ООО "АМИКОН"

УТВЕРЖДЕН

ПЕРС.26.20.40.140.003РЭ-ЛУ

Программно-аппаратный комплекс

"ФПСУ-IP 3.X"

Руководство по эксплуатации

ПЕРС.26.20.40.140.003РЭ

Листов 332

2021

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением программно-аппаратных комплексов "ФПСУ-IP 3.X" (версии ПО 3.20.1, 3.20.2, 3.20.8). В документе содержатся общие сведения о программно-аппаратном комплексе "ФПСУ-IP 3.X", приведен перечень необходимых организационно-технических мер и дано описание последовательности действий при настройке параметров функционирования комплекса в процессе эксплуатации и в аварийных ситуациях.

Одним из наиболее существенных факторов, обеспечивающих нормальную работу сети под защитой программно-аппаратного комплекса "ФПСУ-IP 3.X" и требуемый уровень безопасности, является отсутствие ошибок при конфигурировании комплекса. Поэтому конфигурирование программно-аппаратного комплекса "ФПСУ-IP 3.X" должно производиться квалифицированным специалистом, хорошо знакомым с топологией сети, имеющим опыт работы с различным сетевым оборудованием и его программным обеспечением, а также внимательно изучившим принципы, методику и конкретные процедуры конфигурирования, изложенные в соответствующих разделах данного документа. Рекомендуется обратить особое внимание на примеры конфигурирования программно-аппаратного комплекса "ФПСУ-IP 3.X" для различных сетевых топологий, представленные в разделе "Примеры настройки ФПСУ-IP".

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

Отзывы и предложения по документации просьба высылать на электронную почту.

Контакты:

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

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

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

Электронная почта: info@amicon.ru

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

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

Рисунок 280 - Окно общих параметров ФПСУ-IP

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

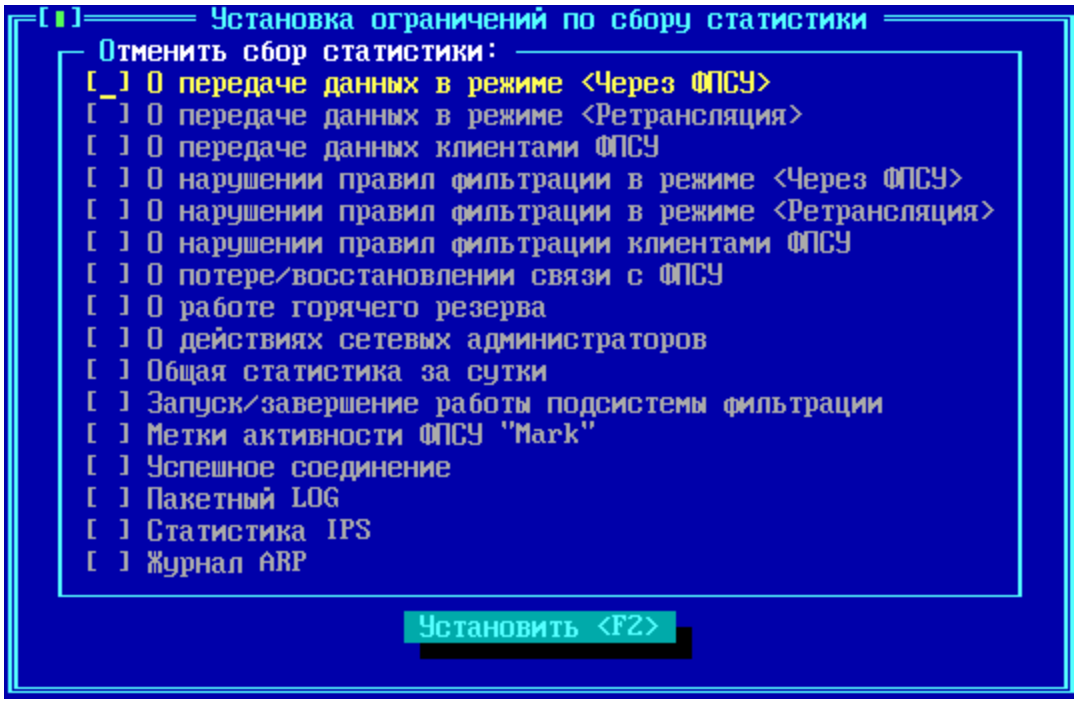

Рисунок 281 - Окно ограничения сбора статистики

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

14. Восстановление работы ФПСУ-IP после сбоев

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

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

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

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

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

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

администратор может восстановить конфигурацию ФПСУ-IP с внешнего носителя, после чего заново установить ключи парно-выборочной связи и общесистемные ключи клиентов, а также настроить сетевые адаптеры. Для осуществления указанных действий необходимы права администратора или главного администратора.

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

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

15. Примеры настройки ФПСУ-IP

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

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

Основные принципы конфигурирования маршрутизации на ФПСУ-IP:

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

пакетов (переключатель "Только Broadcast" выключить нельзя).

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

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

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

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

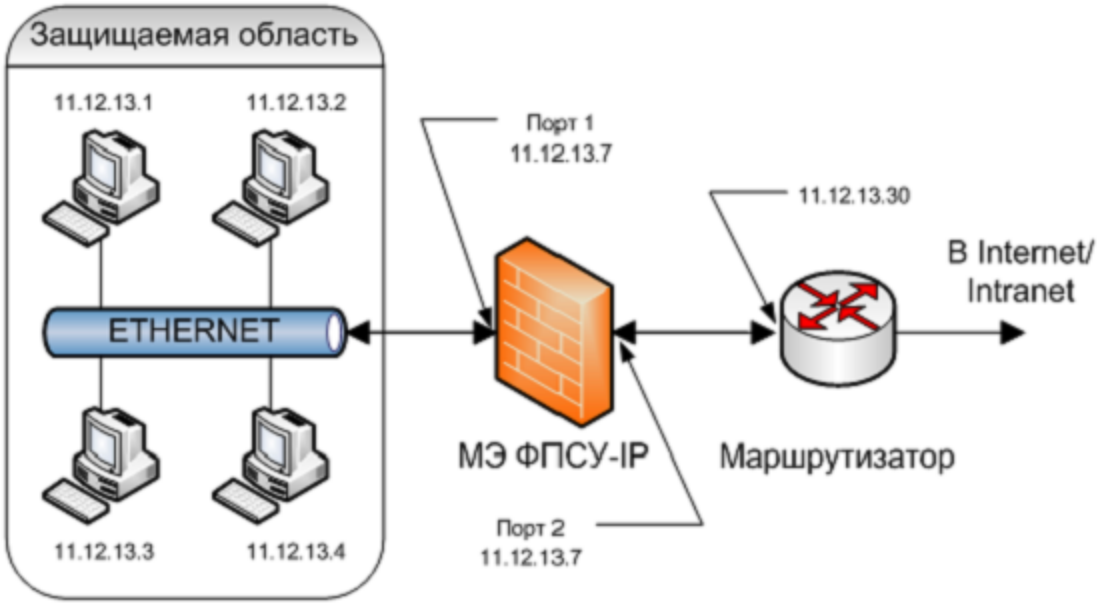

Рисунок 282 - Применение ФПСУ-IP для защиты оконечной области

Конфигурация МЭ должна содержать следующие установки:

==========

Порт 1:

Номер 1

Адрес 11.12.13.7

Маска 255.255.255.0 (24 разряда)

ФПСУ не определены

Маршрутизаторы не определены

Абоненты:

Подсеть; Адрес 11.12.13.0; Маска 255.255.255.0;

режим работы ретрансляция;

режим партнера этого порта — выключен;

режим партнера другого порта - включен только в ретрансляции;

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

Хост; 11.12.13.1;

режим работы ретрансляция;

режим партнера этого порта - выключен;

режим партнера другого порта - включен только в ретрансляции;

переключатель "Отвечать на Ping" - на усмотрение администратора;

переключатель "Работа разрешена" включен.

Порт 2:

Номер 2;

Адрес 11.12.13.7;

Маска 255.255.255.0 (24 разряда;

ФПСУ не определены;

Маршрутизаторы 11.12.13.30;

```
      протоколы маршрутизации выключены;

      переключатель "Отвечать на Ping" - на усмотрение администратора.

Абоненты: Любой хост

режим работы ретрансляция;

через маршрутизатор 11.12.13.30;

      переключатель "Работа разрешена" включен.

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

При необходимости администратор может регламентировать доступ к хостам своей подсети только по определенным протоколам и/или TCP/UDP-портам (через включение дополнительных правил межсетевого экрана, см. раздел "Правила трафика межсетевого экрана", в данном примере их настройка не рассматривается).

Остальные параметры конфигурации (например, обработка IP-опций или сокрытие фильтрующих свойств комплекса) описываются на усмотрение администратора.

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

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

Такая организация защищаемой подсети приведет к следующей логике конфигурирования:

На порту 1 ФПСУ-IP должны быть описаны две различные IP-подсети и для каждой подсети (или ее отдельных абонентов) должна быть разрешена работа с партнером своего порта в режиме "ретрансляции". Кроме того, все хосты защищаемой области должны быть сконфигурированы таким образом, чтобы в качестве маршрутизатора по умолчанию у них был указан маршрутизатор с адресом 11.12.13.30 или IP-адрес 1-го порта ФПСУ-IP.

На работу подсети наложены следующие ограничения:

- хост с IP-адресом 11.12.13.1 является администратором маршрутизатора, обмен IP-пакетами с подсетью 2 ему запрещен; кроме того, он должен иметь

круглосуточный доступ в сеть Internet/Intranet;

- остальные хосты подсети 1 и хосты подсети 2 имеют доступ друг к другу и не должны взаимодействовать с Internet/Intranet.

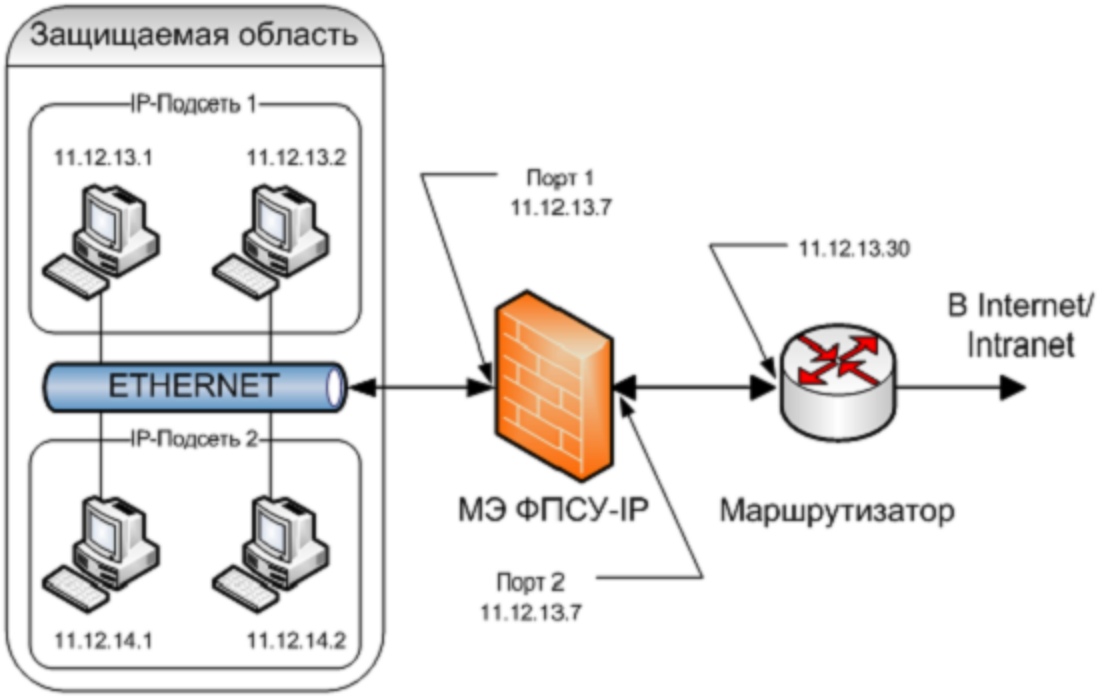

Рисунок 283 - Защита двух подсетей

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

- со стороны внутреннего порта комплекса (порта 1) существуют две отдельные IP подсети, маршрутизаторы и ФПСУ-IP отсутствуют;
- со стороны порта 2 абоненты не определены, доступ к ним будет осуществляться через маршрутизатор (по IP-адресу связанного с ФПСУ-IP порта), а другие ФПСУ-IP отсутствуют;
- обмен администратора защищаемой области с абонентами общедоступной сети передачи данных может производиться только в режиме ретрансляции, сжатие и криптозащита не применяются;
- работа с ключевыми данными при такой топологии не требуется;
- абонентам подсетей 1 и 2 работа разрешается только с абонентами со стороны своего порта, причем администратор маршрутизатора не должен участвовать в таких

обменах;

- абонент с IP-адресом 11.12.13.1 должен обмениваться пакетами с абонентами со стороны порта 2 и должен быть допущен к управлению маршрутизатором.

Конфигурация ФПСУ-IP должна содержать следующие установки:

==========

Порт 1:
Номер 1,
Адрес 11.12.13.7,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены,
Абоненты:
Подсеть; 11.12.13.0; 255.255.255.0 (24 разряда),
режим работы ретрансляция;
режим партнера этого порта - включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Подсеть; 11.12.14.0; 255.255.255.0 (24 разряда),
режим работы ретрансляция;
режим партнера этого порта - включен только в ретрансляции;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Хост; 11.12.13.1,
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Порт 2:
Номер 2;
Адрес 11.12.13.7;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы
11.12.13.30,
протоколы маршрутизации выключены;
переключатель "Отвечать на Ping" - на усмотрение администратора.

