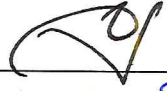


СОГЛАСОВАНО

Начальник 2 управления
ФСТЭК России


_____ Д.Н. Шевцов
«27» декабря 2018 года

УТВЕРЖДАЮ

Генеральный директор
ООО «С-Терра СиЭсПи»



_____ С.В.Мещеряков
_____ 2018 года

Программно-аппаратный комплекс

С-Терра Шлюз

Версия 4.2

Формуляр

ЛИСТ УТВЕРЖДЕНИЯ

РЛКЕ.00019-01 30 01-ЛУ

Листов 1

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

ООО "С-Терра СиЭсПи"

УТВЕРЖДЕН
РЛКЕ.00019-01 30 01-ЛУ

Программно-аппаратный комплекс

С-Терра Шлюз

Версия 4.2

Формуляр

РЛКЕ.00019-01 30 01
Листов 27

2017

Содержание

1	ОБЩИЕ УКАЗАНИЯ.....	3
2	ОБЩИЕ СВЕДЕНИЯ.....	4
3	ОСНОВНЫЕ ХАРАКТЕРИСТИКИ.....	7
4	КОМПЛЕКТНОСТЬ.....	13
5	ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА.....	17
6.	СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ.....	18
7	СВИДЕТЕЛЬСТВО О ПРИЕМКЕ.....	19
8	СВЕДЕНИЯ О РЕКЛАМАЦИЯХ.....	20
9	СВЕДЕНИЯ О ХРАНЕНИИ.....	21
10	СВЕДЕНИЯ ОБ УСТАНОВКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	22
11	УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ.....	23
12	КОНТРОЛЬ СОСТОЯНИЯ ИЗДЕЛИЯ И ВЕДЕНИЯ ФОРМУЛЯРА.....	26

1 ОБЩИЕ УКАЗАНИЯ

1.1 Формуляр на изделие «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» является документом, удостоверяющим основные параметры и технические характеристики изделия, отражающим его техническое состояние и содержащим сведения по его эксплуатации.

1.2 Перед эксплуатацией изделия необходимо внимательно ознакомиться с комплектом документации изделия и принять защитные организационные меры, рекомендуемые в документации.

1.3 Состав комплекта поставки изделия определяется в соответствии с заявкой заказчика и указывается в разделе 4 Формуляра.

1.4 В случае обнаружения дефектов следует обращаться к поставщику изделия.

1.5 Формуляр должен находиться у ответственного должностного лица (администратора), отвечающего за эксплуатацию изделия. Все записи в Формуляре производятся только чернилами отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления ЗАПРЕЩАЮТСЯ. Неправильная запись должна быть аккуратно зачеркнута и рядом записана новая, которую заверяет ответственное лицо. После подписи проставляют фамилию и инициалы ответственного лица (штамп исполнителя).

2 ОБЩИЕ СВЕДЕНИЯ

2.1 Наименование изделия

Полное наименование изделия: «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2».

Краткое наименование изделия: ПАК «С-Терра Шлюз».

Условное обозначение: РЛКЕ.00019-01.

2.2 Поставщик

Общество с ограниченной ответственностью «С-Терра СиЭсПи» (ООО «С-Терра СиЭсПи»): 124498, г.Москва, Зеленоград, Георгиевский проспект, дом 5, помещение I, комната 33, тел. (499) 940-9061.

2.3 Изготовитель

Общество с ограниченной ответственностью «С-Терра СиЭсПи» (ООО «С-Терра СиЭсПи»): 124498, г.Москва, Зеленоград, Георгиевский проспект, дом 5, помещение I, комната 33, тел. (499) 940-9061.

2.4 Модификация

ПАК «С-Терра Шлюз». Версия 4.2.

2.5 Сведения о сертификации

ПАК «С-Терра Шлюз» сертифицирован в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 и соответствует документу «Требования к межсетевым экранам», утвержденному приказом ФСТЭК России от 9 февраля 2016 г. № 9, документу «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» (ФСТЭК России, 2016) по оценочному уровню доверия ОУД 3, усиленному компонентами ADV_FSP.4 «Полная функциональная спецификация», ADV_IMP.2 «Полное отображение представления реализации ФБО», ADV_TDS.3 «Базовый модульный проект», ALC_CMC.4 «Поддержка генерации, процедуры приемки и автоматизация», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VAN.5 «Усиленный методический анализ», расширенный компонентами ADV_IMP_EXT.3 «Реализация ОО», ALC_FPU_EXT.1 «Процедуры обновления программного обеспечения меж сетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность меж сетевого экрана».

