|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ:  Начальник управления корпоративных и технологических автоматизированных систем управления АО «Тываэнерго»  \_\_\_\_\_\_\_\_\_\_\_\_ О.А. Мамонтова  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на поставку неисключительных (пользовательских) прав на использование программного обеспечения Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 250-499 Node 1 year Renewal License.

1. **Общие положения**

1. Общие положения

1.1. Заказчик: Акционерное общество «Тываэнерго» - (далее – АО «Тываэнерго»).

1.2. Предмет закупки: Неисключительные (пользовательские) права на использование программного обеспечения Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 250-499 Node 1 year Renewal License.

1. **Место, срок и условия поставки**

2.1. Место оказания услуг: АО «Тываэнерго», Республика Тыва, г. Кызыл, ул. Рабочая, д. 4.

2.2. Срок предоставления прав пользования: предоставление права на использование программного обеспечения Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 250-499 Node 1 year Renewal License осуществляется в течение 30 (тридцати) календарных дней с момента подписания Сторонами Договора.

**3. Перечень и объемы поставки**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Ед. изм.** | **Кол-во** | **Планируемая (предельная) цена договора, руб.** | | | |
|
| **Цена за ед. без НДС** | **Цена за ед. с НДС** | **Всего без НДС** | **Всего с НДС** |
|
|
| **1** | **2** | **4** | **5** | **6** | **7** | **8** | **9** |
| 1 | Неисключительные (пользовательские) права на использование программного обеспечения Kaspersky Endpoint Security для бизнеса - Расширенный Russian Edition. 250-499 Node 1 year Renewal License.\* | шт. | 275 | 1206,00 | 1206,00 | 331650,00 | 331650,00 |
| **ИТОГО** | | | | | | **331650,00** | **331650,00** |

\* НДС не облагается в соответствии с подпунктом 26 пункта 2 статьи 149 Налогового кодекса Российской Федерации.

3.1. Все налоги, сборы, отчисления и другие платежи, включая таможенные платежи и сборы, расходы на транспортировку продукции до места поставки и ее разгрузку, стоимость тары и упаковки, гарантийные обязательства включены в стоимость заявки/предложения участника.

**4. Общие технические требования программному обеспечению**

4.1. Требования к Системе.

В качестве основных объектов защиты в контексте функционирования Системы рассматриваются:

а) АРМ работников;

б) мобильные АРМ работников;

в) мобильные устройства;

г) серверы.

На всех указанных объектах должны быть установлены программные модули Системы. При этом состав модулей Системы на различных типах объектов различается в зависимости от условий функционирования и программного окружения объекта.

4.2.Требования к архитектуре Системы.

Архитектура Системы антивирусной защиты создается в составе следующих модулей:

а) модуль антивирусной защиты рабочих станций и серверов;

б) модуль антивирусной защиты мобильных устройств;

в) модуль централизованного управления Системы.

4.3. Требования к модулю защиты рабочих станций и серверов.

Модуль должен обеспечивать выполнение следующих функций (полностью для рабочих станций и частично для серверов):

а) резидентный антивирусный мониторинг, включая:

- эвристический анализ, обеспечивающий распознавание и блокирование ранее неизвестного вредоносного кода;

- анализ поведения программного обеспечения и контроля изменений системного реестра, с возможностью автоматического восстановления изменённых вредоносной программой значений системного реестра;

- анализ по облачной репутационной базе производителя;

б) сканирование на наличие вредоносного кода:

- по команде пользователя или администратора;

- по расписанию;

- при запуске операционной системы;

в) проверка на наличие вредоносного кода и лечение (при возможности):

- файлов упакованных специализированными программами;

- файлов в архивах, в том числе и защищенных паролем;

- скриптов, обрабатываемых в Microsoft Internet Explorer, а также WSH-скриптов (таких как Java Script, Visual Basic Script и др.);

- проверка почтовых сообщений, как на наличие вредоносного кода, так и на спам, с проверкой трафика в следующих протоколах: IMAP, SMTP, POP3, MAPI, HTTP;

- трафика по протоколам HTTP, FTP;

- трафика ICQ и MSN на наличие вредоносного кода;

г) обнаружение и блокирование:

- скрытых процессов;

- программ-маскировщиков, программ автодозвона на платные сайты;

- баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц;

- фишинг-сайтов;

д) контроль запуска программного обеспечения по:

- пути нахождения;

