

ЗАО "С-Терра СиЭсПи"

УТВЕРЖДЕНО

РЛКЕ.00005-01 90 02-ЛУ

ПРОГРАММНЫЙ КОМПЛЕКС CSP VPN Gate

ВЕРСИЯ 3.1

Правила пользования

РЛКЕ.00005-01 90 02

Листов 19

2010

СОДЕРЖАНИЕ

1. Аннотация	3
2. Назначение	3
3. Требования к системному ПО	3
4. Требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации ПК	4
4.1. Общие требования	4
4.2. Требования по размещению СВТ с установленным ПК	4
4.3. Административные меры безопасности	5
4.4. Требования по защите ПК от НСД	6
4.5. Требования по установке ПК на ПЭВМ	9
4.6. Требования по криптографической защите	11
4.7. Требования к обращению с ключевыми документами	12
4.8. Требования к процедурам конфигурирования ПК «CSP VPN Gate»	13
4.9. Требования к процедурам использования ПК «CSP VPN Gate» на МСМ	16
4.10. Требования к инфраструктуре и политике безопасности	17

1. Аннотация

Настоящий документ содержит описание правил пользования Программным комплексом «CSP VPN Gate» версии 3.1 (ПК РЛКЕ.00005-01, далее ПК).

2. Назначение

ПК РЛКЕ.00005-01 версии 3.1 является новым СКЗИ.

Программный комплекс предназначен для обеспечения:

- криптографической защиты передаваемой в режиме on-line по TCP/IP протоколу информации, не содержащей сведений, составляющих государственную тайну, между ПЭВМ абонентов;
- двусторонней криптографической аутентификации абонентов при установлении соединения в соответствии с протоколом ISAKMP.

СКЗИ «CSP VPN Gate» удовлетворяет «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классам КС1/КС2 в зависимости от комплектации исполнения.

3. Требования к системному ПО

ПК «CSP VPN Gate» функционирует на ПЭВМ с архитектурой Intel x86, в т.ч. на изделии “Модуль сетевой модернизированный”¹ (далее – МСМ), под управлением операционных систем, указанных в формуляре РЛКЕ.00005-01 30 01.

¹ Модуль, выпускаемый ЗАО «С-Терра СиЭсПи» согласно «Порядку организации производства изделия Модуль Сетевой Модернизированный (МСМ) в рамках подконтрольного технологического процесса на территории Российской Федерации»

4. Требования по организационно-техническим и административным мерам обеспечения безопасности эксплуатации ПК

4.1. Общие требования

Для безопасной эксплуатации ПК и программного обеспечения должны выполняться организационно-технические и административные требования. К ним относятся требования по физическому размещению ПК, установке программного обеспечения на ПК, средствам защиты от несанкционированного доступа (НСД) к ОС и управлению комплексом, обеспечению бесперебойного режима работы ПК.

При эксплуатации СКЗИ «CSP VPN Gate» требуется выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе по каналу связи (например, СТР-К).

При размещении ПЭВМ с СКЗИ в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну или конфиденциального характера, данные ПЭВМ должны иметь соответствующее разрешение.

4.2. Требования по размещению ПК

При размещении ПК на предприятии помещения должны удовлетворять следующим требованиям физической безопасности:

- обеспечение круглосуточной охраны корпусов предприятия
- обеспечение контроля внешнего периметра и внутренних помещений
- обеспечение пропускного режима
- рядом с окнами помещений не должно быть пожарных лестниц и водосточных труб
- двери должны быть прочными и оборудованы надежными механическими замками
- оборудование помещений системой пожарной сигнализации

- ведение Журнала выдачи ключей от входных дверей в офисы, в котором регистрируется время сдачи и выдачи ключей, фамилия сотрудника, взявшего или сдавшего ключ дежурному вахтеру по зданию
- для всех исполнений, кроме исполнения 2, принять меры по исключению несанкционированного доступа в помещения, в которых размещены ПК с установленным СКЗИ, посторонних лиц, не являющихся персоналом, допущенным к работе в этих помещениях. В случае необходимости присутствия посторонних лиц в указанных помещениях, должен быть обеспечен контроль и обеспечена невозможность каких-либо действий с их стороны на ПК
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им ПК, конфиденциальной информации, в том числе ключевой информации.

