

## **Техническая спецификация закупаемых услуг**

### **Наименование закупки:**

Услуги по предоставлению лицензий на право использования программного обеспечения: Антивирусная многоуровневая защита конечных устройств и файловых серверов для бизнеса (с локальным управлением В5) в виде подписки на 36 месяцев корпоративной лицензии с единым ключом активации для - 7 рабочих станций ГО "Боровое" филиала "ИГИ" РГП "НЯЦ РК".

### **Гарантийный срок (в месяцах):**

36

### **Описание требуемых характеристик, параметров и иных исходных данных:**

Руководствуясь соблюдением норм информационной безопасности, своевременным обновлением программного обеспечения. Лицензия антивирусной программы с многоуровневой защитой конечных устройств и файловых серверов для бизнеса (с локальным управлением В5), должна быть выписанной на (ГО "Боровое" филиала "ИГИ" РГП "НЯЦ РК") и заранее не активированной.

### **Функциональные характеристики:**

- 1) Система должна быть построена по клиент-серверной архитектуре с возможностью установки антивирусного сервера централизованного управления не только на серверные ОС MS Windows, но и на рабочие станции под управлением MS Windows 7/8/10/11/Home/Pro/Server. Основным протокол межсетевого взаимодействия – TCP/IP. Кроме того, должна быть реализована возможность установки сервера централизованного управления на ОС UNIX, включая FreeBSD и Solaris и поддержка операционных систем семейства NovellNetware с протоколом межсетевого взаимодействия IPX/SPX.
- 2) Наличие полноценного сервера обновлений вирусных баз и компонентов от производителя на территории Республики Казахстан, с проверкой хеш-сумм и авторизацией пользователя.
- 3) Интерфейс управления Системы должен быть реализован на основе Web-интерфейса, поддерживающего Web-браузеры MozillaFirefox, Opera и GoogleChrome. Web-интерфейс должен обеспечивать централизованное управление и мониторинг.
- 4) Система должна быть доступной из любой операционной системы, в том числе ОС типа UNIX (Linux, FreeBSD, Solaris), NovellNetware без доустановки какого-либо программного обеспечения.
- 5) Программные средства Системы должны обеспечивать осуществление антивирусной и антиспам защиты на рабочих станциях, включая постоянную защиту от руткит-технологий, наличие резидентного антируткит драйвера.
- 6) Система должна поддерживать возможность установки своих компонентов на зараженные вирусами или другими вредоносными программами рабочие станции сети без их предварительного лечения. Для установки должен использоваться защищенный антируткитом инсталлятор.
- 7) Система должна иметь защиту от намеренных/непреднамеренных действий пользователей посредством блокировки доступа к локальным и сетевым ресурсам. В том числе сменным носителям информации, локальным файлам и каталогам.

### **Технические характеристики:**

Для Сервера управления: 1) Использование независимого агента, который позволяет осуществлять удаленное управление антивирусным продуктом на конечных точках, а также контролировать уровень антивирусной защиты на рабочих станциях и состояние операционной системы; 2) Поддержка инструментом удаленного администрирования следующих баз данных: MS SQL Server, MySQL; 3) Наличие функционала для определения администратора площадки или филиала с соответствующей частью лицензии; 4) Наличие предустановленных шаблонов в системе уведомлений для информирования о некорректной идентификации клонированных машин, что дает возможность оповещать о некорректно настроенной интеграции с системами VDI; 5) Наличие функционала создания площадок в соответствии с филиалами компании, что дает возможность назначить определенную часть лицензии отдельным филиалам. 6) Централизованное управление

антивирусной защитой всей сетевой инфраструктуры; 7) Построение иерархической структуры администрирования, главного и подчиненных серверов, осуществлять централизованное управление антивирусной защитой рабочих станций и мобильных устройств, как главному, так и региональным подразделениям; 8) Удаленно активировать и деактивировать модули защиты, персональный брандмауэр, защита в режиме реального времени, защита почтового клиента, защита доступа в Интернет, контроль устройств, веб-контроль, антиспам на отдельно взятом клиенте; 9) Выполнять с помощью инструмента удаленного управления дополнительные сетевые действия: завершение работы и перезагрузка, отправка сигнала пробуждения компьютера, отправка сообщений, выполнение конкретных инструкций командной строки на клиентском компьютере, старт обновления операционной системы клиентского компьютера. 10) Создание зеркала обновлений на основе сторонних HTTP-серверов; 11) Настраивать параметры журналов и отчетов из более чем 50 шаблонов для различных систем/клиентов; 12) Отслеживать установленное на рабочей станции ПО, а также удалять установленное ПО на выбор; 13) Деактивировать лицензию антивирусных продуктов на рабочих станциях, к которым нет физического или удаленного доступа; 14) Определять, какая виртуальная машина будет являться источником для копирования или клонирования в системах VDI.

