ЗАО "С-Терра СиЭсПи"

УТВЕРЖДЕНО

РЛКЕ.00010-01 90 02-01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС С-Терра VPN

ВЕРСИЯ 4.1

Правила пользования для группы исполнений СКЗИ со встроенной криптографической библиотекой

РЛКЕ.00010-01 90 02-01
Листов 38

2014

СОДЕРЖАНИЕ

Copyright © S-Terra CSP

1. Аннотация

Настоящий документ содержит описание правил пользования следующими исполнениями Программно-аппаратного комплекса «С-Терра VPN» версии 4.1 (ПАК РЛКЕ.00010-01, далее ПАК):

Таблица 1. Группа исполнений СКЗИ со встроенной криптографической библиотекой

С-Терра Клиент ST КС1	"1-1"
С-Терра Клиент ST КС2	"1-3"
С-Терра Клиент-М ST КС1	"2-1"
С-Терра Клиент-М ST КС2	"2-3"
С-Терра Шлюз ST КС1	"3-1"
С-Терра Шлюз ST КС2	"3-3"
С-Терра Шлюз ST КС3	"3-5"

В зависимости от исполнения, ПАК состоит из ПО (ПК «С-Терра Клиент 4.1» или ПК «С-Терра Клиент-М 4.1» или ПК «С-Терра Шлюз 4.1», ПК «С-Терра КП 4.1»), аппаратной платформы общего назначения (x86-совместимую ПЭВМ, устройство архитектуры ARM, смартфон или планшет) или специализированной (семейства модулей МСМ), а так же может включать в свой состав специализированные устройства (АПМДЗ, СПДС).

Комплектность исполнений указана в Формуляре РЛКЕ.00010-01 30 01.

2. Назначение

ПАК РЛКЕ.00010-01 является модификацией СКЗИ РЛКЕ.00005-02.

ПАК 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:

Copyright © S-Terra CSP

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.

ПАК РЛКЕ.00010-01 удовлетворяет «Требованиям к шифровальным (криптографическим) средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классам КС1/КС2/КС3 а также «Требованиям к устройствам типа межсетевой экран» по классам 4 и 3, в зависимости от комплектации исполнения.

3. Требования к системному ПО

ПО ПАК РЛКЕ.00010-01 функционирует на ПЭВМ различных типов и под управлением операционных систем, указанных в формуляре РЛКЕ.00010-01 30 01.

ПАК РЛКЕ.00010-01 указанных в таблице «Таблица 1. Группа исполнений СКЗИ со встроенной криптографической библиотекой» исполнений поддерживает работу с носителями ключей и АПМДЗ с ФДСЧ.

Copyright © S-Terra CSP

В качестве исходного материала для инициализации программного датчика случайных чисел могут быть использованы:

программно-аппаратное средство с физическим датчиком случайных чисел "Соболь" версии 2.1 УВАЛ.00300-58-01 ТУ или версии 3.0 RU.40308570.501410.001 (при подключении ФДСЧ непосредственно к ПАК или[1] к АРМ администратора);

программно-аппаратное средство "Аккорд-АМДЗ" 4012-006-11443195-2005 ТУ;

биологический датчик случайных чисел, входящий в состав ПАК (кроме случаев применения СКЗИ в виртуальной среде).

Перечень поддерживаемых носителей ключей подписи:

«eToken Java 72K»;

«JaCarta ГОСТ», в том числе вариант «JaCarta ГОСТ/Flash форм-фактор Secure MicroSD»;

«Рутокен ЭЦП», в том числе варианты «Рутокен ЭЦП micro», «Рутокен ЭЦП Bluetooth»;

специальный загрузочный носитель - СЗН «СПДС-USB-01» по ТУ 4024-001-70221576-2011.

Допускается хранение ключей на файловой системе обычных носителей (жёстких дисков, USB-накопителей и т.п.) при условии распространения на такой носитель или на ПАК с этим носителем требований по обращению с ключевыми носителями.

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

[1] При использовании ФДСЧ, подключенного к АРМ администратора, должна производиться передача на СКЗИ исходного материала, полученного с ФДСЧ, в формате, совместимом с «АРМ выработки внешней гаммы» производства компании «Крипто-Про».

Copyright © S-Terra CSP

4.1. Общие требования

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

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

Copyright © S-Terra CSP

4.2. Требования по размещению ПАК

При размещении ПАК 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 исполнений «1-2», «3-2» принять меры по исключению несанкционированного доступа в помещения, в которых размещены ПАК 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 ПАК

Copyright © S-Terra CSP

- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им ПАК, конфиденциальной информации, в том числе ключевой информации.

Copyright © S-Terra CSP

4.3. Административные меры безопасности

Безопасная эксплуатация ПАК 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. Обязательно наличие опечатываемого сейфа для хранения СКЗИ, тестовых ключей, эталонных CD дисков с ПО ПАК, 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.

Copyright © S-Terra CSP

4.4. Требования по защите ПАК от НСД

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

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

- Администратором ПАК назначается администратор безопасности.
- Контроль целостности программной и информационной части ПО ПАК «С-Терра VPN», необходимо осуществлять с помощью ПО ПАК не реже 1 раза в месяц при проведении периодического тестирования работоспособности ПАК «С-Терра VPN». Также для исполнений «1-3», «3-3», «3-5», оснащённых сертифицированным АПМДЗ, контролю целостности должны подвергаться файлы ОС в соответствии с эксплуатационной документацией АПМДЗ.
- Целостность ПО ПАК исполнений «3-3», «3-5», оснащённых устройством СЗН «СПДС-USB-01» по ТУ 4024-001-70221576-2011, обеспечивается устройством СЗН «СПДС-USB-01».
- Целостность ПО ПАК исполнений «3-3», «3-5», на базе МСМ обеспечивается организационными мерами и контролируется загрузчиком ОС, входящим в состав МСМ.
- Администратор безопасности должен ознакомиться со всей документацией, прилагаемой к ПАК.
- Аутентификация администратора безопасности для исполнений

Copyright © S-Terra CSP

«1-1», «3-1» 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 ПО ПАК.

- Для исполнений «1-3», «3-3», «3-5», оснащённых сертифицированным АПМДЗ, осуществляется дополнительная аутентификация посредством АПМДЗ согласно соответствующему руководству пользователя.
- Для исполнений «3-3», «3-5» с СЗН СПДС аутентификация производится при помощи СЗН «СПДС-USB-01» согласно Руководству администратора ПАК, а сеанс работы необходимо завершать выключением питания ПАК, или извлечением специального загрузочного носителя.
- Для исполнений «3-3» на МСМ и «3-5» на всех аппаратных платформах производится дополнительная ролевая однофакторная или двухфакторная аутентификация до приведения СКЗИ в состояние готовности, при помощи модуля разграничения доступа, входящего с состав ПАК.
- Право доступа к режиму управления комплексом (пользовательскому интерфейсу ПАК) имеет только администратор.
- Имя администратора должно быть уникальным и не превышать 8

Copyright © S-Terra CSP

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 ПАК (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 ПАК.
- Необходимо разработать политику назначения и смены паролей (для входа в ОС, для доступа к управлению комплексом) в соответствии со следующими правилами:
  - 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

Copyright © S-Terra CSP

предыдущего не менее чем на 4 символа;

- Периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 1 год.

Запрещается:

- оставлять без контроля ПАК;
- 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 ПАК;
- записывать на ключевые носители постороннюю информацию.

Защита ПАК 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

Copyright © S-Terra CSP

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).

Copyright © S-Terra CSP

4.5. Требования по установке ПО ПАК на ПЭВМ

При поставке исполнений «3-1», «3-3», «3-5» в составе программно-аппаратного комплекса операционная система и СКЗИ предустанавливаются. При этом администратору безопасности **запрещается** несанкционированное изменение среды функционирования ПО ПАК, а именно:

- модернизация ОС, включая установку штатных обновлений;
- добавление/отключение отдельных сервисов операционной системы (по отношению к состоянию операционной системы на момент поставки ПАК);
- установка дополнительных приложений;
- внесение изменений в ПО ПАК;
- 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 ПО ПАК и приводит к срыву заявленной функциональности ПАК, и является основанием для отказа в сервисе технического сопровождения и поддержки ПАК.

ПАК в исполнении «3-5» поставляется с замкнутой программной средой, состав которой не может быть штатным образом изменён администратором ПАК.

Copyright © S-Terra CSP

При эксплуатации всех исполнений ПАК 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,

Copyright © S-Terra CSP

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.

При эксплуатации исполнений ПАК исполнений «3-3», «3-5» с СПДС 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 ПАК, необходимо обеспечить контроль целостности этой информации;
- в ходе работы с ПАК не допускается подключение носителей в разъемы ПЭВМ, за исключением носителей с ключевой информацией ПАК «С-Терра VPN» и выделенных носителей, специально предусмотренных для работы ПАК;

Запрещается эксплуатировать ПО ПАК с СПДС на СВТ, которые не удовлетворяют требованиям настоящих Правил пользования.

При эксплуатации ПАК исполнений «1-1», «1-3» под управлением ОС семейства Windows необходимо деактивировать системную службу Windows Error Reporting, для чего присвоить значение 1 параметру Disabled в следующих ключах реестра:

Copyright © S-Terra CSP

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.

Copyright © S-Terra CSP

4.6. Требования по криптографической защите

При инсталляции СКЗИ должны быть обеспечены организационно-технические меры по исключению подмены дистрибутива и внесения изменений в СКЗИ после установки.

Ключевая информация и внешняя гамма, используемая для инициализации состояния программного ДСЧ, являются конфиденциальными.

Периодичность тестового контроля криптографических функций - 10 минут.

ПАК следует перезагружать один раз в сутки, и останавливать для проверки системы охлаждения процессора один раз в месяц.

При функционировании СКЗИ должны выполняться требования эксплуатационной документации на используемый ПАК защиты от НСД.

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).

При наличии канала обмена информацией между ПЭВМ пользователя СКЗИ и незащищёнными автоматизированными системами, средства антивирусной защиты должны устанавливаться непосредственно на ПЭВМ пользователя СКЗИ, или на выделенный носитель ПЭВМ пользователя СКЗИ или предустанавливаться на СЗН (например, для бездисковой рабочей станции). При отсутствии такого канала обмена

Copyright © S-Terra CSP

информацией, достаточно использование средств антивирусной защиты, устанавливаемых на сервер централизованной антивирусной защиты.

Copyright © S-Terra CSP

4.7. Требования к обращению с ключевыми документами

Срок действия закрытых ключей ЭП (ЭЦП) – 1 год 3 месяца. По истечении срока действия ключи не смогут использоваться для работы ПАК и должны быть уничтожены на ключевых носителях средствами ПАК или физически вместе с носителями.

В ПАК «С-Терра VPN» 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 ПАК «С-Терра VPN» должны выпускаться без расширения deltaCRLIndicator.

Списки аннулированных сертификатов могут доставляться на ПАК «С-Терра VPN» 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

Copyright © S-Terra CSP

доступных средств. Доставка списков аннулированных сертификатов должна производиться доверенным[2] способом.

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[3] по предотвращению доступа пользователя, ключ которого аннулирован.

[2] 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.

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

Copyright © S-Terra CSP

4.8. Требования к процедурам конфигурирования ПАК «С-Терра VPN»

Первоначальное конфигурирование ПАК, 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 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 ПАК, в которой для выполнения конфигурационных действий должен применять утилиты командной строки, описанные в Руководстве администратора ПАК. Администратор должен получать настройки для конфигурирования ПАК по надёжному каналу, исключающему их искажение. Хранение настроек ПАК на АРМ управления допускается только при условии обеспечения контроля их целостности программой cpverify компании «КриптоПро» или средствами ПАК.

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 пользования.

Требования к рабочему месту администратора:

- рабочее место администратора (АРМ управления или ПЭВМ)

Copyright © S-Terra CSP

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»;
- 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 Руководством администратора безопасности «КриптоПро CSP», в том числе, администратором безопасности должен осуществляться периодический контроль целостности установленного ПО (включая коммуникационную программу);
- при выполнении первоначального конфигурирования ПАК «С-Терра VPN» рабочее место администратора не должно иметь активных сетевых соединений;

Copyright © S-Terra CSP

- разрешается применять рабочее место администратора для конфигурирования ПАК «С-Терра VPN», «CSP VPN Gate 3.11» и для формирования ключей ЭП, в том числе – для управления при помощи программных продуктов «С-Терра КП».

В ходе первоначального конфигурирования ПАК 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 ПАК к удалённому управлению должна производиться в соответствии с Руководством администратора ПАК.

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.

Copyright © S-Terra CSP

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 ПАК «С-Терра VPN» может выполняться как с использованием ПО ЖТЯИ.00067-01 «КриптоПро УЦ» (централизованно), так и с использованием ПАК или сертифицированного СКЗИ «КриптоПро» (в том числе на рабочих местах пользователей, или на АРМ управления). Запрещается формировать ключи ЭП с использованием СКЗИ «КриптоПро CSP» 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

Copyright © S-Terra CSP

Доставка контейнеров ключей ЭП и внешней гаммы ПДСЧ на устройство должна производиться аутентифицированным администратором на носителях, поддерживаемых ПАК и перечисленных в разделе 3, которые могут быть подключены к конфигурируемому устройству, либо по защищённому сетевому соединению.

Подготовка Сервера управления к работе должна производиться в соответствии с Руководством администратора ПАК 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.

Copyright © S-Terra CSP

Рекомендуется в каждом ПАК «С-Терра VPN 4.1» 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.

Copyright © S-Terra CSP

4.9. Требования к процедурам использования ПАК «С-Терра VPN» на базе МСМ

При конфигурировании устройства МСМ должны соблюдаться требования главы 4.8 «Требования к процедурам конфигурирования ПАК «С-Терра VPN» 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 ПАК «С-Терра VPN» на базе МСМ таким образом, чтобы защищённый

Copyright © S-Terra CSP

протоколом IPsec трафик возвращался в защищаемую сеть. Для этого при конфигурировании ПАК в соответствии с Руководством администратора ПАК необходимо:

- структуры FilterChain, определяющие параметры защищаемого трафика, привязывать к структурам NetworkInterface, соответствующим интерфейсам, подключенным 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 PeerIPAddress задавать значение, не пересекающееся с адресным пространством защищаемой сети;

Доставка контейнеров ключей ЭЦП и внешней гаммы ПДСЧ на устройство МСМ должна производиться на носителях, поддерживаемых ПАК, которые могут быть подключены к устройству МСМ через интерфейс USB, либо по защищённому сетевому соединению.

Copyright © S-Terra CSP

4.10. Требования к инфраструктуре и политике безопасности

ПАК «С-Терра VPN» может обеспечивать раздельное или совместное выполнение функций безопасности – фильтрация, обеспечение конфиденциальности, имитозащита, аутентификация абонентов. При установке параметров, позволяющих создавать криптографически незащищенные соединения, должны быть приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации. Администратор безопасности должен описать в политике безопасности ПАК «С-Терра VPN» все необходимые функции безопасности, исходя из модели угроз. Трафик считается незащищенным, если к нему не применяется определяемый администратором набор функций безопасности из перечисленных ниже. Проверка достаточности принятых мер защиты проводится при аттестации объекта информатизации с ПАК «С-Терра VPN» по требованиям информационной безопасности.

Для указания выполняемых ПАК функций безопасности администратором должна быть написана политика безопасности, с использованием структур основных типов Filter (описание трафика), IPsecAction (описание параметров соединения ESP или AH), IKERule (описание параметров соединения ESP или AH). Формат описания и взаимосвязи структур и атрибутов описаны в Руководстве администратора ПАК.

Copyright © S-Terra CSP

Для обеспечения конфиденциальности информации в канале связи с сохранением возможности встречной работы с СКЗИ «CSP VPN Gate 3.1» необходимо:

- присвоить атрибуту CipherAlg в структуре ESPTransform значение "G2814789CPRO1-K256-CBC-254".

Для обеспечения имитозащиты информации в канале связи с сохранением возможности встречной работы с СКЗИ «CSP VPN Gate 3.1» необходимо:

- присвоить атрибуту IntegrityAlg в структуре ESPTransform значение "GR341194CPRO1-H96-HMAC-65534” или в структуре AHTransform значение "GR341194CPRO1-H96-HMAC-254”.

Для обеспечения имитозащиты информации в канале связи без сохранения возможности встречной работы с СКЗИ «CSP VPN Gate 3.1» необходимо:

- присвоить атрибуту IntegrityAlg в структуре ESPTransform значение "G2814789CPRO1-K256-MAC-65535" или в структуре AHTransform значение "G2814789CPRO1-K256-MAC-255".

Для применения комплексного преобразования ESP_GOST-4M-IMIT (в соответствии с методическими рекомендациями ТК26), обеспечивающего конфиденциальность и имитозащиту информации в канале связи без сохранения возможности встречной работы с СКЗИ «CSP VPN Gate 3.1» необходимо:

- атрибуту CipherAlg в структуре ESPTransform присвоить значение "G2814789CPRO1-K288-CNTMAC-253".

Copyright © S-Terra CSP

Для обеспечения аутентификации абонентов с использованием электронной подписи по стандартам ГОСТ Р 34.10–2012 или ГОСТ Р 34.10–2001 (алгоритм определяется сертификатом ключа подписи) необходимо:

- присвоить атрибуту MainModeAuthMethod или AggrModeAuthMethod в структуре IKERule значение типа AuthMethodGOSTSign;
- добавление, просмотр, удаление сертификатов должны производиться администратором безопасности в соответствии с Руководством администратора ПАК;
- создание ключей подписи и сертификатов должно производиться администратором безопасности в соответствии с Руководством администратора ПАК, при помощи сертифицированного СКЗИ;
- доставка ключей[4] подписи и доверенных (trusted) сертификатов должна производиться администратором безопасности в соответствии с Руководством администратора ПАК, доверенным способом.

Рекомендуется в каждом ПАК «С-Терра VPN 4.1» 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.

[4] Ключи подписи, созданные с помощью «КриптоПро УЦ», должны устанавливаться в ПАК «С-Терра VPN» с помощью входящих в его состав утилит cpkey_conv и cpkey_conv_exp, в соответствии с Руководством администратора ПАК.

Copyright © S-Terra CSP

Для обеспечения работы протокола ISAKMP с целью выполнения любых криптографических функций безопасности с сохранением возможности встречной работы с СКЗИ «CSP VPN Gate 3.1» необходимо:

- присвоить атрибуту CipherAlg в структуре IKETransform значение "G2814789CPRO1-K256-CBC-65534";
- присвоить атрибуту HashAlg в структуре IKETransform значение "GR341194CPRO1-65534";
- присвоить атрибуту GroupID в структуре IKETransform значение VKO_1B.

Для обеспечения работы протокола ISAKMP с целью выполнения любых криптографических функций безопасности с использованием криптографических алгоритмов ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2012, без сохранения возможности встречной работы с СКЗИ «CSP VPN Gate 3.1», необходимо:

- присвоить атрибуту CipherAlg в структуре IKETransform значение "G2814789CPRO1-K256-CBC-65534";
- присвоить атрибуту HashAlg в структуре IKETransform значение "GR341112_256TC26-65128";
- присвоить атрибуту GroupID в структуре IKETransform значение VKO2_1B.

Copyright © S-Terra CSP

Таблица 2. Совместимость по криптографическим алгоритмам

Версии СКЗИ	**3.1**	**3.11**	**4.1 CP**	**4.1 ST**
Алгоритмы шифрования протокола ESP (CipherAlg)				
G2814789CPRO1-K256-CBC[5]	+	+	+	+
Алгоритмы имитозащиты протоколов ESP и AH (IntegrityAlg)				
GR341194CPRO1-H96-HMAC[6]	+	+	+	+
G2814789CPRO1-K256-MAC[7]			+	+
Алгоритмы шифрования и имитозащиты протокола ESP (CipherAlg)				
G2814789CPRO1-K288-CNTMAC[8]		+	+	+
Алгоритмы хэширования протокола ISAKMP (HashAlg)				
GR341194CPRO1[9]	+	+	+	+
GR341112_256TC26[10]				+
Алгоритмы согласования ключей протокола ISAKMP (GroupID)				
VKO_1B[11]	+	+	+	+
VKO2_1B[12]				+

Примечания:
3.1 СКЗИ CSP VPN Gate 3.1, РЛКЕ.00005-1
3.11 СКЗИ CSP VPN Gate 3.11, РЛКЕ.00005-2
4.1 CP СКЗИ С-Терра VPN 4.1, РЛКЕ.00010-1, исполнения “1-2”, “1-4”, “3-2”, “3-4”, “3-6”.
4.1 ST СКЗИ С-Терра VPN 4.1, РЛКЕ.00010-1, исполнения “1-1”, “1-3”, “2-1”, “2-3”, “3-1”, “3-3”, “3-5”.

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 алгоритмов "G2814789CPRO1-K256-

[5] Алгоритм шифрования по ГОСТ 28147-89
[6] Алгоритм ключевого хэширования на основе ГОСТ Р 34.11-94
[7] Алгоритм выработки имитовставки по ГОСТ 28147-89
[8] Комбинированное преобразование ESP_GOST-4M-IMIT в соответствии с документом «ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ ПО ИСПОЛЬЗОВАНИЮ ГОСТ 28147-89 ПРИ ШИФРОВАНИИ ВЛОЖЕНИЙ В ПРОТОКОЛЕ IPSEC ESP»
[9] Алгоритм хэширования по ГОСТ Р 34.11-94
[10] Алгоритм хэширования по ГОСТ Р 34.11-2012
[11] Алгоритм VKO GOST R 34.10-2001 в соответствии с RFC4357
[12] Алгоритм VKO_GOSTR3410_2012_256 в соответствии с документом «МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО КРИПТОГРАФИЧЕСКИМ АЛГОРИТМАМ, СОПУТСТВУЮЩИМ ПРИМЕНЕНИЮ СТАНДАРТОВ ГОСТ Р 34.10-2012 И ГОСТ Р 34.11-2012»

Copyright © S-Terra CSP

CBC-254" и "G2814789CPRO1-K256-MAC" в структурах ESPTransform и AHTransform необходимо присвоить значение не более 4032. При превышении рекомендуемого значения LifetimeKilobytes в момент создания защищённого соединения регистрируется событие MSG_ID_LP_IPSEC_HI_TTL_TRAFFIC (см. ID 00100140 в таблице “Таблица 3. Критически важные сообщения“).

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

Для шифрования, контроля целостности (имитозащиты) и аутентификации не должны использоваться алгоритмы, отличные от основанных на российских стандартах ГОСТ 28147-89, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, перечисленных в таблице “Таблица 2. Совместимость по криптографическим алгоритмам”.

При эксплуатации ПАК «С-Терра VPN» возможна фильтрация сообщений, регистрируемых в журнале. Администратор не должен блокировать следующие критически важные сообщения:

Таблица 3. Критически важные сообщения

ID	Описание
00100119	Создано IPsec-соединения (IKE Quick Mode завершилась успешно). %{1} - номер созданного IPsec-соединения %{2} - IKE traffic request/phase 2id/селектор IPsec SA %{3} - название фильтра %{4} - имя IPsec-правила

Copyright © S-Terra CSP

	%{5} - имя IKE-правила
0010011A	Попытка создания IPsec SA закончилась неудачей. %{1} - стадия ike, где обнаружена ошибка %{2} - причина ошибки %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила %{6} - порядковый номер запроса на создание IPsec-соединения
00100140	В созданном IPsec SA ограничение по трафику не соответствует допустимому ограничению для используемого криптографического алгоритма. %{1} - ограничение, которое будет использовано в созданном IPsec SA (0 - без ограничений)
00200002	Добавление Сертифицирующего Центра в базу данных
00200003	Удаление локального сертификата, либо Сертифицирующего Центра из базы данных

В комплект поставки ПО ПАК «С-Терра VPN» включен программный модуль, реализующий международные стандарты шифрования и хэширования. Данный программный модуль не является частью сертифицированного ПАК «С-Терра VPN» и может применяться только для плавной миграции всех взаимодействующих устройств с ранее выпущенных версий «CSP VPN Gate» или иных продуктов. При использовании исполнений «2-1» - «С-Терра Клиент-М ST КС1» или «2-2» - «С-Терра Клиент-М ST КС2» необходимо выбирать вариант конфигурирования на российских алгоритмах. При использовании

Copyright © S-Terra CSP

остальных исполнений 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.

Copyright © S-Terra CSP