СОГЛАСОВАНО
Начальник 2 управления
ФСТЭК России

_____ В.С. Лютиков
«_17_» _декабря_ 2015 г.

УТВЕРЖДАЮ
Генеральный директор
ООО «НПП «ИТБ»

_____ А.Ю. Щеглов
«___» _____ 201___ г.

Программное обеспечение
«Комплексная система защиты информации
«Панцирь+» для ОС Microsoft Windows»
Формуляр
ЛИСТ УТВЕРЖДЕНИЯ
643.53262993.00021-01 30-ЛУ

2014

Инв.№ подл.	Подп. и дата	Взам.инв.№	Инв.№ дубл.	Подп. и дата

УТВЕРЖДЕН

643.53262993.00021-01 30-ЛУ

Программное обеспечение

«Комплексная система защиты информации

«Панцирь+» для ОС Microsoft Windows»

Формуляр

643.53262993.00021-01 30

Листов 25

Инв.№ подл	Подп. и дата	Взам.инв.№	Инв.№ дубл.	Подп. и дата

2014

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

Сокращение	Описание
АРМ	автоматизированное рабочее место
КС	контрольные суммы
МЭ	межсетевой экран
ПО	программное обеспечение
ПЭВМ	персональная электронно-вычислительная машина
ТУ	технические условия
TCP/IP	Transport Control Protocol/Internet Protocol - Протокол потока байтов, используемый сетью Internet для связи компьютеров по различным физическим каналам
НСД	Несанкционированный доступ
ОС	Операционная система

1. ОБЩИЕ УКАЗАНИЯ

1.1. Ввод в эксплуатацию программного обеспечения «Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows», обозначение 643.53262993.00021-01 (далее по тексту КСЗИ) проводится в соответствии с формуляром и другими эксплуатационными документами.

1.2. Перед началом эксплуатации КСЗИ необходимо внимательно ознакомиться с содержанием эксплуатационной документации на нее и обеспечить выполнение всего комплекса предписанных организационно-технических мероприятий.

1.3. КСЗИ поставляется в программном исполнении, а его комплектность определена в разделе 4 настоящего формуляра.

1.4. Формуляр должен находиться у должностного лица (администратора службы безопасности информации), ответственного за эксплуатацию КСЗИ. Все записи в формуляре должны производиться только чернилами, отчетливо и аккуратно. Подчистки, помарки и незаверенные исправления НЕ ДОПУСКАЮТСЯ.

1.5. В случае обнаружения дефектов изделия следует обращаться к предприятию-поставщику КСЗИ.

1.6. Все предъявленные рекламации должны отмечаться в разделе 10 настоящего формуляра.

2. ОБЩИЕ СВЕДЕНИЯ

2.1. Наименование продукта: программное обеспечение «Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows», обозначение 643.53262993.00021-01.

2.2. КСЗИ предназначена для реализации защиты рабочих станций и серверов, функционирующих под управлением ОС семейства Microsoft Windows:

- Microsoft Windows XP в 32-х битном режиме SP3 (включительно);
- Microsoft Windows XP в 64-х битном режиме SP2 (включительно);
- Microsoft Windows 2003 в 32-х, 64-х битных режимах SP2 (включительно);
- Microsoft Windows 2003 R2 в 32-х, 64-х битных режимах SP2 (включительно);
- Microsoft Windows Vista в 32-х, 64-х битных режимах SP2 (включительно);
- Microsoft Windows 7 в 32-х, 64-х битных режимах SP1 (включительно);
- Microsoft Windows Server 2008 в 32-х,64-х битных режимах SP2 (включительно);
- Microsoft Windows Server 2008 R2 64-х битный режим SP1 (включительно);
- Microsoft Windows 8 в 32-х,64-х битных режимах;
- Microsoft Windows Server 2012 в 64-х битном режиме;
- Microsoft Windows 8.1 32-х,64-х битных режимах;
- Microsoft Windows Server 2012 R2 в 64-х битном режиме (включительно).

2.3. Тип продукта: программное обеспечение, разработанное на языке программирования C++.

2.4. Разработчик и производитель продукта: ООО «НПП «ИТБ» (юридический и фактический адрес: Российская Федерация, г. Санкт-Петербург, пр. Большой Сампсониевский, д. 32, Литер А, оф. 2С 334).

2.5. КСЗИ сертифицировано в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 и имеет сертификат соответствия требованиям по безопасности информации от «17» декабря 2015 года № 3473, согласно которому КСЗИ соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по **5** классу защищенности, «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) – по **4** классу защищенности, **технических условий ТУ 50 14107-021-53262993-2014**, руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по **4** уровню контроля, при выполнении ограничений по применению, указанных в разделе 5 настоящего формуляра. КСЗИ может применяться в государственных информационных системах до **1** класса защищенности включительно. КСЗИ может применяться для защиты информационных систем персональных данных до **1** уровня защищенности включительно, для которых к актуальным отнесены угрозы **2**-го и **3**-го типа.

3. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

3.1. КСЗИ представляет собою систему защиты информации в локальной вычислительной сети (ЛВС) предприятия с выделенным рабочим местом администратора безопасности ЛВС, либо защиты автономных компьютеров.

3.2. КСЗИ состоит из следующих отдельно устанавливаемых программных средств:

1. Клиентская часть.
2. Сервер безопасности.
3. Сервер аудита.
4. Программа тиражирования настроек

Клиентская часть КСЗИ предназначена для непосредственной защиты информации – в ней реализуются все механизмы защиты, как для защиты компьютеров в составе локальной вычислительной сети (ЛВС) предприятия с выделенным рабочим местом администратора безопасности ЛВС, так и для защиты автономных компьютеров. Устанавливается на защищаемые объекты информатизации: рабочие станции и серверы.

Сервер безопасности КСЗИ предназначен для удаленного управления клиентскими частями и обработки журналов аудита в интерактивном режиме, предоставляет администратору безопасности всю необходимую ему для принятия решений справочную информацию (по вычислительным средствам и пользователям информационных ресурсов, обрабатываемых в корпоративной сети). Устанавливается на выделенный компьютер администратора безопасности.

Сервер аудита КСЗИ предназначен для удаленного сбора и обработки аудита реального времени со всех компьютеров в составе сети, на которые устанавливается клиентская часть КСЗИ. Устанавливается на выделенный компьютер администратора безопасности. Контролируемые события по всем защищаемым объектам в реальном времени отображаются на сервере аудита в окне интерфейса. Сервер аудита может устанавливаться, как на том же компьютере, что и сервер безопасности, так и на отдельном компьютере.

Программа тиражирования настроек КСЗИ «Панцирь+» предназначена для проведения первичной настройки клиентских частей, подключенных к серверной части (сервер безопасности) КСЗИ «Панцирь+». Программа входит в состав серверной части (сервер безопасности) КСЗИ «Панцирь+» на одном компьютере.

3.3. КСЗИ обеспечивает выполнение следующих требований:

3.3.1. КСЗИ выполняет требования 5 класса защищенности Руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

3.3.2. КСЗИ выполняет требования 4 класса защищенности Руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

3.3.3. КСЗИ выполняет требования Технических условий КСЗИ «Панцирь+» ТУ 50 14107-021-53262993-2014.

4. КОМПЛЕКТНОСТЬ

4.1. КСЗИ является программным обеспечением и поставляется в составе, представленном в таблице 1.

Таблица 1 – Комплектность поставки КСЗИ

№ п/п	Наименование	Обозначение	Количество	Примечание
1.	Сертифицированный дистрибутив ПО КСЗИ «Панцирь+»	643.53262993.00021-01	1	В электронном виде на оптическом носителе
2.	Документация на ПО КСЗИ «Панцирь+» на русском языке, в т.ч.: − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Руководство администратора. Локальное администрирование 643.53262993.00021-01 33 01; − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Руководство администратора. Удаленное администрирование 643.53262993.00021-01 33 02; − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Руководство администратора. Программа тиражирования настроек 643.53262993.00021-01 33 03; − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Руководство пользователя 643.53262993.00021-01 34; − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Описание применения 643.53262993.00021-01 31 − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Описание программы 643.53262993.00021-01 13; − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Технические условия ТУ 50 14107-021-53262993-2014; − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Тестовая документация. Том 1 643.53262993.00021-01 91 01; − Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Ведомость эксплуатационных	б/н	1	В электронном виде на оптическом носителе, каталог «Документация»

№ п/п	Наименование	Обозначение	Количество	Примечание
	документов 643.53262993.00021-01 20; – Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Спецификация 643.53262993.00021-01 Sp.			
3.	Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows. Формуляр 643.53262993.00021-01 30	643.53262993.00021-01 30	1	На бумажном носителе
4.	Заверенная копия выданного ФСТЭК России сертификата соответствия КСЗИ «Панцирь+» требованиям по безопасности информации	б/н	1	На бумажном носителе
5.	Знак соответствия для маркирования сертифицированной продукции	б/н	1	Наносится на лицевую часть коробки упаковочной в правый верхний угол
6.	Коробка упаковочная с наклеенным знаком соответствия сертифицированной продукции	б/н	1	

4.2. Перед установкой сертифицированной версии КСЗИ производится его контроль с использованием специализированных программ. Контрольные суммы дистрибутивного комплекта, а также контрольные суммы неизменяемых файлов КСЗИ, рассчитанные по алгоритму «Уровень-1 (программно)» с помощью программы фиксации и контроля исходного состояния программного комплекса «ФИКС», версия 2.0.2, имеющей сертификат соответствия №1548 (выдан ФСТЭК России 15 января 2008 г., продлён до 15 января 2017 г.), представлены в электронном приложении к настоящему документу:

– контрольные суммы неизменяемых исполняемых файлов и библиотек ПО КСЗИ представлены в файле ispf.doc, который находится в электронном приложении в папке «Контрольные суммы» и подпапке «Неизменяемые файлы»;

– контрольные суммы дистрибутива ПО КСЗИ представлены в электронном приложении в файле DVD1.doc, который находится в папке «Контрольные суммы».

5. УКАЗАНИЯ ПО ЭКСПЛУАТАЦИИ

5.1. Перед эксплуатацией программного обеспечения КСЗИ необходимо внимательно ознакомиться с эксплуатационной документацией.

5.2. Программное обеспечение КСЗИ должно эксплуатироваться на компьютерах, аппаратная и программная часть которых соответствует требованиям, указанным в эксплуатационной документации.

5.3. При эксплуатации КСЗИ на объектах информатизации, где производится обработка конфиденциальной информации, необходимо выполнение следующих **ограничений**:

– запрет на использования КСЗИ для обработки информации, содержащей сведения, составляющие государственную тайну;

– использование сертифицированной версии КСЗИ;

– использование сертифицированных ФСТЭК России электронных ключей.

5.4. Для повышения защищенности объектов информатизации при использовании КСЗИ **рекомендовано** обеспечить следующее:

– создание административной группы или подразделения, обеспечивающего установку, настройку и сопровождение изделия;

– наличие администратора безопасности (администратора КСЗИ), отвечающего за корректную настройку и эксплуатацию КСЗИ;

– уведомление пользователей предприятия о разрешенных им разграничительной политикой правах доступа к ресурсам вычислительной системы;

– разработка нормативных документов, определяющих порядок допуска пользователей к программному обеспечению КСЗИ и назначения их полномочий;

– применение и настройка механизмов защиты из состава КСЗИ в соответствии с разграничительной политикой доступа к ресурсам, разрабатываемой на основе созданной для предприятия модели угроз;

– реализация необходимых организационных мер защиты, усиливающих возможности КСЗИ.

5.5. Порядок и процедура обновления КСЗИ.

5.5.1. Порядок обновления КСЗИ в случае выявления уязвимости в программном обеспечении, требующей немедленного исправления (ошибка, связанная с нарушением безопасности):

1. Уведомление потребителей об обнаружении уязвимости и о предлагаемых организационно-технических мерах по реализации защиты от атак на эту уязвимость.

2. В течение 5 рабочих дней после исправления выявленной уязвимости, предоставление потребителям обновленного дистрибутива в электронном виде и подача обновленного дистрибутива на инспекционный контроль. Обновление дистрибутива для потребителя обязательно.

3. В течение 5 рабочих дней после завершения процедуры инспекционного контроля, предоставление потребителям в электронном виде формуляра с обновленными контрольными суммами программного обеспечения.

5.5.2. Порядок обновления КСЗИ в случае выявления ошибок в программном обеспечении, не связанных с нарушением безопасности, или доработки программного обеспечения по инициативе разработчика:

1. В течение 10 рабочих дней после исправления ошибки либо проведения доработки, уведомление потребителей о появлении новой несертифицированной версии программного обеспечения с комментариями об отличии от предыдущей версии.
2. Предоставление обновленного дистрибутива в электронном виде по запросу потребителя.
3. Подача обновленного дистрибутива на инспекционный контроль по мере накопления изменений в программном обеспечении, но не реже одного раза в полгода (при наличии изменений).
4. В течение 10 рабочих дней после завершения процедуры инспекционного контроля, предоставление потребителям в электронном виде обновленного дистрибутива и формуляра с обновленными контрольными суммами программного обеспечения.

5.6. Должны быть реализованы организационно-распорядительные меры, предусмотренные мерами защиты согласно Приказу ФСТЭК России от 11 февраля 2013 г. № 17, Приказу ФСТЭК России от 18 февраля 2013 г. № 21, Методическому документу «Меры защиты информации в государственных информационных системах» (Утвержден ФСТЭК России 11 февраля 2014 г.):

- Должны быть регламентированы в организационно-распорядительных документах по защите информации:
  - согласно ИАФ.1 правила и процедуры идентификации и аутентификации пользователей;
  - согласно ИАФ.2 правила и процедуры идентификации и аутентификации устройств;
  - согласно ИАФ.3 правила и процедуры управления идентификаторами;
  - согласно ИАФ.4 правила и процедуры управления средствами аутентификации (аутентификационной информацией);
  - согласно УПД.1 правила и процедуры управления учетными записями пользователей;
  - согласно УПД.2 правила разграничения доступа;
  - согласно УПД.3 правила и процедуры управления информационными потоками;
  - согласно УПД.4 полномочия пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий;
  - согласно УПД.5 роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий;
  - согласно УПД.6 ограничение количества неуспешных попыток входа в информационную систему (доступа к информационной системе) за период времени, установленный оператором;
  - согласно УПД.10 правила и процедуры блокирования сеансов доступа;

- согласно УПД.12 правила и процедуры поддержки и сохранения атрибутов безопасности;
- согласно ОПС.1 правила и процедуры управления запуском программного обеспечения (в том числе списки программного обеспечения, ограничения запуска, параметры запуска компонентов программного обеспечения);
- согласно ОПС.4 порядок очистки (стирания) временных файлов;
- согласно ЗНИ.2 правила и процедуры доступа к машинным носителям информации;
- согласно ЗНИ.5 правила и процедуры контроля использования интерфейсов ввода (вывода);
- согласно ЗНИ.6 правила и процедуры контроля ввода (вывода) информации на машинные носители информации;
- согласно ЗНИ.7 правила и процедуры контроля подключения машинных носителей информации;
- согласно ЗНИ.8 процедуры уничтожения (стирания) информации на машинных носителях, а также контроля уничтожения (стирания) информации;
- согласно РСБ.2 состав и содержание информации о событиях безопасности, подлежащих регистрации;
- согласно РСБ.3 правила и процедуры сбора, записи и хранения информации о событиях безопасности;
- согласно РСБ.4 правила и процедуры реагирования на сбои при регистрации событий безопасности;
- согласно РСБ.7 правила и процедуры защиты информации о событиях безопасности;
- согласно РСБ.8 правила и процедуры просмотра и анализа информации о действиях отдельных пользователей;
- согласно ОЦЛ.1 правила и процедуры контроля целостности программного обеспечения;
- согласно ОЦЛ.3 правила и процедуры восстановления (в том числе планы по действиям персонала порядок применения компенсирующих мер);
- согласно ОЦЛ.6 ограничения прав пользователей по вводу информации в информационную систему;
- согласно ЗИС.5 перечень периферийных устройств, для которых допускается возможность удаленной активации;
- согласно ЗИС.8 правила и процедуры контроля использования технологий передачи речи;
- согласно ЗИС.9 правила и процедуры контроля передачи видеоинформации;
- согласно ЗИС.23 правила и процедуры защиты периметра информационной системы.

– Согласно ИАФ.4 смена пароля должна производиться не более чем через 180, 120, 90 или 60 дней в зависимости от класса защищенности информационной системы

– Согласно АН3.5 оператором должен обеспечиваться контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации оператора. Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе проводится с периодичностью, установленной оператором в организационно- распорядительных документах по защите информации.

5.7. Органам государственной власти и организациям, использующим для защиты информации сертифицированные ФСТЭК России версии операционной системы Windows XP, рекомендуется:

1. Спланировать мероприятия по переводу до декабря 2016 г. информационных систем на сертифицированные по требованиям безопасности информации операционные системы, поддерживаемые их производителями.

2. До перехода на сертифицированные по требованиям безопасности информации операционные системы с учетом моделей угроз безопасности информации принять следующие дополнительные меры защиты информации, направленные на минимизацию рисков реализации угроз безопасности информации:

- установить все актуальные обязательные сертифицированные обновления сертифицированных версий операционной системы Windows XP, выпущенные российскими производителями (заявителями);

- установить запрет на автоматическое обновление сертифицированных версий операционной системы Windows XP;

- провести настройку и обеспечивать периодический контроль механизмов защиты сертифицированных версий операционной системы Windows XP в соответствии с руководствами по безопасной настройке и контролю сертифицированных версий операционной системы Windows XP;

- по возможности исключить подключение к сети Интернет и к ведомственным (корпоративным) локальным вычислительным сетям средств вычислительной техники или сегментов информационных систем, работающих под управлением операционной системы Windows XP;

- при невозможности отключения от сети Интернет и (или) от ведомственных (корпоративных) локальных вычислительных сетей средств вычислительной техники или сегментов информационных систем, работающих под управлением операционной системы Windows XP, применять в обязательном порядке меры по сегментированию информационных систем и защите периметра информационной системы и выделенных сегментов (в том числе путем применения сертифицированных межсетевых экранов, средств антивирусной защиты, систем обнаружения вторжений, средств защиты от несанкционированной передачи (вывода) информации (DLP - систем), средств управления потоками информации);

- обеспечить регулярное резервное копирование информации, программного обеспечения и средств защиты информации, содержащихся на средствах вычислительной техники или в сегментах информационных систем, работающих под управлением операционной системы Windows XP, на внешние носители информации;

- регламентировать и обеспечивать контроль за применением съемных машинных носителей информации, исключив при этом использование не зарегистрированных в информационной системе машинных носителей информации и не проверенных средствами антивирусной защиты;

- проводить периодический анализ уязвимостей сегментов информационных систем, работающих под управлением операционной системы Windows XP, с использованием сертифицированных средств контроля (анализа) защищенности информации, а также периодический контроль целостности установленных операционных систем;
- проводить мониторинг общедоступных источников, публикующих сведения об уязвимостях, на предмет появления в них информации об уязвимостях в операционной системе Windows XP и принимать меры, направленные на устранение выявленных уязвимостей или исключающие возможность использования нарушителями выявленных уязвимостей (в том числе за счет применения дополнительных средств защиты информации);
- разработать и внедрить правила и процедуры действий должностных лиц в случае выявления уязвимостей в операционной системе Windows XP или возникновения инцидентов информационной безопасности, связанных с ее применением.

