ООО «АМИКОН»

УТВЕРЖДЕН

ПЕРС.26.20.40.140.001ОП-ЛУ

Семейство средств защиты информации

«ФПСУ-IP»

Описание применения

ПЕРС.26.20.40.140.001ОП

Листов 80

2023

Аннотация

Документ предназначен для сотрудников службы безопасности и администраторов безопасности систем защиты от несанкционированного доступа с применением средств защиты информации семейства «ФПСУ-IP».

В документе приводится описание применения следующих средств защиты информации, входящих в семейство «ФПСУ-IP»:

- Программно-аппаратный комплекс «ФПСУ-IP» версии 3;
- «ФПСУ-IP Int» версии 3;
- Удаленный администратор «ФПСУ-IP»;
- Удаленный администратор «ФПСУ-IP Int»;
- Центр выработки ключей «ФПСУ-IP»;
- Центр выработки ключей «ФПСУ-IP Int»
- Центр генерации ключей ФПСУ-IP/Клиентов;
- ФПСУ-IP/Клиент для Android;
- ФПСУ-IP/Клиент для IOS;
- ФПСУ-IP/Клиент для Windows;
- ФПСУ-IP/Клиент для Linux;
- ФПСУ-IP/Клиент для MacOS.

По всем вопросам и предложениям, обращайтесь непосредственно в ООО «АМИКОН». Вам всегда будут представлены консультации по телефону или электронной почте. Отзывы и предложения по документации просьба высылать на электронную почту.

Контакты:

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

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

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

Электронная почта: info@amicon.ru

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

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

Содержание

1. Список используемых сокращений и определений

APR	«Address Resolution Protocol», протокол для отображения IP-адреса рабочей станции сети в её аппаратный адрес;
ICMP	«Internet Control Message Protocol», протокол для передачи команд и сообщений об ошибках;
IP	«Internet Protocol», базовый протокол Интернет;
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;
WAN	«Wide-Area Network», глобальная сеть, связывающая географически разделенные рабочие станции и LAN;
ЛВС	локальная вычислительная сеть;
НСД	несанкционированный доступ к информации;
ПАК	программно-аппаратный комплекс;
ПО	программное обеспечение;
ПЭВМ	персональная электронная вычислительная машина, компьютер;
СКЗИ	средство криптографической защиты информации;
СКЗИ «ФПСУ-IP»	средство криптографической защиты информации «Программно-аппаратный комплекс шифрования «ФПСУ-IP» (ИНФК.11485466.4012.024) или средство криптографической защиты «Программно-аппаратный комплекс шифрования «ФПСУ-IP Int» (ИНФК.11485466.4012.011.026);
ТМ	(ТМ-идентификатор) - электронный идентификатор «touch-memory», iButton DS1993 – DS1996 или микроэлектронное USB-устройство «TM-Key» ПЕРС.466226.004 (ООО «АМИКОН»);
«ФПСУ-IP»	программно-аппаратный комплекс «ФПСУ-IP» версии 3 (версия ПО 3.20.1, 3.20.8) (Фильтр Пакетов Сетевого Уровня), являющийся СКЗИ «ФПСУ-IP» или «ФПСУ-IP Int», изделием Криптомаршрутизатор;
«ФПСУ-IP/Клиент»	общее название для программных и программно-аппаратных комплексов «ФПСУ-IP/Клиент для Windows», «ФПСУ-IP/Клиент для Linux», «ФПСУ-IP/Клиент для MacOS», «ФПСУ-IP/Клиент для IOS», «ФПСУ-IP/Клиент для Android», являющихся изделиями из состава СКЗИ «ФПСУ-IP/Клиент» или «ФПСУ-IP/Клиент Int»;
ПЗУ	постоянное запоминающее устройство, внутренний накопитель данных ПЭВМ (HDD, SSD, Flash);

УА ФПСУ-IP Программный комплекс «Удаленный администратор «ФПСУ-IP» являющийся изделием АРМ УА из состава СКЗИ «ФПСУ-IP» или «ФПСУ-IP Int»;

Хост узел сети, не являющийся маршрутизатором, т.е. не передающий информацию из одной сети в другую.

ЦВК программно-аппаратный комплекс «Центр выработки ключей «ФПСУ-IP», являющийся изделием ЦВК из состава СКЗИ «ФПСУ-IP» или «ФПСУ-IP Int»;

ЦГКК Программное обеспечение «Центр генерации ключей ФПСУ-IP/Клиентов», являющееся изделием Центр генерации ключей клиентов из состава СКЗИ «ФПСУ-IP/Клиент» или «ФПСУ-IP/Клиент Int».

2. Назначение и характеристики «ФПСУ-IP»

Программные и программно-технические решения семейства «ФПСУ-IP» являются средствами защиты от несанкционированного доступа к информации. Решения семейства «ФПСУ-IP» направлены на выполнение функции межсетевого экранирования и построения виртуальных частных сетей поверх глобальных и локальных вычислительных сетей.

В составе решений семейства «ФПСУ-IP» используются средства криптографической защиты информации, что позволяет осуществлять криптографическую защиту передаваемой информации.

Центральным элементом семейства средств защиты информации «ФПСУ-IP» является Программно-аппаратный комплекс «ФПСУ-IP» версии 3 (версии ПО 3.20.1, 3.20.8).

«ФПСУ-IP» разработан для применения в вычислительных сетях, использующих стек протоколов TCP/IP и среду передачи данных Ethernet (тип кадра Ethernet_II).

«ФПСУ-IP» совмещает в себе функции межсетевого экрана, пакетного коммутатора сетевого уровня и организатора виртуальных частных сетей (VPN) поверх локальных и глобальных вычислительных сетей изготавливается в двух вариантах:

- специализированное программно-аппаратное устройство;
- программное решение для установки в виртуальную среду (виртуальная машина).

«ФПСУ-IP» устанавливается аппаратно (в случае специализированного программно-аппаратного устройства) или логически (в случае виртуальной машины) на выходе из защищаемой локальной сети в общие сети и осуществляет скоростную фильтрацию передаваемых пакетов данных, анализируя их по совокупности критериев и принимая решение о возможности их дальнейшей передачи. В качестве критериев фильтрации могут выступать IP-адреса отправителей и получателей пакетов, разрешённые номера IP-протоколов, номера портов TCP/UDP, направление передачи пакета, время работы и разрешённые парные связи между конкретными абонентами. Таким образом, «ФПСУ-IP» позволяет реализовать контроль и управление потоками информации, а также их коммутацию из одной локальной сети в другую, что обеспечивает разграничение доступа и защиту сегментов ЛВС от атак злоумышленников.

«ФПСУ-IP» может использоваться для разграничения доступа абонентов одной локальной сети друг к другу и/или для выделения в локальной сети участков с повышенной степенью защиты от НСД.

Безопасность передачи информации при взаимодействии абонентов территориально распределённых ЛВС, защищённых «ФПСУ-IP» и использующих «ФПСУ-IP» в качестве

пакетных сетевых фильтров, повышается за счёт организации межсетевых туннелей между каждой парой «ФПСУ-IP».

При этом в таких туннелях обеспечиваются:

- начальные идентификация и аутентификация взаимодействующих «ФПСУ-IP»;
- сеансовые идентификация и аутентификация взаимодействующих «ФПСУ-IP»;
- идентификация, аутентификация и контроль целостности принимаемых по туннелю данных;
- сжатие отфильтрованных пакетов специализированным встроенным компрессором;
- 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.

Таким образом, с использованием защищённых межсетевых туннелей несколько территориально-распределённых ЛВС могут быть объединены в единую виртуальную частную сеть (virtual private network, VPN).

При этом обеспечиваются:

- безопасное взаимодействие абонентов ЛВС через общедоступные WAN-сети;
- проверка подлинности сетевых ресурсов;
- проверка подлинности источника и приемника данных принимаемых сообщений;
- контроль доступа к ресурсам сети.

Аутентификация взаимодействующих «ФПСУ-IP» и преобразование передаваемой в межсетевых туннелях информации производятся с использованием ключей парно-выборочной связи, вырабатываемых для каждого «ФПСУ-IP» при помощи программно-аппаратного комплекса «Центр выработки ключей «ФПСУ-IP».

Виртуальные частные сети, построенные на основе комплексов «ФПСУ-IP», защищающих подсети, расширяются за счёт организации аналогичных VPN-туннелей между «ФПСУ-IP» и программными и программно-аппаратными комплексами «ФПСУ-IP/Клиент», используемых для защиты межсетевого взаимодействия отдельных рабочих станций и устройств.

«ФПСУ-IP» осуществляет фильтрацию IP-пакетов протоколов маршрутизации (RIP, RIP 2, IGRP, EIGRP, OSPF, OSPF2, LDP).

Для повышения надёжности и обеспечения бесперебойной работы защищаемых подсетей в ситуации аппаратных отказов, «ФПСУ-IP» может быть задействован в режиме «горячего» резервирования, позволяющую вместо одного «ФПСУ-IP» использовать пару

«ФПСУ-IP», один из которых выполняет все функциональные операции, а второй находится в ожидании, готовый принять управление на себя в случае неполадок на основном «ФПСУ-IP».

«ФПСУ-IP» поддерживает возможность отправки сообщений о происходящих на нем событиях (логов) по протоколу SysLog. Для это разработана специальная подсистема, которая отслеживает происходящие на «ФПСУ-IP» события и отправляет их на внешний сервер, работающий как хранилище Syslog-сообщений.

«ФПСУ-IP» может принимать участие в построении VLAN (IEEE 802.1Q) локальной сети, выполняя функции маршрутизатора VLAN. На портах «ФПСУ-IP» поддерживается до 4093 тегов VLAN. Для этого на «ФПСУ-IP» должна быть установлена специальная подсистема поддержки VLAN.

Администрирование и непосредственный контроль процесса фильтрации на «ФПСУ-IP» производятся как локально, так и дистанционно, с любой рабочей станции IP-сети, оборудованной программно-аппаратным комплексом «Удаленный администратор ФПСУ-IP». Один УА ФПСУ-IP позволяет обслуживать до 32000 территориально-удалённых «ФПСУ-IP», обеспечивая при этом выполнение практически полного набора функций по настройке, контролю и управлению работой комплексов «ФПСУ-IP». Соединения удалённых администраторов с «ФПСУ-IP» осуществляются через специализированные туннели, в которых производятся аутентификация администратора и криптографическая защита передаваемых данных от НСД.

Программно-аппаратный комплекс «ФПСУ-IP» не сложен в эксплуатации. Установка комплекса зачастую не требует изменения топологии сети, реконфигурирования сетевого оборудования и изменения IP-адресов абонентов. Вырабатываемый комплексом служебный трафик незначителен и не приводит к существенному увеличению расходов на эксплуатацию сети передачи данных, кроме того, использование подсистемы сжатия передаваемых данных позволяет в отдельных случаях уменьшить существующие расходы организации.

Программное обеспечение комплекса поддерживает такие протоколы, как ARP (с расширением ARP-proxy), IP и ICMP, удовлетворяя при этом требованиям стандартов RFC 768, 791, 792, 793, 826, 894, 919, 922, 950, 1122, 1256, 1305, 1393, 1475, 1519, 1700, 1812, 3069 и др. с некоторыми ограничениями, накладываемыми требованиями защиты от НСД.

«ФПСУ-IP» позволяет создавать различные уровни защиты для отдельных участков сети. Полный интегрированный набор средств защиты от НСД межсетевого сообщения с применением «ФПСУ-IP», обеспечивающий максимальный уровень защиты, включает следующие механизмы:

- фильтрацию сетевых пакетов в соответствии с типами отправителя и получателя (абонент, маршрутизатор, удалённый «ФПСУ-IP», «ФПСУ-IP/Клиент», удалённый администратор) по задаваемым администратором правилам, IP-адресам отправителя и получателя, типам фреймов, инкапсулированных в IP протоколов, времени, направлению и дате передачи пакета, разрешённым портам абонентов (для TCP/UDP-пакетов);
- принцип передачи через «ФПСУ-IP» пакетов осуществляется по принципу «запрещено всё, что не разрешено», что защищает от нападений, основанных на новых, незнакомых или неясных IP-сервисах, а также ошибок конфигурации;
- сокрытие сетевых адресов отправителя и получателя, прикладных функций защищаемой сети и используемых ими сетевых протоколов;
- возможность идентификации и аутентификации «ФПСУ-IP/Клиентов», удалённых «ФПСУ-IP» и удалённых администраторов методами, устойчивыми к активному перехвату информации в сети;
- возможность идентификации, аутентификации и контроля целостности данных, принятых от «ФПСУ-IP/Клиентов», удалённых «ФПСУ-IP» и удалённых администраторов методами, устойчивыми к активному перехвату информации в сети;
- возможность сжатия межсетевого трафика специализированным высокоэффективным компрессором с целью повышения скорости передачи данных и уменьшения расходов на эксплуатацию сети;
- возможность организации туннелированной передачи данных с пакетным шифрованием;
- возможность сокрытия топологии сети и факта функционирования «ФПСУ-IP» как средства защиты с фильтрующими возможностями;
- возможность запрещения TCP/UDP-соединений с отдельными абонентами защищаемой области по портам и направлению соединения;
- специфическую обработку IP-опций, способствующих раскрытию топологии сети;
- возможность защиты каналов управления и мониторинга пограничными маршрутизаторами из защищённых областей;
- создание и поддержку баз регистрационных данных с осуществлением процедур автоматического поиска по заданным условиям для анализа, защищаемых по доступу к ним на персональных электронных ТМ-идентификаторах;
- учет и регистрацию действий администраторов и различных параметров работы абонентов, включая попытки нарушения правил фильтрации, в базе данных, организованной без возможности удаления регистрационных данных с целью предотвращения их несанкционированного изъятия;
- обеспечение защиты от несанкционированного доступа при работе администратора

«ФПСУ-IP» посредством идентификации по защищенному от дублирования уникальному идентификатору и содержимому памяти электронного ТМ-идентификатора, а также аутентификации по паролю;

- разделение прав на доступ к работе «ФПСУ-IP» для различных классов администраторов (как локальных, так и удалённых);
- регистрацию, учет и возможность проверки корректности электронных ТМ-идентификаторов администраторов различных классов, посредством которых возможен доступ к комплексу;
- регистрацию и учёт прикреплённых к «ФПСУ-IP» пользователей «ФПСУ-IP/Клиент»;
- функционирование комплекса с использованием собственной защищенной операционной среды, что обеспечивает защиту регистрационной информации и автоматический контроль целостности исполняемых модулей, исключающий их несанкционированную модификацию и внедрение разрушающих программных воздействий; кроме того, возможна выдача контрольных значений всех исполнимых модулей подсистем инсталлированного комплекса с целью сравнения их с контрольными данными;
- защиту от несанкционированного доступа при работе удалённого администратора методами, устойчивыми к активному перехвату информации в сети посредством двусторонней аутентификации на основе взаимно зарегистрированных открытых ключах, а также защиту от НСД самой подсистемы удалённого администрирования посредством аутентификации администратора по паролю и возможности блокирования работы до введения пароля;
- локальную и дистанционную, с программируемой реакцией, сигнализацию нарушений правил фильтрации и изменения правил фильтрации администраторами;
- регистрацию, учет и контроль удаленных администраторов, имеющих доступ к «ФПСУ-IP», с назначаемыми правами на доступ;
- графический интерфейс для визуального контроля состояния и дистанционного управления всеми зарегистрированными удалёнными «ФПСУ-IP» с программируемой реакцией на возникающие на них события;
- автоматический мониторинг состояния удаленных «ФПСУ-IP» с автоматическим анализом регистрационной информации и программируемой реакцией результатов анализа.

Применение всех указанных механизмов защиты позволяет предотвратить множество распространённых в сети Интернет пассивных и активных атак злоумышленников, наиболее опасными из которых являются:

- непосредственное считывание трафика сети или «прослушивание», что легко

реализуется практически на любом пакетном коммутаторе с использованием его собственных средств трассировки и анализа проходящего через него трафика или с использованием специальной аппаратуры, подключаемой к линии;

- выяснение топологии сети и наличия в ней средств защиты посредством использования стандартных команд типа traceroute или других средств (широко распространённых в Интернет) с целью определения местоположения важных хостов, на которые в последующем могут производиться другие атаки;
- блокирование работы особо важных узлов сети путём выдачи на них большого количества ненужных пакетов, приводящее к переполнению входной очереди интерфейса и попаданию большинства систем в состояние перегрузки, при котором приём и дальнейшая передача пакетов не могут осуществляться в течение длительного времени. При этом злоумышленник постоянно поддерживает атакуемый узел в нерабочем состоянии;
- SYN-атаки на TCP, блокирующие TCP-модули, реализующиеся через подачу большого количества SYN-пакетов на входной интерфейс хоста. При этом системы, имеющие виртуальные менеджеры памяти, отображаемые на диск, входят в состояние «резонанса» - запрос на выделение памяти под соединение TCP приводит к бесконечному перераспределению памяти, занимающее все ресурсы ЦПУ;
- перехват TCP-соединений с другими абонентами с целью получения доступа, минуя средства защиты, используемый вместе с атаками, позволяющими блокировать работу одного из абонентов;
- атаки, основанные на ошибках реализации конкретных протоколов IP-стека.

Программное обеспечение «ФПСУ-IP» разработано ООО «АМИКОН», лицензия Федеральной службы безопасности Российской Федерации № 122531 П от 08 июня 2012 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических), информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя); лицензии Федеральной службы по техническому и экспортному контролю №0307 от 21 ноября 2006 г., №0536 от 21 ноября 2006 г: на деятельность по разработке и(или) производству средств защиты конфиденциальной информации; на

деятельность по технической защите конфиденциальной информации).

3. Общие принципы функционирования «ФПСУ-IP»

Программно-аппаратный комплекс «ФПСУ-IP» версии 3 является центральным элементом семейства средств защиты информации «ФПСУ-IP».

Функциональные возможности «ФПСУ-IP» по защите от НСД могут быть расширены следующими отдельными изделиями:

- программно-аппаратным комплексом «Удаленный администратор «ФПСУ-IP», предназначенным для централизованного дистанционного контроля и управления комплексами «ФПСУ-IP»;
- программно-аппаратным комплексом «Центр выработки ключей «ФПСУ-IP», предназначенным для выработки ключевой информации парно-выборочной связи, применяемых «ФПСУ-IP» для взаимных идентификации и аутентификации, а также для построения между «ФПСУ-IP» криптографически защищенных VPN-туннелей поверх глобальных сетей;
- программными и программно-аппаратными комплексами семейства «ФПСУ-IP/Клиент», выполняющих роль VPN-клиентов для выступающего VPN-шлюзом «ФПСУ-IP». «ФПСУ-IP/Клиенты» устанавливаются на отдельные устройства для защиты их подключений к защищенной «ФПСУ-IP» локальной сети;
- программой «Центр генерации ключей ФПСУ-IP/Клиентов», предназначенной для создания ключевых систем защиты обмена данными между пользователями «ФПСУ-IP/Клиент» и «ФПСУ-IP».

3. 1. Программно-аппаратный комплекс «ФПСУ-IP»

Программно-аппаратный «ФПСУ-IP» **аппаратно подключается в разрыв цепи** между защищаемой областью и остальной частью локальной сети парой физических линий (одна к защищаемой области, другая к остальной сети) таким образом, чтобы все входящие и исходящие из области потоки данных проходили через «ФПСУ-IP». Если область связана с сетью более чем в одной точке (транзитная область), «ФПСУ-IP» должны быть установлены на каждом выходе из неё.

Вследствие поддержки программным обеспечением «ФПСУ-IP» 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.

Основная функция «ФПСУ-IP» заключается в том, что в соответствии с установленными администратором правилами он анализирует входящие и исходящие пакеты данных IP-протокола по совокупности критериев, осуществляет контроль доступа к

ресурсам сети и определяет возможность передачи данных.

На начальном этапе анализа все пакеты, поступающие на каждый из интерфейсов «ФПСУ-IP», 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-IP».

Фильтрация пакетов IP-протокола, производимая «ФПСУ-IP», 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.

