

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

Программный комплекс

С-Терра СОВ

Версия 4.2

Формуляр

ЛИСТ УТВЕРЖДЕНИЯ

РЛКЕ.00021-01 30 01-ЛУ

Листов 23

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

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 23

2018

Содержание

1	ОБЩИЕ УКАЗАНИЯ.....	3
2	ОБЩИЕ СВЕДЕНИЯ.....	4
3	ОСНОВНЫЕ ХАРАКТЕРИСТИКИ.....	6
4	КОМПЛЕКТНОСТЬ.....	9
5	ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА.....	12
6.	ПРОЦЕДУРА ОБНОВЛЕНИЯ ОО ПРИ ОБНАРУЖЕНИИ И УСТРАНЕНИИ УЯЗВИМОСТЕЙ	14
7.	СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ.....	15
8	СВИДЕТЕЛЬСТВО О ПРИЕМКЕ.....	16
9	СВЕДЕНИЯ О РЕКЛАМАЦИЯХ.....	17
10	СВЕДЕНИЯ О ХРАНЕНИИ.....	18
11	СВЕДЕНИЯ ОБ УСТАНОВКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	19
12	УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ.....	20
13	КОНТРОЛЬ СОСТОЯНИЯ ИЗДЕЛИЯ И ВЕДЕНИЯ ФОРМУЛЯРА.....	22

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 требованиям руководящих документов «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности» (ФСТЭК России, 2013) по оценочному уровню доверия ОУД 3, усиленный компонентами ADV_IMP.2 «Реализация функций безопасности объекта оценки», ADV_LLD.1 «Описательный проект нижнего уровня», ALC_FLR.1 «Базовое устранение недостатков», ALC_TAT.1 «Полностью определенные инструментальные средства разработки», AVA_VLA.3 «Умеренно стойкий», расширенный

компонентами ALC_UPI_EXT.1 «Процедуры обновления базы решающих правил» и AMA_SIA_EXT.3 «Экспертиза анализа влияния обновлений базы решающих правил на безопасность ОО; «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011); «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» (ФСТЭК России, 2012) по 4 классу защиты.

«Программный комплекс С-Терра СОВ. Версия 4.2» может использоваться в государственных информационных системах до 1 класса защищенности включительно, а также в информационных системах персональных данных, обеспечивающих до 1 уровня защищенности персональных данных включительно.

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 веб-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`, `sftp`;

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.

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»		
<u>Программные средства</u>		
С-Терра СОВ. Дистрибутив, в том числе БРП	1	Каталог STerra_IDS
С-Терра Шлюз ST. Дистрибутив ¹	1	Каталог STerra_Gate_ST_KC1_KC2
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_mgg 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 VPN и COB. Версия 4.2»	
<u>Документация</u>	
«Программный комплекс С-Терра COB. 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 COB. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00021-01 30 01	Каталог Formular_Rules
«Программный комплекс С-Терра Шлюз. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00017-01 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 COB. Версия 4.2»	Каталог Certificates
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 COB. Версия 4.2», функционирующего в виртуальной среде, указан в Таблице 4.

Таблица 4

Наименование	Размещение на DVD диске
DVD-диск «С-Терра Виртуальный COB. Версия 4.2»	
<u>Программные средства</u>	
Образ виртуальной машины в формате OVA или в архиве zip (в том числе БРП)	Каталог STerra_IDS
<u>Документация</u>	
«Программный комплекс С-Терра COB. Версия 4.2» Ру- ководство администратора и пользователя. РЛКЕ.00021- 01 90 01	Каталог Documentation
«Программный комплекс С-Терра Шлюз. Версия 4.2» Ру- ководство администратора. РЛКЕ.00017-01 90 01	
«Программный комплекс С-Терра COB. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00021-01 30 01	Каталог Formular_Rules
«Программный комплекс С-Терра Шлюз. Версия 4.2». Формуляр (ФСТЭК России). РЛКЕ.00017-01 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 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»;
- 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»;
- 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 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. ПРОЦЕДУРА ОБНОВЛЕНИЯ ОО ПРИ ОБНАРУЖЕНИИ И УСТРАНЕНИИ УЯЗВИМОСТЕЙ

При обнаружении уязвимостей и ошибок в ПК «С-Терра СОВ» или среде функционирования поставщик выпускает обновление (патч) для устранения выявленных уязвимостей и ошибок.

ООО «С-Терра СиЭсПи» предоставляет конечным пользователям обновление (патч) в результате выполнения следующих мероприятий:

- изготовитель на сайте своей компании в разделе «Поддержка» (<https://www.s-terra.ru/podderzhka/>) размещает сообщение о выявленных критических ошибках, уязвимостях;
- изготовитель размещает на FTP-сервере компании или другом ресурсе обновление (патч), инструкцию по установке патча и контрольную сумму обновления;
- изготовитель оповещает по электронной почте конечных пользователей о мерах по устранению ошибок, уязвимостей. Конечному пользователю предоставляется логин и пароль для доступа к предоставленному ресурсу компании для загрузки патча.

Конечный пользователь загружает обновление с предоставленного ресурса, проверяет целостность полученного патча (контрольную сумму) и согласно прилагаемой инструкции устанавливает патч на ПК «С-Терра СОВ». Контрольные суммы патча рассчитываются по алгоритму ГОСТ Р 34.11-2012 с длиной ключа 256 бит с использованием сертифицированной утилиты stverify, разработанной компанией «С-Терра СиЭсПи» или по алгоритму ГОСТ Р 34.11-94 с использованием ПО ФИКС, версия 2.0.2.

Изготовитель при выпуске обновления (патча) предоставляет обновление в испытательную лабораторию для проведения внешнего инспекционного контроля. Также предоставляется анализ влияния обновления на функции безопасности ПК «С-Терра СОВ» или отсутствие такого влияния. По результатам инспекционного контроля конечному пользователю предоставляются документы с изменениями – сертификат, Формуляр, а также вносятся изменения в пользовательскую документацию.

При невозможности устранения выявленной уязвимости и ошибок изготовитель предоставляет конечному пользователю перечень организационных мер для невозможности использования уязвимости либо разрабатывает ограничения по применению ПК «С-Терра СОВ».

7. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

Изделие «Программный комплекс С-Терра СОВ. Версия 4.2» упаковано согласно требованиям, предусмотренным в действующей технической документации.

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

должность

подпись

расшифровка подписи

число, месяц, год

М.П.

8 СВИДЕТЕЛЬСТВО О ПРИЕМКЕ

Изделие «Программный комплекс С-Терра СОВ. Версия 4.2» 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.

10 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°С до плюс 35°С, 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°С/ч) и воздействия внешних магнитных полей напряженностью более 4000А/м.

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

11 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

12 УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

«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 сбоя/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.

