

ИЗВЕЩЕНИЕ О ЗАКУПКЕ
услуг по приобретению (предоставлению, продлению) права использования
лицензий антивирусного программного обеспечения «Касперский»

ООО «КАМАЗжилбыт», именуемый в дальнейшем Организатор закупки, приглашает Вас принять участие в конкурентной процедуре закупки.

Для прохождения предварительного отбора и принятия участия в закупочной процедуре предлагаем Вам заполнить краткую анкету контрагента, и представить коммерческое предложение участника закупки.

Срок подачи предложений: до 22.01.2026г.

Сроки рассмотрения предложений: с 27.01.2026г. по 09.02.2026г.

Непредоставление коммерческого предложения в установленные сроки считается автоматическим отказом от участия.

Прошу условия Вашего коммерческого предложения распространять на все организации ПАО «КАМАЗ», закупающие идентичный товар, работу или услугу. Коммерческое предложение подлежит рассмотрению как в полном объеме, так и попозиционно.

Все необходимые разъяснения и интересующие Вас сведения Вы можете получить, связавшись с лицом, ответственным за организацию закупочной процедуры:

Все необходимые разъяснения и интересующие Вас сведения Вы можете получить, связавшись с лицом, ответственным за организацию закупочной процедуры:

Гиззатуллина Татьяна Викторовна, e-mail: gtv@kamgb.ru, тел. 8 (8552) 91-02-77, сот. 8-960-075-27-26.

Проведение закупочной процедуры не является предварительным договором либо иным обязательством Общества заключить договор в будущем.

При выявлении признаков коррупции, злоупотреблением полномочиями или халатности со стороны сотрудников ПАО «КАМАЗ» просим обращаться:

- 8-800-551-80-08 (звонки из любой точки РФ бесплатные);
- +7(960)070-61-11 мессенджеры WhatsApp, Viber, Telegram;
- compliance@kamaz.org;
- официальный сайт ПАО «КАМАЗ» посредством заполнения формы: <https://kamaz.ru/about/compliance/hotline/feedback>.

Гарантируется полная анонимность, исключается какое бы то ни было негативное воздействие на обратившихся, даже в том случае, если сообщённая информация не получила подтверждения в ходе внутреннего расследования.

Организатор закупки:

Генеральный директор
(должность)


(подпись)

28.12.25
дата)

Михеев А.В.
(Ф.И.О.)

ТРЕБОВАНИЯ К ПРЕДМЕТУ ЗАКУПКИ И ПОСТАВЩИКУ

1. Требования к предмету закупки

Услуги по приобретению (предоставлению, продлению) права использования лицензий антивирусного программного обеспечения «Касперский».

Количество: 120 лицензий антивируса Касперского (Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 5000+ Node 3 year Base License, 120 ПК на 3 года

Заказчик на момент закупки не имеет действующего соглашения правообладателя АО «Лаборатория Касперского».

2. Количество поставляемых товаров: 120 лицензий

Спецификации

Наименование	Кол-во, шт.	Срок действия лицензии, год
Программный продукт "KL4867RAYTS Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 5000+ Node 3 year Base License - Лицензия"	120	3

3. Условия поставки товаров: лицензии на продление антивируса должны действовать в течение 3 лет с момента активации.

Программные средства антивирусной защиты рабочих станций и серверов должны обеспечивать реализацию следующих функциональных возможностей:

- Антивирусная защита рабочих станций и серверов;
- Централизованное управление, мониторинг и обновление программных средств;
- Обновление базы данных сигнатур вредоносных программ и атак;

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

- Microsoft Windows 7 Professional/Enterprise/Ultimate и выше;
- Microsoft Windows 7 Professional/Enterprise/Ultimate x64 и выше;
- Microsoft Windows 10 Home/Pro/ Enterprise
- Microsoft Windows 11 Home/Pro/ Enterprise и выше

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

- Windows Server (x32&64) 2012 и выше.

Программные средства антивирусной защиты систем рабочих станций под управлением семейства ОС Microsoft Windows должны обеспечивать реализацию следующих функциональных возможностей:

резидентный антивирусный мониторинг;

адаптивный контроль аномалий;

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;

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;

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, с возможностью создавать доверенные устройства по их идентификатору и возможностью предоставлять привилегии, для запуска внешних устройств, определенным пользователям; блокирование функции автозапуска; запускать специальную задачу для обнаружения уязвимостей в приложениях, установленных на компьютере пользователя, с возможностью предоставления отчета по обнаруженным уязвимостям; 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.

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;

настройки проверки критических областей сервера в качестве отдельной задачи;

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.

4. Платежные условия договора:

- по безналичному расчету в течение 30-ти календарных дней с момента предоставления права пользования (с даты подписания сторонами акта выполненных работ, услуг).

5. Общие требования к товарам:

- поставка и продление неисключительного права на использование и воспроизведение антивирусного программного обеспечения «Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition»

- предоставление комплекта документации;

- предоставление консультаций Заказчику по вопросам инсталляции программного обеспечения, авторизации программного обеспечения, описанию основных функциональных возможностей программного обеспечения и области его применения, ответы на вопросы по описанию новых функций новых версий программного обеспечения.

6. Требования к качеству товаров, качественным (потребительским) свойствам товаров:

- срок предоставления гарантии качества услуг – на весь период продления неисключительного права на использование и воспроизведение антивирусного программного обеспечения «Антивирус Касперского»

- поставляемый товар должен соответствовать требованиям качества и безопасности товаров в соответствии с действующими стандартами, утвержденными в отношении данного вида товара, и подтверждаться соответствующими документами, оформленными в соответствии с действующим российским законодательством.

- Поставщик не должен разглашать третьим лицам конфиденциальную информацию, к которой он получит доступ при заключении договора, в ходе его исполнения и после прекращения его действия.

Главный специалист
по системному администрированию

Заместитель генерального директора
по правовым и кадровым вопросам

В.Н. Антропов

О.А. Виноградова