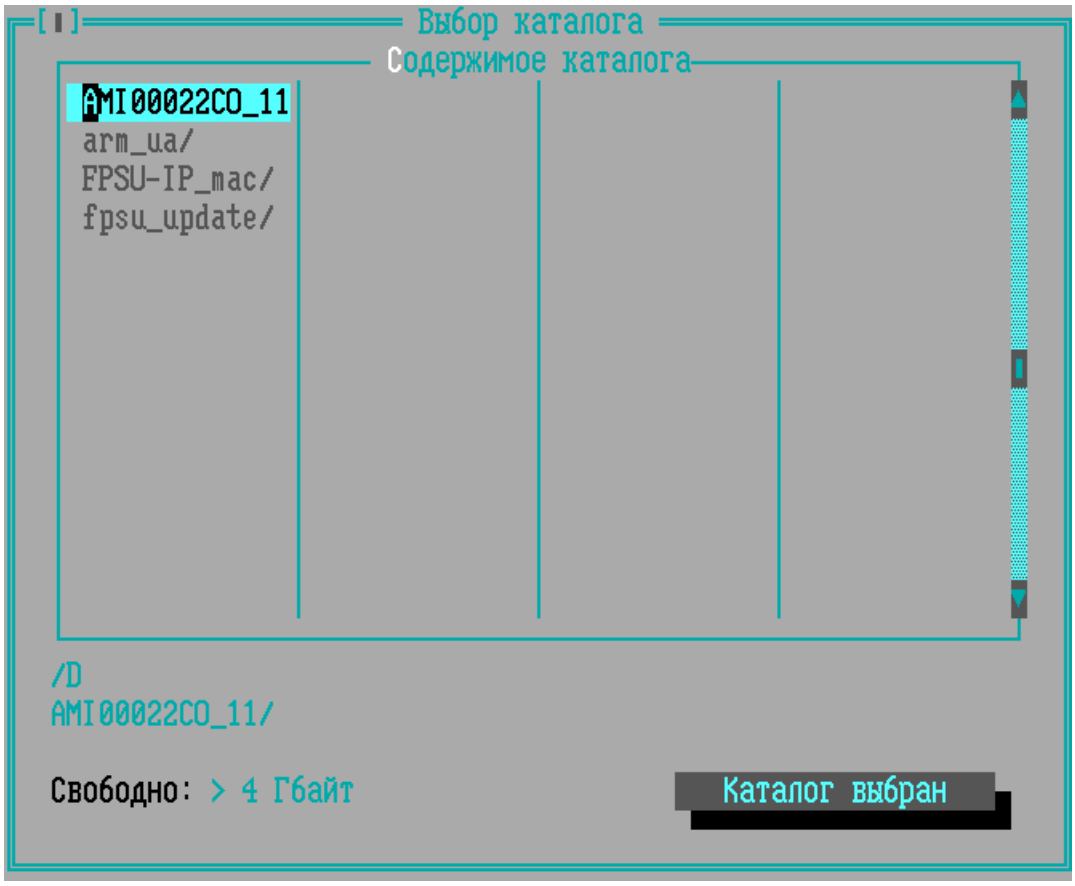


Рисунок 520 - Выбор каталога для выгрузки журнала

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

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

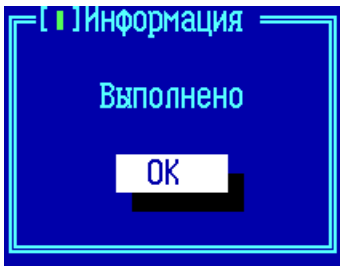


Рисунок 521 - Сообщение о завершении процедуры

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

14. 4. Ограничение сбора статистики

Администратор может ввести ограничения на типы статистики, собираемой ФПСУ. По умолчанию никаких ограничений не задано, собирается статистическая информация о всех происходящих на ФПСУ 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.

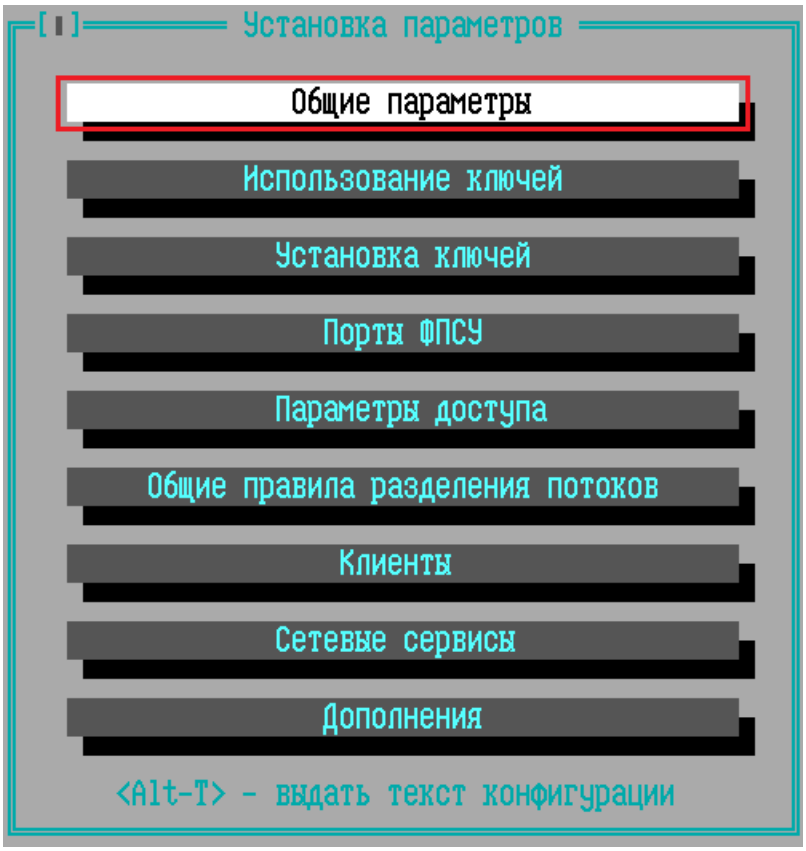


Рисунок 522 - Вход в общие настройки из основного меню конфигурации ФПСУ

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

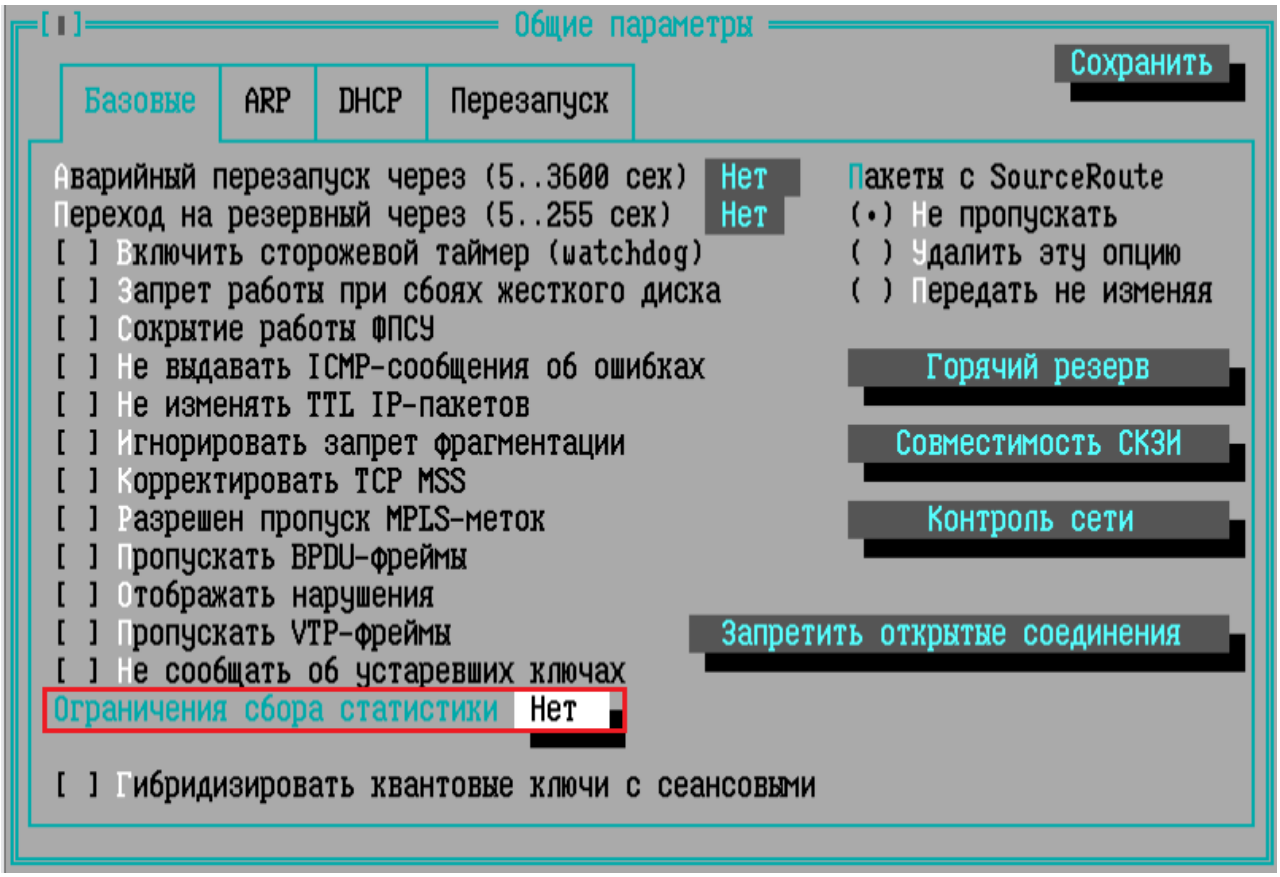


Рисунок 523 - Окно общих параметров ФПСУ

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

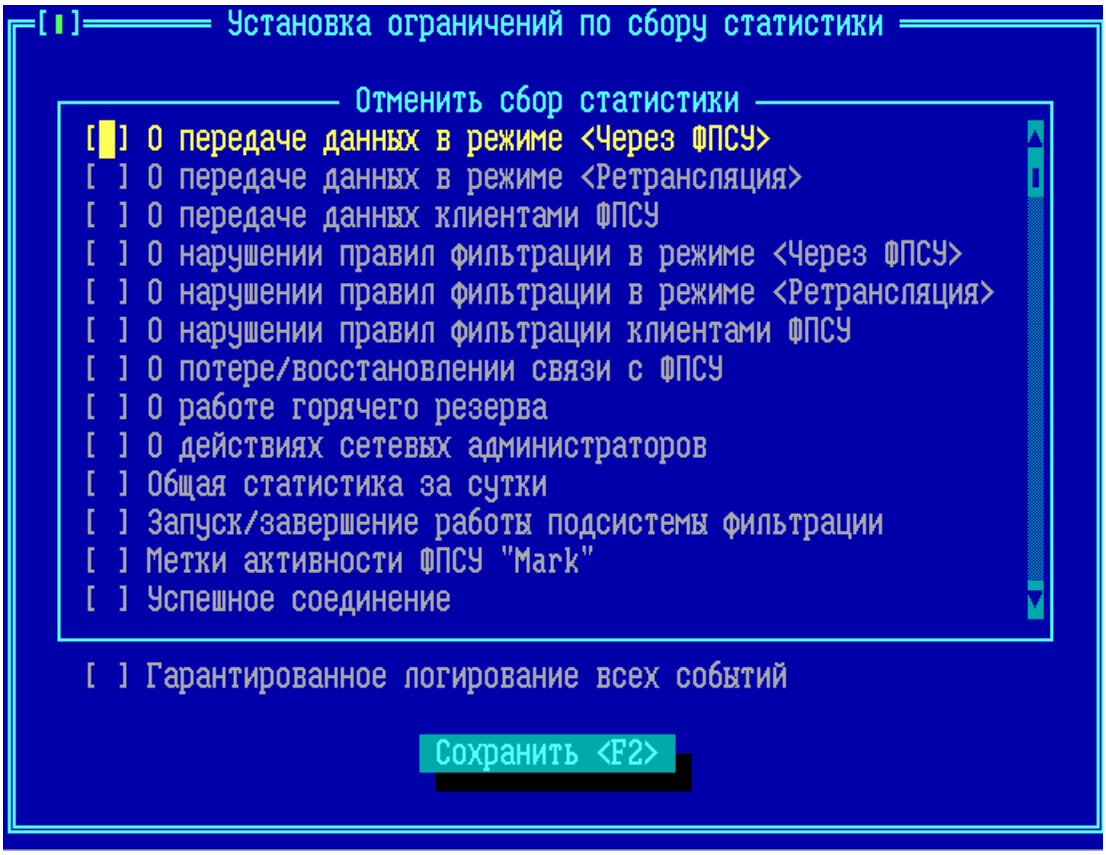


Рисунок 524 - Окно ограничения сбора статистики

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ВНИМАНИЕ! Все отказы в статистике значительно увеличивают нагрузку на ЦПУ и могут приводить к снижению производительности комплекса, особенно это заметно в случае включенного МЭ. В таких случаях рекомендуется выключить сбор статистики по отказам и настроить учёт отвергнутого трафика в IPFIX drop.

15. Восстановление работы ФПСУ после сбоев

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

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

Работоспособность сетевых адаптеров ФПСУ 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 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»). Если работоспособность восстановить не удается, ФПСУ 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 может быть переставлено на другой ФПСУ (ПЗУ на ФПСУ должен оставаться единственным).

Аварии ПЗУ (SSD) ФПСУ, влекущие за собой необходимость его замены и повторной установки ПО ФПСУ на новый, наиболее критичны в смысле времени восстановления работоспособности ФПСУ и защищаемой им ЛВС, поскольку все рабочие установки ФПСУ и записанные на носитель данные будут потеряны. Одна из опций конфигурации ФПСУ позволяет настроить его на такой режим работы, что при возникновении фатальной ошибки в результате сбоя или отказа ПЗУ ФПСУ продолжит функционировать без регистрации событий в хранилище ФПСУ (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 программы «Удаленный администратор ФПСУ-IP».

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

установить ключи парно-выборочной связи и общесистемные ключи клиентов, а также настроить сетевые адаптеры. Для осуществления указанных действий необходимы права классов *«Администратор»* или *«Главный администратор»* (см. пункт «Разграничение доступа и пользователи», Таблица 3).

Для возобновления работы ФПСУ после сбоев электропитания без участия оператора ФПСУ комплектуется **подсистемой автозапуска**.

Во избежание нарушений межсетевого взаимодействия защищенных фрагментов локальных сетей, связанных с неполадками или отказами аппаратуры ФПСУ, рекомендуется использовать комплект из двух ФПСУ, работающих в режиме «горячего» резервирования. В такой паре один из ФПСУ выполняет функциональные операции и считается активным, а второй находится в режиме ожидания. В случае аппаратных неполадок на активном ФПСУ, 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, на котором произошли аппаратные неполадки, также может быть достаточно быстро восстановлена (см. раздел «Принудительная синхронизация данных»).

16. Примеры настройки ФПСУ

В данном пункте даются пояснения по конфигурированию ФПСУ для некоторых стандартных сетевых топологий и удовлетворения определенных требований, налагаемых на работу подсетей. Эти примеры не являются реальными типичными схемами применения комплекса ФПСУ 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:

- принцип белого листа (все, что явно не описано, считается запрещенным к передаче).
- описатели типа «Хост» используются для регламентации передачи индивидуальных пакетов (unicast);
- описатели типа «Подсеть» и «Любой Хост» используются для регламентации передачи как индивидуальных, так и широковещательных пакетов;
- индивидуальные IP-адреса абонентов (описатели типа «Хост») не могут быть дублированы. Однако IP-адреса, принадлежащие указанным в конфигурации маршрутизаторам, могут повторно указываться в разделе описания абонентов на соответствующем порту, а IP-адреса, принадлежащие указанным в конфигурации ФПСУ, могут повторно указываться в разделе описания маршрутизаторов;
- создание со стороны одного порта описателя хоста или подсети, принадлежащих или включающих в себя описатель (по IP-адресу и маске, для подсети), который уже определен на другом порту, разрешено. При этом ФПСУ автоматически «вычеркнет» из более общего описателя на соответствующем порту более конкретный описатель и со стороны этого порта хосты, принадлежащие более конкретному описателю, будут считаться отсутствующими, т.е. не описанными в конфигурации порта;

- подсеть с одним и тем же IP-адресом и той же маской в общем случае (для передачи как индивидуальных, так и широковещательных пакетов) нельзя описать на двух портах одновременно. При попытке дублирования уже существующего на противоположном порту описателя типа «Подсеть» создаваемая запись типа «Подсеть» может быть использована только для передачи широковещательных пакетов (флаг «Только Broadcast» выключить нельзя).

16. 1. Базовая настройка ФПСУ для ретрансляции пакетов локальной сети

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

С точки зрения конфигурирования ФПСУ 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, 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 порта), а другие ФПСУ 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.

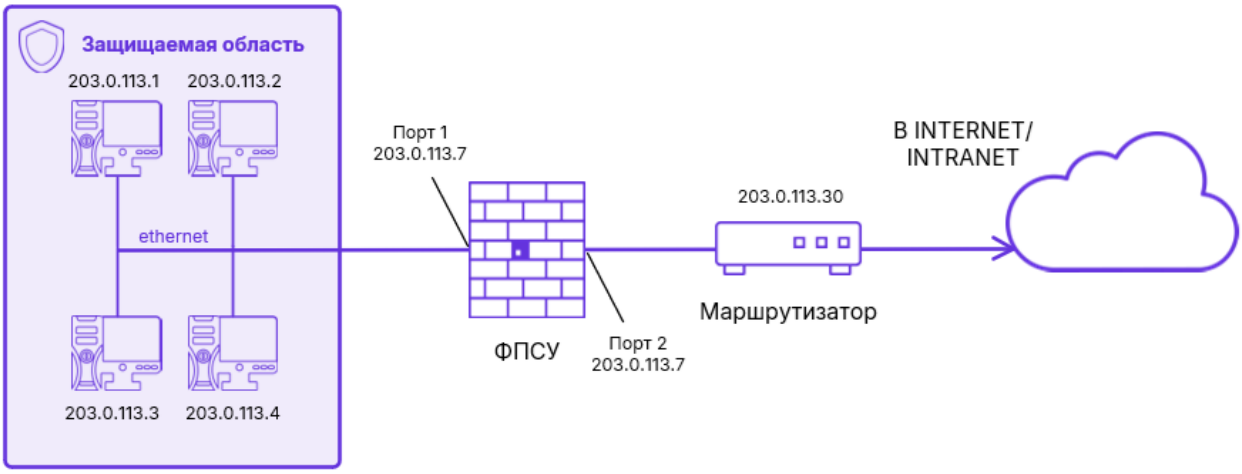


Рисунок 525 - Применение ФПСУ для защиты оконечной области

Конфигурация ФПСУ должна содержать следующие установки:

==========

Порт 1:

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

Порт 2:

Номер 2;
Адрес 203.0.113.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;

```
Маршрутизаторы 203.0.113.30;
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.
Абоненты: Любой хост
режим работы ретрансляция;
через маршрутизатор 203.0.113.30;
флаг "Работа разрешена" включен.
```

==========

При необходимости, администратор может регламентировать доступ к хостам своей подсети только по определенным протоколам и/или TCP/UDP-портам (через включение дополнительных правил межсетевого экрана, см. раздел «Параметры доступа, правила трафика межсетевого экрана», в данном примере их настройка не рассматривается).

Остальные параметры конфигурации (например, обработка IP-опций или сокрытие фильтрующих свойств комплекса) описываются на усмотрение администратора.

16. 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. В таком случае пакеты от абонентов IP-подсети 1 будут передаваться на порт 1 комплекса ФПСУ, с которого они будут передаваться обратно в защищаемую область и доставляться абонентам IP-подсети 2 (аналогично будут передаваться пакеты абонентов подсети 2, направленные абонентам подсети 1). IP-адреса 1 и 2 портов ФПСУ совпадают, для ФПСУ это допустимо, если в локальной сети доступно ограниченное количество свободных IP-адресов.

Такая организация защищаемой подсети приведет к следующей логике конфигурирования:

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

На работу подсети наложены следующие ограничения:

- хост с IP-адресом 192.168.1.1 является администратором маршрутизатора, обмен IP-пакетами с подсетью 2 ему запрещен; кроме того, он должен иметь круглосуточный доступ в сеть Internet/Intranet;

- остальные хосты подсети 1 и хосты подсети 2 имеют доступ друг к другу и не должны взаимодействовать с Internet/Intranet.

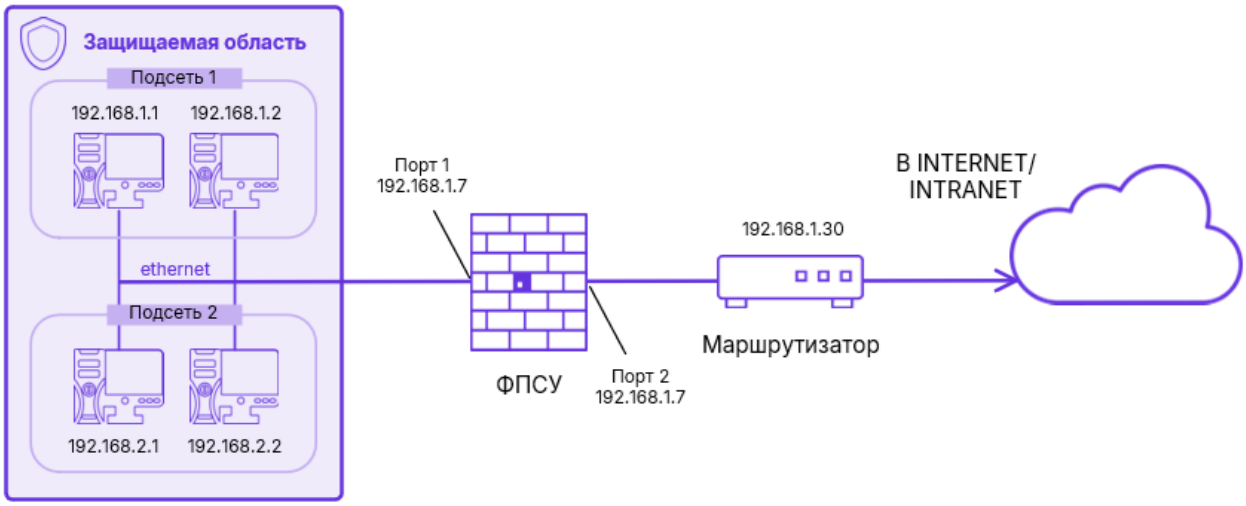


Рисунок 526 - Защита двух подсетей

С точки зрения конфигурирования ФПСУ 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 отсутствуют;
- со стороны порта 2 абоненты не определены, доступ к ним будет осуществляться через маршрутизатор (по IP-адресу связанного с ФПСУ порта), а другие ФПСУ отсутствуют;
- обмен администратора защищаемой области с абонентами общедоступной сети передачи данных может производиться только в режиме ретрансляции, сжатие и криптозащита не применяются;
- работа с ключевыми данными при такой топологии не требуется;
- абонентам подсетей 1 и 2 работа разрешается только с абонентами со стороны своего порта, причем администратор маршрутизатора не должен участвовать в таких обменах;
- абонент с IP-адресом 192.168.1.1 должен обмениваться пакетами с абонентами со стороны порта 2 и должен быть допущен к управлению маршрутизатором.

Конфигурация ФПСУ должна содержать следующие установки:

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

Порт 1:
Номер 1;
Адрес 192.168.1.7;
Маска 255.255.255.0 (24 разряда);
```

ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть; 192.168.1.0; 255.255.255.0 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта - включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть; 192.168.2.0; 255.255.255.0 (24 разряда);
режим работы ретрансляция;
режим партнера этого порта - включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Хост; 192.168.1.1;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.1.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы
192.168.1.30;
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.
Абоненты:
Любой хост;
режим работы ретрансляция;
через маршрутизатор 192.168.1.30;
флаг "Работа разрешена" включен.

==========

Для выполнения дальнейших настроек рекомендуется ознакомиться с разделом «Параметры доступа, правила трафика межсетевого экрана».

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

1. Правило, разрешающее взаимодействие абонента 192.168.1.1 (источник) с маршрутизатором 192.168.1.30 (назначение);
2. Правило, разрешающее взаимодействие абонента 192.168.1.1 (источник), и абонента Любой хост 2 порта ФПСУ (назначение);
3. Правило, разрешающее взаимодействие абонентов всех абонентов подсетей 1 и 2 (источник), и абонентов подсетей 1 и 2 (назначение);
4. Правило, запрещающее взаимодействия абонента 192.168.1.1 (и в качестве источника, и в качестве назначения), с абонентами подсети 2 (источник и назначение). Причем это правило должно иметь приоритет выше, чем правило из пункта 3.

Дополнительно, администратор может регламентировать доступ по времени (через выбор из ранее созданных интервалов времени в выпадающем списке «Время работы» правила доступа, см. пункт «Интервалы времени»).

Остальные параметры конфигурации (например, обработка IP-опций или сокрытие фильтрующих свойств комплекса) описываются на усмотрение администратора.

В данном примере функциональное отделение абонента 192.168.1.1 от IP-подсети 2 (запрещение обменов) производится двумя независимыми друг от друга ограничениями:

1. По настройке абонента 192.168.1.1 в разделе конфигурации «Порты ФПСУ», по признаку «Режим партнера – Данного порта» (режим «Ретрансляция» выключен);
2. Правилом 4. межсетевого экрана из списка выше.

Несмотря на то, что хостам со стороны порта 1 (исключая администратора) запрещено выходить в общедоступную сеть передачи данных, режим работы с партнером другого порта (ретрансляция) для них включен. Это объясняется тем, что данный режим отключить нельзя, поскольку отключение обоих режимов работы с партнером другого порта (по недосмотру или ошибке администратора) может привести к тому, что обмен пакетами через ФПСУ окажется невозможен и абоненты защищаемой области окажутся отрезанными от сети. Запрещение работы этим хостам будет обеспечиваться тем, что единственный абонент, описанный со стороны порта 2 через запись «Любой хост», включен только в одно правило доступа, разрешающее взаимодействие лишь с абонентом 192.168.1.1.

16. 3. Разделение подсети на два фрагмента ФПСУ на уровне маршрутизации

Представим теперь, что до установки ФПСУ существовала одна IP-подсеть с адресом 203.0.113.0 и маской 255.255.255.0, которую необходимо разделить физически на два независимых фрагмента (например, по функциональному признаку) без переконфигурирования программного обеспечения хостов, причем требуется регламентировать обмены данными между хостами независимых фрагментов. Отметим, что

в предыдущем примере (см. пункт «Защита локальной сети, состоящей из двух IP-подсетей») разделение абонентов на две подсети было логическим, то есть для его осуществления была необходима особая конфигурация TCP/IP-стека защищаемых хостов, при изменении которой выполнение наложенных в примере требований было бы невозможно. В данном примере рассматривается физическое разделение подсети, при котором абоненты отдельных фрагментов физически не могут обмениваться пакетами друг с другом в обход комплекса ФПСУ.

IP-адреса 1 и 2 портов ФПСУ совпадают, для ФПСУ это допустимо, если в локальной сети доступно ограниченное количество свободных IP-адресов.

После установки ФПСУ сеть имеет вид, изображенный на рисунке ниже.

Помимо физического разделения на работу двух подсетей накладываются следующие требования:

- хосты области 1, исключая хост 203.0.113.1, и все хосты области 2 должны иметь полный доступ друг к другу, в том числе должна обеспечиваться возможность поиска и подключения сетевых дисков;
- хост 203.0.113.1 не должен иметь доступа в область 2.

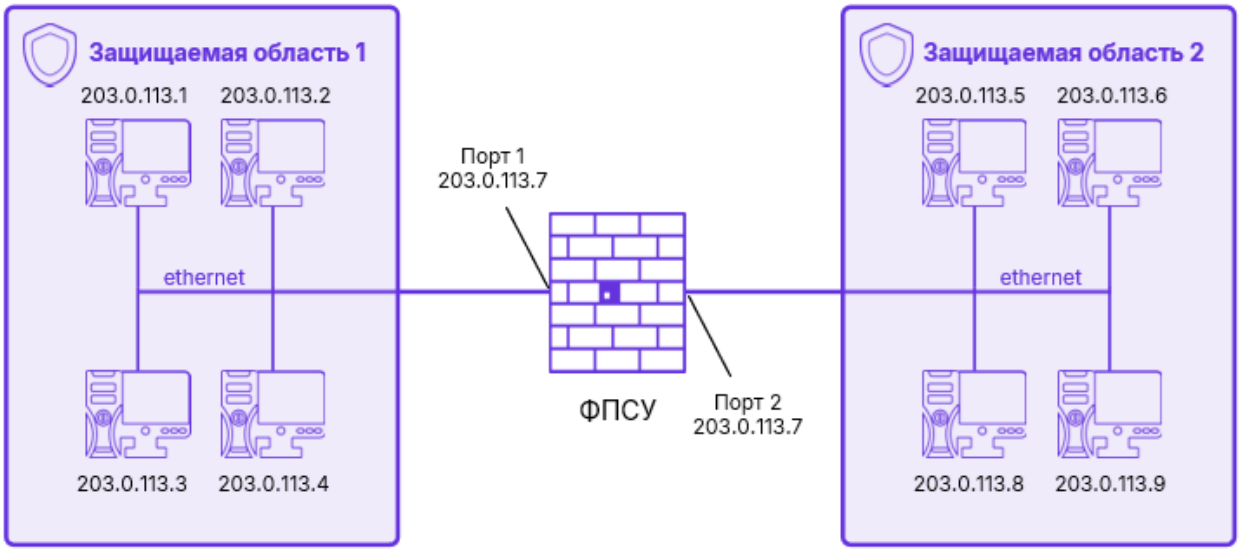


Рисунок 527 - Разбиение сети на фрагменты

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

- со стороны портов 1 и 2 ФПСУ существует одна и та же IP-подсеть, маршрутизаторы и другие ФПСУ отсутствуют;
- обмен хостов через комплекс может производиться только в режиме ретрансляции,

сжатие и криптозащита не применимы;

- работа с ключевыми данными при такой топологии не производится;
- абоненту с IP-адресом 203.0.113.1 должен быть запрещен обмен пакетами с абонентами со стороны порта 2;
- для обеспечения поиска и подключения сетевых дисков необходимо разрешить передачу через ФПСУ широковещательных пакетов.

Конфигурация ФПСУ должна содержать следующие установки:

Порт 1:

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

Порт 2:

Номер 2;
Адрес 203.0.113.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть 203.0.113.0; 255.255.255.0 (24 разряда);
режим работы ретрансляция;
флаг "Только Broadcast" включен;
флаг "Работа разрешена" включен.
Хост; 203.0.113.5;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;

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

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

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

16. 4. Использование ФПСУ 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 (со стороны внутреннего порта пограничного маршрутизатора) и организовать между ФПСУ VPN-туннели через WAN-сеть общего доступа, по которым данные абонентов будут передаваться

с использованием всех механизмов защиты, включая аутентификацию и, возможно, сжатие.

Предположим, что организация использует следующие IP-адреса:

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

Для ФПСУ в каждой подсети будут выделены адреса .50.

На работу сети наложены следующие ограничения:

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

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

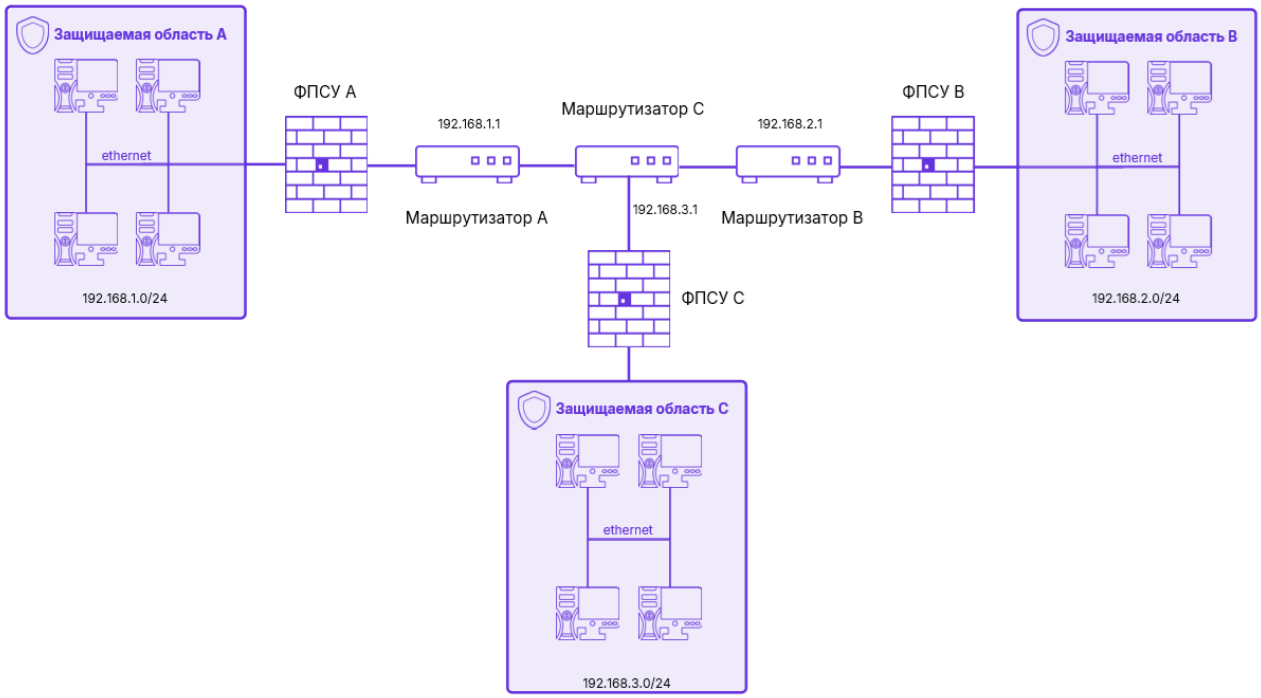


Рисунок 528 - Схема локальной сети с применением ФПСУ

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

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

В данном случае возможны два различных варианта конфигурации ФПСУ, которые описаны ниже.

16. 4. 1. Использование раздельных VPN-туннелей

В данном варианте конфигурации на каждом ФПСУ будет создаваться по два VPN-туннеля.

Всего будет создано три VPN-туннеля. При этом для обмена данными защищаемые области будут использовать следующие туннели:

- VPN-1 - обмен области A с областью C;
- VPN-2 - обмен области B с областью C;
- VPN-3 - обмен области A с областью B.

На рисунке ниже показаны организованные VPN-туннели.



Рисунок 529 - Схема подключения с раздельными туннелями

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

Конфигурация ФПСУ должна содержать следующие установки:

Для ФПСУ А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 в настройках ФПСУ А указаны как используемые.

Порт 1:
Номер 1;
Адрес 192.168.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены.
Абоненты:
Подсеть; 192.168.1.0; 255.255.255.0 (24 разряда),
режим работы - ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;

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

Порт 2:

Номер 2;
Адрес 192.168.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ
192.168.2.50, ключевые данные - 2.1; смена через 30 сек,
сжатие и криптозащита - "*желательно*" или "*обязательно*",
через маршрутизатор 192.168.1.1;
192.168.3.50, ключевые данные - 3.1; смена через 30 сек,
сжатие и криптозащита - "*желательно*" или "*обязательно*",
через маршрутизатор 192.168.1.1;
Маршрутизаторы
192.168.1.1;
протоколы маршрутизации - на усмотрение администратора,
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда),
через ФПСУ 192.168.2.50,
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда),
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Для ФПСУ B:

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

Порт 1:

Номер 1;
Адрес 192.168.2.50;
Маска 255.255.255.0 (24 разряда);

ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда), ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.2.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.1.50, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.2.1;
192.168.3.50, ключевые данные - 3.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.2.1;
Маршрутизаторы:
192.168.2.1, протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть; 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Для ФПСУ С:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3. Ключи номер 3 в настройках ФПСУ С указаны как используемые.

Порт 1:
Номер 1;
Адрес 192.168.3.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть; 192.168.3.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:
Номер 2;
Адрес 192.168.3.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.1.50, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 192.168.3.1
192.168.2.50, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 192.168.3.1
Маршрутизаторы:
192.168.3.1, протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Только на ФПСУ С для подсети 192.168.3.0 должно быть разрешено управление

маршрутизаторами 192.168.1.1, 192.168.2.1, 192.168.3.1 (см. пункт «DHCP-Relay»).

Необходимо также перенастроить пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

16. 4. 2. Использование совмещенных VPN-туннелей

ФПСУ С является центральным сервером VPN-сети, организованной по топологии "звезда". В данном варианте конфигурации будут созданы всего два VPN-туннеля, показанные на рисунке ниже:

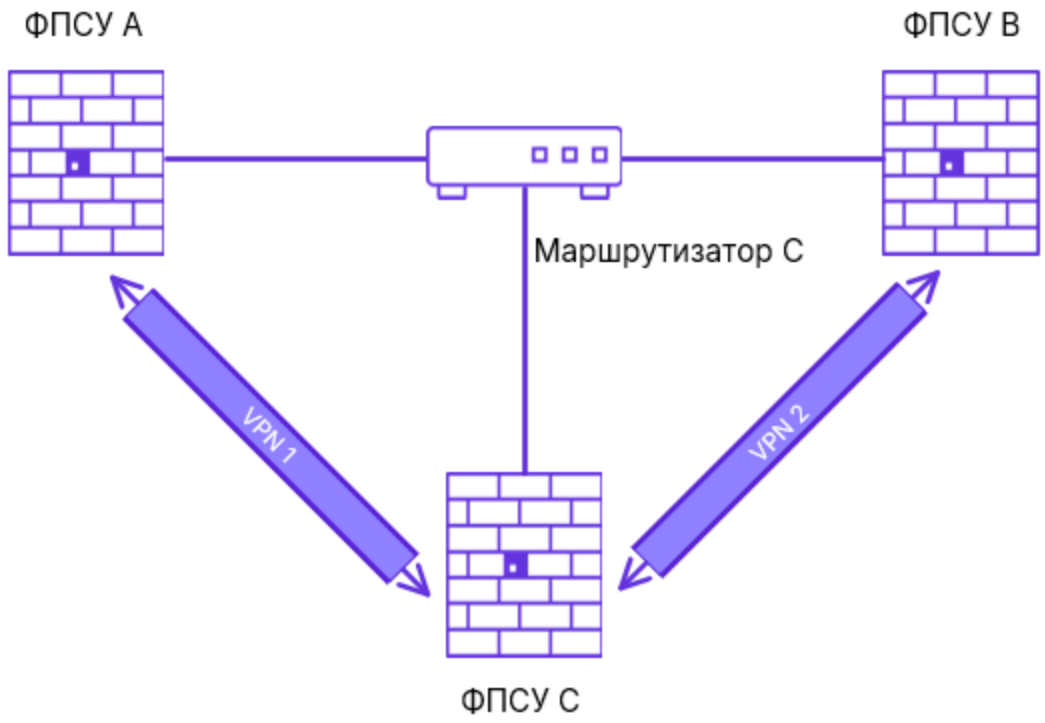


Рисунок 530 - Схема подключения с последовательными туннелями

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 А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи

номер 1 в настройках ФПСУ А указаны как используемые.

Порт 1:

Номер 1;
Адрес 192.168.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.3.50, ключевые данные - 3.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.1.1;
Маршрутизаторы
192.168.1.1, протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Для ФПСУ В:

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

Порт 1:

Номер 1;
Адрес 192.168.2.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 192.168.2.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.3.50, ключевые данные - 3.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.2.1
Маршрутизаторы:
192.168.2.1, протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Для ФПСУ С:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3. Ключи номер 3 в настройках ФПСУ С указаны как используемые.

Порт 1:
Номер 1;
Адрес 192.168.3.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Порт 2:
Номер 2;
Адрес 192.168.3.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.1.50, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.3.1
192.168.2.50, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 192.168.3.1
Маршрутизаторы:
192.168.3.1,
протоколы маршрутизации - на усмотрение администратора;
флаг "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Только Broadcast" выключен;

```
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.
```

Только на ФПСУ С для подсети 192.168.3.0 должно быть разрешено управление маршрутизаторами 192.168.1.1, 192.168.2.1, 192.168.3.1 (см. раздел «DHCP-Relay»).

Необходимо также переконфигурировать пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

16. 5. Использование ФПСУ в режиме моста (L2 шифрование)

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

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

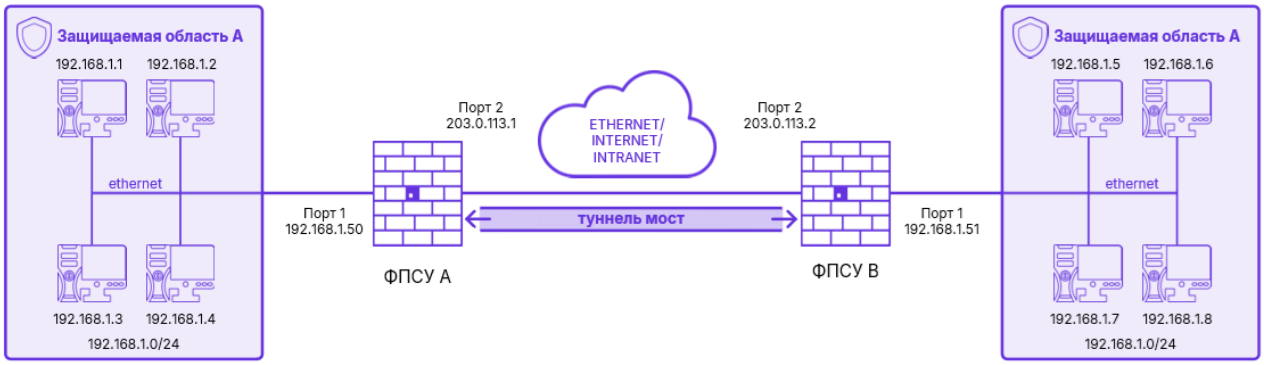


Рисунок 531 - L2-туннель типа «мост»

Используются следующие IP-адреса:

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

С точки зрения конфигурирования ФПСУ А для работы в условиях такой топологии

принципиальным является следующее:

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

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

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

Конфигурация ФПСУ должна содержать следующие установки:

Для ФПСУ А:

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

Порт 1:
Номер 1,
Адрес 192.168.1.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты: не определены;
Порт 2:
Номер 2,
Адрес 203.0.113.1,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
203.0.113.2, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
мост - включен;
Маршрутизаторы: не определены;
Абоненты: не определены.

Для ФПСУ B:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 указаны как используемые.

Порт 1:
Номер 1,
Адрес 192.168.1.51,
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты: не определены;
Порт 2:
Номер 2,
Адрес 203.0.113.2,
Маска 255.255.255.0 (24 разряда),
ФПСУ:
203.0.113.1, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
мост - включен;
Маршрутизаторы: не определены;
Абоненты: не определены.

16. 6. Каскадная схема установки ФПСУ в локальной сети

В документе «Описание применения» ПАК ФПСУ приведена каскадная схема установки двух ФПСУ в одной защищаемой области, при которой хосты оконечной области (защищенной двумя ФПСУ) будут обмениваться пакетами с хостами сетевых фрагментов, находящихся со стороны внешнего порта внешнего ФПСУ, через VPN-туннель, создаваемый в самой защищаемой области, а хосты защищаемой области - через внешний ФПСУ 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, причем в одной из подсетей существует особо ответственная IP-сеть, для которой необходимо обеспечить режим усиленной защиты. После установки комплексов сеть организации примет вид, отображенный на рисунке ниже.

Используются следующие IP-адреса:

- защищаемая область A - 192.168.1.0, маска 255.255.255.0 (24 бита);
- защищаемая область B - 192.168.2.0, маска 255.255.255.0 (24 бита);

- защищаемая область С - 192.168.3.0, маска 255.255.255.0 (24 бита);
- внутренний порт маршрутизатора А -192.168.2.1;
- внутренний порт маршрутизатора В -192.168.3.51.

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 А для работы в условиях такой топологии и удовлетворения наложенных требований принципиальным является следующее:

- со стороны внутреннего порта ФПСУ (порта 1 со стороны области А) существует одна IP- подсеть, а со стороны порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы и ФПСУ отсутствуют;
- со стороны порта 2 существуют: IP-подсеть В, доступ к которой необходимо запретить; IP-подсеть С, доступ в которую будет производиться через ФПСУ В, а также мировая сеть, доступ в которую предоставлен не будет; существует также маршрутизатор А, находящийся с внешнего порта ФПСУ 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 VPN-туннелей с проведением двусторонней аутентификации и использованием дополнительных процедур сжатия и криптозащиты;
- на ФПСУ А должны быть установлены, и указаны как используемые, ранее выработанные ЦВК криптографические ключи номер 1;
- со стороны внешнего порта ФПСУ (порта 2) присутствует пограничный маршрутизатор А, управление которым из защищаемой области А не должно осуществляться.

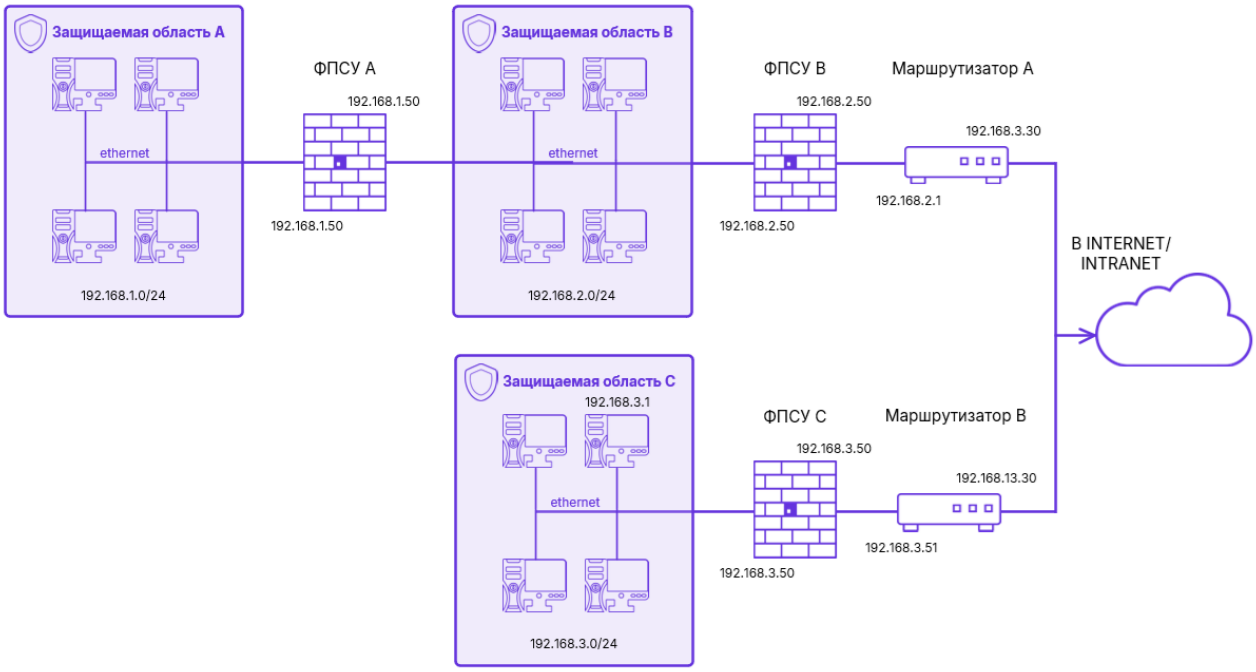


Рисунок 532 - Каскадное подключение ФПСУ

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

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

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

- со стороны внутреннего порта (порта 1 со стороны области C) существует IP-

подсеть С, а со стороны порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы и ФПСУ 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 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 VPN-туннелей;
- на ФПСУ С должны быть установлены и указаны как используемые ранее выработанные ключи номер 3;
- со стороны внешнего порта ФПСУ С существует пограничный маршрутизатор В, управление которым должно осуществляться только из защищаемой области В, причем канал управления маршрутизатором за пределами его внешнего порта должен быть защищен ФПСУ В.

Конфигурация ФПСУ должна содержать следующие установки:

Для ФПСУ А:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 1. Ключи номер 1 в настройках ФПСУ А указаны как используемые.

Порт 1:

Номер 1,
Адрес 192.168.1.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
A_to_C

Порт 2:

Номер 2,
Адрес 192.168.1.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.2.50, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";

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

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

Для ФПСУ В:

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

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

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

сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
to routers
Internet_B

Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2,
Адрес 192.168.2.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ:
192.168.3.50, ключевые данные - 3.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 192.168.2.1.
Маршрутизаторы:
192.168.2.1, протоколы маршрутизации - все выключены;
Абоненты:
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.
Любой хост;
флаг "Работа разрешена" включен;
через маршрутизатор 192.168.2.1;
Хост, 192.168.3.51; через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.

Правила МЭ:

1 to routers
Общие
Действие : Accept

```
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Сеть            :   192.168.002.000 192.168.000.000/24
      Назначение
        Хост            :   192.168.002.001 192.168.002.001/32
        Хост            :   192.168.003.051 192.168.003.051/32
      Служба          : Любая
2 Internet_B
      Общие
        Действие        : Accept
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Сеть            :   192.168.002.000 192.168.000.000/24
      Назначение      : Любой
      Служба          : Любая

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

Для ФПСУ С:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 3. Ключи номер 3 указаны как используемые.

