УТВЕРЖДАЮ
Руководитель
отделения _____

«06» 11 2013 г.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

1. Наименование закупки:

Поставка антивирусного программного обеспечения.

2. Технические требования к поставке товара/выполнению работ/оказанию услуг:

№ п/п	Парт номер	Описание	Кол-во
1	KL4863RAVFS	Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 1000-1499 Node 1 year Base License	1000

Предложение аналогов не допускается в соответствии с п.12.2.2 ст. 12.2 ЕОСЗ и на основании приказа ОАО «Атомэнергомаш» №33/307-П от 19.09.2012

Общие требования

Антивирусное программное обеспечение должно включать:

- программные средства антивирусной защиты для рабочих станций Windows;
- программные средства антивирусной защиты для рабочих станций Mac OS;
- программные средства антивирусной защиты для рабочих станций Linux;
- программные средства антивирусной защиты для файловых серверов Windows;
- программные средства антивирусной защиты для файловых серверов Mac OS;
- программные средства антивирусной защиты для файловых серверов Linux;
- программные средства антивирусной защиты для файловых серверов Novell Netware;
- программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows;
- 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 антивирусному программному обеспечению для защиты рабочих станций Windows

Антивирусное программное обеспечение для защиты рабочих станций Windows должно функционировать на рабочих станциях, работающих под управлением операционных систем следующих версий:

- Microsoft Windows XP Professional SP2 и выше
- Microsoft Windows XP Professional x64 Edition SP2
- 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

Антивирусное программное обеспечение для защиты рабочих станций Windows должно 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 от вредоносных программ, 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.
- 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.
- 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 антивирусному программному обеспечению для защиты файловых серверов Windows

Антивирусное программное обеспечение для защиты файловых серверов Windows должно функционировать на серверах, работающих под управлением операционных систем следующих версий:

- Microsoft Small Business Server 2011 Essentials x64 Edition
- Microsoft Small Business Server 2011 Standard x64 Edition
- Microsoft Windows Server 2012 Foundation x64 Edition
- Microsoft Windows Server 2012 Essentials x64 Edition
- Microsoft Windows Server 2012 Standard x64 Edition
- Microsoft Windows Server 2008 R2 Standard / Enterprise x64 Edition SP0 и выше
- Microsoft Windows Server 2008 Standard / Enterprise x64 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 x64 Edition SP2 и выше
- Microsoft Windows Server 2003 Standard SP2
- Microsoft Windows Server 2003 Standard x64 Edition SP2

Антивирусное программное обеспечение для защиты файловых серверов Windows должно 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 системе управления антивирусным программным обеспечением

Программные средства управления для защищаемых рабочих станций, файловых серверов 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;
- 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;
- 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 антивирусным программным обеспечением, должна детально описывать процесс установки, настройки и эксплуатации соответствующего антивирусного программного обеспечение.

3. Требования к гарантии качества

Поставщик должен обладать необходимыми лицензиями или свидетельствами о допуске на поставку продукции, подлежащей лицензированию в соответствии с действующим законодательством РФ, обладать необходимыми сертификатами на продукцию в соответствии с действующим законодательством РФ.

4. Требования к гарантийному сроку и условиям гарантийного обслуживания

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.

5. Требования к объему технической 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.

6. Место поставки товара/выполнения работ/оказания услуг:

ОАО ОКБ «Гидропресс»,142103, Московская область, г. Подольск, ул. Орджоникидзе, д.21.

Оригиналы документов доставляются курьером Исполнителя.

7. Срок поставки товара/выполнения работ/оказания услуг:

Срок поставки лицензий 20 рабочих дней со дня подписания договора обеими Сторонами.

Подписи:

Руководитель отдела А.В.Саблин

06.11.13