- метаданным;

- контрольной сумме MD5;

е) контроль активности программного обеспечения, ограничивающий выполнение опасных действий;

ж) защита от сетевых атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для приложений при работе в вычислительных сетях любого типа, включая беспроводные и протокол IPv6;

з) контроль работы с внешними устройствами ввода/вывода, с ограничением доступа к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям;

и) ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

к) обнаружение уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;

л) интеграция с системой обновления Windows Update для установки патчей, закрывающих обнаруженные уязвимости;

м) автоматическое и ручное обновление компонентов модуля и баз сигнатур;

н) гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

о) регистрация событий, связанных с работой модуля;

п) сбор статистики;

р) самозащита приложения:

- защита от отключения или блокирования;

- защита от удаленного несанкционированного управления сервисом приложения;

- защита от несанкционированного доступа к параметрам приложения с помощью пароля;

с) шифрование файлов;

- на локальных дисках компьютера с возможностью формирования списков из файлов по расширению или группам расширений и папок, расположенных на локальных дисках компьютера;

- на съемных носителях с возможностью указания правила шифрования по умолчанию, в соответствии с которым программное средство выполняет одинаковое действие по отношению ко всем съемным носителям и указания правила шифрования отдельных съемных носителей;

- которые создают или изменяют заданные программы с возможностью формирования списка программ, для которых файлы, которые они создают или изменяют как на жестких дисках, так и на съемных носителях, будут зашифрованы;

- обеспечивающее возможность работы с зашифрованными файлами на съемном носителе в портативном режиме. После включения портативного режима становится доступной работа с зашифрованными файлами на съемных носителях, подключенных к компьютеру с недоступной функциональностью шифрования;

- обеспечивающее возможность управление правами доступа программ к зашифрованным файлам с возможностью определения правила доступа к зашифрованным файлам для любой программы, запрещающее доступ к зашифрованным файлам или разрешающее доступ к зашифрованным файлам только в виде шифротекста.

- обеспечивающее возможность создание зашифрованных архивов с возможностью создания зашифрованных архивов и защиты доступа к этим архивам паролем. Доступ к содержимому зашифрованных архивов можно получить только после ввода пароля, которым был защищен архив.

т) шифрование жестких дисков:

- обеспечивающее возможность указания правила шифрования жестких дисков по умолчанию и возможность формирования списка жестких дисков для исключения из шифрования. После шифрования жестких дисков доступ к данным, хранящимся на них, а также загрузка операционной системы возможны только после прохождения процедуры аутентификации в агенте аутентификации;

- обеспечивающее возможность управления правами пользователей на загрузку ОС на компьютерах с зашифрованными жесткими дисками. Возможность создания учетных записей пользователей, параметры которых разрешают или запрещают пользователям доступ к данным, хранящимся на зашифрованных жестких дисках, после прохождения процедуры аутентификации в агенте аутентификации;

- обеспечивающее возможность восстановления зашифрованных устройств. В случае порчи зашифрованного жесткого диска или съемного носителя необходимо наличие возможности восстановления содержимого данных устройств с помощью специальной утилиты восстановления.

у) шифрование съемных носителей, обеспечивающее возможность указания правила шифрования по умолчанию, в соответствии с которым программное средство выполняет одинаковое действие по отношению ко всем съемным носителям, и возможность установки правила шифрования для отдельных съемных носителей.

ф) удаленное управление с помощью модуля централизованного управления.

4.4. Требования к модулю мобильных устройств.

Модуль должен обеспечивать выполнение следующих функций:

а) защита от вредоносного кода, спама и фишинга;

б) защита от кражи;

в) сканирование по запросу или расписанию;

г) автоматическое и ручное обновление компонентов модуля и баз сигнатур;

д) обнаружение несанкционированной перепрошивки;

е) регистрация событий, связанных с работой модуля;

ж) сбор статистики;

з) защита приложений и данных в контейнерах:

и) шифрование всех данных в контейнерах;

к) запрет копирования данных за пределы контейнера;

л) повторная авторизация после некоторого периода неактивности;

м) удаленное удаление данных;

н) контроль приложений;

о) доступ к порталу самообслуживания.

4.5. Требования к модулю централизованного управления

Модуль должен обеспечивать выполнение следующих функций:

а) централизованное выполнение задач по управлению и обслуживанию системы защиты;

б) предоставление детальной информации об уровне безопасности;

в) централизованное распространение и конфигурирование политик компонентов защиты других модулей Системы;

г) установка системы антивирусной защиты из единого дистрибутива;

д) создание групп логической сети на основе структуры системы службы каталогов Active Directory;

е) автоматическое распределение компьютеров по группам управления, в случае появления новых компьютеров в сети;

ж) централизованная установка, обновление и удаление программных средств антивирусной защиты, настройка, администрирование, просмотр отчетов и статистической информации по их работе;

з) централизованное удаление несовместимых приложений;

и) централизованное управление установкой и запуском программ на компьютерах пользователей с возможностью контроля программ по пути нахождения программы, метаданным, MD5 контрольной сумме и возможностью присвоения привилегий определенным пользователям;

к) централизованное управление доступом к веб-ресурсам с компьютеров пользователей с возможностью фильтрации по категориям и типу данных загружаемого контента, гибко задавать параметры времени действия правил и возможностью присвоения привилегий определенным пользователям;

л) поддержка различных методов установки антивирусных приложений: для удаленной установки - RPC, GPO, агент администрирования, для локальной установки - автономный пакет установки;

м) удаленная установка программных средств антивирусной защиты с последней версией баз приложения;

н) автоматизированный поиск уязвимостей в установленных приложениях и операционной системе на рабочих станциях и серверах;

о) тестирование загруженных обновлений средствами сервера администрирования перед распространением на клиентские машины;

п) доставка обновлений на рабочие места пользователей сразу после их получения;

р) распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;

с) централизованный контроль работы пользователя с внешними устройствами ввода/вывода, с возможностью ограничения доступа 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;

т) построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;

у) создание виртуальных серверов управления антивирусным приложением;

ф) защищенное взаимодействие с другими центрами управления;

х) доступ к облачным серверам производителя антивирусного ПО через сервер управления; ц) автоматическое распространение лицензии на клиентские компьютеры;

ч) обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации:

- регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз анти-спама 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. ш) централизованный сбор информации и создание отчетов о состоянии антивирусной защиты;

щ) централизованная инвентаризация установленного ПО и оборудования на компьютерах пользователей;

ы) наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройку рассылки почтовых уведомлений о них;

э) встроенная система управления образами ОС: создание образа ОС с шаблонного компьютера с возможностью установки этого образа на определенные компьютеры;

ю) централизованная установка приложений сторонних производителей на все или выбранные компьютеры;

я) функция для управления мобильными устройствами через сервер Exchange ActiveSync;

аа) функция для управления мобильными устройствами через сервер iOS MDM;

бб) возможность отправки SMS-сообщений мобильным пользователям;

вв) централизованная установка приложений на управляемые мобильные устройства;

гг) централизованная установка сертификатов на управляемые мобильные устройства;

дд) поддержка функциональности управления шифрованием данных;

ее) централизованный сбор информации о всех установленных на клиентских компьютерах приложениях;

жж) интеграция с CISCO NAC и MS NAP;

зз) контроль доступа к сети организации - NAC;

ии) централизованное управление шифрованием информации, хранящейся на жестких дисках устройств и съемных носителях, и доступом пользователей к зашифрованным данным экспорт отчетов в файлы форматов PDF и XML;

кк) централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено агентское ПО Системы;

лл) формирование уведомлений по всем операциям и событиям работы других модулей системы; мм) ведение локальной базы аутентификации учетных записей для аутентификации на сервере управления;

нн) создание резервной копии системы управления; оо) поддержка WFC;

пп) поддержка веб-консоли управления приложением;

рр) наличие системы контроля возникновения вирусных эпидемий.

сс) Модуль должен состоять из следующих компонентов:

тт) сервер администрирования;

уу) консоль администрирования;

фф) агент администрирования.

**5. Требования к Сублицензиару**.

Сублицензиар должен иметь опыт работы на рынке поставок и оказания услуг по приобретению неисключительных (пользовательских) прав на антивирусное программное обеспечение, что подтверждается наличием у Сублицензиара авторизации (сертификата) от правообладателя.

**6. Требования к гарантии.**

Срок предоставления гарантий качества составляет не менее 12 месяцев с момента подписания сторонами Акта приема – передачи прав.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Дата | Должность | Подпись | ФИО |
| 1 |  | Начальник отдела бизнес-приложений |  | Минин В.В. |