СОГЛАСОВАНО

Начальник 2 управления

ФСТЭК России

_____ Д.Н. Шевцов

«17» декабря 2018 года

УТВЕРЖДАЮ

Генеральный директор

ООО «С-Терра СиЭсПи»

_____ С.В.Мещеряков

«___» _____ 2017 года

Программный комплекс

С-Терра Клиент

Версия 4.2

Формуляр

ЛИСТ УТВЕРЖДЕНИЯ

РЛКЕ.00018-01 30 01-ЛУ
Листов 1

2017

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

ООО "С-Терра СиЭсПи"

УТВЕРЖДЕН

РЛКЕ.00018-01 30 01-ЛУ

Программный комплекс

С-Терра Клиент

Версия 4.2

Формуляр

РЛКЕ.00018-01 30 01
Листов 26

2017

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

СОДЕРЖАНИЕ

1 Общие указания

1.1 Формуляр на изделие «Программный комплекс С-Терра Клиент. 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: «Программный комплекс С-Терра Клиент. Версия 4.2».

Краткое наименование изделия: ПК «С-Терра Клиент», ПК.

Условное обозначение: РЛКЕ.00018-01.

2.2 Правообладатель

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

ПК «С-Терра Клиент». Версия 4.2. Релиз 18579.

2.5 Сведения о сертификации

ПК «С-Терра Клиент» сертифицирован в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 и соответствует документам «Требованиям к межсетевым экранам», утвержденным приказом ФСТЭК России от 9 февраля 2016 г. № 9 и «Профиль защиты межсетевых экранов типа «В» 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 межсетевого экрана» и AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность межсетевого 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 Клиент ST КС1, КС2. Версия 4.2. Релиз 18579»		
STerra_Client_ST_KC1_KC2 STerra_Client_ST_KC1_KC2.zip	467C6F3B86E0955B7882CF7264F32CC4 2E2B6744D0196DE98BE97F3B697C6CF1	64c7f6b3680e59b58728fc27463fc24c e2b276440d91d69eb89ef7b396c7c61f
smartfw-win.zip	97E66CB7A3E2049AB743271956AA2732 93A9069053E27E0010139AF7F1262E42	796ec67b3a2e40a97b34729165aa7223 399a6009352ee7000131a97f1f62e224
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE 9AF8224C9CBE758F363AA418A03F8A8E	070daee08f1785d14379d05330989cec a98f22c4c9eb57f863a34a810af3a8e8
CD диск «С-Терра Клиент CP КС1, КС2. Версия 4.2. Релиз 18579»		
STerra_Client_CP_KC1_KC2 STerra_Client_CP_KC1_KC2.zip	A2B3662592F0B52942DF9536E8DD3D64 DB12E6EAC942BE18F9B3728D226FF670	2a3b6652290f5b9224fd59638eddd346 bd216eae9c24eb819f3b27d822f66f07
smartfw-win.zip	97E66CB7A3E2049AB743271956AA2732 93A9069053E27E0010139AF7F1262E42	796ec67b3a2e40a97b34729165aa7223 399a6009352ee7000131a97f1f62e224
STerra_KP STerra_KP.zip	70D0EA0EF871581D34970D350389C9CE 9AF8224C9CBE758F363AA418A03F8A8E	070daee08f1785d14379d05330989cec a98f22c4c9eb57f863a34a810af3a8e8

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

Является программным средством защиты индивидуального рабочего места (пользователя) от несанкционированного доступа.

3.2 «Программный комплекс С-Терра Клиент. Версия 4.2» обеспечивает:

- возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации и всех операций перемещения контролируемой ПК информации к узлам информационной системы и от них;
- возможность обеспечить, чтобы в ПК на все операции перемещения через ПК информации к узлам информационной системы и от них распространялась фильтрация;
- возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности субъектов: сетевой адрес узла отправителя; сетевой адрес узла получателя;
- возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности информации: сетевой протокол, который используется для взаимодействия; транспортный протокол, который используется для взаимодействия, порты источника и получателя в рамках сеанса (сессии); разрешенные (запрещенные) команды, разрешенный (запрещенный) мобильный код; разрешенные (запрещенные) протоколы прикладного уровня;
- возможность явно разрешать информационный поток, базируясь на устанавливаемых администратором ПК наборе правил фильтрации, основанном на идентифицированных атрибутах;
- возможность явно запрещать информационный поток, базируясь на устанавливаемых администратором ПК наборе правил фильтрации, основанном на идентифицированных атрибутах;
- возможность осуществлять политику фильтрации пакетов с учетом управляющих команд от взаимодействующих с ПК 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 сетевых ресурсов, содержащих мобильный код, для которого администратором ПК установлены разрешительные или запретительные атрибуты безопасности;
- 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 ПК 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 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 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 ПК до разрешения любого действия, выполняемого при посредничестве ПК от имени этого администратора;
- возможность аутентификации администратора ПК до разрешения любого действия, выполняемого при посредничестве ПК от имени этого администратора;
- поддержка определенных ролей по управлению ПК;
- возможность со стороны администраторов ПК управлять режимом выполнения функций безопасности ПК;
- возможность со стороны администраторов ПК управлять данными МЭ, используемыми функциями безопасности ПК;
- возможность со стороны администраторов ПК управлять атрибутами безопасности;
- возможность ведения для каждого типа мест расположения узла с установленным ПК отдельных профилей проверок;
- предоставление возможности администраторам ПК изменения области значений профилей проверок;
- возможность присвоения профилям проверок допустимых значений, таких как профиль проверок для использования внутри информационной системы, профиль проверок для использования за пределами информационной системы и других допустимых профилей проверок;
- возможность изменения области значений информации состояния соединения со стороны администраторов ПК;
- 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 ПК назначать, модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности для прикладного программного обеспечения (приложений) с целью последующего осуществления фильтрации;
- предоставление возможности администраторам ПК модифицировать, удалять разрешительные и (или) запретительные атрибуты безопасности использования сете-

вых ресурсов, содержащих отдельные типы мобильного кода, для осуществления ПК фильтрации;

- возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата ПК к штатному режиму функционирования;
- возможность тестирования (самотестирования) функций безопасности ПК (контроль целостности исполняемого кода ПК);
- возможность согласованно интерпретировать управляющие команды, атрибуты сетевого трафика и иные данные, получаемые от взаимодействующих с ПК средств защиты информации других видов;
- поддержка правил интерпретации данных, получаемых от взаимодействующих с ПК средств защиты информации других видов;
- возможность осуществлять выдачу предупреждающих сообщений пользователю ПК при обнаружении возможного нарушения безопасности.

3.3 Управление «Программным комплексом С-Терра Клиент. Версия 4.2» производится администратором безопасности с использованием «Программного продукта С-Терра КП. Версия 4.2».

3.4 «Программный комплекс С-Терра Клиент. Версия 4.2» функционирует на аппаратной платформе Intel (x86/x86-64 совместимых) под управлением операционных систем Windows 7 Home Premium Russian (32-bit,64-bit), Windows 8 Home Premium Russian (32-bit,64-bit), Windows 8.1 Home Premium Russian (32-bit,64-bit), Windows 10 Russian (32-bit,64-bit), 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 ПК, определяются производителями операционных систем.

3.5 ПК «С-Терра Клиент» (КС1) может функционировать в виртуальных средах, обновленных в соответствии с Приложением 2 к Формуляру:

- VMWare vSphere ESXi/ESX, 5.5, 6.0, 6.5;
- VMWare Workstation 12.5.8, 14;
- KVM: libvirt 2.x, 3.x; qemu/qemu-kvm 2.11.0-rc2 и выше;
- Hyper-V Windows Server 2012R2, 2016;
- XenServer 6.5, 7.0, 7.1, 7.2;
- Huawei Fusion V100R006C00, V100R006C10;
- Parallels Virtuozzo 6.0, 7.0;
- VirtualBox 5.2.

3.6 Обновления изделия осуществляются согласно условиям договора о поставке и технического сопровождения.

3.7 «Программный комплекс С-Терра Клиент. Версия 4.2» поставляется в виде дистрибутивов на отдельном CD диске.

