|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Краевое государственное бюджетное учреждение здравоохранения |  | Руководителю |  |  |
| Краевая клиническая больница |  |  |  |  |  |
| ул. П. Железняка, 3, г. Красноярск, 660022 |  |  |  |  |  |
| Телефон: 8 (391) 220-16-13 |  |  |  |  |  |
| Факс: 8 (391) 220-16-23 |  |  |  |  |  |
| Е-mail: kkb@ medqorod. ru |  |  |  |  |  |
| Http://www.kkb1. krasu.ru |  |  |  |  |  |
| ОКПО 01913234 |  |  |  |  |  |
| ИНН/КПП 2465030876/246501001 |  |  |  |  |  |
| 07.08.2019 г. №.652-19 |  |  |  |  |  |
| На №\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| О коммерческом предложении |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **Уважаемые господа!** |  |
| Прошу Вас предоставить коммерческое предложение на право поставки следующего товара: |
| **№ п/п** | **Наименование** | **Характеристики** | **Ед. изм.** | **Кол-во, шт** | **Цена, рублей** |
| 1 | Продление лицензий антивируса Касперского | Общие требованияАнтивирусные средства должны включать:• Программные средства антивирусной защиты для рабочих станций Windows.• Программные средства антивирусной защиты для рабочих станций MacOS.• Программные средства антивирусной защиты для рабочих станций Linux.• Программные средства антивирусной защиты для файловых серверов Windows.• Программные средства антивирусной защиты для файловых серверов Linux.• Программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов).• Программные средства централизованного управления, мониторинга и обновления.• Обновляемые базы данных сигнатур вредоносных программ и атак.• Эксплуатационную документацию на русском языке.Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.Требования к программным средствам антивирусной защиты для рабочих станций WindowsПрограммные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:• Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64;• Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64 SP1 и выше;• Microsoft Windows 8 Professional / Enterprise x86 / x64;• Microsoft Windows 8.1 Professional / Enterprise x86 / x64;• Microsoft Windows 10 Pro / Enterprise x86 / x64.Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:• Антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;• антивирусное сканирование по расписанию;• антивирусное сканирование подключаемых устройств;• эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;• нейтрализация действий активного заражения;• анализ поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;• анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;• блокирование действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;• возможность совершить откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;• возможность ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений. Динамически обновляемые настраиваемые списки приложений с определением уровня доверия;• облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;• антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE в том числе и защищенных паролем;• защита электронной почты от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP;• фильтр почтовых вложений с возможностью переименования или удаления заданных типов файлов;• Проверка трафика, поступающего на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;• блокировка баннеров и всплывающих окон на загружаемых Web-страницах;• распознавание и блокировка фишинговых и небезопасных сайтов;• наличие встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;• защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;• контроль сетевых соединений, устанавливаемых с помощью сетевых мостов, с возможностью блокировки одновременной установки нескольких сетевых соединений.• Наличие компонента, дающего возможность создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп). Компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме MD5 или SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения. Компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;• осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;• возможность записи в журнал событий о записи и/или удалении файлов на съемных дисках;• осуществление контроля работы пользователя с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;• наличие механизмов защиты от атак типа BadUSB;• запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.• Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;• возможность установки только выбранных компонентов программного средства антивирусной защиты;• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;• запуск задач по расписанию и/или сразу после загрузки операционной системы;• гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;• ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;• возможность проверки целостности антивирусной программы;• возможность добавления исключений из антивирусной проверки по хеш сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;• наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;• наличие защищенного хранилища для отчетов о работе антивируса;• возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;Требования к программным средствам централизованного управления, мониторинга и обновленияПрограммные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:• Microsoft Windows 10 Pro 32-разрядная / 64-разрядная.• Microsoft Windows 10 RS2 32-разрядная / 64-разрядная.• Microsoft Windows 10 Enterprise 32-разрядная / 64-разрядная.• Microsoft Windows 10 Education 32-разрядная / 64-разрядная.• Microsoft Windows 10 Pro RS1 32-разрядная / 64-разрядная.• Microsoft Windows 10 Enterprise RS1 32-разрядная / 64-разрядная.• Microsoft Windows 10 Education RS1 32-разрядная / 64-разрядная.• Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная.• Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная.• Microsoft Windows 8 Pro 32-разрядная / 64-разрядная.• Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная.• Microsoft Windows 7 Professional SP1 32-разрядная / 64-разрядная.• Microsoft Windows 7 Enterprise SP1 32-разрядная / 64-разрядная.• Microsoft Windows 7 Ultimate SP1 32-разрядная / 64-разрядная.• Microsoft Small Business Server 2008 Standard 64-разрядная.• Microsoft Small Business Server 2008 Premium 64-разрядная.• Microsoft Small Business Server 2011 Essentials 64-разрядная.• Microsoft Small Business Server 2011 Premium Add-on 64-разрядная.• Microsoft Small Business Server 2011 Standard 64-разрядная.• Microsoft Windows Server 2008 Datacenter SP1 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008 SP1 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008.• Microsoft Windows Server 2008 R2 Server Core 64-разрядная.• Microsoft Windows Server 2008 R2 Datacenter 64-разрядная.• Microsoft Windows Server 2008 R2 Datacenter SP1 64-разрядная.• Microsoft Windows Server 2008 R2 Enterprise 64-разрядная.• Microsoft Windows Server 2008 R2 Enterprise SP1 64-разрядная.• Microsoft Windows Server 2008 R2 Foundation 64-разрядная.• Microsoft Windows Server 2008 R2 Foundation SP1 64-разрядная.• Microsoft Windows Server 2008 R2 SP1 Core Mode 64-разрядная.• Microsoft Windows Server 2008 R2 Standard 64-разрядная.• Microsoft Windows Server 2008 R2 Standard SP1 64-разрядная.• Microsoft Windows Server 2012 Server Core 64-разрядная.• Microsoft Windows Server 2012 Datacenter 64-разрядная.• Microsoft Windows Server 2012 Essentials 64-разрядная.• Microsoft Windows Server 2012 Foundation 64-разрядная.• Microsoft Windows Server 2012 Standard 64-разрядная.• Microsoft Windows Server 2012 R2 Server Core 64-разрядная.• Microsoft Windows Server 2012 R2 Datacenter 64-разрядная.• Microsoft Windows Server 2012 R2 Essentials 64-разрядная.• Microsoft Windows Server 2012 R2 Foundation 64-разрядная.• Microsoft Windows Server 2012 R2 Standard 64-разрядная.• Windows Storage Server 2008 R2 64-разрядная.• Windows Storage Server 2012 64-разрядная.• Windows Storage Server 2012 R2 64-разрядная.• Microsoft Windows Server 2016 64-разрядная.Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:• Microsoft SQL Server 2008 Express 32-разрядная.• Microsoft SQL 2008 R2 Express 64-разрядная.• Microsoft SQL 2012 Express 64-разрядная.• Microsoft SQL 2014 Express 64-разрядная.• Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная.• Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная.• Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная.• Microsoft SQL Server 2012 (все редакции) 64-разрядная.• Microsoft SQL Server 2014 (все редакции) 64-разрядная.• Microsoft SQL Server 2016 (все редакции) 64-разрядная.• Microsoft Azure SQL Database.• MySQL 5.5 32-разрядная / 64-разрядная.• MySQL Enterprise 5.5 32-разрядная / 64-разрядная.• MySQL 5.6 32-разрядная / 64-разрядная.• MySQL Enterprise 5.6 32-разрядная / 64-разрядная.• MySQL 5.7 32-разрядная / 64-разрядная. MySQL Enterprise 5.7 32-разрядная / 64-разрядная.Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:• Установка системы управления антивирусной защиты из единого дистрибутива.• Выбор установки в зависимости от количества защищаемых узлов.• Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.• Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.• Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.• Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.• Централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления.• Сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;• Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки.• Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности. Должна быть реализована возможность поддержки иерархии таких триггеров.• Автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.• Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения.• Распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере.• Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне.• Создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня.• Поддержка мультиарендности (multi-tenancy) для серверов управления.• Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.