**ПРИЛОЖЕНИЕ № 2**

к государственному контракту № \_\_\_\_\_\_\_\_\_\_\_\_

от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2020г.

**ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ (КОМПЛЕКТАЦИЯ, ФУНКЦИОНАЛЬНЫЕ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ТОВАРА)**

| **№ п/п** | **Наименование товара (с указанием марки, модели)** | ОКПД 2 ОК 034-2014 (КПЕС 2008) или код позиции КТРУ | **Ед. изм.** | **Кол-во** |
| --- | --- | --- | --- | --- |
| 1 | Системный блок | 26.20.15.000 | Штука | 279 |
| 2 | Системный блок | 26.20.15.000 | Штука | 415 |
| 3 | Монитор, подключаемый к компьютеру | 26.20.17.110-00000011 | Штука | 694 |
| 4 | Клавиатура | 26.20.16.110-00000002 | Штука | 694 |
| 5 | Мышь компьютерная | 26.20.16.170-00000002 | Штука | 694 |
| 6 | Источник бесперебойного питания | 26.20.40.110-00000009 | Штука | 694 |
| 7 | Фильтр сетевой | 26.20.40.190 | Штука | 694 |

**Общие требования:** Поставляемое компьютерное оборудование со средствами защиты информации предназначено для организации работы медицинского персонала учреждений здравоохранения Республики Алтай в региональном сегменте Единой государственной информационной системы в сфере здравоохранения (РС ЕГИСЗ) и должно быть совместимо с существующей у Заказчика системой управления и эксплуатацией, и системой информационной безопасности. Программное обеспечение в составе системного блока должно быть установлено и настроено для работы в медицинской информационной системе Заказчика. Установка и настройка средств защиты информации, поставляемых в рамках исполнения обязательств по контракту, должна выполнена в соответствии с требованиями руководящих документов ФСТЭК России.

Установка и настройка средств защиты информации должна включать:

установку и настройку программного модуля доверенной загрузки: -проведение испытаний совместимости с аппаратной платформой; -установка программного модуля доверенной загрузки; -настройка служебных параметров в соответствии с требованиями руководящих документов ФСТЭК России; -создание пользователей;- настройка пользователей; -тестирование корректности установки и настройки программного модуля доверенной загрузки.

установку и настройку средства защиты информации от несанкционированного доступа: -проведение испытаний совместимости с операционной системой; -установка Средство защиты информации от несанкционированного доступа; -настройка служебных параметров в соответствии с требования руководящих документов ФСТЭК России; -создание пользователей; -настройка пользователей; -настройка подсистем регистрации и учета; -настройка зачистки информации; -настройка контроля целостности; -тестирование корректности установки и настройки.

Установка и наладка средств защиты информации в составе системного блока должна производиться специализированной организацией, имеющей право на работы по технической защите конфиденциальной информации.

Поставщик в течении 5 (пяти) календарных дней с даты заключения Контракта должен предоставить Заказчику:

Копию действующей лицензии ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации (согласно п.5 ч.1 статьи 12 Федерального закона от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности», Постановления Правительства Российской Федерации от 03.02.2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (пп. е п. 4 - услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).)), выданной Исполнителю, или партнерское соглашение (договор) с соисполнителем, имеющим вышеуказанную лицензию, с приложением её копии.

Копию действующего сертификата соответствия ФСТЭК России, подтверждающего возможность использования Средства защиты информации от несанкционированного доступа:

- в государственных информационных системах до 2 класса защищенности включительно;

- в информационных системах персональных данных до 2 уровня защищенности включительно

Копию действующего сертификата соответствия ФСТЭК России, подтверждающего возможность использования модуля доверенной загрузки:

* в государственных информационных системах до 2 класса защищенности включительно;
* в информационных системах персональных данных до 2 уровня защищенности включительно.

**Сроки поставки товара или завершения работы либо график оказания услуг**: Поставка должна быть осуществлена в полном объеме в течение 60 рабочих дней с момента заключения Контракта по адресу Получателей товара согласно Приложения №4 к настоящему контракту.

Поставщик за 5 рабочих дней до осуществления поставки Товара направляет Заказчику уведомление о дате фактической передачи Товара, по адресу электронной почты, либо с использованием иных средств связи и доставки, обеспечивающих фиксирование такого уведомления и получение Поставщиком подтверждения о его вручении Заказчику и Получателю.

**Требования к гарантийному сроку и (или) объему предоставления гарантий качества товара, работы, услуги:** Гарантийный срок на поставляемое оборудование составляет 36 месяцев и исчисляется с момента подписания Сторонами акта приема-передачи товара и распространяется на весь поставленный объем.

Поставщик гарантирует, что все средства защиты информации, поставляемые в рамках исполнения обязательств по контракту, установлены и настроены в соответствии с требованиями руководящих документов ФСТЭК России. В случае сбоев в работе средств защиты информации, произошедших по вине Поставщика, Поставщик гарантирует что в течение всего гарантийного срока, при необходимости Поставщиком либо субподрядной организацией, будет произведена установка и наладка средств защиты информации. Работы должны быть проведены в течении 5 (пяти) рабочих дней, с момента обращения Заказчика, по адресу Республика Алтай, г.Горно-Алтайск, пр.Коммунистический,54 в соответствии с требованиями руководящих документов ФСТЭК России.

