Приложение к извещению №14 от 20.09 2021 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на передачу неисключительного права использования программного обеспечения:

1. Антивирус Kaspersky Endpoint Security для бизнеса на 1 год;

1. Требования, установленные Заказчиком:

1.1. ***- требования Заказчика к наименованию и количеству поставляемых услуг***

№ п\п	Наименование услуги	Ед. измерения	Кол-во, шт.
1	Передача неисключительного права использования программного обеспечения Антивирус Kaspersky Endpoint Security на 1 год	Шт.	56

1.2 ***- требования Заказчика к свойствам и характеристикам услуг***

№ п/п	Наименование услуги	Требования *к свойствам и характеристикам услуг*
1	Передача неисключительного права использования программного обеспечения Антивирус Kaspersky Endpoint Security на 1 год	Передача неисключительного права использования программного обеспечения для обработки персональных данных (далее ПД) на ЭВМ с использованием сети Интернет и без нее, подпадающих под тип ПД: Б второго класса защиты, В второго класса защиты, Г второго класса защиты, согласно параметрам 152 ФЗ «О защите персональных данных». Для исполнения 152 ФЗ «О защите персональных данных» с технической стороны – необходимо сертифицированное средство антивирусной защиты информации и соответствующее требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВ3.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВ3.В2.ПЗ» (ФСТЭК России, 2012) и «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВ3.Г2.ПЗ» (ФСТЭК России, 2012), интеграция с уже имеющейся в учреждении системой информационной безопасности основанной на продуктах ЗАО «Лаборатория Касперского» с возможностью расширения и централизованного управления.

1.3 ***- требования к качеству поставляемой услуги***

Услуга должна соответствовать характеристикам, указанным в п.1.2. настоящего технического задания

1.4 ***- требование к безопасности поставляемой услуги***

Услуга не должна представлять опасности для жизни и здоровья граждан

1.5 ***- показатели соответствия поставляемой услуги и отгрузки услуги потребностям Заказчика***

1. Поставка услуги осуществляется силами и средствами Поставщика, с предоставлением действующих сертификатов соответствия, технических паспортов производителя услуги на русском языке, для подтверждения соответствия *поставляемой услуги* характеристикам, указанным в пункте 1.2. настоящего технического задания.
2. Наименование услуги и производитель *поставляемой услуги,* должны соответствовать наименованию услуги и ее производителю, указанным в представляемых при поставке услуги документах.
3. Поставка услуги должна осуществляться транспортом Поставщика.
4. Отсутствующая в заявке Заказчика услуга Поставщиком не поставляется, Заказчиком не принимается и не оплачивается.
5. В случае обнаружения Заказчиком дефектов *поставляемой услуги* Поставщик должен заменить дефектную услугу в течение 10 дней со дня получения извещения о выявлении таких дефектов.
6. В случае обнаружения Заказчиком дефектов в течение гарантийного срока завода изготовителя услуги такие дефекты должны быть устранены Поставщиком в течение 10 дней со дня получения извещения о выявлении дефектов.
7. Поставщик гарантирует поставку всей услуги надлежащего качества.
8. На Услугу устанавливается гарантийный срок 12 месяцев с даты поставки услуги, если больший срок не установлен производителем услуги.

1.6 ***Место использования программного обеспечения и количество лицензий на 1 рабочее место***

1. Компьютеры ВЭК - 36 шт.
2. ПРМО ст. Абакан - 1 шт.
3. ПРМО ст. Минусинск – 1 шт.
4. ПРМО ст. Черногорские копи - 1 шт.
5. ПРМО ст. Курагино - 1 шт.
6. ПРМО ст. Кошурникова – 2 шт.

7. ПРМО ст. Аскиз – 1 шт.
8. ПРМО ст. Бискамжа – 2 шт.
9. АСПО Психофизиолога ст. Междуреченск – 1 шт.
10. АСПО Психофизиолога ст. Кошурникова – 1 шт.
11. АСПО Психофизиолога ст. Абакан – 1 шт.
12.Психофизиологи ст. Абакан – 3 шт.
13. Приемная гл. врача, ПК секретаря – 1 шт.
14. АСПО поликлиники – 3 шт.
ИТОГО: 55 шт.

1. **Сервер ВЭК – 1 шт.**

Лицензия для программного обеспечения должна обеспечить:

Общие требования

Средства антивирусной защиты, предназначенные для развертывания в государственных организациях, должны быть сертифицированы уполномоченным органом (ФСТЭК) на соответствие требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по уровню контроля не ниже 4 и требованиям технических условий.

В рамках всей организации должны использоваться единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие ПК, то есть не подключённые к единой системе антивирусной защиты, в том числе находящиеся на удаленных территориях, должны быть защищены интегрированным программным продуктом, включающим в себя защиту от всех типов вредоносных программ (антивирус), спама (персональный антиспам) и сетевых атак (персональный межсетевой экран), и обеспечивать возможность их включения в единую систему антивирусной защиты.

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.

Антивирусные средства должны включать:

- программные средства антивирусной защиты рабочих станций и серверов;
- программные средства централизованного управления, мониторинга и обновления;
- обновляемые базы данных сигнатур вредоносных программ и атак;
- эксплуатационную документацию на русском языке.

Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows

Программные средства антивирусной защиты систем рабочих станций под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

- Microsoft® Windows® 10
- Microsoft Windows 2000 Professional (Service Pack 4 Rollup1);
- Microsoft Windows XP Professional (Service Pack 2 или выше);
- Microsoft Windows XP Professional x64 Edition (Service Pack 2 или выше);
- Microsoft Windows Vista Business/Enterprise/Ultimate (Service Pack 1 или выше);
- Microsoft Windows Vista Business/Enterprise/Ultimate x64 (Service Pack 1 или выше);
- Microsoft Windows 7 Professional/Enterprise/Ultimate;
- Microsoft Windows 7 Professional/Enterprise/Ultimate x64.

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;
- облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
- 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;
- автоматический контроль программ запускаемых на компьютере пользователя, осуществляющий контроль активности программ и ограничивающий выполнение опасных действий;
- 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;
- проверка протокола IPv6;
- защиту от программ-маскировщиков, программ автодозвона на платные сайты, блокировку баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц и распознавание фишинг-сайтов;
- наличие компонента дающего возможность создания специальных правил запрещающих установку/запуск программ, компонент должен контролировать приложения по пути нахождения программы, метаданным, MD5 контрольной сумме;
- осуществлять контроль 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;
- блокирование функции автозапуска;
- ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
- запускать специальную задачу для обнаружения уязвимостей в приложениях, установленных на компьютере пользователя, с возможностью предоставления отчета по обнаруженным уязвимостям;
- интеграция с системой обновления Windows Update, для установки патчей закрывающие обнаруженные уязвимости;
- 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;
- возможность устанавливать не все, а только выбранные компоненты антивирусной защиты;
- централизованно управляться с помощью единой системы управления.

Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows

Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:

- Windows 2000 Server/Advanced Server (Service Pack 4 Rollup1);
- Windows Server 2003 Standard/Enterprise (Service Pack 2);
- Windows Server 2003 x64 Standard/Enterprise (Service Pack 2);
- Windows Server 2003 R2 Standard/Enterprise Edition (Service Pack 2);
- Windows Server 2003 R2 x64 Standard/Enterprise Edition (Service Pack 2);
- Windows Server 2008 Standard/Enterprise (Service Pack 1 или выше);
- Windows Server 2008 x64 Standard/Enterprise (Service Pack 1 или выше);
- Windows Server 2008 R2 x64 Standard/Enterprise.
- Windows Small Business Server 2003;
- Windows Small Business Server 2008;
- Windows Essential Business Server 2008.

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;
- 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 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.

4. Требования к качеству:

4.1. Товар должен соответствовать требованиям настоящего Технического задания, правилам безопасности, нормам производства и реализации.

4.2. Поставщик несет полную ответственность за качество и безопасность поставляемого товара, при условии его правильной эксплуатации.