Экз. №2

СОГЛАСОВАНО
От Центра защиты информации
и специальной связи ФСБ России

_____

“ 27 ” 05 2025 г.

УТВЕРЖДАЮ
Генеральный директор
ООО «С-Терра СиЭсПи»

_____ М.Н. Иванов

“ ____ ” _____ 20 г.

Инв № подл	Подпись и дата	Взам инв №	Инв № дубл	Подпись и дата

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «С-Терра Шлюз» Исполнения «3М3», «3М5»

ВЕРСИЯ 5.0

Правила пользования

ЛИСТ УТВЕРЖДЕНИЯ

РЛКЕ.00033-01 90 03-ЛУ
Листов 1

2025

ООО "С-Терра СиЭсПи"

УТВЕРЖДЕНО

РЛКЕ.00033-01 90 03-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «С-Терра Шлюз» Исполнения «3М3», «3М5»

ВЕРСИЯ 5.0

Правила пользования

РЛКЕ.00033-01 90 03
Листов 50

2025

СОДЕРЖАНИЕ

1. Предисловие 4

2. Перечень используемых терминов и сокращений 5

3. Назначение СКЗИ и его основные характеристики 6

4. Ключевая система и ключевые документы 10

4.1. Характеристики ключевой системы 10

4.2. Управление ключевой информацией 10

5. Порядок распространения и учёта СКЗИ 18

5.1. Способы передачи и хранения СКЗИ 18

5.2. Поэкземплярный учет СКЗИ 18

6. Требования по обеспечению безопасности при вводе СКЗИ в эксплуатацию 19

6.1. Требования к встраиванию СКЗИ в прикладные системы и к проведению исследований СФ СКЗИ 19

6.2. Требования к аппаратной среде функционирования 19

6.3. Требования по размещению 19

6.4. Требования к персоналу, обслуживающему СКЗИ 22

6.5. Инициализация и ввод СКЗИ в эксплуатацию 22

6.5.1 Задание политики безопасности с помощью файла (LSP) 30

6.5.2 Задание политики безопасности с помощью cs_console..... 36

6.5.3 Общие ограничения на применение криптографических алгоритмов..... 40

7. Требования по обеспечению безопасности при эксплуатации СКЗИ 42

7.1. Общие требования по защите от НСД 42

7.2. Требования к аутентификации и разграничению доступа 42

7.3. Требования по обеспечению целостности СКЗИ 45

7.4. Порядок обеспечения работоспособности СКЗИ 47

© ООО "С-Терра СиЭсПи"

8. Требования по обеспечению безопасности при выводе СКЗИ из эксплуатации и передаче в ремонт 50

© ООО "С-Терра СиЭсПи"

1. Предисловие

Настоящие правила пользования предназначены для пользователей СКЗИ «С-Терра Шлюз» Версия 5.0.

Настоящие правила пользования составлены в соответствии с технической спецификацией ТК 26 ТС 26.2.001-2020 «Состав и содержание правил пользования средств криптографической защиты информации».

© ООО "С-Терра СиЭсПи"

2. Перечень используемых терминов и сокращений

АС – аппаратные средства.

НСД – Несанкционированный доступ.

ПАК – программно-аппаратный комплекс.

ПК – программный комплекс.

СКЗИ – средство криптографической защиты информации.

ФДСЧ – физический датчик случайных чисел.

© ООО "С-Терра СиЭсПи"

3. Назначение СКЗИ и его основные характеристики

СКЗИ «С-Терра Шлюз» предназначено для защиты от несанкционированного доступа к 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[1] передаваемой в сетях информации, на уровне протоколов семейства TCP/IP;
- шифрование конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, передаваемой посредством сетевых протоколов, при помощи протокола IPsec ESP, по алгоритмам ГОСТ 28147-89, ГОСТ 34.12-2018 (ГОСТ Р 34.12-2015), ГОСТ 34.13-2018 (ГОСТ Р 34.13-2015);
- имитозащита трафика при помощи протокола IPsec ESP, по алгоритмам ГОСТ 28147-89, ГОСТ 34.12-2018 (ГОСТ Р 34.12-2015), ГОСТ 34.13-2018 (ГОСТ Р 34.13-2015);
- двусторонняя криптографическая аутентификация абонентов при установлении соединения по протоколам IKEv1 и IKEv2, с использованием алгоритмов ГОСТ 34.10-2018 (ГОСТ Р 34.10-2012), ГОСТ 34.11-2018 (ГОСТ Р 34.11-2012);
- проверка электронной подписи областей памяти и файлов по алгоритмам ГОСТ Р 34.10-2001, ГОСТ 34.10-2018 (ГОСТ Р 34.10-2012) в целях контроля целостности;

[1] Функциональность фильтрации не покрывается сертификатом ФСБ России

© ООО "С-Терра СиЭсПи"

- формирование электронной подписи областей памяти и файлов по алгоритму ГОСТ 34.10-2018 (ГОСТ Р 34.10-2012) в целях контроля целостности.

СКЗИ «С-Терра Шлюз» удовлетворяет «Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» по классам соответственно таблице «Таблица 1. Перечень исполнений и классов» и «Специальным требованиям к средствам криптографической защиты, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и эксплуатируемым на территории Российской Федерации» по уровню $КС_Б$.

Таблица 1. Перечень исполнений и классов

Наименование	Обозначение	Класс СКЗИ
С-Терра Шлюз STM КС2	"3М3"	КС2
С-Терра Шлюз STM КС3	"3М5"	КС3

СКЗИ «С-Терра Шлюз» не предоставляет программных интерфейсов для встраивания его в прикладное ПО.

СКЗИ «С-Терра Шлюз» реализует следующие протоколы, применяемые для обеспечения защиты конфиденциальной информации:

- IKEv1 на базе RFC2409 (для совместимости с ранее выпущенными версиями СКЗИ «С-Терра VPN» и другими изделиями);
- IKEv1 по спецификации ТС 26.2.001-2015 (для совместимости с ранее выпущенными версиями СКЗИ «С-Терра VPN» и другими изделиями);
- IKEv2 по спецификации Р 1323565.1.048–2023;
- IPsec ESP на базе RFC4303 (для совместимости с другими изделиями);

© ООО "С-Терра СиЭсПи"

- IPsec ESP по ТС 26.2.002-2014 (для совместимости с другими изделиями);
- IPsec ESP по спецификации Р 1323565.1.035–2021;
- IPsec AH на базе RFC4303 (для совместимости с другими изделиями).

Требования к АС указаны в формуляре.

Исполнение «3М5» СКЗИ реализует замкнутую программную среду. Администратору не предоставляется возможности менять состав среды, кроме установки ПО, предоставленного разработчиком СКЗИ.

СКЗИ предоставляет пользователю командно-строчный интерфейс управления и мониторинга посредством локального (монитор, клавиатура, консольное подключение по последовательному порту или его эмуляция) или удалённого (подключение по сетевому соединению) доступа.

Организация и обеспечение безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации сведений, составляющих конфиденциальную информацию, осуществляются в соответствии с документами:

- Приказ ФАПСИ от 13.06.2001 N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»
- Приказ ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации

© ООО "С-Терра СиЭсПи"

шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

© ООО "С-Терра СиЭсПи"

4. Ключевая система и ключевые документы

4.1. Характеристики ключевой системы

СКЗИ «С-Терра Шлюз» использует асимметричную ключевую систему на базе ключей подписи ГОСТ 34.10-2018 размером 256 и 512 битов. Срок действия закрытых ключей, извлекаемых с носителя – до 15 месяцев. Срок действия неизвлекаемых ключей на носителе, сертифицированном ФСБ России, определяется эксплуатационной документацией носителя. Извлекаемые с носителя ключи подписи ГОСТ 34.10-2018 создаются и применяются в формате PKCS#15 с использованием отечественных криптографических алгоритмов.

Применяются также симметричные предварительно распределенные ключи размером 256 битов. Срок действия симметричных предварительно распределенных ключей – до 15 месяцев.

Далее по тексту документа ключи подписи и симметричные предварительно распределенные ключи будут называться термином «ключи» или «ключевая информация», если в контексте упоминания различие не важно.

4.2. Управление ключевой информацией

Администратор СКЗИ должен обеспечивать сохранность и конфиденциальность ключевой информации. Администратор СКЗИ может создавать одну или несколько учётных записей привилегированных пользователей, которым разрешается управлять настройками СКЗИ.

Ключевая информация может вырабатываться непосредственно на местах эксплуатации СКЗИ или на выделенном рабочем месте

© ООО "С-Терра СиЭсПи"

администратора, с последующим вводом в СКЗИ. Выработка ключевой информации должна осуществляться средствами СКЗИ, инициализированного в соответствии с эксплуатационной документацией СКЗИ. В процессе инициализации СКЗИ должна проводиться инициализация ДСЧ при помощи инициализирующей последовательности, получаемой с ФДСЧ (при наличии) или из файла гаммы (при наличии) или с биологического ДСЧ, входящего в состав СКЗИ. СКЗИ поддерживает получение инициализирующей последовательности со следующих ФДСЧ:

- ФДСЧ АПМДЗ «Аккорд-АМДЗ»;
- ФДСЧ «Криптон USB-ДСЧ».

СКЗИ также поддерживает получение инициализирующей последовательности с биологического программно-клавиатурного датчика случайных чисел, входящего в состав ПО СКЗИ (кроме случаев применения СКЗИ в виртуальной среде). Ключевая информация может храниться на сменных носителях. Поддерживаются следующие типы ключевых носителей для ключей подписи:

- Jacarta;
- Rutoken;
- USB – flash;
- внутренний накопитель аппаратной платформы СКЗИ.

Поддерживаются следующие типы ключевых носителей для симметричных предварительно распределенных ключей:

- USB – flash;
- внутренний накопитель аппаратной платформы СКЗИ.

© ООО "С-Терра СиЭсПи"

При хранении ключевой информации на внутреннем накопителе аппаратной платформы СКЗИ к аппаратной платформе СКЗИ должны предъявляться требования по защите от НСД, как к ключевому носителю.

СКЗИ поддерживает использование неизвлекаемых ключей подписи, размещённых на носителях следующих типов:

- Рутокен ЭЦП 2.0;
- Рутокен ЭЦП 3.0;
- JaCarta 2 ГОСТ.

Носители неизвлекаемых ключей подписи должны использоваться в соответствии с требованиями эксплуатационной документации носителя и только при наличии сертификата ФСБ России на носитель.

Для инициализации программного датчика случайных чисел при помощи ФДСЧ без непосредственного подключения к СКЗИ должна производиться передача на СКЗИ исходного материала, полученного с ФДСЧ, в ключевом контейнере PKCS#15 или файле формата, совместимого с «АРМ выработки внешней гаммы» СКЗИ «КриптоПро CSP» версии 5.0 R3 производства компании «Крипто-Про». СКЗИ обеспечивает однократное использование отрезков исходного материала (гаммы), содержащихся в файле. Тиражирование и повторное использование файла гаммы запрещается. Содержимое файла гаммы конфиденциально. Требования по обращению к ключевому носителю, приведённые в данном документе, распространяются также на носитель, применяемый для доставки файла гаммы.

В ПАК «С-Терра Шлюз» применяются сертификаты ключа проверки ЭП, созданные в соответствии с международными рекомендациями ITU-T X.509, и

© ООО "С-Терра СиЭсПи"

протокол аннулирования сертификата ключа проверки ЭП с опциональным использованием списков аннулированных сертификатов.

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

Рекомендуется в каждом СКЗИ «С-Терра Шлюз» вести список допущенных пользователей, в котором производится привязка пользователя к информации, содержащейся в сертификате пользователя, или иному идентификатору, при этом устанавливать защищённое соединение разрешается только с допущенными пользователями.

Для получения сертификатов открытых ключей на основе ключевой информации должен быть сформирован запрос на сертификат в формате PKCS#10 утилитами cont_mgr, excont_mgr или cert_mgr из состава СКЗИ. Запрос на сертификат должен быть отправлен в центр выдачи сертификатов. Организация выпуска сертификатов должна производиться в соответствии с регламентом центра выдачи сертификатов. При передаче запроса должна обеспечиваться защита от подмены запроса, удовлетворяющая требованиям центра выдачи сертификатов. Например, при передаче запроса по незащищённому каналу для защиты от подмены может проводиться проверка содержимого открытого ключа по телефону, голосом.

Срок действия открытого ключа должен устанавливаться в пределах срока действия закрытого ключа (см. п.4.1) и указываться в сертификате открытого ключа (поле Validity). СКЗИ не допускает использования закрытого и открытого ключа до начала и после окончания срока действия сертификата

© ООО "С-Терра СиЭсПи"

открытого ключа. Для отслеживания срока действия ключа администратор должен использовать утилиту cert_mgr из состава СКЗИ.

Центр выдачи сертификатов (далее - ЦВС) должен обеспечивать корректную обработку полей сертификата, в частности битов keyCertSign и cRLSign дополнения keyUsage для корневых и промежуточных сертификатов ЦВС. Списки аннулированных сертификатов для использования в ПАК «С-Терра Шлюз» должны выпускаться без расширения deltaCRLIndicator.

ПАК «С-Терра Шлюз» поддерживает загрузку списков аннулированных сертификатов автоматически по протоколу LDAP по адресу, указанному центром выдачи сертификатов в поле CRLDistributionPoints сертификата, или по адресу, задаваемому в политике безопасности СКЗИ, см. главу 6.5), а также загрузку администратором при помощи иных доступных средств. Доставка списков аннулированных сертификатов может производиться по сети или на носителях, защита при передаче не требуется.

Симметричные предварительно распределенные ключи должны вырабатываться утилитой genpskey и импортироваться утилитой key_mgr из состава СКЗИ с указанием срока действия, не превышающего 15 месяцев от момента ввода.

Администратор должен установить допустимое время аннулирования ключа пользователя. При невозможности выпуска центром выдачи сертификатов списка аннулированных сертификатов и его доставки за установленное время администратором должны быть приняты меры по предотвращению доступа пользователя, ключ которого аннулирован (например, исключение пользователя из списка допущенных пользователей в политике безопасности СКЗИ).

© ООО "С-Терра СиЭсПи"

Удаление ключевой информации пользователя должно производиться администратором СКЗИ в следующем порядке:

- Для воспрепятствования использованию ключевой информации, подлежащей удалению, выполнить одно из действий:
  - блокировать пользователя в политике безопасности по имени, записанному в сертификате, на всех взаимодействующих устройствах в сети информационной системы;
  - если отзыв поддерживается центром выдачи сертификатов, отозвать сертификат средствами центра выдачи сертификатов и доставить список аннулированных сертификатов на все взаимодействующие устройства в сети информационной системы.
- Уничтожить ключ на ПАК при помощи утилит key_mgr, cont_mgr или excont_mgr из состава СКЗИ. В случае размещения ключей на твердотельных накопителях надёжное удаление ключей указанными утилитами не гарантируется. Необходимо выполнять отзыв сертификата или блокировку пользователя, как описано выше.

