УТВЕРЖДЕН

ЛКНВ.466217.002 Д31-ЛУ

МЕЖСЕТЕВОЙ ЭКРАН ИВК КОЛЬЧУГА-К

(МЭ ИВК КОЛЬЧУГА-К)

Описание применения

ЛКНВ.466217.002 Д31

Листов 22

2023

Литера О

Подп. и дата	
Инв. № дубл.	
Взам. инв. №	
Подп. и дата	
Инв. № подл.	

АННОТАЦИЯ

Настоящий документ содержит основные сведения о применении изделия «Межсетевой экран ИВК КОЛЬЧУГА-К» (сокращенное наименование – МЭ ИВК КОЛЬЧУГА-К).

Описание применения состоит из четырех основных частей, в которых раскрываются основные вопросы применения и функционирования МЭ ИВК КОЛЬЧУГА-К. Также, рассматриваются организация входных и выходных данных в системе, и конфигурация технических средств, необходимых для применения МЭ ИВК КОЛЬЧУГА-К.

В первом разделе приводятся назначение, основные принципы организации, возможности МЭ ИВК КОЛЬЧУГА-К, ее основные характеристики, ограничения, накладываемые на область ее применения.

Во втором разделе указываются условия, необходимые для функционирования МЭ ИВК КОЛЬЧУГА-К, структура технических и программных средств и требования к ним, общие характеристики входной и выходной информации, а также требования и условия организационного, технического и технологического характера и т. п.

В третьем разделе указываются определения задачи и методы ее решения, приводится общая структура и алгоритмы функционирования МЭ ИВК КОЛЬЧУГА-К.

В четвертом разделе приводятся сведения о входных и выходных данных. Указываются их характер и организация, частота обновления и пр.

Описание применения разработано в соответствии с ГОСТ 19.502–78 «Единая система программной документации. Описание применения. Требования к содержанию и оформлению».

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ МЭ ИВК КОЛЬЧУГА-К

1.1. Назначение

МЭ ИВК КОЛЬЧУГА-К предназначен для реализации контроля за информацией, поступающей в автоматизированную систему (АС) и (или) выходящей из АС, и обеспечения защиты АС посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в(из) АС.

МЭ ИВК КОЛЬЧУГА-К может применяться для обеспечения защиты распространения информации АС по каналам компьютерных сетей в условиях автономной работы в круглосуточном режиме эксплуатации.

Возможности, заложенные в МЭ ИВК КОЛЬЧУГА-К, могут служить элементом основы для разработки политики безопасности АС в области организации защиты сетей предприятий, организаций и учреждений всех возможных типов, направлений и форм собственности, где должна быть обеспечена защита данных на конфиденциальном уровне.

МЭ ИВК КОЛЬЧУГА-К предназначен для применения в значимых объектах критической информационной инфраструктуры 1 категории, в государственных информационных системах 1 класса защищенности, в автоматизированных системах управления производственными и технологическими процессами 1 класса защищенности, в информационных системах персональных данных при необходимости обеспечения 1 уровня защищенности персональных данных, в информационных системах общего пользования II класса.

1.2. Функциональные возможности и основные характеристики

МЭ ИВК КОЛЬЧУГА-К представляет собой программно-аппаратный комплекс, реализующий функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков, применяется в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа.

МЭ ИВК КОЛЬЧУГА-К обеспечивает нейтрализацию следующих угроз безопасности информации:

- несанкционированный доступ к информации, содержащейся в информационной системе;
- отказ в обслуживании информационной системы и(или) ее отдельных компонентов;
- несанкционированная передача информации из информационной системы в информационно-телекоммуникационные сети или иные информационные системы;
- несанкционированное воздействие на МЭ ИВК КОЛЬЧУГА-К, целью которого является нарушение его функционирования, включая преодоление или обход его функций безопасности;
- несанкционированное получение сведений о сети информационной системы (автоматизированной системы управления), а также об ее узлах;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внешних нарушителей, действующих из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена;
- преднамеренный несанкционированный доступ или специальные воздействия на информацию (носители информации) со стороны внутренних нарушителей, обладающих правами и полномочиями на доступ к информации в информационной системе.

Структура и содержание КСЗ МЭ ИВК КОЛЬЧУГА-К обеспечивает выполнение функций безопасности в объеме требований, изложенных в методических документах ФСТЭК России «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты ИТ.МЭ.А4.ПЗ», «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ:

- контроль и фильтрация;
- идентификация и аутентификация;
- регистрация событий безопасности (аудит);

- обеспечение бесперебойного функционирования и восстановление;
- тестирование и контроль целостности;
- преобразование сетевых адресов;
- маскирование;
- приоритизация информационных потоков;
- управление (администрирование);
- взаимодействие с другими средствами защиты информации;
- функции системы обнаружения вторжений (СОВ):
    а) разграничение доступа к управлению системой обнаружения вторжений;
    б) управление работой системы обнаружения вторжений;
    в) управление параметрами системы обнаружения вторжений;
    г) управление установкой обновлений (актуализации) базы решающих правил системы обнаружения вторжений;
    д) анализ данных системы обнаружения вторжений;
    е) аудит безопасности системы обнаружения вторжений;
    ж) сбор данных о событиях и активности в контролируемой информационной системе;
    и) реагирование системы обнаружения вторжений.

В среде, в которой функционирует МЭ ИВК КОЛЬЧУГА-К, должны быть реализованы следующие функции безопасности среды:

- исключение каналов связи в обход правил фильтрации;
- обеспечение доверенного канала;
- обеспечение доверенного маршрута;
- обеспечение безопасного функционирования;
- физическая защита;
- обеспечение взаимодействия с сертифицированными средствами защиты информации;
- управление атрибутами безопасности.

Функции безопасности МЭ ИВК КОЛЬЧУГА-К обладают составом функциональных возможностей (функциональных требований безопасности), обеспечивающих реализацию этих функций.

Состав функциональных возможностей МЭ ИВК КОЛЬЧУГА-К:

- возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации и всех операций передачи, контролируемой МЭ информации к узлам информационной системы и от них;
- возможность обеспечения фильтрации для всех операций перемещения через МЭ информации к узлам информационной системы и от них;
- возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности субъектов: сетевой адрес узла отправителя; сетевой адрес узла получателя; интерфейс МЭ (на уровне сетевого адреса), через который проходит пакет;
- возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности информации: сетевой протокол, который используется для взаимодействия; атрибуты, указывающие на фрагментацию пакетов; транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии); разрешенные (запрещенные) команды, разрешенный (запрещенный) мобильный код;
- возможность явно разрешать информационный поток, базируясь на устанавливаемых администратором МЭ наборе правил фильтрации, основанном на идентифицированных атрибутах;
- возможность явно запрещать информационный поток, базируясь на устанавливаемых администратором МЭ наборе правил фильтрации, основанном на идентифицированных атрибутах;
- возможность блокирования всех информационных потоков, проходящих через нефункционирующий или функционирующий некорректно МЭ;
- возможность осуществлять политику фильтрации пакетов с учетом управляющих команд от взаимодействующих с МЭ средств защиты

информации других видов;

- возможность осуществлять проверку каждого пакета по таблице состояний для определения того, не противоречит ли состояние (статус, тип) пакета ожидаемому состоянию;
- возможность осуществлять проверку использования пользователями отдельных команд, для которых администратором МЭ установлены разрешительные или запретительные атрибуты безопасности;
- возможность осуществлять проверку использования сетевых ресурсов, содержащих мобильный код, для которого администратором МЭ установлены разрешительные или запретительные атрибуты безопасности;
- возможность осуществлять фильтрацию, основанную на атрибутах: разрешенные/ запрещенные протоколы прикладного уровня;
- возможность разрешать информационный поток, основываясь на результатах проверок;
- возможность запрещать информационный поток, основываясь на результатах проверок;
- возможность осуществлять фильтрацию пакетов с учетом управляющих команд от взаимодействующих с МЭ средств защиты информации других видов, основанную на атрибутах, указывающих на признаки нарушения безопасности в информации сетевого трафика;
- возможность разрешать информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на отсутствие нарушений безопасности информации;
- возможность запрещать информационный поток, если значения атрибутов безопасности, установленные взаимодействующими средствами защиты информации для контролируемого сетевого трафика, указывают на наличие нарушений безопасности информации;
- возможность осуществлять фильтрацию при импорте (перехвате) информации сетевого трафика из-за пределов МЭ;

