**ООО "С-Терра СиЭсПи"**

---

**УТВЕРЖДЕНО**

**РЛКЕ.00005-02 90 02-ЛУ**

# ПРОГРАММНЫЙ КОМПЛЕКС CSP VPN Gate

ВЕРСИЯ 3.11

# Правила пользования

РЛКЕ.00005-02 90 02
Листов 32

**2015**

# СОДЕРЖАНИЕ

## 1. Аннотация

Настоящий документ содержит описание правил пользования Программным комплексом «CSP VPN Gate» версии 3.11 (ПК РЛКЕ.00005-02, далее ПК).

## 2. Назначение

ПК РЛКЕ.00005-02 является модификацией СКЗИ РЛКЕ.00005-01.

Программный комплекс предназначен для защиты от несанкционированного доступа конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в произвольных информационно-телекоммуникационных системах, в том числе построенных на основе протоколов семейства TCP/IP, с выполнением следующих функций:

фильтрация передаваемой в сетях информации, на уровне протоколов семейства TCP/IP;

обеспечение криптографической защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, передаваемой по протоколам семейства TCP/IP;

двусторонняя криптографическая аутентификация абонентов при установлении соединения

контроль целостности пакетов с использованием хэш-функции

имитозащита трафика при помощи протоколов IPsec AH и/или IPsec ESP.

СКЗИ «CSP VPN Gate» удовлетворяет «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную

тайну» по классам КС1/КС2/КС3 в зависимости от комплектации исполнения.

## 3. Требования к системному ПО

ПК «CSP VPN Gate» функционирует на ПЭВМ различных типов и под управлением операционных систем, указанных в формуляре РЛКЕ.00005-02 30 01.

## 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 оснащённых сертифицированным АПМДЗ а также «3-2» - «CSP VPN Gate КС2 (МСМ)», «3-3» - «CSP VPN Gate КС3 (МСМ)», 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:

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

которые следует разработать согласно требованиям Руководства администратора безопасности СКЗИ “КриптоПро CSP”.

Обязательно наличие опечатываемого сейфа 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» и СФК, включая файлы, указанные в разделе «Требования по криптографической защите» Руководства администратора безопасности соответствующего исполнения СКЗИ «КриптоПро CSP», необходимо осуществлять с помощью ПО ПК не реже 1 раза в месяц при проведении периодического тестирования работоспособности ПК «CSP VPN Gate». Также для вариантов комплектации, оснащённых сертифицированным АПМДЗ, контролю целостности должны подвергаться файлы ОС в соответствии с эксплуатационной документацией АПМДЗ. Взаимодействие АПМДЗ с СКЗИ должно производиться в соответствии с документом «Руководство администратора безопасности» КриптоПро CSP. Для вариантов комплектации «4-4» - «CSP VPN Gate КС2 (С274 СПДС)», «4-1» - «CSP VPN Gate КС3 (С274 СПДС)» целостность файлов ОС и ПК обеспечивается устройством СЗН «СПДС-USB-01» по ТУ 4024-001-70221576-2011. Для вариантов комплектации «3-2» - «CSP VPN Gate КС2 (МСМ)», «3-3» - «CSP VPN Gate КС3 (МСМ)» целостность файлов ОС и ПК

обеспечивается организационными мерами и контролируется загрузчиком ОС, входящим в состав МСМ.

- Необходимо соблюдать правила, описанные в документе «Руководство администратора безопасности» КриптоПро CSP.
- Право доступа к ПК имеет только администратор безопасности. Примечание: для исполнений «1-1» - «CSP VPN Client КС1», «1-2» - «CSP VPN Client КС2», «2-1» - «CSP VPN Server КС1», «2-2» - «CSP VPN Server КС2» допускается использование ПК пользователем согласно принятой политики безопасности.
- Администратор безопасности должен ознакомиться со всей документацией, прилагаемой к ПК.
- Аутентификация администратора безопасности для программных исполнений СКЗИ («1-1» - «CSP VPN Client КС1», «2-1» - «CSP VPN Server КС1», «3-1» - «CSP VPN Gate КС1 (С128)», «4-2» - «CSP VPN Gate КС1 (С274)», «5-1» - «CSP VPN Gate КС1 Crossbeam») 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 исполнений, оснащённых сертифицированным АПМДЗ согласно формуляру РЛКЕ.00005-02 30 01 («1-2» - «CSP VPN Client КС2», «2-2» - «CSP VPN Server КС2», «4-3» - «CSP VPN Gate

КС2 (С274)», «4-5» - «CSP VPN Gate КС3 (С274)»), осуществляется дополнительная аутентификация посредством АПМДЗ согласно соответствующему руководству пользователя.

