

**Общество с ограниченной  
ответственностью  
«НИИАР-ГЕНЕРАЦИЯ»**

Руководителю

433510, РФ, Ульяновская обл.,  
г. Димитровград, пр. Димитрова 16  
Тел. (84235)3-15-40, факс (84235)3-15-40,  
ОКПО 87810621, ОГРН 1127329003163,  
ИНН/КПП 7329008990/732901001

03.05.2018 № ЗР-2018

Запрос коммерческого предложения

ООО «НИИАР - ГЕНЕРАЦИЯ» в 2018 году планирует провести мелкую закупку на оказание услуг по предоставлению неисключительных прав на использование программного обеспечения Kaspersky EndPoint Security на 2018 год.

Объем оказываемых услуг.

Наименование	Количество лицензий
Неисключительные права Kaspersky Endpoint Security для бизнеса – Стандартный 50-99 Renewal Licence Pack  № лицензии: 13C8170526081454953776 PN: KL4863RAQFR	60

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском языке.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке.

**Требования к программным средствам антивирусной защиты для рабочих станций  
Windows**

Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows XP Professional SP3 x32/x64
- Microsoft Windows 7 Professional / Enterprise /Ultimate x32/x64
- Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 и выше x32/x64
- Microsoft Windows 8 Professional / Enterprise x32/x64
- Microsoft Windows 8.1 Professional / Enterprise x32/x64

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:

- Резидентный антивирусный мониторинг.
- Защита от программ-маскировщиков, программ автодозвона на платные сайты.
- Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.
- Антивирусное сканирование по команде пользователя или администратора и по расписанию.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.
- Антивирусная проверка 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 ресурсам производителя, для получения вердикта по запускаемой программе или файлу.

- Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP — независимо от используемого почтового клиента;
- Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных сайтов.
- Блокировка баннеров и всплывающих окон загружаемых с Web-страниц.
- Распознавание и блокировка фишинг-сайтов.
- Защита от еще не известных вредоносных программ на основе анализа их поведения.
- Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения. Возможность совершить откат действий вредоносного программного обеспечения при лечении.
- Возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы.
- 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 (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные.
- Осуществление контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из AD.
- Осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.). Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из AD.
- Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
- Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
- Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
- 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.
- Возможность установки только выбранных компонентов программного средства антивирусной защиты.
- Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

### **Требования к программным средствам антивирусной защиты для файловых серверов Windows**

Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows Server 2008 Standard/Enterprise SP1 x32/x64
- Microsoft Windows Server 2008 R2 x64 Standard/Enterprise
- Microsoft Windows Server 2008 R2 x64 Standard/Enterprise SP1 и выше

- Microsoft Windows Server 2008 Foundation
- Microsoft Windows Server 2008 R2 Foundation
- Microsoft Windows Server 2012 Foundation x64
- Microsoft Windows Server 2012 Standard/Essentials x64
- Microsoft Windows Server 2012 R2 Standard/Essentials x64 Edition

Программные средства антивирусной защиты для файловых серверов 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.
- Запуск задач по расписанию и/или сразу после загрузки операционной системы.
- Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу.
- 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 (IDS/IPS) 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, с возможностью предоставления отчета по обнаруженным уязвимостям.
- Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем.
- Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
- Настройки проверки критических областей сервера в качестве отдельной задачи.
- Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме.
- Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий).
- 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.

#### **Требования к программным средствам централизованного управления, мониторинга и обновления**

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- Microsoft Windows XP Professional x32/x64SP3
- Microsoft Windows Vista x32/x64SP1 и выше
- Microsoft Windows 7 Professional/Enterprise/Ultimate x32/x64
- Microsoft Windows 8 Professional / Enterprise x32/x64
- Microsoft Windows 8.1 Professional / Enterprise x32/x64

- Microsoft Windows Server 2008 x32/x64
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:

- Установка системы управления антивирусной защиты из единого дистрибутива.
- Выбор установки в зависимости от количества защищаемых узлов.
- 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 OU AD
- 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 и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.
- 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.
- Тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; доставку обновлений на рабочие места пользователей сразу после их получения.
- Обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации.
- Доступ к облачным серверам производителя антивирусного ПО через сервер управления.
- 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 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.
- Экспорт отчетов в файлы форматов PDF и XML.
- Централизованное управление объектами резервных хранилищ и карантин по всем ресурсам сети, на которых установлено антивирусное программное обеспечение.

- Создание резервной копии системы управления встроенными средствами системы управления.

### **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.
- Множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации.
- Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Исполнитель должен являться правообладателем в рамках лицензионного договора с разработчиком, либо действовать в пределах прав и полномочий, предоставленных ему правообладателем программного обеспечения АО «Лаборатория Касперского»

При оказании услуг Исполнитель представляет Заказчику:

- лицензионное соглашение, определяющее условия использования Заказчиком программного обеспечения и подтверждающее права Заказчика на обновление и поддержку;
- лицензионный ключ официального исполнения.

Исполнитель предоставляет Заказчику неисключительные права на использование программного обеспечения Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ - сроком на один год (продление) на 60 рабочих мест, в течение 15 рабочих дней с момента подписания договора.

Заказчик оплачивает услуги в течение 30 (тридцати) календарных дней со дня подписания Сторонами Акта сдачи-приёмки оказанных услуг, при условии предоставления Исполнителем оригиналов платежных документов.

Из ответа на запрос должны однозначно определяться цена единицы услуг (с НДС, без НДС) и общая цена договора на условиях, указанных в запросе.

Проведение данной процедуры сбора информации не влечёт за собой возникновения каких-либо обязательств заказчика.

Срок действия коммерческого предложения должен составлять не менее 60-ти календарных дней с даты подачи предложения.

Исполнительный директор



Бочкарев А.И.

Исп. Ведущий специалист ИТ

Никитин В.В.

89278379040