**Описание объекта закупки (техническое задание)**

1. Поставляемый товар должен соответствовать требованиям законодательства Российской Федерации.

2. Поставляемый товар должен быть новым. Поставляемый товар должен быть свободным от прав третьих лиц.

3. Поставляемый товар не должен иметь дефектов, связанных с конструкцией, материалами или работой по их изготовлению.

4. Гарантийный срок товара должен составлять не менее 1 (одного) года с момента подписания Заказчиком акта о приемке результатов исполнения государственного контракта.

5. Гарантийное обслуживание осуществляется силами и за счет средств Поставщика, включая доставку, замену, ремонт и т.п., без каких-либо дополнительных расходов со стороны Заказчика.

6. При использовании товара по назначению не должно создаваться угрозы для жизни и здоровья потребителя, окружающей среды, а также использование товара не должно причинять вред имуществу Заказчика.

7. Товар должен поставляться в фирменной упаковке, защищающей от повреждений и воздействия внешней среды.

8. Отгрузка товара должна осуществляться в здание по адресу: Санкт-Петербург, ул. Малая Монетная, д.2 лит.Ч, в помещения, указанные Заказчиком. Время доставки товара должно быть согласовано с Заказчиком.

9. Поставляемый товар должен иметь в своем составе средство защиты от несанкционированного доступа и модуль доверенной загрузки, который функционирует до начала загрузки операционной системы и выполняет, как минимум, следующие функции:

– предотвращение несанкционированного доступа к ресурсам компьютера;

– идентификация и аутентификация пользователей при допуске к средствам вычислительной техники (СВТ), к встроенным модулям настройки и администрирования средства защиты информации по уникальному персональному идентификатору пользователя и по паролю временного действия длиной от 0 до 12 буквенно-цифровых символов, введенных с клавиатуры;

– предотвращение загрузки операционной системы с внешнего носителя (FDD, CD ROM, ZIP Drive, USB-накопителей);

– контроль целостности программной среды компьютера с поддержкой файловых систем FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, VMFS3, VMFS5 (ESXi).

– контроль целостности загружаемой операционной системы (объектов файловой системы, областей жесткого диска, реестра) и блокировку загрузки ОС при нарушении целостности контролируемых объектов;

– контроль состава компонентов аппаратного обеспечения ЭВМ (в том числе BIOS CMOS) и блокировка загрузки операционной системы при обнаружении несанкционированного изменения состава аппаратных компонентов ЭВМ;

– обеспечение режима двухфакторной аутентификации пользователей и возможности добавления не менее 30 пользователей;

– обеспечение функциональной возможности «сторожевого таймера» или подключение сторожевого таймера через разъём «Power» на ЭВМ;

– обеспечение перезагрузки СВТ при выявлении попыток обхода модуля доверенной загрузки;

– наличие датчиков вскрытия корпуса, для обеспечения блокировки входа в систему при вскрытии корпуса;

– наличие собственных часов с независимым источником питания;

– ведение журнала регистрации в энергонезависимой памяти устройства. Журнал регистрации должен содержать информацию о следующих событиях:

* + - успешная аутентификация;
    - неуспешная аутентификация;
    - нарушение целостности во время проверки списков контроля целостности программной среды компьютера;
    - аудит действий администратора;
    - Хранение ключевой, служебной и другой необходимой информации в энергонезависимой памяти платы;
    - Администрирование модуля доверенной загрузки должно проводиться без использования ресурсов загружаемой штатной ОС.

Программные компоненты средства защиты от несанкционированного доступа должны интегрироваться в состав операционной системы и выполнять следующие функции:

– временная блокировка экрана и клавиатуры по команде пользователя или по истечению установленного интервала «неактивности» пользователя;

– создание и поддержка изолированной программной среды, а также возможность реализации функционально замкнутых информационных систем;

– формирование списков контроля целостности элементов программной среды компьютера (логических дисков, каталогов и файлов), индивидуальных для каждого пользователя, или группы пользователей;

– регистрация событий доступа (в том числе несанкционированных) к ресурсам компьютера;

– очистка освобождаемой оперативной памяти и дискового пространства на стационарных и внешних носителях;

– контроль печати документов, протоколирование процесса печати и маркировка распечатываемых листов специальными пометками, грифами;

– аутентификация пользователей встроенного средства защиты от несанкционированного доступа должна проводиться с помощью идентификаторов одного из следующих типов: электронный ключ (iButton), USB идентификатор, электронный ключ считывателей CCID со смарт-картами, смарт-карты и USB-токены ESMART.

Встроенный модуль доверенной загрузки должен сохранять работоспособность во всех случаях замены операционной системы, вне зависимости от типа устанавливаемой/переустанавливаемой операционной системы.

Средство защиты от несанкционированного доступа должно обеспечивать выполнение требований руководящих документов:

– «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации» (Гостехкомиссия России, 1992 г.) – по 5 классу защищенности;

– «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 уровня контроля.

Средство защиты от несанкционированного доступа должно обеспечивать возможность использования при создании автоматизированных систем до класса защищенности 1Г включительно и для защиты информации в информационных системах персональных данных до 1 уровня защищенности включительно.

Средство защиты от несанкционированного доступа должно иметь в своем составе:

– Предустановленное программное обеспечение, реализующее возможность мультифакторной аутентификации;

– Предустановленное программное обеспечение, позволяющее ограничивать доступ к внешним устройствам, в соответствии с политиками доступа;

– Предустановленное программное обеспечение для безопасного удаления файлов;

– Предустановленное программное обеспечение для поддержки надлежащего уровня производительности и задания настроек системы.

10. На системный блок должна быть предустановлена и активирована лицензионная операционная система, сертифицированная Федеральной службой по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) по требованиям безопасности информации, в комплекте с лицензионным носителем информации (дистрибутивом).

Для сертифицированного программного обеспечения должно быть обеспечено получение обновлений, прошедших соответствующие проверки в испытательных лабораториях, на физическом носителе, либо через Интернет по защищенным каналам.

Должен быть поставлен базовый пакет для сертифицированной версии операционной системы, обеспечивающий выполнение основных требований руководящих и нормативных документов по защите конфиденциальной информации и персональных данных, применяющийся в качестве сертифицированного средства защиты информации от НСД для построения автоматизированных систем, показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – по классу защищенности не ниже 5 и должен иметь возможность использоваться при создании автоматизированных систем до класса защищенности 1Г включительно и при создании информационных систем персональных данных до 2 класса включительно.

Вместе с товаром должна быть поставлена лицензия на использование программы контроля сертифицированной версии операционной системы.

Вместе с товаром должен быть предоставлен пакет эксплуатационной документации, формуляр на сертифицируемое программное обеспечение, промаркированный Голографическим специальным знаком соответствия ФСТЭК России, формуляр на программу контроля сертифицированной версии программного обеспечения Check и гарантийный талон.

Все лицензии на поставляемое программное обеспечение должны быть бессрочными, то есть не должны содержать ограничений по срокам на использование лицензиатом данных программных продуктов.

Приложение 1

Характеристики товара

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Наименование объекта закупки по КТРУ** | **Наименование характеристики** | **Значение характеристики** | **Единица измерения характеристики** | **ГОСТ, технический регламент/обоснование показателя (в том числе его характеристика)** | **Кол-во, шт.** |
| Системный блок | тип процессора - Х86 не более 4 ядер | наличие |  | Соответствие приказу Фонда от 15.09.2017 г. № 425 | 23 |
| частота процессора, ГГц | не менее 3 и не более 4 |
| Объем оперативной памяти | 16 | Гигабайт | В соответсвие с КТРУ |
| объем накопителя | 1 | Терабайт | В соответсвие с КТРУ |
| тип жесткого диска - HDD и/или SSD | наличие |  |  |
| оптический привод - встроенный привод не ниже DVD-R и не выше BD-RW | наличие |
| тип видеоадаптера - интегрированный и/или дискретный | наличие |
| Предустановлена и активирована операционная система не ниже Microsoft Windows 7 Pro (русская версия) и не выше Microsoft Windows 10 Pro (русская версия) | наличие |
| Сертификат Федеральный службы по техническому и экспортному контролю РФ (ФСТЭК) на операционную систему | наличие |
| Лицензия на использование программы контроля сертифицированной версии операционной системы | наличие |
| Лицензионный дистрибутив операционной системы, соответствующий требованиям ФСТЭК | наличие |
| Средство защиты от несанкционированного доступа и аппаратно-программный модуль доверенной загрузки | наличие |
| Датчики вскрытия корпуса, обеспечивающие блокировку входа в систему при вскрытии корпуса | наличие |
| Форм-фактор - Slim-Desktop | наличие |