**Приложение № 2 к Документации об электронном Аукционе**

**Техническое задание**

**на поставку серверного оборудования**

1. Описание объекта закупки

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  **п/п** | **Наименование** | **Характеристика** | **Кол-во** |
| 1 | Серверный кластер | Серверный кластер, позволяет запускать экземпляры гостевых машин, эмулируя для них оборудование и организовывать управление ими из единого центра администрирования;  Обеспечивать динамическое выделение ресурсов, возможность изменять количество выделяемых ресурсов для работающих гостевых машин, уметь перераспределять память от простаивающих гостевых машин к активным;  Серверный кластер обеспечивает высокую отказоустойчивость и при сбое, который определяется отказом узла устройства или зависанием гостевой машины, гостевая машина стартует на другом максимально подходящем узле кластера.  Серверный кластер занимает не более 4 монтажных единиц в поставляемой конфигурации;  Серверный кластер обеспечивает монтажную глубину не менее до 750мм;  Серверный кластер имеет монтажный комплект для установки в 19” стойку;  Количество узлов в поставляемой конфигурации не менее 2;  Для предотвращения конфликтов одновременного обращения узлов устройства к LUN системы хранения данных, необходимо что бы кластер умел назначать идентификатор хоста (HLU ID). Кластер обеспечивает режим работы «Активный-Активный» с возможностью резервирования и «горячей» замены;  Возможность модернизации узлов кластера на более производительные с сохранением данных и без остановки кластера;  Наличие индикации для отображения состояния питания, состояния систем и их компонентов с возможность управления питанием каждого узла кластера;  Индикатор активности дисковой подсистемы кластера;  Наличие индикации активности сети каждого узла;  Каждый узел кластера имеет VGA порт задней панели;  Каждый узел кластера имеет не менее 2 портов USB 3.0 на задней панели.  На задней панели каждого узла размещены:  • Порт удаленного управления реализованный по средствам выделенного порта RJ-45;  • Порт Ethernet 10 Гбит/с SFP+ 2 штуки;  • Порт Ethernet 10 Гбит/с SFP+ 2 штуки c трансивером 1 Гбит/с RJ-45;  • Порт FibreChannel 16 Гбит/с SFP+ DuplexLC 2 штуки;  Интегрированный контроллер удалённого управления КВМ и мониторинга, использующий выделенный сетевой порт, пропускной способностью не менее 1Гб/с, обеспечивает следующий функционал:  • Поддержка протоколов управления: Web-based GUI;  • Удаленный доступ к консоли управления узла через интерфейс веб-браузера;  • Автоматическое информирование администратора о сбоях и предсказаниях нарушения функционирования дисковой подсистемы, модулей памяти, блоков питания, вентиляторов и процессоров по средствам электронной почты;  • Удаленная перезагрузка, включение/выключение узла;  • Удаленная загрузка операционной системы узла, в том числе загрузка с оптического диска или ISO образа, расположенного на ПК администратора;  • Мониторинг оборудования (температура, напряжение и т.д.) независимый от состояния операционной системы;  Кластер имеет предустановленные накопители SATA SSD не менее 3 штук объёмом не менее 240ГБ;  Кластер предоставляет возможность использования не менее 2 разъемов  PCIe x16 и не менее 4 разъемов PCIe x8 одномоментно;  Узлы кластера защищены от непреднамеренного отсоединения кабелей питания;  Кластер обеспечивает возможность управления вентиляторами узлов в количестве не менее 4 штук;  Кластер обладает не менее 64 вычислительными ядрами и равно распределенными по узлам;  Кластер одномоментно обеспечивает не менее 128 обрабатываемых потока в 64-разрядных приложениях;  Базовая частота каждого ядра процессора не менее 2.1 ГГц;  Каждый узел обеспечивает не менее 44 МБ процессорного КЭШа;  Суммарное тепловыделение применяемых центральных процессоров в кластере не более 400Вт;  Каждый центральный процессор узла обладает встроенным контроллером памяти с кодом коррекции ошибок;  Каждый центральный процессор узла обладает защитой системы от программных ошибок;  Каждый центральный процессор узла обладает защитой от переполнения буфера в результате вирусных атак;  Кластер имеет возможность расширение объема оперативной памяти до 6 ТБ включительно;  Каждый узел кластера в поставляемой конфигурации имеет возможность монопольно использовать от 512ГБ оперативной памяти включительно;  Кластер блоками питания с резервированием не ниже N+1 и КПД не ниже 94% при нагрузке в 50%;  Суммарная мощность блоков питания не более 3200кВт;  Кластер должен поставляться с не менее чем тремя бессрочными лицензиями на операционную систему, удовлетворяющую следующим требованиям:  OC должна иметь подтверждение возможности её применения для построения информационных (автоматизированных) систем, обрабатывающих информацию ограниченного доступа в виде сертификатов соответствия требованиям нормативных документов:  • «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016);  • «Профиль защиты операционных систем типа «А» не ниже 3 класса ИТ.ОС.А3.ПЗ (ФСТЭК России, 2017);  • «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) не ниже 3 уровня;  • «Требования по безопасности информации к средствам виртуализации» (ФСТЭК России, 2022) не ниже 3 класса защиты;  • «Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022) не ниже 3 класса защиты.  Операционная система должна включать в свой состав сертифицированные средства виртуализации, обеспечивающие доверенную загрузку виртуальных машин, контроль целостности, регистрацию событий, управление доступом и другие функции безопасности, резервное копирование виртуальных машин и идентификацию пользователей.  Операционная система должна включать в свой состав сертифицированные средства контейнеризации, обеспечивающие изоляцию контейнеров, контроль целостности контейнеров и их образов, регистрацию событий безопасности, идентификацию и аутентификацию пользователей.  Требования к встроенному комплексу средств защиты информации операционной системы  Операционная система должна обеспечивать встроенными сертифицированными средствами:  • управление средствами аутентификации;  • управление учетными записями пользователей, разграничение полномочий и назначение прав пользователям;  • реализацию дискреционного и мандатного разграничения доступа;  • возможность создания защищенной среды виртуализации;  • возможность создания среды выполнения контейнеров и обеспечение работы с ними;  • технологию контейнеризации с поддержкой изоляции процессов;  • возможность маркировки документов при выводе на печать;  • управление доступом к защищаемым ресурсам БД на основе иерархических и не иерархических меток доступа;  • функционирование web-сервера с учетом политик мандатного управления доступом;  • реализацию мандатного управления доступом к почтовым сообщениям, а также автоматическую маркировку создаваемых пользователем почтовых сообщений.  В составе операционной системы должна быть реализована возможность защиты аутентификационной информации с использованием функции хэширования.  В состав операционной системы должен входить комплекс программ объектно-реляционной защищённой СУБД с сертифицированными функциями безопасности.  В составе операционной системы должна быть реализована возможность внедрения в сетевые пакеты протоколов IPv4 и IPv6 классификационных меток в соответствии с ГОСТ Р 58256-2018. В составе операционной системы должна быть реализована возможность внедрения в сетевые пакеты протоколов IPv4 и IPv6 классификационных меток в соответствии с ГОСТ Р 58256-2018 для обеспечения:  • организации сетевого взаимодействия прикладных процессов на основе их классификационных меток;  • фильтрации сетевого трафика на основе классификационных меток.  В составе операционной системы должны быть графические средства создания единого пространства пользователей с целью реализации централизованного хранения информации об окружении пользователей и сетевой аутентификации через ldap и kerberos.  Операционная система должна иметь графическое средство настройки ограничений пользователя по запуску программ в изолированном окружении с использованием механизма пространств имён и фильтрации системных вызовов, обеспечивающих:  • ограничение прав пользователя на запуск приложений ядром системы;  • ограничение прав пользователя средствами графического интерфейса;  • разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности.  Обеспечение запрета запуска (исполнения) пользователем созданных самостоятельно (с использованием текстовых редакторов или непосредственно в командной строке) программ с использованием интерпретируемых языков программирования.  В составе операционной системы должны быть графические средства настройки защиты машинных носителей, обеспечивающие:  • идентификацию устройств и сопоставление пользователя с устройством;  • контроль подключения носителей информации;  • учет носителей информации;  • управление доступом к носителям информации;  • контроль использования интерфейсов ввода/вывода информации;  • ввод-вывод информации на носитель при условии совпадения маркировки носителя и объёма прав пользователя.  Операционная система должна включать в свой состав программное обеспечение, реализующее задачи аудита и журналирования (регистрации) событий безопасности.  Операционная система должна включать в состав графические средства контроля целостности:  • контроль целостности дистрибутива;  • контроль объектов файловой системы;  • контроль целостности исполняемых файлов, обеспечивающий проверку их неизменности и подлинности.  В составе операционной системы должна быть реализована возможность ограничения полномочий пользователей по использованию консолей.  В составе операционной системы должно присутствовать ядро с функциями очистки и ограничения работы с оперативной памятью.  Должно быть обеспечено наличие регулярного включения информации об уязвимостях программного обеспечения операционной системы в банк данных угроз безопасности информации ФСТЭК России, устраняющих неисправности прикладного программного обеспечения и уязвимости операционной системы с подтверждением информации об исправленных уязвимостях путём размещения таких сведений в банке данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru/vul).  Механизмами безопасности операционной системы должна быть обеспечена защита системных и привилегированных процессов от несанкционированного доступа и управления (исключение возможности повышения привилегий пользователей и управления привилегированными процессами в случае использования дефектов/уязвимостей в программном обеспечении информационной системы).  Операционная система должна обеспечивать запрет операций записи в системные каталоги и файлы (программы, файлы конфигурации), а также установки программного обеспечения, запуска и остановки системных процессов операционной системы, вне зависимости от изменения пользователем своих привилегий в текущем сеансе работы.  Операционная система должна обеспечивать возможность контроля целостности исполняемых файлов и файлов библиотек: EXE, DLL, .NET 7  Требования к функциональным возможностям операционной системы  Операционная система должна быть предназначена для функционирования на средствах вычислительной техники с аппаратной платформой х86-64 включая процессоры Intel не ниже 10-го поколения.  Операционная система должна поддерживать работу на ядре Linux версии не ниже 6.1.  Операционная система должна обеспечивать функционал в графическом исполнении:  • наличие средств создания, настройки и управления несколькими служебными репозиториями используемого программного обеспечения, с поддержкой проверки зависимостей пакетной базы и автоматической публикацией в сети по протоколам http и ftp;  • наличие графического инструмента управления регистрацией событий, включающий в себя управление сервисом системных событий, настройку ротации событий и настройку параметров сбора системных событий, графическое средство просмотра системных событий;  • наличие графического инструмента для редактирования значения переменных окружения (изменять значение и описание переменных, удалять и объявлять переменные);  • наличие графической утилиты управления и мониторинга компонентов подсистемы безопасности;  • наличие средств расчёта контрольных сумм файлов и их сравнения;  • наличие средств для оповещения пользователя о конфликте IP-адресов при подключении к сети;  • наличие средств работы с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso).  ОС должна обеспечивать поддержку файловых систем и сетевых протоколов:  • ext2/3/4, fat, ntfs, XFS, ZFS, BTRFS;  • TCP/IP, DHCP, DNS, FTP, TFTP, SMTP, IMAP, HTTP(S), NTP, SSH, NFS, SMB;  • поддержка стандарта ISO9660;  • наличие средств организации распределенной файловой системы;  • наличие средств подключения ресурсов WebDAV в качестве локальной файловой системы для возможности использования их стандартными приложениями операционной системы.  Операционная система должна обеспечивать возможность создания точек восстановления (снапшотов) для последующего возвращения системы к исходному состоянию в случае сбоя.  Операционная система должна обеспечивать среду функционирования для сертифицированных средств криптографической защиты информации, предназначенных для создания и проверки электронной подписи, сквозного шифрования сетевых соединений и каналов связи, установления защищенного соединения и обмена зашифрованными данными.  Дополнительные функциональные компоненты:  web-сервер Apache или эквивалент;  почтовые сервисы и системы передачи почты: Exim, Dovecot, Postfix или эквивалент;  средства мониторинга;  средства удаленного и терминального доступа: VNC, RDP(xRDP), RemoteApp (freerdp) или эквивалент;  защищенный сервер печати;  службы резервного копирования: Bacula, Rsync или эквивалент;  аудит и журналирование событий безопасности;  набор программ для воспроизведения аудио и видео файлов;  редактор растровой графики;  запись оптических дисков;  программа сканирования;  защищённый графический сервер X.Org Xserver или эквивалент;  защищённый рабочий стол;  системные библиотеки libc или эквивалент;  компилятор GCC или эквивалент;  QT или эквивалент.  Срок действия технической поддержки от производителя оборудования не менее 36 месяцев.  Серверный кластер должен быть оснащен двумя или более лицензиями на систему резервного копирования, для обеспечения сохранности данных.    Системные требования:  • ПО имеет возможность резервного копирования и восстановления виртуальных машин в двух режимах:  o «Безагентном», т.е., внутри виртуальной машины не устанавливается агент.  o «Агентном», т.е., внутри виртуальной машины устанавливается агент.  • ПО поддерживает безагентный режим для следующих платформ виртуализации:  o VMWare, Hyper-v, OpenStack, Rosa Virtualization, oVirt, zVirt, Red Hat Virtualization, ECP Veil, SpaceVM, Кибер Инфраструктура, РедВиртуализация  • В качестве гостевых ОС (х86 / х64) в среде виртуализации поддерживаются следующие системы:  o •Российские ОС: Альт 8 СП, Альт Сервер 9, 10 Альт Рабочая станция 9, 10 РОСА Кобальт 7.9, ROSA Enterprise Linux, Astra Linux SE 1.6, 1.7.0–1.7.3, Red OS 7.2, 7.3  o •Windows 7, Windows 8/8.1, Windows 10 — выпуски Home, Pro, Education, Enterprise, и IoT Enterprise  o •Windows Server 2008R2, Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022  o •Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016  o •ОС Linux различные дистрибутивы с версией ядра от 3.0 до 6.2 и glibc 2.3.4 или более поздней версии  o •Red Hat Enterprise Linux 7.x, 8.0, 8.1, 8.2, 8.3, 8.4  o •Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS  o •SUSE Linux Enterprise Server 12, 15 — поддерживается в файловых системах, за исключением Btrfs  o •Debian 10, 11  o •CentOS 7,x, 8,0 - 8.3  o •Oracle Linux 7.x, 8.0, 8.1, 8.2, 8.3, 8.4— Unbreakable Enterprise Kernel и Red Hat Compatible Kernel  o •AlmaLinux 7.x, 8.x\*  o •AlterOS 7.5  o •ОСнова 2.7  • ПО поддерживает следующие системы виртуализации:  o Microsoft Hyper-V: Windows Server 2008/2008 R2 с Hyper-V, 2012/2012 R2 с Hyper-V, 2016 с Hyper-V, Microsoft Hyper-V Server 2016, Microsoft Hyper-V Server 2019  o VMware vSphere: 4.1; 5.0; 5.1; 5.5; 6.0, 6.5, 6.7, 7.0.  o ПО поддерживает следующие версии Space VM версии 6.0.5 и выше  o ПО поддерживает следующие версии OpenStack: Ussuri, Victoria, Wallaby, Xena, Yoga, Zed  o ROSA Virtualization: 2.0, 2.1  o Red Hat Enterprise Virtualization (RHEV): 4.2, 4.3, 4.4  o oVirt 4.2, 4.3, 4.4, 4.5  o zVirt 3.0, 3.1, 3.2, 3.3  o ECP VeiL версии 4.7–5.1  o Ред Виртуализация 7.2, 7.3  o HOSTVM 4  o Виртуализация Кибер Инфраструктуры 4.0 и выше  o Astra Linux «Брест» и Р-Виртуализация. Резервное копирование изнутри гостевой ОС  o Citrix XenServer: 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2 и 6.5. Резервное копирование изнутри гостевой ОС  o Oracle VM Server 3.0 и 3.3, Oracle VM VirtualBox 4.x. Резервное копирование изнутри гостевой ОС  o Citrix XenServer в «агентном» режиме: 6.0–6.5, 7.0–7.6. Резервное копирование изнутри гостевой ОС  o Oracle VM Server 3.0, 3.3, 3.4. Резервное копирование изнутри гостевой ОС.  o Oracle VM VirtualBox 4.x. Резервное копирование изнутри гостевой ОС.  • ПО поддерживает копирование следующих приложений:  o Microsoft Exchange Server 2013, 2016, 2019  o Microsoft SQL Server 2012, 2014,2016, 2017,2019  o Microsoft Active Directory  o Oracle Database 11g, 12c все выпуски  o Postgre SQL 11, 12, 13, 14, 15, 16  o Postgre Pro Enterprise 11, 12, 13, 14, 15, 16  o СУБД «Jatoba»  o СУБД Tantor  o Proxima DB  o СУБД MySQL  o СУБД Maria DB  o Ред База Данных 3.0  o CommuniGate Pro  o VK WorkMail  • ПО поддерживает следующие файловые системы:  o FAT16/32, NTFS, ReFS, Ext2/Ext3/Ext4, Linux SWAP, ReiserFS3/4, XFS, JFS  • ПО поддерживает размещение резервных копий на следующих системах хранения:  o Локальные диски и съёмные носители  o Сетевые устройства хранения, доступные по SMB/CIFS/DFS, папки NFS  o SFTP сервер  o Программно-определяемое хранилище Кибер Инфраструктуры  o Ленточные накопители одно- и многоразовой перезаписи стандарта LTO-5, LTO-6, LTO-7, LTO-8, LTO9  o Хранилище, определяемое сценарием (скриптом) хранилище  Функциональные особенности:  • ПО обеспечивает резервное копирование и аварийное восстановление дисков и томов со всеми хранящимися на них данными, включая приложения.  • ПО обеспечивает резервное копирование и аварийное восстановление папок и файлов  • Все основные компоненты системы - Сервер управления и Узел Хранения (Медиа сервер) устанавливаются на операционные системы семейства Windows и Linux.  • В ПО поддерживается отказоустойчивость Сервера Управления в кластерной конфигурации под управлением на ОС Linux.  • ПО ограничивает доступ к управлению резервным копированием и восстановлением данных для пользователя и групп пользователей путём авторизации  • В ПО присутствует WEB интерфейс управления системой.  • В ПО поддерживается разделение ролей администраторов  • ПО содержит возможность мониторинга процессов резервного копирования и построения отчетов. Данные мониторинга доступны для внешних систем мониторинга через публичный API.  • Настройка почтовых уведомлений о совершённых операциях, сводках за период времени и возникающих ошибках.  Возможности резервного копирования:  • ПО обеспечивает возможность резервного копирования ОС на уровне образов, на уровне томов, а также на уровне отдельных файлов, с сохранением состояния приложений  • Создание полных, дифференциальных и инкрементных резервных копий  • ПО обеспечивает блочное и файловое резервное копирование, а также резервное копирование с помощью технологии Changed Block Tracking (CBT) и Microsoft Volume Shadow Copy Service (VSS).  • Платформа резервного копирования поддерживает использование аппаратных снимков СХД NetApp и Huawei Dorado для резервного копирования, с возможностью обеспечения целостности приложений внутри виртуальных машин.  • ПО поддерживает исключение файлов из копирования.  • Поддерживается автоматическое или ручное разбиение резервных копий.  • Поддерживаются механизмы дедупликации и сжатия резервных копий для минимизации объема хранимых данных;  • При копировании на магнитные ленты поддерживаются режимы многопоточности (мультистриминга и мультиплексинга), возможность объединять ленточные накопители в пул с разных ленточных библиотек, а также возможность использовать одновременно все записывающие устройства на ленточной библиотеке при копировании на магнитную ленту.  • ПО поддерживает выполнение скриптов до и после резервного копирования (Pre и Post команды)  • ПО позволяет выполнять полное и инкрементное резервное копирование СУБД MS SQL Server, MySQL, MariaDB  • ПО позволяет выполнять полное и инкрементное резервное копирование серверов почтовых систем MS Exchange, CommunigatePro, VK WorkMail.  Возможности восстановления из резервных копий.  • ПО поддерживает восстановление данных на уровне образа ОС, уровне томов, уровне отдельных объектов файловой системы;  • ПО предоставляет возможность создания универсального аварийного загрузочного носителя на основе Linux и WinPE для восстановления для физических машин всей системы целиком в режиме bare-metal, а также на целевую систему с отличающейся аппаратной конфигурацией от исходной  • ПО имеет несколько режимов восстановления: весь сетевой ресурс целиком, отдельные файлы и папки. Предоставляется возможность выбора исторической версии файла при восстановлении;  • Поддерживается восстановление файлов, с сохранением настроек безопасности  • ПО предоставляет возможность восстановления резервной копии диска в новую виртуальную машину  • ПО предоставляет возможность восстановления виртуальной машины в другой системе виртуализации.  • Для почтовых систем MS Exchange Server, CommunigatePro, VK WorkMail поддерживается восстановление серверов целиком  • Для почтовых систем MS Exchange Server, поддерживается гранулярное восстановление почтовых ящиков и элементов почтовых ящиков  • Поддерживается копирование отдельных файлов или папок из резервной копии с помощью Windows Explorer.  ПО поддерживает следующие функции и возможности управления резервными копиями:  • Поддерживается шифрование резервных копий, защита с помощью пароля  • Платформа резервного копирования имеет возможность автоматического тестирования целостности резервных копий. Проверка осуществляется подсчётом контрольной суммы, а также с помощью запуска виртуальной машины из резервной копии по отдельному расписанию  • Поддерживается возможность репликации резервных копий по отдельному расписанию с использованием имеющихся каналов передачи данных.  • Поддерживается управление продолжительностью хранения резервных копий, удаление устаревших копий на основании возраста, количества копий, возраст копии, занимаемое место в хранилище  • Поддерживается создание резервной копии вместе с загрузочными компонентами на съемный загрузочный носитель для возможности аварийного восстановления.  Дополнительные возможности.  • Миграция систем с физической на виртуальную и с виртуальной на физическую.  • Защита от вирусов-шифровальщиков.  • Поиск и оценка уязвимостей  • Единый план защиты – для резервного копирования, оценки уязвимостей и защиты от вирусов шифровальщиков  • Автоматическое обнаружение устройств в сети и установка на них агентов резервного копирования  • ПО включено в Единый реестр российских программ для электронных вычислительных машин и баз данных  Описание Технической поддержки:  • ПО сопровождается подпиской на техническую поддержку на период от одного года.  • Контакт со службой технической поддержки посредством телефона, электронной почты.  • Техническая поддержка доступна на русском языке в рабочие часы, в будни.  • Обозначение критичности проблемы при создании заявки в службе технической поддержке.  • В критичных случаях при обращении в службу технической поддержки первая реакция инженера следует в течение нескольких часов.  • Подписка на техническую поддержку в период своего действия гарантирует бесплатные обновления продукта, в том числе переход на новую версию продукта.  • Служба технической поддержки регулярно обновляет базу знаний, содержащую исчерпывающие сведения о распространенных проблемах продукта и дополнительную техническую информацию  Работы по пуско-наладке кластера виртуализации:  1. Монтаж и установка серверного кластера в стойку в помещении ЦОД, расположенному по адресу г. Улан-Удэ, улица Ленина, дом 54.  2. Установка операционных систем под гипервизор с переносом существующих лицензий на новое кластерное оборудование. Настройка IP-адресов, FQDN, учетных записей на узлах кластера.  3. Миграция виртуальных машин и данных с существующего кластера на вновь устанавливаемый.  4. Маркировка и укладка кабелей.  5. Составление итоговой документации. Передача заказчику логинов, паролей и адресов для доступа к узлам кластера.  6. Установка операционной системы на 3 виртуальных сервера. | 1 шт |
| 2 | Система хранения данных | Высота, занимаемая в шкафу в текущей конфигурации не более 4U  Текущая конфигурация должна поддерживать единовременную установку не менее 24 дисков 3,5” с интерфейсом SAS с возможностью «горячей» замены с доступом с лицевой стороны устройства  Возможность использования дисков 2.5” вместо 3,5” без использования дополнительных опций  Наличие поддержки дисков и SSD сторонних производителей с интерфейсом SAS.  Не допускается использование лицензий (дополнительных платных опций) для добавления новых дисков либо в состав системы должна быть включена лицензия на максимальное количество дисков, поддерживаемых системой.  Поддержка расширения при помощи полок через интерфейс SAS со скоростью не ниже 12Gb/s  Наличие поддержки подключения полок расширения сторонних производителей  Максимальное количество поддерживаемых дисков системой: не менее 544 шт.  Интерфейс установленных накопителей (тип 1): SAS  Стандарт интерфейса установленных накопителей: SAS-3  Количество установленных накопителей с поддержкой горячей замены (тип 1): не менее 10 шт.  Объем каждого установленного накопителя: не менее 1920 Гбайт  Тип установленных накопителей: SSD  - предназначены для работы в режиме 24/7 (24 часа, 7 дней в неделю);  - R2100/W1800Mb/s.  - IOPS(R4K) 430K/60K.  Ресурс на запись дисков SSD - количество перезаписей всего объема накопителя в день (DWPD) не менее 1  Интерфейс установленных накопителей (тип 2): SAS  Стандарт интерфейса установленных накопителей: SAS-3  Количество установленных накопителей с поддержкой горячей замены (тип 2): не менее 14 шт.  Объем каждого установленного накопителя: не менее 6000 Гбайт  Тип установленных накопителей: HDD  Скорость вращения дисков в накопителе HDD: не менее 7200 оборотов в минуту.  - предназначены для работы в режиме 24/7 (24 часа, 7 дней в неделю);  RAID контроллеры:  Наличие не менее двух «Активный-Активный» с возможностью резервирования и «горячей» замены.  Наличие защиты КЭШа контроллера при помощи конденсатора с сохранением его состояния во флэш память с возможностью «горячей замены»  Возможность обслуживания и замены модулей защиты КЭШа контроллера без отключения и извлечения из корпуса системы контроллеров и блоков питания  Технические характеристики одного RAID контроллера:  Наличие процессора с типом не хуже Xeon с количеством ядер не менее 4  Наличие не менее 8GB памяти поколения стандарта не ниже DDR4  Наличие возможности расширения памяти до 256GB поколения стандарта не ниже DDR4  Наличие поддержки уровней RAID: 0,1,0+1,3,5,6,10,30,50,60,5EE,6EE,50EE,60EE.  Внутренний интерфейс для дисков SAS со скоростью не ниже 12Gb/s  Наличие не менее двух портов SAS 12 Гбит/сек для подключения дисковых полок  Наличие не менее четырех портов 10 Гбит/сек iSCSI SFP+ с трансиверами типа SR (не менее 2 шт) и типа RJ-45 (не менее 2 шт)  Наличие не менее двух портов 16 Гбит/сек Fibre Channel с трансиверами типа SR  Наличие возможности установки дополнительных интерфейсов не менее четырех портов 10 Гбит/сек iSCSI SFP+ или не менее двух портов 25 Гбит/сек iSCSI или не менее четырех портов 16 Гбит/сек Fibre Channel или не менее двух портов 32 Гбит/сек Fibre Channel  Наличие поддержки глобального (может использоваться для замены любого вышедшего из строя жесткого диска такого же или меньшего размера) и выделенного «диска горячего резерва».  Наличие поддержки сквозного кэширования и кэширования данных с отложенной записью.  Наличие поддержки расширение тома и пула без прерывания записи и чтения.  Наличии технологии оптимизации процесса обработки трафика, позволяющей использовать выделенное ядро центрального процессора для обработки пакетов iSCSI и Fibre Channel.  Поддержка iSCSI jumbo frame (jumbo кадр).  Поддержка режимов Header/Data digest.  Поддержка аутентификация CHAP.  Поддержка технологии Multipath I/O и балансирования нагрузки (Microsoft MPIO, MC/S, транкинг, LACP).  Наличие встроенной технологии по созданию «мгновенных снимков» и полных копий томов.  Возможность использовать созданные снимки в режиме «записи»  Наличие встроенной технологии асинхронной репликации томов на аналогичную систему хранения.  Наличие встроенной технологии синхронной репликации томов на аналогичную систему хранения (дополнительная опция).  Поддержка службы фонового копирования тома Microsoft VSS.  Поддержка восстановления конфигурации массива.  Возможность выделения пространства по требованию (thin provisioning) с возможностью возврата неиспользуемых блоков обратно в пул хранения  Возможность использования SSD дисков для организации КЭШа на чтение и запись (опция в комплекте поставки).  Возможность автоматического перемещения данных между различными типами дисков в рамках одного пула (дополнительная опция).  Возможность ускоренного восстановления RAID группы при отказе диска за счет копирования только занятых блоков данных  Возможность осуществлять мониторинг производительности системы в целом и отдельных томов с глубиной просмотра до одного года и с возможностью сохранения отчета  Возможность управления питанием от источников бесперебойного питания (ИБП). Подключение ИБП к СХД должно осуществляется через последовательный порт или сеть Ethernet.  Поддержка автоматического включения и выключения полок расширения через интерфейс SAS (дополнительная опция).  Система хранения данных должна иметь не менее двух блоков питания, мощность каждого не менее 850Вт, с возможностью «горячей замены».  Система хранения данных должна иметь не менее двух модулей охлаждения, с возможностью «горячей замены».  Возможность обслуживания и замены модулей охлаждения без отключения и извлечения из корпуса системы контроллеров и блоков питания  Выделенный порт управления со скоростью не ниже 1 Гбит/сек Ethernet на каждом контроллере  Управление системой может осуществляться с любого рабочего места по локальной сети через WEB-интерфейс.  Поддержка управления через протоколы HTTP, HTTPS, SSH  Возможность подключения дисплея через порт USB для конфигурирования и мониторинга системы (дополнительная опция)  Оповещение об ошибках: Email; SNMP trap; Syslog.  Поддержка операционных систем: Windows; Linux; Mac.  Поддержка виртуальных сред: VMWare; Hyper-V; Citrix.  Все компоненты системы хранения данных должны быть обладать 100% совместимостью и должны быть предназначены для эксплуатации на территории Российской Федерации.  Гарантия на систему хранения и все её компоненты должна составлять не менее 60 месяцев и обслуживаться через единый сервисный центр.  Проверка статуса гарантии и поддержки осуществляется при помощи письменного запроса производителю системы хранения данных.  1. Прием запросов по настройке, базовому администрированию оборудования и ПО, по проблемам с оборудованием и ПО, включающих полную или частичную потерю работоспособности через различные каналы приема информации (телефон, эл. почта).  Прием запросов осуществляется в режиме 8х5 (в рабочее время в рабочие дни).  Техническая поддержка осуществляется на русском языке.  2. Замена неисправных деталей оборудования.  В случае выхода из строя обслуживаемого оборудования обеспечивается удаленная диагностика, ремонт, предоставление эквивалентных аналогов неисправных компонентов.  3. Предоставление новых версий обслуживаемого ПО и кодов программных коррекций (patches) по мере их выпуска производителем.  Централизованная аппаратно-ориентированная система:  Функции централизованной аппаратно-ориентированной системы мониторинга и управления:  Централизованная система управления и мониторинга, не требующая дополнительных финансовых затрат в процессе эксплуатации.  Русский язык интерфейса централизованной системы управления и мониторинга.  Наличие руководства пользователя, руководства администратора на русском языке.  Техническая поддержка от производителя оборудования на русском языке.  Совместимость со всеми устройствами Оборудования, поставляемыми в рамках договора  Функциональные возможности централизованной системы управления и мониторинга:  - мониторинг и управление всеми типами (серверы, коммутаторы, СХД, ИБП) устройств из единого web-интерфейса;  - доступ к инвентарной информации, включая версии микрокода, из центральной консоли управления;  - контроль изменений управляемых систем.  Удаленное управление программно-техническими средствами в централизованной системе управления и мониторинга: включения/выключения, перезагрузка, получение текущего статуса устройств, графический доступ к удаленной системе.  Функциональные возможности мониторинга серверной инфраструктуры безагентно, то есть без установки служб в операционную систему:  - инвентаризация аппаратной конфигурации (включая версии микрокодов),  - контроль энергопотребления (устройства, серверного шкафа),  - контроль температурного режима,  - уровень загрузки ресурсов.  Визуальное отображение информации, которое позволяет определить:  - размещение оборудования в стойке,  - общий вид устройства (изображение фронтальной и обратной стороны),  - текущий статус устройства.  Функциональные возможности группового управления удаленными системами в централизованной системе управления и мониторинга:  - поиск систем по ключевым событиям, статусу, типам;  - аудит аппаратных систем с формированием отчетности;  - применение к группам устройств политик и правил.  Наличие мобильного приложения под платформы iOS, Android для ПО управления и мониторинга с функциями:  - отображения статуса оборудования,  - расположения оборудования в стойке.  Функциональные возможности управления учетными записями пользователей системы мониторинга и управления:  - ролевая модель доступа;  - поддержка интеграции с службами каталогов LDAP включая Microsoft Active Directory Services;  - возможность определения роли пользователя системы на основании членства в группах LDAP;  - возможность распределения прав доступа к объектам мониторинга пользователям системы;  - логгирование действий пользователей.  Возможность управления электропитанием оборудования по заданному расписанию.  Система мониторинга включена в единый реестр российских программ для электронных вычислительных машин и баз данных.  Срок действия технической поддержки от производителя оборудования не менее 60 месяцев.  Объем технической поддержки от производителя:  Консультации технических специалистов по телефону («горячая линия»), ремонт техники в Сервисном центре в течение 21 рабочего дня.  Поддержка системного ПО оборудования.  Доступ к web-порталу технической поддержки производителя 24x7.  Работы по пуско-наладке системы хранения данных:  1. Монтаж системы хранения данных в стойку. Номер стойки и место согласовывается совместно с Заказчиком.  2. Настройка системы хранения. Разметка по RAID и LUN. По договоренности с Заказчиком обсуждаются все используемые технологии. Адреса и FQDN выдаются Заказчиком или уполномоченным со стороны Владельца площадки, где будет размещаться СХД.  3. Миграция данных, образов, виртуальных дисков с текущего хранилища на новое. По договоренности с Заказчиком и уполномоченным со стороны Владельца текущих мощностей согласовываются все решения необходимые для переноса. Дополнительные материалы предоставляет Исполнитель.  4. Составление итоговой документации. Передача Заказчику таблицы с разбивками по LUN и RAID, а также все доступы к устройствам. | 1 шт |

**2. Место поставки и монтажа:** Россия, Республика Бурятия, г. Улан-Удэ, ул. Ленина, 54

**3. Срок поставки и монтажа:** в течение 16 (шестнадцати) недель с даты заключения договора.

**4. Требования к качеству, безопасности товара:**

4.1. Поставляемый товар должен соответствовать заданным функциональным и качественным характеристикам;

4.2. Поставляемый товар должен быть разрешен к использованию на территории Российской Федерации, иметь торговую марку и товарный знак, качество поставляемого товара должно полностью соответствовать установленным требованиям Российской Федерации, ГОСТ, ОСТ, нормативно-технической документации (сертификатам качества, декларациям о соответствии и (или) другим документам, подтверждающим качество товара);

4.3. Поставляемый Товар должен являться новым, ранее не использованным (все составные части Товара должны быть новыми), не должен иметь дефектов, связанных с конструкцией, материалами или функционированием при штатном их использовании;

4.4. Товар должен быть безопасным и отвечать требованиям законодательства Российской Федерации, требованиям безопасности, ГОСТ, нормам и правилам безопасности его эксплуатации и другой нормативно-технической документации;

4.5. Товар должен отвечать требованиям безопасности жизни и здоровья, окружающей среды в течение установочного срока годности при обычных условиях его использования, хранения, транспортировки и утилизации;

4.6. Гарантийные обязательства должны распространяться на каждую единицу товара с момента приемки товара Заказчиком. Гарантийный срок составляет не менее срока указанного заводом изготовителем (производителем). В течение гарантийного срока обнаруженные недостатки товара подлежат устранению силами и средствами Поставщика;

**5. Требования к упаковке, маркировке товара:**

5.1. Поставщик должен обеспечить упаковку товара, способную предотвратить его повреждение или порчу во время перевозки к конечному пункту назначения – Заказчику;

5.3. Поставщик несет ответственность за ненадлежащую упаковку, не обеспечивающую сохранность товара при его хранении и транспортировании.