Для Защиты рабочих станций: 1) Предоставление защиты от вредоносного ПО – определенного вредоносного кода, который добавляется в начало или конец кода файлов на компьютере. Выявление вредоносного ПО должно осуществляться ядром обнаружения в сочетании с компонентом машинного обучения; 2) Предоставление защиты от потенциально нежелательных программ, которые нельзя однозначно отнести к вредоносному ПО по аналогии с такими безусловно вредоносными программами, как вирусы или трояны, но эти программы могут устанавливать дополнительное нежелательное ПО, менять настройки системы, а также выполнять неожиданные действия или действия, не подтвержденные пользователем; 3) Предоставление защиты от опасных программ руткитов, которые предоставляют злоумышленникам из Интернета неограниченный доступ к системе, в то же время скрывая свое присутствие в операционной системе; 4) Обеспечение антивирусной защиты в режиме реального времени; 5) Антивирусное сканирование по требованию пользователя или администратора и в соответствии с графиком; 6) Наличие дополнительного модуля, который позволяет запускать браузеры в защищенном режиме с целью блокирования попыток вмешательства в область памяти браузера и содержимого его окон, а также дополнительной защиты критических Интернет-соединений, таких как Интернет-платежи и Интернет-банкинг и т.д; 7) Наличие в персональном брандмауэре режима обучения, что позволяет администратору удаленно настраивать разрешительные правила для сетевых приложений и оборудования; 8) Наличие дополнительного функционала персонального брандмауэра, который способен обнаруживать те изменения в сетевых программах, которые повлекли за собой новые несанкционированные сетевые соединения; 9) Получение обновления клиентов из локального хранилища на сервере, что позволяет поддерживать актуальность антивирусной защиты в закрытых изолированных сетях, у которых нет доступа к сети Интернет. 10) Делать исключения из сканирования определенных файлов, которые не вредоносные, но сканирование которых может привести к отклонениям в работе или влиять на продуктивность системы; 11) Использование технологий машинного обучения для углубленного анализа кода, выявления вредоносного поведения и характеристик вредоносного программного обеспечения; 12) Создавать группы разрешенных или запрещенных внешних устройств; 13) Использовать в персональном брандмауэре дополнительную аутентификацию сети для предотвращения несанкционированного подключения ПК к неизвестным опасным сетям; 14) Обновления в режиме получения регулярных, тестовых и отложенных обновлений; 15) Определение уровня критичности (опасный, неизвестный, малоизвестный, безопасный) значений различных параметров операционной системы для выявления несанкционированных и опасных изменений в системе.

Для Защиты серверов: 1) Использование эвристических технологий во время сканирования; 2) Предоставление защиты от вредоносных программ, троянского ПО, клавиатурных шпионов, рекламного ПО, фишинга, шпионского ПО, руткитов, скриптов, потенциального нежелательного и опасного ПО; 3) Регламентное обновление вирусных баз не менее 24 раз в сутки; 4) Наличие инструмента для диагностики системы, который может создавать снимки состояния операционной

системы для дальнейшего глубоко анализа различных аспектов работы операционной системы, включая запущенные процессы, контент реестра, установленное ПО, сетевые соединения. Благодаря умению сравнивать различные снимки состояния системы, этот инструмент может обнаружить изменения, которые произошли в системе. Также он может создавать и выполнять скрипты, что позволит останавливать запущенные процессы, удалять ветки реестра, блокировать сетевые соединения. 5) Указать резервные серверы администрирования помимо основного; 6) Настройка режима запуска путем отключения графического интерфейса для терминальных пользователей, что позволяет уменьшить нагрузку на сервер, работающий в режиме сервера терминалов.

***Качественные характеристики:***

Все компоненты Системы должны принадлежать одной торговой марке с единой службой технической поддержки. Техническая поддержка должна предоставляться непосредственно производителем поставляемых программных продуктов. Наличие службы технической поддержки производителя Системы на территории Республики Казахстан как на русском, так и на казахском языке.

Поставщик должен осуществить предоставление срока действия лицензии на 36 месяцев антивирусной программы с многоуровневой защитой конечных устройств и файловых серверов для бизнеса (с локальным управлением B5) количеством на 7 рабочих станций.

***Эксплуатационные характеристики:***

Система должна поддерживать следующие операционные системы: Microsoft Windows XP Professional/Server; Microsoft Windows Vista (Professional/Server или выше); Microsoft Windows 7 (Professional/Server или выше); Microsoft Windows 8 (Professional/Server или выше); Microsoft Windows 8.1 (Professional/Server или выше); Microsoft Windows 10.

**Место оказания услуги:** Акмолинская область, Бурабайский район, Бурабай, Окжетпес, микрорайон Самал, земельный участок 8

**Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора:**

Поставщик должен предоставлять гарантийное обслуживание и техническую поддержку программного обеспечения в течение срока действия лицензии.

**Начальник ГО «Боровое»**



**Асафова Л.В.**