ПРИГЛАШЕНИЕ К УЧАСТИЮ В ЗАКУПКЕ лицензии Kaspersky for MS Exchange для нужд ОАО «Керемет Банка»

Дата: «____» _____

Кому: ОАО «Керемет Банк»

---

1. ОАО «Керемет Банк» выражает заинтересованность в закупке Лицензии Kaspersky for MS Exchange.
2. Для участия в запросе цен, Вам требуется предоставить коммерческое предложение на русском или кыргызском языках, предложение должно сопровождаться соответствующим сертификатом качества оказываемых услуг, цены и сроки поставки.
3. Формат обращения нарочно по указанному адресу или электронно по почте:

Административный отдел ОАО «Керемет Банк»
Кыргызской Республики
г. Бишкек, ул. Тоголок Молдо 40/4, каб. № 209
Бейшеналиев Санжар.
Зав.сектором закупок.
Административный отдел.
ОАО "Керемет Банк"
Кыргызстан, 720001
г. Бишкек, ул. Тоголок Молдо 40/4 (2-10 этаж)
Электронная почта
tender@keremetbank.kg

3. Цена должна быть указана KGS\USD, с учетом:

- всех налогов и сборов, предусмотренных законодательством Кыргызской Республики,
- должна действовать не менее 30 дней. Крайний срок предоставления Вашего ценового предложения «17» января 2022 года, 11:00 местного времени. Заявки от участников принятые позже указанного срока рассмотрению не подлежат.

4. Вы должны указать **окончательную стоимость продажи без оговорок**, предпочтение будет дано участнику, соответствующему всем требованиям технической спецификации и предложившему наименьшую стоимость.

5. Предоставить информацию о наличии опыта аналогичных услуг, не менее 1 (одного) года. (письма, список договоров с указанием сумм поставки и контактных номеров Заказчиков) (желательно)

По итогам рассмотрения коммерческого предложение заявки Участников закупки не подлежат изменению в части условий поставок по срокам, цены в сторону увеличения и условий оплаты. В случае несоответствия условий поставок или не согласия со стороны Победителя закупки, при заключении договора Поставки, данный Поставщик будет включен в Черный список поставщиков Банка.

Техническое задание

г.Бишкек **21.12.2021**

Предмет закупки: лицензии для Kaspersky for Microsoft Exchange Server

1. **Комплект поставки должен в себя включать**

Наименование	Количество лицензий	Срок действия
Продление лицензии на Kaspersky for Microsoft Exchange Server	650 шт.	6 месяцев

2. **Требования к программным средствам антивирусной защиты и фильтрации спама для**

серверов Microsoft Exchange

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2019;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2012 R2 Standard или Datacenter;
- Microsoft Windows Server 2012 Standard или Datacenter;
- Microsoft Windows Small Business Server 2011 SP1 Standard;

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать с программным обеспечением Microsoft Exchange Server следующих версий:

- Microsoft Exchange Server 2010;
- Microsoft Exchange Server 2013;
- Microsoft Exchange Server 2013;
- Microsoft Exchange Server 2016;
- Microsoft Exchange Server 2019.

Программные средства антивирусной защиты для серверов Microsoft Exchange должны функционировать с серверами баз данных следующих версий:

- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2019

Консоль управления программными средствами антивирусной защиты для серверов Microsoft
Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows 10;
- Microsoft Windows 8.1;

- Microsoft Windows 8;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2012 R2 Standard или Datacenter;
- Microsoft Windows Server 2012 Standard или Datacenter;
- Microsoft Windows Small Business Server 2011 SP1 Standard;
- Microsoft Windows 7 SP1 Professional, Enterprise или Ultimate; Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей:
- Проверять входящие, исходящие, а также хранящиеся на сервере Microsoft Exchange (в том числе и в общих папках) сообщения на присутствие вредоносных объектов.
- Фильтровать почтовый трафик от нежелательной почты (спама).
- Использовать для дополнительной проверки сообщений на спам облачный репутационный сервис Reputation Filtering, который помещает сообщения в специальное временное хранилище – карантин – и присваивает им статус после повторной проверки.
- Проверять почтовый поток на наличие фишинговых ссылок.
- Сохранять резервные копии обнаруженных объектов и спам-сообщений перед лечением или удалением;
- Уведомлять отправителя, получателя и администратора антивирусной безопасности о сообщениях, содержащих вредоносные объекты.
- Вести журналы событий, собирать статистику и создавать регулярные отчеты о работе программы;
- Настраивать параметры проверки сообщений в соответствии с политикой безопасности компании, в частности формировать белые и черные списки отправителей и получателей;
- Поддерживать базы Антивируса и Анти-Спама в актуальном состоянии с помощью обновления в автоматическом и ручном режимах;
- Управлять антивирусной защитой на уровне хранилищ и формировать список защищаемых хранилищ;
- Централизованно управлять одинаковыми параметрами в группе серверов Microsoft Exchange с помощью профилей;
- Управлять лицензиями Серверов безопасности, в том числе централизованно с помощью профилей при работе с группой серверов Microsoft Exchange;
- Выполнять фильтрацию вложений;
- Наличие эвристических методов детектирования.
- Проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер.
- Возможность лечить зараженные архивы.
- Возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях.
- Возможность детектирования вредоносных и фишинговых ссылок в теле письма.
- Сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта. Широкий набор параметров поиска для удобства нахождения объекта в резервном хранилище.
- Наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки ранее неизвестных угроз
- Проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения.

- Фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- Проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL).
- Проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF).
- Проверка с помощью сервиса SPAM URI Realtime Block lists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма.
- Проверка графических вложений на совпадение с известными сигнатурами спам-сообщений.
- Создание отчетов по работе системы защиты. Возможность автоматической рассылки отчетов администраторам по расписанию.
- Возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации.
- Детальные отчеты в формате HTML.
- Интеграция с Active Directory.
- Возможность управления всеми серверами защиты с помощью одной консоли.