Для защиты ключевой информации от компрометации необходимо принимать следующие меры:

- пароли пользователей СКЗИ порядок их смены должны удовлетворять требованиям главы 7.2 правил пользования;
- при наличии оснований считать, что пароль был скомпрометирован, необходимо проверить и при необходимости восстановить целостность СКЗИ и СФ, выполнить смену пароля, восстановить политику безопасности из надёжного источника, выполнить процедуру смены ключевой информации данного устройства;

© ООО "С-Терра СиЭсПи"

- должны выполняться требования по защите от НСД, приведённые в главе 7.1;
- ввод ключевой информации должен производиться на носителе с участием уполномоченного лица согласно установленной процедуре.

По истечении срока действия ключи не должны использоваться для работы ПАК и должны быть уничтожены на ключевых носителях средствами ПАК или физически вместе с носителями.

По отношению к носителям, на которых записана ключевая информация, запрещено:

- осуществлять несанкционированное копирование содержимого носителя;
- разглашать содержимое или передавать посторонним лицам, выводить на экран или на печать;
- устанавливать ключевую информацию на компьютеры, кроме тех СКЗИ, для которых она предназначена;
- записывать на носители постороннюю информацию;
- оставлять носители без присмотра.

Резервное копирование ключевой информации должно проводиться с соблюдением мер безопасности – защита конфиденциальности, целостности и подлинности ключей. Резервная копия ключа должна создаваться администратором СКЗИ путём копирования файла ключевого контейнера на резервный носитель. Требования по обращению к ключевому носителю, приведённые в данном документе, распространяются также на резервный носитель. Резервный носитель должен помечаться идентификатором, позволяющим установить принадлежность и оригинальное расположение

© ООО "С-Терра СиЭсПи"

ключа, и сохраняться в сейфе, ключ от которого должен находиться у администратора СКЗИ. При этом дубликаты ключа от сейфа должны находиться у руководителя организации или уполномоченных им лиц. Восстановление ключа из резервной копии должно осуществляться администратором СКЗИ путём копирования надлежащего файла ключевого контейнера с резервного носителя в его оригинальное расположение или путём ввода ключа по стандартной процедуре, описанной в эксплуатационной документации СКЗИ.

© ООО "С-Терра СиЭсПи"

5. Порядок распространения и учёта СКЗИ

5.1. Способы передачи и хранения СКЗИ

СКЗИ должно распространяться в соответствии с ПКЗ-2005. Хранение и передача СКЗИ должны производиться в соответствии с требованиями «Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». Доставка аппаратных средств (при наличии), программного обеспечения и эксплуатационной документации должна производиться способом, исключающим необнаруживаемое изменение состава, состояния и содержания, например, в разрушающейся при вскрытии упаковке. Эксплуатация повреждённого экземпляра СКЗИ не допускается. При обнаружении повреждений администратор должен обратиться к производителю СКЗИ за разъяснениями.

5.2. Поэкземплярный учет СКЗИ

Учёт СКЗИ должен производиться в соответствии с требованиями положения ПКЗ-2005. Учёт произведённых СКЗИ осуществляется производителем. Учёт эксплуатируемых СКЗИ осуществляется заказчиком (пользователем).

© ООО "С-Терра СиЭсПи"

6. Требования по обеспечению безопасности при вводе СКЗИ в эксплуатацию

6.1. Требования к встраиванию СКЗИ в прикладные системы и к проведению исследований СФ СКЗИ

СКЗИ поставляется как функционально законченное изделие. В случае обработки информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, устройства, на которых установлено СКЗИ «С-Терра Шлюз», должны эксплуатироваться в условиях, предусмотренных производителями в инструкциях по их эксплуатации, а использование стороннего ПО возможно только по результатам исследований оценки его влияния на СКЗИ по документированным возможностям.

6.2. Требования к аппаратной среде функционирования

СКЗИ предназначено для функционирования на аппаратных платформах (АП), удовлетворяющих условиям, описанным в формуляре СКЗИ.:

6.3. Требования по размещению

СКЗИ должно размещаться в условиях, соответствующих климатическим, пылевлагозащитным, вибрационным и прочим физическим характеристикам применяемых АС. Помещения, в которых размещается СКЗИ, должны удовлетворять следующим требованиям физической безопасности:

- обеспечение круглосуточной охраны помещений;
- обеспечение контроля внешнего периметра и внутренних помещений;
- обеспечение пропускного режима;
- двери должны быть прочными и оборудованы надежными механическими замками;

© ООО "С-Терра СиЭсПи"

- оборудование помещений системой пожарной сигнализации;
- ведение журнала выдачи ключей от входных дверей, в котором регистрируется время сдачи и выдачи ключей, фамилия сотрудника, взявшего или сдавшего ключ дежурному вахтеру по зданию;
- внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им СКЗИ, конфиденциальной информации, в том числе ключевой информации.

ПАК «С-Терра Шлюз» должен эксплуатироваться на территории РФ. Исполнение «ЗМЗ» должно эксплуатироваться в составе оборудования, размещенного внутри контролируемой зоны. СКЗИ не должны размещаться и использоваться в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

Проверка достаточности соблюдения требований к размещению ПАК «С-Терра Шлюз» должна производиться на основе модели угроз безопасности информации информационной системы, в которой эксплуатируется СКЗИ.

В случае обработки информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, при эксплуатации СКЗИ требуется выполнение действующих в Российской Федерации требований по защите информации от утечки по техническим каналам, в том числе по каналу связи (например, СТР-К). Данное требование не предъявляется при обработке открытой информации, доступ к которой не ограничивается согласно законодательству Российской Федерации.

© ООО "С-Терра СиЭсПи"

Безопасность эксплуатации СКЗИ «С-Терра Шлюз» обеспечивается при его установке на технические средства, для которых выполнены действующие в Российской Федерации требования по защите информации от утечки по техническим каналам, в том числе по каналу связи. При этом, если технические средства не входят в состав объекта информатизации, который аттестован на соответствие установленным требованиям по защите информации с учётом канала связи, то при подключении таких технических средств к каналам связи, выходящим за пределы контролируемой территории, для обеспечения защиты ключевой и цифровой открытой информации СКЗИ «С-Терра Шлюз» по уровню $КС_Б$ от утечки по каналу связи достаточно, чтобы канал связи был реализован в виде:

- ВОЛС, уходящей за пределы контролируемой зоны;
- радиоканалов GSM, GPRS, 3G/4G, Wi-Fi, а также других современных каналов мобильной или беспроводной связи с цифровой модуляцией штатного информационного сигнала;
- проводного канала связи с установкой в нем волоконно-оптической развязки.

Аппаратные средства, на которых выполняется СКЗИ, а также взаимодействующие с СКЗИ технические средства (носители ключей электронной подписи, в том числе использующихся для аутентификации), в случае планирования размещения СКЗИ в помещениях, где присутствует речевая акустическая и визуальная информация, содержащая сведения, составляющие государственную тайну, и (или) установлены технические средства и системы приёма, передачи, обработки, хранения и отображения информации, содержащей сведения, составляющие государственную тайну,

© ООО "С-Терра СиЭсПи"

должны быть подвергнуты специальной проверке в объёме требований к техническим средствам, предназначенным для установки в помещения соответствующей категории.

6.4. Требования к персоналу, обслуживающему СКЗИ

Персонал, обслуживающий СКЗИ, должен быть ознакомлен с эксплуатационной документацией СКЗИ.

6.5. Инициализация и ввод СКЗИ в эксплуатацию

СКЗИ должны вводиться в эксплуатацию администратором СКЗИ или уполномоченным им персоналом.

При вводе СКЗИ «С-Терра Шлюз» в эксплуатацию администратор СКЗИ должен выполнить следующие действия:

- ознакомиться с эксплуатационной документацией;
- выполнить смену (установку) паролей;
- определить сетевые порты, подключаемые к защищаемым ресурсам и к внешним сетям;
- опломбировать корпус, неиспользуемые разъёмы ПАК и прочие элементы, в соответствии с требованиями по защите от НСД, приведённые в главе 7.1;
- сгенерировать и установить ключи;
- разработать и активировать политику безопасности.

Первоначальное конфигурирование ПАК, обладающих стандартными средствами ввода-вывода (монитор и клавиатура), должно производиться непосредственно с их использованием или при помощи АРМ администратора. Первоначальное конфигурирование ПАК, не обладающих стандартными

© ООО "С-Терра СиЭсПи"

средствами ввода-вывода, должно производиться при помощи АРМ администратора.

Требования к рабочему месту администратора (АРМ администратора):

- рабочее место администратора должно функционировать в программно-аппаратной среде Windows или Linux на x86-совместимой платформе и размещаться в контролируемой зоне;
- на рабочем месте администратора следует устанавливать только лицензионное ПО фирм-изготовителей, необходимое для целей управления;
- на рабочем месте администратора должно быть установлено сертифицированное ФСБ России СКЗИ «С-Терра Шлюз» или «С-Терра Клиент» (при необходимости вырабатывать ключи для управляемого СКЗИ);
- на рабочем месте администратора должна быть установлена коммуникационная программа (например, putty для Windows, minicom для Linux), позволяющая работать с соединениями по последовательному интерфейсу RS-232 (в том числе эмулируемому) и/или сетевому соединению по протоколу ssh;
- рабочее место администратора должно быть защищено от НСД сертифицированными ФСБ России средствами или организационно-техническими мерами, исключающими доступ к нему посторонних лиц, в соответствии с моделью угроз безопасности информации информационной системы;
- в отношении рабочего места администратора должны выполняться

© ООО "С-Терра СиЭсПи"

требования по защите от НСД в соответствии с правилами пользования, в том числе, администратором безопасности должен осуществляться периодический контроль целостности установленного ПО (включая коммуникационную программу);

- при выполнении первоначального конфигурирования ПАК «С-Терра Шлюз» рабочее место администратора и ПАК «С-Терра Шлюз» должны размещаться в контролируемой зоне в одном сегменте сети (при подключении через сетевые интерфейсы) и не должны иметь подключений к каналам связи общего доступа, а используемые каналы связи должны быть защищены организационно-техническими мерами или сторонним СКЗИ;
- разрешается применять рабочее место администратора для конфигурирования СКЗИ «С-Терра Клиент» версии 5.0, СКЗИ «С-Терра Шлюз» версии 5.0 и СКЗИ «С-Терра VPN» версии 4.3 при помощи ПК «С-Терра ГСУ» или терминальных программ minicom и putty.

Конфигурирование СКЗИ «С-Терра Шлюз» при помощи АРМ администратора должно осуществляться удаленно по сетевому соединению или с использованием подключения по последовательному интерфейсу RS-232. Администратор 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. Администратор должен получать настройки для конфигурирования ПАК от доверенного лица на носителе или по каналу связи, защищенному сертифицированным ФСБ России СКЗИ, с обеспечением

© ООО "С-Терра СиЭсПи"

защиты конфиденциальности и целостности. Хранение настроек ПАК на АРМ администратора допускается только при условии обеспечения контроля их целостности средствами сертифицированного ФСБ России СКЗИ.

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 в ОС. Подготовка ПАК к удалённому управлению должна производиться в соответствии с Руководством администратора.

Последующие сеансы конфигурирования могут проводиться локально (аналогично первоначальному конфигурированию) или удалённо (с использованием протоколов SSHv1 и SSHv2 или с использованием ПК «С-Терра ГСУ»), 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, при этом защита канала от несанкционированного доступа должна осуществляться организационно-техническими мерами[2];
- из-за пределов контролируемой зоны или из контролируемой зоны при возможности подключения к этому каналу нарушителя только по защищённым средствами сертифицированного ФСБ России СКЗИ

[2] Например: видеонаблюдение за кабелем проложенным в помещениях (коридорах), где могут оказаться посторонние; отключение неиспользуемых портов на коммутаторах; выделение сети управления в отдельный VLAN.

© ООО "С-Терра СиЭсПи"

соединениям, с обязательной аутентификацией при помощи ЭП администратора как удалённого пользователя.

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.

Все указанные в настоящих правилах ограничения удаленного управления относятся как к сетевым соединениям между компонентом «Сервер управления» ПК «С-Терра ГСУ» и управляемым СКЗИ, так и к сетевым соединениям между компонентами «Сервер управления» и «Консоль управления» ПК «С-Терра ГСУ».

ПО ПАК допускает настройку отправки журнала событий на удалённый сервер по протоколу syslog. В качестве удалённого сервера syslog в этом случае должен использоваться компьютер, защищаемый от НСД при помощи сертифицированных ФСБ России средств, например, ПАК «С-Терра Шлюз», в том числе – АРМ администратора. Связь с сервером syslog должна осуществляться по каналу, в котором исключено наличие нарушителя (при этом защита канала от несанкционированного доступа должна осуществляться организационно-техническими мерами), либо должна защищаться сертифицированным ФСБ России СКЗИ.

Формирование ключей для СКЗИ «С-Терра Шлюз» может выполняться с использованием средств самого СКЗИ или другого сертифицированного ФСБ

© ООО "С-Терра СиЭсПи"

России СКЗИ «С-Терра Шлюз» или СКЗИ «С-Терра Клиент» (в том числе на рабочих местах пользователей, или на АРМ администратора).

Ввод корневых доверенных сертификатов, контейнеров ключей ЭП и внешней гаммы ПДСЧ в СКЗИ должен производиться аутентифицированным администратором на носителях, поддерживаемых ПАК и перечисленных в разделе 3, которые могут быть подключены к конфигурируемому устройству.

При обновлении версии СКЗИ администратор должен убедиться в том, что устанавливаемая версия СКЗИ прошла сертификацию ФСБ России. ПО СКЗИ разрешается обновлять только на версию, имеющую положительное заключение 8 Центра ФСБ России. Перед установкой обновления администратор должен произвести расчёт контрольных сумм и их сравнение с эталонными значениями, полученными доверенным способом. Обновление должно выполняться в соответствии с эксплуатационной документацией устанавливаемой версии СКЗИ.

Доверенным считается способ передачи информации (контрольных сумм, настроек) по каналу, защищённому при помощи сертифицированного ФСБ России 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.

СКЗИ «С-Терра Шлюз» может обеспечивать раздельное или совместное выполнение функций безопасности – фильтрация, шифрование, имитозащита, аутентификация абонентов. При установке параметров, позволяющих создавать криптографически незащищенные соединения, должны быть

© ООО "С-Терра СиЭсПи"

приняты меры, исключающие утечку требующей защиты информации с защищаемого объекта информатизации. Администратор СКЗИ должен описать в политике безопасности СКЗИ «С-Терра Шлюз» все необходимые функции безопасности, исходя из модели угроз. Трафик считается незащищенным, если к нему не применяется определяемый администратором набор функций безопасности из перечисленных ниже в тексте (в зависимости от способа задания политики безопасности). Проверка достаточности принятых мер защиты проводится на основе модели угроз безопасности информации информационной системы, в которой эксплуатируется СКЗИ.

При использовании СКЗИ «С-Терра Шлюз» обязательно включение функции имитозащиты путём указания в политике безопасности хотя бы одного алгоритма имитозащиты или комбинированного преобразования из числа приведённых в данном разделе настоящих правил. Эксплуатация СКЗИ без имитозащиты не допускается.

При эксплуатации СКЗИ «С-Терра Шлюз» возможна фильтрация сообщений, регистрируемых в журнале. Администратор не должен блокировать следующие критически важные сообщения, перечисленные в таблице 3:

Таблица 2. 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 %{5} - имя IKE-правила
0010011A	Попытка создания IPsec SA закончилась неудачей.

© ООО "С-Терра СиЭсПи"

	%{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

© ООО "С-Терра СиЭсПи"

Для указания выполняемых СКЗИ функций безопасности администратором должна быть написана политика безопасности с помощью конфигурационного файла безопасности (в формате LSP), либо с помощью cs_console. Для СКЗИ, сконфигурированных указанными способами, обеспечивается возможность встречной работы при условии использования одинаковых режимов работы протоколов и алгоритмов.

6.5.1 Задание политики безопасности с помощью файла (LSP)

Для указания выполняемых СКЗИ 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 ISAKMP). Формат описания и взаимосвязи структур и атрибутов описаны в разделе «Создание конфигурационного файла» Руководства администратора.

Далее в общей структуре политики безопасности указаны настройки, определяющие все возможные режимы защищённого взаимодействия и параметры безопасности:

```
GlobalParameters(
   CRLHandlingMode          = …%режим работы со списками аннулированных сертификатов – см. параграф «Атрибут CRLHandlingMode» в разделе «Создание конфигурационного файла» Руководства администратора %
)

IKEParameters(
%нет параметров безопасности%
)

IKETransform crypto:isakmp:policy:1
(
   CipherAlg     = %алгоритм шифрования из перечисленных далее в этом разделе Правил%
```

```
   HashAlg        = %алгоритм хэширования из перечисленных далее в этом разделе Правил%
   GroupID        = %алгоритм выработки разделяемого ключа из перечисленных далее в этом разделе Правил%
   LifetimeSeconds = %время жизни ISAKMP соединения в секундах, ограничение приведено далее в этом разделе Правил%
)

ESPProposal TSET:ESP
(
   Transform* = ESPTransform %или ESPTC26Transform%
   (
      CipherAlg*          = %алгоритм шифрования трафика из перечисленных далее в этом разделе Правил%
      IntegrityAlg*       = %алгоритм имитозащиты трафика из перечисленных далее в этом разделе Правил%
      CombinedAlg*        = %алгоритм комбинированного преобразования трафика из перечисленных далее в этом разделе Правил%
      LifetimeSeconds     = %время жизни IPsec соединения в секундах, ограничение приведено далее в этом разделе Правил%
      LifetimeKilobytes   = %разрешённый объём данных, обрабатываемых в рамках одного IPsec соединения в килобайтах, ограничение приведено далее в этом разделе Правил%
   )
)

AuthMethodGOSTSign GOST:Sign
(
   RemoteID        = %описание сертификата партнёра, см. параграф «Атрибут RemoteID» в разделе «Создание конфигурационного файла» Руководства администратора%
)

IKERule IKERule:CMAP:1
(
   IKEPeerIPFilter = %IP-адрес партнёра по взаимодействию%
   Transform = crypto:isakmp:policy:1
   AggrModeAuthMethod  = %привязка к описанной ранее структуре параметров безопасности - GOST:Sign%
   MainModeAuthMethod  = %привязка к описанной ранее структуре параметров безопасности - GOST:Sign%
)

IPsecAction IPsecAction:CMAP:1
(
   TunnelingParameters = TunnelEntry(
      PeerAddress = %IP-адрес партнёра по взаимодействию для туннельного режима работы IPsec%
   )
```

© ООО "С-Терра СиЭсПи"

ContainedProposals = (%привязка к описанной ранее структуре параметров безопасности - TSET:ESP%)
GroupID = %опциональный алгоритм выработки разделяемого ключа для технологии PFS, из перечисленных далее в этом разделе Правил%
IKERule = %привязка к описанной ранее структуре параметров безопасности - IKERule:CMAP:1%
)

IKEParameters2(
%нет параметров безопасности%
)

IKEProposal2 crypto:ikev2:policy:1
(
EncryptionAlg = %алгоритм шифрования из перечисленных далее в этом разделе Правил%
PrfAlg = %алгоритм хэширования из перечисленных далее в этом разделе Правил%
IntegrityAlg = %алгоритм имитозащиты из перечисленных далее в этом разделе Правил%
KeyAlg = %алгоритм выработки разделяемого ключа из перечисленных далее в этом разделе Правил%
Limits = ConnectionLimits(
Seconds = %время жизни IKEv2 соединения в секундах, ограничение приведено далее в этом разделе Правил%
)
)

IPsecProposal2 TSET:ESP2
(
ESPEncryptionAlg = %алгоритм шифрования трафика из перечисленных далее в этом разделе Правил%
ESPIntegrityAlg = %алгоритм имитозащиты трафика из перечисленных далее в этом разделе Правил%
PFSAlg = %опциональный алгоритм выработки разделяемого ключа для технологии PFS, из перечисленных далее в этом разделе Правил%
Limits = ConnectionLimits(
Seconds = %время жизни IPsec соединения в секундах, ограничение приведено далее в этом разделе Правил%
Kilobytes = %разрешённый объём данных, обрабатываемых в рамках одного IPsec соединения в килобайтах, ограничение приведено далее в этом разделе Правил%
)
)

IKEAuth2 IKEAuth2:Remote
(
Identity = %описание сертификата партнёра, см. параграф «Атрибут RemoteID» в разделе «Создание конфигурационного файла» Руководства администратора%

© ООО "С-Терра СиЭсПи"

```
)

IKERule2 IKERule2:CMAP:1
(
   IKEPeerIPFilter = %IP-адрес партнёра по взаимодействию%
   Proposals = crypto:ikev2:policy:1
   RemoteAuth = %привязка к описанной ранее структуре параметров безопасности - IKEAuth2:Remote%
)

IPsecAction2 IPsecAction2:CMAP:1
(
   TunnelingParameters = TunnelEntry(
      PeerAddress = %IP-адрес партнёра по взаимодействию для туннельного режима работы IPsec%
   )
   ContainedProposals = (%привязка к описанной ранее структуре параметров безопасности - TSET:ESP2% )
   IKERule = %привязка к описанной ранее структуре параметров безопасности – IKERule2:CMAP:1%
)

FilterChain IPsecPolicy:CMAP (
   IPv4Filters = Filter (
      SourceIP, DestinationIP, ProtocolID, SourcePort, DestinationPort = <описание сетевых параметров защищаемых ресурсов>
      Action = <выбор действия: PASS – пропустить трафик, DROP – фильтровать>
      ExtendedAction = ipsec< sa = %привязка к описанной ранее структуре параметров безопасности - IPsecAction:CMAP:1%, %привязка к описанной ранее структуре параметров безопасности – IpsecAction2:CMAP:1% >
   ),
   Filter (
   …
   )
   IPv6Filters = Filter (
   …
   ),
   Filter (
   …
   )
)

NetworkInterface (
   LogicalName = %имя сетевого интерфейса, к которому привязываются параметры безопасности, для примера - GigabitEthernet1/3%
   IPsecPolicy = %привязка к описанной ранее структуре параметров безопасности - IPsecPolicy:CMAP%
)
```

© ООО "С-Терра СиЭсПи"

Для применения комбинированного преобразования ENCR_KUZNYECHIK_MGM_KTREE, обеспечивающего конфиденциальность и имитозащиту информации в канале связи с сохранением возможности встречной работы с СКЗИ «С-Терра VPN» версии 4.3, необходимо:

- атрибуту CombinedAlg в структуре ESPTransform присвоить значение "GR341215K-K352-MGM-251".

