ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ
ЯРОСЛАВСКОЙ ОБЛАСТИ
«ИНФОРМАЦИОННОЕ АГЕНТСТВО «ВЕРХНЯЯ ВОЛГА»

150000, г. Ярославль, ул. Максимова, д.17/27. E-mail: zakazchik@vvolga-yar.ru Тел./факс (4852) 30-57-39

от «26» ноября 2020г.

Заинтересованным лицам

Запрос в целях формирования
представления о рыночных ценах
на оказание услуг по предоставлению неисключительных прав
на использование лицензионного программного обеспечения
Kaspersky Endpoint Security для бизнеса – Стандартный
(продление лицензий на антивирусное программное обеспечение) для нужд Заказчика

В настоящее время ГАУ ЯО «Информационное агентство «Верхняя Волга» в целях формирования стоимости договора на оказание услуг по предоставлению неисключительных прав на использование лицензионного программного обеспечения Kaspersky Endpoint Security для бизнеса – Стандартный (продление лицензий на антивирусное программное обеспечение) осуществляет анализ предложений поставщиков.

В срок до «04» декабря 2020 г. просим представить предложения по цене договора на оказание услуг по предоставлению неисключительных прав на использование лицензионного программного обеспечения Kaspersky Endpoint Security для бизнеса – Стандартный (продление лицензий на антивирусное программное обеспечение), проект которого изложен в приложении № 3 к настоящему запросу.

Порядок направления предложений – в простой письменной форме по почте и/или курьером и/или в форме скана указанного предложения на электронную почту Заказчика: zakazchik@vvolga-yar.ru (документ должен быть подписан уполномоченным лицом, скреплен печатью организации).

Направление предложения от поставщика является подтверждением факта установления поставщиком цены договора в соответствии с условиями проекта договора, в том числе техническим характеристикам, установленным в приложении № 2 к настоящему запросу.

Настоящий запрос не является извещением о проведении закупки, офертой или публичной офертой и не влечет возникновения никаких обязанностей у заказчика.

Форма предоставления предложения по цене договора – в приложении №1 к настоящему запросу.

Техническое задание – в приложении № 2 к настоящему запросу.

Проект договора – в приложении № 3 к настоящему запросу.

И.о. директора ГАУ ЯО «Информационное агентство
«Верхняя Волга» Н.В. Болотова

Приложение № 1 к запросу в целях формирования представления о рыночных ценах
ФОРМА
предоставления цены по договору, проект которого изложен в приложении № 3

НА БЛАНКЕ ОРГАНИЗАЦИИ

ПРЕДЛОЖЕНИЕ О ЦЕНЕ ДОГОВОРА

В ГАУ ЯО «Информационное агентство «Верхняя Волга»

от:_____
(полное наименование участника, юридический и почтовый адрес)

«___» _____ 2020 г.

В соответствии с условиями договора на оказание услуг по предоставлению неисключительных прав на использование лицензионного программного обеспечения Kaspersky Endpoint Security для бизнеса – Стандартный (продление лицензий на антивирусное программное обеспечение) для нужд Заказчика, проект, которого изложен в запросе в целях формирования представления о рыночных ценах от 26.11.2020г., размещенном на сайте вволга.рф, предлагает _____ *(название организации)* общую стоимость, включающую в себя все расходы по выполнению договора, в том числе налоговые: _____(*сумма указывается цифровым значением и прописью*) рублей, в том числе НДС_____/НДС не облагается.

№ п/п	Наименование товара, товарный знак (при наличии), производитель Товара	Кол-во, штук	Функциональные характеристики (потребительские свойства) и качественные характеристики товара Предложения Участника	Срок действия лицензии	Страна происхождения товара	Стоимость за шт., руб. (в т.ч. НДС 20%)	Общая стоимость, руб. (в т.ч. НДС 20%)
1.							
НДС 20%/НДС не облагается							
ИТОГО:							

Руководитель (***должность)*** _____ (Ф.И.О. Руководителя)

М.П.

****Инструкции по заполнению***
1. Участник указывает свое полное фирменное наименование (в т.ч. организационно-правовую форму) и свой юридический и почтовый адрес.
2. Цены указанные в коммерческом предложении должны включать все таможенные пошлины, налоги (включая НДС) и другие обязательные платежи в соответствии с действующим законодательством Российской Федерации, все транспортные и страховые расходы, расходы на погрузку-разгрузку и т.д.
3. В своем коммерческом предложении Участник должен представить заполненную форму подписанную лицом, имеющим право в соответствии с законодательством Российской Федерации действовать от лица Участника без доверенности, или надлежащим образом уполномоченным им лицом на основании доверенности, скрепить печатью Участника.
4. На все закупаемые товары, где указаны товарные знаки, Участник может предложить эквивалент, который в свою очередь должен точно соответствовать техническим характеристикам, указанным в техническом задании или превышать их и не уступать по качеству затребованным товарам.

Приложение № 2 к запросу в целях формирования представления о рыночных ценах

Техническое задание
на предоставление лицензионных прав на пользование программным обеспечением Kaspersky Endpoint Security для бизнеса – Стандартный

1.	Предмет закупки, характеристики	Оказание услуг по предоставлению неисключительных прав на использование лицензионного программного обеспечения Kaspersky Endpoint Security для бизнеса – Стандартный (продление лицензий на антивирусное программное обеспечение) для нужд Заказчика сроком на 12 месяцев.
2.	Количество/Место оказания услуг	132 штуки (лицензии)/150000, г. Ярославль ул. Максимова, д. 17/27
3.	Срок действия лицензии	12 месяцев с момента активации лицензии (ключей)
4.	Требования к характеристикам товара	**Общие требования** Антивирусные средства должны включать: • программные средства антивирусной защиты для рабочих станций Windows; • программные средства антивирусной защиты для рабочих станций Linux; • программные средства антивирусной защиты для файловых серверов Windows; • программные средства централизованного управления, мониторинга и обновления; • обновляемые базы данных сигнатур вредоносных программ и атак; • эксплуатационную документацию на русском языке. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке. **Требования к программным средствам антивирусной защиты для рабочих станций Windows** Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий: • Windows 7 Home / Professional / Enterprise (32 / 64-разрядная); • Windows 8 Professional / Enterprise (32 / 64-разрядная); • Windows 8.1 Professional / Enterprise (32 / 64-разрядная); • Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная). В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта; • антивирусное сканирование по расписанию; • антивирусное сканирование подключаемых устройств; • эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; • нейтрализации действий активного заражения; • анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; • анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; • откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; • ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые

		настраиваемые списки приложений с определением уровня доверия; • облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP; • фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов; • проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики; • блокировку баннеров и всплывающих окон на загружаемых Web-страницах; • распознавания и блокировку фишинговых и небезопасных сайтов; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; • возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; • контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений; • создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; • 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; • возможность управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств; • записи в журнал событий о записи и/или удалении файлов на съемных дисках; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защиты от атак типа BadUSB; • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля; • установки только выбранных компонентов программного средства антивирусной защиты; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • запуск задач по расписанию и/или сразу после запуска приложения;

		• гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • возможность проверки целостности антивирусной программы; • возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи; • наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; • наличие защищенного хранилища для отчетов о работе антивируса; • возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей; • возможность интеграции с Windows Defender Security Center; • наличие поддержки Antimalware Scan Interface (AMSI); • наличие поддержки Windows Subsystem for Linux (WSL); • возможность защитить паролем восстановление объектов из резервного хранилища. **Требования к программным средствам антивирусной защиты для серверов Windows** Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий: • Windows Small Business Server 2008 Standard / Premium (64-разрядная); • Windows Small Business Server 2011 Essentials / Standard (64-разрядная); • Windows MultiPoint Server 2011 (64-разрядная); • Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная); • Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная); • Windows Server 2012 Foundation / Essentials / Standard (64-разрядная); • Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная); • Windows Server 2016 (64-разрядная) (с ограничениями); • Windows Server 2019 (64-разрядная) (с ограничениями). В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта; • антивирусное сканирование по расписанию; • антивирусное сканирование подключаемых устройств; • эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; • нейтрализации действий активного заражения; • анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; • анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; • откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; • ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия; • облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

		• антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; • создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • защиты 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; • установки только выбранных компонентов программного средства антивирусной защиты; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • возможность проверки целостности антивирусной программы; • возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи; • наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; • наличие защищенного хранилища для отчетов о работе антивируса; • возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей; • возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий); • возможность интеграции с Windows Defender Security Center; • наличие поддержки Antimalware Scan Interface (AMSI); • наличие поддержки Windows Subsystem for Linux (WSL); • возможность защитить паролем восстановление объектов из резервного хранилища. • **Требования к программным средствам антивирусной защиты для рабочих станций Linux** Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий: • Ubuntu 16.04 LTS и выше; • Red Hat® Enterprise Linux® 6.7 и выше; • CentOS 6.7 и выше; • Debian GNU / Linux 9.4 и выше; • Debian GNU / Linux 10;

		• Linux Mint 18.2 и выше; • Linux Mint 19 и выше; • Альт Линукс СПТ 8.0.0 Рабочая станция; • Альт Линукс СПТ 8.0.0 Сервер; • Альт Линукс 8.3 Рабочая станция; • Альт Линукс 8.3 Рабочая станция К; • Альт Линукс 8.3 Сервер; • Альт Линукс 8.3 Образование; • Альт Линукс 9 Рабочая станция; • Альт Линукс 9 Образование; • Гослинукс 6.6; Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 64-битных операционных систем следующих версий: • Ubuntu 16.04 LTS и выше; • Ubuntu 18.04 LTS и выше; • Red Hat Enterprise Linux 6.7 и выше; • Red Hat Enterprise Linux 7.2 и выше; • Red Hat Enterprise Linux 8.0 и выше; • CentOS 6.7 и выше; • CentOS 7.2 и выше; • CentOS 8.0 и выше; • Debian GNU / Linux 9.4 и выше; • Debian GNU / Linux 10.1 и выше; • OracleLinux 7.3 и выше; • SUSE® Linux Enterprise Server 15 и выше; • openSUSE® Leap 15 и выше; • Альт Линукс СПТ 8.0.0 Рабочая станция; • Альт Линукс СПТ 8.0.0 Сервер; • Альт Линукс 8.3 Рабочая станция; • Альт Линукс 8.3 Рабочая станция К; • Альт Линукс 8.3 Сервер; • Альт Линукс 8.3 Образование; • Альт Линукс 9 Рабочая станция; • Альт Линукс 9 Сервер; • Альт Линукс 9 Образование; • Amazon Linux AMI; • Linux Mint 18.2 и выше; • Linux Mint 19 и выше; • Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды); • Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды); • Astra Linux Common Edition «Орел» 2.12; • ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем; • ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем; • Гослинукс 6.6; • Гослинукс 7.2; В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • резидентного антивирусного мониторинга; • облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • проверку ресурсов доступных по SMB / NFS; • эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; • антивирусное сканирование по команде пользователя или администратора и по расписанию;

		• антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.; • проверку сообщений электронной почты в текстовом формате (Plain text); • наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); • защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; • помещение подозрительных и поврежденных объектов на карантин; • проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов; • возможность перехвата и проверки файловых операций на уровне SAMBA; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность экспортировать и сохранять отчеты в форматах HTML и CSV; • гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; • возможность управления через пользовательский графический интерфейс без root прав; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления. **Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows** Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: **32-разрядных операционных систем Microsoft Windows** • Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше. **64-разрядных операционных систем Microsoft Windows** • Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Microsoft Small Business Server 2008 Standard / Premium; • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше; • Microsoft Small Business Server 2011 Essentials / Standard; • Microsoft Windows MultiPoint™ Server 2011 Standard / Premium; • Windows Server 2012 Foundation / Essentials / Standard / Datacenter; • Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;

		• Microsoft Windows MultiPoint Server 2012 Standard / Premium; • Windows Storage Server 2012; • Windows Hyper-V Server 2012; • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; • Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; • Windows Storage Server 2012 R2; • Windows Hyper-V Server 2012 R2; • Windows Server 2016 Essentials / Standard / Datacenter; • Windows Server 2016 MultiPoint; • Windows Server 2016 Core Standard / Datacenter; • Microsoft Windows MultiPoint Server 2016; • Windows Storage Server 2016; • Windows Hyper-V Server 2016; • Windows Server 2019 Essentials / Standard / Datacenter; • Windows Server 2019 Core; • Windows Storage Server 2019; • Windows Hyper-V Server 2019. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов; • 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; • антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB; • защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков; • непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными. • анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • возможность проверки контейнеров Microsoft Windows; • защиты от эксплуатирования уязвимостей в памяти процессов; • должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться; • возможность добавлять процессы в список защищаемых; • ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи; • 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); • ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;

		• возможность интеграции с SIEM системами; • возможность указания количества рабочих процессов антивируса вручную; • возможность отключить графический интерфейс; • наличие удаленной и локальной консоли управления; • управления параметрами антивируса из командной строки; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил. **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 7 32-разрядная / 64-разрядная; • Microsoft Windows 8 32 разрядная / 64-разрядная; • Microsoft Windows 8;1 32-разрядная / 64-разрядная; • Microsoft Windows 10 32-разрядная / 64-разрядная; • Windows Server 2012, 2012 R2 64-разрядная; • Windows Server 2016 64-разрядная; • Windows Server 2019 Standard, Datacenter. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: • VMware vSphere 6; • VMware Workstation 15 Pro; • Microsoft Hyper-V Server 2012, 2012 R2; • Citrix XenServer 7; • Citrix XenServer 8.x; • Parallels Desktop 14 для Mac; • Oracle VM VirtualBox 6. Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: • Microsoft SQL 2012 Express, 2014 Express 64-разрядная; • Microsoft SQL Server 2012 (все редакции) 64-разрядная; • Microsoft SQL Server 2014 (все редакции) 64-разрядная; • Microsoft SQL Server 2016 (все редакции) 64-разрядная; • Microsoft SQL Server 2017 (для Windows) 64-разрядная; • Microsoft Azure SQL Database; • MySQL 5.7 32-разрядная / 64-разрядная; • MySQL Enterprise 5.7 32-разрядная / 64-разрядная. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов; • возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации; • возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD; • 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; • централизованные установка, обновление и удаление программных средств антивирусной защиты; • централизованная настройка, администрирование; • просмотр отчетов и статистической информации по работе средств защиты; • централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; • сохранение истории изменений политик и задач, возможность выполнить откат к

