СОГЛАСОВАНО

Начальник 2 управления

ФСТЭК России

_____ Д.Н.Шевцов

«25» декабря 2018 года

УТВЕРЖДАЮ

Генеральный директор

ООО «С-Терра СиЭсПи»

_____ С.В.Мещеряков

« » _____ 2018 года

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

Программный комплекс

С-Терра СОВ

Версия 4.2

Формуляр

ЛИСТ УТВЕРЖДЕНИЯ

РЛКЕ.00021-01 30 01-ЛУ
Листов 23

2018

СОГЛАСОВАНО

Начальник 2 управления

ФСТЭК России

_____ Д.Н. Шевцов

«29» мая 2020 года

УТВЕРЖДАЮ

Директор

ООО «С-Терра СиЭсПи»

_____ С.В.Мещеряков

«09» 09 2019 года

Извещение № РЛКЕ.00021-01.01-2019

об изменении формуляра РЛКЕ.00021-01 30 01

Программный комплекс

С-Терра СОВ

Версия 4.2

2019

ООО "С-Терра СиЭсПи"

УТВЕРЖДЕН

РЛКЕ.00021-01 30 01-ЛУ

Программный комплекс

С-Терра СОВ

Версия 4.2

Формуляр

РЛКЕ.00021-01 30 01
Листов 25

2019

Содержание

1 ОБЩИЕ УКАЗАНИЯ

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

Краткое наименование изделия: ПК «С-Терра СОВ».

Условное обозначение: РЛКЕ.00021-01.

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 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.

2.5 Модификация

ПК «С-Терра СОВ». Версия 4.2. Релиз 18772.

2.6 Сведения о сертификации

ПК «С-Терра СОВ» сертифицирован в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 и соответствует документам - «Требования к системам обнаружения вторжений», утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638; «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» (ФСТЭК России, 2012 г.); «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденные приказом ФСТЭК России от 30 июля 2018 г. № 131 - по 4 (четвертому) уровню доверия.

2.7 Контрольные суммы дистрибутива

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 34.11-94 с использованием ПО ФИКС, версия 2.0.2
CD диск «С-Терра СОВ. Версия 4.2»		
STerra_IDS STerra_IDS.zip	13464AACFD6CBBF722A3AAD9BFF10AC8A04383F4831CD44A5B507B8C0AE7F8B6	ed74e6599728e96eac64b291e44c3c39b666327f6742e9bafd2bc50cbea186d1
STerra_Gate_ST_KC1_KC2 STerra_Gate_ST_KC1_KC2.zip	5CF4C100F111DB63910B532555478EA6019B90CFA38CE3DBD64B475A96F314F9	19b91a30eb995be5361aea7ae091003a5de3d7d270932794bb0592fe0fed25dd

Примечание: Контрольные суммы файлов дистрибутивов подсчитаны по алгоритму ГОСТ Р 34.11-2012 с длиной ключа 256 бит с использованием сертифицированной утилиты stverify, разработанной компанией «С-Терра СиЭсПи».

Контрольные суммы для исполняемых файлов, подсчитанные по алгоритму ГОСТ Р 34.11-2012 с использованием утилиты stverify, приведены в Приложении 1 к Формуляру.

Контрольные суммы для исполняемых файлов, подсчитанные по алгоритму ГОСТ Р 34.11-94 с использованием ПО ФИКС, версия 2.0.2, приведены в Приложении 2 к Формуляру.

3 ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1 «Программный комплекс С-Терра СОВ. Версия 4.2» представляет собой программное средство, предназначенное для выявления инцидентов, которые могут быть классифицированы как компьютерные атаки или несанкционированные вторжения в локальную сеть и информационную среду пользователя/организации.

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

- возможность сбора информации о сетевом трафике;
- возможность выполнения анализа собранных данных СОВ о сетевом трафике в режиме, близком к реальному масштабу времени, и по результатам анализа фиксировать информацию о дате и времени, результате анализа, идентификаторе источника данных, протоколе, используемом для проведения вторжения;
- возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием сигнатурного и эвристических методов;
- возможность выполнения анализа собранных данных с целью обнаружения вторжений с использованием эвристических методов, основанных на методах выявления аномалий сетевого трафика на заданном уровне эвристического анализа;
- возможность обнаружения вторжений на основе анализа служебной информации протоколов сетевого уровня базовой эталонной модели взаимосвязи открытых систем;
- возможность фиксации факта обнаружения вторжений или нарушений безопасности в журналах аудита;
- уведомление администратора СОВ об обнаруженных вторжениях по отношению к контролируемым узлам ИС и нарушениях безопасности с помощью отображения соответствующего сообщения на консоли управления;
- возможность автоматизированного обновления базы решающих правил;
- возможность тестирования (самотестирования) функций безопасности СОВ;
- возможность со стороны уполномоченных администраторов (ролей) управлять режимом выполнения функций безопасности СОВ;
- возможность со стороны уполномоченных администраторов (ролей) управлять данными СОВ;
- поддержка определенных ролей для СОВ и их ассоциации с конкретными администраторами СОВ и пользователями ИС;

- возможность администрирования СОВ;
- возможность генерации записей аудита для событий, потенциально подвергаемых аудиту;
- возможность ассоциации каждого события аудита с идентификатором субъекта, его инициировавшего;
- возможность предоставлять возможность читать информацию из записей аудита;
- ограничение доступа к чтению записей аудита;
- поиск, сортировка, упорядочение данных аудита;
- идентификация и аутентификация пользователей.

3.3 Управление «Программным комплексом С-Терра СОВ. Версия 4.2» производится администратором безопасности локально или удаленно с использованием графического интерфейса управления.

3.4 «Программный комплекс С-Терра СОВ. Версия 4.2» предназначен для работы на вычислительных системах в архитектуре Intel (x86-64 совместимых) универсального назначения.

3.5 ПК «С-Терра СОВ» работает под управлением операционной системы Debian GNU/Linux 7 с установленными последними обновлениями безопасности.

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

3.6 ПК «С-Терра СОВ» может функционировать в виртуальных средах, с установленными последними обновлениями безопасности:

- 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.

3.7 «Программный комплекс С-Терра СОВ. Версия 4.2» поставляется в виде дистрибутива на отдельном CD-диске либо на аппаратной платформе, указанной в п.3.4, в установленном состоянии.

3.8 «Программный комплекс С-Терра СОВ. Версия 4.2» обеспечивает реализацию следующих мер защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах до 1 класса защищенности включительно и соответствующих Приказу ФСТЭК России от 11 февраля 2013 г. №17, Приказу ФСТЭК Рос-

сии от 18.02.2013 №21 и методическому документу «Меры защиты информации в государственных информационных системах», утвержденному ФСТЭК России 11 февраля 2014 г.:

СОВ.1 Обнаружение вторжений

ПК «С-Терра СОВ» обеспечивает обнаружение вторжений, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к ней.

ПК «С-Терра СОВ» представляет собой систему, включающую регистрацию событий безопасности, анализ событий безопасности, распознавание компьютерных атак и базу решающих правил, содержащую информацию о характерных признаках компьютерных атак.

ПК «С-Терра СОВ» обеспечивает обнаружение вторжений на внешней границе информационной системы.

Права по администрированию системой обнаружения вторжений должны предоставляться только уполномоченным пользователям.

Усиление СОВ.1 для 1 и 2 класса

ПК «С-Терра СОВ» предоставляет удаленное администрирование через web-интерфейс.

СОВ.2 Обновление базы решающих правил

Уведомление о наличии обновления базы решающих правил осуществляется по электронной почте с указанием контрольной суммы файла-архива с обновлением.

Доставка обновлений осуществляется по доверенному VPN каналу.

Контроль целостности обновлений базы решающих правил осуществляется с помощью утилиты integr_mgr, входящей в состав ПК «С-Терра СОВ».

Усиление СОВ.2 для 1 класса

1) ПК «С-Терра СОВ» позволяет выполнять автоматическое обновление (по умолчанию 1 раз в сутки) базы решающих правил с централизованного хранилища, настроенным администратором, по протоколам http, ftp, scp;

2) уполномоченным администраторам предоставляется возможность редактирования базы решающих правил (добавление и (или) исключение решающих правил) для предотвращения определенных администратором компьютерных атак и (или) сокращения нагрузки на ПК «С-Терра СОВ», а также минимизации ложных срабатываний;

3) ПК «С-Терра СОВ» регистрирует факт изменения базы решающих правил и измененные данные.

3.9 «Программный комплекс С-Терра СОВ. Версия 4.2» может применяться:

- в значимых объектах критической информационной инфраструктуры (КИИ) до 1 категории включительно;
- в государственных информационных системах (ГИС) до 1 класса защищенности включительно;
- в автоматизированных системах управления производственными и технологическими процессами (АСУТП) до 1 класса защищенности включительно;
- в информационных системах персональных данных (ИСПДн), обеспечивающих 1, 2, 3 и 4 уровни защищенности персональных данных;
- в информационных системах общего пользования (ИСОП) II класса.

4 КОМПЛЕКТНОСТЬ

4.1 «Программный комплекс С-Терра СОВ. Версия 4.2» поставляется в виде дистрибутива на указанных ниже CD-дисках либо в следующем виде:

1) аппаратная платформа с установленным «Программным комплексом С-Терра СОВ. Версия 4.2» и готовым к инициализации;

2) CD-диск с дистрибутивами, указанный в Таблице 2;

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

4) CD-диск «S-Terra Disk Image» - образ жесткого диска и Приложение к Инструкции по восстановлению ПК;

5) диск «S-Terra Recovery CD/DVD» - ПО для восстановления образа диска и Инструкция по восстановлению ПК;

6) документация в печатном виде, перечисленная в разделе 4.6.

4.2 «Программный комплекс С-Терра СОВ. Версия 4.2», функционирующий в виртуальной среде, поставляется в следующем виде:

1) CD-диск с дистрибутивами, указанный в Таблице 2;

2) DVD-диск с образом виртуальной машины в формате OVA или в архиве zip, и документацией, указанный в Таблице 4;

3) документация в печатном виде, перечисленная в разделе 4.6.

4.3 Состав CD диска с дистрибутивами и документацией указан в Таблице 2.

Таблица 2

Наименование	**Кво**	**Размещение на CD-диске**
CD-диск «С-Терра СОВ. Версия 4.2»		
Программные средства		
С-Терра СОВ. Дистрибутив, в том числе БРП	1	Каталог STerra_IDS
С-Терра Шлюз ST. Дистрибутив[1]	1	Каталог STerra_Gate
stverify	1	

В состав дистрибутива ПК «С-Терра СОВ» входит база решающих правил (БРП), которая должна периодически обновляться.

[1] Содержит модуль auth_login и утилиту integr_mgr входящие в состав ПК «С-Терра СОВ».

4.4 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 СОВ. Версия 4.2» Руководство администратора и пользователя. РЛКЕ.00021-01 90 01	Каталог STerra_IDS
«Программный комплекс С-Терра Шлюз. Версия 4.2» Руководство администратора. РЛКЕ.00017-01 90 01	Каталог STerra_Gate
«Программный комплекс С-Терра СОВ. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00021-01 30 01	Каталог Formular_Rules
«Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00019-01 30 01	
«Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2». Формуляр (ФСБ России). РЛКЕ.00016-01 30 02	
«Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2». Правила пользования. РЛКЕ.00016-01 90 02	
Копия сертификата соответствия ФСТЭК России на «Программный комплекс С-Терра СОВ. Версия 4.2»	Каталог Certificates
Копия сертификата соответствия ФСТЭК России на «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2»	
Копия сертификата соответствия ФСБ России на «Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2» (исполнение 3-1: «С-Терра Шлюз ST КС1»)	

4.5 Состав DVD диска для «Программного комплекса С-Терра СОВ. Версия 4.2», функционирующего в виртуальной среде, указан в Таблице 4.

Таблица 4

Наименование	**Размещение на DVD диске**
DVD-диск «С-Терра Виртуальный СОВ. Версия 4.2»	
Программные средства	
Образ виртуальной машины в формате OVA или в архиве zip (в том числе БРП)	Каталог S-Terra_Gate_ST_IDS_KC1
Документация	
«Программный комплекс С-Терра СОВ. Версия 4.2» Руководство администратора и пользователя. РЛКЕ.00021-01 90 01	Каталог Documentation\STerra_IDS
«Программный комплекс С-Терра Шлюз. Версия 4.2» Руководство администратора. РЛКЕ.00017-01 90 01	Каталог Documentation\STerra_Gate