2.6 Контрольные суммы дистрибутивов

Таблица 1

Каталог с дистрибутивами	Контрольная сумма файла дистрибутива, подсчитанная по алгоритму ГОСТ Р 34.11-2012 с использованием утилиты stverify	Контрольная сумма файла дистрибутива, подсчитанная по алгоритму ГОСТ Р 34.11-2012 (256 бит) с использованием «РСП-Контроль»
CD-диск «С-Терра Шлюз ST KC1, KC2. Версия 4.2. Релиз 18201»		
STerra_Gate_ST_KC1_KC2 STerra_Gate_ST_KC1_KC2.zip	5CF4C100F111DB63910B532555478EA6019B90CFA38CE3DBD64B475A96F314F9	C54F1C001F11BD3619B035525574E86A10B909FC3AC83EBD6DB474A5693F419F
STerra_SmartFW Smartfw-intel.zip	A76BD2829AAFDD907D6613726974FAE4A907DAD098566BF20E5978F7DB42BE84	7AB62D28A9FADD09D76631279647AF4E9A70AD0D8965B62FE095877FBD24EB48
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE9AF8224C9CBE758F363AA418A03F8A8E	070DAEE08F1785D14379D05330989CECA98F22C4C9EB57F863A34A810AF3A8E8
CD-диск «С-Терра Шлюз ST KC3. Версия 4.2. Релиз 18201»		
STerra_Gate_ST_KC3 STerra_Gate_ST_KC3.zip	89D3C1FDA5C21485774B438A19E37423B7423D64C3261FA46EBAB2DA171D405C	983D1CDF5A2C415877B434A8913E47327B24D3463C62F14AE6AB2BAD71D104C5
STerra_SmartFW Smartfw-intel.zip	A76BD2829AAFDD907D6613726974FAE4A907DAD098566BF20E5978F7DB42BE84	7AB62D28A9FADD09D76631279647AF4E9A70AD0D8965B62FE095877FBD24EB48
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE9AF8224C9CBE758F363AA418A03F8A8E	070DAEE08F1785D14379D05330989CECA98F22C4C9EB57F863A34A810AF3A8E8
CD-диск «С-Терра Шлюз DP ST KC1, KC2. Версия 4.2. Релиз 18201»		
STerra_Gate_DP_ST_KC1_KC2 STerra_Gate_DP_ST_KC1_KC2.zip	0A7E3EB983E5C76E7EC7EEDA95886BDF27C7A84C74CD48FBDAE1EC096815BD7F	A0E7E39B385E7CE6E77CEEAD5988B6FD727C8AC447DC84BFAD1ECE908651DBF7
STerra_SmartFW Smartfw-intel.zip	A76BD2829AAFDD907D6613726974FAE4A907DAD098566BF20E5978F7DB42BE84	7AB62D28A9FADD09D76631279647AF4E9A70AD0D8965B62FE095877FBD24EB48
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE9AF8224C9CBE758F363AA418A03F8A8E	070DAEE08F1785D14379D05330989CECA98F22C4C9EB57F863A34A810AF3A8E8
CD-диск «С-Терра Шлюз DP ST KC3. Версия 4.2. Релиз 18201»		
STerra_Gate_DP_ST_KC3 STerra_Gate_DP_ST_KC3.zip	15D3C0C3EA890E47CC68BE29F6A0D1F79E4A56A0EA3FF42F3C865DC566907938	513D0C3CAE98E074CC86EB926F0A1D7FE9A4650AAEF34FF2C368D55C66099783
STerra_SmartFW Smartfw-intel.zip	A76BD2829AAFDD907D6613726974FAE4A907DAD098566BF20E5978F7DB42BE84	7AB62D28A9FADD09D76631279647AF4E9A70AD0D8965B62FE095877FBD24EB48
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE9AF8224C9CBE758F363AA418A03F8A8E	070DAEE08F1785D14379D05330989CECA98F22C4C9EB57F863A34A810AF3A8E8
CD-диск «С-Терра Шлюз CP KC1, KC2. Версия 4.2. Релиз 18579»		
STerra_Gate_CP_KC1_KC2 STerra_Gate_CP_KC1_KC2.zip	295F45CE1BE23B3E8C7FA4850B6247C40F5E61E82AE50E7CC0BC091286610FC3	92F554ECB12EB3E3C8F74A58B026744CF0E5168EA25EE0C70CCB90216816F03C
STerra_SmartFW Smartfw-intel.zip	A76BD2829AAFDD907D6613726974FAE4A907DAD098566BF20E5978F7DB42BE84	7AB62D28A9FADD09D76631279647AF4E9A70AD0D8965B62FE095877FBD24EB48
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE9AF8224C9CBE758F363AA418A03F8A8E	070DAEE08F1785D14379D05330989CECA98F22C4C9EB57F863A34A810AF3A8E8