```
Абоненты:
Любой хост;
режим работы ретрансляция;
через маршрутизатор 11.12.13.30;
переключатель "Работа разрешена" включен.
```

==========

Для выполнения дальнейших настроек рекомендуется ознакомиться с разделом "Правила трафика межсетевого экрана".

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

1. правило, разрешающее взаимодействие абонента 11.12.13.1 (источник) с маршрутизатором 11.12.13.30 (назначение);
2. правило, разрешающее взаимодействие абонента 11.12.13.1 (источник), и абонента Любой хост 2 порта ФПСУ (назначение);
3. правило, разрешающее взаимодействие абонентов всех абонентов подсетей 1 и 2 (источник), и абонентов подсетей 1 и 2 (назначение);
4. правило, запрещающее взаимодействия абонента 11.12.13.1 (и в качестве источника, и в качестве назначения), с абонентами подсети 2 (источник и назначение). Причем это правило должно иметь приоритет выше, чем правило из пункта 3.

Дополнительно, администратор может регламентировать доступ по времени (через выбор из ранее созданных интервалов времени в выпадающем списке "Время работы" правила доступа, см. пункт "Интервалы времени").

Остальные параметры конфигурации (например, обработка IP-опций или сокрытие фильтрующих свойств комплекса) описываются на усмотрение администратора.

В данном примере функциональное отделение абонента 11.12.13.1 от IP-подсети 2 (запрещение обменов) производится двумя независимыми друг от друга ограничениями:

1. по настройке абонента 11.12.13.1 в разделе конфигурации "Порты ФПСУ", по признаку "Режим партнера – Данного порта" (режим "Ретрансляция" выключен);
2. Правилом 4. межсетевого экрана из списка выше.

Несмотря на то, что хостам со стороны порта 1 (исключая администратора) запрещено выходить в общедоступную сеть передачи данных, режим работы с партнером другого порта (ретрансляция) для них включен. Это объясняется тем, что данный режим отключить нельзя, поскольку отключение обоих режимов работы с партнером другого порта (по недосмотру или ошибке администратора) может привести к тому, что обмен пакетами через ФПСУ-IP

окажется невозможен и абоненты защищаемой области окажутся отрезанными от сети. Запрещение работы этим хостам будет обеспечиваться тем, что единственный абонент, описанный со стороны порта 2 через запись "Любой хост", включен в только в одно правило доступа, разрешающее взаимодействие лишь с абонентом 11.12.13.1.

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

Представим теперь, что до установки ФПСУ-IP существовала одна IP-подсеть с адресом 11.12.13.0 и маской 255.255.255.0, которую необходимо разделить физически на два независимых фрагмента (например, по функциональному признаку) без переконфигурирования программного обеспечения хостов, причем требуется регламентировать обмены данными между хостами независимых фрагментов. Отметим, что в предыдущем примере ("Защита локальной сети, состоящей из двух IP-подсетей") разделение абонентов на две подсети было логическим, то есть для его осуществления была необходима особая конфигурация 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.

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

Помимо физического разделения на работу двух подсетей накладываются следующие требования:

- хосты области 1, исключая хост 11.12.13.1, и все хосты области 2 должны иметь полный доступ друг к другу, в том числе должна обеспечиваться возможность поиска и подключения сетевых дисков;
- хост 11.12.13.1 не должен иметь доступа в область 2.

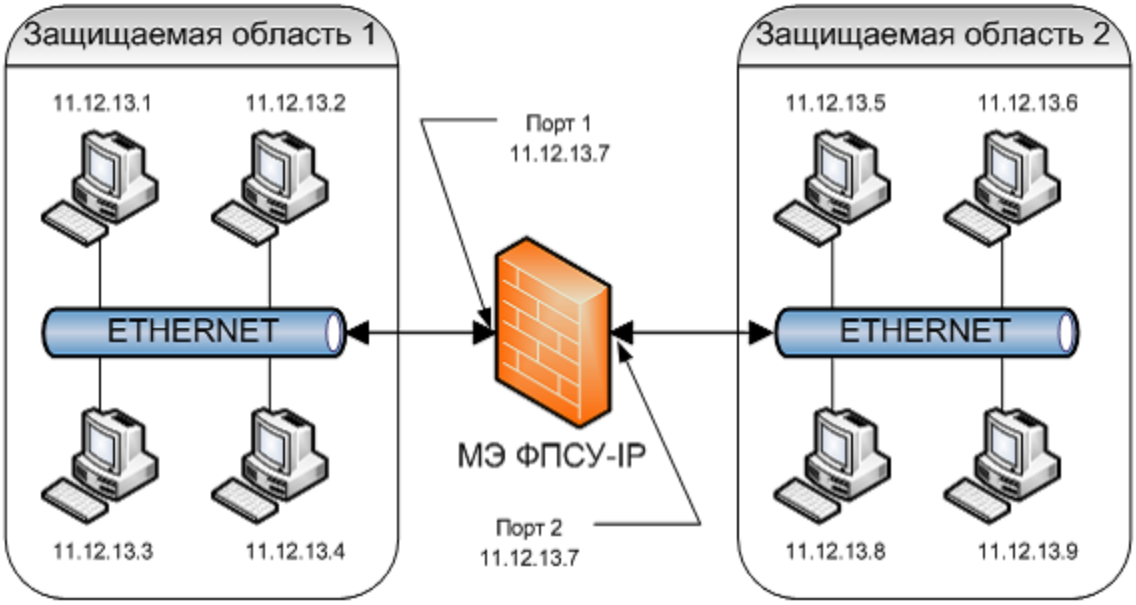

Рисунок 284 - Разбиение сети на фрагменты

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

- со стороны портов 1 и 2 ФПСУ-IP существует одна и та же IP-подсеть, маршрутизаторы и другие ФПСУ-IP отсутствуют;
- обмен хостов через комплекс может производиться только в режиме ретрансляции, сжатие и криптозащита невозможны;
- работа с ключевыми данными при такой топологии не производится;
- абоненту с IP-адресом 11.12.13.1 должен быть запрещен обмен пакетами с абонентами со стороны порта 2;
- для обеспечения поиска и подключения сетевых дисков необходимо разрешить передачу через ФПСУ-IP широковещательных пакетов.

Конфигурация ФПСУ-IP должна содержать следующие установки:

Порт 1:
Номер 1,
Адрес 11.12.13.7,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены,
Абоненты:
Подсеть; 11.12.13.0; 255.255.255.0 (24 разряда),
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;

переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Хост; 11.12.13.1;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - выключен;
переключатель "Работа разрешена" выключен.

Порт 2:

Номер 2,
Адрес 11.12.13.7,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены,
Абоненты:
Подсеть 11.12.13.0; 255.255.255.0 (24 разряда),
режим работы ретрансляция;
переключатель "Только Broadcast" включен;
переключатель "Работа разрешена" включен.
Хост; 11.12.13.5,
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Хост; 11.12.13.6,
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Хост; 11.12.13.8,
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Хост; 11.12.13.9;
режим работы ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только в ретрансляции;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

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

Для абонента 11.12.13.1 запрещение работы с абонентами области 2 осуществляется через выключение переключателя "Работа разрешена".

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

Рассмотрим ситуацию, когда сеть организации представляет из себя отдельные локальные IP-подсети, разделенные территориально и связанные через участки WAN-сети общего пользования. В таком случае, для обеспечения защищенного взаимодействия локальных подсетей, необходимо на выходе каждой из них установить ФПСУ-IP (со стороны внутреннего порта пограничного маршрутизатора) и организовать между ФПСУ-IP VPN-туннели через WAN-сеть общего доступа, по которым данные абонентов будут передаваться с использованием всех механизмов защиты, включая аутентификацию и, возможно, сжатие.

Предположим, что организация использует следующие IP-адреса:

- защищаемая область A - 11.12.1.0, маска 255.255.255.0 (24 бита);
- защищаемая область B - 11.12.2.0, маска 255.255.255.0 (24 бита);
- защищаемая область C - 11.12.3.0, маска 255.255.255.0 (24 бита);
- внутренний порт маршрутизатора A -11.12.1.1;
- внутренний порт маршрутизатора B -11.12.2.1;
- внутренний порт маршрутизатора C -11.12.3.1.

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

На работу сети наложены следующие ограничения:

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

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

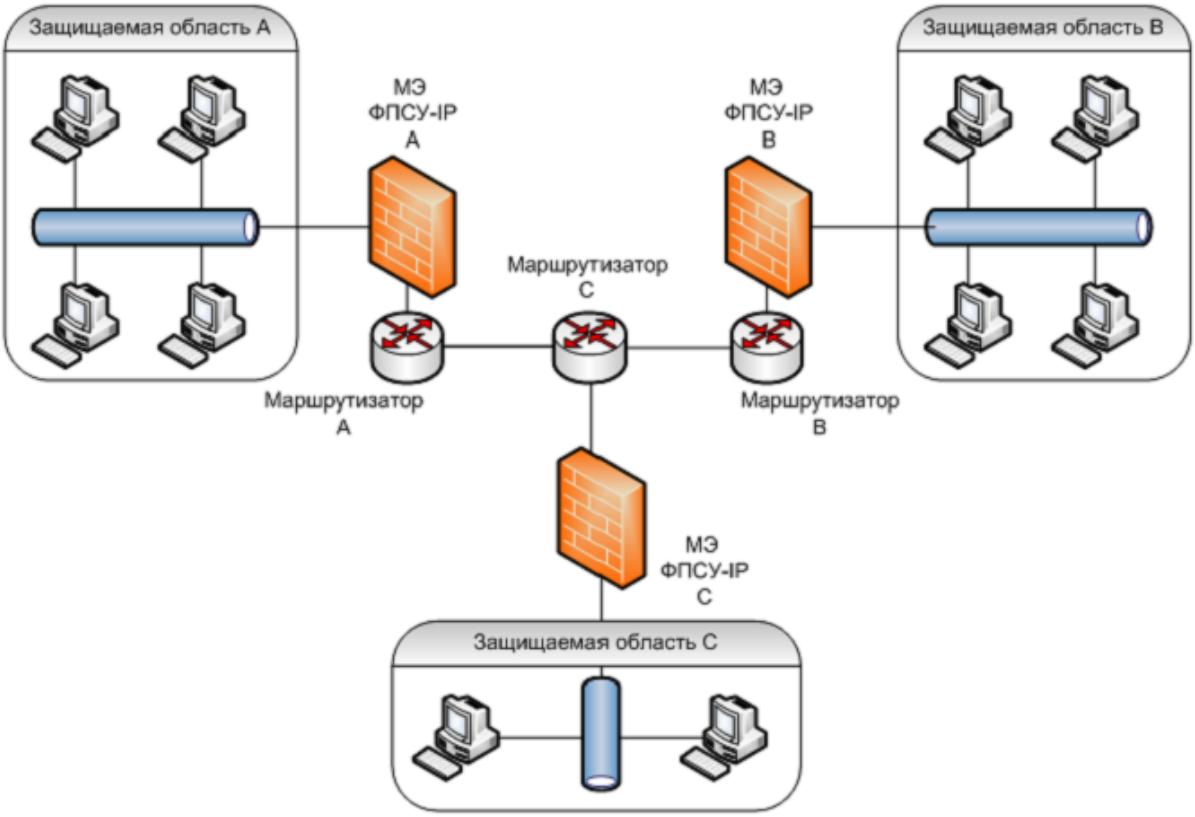

Рисунок 285 - Схема виртуальной частной сети на ФПСУ-IP

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

- со стороны внутреннего порта каждого ФПСУ-IP (например, порта 1) существует одна соответствующая IP-подсеть, а со стороны порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы и ФПСУ-IP отсутствуют;
- со стороны порта 2 существуют две IP-подсети, а со стороны порта 1 хостов, принадлежащих этим подсетям, нет; доступ к ним будет осуществляться через соответствующий удаленный ФПСУ-IP;
- обмен между защищаемыми областями должен производиться только внутри организованных ФПСУ-IP VPN-туннелей;
- на каждом ФПСУ-IP должны быть установлены ранее выработанные криптографические ключи парно-выборочной связи. Причем на ФПСУ-IP A указан собственный номер ключа 1, на ФПСУ-IP B - номер 2 и на ФПСУ-IP C - номер 3;

- со стороны внешнего порта ФПСУ-IP установлены пограничные маршрутизаторы, управление которыми должно осуществляться только из защищаемой области С, причем каналы управления маршрутизаторами за пределами их внешних портов должны быть защищены ФПСУ-IP.

В данном случае возможны два различных варианта конфигурации ФПСУ-IP, которые описаны ниже.

15. 4. 1. Использование раздельных VPN-туннелей

В данном варианте конфигурации на каждом ФПСУ-IP будет создаваться по два VPN-туннеля.

Всего будет создано три VPN-туннеля. При этом для обмена данными защищаемые области будут использовать следующие туннели:

- VPN-1 - обмен области А с областью С;
- VPN-2 - обмен области В с областью С;
- VPN-3 - обмен области А с областью В.

На рисунке ниже показаны организованные VPN-туннели.

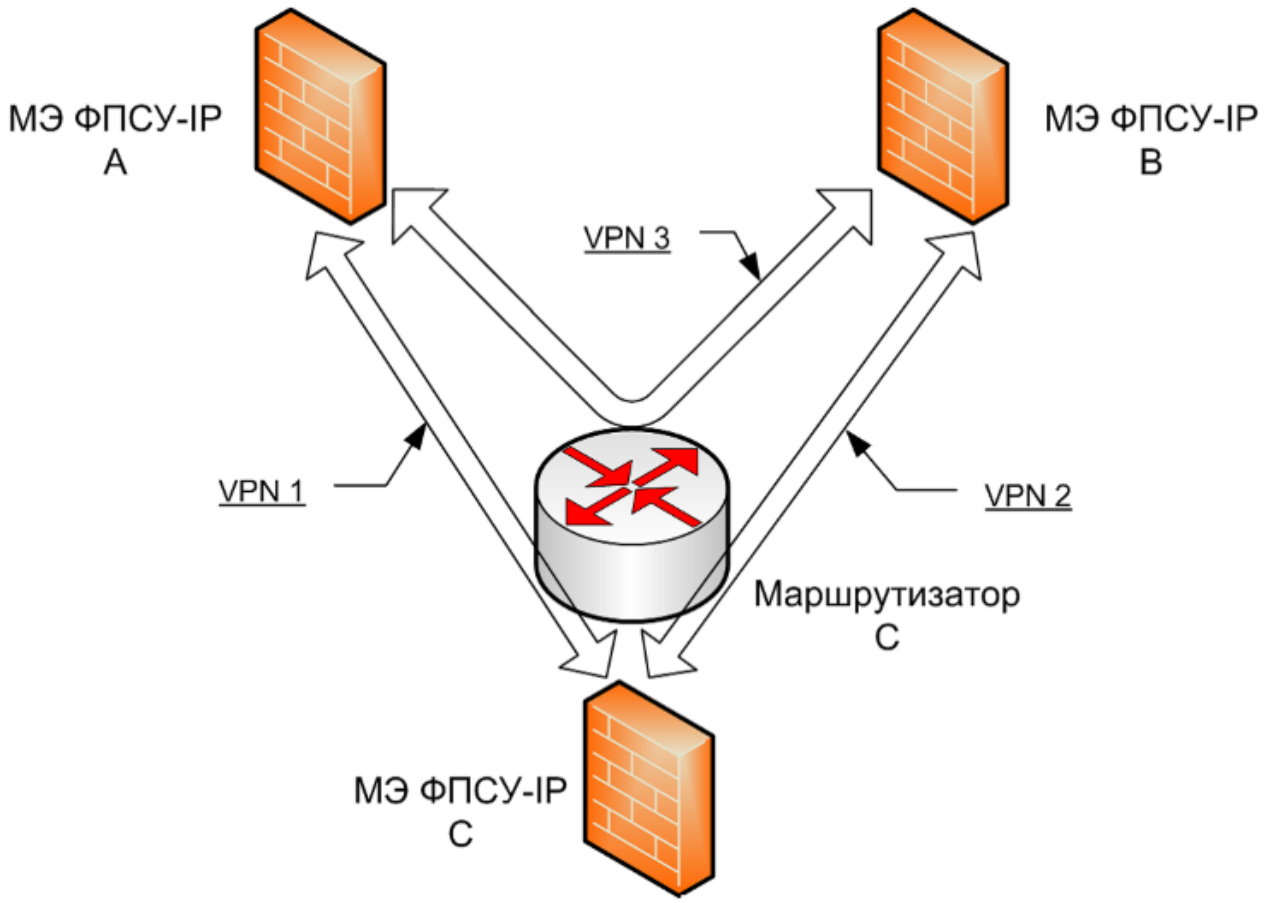

Рисунок 286 - Схема подключения с раздельными туннелями

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

Конфигурация ФПСУ-IP должна содержать следующие установки:

⇒ **Для ФПСУ-IP А:**

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