- Для исполнений с СЗН СПДС ( «4-4» - «CSP VPN Gate КС2 (С274 СПДС)», «4-1» - «CSP VPN Gate КС3 (С274 СПДС)») аутентификация производится при помощи СЗН «СПДС-USB-01» согласно документу «РЛКЕ.00005-02 90 03 Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.11 ”Руководство администратора».
- Для исполнений «3-2» - «CSP VPN Gate КС2 (МСМ)», «3-3» - «CSP VPN Gate КС3 (МСМ)», «4-5» - «CSP VPN Gate КС3 (С274)», «4-1» - «CSP VPN Gate КС3 (С274 СПДС)» производится дополнительная ролевая однофакторная или двухфакторная аутентификация до приведения СКЗИ в состояние готовности, при помощи модуля разграничения доступа, входящего с состав ПК.
- Для исполнений «4-4» - «CSP VPN Gate КС2 (С274 СПДС)», «4-1» - «CSP VPN Gate КС3 (С274 СПДС)» сеанс работы пользователя с СКЗИ РЛКЕ.00005-02 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 с правилами, изложенными в Руководстве администратора безопасности КриптоПро CSP:
  - 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;
- необходимо соблюдать правила, описанные в Руководстве администратора безопасности КриптоПро CSP.

**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.

При эксплуатации «С-Терра Клиент» для ограничения возможностей нарушителя по подбору пароля требуется задать в ОС политику

блокирования учетных данных при помощи программы secpol.msc или непосредственно в реестре ОС. Например, для того, чтобы при обнаружении 10 последовательных неудачных попыток входа, учётная запись блокировалась на 1 час, необходимо:

параметру Account Lockout Threshold присвоить значение 10 (попыток);

параметру Account Lockout Duration присвоить значение 60 (минут).

### 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 инсталлированным ПО ПК. При этом администратору безопасности

**- запрещается** несанкционированное изменение среды функционирования ПК, а именно:

- модернизация ОС, включая установку штатных обновлений (кроме исполнений «1-1» - «CSP VPN Client КС1», «1-2» - «CSP VPN Client КС2», «2-1» - «CSP VPN Server КС1», «2-2» - «CSP VPN Server КС2»);
- 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.

СКЗИ в вариантах комплектации «3-3» - «CSP VPN Gate КС3 (МСМ)», «4-5» - «CSP VPN Gate КС3 (С274)», «4-1» - «CSP VPN Gate КС3 (С274 СПДС)» поставляется в виде замкнутой программной среды, состав которой не может быть штатным образом изменён администратором СКЗИ.

Для всех исполнений СКЗИ для исключения возможности влияния аппаратных компонентов 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 СВТ, на котором установлено ПО ПАК "С-Терра VPN", 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 ПАК, исключающее возможность бесконтрольного изменения аппаратной части рабочей станции.

В случае обработки информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, допускается совместное с СКЗИ использование на ПАК только ПО, входящего в состав ОС, либо разработанного производителем ОС или СКЗИ. Использование другого ПО в этом случае возможно только по результатам исследований оценки его влияния на СКЗИ по документированным возможностям.

Для исполнений «4-4» - «CSP VPN Gate КС2 (С274 СПДС)», «4-1» - «CSP VPN Gate КС3 (С274 СПДС)» СКЗИ РЛКЕ.00005-02 должны быть выполнены требования:

- перед началом сеанса работы пользователь должен убедиться, что BIOS ПЭВМ сконфигурирован на запуск ОС с USB (кроме платформ семейства MCM, где BIOS не имеет интерфейса пользователя);
- 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 «4-4» и «4-1» на СВТ, которые не удовлетворяют требованиям настоящих Правил пользования

При эксплуатации ПК под управлением ОС семейства Windows необходимо деактивировать системную службу Windows Error Reporting, для чего присвоить значение 1 параметру Disabled в следующих ключах реестра:

HKEY_CURRENT_USER\Software\Microsoft\Windows\Windows Error Reporting

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting

Также должна быть отключена функциональность стороннего ПО для отправки дампов памяти.

