# **ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**на поставку антивирусного программного обеспечения для нужд ООО «УК «ВОЛМА»»**

* 1. **Предмет договора:** Поставка антивирусного программного обеспечения для нужд ООО «УК «ВОЛМА»» согласно спецификации:

|  |  |
| --- | --- |
| **Наименование товара (выполнение работ, оказание услуг), кол-во** | **Требования к техническим характеристикам, потребительским свойствам, характеристикам безопасности, упаковке, и иные показатели.**  |
| Антивирусное программное обеспечение Kaspersky Total Security для бизнеса 250-499 Node 1 year Renewal Licenseдля ОС Windows для рабочих станций (или эквивалент)**Колическтво – 400 шт.** | **Наименование:** Система антивирусной защиты (далее - Система)1. **Общие требования**
	1. Все компоненты Системы должны принадлежать одной торговой марке с единой службой технической поддержки на русском языке. Техническая поддержка должна предоставляться непосредственно производителем поставляемых программных продуктов.
	2. В рамках всей организации должны использоваться единые антивирусные средства независимо от степени конфиденциальности обрабатываемой информации. Отдельно стоящие ПК, 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 проникновения и активации всех типов вредоносных программ (антивирус), спама (персональный антиспам) и обеспечивать возможность их включения в единую систему антивирусной защиты.
	3. Поставляемые средства защиты должны представлять масштабируемое решение, обеспечивающее устойчивое функционирование в локальной сети заказчика.
	4. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.
	5. Все антивирусные средства, функционирующие под операционной системой типа Windows, включая средства управления, должны обладать контекстной справочной системой на русском языке.
	6. Участник конкурса должен предоставить единый серийный номер для всех поставляемых по условиям конкурса продуктов.
	7. Поставляемый серийный номер должен иметь возможность отложенной активации. Срок действия лицензионных ключевых файлов на все поставляемые по условиям конкурса программные продукты должен начинаться с момента активации серийного номера.
	8. Антивирусные средства должны включать:

- программные средства защиты рабочих станций и файловых серверов;- обновляемые базы данных сигнатур вредоносных программ всех типов и атак;- эксплуатационную документацию на русском языке.1. **Требования к программным средствам**
	1. **Общие требования к системе антивирусной защиты**
		1. Программные средства Системы должны обеспечивать определение угроз следующих типов:
			1. классических вирусов;
			2. троянских программ;
			3. руткитов;
			4. сетевых червей;
			5. рекламных программ;
			6. программ автодозвона на платные сайты;
			7. потенциально опасных приложений;
			8. прочих вредоносных программ.
		2. Антивирусная защита должна обеспечивать:
			1. обнаружение и удаление вирусов из файлов, упакованных программами типа PKLITE, LZEXE, DIET, COM2EXE и т.п.;
			2. обнаружение и удаление вирусов, скрытых под неизвестными упаковщиками;
			3. обнаружение вирусов внутри контейнеров и архивных файлов формата ACE (до версии 2.0), BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, ARJ, JAR, ISO (включая NRG, образы с нестандартным форматом сектора и не имеющие сигнатур), ZLIB, VCLZIP, VISE, PST, DMG, PDF, GHOST INSTALLER с зашифрованными контейнерами и т.д. без ограничений на уровень вложенности проверяемых объектов;
			4. антивирусную проверку в самораспаковывающихся архивах и упакованных файлах
			5. защиту от еще неизвестных вредоносных программ, принадлежащих зарегистрированным семействам, как на основе эвристического анализа, так и с помощью технологии поиска похожих вирусов, основанной на анализе расположения участков кода в файле;
	2. **Требования к программным средствам антивирусной защиты рабочих станций под управлением ОС семейства Microsoft Windows**
		1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
			1. осуществление антивирусной (включая постоянную защиту от руткит-технологий) защиты на рабочих станциях.
		2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов
		3. Система, используя актуальную на момент проведения тендера версию, должна обеспечивать защиту рабочих станций под управлением операционных систем:
			1. Microsoft Windows XP;
			2. Microsoft Windows Vista;
			3. Microsoft Windows 7.
			4. Microsoft Windows 8
			5. Microsoft Windows 8.1
			6. Microsoft Windows 8.2
			7. Microsoft Windows 10
		4. Компоненты антивирусной защиты Системы должны устойчиво функционировать на компьютерах класса Pentium IV с частотой 1.6 ГГц в условиях их минимальной и максимальной загрузки без существенного снижения производительности защищаемых рабочих станций. Компоненты системы должны поддерживать механизм динамического выделения оперативной памяти, учитывающий производительность системы, а также потребности в ресурсах задач, выполняемых пользователем и операционной системой во время проверки.
		5. Система должна поставляться в конфигурации, обеспечивающей антивирусную защиту при работе в локальной сети и в Интернет с Web-страницами, электронной почтой, локальными жесткими дисками и съемными носителями, а также с сетевыми ресурсами. Должна обеспечиваться защита входящей и исходящей электронной корреспонденции, как от вредоносных программ. Должно обеспечиваться обнаружение и удаление вирусов всех типов, как из тела сообщения, так и, если это возможно, из вложенных файлов.
		6. Антивирусное программное обеспечение должно по умолчанию иметь настройки, оптимальные с точки зрения безопасности и производительности работы.
		7. В Системе должна быть реализована возможность выбора приоритета сканирования, а также приостановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
		8. Система должна предоставлять возможность автоматического поиска и деинсталляции ранее установленных средств антивирусной защиты перед установкой антивирусного пакета на клиентские рабочие станции.
		9. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения с последующим лечением системы.
		10. Дополнительно к вышеперечисленному система должна обеспечивать на рабочих станциях:
			1. поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
			2. проверку любых объектов на защищаемых рабочих станциях, в том числе внутри архивов без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора;
			3. 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. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
			4. блокировку опасных макросов VBA в реальном времени;
			5. защиту от вредоносных сценариев, загружаемых с Web-страниц;
			6. помещение найденных зараженных файлов в специальное место на жестком диске -«карантин»;
			7. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			8. запуск задач по расписанию и/или сразу после загрузки операционной системы;
			9. возможность запуска проверки при обращении пользователя, операционной системы или какой-либо программы к любому объекту, подлежащему проверке.
		11. Система защиты рабочих станций должна обеспечивать проверку протоколов:
			1. IMAP, SMTP, POP3 независимо от используемого почтового клиента;
			2. NNTP (только проверка на вирусы), независимо от почтового клиента.
		12. Система должна обеспечивать проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов (компьютерных вирусов, троянских программ, Интернет-червей, макро-вирусов, опасных Java-апплетов, ActiveX и др.) посредством:
			1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
			2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.
		13. В Системе должна быть реализована самозащита для всех своих объектов, в том числе, критических файлов, процессов, окон, ключей и прочего от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
		14. В Системе должна быть реализована защита работы собственных модулей от сбоев и случайного изменения.
	3. **Требования к программным средствам антивирусной защиты серверов под управлением ОС семейства Microsoft Windows**
		1. Программные средства Системы должны обеспечивать реализацию следующих функциональных возможностей:
			1. Осуществление антивирусной защиты на серверах, включая защиту от руткит-технологий.
		2. Программные средства Системы должны обеспечивать определение в объектах файловой системы вредоносных программ всех типов.
		3. Система), используя актуальную на момент проведения тендера версию, должна обеспечивать защиту серверов под управлением операционных систем:
			1. Microsoft Windows 2003 Server;
			2. Microsoft Windows 2008 Server. Включая R2
			3. Microsoft Windows 2012 Server.
		4. Компоненты Системы должны устойчиво функционировать на серверах в условиях их минимальной и максимальной загрузки без существенного снижения производительности.
		5. Компоненты системы должны иметь возможность управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
		6. Антивирусное программное обеспечение должно по умолчанию иметь оптимальные настройки с точки зрения безопасности и производительности работы..
		7. Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами серверы без их предварительного лечения с последующим лечением системы.
		8. В Системе должна быть реализована возможность выбора приоритета сканирования, а также остановки выполняющихся заданий (в том числе антивирусного сканирования) в целях высвобождения системных ресурсов.
		9. Система должна обеспечивать проверку любых объектов на защищаемых серверах, в том числе внутри архивов, без ограничений на уровень вложенности проверяемых объектов и тип используемого архиватора.
		10. Система должна обеспечивать:
			1. поиск и удаление вирусов всех известных типов в файлах, загрузочных секторах и оперативной памяти компьютера;
			2. 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. Учет синтаксиса скриптовых языков при проверке по антивирусным базам;
			3. блокировку опасных макросов VBA в реальном времени;
			4. защиту от вредоносных сценариев, загружаемых с веб-страниц;
			5. помещение найденных зараженных файлов в специальное место на жестком диске —«карантин»;
			6. автоматический запуск антивирусного программного обеспечения и других необходимых компонентов вместе с загрузкой ОС;
			7. запуск задач по расписанию и/или сразу после загрузки операционной системы.
		11. Система защиты серверов под управлением семейства ОС Microsoft Windows должна обеспечивать реализацию следующих функциональных возможностей:
			1. проверку файлов и системных областей на предмет наличия вредоносных объектов всех типов посредством:
				1. антивирусного сканирования, заключающегося в однократной полной или выборочной проверке на наличие угроз и проводимого как по команде пользователя или администратора, так и по расписанию;
				2. проверки объектов «на лету», при доступе к ним с помощью антивирусной резидентной программы.
		12. В Системе должна быть реализована самозащита для всех ее объектов, в том числе критических файлов, процессов, окон, ключей и прочего, от несанкционированного доступа пользователей и вредоносного программного обеспечения, которая должна работать на самом низком системном уровне и обеспечивать невозможность выгрузки и остановки драйверов антивирусной Системы.
	4. **Требования по комплектности поставке**
		1. В состав Системы должны входить:
			1. программные средства антивирусной защиты, необходимые для выполнения требований данного технического задания;
			2. обновляемые базы данных сигнатур всевозможных вредоносных программ.
		2. Комплект поставки должен содержать:
			1. необходимый набор серийных номеров либо ключевых файлов;
			2. дистрибутив Системы;
			3. файлы эксплуатационной документации в формате pdf (Adobe Acrobat Reader), в том числе руководство пользователя (администратора). Поставляемая документация должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.
	5. **Требования по технической поддержке Системы**
		1. Техническая поддержка должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.
		2. Техническая поддержка должна обеспечивать возможность получения специалистами и пользователями Заказчика информационной помощи по установке Системы и ее компонентов, в том числе:
			1. ответов на вопросы, а также получение инструкций относительно процесса установки и применения программного обеспечения;
			2. ответов на вопросы о наличии проблем в работе программного обеспечения, а также помощи в определение того, является ли данная проблема результатом сбоя программного обеспечения, ошибок настройки или же она вызвана проблемами, связанными с внешними условиями существования или установкой программного обеспечения.