6. ПЕРИОДИЧЕСКИЙ КОНТРОЛЬ ОСНОВНЫХ ХАРАКТЕРИСТИК ПРИ ЭКСПЛУАТАЦИИ И ХРАНЕНИИ

Отметки о прохождении КСЗИ сертификационных и периодических испытаний заносятся в таблицу 2.

Таблица 2 - Периодический контроль основных характеристик изделия

Проверяемая характеристика		Дата проведения измерения					
Наименование измерения	Величина	20__г		20__г		20__г	
		Фактическая величина	Замерил (должность и подпись)	Фактическая величина	Замерил (должность и подпись)	Фактическая величина	Замерил (должность и подпись)

7. СВИДЕТЕЛЬСТВО О ПРИЁМКЕ

Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows, серийный номер _____ проверено, соответствует техническим условиям ТУ 50 14107-021-53262993-14 и признано годным для эксплуатации.

Дата выпуска_____

Подпись лиц, ответственных за приемку_____

М.П.

8. СВИДЕТЕЛЬСТВО ОБ УПАКОВКЕ И МАРКИРОВКЕ

Свидетельство об упаковке

Комплексная система защиты информации «Панцирь+» для ОС Microsoft Windows
наименование

643.53262993.00021-01 _____
обозначение серийный номер изделия

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

_____
номер знака соответствия

упаковано _____
наименование или код предприятия (организации)

согласно требованиям, предусмотренным инструкцией _____
обозначение

Дата упаковки: «____» _____ 20___ года

Упаковку произвел: _____
(подпись)

Изделие после упаковки принял: _____
(подпись)

М.П.

_____
Примечание. Форму заполняют на предприятии, производившем упаковку

9. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

9.1. Потребитель, приобретая КСЗИ, несет ответственность за его использование в соответствии с рекомендациями, изложенными в эксплуатационной документации.

9.2. Производитель КСЗИ гарантирует его работоспособность в соответствии с объявленными характеристиками при соблюдении потребителем правил эксплуатации, транспортирования и хранения, указанных в документации на КСЗИ.

9.3. Гарантийный срок эксплуатации изделия – 12 (двенадцать) месяцев.

9.4. Датой исчисления гарантийного срока эксплуатации изделия является дата его поставки потребителю.

9.5. Изготовитель в течение гарантийного срока гарантирует, что:

- оптический носитель не содержит дефектов, приводящих их к неработоспособности;
- на оптическом носителе КСЗИ содержится в полном объеме;
- выполняемые КСЗИ функции соответствуют указанным в разработанной на него документации.

9.6. В случае выявления в изделии дефектов, не связанных с нарушением потребителя правил эксплуатации, КСЗИ подлежит рекламации. Рекламации направляются производителю изделия. Производитель изделия обязуется при получении рекламации в течение 2 недель принять меры по устранению дефектов, включая замену дефектного изделия на исправное.

9.7. Действие гарантийных обязательств прекращается, если:

- закончился гарантийный срок;
- потребителем в гарантийный период были нарушены правила эксплуатации КСЗИ, транспортирования и хранения оптического носителя;
- потребителем были внесены изменения в КСЗИ без согласования с производителем;
- КСЗИ была передана другому потребителю.

10. СВЕДЕНИЯ О РЕКЛАМАЦИЯХ

10.1. Рекламации, связанные с эксплуатацией сертифицированного КСЗИ, должны направляться в письменном виде производителю – ООО «НПП «ИТБ» (юридический и фактический адрес: Российская Федерация, г. Санкт-Петербург, пр. Большой Сампсониевский, д. 32, Литер А, оф. 2С 334).

