Техническое задание на закупку

Форма технического задания на закупку товаров

АО «Аэропорт Салехард»

Отдел ИТиС

наименование структурного подразделения

Товары, поставляемые в рамках договора, должны быть новыми и неиспользованными.

Товары, не должны иметь дефектов, связанных с разработкой, материалами и качеством изготовления, либо проявляющихся в результате действия или упущения Поставщика при нормальном использовании поставленных товаров в условиях, обычных для России.

Срок поставки программного обеспечения не может превышать 30 дней.

Поставляется программное обеспечение, указанное в данном Техническом Задании .

№ п/п	Разделы	Описание характеристик и требований к товару
1.	Наименование товара	Программное средство антивирусной защиты для рабочих станций.
2.	Количество, единица измерения товара	Одна лицензия на сто пользователей
3.	Максимальная цена (с НДС) за единицу	
4.	Порядок формирования цены договора (с учетом или без учета расходов на перевозку, страхование, уплату таможенных пошлин, налогов и других обязательных платежей)	123 420 (сто двадцать три тысячи четыреста двадцать) рублей.
5.	Условия оплаты: Форма (наличная/безналичная) Срок Порядок оплаты, в т.ч. условия предварительной оплаты, рассрочки, отсрочки)	Форма оплаты безналичная. По факту поставки
6.	Сроки поставки (начало, окончание, периодичность)	В течение 30 дней.
7.	Место доставки товаров (фактический адрес)	629004, г. Салехард, ЯНАО, АО «Аэропорт Салехард», отдел ИТиС.
8.	Порядок доставки товаров (самовывоз, доставка собственными силами, отправка груза)	Доставка собственными силами Поставщика.
9.	Способ доставки (авиа, ж/д, авто, водный транспорт)	Любой
10.	Момент перехода права собственности на товар и момент перехода риска случайной гибели (передачи первому перевозчику, доставки Заказчику)	В момент подписания товарной накладной и акта приема - сдачи.
	Технические характеристики товара	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 7 Professional / Enterprise /Ultimate x86 / x64; Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 и выше x86 / x64; Microsoft Windows 8 Professional / Enterprise x86 / x64; Microsoft Windows 8.1 Professional / Enterprise x86 / x64; Microsoft Windows 10 Pro / Enterprise x86 / x64; Microsoft Windows Server 2012 R2 Standard x64; Microsoft Windows Server 2016; Microsoft Windows Server 2012 Standard / Foundation x64; Microsoft Small Business Server 2011 Standard x64; Microsoft Windows Server 2008 R2 Standard / Enterprise x64 SP1; Microsoft Windows Server 2008 Standard / Enterprise x86 / x64 SP2; Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей: • Антивирусное сканирование в режиме реального времени и по запросу. • Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы. • Антивирусное сканирование 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 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. • Проверка трафика ICQ и MSN, для обеспечения

		безопасности работы с интернет-пейджерами. • Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения. Возможность совершить откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных вредоносными программами файлов. • Возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам. Автоматическое определение уровней ограничения на основании репутации программы. • Наличие механизмов защиты от атак типа BadUSB. • 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. • Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме MD5 или SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory. • 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 Active Directory. • 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 Active Directory. • 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.
	Функциональные характеристики товара (потребительские свойства)	Установка лицензированного программного обеспечения (ключа) на ЭВМ
	Комплектность товара	Лицензии для ста пользователей
	Гарантийное и техническое обслуживание (сроки, место осуществления обслуживания, стоимость, субъекты, которые оказывают такое обслуживание, объем гарантийного и технического обслуживания – перечень работ)	Не менее 2 год.
	Перечень передаваемой с товаром документации (технические паспорта, инструкции по эксплуатации, сертификаты соответствия и иные сопроводительные документы)	Требования к эксплуатационной документации Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе: • Руководство пользователя (администратора). Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.
	Предлагаемые критерии выбора Поставщика	Цена, срок поставки, гарантийное обслуживание, лучшие технические характеристики.
	Ответственное лицо за исполнение договора, наименование службы, контактный телефон	Фирсов Леонид Владиславович, инженер-программист ОИТиС, тел. 8-982-404-28-08