ЧАКЫРУУ
«Керемет Банк» ААКнын муктаждыктары үчүн Kaspersky Security Center программасына карата лицензияларды узартууну сатып алууга катышууга

**Күнү:** «____» _____

**Кимге: «Керемет Банк» ААК**

---

1. «Керемет Банк» ААК Банк муктаждыктары үчүн Kaspersky Security Center программасына карата лицензияларды узартууну сатып алууга кызыкдар экендигин билдирет.
2. Бааларды суроо-талапка катышуу үчүн кыргыз же орус тилдеринде коммерциялык сунуш берүүңүз зарыл, сунуш көрсөтүлүп келе жаткан котормочулук кызматтардын тиешелүү сертификаты, котормо наркы жана мөөнөттөрү менен коштолууга тийиш.
3. Кайрылуу форматын төмөнкү дарек боюнча колмо-кол же электрондук почта аркылуу тапшырууга болот:

«Керемет Банк» ААКнын административдик бөлүмү
Кыргыз Республикасы
Бишкек шаары, Тоголок Молдо көч, 40/4, № 209 каб.
Административдик бөлүм
Сатып алуулар секторунун башчысы
Бейшеналиев С.К.
Тел: (312) 313173 д/н 2080
Электрондук почта
tender@keremetbank.kg

4. Баа KGS\USD валютасында көрсөтүлүүсү зарыл, төмөнкүлөрдү эске алуу менен:

- Кыргыз Республикасынын мыйзамдарында каралган бардык салыктарды жана жыйымдарды, ал кеминде 30 күн жарактуу болууга тийиш. Баа боюнча сунуштарды **жергиликтүү убакыт боюнча 2022-жылдын «__27___» майында саат 11.00дөн** кечиктирбей жөнөтүү зарыл. Катышуучулардын көрсөтүлгөн мөөнөттөн кечигип калган табыштамалары каралбайт.

5. **Сатуулардын соңку баасы шартсыз көрсөтүлүүсү керек,** техникалык спецификациялардын бардык талаптарына жооп берген жана эң төмөнкү бааны көрсөткөн катышуучуга артыкчылык берилет.

6. Бул өңдүү камсыздоолор менен иш алып баруу боюнча кеминде 1 жылдык тажрыйбасы тууралуу маалымат берүү (кат, камсыздоо суммасы көрсөтүлгөн келишимдин тизмеси жана Заказчылардын байланыш номурлары). (мүмкүн болсо)

*Коммерциялык сунуштарды караштыруунун жыйынтыгында Сатып алуу иштеринин катышуучуларынын табыштамаларында көрсөтүлгөн ташып жеткирүү мөөнөтү, ошондой эле төлөм шарттары өзгөртүлбөйт жана бааларды көтөрүү сунуштары каралбайт. Камсыздоо шарттары талапка ылайык келбесе же сатып алуулардын Жеңүүчүсү шарттарга*

*макул болбосо, Камсыздоо келишимин түзүү учурунда аталган Камсыздоочу Банк камсыздоочуларынын Кара тизмесине киргизилет.*

**Техническое задание**

**г.Бишкек** **16.05.2022**

Предмет закупки:
ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на поставку неисключительных (пользовательских) лицензионных прав на программное обеспечение «Kaspersky Endpoint Security» в количестве 600 штук.

г. Бишкек 26.04.2022 года.

Установленное средство антивирусной защиты у: «Kaspersky Endpoint Security for Business - Advanced: Kaspersky Security for WS and FS (Номер лицензии: 2A0E-000451-576768E9)» и «Kaspersky Endpoint Security for Business – Advanced: Security Center (Номер лицензии: 2A0E-000451-576768E8)».

Средства антивирусной защиты для серверов под управлением ОС Microsoft Windows, предназначенные для развертывания в государственных организациях должны быть сертифицированы уполномоченным органом на соответствие требованиям средств защиты информации.
Программные средства антивирусной защиты систем серверов под управлением семейства ОС Microsoft Windows должны функционировать на следующих версиях ОС:
- Microsoft Windows Server 2012 и новее