4.3. Административные меры безопасности

Безопасная эксплуатация ПК и обращения с СКЗИ должны регламентироваться следующими документами, которые следует разработать:

- Инструкция по обращению с сертифицированными ФСБ шифровальными средствами (средствами криптографической защиты информации) на предприятии
- Журнал учета СКЗИ, тестовых ключей
- Журнал регистрации администраторов безопасности
- Журнал учета обращения эталонных CD дисков.

которые разрабатываются согласно Требованиям ООО «Крипто-Про» на СКЗИ “КриптоПро CSP” версии 3.6, изложенным в документе «ЖТЯИ.00050-01 90 02. Руководство администратора безопасности. Общая часть» или «ЖТЯИ.00050-02 90 02. Руководство администратора

безопасности. Общая часть» при использовании СКЗИ «КриптоПро CSP» версии 3.6R2.

Обязательно наличие опечатываемого сейфа, оборудованного двумя внутренними замками, для хранения СКЗИ, тестовых ключей, эталонных CD дисков с ПО ПК, другой конфиденциальной информации. Для сейфа должно быть два ключа - основной ключ хранится у сотрудника, отвечающего за СКЗИ, а дубликат - в опечатанном его личной печатью пенале в сейфе Генерального директора.

4.4. Требования по защите ПК от НСД

В функции администратора безопасности входит выпуск сертификатов и конфигурирование продукта, включая управление перечнем доверенных сертификатов.

При организации работ на ПК должны быть выполнены следующие требования по защите ПК от НСД:

- администратором ПК назначается администратор безопасности
- контроль целостности программной и информационной части ПК «CSP VPN Gate» необходимо осуществлять с помощью ПО ПК не реже 1 раза в месяц при проведении периодического тестирования работоспособности ПК «CSP VPN Gate». Также для варианта комплектации 2 контролю целостности должны подвергаться файлы ОС в соответствии с эксплуатационной документацией АПМДЗ. Взаимодействие АПМДЗ с СКЗИ должно производиться в соответствии с документом «ЖТЯИ.00050-01 90 02. Руководство администратора безопасности. Общая часть» или «ЖТЯИ.00050-02 90 02. Руководство администратора безопасности. Общая часть» при использовании СКЗИ «КриптоПро CSP» версии 3.6R2. Для варианта комплектации 4 целостность файлов ОС и ПК обеспечивается устройством «МАРШ!-CF» по ТУ 4024-034-11443195-2010. Для варианта комплектации 5 целостность файлов ОС и ПК обеспечивается устройством «МАРШ!-USB» по ТУ 4024-033-11443195-2010 или СЗН «СПДС-USB-01» по ТУ 4024-001-70221576-2011.

- необходимо соблюдать правила, описанные в документе «ЖТЯИ.00050-01 90 02 Руководство администратора безопасности. Общая часть» или «ЖТЯИ.00050-02 90 02 Руководство администратора безопасности. Общая часть» при использовании СКЗИ «КриптоПро CSP» версии 3.6R2
- право доступа к ПК имеет только администратор безопасности. Примечание: для исполнения «CSP VPN Client» допускается использование ПК пользователем согласно принятой политики безопасности
- администратор безопасности должен ознакомиться со всей документацией, прилагаемой к ПК
- аутентификация администратора безопасности основана на пароле, который должен вводиться им с клавиатуры собственноручно при осуществлении доступа в ОС, не отображаясь на экране монитора в явном виде, идентификация основана на идентификаторе, который вводится с клавиатуры. При первом доступе администратор безопасности должен заменить пароль на отличный от установленного при инсталляции ПК. Для варианта комплектации 2 согласно формуляру РЛКЕ.00005-01 30 01 аутентификация осуществляется также посредством АПМДЗ согласно соответствующему руководству пользователя. Для варианта комплектации 4 аутентификация осуществляется при помощи устройства «МАРШ!-CF» согласно документу 11443195.4024-034 ПП «СЗН «МАРШ!-CF». Правила пользования». Для варианта комплектации 5 аутентификация осуществляется при помощи устройства «МАРШ!-USB» согласно документу 11443195.4024-033 ПП «СЗН «МАРШ!-USB». Правила пользования», или при помощи СЗН «СПДС-USB-01» согласно документу «РЛКЕ.00005-01 90 03 Программный комплекс "Шлюз безопасности CSP VPN Gate. Версия 3.1 "Руководство администратора».
- для вариантов комплектации 4 и 5 сеанс работы пользователя с

СКЗИ РЛКЕ.00005-01 необходимо завершать выключением питания ПЭВМ, на котором функционирует СКЗИ, или извлечением специального загрузочного носителя

- право доступа к режиму управления комплексом (пользовательскому интерфейсу ПК) имеет только администратор
- имя администратора должно быть уникальным и не превышать 8 символов
- имя администратора должно начинаться с буквы латинского алфавита (строчной или прописной). Далее могут идти буквы латинского алфавита (строчные или прописные), цифры, _ (подчеркивание) и - (дефис)
- настройку ПК (назначение IP-адресов интерфейсам, создание политики безопасности, регистрацию сертификатов, другие дополнительные настройки) осуществляет только администратор безопасности в соответствии с Руководством администратора
- необходимо организовать систему протоколирования и аудита, и вести регулярный анализ результатов аудита с целью выявления нарушений несанкционированного доступа к ПК
- необходимо разработать политику назначения и смены паролей (для входа в ОС, для доступа к управлению комплексом) в соответствии со следующими правилами, изложенными в документах «ЖТЯИ.00050-01 90 02 Руководство администратора безопасности. Общая часть» и «ЖТЯИ.00050-02 90 02 Руководство администратора безопасности. Общая часть»:
 - длина пароля должна быть не менее 6 символов
 - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, \$, &, *, % и т.п.)
 - пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т. д.), а также общепринятые сокращения (USER, ADMIN и т. д.)

- при смене пароля новое значение должно отличаться от предыдущего не менее чем на 4 символа
- администратор безопасности не имеет права сообщать никому пароль доступа к ПК
- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 год.

Запрещается:

- оставлять без контроля ПЭВМ с ПК
- осуществлять несанкционированное вскрытие ПЭВМ
- осуществлять несанкционированное администратором безопасности копирование ключевых носителей
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации
- использовать ключевые носители в режимах, не предусмотренных функционированием ПК
- записывать на ключевые носители постороннюю информацию.

Защита ПК и ключевой информации от НСД должна обеспечиваться не только в режиме функционирования, но и при проведении ремонтных и регламентных работ.

4.5. Требования по установке ПК на ПЭВМ

При поставке ПК в составе программно-аппаратного комплекса ПК «CSP VPN Gate» поставляется с настроенной операционной системой и установленным ПО ПК. При этом администратору безопасности - **запрещается** несанкционированное изменение среды функционирования ПК, а именно:

- модернизация ОС, включая установку штатных обновлений (кроме исполнения «CSP VPN Client»)
- добавление/отключение отдельных сервисов операционной

системы (по отношению к состоянию операционной системы на момент поставки ПК)

- установка дополнительных приложений
- внесение изменений в ПО ПК
- модификация файлов, содержащих исполняемые коды, при их хранении на жестком диске
- добавление/удаление аппаратных компонент (в том числе сетевых карт, жестких дисков и т.п.).

Нарушение этих ограничений рассматривается как нарушение целостности ПК и приводит к срыву заявленной функциональности ПК, и является основанием для отказа в сервисе технического сопровождения и поддержки ПК.

Перед инсталляцией CSP VPN Gate исп.3 должна быть отключена служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности» (внутреннее название – IKEEXT) в соответствии с документом «РЛКЕ.00005-02 90 03 Программное средство “Клиент безопасности CSP VPN Client. Версия 3.1” Руководство администратора».