Создано и активировано разрешающее правило трафика, в которое включены подсети 192.168.1.0 и 192.168.3.0. Подсети 192.168.2.0 со стороны порта 2 разрешено управление маршрутизатором 192.168.3.1.

Порт 1:
Номер 1,
Адрес 192.168.3.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;

Абоненты:
Подсеть, 192.168.3.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
C_to_A

Порт 2:
Номер 2,
Адрес 192.168.3.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
192.168.2.50, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 192.168.3.51.
Маршрутизаторы не определены;
Абоненты:
Подсеть, 192.168.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.
Подсеть, 192.168.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 192.168.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
флаг "Работа разрешена" включен.

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

```
    Время работы     : Любое
    Лог              : Не вести лог
    Активно          : Да
  Источник         : Любой
  Назначение       : Любой
  Служба           : Любая
```

В конфигурациях ФПСУ приведены только необходимые для работоспособности схемы настройки, дополнительно для абонентов должен быть выключен флаг «Только Broadcast», флаг «Отвечать на Ping» устанавливается на усмотрение администратора.

Необходимо также переконфигурировать пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

Поскольку конфигурирование нескольких совместно работающих ФПСУ 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 А:

- абоненты области А не получат 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 не описан со стороны порта 2;
- Доступ от абонентов области А к абонентам области С осуществляется через ФПСУ В, задан правилом трафика, разрешающим доступ в область С.

В соответствии с установленной конфигурацией через ФПСУ 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 для области В не задано правило трафика, разрешающее доступ в область А;
- абонентам области В разрешено управление маршрутизатором А и В, а также доступ в общедоступную сеть передачи данных правилами МЭ;
- доступ к маршрутизатору В от абонентов области В обеспечивается тем, что он указан как абонент на порту 2 и будет осуществляться только через ФПСУ В;
- к абонентам области С (исключая маршрутизатор В, описанный отдельно)

абоненты области B доступа не получат, поскольку для области B не задано правило трафика, разрешающее доступ в область C.

В соответствии с установленной конфигурацией через ФПСУ C:

- отсутствие доступа абонентов области C к маршрутизаторам A и в область B обеспечивается тем, что маршрутизатор A не описан как абонент со стороны внешнего порта 2, область C не входит в правило трафика, разрешающее доступ в область B;
- доступ абонентов области C к мировой сети невозможен - они не указаны на порту 2; кроме того, у абонентов C указан режим работы с абонентами противоположного порта только через ФПСУ;
- доступ от абонентов области C к маршрутизатору B невозможен, поскольку, во-первых, управление маршрутизатором не разрешено, во-вторых, он не описан как абонент, в-третьих, у абонентов C указан режим работы с абонентами противоположного порта только через ФПСУ.

16. 7. Использование ФПСУ для контроля доступа в интернет с NAT

Рассмотрим ситуацию, когда сеть организации использует внутренние локальные адреса, доступ ко внешним ресурсам в интернет осуществляется с помощью технологии NAT. ФПСУ выполняет процесс NAT, преобразуя серый IP-адрес в белый IP-адрес из диапазона адресов NAT.

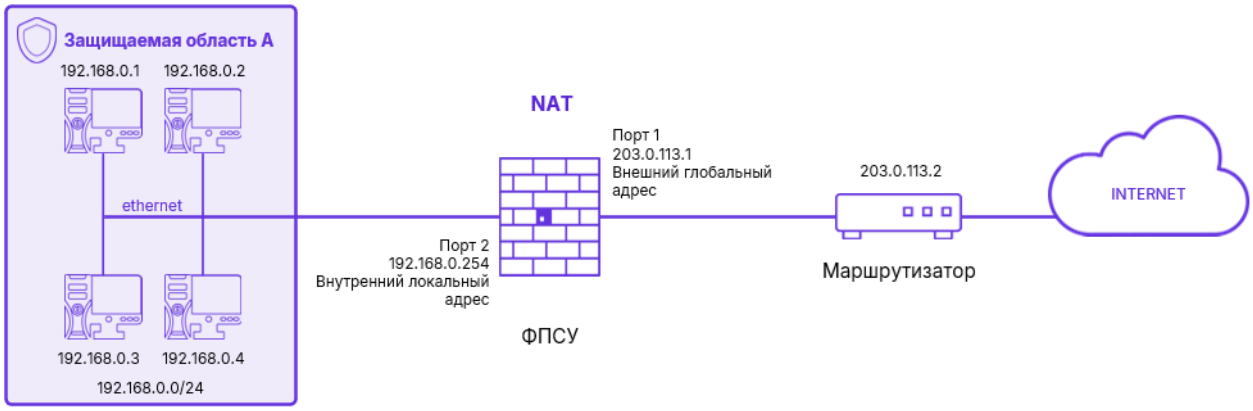


Рисунок 533 - Применение ФПСУ для доступа в интернет с NAT

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

- со стороны внутреннего порта комплекса (порта 2) существует одна IP подсеть, маршрутизаторы отсутствуют;
- со стороны внешнего порта (порта 1) установлен пограничный маршрутизатор,

через который осуществляется доступ в интернет;

- межсетевым экраном разрешены исходящие соединения всем хостам IP подсети, кроме хоста 192.168.0.1, в интернет, но запрещены любые входящие соединения из интернет.

Конфигурация ФПСУ должна содержать следующие установки:

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

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

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

Порт 2:
Номер 2,
Адрес 192.168.000.254,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.000.000; Маска 255.255.255.000;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;

```
режим партнера другого порта - включен только в ретрансляции;
флаг "Только Broadcast" выключен;
флаг "Отвечать на Ping" - на усмотрение администратора;
флаг "Работа разрешена" включен.

Правила межсетевого экрана на ФПСУ (подробности см. ниже)
DNS
block 192.168.0.1
Internet_All
```

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

1. Правило, разрешающее исходящие соединения с порта 2 для службы DNS (DNS-запросы по протоколу TCP/UDP с портом назначения 53);
2. Правило, запрещающее любые межсетевые исходящие соединения абонента 192.168.0.1 (в том числе будет запрещен интернет);
3. Правило, разрешающее исходящие соединения IP подсети через NAT в интернет;
4. Правило "Block other traffic", запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

```
Правила МЭ:
1 DNS
      Общие
        Действие         : Accept
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник
        Интерфейс        :   port2 iface2 192.168.000.254
      Назначение       : Любой
      Служба           : DNS

2 block 192.168.0.1
      Общие
        Действие         : Drop
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник
        Адрес            :   192.168.000.001/32 192.168.000.001
      Назначение         : Любой
```

```
      Служба          : Любая

3 Internet_All
      Общие
        Действие        : Accept
        Nat             : port1 iface1 203.000.113.001
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
      Источник
        Сеть            :   192.168.000.000 192.168.000.000/24
      Назначение      : Любой
      Служба          : Любая

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

Службы:
    DNS
      Общие
        Протокол        : TCP/UDP
        Порт источника  : Любой
        Порт назначения : 53 (Domain Name Server)
```

16. 8. Использование ФПСУ для контроля доступа ФПСУ-IP/Клиентов

Рассмотрим ситуацию, когда в сеть организации разрешен доступ ФПСУ-IP/Клиентам, которые подключаются удаленно через Интернет. ФПСУ-IP/Клиентам должны быть доступны внутренние ресурсы, но при этом эти ресурсы должны быть закрытыми для общего доступа через Интернет.

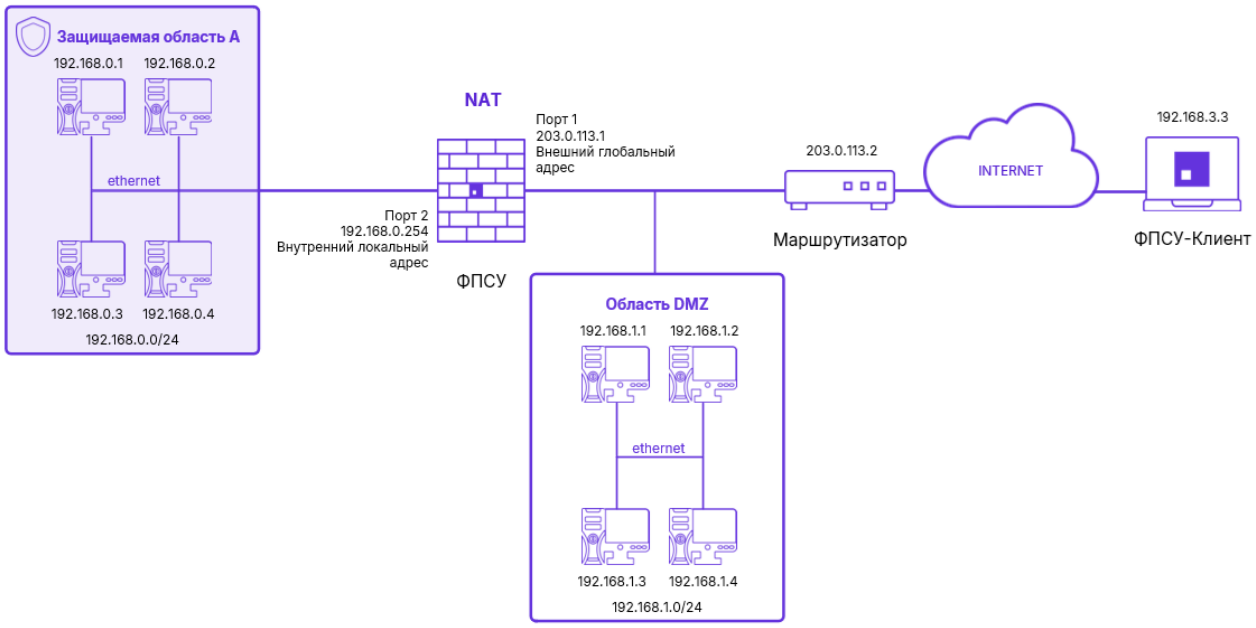


Рисунок 534 - Схема подключения ФПСУ-IP/Клиентов

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

- со стороны внутреннего порта комплекса (порта 2) существует IP подсеть 2, маршрутизаторы отсутствуют;
- со стороны внешнего порта (порта 1) существует содержащий общедоступные сервисы сегмент сети - область DMZ, в которой существует локальная IP подсеть 1, и установлен пограничный маршрутизатор, через который осуществляется доступ в интернет и подключаются Клиенты ФПСУ;
- Клиенты ФПСУ объединены в IP подсеть 3;
- Клиентам ФПСУ разрешен доступ в подсети 1 и 2.

Конфигурация ФПСУ должна содержать следующие установки:

Порт 1:
Номер 1,
Адрес 203.0.113.1,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы:203.0.113.2,
протоколы маршрутизации выключены;
флаг "Отвечать на Ping" - на усмотрение администратора.
Правила межсетевого экрана для этого маршрутизатора
Client_local

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

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

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

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

```
Client_local
Internet_All
```

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

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

Описатель Клиентов:

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

Параметры для портов ФПСУ

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

Правила межсетевого экрана для клиентов этого диапазона
Client_local

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

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

Правила МЭ:

1 DNS

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

```
    Лог             : Не вести лог
    Активно         : Да
  Источник
    Интерфейс       :   port2 iface2 192.168.000.254
  Назначение      : Любой
  Служба          : DNS
```

2 Client_local

```
  Общие
    Действие        : Accept
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник
    Клиент          :     СисCrypt Грп1
    Клиент          :   Мобильные клиенты  СисCrypt Грп1
    Клиент          :   example.com  СисCrypt Грп1
  Назначение
    Сеть            :   192.168.000.000 192.168.000.000/24
    Сеть            :   192.168.001.000 192.168.001.000/24
    Интерфейс       :   port1 iface1 203.0.113.001
    Интерфейс       :   port2 iface2 192.168.000.254
  Служба          : Любая
```

3 Internet_All

```
  Общие
    Действие        : Accept
    Nat             : port1 iface1 203.0.113.1
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник
    Сеть            :   192.168.000.000 192.168.000.000/24
    Сеть            :   192.168.001.000 192.168.001.000/24
  Назначение      : Любой
  Служба          : Любая
```

4 Block other traffic

```
  Общие
    Действие        : Drop
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник        : Любой
```

```
    Назначение      : Любой
    Служба          : Любая

Службы:
  DNS
    Общие
      Протокол        : TCP/UDP
      Порт источника  : Любой
      Порт назначения : 53 (Domain Name Server)
```

16. 9. Использование ФПСУ для объединения офисов с одинаковой внутренней адресацией

Предположим, что есть две территориально разделенные сети с одинаковой адресацией, для защиты которых применяются ФПСУ, необходимо обеспечить доступ хостов одной сети в другую через ФПСУ-туннель. Например, если в одной из сетей расположен сервер, защищенный доступ к которому предоставляется хостам из другой сети.

Такая организация защищаемых подсетей приведет к следующей логике конфигурирования:

- обмен между защищаемыми областями должен производиться только внутри организованного ФПСУ VPN-туннеля;
- на каждом ФПСУ должны быть установлены ранее выработанные криптографические ключи парно-выборочной связи. Причем на ФПСУ А указан используемый номер ключа 1, на ФПСУ В - номер 2;

ФПСУ А

- со стороны внутреннего порта 1 существует одна подсеть; маршрутизаторы и другие ФПСУ, через которые абоненты будут доступны с порта 1, отсутствуют;
- со стороны порта 1 описана подсеть, обмен хостов которой через комплекс производится в режиме ретрансляции;
- со стороны порта 1 описан абонент 192.168.0.1, обмен данными с которым определяется правилом МЭ, в правиле определена трансляция сетевых адресов и задана переадресация порта;
- со стороны внешнего порта 2 определен ФПСУ В и описан как абонент, обмен данными с которым определяется правилом МЭ, в правиле определена трансляция сетевых адресов и задана переадресация порта;

ФПСУ В

- со стороны внутреннего порта 1 существует одна подсеть; маршрутизаторы и другие ФПСУ, через которые абоненты будут доступны с порта 1, отсутствуют;

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

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

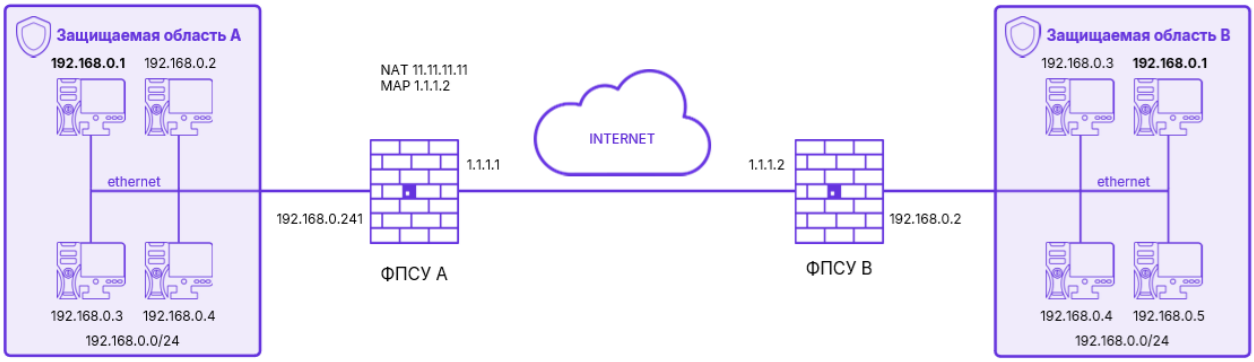


Рисунок 535 - Схема подключения разделенных сетей с одинаковой адресацией

ФПСУ А

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

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

Абоненты:
Подсеть; Адрес 192.000.000.000; Маска 255.000.000.000 (8 разряда);
режим работы ретрансляция;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен.

Хост; Адрес 192.168.000.001;
режим работы ретрансляция;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен;
Правила межсетевого экрана для этого абонента
ping over nat.

Порт 2:
Номер 2,
Адрес 001.001.001.001,
Маска 255.255.255.000 (24 разряда),
VLAN Нет;
Адрес 011.011.011.011,
Маска 255.255.255.000 (24 разряда),
VLAN 111;
ФПСУ:
001.001.001.002, ключевые данные - 1; смена через 120 сек;
сжатие и криптозащита - "запрещено" и "обязательно";
мост - выключен;
Маршрутизаторы: не определены,
протоколы маршрутизации выключены;

Абоненты:
Хост; Адрес 192.168.000.002;
режим работы Через ФПСУ 001.001.001.002;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен;

Правила межсетевого экрана для этого ФПСУ
ping over nat.

Службы межсетевого экрана для этого ФПСУ:
PING

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

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

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

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

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

ФПСУ B

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 указаны на ФПСУ В как используемые.

Порт 1:

Номер 1,
Адрес 192.168.000.002,
Маска 255.255.255.000 (24 разряда),
VLAN Нет;
ФПСУ не определены,
Маршрутизаторы: не определены,
протоколы маршрутизации выключены;

Абоненты:
Подсеть; Адрес 192.168.000.000; Маска 255.255.255.000 (24 разряда);
режим работы ретрансляция;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен.

Порт 2:

Номер 1,
Адрес 001.001.001.002,
Маска 255.255.255.000 (24 разряда),
VLAN Нет;
ФПСУ:
001.001.001.001, ключевые данные - 2.1; смена через 120 сек;
сжатие и криптозащита - "запрещено" и "обязательно";
мост - выключен;
Правила межсетевого экрана для этого ФПСУ
map.

Маршрутизаторы: не определены,
протоколы маршрутизации выключены;

Абоненты:
Хост; Адрес 011.011.011.011;
режим работы Через ФПСУ 001.001.001.001;
режим партнера данного порта — включен Ретрансляция Через ФПСУ;
режим партнера другого порта - включен Ретрансляция Через ФПСУ;
флаг "Работа разрешена" включен;

Правила межсетевого экрана для этого ФПСУ
map

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

1. Правило, разрешающее входящие соединения по протоколу ICMP с IP-адреса 11.11.11.11 на внешний порт ФПСУ B, IP-адрес назначения подменяется по заданному правилу MAP;
2. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

```
Правила МЭ:
1. map
      Общие
        Действие         : Accept
        Map              : 192.168.000.001
        Время работы     : Любое
        Лог              : Не вести лог
        Активно          : Да
      Источник
        Адрес            :   011.011.011.011/32 011.011.011.011
      Назначение
        Интерфейс        :   port2 iface2 001.001.001.002
      Служба
        PING

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

В конфигурациях ФПСУ приведены только необходимые для работоспособности схемы настройки, дополнительно для абонентов должен быть выключен флаг «Только Broadcast», флаг «Отвечать на Ping» устанавливается на усмотрение администратора.

16. 10. Использование ФПСУ для смены порта назначения трафика, направляемого в адрес абонента

В качестве назначения MAP в правиле межсетевого экрана можно ставить одиночный адрес, равный MAP-адресу с установкой порта назначения. При такой настройке ФПСУ будет менять порт назначения у всех пакетов, подпадающих под действие правила, на указанный администратором.

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

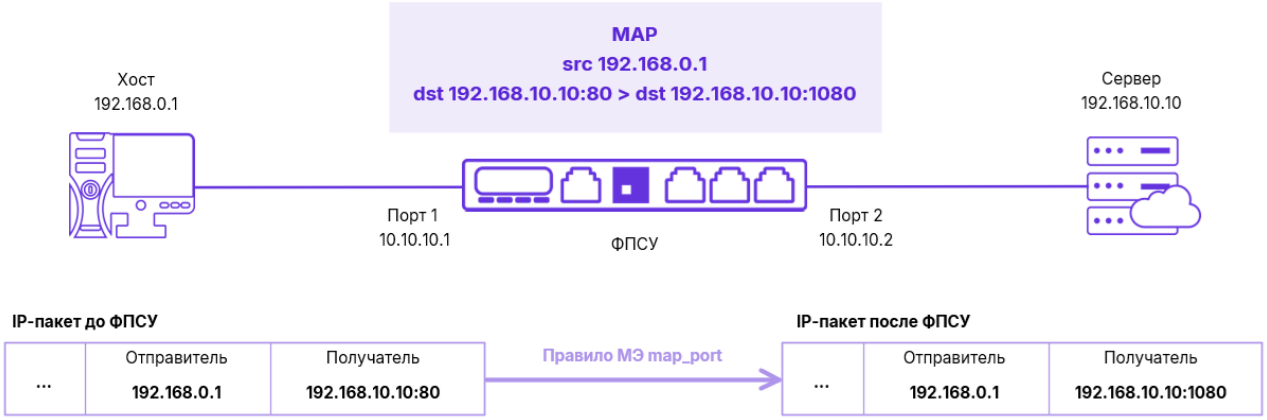


Рисунок 536 - Схема перенаправления пакетов на другой порт сервера

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

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

Конфигурация ФПСУ должна содержать следующие установки:

```
Порт 1      Адрес            Маска        VLAN
        010.010.010.001  255.255.255.000   Нет

 АБОНЕНТЫ
  Адрес 192.168.000.001   Хост
  Имя   192.168.000.001
  Режим работы     Ретрансляция
  Режим партнера
   Данного порта   Ретрансляция  Через ФПСУ
   Другого порта   Ретрансляция  Через ФПСУ
  Работа разрешена

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

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

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

1. Правило, разрешающее любые входящие соединения по протоколу TCP/UDP с портом назначения 80, для указанных соединений порт назначения преобразуется по заданному правилу MAP на номер 1080. В правиле межсетевого экрана во вкладке «Назначение» должен быть указан один и только один адрес назначения, адрес сервера. Во вкладке «Источник» может быть явно указан хост или подсеть, отправляющие запросы. Если вкладка «Источник» пустая, ФПСУ будет принимать и менять порт у любых входящих соединений с сервером и портом назначения 80. Во вкладке «Общие» в поле «MAP» указывается тот же IP-адрес сервера, что и во

вкладке назначения, и новый порт 1080, на который должны перенаправляться запросы. Данное правило применяется на порту 2 ФПСУ к абоненту сервер, указанному как хост;

2. Правило, запрещающее любые входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

Межсетевой экран активен: Да

Правила трафика

1. map_port

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

2. Block other traffic

```
    Общие
      Действие        : Drop
      Время работы    : Любое
      Лог             : Не вести лог
      Активно         : Да
    Источник        : Любой
    Назначение      : Любой
    Служба          : Любая
```

Службы

1. TCP/UDP

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

16. 11. Использование ФПСУ для балансировки нагрузки на порты внутреннего сервера

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

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

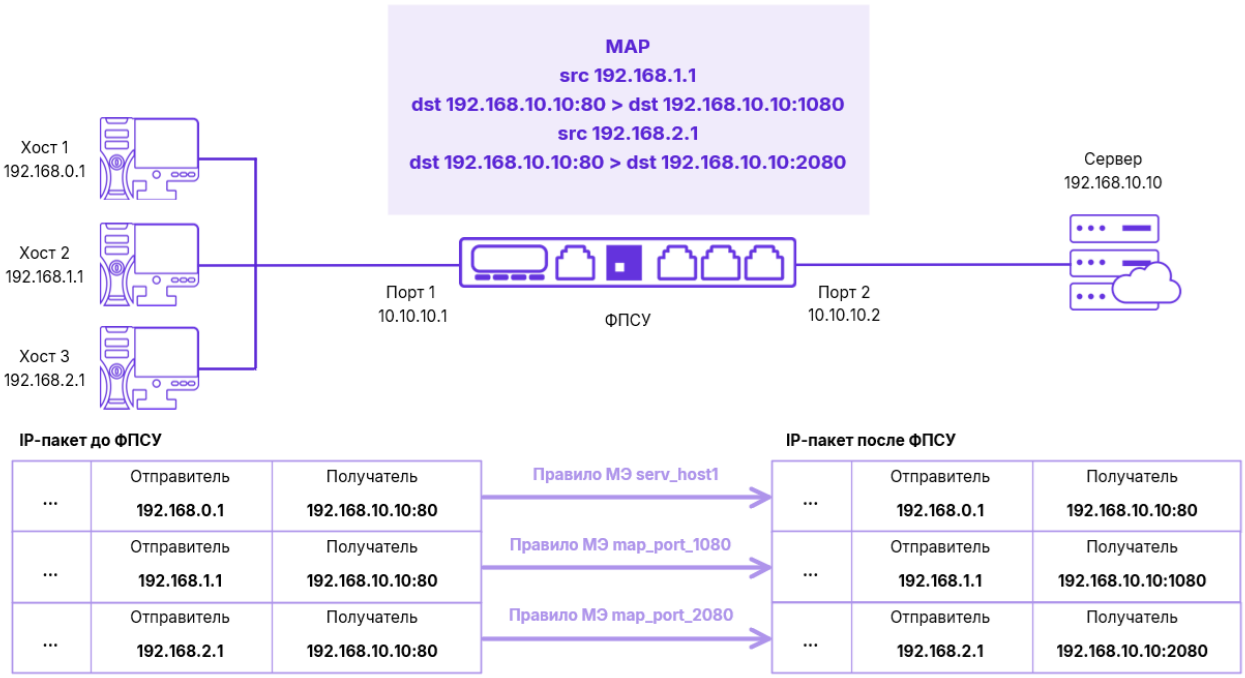


Рисунок 537 - Схема перенаправления пакетов на другие порты сервера

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

- в поле опции MAP, IP-адрес назначения и новый порт;

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

Конфигурация ФПСУ должна содержать следующие установки:

```
Порт 1      Адрес            Маска         VLAN
         010.010.010.001  255.255.255.000   Нет

  АБОНЕНТЫ
Адрес 192.168.000.001   Хост
   Имя   192.168.001.001
   MAC   Не задан
   Режим работы     Ретрансляция
   Режим партнера
    Данного порта   Ретрансляция  Через ФПСУ
    Другого порта   Ретрансляция  Через ФПСУ
   Работа разрешена
   Правила межсетевого экрана для этого абонента
    serv_host1

Адрес 192.168.001.001   Хост
   Имя   192.168.001.001
   MAC   Не задан
   Режим работы     Ретрансляция
   Режим партнера
    Данного порта   Ретрансляция  Через ФПСУ
    Другого порта   Ретрансляция  Через ФПСУ
   Работа разрешена
   Правила межсетевого экрана для этого абонента
    map_port_1080

   Адрес 192.168.002.001   Хост
   Имя   192.168.002.001
   MAC   Не задан
   Режим работы     Ретрансляция
   Режим партнера
    Данного порта   Ретрансляция  Через ФПСУ
    Другого порта   Ретрансляция  Через ФПСУ
   Работа разрешена
   Правила межсетевого экрана для этого абонента
```

```
    map_port_2080

 Порт 2      Адрес            Маска         VLAN
        010.010.010.002  255.255.255.000   Нет
  АБОНЕНТЫ
Адрес 192.168.010.010   Хост
   Имя   192.168.010.010
   MAC   Не задан
   Режим работы     Ретрансляция
   Режим партнера
    Данного порта   Ретрансляция  Через ФПСУ
    Другого порта   Ретрансляция  Через ФПСУ
   Работа разрешена
   Правила межсетевого экрана для этого абонента
    serv_host1
    map_port_1080
    map_port_2080
```

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

1. Правило, разрешающее входящие соединения по протоколу TCP/UDP хоста 192.168.0.1 в адрес сервера 192.168.10.10 на порт 80 (по умолчанию). Данное правило будет применено к абоненту 192.168.0.1 на порту 1 ФПСУ, а также на порту 2 ФПСУ к абоненту сервер 192.168.10.10, указанному как хост;
2. Правило, разрешающее входящие соединения по протоколу TCP/UDP хоста 192.168.1.1 в адрес сервера 192.168.10.10, порт IP-адреса назначения - по умолчанию 80 подменяется на другой порт 1080 по заданному правилу MAP. В правиле во вкладке «Назначение» обязательно должен быть указан один и только один IP-адрес - адрес сервера. Во вкладке «Источник» явно указан источник - хост 192.168.1.1. Во вкладке «Общие» в поле MAP необходимо указать тот же IP-адрес сервера, что указан в адресе назначения, и новый порт 1080. Данное правило будет применено к абоненту 192.168.1.1 на порту 1 ФПСУ, а также на порту 2 ФПСУ к абоненту сервер 192.168.10.10;
3. Правило, разрешающее входящие соединения по протоколу TCP/UDP хоста 192.168.2.1 в адрес сервера 192.168.10.10, порт IP-адреса назначения - по умолчанию 80 подменяется на другой порт 2080 по заданному правилу MAP. В правиле во вкладке «Назначение» обязательно должен быть указан один и только один IP-адрес - адрес сервера. Во вкладке «Источник» явно указан источник - хост 192.168.2.1. Во вкладке «Общие» в поле MAP необходимо указать тот же IP-адрес сервера, что указан в адресе назначения, и новый порт 2080. Данное правило

будет применено к абоненту 192.168.2.1 на порту 1 ФПСУ, а также на порту 2 ФПСУ к абоненту сервер 192.168.10.10;

4. Правило, запрещающее все остальные не указанные выше входящие и исходящие соединения, обязательно присутствует последним правилом в правилах МЭ при активации межсетевого экрана.

```
  Межсетевой экран активен: Да

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

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

3. map_port_2080
      Общие
        Действие        : Accept
        Мар             : 192.168.010.010 2080
        Время работы    : Любое
        Лог             : Не вести лог
        Активно         : Да
```

```
      Источник
        Адрес            :   192.168.002.001 192.168.002.001
      Назначение
        Адрес            :   192.168.010.010 192.168.010.010
      Служба
        TCP/UDP

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

Службы

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

В конфигурациях ФПСУ приведены только необходимые для работоспособности схемы настройки, дополнительно для абонентов должен быть выключен флаг «Только Broadcast», флаг «Отвечать на Ping» устанавливается на усмотрение администратора.

16. 12. Использование ФПСУ на медленных каналах. Спутник, spoofing

Рассмотрим ситуацию, когда сеть организации представляет отдельные локальные IP-подсети, разделенные территориально и для передачи данных используется спутниковый канал связи. Защищенное взаимодействие каждой из локальных подсетей обеспечивается ФПСУ, подключенного со стороны внутреннего порта пограничного маршрутизатора, предоставляющего доступ к сети Интернет с использованием технологий спутниковой связи (подробнее о настройках см. пункт «Дополнительные параметры и защита от flood-атак»).

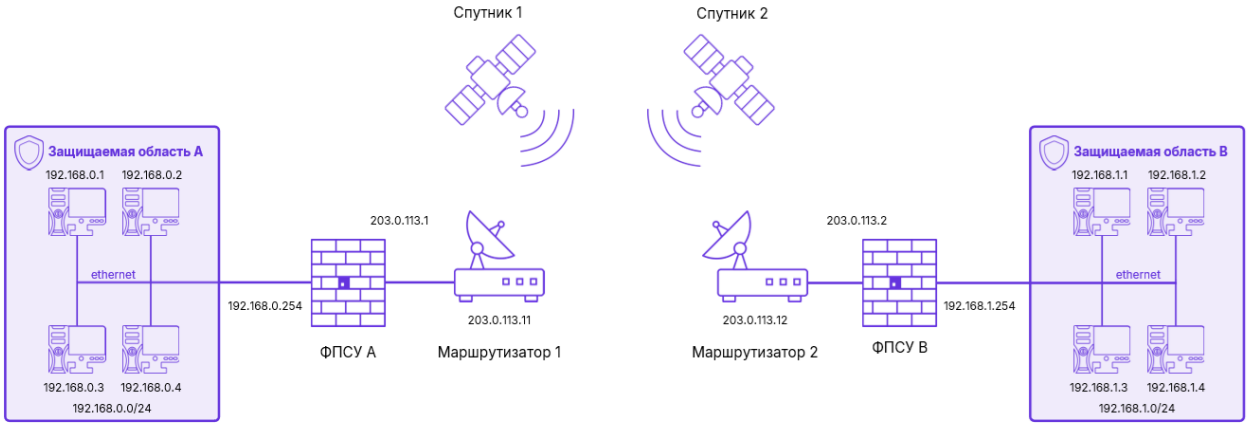


Рисунок 538 - Передача данных через спутниковый канал связи

Рассмотрим пример, когда абонент области А отправляет данные абоненту области В. При настройке спуфинга важно учитывать в каком направлении строится сессия TCP. Настройки спуфинга устанавливаются на принимающей стороне, ФПСУ В. Необходимо задать правило МЭ для входящего трафика от абонентов области А с включением функции спуфинга, включить настройки спуфинга в параметрах доступа на ФПСУ В. Спуфинг позволяет ФПСУ В отправлять подтверждение о получении TCP пакета от абонента области А не дожидаясь подтверждения его получения. На ФПСУ А достаточно задать правило МЭ для исходящего трафика. При обмене пакетами спуфинг на ФПСУ А включается автоматически, с настройками спуфинга по умолчанию.

Используются следующие IP-адреса:

- защищаемая область А - 192.168.0.0, маска 255.255.255.0 (24 бита);
- защищаемая область В - 192.168.1.0, маска 255.255.255.0 (24 бита).

Конфигурация ФПСУ должна содержать следующие установки:

Для ФПСУ А:

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

Порт 1:
Номер 1,
Адрес 203.000.113.001,
Маска 255.255.255.000 (24 разряда),
ФПСУ
203.000.113.2, ключевые данные - 2.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы:203.000.113.011,
протоколы маршрутизации выключены;

Абоненты:
Адрес 192.168.001.000; Маска 255.255.255.000;
Доступен через маршрутизатор 203.000.113.011
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2,
Адрес 192.168.000.254,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.000.000; Маска 255.255.255.000;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
Change

Правила МЭ:

1 Change
Общие
Действие : Accept
Время работы : Любое
Лог : Не вести лог
Активно : Да
Источник
Сеть : 192.168.000.000 192.168.000.000/24
Назначение
Сеть : 192.168.001.000 192.168.001.000/24
Служба : Любая

2 Block other traffic
Общие
Действие : Drop
Время работы : Любое
Лог : Не вести лог
Активно : Да

```
Источник        : Любой
Назначение      : Любой
Служба          : Любая
```

Для ФПСУ В:

Установлены выработанные ЦВК ключи парно-выборочной связи номер 2. Ключи номер 2 указаны как используемые.

Порт 1:

Номер 1,
Адрес 203.000.113.002,
Маска 255.255.255.000 (24 разряда),
ФПСУ
203.000.113.1, ключевые данные - 1.1; смена через 30 сек;
сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы:203.000.113.012,
протоколы маршрутизации выключены;

Абоненты:
Адрес 192.168.000.000; Маска 255.255.255.000;
Доступен через маршрутизатор 203.000.113.012
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.

Порт 2:

Номер 2,
Адрес 192.168.001.254,
Маска 255.255.255.000 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; Адрес 192.168.001.000; Маска 255.255.255.000;
режим работы ретрансляция;
режим партнера этого порта — включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
флаг "Работа разрешена" включен.
Правила межсетевого экрана для этого абонента
Spoof

Правила МЭ:
1 Spoof
Общие

```
    Действие        : Accept
    Время работы    : Любое
    Лог             : Не вести лог
    Spoof           : Да
    Активно         : Да
  Источник
    Сеть            :   192.168.000.000 192.168.000.000/24
  Назначение
    Сеть            :   192.168.001.000 192.168.001.000/24
  Служба          : TCP

2 Block other traffic
  Общие
    Действие        : Drop
    Время работы    : Любое
    Лог             : Не вести лог
    Активно         : Да
  Источник        : Любой
  Назначение      : Любой
  Служба          : Любая

Службы:
  1. TCP
    Общие
      Протокол        : TCP
      Порт источника  : Любой
      Порт назначения : Любой

меню Параметры доступа→Параметры→Spoofing:
Таймаут повторной пересылки задержанного пакета 250,
Шаг увеличения таймаута 125,
```

В конфигурациях ФПСУ приведены только необходимые для работоспособности схемы настройки, дополнительно для абонентов должен быть выключен флаг «Только Broadcast», флаг «Отвечать на Ping» устанавливается на усмотрение администратора.

Достаточно настроить спуфинг на одном ФПСУ, где используется спутниковая связь. Межсетевой экран ФПСУ должен быть задействован. Созданное правило межсетевого экрана должно быть задействовано. Межсетевым экраном контролируется каждая сессия, поэтому достаточно описать правило трафика из защищенной области А в защищенную область В.

16. 13. Применение prefix-list в протоколе BGP

Рассмотрим пример базовой настройки протокола BGP, ограничение трафика из одной автономной системы в другую организуется с помощью prefix-list. ФПСУ расположены в разных автономных системах.

Для установления eBGP-сессии между двумя ФПСУ необходимо на каждом ФПСУ:

- указать номер автономной системы Local AS, в которой находится ФПСУ;
- задать идентификатор Router ID для включения ФПСУ в протокол BGP;
- включить протокол BGP на вкладке «General»;
- объявить подсети в данной автономной системе;
- предварительно создать prefix-list для входящих и исходящих маршрутов (по необходимости);
- задать соседа на вкладке «Peers»;
- запустить ФПСУ.

Ограничим исходящие и входящие маршруты в таблицах маршрутизации ФПСУ:

- В таблицах маршрутизации ФПСУ описаны по 5 подсетей.
- ФПСУ А объявляет ФПСУ В только подсеть 100.0.1.0/24 по протоколу eBGP.
- ФПСУ А отклоняет объявление подсетей 100.0.2.0/24 и 200.0.2.0/24 от ФПСУ В по протоколу eBGP.

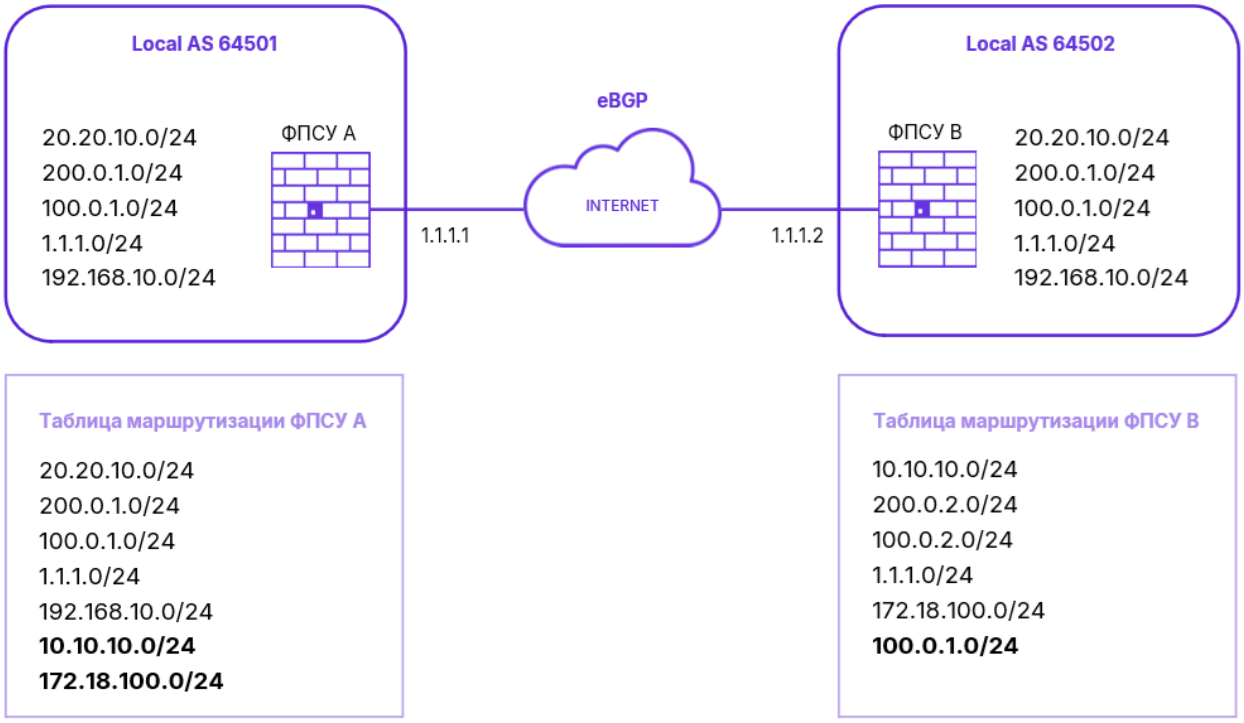


Рисунок 539 - Ограничение исходящих и входящих маршрутов на ФПСУ

ФПСУ А

Local AS 64501
Router ID 1.1.1.1
Graceful restart X
Require police on eBGP X
Активно X

Networks
1.1.1.0/24, описание N1, Активно X
100.0.1.0/24, описание N2, Активно X
200.0.1.0/24, описание N3, Активно
20.20.10.0/24, описание N4, Активно X
192.168.10.0/24, описание N5, Активно X

Peers
Адрес 1.1.1.2, описание ФПСУ В
Remote AS 64502
Keepalive time 60
Hold time 180
Graceful restart X
prefix-list pref1
Активно X

Prefix-list
Имя pref1, описание out
Prefix
Sequence 100, action Permit, адрес 100.0.1.0, маска 255.255.255.0

Имя pref1, описание in
Prefix
Sequence 100, action Deny, адрес 200.0.2.0, маска 255.255.255.0
Sequence 110, action Deny, адрес 100.0.2.0, маска 255.255.255.0
Sequence 120, action Permit, Any

ФПСУ B

Local AS 64502
Router ID 1.1.1.2
Graceful restart X
Require police on eBGP X
Активно X

Networks
10.10.10.0/24, описание N1, Активно X
100.0.2.0/24, описание N2, Активно X
200.0.2.0/24, описание N3, Активно X
1.1.1.0/24, описание N4, Активно X
172.18.100.0/24, описание N5, Активно X

Peers
Адрес 1.1.1.1, описание ФПСУ A
Remote AS 64501
Keepalive time 60
Hold time 180
Graceful restart X
Активно X

17. Способы разрешения возможных проблем при работе ФПСУ

17. 1. Первый запуск ФПСУ

Несмотря на то, что установка ФПСУ 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 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 введены специальные процедуры, позволяющие обновлять «недостоверные» ARP-записи в ARP-таблицах как пограничных маршрутизаторов, так и хостов, находящихся со сторон его портов. Однако обновление производится только при попытке обмена пакетами хостов защищаемой области с другими хостами или сетевым оборудованием (когда установленный комплекс «знакомится» с хостами или оборудованием, смежными с ним). Если в защищаемой области окажется сервер (передающий пакеты только в ответ на посылаемый запрос, которого он не может получить, поскольку маршрутизирующему оборудованию известен «недостоверный» адрес сетевого адаптера сервера, которому он должен передавать запросы) или другой хост, работающий в пассивном режиме, они будут недоступны в течение «времени старения» соответствующих записей в ARP-таблицах.

Для нормализации работы сети в данной ситуации рекомендуется принять следующие меры:

1. В случае, если ФПСУ устанавливается между защищаемой областью и ее пограничными маршрутизаторами - очистить ARP-таблицы пограничных маршрутизаторов или перезапустить маршрутизаторы;
2. Если между защищаемой областью и ФПСУ 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.

17. 2. Устранение неполадок, связанных с работой сетевого оборудования

Одна из возможных причин возникновения большого количества ошибок в работе сети, или неэффективной работы ФПСУ, выражающейся в резком падении скорости приема/передачи пакетов, связана с несовместимыми режимами работы сетевых адаптеров как самого ФПСУ, 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 19. Причины возникновения неполадок

Неполадки	Возможные причины неполадок	Методы определения и/или устранения
Отсутствие принимаемых пакетов на соответствующем порту ФПСУ.	Несоответствующий тип соединительного кабеля между ФПСУ и смежным оборудованием	Проверить тип применяемого кабеля и убедиться в его соответствии подключенному оборудованию
Отсутствие принимаемых пакетов на соответствующем порту ФПСУ или появление большого количества ошибочных пакетов (см. пункт «Окно состояния рабочих LAN портов»)	Дефект соединительного кабеля между ФПСУ и смежным оборудованием	Проверить работоспособность применяемого кабеля и при обнаружении неисправности заменить кабель

Отсутствие принимаемых пакетов на соответствующем порту ФПСУ	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 большого количества ошибочных пакетов (см. пункт «Окно состояния рабочих LAN портов») снижение скорости передачи или невозможность передачи данных через ФПСУ.	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.

18. Диагностика ошибок ФПСУ

При отладке работы ФПСУ сразу после его установки, а также в процессе его дальнейшей работы администратор имеет возможность отслеживать процессы, происходящие в различных подсистемах ФПСУ. Сообщения об ошибках или неполадках, обнаруженных работающим ФПСУ, выдаются на экран монитора (если к ФПСУ подключен монитор) и в регистрационные записи статистики (см. разделы «Окно состояния работы пользователей» и «Просмотр статистики»). Данный раздел поясняет выдаваемые диагностические сообщения и представляет возможные причины возникновения ошибок и методы их устранения.

Таблица 20. Ошибки формата принимаемых IP-пакетов

Диагностика	Пояснение	Причина возникновения
Короткий пакет	Длина принятых данных короче, чем указано в IP заголовке принятого пакета.	Сбой или коллизии локальной сети; сбой у станции отправителя.
Ошибка фрагментации	Суммарная длина собранного из фрагментов IP-пакета больше 65536 байт.	Некорректная работа программного обеспечения станции-отправителя. Если при передаче данных используется протокол TCP, ошибки можно избежать, включив опцию «Корректировать TCP MSS» (см. пункт «Общие параметры конфигурации ФПСУ»)
Отмена фрагментации	Размер пакета превышает максимальный размер пакета, MTU, но установленный флаг запрета фрагментации не дает разбивать его на несколько пакетов.	Такая ситуация обычно возникает при попытке передачи пакетов TCP/UDP по протоколу FTP и некоторым другим протоколам, и носит временный характер. Если ошибка возникает постоянно, необходимо проанализировать (и, при необходимости, скорректировать) конфигурацию сетевых адаптеров и/или уменьшить MTU до 1400 байт на оборудовании, от которого приходят большие пакеты с флагом запрета фрагментации.

Диагностика	Пояснение	Причина возникновения
Ошибочный фрагмент	Начало фрагментированного пакета не выровнено на 8 байтовую границу.	Некорректная работа программного обеспечения станции-отправителя.
Неверен список опций	Список IP-опций в заголовке IP пакета не отвечает принятым в сообществе Интернет правилам.	Некорректная работа программного обеспечения станции-отправителя.
Мало памяти	Недостаточно оперативной памяти для приема и/или обработки пакета.	Если такая ошибка указывается для разных IP адресов, причина возникновения - «шторм» в IP сети. Если ошибка возникает только для одного конкретного адреса - вероятно проведение атаки на ФПСУ с целью вывода его из строя через создание сетевой перегрузки.

Таблица 21. Ошибки, связанные с обработкой принимаемых пакетов

Диагностика	Пояснение	Причина возникновения
Маршрут неизвестен	Не известен адрес сетевого адаптера для соответствующего IP-адреса абонента-получателя.	Если ошибка возникает постоянно - либо станции с таким IP-адресом в сети нет или она не работает, либо режимы смежных сетевых адаптеров несовместимы. Если ошибка возникает эпизодически - неполадки отсутствуют, в момент поступления запроса адрес сетевого адаптера был неизвестен, после чего он был автоматически определен ФПСУ за непродолжительное время.

Диагностика	Пояснение	Причина возникновения
Сбой LAN карты	Сбой указанного сетевого адаптера при попытке передачи фрейма	Неустойчивая работа сбойного сетевого адаптера - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.
MAC-адрес станции совпадает с адресом ФПСУ	получен фрейм, MAC-адрес отправителя которого совпадает с MAC-адресом одного из сетевых портов ФПСУ	Сетевые пакеты от станции, MAC-адрес которой совпадает с MAC-адресом одного из портов ФПСУ, будут сброшены. Требуется изменить MAC-адрес у рабочей станции или у ФПСУ.
Дублирование адресов	В сети со стороны указанного порта обнаружена станция, имеющая IP адрес, совпадающий с одним из портов ФПСУ, или адрес сетевого адаптера которой совпадает с адресом сетевого адаптера ФПСУ.	Это может произойти при образовании маршрутной петли - проверьте правильность конфигурации маршрутизирующего оборудования. В сети на самом деле существует такая станция — смените адреса на ФПСУ или указанной станции.
Неверен IP адрес	Неверен один из IP-адресов в заголовке IP пакета.	IP-адрес отправителя является широковещательным в известные ФПСУ подсети. Отправитель пакета не является известным ФПСУ маршрутизатором, а IP-адрес получателя является либо групповым (multicast), либо широковещательным во все подсети (255.255.255.255). IP-адрес отправителя пакета — 255.255.255.255.
Истекло время	Время жизни пакета истекло, или исчерпан лимит времени ожидания сборки пакета	У принятого пакета истекает время жизни.

Диагностика	Пояснение	Причина возникновения
		Если данная ошибка проявляется часто, причем получателем является данный ФПСУ, а отправителем - другой ФПСУ, рекомендуется в конфигурации обоих ФПСУ изменить значение MTU (см. раздел «Описание параметров туннелей с другими ФПСУ»)
Протокол недоступен	Обращение к одному из портов ФПСУ по протоколу, который ФПСУ не поддерживает.	ФПСУ 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.

Таблица 22. Ошибки, связанные с попытками нарушения установленных правил фильтрации

Диагностика	Пояснение	Причина возникновения
Входящий не описан	Отправитель пакета не описан в конфигурации	Отправитель пакета не описан в конфигурации портов ФПСУ.
Получатель не описан	Получатель пакета не описан в конфигурации.	Не описан абонент-получатель в конфигурации портов ФПСУ. Для межмаршрутизаторного обмена - нет маршрутизаторов со стороны противоположного порта, использующих данный протокол.
Запрет работы	Отказ в доступе абоненту-отправителю пакета	Выключен флаг «Работа Разрешена» у отправителя или получателя пакета. Попытка приема или передачи в индивидуальный адрес при включенном флаге «Только Broadcast». Попытка межмаршрутизаторного обмена по неразрешенному протоколу маршрутизации для маршрутизатора-отправителя пакета.

Диагностика	Пояснение	Причина возникновения
		«Ping» - попытка ФПСУ от прописанного абонента или маршрутизатора при выключенном флаге «Отвечать на Ping». «Ping» - попытка ФПСУ длинным пакетом. Не «Ping» - попытка обращения прописанного абонента к удаленному ФПСУ или абонент не является удаленным администратором или ФПСУ.
Запрет по доступу	Запрет по режиму работы с партнером.	Запрет по режиму работы с партнером данного или противоположного порта.
Запрет SourceRoute	Запрет доступа по опции SourceRoute в IP-пакете.	В принятом IP-пакете присутствует одна из опций, требующая записывать маршрут прохождения пакета, а в конфигурации ФПСУ установлен флаг «Пакеты с опцией SourceRoute» - «Не пропускать».
Абонент через ФПСУ	Абонент должен работать в режиме ретрансляции.	Принят пакет из VPN-туннеля от абонента, для которого на данном ФПСУ установлен режим работы «Ретрансляция».
Абонент миновал ФПСУ	Абонент должен работать через ФПСУ.	Принят пакет не из VPN-туннеля от абонента, для которого на данном ФПСУ установлен режим работы «Через ФПСУ».
ФПСУ не работает	Удаленный ФПСУ не работает.	Не включен удаленный ФПСУ или с ним нет связи. Не работает сетевой адаптер - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.
Нет ФПСУ-туннеля	Отсутствие взаимодействия между ФПСУ.	VPN-туннель между двумя ФПСУ не установлен к моменту попытки передачи через него пакетов от абонентов. Не включен удаленный ФПСУ или с ним нет связи. Неустойчивая работа сбойного сетевого адаптера - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.

Диагностика	Пояснение	Причина возникновения
Ложный ФПСУ	Станция-отправитель использует ошибочный протокол установки соединения или поддержания VPN-туннеля	Попытка передачи пакетов в IP-адрес местного ФПСУ от рабочей станции, зарегистрированной как удаленный ФПСУ, но не являющейся таковой.
Ошибочный ФПСУ-пакет	Ошибочный пакет от ФПСУ.	На местном или удаленном ФПСУ указаны неверные значения номеров ключевых данных удаленных ФПСУ. В процессе установки или поддержания VPN-туннеля произошел кратковременный сбой, что обычно очень редко проявляется в момент первичной установки VPN-туннеля. Попытка навязывания местному ФПСУ VPN-данных или повторения ранее переданных удаленным ФПСУ данных от «вредоносной» станции.
Ошибка клиент-пакет	Искажены или повреждены находящиеся в полученном от ФПСУ-IP/Клиента пакете данные.	Сообщение возникает на экране мониторинга подключенных ФПСУ-IP/Клиентов. Такие пакеты будут сброшены ФПСУ.

Таблица 23. Ошибки, связанные с ключевыми данными

Служебное сообщение	Пояснение	Действия администратора
The TM does not contain the key	Ошибка возникает при попытке запуска ФПСУ с помощью ТМ-идентификатора, на котором находится искаженный ключ запуска.	Если искажен ключ запуска Главного администратора - обратитесь к поставщику ФПСУ для замены ТМ-идентификатора Главного администратора. Если искажен ключ запуска пользователя другого класса - повторно перезапишите ТМ-идентификатор пользователя средствами ФПСУ (Настройка системы - Регистрация ТМ-идентификаторов)
Внимание! Повреждены критические компоненты комплекса. ВСЕ установленные ключевые данные и ТМ утрачены. Комплекс переведен в технологический режим. Возможно, потребуется переустановка комплекса	ПО ФПСУ обнаружило искажение ключа для хранения долговременных ключей. Требуется вмешательство администратора	Требуется выполнить повторный перевод ФПСУ из технологического режима в рабочий режим, заново зарегистрировать все ТМ-идентификаторы пользователей и переустановить ключевые данные ЦВК и удаленных администраторов. В случае ошибки перевода ФПСУ из технологического режима в рабочий режим, выполнить полную переустановку ПО ФПСУ.
Внимание! Поврежден компонент комплекса. Необходима инициализация ДСЧ	ПО ФПСУ обнаружило искажение ключа ПДСЧ. Требуется вмешательство администратора	Требуется выполнить повторный перевод ФПСУ из технологического режима в рабочий режим.
Внимание! ФПСУ не работоспособен. Искажены данные конфигурации. Ожидание восстановления конфигурации с	ПО ФПСУ обнаружило искажение конфигурации ФПСУ	Восстановить конфигурацию ФПСУ любым из следующих способов: • локально с помощью резервной копии конфигурации;

Служебное сообщение	Пояснение	Действия администратора
резервного комплекса или удаленного администратора		• подключить к ФПСУ комплекс горячего резерва; • установить на ФПСУ новую конфигурацию средствами удаленного администратора.
Ошибка инициализации! Служебный описатель искажен	Сообщение об ошибке выводится на экран просмотра состояний удаленных администраторов ФПСУ. ПО ФПСУ обнаружило искажение секретного ключа ФПСУ подсистемы удаленного администрирования или открытых ключей удаленных администраторов. Удаленное управление ФПСУ с такой ошибкой невозможно.	Заново зарегистрировать удаленных администраторов на ФПСУ. Перерегистрировать ФПСУ на всех удаленных администраторах.
Описатель удаленных администраторов испорчен или несовместимая версия!	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ.	Заново зарегистрировать удаленных администраторов на ФПСУ. Перерегистрировать ФПСУ на всех удаленных администраторах.

Служебное сообщение	Пояснение	Действия администратора
	ПО ФПСУ обнаружило искажение секретного ключа ФПСУ подсистемы удаленного администрирования или открытых ключей удаленных администраторов Удаленное управление ФПСУ с такой ошибкой невозможно.	
**Имя_файла_с_открытым_ключом_удаленного_администратора*----> Поврежден*	Сообщение об ошибке выводится на экране регистрации удаленных администраторов меню настройки системы ФПСУ 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
Состояние туннеля с другим ФПСУ "WaitSynRR" с дополнительными сообщениями в журнале статистики "Аварийное состояние	Хранящиеся на внутреннем накопителе ФПСУ парно-выборочные ключи были искажены.	Заново установить на ФПСУ полученные от администратора ЦВК парно-выборочные ключи.

Служебное сообщение	Пояснение	Действия администратора
ключей/нештатные действия: Ошибка при зачитывании установленных ключей"	Требуется вмешательство администратора	
Данные искажены, пропускаю!	Сообщение об ошибке выводится на экране установки ключей меню конфигурации ФПСУ. Возникает при искажении предъявленного на внешнем USB-носителе парно-выборочного ключа	Заново получить от администратора ЦВК парно-выборочный ключ взамен искаженного.
Испорчены служебные данные горячего резервирования	Сообщение об ошибке выводится на экране мониторинга состояния горячего резерва ФПСУ (основной комплекс системы горячего резервирования). Ошибка возникает при искажении хранящегося на внутреннем накопителе ФПСУ ключа горячего резерва	Считать на ТМ-идентификатор ключ горячего резерва с исправного комплекса (меню локального конфигурирования ФПСУ «Настройка системы» - «Параметры горячего резерва»). Если ключ горячего резерва не считывается с исправного комплекса, создать новый ключ горячего резерва. Повторно зарегистрировать ключ горячего резерва на сообщившем об ошибке ФПСУ.

Служебное сообщение	Пояснение	Действия администратора
ФАТАЛЬНАЯ ОШИБКА. Резервный комплекс не может функционировать, так как испорчены служебные данные горячего резервирования. Возможно, потребуется переустановка комплекса	Сообщение об ошибке выводится при запуске ФПСУ (резервный комплекс системы горячего резервирования). Ошибка возникает при искажении хранящегося на внутреннем накопителе ФПСУ ключа горячего резерва	Считать на ТМ-идентификатор ключ горячего резерва с исправного комплекса (меню локального конфигурирования ФПСУ «Настройка системы» - «Параметры горячего резерва»). Если ключ горячего резерва не считывается с исправного комплекса, создать новый ключ горячего резерва. Повторно зарегистрировать ключ горячего резерва на сообщившем об ошибке ФПСУ.
Испорчен или не установлен ключ центра	Сообщение об ошибке выводится на экране мониторинга действий ФПСУ-IP\Клиентов. Искажен общесистемный ключ Криптосети Клиентов. ФПСУ-IP\Клиенты не могут соединиться с ФПСУ	Заново установить на ФПСУ общесистемный ключ Криптосети Клиентов вместо искаженного.
ТМ испорчена	Сообщение об ошибке выводится при попытке зарегистрировать общесистемный ключ Криптосети Клиентов на ФПСУ. 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

Таблица 24. Ошибки при соединении ФПСУ

Диагностика	Пояснение	Причина возникновения
Не совпадают RKL роли клиент/ФПСУ	Оба участника ФПСУ-IP/Клиент и ФПСУ при соединении должны поддерживать удаленную загрузку ключевых данных	На ФПСУ с установленной подсистемой RKL (подсистемой удаленной загрузки ключевых данных) пытается соединиться ФПСУ-IP/Клиент, VPN-Key которого не поддерживает удаленную загрузку ключевых данных, или наоборот, к ФПСУ без подсистемы RKL соединяется ФПСУ-IP/Клиент, VPN-Key которого поддерживает удаленную загрузку ключевых данных

18. 1. Выдача файла Kmsg

Команда «Выдать kmsg» окна просмотра статистики ФПСУ («Статистика ФПСУ») позволяет выдать на внешний носитель (USB-flash) файл для анализа сообщений ядра и использования памяти в случае падения ядра Linux.

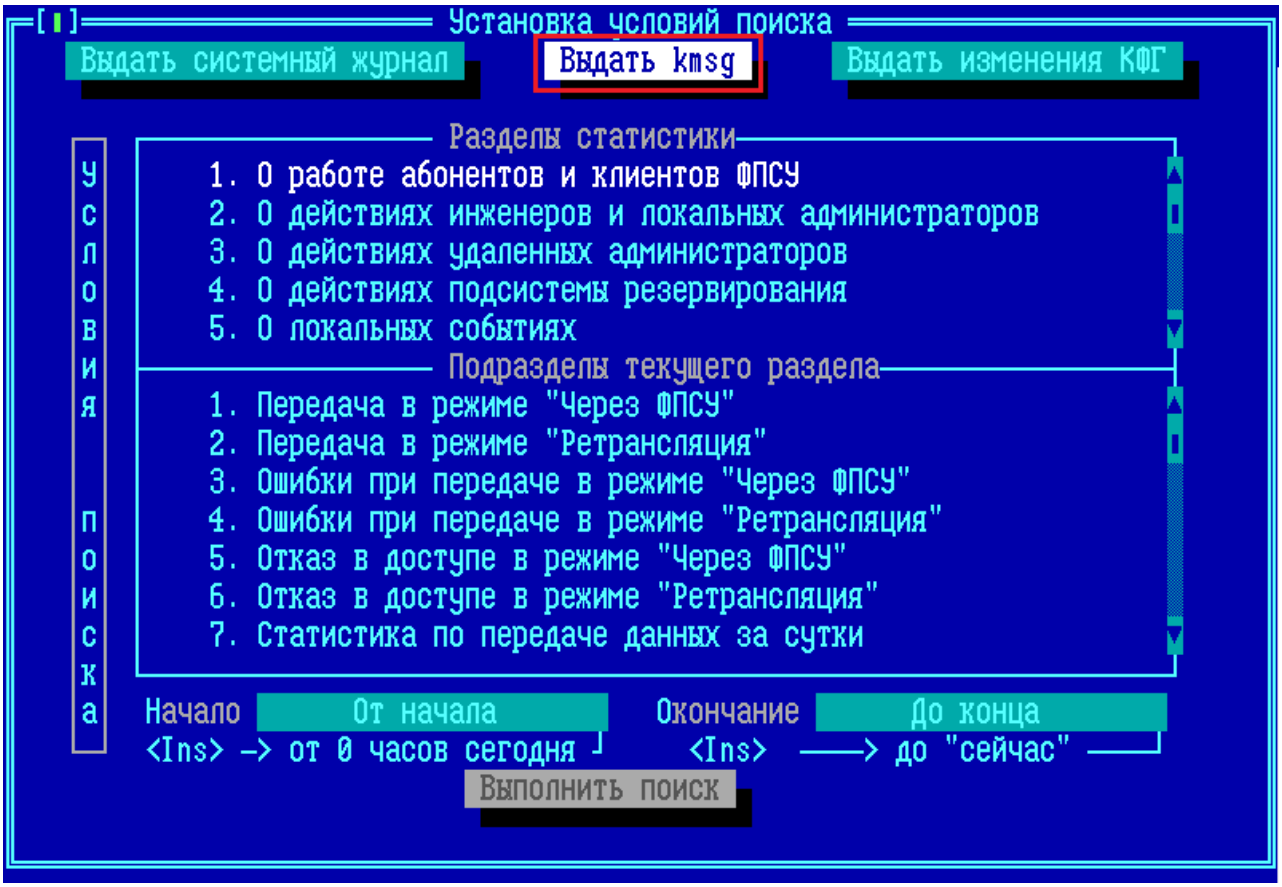


Рисунок 540 - Команда выдачи журнала изменений конфигурации межсетевого экрана

После выполнения команды система предложит подключить USB-носитель, на который будет выдан файл, к ФПСУ:

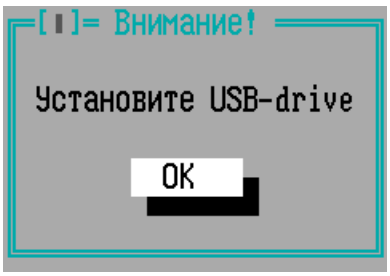


Рисунок 541 - Предложение подключить USB-носитель

Подключите носитель к ФПСУ и подтвердите выполнение команды, нажав клавишу Enter. Если USB-носитель будет обнаружен ФПСУ, то откроется окно диалога, в котором следует выбрать каталог на носителе.

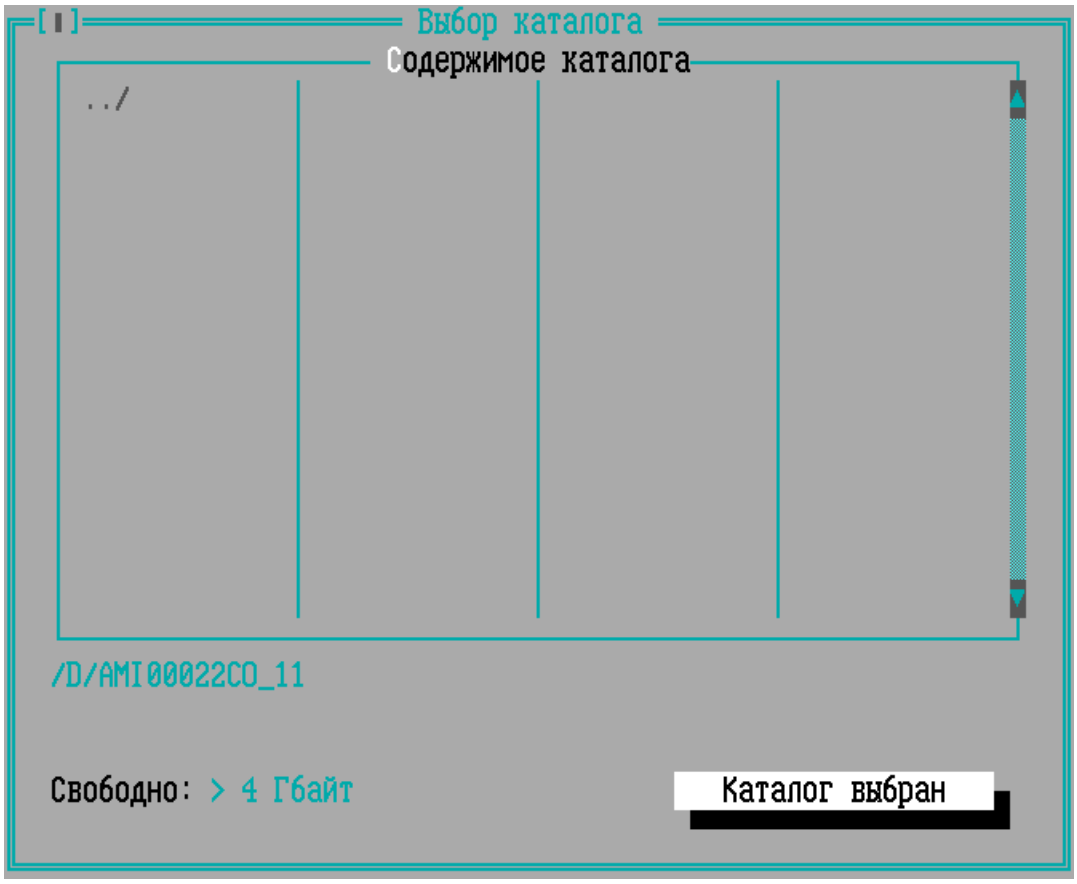


Рисунок 542 - Выбор каталога для выгрузки файла

Подтвердите место выгрузки файла, выполнив команду «Каталог выбран».

После выгрузки файла, ФПСУ выдаст системное оповещение о завершении процедуры:

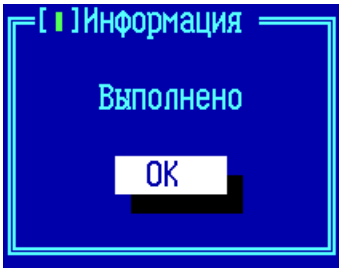


Рисунок 543 - Сообщение о завершении процедуры

18. 2. Выдача файла отладки OSPF

Команда меню «Настройка дополнений → FRR → Скопировать логи» позволяет выдать на внешний носитель (USB-flash) файл отладки OSPF. Перед выполнением команды необходимо подключить USB-носитель, на который будет выдан файл, к ФПСУ и запустить

команду. На внешнем носителе будет создан каталог frr.log и записан отладочный файл ospf.log.

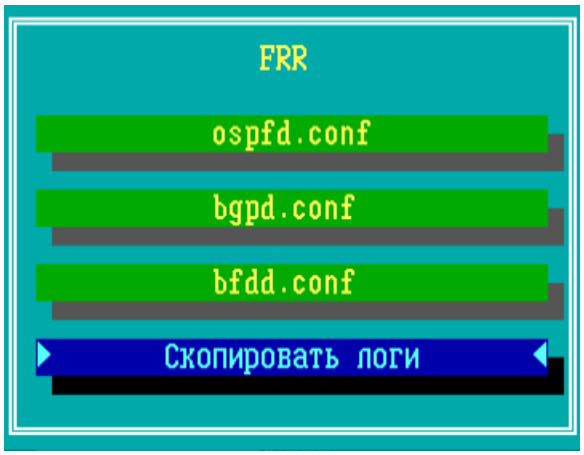


Рисунок 544 - Меню «Configure frr»

18. 3. Диагностика ошибок с помощью mlog

Зарегистрированные события на ФПСУ могут быть выданы в текстовом формате. Подпрограмма mlog записывает события в журнал. Журнал может быть использован для диагностики и выявления ошибок при старте ФПСУ, запуске аддонов, установлении соединений, установлении туннелей с другими ФПСУ, подключении Клиентов и при других событиях ФПСУ.

В главном меню по команде «Сервисные функции» отображается подменю с командами для работы с утилитой mlog.

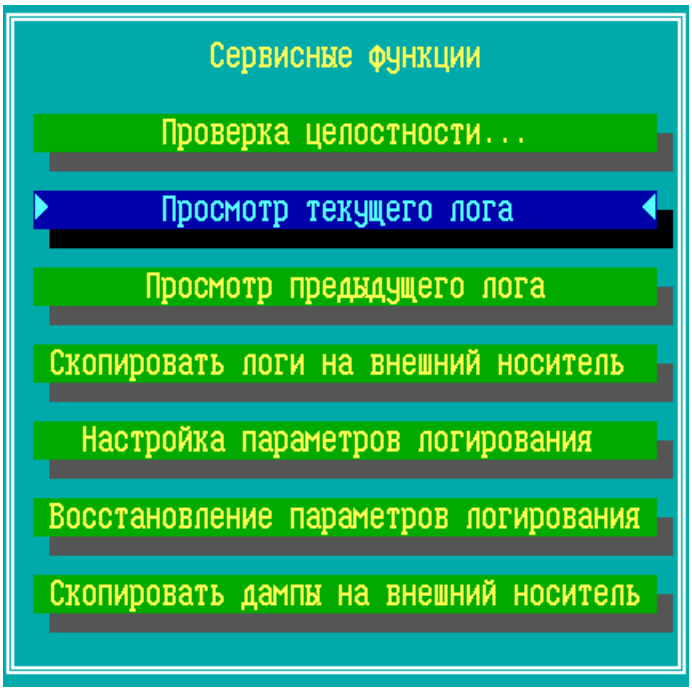


Рисунок 545 - Команды для работы с утилитой mlog

При выполнении операции необходимо подтверждение полномочий в зависимости от выполняемой команды.

Просмотр текущего лога – команда просмотра файла mlog.txt. Операция доступна администраторам класса *Администратор* или *Инженер*.

Просмотр предыдущего лога – команда просмотра файла mlog.txt.old. Операция доступна администраторам класса *Администратор* или *Инженер*.

Скопировать логи на внешний носитель – с помощью данной команды файл mlog.txt будет сохранен на внешний носитель. Перед вызовом команды необходимо подключить USB-носитель к USB-порту ФПСУ. Операция доступна администраторам класса *Администратор*.

Настройка параметров логирования – по команде открывается файл mlog.dsr в текстовом редакторе для просмотра и внесения изменений параметров логирования. Операция доступна администраторам класса *Администратор*.

Восстановление параметров логирования – по команде сбрасываются настройки файла mlog.dsr до базовых. Операция доступна администраторам класса *Администратор*.

События диагностики записываются в файл mlog.txt.

Примечание. Данные сетевого трафика выводятся в файлы .pcap, необходимо

дополнительно описать эти параметры.

Запись журнала ведется в файл mlog.txt, данная запись называется текущим логом. После начала записи лога существующий файл mlog.txt становится предыдущим логом и изменяет название на mlog.txt.old, новый вывод mlog становится текущим.

Лог записывается следующими способами:

- ***С помощью перезагруки комплекса.***

Необходимы следующие действия:

1. Перейти в режиме конфигурирования ФПСУ в главном меню и подключить USB-носитель с утилитой mlog.dsr для записи журнала.
2. Запустить ФПСУ в режиме фильтрации пакетов по команде главного меню «Запуск».
3. Подождать воспроизведения возникшей ошибки, затем выйти в главное меню ФПСУ.
4. Отключить USB-носитель. Перед отключением USB-носителя рекомендуется подождать 10 секунд для корректной записи лога.

- ***С помощью комбинации клавиш <Alt+L>.***

Необходимы следующие действия:

1. Перейти в режиме конфигурирования ФПСУ в главном меню и подключить USB-носитель с утилитой mlog.dsr для записи журнала.
2. Запустить ФПСУ в режиме фильтрации пакетов по команде главного меню «Запуск».
3. Нажать комбинацию клавиш <Alt+L>.
3. Подождать воспроизведения возникшей ошибки.
4. Завершить запись текущего лога по той же комбинации клавиш <Alt+L>.
5. Отключить USB-носитель. Перед отключением USB-носителя рекомендуется подождать 10 секунд для корректной записи лога.

- ***С помощью УА ФПСУ.***

Необходимые действия изложены в руководстве «Удаленный администратор ФПСУ-IP».

После нажатия комбинации клавиш <Alt+L> на экран ФПСУ будет выдано сообщение о записи лога, при записи диагностики mlog на экране ФПСУ отображается индикация активности красным цветом, показывающая продолжительность записи mlog и текущее время на ФПСУ.

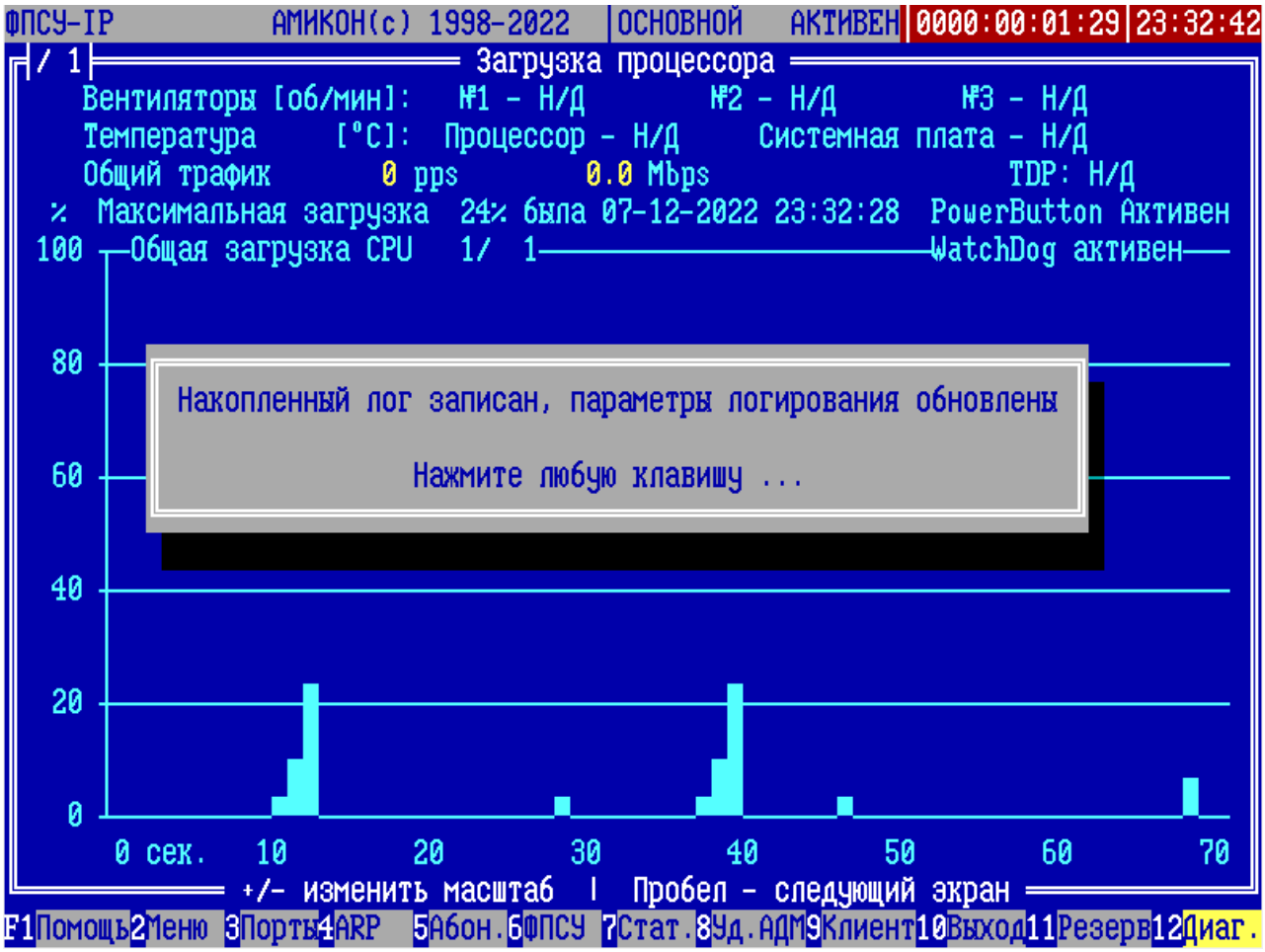


Рисунок 546 - Индикация активности при записи диагностики mlog

Утилита mlog определяет ведение статистики на 7 уровнях логирования. Чем выше уровень, тем больший размер лога необходимо установить, чтобы лог не перезаписывался.

В случае возникновения проблем в работе ФПСУ, во время отладки и снятия результатов работы подпрограммы mlog необходимо убрать излишнюю детализацию лога, отключив вывод параметров, не влияющих на анализируемое событие, тем самым сократив выводимый трафик, а также подобрать уровень логирования, позволяющий выявить проблему, не увеличивая размер лога. .

Размер файла mlog

На ФПСУ во внутренней памяти выделяется не более 100 Мб для записи лога, размер файла mlog зависит от установленных параметров логирования и свободного места на USB-носителе.

Для просмотра или изменения размера файла mlog.txt следует по команде меню «Сервисные функции → Настройка параметров логирования» зайти в редактор утилиты и найти следующий параметр с установленным размером в килобайтах в начале файла:

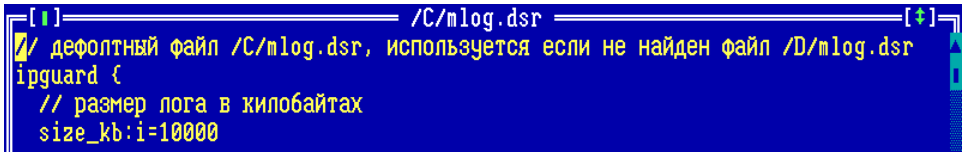


Рисунок 547 - Установленный размер журнала mlog

Вывод данных сетевого трафика

Дополнительно в вывод утилиты может быть добавлен вывод данных сетевого трафика, для этого в конце файла mlog.dsr в текстовом редакторе требуется добавить текст со следующими параметрами:

```
pcap {
   eth0 {
     flush_to_file="/D/test1.pcap"
     size_kb:i=3000
   }
   eth1 {
     flush_to_file="/D/test2.pcap"
     size_kb:i=3000
   }
   tun0 {
      flush_to_file="/D/tun0.pcap"
      size_kb:i=3000
    }
    tun1 {
      flush_to_file="/D/tun1.pcap"
      size_kb:i=3000
    }
  ip_rkl {
      flush_to_file="/D/rkl.pcap"
      size_kb:i=1000
    }
  }
```

Для каждого выводимого файла трафика указан размер файла в килобайтах.

18. 4. Дампы

Дамп памяти позволяет записывать критические ошибки в работе ФПСУ без необходимости приостанавливать его работу. В случае если дамп сформирован, администратор имеет возможность загрузить дамп памяти в виде архива на внешний носитель для дальнейшего анализа.

Дамп памяти ФПСУ сохраняется автоматически, когда ФПСУ перезагружается из-за критической ошибки.

В главном меню по команде «Сервисные функции → Скопировать дампы на внешний носитель» дампы памяти могут быть выгружены на внешний носитель.

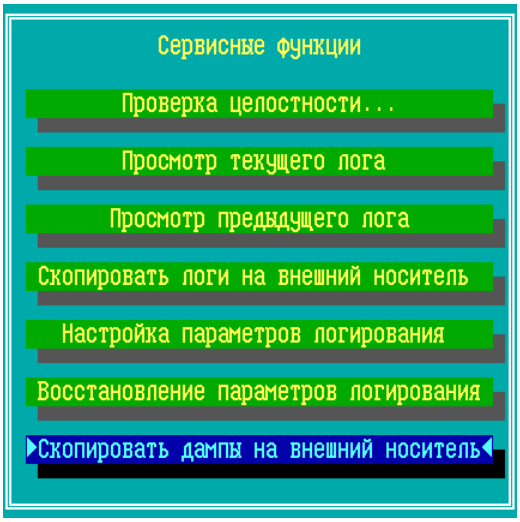


Рисунок 548 - Меню «Сервисные функции»

При копировании на внешний носитель переносятся все найденные в памяти ФПСУ дампы, после завершения операции дампы удаляются из внутренней памяти ФПСУ.

Операция доступна администраторам класса *Администратор* и выше (см. пункт «Разграничение доступа и пользователи», Таблица 3).



Рисунок 549 - Подтверждение полномочий и ввод пароля ТМ

19. Удаление программного обеспечения ФПСУ

19. 1. Удаление СКЗИ

Локальному администратору ФПСУ классов *«Администратор»* или *«Главный администратор»* доступна возможность форматирования внутреннего накопителя ФПСУ с удалением операционной системы ФПСУ и хранящихся файлов, в том числе ключевой информации СКЗИ, программных и служебных модулей СКЗИ, и программного обеспечения BIOS/UEFI.

Для запуска процедуры форматирования внутреннего накопителя:

1. Выполните команду «Настройка системы» главного меню:

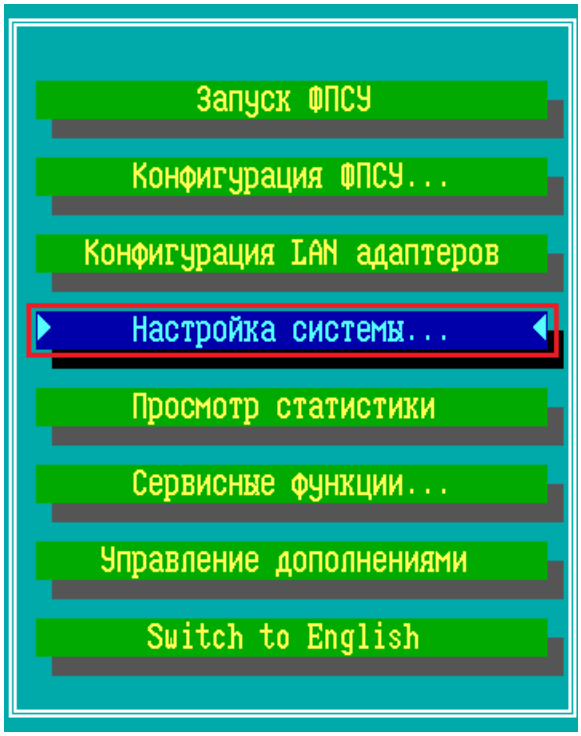


Рисунок 550 - Главное меню ФПСУ

2. Выполните команду «Настройки СКЗИ» меню настройки системы:



Рисунок 551 - Меню настройки системы ФПСУ

3. Выполните команду «Удаление СКЗИ» меню настройки СКЗИ.

ВНИМАНИЕ! Если при выполнении команды «Удаление СКЗИ» к ФПСУ подключен USB ТМ-идентификатор ТМ-Key с правами *«Администратор»* или *«Главный администратор»,* то последующего окна с подтверждением полномочий не будет выведено на экран. Процедура удаления СКЗИ начнется сразу после выполнения команды «Удаление СКЗИ»!



Рисунок 552 - Запуск процедуры удаления СКЗИ

Если USB TM-идентификатор TM-Key не был подключен к ФПСУ, появится окно с предложением подтвердить полномочия администратора или Главного администратора (права классов *«Администратор»* или *«Главный администратор»,* см. пункт «Разграничение доступа и пользователи», Таблица 3).

ВНИМАНИЕ! Сразу после приложения к TM-считывателю ФПСУ TM-идентификатора, подтверждающего права классов *«Администратор»* или *«Главный администратор»*, будет запущен необратимый процесс форматирования внутреннего накопителя!

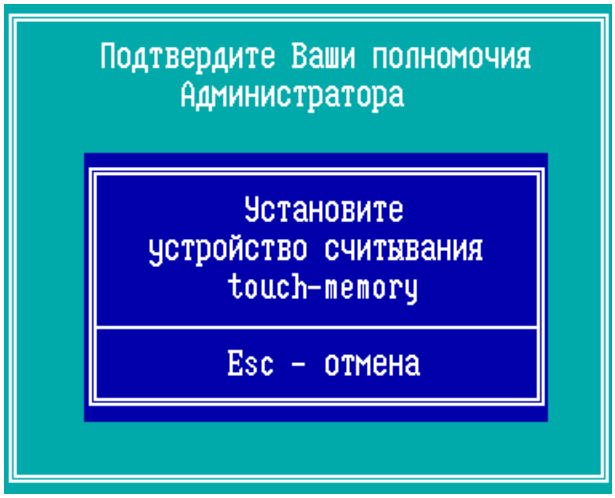


Рисунок 553 - Подтвердите полномочия для удаления СКЗИ

После подтверждения прав администратора, ФПСУ начнет форматирование

внутреннего накопителя, после чего перезагрузит операционную систему. Удаление операционной системы ФПСУ и хранящихся на внутреннем накопителе файлов, в том числе ключевой информации СКЗИ, программных и служебных модулей СКЗИ, и программного обеспечения BIOS/UEFI, завершено.

19. 2. Удаление ПО с помощью USB-носителя со средством восстановления

Для полного удаления программного обеспечения ФПСУ с его ПЗУ, следует запустить процедуру повторной установки программного обеспечения (см. пункт «Установка ПО ФПСУ с установочного носителя»). Для успешного удаления программного обеспечения потребуются:

- ФПСУ;
- инсталляционный комплект программного обеспечения ФПСУ, состоящий из USB-носителя с дистрибутивом.

Порядок действий при удалении программного обеспечения с ПЗУ ФПСУ следующий:

1. Подключите USB-носитель с дистрибутивом программного обеспечения к ФПСУ.
2. При включении ФПСУ следует отменить загрузку подсистемы контроля ACCESS BIOS (названия могут меняться, например на Access Bios/PnP или FPSU Access BIOS), запрещающей загружать операционную систему иначе как с защищенной внутренней памяти, и выбрать загрузку с USB. Это можно сделать при выборе Boot Options (обычно при нажатии F10) после включения ФПСУ, или напрямую зайдя в BIOS и установив в Boot Options загрузку **USB2.0** вместо **Access BIOS**.

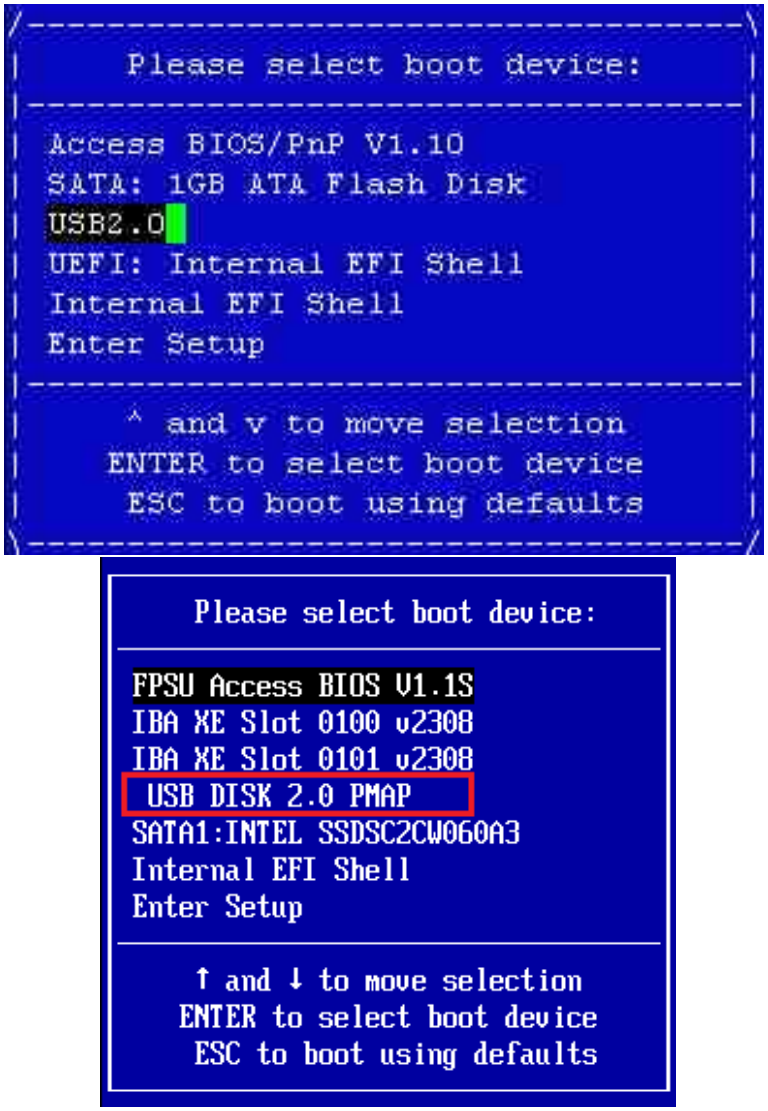


Рисунок 554 - Выбор загрузки с USB

3. Загруженная с инсталляционного USB-носителя программа начнет первый этап установки с проверки ранее установленного программного обеспечения ФПСУ. Если система была ранее установлена на комплекс, будет выдано следующее сообщение:

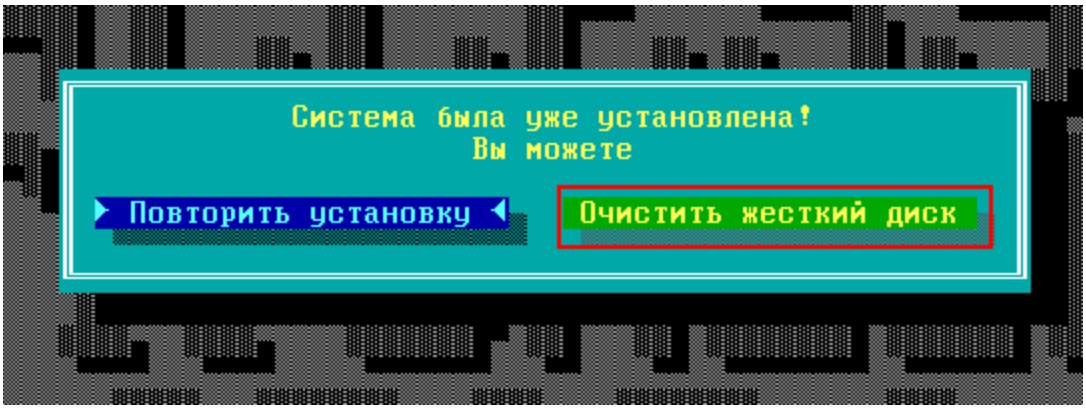


Рисунок 555 - Операционная система ФПСУ уже установлена

4. Выберите команду *<Очистить жесткий диск>* и подтвердите выполнение операции.

После выполнения операции «Очистить жесткий диск», питание ФПСУ можно выключать. Операционная система, ключевая информация СКЗИ, программные и служебные модули СКЗИ полностью удалены с ПЗУ ФПСУ.

Уничтожение программных модулей СКЗИ на дистрибутивном USB-носителе осуществляется форматированием носителя штатными средствами операционной системы. В случае невозможности форматирования, носитель следует разрушить, с уничтожением микросхем, с помощью кусачек или других инструментов .