CD-диск «С-Терра Шлюз CP KC3. Версия 4.2. Релиз 18579»		
STerra_Gate_CP_KC3 STerra_Gate_CP_KC3.zip	8A3D78201323070285DCDD3DF7C05A786 1E08D167828F00AD0A3D53185F23480	A8D387023132702058CDDDD37F0CA587 160ED86187820FA00D3A5D13582F4308
STerra_SmartFW Smartfw-intel.zip	A76BD2829AAFDD907D6613726974FAE4A 907DAD098566BF20E5978F7DB42BE84	7AB62D28A9FADD09D76631279647AF4E 9A70AD0D8965B62FE095877FBD24EB48
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE9 AF8224C9CBE758F363AA418A03F8A8E	070DAEE08F1785D14379D05330989CECA 98F22C4C9EB57F863A34A810AF3A8E8
CD-диск «С-Терра Шлюз ESR ST KC2. Версия 4.2. Релиз 18095»		
STerra_Gate_ESR_ST_KC2 STerra_Gate_ESR_ST_KC2.zip	F845FD6C2708218F6F84AA0DBACF8524 486CECA653B10BD8A0499E7F9C2DA7D	8F54DFC6728012F8F648AA00BDCA8F25 4468ECAC56B301DBA840997E9F2CADD7
STerra_SmartFW Smartfw-ESR.zip	AA84BBACD4BE1D872A36E8198FA786CF3 4410806F2AE85B40619152F4A54134E	AA48BBCA4DEBD178A2638E91F87A68FC 431480602FEA584B609151F2A44531E4
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE9 AF8224C9CBE758F363AA418A03F8A8E	070DAEE08F1785D14379D05330989CECA 98F22C4C9EB57F863A34A810AF3A8E8
CD-диск «С-Терра Шлюз ESR ST KC3. Версия 4.2. Релиз 18095»		
STerra_Gate_ESR_ST_KC3 STerra_Gate_ESR_ST_KC3.zip	F3363EA97DA5D644630D72F0A6899BC34 17B6E02A7B813B6E04115597DE41781	3F63E39AD75A6D4436D0270F6A98B93C 14B7E6207A8B316B0E145195D74E7118
STerra_SmartFW Smartfw-ESR.zip	AA84BBACD4BE1D872A36E8198FA786CF3 4410806F2AE85B40619152F4A54134E	AA48BBCA4DEBD178A2638E91F87A68FC 431480602FEA584B609151F2A44531E4
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE9 AF8224C9CBE758F363AA418A03F8A8E	070DAEE08F1785D14379D05330989CECA 98F22C4C9EB57F863A34A810AF3A8E8

Примечание: Контрольные суммы файлов дистрибутива подсчитаны по алгоритму ГОСТ Р 34.11-2012 с использованием утилиты stverify, входящей в состав продукта и «РСП-Контроль» (версия 1.2, ООО ЦРИОИТ, сертификат ФСТЭК России №2053 от 16 марта 2010 г.) по алгоритму ГОСТ Р 34.11-2012 (256 бит).