На рабочих местах под управлением Windows необходимо отключить удалённое управление рабочим столом или обеспечить защиту управляющего соединения при помощи сертифицированного СКЗИ.

### 4.6. Требования по криптографической защите

Требования по криптографической защите изложены в документе «Руководство администратора безопасности» КриптоПро CSP, за исключением следующих особенностей антивирусной защиты:

- Исполнения «3-1» - «CSP VPN Gate КС1 (С128)», «3-2» - «CSP VPN Gate КС2 (МСМ)», «3-3» - «CSP VPN Gate КС3 (МСМ)», , «4-2» - «CSP VPN Gate КС1 (С274)», «4-3» - «CSP VPN Gate КС2 (С274)», «4-5» - «CSP VPN Gate КС3 (С274)», «5-1» - «CSP VPN Gate КС1 Crossbeam»

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).

- Исполнения «1-1» - «CSP VPN Client КС1», «1-2» - «CSP VPN Client КС2», «2-1» - «CSP VPN Server КС1», «2-2» - «CSP VPN Server КС2»

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

- Исполнения «4-4» - «CSP VPN Gate КС2 (С274 СПДС)», «4-1» - «CSP VPN Gate КС3 (С274 СПДС)»

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 «Руководство администратора безопасности» КриптоПро CSP, согласно которому срок действия закрытых ключей ЭП (ЭЦП) – 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.00050-03 90 03. Инструкция по использованию» при использовании СКЗИ “КриптоПро CSP” версии 3.6.1 (или «ЖТЯИ.00050-02 90 03. Инструкция по использованию» при использовании СКЗИ “КриптоПро CSP” версии 3.6R2).

В ПК «CSP VPN Gate» применяются сертификаты ключа проверки ЭП, созданные в соответствии с международными рекомендациями ITU-T X.509, и протокол аннулирования сертификата ключа проверки ЭП с использованием списков аннулированных сертификатов.

Сертификаты ключей проверки ЭП и списки аннулированных сертификатов должны быть выпущены в формате, совместимом с сертифицированным УЦ «КриптоПро», и подписаны с использованием сертифицированного СКЗИ.

Удостоверяющий центр должен обеспечивать корректную обработку полей сертификата, в частности битов keyCertSign и cRLSign дополнения keyUsage для корневых и промежуточных сертификатов УЦ.

Списки аннулированных сертификатов для использования в ПК «CSP VPN Gate» должны выпускаться без расширения deltaCRLIndicator.

Списки аннулированных сертификатов могут доставляться на ПК «CSP VPN Gate» автоматически путём публикации удостоверяющим центром при помощи протокола LDAP (с использованием поля CRLDistributionPoints в сертификате или заданием пути публикации в политике безопасности СКЗИ) или администратором при помощи иных доступных средств. Доставка списков аннулированных сертификатов должна производиться доверенным[1] способом.

[1] Здесь и далее **доверенным** считается способ передачи по каналу, защищённому при помощи сертифицированного СКЗИ, имеющего среди целевых функций контроль целостности (имитозащиту) передаваемых данных и аутентификацию криптографическими методами, при условии аутентификации источника, либо в соответствии с правилами обращения с ключевыми документами, либо физически с участием уполномоченного лица согласно установленной процедуре.

Принятой в организации политикой безопасности должно быть установлено допустимое время аннулирования ключа пользователя. При невозможности выпуска удостоверяющим центром списка аннулированных сертификатов и его доставки за установленное время администратором должны быть приняты меры[2] по предотвращению доступа пользователя, ключ которого аннулирован.

### 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 непосредственно с их использованием или при помощи АРМ управления. Первоначальное конфигурирование ПАК, не обладающих стандартными средствами ввода-вывода, 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.00005-02 90 03 Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.11” Руководство администратора. Специализированные команды». Администратор должен получать настройки для конфигурирования ПК «CSP VPN Gate»

[2] Например, исключение пользователя из списка допущенных пользователей в политике безопасности СКЗИ.

