Приложение №4

к извещению об осуществлении закупки

**МУНИЦИПАЛЬНЫЙ КОНТРАКТ\_\_\_\_\_\_\_**

 НА ОКАЗАНИЕ УСЛУГ ПО ПРОДЛЕНИЮ ЛИЦЕНЗИЙ НА ПОДСИСТЕМУ ЦЕНТРАЛИЗОВАННОЙ АНТИВИРУСНОЙ ОБРАБОТКИ.

ИКЗ № 233862201554386220100100170016311244

г. Югорск «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_\_г.

Муниципальное казенное учреждение «Центр материально-технического и информационно-методического обеспечения, именуемый в дальнейшем «Заказчик», в лице директора Виктории Ивановны Паньшиной, действующего на основании Устава, 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 Заказчика от \_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_ об осуществлении закупки у единственного исполнителя в соответствии с пунктом \_\_\_\_\_\_\_\_ части 1 статьи 93 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» заключили настоящий муниципальный контракт, именуемый в дальнейшем «Контракт», о нижеследующем:

1. Предмет контракта

1.1. Исполнитель обязуется своевременно оказать на условиях Контракта услуги по оказанию услуг 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 №1) и Спецификации (Приложение №2) к Контракту.

1.3. Место оказания услуг:

- 628260, Тюменская обл., Ханты - Мансийский автономный округ - Югра, г. Югорск, ул. Ленина, д.29;

- 628260, Тюменская обл., Ханты - Мансийский автономный округ - Югра, г. Югорск, ул. Геологов, д.9.

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 2023 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.

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.

2.3. В общую цену Контракта включены все расходы Исполнителя, необходимые для осуществления им своих обязательств по Контракту в полном объеме и надлежащего качества, в том числе все подлежащие к уплате налоги, сборы и другие обязательные платежи и иные расходы, связанные с оказанием услуг.

2.4. Расчеты по Контракту производятся в следующем порядке:

2.4.1. Оплата производится в безналичном порядке путём перечисления Заказчиком денежных средств на указанный в Контракте расчётный счёт Исполнителя.

2.4.2. Оплата производится в рублях Российской Федерации.

2.4.3. Расчёт за оказанные услуги осуществляется в течение 7 (семи) рабочих дней со дня

подписания Заказчиком структурированного документа о приёмке.

2.5. В случае уменьшения Заказчику соответствующими муниципальными органами 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) объему услуг.

3. Права и обязанности сторон

3.1. Заказчик имеет право:

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

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

3.1.3. 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 и объеме предусмотренные Контрактом и Техническим заданием (Приложение№1).

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.

4. Сроки оказания услуг

4.1. Услуги должны быть оказаны с даты подписания муниципального контракта по 31.07.2023 года включительно.

4.2. Досрочная сдача результатов услуг допускается только по согласованию с Заказчиком. В случае согласования досрочного оказания услуг Заказчик обязуется принять услуги и подписать акт оказанных услуг 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 возмещению убытков и выплате неустойки (штрафа, пени), Стороны после наступления указанной даты не вправе требовать исполнения Контракта в части оказания услуг и их приемки.

5. Порядок сдачи и приемки услуг

5.1. Приемка услуг на соответствие их объема и качества требованиям, установленным, в Контракте производится в соответствии с техническим заданием и спецификацией (Приложение №2) к Контракту.

5.2. Исполнитель не позднее 5 (пяти) дней, направляет в адрес Заказчика извещение (уведомление) о готовности услуг к сдаче и акт оказанных услуг или в случае, предусмотренном пунктом 5.7. настоящего контракта, формирует и направляет структурированный документ о приемке в единой информационной системе в сфере закупок.

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 акт оказанных услуг в течение 5 дней со дня получения акта или в случае, предусмотренном пунктом 5.7. контракта структурированного документа о приемке в единой информационной системе в сфере закупок.

5.5. 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.

5.6. Приемка услуг оформляется актом 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, акт оказанных услуг составляется в трех экземплярах и подписывается Исполнителем, Заказчиком (в случае создания приемочной комиссии подписывается всеми членами приемочной комиссии и утверждается Заказчиком) и Исполнителем.

5.7. Стороны по настоящему контракту вправе осуществлять с использованием единой информационной системы электронную приемку оказанных услуг в порядке и сроки, предусмотренные ст. 94 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

6. Обеспечение исполнения контракта

6.1. Исполнение контракта, гарантийные обязательства обеспечиваются предоставлением независимой гарантии, выданной банком и соответствующей требованиям Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», или внесением денежных средств на указанный заказчиком счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими заказчику.