19. 3. Удаление экземпляра СКЗИ с USB-носителя в ОС Windows

Уничтожение программных модулей СКЗИ на дистрибутивном USB-носителе осуществляется форматированием носителя штатными средствами операционной системы.

Далее приведен пример удаления разделов и форматирования дистрибутивного USB-носителя средствами операционной системы Windows 10.

При подключении к компьютеру с операционной системой Windows 10 инсталляционный USB-носитель отображается как три отдельных диска, буквы дискам присваиваются динамически при подключении.

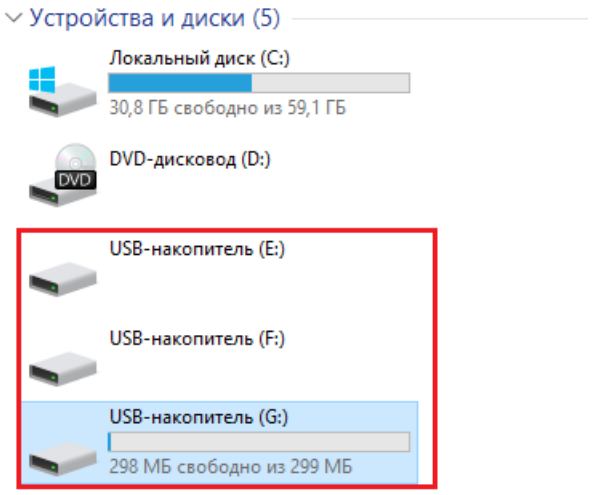


Рисунок 556 - Отображение USB-носителя

Сразу же отображается запрос на форматирование каждого из этих дисков:

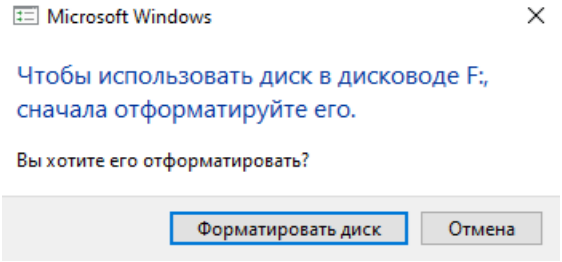


Рисунок 557 - Запрос на форматирование USB-носителя

Закройте сообщение для каждого диска.

Необходимо убедиться, что съемный диск является дистрибутивным USB-носителем, на не пустом съемном диске откройте файл install.txt и проверьте инсталляционную информацию.

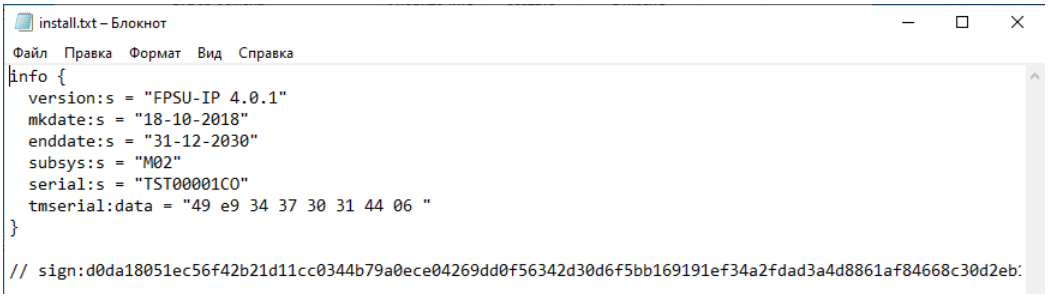


Рисунок 558 - Информация о USB-носителе

Откройте окно Windows «Управление компьютером → Управление дисками».

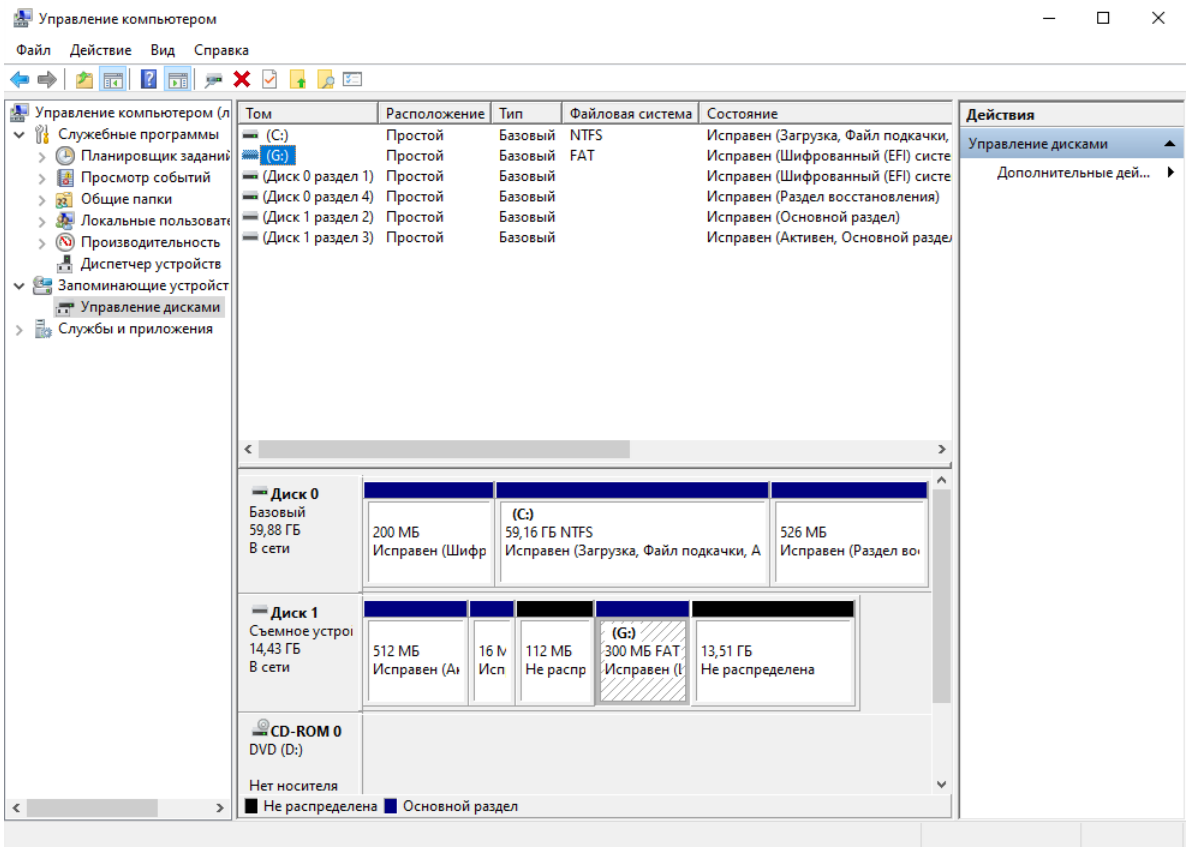


Рисунок 559 - Подключенный USB-носитель

У подключенного съемного USB-носителя необходимо удалить все разделы.

Выделите раздел (диск 1 раздел 3 - Основной раздел съемного устройства) и нажмите команду «Удалить» (красный крест на панели команд). В отобразившемся сообщении необходимо подтвердить действие.

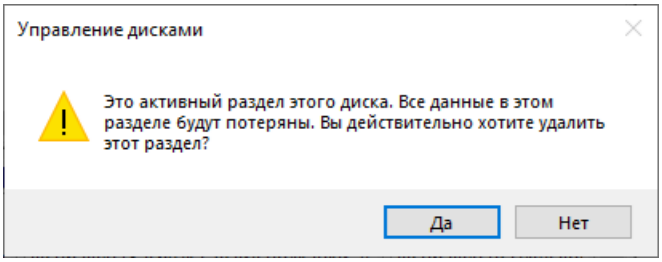


Рисунок 560 - Удаление раздела

Для следующего раздела необходимо также подтвердить удаление.

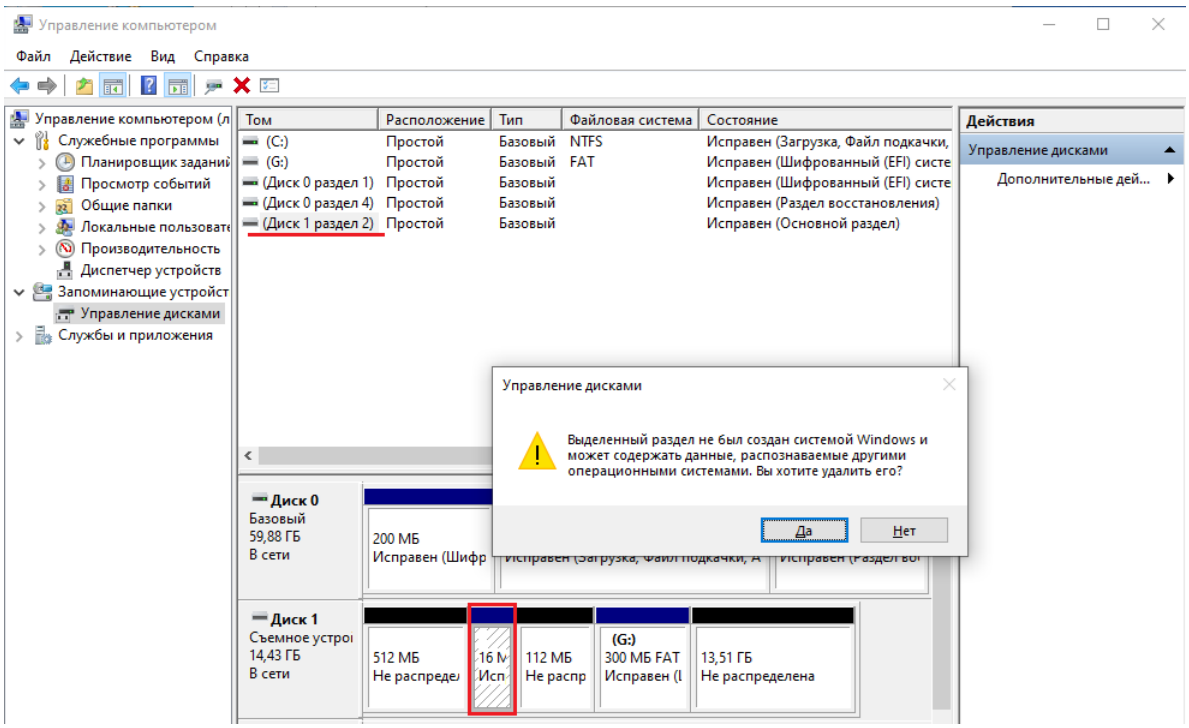


Рисунок 561 - Удаление раздела

Для раздела отмеченного буквой необходимо также подтвердить удаление.

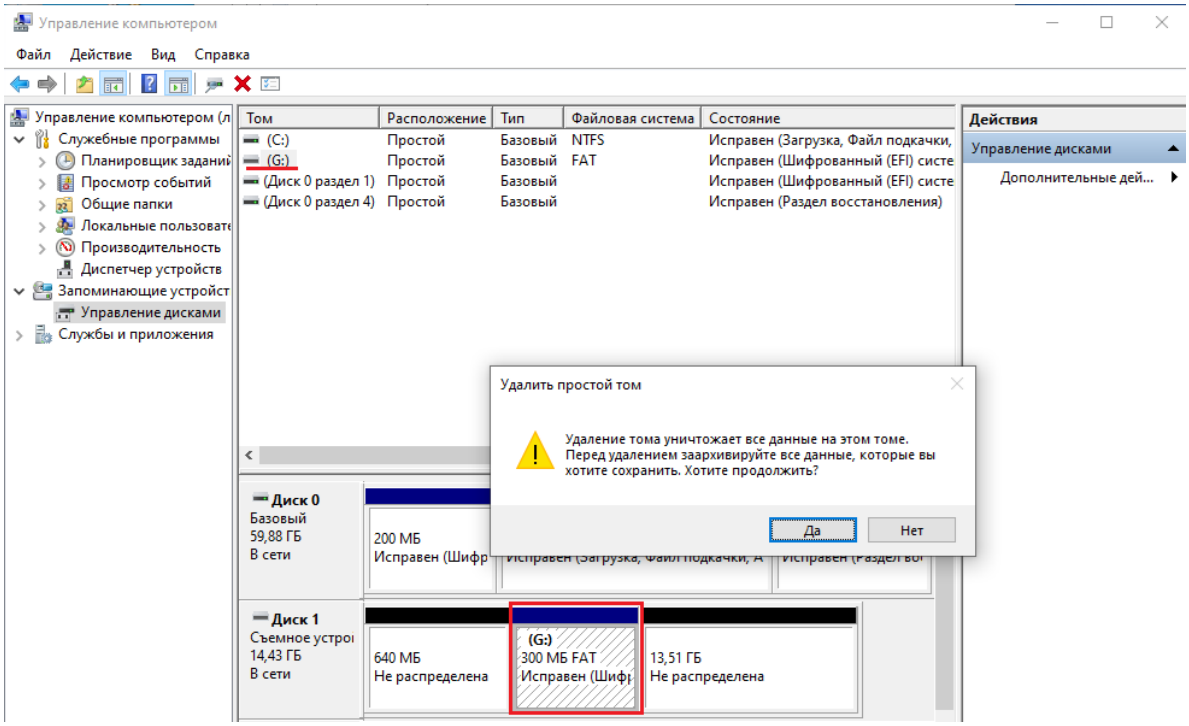


Рисунок 562 - Удаление раздела

USB-носитель примет вид неразмеченного диска, он не будет отображаться в списке томов, создайте простой том на этом диске, выбрав команду в контекстном меню.

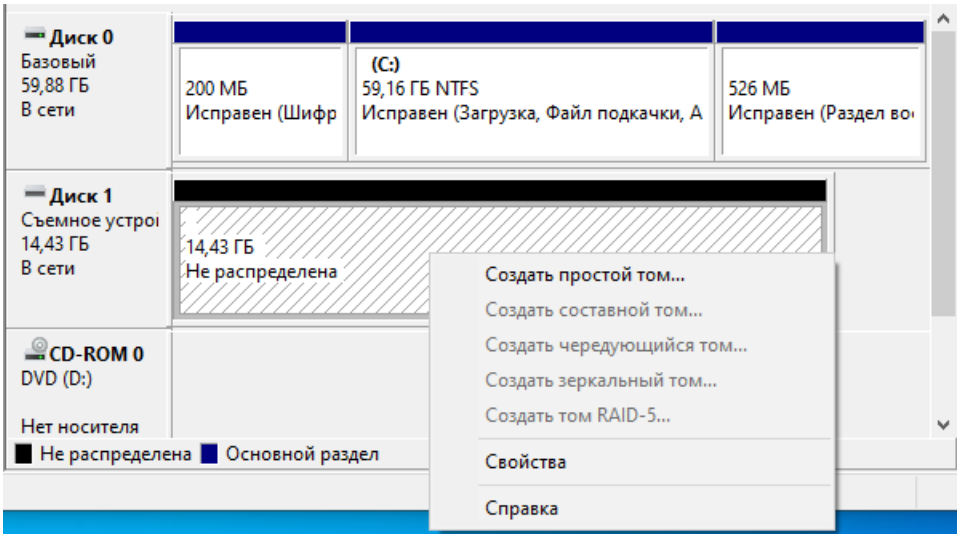


Рисунок 563 - USB-носитель

Откроется окно мастера по созданию простого тома.

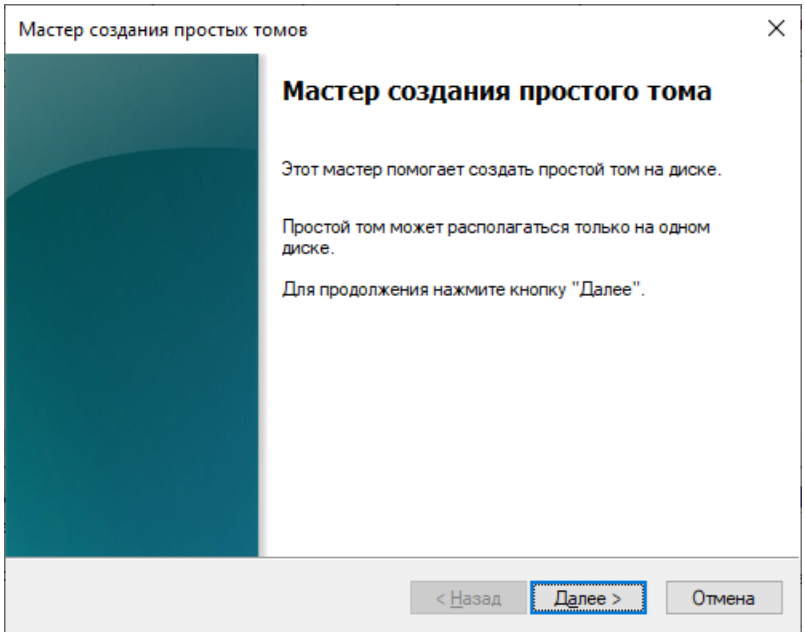


Рисунок 564 - Создание простого тома

Укажите размер тома или оставьте параметры по умолчанию.

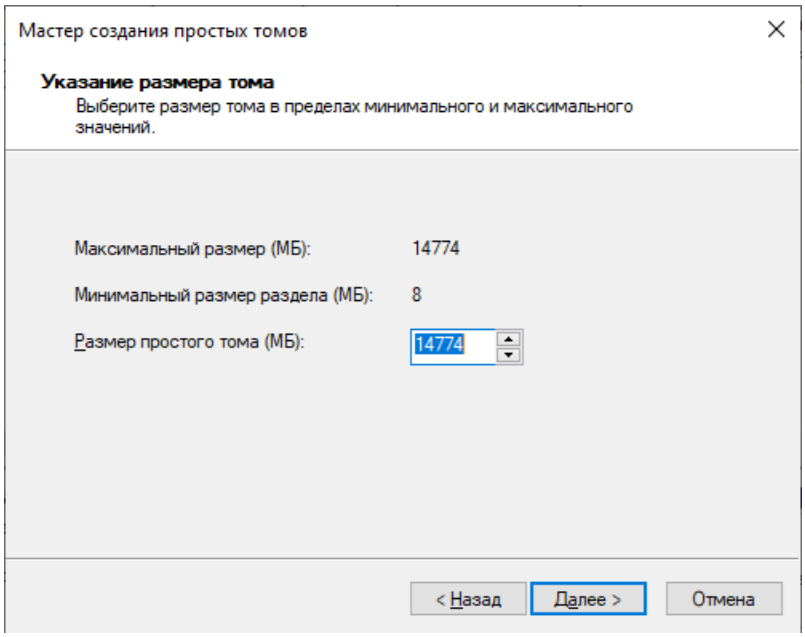


Рисунок 565 - Размер создаваемого тома

Назначьте букву диску или оставьте по умолчанию, есть возможность указать путь к диску.

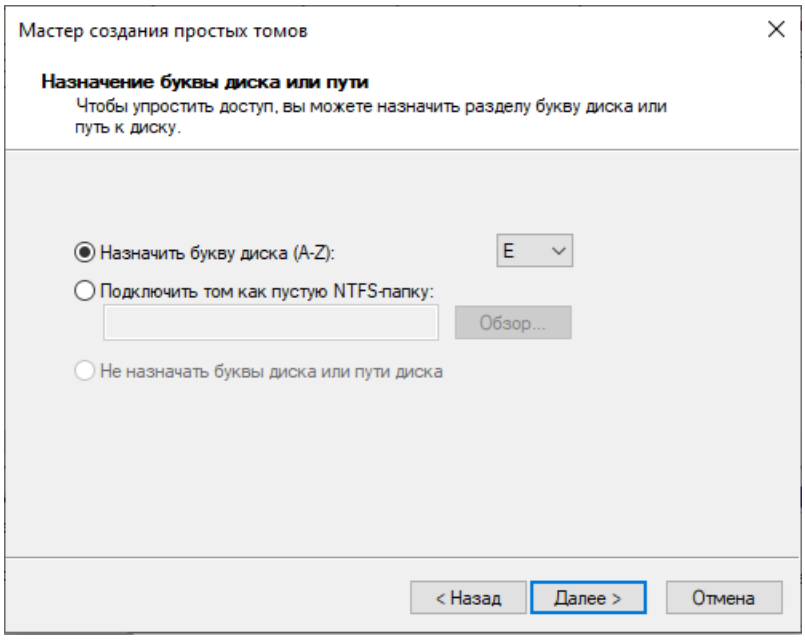


Рисунок 566 - Буква диска

Отметьте параметры форматирования файловой системы.

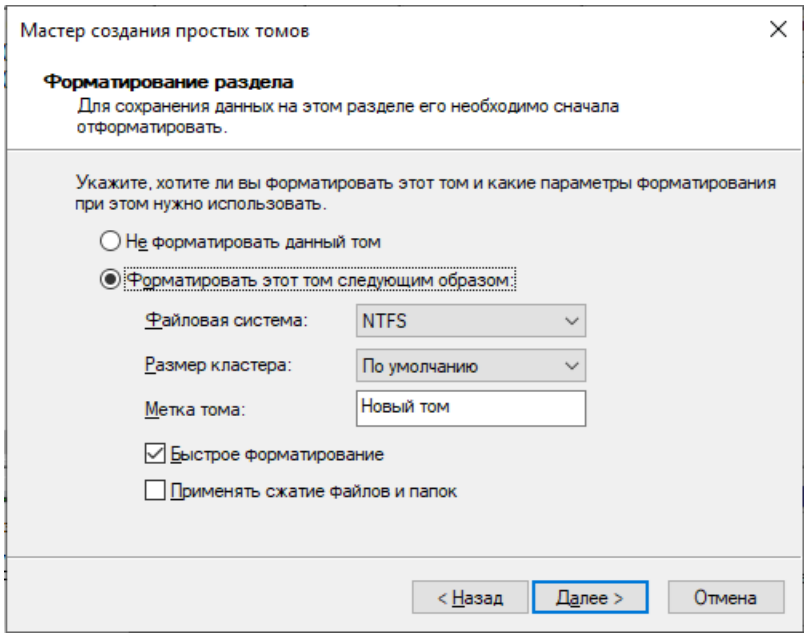


Рисунок 567 - Выбор файловой системы

На экран будет выдано окно завершения работы мастера.

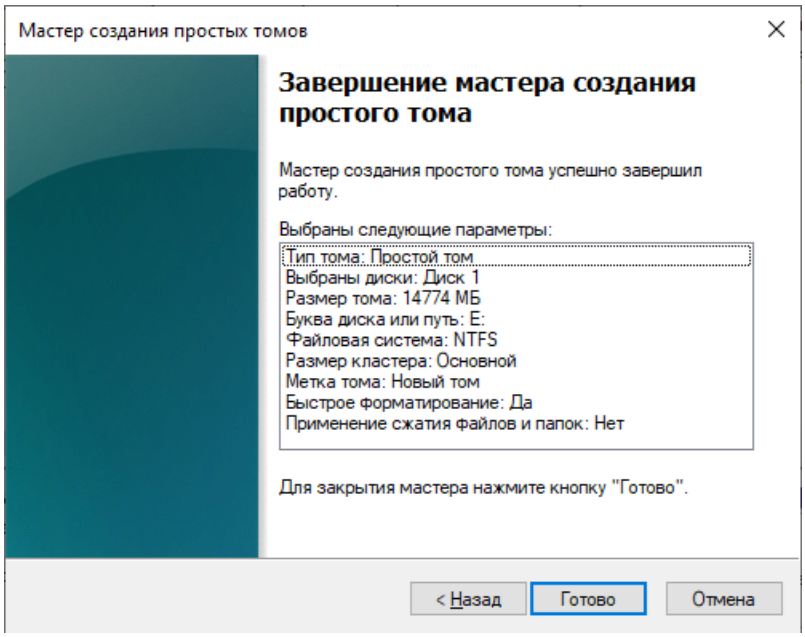


Рисунок 568 - Завершение работы мастера

USB-носитель отображается в списке томов и размечен как Основной раздел.

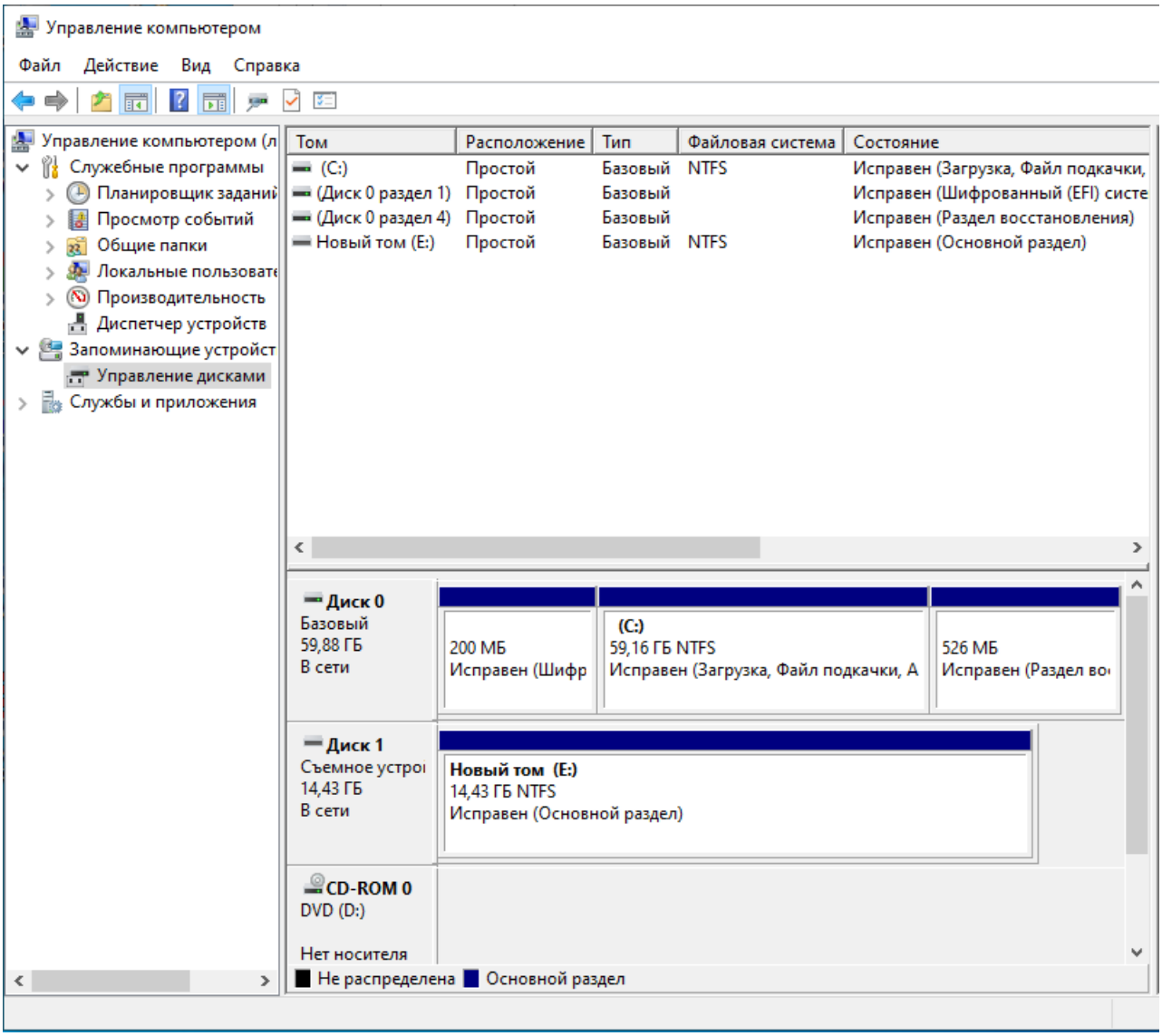


Рисунок 569 - USB-носитель размечен как Основной раздел

Вся информация об экземпляре СКЗИ была удалена с USB-носителя при удалении разделов, USB-носитель отформатирован при создании основного раздела на нем.

19. 4. Удаление экземпляра СКЗИ с USB-носителя в ОС Ubuntu

Уничтожение программных модулей СКЗИ на дистрибутивном USB-носителе осуществляется форматированием носителя штатными средствами операционной системы.

Далее приведен пример удаления разделов и форматирования дистрибутивного USB-носителя средствами операционной системы 22.04.5 LTS.

Для уничтожение программных модулей СКЗИ с дистрибутивного USB-носителя необходимо подключить к компьютеру дистрибутивный USB-носитель ФПСУ. Убедитесь, что к компьютеру подключено только это съемное устройство.

Далее следует открыть раздел «Диски» можно из меню Dash, задав в строке поиска «disk».

В открывшемся окне отобразится USB-носитель с размеченными разделами.

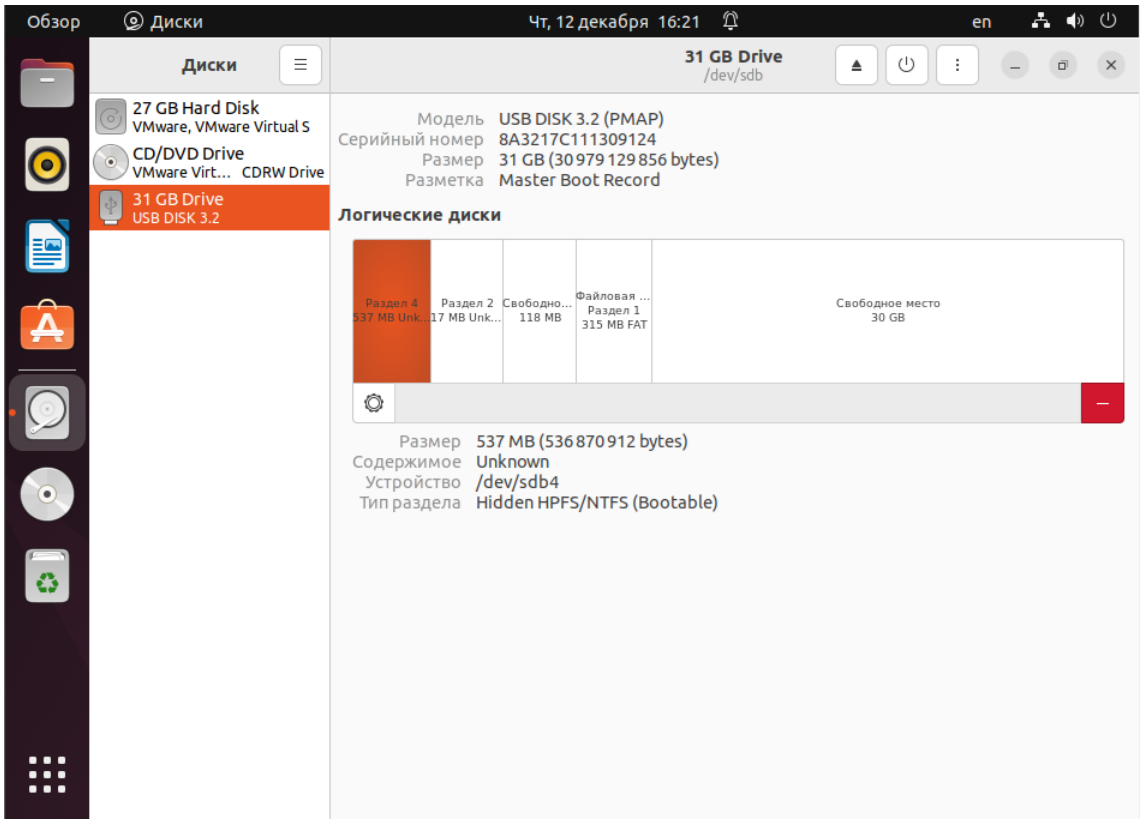


Рисунок 570 - Подключенный USB-носитель

Требуется удалить все разделы USB-носителя.

Выделите раздел (раздел 4) и нажмите команду «Удалить выбранный раздел» (красная кнопка в правом углу разметки диска). В отобразившемся сообщении необходимо подтвердить действие.

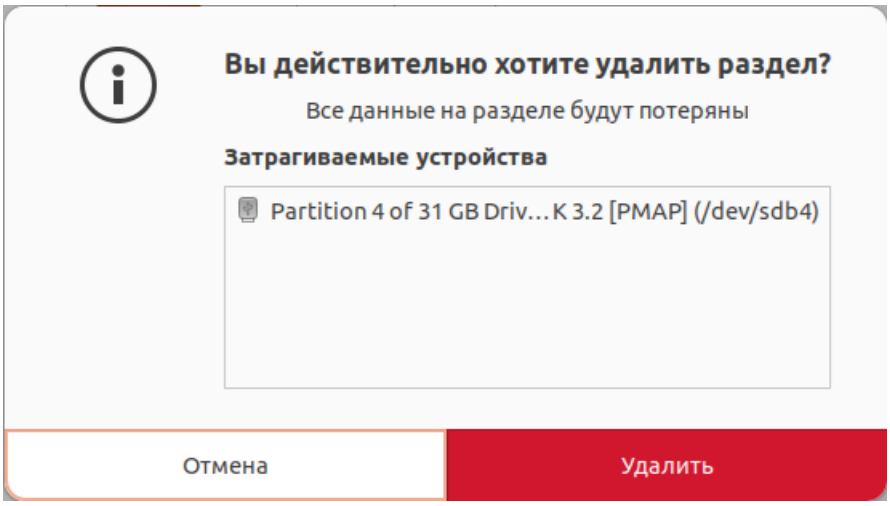


Рисунок 571 - Удаление 4 раздела

Для следующего раздела необходимо также подтвердить удаление.

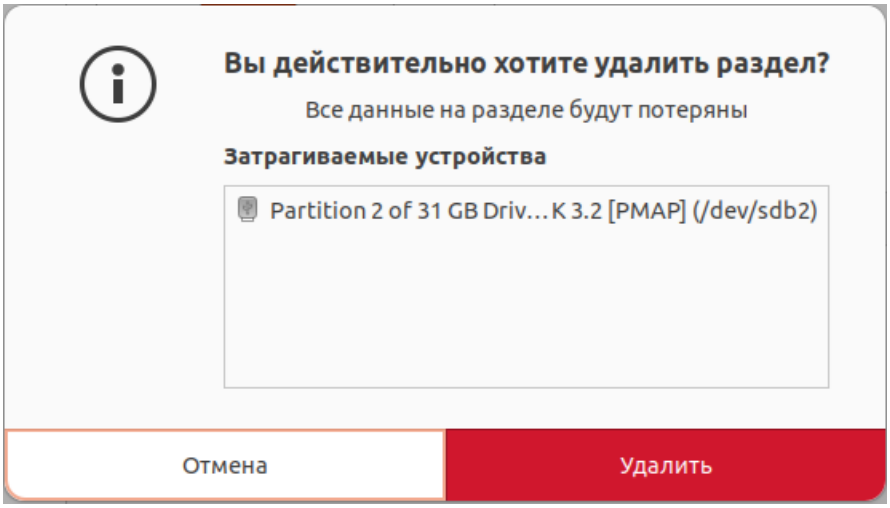


Рисунок 572 - Удаление 2 раздела

Для последнего, третьего раздела необходимо также подтвердить удаление.

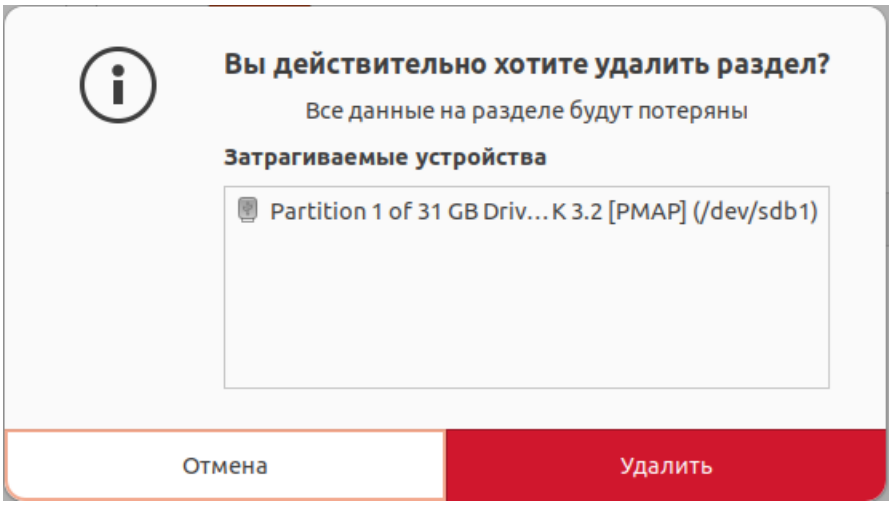


Рисунок 573 - Удаление 1 раздела

USB-носитель примет вид неразмеченного диска.

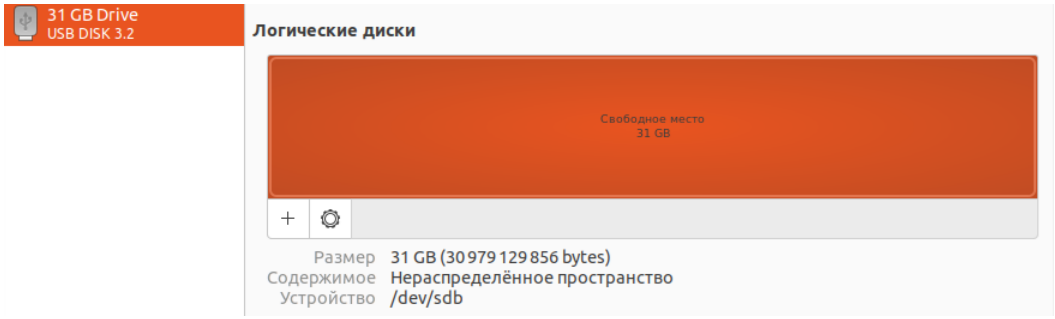


Рисунок 574 - USB-носитель

Далее необходимо создать раздел на неразмеченном диске и форматировать логический диск.

Создайте раздел на этом диске по кнопке «+» в левом углу разметки диска. Откроется окно по созданию раздела, нажмите «Далее» для продолжения.

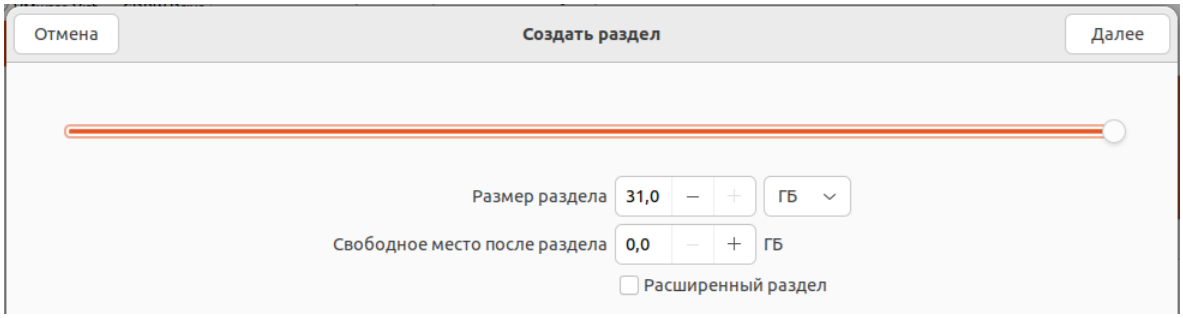


Рисунок 575 - Создание раздела

Отметьте параметры форматирования файловой системы или оставьте настройки по умолчанию, создайте раздел, нажав на кнопку «Создать».

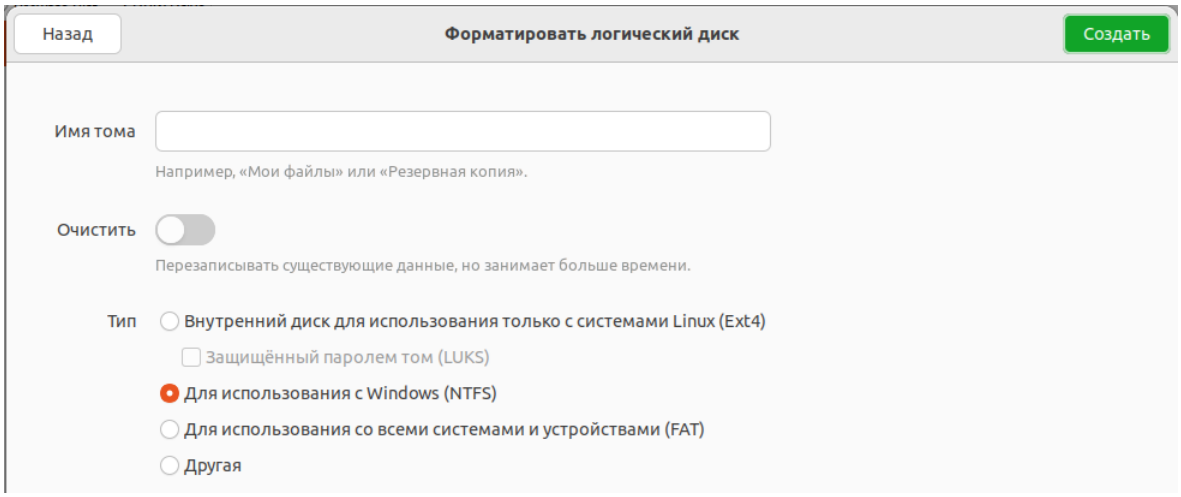


Рисунок 576 - Настройки форматирования

USB-носитель размечен одним разделом.

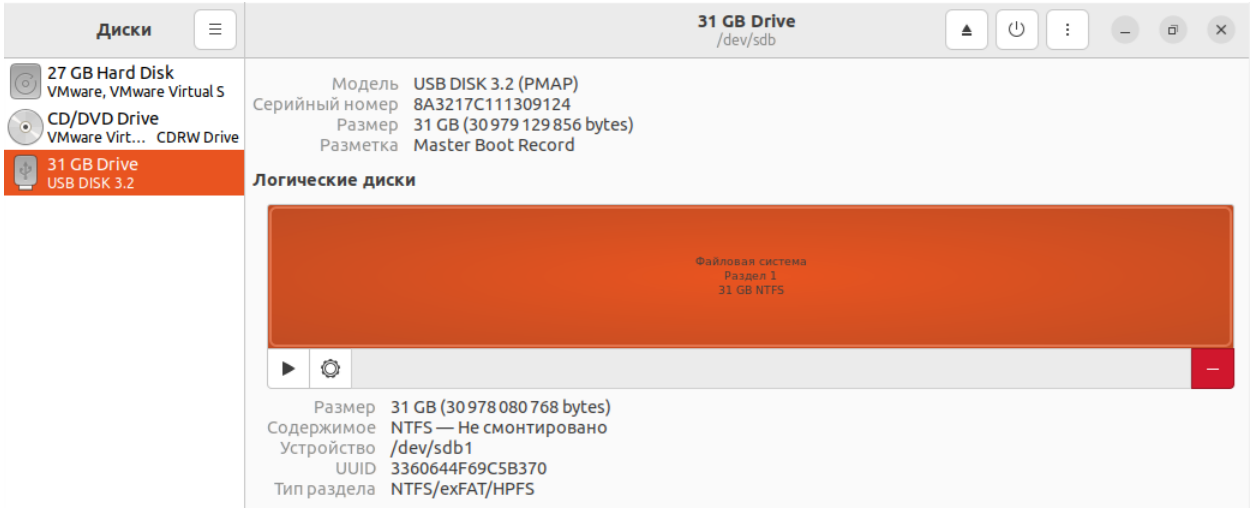


Рисунок 577 - USB-носитель размечен одним разделом

Вся информация об экземпляре СКЗИ была удалена с USB-носителя при удалении разделов, USB-носитель отформатирован при создании основного раздела на нем.