Контрольные суммы для исполняемых файлов, подсчитанные по алгоритму ГОСТ Р 34.11-2012 с использованием утилиты stverify и по алгоритму ГОСТ Р 34.11-2012 (256 бит) с использованием «РСП-Контроль» (версия 1.2, ООО ЦРИОИТ, сертификат ФСТЭК России №2053 от 16 марта 2010 г.), приведены в Приложении 1 к Формуляру.

3 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1 «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» является межсетевым экраном, реализующим функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков и используемое в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа.

Является программно-аппаратным средством защиты сетей, подсетей, офисов и самого шлюза от несанкционированного доступа.

3.2 «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» обеспечивает:

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

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

- возможность осуществлять посредничество в передаче информации сетевого трафика, основанное на типе сетевого трафика;
- возможность маскирования наличия МЭ способами, затрудняющими нарушителем его выявление;
- возможность регистрации и учета выполнения проверок информации сетевого трафика;
- возможность читать информацию из записей аудита уполномоченным администраторам;
- возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита;
- возможность оповещения уполномоченных лиц о критичных видах событий безопасности, в том числе сигнализация о попытках нарушения правил межсетевого экранирования;
- возможность выборочного просмотра данных аудита (поиск, сортировка, упорядочение данных аудита);
- возможность регистрации возникновения событий, которые в соответствии с национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК 15408-2-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности» включены в базовый уровень аудита;
- возможность идентификации администратора МЭ до разрешения любого действия (по администрированию), выполняемого при посредничестве МЭ от имени этого администратора;
- возможность аутентификации администратора МЭ до разрешения любого действия (по администрированию), выполняемого при посредничестве МЭ от имени этого администратора;
- возможность осуществления идентификации субъектов межсетевого взаимодействия до передачи МЭ информационного потока получателю;
- поддержка определенных ролей по управлению МЭ;
- возможность со стороны администраторов управлять режимом выполнения функций безопасности МЭ;
- возможность со стороны администраторов управлять данными МЭ, используемыми функциями безопасности МЭ;
- возможность со стороны администраторов управлять атрибутами безопасности;
- возможность поддержки списка типов сетевого трафика для осуществления посредничества в передаче, предусматривающего разделение трафика по типам;

- обеспечение ассоциации типов сетевого трафика из списка с конкретным сетевым трафиком для осуществления посредничества в передаче и обработки соответствующих типов сетевого трафика прокси- агентами;
- возможность изменения области значений информации состояния соединения со стороны администраторов МЭ;
- возможность присвоения информации состояния соединения допустимых значений, таких как установление соединения, использование соединения, завершение соединения и других;
- возможность ведения для каждого соединения таблицы состояний, основанной на информации состояния соединения;
- предоставление возможности администраторам МЭ модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для используемых пользователями отдельных команд для осуществления МЭ фильтрации;
- предоставление возможности администраторам МЭ модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности использования сетевых ресурсов, содержащих отдельные типы мобильного кода, для осуществления МЭ фильтрации;
- возможность обеспечения надежных меток времени при проведении аудита безопасности;
- возможность тестирования (самотестирования) функций безопасности МЭ (контроль целостности исполняемого кода МЭ);
- возможность сохранения штатного функционирования МЭ при некритичных типах сбоев;
- возможность согласованно интерпретировать управляющие команды, атрибуты сетевого трафика и иные данные, получаемые от взаимодействующих с МЭ средств защиты информации других видов;
- поддержка правил интерпретации данных, получаемых от взаимодействующих с МЭ средств защиты информации других видов;
- возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования;
- возможность кластеризации МЭ;
- возможность приоритизации контроля и фильтрации разных информационных потоков, а также выделения ресурсов, доступных для разных информационных потоков, обрабатываемых одновременно (в течение определенного периода времени).

3.3 Управление «Программно-аппаратным комплексом С-Терра Шлюз. Версия 4.2» производится администратором безопасности удаленно с использованием «Программного продукта С-Терра КП. Версия 4.2» или локально.

3.4 «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» включает:

- программное обеспечение «Программный комплекс С-Терра Шлюз. Версия 4.2»;
- программное обеспечение «Программный продукт С-Терра КП. Версия 4.2»;
- аппаратную платформу.

«Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» предназначен для работы на аппаратных платформах в архитектуре Intel (x86-64 совместимых) универсального назначения, а именно:

- платформах LN-S, LN-M, LN-L, LN-XL на базе материнских плат Lanner;
- маршрутизаторах ESR-100-ST, ESR-200-ST, ESR-1000-ST, разработанных и производимых ООО «Предприятие «ЭЛТЕКС».

3.5 ПАК «С-Терра Шлюз» работает под управлением операционной системы Debian GNU/Linux 7 с установленными последними обновлениями безопасности. Сервер управления из «Программного продукта С-Терра КП» функционирует под управлением ОС Windows Server 2008 SP2 (32-bit, 64-bit), Windows Server 2008R2 SP1 (64-bit), Windows Server 2012 (64-bit), Windows Server 2012R2 (64-bit), Windows Server 2016 (64-bit), обновленных в соответствии с Приложением 2 к Формуляру. Для функционирования Сервера управления необходимо также наличие следующих компонентов среды функционирования:

- Microsoft Visual C++ 2008 Redistributable – 10.0.40219;
- Microsoft Visual C++ 2010 Redistributable – 9.0.30729;
- FileZilla Server 0.9.54;
- PostgreSQL Server 9.2.24-1;
- Java JRE 8 Update 151;
- Apache Tomcat Server 7.0.82;
- OpenSSL 1.1.0.

Примечание. Порядок и сроки эксплуатации операционных систем, в среде которых функционирует ПАК, определяются производителями операционных систем.

3.6 «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» использует внешние криптографические библиотеки СКЗИ «КриптоПро CSP 4.0», разработанного компанией «Крипто-Про», или СКЗИ, разработанного компанией «С-Терра СиЭсПи», и сертифицированные ФСБ России.

3.7 ПО «Программно-аппаратного комплекса С-Терра Шлюз. Версия 4.2» поставляется в виде дистрибутива на отдельном CD-диске либо предустановленным на аппаратную платформу».

3.8 «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» применяется для защиты от несанкционированного доступа к информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в государственных информационных системах до 1 класса защищенности включительно, в том числе обеспечивающих 1, 2, 3 и 4 уровни защищенности персональных данных.

4 КОМПЛЕКТНОСТЬ

4.1 «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» поставляется в следующем виде:

1) аппаратная платформа (LN-S, LN-M, LN-L, LN-XL на базе материнских плат Lanper; ESR-100-ST, ESR-200-ST, ESR-1000-ST, производимых ООО «Предприятие «ЭЛТЕКС»);

2) ПО «Программно-аппаратного комплекса С-Терра Шлюз. Версия 4.2» поставляется в виде дистрибутива на одном из CD-дисков, указанных в Таблице 2, либо предустановленным на аппаратную платформу;

3) CD диск с документацией, указанный в Таблице 3;

4) CD-диск «S-Terra Disk Image» с образом жесткого диска и Приложением к Инструкции по восстановлению ПАК;

5) диск «S-Terra Recovery CD/DVD» с ПО для восстановления образа диска и Инструкцией по восстановлению ПАК (кроме ПО «С-Терра Шлюз ESR ST»);

6) документация в печатном виде, перечисленная в разделе 4.4.

4.2 Состав CD-дисков с дистрибутивами указан в Таблице 2

Таблица 2

Наименование	Размещение на CD-диске
CD-диск «С-Терра Шлюз¹ ST² KC1, KC2. Версия 4.2. Релиз 18201»	
<u>Программные средства</u>	
С-Терра Шлюз ST KC1, KC2. Дистрибутив	Каталоги STerra_Gate_ST_KC1_KC2, STerra_SmartFW
С-Терра КП. Дистрибутив	Каталог STerra_KP
stverify	
CD-диск «С-Терра Шлюз ST KC3. Версия 4.2. Релиз 18201»	
<u>Программные средства</u>	
С-Терра Шлюз ST KC3. Дистрибутив	Каталоги STerra_Gate_ST_KC3, STerra_SmartFW

¹ ПО «С-Терра Шлюз. Версия 4.2» устанавливается на аппаратные платформы в архитектуре Intel (x86-64 совместимых) универсального назначения и др.