• Доступ к облачным серверам производителя антивирусного ПО через сервер управления.• Автоматическое распространение лицензии на клиентские компьютеры.• Инвентаризация установленного ПО и оборудования на компьютерах пользователей.• Возможность подключения по RDP или штатными средствами из консоли управления. Пользователю должен выводиться запрос на разрешение дистанционного подключения.• Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.• Функция управления мобильными устройствами через сервер Exchange ActiveSync.• Функция управления мобильными устройствами через сервер iOS MDM.• Возможность отправки SMS-оповещений о заданных событиях.• Централизованная установка приложений на управляемые мобильные устройства.• Централизованная установка сертификатов на управляемые мобильные устройства.• Поддержка функциональности управления шифрованием данных.• Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.• Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления.• Построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд.• Наличие преднастроенных стандартных отчетов о работе системы.• Экспорт отчетов в файлы форматов PDF и XML.• Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.• Создание внутренних учетных записей для аутентификации на сервере управления.• Создание резервной копии системы управления встроенными средствами системы управления.• Поддержка Windows Failover Clustering.• Поддержка интеграции с Windows сервисом Certificate Authority.• Наличие веб-консоли управления приложением.• Наличие портала самообслуживания пользователей. Портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя.• Наличие системы контроля возникновения вирусных эпидемий.Требования к обновлению антивирусных базОбновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:• Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток.• Множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации.• Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.Требования к эксплуатационной документацииЭксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:• Руководство пользователя (администратора).Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.Требования к технической поддержкеТехническая поддержка антивирусного программного обеспечения должна:• Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет.• Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов. | шт. | 750 |  |
| 2 | Продление лицензий антивируса Касперского | Общие требованияАнтивирусные средства должны включать:• Программные средства антивирусной защиты для рабочих станций Windows.• Программные средства антивирусной защиты для рабочих станций MacOS.• Программные средства антивирусной защиты для рабочих станций Linux.• Программные средства антивирусной защиты для файловых серверов Windows.• Программные средства антивирусной защиты для файловых серверов Linux.• Программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов).• Программные средства централизованного управления, мониторинга и обновления.• Обновляемые базы данных сигнатур вредоносных программ и атак.• Эксплуатационную документацию на русском языке.Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.Требования к программным средствам антивирусной защиты для файловых серверов WindowsПрограммные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:Поддерживаемые 32-битные операционные системы:• Windows Server 2003 Standard / Enterprise / Datacenter с SP2 или выше.• Windows Server 2003 R2 Standard / Enterprise / Datacenter с SP2 или выше.• Windows Server 2008 Standard / Enterprise / Datacenter с SP1 или выше.• Windows Server 2008 Core Standard / Enterprise / Datacenter с SP1 или выше.Поддерживаемые 64-битные операционные системы:• Windows Server 2003 Standard / Enterprise / Datacenter с SP2 или выше.• Windows Server 2003 R2 Standard / Enterprise / Datacenter с SP2 или выше.• Windows Server 2008 Standard / Enterprise / Datacenter с SP1 или выше.• Windows Server 2008 Core Standard / Enterprise / Datacenter с SP1 или выше.• Microsoft Small Business Server 2008 Standard / Premium.• Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с SP1 или выше.• Windows Server 2008 R2 Core/Standard/Enterprise/Datacenter с SP1 или выше.• Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше.• Microsoft Small Business Server 2011 Essentials / Standard.• Windows Server 2012 Foundation / Essentials / Standard / Datacenter / MultiPoint Server.• Windows Server 2012 Core Standard / Datacenter.• Windows Storage Server 2012.• Windows Hyper-V Server 2012.• Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter.• Windows Server 2012 R2 Core Standard / Datacenter.• Windows Storage Server 2012 R2.• Windows Hyper-V Server 2012 R2.• Windows Server 2016 Essentials / Standard / Datacenter / MultiPoint Premium Server.• Windows Server 2016 Core Standard / Datacenter.• Windows Storage Server 2016.• Windows Hyper-V Server 2016.Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:• Антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: Серверов терминалов и принт-серверов; Серверов приложений и контроллеров доменов; Файловых серверов;• антивирусное сканирование по команде пользователя или администратора и по расписанию;• запуск задач по расписанию и/или сразу после загрузки операционной системы;• облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;• антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем;• защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;• непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting). Проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными. Анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;• Возможность проверки контейнеров Microsoft Windows.• Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;• Механизмы защиты от эксплуатирования уязвимостей в памяти процессов с помощью техник снижения рисков;• ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;• проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;• настройки проверки критических областей сервера в качестве отдельной задачи;• регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;• Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);• ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;• возможность указания количества рабочих процессов антивируса в ручную;• возможность отключить графический интерфейс;• наличие удаленной и локальной консоли управления;• управления параметрами антивируса из командной строки;• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;• управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;Требования к программным средствам централизованного управления, мониторинга и обновленияПрограммные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:• Microsoft Windows 10 Pro 32-разрядная / 64-разрядная.• Microsoft Windows 10 RS2 32-разрядная / 64-разрядная.• Microsoft Windows 10 Enterprise 32-разрядная / 64-разрядная.• Microsoft Windows 10 Education 32-разрядная / 64-разрядная.• Microsoft Windows 10 Pro RS1 32-разрядная / 64-разрядная.• Microsoft Windows 10 Enterprise RS1 32-разрядная / 64-разрядная.• Microsoft Windows 10 Education RS1 32-разрядная / 64-разрядная.• Microsoft Windows 8.1 Pro 32-разрядная / 64-разрядная.• Microsoft Windows 8.1 Enterprise 32-разрядная / 64-разрядная.• Microsoft Windows 8 Pro 32-разрядная / 64-разрядная.• Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная.• Microsoft Windows 7 Professional SP1 32-разрядная / 64-разрядная.• Microsoft Windows 7 Enterprise SP1 32-разрядная / 64-разрядная.• Microsoft Windows 7 Ultimate SP1 32-разрядная / 64-разрядная.• Microsoft Small Business Server 2008 Standard 64-разрядная.• Microsoft Small Business Server 2008 Premium 64-разрядная.• Microsoft Small Business Server 2011 Essentials 64-разрядная.• Microsoft Small Business Server 2011 Premium Add-on 64-разрядная.• Microsoft Small Business Server 2011 Standard 64-разрядная.• Microsoft Windows Server 2008 Datacenter SP1 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008 Enterprise SP1 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008 Foundation SP2 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008 SP1 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008 Standard SP1 32-разрядная / 64-разрядная.• Microsoft Windows Server 2008.• Microsoft Windows Server 2008 R2 Server Core 64-разрядная.• Microsoft Windows Server 2008 R2 Datacenter 64-разрядная.• Microsoft Windows Server 2008 R2 Datacenter SP1 64-разрядная.• Microsoft Windows Server 2008 R2 Enterprise 64-разрядная.• Microsoft Windows Server 2008 R2 Enterprise SP1 64-разрядная.• Microsoft Windows Server 2008 R2 Foundation 64-разрядная.• Microsoft Windows Server 2008 R2 Foundation SP1 64-разрядная.• Microsoft Windows Server 2008 R2 SP1 Core Mode 64-разрядная.• Microsoft Windows Server 2008 R2 Standard 64-разрядная.• Microsoft Windows Server 2008 R2 Standard SP1 64-разрядная.• Microsoft Windows Server 2012 Server Core 64-разрядная.• Microsoft Windows Server 2012 Datacenter 64-разрядная.• Microsoft Windows Server 2012 Essentials 64-разрядная.• Microsoft Windows Server 2012 Foundation 64-разрядная.• Microsoft Windows Server 2012 Standard 64-разрядная.• Microsoft Windows Server 2012 R2 Server Core 64-разрядная.• Microsoft Windows Server 2012 R2 Datacenter 64-разрядная.• Microsoft Windows Server 2012 R2 Essentials 64-разрядная.• Microsoft Windows Server 2012 R2 Foundation 64-разрядная.• Microsoft Windows Server 2012 R2 Standard 64-разрядная.• Windows Storage Server 2008 R2 64-разрядная.• Windows Storage Server 2012 64-разрядная.• Windows Storage Server 2012 R2 64-разрядная.• Microsoft Windows Server 2016 64-разрядная.Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:• Microsoft SQL Server 2008 Express 32-разрядная.• Microsoft SQL 2008 R2 Express 64-разрядная.• Microsoft SQL 2012 Express 64-разрядная.• Microsoft SQL 2014 Express 64-разрядная.• Microsoft SQL Server 2008 (все редакции) 32-разрядная / 64-разрядная.• Microsoft SQL Server 2008 R2 (все редакции) 64-разрядная.• Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная.• Microsoft SQL Server 2012 (все редакции) 64-разрядная.• Microsoft SQL Server 2014 (все редакции) 64-разрядная.• Microsoft SQL Server 2016 (все редакции) 64-разрядная.• Microsoft Azure SQL Database.• MySQL 5.5 32-разрядная / 64-разрядная.• MySQL Enterprise 5.5 32-разрядная / 64-разрядная.• MySQL 5.6 32-разрядная / 64-разрядная.• MySQL Enterprise 5.6 32-разрядная / 64-разрядная.• MySQL 5.7 32-разрядная / 64-разрядная. MySQL Enterprise 5.7 32-разрядная / 64-разрядная.Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:• Установка системы управления антивирусной защиты из единого дистрибутива.• Выбор установки в зависимости от количества защищаемых узлов.• Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.• Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.• Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.• Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.• Централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления.• Сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;• Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки.• Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности. Должна быть реализована возможность поддержки иерархии таких триггеров.• Автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.• Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставка обновлений на рабочие места пользователей сразу после их получения.• Распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере.• Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне.• Создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня.• Поддержка мультиарендности (multi-tenancy) для серверов управления.• Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.• Доступ к облачным серверам производителя антивирусного ПО через сервер управления.• Автоматическое распространение лицензии на клиентские компьютеры.• Инвентаризация установленного ПО и оборудования на компьютерах пользователей.• Возможность подключения по RDP или штатными средствами из консоли управления. Пользователю должен выводиться запрос на разрешение дистанционного подключения.• Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.• Функция управления мобильными устройствами через сервер Exchange ActiveSync.• Функция управления мобильными устройствами через сервер iOS MDM.• Возможность отправки SMS-оповещений о заданных событиях.• Централизованная установка приложений на управляемые мобильные устройства.• Централизованная установка сертификатов на управляемые мобильные устройства.• Поддержка функциональности управления шифрованием данных.• Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.• Возможность указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления.• Построение графических отчетов как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд.• Наличие преднастроенных стандартных отчетов о работе системы.• Экспорт отчетов в файлы форматов PDF и XML.• Централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.• Создание внутренних учетных записей для аутентификации на сервере управления.• Создание резервной копии системы управления встроенными средствами системы управления.• Поддержка Windows Failover Clustering.• Поддержка интеграции с Windows сервисом Certificate Authority.• Наличие веб-консоли управления приложением.• Наличие портала самообслуживания пользователей. Портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя.• Наличие системы контроля возникновения вирусных эпидемий.Требования к обновлению антивирусных базОбновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:• Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток.• Множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации.• Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.Требования к эксплуатационной документацииЭксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:• Руководство пользователя (администратора).Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.Требования к технической поддержкеТехническая поддержка антивирусного программного обеспечения должна:• Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет.• Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов. | шт. | 10 |  |  |  |
|  |  |  |  |  |  |  |  |
| Срок оказания услуг: с 01 января 2020г. по 31 декабря 2020г... |
|  |  |  |  |  |  |  |  |
| Цена должна быть указана с учетом доставки до КГБУЗ «Краевая клиническая больница» г.Красноярск, ул. Партизана Железняка, 3. |
|  |  |  |  |  |  |  |  |
| Информацию необходимо направить по факсу +7 (391) 220-16-23, электронной почте zakupki@medgorod.ru или по адресу г. Красноярск, ул. Партизана Железняка 3-б, отдел обеспечения государственных закупок, тел. 220-16-04 |
|  |  |  |  |  |  |  |  |
| Предложения принимаются в срок до 15.08.2019 17:00:00 по местному времени. |
|  |  |  |  |  |  |  |  |
| Руководитель контрактной службы\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Куликова И.О./ |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |