**II. ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

1. **Предмет муниципального контракта:** оказание услуг по продлению лицензий на подсистему централизованной антивирусной обработки.
2. **Сроки передачи прав:** с момента заключения муниципального контракта до 31 июля 2020 г.
3. **Место передачи прав:** 628260, Ханты-Мансийский автономный округ Югра, г. Югорск, ул. Геологов, 9.
4. **Количество мест:** 42

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование услуг | Характеристика предоставляемых услуг | Ед. изм. | Кол-во |
| 1 | Продление лицензий на подсистему централизованной антивирусной обработки | Продление действующей лицензии на антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition на срок 1 год с учётом имеющейся у Заказчика лицензии (Лицензия Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 25-49 Node 1 Year Renewal License)  № лицензии: 1AF2-190705-063355-380-1957 | мест | 42 |

**Общие требования**

Антивирусные 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 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 компьютерах, работающих под управлением операционных систем следующих версий:

• Microsoft Windows XP Professional SP3 x86 / x64

• Microsoft Windows Vista SP2 x86 /x64

• Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64

• Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 и выше x86 / x64

• Microsoft Windows 8 Professional / Enterprise x86 / x64

• Microsoft Windows 8.1 Professional / Enterprise x86 / x64

• Microsoft Windows Embedded Standard 7 SP1 x86 / x64

• Microsoft Windows Embedded POSReady 7 x86 / х64

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:

• Резидентный антивирусный мониторинг.

• Защита от программ-маскировщиков, программ автодозвона на платные сайты.

• Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.

• Антивирусное сканирование по команде пользователя или администратора и по расписанию.

• Запуск задач по расписанию и/или сразу после загрузки операционной системы.

• 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 ресурсам производителя, для получения вердикта по запускаемой программе или файлу.

• Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP — независимо от используемого почтового клиента;

• Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных сайтов.

• Блокировка баннеров и всплывающих окон загружаемых с Web-страниц.

• Распознавание и блокировка фишинг-сайтов.

• Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами.

• Защита от еще не известных вредоносных программ на основе анализа их поведения.

• Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения. Возможность совершить откат действий вредоносного программного обеспечения при лечении.

• Возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы.

• Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ

• 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.

• Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.

• Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.

• 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.

**Требования к программным средствам антивирусной защиты для рабочих станций Mac**

Программные средства антивирусной защиты для рабочих станций Mac должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

• Mac OS X 10.9 (Mavericks)

• Mac OS X 10.8 (Mountain Lion)

• Mac OS X 10.7 (Lion)

• Mac OS X 10.6 (Snow Leopard)

• Mac OS X 10.5 (Leopard)

• Mac OS X 10.4 (Tiger)

• Mac OS XServer 10.6

• Mac OS XServer 10.7

Программные средства антивирусной защиты для рабочих станций Mac должны обеспечивать реализацию следующих функциональных возможностей:

• Резидентный антивирусный мониторинг.

• Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.

• Антивирусное сканирование по команде пользователя или администратора и по расписанию.

• Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.

• Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

**Требования к программным средствам антивирусной защиты для рабочих станций Linux**

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

• Canaima 3x86 / x64

• Red Flag Desktop 6.0 SP2 x86 / x64

• Red Hat Enterprise Linux 5.8 Desktop x86 / x64

• Red Hat Enterprise Linux 6.2 Desktopx86 / x64

• Fedora 16x86 / x64

• CentOS-6.2x86 / x64

• SUSE Linux Enterprise Desktop 10 SP4x86 / x64

• SUSE Linux Enterprise Desktop 11 SP2x86 / x64

• openSUSE Linux 12.1x86 / x64

• openSUSE Linux 12.2x86 / x64

• Debian GNU/Linux 6.0.5x86 / x64

• Mandriva Linux 2011 x86

• Ubuntu 10.04 LTSx86 / x64

• Ubuntu 12.04 LTSx86 / x64

Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:

• Резидентный антивирусный мониторинг.

• Проверка ресурсов доступных по SMB/ CIFS/ NFS

• Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.

• Антивирусное сканирование по команде пользователя или администратора и по расписанию.

• Антивирусная проверку и лечение файлов в архивах.

• Запуск задач по расписанию и/или сразу после загрузки операционной системы.

• Помещение подозрительных и поврежденных объектов на карантин.

• Возможность экспортировать и сохранять отчеты в форматах HTML и CSV.

• Возможность перехвата и проверки файловых операций на уровне SAMBA.

• Гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.

• Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность.

• Возможность управления через пользовательский графический интерфейс.

• Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

**Требования к программным средствам централизованного управления, мониторинга и обновления**

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

• Microsoft Windows XP Professional x86 / x64 SP3

• Microsoft Windows Vista x86 / x64 SP1 и выше

• Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64

• Microsoft Windows 8 Professional / Enterprise x86 / x64

• Microsoft Windows 8.1 Professional / Enterprise x86 / x64

• Microsoft Windows Server 2003 x86 / x64 SP2

• Microsoft Windows Server 2008 x86 / x64

• Microsoft Windows Server 2008 R2

• Microsoft Windows Server 2012

• Microsoft Windows Server 2012 R2

• Microsoft Windows Small Business Server 2003 SP2

• Microsoft Windows Small Business Server 2008

• Microsoft Windows Small Business Server 2011

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

• Microsoft SQL Express 2005/2008/2008R2/2012

• Microsoft SQL Server 2005/2008/2008R2/2012

• 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

Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий:

• VMware (Workstation 6.0/ Esxi 4.0 и выше)

• Microsoft Hyper-V

• KVM интегрированный с Ubuntu 10.10

• Microsoft VirtualPC 6.0.156.0

• Parallels 4.0.6630

• CitrixXenServer 5.6.1 FP1ивыше

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 AD, с целью получения данных об учетных записях компьютеров в организации

• 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 OUAD

• Централизованные установка, обновление и удаление программных средств антивирусной защиты. Настройка, администрирование, просмотр отчетов и статистической информации по их работе.

• Централизованное удаление(ручное и автоматическое) несовместимых приложений средствами центра управления.

• Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, агент администрирования, для локальной установки - автономный пакет установки.

• Удаленная установка программных средств антивирусной защиты с последней версией антивирусных баз.

• Автоматизированное обновление программных средств антивирусной защиты и антивирусных баз.

• Автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.

• Тестирование загруженных обновлений средствами ПО централизованного управления 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 иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня.

• Поддержка мультиарендности 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.

• Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройку рассылки почтовых уведомлений о них.

• Централизованная установка приложений сторонних производителей на все или выбранные компьютеры.

• 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.

• 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.

• 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.

• 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.