**Функциональные, технические и качественные характеристики товара, работы, услуги, эксплуатационные характеристики товара, результата работы, услуги (при необходимости), используемые для определения соответствия потребностям заказчика или эквивалентности предлагаемого к поставке или к использованию при выполнении работ, оказании услуг товара максимальные и (или) минимальные значения показателей товара и показатели, значения которых не могут изменяться**

Таблица № 1.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Наименование товара, его количество | Наименование показателя  товара | Ед. изм. | Значение показателя товара, которое не может изменяться участником закупки при подаче заявки | Значение показателя товара,  при определении которого участником закупки используются только точные цифровые или иные параметры | Значение показателя товара,  при определении которого участником закупки могут не использоваться точные цифровые или иные параметры | Обоснование характеристик, запрошенных дополнительно к стандартным по КТРУ |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1. | Системный блок, 279 штук | Корпус |  |  |  |  |  |
|  |  | Материал стенок корпуса |  | Сталь |  |  | Для повышения надежности |
|  |  | Толщина стенок корпуса | мм |  | ≥ 0,6 |  | Для надежной шумоизоляции |
|  |  | Мощность блока питания | Вт |  | ≤ 200 |  | Для обеспечения работоспособности всех компонентов системного блока |
|  |  | Крепление VESA |  | Наличие |  |  | Для удобства размещения |
|  |  | Габариты (ШхВхГ) | мм |  | ≤ 97x240x250 |  | Для удобства размещения |
|  |  | Физическая энергонезависимая блокировка доступа к внутренним компонентам системного блока с ключевым доступом без использования навесных снимаемых замков. |  | Наличие |  |  | Для повышения надежности |
|  |  | Блокировка самопроизвольной отстыковки кабеля электропитания 220 В. |  | Наличие |  |  | Для повышения надежности |
|  |  | Электромеханическое устройство, обеспечивающее защиту от несанкционированного включения ПК |  | Выключатель с ключом на лицевой панели (не должно занимать отсеков 5,25 и 3,5 дюйма) |  |  | Для повышения надежности |
|  |  | Процессор |  |  |  |  |  |
|  |  | Тактовая частота | Мгц |  | ≥ 3600 |  | Для высокой производительности |
|  |  | Объем кэша L3 | Кб |  | > 6000 |  | Для высокой производительности |
|  |  | Количество ядер | Шт |  | ≥ 4 |  | Для высокой производительности |
|  |  | Количество потоков | Шт |  | ≥ 4 |  | Для высокой производительности |
|  |  | Встроенная графическая система |  | Наличие |  |  | Для обработки графической информации |
|  |  | Система охлаждения |  | Наличие |  |  | Для защиты от перегрева процессора |
|  |  | Оперативная память |  |  |  |  |  |
|  |  | Количество модулей | Шт |  | ≥ 2 |  | Для обеспечения работоспособности системного блока |
|  |  | Объем оперативной памяти | Гб |  | ≥ 8 |  | Для обеспечения нужд заказчика |
|  |  | Частота оперативной памяти | Мгц |  | ≥ 2400 |  | Частота, обеспечивающая наименьшее энергопотребление и тепловыделение из производимых на данный момент типов памяти |
|  |  | Тип |  | DDR4 |  |  | Для поддержания высокой производительности работы |
|  |  | Накопитель |  |  |  |  |  |
|  |  | Тип накопителя |  | SSD |  |  | Для обеспечения нужд заказчика |
|  |  | Объем SSD | Гб |  | ≥ 240 |  | Для обеспечения нужд заказчика |
|  |  | Системная плата |  |  |  |  |  |
|  |  | Количество слотов памяти | Шт |  | ≥ 2 |  | Для установки оперативной памяти |
|  |  | Количество слотов расширения PCI-E x16 |  |  | ≥ 1 |  | Для установки плат расширения |
|  |  | Сеть | Мбит/с |  | ≥ 1000 |  | Для подключения к локальной сети |
|  |  | Количество портов USB | Шт |  | ≥ 8 |  | Для подключения устройств ввода/вывода |
|  |  | Интерфейсы |  | DVI, HDMI, DisplayPort |  |  | Для подключения устройств ввода/вывода |
|  |  | Отсек для установки привода оптических дисков |  | Наличие |  |  | Для возможности установки привода оптических дисков |
|  |  | Система контроля несанкционированного перемещения корпуса системного блока,  фиксирующая факт изменения местоположения корпуса при его отклонении от точки установки не более чем на 2 см в трех плоскостях. |  | Налиие |  |  | В целях предотвращения хищения информации и оборудования |
|  |  | Функции звукового оповещения о факте несанкционированного перемещения корпуса системного блока. |  | Налиие |  |  | В целях предотвращения хищения информации и оборудования |
|  |  | Программный модуль доверенной загрузки (ПМДЗ) |  |  |  |  |  |
|  |  | Функциональные требования |  | ПМДЗ должен представлять собой программное средство, которое встраивается в базовую систему ввода-вывода (BIOS) и осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, предоставляет доступ к информационным ресурсам в случае успешной проверки подлинности загружаемой операционной системы и прав на основе идентификации и аутентификации пользователя.  ПМДЗ должен обеспечивать контроль завершенности транзакций в журналах файловых систем EXT3, EXT4 и контроль программных прерываний системного режима управления (SMI)  ПМДЗ должен иметь возможность задать настройки сессии аутентификации  ПМДЗ должен иметь возможность обеспечения загрузки корневых сертификатов и списка отзыва сертификатов  ПМДЗ должен иметь возможность импорта и экспорта настроек  ПМДЗ должен вести аудит действий пользователя и администратора. Все события должны записывать в журнал. Режимы ведения журнала:   * Внутренний, циклический; * Внутренний, экспортируемый; * Внешний (на диске).   ПМДЗ должен обеспечивать защиту BIOS от перезаписи, чтения и от изменения EFI-переменных.  Активация/деактивация ПМДЗ должна осуществляться программно, без механических операций вскрытия и установки/извлечения компонентов.  Обновление ПМДЗ должно производиться программно, из меню настроек замка. |  |  | Для построения системы защиты информации |
|  |  | Требования к обеспечению контроля целостности |  | ПМДЗ должен обеспечивать контроль целостности, следующих компонентов:   * образа BIOS и программного обеспечения ПМДЗ; * файлов на файловых системах: EXT2, EXT3, EXT4; * MBR на носителях информации; * таблиц ACPI; * таблиц SMBIOS; * карты распределения памяти; * ресурсов конфигурационного пространства PCI/PCIe; * контроль целостности CMOS (содержимого энергонезависимой памяти). |  |  | Для построения системы защиты информации |
|  |  | Требования к аутентификации |  | ПМДЗ должен обеспечивать двухфакторную аутентификацию в том числе и с применением сертификатов электронной подписи (далее – ЭП). Авторизация должна происходить на уровне BIOS до загрузки основных компонентов операционной системы. Должны поддерживаться следующие способы аутентификации:   * пароль; * электронный идентификатор с сертификатом; * сочетание способов электронный идентификатор и пароль; * пароль на электронном идентификаторе; * пароль на LDAP; * сертификат на LDAP;   ПМДЗ должен поддерживать токены – Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken Lite, JaCarta PKI, Guardant ID, JaCarta-2 ГОСТ  ПМДЗ должен обеспечивать возможность аутентификации пользователей в LDAP, в том числе и по сертификатам |  |  | Для выполнения требований по защите информации в соответствии с Приказом ФСТЭК России от 18 февраля 2013г №21, приказом ФСТЭК России от 11 февраля 2013г №17. |
|  |  | Требования по нейтрализации угроз информационной безопасности |  | ПМДЗ должен обеспечивать нейтрализацию следующих угроз безопасности информации:   * несанкционированный доступ к информации за счет загрузки нештатной операционной системы и, тем самым, обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы; * несанкционированную загрузку штатной операционной системы и получение несанкционированного доступа к информационным ресурсам; * нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе; * нарушение целостности программного обеспечения средства доверенной загрузки; * отключение и (или) обход нарушителями компонентов средств доверенной загрузки; * несанкционированное изменение конфигурации (параметров) средства доверенной загрузки; * преодоление или обход функций безопасности средств доверенной загрузки; * получение остаточной информации средства доверенной загрузки из памяти средства вычислительной техники после завершения работы средства доверенной загрузки; * получение доступа к ресурсам средства доверенной загрузки из программной среды средства вычислительной техники после завершения работы средства доверенной загрузки. |  |  | Для построения системы защиты информации |
|  |  | Требования к централизованному наблюдению |  | ПМДЗ должен поддерживать функции информационного взаимодействия с программным обеспечением, реализующим функции централизованного лицензирования и сбора журналов, в части:   * передачи информации об установленной версии ПМДЗ; * передачи IP-адреса устройства, на котором установлен ПМДЗ; * удалённая регистрация лицензий, с возможностью группового лицензирования; * выгрузки журналов ПМДЗ, с возможностью групповой выгрузки |  |  | Для получения оперативной информации о текущем состоянии функционирующих в системе ПМДЗ |
|  |  | Требования к сертификации |  | Модуль доверенной загрузки должен иметь действующий сертификат соответствия ФСТЭК России, позволяющий использовать:  - в государственных информационных системах до 2 класса защищенности включительно;  - в информационных системах персональных данных до 2 уровня защищенности включительно. |  |  | Приказ ФСТЭК России от 18 февраля 2013г №21.  В соответствии с п.11 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах утвержденных приказом ФСТЭК России от 11 февраля 2013г №17. |
|  |  | Средство защиты информации от несанкционированного доступа |  |  |  |  |  |
|  |  | Функциональные требования |  | Средство защиты информации от несанкционированного доступа (СЗИ НСД) должно обеспечивать выполнение следующих функций: регистрацию пользователей. Возможность задать пароль пользователя. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества сессий пользователей на одном компьютере; возможность принудительной блокировки пользователей и автоматической блокировки в случае нарушения политик безопасности;  идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной аутентификации по паролю и аппаратному идентификатору; возможность сохранения авторизационных данных пользователя на аппаратном идентификаторе;реализацию настроек сложности паролей (длины парольной строчки, контроля наличия цифр и специальных символов) и срока их действия; возможность настройки разграничения прав доступа к объектам файловой системы, съемным накопителям, разграничения прав на доступ к устройствам печати;возможность контроля целостности аппаратной конфигурации компьютера;регистрацию и учет (аудит) действий пользователей (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, вывод на печать информации, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки записей;  возможность периодического архивирования журналов событий;  возможность экспорта журналов безопасности в форматы PDF и ODS;возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);возможность администрирования через графическую оболочку СЗИ НСД, функционирующую в операционных системах на базе Linux;  возможность контроля целостности программно-аппаратной среды (в том числе отдельных каталогов) и произвольных объектов файловой системы при загрузке ПЭВМ, по команде администратора или периодически. Возможность восстановления объекта доступа в случае обнаружения нарушения его целостности;  контроль целостности объектов СЗИ;  очистку остаточной информации (освобождаемого дискового пространства, освобождаемых областей оперативной памяти, зачистку определенных файлов и папок по команде пользователя); возможность проверки корректности функционирования СЗИ НСД, самотестирования;  защиту от подмены ядра операционной системы и процедур инициализации;  возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;  возможность синхронизации времени с аппаратной платой средства доверенной загрузки для регистрации событий безопасности;  возможность сетевого режима функционирования c удаленным управлением учетными записями пользователей, получением информации о состоянии работы защищаемых ПЭВМ, удаленным просмотром журналов на ПЭВМ, входящих в домен безопасности;  централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должна выполняться синхронизация учетных записей в рамках защищаемого контура, синхронизация политик безопасности, удаленное развертывание и удаление клиентских частей СЗИ НСД;  возможность оповещения при некоторых событиях НСД;  наличие собственного механизма дискреционного управления доступом.  СЗИ НСД должен быть включен в Единый реестр российских программ для электронных вычислительных машин и баз данных в соответствии с постановлением Правительства РФ от 16 ноября 2015 г. N 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд". |  |  | Для построения системы защиты информации |
|  |  | Требования к сертификации |  | СЗИ НСД должно иметь действующий сертификат, соответствия ФСТЭК России, позволяющий использовать:  - в государственных информационных системах до 2 класса защищенности включительно;  - в информационных системах персональных данных до 2 уровня защищенности включительно |  |  | Приказ ФСТЭК России от 18 февраля 2013г №21.  В соответствии с п.11 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах утвержденных приказом ФСТЭК России от 11 февраля 2013г №17. |
|  |  | Операционная система «Astra Linux Common Edition» \* |  |  |  |  |  |
|  |  | Функциональные требования |  | Операционная система для рабочих станций должна отвечать следующим требованиям и обеспечивать:  возможность задания хешей паролей пользователей в соответствии с ГОСТ Р 34.11-2012;  возможность создания ssh-тунелей с кодированием передаваемой информации в соответствии с ГОСТ Р 34.12–2015  возможность создания защищенных VPN-тунелей, использующих контроль целостности заголовков IP-пакетов в соответствии с **ГОСТ** Р 34.12–**2015**  позволять выполнять защитное преобразование файлов и каталогов по ГОСТ Р 34.12–2015 встроенное в файловый менеджер;  возможность ограничения полномочий пользователей по использованию консолей;  возможность ограничения работы с интерпретируемыми языками для непривилегированных пользователей  возможность блокировки макросов в приложениях  иметь в составе ядро не ниже 4.15 и актуальный набор драйверов для совместимости с имеющимся периферийным оборудованием и обеспечения корректного функционирования современных средств вычислительной техники.  графическое средство настройки выделяемых ресурсов памяти пользователям (квоты)  графическое средство ввода рабочей станции в домены Active Directory и FreeIPA  графические средства настройки подключения к сетевой файловой системе Samba  графическое средство настройки сохранения и восстановления сессии пользователя (восстановление при старте запущенных программ и их расположения после полного отключения электропитания АРМ).  графическое средство настроек потребления электроэнергии (яркость экрана, потухание или выключение монитора, переход в ждущий режим, сон или гибернацию) в случае изменения настроек электропитания (питание от сети, питание от батареи, низкий заряд батареи) с возможностью мгновенного тестирования настроек.  графические средства запуска работы с удаленными, отдельными или вложенными графическими сессиями  графические средства настройки планирования времени завершения работы без участия пользователя (завершение сессии, выключение АРМ, перехода в энергосберегающие режимы) с настройкой уведомления о событии.  возможность автоматического брендирования рабочего стола с графическими инструментами настройки расположения логотипа.  возможность ввода логина и пароля пользователя как при входе в систему, так и при разблокировке экрана после бездействия, как с физической, так и с виртуальной клавиатуры  графический инструмент регулировки яркости экрана ноутбука или мобильных устройств  графические средства запуска приложений с изменением приоритета выполнения, либо от имени другого пользователя без доступа к консоли.  графический инструмент настройки параметров загрузчика операционной системы(загружаемая операционная система по умолчанию, передаваемые параметры ядра, таймаут для ожидания действий пользователя, выбора источника ввода данных при загрузке, выбор терминала для вывода информации).  поставляться с интернет-браузером, с поддержкой ГОСТ TLS (при наличии установленного в ОС комплекта программ КриптоПро CSP)  Графический менеджер файлов должен обеспечивать:  возможность расчета контрольных сумм файлов и их сравнения по алгоритмам ГОСТ Р 34.11-2012, MD5, SHA1, SHA256 без доступа к консоли.  поиск файлов как по шаблону, так и по содержимому в документах формата ODF, а также по времени создания или изменения, а также размеру файла без доступа к консоли..  создания из контекстного меню архивации файлов или каталогов с возможностью создания многотомного архива, архива с паролем и выбора степени сжатия данных без доступа к консоли.  Файловый менеджер должен обеспечивать:  возможность работать с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso), как с папками (с возможностью как замены файлов так и работы в режиме только чтение)  без доступа к консоли.  поддержку работы с файловыми системами ext2/3/4, fat,ntfs, iso9660.  Операционная система должна быть включена в Единый реестр российских программ для электронных вычислительных машин и баз данных в соответствии с постановлением Правительства РФ от 16 ноября 2015 г. N 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд". |  |  | Для обеспечения работоспособности |
|  |  | Требования к составу программного обеспечения |  | Для обеспечения совместимости с существующей инфраструктурой Заказчика и медицинских организаций, а также функционирования медицинской информационной системы, должно быть установлено следующее программное обеспечение: Крипто Про CSP версии 5 (Лицензии приобретаются Заказчиком отдельно); VipNet Client версии 4.х (Лицензии приобретаются Заказчиком отдельно); Агент Zabbix (свободно распространяемое программное обеспечение). Поставщик должен предоставить образ для восстановления. |  |  | Для обеспечения совместимости с существующей инфраструктурой и имеющимися у Заказчика лицензиями. |
|  |  | Корпоративный браузер «Спутник». \* |  |  |  |  |  |
|  |  | Функциональные требования |  | Браузер должен отвечать следующим требованиям:   * Поддержка отображения: веб-документов, созданных в соответствии со спецификацией XML; популярных открытых аудио и видео-форматов (Ogv, Ogg, WebM); популярных графических форматов (PNG, JPEG, GIF); документов других форматов (например, PDF) при использовании специально подключаемых модулей (расширений для интернет-обозревателя). * Использование «умной» адресной строки (ввод URL-адреса приводит к открытию соответствующего веб-сайта, ввод поискового запроса приводит к открытию страницы с результатами поиска в текущей выбранной поисковой системе). * Восстановление последних закрытых вкладок. * Блокирование установки плагинов. * Оффлайн инсталляция. * Прямой доступ к web-ресурсам (виджеты на главной). * Поддержка отечественной криптографии. * Поддержка установки защищенного соединения с информационным системам и ресурсам по протоколу TLS 1.0 и TLS 1.2 с использованием российских криптографических алгоритмов (хеш-функция - ГОСТ Р 34.11-2012, шифрование – ГОСТ 28147-89, ЭП – ГОСТ Р 34.10-2012).   Защищенный браузер должен быть включен в Единый реестр российских программ для электронных вычислительных машин и баз данных, в соответствии с постановлением Правительства РФ от 16 ноября 2015 г. N 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд" |  |  | Для обеспечения работоспособности и совместимости с медицинской информационной системой |
| 2. | Системный блок, 415 штук | Корпус |  |  |  |  |  |
|  |  | Материал |  | Сталь |  |  | Для повышения надежности |
|  |  | Толщина стенок корпуса | мм |  | ≥ 0,6 |  | Для надежной шумоизоляции |
|  |  | Мощность блока питания | Вт |  | ≤ 200 |  | Для обеспечения работоспособности всех компонентов системного блока |
|  |  | Крепление VESA |  | Наличие |  |  | Для удобства размещения |
|  |  | Габариты (ШхВхГ) | мм |  | ≤ 97x240x250 |  | Для удобства размещения |
|  |  | Физическая энергонезависимая блокировка доступа к внутренним компонентам системного блока с ключевым доступом без использования навесных снимаемых замков. |  | Наличие |  |  | Для повышения надежности |
|  |  | Блокировка самопроизвольной отстыковки кабеля электропитания 220 В. |  | Наличие |  |  | Для повышения надежности |
|  |  | Электромеханическое устройство, обеспечивающее защиту от несанкционированного включения ПК |  | Выключатель с ключом на лицевой панели (не должно занимать отсеков 5,25 и 3,5 дюйма) |  |  | Для повышения надежности |
|  |  | Процессор |  |  |  |  |  |
|  |  | Тактовая частота | Мгц |  | ≥ 3600 |  | Для высокой производительности |
|  |  | Объем кэша L3 | Кб |  | > 6000 |  | Для высокой производительности |
|  |  | Количество ядер | Шт |  | ≥ 4 |  | Для высокой производительности |
|  |  | Количество потоков | Шт |  | ≥ 4 |  | Для высокой производительности |
|  |  | Встроенная графическая система |  | Наличие |  |  | Для обработки графической информации |
|  |  | Система охлаждения |  | Наличие |  |  | Для защиты от перегрева процессора |
|  |  | Оперативная память |  |  |  |  |  |
|  |  | Количество модулей | Шт |  | ≥ 2 |  | Для обеспечения работоспособности системного блока |
|  |  | Объем оперативной памяти | Гб |  | ≥ 8 |  | Для обеспечения нужд заказчика |
|  |  | Частота оперативной памяти | Мгц |  | ≥ 2400 |  | Частота, обеспечивающая наименьшее энергопотребление и тепловыделение из производимых на данный момент типов памяти |
|  |  | Тип |  | DDR4 |  |  | Для поддержания высокой производительности работы |
|  |  | Накопитель |  |  |  |  |  |
|  |  | Тип накопителя |  | SSD |  |  | Для обеспечения нужд заказчика |
|  |  | Объем SSD | Гб |  | ≥ 240 |  | Для обеспечения нужд заказчика |
|  |  | Системная плата |  |  |  |  |  |
|  |  | Количество слотов памяти | Шт |  | ≥ 2 |  | Для установки оперативной памяти |
|  |  | Количество слотов расширения PCI-E x16 |  |  | ≥ 1 |  | Для установки плат расширения |
|  |  | Сеть | Мбит/с |  | ≥ 1000 |  | Для подключения к локальной сети |
|  |  | Количество портов USB | Шт |  | ≥ 8 |  | Для подключения устройств ввода/вывода |
|  |  | Интерфейсы |  | DVI, HDMI, DisplayPort |  |  | Для подключения устройств ввода/вывода |
|  |  | Отсек для установки привода оптических дисков |  | Наличие |  |  | Для возможности установки привода оптических дисков |
|  |  | Система контроля несанкционированного перемещения корпуса системного блока,  фиксирующая факт изменения местоположения корпуса при его отклонении от точки установки не более чем на 2 см в трех плоскостях. |  | Налиие |  |  | В целях предотвращения хищения информации и оборудования |
|  |  | Функции звукового оповещения о факте несанкционированного перемещения корпуса системного блока. |  | Налиие |  |  | В целях предотвращения хищения информации и оборудования |
|  |  | Требования к составу программного обеспечения |  | Для обеспечения совместимости с существующей инфраструктурой Заказчика и медицинских организаций, а также функционирования медицинской информационной системы, должно быть установлено следующее программное обеспечение: Операционная система «Astra Linux Common Edition» (Лицензия предоставляется Заказчиком); Корпоративный браузер «Спутник». (Лицензия предоставляется Заказчиком); Крипто Про CSP версии 5 (Лицензии приобретаются Заказчиком отдельно);  VipNet Client версии 4.х (Лицензии приобретаются Заказчиком отдельно);  Агент Zabbix (свободно распространяемое программное обеспечение).  Поставщик должен предоставить образ для восстановления. |  |  | Для обеспечения совместимости с существующей инфраструктурой и имеющимися у Заказчика лицензиями |
|  |  | Программный модуль доверенной загрузки (ПМДЗ) |  |  |  |  |  |
|  |  | Функциональные требования |  | ПМДЗ должен представлять собой программное средство, которое встраивается в базовую систему ввода-вывода (BIOS) и осуществляет блокирование попыток несанкционированной загрузки нештатной операционной системы, предоставляет доступ к информационным ресурсам в случае успешной проверки подлинности загружаемой операционной системы и прав на основе идентификации и аутентификации пользователя.  ПМДЗ должен обеспечивать контроль завершенности транзакций в журналах файловых систем EXT3, EXT4 и контроль программных прерываний системного режима управления (SMI)  ПМДЗ должен иметь возможность задать настройки сессии аутентификации  ПМДЗ должен иметь возможность обеспечения загрузки корневых сертификатов и списка отзыва сертификатов  ПМДЗ должен иметь возможность импорта и экспорта настроек  ПМДЗ должен вести аудит действий пользователя и администратора. Все события должны записывать в журнал. Режимы ведения журнала:   * Внутренний, циклический; * Внутренний, экспортируемый; * Внешний (на диске).   ПМДЗ должен обеспечивать защиту BIOS от перезаписи, чтения и от изменения EFI-переменных.  Активация/деактивация ПМДЗ должна осуществляться программно, без механических операций вскрытия и установки/извлечения компонентов.  Обновление ПМДЗ должно производиться программно, из меню настроек замка. |  |  | Для построения системы защиты информации |
|  |  | Требования к обеспечению контроля целостности |  | ПМДЗ должен обеспечивать контроль целостности, следующих компонентов:   * образа BIOS и программного обеспечения ПМДЗ; * файлов на файловых системах: EXT2, EXT3, EXT4; * MBR на носителях информации; * таблиц ACPI; * таблиц SMBIOS; * карты распределения памяти; * ресурсов конфигурационного пространства PCI/PCIe; * контроль целостности CMOS (содержимого энергонезависимой памяти). |  |  | Для построения системы защиты информации |
|  |  | Требования к аутентификации |  | ПМДЗ должен обеспечивать двухфакторную аутентификацию в том числе и с применением сертификатов электронной подписи (далее – ЭП). Авторизация должна происходить на уровне BIOS до загрузки основных компонентов операционной системы. Должны поддерживаться следующие способы аутентификации:   * пароль; * электронный идентификатор с сертификатом; * сочетание способов электронный идентификатор и пароль; * пароль на электронном идентификаторе; * пароль на LDAP; * сертификат на LDAP;   ПМДЗ должен поддерживать токены – Rutoken ЭЦП, Rutoken ЭЦП 2.0, Rutoken Lite, JaCarta PKI, Guardant ID, JaCarta-2 ГОСТ  ПМДЗ должен обеспечивать возможность аутентификации пользователей в LDAP, в том числе и по сертификатам |  |  | Для выполнения требований по защите информации в соответствии с Приказом ФСТЭК России от 18 февраля 2013г №21, приказом ФСТЭК России от 11 февраля 2013г №17. |
|  |  | Требования по нейтрализации угроз информационной безопасности |  | ПМДЗ должен обеспечивать нейтрализацию следующих угроз безопасности информации:   * несанкционированный доступ к информации за счет загрузки нештатной операционной системы и, тем самым, обхода правил разграничения доступа штатной операционной системы и (или) других средств защиты информации, работающих в среде штатной операционной системы; * несанкционированную загрузку штатной операционной системы и получение несанкционированного доступа к информационным ресурсам; * нарушение целостности программной среды средств вычислительной техники и (или) состава компонентов аппаратного обеспечения средств вычислительной техники в информационной системе; * нарушение целостности программного обеспечения средства доверенной загрузки; * отключение и (или) обход нарушителями компонентов средств доверенной загрузки; * несанкционированное изменение конфигурации (параметров) средства доверенной загрузки; * преодоление или обход функций безопасности средств доверенной загрузки; * получение остаточной информации средства доверенной загрузки из памяти средства вычислительной техники после завершения работы средства доверенной загрузки; * получение доступа к ресурсам средства доверенной загрузки из программной среды средства вычислительной техники после завершения работы средства доверенной загрузки. |  |  | Для построения системы защиты информации |
|  |  | Требования к централизованному наблюдению |  | ПМДЗ должен поддерживать функции информационного взаимодействия с программным обеспечением, реализующим функции централизованного лицензирования и сбора журналов, в части:   * передачи информации об установленной версии ПМДЗ; * передачи IP-адреса устройства, на котором установлен ПМДЗ; * удалённая регистрация лицензий, с возможностью группового лицензирования; * выгрузки журналов ПМДЗ, с возможностью групповой выгрузки |  |  | Для получения оперативной информации о текущем состоянии функционирующих в системе ПМДЗ |
|  |  | Требования к сертификации |  | Модуль доверенной загрузки должен иметь действующий сертификат соответствия ФСТЭК России, позволяющий использовать:  - в государственных информационных системах до 2 класса защищенности включительно;  - в информационных системах персональных данных до 2 уровня защищенности включительно. |  |  | Приказ ФСТЭК России от 18 февраля 2013г №21.  В соответствии с п.11 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах утвержденных приказом ФСТЭК России от 11 февраля 2013г №17. |