² ПО «С-Терра Шлюз. Версия 4.2» использует криптографические библиотеки СКЗИ, разработанного компанией С-Терра СиЭсПи, и сертифицированного ФСБ России.

С-Терра КП. Дистрибутив	Каталог STerra_KP
stverify	
CD-диск «С-Терра Шлюз DP³ ST KC1, KC2. Версия 4.2. Релиз 18201»	
<u>Программные средства</u>	
С-Терра Шлюз DP ST KC1, KC2. Дистрибутив	Каталоги STerra_Gate_DP_ST_KC1_KC2, STerra_SmartFW
С-Терра КП. Дистрибутив	Каталог STerra_KP
stverify	
CD-диск «С-Терра Шлюз DP ST KC3. Версия 4.2. Релиз 18201»	
<u>Программные средства</u>	
С-Терра Шлюз DP ST KC3. Дистрибутив	Каталоги STerra_Gate_DP_ST_KC3, STerra_SmartFW
С-Терра КП. Дистрибутив	Каталог STerra_KP
stverify	
CD-диск «С-Терра Шлюз CP⁴ KC1, KC2. Версия 4.2. Релиз 18579»	
<u>Программные средства</u>	
С-Терра Шлюз CP KC1, KC2. Дистрибутив	Каталоги STerra_Gate_CP_KC1_KC2, STerra_SmartFW
С-Терра КП. Дистрибутив	Каталог STerra_KP
stverify	
CD-диск «С-Терра Шлюз CP KC3. Версия 4.2. Релиз 18579»	
<u>Программные средства</u>	
С-Терра Шлюз CP KC3. Дистрибутив	Каталоги STerra_Gate_CP_KC3, STerra_SmartFW
С-Терра КП. Дистрибутив	Каталог STerra_KP
stverify	
CD-диск «С-Терра Шлюз ESR⁵ ST KC2. Версия 4.2. Релиз 18095»	
<u>Программные средства</u>	

³ ПО «С-Терра Шлюз. Версия 4.2» устанавливается на аппаратные платформы в архитектуре Intel (x86-64 совместимых) универсального назначения, оснащенных сетевыми интерфейсами, поддерживающими технологию DPDK прямого доступа к сетевым пакетам, минуя сетевой стек ОС.

⁴ ПО «С-Терра Шлюз. Версия 4.2» использует криптографические библиотеки СКЗИ «КриптоПро CSP 4.0», разработанного компанией «Крипто-Про».

⁵ ПО «С-Терра Шлюз. Версия 4.2» устанавливается на маршрутизаторы ESR-100-ST, ESR-200-ST или ESR-1000-ST.

С-Терра Шлюз ESR ST KC2. Дистрибутив	Каталоги STerra_Gate_ESR_ST_KC2, STerra_SmartFW
С-Терра КП. Дистрибутив	Каталог STerra_KP
stverify	
CD-диск «С-Терра Шлюз ESR ST KC3. Версия 4.2. Релиз 18095»	
<u>Программные средства</u>	
С-Терра Шлюз ESR ST KC3. Дистрибутив	Каталоги STerra_Gate_ESR_ST_KC3, STerra_SmartFW
С-Терра КП. Дистрибутив	Каталог STerra_KP
stverify	

4.3 Состав CD-диска с документацией указан в Таблице 3.

Таблица 3

CD-диск «Документация на продукты С-Терра. Версия 4.2»	
<u>Документация</u>	
«Программный продукт С-Терра КП. Версия 4.2». Руководство администратора. РЛКЕ.00020-03 90 01	Каталог STerra_KP
«Программный комплекс С-Терра Шлюз. Версия 4.2» Руководство администратора. РЛКЕ.00017-01 90 01	Каталог STerra_Gate
«Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00019-01 30 01	Каталог Formular_Rules
«Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2». Правила пользования.	
Копия сертификата соответствия ФСТЭК России на «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2»	Каталог Certificates

4.4 В комплект поставки в печатном виде входят:

- Лицензия на использование «Программно-аппаратного комплекса С-Терра Шлюз. Версия 4.2»;
- Лицензия на использование программного продукта КриптоПро CSP Driver версии 3.9/4.0 (при использовании КриптоПро CSP);
- Копия сертификата соответствия ФСТЭК России на «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2»;
- Знак соответствия ФСТЭК России;

- Формуляр (ФСТЭК России) на «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2».

