**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на предоставление неисключительного права использования средства защиты информации от несанкционированного доступа**

1. **Наименование объекта закупки:**

|  |  |  |
| --- | --- | --- |
| **№****п/п** | **Наименование** | **Кол-во шт.** |
| 1. | Неисключительное право на использование ПО (СЗИ НСД, СКН, МЭ) (программное обеспечение) | 100 |
| 2. | Сервер безопасности для ПО. Право на использование. Бессрочная лицензия. | 1 |
| 3. | Сертифицированный комплект для установки ПО | 2 |

1. **Описание объекта закупки:**
	1. **Требования к программному обеспечению**

СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах (ОС) семейства Windows с возможностью подключения аппаратных идентификаторов.

СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 в многопользовательском режиме их эксплуатации.

СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем.

СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.

СЗИ НСД должна быть сертифицирована на соответствие требованиям руководящих документов к 5-му классу защищенности от НСД для СВТ (РД СВТ, Гостехкомиссия России, 1992) и 4-му уровню доверия («Требования по безопасности информации, устанавливающие уровни доверия к СТЗИ и СОБИТ», ФСТЭК России, 2020), разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере.

Модуль МЭ должен быть сертифицирован на соответствие требованиям ФСТЭК России к межсетевым экранам по 4-му классу защиты в соответствии с профилем защиты межсетевых экранов типа «В» четвертого класса защиты (ИТ.МЭ.В4.ПЗ).

Модуль СКН должен быть сертифицирован на соответствие требованиям ФСТЭК России к средствам контроля съемных машинных носителей информации по 4-му классу защиты в соответствии с профилем защиты средств контроля подключения съемных машинных носителей информации (ИТ.СКН.П4.ПЗ).

СЗИ НСД может быть использована:

* при создании защищенных автоматизированных систем до класса защищенности 1Г включительно;
* в государственных информационных системах до 1 класса защищенности включительно;
* в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно;
* в информационных системах персональных данных до 1 уровня защищенности включительно;
* при защите значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно.

СЗИ НСД должна обеспечивать:

* + регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере. Возможность автоматического блокирования неактивных учетных записей пользователей;
	+ идентификацию и проверку подлинности пользователей при входе в ОС. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность задать расписание работы пользователей. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Возможность запрета повторного использования идентификатора. Возможность ограничения количества неуспешных попыток входа и блокирования устройства. Возможность автоматизированно сохранять авторизационные данные пользователя в системном кэше ОС при использовании (установке) СЗИ НСД. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows. Поддержку аутентификации пользователей с применением биометрии и токенов JaCarta PKI/BIO;
	+ реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам;
	+ возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в ОС;
	+ возможность настройки принудительной двухфакторной аутентификации для учетной записи с правами администратора и/или пользователя;
	+ возможность средствами СЗИ НСД выполнить настройку периода действия учетной записи;
	+ возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации;
	+ возможность при создании учетной записи выбрать тип учетной записи (внутренний, внешний, системный, приложение, гостевой, временный);
	+ независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съемным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных;
	+ контроль аппаратной конфигурации компьютера и следующих подключаемых устройств:
	+ Android-устройств;
	+ iOS-устройств;
	+ Bluetooth-устройств;
	+ DVD- и CD-ROM-дисководов;
	+ устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital;
	+ USB-контроллеров;
	+ беспроводных устройств (Wireless Communication Devices);
	+ биометрических устройств;
	+ дисководов магнитных дисков;
	+ звуковых, видео- и игровых устройств;
	+ инфракрасных устройств (IrDA);
	+ контроллеров магнитных дисков;
	+ ленточных накопителей;
	+ модемов;
	+ переносных устройств;
	+ портов (COM и LPT);
	+ сенсоров;
	+ сетевых адаптеров;
	+ сканеров и цифровых фотоаппаратов;
	+ принтеров;
	+ съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей).
	+ контроль устройств, подключаемых к терминальному серверу с RDP‑клиентов (контроль перенаправления устройств);
	+ предотвращение утечки информации с использованием съемных носителей информации. СЗИ НСД должна позволять разграничивать доступ как к отдельным типам носителей, так и к конкретным экземплярам;
	+ возможность запретить запуск (без команды пользователя) ПО, используемого для взаимодействия со съемными носителями информации;
	+ возможность запретить установку драйверов съемных носителей информации;
	+ преобразование информации:
* при работе с виртуальными дисками (преобразование выполняется незаметно для пользователя);
* при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи.
	+ блокировку виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора;
	+ сохранение теневых копий файлов, записываемых на съемные носители;
	+ автоматическое ограничение доступа к теневой копии, сделанной СЗИ НСД при копировании документа, содержащего информацию ограниченного доступа, на сменный машинный носитель;
	+ использование дискреционного принципа контроля доступа, обеспечивающего доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа);
	+ возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа);
	+ регистрацию и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и автоматической архивации по истечении установленного интервала времени;
	+ расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТ), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов;
	+ возможность добавления произвольного комментария к зарегистрированным событиям НСД;
	+ возможность экспорта журналов событий в syslog, возможность настройки кодировки экспортируемых в syslog событий;
	+ возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки;
	+ блокировку доступа к файлам по расширению;
	+ возможность разграничения доступа к буферу обмена;
	+ возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);
	+ возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности;
	+ очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Возможность определения метода зачистки. Контроль зачистки при полной зачистке логического диска. Очистку данных сеанса пользователя в оперативной памяти за счет запрета смены пользователя без перезагрузки;
	+ возможность проверки цифровой подписи объектов файловой системы, находящихся под контролем целостности, при их обновлении;
	+ выполнение регистрации действий по зачистке остаточной информации;
	+ самодиагностика основных функциональных возможностей СЗИ НСД и сохранение информации в виде отчета;
	+ возможность сохранения конфигурации для последующего восстановления СЗИ НСД;
	+ возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;
	+ возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ;
	+ ведение двух копий программных средств защиты информации и возможность возврата к настройкам по умолчанию;
	+ возможность сигнализации администратору безопасности о следующих инцидентах безопасности (ситуациях сбоя функционирования и ситуациях несанкционированного доступа на клиентских рабочих станциях):
	+ нарушение контроля целостности объекта;
	+ попытка работы после блокировки при нарушении целостности;
	+ попытка входа на клиентскую рабочую станцию с неправильным паролем;
	+ блокировка пользователя после многократного ввода неправильного пароля;
	+ СЗИ НСД на клиенте не отвечает (возможная причина - несанкционированная деактивация системы защиты);
	+ клиент недоступен долгое время (с возможностью задания периода времени);
	+ попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.
	+ централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями информации. Должна поддерживаться многоуровневая иерархия групп компьютеров и наследование установленных параметров. Также этим модулем должен осуществляться периодический сбор журналов со всех защищенных рабочих станций. Возможность блокировки компьютера, завершения сеанса работы пользователя по команде администратора;

Централизованное управление СЗИ НСД должно обеспечивать:

* + возможность настройки репликации серверов безопасности (модулей централизованного управления);
	+ возможность по управлению доменными учетными записями (создание, удаление, блокировка, перемещение) и группами Active Directory с учетом приоритета механизмов СЗИ над механизмами Active Directory (во избежание злоупотребления доменных администраторов своими полномочиями);
	+ централизованное управление контролем целостности объектов ФС, системного реестра;
	+ централизованное управление аппаратными идентификаторами;
	+ централизованное управление сессиями-исключениями;
	+ возможность блокирования сеанса доступа через средства централизованного и удаленного администрирования СЗИ НСД после установленного времени бездействия;
	+ возможность нотификации о наличии обновлений для СЗИ НСД на сервере компании-разработчика СЗИ НСД;
	+ возможность использования SQL базы данных для централизованного хранения событий аудита;
	+ возможность построения иерархии управления при помощи специального модуля — менеджера, управляющего несколькими модулями централизованного управления;
	+ возможность использования механизма удаленной установки и обновления СЗИ НСД средствами модуля централизованного управления самой СЗИ или средствами групповых политик Active Directory с отображением сообщения об окончании удаленной установки с указанием необходимости выполнения перезагрузки. Возможность удаления СЗИ через Active Directory без перезагрузки удаленных ПК. Проверка подписи файлов при обновлении СЗИ НСД;
	+ возможность визуализации сети защищаемых компьютеров;
	+ возможность подключения к модулям администрирования пользователя с ограниченными правами (права только на просмотр настроек; только на просмотр журналов аудита; полные права с возможностью делегирования);
	+ возможность выполнять синхронизацию времени между сервером безопасности и клиентами;
	+ возможность интеграции с SIEM-системами;
	+ возможность интеграции с антивирусными системами.

Должен быть реализован модуль контроля подключения съемных машинных носителей информации (СКН).

Модуль СКН должен обеспечивать:

* + контроль использования интерфейсов ввода/вывода средств вычислительной техники, подключения внешних программно-аппаратных устройств и конкретных съемных машинных носителей информации;
	+ возможность назначения прав доступа к конкретному накопителю;
	+ возможность установить описание для сменного накопителя.

Реализация СЗИ НСД должна быть полностью программной с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, а также аппаратных идентификаторов:

* USB-флэш-накопители;
* электронные ключи Touch Memory (iButton);
* HID Proximity-карты;
* USB-ключи Aladdin eToken Pro/Java;
* смарт-карты Aladdin eToken Pro/SC;
* USB-ключи и смарт-карты Рутокен (Rutoken), Рутокен ЭЦП, Рутокен ЭЦП 2.0;
* USB-ключи и смарт-карты JaCarta, JaCarta-2, JaCarta PRO, JaCarta LT, JaCarta PKI/BIO;
* USB-ключи и смарт-карты ESMART;
* NFC-метки и смарт-карты семейства MIFARE.

Поставка СЗИ НСД должна осуществляться в форме передачи неисключительных прав на использование программного обеспечения с указанием всех необходимых модулей и требуемого количества лицензий по каждому модулю. Поставка модуля контроля за изменением состава программного обеспечения и контроля целостности файлов программного обеспечения должна осуществляться совместно с модулем централизованного управления, лицензируются при этом подключения к модулю. Варианты формулировок:

* неисключительное право на использование СЗИ (НСД, СКН) (программное обеспечение);
* неисключительное право на использование сервера безопасности для СЗИ НСД (программное обеспечение);
* неисключительное право на использование сервера лицензий для СЗИ НСД (программное обеспечение);
* неисключительное право на подключения к серверу конфигураций для СЗИ НСД;
* неисключительное право на терминальное подключение СЗИ НСД (программное обеспечение).

Должен быть реализован модуль межсетевого экрана (МЭ). Данный модуль должен обеспечивать защиту рабочих станций и серверов от НСД посредством осуществления контроля и фильтрации проходящих через сетевые интерфейсы рабочих станций сетевых пакетов в соответствии с заданными администратором правилами.

Модуль МЭ должен обеспечивать:

* + возможность настройки правил фильтрации сетевых пакетов;
	+ возможность активации более строгих правил МЭ при отсутствии на защищаемом ПК антивируса, обновлений или при нарушении контроля целостности;
	+ фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
	+ возможность задавать правила фильтрации для приложений (процессов), в том числе используя возможность задавать и анализировать командную строку;
	+ возможность «пакетного» управления правилами МЭ, которая позволяет формировать и применять отдельные группы правил МЭ;
	+ возможность фильтрации по HTTP-заголовку для выявления аномальности трафика;
	+ анализ типов данных по расширению в сетевом трафике (текст, таблицы, видео, аудио) за счет анализа MIME заголовка;
	+ возможность настройки расписания работы правил фильтрации;
	+ регистрацию событий безопасности, связанных с фильтрацией сетевых пакетов;
	+ самотестирование функциональных возможностей МЭ;
	+ возможность выполнения режима «обучения» МЭ;
	+ контент-фильтрацию для контроля доступа к веб-сайтам, а также вывод детализированного уведомления при блокировке контента;
	+ оперативную полную блокировку и разрешение всех пакетов по команде пользователя;
	+ возможность выполнения режима «наблюдения» за журналами – обновление новых записей и перемотка на конец журнала в режиме близком к реальному времени;
	+ возможность выполнения групповых операций над правилами МЭ.

#

#  Требования к технической поддержке

Техническая поддержка программного обеспечения средства защиты от несанкционированного доступа должна предоставляться сроком на 1 год, согласно сроку действия лицензии, а также:

* Предоставляться на русском языке сертифицированными специалистами производителя программного обеспечения и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет.
* Web-сайт производителя ПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке ПО, пополняемую базу знаний, а также форум пользователей программных продуктов.
	1. **Требования к серверу безопасности**

Сервер безопасности (СБ) должен представлять собой отдельный программный модуль с аппаратным лицензионным ключом (или без аппаратного ключа при наличии дополнительных программных модулей) в операционных системах семейства Windows, предназначенный для удаленного и централизованного управления средствами защиты информации (СЗИ).

СБ должен быть предназначен для ПЭВМ типа IBM PC под управлением операционных систем Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 в многопользовательском режиме их эксплуатации.

СБ должен поддерживать 32- и 64-битные версии операционных систем.

СБ должен быть предназначен для использования на персональных компьютерах, портативных компьютерах (ноутбуках), серверах, также поддерживать виртуальные среды.

СБ должен быть сертифицирован на соответствие 4-му уровню доверия («Требования по безопасности информации, устанавливающие уровни доверия к СТЗИ и СОБИТ», ФСТЭК России, 2020), разрабатываться и производиться на основании лицензии федеральных органов, имеющих полномочия в указанной сфере.

СБ может быть использован:

* при создании защищенных автоматизированных систем до класса защищенности 1Г включительно;
* в государственных информационных системах до 1 класса защищенности включительно;
* в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно;
* в информационных системах персональных данных до 1 уровня защищенности включительно;
* при защите значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно.

СБ должен обеспечивать:

* + централизованное управление защищенными СЗИ НСД или СДЗ рабочими станциями (под управлением ОС семейств Windows и Linux) с возможностью объединения таких станций в группы. Должна поддерживаться многоуровневая иерархия групп и наследование установленных параметров;
	+ возможность централизованного управления СЗИ следующих типов: МЭ, СОВ, СКН;
	+ возможность централизованного управления жизненным циклом резервных копий объектов ФС (включая размещение резервных копий, периодичность и расписание их создания, количество сохраняемых копий, а также восстановление объектов ФС из резервных копий);
	+ возможность удаленной блокировки, выключения или перезагрузки защищенной рабочей станции, завершения сеанса работы пользователя по команде администратора;
	+ централизованное управление учетными записями пользователей и группами учетных записей пользователей на защищенных рабочих станциях;
	+ возможность по управлению доменными учетными записями (создание, удаление, блокировка, перемещение) и группами Active Directory с учетом приоритета механизмов СЗИ над механизмами Active Directory (во избежание злоупотребления доменных администраторов своими полномочиями);
	+ централизованное управление политиками безопасности СЗИ, удаленное управление доступом к ресурсам файловой системы (на основе дискреционного принципа разграничения прав доступа) на защищенных рабочих станциях;
	+ возможность выполнения групповых операций с клиентами в дереве клиентов домена безопасности;
	+ возможность настройки ролевой модели управления доступом, позволяющей разграничить права пользователей с точностью до управления отдельными функциональными блоками и до ограничения данных полномочий в рамках подразделения домена безопасности;
	+ периодический сбор журналов аудита с защищенных рабочих станций;
	+ возможность формирования отчета о событиях НСД, произошедших в рамках защищаемого контура (домена безопасности);
	+ возможность формирования отчета о зарегистрированных аппаратных идентификаторах в домене безопасности;
	+ графическое отображение состояния защищаемых рабочих станций;
	+ централизованную блокировку доступа к файлам по расширению на защищенных рабочих станциях;
	+ централизованный контроль аппаратной конфигурации защищенных рабочих станции и подключаемых устройств;
	+ централизованный контроль целостности объектов ФС, системного реестра;
	+ централизованное управление аппаратными идентификаторами;
	+ централизованное управление сессиями-исключениями;
	+ централизованное управление (регистрацию) сменных накопителей;
	+ централизованное управление преобразованными съемными носителями информации;
	+ возможность сигнализации администратору безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях:
	+ нарушение контроля целостности объекта;
	+ попытка работы после блокировки при нарушении целостности;
	+ попытка входа на клиентскую рабочую станцию с неправильным паролем;
	+ блокировка пользователя после многократного ввода неправильного пароля;
	+ СЗИ НСД на клиенте не отвечает (возможная причина − несанкционированная деактивация системы защиты);
	+ клиент недоступен долгое время (с возможностью задания периода времени);
	+ попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами.
	+ возможность автоматического оповещения о событии НСД на клиенте по электронной почте;
	+ возможность добавления произвольного комментария к событиям НСД;
	+ возможность оповещения администратора о доступных обновлениях сигнатур и «черного списка» IP-адресов;
	+ возможность визуализации сети защищаемых компьютеров;
	+ возможность настройки репликации серверов безопасности (модулей централизованного управления);
	+ возможность использования SQL базы данных для централизованного хранения событий аудита;
	+ возможность выгрузки отчета о действиях пользователя (учетной записи пользователя) на защищаемых технических средствах (ТС) из базы данных SQL;
	+ возможность построения иерархии управления при помощи специального модуля – менеджера, управляющего несколькими модулями централизованного управления (СБ);
	+ возможность удаленной установки, обновления и удаления СЗИ на рабочих станциях в составе домена безопасности с отображением сообщения об окончании удаленной установки / обновления / удаления СЗИ клиентской части СЗИ (с указанием необходимости выполнения перезагрузки) для персонального компьютера;
	+ возможность выполнять синхронизацию времени между сервером безопасности и клиентами;
	+ возможность автоматического сохранения файла конфигурации СБ по настроенному расписанию для последующего восстановления настроек;
	+ возможность мониторинга защищенности системы (защищаемого контура) с отображением оперативных данных и статистики с помощью графической панели;
	+ возможность интеграции с SIEM-системами;
	+ возможность нотификации о наличии обновлений для СБ на сервере компании-разработчика;
	+ возможность включения контроллеров домена ОС Windows в домен безопасности и дальнейшее администрирование средствами СБ;
	+ возможность включения клиентской части СЗИ в домен безопасности по IP‑адресу;
	+ возможность предоставления аналитической информации (журнал информационно-технологического сопровождения). Журнал должен хранить и отображать в консоли сервера безопасности:
	+ события по работе с заявками пользователя в службу технической поддержки;
	+ информационные сообщения, отправленные производителем.
	+ поддержку централизованного взаимодействия с Kaspersky Security Center (получение сведений о состоянии антивируса клиентских ТС, сбор журналов с клиентских ТС, получение информации об инцидентах на клиентских ТС, запуск процесса обновления антивирусных баз данных на клиентских ТС, выполнение принудительного сканирования клиентских ТС).