|  |  | Средство защиты информации от несанкционированного доступа |  |  |  |  |  |
|  |  | Функциональные требования |  | Средство защиты информации от несанкционированного доступа (СЗИ НСД) должно обеспечивать выполнение следующих функций:  регистрацию пользователей. Возможность задать пароль пользователя. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества сессий пользователей на одном компьютере;  возможность принудительной блокировки пользователей и автоматической блокировки в случае нарушения политик безопасности;  идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной аутентификации по паролю и аппаратному идентификатору;  возможность сохранения авторизационных данных пользователя на аппаратном идентификаторе;  реализацию настроек сложности паролей (длины парольной строчки, контроля наличия цифр и специальных символов) и срока их действия;  возможность настройки разграничения прав доступа к объектам файловой системы, съемным накопителям, разграничения прав на доступ к устройствам печати;  возможность контроля целостности аппаратной конфигурации компьютера;  регистрацию и учет (аудит) действий пользователей (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, вывод на печать информации, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки записей;  возможность периодического архивирования журналов событий;  возможность экспорта журналов безопасности в форматы PDF и ODS;  возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов);  возможность администрирования через графическую оболочку СЗИ НСД, функционирующую в операционных системах на базе Linux;  возможность контроля целостности программно-аппаратной среды (в том числе отдельных каталогов) и произвольных объектов файловой системы при загрузке ПЭВМ, по команде администратора или периодически. Возможность восстановления объекта доступа в случае обнаружения нарушения его целостности;  контроль целостности объектов СЗИ;  очистку остаточной информации (освобождаемого дискового пространства, освобождаемых областей оперативной памяти, зачистку определенных файлов и папок по команде пользователя);  возможность проверки корректности функционирования СЗИ НСД, самотестирования;  защиту от подмены ядра операционной системы и процедур инициализации;  возможность настройки всех параметров СЗИ НСД из единой консоли администрирования;  возможность синхронизации времени с аппаратной платой средства доверенной загрузки для регистрации событий безопасности;  возможность сетевого режима функционирования c удаленным управлением учетными записями пользователей, получением информации о состоянии работы защищаемых ПЭВМ, удаленным просмотром журналов на ПЭВМ, входящих в домен безопасности;  централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должна выполняться синхронизация учетных записей в рамках защищаемого контура, синхронизация политик безопасности, удаленное развертывание и удаление клиентских частей СЗИ НСД;  возможность оповещения при некоторых событиях НСД;  наличие собственного механизма дискреционного управления доступом.  СЗИ НСД должен быть включен в Единый реестр российских программ для электронных вычислительных машин и баз данных в соответствии с постановлением Правительства РФ от 16 ноября 2015 г. N 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд". |  |  | Для построения системы защиты информации |
|  |  | Требования к сертификации |  | СЗИ НСД должно иметь действующий сертификат соответствия ФСТЭК России, позволяющий использовать:  -  в государственных информационных системах до 2 класса защищенности включительно;  - в информационных системах персональных данных до 2 уровня защищенности включительно |  |  | Приказ ФСТЭК России от 18 февраля 2013г №21.  В соответствии с п.11 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах утвержденных приказом ФСТЭК России от 11 февраля 2013г №17. |
| 3 | Клавиатура, 694 шт | Тип подключения |  | Проводная |  |  | Соответствует КТРУ |
|  |  | Интерфейс |  | USB |  |  | Универсальный интерфейс подключения |
|  |  | Количество клавиш | Шт |  | ≥ 104 |  | Для увеличения скорости работы |
| 4 | Мышь компьютерная, 694 шт | Тип подключения |  | Проводная |  |  | Соответствует КТРУ |
|  |  | Интерфейс |  | USB |  |  | Универсальный интерфейс подключения |
| 5 | Монитор, подключаемый к компьютеру, 694 шт | Размер диагонали | Дюйм |  | Больше или равно 23 |  | Соответствует КТРУ |
|  |  | Тип матрицы |  |  | IPS |  | Соответствует КТРУ |
|  |  | Крепление VESA |  | Наличие |  |  | Для обеспечения совместного использования с системным блоком |
| 6 | Источник бесперебойного питания, 694 шт | Полная мощность | ВА |  | ≥ 500 |  | Соответствует КТРУ |
|  |  | Форм-фактор |  | Отдельно стоящий |  |  | Соответствует КТРУ |
|  |  | Наличие дополнительных функций |  | Встроенный автоматический стабилизатор напряжения (AVR) |  |  | Соответствует КТРУ |
|  |  | Время переключения | мс |  | Не более 4 |  | Для обеспечения бесперебойного функционирования информационных систем |
|  |  | Защита от перегрузок |  | Наличие |  |  | От обеспечения отказоустойчивости |
|  |  | Защита от короткого замыкания |  | Наличие |  |  | От обеспечения отказоустойчивости |
|  |  | Емкость батареи | АЧ |  | Не менее 7,2 |  | Для обеспечения необходимого времени автономной работы на максимальной нагрузке |
|  |  | Время перезарядки | час |  | Не более 4 |  | Для обеспечения быстрого восстановления заряда батареи |
| 7 | Фильтр сетевой, 694 шт | Количество розеток | Шт |  | Не менее 6 |  | Для подключения оборудования |
|  |  | Длина шнура | М |  | Не менее 1.8 |  | Для подключения к сети питания |
|  |  | Общий выключатель розеток |  | Наличие |  |  | Для отключения сети питания |