5 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

5.1 Гарантийные обязательства предприятия-изготовителя (поставщика) изложены в «Лицензионном Соглашении о праве пользования «Программно-аппаратным комплексом С-Терра Шлюз. Версия 4.2» производства ООО «С-Терра СиЭсПи».

5.2 Согласно Лицензионному Соглашению, Конечному Пользователю предоставляются ограниченные гарантии, состоящие в том, что:

5.2.1 Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки ПАК «С-Терра Шлюз» дефекты в составе информационных носителей или некомплектность ПАК «С-Терра Шлюз», то информационные носители будут заменены, а комплектность ПАК «С-Терра Шлюз» восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности изделия и/или дефектам носителей информации рассматриваться не будут.

5.3 Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию ПАК «С-Терра Шлюз» любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации ПАК «С-Терра Шлюз» и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

5.4 На аппаратные платформы в обязательном порядке предоставляются гарантии производителя. Срок действия гарантийных обязательств и адрес точки предоставления гарантийного обслуживания указаны в документации, сопровождающей аппаратную платформу. При этом состав и условия предоставления сервиса гарантийного обслуживания аппаратных платформ определяются производителем аппаратных платформ.

6. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

6.1 Изделие «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2»

РЛКЕ.00019-01

обозначение изделия

серийный номер изделия

упаковано согласно требованиям, предусмотренным в действующей технической документации.

6.2 Маркировано знаком соответствия системы сертификации средств защиты информации по требованиям безопасности информации: №РОСС RU.0001.01БИ00 № _____.

Место
нанесения
знака соответствия

должность

подпись

расшифровка подписи

число, месяц, год

М.П.

7 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

7.1 Изделие «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2»

РЛКЕ.00019-01

обозначение изделия

серийный номер изделия

принято в соответствии с обязательными требованиями национальных стандартов,
действующей технической документацией и признано годным для эксплуатации.

должность

подпись

расшифровка подписи

число, месяц, год

М.П.

9 СВЕДЕНИЯ О ХРАНЕНИИ

9.1 В процессе эксплуатации CD диски с дистрибутивным программным обеспечением и эксплуатационными документами хранятся в вертикальном положении на предназначенном для этой цели стеллаже в упаковке, поставленной изготовителем, при температуре окружающего воздуха от от плюс 5°C до плюс 35°C, относительной влажности воздуха не более 65 %.

9.2 В помещении для хранения не должно быть агрессивных примесей (паров кислот, щелочей), конденсата.

9.3 При хранении не допускаются резкие изменения температуры окружающего воздуха (более 20°C/ч) и воздействия внешних магнитных полей напряженностью более 4000А/м.

9.4 Организация, эксплуатирующая изделие несет ответственность за его несанкционированное размножение.

10 СВЕДЕНИЯ ОБ УСТАНОВКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

10.1 Установка изделия «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» осуществляется потребителем самостоятельно или предприятием-поставщиком (изготовителем) согласно договору на поставку.

11 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

11.1 «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2» соответствует требованиям по безопасности информации при выполнении следующих условий эксплуатации:

- регламентация запрета на использование ПАК «С-Терра Шлюз» для обработки сведений, составляющих государственную тайну;
- должна быть обеспечена поставка, установка, управление и функционирование ПАК «С-Терра Шлюз» безопасным образом и в соответствии с поставляемыми руководствами;
- должна быть обеспечена защита компьютера с установленным ПАК «С-Терра Шлюз», сетевого и кроссового оборудования, системы электропитания от несанкционированного физического воздействия, и доступность их только для обслуживающего персонала;
- администраторы ПАК «С-Терра Шлюз» должны пройти проверку на благонадежность и компетентность, а также действовать согласно правилам и процедурам, установленным в эксплуатационной документации;
- периодически должен выполняться регламентный контроль целостности ПАК «С-Терра Шлюз» с использованием утилиты `csrvpn_verify` компании «С-Терра СиЭсПи», а также при восстановлении после сбоев/отказов программного обеспечения и/или оборудования;
- должен быть обеспечен доверенный маршрут между ПАК «С-Терра Шлюз» и удаленным рабочим местом администратора, управляемые данные должны передаваться по защищенному соединению;
- должен обеспечиваться доверенный канал передачи данных между защищаемой информационной системой и ПАК «С-Терра Шлюз», а также между ПАК «С-Терра Шлюз» и Сервером управления, с которого выполняется управление им;
- должно обеспечиваться исключение каналов связи защищаемой информационной системы с иными информационными системами в обход ПАК «С-Терра Шлюз»;
- должно обеспечиваться взаимодействие ПАК «С-Терра Шлюз» с сертифицированными на соответствие требованиям безопасности информации по соответствующему классу защиты средствами защиты информации (системами обнаружения вторжений и другими), от которых ПАК «С-Терра Шлюз» получает управляющие сигналы;

- должна быть обеспечена поддержка средств аудита, используемых в ПАК «С-Терра Шлюз»;
- должен быть исключен или (если невозможно) ограничен доступ к ПАК «С-Терра Шлюз» по сетевому протоколу SSH:
 - запретить использование протокола SSHv1;
 - изменить по возможности используемый по умолчанию порт подключения;
 - разрешить доступ по протоколу SSH только через сетевой интерфейс, выделенный для администрирования;
 - разрешить доступ по протоколу SSH только с определенных IP-адресов;
 - отключить возможность авторизации под суперпользователем.
- при выпуске разработчиком обновления (патча) для устранения выявленных недостатков, уязвимостей и ошибок:
 - конечный пользователь должен загрузить обновление (патч) с FTP-сервера, должен проверить целостность полученного обновления (патча) (контрольную сумму) и согласно прилагаемой инструкции должен установить обновление (патч) на ПАК «С-Терра Шлюз»;
 - перед установкой обновления (патча) на ПАК «С-Терра Шлюз» по возможности необходимо провести тестирование с использованием тестового стенда, описанного в документе «Технические условия», на котором следует установить обновление (патч) и выполнить несколько тестов на проверку правил фильтрации;
 - после успешного тестирования обновления (патча) установить его на ПАК «С-Терра Шлюз» согласно приложенной к обновлению (патчу) инструкции. Для контроля установки обновления (патча) конечный пользователь должен проверить контроль целостности ПАК «С-Терра Шлюз», доступность интерфейсов для управления. Для верификации применения обновления (патча) по возможности необходимо выполнить тесты из документа «Технические условия».

11.2 Для платформ, для которых это применимо, необходимо в обязательном порядке загрузить с официального сайта компании-разработчика и применить обновление, нейтрализующее уязвимость BDU:2017-02217 (сведения о появлении указанного обновления будут размещены в банке данных угроз безопасности информации в поле «Информация об устранении» уязвимости BDU:2017-02217).

До применения указанного обновления необходимо принять следующие основные меры, направленные на исключение возможности эксплуатации уязвимости BDU:2017-02217:

- обеспечить защиту от несанкционированного физического доступа к аппаратным компонентам средств вычислительной техники;
- исключить каналы связи, обеспечивающие доступ в обход заданных правил управления доступом к средствам вычислительной техники (их программному обеспечению и настройкам), а также правил контроля и фильтрации информационных потоков;
- произвести отключение механизма удаленного управления средствами вычислительной техники Intel Active Management Technology (Intel AMT) путём применения соответствующих настроек базовой системы ввода-вывода;
- обеспечить защиту настроек базовой системы ввода-вывода от несанкционированного доступа путем применения пароля;
- обеспечить защиту от несанкционированного использования USB-портов средств вычислительной техники (в том числе при помощи их опечатывания, а также отключения путем применения соответствующих настроек базовой системы ввода-вывода);
- обеспечить ограничение установки (инсталляции) и исполнения в операционной системе программ в части установления возможности установки (инсталляции) и исполнения только программного обеспечения и (или) его компонентов в соответствии с разрешительными атрибутами безопасности.

11.3 Устранение уязвимостей типа Meltdown и Spectre должно выполняться в соответствии с рекомендациями разработчиков используемого программного обеспечения (применение патча при его наличии, применение мер в соответствии с рекомендациями разработчика).

