**Техническая спецификация товара**

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование товара** | **Кол-во** | **Сумма в тенге без учета НДС** | **Технические характеристики** |
| Продление лицензии на антивирусное ПО | 200 | 2 945 400 | **Продление программных средств антивирусной защиты рабочих станций, серверов и мобильных устройств в количестве 200 штук со сроком действия 3 года, Kaspersky Endpoint Security for Business – Select 3 year Renewal License****Общие требования** 1. Во избежание конфликтов антивирусных программ разных разработчиков, и с учетом того, что для защиты компьютерной сети, персональных автоматизированных рабочих мест (ПК) и серверов предприятия уже используются продукты Лаборатории Касперского, требуется продлить антивирусное программное обеспечение того же производителя.2. 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 и сетевых атак, и обеспечивать возможность их включения в единую систему антивирусной защиты.3. Антивирусные средства должны включать:- программные средства антивирусной защиты рабочих станций и серверов;- программные средства антивирусной защиты мобильных устройств (смартфонов);- программные средства централизованного управления, мониторинга и обновления;- обновляемые базы данных сигнатур вредоносных программ и атак;- эксплуатационную документацию на русском языке.4. Срок действия лицензии должен составлять не менее 36 календарных месяцев с момента активации лицензии.5. АО "Казахстанская фондовая биржа" имеет лицензию антивируса Kaspersky Endpoint Security for Business Select 150-249 Node 1 year Renewal License (№ лицензий 1FF0-180130-113941-453-1320) на 150 защищаемых объектов. Необходимо продлить данную лицензию с увеличением до 200 защищаемых объектов.6. Потенциальный поставщик должен являться официальным партнером Лаборатории Касперского на территории Республики Казахстан (предоставить копию сертификата), а также в целях оперативного реагирования на запросы и оказания квалифицированной технической поддержки потенциальный поставщик в своем штате должен иметь 2 (двух) сертифицированных технических специалистов со статусами Kaspersky Lab Certified System Engineer и Kaspersky Lab Certified Professional (предоставить копии сертификатов).**Защита рабочих станций**Программные средства антивирусной защиты 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; 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;• 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. |