Для обеспечения работы протокола ISAKMP с целью выполнения любых криптографических функций безопасности с использованием криптографических алгоритмов ГОСТ 34.11-2018 и ГОСТ 34.10-2018, с сохранением возможности встречной работы с СКЗИ «С-Терра VPN» версии 4.3, необходимо:

- присвоить атрибуту CipherAlg в структуре IKETransform значение "G2814789CPRO1-K256-CBC-65534" или "GR341215K-K256-CFB-65528";
- присвоить атрибуту HashAlg в структуре IKETransform значение "GR341112_256TC26-65128" или "GR341194CPRO1-65534";
- присвоить атрибуту GroupID в структуре IKETransform значение VKO2_1B.

Для обеспечения аутентификации абонентов с использованием электронной подписи по стандарту ГОСТ 34.10–2018 необходимо:

- присвоить атрибуту MainModeAuthMethod или AggrModeAuthMethod в структуре IKERule (IKERule2) значение типа AuthMethodGOSTSign;
- добавление, просмотр, удаление сертификатов должны производиться администратором безопасности в соответствии с Руководством администратора;

© ООО "С-Терра СиЭсПи"

- создание симметричных предварительно распределенных ключей, ключей подписи и сертификатов должно производиться администратором безопасности в соответствии с Руководством администратора, при помощи сертифицированного ФСБ России СКЗИ;
- доставка симметричных предварительно распределенных ключей, ключей подписи и доверенных (trusted) сертификатов должна производиться администратором безопасности в соответствии с Руководством администратора, доверенным способом.

СКЗИ «С-Терра Шлюз» версии 5.0 поддерживает встречную работу по протоколам, соответствующим спецификациям TK26IKE и TK26ESP с сертифицированным ФСБ России СКЗИ «КриптоПро CSP» версии 5.0R2. При конфигурировании такого соединения следует использовать в СКЗИ «С-Терра Шлюз» следующие настройки:

IKETC26Transform CipherAlg = GOST_B_CFB_IMIT

IKETC26Transform HashAlg = GOST_R_34_11_2012_512

ESPTC26Transform CombinedAlg = GOST_Z_4M_IMIT

Полное описание порядка конфигурирования приведено в руководстве администратора.

СКЗИ «С-Терра Шлюз» версии 5.0 поддерживает встречную работу по протоколам, соответствующим спецификациям Р 1323565.1.048–2023 (IKEv2) и Р1323565.1.035-2021 (ESP). Полное описание порядка конфигурирования приведено в руководстве администратора.

Объём информации, обрабатываемой на одном ключе, должен быть ограничен. Ограничения по трафику, реализуемые с помощью атрибута

© ООО "С-Терра СиЭсПи"

LifetimeKilobytes политики безопасности, перечислены в таблице 5. При превышении рекомендуемого значения LifetimeKilobytes в момент создания защищённого соединения регистрируется событие MSG_ID_LP_IPSEC_HI_TTL_TRAFFIC (см. ID 00100140 в таблице 3).

Таблица 3. Ограничения объёма трафика для различных алгоритмов и протоколов

Протокол	Алгоритм	LifetimeKilobytes
IKETransform	G2814789CPRO1-K256-CBC	1984
ESPTransform	G2814789CPRO1-K256-CBC	4032

Для алгоритмов, не упомянутых в таблице 5, объём трафика ограничивается только пропускной способностью сетевых интерфейсов за время жизни защищённого соединения. Время жизни защищённого соединения не должно превышать 1 суток, для чего атрибуту LifetimeSeconds должно быть присвоено значение не более 86400, независимо от наличия ограничения по объёму трафика.

6.5.2 Задание политики безопасности с помощью cs_console

Для указания выполняемых ПАК функций безопасности администратором должна быть написана политика безопасности, с использованием структур crypto map (описание трафика), crypto ipsec (описание параметров соединения ESP или AH), crypto isakmp (описание параметров соединения ISAKMP). Формат описания и взаимосвязи структур и атрибутов соответствует определенным для команд Cisco.

Далее в общей структуре политики безопасности указаны настройки, определяющие все возможные режимы защищённого взаимодействия и параметры безопасности:

crypto pki trustpoint WORD

© ООО "С-Терра СиЭсПи"

revocation-check %режим работы со списками аннулированных сертификатов%

!

crypto isakmp policy <1-10000>

encr %алгоритм шифрования из перечисленных далее в этом разделе Правил%

hash %алгоритм хэширования из перечисленных далее в этом разделе Правил%

group %алгоритм выработки разделяемого ключа из перечисленных далее в этом разделе Правил%

authentication %метод аутентификации сторон%

set lifetime kilobytes % разрешённый объём данных, обрабатываемых в рамках одного ISAKMP соединения в килобайтах, ограничение приведено далее в этом разделе Правил%

set lifetime seconds %время жизни ISAKMP соединения в секундах, ограничение приведено далее в этом разделе Правил%

!

crypto ipsec security-association lifetime seconds %время жизни IPsec соединения в секундах, ограничение приведено далее в этом разделе Правил%

crypto ipsec security-association lifetime kilobytes %разрешённый объём данных, обрабатываемых в рамках одного IPsec соединения в килобайтах, ограничение приведено далее в этом разделе Правил%

crypto ipsec transform-set WORD %алгоритм шифрования или комбинированного преобразования трафика из перечисленных далее в этом разделе Правил%

ip access-list extended WORD

<выбор действия: permit – применить правило, deny – не применять правило> <описание сетевых параметров защищаемых ресурсов>

!

crypto map CMAP %привязка к описанной ранее структуре параметров безопасности - crypto isakmp policy% ipsec-isakmp

set peer %IP-адрес партнёра по взаимодействию%

set transform-set %привязка к описанной ранее структуре параметров безопасности – «crypto ipsec transform-set»%

set pfs %опциональный алгоритм выработки разделяемого ключа для технологии PFS, из перечисленных далее в этом разделе Правил%

match address %привязка к описанной ранее структуре параметров безопасности – «ip access-list extended»%

!

Interface %имя сетевого интерфейса, к которому привязываются параметры безопасности, для примера - GigabitEthernet1/3%

crypto map %привязка к описанной ранее структуре параметров безопасности - IPsecPolicy:CMAP%

!

Для применения комбинированного преобразования ENCR_KUZNYECHIK_MGM_KTREE, обеспечивающего конфиденциальность и

© ООО "С-Терра СиЭсПи"

имитозащиту информации в канале связи с сохранением возможности встречной работы с СКЗИ «С-Терра VPN» версии 4.3, необходимо:

- использовать в структуре crypto ipsec transform-set WORD значение "esp-cipher-gost341215k-mgm".

Для обеспечения работы протокола ISAKMP с целью выполнения любых криптографических функций безопасности с использованием криптографических алгоритмов ГОСТ 34.11-2018 и ГОСТ 34.10-2018, с сохранением возможности встречной работы с СКЗИ «С-Терра VPN» версии 4.3, необходимо:

- присвоить атрибуту encr в структуре «crypto isakmp policy <1-10000>» значение "gost";
- присвоить атрибуту hash в структуре «crypto isakmp policy <1-10000>» значение "gost341112-256-tc26" или "gost";
- присвоить атрибуту group в структуре «crypto isakmp policy <1-10000>» значение vko2.

Для обеспечения аутентификации абонентов с использованием электронной подписи по стандарту ГОСТ 34.10–2018 необходимо присвоить атрибуту authentication в структуре «crypto isakmp policy <1-10000>» значение типа gost-sig, при этом:

- добавление, просмотр, удаление сертификатов должны производиться администратором безопасности в соответствии с Руководством администратора;
- создание ключей подписи и сертификатов должно производиться администратором безопасности в соответствии с Руководством

© ООО "С-Терра СиЭсПи"

администратора, при помощи сертифицированного ФСБ России СКЗИ;

- доставка ключей подписи и доверенных (trusted) сертификатов должна производиться администратором безопасности в соответствии с Руководством администратора, доверенным способом.