- возможность осуществлять МЭ передачу информационных потоков с переназначением сетевых адресов отправителя и (или) получателя (трансляция адресов и посредничество в передаче), фильтрацию при экспорте (передаче от своего имени) информации сетевого трафика за пределы МЭ;
- возможность экспортировать (передавать от своего имени) информацию сетевого трафика при положительных результатах фильтрации и других проверок;
- возможность осуществлять посредничество в передаче информации сетевого трафика, основанное на типе сетевого трафика;
- возможность маскирования наличия МЭ способами, затрудняющими нарушителям его выявление;
- возможность регистрации и учета выполнения проверок информации сетевого трафика;
- возможность читать информацию из записей аудита уполномоченным администраторам;
- возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита;
- возможность оповещения уполномоченных лиц о критичных видах событий безопасности, в том числе сигнализация о попытках нарушения правил межсетевого экранирования;
- возможность выборочного просмотра данных аудита (поиск, сортировка, упорядочение данных аудита);
- возможность регистрации возникновения событий, которые в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» включены в базовый уровень аудита»;
- возможность идентификации администратора МЭ до разрешения любого

действия (по администрированию), выполняемого при посредничестве МЭ от имени этого администратора;

- возможность аутентификации администратора МЭ до разрешения любого действия (по администрированию), выполняемого при посредничестве МЭ от имени этого администратора;
- возможность осуществления идентификации и аутентификации субъектов межсетевого взаимодействия до передачи МЭ информационного потока получателю;
- поддержка определенных ролей по управлению МЭ;
- возможность со стороны администраторов управлять режимом выполнения функций безопасности МЭ;
- возможность со стороны администраторов управлять данными МЭ, используемыми функциями безопасности МЭ;
- возможность со стороны администраторов управлять атрибутами безопасности;
- возможность поддержки списка типов сетевого трафика для осуществления посредничества в передаче, предусматривающего разделение трафика по типам;
- обеспечение ассоциации типов сетевого трафика из списка с конкретным сетевым трафиком для осуществления посредничества в передаче и обработки соответствующих типов сетевого трафика прокси-агентами;
- возможность изменения области значений информации состояния соединения со стороны администраторов МЭ;
- возможность присвоения информации состояния соединения допустимых значений, таких как установление соединения, использование соединения, завершение соединения и других;
- возможность ведения для каждого соединения таблицы состояний, основанной на информации состояния соединения;
- предоставление возможности администраторам МЭ модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для

используемых пользователями отдельных команд для осуществления МЭ фильтрации;

- предоставление возможности администраторам МЭ модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности использования сетевых ресурсов, содержащих отдельные типы мобильного кода, для осуществления МЭ фильтрации;
- возможность обеспечения надежных меток времени при проведении аудита безопасности;
- возможность тестирования (самотестирования) функций безопасности МЭ (контроль целостности исполняемого кода МЭ);
- возможность сохранения штатного функционирования МЭ при некритичных типах сбоев;
- возможность согласованно интерпретировать управляющие команды, атрибуты сетевого трафика и иные данные, получаемые от взаимодействующих с МЭ средств защиты информации других видов;
- поддержка правил интерпретации данных, получаемых от взаимодействующих с МЭ средств защиты информации других видов;
- возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования;
- возможность кластеризации МЭ;
- возможность приоритизации контроля и фильтрации разных информационных потоков, а также выделения ресурсов, доступных для разных информационных потоков, обрабатываемых одновременно (в течение определенного периода времени;
- возможность сбора информации о сетевом трафике;
- возможность выполнения анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для

проведения вторжения;

- возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов;
- возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа;
- возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;
- возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;
- уведомление администратора СОВ об обнаруженных вторжениях по отношению к контролируемым узлам ИС и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления;
- возможность автоматизированного обновления базы решающих правил;
- возможность тестирования (самотестирования) функций безопасности СОВ;
- возможность со стороны уполномоченных администраторов (ролей) управлять режимом выполнения функций безопасности СОВ;
- возможность со стороны уполномоченных администраторов (ролей) управлять данными СОВ;
- поддержка определенных ролей для СОВ и их ассоциации с конкретными администраторами СОВ и пользователями ИС;
- возможность администрирования СОВ;
- возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- возможность предоставлять возможность читать информацию из записей

аудита;

- ограничение доступа к чтению записей аудита;
- поиск, сортировка, упорядочение данных аудита.

1.3. Ограничения применения

Использование МЭ ИВК КОЛЬЧУГА-К ограничивается применением в АС класса не выше 1В.

Все технические средства (ТС), на которых развертывается МЭ ИВК КОЛЬЧУГА-К, должны находиться в пределах контролируемой зоны (КЗ).

Администрирование МЭ ИВК КОЛЬЧУГА-К должно осуществляться только штатным администратором АС.

