1. **ПРОЕКТ КОНТРАКТА**

Муниципальный контракт № \_\_\_\_\_\_

на Оказание услуг по продлению лицензий на подсистему централизованной антивирусной обработки

(идентификационный код закупки 213862201554386220100100050026311244)

г. Югорск «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2021г.

Муниципальное казенное учреждение «Центр материально-технического и информационно-методического обеспечения», именуемое в дальнейшем «Заказчик», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуем\_\_ в дальнейшем «Исполнитель», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, вместе именуемые «Стороны», в соответствии с законодательством Российской Федерации и иными нормативными правовыми актами о контрактной системе в сфере закупок, и на основании решения Единой комиссии по осуществлению закупок для обеспечения муниципальных нужд города Югорска (протокол\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_ № \_\_\_\_\_) заключили настоящий муниципальный контракт, именуемый в дальнейшем «Контракт», о нижеследующем:

1. Предмет контракта

1.1. Исполнитель обязуется своевременно оказать на условиях Контракта услуги по продлению лицензий на подсистему централизованной антивирусной обработки, а Заказчик обязуется принять и оплатить их.

1.2. Состав и объем услуг определяется в техническом задании (приложение) к Контракту.

1.3. Место оказания услуг: г. Югорск Ханты-Мансийского автономного округа-Югры, на территории исполнителя.

2. Цена контракта и порядок расчетов

2.1. Цена Контракта является твердой, не может изменяться в ходе заключения и исполнения Контракта, за исключением случаев, установленных Контрактом и (или) предусмотренных законодательством Российской Федерации.

Источник финансирования: бюджет города Югорска на 2021 год.

2.2. Общая цена Контракта составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_ копеек, включая налог на добавленную стоимость (\_\_ %): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_ копеек/ *НДС не облагается в соответствии с п. \_\_\_ ст. \_\_\_\_ Налогового кодекса Российской Федерации.\*. (В случае если Исполнитель не является плательщиком НДС, Заказчик указывает: «НДС не облагается»).*

Сумма, подлежащая уплате Исполнителю, уменьшается, на размер налогов, сборов и иных обязательных платежей в бюджеты бюджетной системы Российской Федерации, связанных с оплатой контракта, если в соответствии с законодательством Российской Федерации о налогах и сборах такие налоги, сборы и иные обязательные платежи подлежат уплате в бюджеты бюджетной системы Российской Федерации заказчиком.

*Стоимость единицы услуги указана в Техническом задании (Приложение № 1).*

2.3. В общую цену Контракта включены все расходы Исполнителя: стоимость услуг, расходы на эксплуатацию медицинского оборудования, заработная плата, НДС (если предусмотрен), налоги, сборы и иные обязательные платежи Исполнителя, связанные с исполнением настоящего контракта.

2.4. Расчеты по Контракту производится в следующем порядке:

2.4.1. Оплата производится в безналичном порядке путем перечисления Заказчиком денежных средств на указанный в Контракте расчетный счет Исполнителя.

2.4.2. Оплата производится в рублях Российской Федерации.

2.4.3. Авансовые платежи по Контракту не предусмотрены.

2.4.4. Расчет за оказанные услуги осуществляется в течение 15 рабочих дней со дня подписания Заказчиком Акта об оказанных услугах или универсального передаточного документа предусмотренного Контрактом.

2.5. В случае уменьшения Заказчику соответствующим финансовым органом в установленном порядке ранее доведенных лимитов бюджетных обязательств, приводящего к невозможности исполнения Заказчиком обязательств по Контракту, о чем Заказчик уведомляет Исполнителя, Стороны согласовывают в соответствии с законодательством Российской Федерации новые условия, в том числе по цене и (или) количеству товаров.

3. Права и обязанности сторон

3.1. Заказчик имеет право:

3.1.1. Досрочно принять и оплатить услуги в соответствии с условиями Контракта.

3.1.2. По согласованию с Исполнителем изменить объем услуг в соответствии с пунктом 12.6 Контракта.

3.1.3. Требовать возмещения неустойки и (или) убытков, причиненных по вине Исполнителя.

3.1.4. Привлекать экспертов, экспертные организации для проверки соответствия качества оказываемых услуг требованиям, установленным Контрактом.

3.1.5. Осуществлять иные права, предусмотренные Контрактом и (или) законодательством Российской Федерации.

3.2. Заказчик обязан:

3.2.1. Обеспечить приемку оказанных по Контракту услуг по объему и качеству.

3.2.2. Оплатить услуги в порядке, предусмотренном Контрактом.

3.2.3. Своевременно предоставить Исполнителю информацию, необходимую для исполнения Контракта.

3.2.4. Выполнять иные обязанности, предусмотренные Контрактом.

3.3. Исполнитель обязан:

3.3.1. Оказать услуги в сроки, предусмотренные Контрактом.

3.3.2. Соблюдать действующие у Заказчика правила внутреннего трудового распорядка, правила техники безопасности и пожарной безопасности, а также пропускной режим.

3.3.3. Не предоставлять другим лицам или разглашать иным способом конфиденциальную информацию, полученную в результате исполнения обязательств по Контракту.

3.3.4. По требованию Заказчика своими средствами и за свой счет в срок, согласованный с Заказчиком устранить допущенные по своей вине в оказанных услугах недостатки или иные отступления от условий Контракта.

3.3.5. Предоставлять своевременно достоверную информацию о ходе исполнения своих обязательств, в том числе о сложностях, возникающих при исполнении Контракта.

3.3.6. Выполнять иные обязанности, предусмотренные Контрактом.

3.4. Исполнитель вправе:

3.4.1. Требовать приемки и оплаты услуг в объеме, порядке, сроки и на условиях, предусмотренных Контрактом.

3.4.2. По согласованию с Заказчиком досрочно оказать услуги. Заказчик вправе досрочно принять и оплатить услуги в соответствии с условиями Контракта.

4. Сроки оказания услуг

4.1. Услуги должны быть оказаны с даты подписания муниципального контракта по 25 июля 2021 года.

4.2. Досрочная сдача результатов услуг допускается только по согласованию с Заказчиком. В случае согласования досрочного оказания услуг Заказчик обязуется принять услуги и подписать документ о приемке в порядке, установленном Контрактом.

4.3. В случае, если в п. 11.1 Контракта указана дата, при наступлении которой обязательства сторон прекращаются, за исключением обязательств по оплате услуг, гарантийных обязательств, обязательств по возмещению убытков и выплате неустойки (штрафа, пени), Стороны после наступления указанной даты не вправе требовать исполнения Контракта в части оказания услуг и их приемки. При наступлении указанной даты (в случае, если она установлена) Заказчиком в двух экземплярах составляется Акт взаимосверки обязательств по Контракту, в котором указываются сведения о прекращении действия Контракта; сведения о фактически исполненных обязательствах по Контракту; сумма, подлежащая оплате в соответствии с условиями Контракта.

Исполнитель обязан подписать Акт взаимосверки обязательств. В случае уклонения Исполнителя от подписания данного акта Заказчик проставляет в нем соответствующую отметку. Акт взаимосверки обязательств является основанием для проведения взаиморасчетов между Сторонами.

4.4. В случае, установленном в п. 4.3. Контракта акт взаимосверки признаётся документом подтверждающим приёмку, в части фактически исполненных обязательствах по Контракту, в связи, с чем взаиморасчеты между Сторонами осуществляются в срок, установленный в п. 2.4.4. Контракта.

5. Порядок сдачи и приемки услуг

5.1. Приемка услуг на соответствие их объема и качества требованиям, установленным в Контракте производится за отчетный месяц.

5.2. Исполнитель после оказания услуг, в срок не более 5 дней, направляет в адрес Заказчика извещение (уведомление) о готовности услуг к сдаче и документ о приемке.

5.3. Заказчик вправе создать приемочную комиссию, состоящую из не менее пяти человек, для проверки соответствия качества услуг требованиям, установленным Контрактом. Проверка соответствия качества оказываемых услуг требованиям, установленным Контрактом, может также осуществляться с привлечением экспертов, экспертных организаций.

5.4. Стороны подписывают документ о приемке в течении 5 дней с момента получения.

5.5. В случае обнаружения недостатков в объеме и качестве оказанных услуг Заказчик направляет Исполнителю уведомление в порядке, предусмотренном п. 5.7 Контракта.

5.6. В случае если Исполнитель не согласен с предъявляемой Заказчиком претензией о некачественной услуге, Исполнитель обязан самостоятельно подтвердить качество услуг заключением эксперта, экспертной организации и оригинал экспертного заключения представить Заказчику. Выбор эксперта, экспертной организации осуществляется Исполнителем и согласовывается с Заказчиком. Оплата услуг эксперта, экспертной организации, а также всех расходов для экспертизы осуществляется Исполнителем.

5.7. Обо всех нарушениях условий Контракта об объеме и качестве услуг Заказчик извещает Исполнителя не позднее трех рабочих дней с даты обнаружения указанных нарушений. Уведомление о невыполнении или ненадлежащем выполнении Исполнителем обязательств по Контракту составляется Заказчиком в письменной форме и направляется Исполнителю по почте, факсу, электронной почте либо нарочным. Адресом электронной почты для получения уведомления является: \_\_\_\_\_\_\_\_\_. Номером факса для получения уведомления является: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

5.8. Исполнитель в установленный в уведомлении (п. 5.7) срок обязан устранить все допущенные нарушения. Если Исполнитель в установленный срок не устранит нарушения, Заказчик вправе предъявить Исполнителю требование о возмещении своих расходов на устранение недостатков услуг и (или) направить Исполнителю требование о расторжении Контракта по соглашению сторон, в случае, если устранение нарушений потребует больших временных затрат, в связи с чем Заказчик утрачивает интерес к Контракту.

5.9. Приемка услуг в целом (или отдельными этапами, в случае, когда согласно Графику предусматриваются поэтапные услуги, оформляется документом о приемке\* (Акта оказанных услуг), который составляется в двух экземплярах и подписывается Заказчиком (в случае создания приемочной комиссии подписывается всеми членами приемочной комиссии и утверждается Заказчиком) и Исполнителем. В случае, когда оказание услуг осуществляется в интересах Исполнителя, документ о приёмке составляется в трех экземплярах и подписывается Исполнителем, Заказчиком (в случае создания приемочной комиссии подписывается всеми членами приемочной комиссии и утверждается Заказчиком) и Исполнителем.

\*Заказчик вправе дополнительно расшифровать, какие документы будут подтверждать приёмку услуг, сделав на них ссылку в п. 5.9. Контракта.

5.10. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом приемка услуг оформляется документом о приемке, в котором указываются: сведения о фактически исполненных обязательствах по Контракту, сумма, подлежащая оплате в соответствии с условиями настоящего Контракта; размер неустойки (штрафа, пени) и (или) убытков, подлежащей взысканию; основания применения и порядок расчета неустойки (штрафа, пени) и (или) убытков; итоговая сумма, подлежащая оплате Исполнителю по контракту. Документ составляется в двух экземплярах, подписывается Заказчиком (в случае создания приемочной комиссии подписывается всеми членами приемочной комиссии и утверждается Заказчиком) и Исполнителем. В случае, когда оказание услуг осуществляется в интересах Исполнителя, документ о приёмке составляется в трех экземплярах и подписывается Исполнителем, Заказчиком (в случае создания приемочной комиссии подписывается всеми членами приемочной комиссии и утверждается Заказчиком) и Исполнителем.

5.11.\*\* В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, Заказчик производит удержание неустойки (штрафа, пеней) и (или) возмещения убытков причинённых Исполнителем убытков. Удержание неустойки (штрафа, пеней) и (или) убытков производится Заказчиком на основании документа составленного в соответствии с пунктом 5.10. Контракта, не позднее сроков установленных в пункте 2.4.4. Контракта. При этом исполнение обязательства Исполнителем по перечислению неустойки (штрафа, пени) и (или) убытков в доход бюджета возлагается на Заказчика.

\*\*[Письмо](consultantplus://offline/ref=FA92852B7150A77149948E9A235EEFFC4F77CBB515EEECA9631C39A6B2A03637684A1B3D39C3466Ab9m6N) ФАС России от 10.12.2015 №АЦ/70978/15, Письма Минэкономразвития России от 10.03.2016 [№ОГ-Д28-3630](consultantplus://offline/ref=FA92852B7150A77149949388355EEFFC4F7BC2B113EFECA9631C39A6B2A03637684A1B3D39C3466Bb9m2N), от 02.10.2015 [№ОГ-Д28-12800](consultantplus://offline/ref=FA92852B7150A77149949388355EEFFC467DCDB311EDB1A36B4535A4B5AF69206F03173C39C346b6mDN), от 21.09.2015 [№Д28и-2829](consultantplus://offline/ref=FA92852B7150A77149949388355EEFFC497AC2B113EDB1A36B4535A4B5AF69206F03173C39C347b6mDN).

6. Обеспечение исполнения контракта

6.1. Способами обеспечения исполнения Контракта являются банковская гарантия, выданная банком и соответствующая требованиям п. 6.6 Контракта, или внесение денежных средств на указанный Заказчиком счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими Заказчику. Способ обеспечения исполнения контракта определяется Исполнителем самостоятельно.

6.2. Обеспечение исполнения Контракта предоставляется Заказчику до заключения Контракта. Размер обеспечения исполнения Контракта составляет \_\_\_\_\_\_\_ рублей \_\_\_\_ копеек (5 процентов от цены, по которой в соответствии с Законом о контрактной системе заключается контракт).

В случае если предложенная в заявке участника закупки цена снижена на двадцать пять и более процентов по отношению к начальной (максимальной цене контракта, участник закупки, с которым заключается контракт, предоставляет обеспечение исполнения контракта с учетом положений статьи 37 Федерального закона № 44- ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

6.3. В ходе исполнения Контракта Исполнитель вправе предоставить Заказчику обеспечение исполнения Контракта, уменьшенное на размер выполненных обязательств, предусмотренных Контрактом, взамен ранее предоставленного обеспечения исполнения Контракта. При этом может быть изменен способ обеспечения исполнения Контракта.

6.4. Срок действия обеспечения исполнения Контракта в форме банковской гарантии должен превышать срок действия контракта не менее чем на один месяц.

Срок действия указанного обеспечения может быть прекращен до наступления указанного срока в случае досрочного исполнения Исполнителем всех своих обязательств по Контракту.

6.5. По Контракту должны быть обеспечены обязательства Исполнителя в том числе, по возмещению убытков Заказчика, причиненных неисполнением или ненадлежащим исполнением, просрочкой исполнения обязательств по Контракту, а также обязанность по выплате неустойки (штрафа, пени), возврату аванса и иных долгов, возникших у Исполнителя перед Заказчиком.

6.6. Требования к обеспечению исполнения Контракта, предоставляемому в виде банковской гарантии:

Банковская гарантия оформляется в письменной форме на бумажном носителе или на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью лица, имеющего право действовать от имени банка, на условиях, определенных гражданским законодательством и статьей 45 Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд", с учетом требований установленных постановлением Правительства Российской Федерации от 8 ноября 2013 г. №1005 (с учетом изменений и дополнений).

6.7. Денежные средства возвращаются в полном объёме (либо в части, оставшейся после удовлетворения требований Заказчика, возникших в период действия обеспечения) в срок не превышающий пятнадцать дней с момента подписания Сторонами документов, подтверждающих надлежащее исполнение обязательств по Контракту в полном объеме.

\* Обеспечение исполнения контракта не применяется в случаях, установленных Федеральным законом от 05.04.2013 г. № 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

6.8. Предусмотренное [частями 7](https://login.consultant.ru/link/?rnd=35D11FC4BBD9CC225822D2561C3F808A&req=doc&base=LAW&n=315347&dst=1109&fld=134&date=19.06.2019) статьи 96 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» уменьшение размера обеспечения исполнения контракта осуществляется при условии отсутствия неисполненных Исполнителем требований об уплате неустоек (штрафов, пеней), предъявленных заказчиком в соответствии с Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», а также приемки заказчиком поставленного товара, результатов отдельного этапа исполнения контракта в объеме выплаченного аванса (если контрактом предусмотрена выплата аванса).

6.9. Участник закупки, с которым заключается контракт по результатам определения поставщика (подрядчика, исполнителя) в соответствии с пунктом 1 части 1 статьи 30 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», освобождается от предоставления обеспечения исполнения контракта, в том числе с учетом положений статьи 37 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», об обеспечении гарантийных обязательств в случае предоставления таким участником закупки информации, содержащейся в реестре контрактов, заключенных заказчиками, и подтверждающей исполнение таким участником (без учета правопреемства) в течение трех лет до даты подачи заявки на участие в закупке трех контрактов, исполненных без применения к такому участнику неустоек (штрафов, пеней). Такая информация представляется участником закупки до заключения контракта в случаях, установленных настоящим Федеральным законом для предоставления обеспечения исполнения контракта. При этом сумма цен таких контрактов должна составлять не менее начальной (максимальной) цены контракта, указанной в извещении об осуществлении закупки и документации о закупке.\*(Условие включается в Контракт в случае, если контракт заключается с субъектом малого предпринимательства или социально ориентированной некоммерческой организацией).

6.10. Положения Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» об обеспечении исполнения контракта, включая положения о предоставлении такого обеспечения с учетом положений статьи 37 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», об обеспечении гарантийных обязательств не применяются в случаях установленных Федеральным законом от 05.04.2013. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

7. Ответственность сторон\*

***\*если законодательством Российской Федерации установлен иной порядок начисления штрафа, чем порядок, предусмотренный Правилами, размер такого штрафа и порядок его начисления устанавливается контрактом в соответствии с законодательством Российской Федерации.***

7.1. Стороны несут ответственность за неисполнение и ненадлежащее исполнение Контракта, в том числе за неполное и (или) несвоевременное исполнение своих обязательств по Контракту, в соответствии с положениями Гражданского кодекса Российской Федерации, Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в порядке установленном постановлением Правительства Российской Федерации от 30.08.2017 № 1042 (с учетом изменений и дополнений), за исключением случаев, если законодательством Российской Федерации установлен иной порядок начисления штрафов.

7.2. Размер штрафа устанавливается контрактом в порядке, установленном [пунктами 7.3](http://adm.ugorsk.ru/upload/iblock/f22/f22ffdc95a8036e88a86d827369b8321.doc#P57) – 7.[8](http://adm.ugorsk.ru/upload/iblock/f22/f22ffdc95a8036e88a86d827369b8321.doc#P82), в том числе рассчитываемой как процент цены Контракта, или в случае, если Контрактом предусмотрены этапы исполнения Контракта, как процент этапа исполнения Контракта (далее - цена контракта (этапа)).

7.3. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, размер штрафа устанавливается следующем порядке (за исключением случаев, предусмотренных [пунктами 7.4](http://adm.ugorsk.ru/upload/iblock/f22/f22ffdc95a8036e88a86d827369b8321.doc#P67) – 7.[7](http://adm.ugorsk.ru/upload/iblock/f22/f22ffdc95a8036e88a86d827369b8321.doc#P81)):

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

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

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

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

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

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

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

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

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

7.4. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, заключенным по результатам определения Исполнителя в соответствии с [пунктом 1 части 1 статьи 30](consultantplus://offline/ref=D24FEE69E1B7CD8A16BB8E7671CAA689283A9F94587855EC14DDB06FAEC3FCB85E295C0AE157E7F5VF7DG) Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, размер штрафа устанавливается в размере 1 процента цены контракта (этапа), но не более 5 тыс. рублей и не менее 1 тыс. рублей.

7.5. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, заключенным с победителем закупки (или с иным участником закупки в случаях, установленных Федеральным [законом](consultantplus://offline/ref=D24FEE69E1B7CD8A16BB8E7671CAA689283A9F94587855EC14DDB06FAEVC73G)), предложившим наиболее высокую цену за право заключения Контракта, размер штрафа рассчитывается в порядке, установленном Правилами, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, и устанавливается в следующем порядке:

а) в случае, если цена контракта не превышает начальную (максимальную) цену контракта:

10 процентов начальной (максимальной) цены контракта, если цена контракта не превышает 3 млн. рублей;

5 процентов начальной (максимальной) цены контракта, если цена контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

1 процент начальной (максимальной) цены контракта, если цена контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно);

б) в случае, если цена контракта превышает начальную (максимальную) цену контракта:

10 процентов цены контракта, если цена контракта не превышает 3 млн. рублей;

5 процентов цены контракта, если цена контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

1 процент цены контракта, если цена контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно).

7.6. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательства, предусмотренного Контрактом, которое не имеет стоимостного выражения, размер штрафа устанавливается (при наличии в Контракте таких обязательств) в следующем порядке:

а) 1000 рублей, если цена Контракта не превышает 3 млн. рублей;

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

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

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

7.7. В случае если в соответствии с [частью 6 статьи 30](consultantplus://offline/ref=D24FEE69E1B7CD8A16BB8E7671CAA689283A9F94587855EC14DDB06FAEC3FCB85E295C0AE157E7F7VF75G) Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» Контрактом предусмотрено условие о гражданско-правовой ответственности Исполнителей за неисполнение условия о привлечении к исполнению Контракта, соисполнителей из числа субъектов малого предпринимательства, социально ориентированных некоммерческих организаций в виде штрафа, штраф устанавливается в размере 5 процентов объема такого привлечения, установленного контрактом.

7.8. За каждый факт неисполнения Заказчиком обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств, предусмотренных Контрактом, размер штрафа устанавливается в следующем порядке:

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

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

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

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

7.9. Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного контрактом, начиная со дня, следующего после дня истечения установленного контрактом срока исполнения обязательства, и устанавливается контрактом в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены контракта, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных контрактом и фактически исполненных Исполнителем, за исключением случаев, если законодательством Российской Федерации установлен иной порядок начисления пени.

7.10. В случае просрочки исполнения Заказчиком обязательств, предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Заказчиком обязательств, предусмотренных Контрактом, Исполнитель вправе потребовать уплаты неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Контрактом, начиная со дня, следующего после дня истечения установленного Контрактом срока исполнения обязательства.

7.11. Пеня устанавливается Контрактом в размере одной трехсотой действующей на дату уплаты пеней ключевой ставки Центрального банка Российской Федерации от не уплаченной в срок суммы (пункт 5 статьи 34 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»).

7.12. Общая сумма начисленных штрафов за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных контрактом, не может превышать цену контракта.

Общая сумма начисленных штрафов за ненадлежащее исполнение заказчиком обязательств, предусмотренных контрактом, не может превышать цену контракта.

8. Форс-мажорные обстоятельства

8.1. Стороны освобождаются от ответственности за частичное или полное невыполнение обязательств по Контракту, если оно явилось следствием обстоятельств непреодолимой силы (форс-мажор), а именно: пожара, наводнения, землетрясения, войны, военных действий, блокады, эмбарго, общих забастовок, запрещающих (либо ограничивающих) актов властей, и если эти обстоятельства непосредственно повлияли на исполнение Контракта.

8.2. Сторона, для которой создалась невозможность выполнения обязательств по Контракту, обязана немедленно (в течение 3 (трех) дней) известить другую сторону о наступлении и прекращении вышеуказанных обстоятельств. Несвоевременное извещение об этих обстоятельствах лишает, соответствующую сторону права ссылается на них в будущем.

8.3. Обязанность доказать наличие обстоятельств непреодолимой силы лежит на Стороне Контракта, не выполнившей свои обязательства по Контракту.

Доказательством наличия вышеуказанных обстоятельств и их продолжительности будут служить документы Торгово-промышленной палаты Ханты-Мансийского автономного округа-Югры, или иной торгово-промышленной палаты, где имели место обстоятельства непреодолимой силы.

8.4. Если обстоятельства и их последствия будут длиться более 1 (одного) месяца, то стороны расторгают Контракт. В этом случае ни одна из сторон не имеет права потребовать от другой стороны возмещения убытков.

9. Порядок разрешения споров

9.1. Заказчик и Исполнитель должны приложить все усилия, чтобы путем прямых переговоров разрешить к обоюдному удовлетворению сторон все противоречия или спорные вопросы, возникающие между ними в рамках Контракта.

9.2. При недостижении взаимоприемлемого решения, Стороны вправе передать спорный вопрос на разрешение в Арбитражный суд Ханты-Мансийского автономного округа – Югры.

10. Расторжение Контракта

10.1. Расторжение Контракта допускается по соглашению Сторон, по решению суда, а также в случае одностороннего отказа Стороны Контракта от исполнения Контракта в соответствии с гражданским законодательством.

10.2. Расторжение Контракта по соглашению Сторон совершается в письменной форме и возможно в случае наступления условий, при которых для одной из Сторон или обеих Сторон дальнейшее исполнение обязательств по Контракту не возможно либо возникает нецелесообразность исполнения Контракта.

10.3. В случае расторжения Контракта по соглашению Исполнитель возвращает Заказчику все денежные средства, перечисленные для исполнения обязательств по Контракту, а Заказчик оплачивает расходы (издержки) Исполнителя за фактически исполненные обязательства по Контракту.

10.4. Требование о расторжении Контракта может быть заявлено Стороной в суд только после получения отказа другой Стороны на предложение расторгнуть Контракт либо неполучения ответа в течение 10 (десяти) дней с даты получения предложения о расторжении Контракта.

10.5. Заказчик вправе принять решение об одностороннем отказе от исполнения Контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств. До принятия такого решения Заказчик вправе провести экспертизу оказанных услуг с привлечением экспертов, экспертных организаций.

10.6. Если Заказчиком проведена экспертиза оказанных услуг с привлечением экспертов, экспертных организаций, решение об одностороннем отказе от исполнения Контракта может быть принято Заказчиком только при условии, что по результатам экспертизы оказанных услуг в заключении эксперта, экспертной организации будут подтверждены нарушения условий Контракта, послужившие основанием для одностороннего отказа Заказчика от исполнения Контракта.

10.7. Решение Заказчика об одностороннем отказе от исполнения Контракта не позднее чем в течение трех рабочих дней с даты принятия указанного решения, размещается в единой информационной системе и направляется Исполнителю по почте заказным письмом с уведомлением о вручении по адресу Исполнителя, указанному в разделе 13 Контракта, а также телеграммой, либо посредством факсимильной связи, либо по адресу электронной почты, либо с использованием иных средств связи и доставки, обеспечивающих фиксирование такого уведомления и получение Заказчиком подтверждения о его вручении Исполнителю. Выполнение Заказчиком вышеуказанных требований считается надлежащим уведомлением Исполнителя об одностороннем отказе от исполнения Контракта. Датой такого надлежащего уведомления признается дата получения Заказчиком подтверждения о вручении Исполнителю указанного уведомления либо дата получения Заказчиком информации об отсутствии Исполнителя по его адресу, указанному в разделе 13 Контракта. При невозможности получения указанных подтверждения либо информации датой такого надлежащего уведомления признается дата по истечении тридцати дней с даты размещения решения Заказчика об одностороннем отказе от исполнения Контракта в единой информационной системе.

10.8. Решение Заказчика об одностороннем отказе от исполнения Контракта вступает в силу и Контракт считается расторгнутым через десять дней с даты надлежащего уведомления Заказчиком Исполнителя об одностороннем отказе от исполнения Контракта.

10.9. Заказчик обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения Контракта, если в течение десятидневного срока с даты надлежащего уведомления Исполнителя о принятом решении об одностороннем отказе от исполнения Контракта устранено нарушение условий Контракта, послужившее основанием для принятия указанного решения, а также Заказчику компенсированы затраты на проведение экспертизы, предусмотренной п. 10.5 Контракта. Данное правило не применяется в случае повторного нарушения Исполнителем условий Контракта, которые в соответствии с гражданским законодательством являются основанием для одностороннего отказа Заказчика от исполнения Контракта.

10.10. Заказчик принимает решение об одностороннем отказе от исполнения Контракта, если в ходе исполнения Контракта будет установлено, что Исполнитель не соответствует установленным извещением об осуществлении закупки и (или) документацией о закупке требованиям к участникам закупки или предоставил недостоверную информацию о своем соответствии таким требованиям, что позволило ему стать победителем определения исполнителя.

10.11. Исполнитель вправе принять решение об одностороннем отказе от исполнения Контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств. Такое решение не позднее чем в течение трех рабочих дней, следующих за датой его принятия, направляется Заказчику по почте заказным письмом с уведомлением о вручении по адресу Заказчика, указанному в разделе 13 Контракта, а также телеграммой, либо посредством факсимильной связи, либо по адресу электронной почты, либо с использованием иных средств связи и доставки, обеспечивающих фиксирование такого уведомления и получение Исполнителем подтверждения о его вручении Заказчику. Выполнение Исполнителем вышеуказанных требований считается надлежащим уведомлением Заказчика об одностороннем отказе от исполнения Контракта. Датой такого надлежащего уведомления признается дата получения Исполнителем подтверждения о вручении Заказчику указанного уведомления.

10.12. Решение Исполнителя об одностороннем отказе от исполнения Контракта вступает в силу и Контракт считается расторгнутым через десять дней с даты надлежащего уведомления Исполнителем Заказчика об одностороннем отказе от исполнения Контракта.

10.13. Исполнитель обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения Контракта, если в течение десятидневного срока с даты надлежащего уведомления Заказчика о принятом решении об одностороннем отказе от исполнения Контракта устранены нарушения условий Контракта, послужившие основанием для принятия указанного решения.

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

11.Срок действия Контракта

11.1. Контракт вступает с даты подписания контракта по 25 июля 2021 (включительно). С 26 июля 2021 года обязательства Сторон по Контракту прекращаются, за исключением обязательств по оплате услуг, гарантийных обязательств, обязательств по возмещению убытков и выплате неустойки.

12. Прочие условия

12.1. Контракт составлен в форме электронного документа. После заключения Контракта Стороны вправе изготовить копию Контракта на бумажном носителе в 2 (двух) экземплярах, имеющих одинаковую юридическую силу, по одному для Заказчика и Исполнителя.

12.2.Все приложения к Контракту являются его неотъемной частью.

12.3. К Контракту прилагаются:

- Техническое задание (приложение);

12.4. В случае изменения наименования, адреса места нахождения или банковских реквизитов Стороны, она письменно извещает об этом другую Сторону в течение 3 рабочих дней с даты такого изменения.

12.5. По согласованию Сторон в ходе исполнения Контракта допускается снижение цены Контракта без изменения предусмотренных Контрактом объема работы, качества выполняемой работы и иных условий Контракта.

12.6. Заказчик по согласованию с Исполнителем в ходе исполнения Контракта вправе изменить не более чем на десять процентов предусмотренный Контрактом объем услуг при изменении потребности в услугах, на оказание которых заключен контракт. При этом по соглашению Сторон допускается изменение с учетом положений бюджетного законодательства Российской Федерации цены Контракта пропорционально дополнительному объему услуг исходя из установленной в Контракте цены единицы услуги, но не более чем на десять процентов цены Контракта. При уменьшении предусмотренного Контрактом объема услуг Стороны контракта обязаны уменьшить цену Контракта исходя из цены единицы услуги.

12.7. При исполнении Контракта не допускается перемена Исполнителя, за исключением случаев, если новый Исполнитель является правопреемником Исполнителя по Контракту вследствие реорганизации юридического лица в форме преобразования, слияния или присоединения.

12.8. В случае перемены Заказчика по контракту права и обязанности Заказчика по такому контракту переходят к новому заказчику в том же объеме и на тех же условиях.

Взаиморасчеты между Сторонами, в случае, установленном в настоящем пункте, осуществляются в срок, не превышающий установленный в п. 2.4.4. Контракта.

13. Адреса места нахождения, банковские реквизиты и подписи Сторон

|  |  |
| --- | --- |
| Заказчик  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_ 202\_г.  М.П. | Исполнитель  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_ 202\_г.  М.П. |

Приложение

к Муниципальному контракту

№ \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_ 202\_\_ г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

**1. Предмет муниципального контракта:** оказание услуг по продлению лицензий на подсистему централизованной антивирусной обработки.

**2. Сроки передачи прав:** с момента заключения муниципального контракта по 25 июля 2021 г.

**3. Место передачи прав:** 628260, Ханты-Мансийский автономный округ Югра, г. Югорск, ул. Геологов, 9.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование услуг | Характеристика предоставляемых услуг | Ед. изм. | Кол-во | Цена за ед., руб. | Сумма, руб. |
| 1 | Продление лицензий на подсистему централизованной антивирусной обработки | Продление действующей лицензии на антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition на срок 1 год с учётом имеющейся у Заказчика лицензии (Лицензия Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 25-49 Node 1 Year Renewal License) | Место | 42 |  |  |

Общие требования:

Эквивалент не допускается, на основании пункта 1, ч.1, статьи 33, Федерального закона № 44-ФЗ от 05 апреля 2013 г. Передача права на эквивалентные программные продукты не допустима, так как иные программные средства не обеспечат совместимости с уже эксплуатируемым Заказчиком программным обеспечением и уже имеющимися правами на использование программного обеспечения, что повлечет дополнительные расходы Заказчика по интеграции программного обеспечения и обучению персонала.

Средства антивирусной защиты в рамках указанного количества лицензий могут быть распределены любым образом независимо от количества файловых серверов и рабочих станций

Средства антивирусной защиты должны состоять в едином реестре российских программ для электронных вычислительных машин и баз данных (https://reestr.minsvyaz.ru/reestr/)

Антивирусные средства должны включать:

» программные средства антивирусной защиты для рабочих станций Windows;

» программные средства антивирусной защиты для рабочих станций MacOS;

» программные средства антивирусной защиты для рабочих станций и серверов Linux;

» программные средства антивирусной защиты для файловых серверов Windows;

» программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);

» 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:

o Windows 7 Home / Professional / Enterprise (32 / 64-разрядная);

o Windows 8 Professional / Enterprise (32 / 64-разрядная);

o Windows 8.1 Professional / Enterprise (32 / 64-разрядная);

o 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, c 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;

• 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;

• управления МТР 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;

• назначение приоритета для правил доступа к устройствам с файловой системой;

• 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;

• управления параметрами Kaspersky Endpoint Security через доверенные программы удаленного администрирования;

• установки только выбранных компонентов программного средства антивирусной защиты;

• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

• запуска 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;

• проверки целостности антивирусной программы;

• добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;

• импорта и экспорта списков правил и исключений в XML-формат;

• наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

• наличие защищенного хранилища для отчетов о работе антивируса;

• включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;

• интеграции с Windows Defender Security Center;

• наличие поддержки Antimalware Scan Interface (AMSI);

• наличие поддержки Windows Subsystem for Linux (WSL);

• защитить паролем восстановление объектов из резервного хранилища;

• ограничения сетевого трафика в том случае, если подключение к интернету является лимитным.

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:

o Windows Small Business Server 2011 Essentials / Standard (64-разрядная);

o Windows MultiPoint Server 2011 (64-разрядная);

o Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);

o Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная);

o Windows Server 2012 Foundation / Essentials / Standard (64-разрядная);

o Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная);

o Windows Server 2016 (64-разрядная) (с ограничениями);

o 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;

• 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;

• защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;

• 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;

• проверки целостности антивирусной программы;

• 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;

• включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;

• интеграции с Windows Defender Security Center;

• наличие поддержки Antimalware Scan Interface (AMSI);

• наличие поддержки Windows Subsystem for Linux (WSL);

• защитить паролем восстановление объектов из резервного хранилища.

• импорта и экспорта списков правил и исключений в XML-формат;

• ограничения сетевого трафика в том случае, если подключение к интернету является лимитным.

Требования к программным средствам антивирусной защиты для рабочих станций Mac

Программные средства антивирусной защиты для рабочих станций Mac должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

o macOS 10.13, 10.14, 10.15 или 11.0;

В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:

• резидентный антивирусный мониторинг;

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

• автоматическое обновление антивирусных баз по расписанию;

• резервное копирование зараженных файлов перед их удалением, для возможности восстановления;

• эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;

• 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;

• блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;

• проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);

• контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем

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

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

Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 32-битных операционных систем следующих версий:

o Ubuntu 16.04 LTS и выше;

o Red Hat® Enterprise Linux® 6.7 и выше;

o CentOS 6.7 и выше;

o Debian GNU / Linux 10;

o Linux Mint 19 и выше;

o Альт Линукс 9 Рабочая станция;

o Гослинукс 6.6;

o Mageia 4.

Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:

o Ubuntu 18.04 LTS и выше;

o Red Hat Enterprise Linux 8.0 и выше;

o CentOS 8.0 и выше;

o Debian GNU / Linux 10.1 и выше;

o OracleLinux 8 и выше;

o SUSE® Linux Enterprise Server 15 и выше;

o Альт Линукс 9 Образование;

o Amazon Linux AMI;

o Linux Mint 19 и выше;

o Astra Linux Special Edition 1.6 (обычный режим и режим замкнутой программной среды);

o Astra Linux Common Edition «Орел» 2.12;

o ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;

o Гослинукс 7.2;

o AlterOS 7.5 и выше;

o Pardus OS 19.1.

Полный список программных требований доступен в онлайн-справке - https://support.kaspersky.com/KES4Linux/11.1.0/ru-RU/196583.htm.

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;

• возможность проверки памяти ядра;

• 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;

• включения опции блокирования файлов во время проверки;

• помещение подозрительных и поврежденных объектов на карантин;

• 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;

• 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;

• управления через пользовательский графический интерфейс без root прав;

• централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;

• управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;

• проверки съемных дисков;

• отслеживания во входящем сетевом трафике активности, характерной для сетевых атак

• проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым

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

o Windows Server® 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

o Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;

o Windows Server 2008 Core / Standard / Enterprise

o …

64-разрядных операционных систем Microsoft Windows

o Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

o Windows Server 2008 Core Standard / Enterprise /

o Windows Hyper-V Server 2012;

o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;

o Windows Storage Server 2012 R2;

o Windows Server 2016 Essentials / Standard / Datacenter;

o Windows Hyper-V Server 2016;

o Windows Server 2019 Essentials / Standard / Datacenter;

o Windows Hyper-V Server 2019.

o ...

Полный список программных требований доступен в онлайн-справке - https://support.kaspersky.com/KSWS/11/ru-RU/155510.htm.

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;

• 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;

• 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;

• 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;

• интеграции с SIEM системами;

• указания количества рабочих процессов антивируса вручную;

• 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;

• защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;

• контроль устройств, в том числе сетевых карт и модемов;

Требования к программным средствам антивирусной защиты мобильных устройств

Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:

o Android 4.2-11.0.

o iOS 10.0-14.0 или iPadOS.

В программном средстве антивирусной защиты смартфонов для ОС Android должны быть реализованы следующие функциональные возможности:

• постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;

• проверка файловой системы устройства по требованию и по расписанию;

• мгновенная проверка устанавливаемых приложений

• блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;

• наличие хранилища для изолирования зараженных объектов;

• обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;

• блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;

• поддержка белых списков разрешенных приложений;

• блокировка системных приложений, в рамках контроля запуска приложений;

• отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);

• заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;

• указать параметры подключения к wi-fi сетям;

• указать обязательные к установке приложения;

• блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);

• создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;

• поддержка технологий Samsung KNOX1 и KNOX2.

В программном средстве защиты смартфонов для ОС Apple iOS должны быть реализованы следующие функциональные возможности:

• удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;

• отправки команды блокирования и удаления данных;

• создавать групповые политики безопасности мобильных устройств;

• удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;

• получать отчеты и статистику о работе мобильных устройств пользователей;

• блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;

• централизованного управления с помощью единой консоли управления;

• наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.

Требования к программным средствам централизованного управления, мониторинга и обновления

Программные средства централизованного управления, мониторинга и обновления должны функционировать на компьютерах, работающих под управлением определенных версий операционных систем, поддерживать установку на виртуальных платформах и функционировать с различными СУБД.

Список программных требований доступен в онлайн-справке - https://support.kaspersky.com/ksc/12/ru-RU/96255.htm

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;

• чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;

• 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;

• указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;

• 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;

• инвентаризация установленного ПО и оборудования на компьютерах пользователей;

• 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;

• отправки SMS-оповещений о заданных событиях;

• централизованная установка сертификатов на управляемые мобильные устройства;

• указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;

• 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;

• установки в облачной инфраструктуре Microsoft Azure и Google Cloud;

• интеграции по OpenAPI;

• 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 программ

|  |  |
| --- | --- |
| Заказчик  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_ 2021 г.  М.П. | Исполнитель  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_ 2021 г.  М.П. |