```
Порт 1:
Номер 1;
```

Адрес 11.12.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ не определены;
Маршрутизаторы не определены.
Абоненты:
Подсеть; 11.12.1.0; 255.255.255.0 (24 разряда),
режим работы - ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Порт 2:

Номер 2;
Адрес 11.12.1.50;
Маска 255.255.255.0 (24 разряда);
ФПСУ
11.12.2.50, ключевые данные - 2.1; смена через 30 мин,
сжатие и криптозащита - "*желательно*" или "*обязательно*",
через маршрутизатор 11.12.1.1;
11.12.3.50, ключевые данные - 3.1; смена через 30 мин,
сжатие и криптозащита - "*желательно*" или "*обязательно*",
через маршрутизатор 11.12.1.1;
Маршрутизаторы
11.12.1.1;
протоколы маршрутизации - на усмотрение администратора,
переключатель "Отвечать на Ping" - на усмотрение администратора;
Абоненты
Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда),
через ФПСУ 11.12.2.50,
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда),
через ФПСУ 11.12.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

⇒
Для ФПСУ-IP В:

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

Порт 1:
Номер 1
Адрес 11.12.2.50
Маска 255.255.255.0 (24 разряда)
ФПСУ не определены
Маршрутизаторы не определены
Абоненты:
Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда), ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Порт 2:
Номер 2
Адрес 11.12.2.50
Маска 255.255.255.0 (24 разряда)
ФПСУ:
11.12.1.50, ключевые данные - 1.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 11.12.2.1
11.12.3.50, ключевые данные - 3.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 11.12.2.1
Маршрутизаторы:
11.12.2.1, протоколы маршрутизации - на усмотрение администратора;
переключатель "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;

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

⇒
Для ФПСУ-IP C:

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

Порт 1:
Номер 1,
Адрес 11.12.3.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть; 11.12.3.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Порт 2:
Номер 2,
Адрес 11.12.3.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
11.12.1.50, ключевые данные - 1.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 11.12.3.1
11.12.2.50, ключевые данные - 2.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 11.12.3.1
Маршрутизаторы:

11.12.3.1, протоколы маршрутизации - на усмотрение администратора;
переключатель "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Только на ФПСУ-IP С для подсети 11.12.3.0 должно быть разрешено управление маршрутизаторами 11.12.1.1, 11.12.2.1, 11.12.3.1 (см. пункт "DHCP-Relay").

Необходимо также перенастроить пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

15. 4. 2. Использование совмещенных VPN-туннелей

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

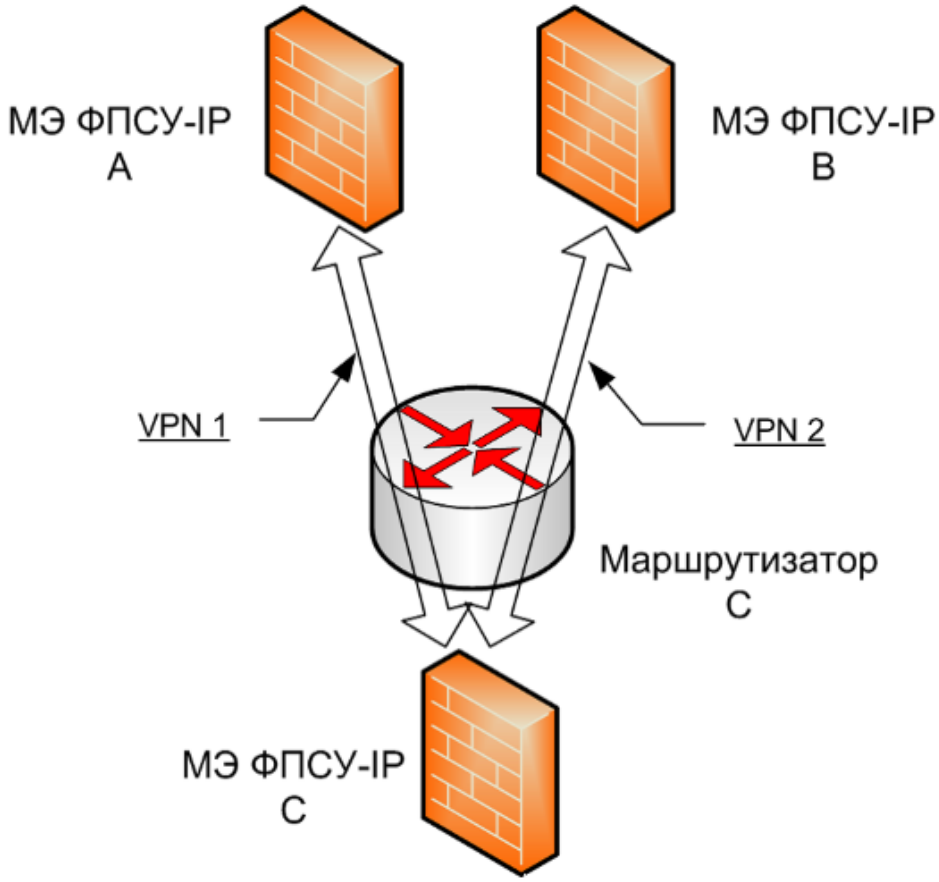

Рисунок 287 - Схема подключения с последовательными туннелями

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

- VPN-1 - обмен области A с областью C;
- VPN-2 - обмен области B с областью C;
- VPN-1 и VPN-2 - обмен области A с областью B.

Конфигурация комплексов должна содержать следующие установки:

⇒
Для ФПСУ-IP A:

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

Порт 1:

Номер 1,
Адрес 11.12.1.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены,
Абоненты:
Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Порт 2:

Номер 2,
Адрес 11.12.1.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
11.12.3.50, ключевые данные - 3.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 11.12.1.1;
Маршрутизаторы
11.12.1.1, протоколы маршрутизации - на усмотрение администратора;
переключатель "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

⇒
Для ФПСУ-IP В:

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

Порт 1:
Номер 1,
Адрес 11.12.2.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Порт 2:
Номер 2,
Адрес 11.12.2.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ:
11.12.3.50, ключевые данные - 3.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "*обязательно*";
через маршрутизатор 11.12.2.1
Маршрутизаторы:
11.12.2.1, протоколы маршрутизации - на усмотрение администратора;
переключатель "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.3.50;
режим партнера этого порта - включен только режим через ФПСУ;

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

⇒
Для ФПСУ-IP С:

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

Порт 1:
Номер 1,
Адрес 11.12.3.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Порт 2:
Номер 2,
Адрес 11.12.3.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
11.12.1.50, ключевые данные - 1.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 11.12.3.1
11.12.2.50, ключевые данные - 2.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 11.12.3.1
Маршрутизаторы:
11.12.3.1,
протоколы маршрутизации - на усмотрение администратора;
переключатель "Отвечать на Ping" - на усмотрение администратора;
Абоненты:

```
Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
```

Только на ФПСУ-IP С для подсети 11.12.3.0 должно быть разрешено управление маршрутизаторами 11.12.1.1, 11.12.2.1, 11.12.3.1 (см. раздел "DHCP-Relay").

Необходимо также переконфигурировать пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

15. 5. Использование ФПСУ-IP для создания в одной области двух защищаемых областей

В документе "Описание применения" ПАК ФПСУ-IP приведена каскадная схема установки двух ФПСУ-IP в одной защищаемой области, при которой хосты оконечной области (защищенной двумя ФПСУ-IP) будут обмениваться пакетами с хостами сетевых фрагментов, находящихся со стороны внешнего порта внешнего ФПСУ-IP, через VPN-туннель, создаваемый в самой защищаемой области, а хосты защищаемой области - через внешний ФПСУ-IP защищаемой области. В данном разделе будут рассмотрены особенности конфигурирования работы комплексов в условиях такой сетевой топологии.

Итак, предположим, что сеть организации представляет из себя два территориально разделенных фрагмента, для защиты которых будут применены ФПСУ-IP, причем в одной из подсетей существует особо ответственная IP-сеть, для которой необходимо обеспечить режим усиленной защиты. После установки комплексов сеть организации примет вид, отображенный на рисунке ниже.

Используются следующие IP-адреса:

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

- внутренний порт маршрутизатора B -11.12.3.1.

На работу сети наложены следующие ограничения:

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

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

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

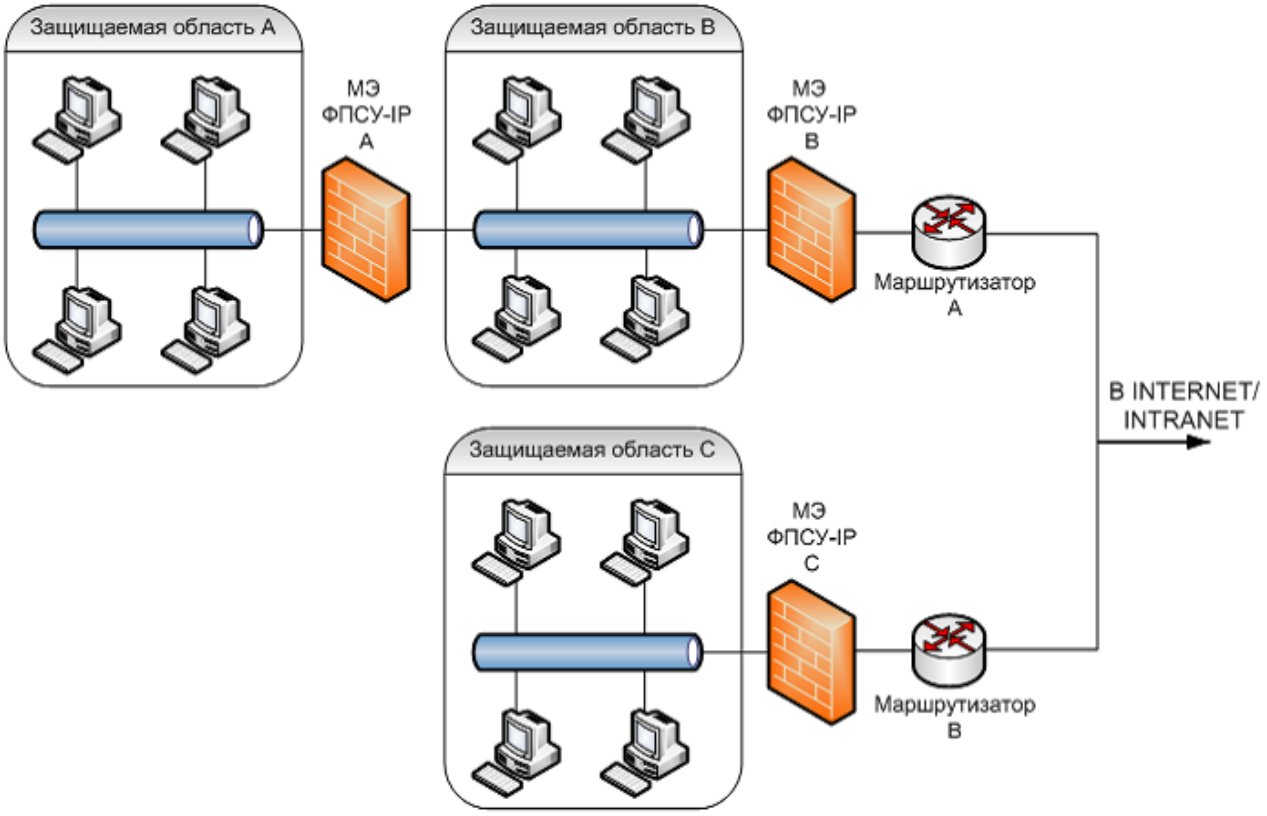

Рисунок 288 - Каскадное подключение ФПСУ-IP

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

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

пределами их внешних портов должны быть защищены ФПСУ-IP B и C.

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

- со стороны внутреннего порта (порта 1 со стороны области C) существует IP-подсеть C, а со стороны порта 2 принадлежащих этой подсети хостов нет; маршрутизаторы и ФПСУ-IP отсутствуют;
- со стороны порта 2 (внешнего) существуют: IP-подсеть B, доступ к которой необходимо запретить; IP-подсеть A, доступ в которую будет производиться через ФПСУ-IP B, а также общедоступная сеть, доступ в которую предоставлен не будет; маршрутизатор B является пограничным;
- обмен между защищаемыми областями A и C должен производиться только внутри организованных ФПСУ-IP VPN-туннелей;
- на ФПСУ-IP C должны быть установлены и указаны как собственные ранее выработанные ключи номер 3;
- со стороны внешнего порта ФПСУ-IP существует пограничный маршрутизатор, управление которым должно осуществляться только из защищаемой области B, причем канал управления маршрутизатором за пределами его внешнего порта должен быть защищен ФПСУ-IP B и C.

Конфигурация ФПСУ-IP должна содержать следующие установки:

⇒
Для ФПСУ-IP A:

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

Порт 1:
Номер 1,
Адрес 11.12.1.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;

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

Порт 2:

Номер 2,
Адрес 11.12.3.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
11.12.2.50, ключевые данные - 2.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы:
11.12.2.1, протоколы маршрутизации - все выключены;
переключатель "Отвечать на Ping" - выключен;
Абоненты:
Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.2.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Хост, 11.12.3.1, ретрансляция;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" выключен.

⇒
Для ФПСУ-IP B:

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

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

Порт 1:

Номер 1,
Адрес 11.12.2.50,

Маска 255.255.255.0 (24 разряда);
ФПСУ:
11.12.1.50, ключевые данные - 1.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "обязательно";
Маршрутизаторы не определены;
Абоненты:
Подсеть, 11.12.2.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.1.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.

Порт 2:

Номер 2,
Адрес 11.12.2.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ:
11.12.3.50, ключевые данные - 3.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 11.12.2.1.
Маршрутизаторы:
11.12.2.1, протоколы маршрутизации - все выключены;
переключатель "Отвечать на Ping" - на усмотрение администратора;
Абоненты:
Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.3.50;
режим партнера этого порта - включен только режим через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Хост, 11.12.3.1; через ФПСУ 11.12.3.50;
режим партнера этого порта - включен только через ФПСУ;
режим партнера другого порта - включены все режимы;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Любой хост;

переключатель "Работа разрешена" включен;
через маршрутизатор 11.12.13.30;

⇒
Для ФПСУ-IP С:

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

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

Порт 1:
Номер 1,
Адрес 11.12.3.50,
Маска 255.255.255.0 (24 разряда),
ФПСУ не определены,
Маршрутизаторы не определены;
Абоненты:
Подсеть, 11.12.3.0; 255.255.255.0 (24 разряда); ретрансляция;
режим партнера этого порта - выключен;
режим партнера другого порта - включен только режим через ФПСУ;
переключатель "Только Broadcast" выключен;
переключатель "Отвечать на Ping" - на усмотрение администратора;
переключатель "Работа разрешена" включен.
Порт 2:
Номер 2,
Адрес 11.12.3.50,
Маска 255.255.255.0 (24 разряда);
ФПСУ:
11.12.2.50, ключевые данные - 2.1; смена через 30 мин;
сжатие и криптозащита - "*желательно*" или "обязательно";
через маршрутизатор 11.12.3.1.
Маршрутизаторы:
11.12.3.1, протоколы маршрутизации - все выключены;
переключатель "Отвечать на Ping" - выключен;
Абоненты:
Подсеть, 11.12.1.0; 255.255.255.0 (24 разряда);
через ФПСУ 11.12.2.50;
режим партнера этого порта - включен только режим через ФПСУ;

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

Необходимо также переконфигурировать пограничные маршрутизаторы с целью запрещения доступа к ним по протоколам сетевого управления с внешних портов.

Поскольку конфигурирование нескольких совместно работающих ФПСУ-IP для разветвленной сетевой топологии может вызвать затруднение у неопытного администратора, рекомендуется после заполнения конфигурационных таблиц произвести аналитическую проверку произведенных установок на предмет соответствия заданным требованиям (ограничениям).

В соответствии с установленной конфигурацией через ФПСУ-IP A:

- абоненты области A не получат доступа к области B, маршрутизатору A и общедоступной сети передачи данных, поскольку все они не описаны со стороны порта 2; кроме того, доступу к ним препятствует также указанный в описателе для абонентов A режим работы с абонентом противоположного порта (только через ФПСУ);
- отсутствие доступа абонентов области A к маршрутизатору A обеспечивается тем, что он описан (специально для этой цели) со стороны порта 2 с выключенным признаком "Работа разрешена" (все остальные установки в описателе, соответствующем маршрутизатору A, не имеют значения);
- Доступ от абонентов области A к абонентам области C осуществляется через ФПСУ-IP B.

В соответствии с установленной конфигурацией через ФПСУ-IP B:

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

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

В соответствии с установленной конфигурацией через ФПСУ-IP C:

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

16. Способы разрешения возможных проблем при работе ФПСУ-IP

16. 1. Первый запуск ФПСУ-IP

Несмотря на то, что установка ФПСУ-IP не требует переконфигурирования сетевого оборудования, при первом его запуске (при подключении его к сети) возможны ситуации, когда для нормализации работы сети необходимо предпринять специальные действия.