КСЗ МЭ ИВК КОЛЬЧУГА-К не предусматривает защиту АС от внешних физических воздействий. Предполагается, что защита от таких операций с целью несанкционированного съема информации должна осуществляться на организационном уровне, тем не менее, для фиксации определенных событий МЭ ИВК КОЛЬЧУГА-К ведет системные журналы, которые администратору рекомендуется чаще просматривать для формирования соответствующих выводов и принятия по ним административно-организационных, технических или иных решений.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

Основными условиями применения МЭ ИВК КОЛЬЧУГА-К являются условия требований политики безопасности, принятые в АС.

2.1. Требования к техническим средствам

Аппаратная часть МЭ ИВК КОЛЬЧУГА-К – БК ПЭВМ ИВК ЛКНВ.466215.004 ТУ, имеет сертификат соответствия ТР ТС 004/2011 и ТР ТС 020/2011 №ЕАЭС RU C-RU.RU.HA88.B.00419/19 от 07.08.2019 г.

Технические характеристики и состав комплектации БК ПЭВМ ИВК определяются спецификацией и эксплуатационной документацией на этот вариант комплектации.

2.2. Требования и условия организационного и технологического характера

Ввод в эксплуатацию и эксплуатация МЭ ИВК КОЛЬЧУГА-К должны производиться в соответствии с указаниями в эксплуатационных документах и документе «Формуляр. ЛКНВ.466217.002 ФО» на изделие.

Технические и эксплуатационные характеристики аппаратной платформы МЭ ИВК КОЛЬЧУГА-К приведены в документе БК ПЭВМ ИВК «Паспорт. ЛКНВ.466215.004.01 ПС».

Обеспечивается функционирование МЭ ИВК КОЛЬЧУГА-К с предустановленными сертифицированными АПМДЗ Программно-аппаратным комплексом «Соболь» (ПАК «Соболь»)/ Программно-аппаратным комплексом средств защиты информации от несанкционированного доступа «Аккорд-АМДЗ» (ПАК СЗИ НСД «Аккорд-АМДЗ») и СКЗИ «Рутокен ЭЦП 2.0»/ «Рутокен ЭЦП 2.0 Flash»/ «Рутокен ЭЦП 3.0» со средством криптографической защиты информации ИВК КРИПТО (СКЗИ ИВК КРИПТО). СКЗИ ИВК КРИПТО поставляется совместно с СКЗИ «Рутокен ЭЦП 2.0»/ «Рутокен ЭЦП 2.0 Flash»/ «Рутокен ЭЦП 3.0», может поставляться с ПАК «Соболь»/ ПАК СЗИ НСД «Аккорд-АМДЗ».

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Определение задачи

Задача применения МЭ ИВК КОЛЬЧУГА-К состоит в обеспечении функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков со стороны внешних компьютерных сетей – Internet (принудительные рассылки, спам, электронная почта, информация поисковых систем и пр.), а так же допущенной (разрешенной) информации, исходящей из внутренней(их) сетей АС (электронная почта, запросы на информацию поисковых систем и адресов `http://www…`, заданных явным образом) в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа.

Изделие предназначено для реализации контроля за информацией, поступающей в АС и(или) выходящей из АС, и обеспечения защиты АС посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в(из) АС в соответствии с принятой политикой безопасности в АС.

Также МЭ ИВК КОЛЬЧУГА-К реализует функции СОВ сбор информации об информационных потоках, передаваемых в рамках сегмента информационной системы, в котором установлены их датчики.

3.2. Методы решения

Методы решения задачи применения МЭ ИВК КОЛЬЧУГА-К заключаются в анализе поступающей информации и принятии решения о ее распространении посредством фильтрации по совокупности критериев, определенных политикой безопасности в АС.

Фильтрация поступающей информации производится на основании анализа заголовков пакетов и ключевых данных, находящихся в самих пакетах по атрибутам безопасности, заложенным в правила фильтрации (сетевые адреса, интерфейсы, протоколы, ключевые слова, ПРД и пр.).

Функции безопасности МЭ ИВК КОЛЬЧУГА-К с помощью NETFLOW iptables осуществляет фильтрацию для отправителей информации, получателей информации, сетевого трафика и всех операций перемещения контролируемой МЭ ИВК КОЛЬЧУГА-К информации сетевого трафика к узлам информационной системы и от них, на которые распространяется политика управления информационными потоками, в том числе с учетом управляющих команд от взаимодействующих с МЭ ИВК КОЛЬЧУГА-К средств защиты информации других видов (СОВ). Управляющие команды передаются на МЭ ИВК КОЛЬЧУГА-К в формате iptables при наличии установленного SSH соединения.