Для исполнений №1 - №5 СКЗИ для исключения возможности влияния аппаратных компонент СФК на функционирование СКЗИ должны быть выполнены следующие требования:

- в случае обработки информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, необходимо проводить исследования ПО BIOS CBT, на котором установлен ПК "CSP VPN Gate", на соответствие требованиям "Временных методических рекомендаций к проведению исследований программного обеспечения BIOS по документированным возможностям"
- в ПО BIOS ПЭВМ должны быть определены установки, исключающие возможность загрузки операционной системы, отличной от установленной на жестком диске
- вход в BIOS ПЭВМ должен быть защищен паролем с длиной не менее 6 символов
- средствами BIOS должна быть исключена возможность работы на ПЭВМ, если во время его начальной загрузки не проходят встроенные тесты
- должно быть проведено опечатывание системного блока с установленным СКЗИ, исключающее возможность бесконтрольного изменения аппаратной части рабочей станции

Для исполнений №4, №5 СКЗИ РЛКЕ.00005-01 должны быть выполнены требования:

- перед началом сеанса работы пользователь должен убедиться, что BIOS ПЭВМ сконфигурирован на запуск ОС с СЗН (USB или CF, соответственно)
- при наличии в ПЭВМ иных носителей необходимо обеспечить отсутствие на них операционной системы, которая могла бы быть загружена средствами BIOS; при размещении на этих носителях какой-либо информации, используемой при работе ПК, необходимо обеспечить контроль целостности этой информации
- в ходе работы с ПК не допускается подключение носителей в разъемы ПЭВМ, за исключением носителей с ключевой информацией ПК «CSP VPN Gate» и выделенных носителей, специально предусмотренных для работы ПК
- запрещается эксплуатировать ПК исполнений №5 и №4 на СБТ, которые не удовлетворяют требованиям настоящих Правил пользования

4.6. Требования по криптографической защите

Требования по криптографической защите изложены компанией «Крипто-Про» в документах «ЖТЯИ.00050-01 90 02. Руководство администратора безопасности. Общая часть» и «ЖТЯИ.00050-02 90 02. Руководство администратора безопасности. Общая часть», за исключением следующих особенностей антивирусной защиты:

- Исполнения 1, 2

СКЗИ в данных исполнениях предоставляет функции защиты транзитного пользовательского трафика защищаемой сети передачи данных. Для антивирусной защиты пользователей защищаемой сети, средства антивирусной защиты должны устанавливаться либо непосредственно на ПЭВМ пользователя сети, либо на сервер централизованной антивирусной защиты, либо на ПАК с установленным СКЗИ (при наличии совместимого средства антивирусной защиты).

- Исполнение 3 («CSP VPN Client»)

СКЗИ в данном исполнении предоставляет функции защиты пользовательского трафика, создаваемого (или принимаемого) непосредственно на ПЭВМ пользователя. При наличии канала обмена информацией между ПЭВМ пользователя СКЗИ и незащищенными

автоматизированными системами, средства антивирусной защиты должны устанавливаться непосредственно на ПЭВМ пользователя СКЗИ.

- Исполнения 4, 5

СКЗИ в данных исполнениях предоставляет функции защиты пользовательского трафика, создаваемого (или принимаемого) непосредственно на ПЭВМ пользователя. При наличии канала обмена информацией между ПЭВМ пользователя СКЗИ и незащищёнными автоматизированными системами, средства антивирусной защиты должны устанавливаться на выделенный носитель ПЭВМ пользователя СКЗИ или предустанавливаться на СЗН (например, для бездисковой рабочей станции). При отсутствии такого канала обмена информацией, достаточно использование средств антивирусной защиты, устанавливаемых на сервер централизованной антивирусной защиты. Запрещается использование для защиты информации ключей ЭЦП ГОСТ Р 34.10-94.

4.7. Требования к обращению с ключевыми документами

Требования к ключам регламентируются документом ООО «Крипто-Про» «ЖТЯИ.00050-01 90 02. Руководство администратора безопасности. Общая часть» (или «ЖТЯИ.00050-01 90 02. Руководство администратора безопасности. Общая часть» при использовании СКЗИ «КриптоПро CSP» версии 3.6R2), согласно которому срок действия открытых и закрытых ключей шифрования – 1 год 3 месяца. По истечении срока действия ключи не смогут использоваться для работы ПК и должны быть уничтожены на ключевых носителях средствами «КриптоПро CSP». Подробности см. в документе «ЖТЯИ.00050-01 90 03. Инструкция по использованию» (или «ЖТЯИ.00050-02 90 03. Инструкция по использованию» при использовании СКЗИ «КриптоПро CSP» версии 3.6R2).

4.8. Требования к процедурам конфигурирования ПК «CSP VPN Gate»

Первоначальное конфигурирование ПК «CSP VPN Gate» на устройствах, не обладающих стандартными средствами ввода-вывода (монитор и клавиатура), должно производиться при помощи АРМ управления.

Конфигурирование ПК «CSP VPN Gate» при помощи АРМ управления должно осуществляться с использованием подключения по последовательному интерфейсу RS-232. При подключении АРМ управления администратор безопасности при помощи коммуникационной программы должен получить доступ к консоли ПК «CSP VPN Gate», в которой для выполнения конфигурационных действий должен применять утилиты командной строки, описанные в документе «РЛКЕ.00005-01 90 03 Программный комплекс "Шлюз безопасности CSP VPN Gate. Версия 3.1" Руководство администратора. Специализированные команды». Администратор должен получать настройки для конфигурирования ПК «CSP VPN Gate» по надёжному каналу, исключающему их искажение. Хранение настроек ПК «CSP VPN Gate» на АРМ управления допускается только при условии обеспечения контроля их целостности программой srverify компании «КриптоПро».

Рабочим местом администратора безопасности может являться либо АРМ управления, либо ПЭВМ, не имеющие открытых сетевых соединений, с установленным и сконфигурированным в соответствии с настоящими правилами ПК «CSP VPN Gate».

Требования к рабочему месту администратора:

- Рабочее место администратора (АРМ управления или ПЭВМ) должно функционировать в программно-аппаратной среде Windows или Linux на x86-совместимой платформе;
- на ПЭВМ, предназначенную для функционирования в качестве рабочего места администратора, следует устанавливать только лицензионное ПО фирм-изготовителей;
- на рабочем месте администратора должно быть установлено СКЗИ «Крипто Про CSP» версия 3.6 или 3.6R2;
- на АРМ управления должна быть установлена коммуникационная программа (например, HyperTerminal для Windows, minicom для Linux), позволяющая работать с соединениями по последовательному интерфейсу RS-232;

- на АРМ управления не должно быть установлено дополнительного ПО;
- в отношении рабочего места администратора должны выполняться требования по защите от НСД в соответствии с документом «ЖТЯИ.00050-01 90 02. Руководство администратора безопасности. Общая часть» (или «ЖТЯИ.00050-02 90 02. Руководство администратора безопасности. Общая часть» при использовании СКЗИ «Крипто Про CSP» 3.6R2), в том числе, администратором безопасности должен осуществляться периодический контроль целостности установленного ПО (включая коммуникационную программу);
- при выполнении первоначального конфигурирования ПК «CSP VPN Gate» АРМ управления не должно иметь активных сетевых соединений;
- разрешается применять АРМ управления для конфигурирования ПК «CSP VPN Gate» и для формирования ключей ЭЦП для ПК «CSP VPN Gate»;
- запрещается применять АРМ управления для иных целей.

Первоначальное конфигурирование ПК «CSP VPN Gate» на устройствах, обладающих стандартными средствами ввода-вывода (монитор и клавиатура) должно производиться локально - с применением этих средств, или с применением АРМ управления.

В ходе первоначального конфигурирования следует установить пароли пользователей ОС, от имени которых может осуществляться удалённое конфигурирование (см. документ «РЛКЕ.00005-01 90 03 Программный комплекс "Шлюз безопасности CSP VPN Gate. Версия 3.1" Руководство администратора. Инициализация CSP VPN Gate при использовании СКЗИ «КриптоПро CSP 3.6»). Удалённое конфигурирование будет возможно только при успешной аутентификации администратора ПК в ОС.

Средствами ПК в соответствии с требованиями п.4.10 должна быть запрещена возможность установления незащищённых соединений из-за пределов контролируемой зоны с ПЭВМ по порту 22 протокола TCP. Для этого конфигурационный трафик (TCP:22) должен попадать либо под общее правило обработки защищаемого трафика, либо под отдельное правило, в котором трафик описан следующим образом:

```
LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_IP_ADDRESSES ProtocolID *= 6 Port *= 22 )
```

Последующие сеансы конфигурирования могут проводиться удалённо с использованием протоколов SSHv1 и SSHv2 при условии установления защищённого протоколом IPsec с использованием ПК «CSP VPN Gate» соединения между рабочим местом администратора безопасности и конфигурируемым устройством, независимо от наличия или отсутствия стандартных средств ввода-вывода (монитор и клавиатура).

Установление не защищенных средствами ПК «CSP VPN Gate» соединений из контролируемой зоны допускается только при невозможности подключения нарушителя к незащищенному каналу управления. Для этого рабочее место администратора при использовании незащищённых управляющих соединений должно размещаться в отдельном сегменте сети, защищенном от доступа посторонних лиц, и подключаться к ПК «CSP VPN Gate» через выделенный физический интерфейс. Запрещается установление незащищенных соединений по беспроводным каналам связи.

Формирование ключей ЭЦП для ПК «CSP VPN Gate» может выполняться как централизованно, с использованием ПО ЖТЯИ.00035-01 «УЦ «Крипто Про»», так и на рабочих местах пользователей, с использованием СКЗИ «Крипто Про» версия 3.6 или 3.6R2 (в том числе на АРМ управления). Запрещается формировать ключи ЭЦП на устройстве, не обладающем стандартными средствами ввода-вывода (монитор и клавиатура), если ПДСЧ «Крипто-Про CSP» не был инициализирован при помощи физического ДСЧ или внешней гаммой в соответствии с документами «ЖТЯИ.00050-01 90 02. Руководство администратора безопасности. Общая часть» и «ЖТЯИ.00050-01 90 04. АРМ выработки внешней гаммы» (или «ЖТЯИ.00050-02 90 02. Руководство администратора безопасности. Общая часть» и «ЖТЯИ.00050-02 90 04. АРМ выработки внешней гаммы» при использовании СКЗИ «Крипто Про CSP» 3.6R2). Администратор может убедиться в том, что ДСЧ инициализирован внешней гаммой, выполнив команду: `/opt/cproscsp/sbin/ia32/cpconfig -hardware rndm -view`

Вывод должен содержать текст:

Nick name: CPSD

Connect name:

Rndm name: cpsd rng

Rndm level: 4

Доставка контейнеров ключей ЭЦП и внешней гаммы ПДСЧ на устройство должна производиться на носителях, поддерживаемых СКЗИ «Крипто Про» версия 3.6 или 3.6R2, которые могут быть подключены к конфигурируемому устройству.

4.9. Требования к процедурам использования ПК «CSP VPN Gate» на MCM

При конфигурировании устройства MCM должны соблюдаться требования главы 4.8 «Требования к процедурам конфигурирования ПК «CSP VPN Gate» с учётом того, что устройство MCM не обладает стандартными средствами ввода-вывода (монитор и клавиатура).

Внешний сетевой интерфейс устройства MCM, помеченный на передней панели устройства как GigE (далее – сетевой интерфейс GigE), должен подключаться к защищаемой сети. Запрещается подключать сетевой интерфейс GigE к информационно-телекоммуникационным сетям общего пользования. Запрещается конфигурировать ПК «CSP VPN Gate» на устройстве MCM таким образом, чтобы защищённый протоколом IPsec трафик возвращался в защищаемую сеть через сетевой интерфейс GigE. Для этого при конфигурировании ПК в соответствии с «РЛКЕ.00005-01 90 03 Программный комплекс "Шлюз безопасности CSP VPN Gate. Версия 3.1" Руководство администратора. Создание конфигурационного файла» необходимо (следующие структуры являются подструктурами вышеупомянутой структуры IPsecAction):

- в структурах FilteringRule, определяющих параметры защищаемого трафика, атрибуту NetworkInterfaces задавать в качестве значения имя интерфейса, подключенного к сети общего пользования;
- в случае объединения сетей с применением IKECFG:
 - маршрутизацию пакетов, адресованных пулу адресов IKECFG, осуществлять через сетевой интерфейс, подключенный к сети общего пользования;
- без объединения сетей:
 - атрибуту PeerIPFilter задавать значение, не пересекающееся с

адресным пространством защищаемой сети;

- допускать маршрутизацию через сетевой интерфейс GigE только пакетов, предназначенных защищаемой сети, то есть имеющих IP адрес места назначения, принадлежащий защищаемой сети.

Доставка контейнеров ключей ЭЦП и внешней гаммы ПДСЧ на устройство MCM должна производиться на носителях, поддерживаемых СКЗИ «Крипто Про» версия 3.6 или 3.6R2, которые могут быть подключены к устройству MCM через интерфейс USB.

4.10. Требования к инфраструктуре и политике безопасности

ПК «CSP VPN Gate» должен быть настроен администратором безопасности в соответствии с документом «РЛКЕ.00005-01 90 03 Программный комплекс "Шлюз безопасности CSP VPN Gate. Версия 3.1" Руководство администратора. Создание конфигурационного файла».

Для описания защищаемого трафика должны применяться структуры типа FilteringRule (подробное описание в вышеупомянутом документе):

```
FilteringRule rulename(  
    LocalIPFilter *= FilterEntry( ... )  
    RemoteIPFilter *= FilterEntry( ... )  
    Action *= ( %ДЕЙСТВИЕ% )  
)
```

где подструктуры типа FilterEntry описывают трафик (IP-адреса, протоколы, порты), а %ДЕЙСТВИЕ% - зарезервированное слово DROP (для уничтожения попавших под описание пакетов) или имя структуры IPsecAction, описывающей IPsec-обработку трафика. Трафик считается незащищенным, если %ДЕЙСТВИЕ% - зарезервированное слово PASS, или установки структуры IPsecAction, её подструктур и атрибутов, отличны от указанных ниже:

- для шифрования, контроля целостности и взаимной аутентификации не должны использоваться алгоритмы отличные от основанных на российских стандартах ГОСТ 28147-89, ГОСТ Р34.10-2001, ГОСТ Р34.11-94;
- для защиты информации в канале связи и обеспечения контроля её целостности:

атрибуту CipherAlg в структуре ESPTransform должно быть присвоено значение "G2814789CPRO1-K256-CBC-254", а

атрибуту IntegrityAlg в структуре ESPTransform или в структуре AHTransform должно быть присвоено значение "GR341194CPRO1-H96-HMAC-65534";

- режим аутентификации с использованием предварительно распределенных паролей может использоваться только в тестовом режиме работы; данный режим запрещается использовать для защиты передаваемой информации;
разрешённый к применению для защиты передаваемой информации режим аутентификации с использованием ЭЦП ГОСТ Р 34.10 – 2001 включается при использовании атрибута типа AuthMethodGOSTSign в структуре IKERule;
- время жизни IKE SA не должно превышать $2 \cdot 10^6$ байт, для чего атрибуту LifetimeKilobytes в структуре IKETransform необходимо присвоить значение не более 2048; время жизни IPsec SA не должно превышать $4 \cdot 10^6$ байт, для чего атрибуту LifetimeKilobytes в структуре ESPTransform необходимо присвоить значение не более 4096;
- доставка сертификатов и ключей должна производиться администратором безопасности на съёмном носителе, или иным доверенным способом, не нарушающим документ «ЖТЯИ.00050-01 90 02. Руководство администратора безопасности. Общая часть» (или «ЖТЯИ.00050-02 90 02. Руководство администратора безопасности. Общая часть» при использовании СКЗИ «Крипто Про CSP» 3.6R2);
- добавление, просмотр, удаление сертификатов должны производиться администратором безопасности в соответствии с документами «РЛКЕ.00005-01 90 03 Программный комплекс "Шлюз безопасности CSP VPN Gate. Версия 3.1" Руководство администратора. Сценарии конфигурирования» и «РЛКЕ.00005-02 90 03 Программное средство "Клиент безопасности CSP VPN Client. Версия 3.1" Руководство администратора».

В комплект поставки ПК «CSP VPN Gate» включен программный модуль, реализующий международные стандарты шифрования и хэширования. Данный программный модуль не является частью сертифицированного СКЗИ «CSP VPN Gate» и может применяться только для плавной миграции всех взаимодействующих устройств с ранее выпущенных версий «CSP VPN Gate». После осуществления миграции данный программный модуль запрещается использовать и его следует деинсталлировать по следующей процедуре:

- **ОС Windows**

Выполнить команду: `sc delete cp_plg1`

Удалить файл `%SystemRoot%\System32\drivers\cp_plg1.sys`

Перезапустить ОС.

- **ОС Solaris**

Удалить файл `/kernel/drv/cp_plg1` и перезапустить ОС.

- **ОС Linux (все варианты)**

Удалить файл `/lib/modules/`uname -r`/cspvpn/cp_plg1.ko` и перезапустить ОС.