Web-сайт производителя Системы должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов производителя. |
|

Ссылки в документации на товарные знаки, знаки обслуживания, фирменные наименования, патенты, полезные модели, промышленные образцы, наименование места происхождения товара или наименование производителя, носят лишь рекомендательный, а не обязательный характер. Участник тендера может представить в своей заявке иные товарные знаки, знаки обслуживания, фирменные наименования, патенты, полезные модели, промышленные образцы, места происхождения товара или производители, при условии, что произведенные замены совместимы между собой, по существу равноценны (эквиваленты) [или превосходят по качеству товар, указанный в технических условиях (аналоги)

**3. Порядок формирования цены**

Цена договора включает в себя: расходы Поставщика на перевозку товара до склада Заказчика, страхование, упаковку, полный комплект документации, налоги и другие обязательные платежи, а также иные расходы Поставщика, связанные с исполнением обязательств, являющихся предметом настоящего тендера.

**4.** **Форма, сроки и порядок оплаты товаров**

Аванс – не предусмотрен.

Порядок оплаты – безналичный расчет. 100% оплата производится в течение 30 банковских дней с момента фактической приемки товара (при наличии всех необходимых документов: паспорта, сертификаты, счета-фактуры, ТТН и т.д.)

**5. Требования к упаковке товара:**

Каждое изделие должно быть упаковано, с обеспечением защиты от внешних воздействий. Наличие маркировки, либо упаковочных бирок. Упаковка товара должна обеспечивать безопасность транспортировки и сохранять его качества в течение гарантийного срока хранения.

6. Срок гарантии качества

Гарантия на работоспособность входящих в поставку файлов ключей активации в течение 12 месяцев с момента их активации Заказчиком.

**7. Место поставки продукции:** Волгоград, ул Крепильная 128

**8. Сроки поставки продукции:** в течение 5 дней со дня заключения договора.

**9**. **Дополнительные условия:** Товар должен быть новым, не заложенным, не являться предметом споров третьих лиц.