		предыдущим версиям; • наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки; • возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; • возможность иерархии триггеров по которым происходит перераспределение; • тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; • доставка обновлений на рабочие места пользователей сразу после их получения; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; • создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня; • поддержка мультиарендности (multi-tenancy) для серверов управления; • 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; • наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них; • функция управления мобильными устройствами через сервер Exchange ActiveSync; • функция управления мобильными устройствами через сервер iOS MDM; • возможность отправки SMS-оповещений о заданных событиях; • централизованная установка сертификатов на управляемые мобильные устройства; • 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 по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ; • наличие преднастроенных стандартных отчетов о работе системы; • экспорт отчетов в файлы форматов PDF и XML; • централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; • создание внутренних учетных записей для аутентификации на сервере управления; • создание резервной копии системы управления встроенными средствами системы управления; • поддержка Windows Failover Clustering; • поддержка интеграции с Windows сервисом Certificate Authority; • наличие портала самообслуживания пользователей; • портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; • наличие системы контроля возникновения вирусных эпидемий;

		• возможность установки в облачной инфраструктуре Microsoft Azure; • возможность интеграции по OpenAPI; • возможность управления антивирусной защитой с использованием WEB консоли. **Требования к обновлению антивирусных баз** Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: • создания правил обновления 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. **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. **Требования к технической поддержке** Техническая поддержка антивирусного программного обеспечения должна: • Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет. • Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.
5.	Сроки и условия оказания услуг	ПО должно быть предоставлено в течение 5 (пяти) рабочих дней с даты заключения договора Пакет документов, подтверждающих право устанавливать и использовать антивирусное программное обеспечение должен быть предоставлен в бумажном виде в течение 5 рабочих дней с даты подписания договора
6.	Порядок передачи прав	Лицензионный ключ в электронном виде направляется на адрес электронной почты Заказчика _____.
7.	Требования к участнику по обладанию правами на предоставление права на использование ПО Kaspersky другим лицам.	Участник гарантирует, что в соответствии с законодательством РФ и /или заключенными договорами с правообладателем, имеет все права, необходимые для передачи экземпляров ПО и исполнения иных обязательств по настоящему Договору. *(Данное требование может быть подтверждено предоставлением одним из следующих документов:* *1. Заверенное участником авторизационное письмо от правообладателя (лицензиара) ПО, подтверждающее партнёрский статус и/или право на поставку со стороны участника закупки ПО* Kaspersky *другим лицам;* *2. Заверенная участником копия Договора, подтверждающего возможность предоставления права на использование ПО* Kaspersky *другим лицам;* *3. Гарантийное письмо участника закупки о том, что он является правообладателем. Примечание: в гарантийном письме указать предмет закупки, заказчика, участника, дату.)*
8.	Требования к качеству услуг	Качество оказанных услуг в сфере информационных технологий по передаче неисключительных прав на ПО должно соответствовать требованиям, предъявляемым к услугам подобного рода (безотказно работать на аппаратном комплексе Заказчика), в соответствии с настоящим техническим заданием.

		Исполнитель гарантирует качество и безопасность передаваемых Лицензий на использование программного обеспечения в соответствии с действующими стандартами и наличием сертификатов, обязательных для данного вида товара, оформленных в соответствии с требованиями Российского Законодательства. Исполнитель несет ответственность за недостатки (дефекты) Лицензий на использование программного обеспечения, в том числе за качество, количество, срок действия Лицензии, обнаруженные Заказчиком в пределах гарантийного срока, и безвозмездно их устраняет по письменному заявлению Заказчика в течение 3-х (трех) рабочих дней с момента составления соответствующего акта. Заказчику должны быть предоставлены права конечного пользователя программного обеспечения на условиях простой (неисключительной) лицензии определенными договором способами в течение 12 месяцев с момента подписания акта приемки-передачи. К разрешенным способам использования программного обеспечения относятся: воспроизведение; хранение ее в памяти ЭВМ (одной ЭВМ или одного пользователя сети); активация; запуск в работу; обновление и актуализация.
9.	Гарантийные обязательства	- Исполнитель гарантирует, что передаваемое ПО обеспечит выполнение функций при условиях, описанных в документации, а также то, что носитель ПО лишен дефектов. Тара и внутренняя упаковка должны обеспечивать сохранность и предохранять ПО от повреждений при транспортировке всеми видами транспорта с учетом погрузочно-разгрузочных работ. Гарантия Исполнителя действует в течение 12 месяцев с момента поставки ПО. Гарантии по качеству работы ПО определяются в соответствии с условиями лицензионного соглашения, прилагаемого к ПО и не могут превышать объема, предусмотренного условиями лицензионного соглашения.
10.	Территорией правомерного использования ПО	Территория Российской Федерации.
11.	Страна происхождения ПО	
11.	Требования к безопасности	Требований, наличия ГОСТ – не предусмотрено.

На все закупаемые товары, где указаны товарные знаки, Участник закупки может предложить эквивалент, который в свою очередь должен точно соответствовать техническим характеристикам, указанным в техническом задании или превышать их и не уступать по качеству затребованным товарам

Приложение № 3 к запросу в целях формирования представления о рыночных ценах

проект

ДОГОВОР № _____

г. Ярославль «___» _____ 20__ г.

Государственное автономное учреждение Ярославской области «Информационное агентство «Верхняя Волга», в лице _____, действующего на основании _____, именуемое в дальнейшем «Заказчик», с одной стороны, и _____, в лице _____, действующего на основании _____, именуемое в дальнейшем «Исполнитель», с другой стороны, а вместе именуемые «Стороны», заключили настоящий договор (далее - Договор) о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Исполнитель обязуется оказать услуги по предоставлению неисключительных прав на использование лицензионного программного обеспечения Kaspersky Endpoint Security для бизнеса – Стандартный (продление лицензий на антивирусное программное обеспечение) для нужд Заказчика, в соответствии с условиями Договора, Технического задания (приложение № 1 к Договору), являющимися неотъемлемой частью Договора (далее – услуги), а Заказчик обязуется принять и оплатить оказанные услуги (результат оказанных услуг) в порядке и на условиях, предусмотренных Договором.

1.2. Продление неисключительных лицензионных прав использования антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса — Стандартный осуществляется в отношении ранее установленного и используемого Заказчиком антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Стандартный.

1.3. Перечень, объем, характеристика (описание), порядок оказания, стоимость услуг указываются в Техническом задании.

1.4. Предоставление неисключительной лицензии осуществляется путем предоставления Исполнителем Заказчику:

- лицензионного соглашения, определяющего условия использования Заказчиком программного обеспечения и подтверждающего права Заказчика на обновление и поддержку (гарантийное сопровождение);
- лицензионного ключа в электронном виде, направляемого на адрес электронной почты Заказчика _____.

1.5. Исполнитель обязан оказать услуги лично, без привлечения третьих лиц.

2. ЦЕНА ДОГОВОРА И ПОРЯДОК РАСЧЕТОВ

2.1. Цена Договора составляет _____ рублей _____ копеек (_____ рублей _____ копеек), в том числе НДС ____ рублей ___ копеек (_____ рублей ___ копеек).

2.2. Цена Договора является твердой и определяется на весь срок его исполнения.

2.3. Цена Договора формируется с учетом общей стоимости услуг, транспортных и других расходов, связанных с оказанием услуг, а также таможенных пошлин, страхования, налогов, сборов и других обязательных платежей, установленных законодательством Российской Федерации.

2.4. Расчет с Исполнителем за оказанные услуги осуществляется Заказчиком в рублях Российской Федерации. Оплата по Договору осуществляется по безналичному расчету путем перечисления Заказчиком денежных средств на расчетный счет Исполнителя, указанный в Договоре.

2.5. Оплата производится Заказчиком в течение 10 (десяти) рабочих дней после подписания Сторонами надлежаще оформленных документов, подтверждающих факт оказания услуг в соответствии с условиями Договора и приложений к нему, если иной порядок оплаты не предусмотрен в Техническом задании к Договору

2.6. Датой (днем) оплаты Договора Стороны считают дату (день) списания денежных средств со счета Заказчика.

2.7. При необходимости Стороны проводят сверку взаиморасчетов путем подписания соответствующего акта.

2.8. Источник финансирования: средства областного бюджета Ярославской области (субсидия).

3. КАЧЕСТВО УСЛУГ И ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

3.1. Качество оказываемых услуг должно соответствовать требованиям документов стандартизации и технического регулирования (ГОСТ, ТУ и других), установленных для данного типа (вида) услуг, подтверждаться документами на русском языке (при наличии). Требования к качеству услуг, порядку их оказания, требования к результатам оказанных услуг указываются в Техническом задании.

3.2. Гарантии Исполнителя и гарантийные обязательства:

3.2.1. Исполнитель гарантирует, что:

3.2.1.1. Исполнение обязательств по Договору не нарушит имущественных и неимущественных прав Заказчика и третьих лиц.

3.2.1.2. Услуги оказаны надлежащего качества, в том числе с применением материалов и оборудования, отвечающих требованиям ГОСТов, ТУ и иным требованиям, установленным действующим законодательством Российской Федерации, квалифицированными специалистами (если при оказании услуг требуется применение материалов и оборудования).

3.3. Извещение (претензия) о выявленных недостатках направляется Заказчиком Исполнителю в течение 15 дней со дня их обнаружения.

3.4. Гарантийный срок на оказанные услуги (результат оказанных услуг), гарантийные обязательства, срок, с которого начинает течь гарантия, требования к гарантийному обслуживанию, к расходам на обслуживание результатов услуг в гарантийный срок, наличие гарантии производителя, условия и срок гарантии производителя, срок, в течение которого Исполнителем должны быть устранены недостатки оказанной услуги, указываются в Техническом задании.

3.5. Гарантийный срок продлевается на время, в течение которого результаты услуги не могли использоваться из-за обнаруженных в них недостатков, при условии извещения Исполнителя о недостатках услуг.

3.6. Исполнитель обязан возместить расходы Заказчика на устранение недостатков оказанной услуг. Если отступления при оказании услуг от условий Договора или иные недостатки результата услуги не были устранены в установленный Заказчиком срок либо являются существенными и неустранимыми, Заказчик вправе отказаться от исполнения Договора и потребовать возмещения причиненных убытков.

3.7. Исполнитель несет ответственность за надлежащее качество предоставленных им материалов и оборудования, используемых при оказании услуг, а также за предоставление материалов и оборудования, обремененных правами третьих лиц (если при выполнении работ требуется применение материалов и оборудования).

3.8. Если Исполнитель не приступает своевременно к исполнению обязательств по Договору или оказывает услуги настолько медленно, что окончание их к сроку становится явно невозможным, Заказчик вправе отказаться от исполнения Договора и потребовать возмещения убытков.

4. СРОК, МЕСТО ОКАЗАНИЯ УСЛУГ, ПОРЯДОК ОКАЗАНИЯ И ПРИЕМА-СДАЧИ ОКАЗАННЫХ УСЛУГ

4.1. Место, сроки (период), порядок оказания и приема-сдачи оказанных услуг, включая перечень информации и (или) документы, необходимые для исполнения обязательств, передаваемых Исполнителем по результатам оказанных услуг, указываются в Техническом задании.

4.2. Право собственности на результат услуг прекращается у Исполнителя с момента приемки услуг Заказчиком в соответствии с условиями Договора, если иное не установлено Техническим заданием.

4.3. Все риски, связанные с оказанием услуг до момента их приемки Заказчиком, несет Исполнитель.

4.4. В случае, если услуги оказаны некачественно, Заказчик вправе потребовать от Исполнителя безвозмездного устранения недостатков в сроки, установленные Заказчиком, а также возмещения расходов на устранение недостатков. Устранение недостатков в результате ненадлежащего качества оказанных услуг осуществляется за счет средств Исполнителя.

4.5. Заказчик, обнаруживший после приемки услуг отступления в ней от Договора или иные недостатки, которые не могли быть установлены при приемке (скрытые недостатки), в том числе такие, которые были умышленно скрыты Исполнителем, обязан известить об этом Исполнителя в течение 10 дней по их обнаружении и вправе потребовать безвозмездного их устранения и возмещения убытков.

4.6. Передача неисключительных прав предусмотренных настоящим Контрактом от Исполнителя Заказчику осуществляется по акту приема-передачи неисключительных прав на использование Программного обеспечения.

5. ПРАВА И ОБЯЗАННОСТИ ЗАКАЗЧИКА

5.1. Заказчик по Договору вправе:

5.1.1. Требовать от Исполнителя надлежащего исполнения принятых им обязательств, а также своевременного устранения выявленных недостатков.

5.1.2. Требовать от Исполнителя предоставления надлежаще оформленных документов, подтверждающих исполнение принятых им обязательств.

5.1.3. Контролировать ход оказания услуг, соблюдение срока оказания услуг, проверять соответствие услуг условиям Договора и приложений к нему.

5.1.4. При обнаружении недостатков оказанных услуг, требовать их устранения. Требование подлежит обязательному выполнению Исполнителем.

5.1.5. Определять лиц, непосредственно участвующих в контроле за ходом оказания услуг.

5.1.6. Осуществлять иные права в соответствии с действующим законодательством Российской Федерации.

5.2. Заказчик по Договору обязан:

5.2.1. Обеспечить приемку оказанных услуг.

5.2.2. Произвести оплату в соответствии с разделом 2 Договора.

5.2.3. Надлежаще исполнять иные принятые на себя обязательства.

6. ПРАВА И ОБЯЗАННОСТИ ИСПОЛНИТЕЛЯ

6.1. Исполнитель по Договору вправе:

6.1.1. Требовать своевременной приемки надлежаще оказанных услуг.

6.1.2. Требовать своевременной оплаты принятых Заказчиком услуг.

6.1.4. Осуществлять иные права в соответствии с действующим законодательством Российской Федерации.

6.2. Исполнитель по Договору обязан:

6.2.1. Оказать услуги в соответствии с принятыми на себя обязательствами.

6.2.2. В соответствии с условиями Договора своевременно предоставлять достоверную информацию о ходе исполнения своих обязательств, в том числе о сложностях, возникающих при исполнении Договора, а также к установленному Договором сроку обязан предоставить Заказчику результаты оказанных услуг, предусмотренные Договором. Срок предоставления информации о ходе исполнения принятых на себя обязательств составляет 10 дней с момента получения запроса Заказчика.

6.2.3. Предоставить надлежаще оформленные документы, предусмотренные Договором и приложениями к нему.

6.2.4. Устранить за свой счет все выявленные недостатки, в том числе скрытые, при оказании услуг.

6.2.5. Немедленно предупредить Заказчика и до получения от него указаний приостановить оказание услуг при обнаружении возможных неблагоприятных для Заказчика последствий оказания услуги или иных не зависящих от Исполнителя обстоятельств, которые грозят качеству оказанных услуг либо создают невозможность их завершения в срок.

6.2.6. При изменении наименования, юридического адреса, реквизитов и иных сведений в течение трех дней со дня изменения таких сведений письменно известить об этом Заказчика.

6.2.7. Хранить в тайне любую информацию и данные, предоставляемые в связи с исполнением Договора, не раскрывать и не разглашать третьим лицам в целом или частично факты и информацию без предварительного письменного согласия Заказчика, не использовать факты или информацию, полученные при исполнении Договора, для любых целей без предварительного согласия Заказчика. Обязательства конфиденциальности, возложенные на Исполнителя Договором, не распространяются на общедоступную информацию.

6.2.8. Обеспечивать конфиденциальность персональных данных и их безопасность при обработке в соответствии с законодательством о персональных данных, а также иных сведений, составляющих тайну в соответствии с действующим законодательством, в случае, если при исполнении обязательств по Договору требуется доступ к таким данным или такие данные стали известными в процессе исполнения обязательств, предусмотренных Договором.

6.2.9. Надлежаще исполнять иные принятые на себя обязательства по Договору.

7. ОТВЕТСТВЕННОСТЬ СТОРОН. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

7.1. За неисполнение или ненадлежащее исполнение обязательств по Договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

7.2. В случае просрочки исполнения Заказчиком обязательств, предусмотренных Договором, а также в иных случаях неисполнения или ненадлежащего исполнения Заказчиком обязательств, предусмотренных Договором, Исполнитель вправе потребовать уплаты неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения Заказчиком обязательства, предусмотренного Договором, начиная со дня, следующего после дня истечения установленного Договором срока исполнения обязательства. При этом размер пени устанавливается в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от не уплаченной в срок суммы.

За каждый факт неисполнения Заказчиком обязательств, предусмотренных Договором, за исключением просрочки исполнения обязательств, предусмотренных Договором, Исполнитель вправе взыскать с Заказчика штраф в размере _____ рублей.

Размер штрафа устанавливается, исходя из цены договора на момент заключения договора, в соответствии с постановлением Правительства Российской Федерации от 30.08.2017 № 1042, определяемой в следующем порядке:

а) 1000 рублей, если цена Договора не превышает 3 млн. рублей (включительно);

б) 5000 рублей, если цена Договора составляет от 3 млн. рублей до 50 млн. рублей (включительно);

в) 10000 рублей, если цена Договора составляет от 50 млн. рублей до 100 млн. рублей (включительно);

г) 100000 рублей, если цена Договора превышает 100 млн. рублей.

7.3. В случае просрочки исполнения Исполнителем обязательств, предусмотренных Договором, начисляется пеня за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного Договором, в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены Договора.

7.4. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Договором, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Договором, Исполнитель выплачивает Заказчику штраф в размере _____ рублей.

Размер штрафа устанавливается, исходя из цены договора на момент заключения договора, в соответствии с постановлением Правительства Российской Федерации от 30.08.2017 № 1042, определяемой в следующем порядке:

а) 10 процентов цены Договора (этапа) в случае, если цена Договора (этапа) не превышает 3 млн. рублей;

б) 5 процентов цены Договора (этапа) в случае, если цена Договора (этапа) составляет от 3 млн. рублей до 50 млн. рублей (включительно);

в) 1 процент цены Договора (этапа) в случае, если цена Договора (этапа) составляет от 50 млн. рублей до 100 млн. рублей (включительно);

г) 0,5 процента цены Договора (этапа) в случае, если цена Договора (этапа) составляет от 100 млн. рублей до 500 млн. рублей (включительно);

д) 0,4 процента цены Договора (этапа) в случае, если цена Договора (этапа) составляет от 500 млн. рублей до 1 млрд. рублей (включительно);

е) 0,3 процента цены Договора (этапа) в случае, если цена Договора (этапа) составляет от 1 млрд. рублей до 2 млрд. рублей (включительно);

ж) 0,25 процента цены Договора (этапа) в случае, если цена Договора (этапа) составляет от 2 млрд. рублей до 5 млрд. рублей (включительно);

з) 0,2 процента цены Договора (этапа) в случае, если цена Договора (этапа) составляет от 5 млрд. рублей до 10 млрд. рублей (включительно);

и) 0,1 процента цены Договора (этапа) в случае, если цена Договора (этапа) превышает 10 млрд. рублей.

7.5. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Договором, Заказчик вправе произвести оплату по Договору за вычетом соответствующего размера неустойки (штрафа, пени).

7.6. В случае просрочки исполнения Исполнителем обязательств (в том числе гарантийного обязательства), предусмотренных Договором, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Договором, Заказчик направляет Исполнителю требование об уплате неустоек (штрафов, пени).

7.7. Общая сумма начисленной неустойки (штрафов, пени) за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных Договором, не может превышать цену Договора.

7.8. Сторона освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного Договором, произошло вследствие непреодолимой силы или по вине другой Стороны.

7.9. К обстоятельствам непреодолимой силы относятся события, на которые Стороны не могут оказывать влияние и за возникновение которых ответственности не несут (землетрясение, наводнение, пожар, и другие

стихийные бедствия, принятие органами законодательной власти ограничительных норм права и другие). Указанные события должны оказывать прямое влияние на невозможность надлежащего исполнения Сторонами принятых обязательств по Договору. К таким обстоятельствам не относятся нарушение обязанностей со стороны контрагентов Исполнителя, отсутствие на рынке нужных для исполнения товаров, отсутствие необходимых денежных средств.

7.10. Сторона, ссылающаяся на обстоятельства непреодолимой силы, обязана в течение 3 (трех) календарных дней известить другую Сторону о наступлении действия или о прекращении действия подобных обстоятельств и предоставить надлежащее доказательство наступления обстоятельств непреодолимой силы. Надлежащим доказательством наличия указанных обстоятельств и их продолжительности будут служить заключения соответствующих компетентных органов.

Если Сторона не направит или несвоевременно направит необходимое извещение, то она обязана возместить другой Стороне убытки, причиненные неизвещением или несвоевременным извещением.

7.11. Стороны могут отказаться от дальнейшего исполнения обязательств по Договору по соглашению Сторон, если обстоятельство непреодолимой силы длится более 30 (тридцати) календарных дней.

7.12. Стороны ни при каких условиях не начисляют проценты, установленные ст. 317.1 Гражданского кодекса Российской Федерации.

8. РАЗРЕШЕНИЕ СПОРОВ

8.1. Все споры и разногласия, которые могут возникнуть в связи с выполнением обязательств по Договору, Стороны будут стремиться разрешать путем переговоров.

8.2. Претензия направляется в письменной форме с указанием допущенных нарушений со ссылкой на соответствующие положения Договора или его приложений, размер неустойки и (или) убытков, а также действия, которые должны быть произведены для устранения нарушений.

8.3. Срок рассмотрения писем, уведомлений или претензий не может превышать 10 (десять) календарных дней со дня их получения.

8.4. В случае если указанные споры и разногласия не могут быть разрешены путем переговоров, они подлежат разрешению в порядке, предусмотренном действующим законодательством Российской Федерации, в Арбитражном суде Ярославской области.

9. Антикоррупционная оговорка

9.1. При исполнении своих обязательств по настоящему Договору, Стороны, их аффилированные лица, работники или посредники не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам, для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества.

9.2. При исполнении своих обязательств по настоящему Договору, Стороны, их аффилированные лица, работники или посредники не осуществляют действия, квалифицируемые применимым для целей настоящего Договора законодательством, как дача или получение взятки, коммерческий подкуп, а также действия, нарушающие требования применимого законодательства и международных актов о противодействии легализации (отмыванию) доходов, полученных преступным путем.

9.3. В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений настоящей Статьи, соответствующая Сторона обязуется уведомить об этом другую Сторону в письменной форме. После письменного уведомления, соответствующая Сторона имеет право приостановить исполнение обязательств по настоящему Договору до получения подтверждения, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение десяти рабочих дней с даты получения письменного уведомления.

Каналы связи «Телефон доверия» Государственного автономного учреждения Ярославской области «Информационное агентство «Верхняя Волга»» 8(4852) 72-92-36.

9.4. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений настоящей Статьи контрагентом, его аффилированными лицами, работниками или посредниками выражающееся в действиях, квалифицируемых применимым законодательством, как дача или получение взятки, коммерческий подкуп, а также в действиях, нарушающих требования применимого законодательства и международных актов о противодействии легализации доходов, полученных преступным путем.

9.5. В случае нарушения одной Стороной обязательств воздерживаться от запрещенных в настоящем разделе Договора действий и/или неполучения другой Стороной в установленный в настоящем разделе Договора срок подтверждения, что нарушения не произошло или не произойдет, другая Сторона имеет право расторгнуть договор в одностороннем порядке полностью или в части, направив письменное уведомление о расторжении. Сторона, по чьей инициативе был расторгнут настоящий Договор в соответствии с положениями настоящей статьи, вправе требовать возмещения реального ущерба, возникшего в результате такого расторжения.

9.6. Любая информация, предоставляемая Сторонами друг другу в рамках настоящего Договора, считается конфиденциальной и не подлежит разглашению без письменного согласия на то другой Стороны, за исключением случаев, установленных законом Российской Федерации.

9.7. Все обязательства в отношении конфиденциальности в вопросах, связанных с исполнением настоящего Договора, Стороны обязуются соблюдать, и после прекращения действия настоящего Договора в течение 3 (Трех) лет.

9.8. Стороны обязуются ограничить распространение информации, связанной с исполнением настоящего Договора, только кругом лиц, имеющих к ней непосредственное отношение. Стороны обязуются принять все необходимые меры безопасности для защиты информации, документов и материалов, используемых в рамках настоящего Договора, от несанкционированного доступа.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Договор вступает в силу с момента подписания его Сторонами и действует до полного исполнения Сторонами взятых на себя по настоящему Договору обязательств. Прекращение (окончание) срока действия Договора не освобождает Стороны от ответственности за неисполнение или ненадлежащее исполнение Договора, если таковые имели место при исполнении условий Договора.

11.2. Любые изменения и дополнения к Договору должны быть совершены в письменной форме и подписаны надлежаще уполномоченными представителями Сторон.

11.3. Изменение условий договора, в том числе изменение цены договора, допускается в случаях, предусмотренных гражданским законодательством Российской Федерации и в случаях, предусмотренных разделом 27 Положения о закупке товаров, работ, услуг государственного автономного учреждения Ярославской области «Информационное агентство «Верхняя Волга».

11.4. Все уведомления и извещения, необходимые в соответствии с Договором, совершаются в письменной форме и должны быть переданы лично или направлены заказной почтой, электронным сообщением, по факсу или иным способом, позволяющим установить факт отправки корреспонденции, с последующим предоставлением оригинала по адресам, указанным Сторонами.

11.5. Договор может быть расторгнут по соглашению Сторон, по решению суда, в случае одностороннего отказа одной из Сторон от исполнения Договора в соответствии с гражданским законодательством.

11.6. Заказчик вправе отказаться от исполнения договора в одностороннем порядке в случае неисполнения (ненадлежащего исполнения) Исполнителем обязательств, предусмотренных договором.

11.7. В случае установления факта представления Исполнителем недостоверных сведений, послуживших основанием для признания его победителем закупки и заключения с ним договора, Принципал вправе расторгнуть такой договор на любом этапе его исполнения.

11.8. При исполнении договора не допускается замена поставщика (подрядчика, исполнителя), за исключением случаев, когда новый поставщик (подрядчик, исполнитель) является правопреемником предыдущего поставщика (подрядчика, исполнителя), с которым заключен договор, в соответствии с гражданским законодательством Российской Федерации (в случае реорганизации юридического лица в форме преобразования, слияния или присоединения). В случае перемены поставщика (подрядчика, исполнителя) его права и обязанности переходят к новому поставщику (подрядчику, исполнителю) на тех же условиях и в том же объеме.

11.9. При расторжении Договора в связи с односторонним отказом Стороны Договора от исполнения Договора другая Сторона Договора вправе потребовать возмещения только фактически понесенного ущерба, непосредственно обусловленного обстоятельствами, являющимися основанием для принятия решения об одностороннем отказе от исполнения Договора.

11.10. В части отношений между Сторонами, неурегулированной положениями Договора, применяется действующее законодательство Российской Федерации.

11.11. Если какое-либо из положений Договора становится недействительным, это не затрагивает действительности остальных его положений.

11.12. Приложение № 1 «Техническое задание» к Договору являются неотъемлемой частью Договора.

11. ЮРИДИЧЕСКИЕ АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Заказчик	**Исполнитель**
_____ /_____	_____ /_____
(подпись)	(подпись)
(м.п.)	(м.п.)

Приложение № 1
к договору № _____ от «___» _____ 20___г.

Техническое задание
на предоставление лицензионных прав на пользование программным обеспечением Kaspersky Endpoint Security для бизнеса – Стандартный

1.	Предмет закупки, характеристики	Оказание услуг по предоставлению неисключительных прав на использование лицензионного программного обеспечения Kaspersky Endpoint Security для бизнеса – Стандартный (продление лицензий на антивирусное программное обеспечение) для нужд Заказчика сроком на 12 месяцев.
2.	Количество/Место оказания услуг	132 штуки (лицензии)/150000, г. Ярославль ул. Максимова, д. 17/27
3.	Срок действия лицензии	12 месяцев с момента активации лицензии (ключей)
4.	Требования к характеристикам товара	**Общие требования** Антивирусные средства должны включать: • программные средства антивирусной защиты для рабочих станций Windows; • программные средства антивирусной защиты для рабочих станций Linux; • программные средства антивирусной защиты для файловых серверов Windows; • программные средства централизованного управления, мониторинга и обновления; • обновляемые базы данных сигнатур вредоносных программ и атак; • эксплуатационную документацию на русском языке. Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке. **Требования к программным средствам антивирусной защиты для рабочих станций Windows** Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий: • Windows 7 Home / Professional / Enterprise (32 / 64-разрядная); • Windows 8 Professional / Enterprise (32 / 64-разрядная); • Windows 8.1 Professional / Enterprise (32 / 64-разрядная); • Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная). В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта; • антивирусное сканирование по расписанию; • антивирусное сканирование подключаемых устройств; • эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; • нейтрализации действий активного заражения; • анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; • анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; • откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; • ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые

		настраиваемые списки приложений с определением уровня доверия; • облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP; • фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов; • проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики; • блокировку баннеров и всплывающих окон на загружаемых Web-страницах; • распознавания и блокировку фишинговых и небезопасных сайтов; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа; • возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; • контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений; • создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; • 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; • возможность управления MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств; • записи в журнал событий о записи и/или удалении файлов на съемных дисках; • контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory; • защиты от атак типа BadUSB; • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля; • установки только выбранных компонентов программного средства антивирусной защиты; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • запуск задач по расписанию и/или сразу после запуска приложения;

		• гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • возможность проверки целостности антивирусной программы; • возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи; • наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; • наличие защищенного хранилища для отчетов о работе антивируса; • возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей; • возможность интеграции с Windows Defender Security Center; • наличие поддержки Antimalware Scan Interface (AMSI); • наличие поддержки Windows Subsystem for Linux (WSL); • возможность защитить паролем восстановление объектов из резервного хранилища. **Требования к программным средствам антивирусной защиты для серверов Windows** Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий: • Windows Small Business Server 2008 Standard / Premium (64-разрядная); • Windows Small Business Server 2011 Essentials / Standard (64-разрядная); • Windows MultiPoint Server 2011 (64-разрядная); • Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная); • Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная); • Windows Server 2012 Foundation / Essentials / Standard (64-разрядная); • Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная); • Windows Server 2016 (64-разрядная) (с ограничениями); • Windows Server 2019 (64-разрядная) (с ограничениями). В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта; • антивирусное сканирование по расписанию; • антивирусное сканирование подключаемых устройств; • эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы; • нейтрализации действий активного заражения; • анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий; • анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов; • откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов; • ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия; • облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

		• антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE; • встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов; • возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства; • создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки; • запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям. • защиты 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; • установки только выбранных компонентов программного средства антивирусной защиты; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • возможность проверки целостности антивирусной программы; • возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи; • наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления; • наличие защищенного хранилища для отчетов о работе антивируса; • возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей; • возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий); • возможность интеграции с Windows Defender Security Center; • наличие поддержки Antimalware Scan Interface (AMSI); • наличие поддержки Windows Subsystem for Linux (WSL); • возможность защитить паролем восстановление объектов из резервного хранилища. • **Требования к программным средствам антивирусной защиты для рабочих станций Linux** Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 32-битных операционных систем следующих версий: • Ubuntu 16.04 LTS и выше; • Red Hat® Enterprise Linux® 6.7 и выше; • CentOS 6.7 и выше; • Debian GNU / Linux 9.4 и выше; • Debian GNU / Linux 10;

		• Linux Mint 18.2 и выше; • Linux Mint 19 и выше; • Альт Линукс СПТ 8.0.0 Рабочая станция; • Альт Линукс СПТ 8.0.0 Сервер; • Альт Линукс 8.3 Рабочая станция; • Альт Линукс 8.3 Рабочая станция К; • Альт Линукс 8.3 Сервер; • Альт Линукс 8.3 Образование; • Альт Линукс 9 Рабочая станция; • Альт Линукс 9 Образование; • Гослинукс 6.6; Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением следующих 64-битных операционных систем следующих версий: • Ubuntu 16.04 LTS и выше; • Ubuntu 18.04 LTS и выше; • Red Hat Enterprise Linux 6.7 и выше; • Red Hat Enterprise Linux 7.2 и выше; • Red Hat Enterprise Linux 8.0 и выше; • CentOS 6.7 и выше; • CentOS 7.2 и выше; • CentOS 8.0 и выше; • Debian GNU / Linux 9.4 и выше; • Debian GNU / Linux 10.1 и выше; • OracleLinux 7.3 и выше; • SUSE® Linux Enterprise Server 15 и выше; • openSUSE® Leap 15 и выше; • Альт Линукс СПТ 8.0.0 Рабочая станция; • Альт Линукс СПТ 8.0.0 Сервер; • Альт Линукс 8.3 Рабочая станция; • Альт Линукс 8.3 Рабочая станция К; • Альт Линукс 8.3 Сервер; • Альт Линукс 8.3 Образование; • Альт Линукс 9 Рабочая станция; • Альт Линукс 9 Сервер; • Альт Линукс 9 Образование; • Amazon Linux AMI; • Linux Mint 18.2 и выше; • Linux Mint 19 и выше; • Astra Linux Special Edition 1.5 (обычный режим и режим замкнутой программной среды); • Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды); • Astra Linux Common Edition «Орел» 2.12; • ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем; • ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем; • Гослинукс 6.6; • Гослинукс 7.2; В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • резидентного антивирусного мониторинга; • облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу; • проверку ресурсов доступных по SMB / NFS; • эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы; • антивирусное сканирование по команде пользователя или администратора и по расписанию;

		• антивирусную проверка файлов в архивах zip; .7z*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.; • проверку сообщений электронной почты в текстовом формате (Plain text); • наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов); • защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования; • помещение подозрительных и поврежденных объектов на карантин; • проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов; • возможность перехвата и проверки файловых операций на уровне SAMBA; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил; • запуск задач по расписанию и/или сразу после загрузки операционной системы; • возможность экспортировать и сохранять отчеты в форматах HTML и CSV; • гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства; • сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность; • возможность управления через пользовательский графический интерфейс без root прав; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления. **Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows** Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: **32-разрядных операционных систем Microsoft Windows** • Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Core / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше. **64-разрядных операционных систем Microsoft Windows** • Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше; • Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Microsoft Small Business Server 2008 Standard / Premium; • Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше; • Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше; • Microsoft Small Business Server 2011 Essentials / Standard; • Microsoft Windows MultiPoint™ Server 2011 Standard / Premium; • Windows Server 2012 Foundation / Essentials / Standard / Datacenter; • Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;

		• Microsoft Windows MultiPoint Server 2012 Standard / Premium; • Windows Storage Server 2012; • Windows Hyper-V Server 2012; • Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter; • Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter; • Windows Storage Server 2012 R2; • Windows Hyper-V Server 2012 R2; • Windows Server 2016 Essentials / Standard / Datacenter; • Windows Server 2016 MultiPoint; • Windows Server 2016 Core Standard / Datacenter; • Microsoft Windows MultiPoint Server 2016; • Windows Storage Server 2016; • Windows Hyper-V Server 2016; • Windows Server 2019 Essentials / Standard / Datacenter; • Windows Server 2019 Core; • Windows Storage Server 2019; • Windows Hyper-V Server 2019. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов; • 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; • антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB; • защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков; • непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными. • анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети; • возможность проверки контейнеров Microsoft Windows; • защиты от эксплуатирования уязвимостей в памяти процессов; • должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться; • возможность добавлять процессы в список защищаемых; • ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось; • проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи; • 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); • ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;