«ФПСУ IP» сертифицирован в Системе сертификации средств защиты информации по требованиям безопасности информации (свидетельство № РОСС RU.0001.01БИ00) и имеет сертификат соответствия № 4269 (выдан ФСТЭК России 6 ноября 2020 года, действителен до 6 ноября 2025 года).

Применяемый «ФПСУ-IP» 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 несколько вариантов применения «ФПСУ-IP» (функциональные схемы приведены ниже) и различные режимы его работы.

В простейшем случае обмен IP-пакетами абонентов сегмента ЛВС с другими абонентами может осуществляться через один «ФПСУ-IP» (см. рисунок ниже). Для оконечной области достаточно установить один «ФПСУ-IP» на выходе из неё, для транзитной области необходимо защитить «ФПСУ-IP» каждый выход.

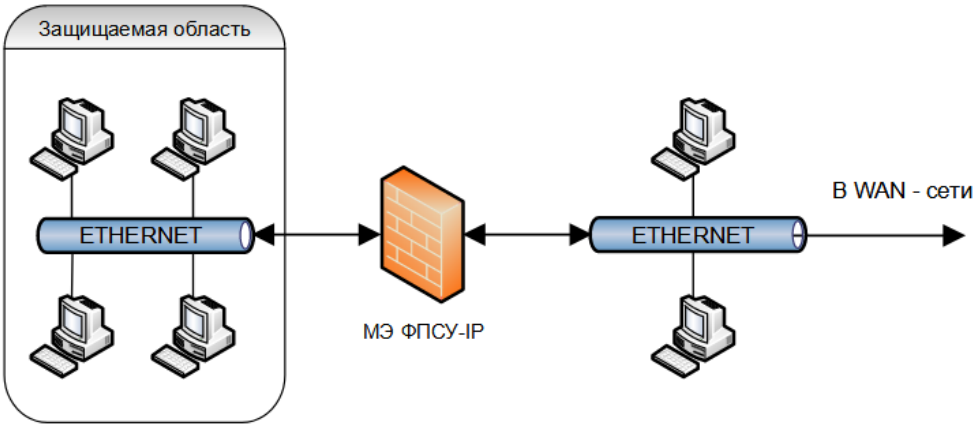

Рисунок 1 - Функциональная схема использования одного «ФПСУ-IP» для защиты оконечной области

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-IP» 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-IP» на выходе из локальной сети в удалённые сети и защитить работу всей локальной сети.

Если обмен пакетами абонентов будет производиться через один «ФПСУ-IP», 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-IP», работающих в паре (см. рисунок ниже). 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, шифрования и туннелирования.

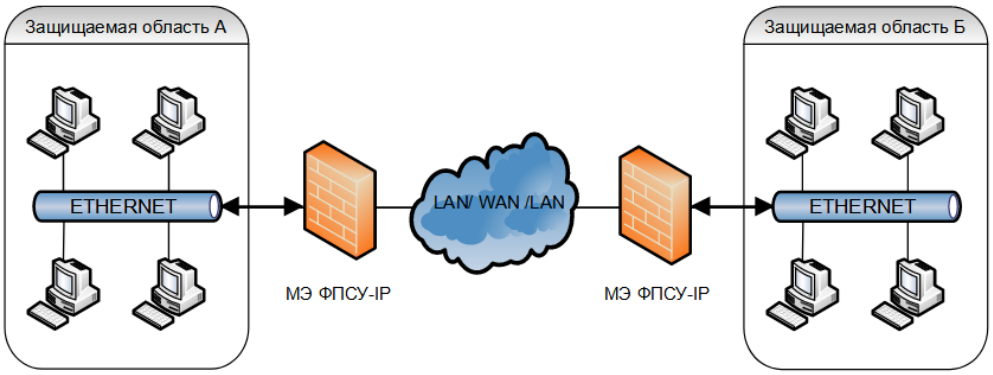

Рисунок 2 - Функциональная схема использования двух «ФПСУ-IP», работающих в паре

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-IP» 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 удалённый «ФПСУ-IP».
- На «ФПСУ-IP», 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-IP», работающим в «каскадном» режиме с первым, причём на втором «ФПСУ-IP» 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-IP» 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-IP» будет фильтровать пакеты только по IP-адресам.

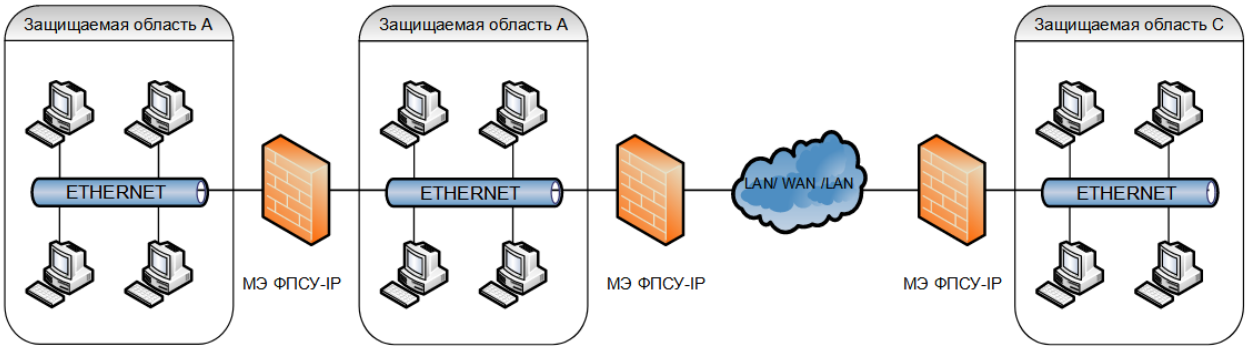

Рисунок 3 - Каскадная установка двух «ФПСУ-IP» в защищаемой области

Защитные функции «ФПСУ-IP» накладывают некоторые ограничения на используемые абонентами стандарты стека протоколов Интернет. «ФПСУ-IP» не отвечает на запросы абонентов и сервисных служб, направленные в его собственный адрес (за исключением специально регламентированных запросов ICMP Ping), а также игнорирует IP-опции, требующие вставить при отправке пакета IP-адрес транзитной машины. Если в заголовке IP-пакета содержится фиксированный маршрут, по которому должен следовать пакет, в соответствии с установками администратора такая опция может быть выполнена, очищена (пакет проследует по маршруту, который предусмотрел для него администратор) или пакет может быть сброшен. Кроме того, «ФПСУ-IP» позволяет скрывать свои защитные и фильтрующие свойства, в случае чего выдача ICMP-сообщений об ошибке по причинам нарушения правил фильтрации подавляется, а посылка других ICMP-сообщений производится от имени абонента-получателя пакета. Включение этого переключателя влечёт за собой также запрещение передачи через «ФПСУ-IP» пакетов других станций, содержащих ICMP-сообщения об истечении времени жизни дейтаграмм, что позволяет скрывать топологию сети.

«ФПСУ-IP» поддерживает такое расширение стандарта IP, как широковещательные передачи, направленные в IP-подсети. Широковещательные передачи всем сетям (с IP-адресом 255.255.255.255) не поддерживаются. Чтобы иметь возможность передавать и получать широковещательные пакеты, направленные в конкретные подсети IP, данные подсети должны быть явно «прописаны» в конфигурации портов.

«ФПСУ-IP» 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-IP» 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-IP» в режиме «клиент/сервер», посылая запрос на доступ, который производится «ФПСУ-IP» только после идентификации и аутентификации. Для передачи данных между «ФПСУ-IP/Клиентом» и «ФПСУ-IP» организуется защищённый межсетевой туннель, в котором производится шифрование информации и (опционально) сжатие.

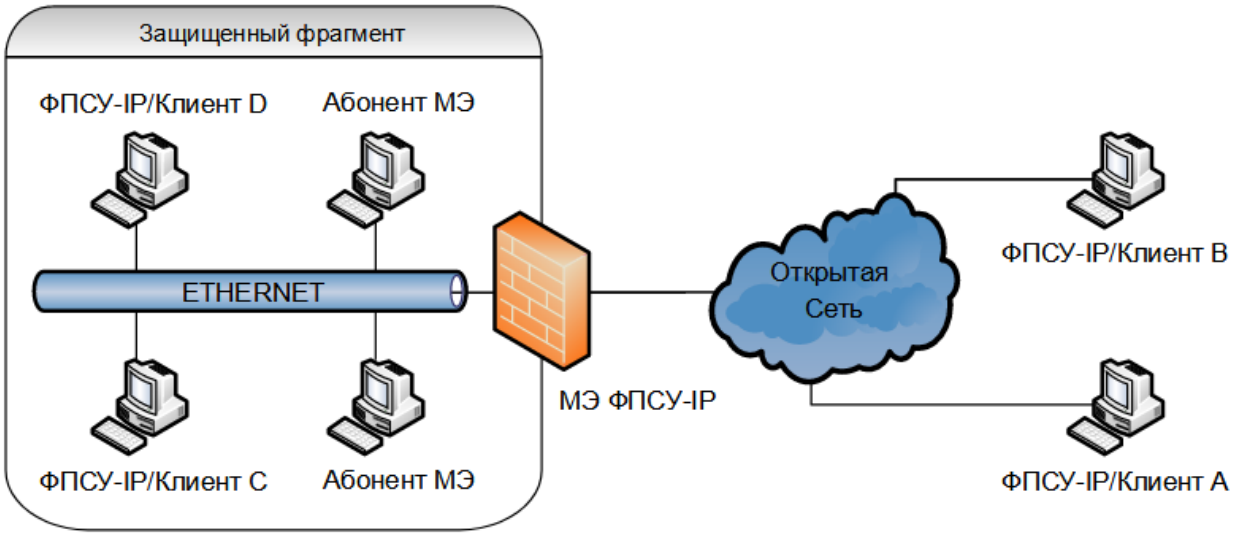

Рисунок 4 - Схема некоторых вариантов применения «ФПСУ-IP» для организации безопасного взаимодействия рабочих станций, оборудованных «ФПСУ IP/Клиент»

На схеме (см. рисунок ниже), «ФПСУ-IP» обеспечивает пользователям «ФПСУ-IP/Клиентов» A и B безопасный доступ к абонентам защищаемой им подсети. Взаимодействуя через «ФПСУ-IP» 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-IP» с «ФПСУ-IP/Клиентами» C и D.

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-IP» рабочим станциям может быть реализован с произвольной рабочей станции, оборудованной «ФПСУ-IP/Клиентом» (более

подробную информацию см. в руководстве пользователя «ФПСУ-IP/Клиента»).

«ФПСУ-IP» имеет средства защиты от вмешательства в логику его работы, а также защиты его информационной и программной частей от несанкционированного доступа. Компьютер, оборудованный «ФПСУ-IP», не может содержать постороннего программного обеспечения.

Специальная подсистема «ФПСУ-IP» создает на компьютере собственную (изолированную и функционально замкнутую) программную среду, предоставляя администраторам возможность управлять его работой - конфигурировать его (устанавливать и редактировать правила фильтрации, настраивать «ФПСУ-IP» на параметры сетевого оборудования, подключать желаемое оборудование и специальное программное обеспечение и т.д.), а также просматривать и записывать на съемные носители регистрационную информацию.

«ФПСУ-IP» осуществляет и разграничивает доступ к своим модулям и подсистемам администраторов по правам.

Локальные администраторы делятся по правам доступа на четыре логических класса: *«оператор», «инженер», «администратор»* и *«Главный администратор»*, для каждого из которых строго определяется область доступных действий. Например, администратор класса *«оператор»* имеет право только запустить «ФПСУ-IP», остальные операции по конфигурации и управлению «ФПСУ-IP» будут ему недоступны. Идентификация и аутентификация администраторов с соответствующими правами осуществляется с использованием электронных идентификаторов touch-memory и символьного пароля. В «ФПСУ-IP» реализован механизм регистрации и учета ТМ-идентификаторов.

При работе «ФПСУ-IP» 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 УА ФПСУ-IP для последующего хранения или анализа.

«ФПСУ-IP» 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-IP» с полномочиями «Администратор».

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

- настройки на «ФПСУ-IP» подсистемы удаленного управления и контроля;
- использования программно-аппаратного комплекса «Удалённый администратор ФПСУ-IP».

Доступ к «ФПСУ-IP» могут получить до тридцати двух (32) различных удалённых администраторов, зарегистрированных на этом «ФПСУ-IP» локальным администратором с фиксированным набором прав на контроль и управление данным «ФПСУ-IP».

3. 2. Программно-аппаратный комплекс «Центр выработки ключей»

Программно-аппаратный комплекс «Центр выработки ключей» и предназначен для выработки ключей парно-выборочной связи, используемых «ФПСУ-IP» для организации между собой VPN-туннелей и применяемых ими в процессе взаимных стартовых идентификации и аутентификации, а также для обмена сеансовыми ключами преобразования передаваемой информации.

Каждому экземпляру ЦВК при изготовлении присваивается уникальное имя, которое идентифицирует конкретную виртуальную частную сеть (Криптосеть).

Так же, как и «ФПСУ-IP», ЦВК имеет средства защиты от вмешательства в логику его работы, а также защиты его информационной и программной частей от несанкционированного доступа. Компьютер, оборудованный ЦВК, не может содержать постороннего программного обеспечения.

Специальная подсистема ЦВК создает на компьютере собственную (изолированную и функционально замкнутую) программную среду, предоставляя администраторам возможность управлять его работой.

Выработка ключей парно-выборочной связи осуществляется в два этапа:

1. Формирование системной таблицы (серии) ключей. Серия ключей вырабатывается на ограниченный период времени, определяемый требованиями по защите информации. Размерность системной таблицы ключей определяется администратором по количеству существующих и предполагаемых к

использованию «ФПСУ-IP», образующих VPN-сеть (группу). Хранение сформированной серии осуществляется на внутреннем накопителе данных ПЭВМ ЦВК в зашифрованном виде на ключе, который выдаётся ЦВК в файл на внешний носитель (USB-flash) или ТМ-идентификатор, без предъявления которого доступ к системной таблице ключей не предоставляется.

2. Выдача ключей парно-выборочной связи для каждого «ФПСУ-IP» на внешние носители. Для каждого «ФПСУ-IP» ЦВК изготавливает комплект ключей. Ключи выдаются на внешние носители (USB-flash).

Выработанные ключи парно-выборочной связи могут быть установлены на «ФПСУ-IP» как локальными, так и удалёнными администраторами «ФПСУ-IP», имеющими соответствующие права.

Работа с ключами должна осуществляться под контролем специально уполномоченного лица - Администратора безопасности «ФПСУ-IP», функциями которого являются учёт и установка ключей на внутренний накопитель данных «ФПСУ-IP», настройка «ФПСУ-IP» на использование действующих ключей, плановая замена и уничтожение старых ключей, а также обеспечение защиты действующих и старых ключей от компрометации.

Надежность защиты от НСД и подлинность передаваемой через «ФПСУ-IP» информации обеспечиваются только при условии сохранности от компрометации (утраты, временной потери контроля, несанкционированного доступа, копирования, подделки и т.п.) действующих ключей парно-выборочной связи.

3. 3. Удаленный администратор ФПСУ-IP

Программный комплекс «Удаленный администратор «ФПСУ-IP» состоит из программного обеспечения «Удаленный администратор «ФПСУ-IP» и специального устройства «VPN-Key/UA».

УА ФПСУ-IP позволяет осуществлять централизованное дистанционное управление работой группы (до 32000) комплексов «ФПСУ-IP» и контроль их функционирования с рабочей станции.

Каждый «ФПСУ-IP» допускает управление и контроль со стороны тридцати двух (32) удалённых администраторов, причём каждый из администраторов может иметь исключительные права на осуществление отдельных операций по дистанционному управлению.

Главный принцип защищенного дистанционного администрирования «ФПСУ-IP» -

обеспечение взаимной идентификации и строгой двухсторонней аутентификации «ФПСУ-IP» и УА ФПСУ-IP. Для этого «ФПСУ-IP» и УА ФПСУ-IP должны быть взаимно зарегистрированы, т.е. каждый УА ФПСУ-IP должен зарегистрировать свои «ФПСУ-IP» и сам быть зарегистрированным этими «ФПСУ-IP», получив при регистрации от локальных администраторов «ФПСУ-IP» конкретные полномочия.

Каждый УА ФПСУ-IP должен иметь уникальное имя (задается пользователем УА ФПСУ-IP), контролируемое «ФПСУ-IP» в процессе регистрации удаленного администратора. «ФПСУ-IP» регистрируются на УА ФПСУ-IP по уникальному серийному номеру. Регистрация производится путём обмена открытыми ключами, вырабатываемыми самостоятельно каждой из регистрируемых сторон. Впоследствии эти данные используются в процессе обращения удалённого администратора к «ФПСУ-IP» с целью обеспечения взаимной идентификации и двухсторонней аутентификации, кроме того, они могут быть использованы УА ФПСУ-IP для установки режима идентификации администратора при запуске и для немедленного восстановления работы администратора после аварий внутреннего накопителя данных компьютера удаленного администратора.

УА ФПСУ-IP предоставляет пользователю (при наличии зарегистрированных полномочий) следующие возможности:

- регистрация новых «ФПСУ-IP» в программе УА ФПСУ-IP, или удаление их из списка зарегистрированных «ФПСУ-IP»;
- внесение изменений в ранее установленные данные «ФПСУ-IP»;
- ограничение или запрет доступа к работе с УА ФПСУ-IP другим лицам;
- запрос, получение (как по сети, так и посредством передачи на носителе), просмотр и анализ конфигурации и правил фильтрации, установленных на подконтрольных «ФПСУ-IP»;
- согласованное изменение и установка (как по сети, так и посредством передачи на носителе) правил фильтрации для группы подконтрольных «ФПСУ-IP» и режимов их работы, причём изменения конфигурации «ФПСУ-IP» могут войти в силу как немедленно, так и в указываемый удаленным администратором момент времени;
- синхронизация времени на подконтрольных «ФПСУ-IP» с текущим временем рабочей станции, на которой функционирует УА ФПСУ-IP, как в автоматическом, так и в ручном режимах;
- запрос, получение, просмотр, анализ и обработка указанной по виду и времени регистрационной информации о событиях на подконтрольных «ФПСУ-IP» как в автоматическом режиме с заданным периодом времени, так и в режиме непосредственного обращения;
- автоматический мониторинг состояния «ФПСУ-IP»;
- программирование автоматического анализа получаемой мониторинговой

информации с оперативно отображаемой графической и многоуровневой звуковой сигнализацией событий по попыткам нарушения правил фильтрации, изменению самих правил фильтрации, изменению даты и времени, установке дополнительного или изменению установленного программного обеспечения, перезагрузке подсистемы фильтрации и т.д.;

- дистанционная установка ключей парно выборочной связи, применяемых «ФПСУ-IP» для создания VPN-туннелей друг с другом;
- дистанционная установка общесистемных ключей «ФПСУ-IP/Клиентов», применяемых при создании VPN-туннелей между «ФПСУ-IP/Клиентами» и «ФПСУ-IP»;
- регистрация и изменение параметров работы «ФПСУ-IP/Клиентов» с «ФПСУ-IP»;
- дистанционная установка дополнительного программного обеспечения (различных опциональных утилит) «ФПСУ-IP» или замена существующего программного обеспечения (в частности, дистанционное обновление установленных программных модулей);
- непосредственный дистанционный контроль за процессами фильтрации, приема/передачи пакетов и данных, идентификации и аутентификации «ФПСУ-IP/Клиентов», удалённых «ФПСУ-IP» и удалённых администраторов.

Права удалённых администраторов на доступ к подсистемам «ФПСУ-IP» устанавливает локальный администратор «ФПСУ-IP» при регистрации на нём удаленного администратора.

Всем зарегистрированным на «ФПСУ-IP» удалённым администраторам автоматически предоставляется право на опрос текущего состояния «ФПСУ-IP» (мониторинг) и получение данных о работе его абонентов и «ФПСУ-IP/Клиентов». Кроме того, при соответствующих указаниях локального администратора любому из удаленных администраторов может быть предоставлена возможность контролировать работу локальных и других удалённых администраторов этого «ФПСУ-IP», а также право на чтение и изменение конфигурации «ФПСУ-IP».