по надёжному каналу, исключающему их искажение. Хранение настроек ПК «CSP VPN Gate» на АРМ управления допускается только при условии обеспечения контроля их целостности программой cpverify 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 рабочем месте администратора следует устанавливать только лицензионное ПО фирм-изготовителей, необходимое для целей управления;
- на рабочем месте администратора должно быть установлено СКЗИ «Крипто Про CSP» версия 3.6.1 или 3.6R2;
- на рабочем месте администратора должна быть установлена коммуникационная программа (например, HyperTerminal для Windows, minicom для Linux), позволяющая работать с соединениями по последовательному интерфейсу RS-232;
- рабочее место администратора должно быть защищено от НСД сертифицированными ФСБ средствами или организационно-техническими мерами, исключающими доступ к ним посторонних лиц;
- в отношении рабочего места администратора должны выполняться требования по защите от НСД в соответствии с документом «Руководство администратора безопасности» КриптоПро CSP, в том числе, администратором безопасности

должен осуществляться периодический контроль целостности установленного ПО (включая коммуникационную программу);

- при выполнении первоначального конфигурирования ПК «CSP VPN Gate» рабочее место администратора не должно иметь активных сетевых соединений;
- разрешается применять рабочее место администратора для конфигурирования ПК «CSP VPN Gate» и для формирования ключей ЭЦП для ПК «CSP VPN Gate», в том числе – для управления при помощи программных продуктов «С-Терра КП 3.11. Клиент управления» и «С-Терра КП 3.11. Сервер управления»;
- управление с использованием компонента «С-Терра КП 3.11» разрешено только для исполнений ПК «CSP VPN Gate» версии 3.11, сертифицированных по классам КС1,КС2.
- на АРМ управления не должно быть установлено дополнительного ПО;
- запрещается применять АРМ управления для иных целей.

В ходе первоначального конфигурирования следует установить пароли пользователей ОС, от имени которых может осуществляться удалённое конфигурирование (управление) с использованием протоколов SSHv1 и SSHv2. Удалённое управление будет возможно только при успешной аутентификации администратора ПАК в ОС.

Подготовка ПК к удалённому управлению должна производиться в соответствии с разделом «Начальная конфигурация для удаленной настройки шлюза» документа «РЛКЕ.00005-02 90 03 Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.11” Руководство администратора. Настройка шлюза».

Последующие сеансы конфигурирования могут проводиться локально (аналогично первоначальному конфигурированию) или удалённо (с использованием протоколов SSHv1 и SSHv2 или при помощи программных продуктов «С-Терра КП»), независимо от наличия или отсутствия у него стандартных средств ввода-вывода (монитор и клавиатура). Удалённое управление должно производиться по безопасным каналам, а именно:

- из контролируемой зоны по незащищенному каналу только при невозможности подключения к этому каналу нарушителя;
- из-за пределов контролируемой зоны или из контролируемой зоны при возможности подключения к этому каналу нарушителя только по защищённым соединениям, с обязательной аутентификацией администратора при помощи ЭП.

При использовании незащищённых управляющих соединений рабочее место администратора должно размещаться в отдельном сегменте сети, защищенном от доступа посторонних лиц, и подключаться к управляемому ПАК через выделенный физический сетевой интерфейс.

Запрещается установление незащищенных управляющих соединений по беспроводным каналам связи.

Формирование ключей ЭП для ПК «CSP VPN Gate» может выполняться как с использованием ПО ЖТЯИ.00067-01 «КриптоПро УЦ» (централизованно), так и с использованием сертифицированного СКЗИ «КриптоПро» (в том числе на рабочих местах пользователей, или на АРМ управления). Запрещается формировать ключи ЭП на устройстве, не обладающем стандартными средствами ввода-вывода (монитор и

клавиатура), если ПДСЧ «КриптоПро CSP» не был инициализирован при помощи физического ДСЧ или внешней гаммой в соответствии с Руководством администратора безопасности СКЗИ «КриптоПро» и документом «АРМ выработки внешней гаммы». Администратор может убедиться в том, что ДСЧ инициализирован внешней гаммой, выполнив команду: 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 аутентифицированным администратором на носителях, поддерживаемых СКЗИ «КриптоПро», которые могут быть подключены к конфигурируемому устройству, либо по защищённому сетевому соединению.

Подготовка Сервера управления к работе должна производиться в соответствии с главой 3 «Установка и настройка Сервера управления» документа «Программный продукт С-Терра КП. Версия 3.11. Руководство администратора» с обязательным выполнением следующих правил:

- ключи подписи, CA сертификат и рабочий сертификат Сервера управления должны создаваться при помощи сертифицированных СКЗИ;
- CA сертификат для целей Сервера управления не должен использоваться для выпуска ключей аутентификации администратора;

- при хранении закрытого ключа подписи Сервера управления в хранилище «Реестр» необходимо обеспечить защиту ПЭВМ Сервера управления от НСД, например, при помощи сертифицированного АПМДЗ.