		• возможность интеграции с SIEM системами; • возможность указания количества рабочих процессов антивируса вручную; • возможность отключить графический интерфейс; • наличие удаленной и локальной консоли управления; • управления параметрами антивируса из командной строки; • централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления; • управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил. **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 7 32-разрядная / 64-разрядная; • Microsoft Windows 8 32 разрядная / 64-разрядная; • Microsoft Windows 8;1 32-разрядная / 64-разрядная; • Microsoft Windows 10 32-разрядная / 64-разрядная; • Windows Server 2012, 2012 R2 64-разрядная; • Windows Server 2016 64-разрядная; • Windows Server 2019 Standard, Datacenter. Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах: • VMware vSphere 6; • VMware Workstation 15 Pro; • Microsoft Hyper-V Server 2012, 2012 R2; • Citrix XenServer 7; • Citrix XenServer 8.x; • Parallels Desktop 14 для Mac; • Oracle VM VirtualBox 6. Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий: • Microsoft SQL 2012 Express, 2014 Express 64-разрядная; • Microsoft SQL Server 2012 (все редакции) 64-разрядная; • Microsoft SQL Server 2014 (все редакции) 64-разрядная; • Microsoft SQL Server 2016 (все редакции) 64-разрядная; • Microsoft SQL Server 2017 (для Windows) 64-разрядная; • Microsoft Azure SQL Database; • MySQL 5.7 32-разрядная / 64-разрядная; • MySQL Enterprise 5.7 32-разрядная / 64-разрядная. В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности: • выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов; • возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации; • возможность настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD; • 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; • централизованные установка, обновление и удаление программных средств антивирусной защиты; • централизованная настройка, администрирование; • просмотр отчетов и статистической информации по работе средств защиты; • централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления; • сохранение истории изменений политик и задач, возможность выполнить откат

		к предыдущим версиям; • наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки; • возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности; • возможность иерархии триггеров по которым происходит перераспределение; • тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины; • доставка обновлений на рабочие места пользователей сразу после их получения; • распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере; • построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне; • создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня; • поддержка мультиарендности (multi-tenancy) для серверов управления; • 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; • наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них; • функция управления мобильными устройствами через сервер Exchange ActiveSync; • функция управления мобильными устройствами через сервер iOS MDM; • возможность отправки SMS-оповещений о заданных событиях; • централизованная установка сертификатов на управляемые мобильные устройства; • 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 по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ; • наличие преднастроенных стандартных отчетов о работе системы; • экспорт отчетов в файлы форматов PDF и XML; • централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение; • создание внутренних учетных записей для аутентификации на сервере управления; • создание резервной копии системы управления встроенными средствами системы управления; • поддержка Windows Failover Clustering; • поддержка интеграции с Windows сервисом Certificate Authority; • наличие портала самообслуживания пользователей; • портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя; • наличие системы контроля возникновения вирусных эпидемий;

		• возможность установки в облачной инфраструктуре Microsoft Azure; • возможность интеграции по OpenAPI; • возможность управления антивирусной защитой с использованием WEB консоли. **Требования к обновлению антивирусных баз** Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей: • создания правил обновления 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. **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. **Требования к технической поддержке** Техническая поддержка антивирусного программного обеспечения должна: • Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет. • Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.
5.	Сроки и условия оказания услуг	ПО должно быть предоставлено в течение 5 (пяти) рабочих дней с даты заключения договора Пакет документов, подтверждающих право устанавливать и использовать антивирусное программное обеспечение должен быть предоставлен в бумажном виде в течение 5 рабочих дней с даты подписания договора
6.	Порядок передачи прав	Лицензионный ключ в электронном виде направляется на адрес электронной почты Заказчика _____.
7.	Требования к участнику по обладанию правами на предоставление права на использование ПО Kaspersky другим лицам.	Участник гарантирует, что в соответствии с законодательством РФ и /или заключенными договорами с правообладателем, имеет все права, необходимые для передачи экземпляров ПО и исполнения иных обязательств по настоящему Договору. *(Данное требование может быть подтверждено предоставлением одним из следующих документов:* *1. Заверенное участником авторизационное письмо от правообладателя (лицензиара) ПО, подтверждающее партнёрский статус и/или право на поставку со стороны участника закупки ПО* Kaspersky *другим лицам;* *2. Заверенная участником копия Договора, подтверждающего возможность предоставления права на использование ПО* Kaspersky *другим лицам;* *3. Гарантийное письмо участника закупки о том, что он является правообладателем. Примечание: в гарантийном письме указать предмет закупки, заказчика, участника, дату.)*
8.	Требования к качеству услуг	Качество оказанных услуг в сфере информационных технологий по передаче неисключительных прав на ПО должно соответствовать требованиям, предъявляемым к услугам подобного рода (безотказно работать на аппаратном комплексе Заказчика), в соответствии с настоящим техническим заданием.

		Исполнитель гарантирует качество и безопасность передаваемых Лицензий на использование программного обеспечения в соответствии с действующими стандартами и наличием сертификатов, обязательных для данного вида товара, оформленных в соответствии с требованиями Российского Законодательства. Исполнитель несет ответственность за недостатки (дефекты) Лицензий на использование программного обеспечения, в том числе за качество, количество, срок действия Лицензии, обнаруженные Заказчиком в пределах гарантийного срока, и безвозмездно их устраняет по письменному заявлению Заказчика в течение 3-х (трех) рабочих дней с момента составления соответствующего акта. Заказчику должны быть предоставлены права конечного пользователя программного обеспечения на условиях простой (неисключительной) лицензии определенными договором способами в течение 12 месяцев с момента подписания акта приемки-передачи. К разрешенным способам использования программного обеспечения относятся: воспроизведение; хранение ее в памяти ЭВМ (одной ЭВМ или одного пользователя сети); активация; запуск в работу; обновление и актуализация.
9.	Гарантийные обязательства	- Исполнитель гарантирует, что передаваемое ПО обеспечит выполнение функций при условиях, описанных в документации, а также то, что носитель ПО лишен дефектов. Тара и внутренняя упаковка должны обеспечивать сохранность и предохранять ПО от повреждений при транспортировке всеми видами транспорта с учетом погрузочно-разгрузочных работ. Гарантия Исполнителя действует в течение 12 месяцев с момента поставки ПО. Гарантии по качеству работы ПО определяются в соответствии с условиями лицензионного соглашения, прилагаемого к ПО и не могут превышать объема, предусмотренного условиями лицензионного соглашения.
10.	Территорией правомерного использования ПО	Территория Российской Федерации.
11.	Страна происхождения ПО	
11.	Требования к безопасности	Требований, наличия ГОСТ – не предусмотрено.

Исполнитель:
Наименование

_____

_____ /_____/
М.П.

Заказчик:
ГАУ ЯО «Информационное агентство «Верхняя Волга»

_____

_____ /_____/
М.П.