Фильтры состоят из правил. Каждое правило – это строка, содержащая в себе критерии, определяющие, подпадает ли пакет под заданное правило, и действие, которое необходимо выполнить в случае удовлетворения критерия. Функции безопасности МЭ обеспечивают распространение фильтрации на все операции перемещения через МЭ информации к узлам информационной системы и от них.

Для iptables в общем виде правила выглядят так:

```
iptables [-t table] command [match] [target/jump]
```

Если в правило не включается спецификатор `[-t table]`, то по умолчанию предполагается использование таблицы filter, если же предполагается использование другой таблицы, то это требуется указать явно. Спецификатор таблицы так же можно указывать в любом месте строки правила, однако наиболее стандартным считается указание таблицы в начале правила.

Далее, непосредственно за именем таблицы должна стоять команда управления фильтром. Если спецификатора таблицы нет, то команда всегда должна стоять первой. Команда определяет действие iptables, например: вставить правило, или добавить правило в конец цепочки, или удалить правило и т. п. Тело команды в общем виде выглядит так:

- команда цепочка;
- ключ команда указывает на то, что нужно сделать с правилом, например, команда `-A` указывает на то, что правило нужно добавить в конец указанной цепочки.

Цепочка указывает в какую цепочку нужно добавить правило. Стандартные цепочки – INPUT, OUTPUT, FORWARD, PREROUTING и POSTROUTING. Они находятся в таблицах фильтра. Не все таблицы содержат все стандартные цепочки. Подробнее таблицы и цепочки описаны ниже.

Раздел match задает критерии проверки, по которым определяется, подпадает ли пакет под действие этого правила или нет. Здесь можно указать самые разные критерии – IP-адрес источника пакета или сети, сетевой интерфейс и т. д. Существует множество критериев, которые будут рассмотрены ниже.

target указывает, какое действие должно быть выполнено при условии выполнения критериев в правиле. Здесь можно передать пакет в другую цепочку правил, «сбросить» пакет и забыть про него, выдать на источник сообщение об ошибке и т. д.

Когда пакет приходит на сетевое устройство (рис. 1), он обрабатывается соответствующим драйвером и далее передается в фильтр в ядре ОС. Далее пакет проходит ряд таблиц и затем передается либо локальному приложению, либо переправляется на другую машину. Функции безопасности МЭ ИВК КОЛЬЧУГА-К осуществляют проверку пакета при его импорте из-за пределов МЭ и экспорте за пределы МЭ, тем самым, исключая прямое взаимодействие между узлами.

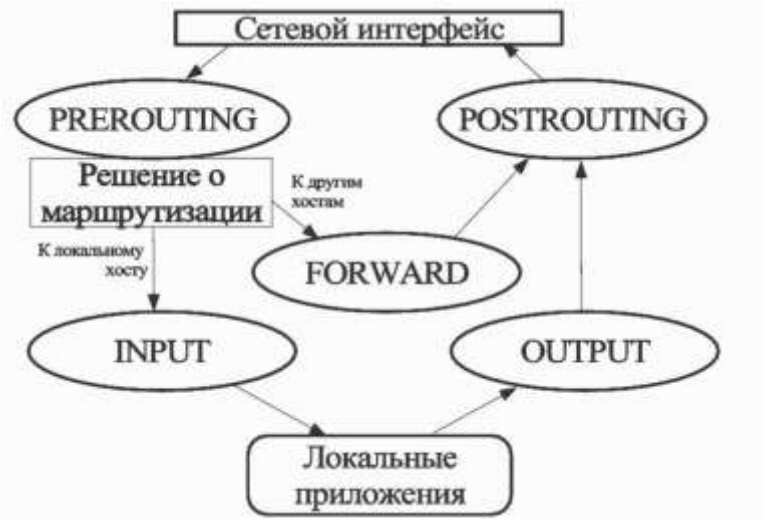

Рис. 1 – Схема движения пакетов в iptables

По умолчанию используется таблица filter. Опция `-t` в правиле указывает на используемую таблицу. С ключом `-t` можно указывать следующие таблицы: nat, mangle, filter.

Таблица filter используется главным образом для фильтрации пакетов. Для примера, здесь можно выполнить DROP, LOG, ACCEPT или REJECT без каких-либо сложностей, как в других таблицах. Имеется три встроенных цепочки FORWARD, INPUT, OUTPUT:

- цепочка FORWARD используется для фильтрации пакетов, идущих транзитом через фильтрующий компьютер;
- цепочка INPUT предназначена для обработки входящих пакетов, направляемых локальным приложениям фильтрующего компьютера;
- цепочка OUTPUT используется для фильтрации исходящих пакетов, сгенерированных локальными приложениями фильтрующего компьютера.