3.8 «Программный комплекс С-Терра Клиент. Версия 4.2» может использоваться 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 «Программный комплекс С-Терра Клиент. Версия 4.2» поставляется в следующем виде:

1) один из CD-дисков с дистрибутивами, указанных в таблице 2;

2) CD-диск с документацией, представленный в таблице 3;

3) 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 Клиент ST[1]. Версия 4.2. Релиз 18579	
Программные средства	
С-Терра Клиент ST. Версия 4.2. Дистрибутив	Каталог STerra_Client_ST_KC1_KC2
С-Терра КП. Версия 4.2. Дистрибутив	Каталог STerra_KP
stverify	
CD диск «С-Терра Клиент CP[2]. Версия 4.2. Релиз 18579»	
Программные средства	
С-Терра Клиент CP. Версия 4.2. Дистрибутив	Каталог STerra_Client_CP_KC1_KC2
С-Терра КП. Версия 4.2. 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»	
Документация	
«Программный комплекс С-Терра Клиент. Версия 4.2» Руководство администратора. РЛКЕ.00018-01 90 03	Каталог STerra_Client
«Программный комплекс С-Терра Клиент. Версия 4.2». Руководство пользователя. РЛКЕ.00018-01 90 04	

[1] ПК «С-Терра Клиент. Версия 4.2» использует криптографические библиотеки СКЗИ, разработанного компанией С-Терра СиЭсПи», и сертифицированного ФСБ России.

[2] ПК «С-Терра Клиент. Версия 4.2» использует криптографические библиотеки СКЗИ «КриптоПро CSP 3.9/4.0», разработанного компанией «Крипто-Про».

«Программный продукт С-Терра КП. Версия 4.2». Руководство администратора. РЛКЕ.00020-01 90 01	Каталог STerra_KP
«Программно-аппаратный комплекс «С-Терра VPN», исполнения 1-1, 1-3. Версия 4.2». Правила пользования. РЛКЕ.00016-01 90 02.03	Каталог Formular_Rules
«Программный комплекс С-Терра Клиент. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00018-01 30 01	
«Программно-аппаратный комплекс «С-Терра VPN», исполнения 1-1, 1-3. Версия 4.2». Формуляр (ФСБ России). РЛКЕ.00016-01 30 03	
Копия сертификата соответствия ФСТЭК России на «Программный комплекс С-Терра Клиент. Версия 4.2»	Каталог Certificates
Копия сертификата соответствия ФСБ России на «Программно-аппаратный комплекс «С-Терра VPN», исполнения 1-1, 1-3. Версия 4.2».	

4.4 В комплект поставки в печатном виде входят:

- «Программный комплекс С-Терра Клиент. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00018-01 30 01;
- копия сертификата соответствия ФСТЭК России на «Программный комплекс С-Терра Клиент. Версия 4.2»;
- копия сертификата соответствия ФСБ России на «Программно-аппаратный комплекс «С-Терра VPN», исполнения 1-1, 1-3. Версия 4.2 (Сертификаты соответствия)»;
- лицензия на право использования «Программного комплекса С-Терра Клиент. Версия 4.2»;
- лицензия на право использования программного продукта КриптоПро CSP Driver версии 3.9/4.0 (для использования совместно с С-Терра КП при условии покупки).

5 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

5.1 Гарантийные обязательства предприятия-изготовителя (поставщика) изложены в «Лицензионном Соглашении о праве пользования «Программным комплексом С-Терра Клиент. 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 В случае, если в ходе эксплуатации Программного комплекса Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель (ООО «С-Терра СиЭсПи») обеспечивает:

а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения;

б) бесплатное предоставление обновлений программного обеспечения Производителя Программного комплекса, в которых устранены Критичные Проблемы.

Примечание 1. Гарантийное обязательство 5.2.1 базируется на следующем определении: Критичная Проблема заключается в том, что Программный комплекс, вследствие ошибки в программном обеспечении, не выполняет основные функции безопасности, а именно - шифрование трафика и контроль доступа, что приводит к нарушению безопасности сети Конечного Пользователя.

Примечание 2. Обновления программного обеспечения в соответствии с гарантийным обязательством п.5.2.1б) предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

5.2.2 Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки «Программного комплекса С-Терра Клиент. Версия 4.2» дефекты в составе информационных носителей или некомплектность Программного комплекса, то информационные носители будут заменены, а комплектность Программного комплекса восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности Программного комплекса и/или дефектам носителей информации рассматриваться не будут.

5.3 Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Программного комплекса любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Программного комплекса и его компонент в установленном поряд-

ке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

6 СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

Программный комплекс С-Терра Клиент. Версия 4.2
наименование программного изделия

РЛКЕ.00018-01 _____
обозначение серийный номер

упакован ООО "С-Терра СиЭсПи"
наименование или код предприятия (организации)

согласно требованиям, предусмотренным ТУ 62.01.29-018-70221576-2017
номер технических условий или стандарта

Маркирован знаком соответствия Системы сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 № _____

Место для нанесения знака соответствия

Дата упаковки «____» _____ 20____ г.

Упаковку произвел _____ _____
подпись расшифровка подписи

Изделие после упаковки принял

_____ _____ _____
должность подпись расшифровка подписи

М.П.

7 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Программный комплекс С-Терра Клиент. Версия 4.2
наименование программного изделия

РЛКЕ.00018-01 _____
обозначение серийный номер

соответствует техническим условиям ТУ 62.01.29-018-70221576-2017
номер технических условий или стандарта

и эталону комплекса, хранящемуся в ООО "С-Терра СиЭсПи", и признан годным для эксплуатации.

Дата выпуска «____» _____ 20____ г.

М.П. Генеральный директор ООО "С-Терра СиЭсПи"

_____ _____
подпись расшифровка подписи

8 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

8.1 Рекламации предъявляются предприятию-поставщику (изготовителю) в письменном виде с указанием даты обнаружения неисправности, содержания и подробного описания условий возникновения неисправности.

8.2 Рекламация подписывается руководителем подразделения, принимающего или эксплуатирующего программное обеспечение.

8.3 Поступающие к поставщику (изготовителю) рекламации регистрируются в журнале учета рекламаций (таблица 4).

Таблица 4

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

9 СВЕДЕНИЯ О ХРАНЕНИИ

9.1 В процессе эксплуатации CD диск с дистрибутивным программным обеспечением и эксплуатационными документами хранится в вертикальном положении на предназначенном для этой цели стеллаже в упаковке, поставленной изготовителем, при температуре окружающего воздуха от от плюс 5^{o}С до плюс 35^{o}С, 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^{o}С/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 осуществляется потребителем самостоятельно или предприятием-поставщиком (изготовителем) согласно договору на поставку.

11 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

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

- регламентация запрета на использование ПК «С-Терра Клиент» для обработки сведений, составляющих государственную тайну;
- должна быть обеспечена поставка, установка, управление и функционирование ПК «С-Терра Клиент» безопасным образом и в соответствии с эксплуатационной документацией;
- должна быть обеспечена физическая защита компьютера с установленным ПК «С-Терра Клиент» от несанкционированного физического воздействия;
- администраторы и пользователи ПК «С-Терра Клиент» должны пройти проверку на благонадежность и компетентность, а также действовать согласно правилам и процедурам, установленным в документации;
- возможность доступа к ПК «С-Терра Клиент» с целью администрирования должна предоставляться только уполномоченному на это администратору;
- идентификация и аутентификация администратора при доступе к управлению ПК «С-Терра Клиент» должна осуществляться продуктом С-Терра КП;
- идентификация и аутентификация пользователя при доступе к ПК «С-Терра Клиент» должна осуществляться средствами ПК «С-Терра Клиент»;
- должна быть обеспечена поддержка средств аудита, используемых в ПК «С-Терра Клиент», и предоставление для них источника меток времени;
- должны быть обеспечены тестирование и контроль целостности аппаратных средств, а также программного обеспечения базовой системы ввода-вывода, загрузчика и операционной системы или средства вычислительной техники, на котором функционирует ПК «С-Терра Клиент». Периодически должен выполняться регламентный контроль целостности ПК «С-Терра Клиент» с использованием утилиты cspvpn_verify компании С-Терра СиЭсПи, а также при восстановлении после сбоев/отказов программного обеспечения;
- должна быть исключена возможность использования не прошедших сертификацию компонентов программно-технического средства, в которое интегрирован ПК «С-Терра Клиент» с иными видами средств защиты информации, при его эксплуатации;
- должно быть обеспечено функционирование ПК «С-Терра Клиент» в среде, сертифицированной на соответствие требованиям безопасности информации по соответ-

ствующему классу защиты операционной системы, или в среде, защищенной путем принятия мер защиты информации, соответствующих классу защищенности информационной системы (автоматизированной системы управления), для использования в которой предназначается ПК «С-Терра Клиент»;

- должно обеспечиваться взаимодействие ПК «С-Терра Клиент» с сертифицированными на соответствие требованиям безопасности информации по соответствующему классу защиты средствами защиты информации (системами обнаружения вторжений, средствами антивирусной защиты и другими), от которых ПК «С-Терра Клиент» получает управляющие сигналы;
- для правильного функционирования ПК «С-Терра Клиент» должны использоваться только сертифицированные криптографические библиотеки;
- 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 ПК «С-Терра Клиент»;
  - перед установкой обновления (патча) на ПК «С-Терра Клиент» 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 ПК «С-Терра Клиент» согласно приложенной к обновлению (патчу) инструкции. Для контроля установки обновления (патча) конечный пользователь должен проверить контроль целостности ПК «С-Терра Клиент», доступность интерфейсов для управления. Для верификации применения обновления (патча) по возможности необходимо выполнить тесты из документа «Технические условия».

11.2 Устранение уязвимостей при эксплуатации ПК «С-Терра Клиент»:

- Администратор безопасности должен выполнять ежемесячный поиск актуальных уязвимостей и сведений об уязвимостях изделия, анализ идентифицированных уязвимостей на предмет возможности их использования для нарушения безопасности;
- В случае обнаружения уязвимостей, должно производиться их устранение в соответствие с приведенными ниже методами и процедурами.

- Процедура устранения уязвимостей ПК «С-Терра Клиент» должна обеспечивать возможность обновления программного обеспечения для устранения актуальных уязвимостей, имеющих критический характер для функционирования ПК «С-Терра Клиент». Устранение уязвимостей должно производиться заявителем (изготовителем) СЗИ с использованием организационно-технических процедур, представленных ниже.
- Изготовитель должен периодически, не реже одного раза в месяц, проводить поиск известных (подтвержденных) уязвимостей в общедоступных источниках информации об уязвимостях. В качестве общедоступных источников в первую очередь должны использоваться база данных уязвимостей в составе банка данных угроз безопасности информации ФСТЭК России (www.bdu.fstec.ru), а также следующие дополнительные источники:
  - https://cve.mitre.org/,
  - https://nvd.nist.gov/,
  - https://www.exploit-db.com/,
  - http://www.rapid7.com/db/,
  - http://www.cvedetails.com/,
  - http://www.securitylab.ru/
  - и другие.
- Поиск информации в базах данных по уязвимостям ПК «С-Терра Клиент» проводят с целью проверки соответствия ПК «С-Терра Клиент» требованиям, указанным в технических условиях.
- Изготовитель должен провести анализ выявленных уязвимостей ПК «С-Терра Клиент».
- При анализе уязвимостей необходимо учитывать следующие критерии:
  - тип ошибки;
  - версию программного обеспечения, подверженную уязвимости;
  - уровни опасности уязвимости: критическая (Critical), высокая (High), средняя (Medium), низкая (Low);
  - информацию об устранении.
- В случае выявления информации об уязвимости ПК «С-Терра Клиент» из различных источников и отсутствия информации об этой уязвимости в БДУ (базе данных уязвимостей), изготовитель предоставляет информацию о данной уязвимости в ФСТЭК России для размещения в БДУ.

- При выявлении уязвимостей ПК «С-Терра Клиент», изготовитель не реже одного раза в шесть месяцев должен осуществить следующие мероприятия:
  - получить от разработчика дистрибутив с устраненными уязвимостями;
  - разместить информационное сообщение об уязвимостях ПК «С-Терра Клиент» на специализированном разделе своего сайта;
  - довести информацию до конечных потребителей ПК «С-Терра Клиент» об организационно-технических мерах по устранению уязвимостей ПК «С-Терра Клиент»;
  - изготовитель самостоятельно осуществляет проверку обновленной версии дистрибутива сертифицированными средствами контроля целостности программных комплексов с фиксацией полученной контрольной суммы;
  - изготовитель оповещает пользователей изделия о необходимости установки обновленной версии ПК «С-Терра Клиент»;
  - изготовитель обеспечивает гарантированную доставку конечным пользователям ПК «С-Терра Клиент» файла с обновленной версией ПК «С-Терра Клиент»;
  - конечные пользователи ПК «С-Терра Клиент» обновляют изделие с соответствующими отметками в разделах формуляра;
  - информацию об изменении версии ПК «С-Терра Клиент» заявитель (изготовитель) заносит в извещение об изменениях на СЗИ, и представляет его в Испытательную лабораторию, ФСТЭК России и доводит до сведения конечных потребителей ПК «С-Терра Клиент»;
  - изготовитель обязан провести работы по инспекционному контролю ПК «С-Терра Клиент» в испытательной лаборатории;
  - при положительном проведении инспекционного контроля, изготовитель должен предоставить конечному пользователю ПК «С-Терра Клиент»:
    - гарантированную доставку файла дистрибутива для обновления версии ПК «С-Терра Клиент» конечному потребителю,
    - копию согласованного ФСТЭК Россией извещения об изменениях и копию согласованного измененного формуляра.
  - в случае отсутствия, на момент проверки информации по выявленным уязвимостям ПК «С-Терра Клиент» доступных релизов ПК «С-Терра Клиент» с устраненными уязвимостями, изготовитель должен предоставить на ПК «С-Терра Клиент» перечень (регламент) организационно–технических мероприятий,

направленных на недопущение конечными пользователями попыток эксплуатации выявленной уязвимости злоумышленниками;

- на основе предоставленных материалов разработчика об уязвимости, не имеющей обновления ПО, изготовитель предоставляет конечному пользователю ПК «С-Терра Клиент» инструкцию по проведению организационно–технических мероприятий, направленных на недопущение конечными пользователями попыток эксплуатации выявленной уязвимости злоумышленниками в соответствующем разделе сайта изготовителя;
- в случае невозможности устранения уязвимостей средства защиты информации, в том числе путем применения обновления, изготовитель разрабатывает ограничения по применению средства защиты информации, которые незамедлительно доводит до испытательной лаборатории;
- если в соответствии с заключением испытательной лаборатории ограничение по применению позволит устранить уязвимость, изготовитель незамедлительно и гарантированно с подтверждением доводит его до пользователей;
- изготовитель вносит необходимые изменения в эксплуатационную документацию и направляет её совместно с заключением испытательной лаборатории в ФСТЭК России. Пользователи реализуют указанное ограничение по применению средства защиты информации;
- если пользователь не может реализовать ограничение по применению средства защиты информации он прекращает его применение;
- если уязвимость не устраняется путем установления ограничений по применению, изготовитель незамедлительно и гарантированно, с подтверждением, сообщает об этом всем пользователям и в ФСТЭК России. Пользователи прекращают применение средства защиты информации.

12 КОНТРОЛЬ СОСТОЯНИЯ ИЗДЕЛИЯ И ВЕДЕНИЯ ФОРМУЛЯРА

Дата	Вид контроля	Должность проверяющего	Заключение и оценка проверяющего		Подпись проверяющего	Отметка об устранении замечания и подпись
			по состоянию изделия	по ведению формуляра		

Лист регистрации изменений

Изм	Номера листов (страниц)				Всего листов (страниц) в докум.	№ докум.	Входящий № сопроводитель ного докум. и дата	Подпись	Дата
	Изме нен ных	Заменен ных	новых	аннулиро ванных					