«Программный комплекс С-Терра СОВ. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00021-01 30 01	Каталог Documentation\Formular_Rules
«Программный комплекс С-Терра Шлюз. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00017-01 30 02	
«Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2». Формуляр (ФСБ России). РЛКЕ.00016-01 30 02	
«Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2». Правила пользования. РЛКЕ.00016-01 90 02	
Копия сертификата соответствия ФСТЭК России на «Программный комплекс С-Терра СОВ. Версия 4.2»	Каталог Documentation\Certificates
Копия сертификата соответствия ФСТЭК России на «Программный комплекс С-Терра Шлюз. Версия 4.2»	
Копия сертификата соответствия ФСБ России на «Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2» (исполнение 3-1: «С-Терра Шлюз ST КС1»)	

4.6 В комплект поставки в печатном виде входят:

- Лицензия на право использования «Программного комплекса С-Терра СОВ. Версия 4.2»;
- Лицензия на право использования «Программного комплекса С-Терра Шлюз. Версия 4.2»/«Программно-аппаратного комплекса С-Терра Шлюз. Версия 4.2»;
- Лицензия на право использования базы решающих правил;
- Копия сертификата соответствия ФСТЭК России на «Программный комплекс С-Терра СОВ. Версия 4.2»;
- Копия сертификата соответствия ФСТЭК России на «Программный комплекс С-Терра Шлюз. Версия 4.2»/«Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2»;
- Копия сертификата соответствия ФСБ России на «Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2» (исполнение 3-1: «С-Терра Шлюз ST КС1»).

По запросу пользователя в печатном виде может предоставляться:

- «Программный комплекс С-Терра СОВ. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00021-01 30 01;
- «Программный комплекс С-Терра Шлюз. Версия 4.2». Формуляр (ФСТЭК России) РЛКЕ.00017-01 30 02 или «Программно-аппаратный комплекс С-Терра Шлюз. Версия 4.2». Формуляр (ФСТЭК России) РЛКЕ.00019-01 30 01;
- «Программно-аппаратный комплекс «С-Терра VPN». Версия 4.2». Формуляр (ФСБ России). РЛКЕ.00016-01 30 02.

5 ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

5.1 Гарантийные обязательства предприятия-изготовителя (поставщика) изложены в «Лицензионном Соглашении о праве использования «Программным комплексом С-Терра СОВ. 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 ПК «С-Терра СОВ» дефекты в составе информационных носителей или некомплектность ПК «С-Терра СОВ», то носители будут заменены, а комплектность ПК «С-Терра СОВ» восстановлена. По истечении 90 дней претензии по некомплектности и/или дефектам носителей информации рассматриваться не будут.

5.3 Поставщик гарантирует работоспособность ПК «С-Терра СОВ» при условии его эксплуатации в соответствии с требованиями, изложенными в документации, и отсутствия несанкционированного вмешательства в работу ПК «С-Терра СОВ».

5.3.1 Под несанкционированным вмешательством понимается хотя бы одно из следующих действий, совершенное без согласования в письменной форме с поставщиком:

- любое изменение структуры и/или содержания базы данных, за исключением произведенного исключительно посредством поставляемых программных модулей в соответствии с документацией, или же согласованное в письменной форме с ООО «С-Терра СиЭсПи»;
- изменение выполняемых, настроечных или вспомогательных файлов (или их конфигураций в операционных средах), поставляемых программных модулей, за исключением согласованного в письменной форме с ООО «С-Терра СиЭсПи»;
- изменение конфигурации, а также выполняемых, настроечных или вспомогательных файлов Изделия, за исключением произведенного в соответствии с его документацией, при условии непротиворечия этих изменений эксплуатационной документации или же согласованного в письменной форме с ООО «С-Терра СиЭсПи»;
- модернизация поставляемой операционной системы, включая установку штатных обновлений;
- добавление/отключение отдельных сервисов операционной системы (по отношению к состоянию операционной системы на момент передачи экземпляра ПК «С-Терра СОВ»);
- установка дополнительных приложений;

– любое самостоятельное изменение состава аппаратных компонент вычислительных систем и др.

5.4 Нарушение этих ограничений рассматривается как нарушение целостности ПК «С-Терра СОВ» и трактуется ООО «С-Терра СиЭсПи» как основание для отказа Конечному Пользователю в сервисе технического сопровождения и поддержки ПК «С-Терра СОВ».

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

5.6 На аппаратные платформы 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

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

РЛКЕ.00021-01 _____
обозначение серийный номер

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

согласно требованиям, предусмотренным ТУ 62.01.29-021-70221576-2019
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

М.П.

7 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

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

РЛКЕ.00021-01 _____
обозначение серийный номер

соответствует техническим условиям ТУ 62.01.29-021-70221576-2019
номер технических условий или стандарта

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

Дата выпуска «____» _____ 20___ г.

_____ _____
подпись расшифровка подписи

М.П

8 СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

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

Рекламация подписывается руководителем подразделения, принимающего или эксплуатирующего программное обеспечение.

Поступающие к поставщику (изготовителю) рекламации регистрируются в журнале учета рекламаций (Таблица 5).

Таблица 5

Дата	**Содержание рекламации**	**Меры, принятые по рекламации**	**Подпись ответственного лица**

9 СВЕДЕНИЯ О ХРАНЕНИИ

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^{o}C до плюс 35^{o}C, относительной влажности воздуха не более 65 %.

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

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

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

10 СВЕДЕНИЯ ОБ УСТАНОВКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Установка изделия «Программный комплекс С-Терра СОВ. Версия 4.2» осуществляется предприятием-поставщиком (изготовителем) согласно договору на поставку.

Компьютер с установленным «Программным комплексом С-Терра СОВ. Версия 4.2» должен отвечать следующим минимальным требованиям (см. Таблицу 6).

Таблица 6

Наименование компонентов	**Состав (количество) компонентов**
Сетевые интерфейсы	2 x 10/100 Мбит/с
Оперативная память	2 Гбайта
Тип процессора	Intel x86-64
Тактовая частота процессора	1,33 ГГц
Объем жестких дисков	36 Гбайт

11 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

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

- запрещается использование ПК «С-Терра СОВ» для обработки информации, содержащей сведения, составляющие государственную тайну;
- администратором ПК «С-Терра СОВ» должна быть обеспечена своевременная установка актуальных обновлений среды функционирования;
- должна быть обеспечена поставка, установка, управление и функционирование ПК «С-Терра СОВ» безопасным образом и в соответствии с поставляемыми руководствами;
- должна быть обеспечена защита компьютера с установленным ПК «С-Терра СОВ», сетевого и кроссового оборудования, системы электропитания от несанкционированного физического воздействия, и доступность их только для обслуживающего персонала;
- администраторы ПК «С-Терра СОВ» должны пройти проверку на благонадежность и компетентность, а также действовать согласно правилам и процедурам, установленным в документации, квалифицированно выполнять обязанности по реализации документированной политики доступа;
- периодически должен выполняться регламентный контроль целостности ПК «С-Терра СОВ» с использованием утилиты integr_mgr компании С-Терра СиЭсПи по алгоритму ГОСТ Р 34.11-2012, а также при восстановлении после сбоев/отказов программного обеспечения и/или оборудования;
- для обеспечения доверенного маршрута между удаленным рабочим местом администратора и ПК «С-Терра СОВ», управляемые данные должны передаваться по защищенному соединению;
- должна быть обеспечена защита журнала аудита от несанкционированного изменения и удаления;
- должен быть обеспечен доступ ПК «С-Терра СОВ» ко всем объектам ИС, которые необходимы для реализации своих функциональных возможностей путем корректной настройки доверенных узлов;
- должна быть обеспечена защищенная область для выполнения функций безопасности ПК «С-Терра СОВ»;

- должен быть обеспечен надлежащий источник меток времени и синхронизация по времени между ПК «С-Терра СОВ» и средой его функционирования;
- должна быть обеспечена совместимость ПК «С-Терра СОВ» с элементами ИС, контроль которой он осуществляет, путем корректной настройки;
- необходимо использовать межсетевой экран соответствующего класса защищенности, сертифицированный по требованиям безопасности информации;
- должен быть ограничен доступ (в том числе физический) к ОО пользователей, кроме администратора, являющегося доверенным лицом и лицом, ответственным за функционирование ОО;
- необходимо отключить возможность удаленного доступа к базе данных MySQL с помощью изменения параметра bind-address в конфигурационном файле /etc/mysql/my.conf следующим образом: 'bind-address = 127.0.0.1' или использовать межсетевой экран соответствующего класса защищенности, сертифицированный по требованиям безопасности информации.

12 УКАЗАНИЯ ПО ОБНОВЛЕНИЮ

12.1 Устранение уязвимостей ПК «С-Терра СОВ» производится изготовителем с использованием организационно-технических процедур, представленных ниже.

12.2 Изготовитель периодически, не реже одного раза в месяц, проводит поиск уязвимостей ПК «С-Терра СОВ», включая заимствованные компоненты, а также известных (подтвержденных) уязвимостей среды функционирования в общедоступных источниках информации об уязвимостях. В качестве общедоступных источников в первую очередь используется 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/,
- http://www.cvedetails.com/,
- и другие.

12.3 Изготовитель проводит анализ выявленных уязвимостей с учетом следующих критериев:

- тип ошибки;
- версия программного обеспечения, подверженная уязвимости;
- уровень опасности уязвимости: критическая (Critical), высокая (High), средняя (Medium), низкая (Low);
- информация об устранении.

12.4 В случае выявления уязвимостей в ПК «С-Терра СОВ» согласно проведенного анализа, изготовитель выпускает обновление (патч), направленное на недопущение конечными пользователями попыток эксплуатации выявленной уязвимости.

12.5 При выпуске изготовителем обновления (патча) для устранения выявленных недостатков, уязвимостей и ошибок:

- изготовитель размещает на сайте своей компании в разделе «Поддержка» сообщение о выявленных критических ошибках, уязвимостях;
- изготовитель оповещает по электронной почте конечных пользователей о мерах по устранению ошибок, уязвимостей. Конечному пользователю также предоставляется логин и пароль для доступа к FTP-серверу компании для загрузки пакета, в который входит патч и ЭП;
- изготовитель размещает на FTP-сервере компании созданный пакет, инструкцию по установке патча;

- согласно полученной инструкции конечный пользователь загружает с FTP-сервера компании-изготовителя подготовленный пакет, предъявив логин и пароль для доступа;
- при проверке ЭП конечный пользователь использует открытый ключ сертификата, предоставляемого совместно с патчем;
- либо, чтобы убедиться в целостности и подлинности патча, конечный пользователь должен вычислить контрольную сумму патча и сравнить ее значение с предоставленным согласно инструкции;
- перед установкой патча на ПК «С-Терра СОВ» конечному пользователю рекомендуется провести тестирование с использованием тестового стенда, описанного в документе «Технические условия». Установите на стенд ПК «С-Терра СОВ» и патч, и выполните необходимые тесты на проверку функционирования;
- после успешного тестирования патча конечный пользователь может установить патч на ПК «С-Терра СОВ» согласно приложенной инструкции. Для контроля установки обновления (патча) нужно выполнить контроль целостности ПК «С-Терра СОВ», проверить доступность интерфейсов для управления;
- в случае, если не удалось проверить подпись, пользователь загружает пакет еще раз. Если патч не установился – повторно инсталлирует его.

12.6 В случае невозможности устранения уязвимостей средства защиты информации путем применения обновления, изготовитель предоставляет конечному пользователю ПК «С-Терра СОВ» инструкцию по проведению организационно–технических мероприятий, направленных на недопущение попыток эксплуатации выявленной уязвимости злоумышленниками в соответствующем разделе сайта изготовителя.

12.7 В случае невозможности проведения организационно–технических мероприятий, изготовитель разрабатывает ограничения по применению средства защиты информации, которые незамедлительно доводит до конечных пользователей. Если пользователь не может реализовать ограничения по применению средства защиты информации, он прекращает его использование.

12.8 При внесении изменений в ПК «С-Терра СОВ» для устранения уязвимостей и ошибок изготовитель обязан провести работы по испытаниям средства защиты информации в испытательной лаборатории ФСТЭК России. При положительном проведении испытаний изготовитель должен предоставить конечному пользователю ПК «С-Терра СОВ»:

- патч для обновления ПК «С-Терра СОВ»;
- копию согласованного ФСТЭК России извещения об изменениях и копию согласованного измененного Формуляра.

13 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 № сопроводительного докум. и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					
1		1,2,4,5,9-23	24-25		25				09.09. 2019