Функция безопасности явно запрещает информационный поток при нарушении функционирования МЭ, в частности осуществляется автоматическое создание правила блокировки трафика в цепочке FORWARD при отключении сервисов аудита, удаленного управления, а также выгрузки модулей iptables: nf_conntrack_ipv4, xt_ndpi.

Функции СОВ МЭ ИВК КОЛЬЧУГА-К реализует с использованием сигнатурного и эвристического методов обнаружении вторжений.

СОВ пропускает весь трафик через базу сигнатур, с которой сравниваются пакеты. Если содержимое пакета совпадает с сигнатурой, пакет блокируется, или применяется иное предопределенное действие. Запись о данном событии заносится в журнал.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1. Входные данные администрирования

Запросы и данные, поступающие с терминальных устройств администратора (запросы на идентификацию и аутентификацию администратора, настройка и занесение правил фильтрации для МЭ ИВК КОЛЬЧУГА-К).

Запросы и данные вводятся с использованием команд командного интерпретатора bash из состава КСЗ МЭ ИВК КОЛЬЧУГА-К и посредством графического интерфейса МЭ ИВК КОЛЬЧУГА-К.

4.2. Выходные данные администрирования

Ответы (отклики) КСЗ МЭ ИВК КОЛЬЧУГА-К на подаваемые администратором запросы на выполнение, принятие (подтверждение) или отмену произведенных действий, ошибок и т. д.

Ответы (отклики) на подаваемые запросы (действия) поступают на монитор администратора в виде системных сообщений КСЗ МЭ ИВК КОЛЬЧУГА-К посредством графического интерфейса МЭ ИВК КОЛЬЧУГА-К или стандартного консольного интерфейса ОС.

Входные и выходные данные администрирования обеспечивают возможность администратору проверять работоспособность МЭ ИВК КОЛЬЧУГА-К, влиять на ход выполнения процессов безопасности, выполняемых КСЗ, и применяются для настройки, контроля и управления МЭ ИВК КОЛЬЧУГА-К.

4.3. Входные данные внешних и внутренних компьютерных сетей

Поступающие входные данные внешних и внутренних компьютерных сетей анализируются по совокупности признаков и правил фильтрации (обработка поступивших заявок (запросов) на владение данными с использованием ПРД, отбор данных по определенным признакам (свой/чужой, доверенный/не доверенный, любые значимые поля сетевых пакетов) – фильтрация сетевых протоколов и данных), правил СОВ.

В соответствии с настройкой правил фильтрации, принятой политикой безопасности АС, не доверенные, запрещенные входные данные игнорируются (отчуждаются). Все отчуждаемые не доверенные, запрещенные входные данные являются несанкционированными попытками доступа к АС, попытки НСД и несанкционированной отправки данных фиксируются в специальном журнале и отсылаются администратору в виде сообщений для принятия решений по данным фактам нарушения правил доступа (границ безопасности).

4.4. Выходные данные внешних и внутренних компьютерных сетей

Отфильтрованные правилами безопасности АС входные данные, не являющиеся с точки зрения КСЗ попытками НСД, пропускаются для дальнейшего их распределения (доставки) адресату.

Выходные данные фиксируются в специальном журнале. Администратор может проверять (просматривать и контролировать) результаты фильтрации выходных данных и в случае подозрений на НСД принимать решения по данным фактам нарушения правил доступа (границ безопасности).

Объем и скорость обрабатываемой МЭ ИВК КОЛЬЧУГА-К входной и выходной информации зависит от технических характеристик (пропускной способности и используемых технологий) каналов передачи данных.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АС – автоматизированная система;

КЗ – контролируемая зона;

КСЗ – комплекс средств защиты;

МЭ – межсетевой экран;

НСД – несанкционированный доступ к информации;

ОС – операционная система;

ПРД – правила разграничения доступа;

РД – руководящий документ;

СОВ – система обнаружения вторжений;

СУ – система управления;

ТС – технические средства;

SSH – протокол Secure shell.

Лист регистрации изменений									
Номера листов (страниц)					*Всего листов (страниц) в докум.*	*№ документа*	*Входящий № сопроводительного докум. и дата*	*Подп.*	*Дата*
Изм.	*измененных*	*замененных*	*новых*	*аннулированных*					