\* В связи с необходимостью обеспечения взаимодействия закупаемого оборудования и программного обеспечения с программным обеспечением, используемым Заказчиком, слово «эквивалент» не включено в описание объекта закупки в соответствии с пунктом 1 части 1 статьи 33 Федеральным законом от 05.04.2013 № 44-ФЗ. У заказчика имеются лицензии на использование Корпоративного браузера «Спутник», лицензии на использование операционной системы «Astra Linux Common Edition». В случае поставки лицензии на использование Корпоративного браузера «Спутник», лицензии на использование операционной системы «Astra Linux Common Edition», Заказчик расширяет количество имеющихся лицензий с целью снижения затрат на покупку и администрирование.

**Требования к качеству:**

Поставляемые системные блоки должны иметь сертификаты соответствия требованиям системы сертификации ЕАС, экспертное заключение, гарантирующие безопасность для здоровья, а также товарный знак, зарегистрированный в Государственном реестре товарных знаков и знаков обслуживания РФ и подтвержденный соответствующим свидетельством. Оборудование должно иметь электронный паспорт изделия: заказчик должен иметь возможность узнать на сайте (указать сайт) дату выпуска изделия, его состав и условия гарантийного обслуживания, указав серийный номер системного блока.

**Обоснование включения дополнительной информации, не предусмотренной КТРУ, в сведения о товаре:**

В связи с тем, что для описания объекта закупки, соответствующей потребностям заказчика, недостаточно показателей, указанных в используемых кодах позиций КТРУ, закупки в соответствии с пунктами 5 и 6 Правил использования каталога товаров, работ, услуг для обеспечения государственных и муниципальных нужд, установлены дополнительные показатели характеристик объекта закупки.

В соответствии с п.2 ст. 33 Федерального закона от 05.04.2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и Федеральным законом от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации» стандартные показатели при описании объекта закупки на некоторые характеристики товаров не применяются, в связи с отсутствием на них технических регламентов, принятых в соответствии с законодательством Российской Федерации о техническом регулировании, документами, разрабатываемыми и применяемыми в национальной системе стандартизации, принятыми в соответствии с законодательством Российской Федерации о стандартизации, связанных с определением соответствия поставляемого товара, потребностям заказчика.

**ПОДПИСИ СТОРОН:**

|  |  |
| --- | --- |
| ***От Поставщика:***  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (должность)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Ф.И.О.)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Подпись)  М.П. | ***От Заказчика:***  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (должность)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Ф.И.О.)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (Подпись)  М.П. |

**Государственный контракт подписан электронно-цифровыми подписями Сторон**