Это обусловлено тем, что ARP-таблицы сетевого оборудования после установки ФПСУ-IP будут содержать устаревшие сведения (ARP-записи) об адресах сетевых адаптеров хостов или другого сетевого оборудования, которые могут обновиться только после истечения "времени жизни" записи. Это время задается в конфигурации сетевого оборудования и может оказаться достаточно большим (например, у маршрутизаторов фирмы Cisco это время может быть равно 4 часам). Понятно, что в течение периода "жизни" устаревших записей необходимо предпринять специальные меры, чтобы восстановить прежнее состояние работы сети и доступ к некоторым хостам защищаемой области.

В ПО ФПСУ-IP введены специальные процедуры, позволяющие обновлять "недостоверные" ARP-записи в ARP-таблицах как пограничных маршрутизаторов, так и хостов, находящихся со сторон его портов. Однако обновление производится только при попытке обмена пакетами хостов защищаемой области с другими хостами или сетевым оборудованием (когда установленный комплекс "знакомится" с хостами или оборудованием, смежными с ним). Если в защищаемой области окажется сервер (передающий пакеты только в ответ на посылаемый запрос, которого он не может получить, поскольку маршрутизирующему оборудованию известен "недостоверный" адрес сетевого адаптера сервера, которому он должен передавать запросы) или другой хост, работающий в пассивном режиме, они будут недоступны в течение "времени старения" соответствующих записей в ARP-таблицах.

Для нормализации работы сети в данной ситуации рекомендуется принять следующие меры:

1. В случае, если ФПСУ-IP устанавливается между защищаемой областью и ее пограничными маршрутизаторами - очистить ARP-таблицы пограничных маршрутизаторов или перезапустить маршрутизаторы;
2. Если между защищаемой областью и ФПСУ-IP пограничные маршрутизаторы отсутствуют — очистить ARP-таблицы "пассивных" хостов или сетевого оборудования, либо перезапустить их, либо осуществить с них попытку обмена пакетами с другими хостами или сетевым оборудованием.

16. 2. Устранение неполадок, связанных с работой сетевого оборудования

Одна из возможных причин возникновения большого количества ошибок в работе сети, или неэффективной работы ФПСУ-IP, выражающейся в резком падении скорости приема/передачи пакетов, связана с несовместимыми режимами работы сетевых адаптеров как самого ФПСУ-IP, так и адаптеров пограничного сетевого оборудования (маршрутизаторы, коммутаторы, концентраторы и т.п.). Ошибки также могут быть связаны с неправильным подбором сетевого кабеля. Многие сетевые LAN-адаптеры при соответствующих установках могут автоматически определять скорость передачи данных по линии и возможность использования полнодуплексного режима приема/передачи.

Однако, при использовании сетевых адаптеров различных фирм-производителей в совместной работе автоматическое определение не всегда производится корректно. Рекомендуется в таком случае отказаться от таких установок и задавать параметры адаптеров вручную в соответствии с требуемым режимом работы.

Таблица обобщает возможные причины возникновения неполадок и рекомендуемые методы проверки аппаратуры или коррекции конфигурации оборудования.

Таблица 7

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

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

17. Диагностика ошибок ФПСУ-IP

При отладке работы ФПСУ-IP сразу после его установки, а также в процессе его дальнейшей работы администратор имеет возможность отслеживать процессы, происходящие в различных подсистемах ФПСУ-IP. Сообщения об ошибках или неполадках, обнаруженных работающим ФПСУ-IP, выдаются на экран монитора (если к ФПСУ-IP подключен монитор) и в регистрационные записи статистики (см. разделы "Окно состояния работы пользователей" и "Просмотр статистики"). Данный раздел поясняет выдаваемые диагностические сообщения и представляет возможные причины возникновения ошибок и методы их устранения.

Ошибки формата принимаемых IP-пакетов:

Диагностика	Пояснение	Причина возникновения
Короткий пакет	Длина принятых данных короче, чем указано в IP заголовке принятого пакета.	Сбой или коллизии локальной сети; сбой у станции отправителя.
Ошибка фрагментации	Суммарная длина собранного из фрагментов IP-пакета больше 65536 байт.	Некорректная работа программного обеспечения станции-отправителя. Если при передаче данных используется протокол TCP, ошибки можно избежать, включив опцию "Корректировать TCP MSS" (см. пункт "Общие параметры конфигурации ФПСУ-IP")
Отмена фрагментации	Размер пакета превышает максимальный размер пакета, MTU, но установленный флаг запрета фрагментации не дает разбивать его на несколько пакетов.	Такая ситуация обычно возникает при попытке передачи пакетов TCP/UDP по протоколу FTP и некоторым другим протоколам, и носит временный характер. Если ошибка возникает постоянно, необходимо проанализировать (и, при необходимости, скорректировать) конфигурацию сетевых адаптеров и/или

		уменьшить MTU до 1400 байт на оборудовании, от которого приходят большие пакеты с флагом запрета фрагментации.
Ошибочный фрагмент	Начало фрагментированного пакета не выровнено на 8 байтовую границу.	Некорректная работа программного обеспечения станции-отправителя.
Неверен список опций	Список IP-опций в заголовке IP пакета не отвечает принятым в сообществе Интернет правилам.	Некорректная работа программного обеспечения станции-отправителя.
Мало памяти	Недостаточно оперативной памяти для приема и/или обработки пакета.	Если такая ошибка указывается для разных IP адресов, причина возникновения - "шторм" в IP сети. Если ошибка возникает только для одного конкретного адреса - вероятно проведение атаки на ФПСУ-IP с целью вывода его из строя через создание сетевой перегрузки.

Ошибки, связанные с обработкой принимаемых IP-пакетов:

Диагностика	**Пояснение**	**Причина возникновения**
Маршрут неизвестен	Не известен адрес сетевого адаптера для соответствующего IP-адреса абонента-получателя.	Если ошибка возникает постоянно - либо станции с таким IP-адресом в сети нет или она не работает, либо режимы смежных сетевых адаптеров несовместимы. Если ошибка возникает эпизодически - неполадки отсутствуют, в момент поступления запроса адрес сетевого адаптера был неизвестен, после чего он был автоматически определен

Диагностика	Пояснение	Причина возникновения
		ФПСУ-IP за непродолжительное время.
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.
Дублирование адресов	В сети со стороны указанного порта обнаружена станция, имеющая IP адрес, совпадающий с одним из портов ФПСУ-IP, или адрес сетевого адаптера которой совпадает с адресом сетевого адаптера ФПСУ-IP.	Это может произойти при образовании маршрутной петли - проверьте правильность конфигурации маршрутизирующего оборудования. В сети на самом деле существует такая станция — смените адреса на ФПСУ-IP или указанной станции.
Неверен IP адрес	Неверен один из IP-адресов в заголовке IP пакета.	IP-адрес отправителя является широковещательным в известные ФПСУ-IP подсети. Отправитель пакета не является известным ФПСУ-IP маршрутизатором, а IP-адрес получателя является либо групповым (multicast), либо широковещательным во все подсети (255.255.255.255). IP-адрес отправителя пакета — 255.255.255.255.
Истекло время	Время жизни пакета истекло, или исчерпан лимит времени ожидания сборки пакета	У принятого пакета истекает время жизни. Если данная ошибка проявляется часто, причем получателем является данный ФПСУ-IP, а отправителем - другой ФПСУ-IP, рекомендуется в конфигурации обоих ФПСУ-IP изменить

Диагностика	Пояснение	Причина возникновения
		значение MTU (см. раздел "Описание параметров удаленных ФПСУ-IP")
Протокол недоступен	Обращение к одному из портов ФПСУ-IP по протоколу, который ФПСУ-IP не поддерживает.	ФПСУ-IP не принимает для обработки пакеты никаких протоколов, кроме собственных протоколов поддержки VPN и администрирования, а также протокола ICMP ECHO REQUEST (Ping) при условии, если это разрешено в конфигурации ФПСУ-IP.

Ошибки, связанные с попытками нарушения установленных правил фильтрации:

Диагностика	Пояснение	Причина возникновения
Входящий не описан	Отправитель пакета не описан в конфигурации	Отправитель пакета не описан в конфигурации портов ФПСУ-IP.
Получатель не описан	Получатель пакета не описан в конфигурации.	Не описан абонент-получатель в конфигурации портов ФПСУ-IP. Для межмаршрутизаторного обмена - нет маршрутизаторов со стороны противоположного порта, использующих данный протокол.
Запрет работы	Отказ в доступе абоненту-отправителю пакета	Выключен переключатель "*Работа Разрешена*" у отправителя или получателя пакета. Попытка приема или передачи в индивидуальный адрес при включенном переключателе "*Только Broadcast*". Попытка межмаршрутизаторного обмена по

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

Диагностика	Пояснение	Причина возникновения
через ФПСУ	работать в режиме ретрансляции.	которого на данном ФПСУ-IP установлен режим работы "*Ретрансляция*".
Абонент миновал ФПСУ	Абонент должен работать через ФПСУ.	Принят пакет не из VPN-туннеля от абонента, для которого на данном ФПСУ-IP установлен режим работы "*Через ФПСУ*".
ФПСУ не работает	Удаленный ФПСУ-IP не работает.	Не включен удаленный ФПСУ-IP или с ним нет связи. Не работает сетевой адаптер - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.
Нет ФПСУ-туннеля	Отсутствие взаимодействия между ФПСУ-IP.	VPN-туннель между двумя ФПСУ-IP не установлен к моменту попытки передачи через него пакетов от абонентов. Не включен удаленный ФПСУ-IP или с ним нет связи. Неустойчивая работа сбойного сетевого адаптера - адаптер необходимо заменить. Несовместимые режимы работы смежных сетевых адаптеров.
Ложный ФПСУ	Станция-отправитель использует ошибочный протокол установки соединения или поддержания VPN-туннеля	Попытка передачи пакетов в IP-адрес местного ФПСУ-IP от рабочей станции, зарегистрированной как удаленный ФПСУ-IP, но не являющейся таковой.

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

Ошибки, связанные с ключевыми данными:

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

Служебное сообщение	**Пояснение**	**Действия администратора**
		ФПСУ-IP (Настройка системы - Регистрация ТМ-идентификаторов)
Внимание! Повреждены критические компоненты комплекса. ВСЕ установленные ключевые данные и ТМ утрачены. Комплекс переведен в технологический режим. Возможно потребуется переустановка комплекса	ПО ФПСУ-IP обнаружило искажение ключа для хранения долговременных ключей. Требуется вмешательство администратора	Требуется выполнить повторный перевод ФПСУ-IP из технологического режима в рабочий режим, заново зарегистрировать все ТМ-идентификаторы пользователей и переустановить ключевые данные ЦВК и удаленных администраторов. В случае ошибки перевода ФПСУ-IP из технологического режима в рабочий режим, выполнить полную переустановку ПО ФПСУ-IP.
Внимание! Поврежден компонент комплекса. Необходима инициализация ДСЧ	ПО ФПСУ-IP обнаружило искажение ключа ПДСЧ. Требуется вмешательство администратора	Требуется выполнить повторный перевод ФПСУ-IP из технологического режима в рабочий режим.
Внимание! ФПСУ не работоспособен. Искажены данные конфигурации. Ожидание восстановления конфигурации с резервного комплекса или удаленного администратора	ПО ФПСУ-IP обнаружило искажение конфигурации ФПСУ-IP	Восстановить конфигурацию ФПСУ-IP любым из следующих способов: • локально с помощью резервной копии конфигурации; • подключить к ФПСУ-IP комплекс горячего резерва; • установить на ФПСУ-IP новую конфигурацию средствами удаленного администратора.

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

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

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

Служебное сообщение	**Пояснение**	**Действия администратора**
		резерва на сообщившем об ошибке ФПСУ-IP.
Испорчен или не установлен ключ центра	Сообщение об ошибке выводится на экране мониторинга действий ФПСУ-IP\Клиентов. Искажен общесистемный ключ криптосети Клиентов. ФПСУ-IP\Клиенты не могут соединиться с ФПСУ-IP	Заново установить на ФПСУ-IP общесистемный ключ криптосети Клиентов вместо искаженного.
ТМ испорчена	Сообщение об ошибке выводится при попытке зарегистрировать общесистемный ключ криптосети Клиентов на ФПСУ-IP. Находящийся на ТМ-идентификаторе общесистемный ключ криптосети Клиентов искажен или испорчен.	Заново получить от администратора ЦГКК общесистемный ключ криптосети Клиентов и повторить процедуру регистрации общесистемного ключа криптосети Клиентов на ФПСУ-IP

17. 1. Выдача файла Kmsg

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

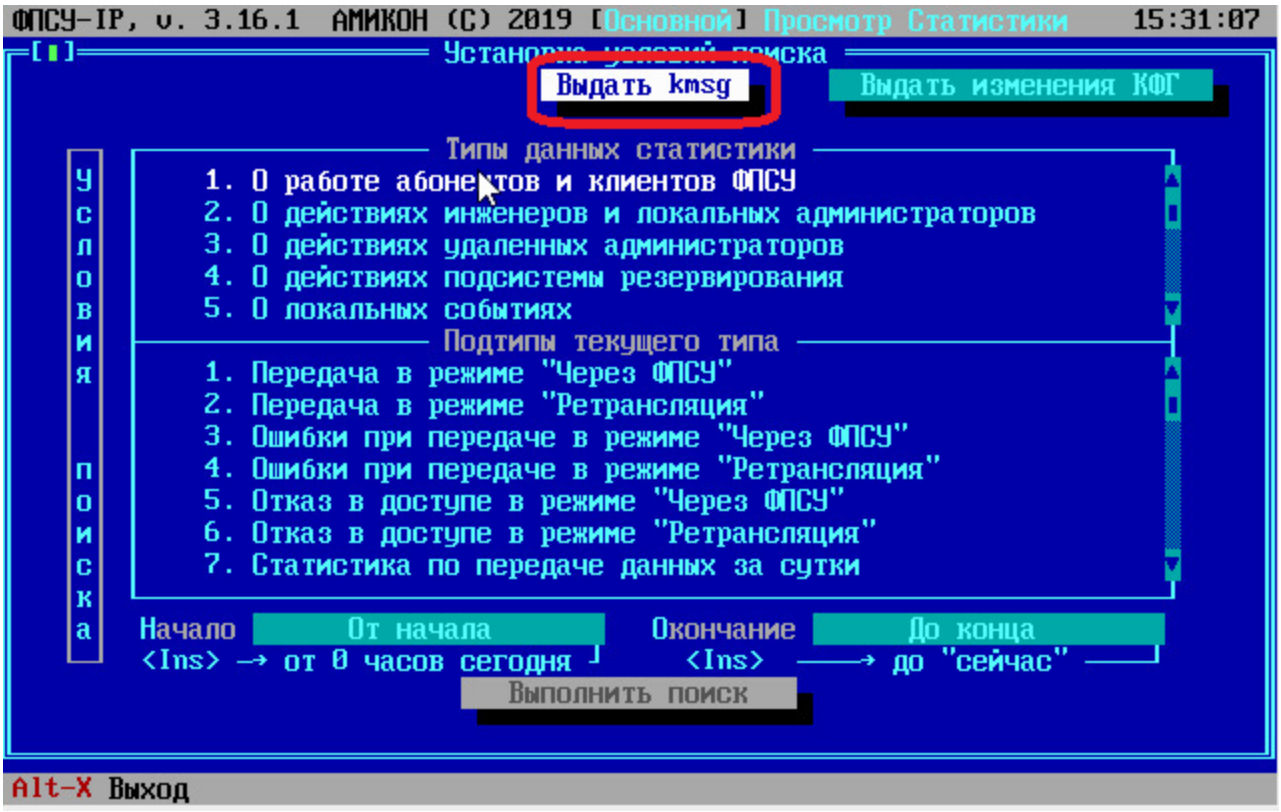

Рисунок 289 - Команда выдачи журнала изменений конфигурации межсетевого экрана

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

Рисунок 290 - Предложение подключить USB-носитель

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

Рисунок 291 - Выбор каталога для выгрузки файла

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

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

Рисунок 292 - Сообщение о завершении процедуры

18. Удаление программного обеспечения ФПСУ-IP

18. 1. Удаление СКЗИ ФПСУ-IP

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

Для запуска процедуры форматирования внутреннего накопителя следует выполнить:

1. Команду "Настройка системы" главного меню:

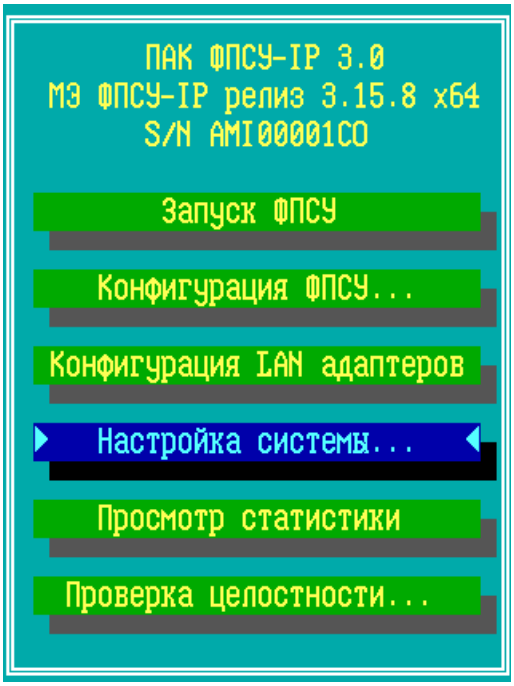

Рисунок 293 - Главное меню ФПСУ-IP

2. Команду "Настройки СКЗИ" меню настройки системы:

Рисунок 294 - Меню настройки системы ФПСУ-IP

3. Команду "Удаление СКЗИ" меню настройки СКЗИ.

Рисунок 295 - Запуск процедуры удаления СКЗИ

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

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

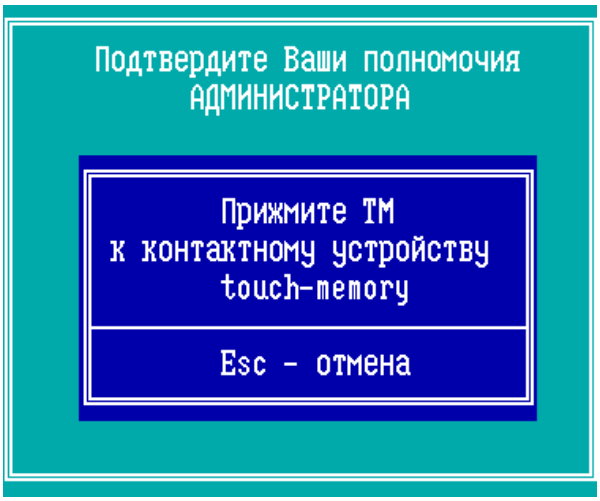

Рисунок 296 - Подтвердите полномочия для удаления СКЗИ

После подтверждения прав администратора, ФПСУ-IP начнет форматирование внутреннего накопителя, после чего перезагрузит операционную систему. Удаление операционной системы ФПСУ-IP и хранящихся на внутреннем накопителе файлов, в том числе ключевой информации СКЗИ, программных и служебных модулей СКЗИ, и программного обеспечения BIOS/UEFI, завершено.

18. 2. Удаление ПО с помощью USB-носителя со средством восстановления

Для полного удаления программного обеспечения ФПСУ-IP с его ПЗУ, следует запустить процедуру повторной установки программного обеспечения (см. пункт "Установка ПО ФПСУ-IP с установочного носителя"). Для успешного удаления программного обеспечения потребуются:

- ФПСУ-IP;
- инсталляционный комплект программного обеспечения ФПСУ-IP, состоящий из USB-носителя с дистрибутивом.

Порядок действий при удалении программного обеспечения с ПЗУ ФПСУ-IP следующий:

1. Подключите USB-носитель с дистрибутивом программного обеспечения к ФПСУ-IP.
2. При включении ФПСУ-IP следует отменить загрузку подсистемы ACCESS-TM SHELL, запрещающей загружать операционную систему иначе как с защищенной внутренней памяти, и выбрать загрузку с USB. Это можно сделать при выборе Boot Options (обычно при нажатии F10) после включения ФПСУ-IP, или напрямую зайдя в BIOS и установив в Boot Options загрузку **USB2.0** вместо **Access BIOS/PnP**.

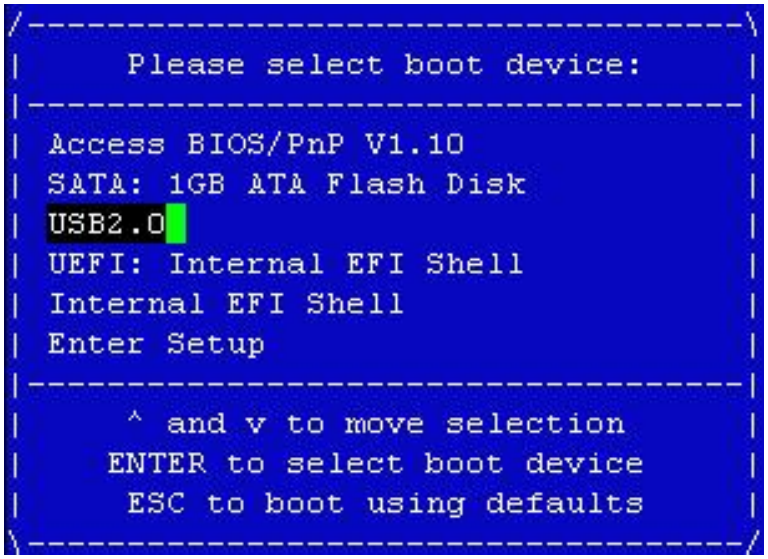

Рисунок 297 - Выбор загрузки с USB

3. Загруженная с инсталляционного USB-носителя программа начнет первый этап установки с проверки ранее установленного программного обеспечения ФПСУ-IP. Если система была ранее установлена на комплекс, будет выдано следующее сообщение:

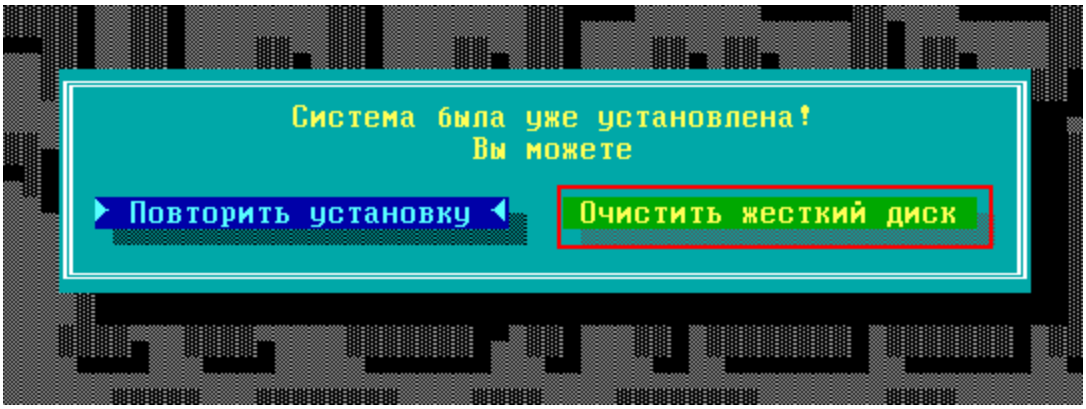

Рисунок 298 - Операционная система ФПСУ-IP уже установлена

4. Выберите команду <*Очистить жесткий диск*> и подтвердите выполнение операции.

После выполнения операции "Очистить жесткий диск", питание ФПСУ-IP можно выключать. Операционная система, ключевая информация СКЗИ, программные и служебные модули СКЗИ полностью удалены с ПЗУ ФПСУ-IP.

Уничтожение программных модулей СКЗИ на дистрибутивном USB-носителе осуществляется путем расплющивания USB-носителя молотком на наковальне.