В сопроводительном письме следует указать дату обнаружения, условия возникновения и характер проявления неисправности. Рекламация подписывается руководителем подразделения, принявшего или эксплуатирующего КСЗИ.

10.2. Поступившие рекламации регистрируются в журнале учета рекламаций. Срок рассмотрения рекламации – не более 2 недель со дня их поступления.

10.3. При несоответствии поставляемого оптического носителя, его тары, упаковки, маркировки и комплектности требованиям сопроводительной документации, потребитель обязан направить рекламацию производителю изделия в течение 60 дней со дня поставки.

10.4. Производитель принимает рекламацию, если не установлена вина потребителя в возникновении дефекта в оптическом носителе или КСЗИ.

10.5. Отметки о рекламациях заносятся в таблицу 3.

Таблица 3 - Сведения о рекламациях

Дата	Содержание рекламации	Меры, принятые по рекламации	Подпись ответственного лица

11. СВЕДЕНИЯ О ХРАНЕНИИ

11.1. Оптический носитель с размещёнными на нём сертифицированным дистрибутивом КСЗИ и комплектом документации, помещенный в защитный пластиковый футляр для хранения оптического носителя, должен храниться в помещении при температуре от + 5°С до + 40°С и относительной влажности воздуха от 10% до 80% при температуре + 23°С, при этом должны быть исключены резкие изменения температуры и влажности воздуха, а также воздействие прямых солнечных лучей.

Оптический носитель с размещёнными на нём КСЗИ и комплектом документации, который был подвергнут воздействию температуры и влаги, отличных от значений, установленных для хранения, необходимо перед использованием и хранением выдержать в нормальных условиях окружающей среды не менее 12 часов.

11.2. При транспортировании и хранении оптического носителя с размещёнными на нём КСЗИ и комплектом документации должны быть исключены механические удары и повреждения.

11.3. В помещениях, где хранится оптический носитель с размещёнными на нём КСЗИ и комплектом документации, необходимо исключить возможность попадания в воздух паров агрессивных веществ (кислот, щелочей, органических растворителей и т.д.), способных вызвать разрушение пластмасс и лакокрасочных покрытий.

11.4. Не допускается хранение оптического носителя с размещёнными на нём КСЗИ и комплектом документации вблизи сильных электромагнитных полей, а также на расстоянии менее чем один метр от нагревательных приборов.

11.5. Контроль условий хранения проводится потребителем ежемесячно. Сведения о хранении заносятся в таблицу 4.

Таблица 4 - Сведения о хранении

Дата		Условия хранения	Должность, фамилия и подпись лица, ответственного за хранение
установки на хранение	снятия с хранения		

12. СВЕДЕНИЯ О ЗАКРЕПЛЕНИИ ИЗДЕЛИЯ ПРИ ЭКСПЛУАТАЦИИ

В таблице 5 указывают фамилии и должности лиц, за которыми закрепляют КСЗИ при эксплуатации.

Таблица 5 - Сведения о закреплении изделия при эксплуатации

Должность ответственного лица	Фамилия, ответственного лица	Номер и дата приказа		Подпись ответственного лица
		о назначении	об освобождении	
1	2	3	4	5

13. СВЕДЕНИЯ ОБ ИЗМЕНЕНИЯХ

В таблице 6 фиксируется следующая информация: основание для внесения изменений, содержание изменения с указанием его порядкового номера, а также должность, фамилию и подпись лица, ответственного за проведение изменения.

Таблица 6 - Сведения об изменениях

Основание (входящий номер сопроводительного документа и дата)	Дата проведения изменения	Содержание изменения	Порядковый номер изменения	Должность, фамилия и подпись лица, ответственного за проведение изменения	Подпись лица, ответственного за эксплуатацию изделия
1	2	3	4	5	6

14. ОСОБЫЕ ОТМЕТКИ

Л И С Т   Р Е Г И С Т Р А Ц И И   И З М Е Н Е Н И Й

Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводительного докум. и дата	Подпись	Дата
Изм.	Измененных	Замененных	Новых	Аннулированных					