**УТВЕРЖДАЮ**

Председатель Конкурсной комиссии

АО «Дальгипротранс»

 «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2020 г.

**ВНИМАНИЕ!**

**Изменения в аукционную документацию открытого аукциона в электронной форме №33/ОАЭ-ДГТ/20 на право заключения договора на передачу неисключительных прав антивирусной программы Kaspersky**

1. **Внести изменения в третий абзац п.п. 1.7. аукционной документации и**

**изложить в следующей редакции:**

Дата окончания срока подачи аукционных заявок 10 часов 00 минут местного времени (03 часа 00 минут московского времени) «11» января 2021 года*.*

1. **Внести изменения в п.п. 1.8. аукционной документации и изложить в**

**следующей редакции:**

Рассмотрение аукционных заявок осуществляется «13» января 2021 года в 11 часов 00 минут местного времени (04 часа 00 минут московского времени) по адресу: г. Хабаровск, ул. Шеронова д. 56, 3 этаж, кабинет № 307*.*

Проведение открытого аукциона осуществляется в 15 часов 00 минут местного времени (08 часов 00 минут московского времени) «15» января 2021 года на электронной площадке ЗАО «Сбербанк-АСТ» (на странице данного открытого аукциона на сайте utp.sberbank-ast.ru), в электронной форме в личном кабинете Участника электронных процедур.

1. Раздел **«Требования к программным средствам антивирусной защиты для файловых серверов Windows»** п.п. 3.1.1. аукционной документации и изложить в следующей редакции:

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

• Microsoft Windows Small Business Server 2008 Standard/Premium x32/x64

• Microsoft Windows Small Business Server 2011 Essentials / Standard х64

• Microsoft Windows MultiPoint Server 2011 x64 edition

• Microsoft Windows Server 2003 Standard/Enterprise SP2 x32/x64

• Microsoft Windows Server 2003 R2 Standard/Enterprise Edition SP2 R2 x32/x64

• Microsoft Windows Server 2008 Standard/Enterprise SP1 x32/x64

• Microsoft Windows Server 2008 R2 x64 Standard/Enterprise

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

• Microsoft Windows Server 2008 Foundation

• Microsoft Windows Server 2008 R2 Foundation

• Microsoft Windows Server 2012 Foundation х64

• Microsoft Windows Server 2012 Standard/Essentials х64

• Microsoft Windows Server 2012 R2 Standard/Essentials х64 Edition

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

• Резидентный антивирусный мониторинг.

• Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы.

• Антивирусное сканирование по команде пользователя или администратора и по расписанию.

• Запуск задач по расписанию и/или сразу после загрузки операционной системы.

• Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу.

• Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых правил для конкретных программ

• Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные.

• Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

• Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем.

• Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.

• Настройки проверки критических областей сервера в качестве отдельной задачи.

• Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме.

• Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий).

• Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.

• Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Раздел **«Требования к программным средствам централизованного управления, мониторинга и обновления»** п.п. 3.1.1. аукционной документации и изложить в следующей редакции:

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

• Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64

• Microsoft Windows 8 Professional / Enterprise x86 / x64

• Microsoft Windows 8.1 Professional / Enterprise x86 / x64

• Microsoft Windows 10 Professional / Enterprise x86 / x64

• Microsoft Windows Server 2003 x86 / x64 SP2

• Microsoft Windows Server 2008 x86 / x64

• Microsoft Windows Server 2008 R2

• Microsoft Windows Server 2012

• Microsoft Windows Server 2012 R2

• Microsoft Windows Small Business Server 2003 SP2

• Microsoft Windows Small Business Server 2008

• Microsoft Windows Small Business Server 2011

Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:

• Microsoft SQL Express 2005/2008/2008R2/2012/2014

• Microsoft SQL Server 2005/2008/2008R2/2012/2014

• MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91

• MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90

Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий:

• VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5)

• Microsoft Hyper-V: 2008, 2008 R2, 2012, 20012 R2

• KVM интегрированный с: RHEL 5.4, 5.x и выше, SLES 11 SPx, Ubuntu 10.10 LTS

• Microsoft VirtualPC 6.0.156.0

• Parallels Desktop 7 и выше

• CitrixXenServer 5.6.1 FP1ивыше

• Oracle VM VirtualBox 4.0.4-70112

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

• Установка системы управления антивирусной защиты из единого дистрибутива.

• Выбор установки в зависимости от количества защищаемых узлов.

• Возможность чтения информации из AD, с целью получения данных об учетных записях компьютеров в организации

• Возможность поиска и обнаружения компьютеров в сети по IP-адресу, имени хоста, имени домена, маске подсети.

• Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу операционной системы, нахождению в OUAD

• Централизованные установка, обновление и удаление программных средств антивирусной защиты. Настройка, администрирование, просмотр отчетов и статистической информации по их работе.

• Централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления.

• Наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, агент администрирования, для локальной установки – возможность создать автономный пакет установки.

• Удаленная установка программных средств антивирусной защиты с последней версией антивирусных баз.

• Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему, а также от того, в каком OU находится компьютер. Должна быть реализована возможность поддержки иерархии таких триггеров.

Согласовано: