Приложение № 2

к Извещению о проведении запроса котировок

от «05» декабря 2013 г. № 38

**Техническое задание на поставку программного обеспечения для МБУЗ «ГКП №4»**

|  |  |  |
| --- | --- | --- |
| **Наименование (торговая марка)** | **Характеристика неисключительных прав (описание)** | **Кол-во, ед. изм.** |
| **Продление лицензии Kaspersky Endpoint Security для бизнеса Стандартный Russian Edition. 1 year Renewal License *(****или эквивалент***)** | Антивирусные средства должны включать:  • программные средства антивирусной защиты для рабочих станций Windows;  • программные средства антивирусной защиты для файловых серверов Windows;  • программные средства антивирусной защиты для файловых серверов Linux;  • программные средства антивирусной защиты для файловых серверов Novell Netware;  • программные средства антивирусной защиты для мобильных устройств (смартфонов);  • 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 языке.  Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке.  **Требования к программным средствам антивирусной защиты для рабочих станций Windows**  Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на рабочих станциях, работающих под управлением операционных систем следующих версий:  • Microsoft Windows XP Professional (SP3 или выше)  •Microsoft Windows Vista Business/Enterprise/ Ultimate (SP2 или выше)  •Microsoft Windows Vista Business/Enterprise/ Ultimate x64 (SP2 или выше)  •Microsoft Windows 7 Professional/Enterprise/ Ultimate  •Microsoft Windows 7 Professional/Enterprise/ Ultimate x64  • Microsoft Windows 8 Professional/Enterprise  • Microsoft Windows 8 Professional/Enterprise x64 Edition  Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:  • Резидентный антивирусный мониторинг.  • Программные средства защиты от сетевых атак.  • Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.  • Обнаружение скрытых процессов.  • Антивирусное сканирование по команде пользователя или администратора и по расписанию.  • Антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.  • Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем.  • Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу.  • Защита электронной корреспонденции, как от вредоносных программ, так и от спама, с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента; независимо от типа протокола (в том числе MAPI, HTTP) — в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и The Bat!.  • Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP.  • Проверка скриптов — проверка скриптов, обрабатываемых в Microsoft Internet Explorer, а также WSH-скриптов (таких как Java Script, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в интернете.  • Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами.  • Запуск задач по расписанию и/или сразу после загрузки операционной системы.  • Защита от еще не известных вредоносных программ на основе анализа их поведения и контроля изменений системного реестра, с возможностью автоматического восстановления изменённых вредоносной программой значений системного реестра.  • Автоматический контроль программ, запускаемых на компьютере пользователя, осуществляющий контроль активности программ и ограничивающий выполнение опасных действий.  • Защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные.  • Проверка протокола IPv6.  • Защита от программ-маскировщиков, программ автодозвона на платные сайты.  • Блокировка баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц.  • Распознавание и блокировка фишинг-сайтов.  • Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения по пути нахождения программы, метаданным, контрольной сумме MD5.  • Осуществление контроля работы пользователя с внешними устройствами ввода/вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям.  • Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.  • Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.  • Интеграция с системой обновления Windows Update для установки патчей, закрывающих обнаруженные уязвимости.  • Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.  • Настройка проверки критических областей компьютера в виде отдельной задачи.  • Технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющие избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.  • Возможность установки только выбранных компонентов программного средства антивирусной защиты.  • Централизованное управление с помощью единой системы управления.  **Требования к программным средствам антивирусной защиты для файловых серверов Windows**  Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на серверах, работающих под управлением операционных систем следующих версий:  • Microsoft Small Business Server 2011 Essentials х64 Edition  • Microsoft Small Business Server 2011 Standard х64 Edition  • Microsoft Windows Server 2012 Foundation х64 Edition  • Microsoft Windows Server 2012 Essentials х64 Edition  • Microsoft Windows Server 2012 Standard х64 Edition  • Microsoft Windows Server 2008 R2 Standard / Enterprise х64 Edition SP0 и выше  • Microsoft Windows Server 2008 Standard / Enterprise х64 Edition SP2 и выше  • Microsoft Windows Server 2008 Standard / Enterprise SP2 и выше  • Microsoft Windows Server 2003 R2 Standard / Enterprise SP2 и выше  • Microsoft Windows Server 2003 R2 Standard х64 Edition SP2 и выше  • Microsoft Windows Server 2003 Standard SP2  • Microsoft Windows Server 2003 Standard х64 Edition SP2  Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:  • резидентный антивирусный мониторинг;  • эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;  • программные средства защиты от сетевых атак;  • защиту от хакерских атак, путем использования межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа;  • облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;  • обнаружение скрытых процессов;  • антивирусное сканирование по команде пользователя или администратора и по расписанию;  • антивирусную проверку и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;  • антивирусную проверку и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем;  • запуск задач по расписанию и/или сразу после загрузки операционной системы;  • защиту от еще не известных вредоносных программ, принадлежащих зарегистрированным семействам, на основе эвристического анализа;  • ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;  • 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;  • наличием множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);  • технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, защита файлов приложения от несанкционированного доступа и изменения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющими избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;  • централизованно управляться с помощью единой системы управления.  **Требования к программным средствам антивирусной защиты для файловых серверов Linux**  Программные средства антивирусной защиты серверов под управлением ОС Linux должны функционировать под управлением следующих платформ:  32-битные платформы:  Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92);  Red Hat Enterprise Linux 5.5 Server 2.6.18-186.el5  Red Hat Enterprise Linux 6 Server 2.6.32-71.el6.i686  Fedora 9 (kernel 2.6.25);  Fedora 13 2.6.33.3-85.fc13.i686.PAE;  CentOS-5.5 2.6.18-194.el5;  Novel Open Enterprise Server 2 (kernel 2.6.16.46-0.12);  Novel Open Enterprise Server 2 SP2 2.6.16.60-0.54.5-default;  SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21);  SUSE Linux Enterprise Server 10 SP3 2.6.16.60-0.54.5-default;  SUSE Linux Enterprise Server 11 SP1 2.6.32.12-0.7-pae;  OpenSUSE Linux 11.0 (kernel 2.6.25);  OpenSUSE Linux 11.3 2.6.34-12-desktop;  Debian GNU/Linux 4.0 r4 (kernel 2.6.24);  Debian GNU/Linux 5.0.5 2.6.26-2-686;  Mandriva Corporate Server 4 (kernel 2.6.12);  Mandriva Enterprise Server 5.1 2.6.27.45-desktop-1mnb;  Ubuntu 8.04.1 Server Edition (kernel 2.6.25);  Ubuntu 10.04 Server Edition 2.6.32-21-generic;  FreeBSD 7.3-RELEASE;  FreeBSD 8.1-RELEASE.  64-битные платформы:  Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92);  Red Hat Enterprise Linux 5.5 server 2.6.18-194.el5;  Red Hat Enterprise Linux 6 Server 2.6.32-71.el6.x86\_64;  Fedora 9 (kernel 2.6.25);  Fedora 13 2.6.33.3-85.fc13.x86\_64;  CentOS-5.5 2.6.18-194.el5;  SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21);  SUSE Linux Enterprise Server 10 SP3 2.6.16.60-0.54.5-default;  SUSE Linux Enterprise Server 11 SP1 2.6.32.12-0.7-default;  Novell Open Enterprise Server 2 SP2 2.6.16.60-0.54.5-default;  OpenSUSE Linux 11.3 2.6.34-12-desktop;  OpenSUSE Linux 11.0 (kernel 2.6.25);  Debian GNU/Linux 5.0.5 2.6.26-2-amd64;  Ubuntu 10.04 Server Edition 2.6.32-21-generic;  FreeBSD 7.3-RELEASE;  FreeBSD 8.1-RELEASE.  Программные средства антивирусной защиты серверов под управлением ОС Linux должны обеспечивать реализацию следующих функциональных возможностей:  резидентный антивирусный мониторинг;  антивирусное сканирование по команде пользователя или администратора и по расписанию;  антивирусную проверку и лечение файлов в архивах;  запуск задач по расписанию и/или сразу после загрузки операционной системы;  помещение подозрительных и поврежденных объектов на карантин;  формирование отчетов в форматах HTML, CSV, PDF и XLS;  возможность перехвата и проверки файловых операций на уровне SAMBA;  сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;  удаленно через веб-браузер управлять антивирусом и настраивать его;  централизованно управляться с помощью единой системы управления.  **Требования к программным средствам антивирусной защиты для файловых серверов Novell Netware**  Программные средства антивирусной защиты файловых систем серверов под управлением ОС Novell Netware должны функционировать на версиях ОС Novell Netware 5.x SP6 или выше, 6.0 SP3 или выше, 6.5 SP3 или выше.  