Техническое задание на поставку сервера.

Сервер поставляется в комплекте с аппаратной (серверное оборудование) и программной частью (операционная система).

1. Техническое описание аппаратной части (серверное оборудование)

Оборудование должно иметь гарантийные стикеры и паспорт устройства.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Наиме-нование | Модель | Характеристики | Кол-во, шт. |
| 1 | Плат-форма | SuperMicro 6019U-TR4 <1U, 2xLGA3647, C621, SVGA, 4x3.5'' HotSwap, 4xGLAN, 24DDR4, 2х750W | Мощность БП: 750 Вт.  Количество вентиляторов: не менее 8.  Горячая замена (Hot Plug) вентиляторов: есть.  Количество сетевых портов: 4.  Горячая замена (Hot Swap) дисков: есть.  Тип дисковой корзины: 3.5" (LFF).  Количество отсеков 3.5" Hot Swap: 4.  Интерфейс накопителей: SATA.  Тип видеокарты: встроенная.  Скорость сетевого адаптера: не менее1 Гбит/c.  Тип оперативной памяти: DDR4.  Высота стойки: 1U.  Макс. количество процессоров: не менее 2.  Сокет процессора: LGA3647.  Интерфейсы:  USB 3.1 Type A не менее 3, DVI, Ethernet Gigabit – RJ-45 x 4, VGA, SATA3.  Тип корпуса: Rack.  Название чипсета: Intel C621.  Поддержка RAID: есть.  Отсеки: 3.5" hot swap x 4. | 1 |
| 2 | Процес-сор | Intel Xeon  Silver 4210R -2.4GHz, 10x1024Kb +13,75Mb, socket LGA 3647 | Socket LGA 3647  Количество ядер 10 Количество потоков 20 Частота процессора 2.4 ГГц Частота процессора в режиме Turbo 3.2 ГГц  Кэш-память 13.75 МБ Технологический процесс 14 нм  Совместимость:  Максимальная конфигурация 2 процессора  Производитель серверов универсальный | 2 |
| 3 | ОЗУ | Серверная оперативная память DDR-4 16Gb ECC REG 2666MHz <PC4-21300> | Поддержка ECC: да  Тип памяти: DDR4 Форм-фактор:  Тактовая частота: 2666 МГц Пропускная способность: 21300 Мб/с | 4 |
| 4 | Накопи-тель | 1Tb WD Gold <7200rpm 128Mb SATA3> #WD1005FBYZ | Объём: 1 ТБ  Буферная память 128 МБ Скорость вращения шпинделя 7200 об/мин  Интерфейс SATA III  HDD lля сервера с наработкой на отказ не менее 2000000 ч:  Форм-фактор: 3,5” | 2 |

1. Техническое описание серверной программной части (операционная система), поставляемой c серверным оборудованием
2. Наименование.

Лицензия на операционную систему специального назначения «Astra Linux Special Edition» для 64-х разрядной платформы на базе процессорной архитектуры х86-64 (очередное обновление 1.7), уровень защищенности «Усиленный» («Воронеж»), РУСБ.10015-01 (ФСТЭК), способ передачи электронный, серверная до 2 сокетов, на срок действия исключительного права, с включенными обновлениями Тип 2 на 12 мес.

1. Требования соответствия законодательным и нормативным документам

Программное обеспечение должно быть включено в Единый реестр российских программ для электронных вычислительных машин и баз данных согласно постановлению правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

Операционная система должна иметь сертификат соответствия требованиям нормативных документов ФСТЭК России:

* «Требования безопасности информации к операционным системам» (ФСТЭК России, 2016);
* «Профиль защиты операционных систем типа «А» не ниже 4 класса ИТ.ОС.А4.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 4 уровня;
* «Требования по безопасности информации к средствам виртуализации» (ФСТЭК России, 2022) не ниже 4 класса защиты;

«Требования по безопасности информации к средствам контейнеризации» (ФСТЭК России, 2022) не ниже 4 класса защиты.

1. Основные требования к операционной системе.

1. Лицензионные права Заказчика операционной системы должны быть оформлены в соответствии с правилами фирмы-разработчика программного обеспечения и предоставлены Заказчику на неограниченное время. Перечень лицензий на право бессрочного обладания операционной системы, срок действия исключительного права, с включенными обновлениями Тип 2 должны быть указаны в личном кабинете пользователя(Заказчика) на электронном ресурсе фирмы-разработчика программного обеспечения (<https://lk-new.astralinux.ru>) во вкладке "Лицензии и сертификаты".

2. Поставляемая операционная система должна содержать следующие компоненты:

-Почтовый сервер\Сервер классических прикладных нагрузок\Сервер сканирования и печати\Сервер удаленных рабочих мест\Сервер для сетевых функций\Корпоративная офисная платформа\Платформа управления инфраструктурой\Сервер хранения файлов\ Сервер виртуализации\Сервер резервного копирования\Сервер домена\Сервер контейнеризации\Программно-определяемое хранилище\Сервер облачной виртуализации\ Сервер баз данных.

IV. 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 разграничения доступа;
* возможность создания защищенной среды виртуализации;
* возможность создания среды выполнения контейнеров и обеспечение работы с ними;

технологию контейнеризации с поддержкой изоляции процессов.

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.

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 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.  
  Должно обеспечиваться разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности.

Должно обеспечиваться 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, кроме указанных явно администратором безопасности.

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>), согласно Регламенту включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в банк данных угроз безопасности информации ФСТЭК России.

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 останова системных процессов операционной системы, вне зависимости от изменения пользователем своих привилегий в текущем сеансе работы.

V. Требования к функциональным возможностям операционной системы.

Операционная система должна быть предназначена для функционирования на средствах вычислительной техники с аппаратной платформой х86-64.

Операционная система должна поддерживать работу на ядре Linux версии не ниже 5.10.

Операционная система должна обеспечивать функционал в графическом исполнении:

* наличие средств создания и настройки служебных репозиториев используемого программного обеспечения, с поддержкой проверки зависимостей пакетной базы;
* 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 работы с архивами (zip, rar, 7zip, tar, tgz, tar.gz, tar.bz, tar.xz, iso).

Операционная система должна обеспечивать возможность создания точек восстановления (снапшотов) для последующего возвращения системы к исходному состоянию в случае сбоя.

Операционная система должна обеспечивать поддержку файловых систем и сетевых протоколов:

* ext2/3/4, fat, ntfs, iso9660, XFS, ZFS, BTRFS;
* TCP/IP, DHCP, DNS, FTP, TFTP, SMTP, IMAP, HTTP(S), NTP, SSH, NFS, SMB;
* 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 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.  
Совместимость операционной системы с средствами криптографической защиты информации (**КриптоПро, VipNet Client**) должна быть подтверждена наличием записи об операционной системе как среды функционирования в формуляре (правилах пользования) средств криптографической защиты информации.

Операционная система должна иметь подтверждённую совместимость со средствами антивирусной защиты.

Дополнительные функциональные компоненты:

* web-сервер Apache или эквивалент;
* почтовые сервисы и системы передачи почты: Exim, Dovecot, Postfix или эквивалент;
* средства мониторинга Zabbix или эквивалент;
* средство для работы с архивами;
* средства удаленного и терминального доступа: LTSP, VNC, RDP, RemoteApp или эквивалент;
* защищенный сервер печати;
* службы резервного копирования: Bacula, Rsync или эквивалент;
* система разграничения доступа к внешним устройствам;
* 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.