Право на согласование времени УА ФПСУ-IP и «ФПСУ-IP» может быть выдано лишь одному из зарегистрированных удаленных администраторов.

В подсистеме УА ФПСУ-IP реализованы следующие механизмы защиты от НСД программной и информационной частей:

- идентификация и аутентификация удалённого администратора при запуске УА ФПСУ-IP;
- защита работы УА ФПСУ-IP путем блокировки любых действий до введения пароля;

- создание и поддержка баз регистрационных данных с осуществлением автоматического поиска их по заданным условиям для анализа;
- обеспечение и контроль целостности программных модулей и баз данных накопленной регистрационной информации на ПЗУ компьютера.

При установлении соединения между «ФПСУ-IP» и УА ФПСУ-IP используется открытый ключ администратора УА ФПСУ-IP. Закрытый ключ уникален для каждого пользователя УА ФПСУ-IP и хранится в USB-устройстве «VPN-Key/UA» для УА ФПСУ-IP.

Без подключенного к USB-порту компьютера устройства «VPN-Key/UA», в котором хранится ключ УА, запуск УА ФПСУ-IP и управление ФПСУ-IP невозможны.

При извлечении устройства «VPN-Key/UA» из USB-порта рабочей станции интерфейс УА ФПСУ-IP становится недоступен пользователю. Таким образом, USB-устройство «VPN-Key/UA» является необходимым для эксплуатации УА ФПСУ-IP физическим ключом, основным средством идентификации и аутентификации администратора УА ФПСУ-IP при запуске и работе с УА ФПСУ-IP.

Ключ УА может быть выдан из «VPN-Key/UA» и записан на специальный носитель, который должна храниться в недоступном посторонним лицам месте. Это позволяет оперативно восстанавливать работу УА ФПСУ-IP (без перерегистрации со всеми подконтрольными «ФПСУ-IP») при авариях внутреннего накопителя или других отказах аппаратуры компьютера, требующих переустановки программного обеспечения.

Удалённый администратор «ФПСУ-IP» имеет возможность осуществить дополнительный контроль целостности ПО УА ФПСУ-IP посредством использования специальной программы контроля целостности программных модулей с использованием нелинейного алгоритма расчета - вычислением значения их хэш-функций и сравнения результатов с априорно известными контрольными данными.

УА ФПСУ-IP может сохранять свои рабочие установки в специальном архиве резервной копии, что позволяет быстро восстанавливать его работу после аварий и сбоев внутреннего накопителя без повторной настройки.

3. 3. 1. Мониторинг событий на «ФПСУ-IP»

УА ФПСУ-IP в том числе предназначен для накопления и отображения информации о состоянии зарегистрированных «ФПСУ-IP», а также для автоматического анализа этой информации с целью оповещения администратора о наступлении на «ФПСУ-IP» ряда событий. Реакция УА ФПСУ-IP на случившееся событие может включать в себя вывод на экран сигнала графического отображения, звуковую сигнализацию (каждому типу события может быть присвоен уникальный звуковой сигнал), отправление оповещения на указанный

адрес электронной почты, вызов другой программы (указывается путь к исполняемому файлу).

Мониторинг событий на «ФПСУ-IP» может осуществляться как автоматически с установленными администратором при регистрации частотами опроса, так и в режиме непосредственного получения информации по запросу администратора. Право на опрос состояния «ФПСУ-IP» автоматически предоставляется всем зарегистрированным на нём администраторам.

Модуль мониторинга предоставляет администратору следующие возможности:

- графическое отображение информации, о случившихся на «ФПСУ-IP» событиях;
- быстрый выбор требуемого для контроля или управления «ФПСУ-IP»;
- немедленное получение информации о состоянии выбранного «ФПСУ-IP»;
- быстрый переход в режим сетевого соединения с выбранным «ФПСУ-IP» для осуществления доступных удалённому администратору действий по контролю и управлению «ФПСУ-IP»;
- получение информации об IP-адресе «ФПСУ-IP»;
- получении информации о версии ПО «ФПСУ-IP»;
- получение информации о состоянии VPN-туннеля с данным «ФПСУ-IP» в момент последнего обращения к нему УА ФПСУ-IP;
- программирование отклика на ряд событий (выбор их из предлагаемого списка), на которые требуется немедленная реакция администратора, для графической, звуковой сигнализации (возможность выбора для каждого события своего звукового сигнала).

Информация, отображаемая графически на экране монитора для всех «ФПСУ-IP», включает:

- информацию о текущем состоянии зарегистрированных «ФПСУ-IP»: были ли они опрошены и работают ли в текущий момент времени;
- графическое отображение (и звуковую сигнализацию) запрограммированных администратором оперативных сообщений о некоторых событиях, произошедших на «ФПСУ-IP».

При вызове соответствующих информационных окон для каждого из подконтрольных «ФПСУ-IP» пользователь УА ФПСУ-IP может получить следующие данные:

- разницу в показаниях системных часов «ФПСУ-IP» и УА ФПСУ-IP;
- время последнего опроса «ФПСУ-IP» подсистемой мониторинга;
- накопленную с определённого времени информацию по зарегистрированным на данном «ФПСУ-IP» событиям: количество изменений его конфигурации (как

локальными, так и удалёнными администраторами), количество запусков подсистемы фильтрации, количество дистанционных установок данных аутентификации, количество изменений времени (как в автоматическом режиме, так и по приказу удалённого администратора), количество установок дополнений/изменений к ПО и номер текущей версии ПО;

- накопленную с определённого времени информацию о состоянии портов «ФПСУ-IP»: тип подключённых к портам линий связи, состояние линий на момент последнего опроса, скорость передачи данных по линиям на момент последнего опроса, время последних приёма и передачи данных по каждой линии, количество принятых и переданных данных в байтах и IP-пакетах по каждой линии, количество отказов в передаче пакета и количество нарушений правил фильтрации по каждой линии.
- информацию по текущей работе «ФПСУ-IP», получаемую в режиме непосредственного соединения: по состоянию его VPN-туннелей с другими «ФПСУ-IP», по состоянию работы абонентов и «ФПСУ-IP/Клиентов» через данный «ФПСУ-IP», по состоянию портов комплекса и его ARP-таблиц, по работе удалённых администраторов, а также данные об обновлениях ПО «ФПСУ-IP» и текущем проценте загрузки ЦПУ;
- информацию о произошедших в подсистеме удалённого администрирования событиях с указанием даты, времени и вида операции.

Администратор может запрограммировать оперативную графическую и звуковую реакцию УА ФПСУ-IP на большой список событий подконтрольных «ФПСУ-IP» (соответствующие временные и количественные параметры также задаются администратором), в том числе:

- перезапуск подсистемы фильтрации «ФПСУ-IP»;
- нарушение правил фильтрации как для индивидуальных IP-пакетов, так и для широковещательных передач;
- изменение конфигурации как локальными, так и удаленными администраторами;
- дистанционная установка данных аутентификации;
- дистанционное изменение времени вручную или в результате автокоррекции;
- установка изменений/дополнений к ПО.

Подробные сведения по использованию мониторинга и описание интерфейса содержатся в руководстве удаленного администратора «ФПСУ-IP».

3. 3. 2. Получение регистрационной информации «ФПСУ-IP»

УА ФПСУ-IP позволяет просматривать и обрабатывать статистическую информацию о работе подконтрольных «ФПСУ-IP». Статистическая информация может поступать в

хранилище удалённого администратора следующими способами:

- в процессе автоматического опроса «ФПСУ-IP»;
- в режиме непосредственного соединения по сети;
- с носителей, на которые она была записана локальными администраторами «ФПСУ-IP» (такой способ передачи регистрационной информации может быть использован при неполадках в работе сети и невозможности непосредственного опроса «ФПСУ-IP», а также при подозрении на утечку данных);
- из архива статистики УА ФПСУ-IP.

УА ФПСУ-IP может получать следующую информацию:

- о соединениях абонентов и «ФПСУ-IP/Клиентов» через «ФПСУ-IP» (передача данных абонентов в открытом виде и через VPN-туннель, ошибки при передаче данных абонентов и «ФПСУ-IP/Клиентов», отказ абонентам в доступе, отказ «ФПСУ-IP/Клиентам» в соединении, отсутствие связи с абонентами, соединения и разъединения «ФПСУ-IP/Клиентов» с «ФПСУ-IP», обмен данными между «ФПСУ-IP/Клиентами» и абонентами, статистика передачи данных за сутки);
- о работе локальных администраторов (запуск «ФПСУ-IP», начало и окончание работы «ФПСУ-IP», регистрация новых локальных администраторов (TM-идентификаторов) и их удаление, изменение общих параметров конфигурации «ФПСУ-IP» и правил фильтрации, смена ключей парно-выборочной связи, установка изменений или дополнений к программному обеспечению «ФПСУ-IP», регистрация удалённых администраторов и т.д.);
- о работе других удалённых администраторов (получение ими статистических данных и правил фильтрации комплексов, изменение текущего времени на «ФПСУ-IP», дистанционная установка изменений или дополнений к программному обеспечению и т.д.).

Статистические записи предоставляются администратору с указанием времени и даты события, вида события, адресов и идентификаторов абонентов, «ФПСУ-IP/Клиентов» и администраторов, а также объёма передаваемой информации и других необходимых данных.

Статистическая информация о работе абонентов и «ФПСУ-IP/Клиентов» предоставляется любому зарегистрированному этим «ФПСУ-IP» администратору.

Данные о работе локальных и удалённых администраторов может получить только удалённый администратор, которому такое право предоставлено локальным администратором «ФПСУ-IP» специально.

После загрузки статистики в базу данных удаленный администратор «ФПСУ-IP»

может:

- просмотреть данные статистики; данные для просмотра могут быть выбраны подсистемой администрирования по требуемым «ФПСУ-IP», за указанный период времени, а также по заданным видам данных статистики;
- выдать просматриваемые данные в файл для обработки и/или печати средствами какого-либо текстового редактора;
- упаковать регистрационную информацию средствами УА ФПСУ-IP в архивные файлы во избежание переполнения хранилища и/или потери информации при возможных авариях внутреннего накопителя данных.

3. 4. Программные и программно-аппаратные комплексы «ФПСУ IP/Клиент»

Программно-аппаратный комплекс «ФПСУ-IP/Клиент» состоит из интеллектуального электронного устройства «VPN-Key/Client», подключаемого к USB-порту рабочей станции пользователя, и программных модулей «ФПСУ-IP/Клиент», устанавливаемых в операционную систему ПЭВМ.

Программные комплексы «ФПСУ-IP/Клиент» состоят только из программных модулей, устанавливаемых в операционную систему устройства.

В качестве программно-аппаратного комплекса могут выступать «ФПСУ-IP/Клиенты» для операционных систем Windows, Linux и macOS.

«ФПСУ-IP/Клиент» предназначен для построения защищённых каналов связи между рабочими станциями и «ФПСУ-IP». Кроме того, «ФПСУ-IP/Клиент» для операционных систем Windows, Linux и macOS может выполнять функции сетевого фильтра, принимая и передавая сетевые пакеты в соответствии с задаваемыми правилами фильтрации.

Механизм защиты канала связи заключается в том, что между Клиентом и «ФПСУ-IP» создаётся VPN-туннель, по которому IP-пакеты передаются в криптографически защищенном виде, что обеспечивает достоверность, целостность и конфиденциальность передаваемой информации.

В VPN-туннеле производятся обязательные взаимные процедуры идентификации и аутентификации взаимодействующих «ФПСУ-IP/Клиента» и «ФПСУ-IP», как при установлении защищённого соединения, так и в процессе приёма данных из VPN-туннеля.

Для установления соединения «ФПСУ-IP/Клиент» обращается к «ФПСУ-IP» на порт получателя UDP 87. Порт отправителя UDP-соединению динамически назначает операционная система рабочей станции, на которую установлен «ФПСУ-IP/Клиент».

Устройство «VPN-Key/Client» обеспечивает хранение ключей программно-аппаратных «ФПСУ-IP/Клиентов» и идентификаторов пользователя, выработку данных необходимых для взаимной аутентификации «ФПСУ-IP/Клиент» и «ФПСУ-IP» и создания сессионных (сеансовых) ключей, хранение конфигурационных данных.

«ФПСУ-IP/Клиент» обеспечивает:

- фильтрацию каждого сетевого пакета на основе IP-адреса получателя в соответствии с установленными администратором правилами (опционально);
- фильтрацию каждого сетевого пакета на основе проверки корректности заполнения и взаимной согласованности значимых полей IP-пакетов в соответствии с рекомендациями RFC;
- фильтрацию каждого сетевого пакета с учетом входного и выходного сетевого интерфейса «ФПСУ-IP» как средство проверки подлинности сетевых адресов;
- фильтрацию пакетов на основе установленных администратором режимов работы и взаимодействия абонентов (опционально);
- построение VPN-туннеля между «ФПСУ-IP» и «ФПСУ-IP/Клиентом»;
- сжатие передаваемых по межсетевым туннелям данных (опционально);
- шифрование передаваемых в межсетевых туннелях данных;
- контроль целостности программной и информационной частей «ФПСУ-IP/Клиент»;
- идентификацию и аутентификацию пользователя/администратора на этапе запуска «ФПСУ-IP/Клиент» и в процессе доступа к средствам локального администрирования;
- разграничение доступа в соответствии с установленными правами для различных классов пользователей;
- блокирование доступа пользователей, подлинность которых при аутентификации не подтвердилась.

3. 5. Центр генерации ключей ФПСУ-IP/Клиентов

Ключевые системы защиты обмена данными между «ФПСУ-IP/Клиентами» и «ФПСУ-IP» создаются при помощи специальной программы «Центр генерации ключей ФПСУ-IP/Клиентов» (далее ЦГКК). В них формируются ключевые данные и организационная структура создаваемой VPN-сети класса клиент-сервер, называемой «Криптосетью Клиентов».

Каждая Криптосеть Клиентов, созданная при помощи ЦГКК, предназначается для обслуживания ограниченного числа пользователей. Криптосеть Клиентов имеет собственное имя и уникальный номер, характеризующие данную Криптосеть Клиентов, а также определённый срок действия (эти параметры фиксируются в специальном файле-

лицензии, поставляемом вместе с программой).

Функциями ЦГКК являются:

- генерация и запись на ТМ-идентификатор общесистемного ключа Криптосети Клиентов, предназначенного для установки на «ФПСУ-IP»;
- создание логической структуры Криптосети Клиентов;
- генерация ключей пользователей Клиентов и запись их на устройства «VPN-Key/Client».

Более подробную информацию можно найти в руководстве по применению Центра генерации ключей ФПСУ-IP/Клиентов.

4. Лицензирование

4. 1. Лицензирование программно-аппаратных комплексов «ФПСУ-IP» версии 3

Программное обеспечение «Программно-аппаратный комплекс «ФПСУ-IP» версии 3» лицензируется в зависимости от способа инсталляции и использования – на специализированных аппаратных платформах ООО «АМИКОН» различных модификаций или на платформах виртуализации (гипервизорах), а также в зависимости от доступного к использованию в базовой поставке функционала. Дистрибутив на материальном носителе (с актуальным на момент выдачи лицензии программным обеспечением) поставляется со встроенной базовой лицензией, дающей указанные в лицензии права и активирующей различный набор функций указанной на дистрибутивном носителе версии/подверсии/релиза программного обеспечения. Срок действия базовой лицензии не ограничен. Право устанавливать и использовать новые версии/подверсии/релизы ПО (выпущенные после даты предоставления лицензии) в течение указанного в базовой лицензии срока включено в стоимость этой лицензии. Срок установки обновлений, исправляющих критические уязвимости, не ограничивается (пока ООО «АМИКОН» осуществляет техническую поддержку и сопровождение поставленной версии/подверсии/релиза ПО).

По умолчанию ПО поставляется в нескольких фиксированных комплектациях:

- **Комплектация 1** – с лицензией на ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3» с правом инсталляции на аппаратной платформе ООО «АМИКОН» линейки **ORD** с одним активированным вычислительным потоком;
- **Комплектация 2** – с лицензией на ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3» с правом инсталляции на аппаратной платформе ООО «АМИКОН» линейки **STD** с одним активированным вычислительным потоком;
- **Комплектация** 3 – с лицензией на ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3» с правом инсталляции на аппаратной платформе ООО «АМИКОН» линейки **EXT** с одним активированным вычислительным потоком;
- **Комплектация 4** – с лицензией на ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3» с правом инсталляции на аппаратной платформе ООО «АМИКОН» линейки **ULT** с 16 активированными вычислительными потоками;
- **Комплектация 5** – с лицензией на ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3» с правом инсталляции на аппаратной платформе ООО «АМИКОН» линейки **ULT10G** с 56 активированными вычислительными потоками;
- **Комплектация 6** – с лицензией на ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3» с правом инсталляции на виртуальной платформе (гипервизоре) с одним активированным вычислительным потоком.

ООО «АМИКОН» оставляет за собой право по своему усмотрению менять набор базовых функций ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3». Для некоторых заказчиков могут согласовываться индивидуальные Комплектации базовых лицензий для ПО «Программно-аппаратного комплекса «ФПСУ-IP» версии 3».

Функциональность ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3» может быть расширена за счет приобретения дополнительных лицензий к базовой лицензии соответствующей комплектации. Расширения привязаны к конкретному серийному номеру базовой лицензии.

В состав ПО «Программно-аппаратного комплекс «ФПСУ-IP» версии 3» входят следующие опциональные модули:

- Расширение базовой лицензии «Модуль-агент активации сервера доступа и обслуживания комплексов «ФПСУ-IP/Клиент». Расширение дает право использовать указанный функционал на одном конкретном экземпляре базового ПО (с указанием или без его Комплектации);
- Расширение базовой лицензии «Модуль-агент активации определённого количества (указывается количество) подключений комплексов «ФПСУ-IP/Клиент». Расширение базовой лицензии дает право единовременно подключиться определенному в указанной лицензии количеству комплексов «ФПСУ-IP/Клиент», не использующих специализированный аппаратный ключ «VPN-Key/Client». Лицензия накопительная, дополнительное количество приобретенных соединений прибавляется к уже имеющемуся путем замещения старой лицензии на новую. Наличие расширения «Сервер доступа и обслуживания комплексов «ФПСУ-IP/Клиент» обязательно;
- Расширение базовой лицензии «Модуль-агент активации установки новых релизов программного обеспечения версии 3». Расширение дает право на установку и использование новых версий/подверсий/релизов программного обеспечения версии 3 на одном экземпляре базового ПО (с указанием или без его Комплектации). Расширение срочное, срок действия права ограничен периодом, указанным в лицензии;
- Расширение базовой лицензии «Модуль-агент активации дополнительного вычислительного потока». Расширение дает право задействовать в работе программного обеспечения указанное в лицензии количество вычислительных устройств (процессоров, ядер процессора, НТ-устройств). Лицензия накопительная, дополнительное количество приобретенных потоков прибавляется к уже имеющемуся путем замещения старой лицензии на новую;
- Расширение базовой лицензии «Модуль-агент активации криптопротокола FAST». Расширение дает право активировать указанный функционал на одном конкретном

экземпляре базового ПО (с указанием или без его Комплектации);

- Расширение базовой лицензии «Модуль-агент активации горячего резервирования». Расширение дает право активировать указанный функционал на одном конкретном экземпляре базового ПО (с указанием или без его Комплектации).

4. 2. Лицензирование «Удаленных администраторов «ФПСУ-IP»

Программное обеспечение «Удаленный администратор «ФПСУ-IP» поставляется с базовой лицензией, позволяющей запускать и использовать актуальную на момент выдачи лицензии версию/подверсию/релиз ПО и удаленно управлять указанным в лицензии количеством комплексов «ФПСУ-IP» (по умолчанию пятью). ООО «АМИКОН» оставляет за собой право по своему усмотрению изменять максимальное количество управляемых комплексов «ФПСУ-IP» в базовой лицензии.

Базовая лицензия может быть расширена за счет приобретения расширений лицензии на право управлять дополнительным количеством комплексов «ФПСУ-IP». Расширения привязаны к конкретному серийному номеру базовой лицензии и называются следующим образом:

«Расширение лицензии ПО «Удаленный администратор «ФПСУ-IP» с правом управлять дополнительным количеством (%*указывается количество*%) комплексов «ФПСУ-IP».

Все выданные расширения накопительные, лицензии суммируются к базовой лицензии.

Каждая **базовая лицензия** и **расширение лицензии** имеют следующие временные ограничения:

- индивидуальный срок действия (лицензия или расширение могут быть бессрочными);
- срок работы с новыми версиями ПО «Удаленный администратор «ФПСУ-IP» (выпущенными после даты предоставления лицензии).

По истечении любого из указанных сроков, пользователь может приобрести обновленную базовую лицензию или расширение.

4. 3. Лицензирование «Центров выработки ключей «ФПСУ-IP»

Программное обеспечение «Центр выработки ключей «ФПСУ-IP» лицензируется в зависимости от класса защищенности по классификации Федеральной Службы Безопасности России.

Дистрибутив ЦВК на материальном носителе поставляется со встроенной базовой лицензией, дающей указанные в лицензии права инсталляции и использования находящейся на дистрибутивном носителе версии/подверсии/релиза программного обеспечения. Срок действия базовой лицензии не ограничен. Право устанавливать обновления ПО в течение указанного в базовой лицензии срока включено в стоимость этой лицензии. Срок установки обновлений, исправляющих критические уязвимости, не ограничивается (пока ООО «АМИКОН» осуществляет техническую поддержку и сопровождение поставленной версии ПО).

По умолчанию ПО ЦВК поставляется в нескольких фиксированных комплектациях:

- **Комплектация 1** – с лицензией на ПО «Центр выработки ключей «ФПСУ-IP», с правом инсталляции на аппаратной платформе ООО «АМИКОН» и правом генерации ключей шифрования по классу КС1.
- **Комплектация 2** – с лицензией на ПО «Центр выработки ключей «ФПСУ-IP», с правом инсталляции на аппаратной платформе ООО «АМИКОН» и правом генерации ключей шифрования по классу КС2.
- **Комплектация 3** – с лицензией на ПО «Центр выработки ключей «ФПСУ-IP», с правом инсталляции на аппаратной платформе ООО «АМИКОН» и правом генерации ключей шифрования по классу КС3.

ООО «АМИКОН» оставляет за собой право по своему усмотрению менять набор базовых функций ПО «Центр выработки ключей «ФПСУ-IP». Для некоторых заказчиков могут согласовываться индивидуальные Комплектации базовых лицензий для ПО «Центр выработки ключей «ФПСУ-IP».

Функциональность ПО «Центр выработки ключей «ФПСУ-IP» может быть расширена за счет приобретения дополнительных расширений к базовой лицензии. Расширения привязаны к конкретному серийному номеру базовой лицензии.

Для ПО «Центр выработки ключей «ФПСУ-IP» предусмотрен один тип расширения базовой лицензии:

- «Модуль-агент активации установки новых релизов программного обеспечения». Соответствующее расширение базовой лицензии дает право на установку и использование новых релизов программного обеспечения на одном экземпляре базового ПО (с указанием или без указания его Комплектации). Расширение срочное, срок действия права на установку новых релизов ПО ограничен периодом, указанным в лицензии.

4. 4. Лицензирование «Центров генерации ключей ФПСУ-IP/Клиентов»

Программное обеспечение «Центр генерации ключей ФПСУ-IP/Клиентов» поставляется с **базовой лицензией**, дающей право запустить на одном рабочем месте актуальную на момент выдачи лицензии версию программного обеспечения. Для инициализации (создание криптографических ключей) комплексов «ФПСУ-IP/Клиент», **базовая лицензия** должна быть дополнена расширением (расширениями) лицензии на право инициализировать определенное количество комплексов. Каждое расширение лицензии именное (имеет уникальный идентификатор), привязано к конкретному серийному номеру **базовой лицензии** и называется:

«Расширение лицензии ПО «Центр генерации ключей ФПСУ-IP/Клиентов» с правом инициализации %указывается количество% комплексов «ФПСУ-IP/Клиент».

Расширения накопительные, дополнительное количество доступных к инициализации комплексов «ФПСУ-IP/Клиентов» прибавляется к уже имеющемуся, путем замещения старой лицензии на новую.

Каждая **базовая лицензия** имеет следующие временные ограничения:

- индивидуальный срок действия базовой лицензии (лицензия может быть бессрочной);
- срок работы с новыми версиями ПО «Центр генерации ключей ФПСУ-IP/Клиентов» (выпущенными после даты предоставления лицензии).

По истечении каких-либо сроков пользователь может приобрести обновленную базовую лицензию.

4. 5. Лицензирование комплексов «ФПСУ-IP/Клиент»

Программное обеспечение комплексов «ФПСУ-IP/Клиент» лицензируется двумя вариантами, в зависимости от набора средств, входящих в его состав.

Первый вариант лицензирования: при использовании ПО комплексов «ФПСУ-IP/Клиент» совместно с USB-устройством «VPN-Key/Client» (программно-аппаратное исполнение) отдельная лицензия не требуется. Приобретение устройства «VPN-Key/Client» в составе комплекса «ФПСУ-IP/Клиент» дает право использовать «ФПСУ-IP/Клиент» на любом рабочем месте, где подключено устройство «VPN-Key/Client» и инсталлировано программное обеспечение «ФПСУ-IP/Клиента» (для всех поддерживаемых операционных систем). Срок использования не ограничивается и зависит от физической возможности использовать устройство. В том числе, использование программного обеспечения «ФПСУ-IP/Клиент» совместно с USB-устройством «VPN-Key/Client» не требует дополнительного

лицензирования на «ФПСУ-IP», позволяющего устанавливать защищенные соединения с комплексами «ФПСУ-IP/Клиент».

Второй вариант лицензирования: использование программного комплекса «ФПСУ-IP/Клиент» (т.е. без USB-устройства «VPN-Key/Client») лицензируется файлами-лицензиями. Для каждой операционной системы требуется своя индивидуальная лицензия. Для соединения с «ФПСУ-IP» используется программный VPN-профиль пользователя. Срок использования «ФПСУ-IP/Клиента» не ограничивается, но лицензией ограничивается срок возможности установки новых версий ПО. По истечении срока возможности установки новых версий ПО пользователь может срок продлить, приобретя обновленную лицензию. Данный вариант лицензирования также требует дополнительного лицензирования на «ФПСУ-IP», позволяющего устанавливать защищенные соединения с комплексами «ФПСУ-IP/Клиент» (см. п. «Лицензирование программно-аппаратных комплексов «ФПСУ-IP» версии 3»).

На одном рабочем месте «ФПСУ-IP/Клиент» может использоваться и с устройством «VPN-Key/Client» и с программным VPN-профилем пользователя. В таком случае лицензирование зависит от типа исполнения «ФПСУ-IP/Клиент», используемого в каждый конкретный момент. При использовании «ФПСУ-IP/Клиентом» для установки защищенного соединения с комплексом «ФПСУ-IP» ключа шифрования, вырабатываемого в подключенном устройстве «VPN-Key/Client» («ФПСУ-IP/Клиент» используется как программно-аппаратный комплекс), действует первый тип лицензирования. При использовании программного VPN-профиля, где ключ шифрования хранится на отчуждаемом или постоянном носителе информации («ФПСУ-IP/Клиент» используется как программный комплекс), действует второй тип лицензирования, даже если к рабочей станции физически подключено устройство «VPN-Key/Client».

5. Условия применения компонентов «ФПСУ-IP»

Комплекс «ФПСУ-IP» предназначен для применения в вычислительных сетях, использующих среду передачи данных Ethernet (тип кадра Ethernet II) и стек протоколов TCP/IP.

Программное обеспечение «ФПСУ-IP» является изделием Криптомаршрутизатор из состава сертифицированного ФСБ России средства криптографической защиты информации «Программно-аппаратный комплекс шифрования «ФПСУ-IP».

5. 1. «ФПСУ-IP»

«ФПСУ-IP» поставляется потребителям в виде комплекта из следующих компонентов:

- «ПО записи дистрибутива ПАК «ФПСУ-IP» на USB»;
- Дистрибутив «ФПСУ-IP»;
- USB-носитель для создания средства автоматизированной инсталляции ПО ПАК «ФПСУ-IP»;
- ТМ-идентификаторы администраторов;
- Аппаратная платформа (в случае программно-аппаратного решения).

Компонент «ПО записи дистрибутива ПАК «ФПСУ-IP» на USB» позволяет на основе файлов дистрибутива «ФПСУ-IP» создать загрузочный USB-носитель, с помощью которого осуществляется установка файлов программного обеспечения «ФПСУ-IP» на аппаратную платформу или в виртуальную среду.

Требования к аппаратному и программному обеспечению для функционирования компонента «ПО записи дистрибутива ПАК «ФПСУ-IP» на USB»:

- ОС: Microsoft Windows 8.1, Microsoft Windows 10;
- Вычислительная платформа общего назначения: в соответствии с требованиями операционной системы.

Для администрирования «ФПСУ-IP» (конфигурирования, регистрации ТМ-идентификаторов, просмотра регистрационной информации и т.д.) к нему необходимо подключить монитор и клавиатуру или выполнить консольное подключение.

Требования к аппаратному и программному обеспечению для функционирования консоли:

- ПО консоли управления: PuTTY 0.70;
- ОС консоли управления: Microsoft Windows 8.1, Microsoft Windows 10;
- Вычислительная платформа общего назначения: в соответствии с требованиями операционной системы.

5. 2. Необходимые организационные меры при эксплуатации комплекса «ФПСУ-IP»

Защитные функции «ФПСУ-IP» гарантируют конфиденциальность, целостность и достоверность передаваемой информации при соблюдении определённых организационно-технических требований, а именно:

- обеспечения физической охраны «ФПСУ-IP» с целью препятствования доступа внутрь их аппаратуры;
- контроля за подключением «ФПСУ-IP» к общей IP-сети и защищаемым IP-фрагментам с целью предотвращения несанкционированного обмена данными в обход «ФПСУ-IP» или существования открытых (незащищённых) выходов;
- предотвращения доступа посторонних лиц к зарегистрированным ТМ-идентификаторам локальных администраторов;
- обеспечения физической охраны инсталляционных носителей «ФПСУ-IP» и инсталляционных ТМ-идентификаторов;
- обеспечения физической охраны носителей с парно-выборочными ключами ЦВК;
- обеспечения физической охраны ТМ-идентификаторов с общесистемными ключами Криптосетей Клиентов «ФПСУ-IP»;
- предотвращения доступа посторонних лиц к УА ФПСУ-IP и средствам удалённого управления «ФПСУ-IP» с применением предусмотренных в УА ФПСУ-IP средств защиты от НСД;
- предотвращения доступа посторонних лиц к ЦВК и обеспечения физической охраны изготовленных ключевых внешних носителей.

При использовании «ФПСУ-IP» следует также руководствоваться эксплуатационными документами на СКЗИ (правила пользования и формуляр).

Для реализации комплексных мер защиты от НСД в эксплуатирующей «ФПСУ-IP» организации должны быть созданы специальные структурные подразделения – отделы безопасности, которые вырабатывают инструкции по обеспечению изложенных выше требований и следят за их неукоснительным соблюдением, а также выявляют попытки нарушения установленной политики безопасности и принимают соответствующие меры по пресечению таких попыток.

6. Структура комплекса «ФПСУ-IP» и взаимосвязь работы его подсистем

Структурная схема комплекса «ФПСУ-IP», отражающая взаимосвязь работы его подсистем, представлена ниже на рисунке:

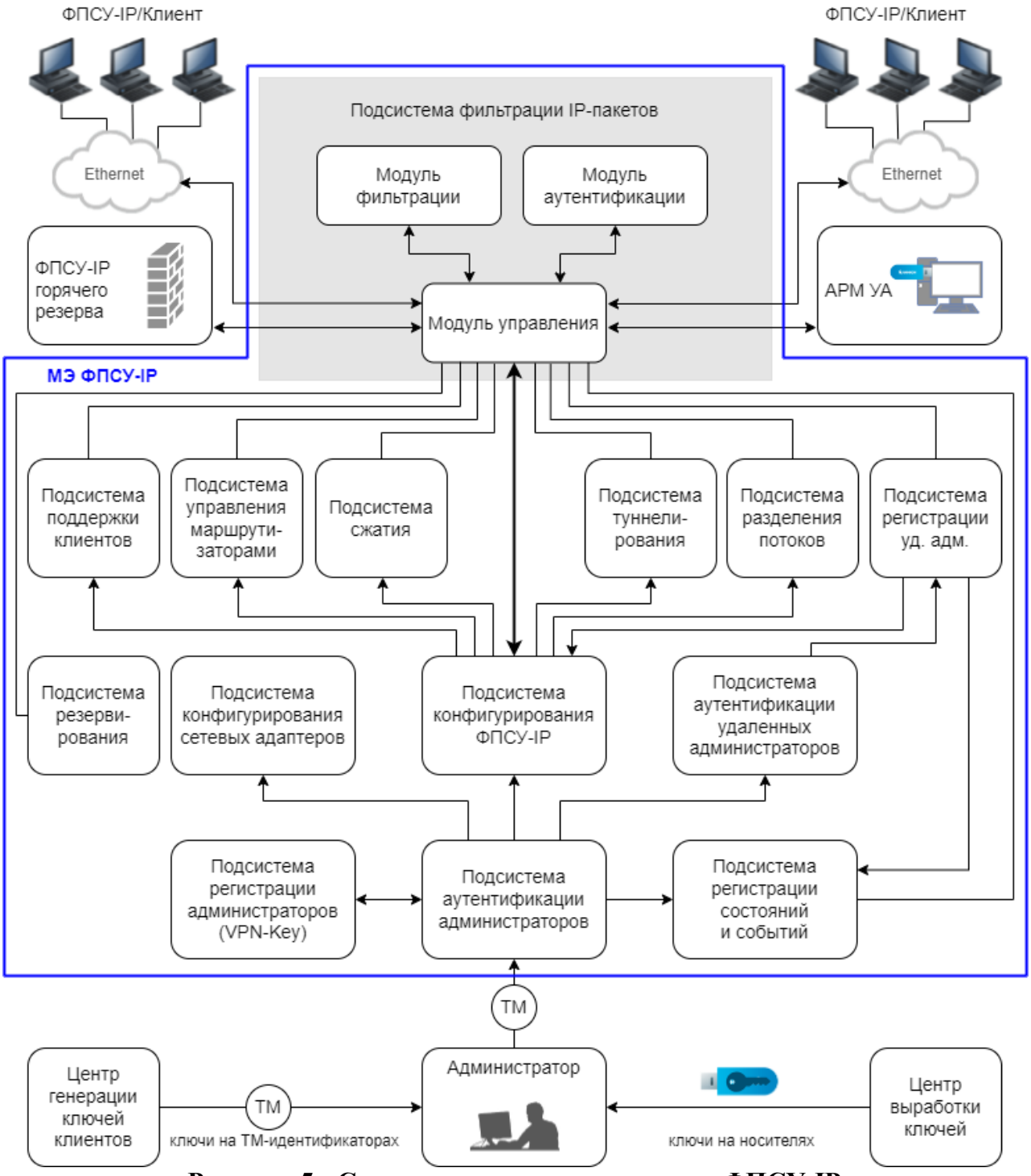

Рисунок 5 - Структурная схема комплекса ФПСУ-IP

В базовом варианте исполнения «ФПСУ-IP» состоит из следующих элементов:

1. **Подсистемы фильтрации пакетов IP-протокола**, осуществляющей:

- предварительную проверку корректности в зависимости от типа пропускаемого

протокола;

- фильтрацию пакетов по устанавливаемым при настройке «ФПСУ-IP» правилам;
- аутентификацию абонентов при работе через два «ФПСУ-IP»;
- сокрытие субъектов и объектов передачи и используемых ими прикладных сервисов;
- коммутацию пакетов, прошедших вышеописанную обработку.

2. **Подсистемы туннелирования**, обеспечивающей построение виртуальных частных сетей за счёт создания межсетевых туннелей между двумя или более «ФПСУ-IP» и шифрование передаваемых в этих туннелях данных.

3. **Подсистемы сжатия**, осуществляющей сжатие передаваемых через межсетевые туннели данных с целью сокрытия трафика, уменьшения объёма передаваемых данных и уменьшения расходов на эксплуатацию сети.

4. **Подсистемы разграничения доступа**, которая:

- разграничивает доступ к «ФПСУ-IP» по зарегистрированным правам для различных классов администраторов;
- обеспечивает целостность программной и информационной частей «ФПСУ-IP», создавая собственную изолированную среду и защищая данные на внутреннем накопителе;
- организует дополнительную защиту доступа к подсистемам настройки «ФПСУ-IP» по паролю;
- обеспечивает возможность доступа к подсистемам конфигурирования «ФПСУ-IP»;
- обеспечивает возможность контроля целостности программных модулей «ФПСУ-IP».

5. **Подсистемы аутентификации администраторов,** обеспечивающей идентификацию и аутентификацию администраторов по предъявлению электронного идентификатора и (опционально) паролю условно-постоянного действия.

6. **Подсистемы регистрации администраторов (ТМ-идентификаторов)**, обеспечивающей регистрацию и учёт электронных идентификаторов touch-memory.

7. **Подсистемы конфигурирования «ФПСУ-IP»**, позволяющей:

- задавать общие параметры работы «ФПСУ-IP» (устанавливать время аварийного перезапуска комплекса в случае сбоя сетевых адаптеров, регулировать функции сокрытия работы «ФПСУ-IP» как фильтрующего средства, указывать способ обработки IP-опции Source Route и т.д.);
- задавать правила фильтрации IP-пакетов, способы контроля доступа и метод

передачи данных независимо для различных групп абонентов;

- устанавливать параметры сетевых адаптеров;
- задавать правила формирования (разделения) потоков данных, отправляемых «ФПСУ-IP» на транзитные маршрутизаторы;
- устанавливать с внешних носителей необходимое программное обеспечение «ФПСУ-IP» (драйверы сетевых плат, обновлённые версии ПО и опциональных подсистем);
- устанавливать с внешних носителей ключи парно-выборочной связи смежных «ФПСУ-IP», регистрационные параметры удалённых администраторов и системные ключи «ФПСУ-IP/Клиентов»;
- контролировать целостность программных модулей «ФПСУ-IP».

8. **Подсистемы конфигурирования сетевых адаптеров**, осуществляющей настройку сетевого оборудования для работы «ФПСУ-IP».

9. **Подсистемы регистрации событий и состояний (статистики)**, которая:

- автоматически выполняет автономный сбор статистической информации о функционировании «ФПСУ-IP», в частности: регистрирует фильтруемый трафик и результаты фильтрации, а также действия локальных и удалённых администраторов;
- осуществляет динамический вывод на экран текущей информации о работе «ФПСУ-IP»;
- предоставляет возможность просмотра статистических данных и записи их на внешний носитель для хранения и/или последующей обработки специальной программой, обеспечивающей чтение, анализ/сортировку и преобразование в стандартный DBF-формат;
- сортирует информацию по типам и времени записи, что позволяет администратору просматривать только необходимую ему информацию и осуществлять быструю выборку и выдачу заказанной информации, не задерживая работу других подсистем «ФПСУ-IP» (в первую очередь, подсистемы фильтрации).

10. **Подсистемы удаленного управления и контроля**, состоящей из:

- **Подсистемы регистрации удалённых администраторов**, позволяющей регистрировать удалённых администраторов для последующей их идентификации и аутентификации с присвоением конкретных прав на доступ к подсистемам «ФПСУ-IP»;
- **Подсистемы аутентификации удалённых администраторов**, осуществляющей идентификацию и аутентификацию удалённого администратора при запросах на доступ, предоставляющей возможность дистанционного доступа к подсистемам

«ФПСУ-IP» и контролирующей права удалённого администратора при запросах на доступ.

11. **Подсистемы разделения IP-потоков на независимые туннели**, позволяющей разделить выдаваемые в VPN-туннель данные на несколько (до 128) различных потоков, то есть поместить в заголовки IP-пакетов передаваемых данных необходимые признаки для поддержки соответствующих функций транзитных маршрутизаторов

12. **Подсистемы автозапуска**, которая обеспечивает автоматическое (без участия оператора) возобновление работы «ФПСУ-IP» после сбоев электропитания.

13. **Подсистемы Syslog**, позволяющей назначить для каждого «ФПСУ-IP» сервер, принимающий отправляемые «ФПСУ-IP» сообщения о происходящих на нем ошибках и событиях по протоколу Syslog.

14. **Подсистемы поддержки сетевого протокола 802.1q (VLAN)**, позволяющей «ФПСУ-IP» принимать участие в построении сетей 802.1q (VLAN) поверх локальных и глобальных сетей, выполняя функции маршрутизатора VLAN. На портах «ФПСУ-IP» поддерживается до 4093 тегов VLAN.

Функциональные возможности базового варианта программного обеспечения «ФПСУ-IP» могут быть расширены за счёт установки следующих дополнительных модулей:

1. **Модуль-агент активации сервера доступа и обслуживания комплексов «ФПСУ-IP/Клиент»**, который:

- обеспечивает установку общесистемных ключей «ФПСУ-IP/Клиентов», применяемых для взаимной аутентификации «ФПСУ-IP» и «ФПСУ-IP/Клиента»;
- обеспечивает формирование правил работы и прав доступа «ФПСУ-IP/Клиентов»;
- выполняет идентификацию и аутентификацию «ФПСУ-IP/Клиентов» при обращении к «ФПСУ-IP»;
- организует защиту канала связи с идентифицированным и аутентифицированным «ФПСУ-IP/Клиентами» (организует VPN-туннель);
- блокирует доступ «ФПСУ-IP/Клиентов», подлинность которых не подтвердилась при аутентификации;
- устанавливает правила обработки «ФПСУ-IP/Клиентами» сторонних по отношению к туннелю пакетов на время взаимодействия с «ФПСУ-IP» в соответствии с заданными параметрами конфигурации «ФПСУ-IP»;
- производит фильтрацию запросов «ФПСУ-IP/Клиентов» на доступ к сетевым ресурсам защищаемой «ФПСУ-IP» локальной сети по установленным критериям;
- в зависимости от заданного в конфигурации «ФПСУ-IP» режима работы получателей отфильтрованного трафика, осуществляет необходимую дальнейшую

обработку пакетов и передаёт их по адресу назначения;

- регистрирует попытки доступа «ФПСУ-IP/Клиентов» к портам «ФПСУ-IP»;
- позволяет использовать на данном «ФПСУ-IP» **«Модуль-агент активации определённого количества (указывается количество) подключений комплексов «ФПСУ-IP/Клиент»**, который дает право единовременно подключиться определенному в указанной лицензии количеству комплексов «ФПСУ-IP/Клиент», не использующих специализированный аппаратный ключ «VPN-Key/Client».

2. **Модуль-агент активации горячего резервирования**, который обеспечивает:

- настройку системы «горячего» резервирования между двумя «ФПСУ-IP»;
- автоматическую передачу управления пассивному «ФПСУ-IP» в случае возникновения аппаратных неполадок на активном «ФПСУ-IP» или отсутствия в течение некоторого времени связи с ним;
- синхронизацию (в ручном или автоматическом режиме) программного обеспечения, а также конфигурационных и ключевых данных на обоих «ФПСУ-IP» системы «горячего» резерва.

3. **Модуль-агент активации дополнительного вычислительного потока**, позволяющий задействовать в работе программного обеспечения «ФПСУ-IP» указанное в лицензии количество вычислительных устройств (процессоров, ядер процессора, HT-устройств). Дополнительный поток увеличивает общую пропускную способность комплекса при активации всех режимов защиты (туннелирование, шифрование, имитозащита) на 70-80% от производительности главного потока.

4. **Модуль-агент активации установки новых релизов программного обеспечения версии 3**, который дает право на установку и использование на данном «ФПСУ-IP» новых версий/подверсий/релизов программного обеспечения версии 3. Срок действия права ограничен периодом, указанным в лицензии. Данный модуль-агент требуется только для тех «ФПСУ-IP», на которые закончился гарантийный срок обслуживания.

5. **Модуль-агент активации криптопротокола FAST**, которой активирует на «ФПСУ-IP» специальный режим работы криптографического протокола МАГМА 34.12-2015, обеспечивающий существенное увеличение производительности криптографической обработки данных по сравнению с алгоритмом ГОСТ 28147-89 и стандартной реализацией МАГМА 34.12-2015. Прирост производительности по сравнению с ГОСТ 28147-89 составляет от 30% до 100%, а для МАГМА 34.12-2015 от 100% до 300%, в зависимости от типа аппаратной платформы «ФПСУ-IP» и длины обрабатываемого сетевого пакета.

7. Механизмы работы отдельных подсистем «ФПСУ-IP»

7. 1. Подсистема разграничения доступа ACCESS-TM SHELL

Подсистема разграничения доступа предназначена для предотвращения несанкционированного доступа к работе «ФПСУ-IP» и базируется на использовании электронных ТМ-идентификаторов.

Функционирование «ФПСУ-IP» под управлением ACCESS-TM SHELL даёт возможность избежать случайного или умышленного вмешательства в работу «ФПСУ-IP», изменения конфигурационной информации, установки ключевых данных, просмотра регистрационных данных и т.п.

Подсистема ACCESS-TM SHELL является неотъемлемой частью «ФПСУ-IP». После установки подсистема разграничения доступа создаёт на компьютере замкнутую изолированную среду, в которой работает «ФПСУ-IP». Вмешательство в логику работы самого «ФПСУ-IP» и любая попытка использовать «ФПСУ-IP» не по назначению будет блокироваться. В то же время собственная среда «ФПСУ-IP» содержит широкий ряд возможностей по управлению «ФПСУ-IP» и его функциями, подключению драйверов используемого оборудования и дополнительного программного обеспечения разработчика, установке или смене ключевых данных, установке ключей «ФПСУ-IP/Клиентов», установке пароля и учёту и контролю используемых ТМ-идентификаторов. Как видно из схемы (см. рисунок ниже), подсистема состоит из следующих основных модулей:

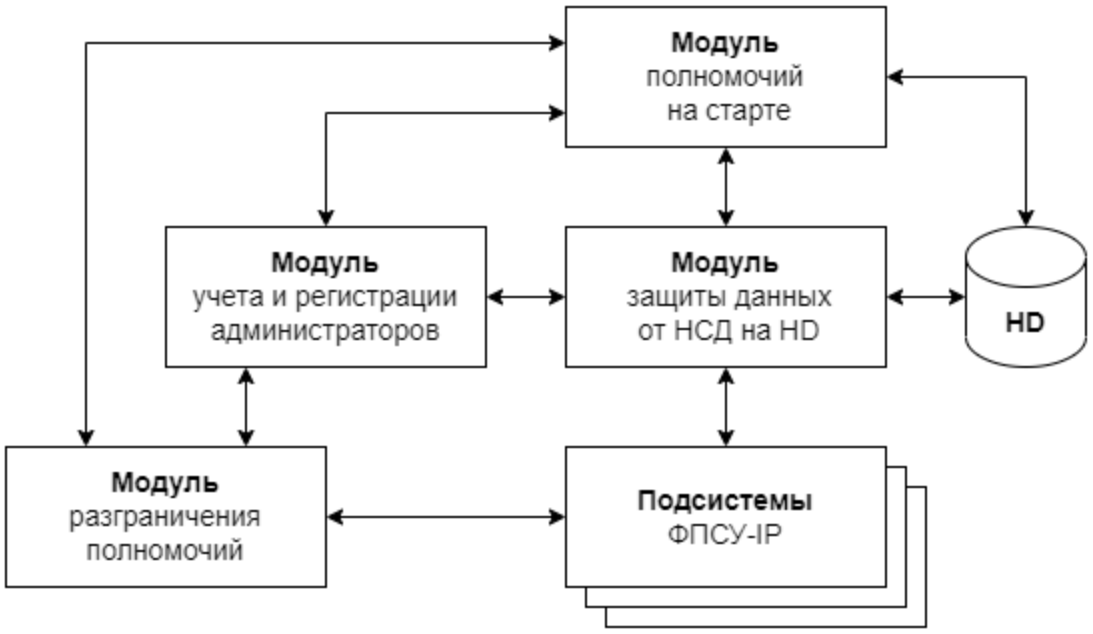

Рисунок 6 - Структурная схема подсистемы ACCESS-TM SHELL

- модуля контроля полномочий на старте «ФПСУ-IP»;
- модуля защиты данных на внутреннем накопителе от НСД;
- модуля разграничения полномочий пользователей;
- модуля регистрации администраторов.

Подсистема ACCESS-TM SHELL функционирует в три этапа:

Этап 1. При включении питания «ФПСУ-IP» после выполнения диагностических тестов BIOS\UEFI компьютера ACCESS-TM SHELL осуществляет запуск модуля контроля полномочий на старте, который проводит идентификацию пользователя (по предъявленному им ТМ-идентификатору) для выдачи разрешения на запуск. Разрешение на запуск «ФПСУ-IP» так же может выдать заранее активированная администратором «ФПСУ-IP» подсистема автоматического старта.

Этап 2. В случае успешной идентификации пользователя загружается модуль защиты от НСД данных на внутреннем накопителе, который будет защищать информацию от просмотра и модификации и пресекать попытку запуска на «ФПСУ-IP» операционной системы со съемного носителя. В случае неполадок в «ФПСУ-IP», внутренний накопитель данных с установленным на нем программным обеспечением «ФПСУ-IP» может быть переставлен на другую аппаратную платформу.

Этап 3. В случае успешного осуществления этапов 1 и 2 выполнение штатной загрузки аппаратного обеспечения будет продолжено и управление передано BIOS\UEFI. После загрузки всей операционной системы «ФПСУ-IP», модуль разграничения полномочий пользователей будет производить контроль за правом доступа пользователей на управление работой «ФПСУ-IP». Контроль доступа осуществляется путем выдачи приглашения на прижатие ТМ-идентификатора к считывателю touch-memory, принятии на основании полученной информации решения о допуске. Администратор, не предъявивший или предъявивший некорректный, незарегистрированный или несоответствующий запрошенной операции ТМ-идентификатор, к управлению допущен не будет.

ACCESS-TM SHELL осуществляет контроль и разграничение доступа локальных администраторов в соответствии с их логическим разделением на 4 различных класса. Таблица 1 отображает реализованные в комплексе «ФПСУ-IP» классы администраторов и доступные для них действия.

ПО «ФПСУ-IP» содержит модуль регистрации и учета электронных ТМ-идентификаторов, идентифицирующих его обслуживающий персонал.

Разграничение доступа допущенных лиц и контроль их полномочий при запуске «ФПСУ-IP» и управлении его работой осуществляется в соответствии с логическим разделением управляющих ФПСУ-IP лиц на две роли и пять условных классов,

представленных в нижеследующей таблице.

Средства «ФПСУ-IP» позволяют регистрировать новые ТМ-идентификаторы по любому необходимому классу, кроме ТМ-идентификатора Главного администратора (она же является инсталляционным ТМ-идентификатором). Если ТМ-идентификатор уже зарегистрирован (на данном «ФПСУ-IP»), он может быть проверен на корректность хранимой в ней информации, очищен или перерегистрирован по другому классу (кроме инсталляционного ТМ-идентификатора).

Таблица 1. Роли и классы пользователей ФПСУ-IP

Роль/Класс	Разрешенные действия
Пользователь/ /Без идентификации пользователя	• переинициализация ПДСЧ; • отключение автозапуска.
Пользователь/ /Оператор	• запуск «ФПСУ-IP»; • остановка режима фильтрации пакетов «ФПСУ-IP»; • просмотр, включение и отключение оповещений о нарушениях правил межсетевого экрана; • передача управления партнеру по горячему резервированию; • удаление текущего соединения из таблицы состояний соединений; • выключение питания «ФПСУ-IP» по кнопке «Power».
Администратор / Инженер	Все права класса Оператор и дополнительно: • конфигурирование сетевых адаптеров; • конфигурирование IP-адресов портов «ФПСУ-IP»; • установка даты и времени; • контроль целостности исполняемых программных модулей «ФПСУ-IP» (только по хранящимся на «ФПСУ-IP» контрольным суммам с выводом результата на экран); • запуск процесса функционального самотестирования межсетевого экрана «ФПСУ-IP»; • сохранение текущей конфигурации «ФПСУ-IP» на USB-flash; • настройка общих параметров работы «ФПСУ-IP» (watchdog, аварийный перезапуск, переход на резервный, гашение экрана, запрет работы при сбоях внутреннего накопителя данных, не

Роль/Класс	Разрешенные действия
	сообщать об устаревших ключах, контроль сети); • просмотр регистрационной информации (статистики).
Администратор/ Администратор	Все права класса Инженер и дополнительно: • восстановление с USB-носителя и редактирование конфигурации «ФПСУ-IP»; • включение режима «Запрет открытых соединений» в общих параметрах работы «ФПСУ-IP»; • регистрация и предоставление полномочий на определенные действия удаленным администраторам; • регистрация ТМ-идентификаторов; • настройка подсистемы автоматического старта; • установка пароля условно-постоянного действия на администрирование; • установка ключей парно-выборочной связи; • установка общесистемных ключей; • установка ключевых данных для реализации защищенного обмена в режиме горячего резервирования; • установка времени действия ключей; • контроль целостности исполняемых программных модулей «ФПСУ-IP» (без ограничений на варианты проверки); • установка изменений и дополнений к программным модулям «ФПСУ-IP»; • контроль целостности конфигурации «ФПСУ-IP».
Администратор / Главный администратор	Все права класса Администратор и дополнительно: • выдача на USB-носитель системного журнала статистики; • переустановка программного обеспечения «ФПСУ-IP» со специального средства восстановления (USB-носителя).

7. 2. Подсистема фильтрации пакетов и правила фильтрации

Подсистема фильтрации пакетов «ФПСУ-IP» выполняет:

- предварительную проверку корректности формата пакета и соответствия стандартам, соответствующего IP-протокола;
- фильтрацию пакетов по установленным администратором правилам;

- идентификацию и аутентификацию других «ФПСУ-IP» при обмене пакетами через туннель между двумя «ФПСУ-IP» с целью защиты межсетевых потоков информации абонентов от НСД (от навязывания сторонней информации, искажения передаваемой информации, подмены IP-адресов и т.д.);
- идентификацию и аутентификацию зарегистрированных на «ФПСУ-IP» «ФПСУ-IP/Клиентов»;
- идентификацию и аутентификацию зарегистрированных на «ФПСУ-IP» администраторов УА ФПСУ-IP;
- сокрытие субъектов и объектов передачи и используемых ими прикладных сервисов;
- коммутацию пакетов, прошедших процедуру фильтрации.

Механизм управления доступом, осуществляемый «ФПСУ-IP», базируется на анализе поступающих на один из его интерфейсов пакетов с целью определения их соответствия правилам и данным, установленным администратором при настройке. Пакеты, удовлетворившие всем требуемым для данного соединения правилам межсетевого экрана, отправляются на сетевой интерфейс для дальнейшей передачи, в противном случае они сбрасываются. При этом (в зависимости от указания администратора) может посылать или не посылать ICMP-сообщение на IP-пакет о недоступности запрашиваемого абонента.

Основными обязательными критериями фильтрации для каждого соединения являются аутентификационные данные «ФПСУ-IP/Клиентов» (если отправителем и/или получателем является «ФПСУ-IP/Клиент»), и IP-адреса отправителя и получателя (для обычных абонентов). Соединение конкретной пары абонентов/»ФПСУ-IP/Клиентов» может быть осуществлено только при условии, что администратор указал данную пару в конфигурации «ФПСУ-IP». Помимо разрешающих правил, могут быть созданы запрещающие правила доступа для взаимодействующих пар абонентов или «ФПСУ-IP/Клиентов».

Комплекс «ФПСУ-IP» поддерживает традиционную классификацию IP-адресов (A, B и C) с расширениями RFC 950 (процедура разбиения на подсети) и RFC 1519 (группирование диапазона адресов в пару IP-адрес/IP-маска подсети). Адрес может быть задан явно, как адрес хоста (рабочей станции), а может принадлежать группе адресов, которую администратор «прописывает» через групповой адрес (пару адрес/маска подсети). В группу адресов могут быть объединены $2^n - 2$ хостов, где $2 \leq n \leq 24$.

Комплекс поддерживает также такое расширение стандарта протокола IP, как широковещательные передачи в подсети, если при конфигурировании администратор это разрешил.

Фильтрация может осуществляться также по ряду дополнительных критериев:

- разрешённым времени и дате соединения;

- состоянию соединения;
- транспортным и прикладным протоколам соединения;
- разрешенным и запрещенным командам прикладных протоколов;
- мобильному коду, передаваемому в http-соединении;
- разрешённым для соединений TCP или UDP портам абонентов;
- инициатору соединения;
- фрагментированным пакетам;
- прочим опциям заголовков IP, TCP, UDP, ICMP и других протоколов.

Для осуществления такой фильтрации администратор создаёт правила доступа межсетевого экрана, определяемые совокупностью специфических параметров доступа, и назначает эти правила группам отдельных абонентов, «ФПСУ-IP/Клиентов» или подсетям, выступающими отправителями или получателями данных.

Таким образом, абоненты могут быть логически разделены, например, по функциональному признаку, и для каждой группы могут быть установлены свои ограничения. Это позволяет быстро и без путаницы установить необходимую конфигурацию, а также эффективно осуществлять фильтрацию по необходимой для каждой группы совокупности критериев.

При использовании правил доступа каждая разрешенное сетевое взаимодействие должно быть явно описана, то есть требуется указать, между какими описателями могут осуществляться соединения. Данные, не подпадающие под разрешительное правило доступа, не будут переданы получателю.

Правилам доступа администратор устанавливает приоритет, и, в случае конфликта указаний в нескольких правил доступа, будет выполнено правило с наивысшим приоритетом.

Один из главных принципов построения комплекса «ФПСУ-IP» заключается в том, что его применение не требует изменения топологии сети и/или настроек сетевого взаимодействия рабочих станций. Для этого в комплексе реализован стандартный механизм ARP-proxy со специфичной ARP-фильтрацией, гарантирующей получение ARP-ответа станции, запрашивающей проход через «ФПСУ-IP» к удалённому ресурсу. Механизм фильтрации реализован с учётом различия пакетов IP и ARP.

Конкретный механизм работы подсистемы фильтрации изложен далее, в подразделе «Механизм работы подсистемы фильтрации пакетов».

При прикреплении абонентов или «ФПСУ-IP/Клиентов» к интерфейсам «ФПСУ-IP» администратор должен указать для каждого описателя (индивидуального или группового)

необходимый режим работы.

Режим работы определяет, будет ли абонент подключён к интерфейсу «ФПСУ-IP» непосредственно (режим «Ретрансляция»), или через туннель к другому «ФПСУ-IP» (режим «Через ФПСУ»). В случае «Через ФПСУ» при передаче пакетов будут задействованы механизмы идентификации и аутентификации (данные механизмы будут подробно описаны ниже, в подразделе «Механизмы идентификации и аутентификации»), а также могут осуществляться сжатие и криптографическая защита передаваемых данных.

Если несколько «ФПСУ-IP» устанавливаются последовательно и работают в «каскадном» режиме, полный механизм фильтрации при передаче пакетов через них задействуется только на ближайших к отправителю и получателю пакетов «ФПСУ-IP», а на транзитных «ФПСУ-IP» будут произведены только двусторонняя аутентификация «ФПСУ-IP» и фильтрация по разрешённым адресам абонентов.

Поддержка «ФПСУ-IP» стандарта IP-протокола в отношении IP-опций имеет некоторые ограничения, которые будут отдельно рассмотрены в подразделе «Обработка IP-опций».

«ФПСУ-IP» не отвечает на IP-запросы абонентов или служб сетевого управления и мониторинга, посланные по его собственным адресам, за исключением следующих случаев:

- при специальном разрешении администратора, «ФПСУ-IP» будет отвечать на ICMP-запросы (Ping), направленные от известных ему (указанных в конфигурации) IP-адресов абонентов и маршрутизаторов, причём только на те запросы, которые поступили на адреса его портов в одном IP пакете (т.е. не были фрагментированы в процессе доставки);
- «ФПСУ-IP» принимает IP-пакеты, посланные в адрес одного из его портов другим «ФПСУ-IP», если последний описан в его конфигурации со стороны данного порта, и только после успешного завершения процесса двусторонней аутентификации взаимодействующих «ФПСУ-IP»;
- «ФПСУ-IP» принимает IP-пакеты, отправленные в его адрес от УА ФПСУ-IP, если этот УА ФПСУ-IP зарегистрирован на данном «ФПСУ-IP», и процедура взаимной аутентификации между ними завершилась успешно;
- «ФПСУ-IP» принимает IP-пакеты, посланные в адрес одного из его портов пользователем комплекса «ФПСУ-IP/Клиент», если этот «ФПСУ-IP/Клиент» описан на «ФПСУ-IP», и успешно прошёл взаимные процедуры идентификации и аутентификации.

7. 2. 1. Сокрытие работы «ФПСУ-IP»

Администратор может указать «ФПСУ-IP» на то, что его защитные функции должны быть невидимы. Для этого «ФПСУ-IP» содержит несколько специальных конфигурационных переключателей. Если включён переключатель сокрытия работы, «ФПСУ-IP» при нарушении правил фильтрации будет сбрасывать пакеты без генерации ICMP-сообщений с соответствующим кодом («абонент недоступен по причине административного запрета»), а в других ICMP-сообщениях об ошибках в качестве адреса отправителя указывать не свой адрес, а адрес того абонента, которому был направлен пакет, вызвавший ошибку. Другие конфигурационные переключатели позволяют дать указание «ФПСУ-IP» вообще не генерировать ICMP-сообщения, кроме сообщений о необходимости изменения MTU, а также не изменять поле «время жизни» (TTL) в заголовке IP-пакета. Подробнее поддержка протокола ICMP будет описана в подразделе «Поддержка ICMP-сообщений».

7. 2. 2. Механизм работы подсистемы фильтрации пакетов

7. 2. 2. 1. Обработка Ethernet-фреймов

При поступлении Ethernet-фрейма на один из интерфейсов «ФПСУ-IP» производится его анализ, и для дальнейшей обработки допускаются только фреймы типа Ethernet II, содержащие дейтаграммы протоколов ARP, IP, MPLS, BPDU, VTP и VLAN (IEEE 802.1Q). Фреймы других типов и/или содержащие другие типы протоколов сбрасываются без сообщений. Далее в соответствии с типом протокола полученной дейтаграммы производится проверка корректности формата пакета и/или его заголовка и содержимого, после чего (в случае положительного результата проверки) пакет будет передан на фильтрацию и обработку соответствующему модулю.

7. 2. 2. 2. Фильтрация ARP-пакетов

При получении «ФПСУ-IP» пакета ARP-запроса на получение сетевого адреса абонента, находящегося со стороны другого интерфейса, после проверки на корректность формата «ФПСУ-IP» автоматически проверяет наличие IP-адресов отправителя и получателя в конфигурационных таблицах портов, описанных администратором.

В случае отрицательного результата поиска адресов - данные адреса или маски их подсетей не указаны администратором в качестве разрешённых для соединений - пакет сбрасывается и доступ удалённой станции не предоставляется, что позволяет скрывать топологию сети от сканирования. Если адреса отправителя и получателя в конфигурационных таблицах найдены, производится поиск в ARP-кэше противоположного порта записи, содержащей IP-адрес получателя.

В случае успеха отправителю высылается ответ, позволяющий ему в дальнейшем посылать IP-пакеты, которые будут профильтрованы по правилам для IP-пакетов. В противном случае «ФПСУ-IP» генерирует ARP-запрос и отправляет его с противоположного интерфейса, по получении ответа, на который он вышлет свой ответ абоненту-отправителю исходного пакета.

Обратите внимание: если «ФПСУ-IP» получает ARP-запрос на получение MAC-адреса, соответствующего одному из собственных IP-адресов комплекса, ответ на ARP-запрос посылается в обязательном порядке, то есть проверка наличия IP-адреса отправителя в конфигурационных таблицах портов не производится. Это позволяет регистрировать удалённых администраторов и «ФПСУ-IP/Клиентов» по уникальным именам и аутентификационным данным, без конкретной привязки к их IP-адресам.

7. 2. 2. 3. Фильтрация IP-пакетов

Подсистема фильтрации «ФПСУ-IP» производит обработку поступающих на один из его интерфейсов IP-пакетов следующим образом:

1. При поступлении IP-пакета осуществляется проверка корректности его IP-заголовка (допустимого формата адресов, правильности контрольной суммы, допустимых опций и т.д.) и соответствия его стандартам IP-протокола. Если пакет некорректен - он сбрасывается, в противном случае подсистема фильтрации анализирует его поля.

2. Проверяется IP-адрес назначения. Если он является одним из собственных IP-адресов «ФПСУ-IP», подсистема фильтрации проверит, соответствует ли данный пакет формату протокола удалённого администрирования. В случае положительного результата будет запущена процедура аутентификации удалённого администратора, при успешном завершении которой подсистема фильтрации прекращает обработку пакета и передаёт запрос соответствующим подсистемам комплекса для выработки ответа (который затем будет обработан и поставлен в очередь на передачу в соответствии с пунктом 11). При неполадках аутентификации пакет будет сброшен.

3. Если формат IP-пакета не соответствует протоколу удалённого администрирования, проверяется наличие IP-адреса отправителя пакета в таблице разрешённых адресов, описанных со стороны данного порта. Если он не найден - пакет будет сброшен с посылкой ICMP-сообщения «Destination Unreachable» с кодом 13 (если администратор не установил иначе).

4. Если IP-адрес отправителя в таблице обнаружен и описан в конфигурации

«ФПСУ-IP» со стороны данного порта как маршрутизатор, проверяется, какому протоколу принадлежит обрабатываемый IP-пакет. В случае, если протокол входит в список разрешённых протоколов маршрутного обмена для данного маршрутизатора, производится проверка корректности формата всего IP-пакета и наличия описания такого протокола маршрутизации на противоположном порту «ФПСУ-IP». При отрицательных результатах проверки пакет сбрасывается, в противном случае - передаётся на другой порт комплекса в очередь на передачу. Если же обнаруженный подсистемой протокол не относится к разрешённым для данного маршрутизатора протоколам маршрутизации, обработка пакета продолжится в соответствии с пунктом 6 и далее.

5. Если IP-адрес отправителя пакета содержится в конфигурационной таблице принимающего порта и описан в ней как другой «ФПСУ-IP», то производится проверка аутентификации на данный пакет. При отрицательных результатах аутентификации пакет сбрасывается, а в случае успеха восстанавливается исходная (инкапсулированная в VPN-туннель) дейтаграмма с IP-адресами отправителя и получателя и используемыми при передаче прикладными сервисами. Далее обработка дейтаграммы производится в соответствии с пунктами 2 и 3, то есть сначала определяется, не работает ли через данный VPN-туннель удалённый администратор (в случае чего будет запущена процедура аутентификации последнего), а затем проверяется, описан ли адрес отправителя детуннелированной дейтаграммы со стороны данного порта как адрес абонента, работающего через данный удалённый «ФПСУ-IP» (если нет - пакет сбрасывается, если содержится - обработка продолжается).

6. Далее проверяется IP-адрес получателя. Если он является собственным адресом «ФПСУ-IP», производится проверка, является ли пакет ICMP-запросом (Ping) и разрешён ли запрос от IP-адреса получателя. При отрицательных результатах проверки пакет сбрасывается; в случае успеха обработка пакета прекращается, а на запрос вырабатывается ответ, который обрабатывается в соответствии с пунктом 11).

7. Если получателем принятого IP-пакета (или детуннелированной дейтаграммы, если пакет пришёл через удалённый комплекс) является не сам обрабатывающий «ФПСУ-IP», выполняется поиск адреса получателя в таблицах разрешённых абонентов; если адрес получателя неизвестен, пакет будет сброшен с посылкой ICMP-сообщения «Destination Unreachable» с кодом 13 (если администратор не установил иначе). В противном случае ищется аппаратный адрес данного абонента в ARP-кэше. В случае отсутствия вступит в силу процедура определения

MAC-адреса, а принятая дейтаграмма сбрасывается и отправителю посылается ICMP-сообщение «Destination Unreachable» с кодом 0.

8. Если получателем пакета является пограничный маршрутизатор, подсистема фильтрации проверит установки конфигурационной таблицы, какой протокол инкапсулирован в IP-пакет и разрешено ли отправителю пакета обращение к данному транзитному маршрутизатору. Если нет, пакет будет сброшен, если результаты проверки положительны - обработка пакета прекращается и пакет будет поставлен в выходную очередь порта приёма.

9. Если пакет был получен от абонента, работающего через удалённый «ФПСУ-IP», и направлен другому (прописанному и разрешенному к работе) абоненту, работающему через следующий удалённый «ФПСУ-IP», то после шифрования пакета с использованием заранее согласованных ключей парно-выборочной связи, он будет поставлен в выходную очередь на передачу. В противном случае процедура фильтрации продолжится.

10. Если на «ФПСУ-IP» задействован межсетевой экран, пакет проверяется на соответствие правилам межсетевого экрана. Фильтрация пакета будет производиться по установленной для данного соединения совокупности правил фильтрации. Каждое соединение между каждой парой абонентов хранится в таблице соединений «ФПСУ-IP» и каждый пакет проверятся на соответствие состоянию, указанному в этой таблице. Каждый пакет абонента проверяется на соответствие описаниям правил межсетевого экрана, под которые он подпадает. Если пакет абонента не соответствует состоянию соединения или правилам межсетевого экрана - пакет будет сброшен, как не прошедший фильтрацию с посылкой ICMP-сообщения «Destination Unreachable» с кодом 13 (если администратор не установил иначе).

11. Далее подсистема фильтрации определяет, какой режим работы указан в конфигурационной таблице соответствующего порта для получателя IP-пакета. Если получателем пакета является абонент, работающий в режиме ретрансляции - пакет ставится в выходную очередь того порта, со стороны которого работает получатель. Если получатель должен работать через другой «ФПСУ-IP» - перед установкой в выходную очередь данные шифруются с использованием заранее согласованных ключей парно-выборочной связи. При этом, если установками конфигурации предусмотрено, что обрабатывающий «ФПСУ-IP» должен поддерживать разделение потоков, подсистема фильтрации поместит в заголовок туннелированного пакета необходимые признаки.

7. 2. 2. 4. Фильтрация ICMP-пакетов

Фильтрация ICMP-пакетов производится после проверки корректности IP-заголовка пакета (допустимого формата адресов, правильности контрольной суммы, допустимых опций и т.д.) и заключается в проверке ICMP-пакета на корректность контрольной суммы, формата и содержимого его полей. Если пакет не соответствует требованиям стандартов IP-протокола, пакет будет сброшен без посылки сообщения.

Пакет, не содержащий ICMP-сообщения об ошибке, обрабатывается как пакет IP с возможностью его передачи абоненту-получателю. Такой пакет, направленный в адрес самого «ФПСУ-IP», будет сброшен.

Если на «ФПСУ-IP» задействован межсетевой экран, выполняется проверка соответствия пакета состоянию соединения и разрешенным типам пакетов ICMP-протокола. Если пакет не соответствует установленным правилам, он будет сброшен.

Если пакет является ICMP-сообщением об ошибке, то будет проверен тип сообщения и его код. Если они соответствует требованиям соответствующих RFC - пакет без фильтрации (в установленном администратором режиме) будет передан абоненту (за исключением случая, когда в результате включения администратором режима сокрытия факта работы «ФПСУ-IP» запрещена передача ICMP-сообщений об истечении времени жизни пакетов).

7. 2. 3. Механизмы идентификации и аутентификации

Идентификация и аутентификация производятся элементами комплекса «ФПСУ-IP» в туннелях, которые могут быть созданы между:

- двумя «ФПСУ-IP»;
- «ФПСУ-IP» и «ФПСУ-IP/Клиентом»;
- «ФПСУ-IP» и УА ФПСУ-IP.

В зависимости от требований политики безопасности для идентификации и аутентификации пакетов абонентов могут быть организованы более сложные (комбинированные) межсетевые туннели типа «ФПСУ-IP» – «ФПСУ-IP» –...– «ФПСУ-IP», обеспечивающие защиту на пути следования от первого «ФПСУ-IP» до последнего, а также туннели типа «ФПСУ-IP/Клиент» – «ФПСУ-IP» – «ФПСУ-IP/Клиент» и «ФПСУ-IP/Клиент»– «ФПСУ-IP»–...– «ФПСУ-IP»– «ФПСУ-IP/Клиент», обеспечивающие защиту на всём пути следования передаваемых данных.

7. 2. 3. 1. Взаимные идентификация и аутентификация «ФПСУ-IP»

Идентификация и аутентификация пакетов абонентов в туннеле между двумя «ФПСУ-IP» осуществляются в том случае, если в конфигурации каждого «ФПСУ-IP» для удалённого абонента установлен режим работы «*Через ФПСУ*».

В комплексе «ФПСУ-IP» реализованы два механизма идентификации и аутентификации: *стартовый* и *сеансовый*. *Стартовые* идентификация и аутентификация взаимодействующих «ФПСУ-IP» осуществляются при запуске одного из «ФПСУ-IP» (или обоих) или при восстановлении работы сети после сбоев оборудования.

До окончания *стартовых* идентификации и аутентификации обоих «ФПСУ-IP» обмен пакетами абонентов между ними не производится.

В процессе *стартовых* идентификации и аутентификации согласуются режимы работы двух «ФПСУ-IP»- вырабатываются и согласуются сеансовые ключи шифрования. Эти ключи будут автоматически меняться независимо на обоих «ФПСУ-IP» по истечении периода времени, указанного при конфигурировании.

После успешного окончания *стартовой* аутентификации происходит выработка и обмен *сеансовыми* ключами, а на каждом из «ФПСУ-IP» возобновляется процесс рассмотрения поступающих на их интерфейсы пакетов абонентов, и для каждого передаваемого пакета будут осуществляться *сеансовые* идентификация и аутентификация.

На этапе *сеансовой* идентификации проверяется, что отправителем пакета является соответствующий «ФПСУ-IP». На этапе *сеансовой* аутентификации проверяется подлинность предъявляемых удалённым «ФПСУ-IP» данных, с учётом сеансовых договорённостей. Шифрование передаваемого пакета производится на производных от сеансовых ключей пакетных ключах, а аутентификация «ФПСУ-IP» - на долговременных ключах парно-выборочной связи.

Схема двусторонней аутентификации «ФПСУ-IP», работающих в паре и создающих VPN-туннель для передачи IP-пакетов, обеспечивает устойчивость передаваемых данных к пассивному и активному перехвату информации.

7. 2. 3. 2. Взаимные идентификация и аутентификация «ФПСУ-IP» и «ФПСУ-IP/Клиент»

При запросах «ФПСУ-IP/Клиента» на доступ к «ФПСУ-IP» процедуры взаимных идентификации и аутентификации «ФПСУ-IP» и «ФПСУ-IP/Клиента» являются обязательными, причём в случае неудачи стартовых процедур доступ Клиенту не предоставляется.

«ФПСУ-IP» идентифицирует «ФПСУ-IP/Клиента» по его уникальным системным номерам (номеру Криптосети, номеру группы и номеру пользователя «ФПСУ-IP/Клиента» в группе), содержащимся в конфигурационной таблице «ФПСУ-IP», а «ФПСУ-IP/Клиент» идентифицирует «ФПСУ-IP» по его IP-адресу, указанному в конфигурации «ФПСУ-IP/Клиента».

Взаимная аутентификация «ФПСУ-IP/Клиента» и «ФПСУ-IP» производится с использованием ключей, созданных при помощи специальной программы «Центр генерации ключей ФПСУ-IP/Клиентов» (ЦГКК). На внутренний накопитель данных «ФПСУ-IP» устанавливается общесистемный ключ Криптосети Клиентов, создаваемый ЦГКК, а пользователю «ФПСУ-IP/Клиента» должны быть переданы пользовательские ключи доступа.

В процессе начальной аутентификации обе стороны на базе ключа доступа «ФПСУ-IP/Клиента» и общесистемного ключа на «ФПСУ-IP» вырабатывают ключ соединения, который действует в течение текущего сеанса связи. Далее обе стороны вырабатывают сеансовые ключи и посылают их друг другу в преобразованном на ключе соединения виде.

После того, как VPN-туннель установлен, по нему начинают передаваться данные, которые преобразуются на сеансовых ключах. Сеансовые ключи автоматически меняются после передачи определенного количества данных или в случае «простоя» туннеля.

В VPN-туннеле производятся обязательные взаимные процедуры сеансовых идентификации и аутентификации данных, принимаемых из туннеля.

7. 2. 3. 3. Идентификация и аутентификация «ФПСУ-IP» и УА ФПСУ-IP

Главный принцип защищенного удаленного администрирования «ФПСУ-IP» – обеспечение взаимной идентификации и строгой двухсторонней аутентификации «ФПСУ-IP» и УА ФПСУ-IP.

Механизмы идентификации и аутентификации при взаимодействии «ФПСУ-IP» и их удалённых администраторов базируются на обязательной процедуре взаимной регистрации, без которой доступ удалённых администраторов к «ФПСУ-IP» не предоставляется.

Для осуществления взаимной регистрации каждая сторона вырабатывает персональную ключевую пару, состоящую из закрытого и открытого ключа: закрытый будет использоваться этой стороной в процессе аутентификации, а открытый предназначен для выдачи на внешний носитель и регистрации на противоположной стороне.

Регистрация производится отдельно для каждой пары субъекта и объекта управления путём обмена открытыми ключами. Кроме того, при регистрации каждого удалённого

администратора на каждом «ФПСУ-IP» локальные администраторы предоставляют удалённым администраторам права на осуществление конкретных операций дистанционного управления, которые будут контролироваться «ФПСУ-IP» в процессе взаимодействия с удалёнными администраторами.

Впоследствии полученные при регистрации от противоположной стороны открытые ключи используются в процессе обращения удалённого администратора к «ФПСУ-IP» с целью обеспечения взаимной двухсторонней аутентификации. Инициатором идентификации и аутентификации всегда является УА ФПСУ-IP.

На этапе взаимной идентификации «ФПСУ-IP» проверяет, что удалённый администратор, осуществляющий запрос, зарегистрирован по уникальному имени и не производит работу с данным «ФПСУ-IP» в текущий момент времени, а посылающая запрос программа удаленного администрирования проверяет, что ответивший на запрос «ФПСУ-IP» является именно тем «ФПСУ-IP», к которому обращался удалённый администратор.

На этапе взаимной аутентификации будет проверено, что удалённый администратор, от которого пришел запрос, обладает теми же заранее зарегистрированными данными, которыми должен обладать администратор с выявленным в процессе идентификации именем, а также что «ФПСУ-IP», к которому обращался удалённый администратор, обладает теми же заранее зарегистрированными данными, которыми должен обладать «ФПСУ-IP» с данным серийным номером.

Взаимная идентификация «ФПСУ-IP» и их удалённых администраторов осуществляется следующим образом. При посылке к «ФПСУ-IP» IP-пакета запроса, программа УА ФПСУ-IP помещает в него уникальное имя администратора (взятое из подключенного к УА ФПСУ-IP устройства «VPN-Key/UA»). При получении этого пакета «ФПСУ-IP» производит поиск имени удалённого администратора в своей регистрационной таблице. В случае отрицательного результата идентификация удалённого администратора на «ФПСУ-IP» считается невыполненной, а полученный запрос будет сброшен (с регистрацией данного события в подсистеме статистики).

В случае положительного результата «ФПСУ-IP» вышлет на УА ФПСУ-IP ответный IP-пакет, снабдив его именем удалённого администратора, которое он обнаружил в своей таблице. УА ФПСУ-IP, приняв пакет, проверяет совпадение посланных и полученных данных. При отрицательном результате проверок идентификация удалённого «ФПСУ-IP» на УА ФПСУ-IP считается невыполненной, а полученный ответ от «ФПСУ-IP» будет сброшен.

Если процесс взаимной идентификации «ФПСУ-IP» и удалённого администратора завершился успешно, УА ФПСУ-IP с использованием открытого ключа «ФПСУ-IP» проверяет, что полученный блок информации был передан именно тем зарегистрированным

«ФПСУ-IP», к которому он обращался. При отрицательном результате проверки аутентификация «ФПСУ-IP» на УА ФПСУ-IP считается невыполненной, а соответствующий IP-пакет сбрасывается (с оповещением администратора УА ФПСУ-IP о данном событии).

В случае успеха, аналогичным образом производится процедура аутентификация удалённого администратора на «ФПСУ-IP». В случае неудачи, процесс обмена информацией между «ФПСУ-IP» и удалённым администратором прекращается.

В случае успешного завершения аутентификации, полученные каждой стороной блоки информации будут являться сеансовыми аутентификаторами, используемыми при передаче каждого блока данных между «ФПСУ-IP» и УА ФПСУ-IP.

Реализованная описанным образом схема взаимной аутентификации удалённого администратора при запросах на доступ к «ФПСУ-IP» с целью контроля или управления обеспечивает устойчивость передачи данных к пассивному и активному перехвату информации в глобальных Интернет-сетях.

7. 2. 4. Поддержка ICMP-сообщений

В соответствии со спецификацией ICMP протокола ICMP-сообщения делятся на две группы:

1. ICMP-сообщения об ошибках (*Destination Unreachable*, *Redirect*, *Source Quench*, *Time Exceeded*, *Parameter Problem*),
2. ICMP-запросы (*Echo*, *Information*, *Timestamp*, *Address Mask*).

«ФПСУ-IP» способен реагировать на определённые события в сети, вырабатывая и отправляя ICMP-сообщения об ошибках типов *Destination Unreachable*, *Time Exceeded*, *Parameter Problem*, если отправка этих сообщений не мешает функционированию «ФПСУ-IP» и не занимает большую часть полосы пропускания. При сокрытии «ФПСУ-IP» своих защитных функций (в соответствии с конфигурацией) он может подавлять посылку ICMP-сообщений о недоступности абонента по причинам административного запрета (вследствие нарушений правил фильтрации), а в других сообщениях в качестве адреса отправителя ICMP-сообщения об ошибке указывать не свой IP-адрес, а адрес получателя вызвавшего ошибку пакета.

Посланные в адрес «ФПСУ-IP» ICMP-сообщения об ошибках типов *Destination Unreachable*, *Time Exceeded*, *Parameter Problem* принимаются после проверки пакетов с сообщением на корректность и учитываются в соответствии с внутренней логикой работы.

ICMP-сообщения об ошибках типа *Redirect* «ФПСУ-IP» не посылаются, а сообщения, направленные в адрес «ФПСУ-IP», принимаются и учитываются дифференцированно

(только от известных и в адрес известных «ФПСУ-IP» маршрутизаторов, явно указанных администратором «ФПСУ-IP» в конфигурации).

ICMP-сообщения типа *Source Quench* не посылаются в соответствии с рекомендациями RFC 1812.

ICMP-запросов «ФПСУ-IP» не посылает. ICMP-запросы, посланные в адрес «ФПСУ-IP», сбрасываются с генерацией соответствующего ICMP-сообщения об ошибке (код которого соответствует рекомендациям RFC 1122), если посылка сообщений не создаёт излишней нагрузки на функционирование «ФПСУ-IP».

Транзитные ICMP-сообщения всех типов, включая ICMP-запросы, доставляются нужному абоненту, если они корректны (соответствуют спецификации RFC 792 и др.) и удовлетворили всем правилам фильтрации в соответствии с установленной администратором конфигурацией. Исключение составляет ситуация, когда «ФПСУ-IP» скрывает свои фильтрующие и защитные свойства (администратором включён соответствующий переключатель конфигурации) - в этом случае транзитные сообщения *Time Exceeded* комплексом пропускаться не будут.

ICMP-сообщения типов, отличных от описанных в указанных RFC, «ФПСУ-IP» не пропускаются (сбрасываются без сообщения об ошибке).

7. 2. 5. Обработка IP-опций

Защитные функции «ФПСУ-IP» накладывают некоторые ограничения на используемые абонентами стандарты стека протоколов TCP/IP. Это связано с тем, что некоторые IP-опции (*Source Route, Record Route, Timestamp*) способствуют возможности раскрытия топологий защищаемых областей и предоставляют возможность обхода фильтрующих защитных комплексов (см. RFC 1812). «ФПСУ-IP» предоставляет администратору возможность указать метод обработки таких опций.

С точки зрения возможных угроз такие опции могут быть разделены на две категории:

1. Опции *(Record Route, Timestamp)*, требующие при передаче пакета вставить IP-адрес транзитной рабочей станции в заголовок пакета, что позволит злоумышленнику определить факт существования некоего сетевого узла (маршрутизатора) и логически увязать этот узел с группой адресов защищаемых абонентов.
2. Опции *(Source Route)*, содержащие требования доставить пакет по фиксированному маршруту, возможно в обход средств защиты и фильтрации.

Первую группу опций «ФПСУ-IP» игнорирует, то есть пакет, содержащий IP-опцию

этой группы, будет передан (если он удовлетворил требованиям фильтрации) без выполнения требований опции, что не вызовет нарушений в работе сети.

Способ обработки второй группы опций должен быть указан администратором при конфигурировании, поскольку невыполнение требований этих опций влияет на работу сети. Опция второй группы может быть выполнена, очищена (пакет проследует по маршруту, который предусмотрел для него администратор) или пакету может быть отказано в передаче (он будет сброшен без оповещения).

Остальные IP-опции обрабатываются комплексом «ФПСУ-IP» в соответствии со стандартом IP-протокола.

7. 3. Подсистема сжатия и подсистема туннелирования

Подсистемы сжатия и туннелирования могут быть задействованы для работы каждой пары абонентов только в том случае, если «ФПСУ-IP» установлены на обоих концах канала связи между ними, причём конфигурации «ФПСУ-IP» должны быть согласованы. Кроме того, подсистема туннелирования автоматически задействуется при работе с «ФПСУ-IP/Клиентами» и УА ФПСУ-IP.

При работе абонентов через пару (или более) «ФПСУ-IP», аутентификация абонентов будет производиться автоматически, а применение сжатия и криптозащита указывается в описателях параметров работы абонентов администраторами. Режимы сжатия и шифрования на «ФПСУ-IP» устанавливаются для работы с каждым отдельно взятым «ФПСУ-IP» независимо друг от друга.

Режим туннелирования может быть включен без режима шифрования, для этого в настройках конфигурирования удаленного ФПСУ-IP необходимо установить режим «криптозащита – запрещено». В этом случае пакеты будут упаковываться в туннель с заменой адресов, но шифроваться не будут.

Подсистема сжатия позволяет осуществить высокоэффективное сжатие передаваемых данных внутренним компрессором «ФПСУ-IP» с целью уменьшения объёма передаваемых данных, сокращения времени их передачи и уменьшения расходов на эксплуатацию сети.

При использовании режима криптозащиты, информация абонентов при передаче зашифровывается в соответствии с ГОСТ 28147-89.

Ответственность за согласование конфигураций двух «ФПСУ-IP», через которые осуществляется соединение абонентов, и соответствие установленных на них режимов несёт администратор. Реальный режим будет зависеть от конфигурации обоих комплексов, а ошибка администратора при установке режима может привести к несоблюдению требуемой

степени защиты и даже к невозможности установления соединения.

Возможные варианты установки каждого из режимов для каждого из двух взаимодействующих «ФПСУ-IP» следующие:

- ***запрещено*** - режим запрещён для данного канала передачи данных;
- ***нежелательно*** - использование режима нежелательно, но допускается при выборе на другом «ФПСУ-IP» режима «желательно» или «обязательно»;
- ***желательно*** - режим будет использован только в тех случаях, когда на другом «ФПСУ-IP» выбран режим «нежелательно», «желательно» или «обязательно»;
- ***обязательно*** - для данного канала передачи данных режим является обязательным.

Таблица, представленная ниже, отображает фактический режим передачи данных абонентов, который будет являться результатом установок работы каждого из двух участвующих в соединении «ФПСУ-IP» с удалённым партнёром.

Таблица 2. Режимы взаимодействия ФПСУ

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

7. 4. Подсистема регистрации (статистики)

7. 4. 1. Регистрация и учет статистической информации при функционировании «ФПСУ-IP»

В «ФПСУ-IP» реализован механизм автоматического автономного сбора статистической информации при функционировании комплекса: о результатах фильтрации (положительных и отрицательных) в различных режимах работы «ФПСУ-IP», а также действиях локальных и удалённых администраторов по управлению комплексом и

изменению правил фильтрации.

В состав «ФПСУ-IP» входит специальная подсистема регистрации (статистики), которая накапливает и хранит информацию, предоставляет администратору средства для просмотра и анализа накопленных данных статистики, а также осуществляет их автоматический анализ и сортировку в соответствии с заданными администратором условиями.

Подсистема статистики позволяет осуществлять регистрацию и учет фильтруемых пакетов с результатами их соответствия установленным правилам фильтрации. В процессе фильтрации регистрируются:

- IP-адреса отправителей и получателей или идентификационные данные «ФПСУ-IP/Клиентов»;
- время наступления события (берется локальное на «ФПСУ-IP»);
- результат фильтрации;
- попытки нарушения правил фильтрации (при этом осуществляется локальная сигнализация на экране монитора, а также звуковая и визуальная сигнализация на УА ФПСУ-IP при условии, что такая сигнализация была установлена администратором УА ФПСУ-IP);
- объём отфильтрованной информации;
- при отрицательном результате фильтрации - причина отказа в пропуске пакета;
- режим фильтрации («Ретрансляция» или «Через ФПСУ»);
- применение сжатия и/или шифрования при работе в режиме «Через ФПСУ».

Механизм автоматического сбора статистической информации о работе «ФПСУ-IP» позволяет также осуществлять регистрацию и учет действий администраторов, как локальных, так и удалённых.

В процессе регистрации действий администраторов фиксируются:

- дата, время и код регистрируемого события;
- результат попытки осуществления регистрируемого события (успешная / не успешная);
- идентификатор администратора, предъявляемый при попытке осуществления регистрируемого события (для локальных администраторов - зарегистрированный ТМ-идентификатор, для удалённых - уникальное имя).

При работе локальных операторов, инженеров и администраторов, обслуживающих комплекс, регистрируются следующие события:

- включение питания «ФПСУ-IP»;
- запуск «ФПСУ-IP» в режим фильтрации пакетов;

- завершение режима фильтрации пакетов на «ФПСУ-IP»;
- регистрация, перерегистрация и снятие с учёта персональных ТМ-идентификаторов администраторов;
- любое изменение конфигурации «ФПСУ-IP», в том числе правил фильтрации;
- изменение конфигурации LAN-портов;
- замена используемых комплектов ключей парно-выборочной связи;
- регистрация, изменение прав и снятие с учёта удалённых администраторов «ФПСУ-IP»;
- установка дополнительного программного обеспечения на «ФПСУ-IP».

При работе удалённых администраторов, взаимно с «ФПСУ-IP» зарегистрированных и аутентифицированных, на комплексе регистрируются следующие события:

- запрос с УА ФПСУ-IP статистической информации;
- ошибочные действия;
- получение конфигурации;
- автоматическое согласование времени;
- коррекция времени по приказу администратора УА ФПСУ-IP;
- указание к использованию новых данных аутентификации;
- изменение общих параметров конфигурации;
- изменение параметров доступа;
- изменение параметров LAN-порта;
- изменение параметров ФПСУ-порта;
- изменение параметров маршрутизаторов;
- изменение параметров абонентов;
- установка дополнительного программного обеспечения на «ФПСУ-IP» и изменений к существующему программному обеспечению.

Все данные об указанных событиях записываются в специальное хранилище на внутреннем накопителе «ФПСУ-IP».

Все записи базы данных снабжены контрольными суммами, которые автоматически проверяются при обращении к записям базы данных.

Хранилище регистрационной информации построено по принципу кольцевого списка: при переполнении начальные записи стираются, а текущая запись добавляется в конец списка. Предусмотрена выдача посуточных статистических отчётов об объёмах обработанной информации, как поступившей для фильтрации на «ФПСУ-IP», так и успешно прошедшей фильтрацию. Информация из хранилища может быть записана администратором на внешний носитель для последующего хранения или анализа или отправлена на УА ФПСУ-IP.

Возможность ручного удаления регистрационных записей «ФПСУ-IP» отсутствует. Это позволяет исключить попытки сокрытия каких-либо событий администраторами.

Регистрационная информация может быть просмотрена как допущенным специалистом, обслуживающим сам «ФПСУ-IP», так и удалённым администратором.

Накапливаемая статистика может автоматически передаваться в базу данных статистики УА ФПСУ-IP, который устанавливает временной период автоматического опроса и нужные ему типы статистики.

Информация в базе данных статистики «ФПСУ-IP» сортируется по типам и хранится с указанием времени записи, что позволяет выдавать для просмотра и записи во внешний файл только необходимую администратору информацию.

7. 4. 2. Контроль процесса фильтрации

«ФПСУ-IP» предоставляет возможность непосредственно контролировать его работу.

При работе комплекса на экран монитора «ФПСУ-IP» (если он подключён к «ФПСУ-IP») может быть выдана текущая информация следующих типов:

- о состоянии работы подсистемы фильтрации пакетов абонентов;
- о состоянии работы сетевых адаптеров «ФПСУ-IP»;
- о состоянии работы ARP-протокола;
- о состоянии туннелей со смежными «ФПСУ-IP»;
- о действиях удалённых администраторов;
- о работе «ФПСУ-IP/Клиентов»;
- о состоянии работы подсистемы «горячего» резервирования;
- накопленная за текущие сутки статистика;
- загруженность процессора за определённый период времени, то есть процент использования времени его работы.

Выводимая на экран информация, в частности, о нарушениях правил фильтрации и причинах отказов в передаче пакетов, позволяет оперативно настраивать работу «ФПСУ-IP» и связанных с ним подсетей, а также оперативно реагировать на попытки несанкционированного доступа к информации.

7. 4. 3. Дистанционный контроль процесса фильтрации

Непосредственный контроль за работой «ФПСУ-IP» (в частности, за состоянием работы подсистемы фильтрации и работы абонентов через «ФПСУ-IP») может также осуществлять и администратор УА ФПСУ-IP.

«ФПСУ-IP» содержит возможность дистанционной сигнализации попыток нарушения правил фильтрации нескольким зарегистрированным на данном комплексе подсистемам удалённого администрирования, а также дистанционного оповещения об изменениях его конфигурации (как локальными, так и удаленными администраторами), дистанционных установках данных аутентификации, дистанционных изменениях текущего времени на «ФПСУ-IP» и установках изменений/дополнений к программному обеспечению «ФПСУ-IP».

УА ФПСУ-IP позволяет с указанной его администратором периодичностью производить опрос подконтрольных «ФПСУ-IP» и автоматически анализировать полученные данные. Администратор УА ФПСУ-IP, используя графический интерфейс, может отслеживать состояние «ФПСУ-IP» и указывать различные типы реакции на произошедшие события как посредством визуального отображения, так и звуковой сигнализации.

7. 5. Подсистема удаленного администрирования

Подсистема удаленного администрирования выполняет следующие функции:

- позволяет регистрировать удалённых администраторов с присвоением им конкретных прав на доступ к управлению «ФПСУ-IP»;
- предоставляет средства для выдачи открытого ключа «ФПСУ-IP» на внешний носитель для регистрации его удалёнными администраторами;
- осуществляет идентификацию и аутентификацию удалённых администраторов при запросах на доступ к «ФПСУ-IP»;
- контролирует права удалённого администратора при запросах на доступ к «ФПСУ-IP»;
- предоставляет возможность дистанционного доступа к подсистемам «ФПСУ-IP».

При регистрации каждого удалённого администратора на «ФПСУ-IP» локальный администратор «ФПСУ-IP» (только классов «*администратор*» или «*главный администратор*») устанавливает права регистрируемого администратора УА ФПСУ-IP на доступ к подсистемам «ФПСУ-IP».

Всем зарегистрированным на «ФПСУ-IP» удалённым администраторам автоматически предоставляются следующие права:

- опрос состояния «ФПСУ-IP», то есть получение текущей информации о состоянии работы абонентов, сетевых адаптеров «ФПСУ-IP», ARP-протокола, смежных «ФПСУ-IP», «ФПСУ-IP/Клиентов» и т.д.;
- получение регистрационных данных о работе абонентов и «ФПСУ-IP/Клиентов».

При разрешении локального администратора «ФПСУ-IP», любому удалённому администратору могут быть предоставлены права на:

- получение регистрационных данных о работе локальных и других удалённых администраторов «ФПСУ-IP»;
- право на чтение текущей конфигурации «ФПСУ-IP»;
- изменение текущей конфигурации «ФПСУ-IP»;
- установка на «ФПСУ-IP» дополнительного ПО и обновление версий существующего ПО;
- изменять установленные на «ФПСУ-IP» параметры LAN-адаптеров;
- регистрировать удалённых администраторов или менять их права на доступ к «ФПСУ-IP»;
- установка и удаление ключей-парно-выборочной связи и общесистемного ключа Криптосети Клиентов для установки межсетевых туннелей со смежными «ФПСУ-IP» и «ФПСУ-IP/Клиентами».

Только один из зарегистрированных удалённых администраторов может получить исключительное право на коррекцию системных часов «ФПСУ-IP» в соответствии со временем операционной системы рабочей станции, на которой функционирует УА ФПСУ-IP, в ручном или автоматическом режимах;

Удалённые администраторы не могут:

- вмешиваться в работу подсистемы фильтрации «ФПСУ-IP» (запускать или прекращать её работу);
- регистрировать или редактировать описатели ТМ-идентификаторов локальных администраторов «ФПСУ-IP»;
- устанавливать или изменять пароль локального администратора;
- производить проверку целостности ПО «ФПСУ-IP».

Все действия удалённых администраторов по контролю и удалённому управлению «ФПСУ-IP», включая ошибочные действия и отказ в доступе, регистрируются в подсистеме статистики «ФПСУ-IP» с указанием времени события и идентификатора администратора.

7. 6. Подсистема разделения IP-потоков

При обмене информацией между двумя «ФПСУ-IP», работающими в паре в режиме защиты передаваемой информации от НСД, данные абонента передаются по сети в туннелированном виде. В процессе упаковки данных абонента в VPN-туннель производится сокрытие объектов/субъектов передачи и прикладных сервисов, так что любая рабочая станция на пути следования IP-пакетов от одного «ФПСУ-IP» к другому может «видеть» в их

IP-заголовках только IP-адреса отправляющего и получающего «ФПСУ-IP» и номер IP-протокола, по которому осуществляется обмен между «ФПСУ-IP».

Поэтому, если на пути следования таких пакетов находится транзитный 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, такой маршрутизатор не может самостоятельно выделить из передаваемых данных необходимые ему для реализации указанных функций признаки.

Для ликвидации этой проблемы и согласования работы «ФПСУ-IP» и транзитных маршрутизаторов разработана специальная подсистема, позволяющая разделить поступающие в VPN-туннель данные на несколько (максимально сто двадцать восемь, 128) различных потоков и помещать в выходные VPN-пакеты признаки (различные номера IP-протоколов), которые могут быть использованы транзитными маршрутизаторами (при соответствующих установках в их конфигурации).

Понятно, что для эффективной совместной работы «ФПСУ-IP» и транзитных маршрутизаторов по разделению и передаче потоков требуется согласование их конфигураций. Однако, если это условие не выполняется, фатальных ошибок при передаче данных не произойдёт и данные по VPN-туннелю будут доставлены в любом случае.

Правила разделения потоков должны быть установлены индивидуально для каждого VPN-туннеля, создаваемого парой совместно работающих «ФПСУ-IP».

В качестве критериев правил формирования потоков могут быть использованы:

- номер IP-протокола, данные которого будут содержать IP-пакеты;
- конкретные номера портов (для протоколов TCP и UDP), по которым направляются IP-пакеты;
- IP-адрес (индивидуальный или диапазон адресов) отправителя;
- IP-адрес (индивидуальный или диапазон адресов) получателя.

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 удалённому «ФПСУ-IP»). Эта проблема может быть решена при помощи «инвертирования» потоков, при котором формируются несколько конкретных потоков для IP-пакетов протоколов, использующих неизменные номера портов, а прочие не описанные явно протоколы направляются в так называемый «поток по умолчанию», который будет передаваться с «ФПСУ-IP» в IP-пакетах, содержащих в заголовке номер IP-протокола, конфигурированного на транзитном маршрутизаторе для требуемого маршрута передачи данных FTP-протокола.

Используя подсистему разделения потоков, можно формировать специальные потоки для обмена данными между «ФПСУ-IP» и их удалёнными администраторами (при условии, что этот обмен производится через ещё один «ФПСУ-IP») и при помощи транзитных маршрутизаторов направлять эти потоки по желаемому маршруту.

7. 7. Подсистема поддержки «ФПСУ-IP/Клиентов»

Подсистема поддержки «ФПСУ-IP/Клиентов» предназначена для организации VPN-туннелей между «ФПСУ-IP» и рабочими станциями, оборудованными комплексами «ФПСУ-IP/Клиент» и использующими «ФПСУ-IP» для регламентированного безопасного доступа к защищаемым «ФПСУ-IP» другим рабочим станциям сети.

В случае работы через «ФПСУ-IP», «ФПСУ-IP/Клиентам» может быть предоставлен безопасный доступ как к абонентам (серверам) защищаемой «ФПСУ-IP» подсети, так и к абонентам открытых или защищённых сетей, на компьютерах которых установлен аналогичный программно-аппаратный комплекс «ФПСУ-IP/Клиент».

При получении запроса «ФПСУ-IP/Клиента» на доступ к «ФПСУ-IP» подсистема поддержки «ФПСУ-IP/Клиентов» производит обязательные процедуры идентификации и аутентификации «ФПСУ-IP/Клиента», причём в случае неудачи доступ «ФПСУ-IP/Клиенту» не предоставляется. Затем между идентифицированным и аутентифицированным «ФПСУ-IP/Клиентом» и «ФПСУ-IP» создаётся VPN-туннель, по которому данные передаются в зашифрованном на сеансовых ключах виде. Сеансовые ключи вырабатываются в процессе аутентификации и автоматически меняются после передачи определенного количества данных или в случае «простоя» туннеля.

Получаемые из VPN-туннеля пакеты контролируются на целостность, расшифровываются и передаются соответствующим подсистемам «ФПСУ-IP» для проведения фильтрации по задаваемой администратором совокупности критериев, в качестве которых могут выступать:

- IP-адреса получателей или идентификационные номера «ФПСУ-IP/Клиентов»;
- номера IP-протоколов;
- порты TCP/UDP;
- время доступа;
- режим соединений (непосредственные или через другие «ФПСУ-IP»).

Далее отфильтрованные запросы «ФПСУ-IP/Клиентов» обрабатываются в зависимости от режима работы, установленного администратором «ФПСУ-IP» для абонентов-получателей, и передаются по назначению. Если получатель находится в защищаемой «ФПСУ-IP» области и может работать с «ФПСУ-IP» напрямую, данные

отправляются ему в открытом виде. Если получателем запроса является другой «ФПСУ-IP/Клиент» (который на текущий момент времени должен установить VPN-туннель с данным «ФПСУ-IP»), данные вновь шифруются с применением сеансовых ключей доступа получателя. Если же получателю разрешено получать пакеты от данного «ФПСУ-IP» только в защищённом режиме, пакеты (как открытые, так и шифрованные) отправляются в VPN-туннель с соответствующим «ФПСУ-IP».

В соответствии с логической структурой пользователей комплексов «ФПСУ-IP/Клиент», каждый «ФПСУ-IP/Клиент» входит в нумерованную логическую группу, а группы объединяются в Криптосети Клиентов, принадлежащие, как правило, отдельным организациям. Каждому «ФПСУ-IP/Клиенту» ставится в соответствие совокупность уникальных системных номеров (номер Криптосети, номер группы и номер пользователя «ФПСУ-IP/Клиента» в группе), используемых подсистемой поддержки с целью идентификации «ФПСУ-IP/Клиентов».

Аутентификация «ФПСУ-IP/Клиентов» производится с использованием общесистемного ключа Криптосети Клиентов, созданного при помощи программы «Центр генерации ключей ФПСУ-IP/Клиентов» (ЦГКК) и установленного на внутренний накопитель «ФПСУ-IP». ЦГКК вырабатывает один общий для Криптосети Клиентов ключ, который может храниться в распределенном виде на нескольких (до восьми) электронных носителях Touch Memory. Ключ может быть воссоздан и установлен на «ФПСУ-IP» только в том случае, если будут предъявлены все ТМ-носители.

В процедурах идентификации и аутентификации не участвует IP-адрес рабочей станции «ФПСУ-IP/Клиента», что обеспечивает пользователям «ФПСУ-IP/Клиента» возможность мобильной работы через «ФПСУ-IP» с любого компьютера или мобильного устройства, оборудованного комплексом «ФПСУ-IP/Клиент» (при условии, что такие миграции пользователей не противоречат политике безопасности организации и разрешены администратором «ФПСУ-IP»).

При передаче запросов «ФПСУ-IP/Клиентов» через какой-либо из портов «ФПСУ-IP», последний может производить трансляцию сетевого адреса (Network Address Translation - NAT) устройства «ФПСУ-IP/Клиента» в IP адрес, не совпадающий ни с одним из доступных «ФПСУ-IP» адресов. Однако использование NAT-трансляции ограничено: её нельзя применять при описании сетевых серверов, на которых установлены комплексы «ФПСУ-IP/Клиент».

«ФПСУ-IP» может дать указание компьютеру «ФПСУ-IP/Клиента» во время существования VPN-туннеля блокировать сторонние исходящие и входящие Интернет-соединения, во избежание динамического перехвата незащищённой информации и/или

использования компьютера «ФПСУ-IP/Клиента» в качестве маршрутизатора.

Чтобы предоставить пользователю «ФПСУ-IP/Клиент» доступ через «ФПСУ-IP» и обеспечить его аутентификацию, администратор «ФПСУ-IP» должен:

- установить на «ФПСУ-IP» общесистемный ключ его Криптосети Клиентов;
- указать системные идентификаторы пользователя (номер Криптосети, номер группы и номер пользователя в группе);
- выдать разрешение на работу пользователю «ФПСУ-IP/Клиента» с указанными выше системными идентификаторами;
- определить общие правила соединения «ФПСУ-IP» с данным «ФПСУ-IP/Клиентом» со стороны каждого из портов.

Далее, с целью обеспечения требований установленной в организации политики безопасности, варьируются другие конфигурационные параметры: применение NAT-трансляции, режим соединений и режим принудительной фильтрации «ФПСУ-IP/Клиентом» сторонних по отношению к VPN-туннелю с «ФПСУ-IP» IP-пакетов.

И, для более точной настройки, указанному пользователю «ФПСУ-IP/Клиента» могут быть назначены правила межсетевого экрана для ограничения доступа через данный «ФПСУ-IP»: определяются доступные пользователю рабочие станции и другие «ФПСУ-IP/Клиенты», допустимое время работы, разрешённые номера IP-протоколов и т.д. Все эти операции доступны администраторам «ФПСУ-IP», имеющим право на конфигурирование «ФПСУ-IP» (локальным и удалённым).

Подсистема поддержки «ФПСУ-IP/Клиентов» является опциональной, то есть может как входить, так и не входить в состав ПО «ФПСУ-IP», а также может быть поставлена отдельно и установлена на уже функционирующий «ФПСУ-IP» в качестве дополнительного программного обеспечения.

7. 8. Подсистема «горячего» резервирования работы «ФПСУ IP»

Подсистема поддержки «горячего» резервирования предназначена для обеспечения бесперебойной работы локальной сети, защищённой «ФПСУ-IP», в условиях возможных отказов аппаратного обеспечения комплекса.

Для реализации резервирования, два «ФПСУ-IP», на каждом из которых установлена описываемая подсистема, объединяются через третью LAN карту при помощи перекрестного сетевого кабеля в пару, называемую кластером (см. рисунок ниже). Оба «ФПСУ-IP» подключаются к локальной сети параллельно, с использованием концентраторов (hub), коммутаторов (switch) или маршрутизаторов.

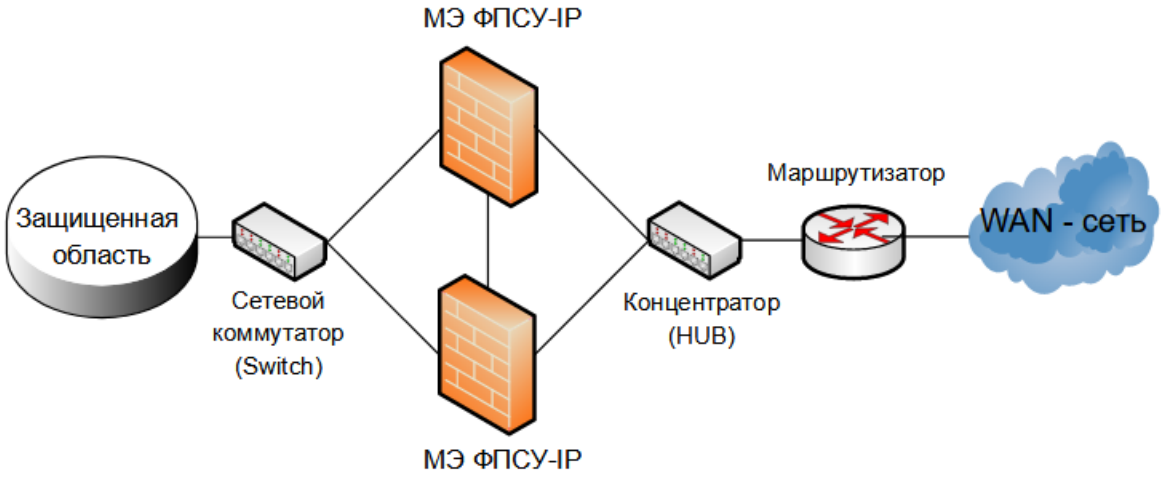

Рисунок 3 - Схема горячего резервирования

При запуске системы «горячего» резервирования в рабочий режим, в каждый момент времени один из «ФПСУ-IP» является активным, выполняя все функциональные операции, а второй находится в режиме ожидания, периодически проверяя работоспособность первого. В случае отсутствия ответа от активного компонента в течение некоторого времени, или при возникновении аппаратных неполадок на активном, резервный «ФПСУ-IP» автоматически принимает управление работой кластера на себя. Передача управления резервному «ФПСУ-IP» может также осуществляться по приказу оператора или удалённого администратора.

Поддержка «горячего» резервирования осуществляется только в том случае, когда оба «ФПСУ-IP» подключены к сети передачи данных и сети электропитания, и на каждом из них запущена подсистема фильтрации.

Для объединения «ФПСУ-IP» в пару на каждом из них должен быть установлен один или два дополнительных сетевых адаптер, которые необходимо конфигурировать как порты резервирования. Физическое соединение «ФПСУ-IP» (подключение и исправность соединительного кабеля) обеспечивается эксплуатирующей организацией.

Для защиты канала связи от НСД во время обмена данными между двумя «ФПСУ-IP», организуется специальный VPN-туннель, в котором производятся аутентификация взаимодействующих «ФПСУ-IP» и шифрование информации с помощью ключа горячего резервирования, который вырабатывается при обязательной регистрации партнёра по резервированию на каждом из «ФПСУ-IP».

Помимо взаимной проверки функционирования во время работы подсистемы резервирования, осуществляется синхронизация конфигурационных данных, ключей парно-выборочной связи с другими «ФПСУ-IP», ключевых данных «ФПСУ-IP/Клиентов»,

обновлений программного обеспечения или изменений текущего времени.

Режим функционирования («основной» «ФПСУ-IP» или «резервный» «ФПСУ-IP») устанавливается один раз при инсталляции программного обеспечения «ФПСУ-IP», однако в процессе работы любой из них может находиться в активном (осуществлять функции «ФПСУ-IP» по переброске и обработке данных) или пассивом состоянии.

Подсистема «горячего» резервирования является опциональной.

8. Контроль целостности программного обеспечения

8. 1. Общие сведения о контроле целостности

«ФПСУ-IP» разработан таким образом, чтобы исключить вмешательство в логику его работы и несанкционированный доступ к информационной и программной частям. Это обеспечивается функционированием «ФПСУ-IP» под управлением собственной, изолированной и функционально замкнутой, операционной среды.

«ФПСУ-IP» не может содержать другого программного обеспечения, кроме собственного ПО, поскольку специальные модули «ФПСУ-IP» осуществляют защиту внутреннего накопителя от изменения записанной на нем информации и загрузки с внешних устройств каких-либо операционных систем. Интерфейс администратора предоставляет ему только функционально обусловленные средства работы, исключающие просмотр системной информации, считывание или запись на внешние носители произвольно выбранных данных и т.д.

Информация на внутреннем накопителе «ФПСУ-IP» хранится в зашифрованном виде, причём ключ находится вне «ФПСУ-IP» (на ТМ-идентификаторах администраторов комплекса), что обеспечивает защиту от просмотра и целостность данных даже в случае кражи внутреннего накопителя данных и попытки прочесть или изменить его содержимое на другом компьютере.

Подсистема ACCESS TM-SHELL при старте «ФПСУ-IP» производит контроль целостности среды функционирования «ФПСУ-IP» по хранящимся на внутреннем накопителе контрольным суммам.

Контроль целостности установочных носителей обеспечивается путем вычисления контрольных сумм инсталляционных файлов перед установкой на внутренний накопитель, и сравнением полученных результатов с эталонными данными.

Во избежание нарушения защитных свойств «ФПСУ-IP» в результате программных или аппаратных сбоев, программное обеспечение «ФПСУ-IP» содержит ряд механизмов проверки целостности своих информационных и программных частей. Конфигурационные данные (включая правила фильтрации) контролируются специальными модулями ПО при каждой попытке их использования по специальным контрольным суммам. Целостность аутентификационных данных и ключей парно-выборочной связи, а также общесистемных ключей Криптосетей Клиентов проверяется при каждом считывании с диска путём подсчёта их имитовставки и сравнения полученных данных с исходным значением.

Главный администратор «ФПСУ-IP» имеет возможность осуществить

дополнительный контроль целостности программных и информационных частей «ФПСУ-IP» с помощью специальной подсистемы проверки целостности модулей, использующей нелинейный алгоритм расчета - вычисление контрольных значений файлов модулей и сравнение результатов с известными эталонными данными (см. п. «Процедура дополнительного контроля целостности ПО «ФПСУ-IP»»).

Аналогичными по возможностям программами проверки целостности ПО снабжены УА ФПСУ-IP, «ФПСУ-IP/Клиент», ЦГКК и ЦВК.

8. 2. Процедура дополнительного контроля целостности ПО «ФПСУ-IP»

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

Дополнительная проверка целостности ПО «ФПСУ-IP» осуществляется из пункта «*Проверка целостности*» основного меню, и имеет три варианта проверки:

«По внутренним данным без записи результатов» – проверка ПО «ФПСУ-IP» происходит по хранящимся на внутреннем накопителе контрольным эталонным суммам, с выводом результата проверки (успешно или обнаружена ошибка) на экран.

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

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

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

После отработки программы результаты проверки будут выданы на экран монитора и в файл **FPSUHASH.LST** на тот же носитель.

Файл **FILEHASH.LST**, представляет из себя список проверяемых модулей, каждый из которых содержит: название модуля, имя проверяемого файла, размер файла, значение

полученной при проверке контрольной суммы и комментарий. В комментарии отражен результат проведения проверки модуля:

- **«РЕЗУЛЬТАТ — ВЕРНО»** в случае совпадения данных проверяемого модуля контрольным данным;
- **«*Ошибка:»** в противном случае, с уточнением несоответствия.

Файл листинга **FILEHASH.LST** содержит текст в кодировке OEM/DOS и может быть открыт любым текстовым редактором, поддерживающим кодировку (например, стандартный Notepad.exe ОС Windows, шрифт Terminal). Результаты контрольных сумм, полученные при проверке, могут быть визуально сверены администратором с эталонными значениями, находящимися в формуляре на изделие.

9. Восстановление работы после сбоев оборудования

Сбои оборудования не влияют на защитные функции комплекса «ФПСУ-IP», однако некоторые аппаратные неполадки могут нарушить работоспособность «ФПСУ-IP», что приведёт к изоляции защищённого им IP-фрагмента. При авариях такого оборудования «ФПСУ-IP», как ЦПУ, материнская плата и др., неисправные устройства могут быть заменены, 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 признаков о неработоспособности, «ФПСУ-IP» полностью перезагружается. Если работоспособность перезагрузкой восстановить не удаётся, «ФПСУ-IP» переходит в режим звукового оповещения администратора для принятия мер по замене неисправного оборудования. Если замена оборудования повлечёт за собой изменения в программных настройках LAN-адаптеров, такая операция доступна только локальному администратору класса не ниже «Инженер».

При необходимости, внутренний накопитель данных «ФПСУ-IP» может быть переставлен на другой «ФПСУ-IP».

Аварии внутреннего накопителя «ФПСУ-IP», влекущие за собой необходимость его замены и переустановки ПО «ФПСУ-IP» на новый внутренний накопитель, наиболее критичны в смысле времени восстановления работоспособности «ФПСУ-IP» и защищаемой им ЛВС, поскольку все рабочие установки «ФПСУ-IP» и записанные на внутренний накопитель 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 внутреннего накопителя, «ФПСУ-IP» продолжит функционировать без регистрации событий в хранилище «ФПСУ-IP» (если политика безопасности организации это допускает). При этом подсистема мониторинга не прекращает своей работы, и контроль за процессом фильтрации может осуществлять удалённый администратор со своего компьютера и УА ФПСУ-IP.

Для быстрого восстановления работы «ФПСУ-IP», следует хранить текущую конфигурацию «ФПСУ-IP» на внешнем USB-носителе и на УА ФПСУ-IP (такая возможность поддерживается программным обеспечением «ФПСУ-IP»). В таком случае при смене внутреннего накопителя и повторной инсталляции ПО «ФПСУ-IP» (или замене всей аппаратной основы «ФПСУ-IP»), администратор может восстановить конфигурацию «ФПСУ-IP» с внешнего носителя, после чего заново установить ключи парно-выборочной связи для работы со смежными «ФПСУ-IP» и общесистемные ключи Криптосетей Клиентов, а также настроить сетевые адаптеры. Для осуществления указанных действий

необходимы права администратора или главного администратора.

Для быстрого возобновления работы «ФПСУ-IP» (и защищаемой ЛВС) после сбоев электропитания, «ФПСУ-IP» комплектуется подсистемой автозапуска. Подсистема автозапуска позволяет автоматически, без участия оператора, запустить «ФПСУ-IP» в режим фильтрации пакетов в случае перезагрузки «ФПСУ-IP» из-за сбоя электропитания.

Неполадки рабочей станции с установленной на ней УА ФПСУ-IP не влияют на работу сети и безопасность передачи информации, однако могут привести ко временной потере контроля за работой «ФПСУ-IP». Если аппаратные сбои УА ФПСУ-IP вызываются нарушениями функций его ПЗУ и влекут за собой переустановку программного обеспечения, то быстрое восстановление настроек производится с использованием устройства «VPN-Key/UA» и резервной копии «УА ФПСУ-IP». Хранящиеся в устройстве «VPN-Key/UA» ключевые данные администратора УА ФПСУ-IP позволяют избежать повторной регистрации администратора УА ФПСУ-IP на подконтрольных «ФПСУ-IP», а в резервной копии хранятся открытые ключи зарегистрированных «ФПСУ-IP» и собственные настройки УА ФПСУ-IP.