Реализация СБ должна быть программной с возможностью подключения аппаратного лицензионного ключа и аппаратных средств считывания индивидуальных идентификаторов пользователей, а также аппаратных идентификаторов:

* USB-флэш-накопители;
* электронные ключи Touch Memory (iButton);
* HID Proximity-карты;
* USB-ключи Aladdin eToken Pro/Java;
* смарт-карты Aladdin eToken Pro/SC;
* USB-ключи и смарт-карты Рутокен (Rutoken), Рутокен ЭЦП, Рутокен ЭЦП 2.0;
* USB-ключи и смарт-карты JaCarta, JaCarta-2, JaCarta PRO, JaCarta LT, JaCarta PKI/BIO;
* USB-ключи и смарт-карты ESMART;
* NFC-метки и смарт-карты семейства MIFARE.
	1. **Требования к установочному комплекту**

Установочный комплект должен включать в себя:

* Оригинальный дистрибутив программного обеспечения СЗИ на оптическом диске;
* Оригинальный формуляр в печатном виде: документ, подтверждающий, что данный(е) CD/DVD действительно содержат сертифицированные приложения, с уникальным номером;
* Копию сертификата соответствия ФСТЭК.

Оптические носители с установочными комплектами ПО должны поставляться в защитной от ударов упаковке и должны иметь необходимую маркировку и этикетку. Тара и упаковка должна соответствовать стандартам, техническим условиям. Упаковка не должна содержать следов вскрытия, вмятин, порезов.

* 1. **Исполнитель обязан:**

Своевременно и надлежащим образом выполнять свои обязательства, предусмотренные Контрактом.

 Гарантировать, что предоставление неисключительного права и оказание услуг по продлению технической поддержкиосуществляется с разрешения правообладателя и подтверждается соответствующими документами, представленными Государственному заказчику вместе с программным обеспечением.

Выполнить в полном объеме все свои обязательства, предусмотренные Договором, а также требования, предусмотренные действующим законодательством.

1. **Условия оказания услуг:**

**3.1.** Исполнитель предоставляет заказчику документы, подтверждающие наличие у исполнителя необходимых прав на использование технологий и иных результатов интеллектуальной деятельности: копию Лицензионного соглашения с правообладателем на право оказания услуг заказчику в объеме согласно требованиям настоящего Технического задания, либо копию свидетельства о государственной регистрации программы, в котором исполнитель является правообладателем программы.

Исполнитель гарантирует, что программное обеспечение свободно от прав третьих лиц, не обременено залогом, притязаниями третьих лиц. При оказании услуг исполнителем не распространяются материалы, информация, запрещённые или ограниченные к распространению, нарушающие права граждан или юридических лиц.

**3.2. Требования к документированию**

Программное обеспечение должно содержать в своем составе следующую документацию на русском языке:

* руководство пользователя;
* руководство по установке;
* руководство по администрированию;
* системные требования.

**3.3. Требования к технической поддержке и обновлению версий**

Право использовать программное обеспечение должно включать обеспечение технической поддержки бессрочно с даты подписания сторонами акта сдачи-приемки оказанных услуг посредством использования телефонной связи и средств электронной почты на русском языке в круглосуточном режиме, в том числе включающей выпуск критических и иных исправлений к указанному программному обеспечению.

**4**. **Требования к качеству оказания услуг:**

Функциональные, технические и качественные характеристики, эксплуатационные характеристики услуг должны соответствовать действующему законодательству Российской Федерации, условиям договора, Техническому заданию.

**5. График оказания услуг**: не исключительное право на использование ПО предоставляются исполнителем заказчику в течении 5 (пяти) рабочих дней с момента получения лицензиаром вознаграждения – авансового платежа в размере 50 (пятьдесят) % от стоимости по настоящему договору.

Лицензии на право использовать компьютерное программное обеспечение предоставляются исполнителем заказчику бессрочно.

**6. Место оказания услуг:** 676282, Российская Федерация, Амурская область, город Тында, улица Красная Пресня, дом 59.

**7. Условия, запреты и ограничения услуг, оказываемых иностранными лицами (в соответствии со статьей 14 Федерального закона от 05.04.2013 №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»):** установлен запрет в соответствии с постановлением Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

Программист А.М. Гаетбаев