Приложение № 2

к Извещению о проведении запроса котировок

от «08» декабря 2011 г. № 106

**Техническое задание на поставку антивирусной программы для МУЗ «ГКП №4»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **наименование** | **Технические характеристики** | **Кол-во** | **Цена** |
| 1 | Лицензия Kaspersky Business Space Security Russian Edition. 150-249 Пользователей  1 год Продление Лицензии | • программные средства антивирусной защиты рабочих станций и серверов;  • программные средства антивирусной защиты мобильных устройств (смартфонов);  • программные средства централизованного управления, мониторинга и обновления;  • обновляемые базы данных сигнатур вредоносных программ и атак;  • эксплуатационную документацию на русском языке. | 163 |  |
|  | **Итог** |  |  | 57 597,68 |

**Технические характеристики АПО.**

**Программные средства антивирусной защиты систем рабочих станций под управлением семейства ОС Microsoft 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;

∙             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;

∙             защиту электронной корреспонденции, как от вредоносных программ, так и от спама. Проверку трафика на следующих протоколах:

* IMAP, SMTP, POP3, независимо от используемого почтового клиента;
* NNTP (только проверка на вирусы), независимо от 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!;

∙             Защиту HTTP-трафика - проверку всех объектов, поступающих на компьютер пользователя по протоколу HTTP, FTP;

∙             Проверку скриптов - проверку всех скриптов, обрабатываемых в Microsoft Internet Explorer, а также любых WSH-скриптов (JavaScript, 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;

∙             защиту от еще не известных вредоносных программ на основе анализа их поведения и контроле изменений системного реестра, с возможностью автоматического восстановления изменённых вредоносной программой значений системного реестра;

∙             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, включая беспроводные;

∙             защиту от программ-маскировщиков, программ автодозвона на платные сайты, блокировку баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц и распознавание фишинг-сайтов;

∙             осуществлять контроль работы пользователя с внешними устройствами ввода / вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных.

∙             ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

∙             гибкого управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

∙             настройки проверки критических областей компьютера в качестве отдельной задачи;

∙             технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющих избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.

**Программные средства антивирусной защиты файловых систем серверов под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей**:

∙             резидентный антивирусный мониторинг;

∙             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;

∙             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.