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 распознавать и блокировать ранее неизвестные вредоносные программы.
• Антивирусное сканирование по команде пользователя или администратора и по расписанию.
• 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 и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные.
• Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере.
• Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB
• Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
• Настройки проверки критических областей сервера в качестве отдельной задачи.
• 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.
• Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
• Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме.
Требования к программным средствам централизованного управления, мониторинга и обновления
Средства централизованного управления, мониторинга и обновления под управлением ОС Microsoft Windows, должны быть сертифицированы в соответствии с мировыми требованиями к средствам антивирусной защиты.
Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
• Microsoft Windows 7 Professional/Enterprise/Ultimate x32/x64
• Microsoft Windows 8 Professional / Enterprise x32/x64
• Microsoft Windows 10 Professional / Enterprise x32/x64
• Microsoft Windows 11 Professional / Enterprise x32/x64
• Microsoft Windows Server 2008 x32
• Microsoft Windows Server 2008 SP1 x64
• Microsoft Windows Server Core 2008 x32/x64
• Microsoft Windows Server 2008 R2
• Microsoft Windows Server Core 2008 R2
• Microsoft Windows Server 2012
• Microsoft Windows Server Core 2012
• Microsoft Windows Small Business Server 2003
• Microsoft Windows Small Business Server 2008
• Microsoft Windows Small Business Server 2011
• Microsoft Windows Server 2016
• Microsoft Windows Server Core 2016
• Microsoft Windows Server 2019
• Microsoft Windows Server Core 2019

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:
• Microsoft SQL Express 2005/2008/2008R2/2012 и более новыми версиями ПО
• Microsoft SQL Server 2005/2008/2008R2/2012 и более новыми версиями ПО

• MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91 и более новыми версиями ПО
• MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90 и более новыми версиями ПО

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 и новее
• Microsoft VirtualPC 6.0.156.0 и новее
• Parallels 4.0.6630 и новее
• Citrix XenServer 5.6.1 FP1 и выше
Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:
• 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
• Централизованная 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.
• 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.
• Поддержка мультиарендности для серверов управления.
• Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.
• 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.
• возможность управления компонентом, запрещающим установку и/или запуск программ.
• возможность управления компонентом, контролирующим работу с внешними устройствами ввода/вывода.
• возможность управления компонентом контроля работы пользователя в сети интернет.
• Функция для управления мобильными устройствами через сервер Exchange ActiveSync.
• Функция для управления мобильными устройствами через сервер iOSMDM.

• 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.
• Наличие веб-консоли управления приложением.
• Наличие системы контроля возникновения вирусных эпидемий.
• Установка системы управления антивирусной защиты из единого дистрибутива.
• Выбор установки в зависимости от количества защищаемых узлов.
• Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставку обновлений на рабочие места пользователей сразу после их получения.
• Возможность отправки SMS-оповещений администратору о заданных событиях.
• Централизованная установка приложений на управляемые мобильные устройства.
• Централизованная установка сертификатов на управляемые мобильные устройства.
• Централизованная установка приложений сторонних производителей на все или выбранные компьютеры.
• Интеграция с CISCO NAC и MS NAP.
• 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.
• Поддержка Windows Failover Clustering.

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;
- Формуляры к антивирусным средствам защиты в состав которого должно входить следующие параметры:
  - Общие указания;
  - Общие сведения;
  - Основные характеристики;

- Функциональные возможности;
- Комплектность;
- Указания по эксплуатации;
- Периодический контроль основных характеристик при эксплуатации и хранении;
- Свидетельство о приемке;
- Свидетельство об упаковке и маркировки;

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 СНГ 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.

Требования к качеству:

Товар должен соответствовать требованиям настоящего Технического задания, правилам безопасности, нормам производства и реализации.
Поставщик несет полную ответственность за качество и безопасность поставляемого товара, при условии его правильной эксплуатации.

Дополнительные требования:

В комплектацию товара должны войти:
- ключ активации на физическом носителе;
- дистрибутивы для установки средств антивирусной защиты для рабочих станций, файловых серверов и программных средств централизованного управления, мониторинга и обновления на физическом носителе;
-оригинал лицензионного соглашения с компанией правообладателем данного программного обеспечения на бумажном носителе;

В случае поставки аналогичной лицензии с совместимым антивирусным программным обеспечением, удовлетворяющим требованиям настоящего технического задания, Исполнитель обязан будет произвести установку и настройку антивирусного программного обеспечения на оборудовании Заказчика.
При поставке аналогичной лицензии с совместимым антивирусным программным обеспечением, в комплектацию товара должны войти:
- ключ активации и дистрибутив антивирусного программного обеспечения на физическом носителе;
- оригинал лицензионного соглашения с компанией правообладателем данного программного обеспечения на бумажном носителе;