При локальном или удалённом (в том числе с помощью «С-Терра КП») обновлении версии СКЗИ Администратор должен убедиться в том, что устанавливаемая версия СКЗИ прошла сертификацию ФСБ. Перед установкой обновления Администратор должен произвести расчёт контрольных сумм и их сравнение с эталонными значениями, полученными доверенным способом.

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

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

Локальное конфигурирование может производиться с АРМ администратора через встроенный USB-порт устройства МСМ при помощи USB-to-serial адаптера, либо через маршрутизатор Cisco, к которому подключено устройство МСМ. При локальном конфигурировании через маршрутизатор Cisco ключевой контейнер администратора, используемый для аутентификации, должен быть размещён на сменном носителе (USB-flash или eToken). При локальном конфигурировании маршрутизатор Cisco, к которому подключено устройство МСМ, и само устройство МСМ должны быть отключены от

сети передачи данных, при этом допускается сетевое соединение только с АРМ администратора.

Внешний сетевой интерфейс устройства МСМ, помеченный на передней панели устройства как GigE (далее – сетевой интерфейс GigE), должен подключаться к защищаемой сети или к информационно-телекоммуникационным сетям общего пользования. При этом весь трафик между защищаемой сетью и сетями общего пользования должен проходить через устройство МСМ. Запрещается подключать сетевые интерфейсы маршрутизатора к той же сети, к которой подключен интерфейс GigE устройства МСМ. Запрещается конфигурировать ПК «CSP VPN Gate» на устройстве МСМ таким образом, чтобы защищённый протоколом IPsec трафик возвращался в защищаемую сеть через сетевой интерфейс GigE. Для этого при конфигурировании ПК в соответствии с «РЛКЕ.00005-02 90 03 Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.11” 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 МСМ должна производиться на носителях, поддерживаемых СКЗИ «Крипто Про» версия 3.6.1 или 3.6R2, которые могут быть подключены к устройству МСМ через интерфейс USB, либо по защищённому сетевому соединению.

## 4.10. Требования к процедурам использования ПК «CSP VPN Gate» на ПАК RSCB-X (Crossbeam)

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

На модуле CPM должен быть обеспечен контроль целостности исполняемых файлов ОС APM и NPM, а также конфигурации виртуальных сетевых соединений.

Контроль целостности исполняемых файлов ОС NPM должен производиться на модуле CPM посредством вычисления программой cpverify значения хэш-функции содержимого файла /tftpboot/npm9.bin.

Контроль целостности исполняемых файлов ОС APM должен производиться на модуле CPM посредством вычисления программой cpverify значения хэш-функции содержимого файлов: /opt/cprocsp/sbin/ia32/cpverify /boot/vmlinuz-2.6.18-164.el5smpx /lib/libc-2.5.so /crossbeam/bin/apm_host_pin /crossbeam/bin/bootdiagd /crossbeam/bin/cbs_apcp_clocksync