Программные средства антивирусной защиты файловых систем серверов под управлением ОС Novell Netware должны обеспечивать реализацию следующих функциональных возможностей:  проверку на присутствие вирусов всех запускаемых и изменяемых файлов, лечение, а при его невозможности – удаление зараженных объектов;  последовательную проверку файлов сервера по запросу администратора или по расписанию с заданной частотой, при этом может производиться лечение и/или удаление зараженных объектов;  обновление антивирусных баз и распространение обновлений на другие серверы сети Novell NetWare. Обновление может происходить по расписанию, рассылкой на предопределённые серверы. Предусмотрена возможность создания резервных копий обновляемых файлов для обеспечения возможности отката антивирусных баз до предыдущей версии;  размещение зараженных или подозрительных файлов в специальном хранилище – карантине. Помещенные на карантин файлы могут быть проанализированы администратором и/или отправлены на исследование в компанию – разработчик антивирусных решений;  создание подробных отчетов по результатам проверок ресурсов сервера по требованию, его постоянной защиты и обновления антивирусных баз. Возможность просмотра журналов и вывода их на печать;  сохранение резервной копии всех подозрительных или зараженных объектов перед лечением или удалением, что позволяет восстановить данные в случае возникновения сбоев или ошибок при лечении или удалении;  информирование администраторов и пользователей о законченных проверках, а также предупреждение о найденных вредоносных объектах средствами сети Novell NetWare и по электронной почте.  **Требования к программным средствам антивирусной защиты смартфонов**  Программные средства для антивирусной защиты смартфонов должны функционировать под управлением мобильных ОС:  • Android 2.2 – 2.x, 4.0; Android 3 for tablets  • iOS 4, 5  • BlackBerry 4.5 – 6.0, 7.0; BlackBerry for tablets  • Windows Mobile 5.0 – 6.5  • Symbian 9.1 – 9.3, Symbian^3, Anna, Belle  Программные средства для антивирусной защиты смартфонов должны обеспечивать следующую функциональность:  • постоянную защиту файловой системы смартфона, перехват и проверку:  • всех входящих объектов, передающихся с помощью беспроводных соединений (инфракрасный порт, Bluetooth), сообщений EMS и MMS, при синхронизации с персональным компьютером и загрузке файлов через браузер;  • файлов, открываемых на смартфоне;  • программ, устанавливаемых из интерфейса смартфона.  • проверку объектов файловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию;  • надежное изолирование зараженных объектов в карантинном хранилище;  • обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов;  • блокирование нежелательных SMS и MMS сообщений;  • шифрование наиболее важных файлов, папок и карты памяти;  • возможность скрывать важные контакты и историю общения с ними;  • осуществлять функцию «антивор», т.е. обеспечивать блокировку мобильного устройства, удаление данных, сообщений и книги контактов, получение координат местоположения, а также определение, у кого находится пропавшее устройство.  **Требования к системе управления антивирусной защитой**  Программные средства управления для защищаемых рабочих станций, файловых серверов и смартфонов должны функционировать на следующих операционных системах:  Сервер администрирования:  • Microsoft Windows XP Professional SP2 и выше  • Microsoft Windows XP Professional x64 и выше  • Microsoft Windows Server 2003 и выше  • Microsoft Windows Server 2003 x64 и выше  • Microsoft Windows Vista SP1 и выше  • Microsoft Windows Vista x64 SP1 и всеми текущими обновлениями  • Microsoft Windows Server 2008  • Microsoft Windows Server 2008, развернутая в режиме Server Core  • Microsoft Windows Server 2008 x64 SP1 и всеми текущими обновлениями  • Microsoft Windows Server 2008 R2  • Microsoft Windows Server 2012  • Microsoft Windows Small Business Server 2003  • Microsoft Windows Small Business Server 2008  • Microsoft Windows Small Business Server 2011  • Microsoft Windows 7 Professional/Enterprise/Ultimate  • Microsoft Windows 7 Professional/Enterprise/Ultimate x64  • Microsoft Windows 8  • Microsoft Windows 8 x64  Сервером администрирования должна использоваться одна из следующих СУБД:  • Microsoft SQL Express 2005  • Microsoft SQL Express 2008  • Microsoft SQL Express 2008 R2  • Microsoft SQL Express 2012  • Microsoft SQL Server 2005  • Microsoft SQL Server 2008  • Microsoft SQL Server 2008 R2  • Microsoft SQL Server 2012  • MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91  • MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90  Консоль администрирования:  • Microsoft Windows XP Professional SP2 и выше  • Microsoft Windows XP Professional x64 и выше  • Microsoft Windows Server 2003 и выше  • Microsoft Windows Server 2003 x64 и выше  • Windows Small Business Server 2003  • Microsoft Windows Vista SP1 и выше  • Microsoft Windows Vista x64 SP1 и всеми текущими обновлениями  • Microsoft Windows Server 2008  • Microsoft Windows Server 2008 x64 SP1 и всеми текущими обновлениями  • Windows Small Business Server 2008 x64  • Microsoft Windows Server 2008 x64 R2  • Microsoft Windows Server 2008 x64 R2 SP1  • Windows Small Business Server 2011 x64  • Microsoft Windows 8  • Microsoft Windows 8 x64  • Microsoft Windows 7 Professional/Enterprise/Ultimate SP1  • Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1  Агент администрирования:  • программные требования должны соответствовать требованиям к программным средствам антивирусной защиты.  Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:  • установка системы антивирусной защиты из единого дистрибутива;  • выбор установки в зависимости от количества защищаемых узлов;  • создание групп логической сети на основе структуры Active Directory;  • автоматическое распределение компьютеров по группам управления, в случае появления новых компьютеров в сети;  • централизованную установку/обновление/удаление программных средств антивирусной защиты, настройку, администрирование, просмотр отчетов и статистической информации по их работе;  • централизованное удаление несовместимых приложений;  • централизованное управление установкой/запуском программ на компьютерах пользователей с возможностью контроля программ по пути нахождения программы, метаданным, MD5 контрольной сумме и возможностью присвоения привилегий определенным пользователям;  • централизованное управление доступом к веб-ресурсам с компьютеров пользователей, с возможностью фильтрации по категориям и типу данных загружаемого контента, гибко задавать параметры времени действия правил и возможностью присвоения привилегий определенным пользователям;  • наличие различных методов установки антивирусных приложений: удаленный - RPC, GPO, агент администрирования, локальный - автономный пакет установки;  • удаленная установка программных средств антивирусной защиты с последней версией баз приложения;  • автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;  • автоматизированный поиск уязвимостей, в установленных приложения и операционной системе, на компьютерах пользователей;  • тестирование загруженных обновлений средствами сервера администрирования перед распространением на клиентские машины; доставку 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;  • централизованное осуществление контроля работы пользователя с внешними устройствами ввода / вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создавать доверенные устройства по их идентификатору и возможностью предоставлять привилегии, для запуска внешних устройств, определенным пользователям;  • построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;  • создание виртуальных серверов управления антивирусным приложением;  • 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;  • централизованный сбор информации и создание отчетов о состоянии антивирусной защиты;  • инвентаризация установленного ПО и оборудования на компьютерах пользователей;  • наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройку рассылки почтовых уведомлений о них;  • встроенная система управления образами ОС: создание образа ОС с шаблонного компьютера с возможностью установки этого образа на определенные компьютеры;  • централизованная установка приложений сторонних производителей на все или выбранные компьютеры;  • функция для управления мобильными устройствами сервер Exchange ActiveSync;  • функция для управления мобильными устройствами сервер iOS MDM;  • возможность отправки SMS-сообщений мобильным пользователям;  • централизованная установка приложений на управляемые мобильные устройства;  • централизованная установка сертификатов на управляемые мобильные устройства;  • централизованный сбор информации о всех установленных на клиентских компьютерах приложениях;  • интеграция с CISCO NAC и MS NAP;  • экспорта 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;  • поддержка Windows Failover Clustering;  • наличие веб-консоли управления приложением;  • наличие системы контроля возникновения вирусных эпидемий.  Требования к обновлению антивирусных баз  Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:  • регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз антиспама не реже одного раза в 5 минут;  • 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 документации  Эксплуатационная 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 поддержке  Техническая поддержка антивирусного программного обеспечения должна:  • Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации круглосуточно без праздников и выходных 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. | Лицензия на 163 устройства |