СКЗИ «С-Терра Шлюз» версии 5.0 поддерживает встречную работу по протоколам, соответствующим спецификациям TK26IKE и TK26ESP с сертифицированным ФСБ России СКЗИ «КриптоПро CSP» версии 5.0R2. При конфигурировании такого соединения следует использовать в СКЗИ «С-Терра Шлюз» следующие настройки:

crypto isakmp policy <1-10000> cipher tc26-ike-gost-b-imit

crypto isakmp policy <1-10000> hash tc26-ike-gost341112-512

crypto ipsec transform-set WORD tc26-esp-gost-z-4m-imit

Объём информации, обрабатываемой на одном ключе, должен быть ограничен. Ограничения по трафику, реализуемые с помощью атрибутов crypto ipsec security-association lifetime kilobytes %LifetimeKilobytes% и crypto isakmp policy <1-10000> set lifetime kilobytes %LifetimeKilobytes% политики безопасности, перечислены в таблице 7. При превышении рекомендуемого значения LifetimeKilobytes в момент создания защищённого соединения регистрируется событие MSG_ID_LP_IPSEC_HI_TTL_TRAFFIC (см. ID 00100140 в таблице 3).

Таблица 4. Ограничения объёма трафика для различных алгоритмов и протоколов

Протокол	Алгоритм	LifetimeKilobytes
crypto isakmp	gost	1984

© ООО "С-Терра СиЭсПи"

crypto ipsec	gost28147	4032

Для алгоритмов, не упомянутых в таблице 7, объём трафика ограничивается только пропускной способностью сетевых интерфейсов за время жизни защищённого соединения. Время жизни защищённого соединения не должно превышать 1 суток, для чего атрибуту LifetimeSeconds должно быть присвоено значение не более 86400, независимо от наличия ограничения по объёму трафика.

6.5.3 Общие ограничения на применение криптографических алгоритмов

Для шифрования, контроля целостности (имитозащиты) и аутентификации не должны использоваться алгоритмы, отличные от основанных на российских стандартах ГОСТ 28147-89, ГОСТ 34.10-2018 (ГОСТ Р 34.10-2012), ГОСТ 34.11-2018 (ГОСТ Р 34.11-2012), ГОСТ 34.12-2018 (ГОСТ Р 34.12-2015), ГОСТ 34.13-2018 (ГОСТ Р 34.13-2015).

Обратите внимание: Криптографические преобразования, ENCR_KUZNYECHIK_MGM_MAC_KTREE, ENCR_MAGMA_MGM_MAC_KTREE, применяемые в протоколе ESP, обеспечивают только имитозащиту и не обеспечивают конфиденциальность передаваемых данных.

Для аутентификации абонентов должен использоваться метод проверки электронной подписи ГОСТ 34.10-2018, задаваемый в политике безопасности идентификатором AuthMethodGOSTSign, или метод аутентификации на симметричных предварительно распределенных ключах с использованием алгоритма ГОСТ 34.11-2018, задаваемый в политике безопасности идентификатором AuthMethodPreshared.

Применение алгоритма ГОСТ 28147-89 в режиме выработки имитовставки в качестве единственного самостоятельного алгоритма

© ООО "С-Терра СиЭсПи"

имитозащиты для IPsec соединения (идентификаторы G2814789CPRO1-K256-MAC, ah-gost28147-mac, esp-gost28147-mac) запрещено. Допускается применение указанного алгоритма только в составе или в дополнение к комбинированному преобразованию (идентификаторы G2814789CPRO2-K288-CNTMAC или GR341215K-K352-MGM, esp-gost28147-4m-imit или esp-cipher-gost341215k-mgm).

Алгоритмы ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2001 запрещается применять для защиты информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.

По умолчанию в ПАК «С-Терра Шлюз» активны и доступны к применению российские криптографические алгоритмы. В комплект поставки ПО ПАК «С-Терра Шлюз» также включен программный модуль, реализующий иностранные криптографические алгоритмы. Данный программный модуль может применяться только для плавной миграции всех взаимодействующих устройств с ранее выпущенных версий «CSP VPN Gate», «С-Терра VPN» или иных продуктов. **Запрещается применять иностранные криптографические алгоритмы для защиты информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.** После осуществления миграции следует деактивировать этот модуль, выполнив в утилите auth_login от имени администратора СКЗИ команду:

crypto algorithms enable gost

Полное описание команды приведено в руководстве администратора.

© ООО "С-Терра СиЭсПи"

7. Требования по обеспечению безопасности при эксплуатации СКЗИ

7.1. Общие требования по защите от НСД

Безопасная эксплуатация СКЗИ регламентируется правилами пользования СКЗИ и перечисленной в формуляре эксплуатационной документацией СКЗИ.

Обязательно наличие опечатываемого хранилища (шкафа, сейфа) для хранения эталонных CD дисков с ПО и эксплуатационной документацией и другой конфиденциальной информации. Ключ от хранилища должен храниться у администратора СКЗИ. Дубликат ключа должен храниться в сейфе руководителя организации или уполномоченного им лица.

Исполнения «3М3», «3М5» необходимо применять только на аппаратных платформах, в ППЗУ которых записан BIOS с встроенным ПК «С-Терра МАЯК» Обозначения платформ (варианты комплектации) и контрольные суммы ПО BIOS, прошедшие тематические исследования в рамках исследований СКЗИ, приведены в формуляре.

7.2. Требования к аутентификации и разграничению доступа

На ПАК «С-Терра Шлюз» исп. «3М3», «3М5» аутентификация проводится до приведения АС в рабочее состояние, средствами ПК «С-Терра МАЯК».

Далее для всех исполнений ПАК «С-Терра Шлюз» производится ролевая аутентификация до приведения СКЗИ в состояние готовности, при помощи утилиты разграничения доступа auth_login, входящей в состав СКЗИ. Аутентификация позволяет различать учётные записи пользователей, обладающих правами на управление СКЗИ (привилегированных

© ООО "С-Терра СиЭсПи"

пользователей) и пользователей, возможности которых ограничиваются до просмотра неконфиденциальной информации о состоянии СКЗИ (непривилегированных пользователей). Привилегированный пользователь выполняет обязанности администратора СКЗИ. В функции администратора СКЗИ входит выпуск ключей и конфигурирование СКЗИ, включая управление перечнем доверенных сертификатов. Утилита auth_login реализует однофакторную (по паролю) и двухфакторную (по паролю и носителю ключа) аутентификацию. Для исполнений «3М5» должна применяться двухфакторная аутентификация, а в случае использования однофакторной аутентификации СКЗИ должно применяться в однопользовательском режиме.

При проведении локальной аутентификации при помощи утилиты разграничения доступа auth_login, производится контроль количества ошибок. При достижении установленного администратором количества ошибок входа подряд учётная запись пользователя блокируется. Разблокировка учётной записи производится автоматически через промежуток времени, устанавливаемый согласно руководству администратора, а также возможна разблокировка командой unblock user модуля разграничения доступа при локальном входе другого привилегированного пользователя. При заводских настройках допускается 10 попыток входа, количество попыток определяет параметр login_attempts_count в /opt/VPNagent/etc/auth_login.ini, его значение не должно увеличиваться. При заводских настройках автоматическая разблокировка заблокированной учётной записи произойдёт через 60 минут, время разблокировки определяется параметром login_long_wait_timeout в файле /opt/VPNagent/etc/auth_login.ini, его значение не должно быть менее 10 минут.

© ООО "С-Терра СиЭсПи"

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

- Администратор СКЗИ должен ознакомиться со всей документацией, прилагаемой к ПАК.
- Право доступа к режиму управления комплексом (пользовательскому интерфейсу СКЗИ) имеет только администратор СКЗИ (далее по тексту - администратор).
- 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 СКЗИ в соответствии с Руководством администратора.
- Необходимо организовать систему протоколирования и аудита, и вести регулярный анализ результатов аудита с целью выявления нарушений и попыток несанкционированного доступа к ПАК.
- Необходимо разработать политику назначения и смены паролей в соответствии со следующими правилами:
    - длина пароля должна быть не менее 8 символов таблицы ASCII;
    - 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

© ООО "С-Терра СиЭсПи"

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;
- периодичность смены пароля определяется принятой в информационной системе политикой безопасности, но не должна превышать 6 месяцев.

7.3. Требования по обеспечению целостности СКЗИ

Целостность ПО СКЗИ исполнений «3М3», «3М5» контролируется средствами СКЗИ.

Администратор должен проводить регламентный контроль целостности ПО СКЗИ «С-Терра Шлюз» не реже 1 раза в месяц. Контрольные суммы ПО приведены в разделе 4 Формуляра. Контрольная сумма одного файла вычисляется утилитой stverify по ГОСТ 34.11-2018 (256 бит) следующим образом:

```
stverify -mk <ИМЯ_ФАЙЛА> -alg GR3411_2012_256 -inverted_halfbytes 0
```

Набор контрольных сумм контролируемых файлов СКЗИ и СФ предустановлен в файле /var/s-terra/hashes.list на файловой системе ПАК.

Контрольная сумма файлов по перечню проверяется утилитой cspvpn_verify.

Для проверки контрольных сумм ПО СКЗИ при проведении регламентного контроля целостности нужно:

1. Получить доступ к ПАК с правами администратора одним из двух вариантов:

© ООО "С-Терра СиЭсПи"

a. Удалённо – с АРМ администратора по протоколу ssh под защитой IPsec соединения.

b. Локально – по последовательному соединению, пройдя локальную аутентификацию на консоли устройства (автоматически запускаемой утилитой auth_login).

2. Проверить целостность перечня контролируемых файлов, для чего выполнить команду:

```
stverify -mk /var/s-terra/hashes.list -alg GR3411_2012_256 -inverted_halfbytes 0
```

и сравнить выведенную строку с приведённым в формуляре значением контрольной суммы перечня файлов.

3. Проверить целостность файлов по перечню, для чего выполнить команду cspvpn_verify и проконтролировать выведенное в терминал сообщение “Verification SUCCESS”.

4. Проверить целостность загрузчика, для чего выполнить команду:

```
stverify -mk /boot/efi/efi/boot/bootx64.efi -alg GR3411_2012_256 -inverted_halfbytes 0
```

и сравнить выведенную строку с приведённым в формуляре значением.

5. Проверить целостность утилиты flash_mgr, для чего выполнить команду:

```
stverify -mk /opt/VPNagent/bin/flash_mgr -alg GR3411_2012_256 -inverted_halfbytes 0
```

и сравнить выведенную строку с приведённым в формуляре значением.

Целостность ПО СКЗИ считается не нарушенной, если все описанные выше проверки выполнены успешно. Если целостность нарушена, администратор должен выполнить процедуру восстановления целостности.

Для восстановления целостности следует выполнить перезапись ПО согласно руководству администратора (раздел «Инструкции по

© ООО "С-Терра СиЭсПи"

восстановлению»), используя эталоны, записанные на отдельном CD-диске, прилагающемся к СКЗИ.

Инструкция по проверке целостности ПО BIOS

Выполнить скрипт вычисления контрольной суммы:

```
/opt/VPNagent/bin/fw_check.sh
```

Сравнить полученную контрольную сумму CRC32 с приведённой в формуляре, в столбце «CRC32 экспл.». При обнаружении несоответствия обратиться к поставщику СКЗИ за инструкциями.

7.4. Порядок обеспечения работоспособности СКЗИ

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

Эксплуатация СКЗИ запрещена при наступлении следующих событий:

- обнаружение несанкционированного вскрытия корпуса или повреждения пломб;
- нарушение целостности ПО ПАК;
- компрометация ключей аутентификации;
- обнаружение неработоспособности ПАК (например - ошибки при прохождении теста BIOS POST).

При наступлении любого из перечисленных событий администратор СКЗИ должен прекратить эксплуатацию СКЗИ, оценить вероятные последствия и принять меры для устранения нарушений.

Запрещается:

- оставлять без контроля СКЗИ;
- осуществлять несанкционированное вскрытие ПАК;

© ООО "С-Терра СиЭсПи"

- 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 СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- вносить изменения в предустановленное ПО и в состав аппаратных средств ПАК;
- эксплуатировать СКЗИ в случае неисправности аппаратных средств ПАК и нарушения целостности ПО.

Администратор СКЗИ должен регулярно проводить анализ журналов событий СКЗИ и применяемых средств защиты от НСД, в соответствии с эксплуатационной документацией.

Для антивирусной защиты пользователей защищаемой сети средства антивирусной защиты должны устанавливаться либо непосредственно на ПЭВМ пользователя сети, либо на сервер централизованной антивирусной защиты.

Производитель СКЗИ публикует информацию о наличии уязвимостей, рекомендации по обходу уязвимостей и информацию о наличии обновлений безопасности на официальном web-сайте в разделе https://www.s-terra.ru/podderzhka/zagruzki/. При невозможности использования web-сайта

© ООО "С-Терра СиЭсПи"

необходимо пользоваться другими официальными каналами связи с производителем СКЗИ. Администратор СКЗИ должен периодически просматривать указанную информацию. Необходимо устанавливать все обновления безопасности, рекомендуемые производителем СКЗИ, а при отсутствии обновлений выполнять рекомендации по обходу уязвимостей. Запрещается исполнять ПО, полученное из недоверенных источников.

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

Файл rnd.bin, располагающийся по пути, определяемом параметром RndStorage в конфигурационном файле skzi.conf, или, по умолчанию, в директории /var/s-terra/, содержит данные, требуемые для работы СКЗИ, которые не должны использоваться вторично. Запрещается восстанавливать файл rnd.bin из резервной копии или препятствовать его штатному изменению при работе СКЗИ. При повреждении или уничтожении файла rnd.bin работоспособность СКЗИ может быть нарушена. После сбоя или восстановления ПО из резервной копии для возобновления работы СКЗИ необходимо удалить повреждённый или ранее использованный файл rnd.bin и инициализировать программный датчик случайных чисел, входящий в состав СКЗИ, выполнив программу rnd_mgr.

© ООО "С-Терра СиЭсПи"

8. Требования по обеспечению безопасности при выводе СКЗИ из эксплуатации и передаче в ремонт

Перед ремонтом и утилизацией СКЗИ «С-Терра Шлюз» администратор СКЗИ должен удалить и отозвать ключевую информацию и очистить накопитель, на котором хранится ПО СКЗИ, выполнив команду очистки в соответствии с руководством администратора - «РЛКЕ.00033-01 92 01 Программный комплекс «С-Терра Шлюз». Версия 5.0. Руководство администратора».

Ремонт и утилизация аппаратных средств после очистки может осуществляться без ограничений, накладываемых на действия с СКЗИ.

Если выполнение очистки накопителей невозможно (например, в случае неработоспособности аппаратной платформы), то ремонт должен осуществляться только лицензиатом ФСБ России, а утилизация должна производиться с физическим уничтожением накопителей информации.

Контроль соответствия возвращаемых после ремонта СКЗИ сертифицированному ФСБ России образцу должен осуществляться с участием производителя СКЗИ.

© ООО "С-Терра СиЭсПи"