/crossbeam/bin/cbs_apm9600_raid_volume_delete.pl /crossbeam/bin/cbs_apps_affinity /crossbeam/bin/cbsappsd /crossbeam/bin/cbs_bdreg /crossbeam/bin/cbs_disk_error /crossbeam/bin/cbsflowagentd /crossbeam/bin/cbs_fmquery /crossbeam/bin/cbsfwcfgagentd /crossbeam/bin/cbs_fwcfg_client.eagle /crossbeam/bin/cbs_fwcfg_client.elsalvador /crossbeam/bin/cbshagentd /crossbeam/bin/cbs_hb /crossbeam/bin/cbs_hbls /crossbeam/bin/cbs_hbquery /crossbeam/bin/cbsinitd /crossbeam/bin/cbslinuxver /crossbeam/bin/cbs_md_check /crossbeam/bin/cbs_net_affinity /crossbeam/bin/cbs_net_affinity_9600 /crossbeam/bin/cbsnprobed /crossbeam/bin/cbsoopsd /crossbeam/bin/cbs_poh_check /crossbeam/bin/cbs_prc_affinity /crossbeam/bin/cbs_script_common /crossbeam/bin/cbs_scsi_disk_info.pl /crossbeam/bin/cbs_smartd_setup /crossbeam/bin/cbs_smart_logging /crossbeam/bin/cbsstatsd /crossbeam/bin/cbs_swatch.sh /crossbeam/bin/cbsvapcfgd /crossbeam/bin/cbsvapcfgd.eagle /crossbeam/bin/cbsvapcfgd.elsalvador /crossbeam/bin/cbs_vdcfg /crossbeam/bin/cbs_vdctl /crossbeam/bin/cbs_vddbg /crossbeam/bin/check_mgmt_intf /crossbeam/bin/checkpointsupport /crossbeam/bin/eepromdiag /crossbeam/bin/flashit /crossbeam/bin/gdbserver /crossbeam/bin/getfwstats /crossbeam/bin/health_diag /crossbeam/bin/i2cdiag /crossbeam/bin/init_apm9600_disk.pl /crossbeam/bin/init_apm_disk_helper.pl /crossbeam/bin/init_apm_disk.pl /crossbeam/bin/initlog /crossbeam/bin/jtagit /crossbeam/bin/lockstat /crossbeam/bin/netifstats.swc /crossbeam/bin/netsdp2.swc /crossbeam/bin/oopsdump /crossbeam/bin/packeteer /crossbeam/bin/post_install_master /crossbeam/bin/post_rpm_install_master /crossbeam/bin/prc_credit /crossbeam/bin/pulse_util /crossbeam/bin/sas2flash /crossbeam/bin/sas2ircu /crossbeam/bin/seemem /crossbeam/bin/swatch /crossbeam/bin/tscmd /crossbeam/bin/turnoff_swap /crossbeam/bin/turnon_swap /crossbeam/bin/ZZsmartctl_longtest /crossbeam/bin/ZZsmartctl_shorttest /etc/rc.d/init.d/bootdiagd /etc/rc.d/init.d/cbsappsd /etc/rc.d/init.d/cbsflowagentd /etc/rc.d/init.d/cbsfwcfgagentd /etc/rc.d/init.d/cbshagentd /etc/rc.d/init.d/cbshagentd_post_proc /etc/rc.d/init.d/cbsinitd /etc/rc.d/init.d/cbsnprobed /etc/rc.d/init.d/cbsoopsd /etc/rc.d/init.d/cbsprobed /etc/rc.d/init.d/cbsstatsd /etc/rc.d/init.d/cbsvapcfgd /etc/rc.d/init.d/cbs_vap_post_net_init /etc/rc.d/init.d/cbs_vnd_watchd /etc/rc.d/init.d/netdump /lib/libOS.so /lib/libvrf.so /lib/libvsxnet.so /sbin/ifup-local /sbin/vethcfg /usr/bin/cbsprobed /usr/bin/cbsprobesnmpd /usr/lib/debug /usr/lib/debug/usr /usr/lib/debug/usr/lib /usr/lib/debug/usr/lib/libalarm_cons.so.1.debug /usr/lib/debug/usr/lib/libalarm_cons.so.debug /usr/lib/debug/usr/lib/libalarm_msg.so.1.debug /usr/lib/debug/usr/lib/libalarm_msg.so.debug /usr/lib/debug/usr/lib/libalarm_prod.so.1.debug /usr/lib/debug/usr/lib/libalarm_prod.so.debug /usr/lib/libalarm_cons.so /usr/lib/libalarm_cons.so.1 /usr/lib/libalarm_msg.so /usr/lib/libalarm_msg.so.1 /usr/lib/libalarm_prod.so /usr/lib/libalarm_prod.so.1 /usr/lib/libpulse_api.so /usr/lib/libpulse_api.so.1 /usr/lib/libPulseAttach.so /usr/lib/libPulseAttach.so.1 /usr/lib/libpulse_cons.so /usr/lib/libpulse_cons.so.1 /usr/lib/libpulse_msg.so /usr/lib/libpulse_msg.so.1 /usr/lib/libpulse_prod.so /usr/lib/libpulse_prod.so.1 /usr/lib/libpulse_utility.so /usr/lib/libpulse_utility.so.1 /usr/lib/libpulse_zlib.so /usr/lib/libpulse_zlib.so.1 /usr/local/lib/libpfring.so

Процедуру следует выполнять для всех VAP, входящих в состав VAP-группы, которая предназначена для установки СКЗИ, то есть во всех директориях вида /tftpboot/<ИМЯ_VAP-ГРУППЫ>_*.

Контроль целостности конфигурации сетевых соединений должен производиться на модуле CPM посредством сравнения текущей конфигурации, получаемой при помощи команды /crossbeam/bin/cli -i "show running" с эталонной. Эталонную конфигурацию администратор должен получить таким же способом по окончании настройки ПАК и должен сохранять в безопасном месте. При конфигурировании виртуальных сетевых соединений необходимо обеспечить прохождение всего трафика между защищаемой сетью и сетями общего пользования только через APM (или VAP-группу), на котором установлен и сконфигурирован в соответствии с настоящими Правилами ПК «CSP VPN Gate».

Доставка контейнеров ключей ЭЦП и внешней гаммы ПДСЧ на ПАК RSCB-X должна производиться на носителях, поддерживаемых СКЗИ «Крипто Про» версия 3.6.1 или 3.6R2, которые могут быть подключены к модулю CPM через интерфейс USB или COM, либо по защищённому сетевому соединению.

### 4.11. Требования к инфраструктуре и политике безопасности

При установке параметров, позволяющих создавать криптографически незащищенные соединения, должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации. Проверка достаточности принятых мер защиты проводится при аттестации объекта информатизации с ПК «CSP VPN Gate» версии 3.11 по требованиям информационной безопасности.

ПК «CSP VPN Gate» должен быть настроен администратором безопасности в соответствии с документом «РЛКЕ.00005-02 90 03 Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия

3.11” Руководство администратора. Создание конфигурационного файла».

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

```
FilteringRule rulename(
  LocalIPFilter *= FilterEntry( … )
  RemotelIPFilter *= 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. 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. Трафик считается незащищенным, если %ДЕЙСТВИЕ% - зарезервированное слово PASS, или установки структуры IPsecAction, её подструктур и атрибутов, отличны от указанных ниже:

- для защиты информации в канале связи и обеспечения контроля её целостности с сохранением возможности встречной работы с СКЗИ «CSP VPN Gate 3.1»:

  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";

- для защиты информации в канале связи и обеспечения контроля её целостности при помощи комбинированного преобразования ESP_GOST-4M-IMIT без сохранения возможности встречной работы с СКЗИ «CSP VPN Gate 3.1»:

  атрибуту CipherAlg в структуре ESPTransform должно быть присвоено значение "G2814789CPRO1-K288-CNTMAC-253".

- 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;

- объём информации, обрабатываемой на одном ключе, не должен превышать $4*10^6$ байт, для чего атрибуту LifetimeKilobytes в структуре IKETransform необходимо присвоить значение не более 1984, а атрибуту LifetimeKilobytes при использовании алгоритма "G2814789CPRO1-K256-CBC-254" в структуре ESPTransform необходимо присвоить значение не более 4032;

- создание ключей подписи и сертификатов должно производиться администратором безопасности в соответствии с документами «РЛКЕ.00005-02 90 03 Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.11 ”Руководство

администратора. Сценарии конфигурирования» и «РЛКЕ.00005-02 90 03 Программное средство “Клиент безопасности CSP VPN Client. Версия 3.11” Руководство администратора», при помощи сертифицированного СКЗИ;

- доставка сертификатов и ключей должна производиться администратором безопасности на съёмном носителе, или иным доверенным способом, не нарушающим Руководство администратора безопасности КриптоПро CSP;
- добавление, просмотр, удаление сертификатов должны производиться администратором безопасности в соответствии с документами «РЛКЕ.00005-02 90 03 Программный комплекс ”Шлюз безопасности CSP VPN Gate. Версия 3.11 ”Руководство администратора. Сценарии конфигурирования» и «РЛКЕ.00005-02 90 03 Программное средство “Клиент безопасности CSP VPN Client. Версия 3.11” Руководство администратора».

Рекомендуется в каждом ПК «CSP VPN Gate» вести список допущенных пользователей, в котором производится привязка пользователя к информации, содержащейся в сертификате пользователя, при этом устанавливать защищённое соединение разрешается только с допущенными пользователями.

Рекомендуется устанавливать время жизни защищённого соединения не более 1 суток, для чего атрибуту LifetimeSeconds должно быть присвоено значение 86400.

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» или иных продуктов. 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 Linux (все варианты)**

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