Способ обеспечения исполнения контракта, гарантийных обязательств, срок действия независимой гарантии определяются в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» участником закупки, с которым заключается контракт, самостоятельно.

6.2. Обеспечение исполнения Контракта предоставляется Заказчику до заключения Контракта. Размер обеспечения исполнения Контракта составляет \_\_\_\_\_\_\_\_\_рубля \_\_\_\_\_\_копейка (5 процентов от цены контракта).

Обеспечение исполнения гарантийных обязательств, предоставляется Заказчику до оформления документа о приемке (за исключением отдельного этапа исполнения контракта). Размер обеспечения гарантийных обязательств составляет 5 606 рублей 82 копейки (10 процентов от начальной (максимальной) цены контракта).

*В случае заключения контракта по результатам определения поставщика 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» размер обеспечения исполнения контракта, в том числе предоставляемого 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», устанавливается* ***от цены****, по которой в соответствии с Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» заключается контракт, но не может составлять менее чем размер аванса.*

*В случае если Исполнителем предложена цена контракта, которая на двадцать пять и более процентов ниже начальной (максимальной) цены контракта, Исполнитель предоставляет обеспечение исполнения контракта в размере, превышающем в полтора раза размер обеспечения исполнения контракта, указанного в извещении о закупке, но не менее чем десять процентов от начальной (максимальной) цены контракта или от цены заключаемого контракта (если контракт заключается 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»), в сумме \_\_\_\_\_\_\_\_ рублей \_\_\_\_\_\_\_\_копеек или информацию, подтверждающую добросовестность Исполнителя, с одновременным предоставлением обеспечения исполнения контракта в размере обеспечения исполнения контракта, указанном в извещении о закупке.*

6.3. В ходе исполнения контракта Исполнитель вправе изменить способ обеспечения исполнения контракта и (или) предоставить Заказчику взамен ранее предоставленного обеспечения исполнения контракта новое обеспечение исполнения контракта, размер которого может быть уменьшен в порядке и случаях, которые предусмотрены частями 7.2 и 7.3 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». Исполнитель вправе изменить способ обеспечения гарантийных обязательств и (или) предоставить заказчику взамен ранее предоставленного обеспечения гарантийных обязательств новое обеспечение гарантийных обязательств.

6.4. Срок действия независимой гарантии должен превышать предусмотренный контрактом срок исполнения обязательств, которые должны быть обеспечены такой гарантией, не менее чем на один месяц, в том числе в случае его изменения в соответствии со статьей 95 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

6.5. В случае отзыва в соответствии с законодательством Российской Федерации у банка, предоставившего независимую гарантию в качестве обеспечения исполнения контракта, лицензии на осуществление банковских операций Исполнитель обязан предоставить новое обеспечение исполнения контракта не позднее одного месяца со дня надлежащего уведомления Заказчиком Исполнителя о необходимости предоставить соответствующее обеспечение.

6.6. Независимая гарантия оформляется в письменной форме на бумажном носителе или в форме электронного документа, подписанного усиленной неквалифицированной электронной подписью лица, имеющего право действовать от имени банка, на условиях, определенных гражданским законодательством, Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», с учетом требований установленных постановлением Правительства Российской Федерации.

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.

6.8. Предусмотренное частями 7 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 оказанных услуг, 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 Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» 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*.

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

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 за исключением случаев, если законодательством Российской Федерации установлен иной порядок начисления штрафов.

7.2. Размер штрафа устанавливается контрактом в порядке, установленном пунктами 7.3 – 7.8, 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 – 7.7):

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 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), 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 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 (отдельного этапа исполнения контракта), уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных контрактом (соответствующим отдельным этапом исполнения контракта) 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: стихийные бедствия (землетрясение, наводнение, ураган), пожар, массовые заболевания (эпидемии), забастовки, военные действия, террористические акты, диверсии, ограничения перевозок, запретительные меры государств, запрет торговых операций, в том числе с отдельными странами, вследствие принятия международных санкций и другие не зависящие от воли Сторон Контракта обстоятельства.

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 все противоречия или спорные вопросы, возникающие между ними в рамках Контракта.

9.2. Любые споры, разногласия и требования, возникающие из Контракта, подлежат разрешению в Арбитражном суде Ханты-Мансийского автономного округа – Югры.

9.3. В случае наличия споров, разногласий и претензий относительно исполнения настоящего Контракта, они рассматриваются сторонами путем направления с использованием функционала ЕИС электронных уведомлений (претензий). Споры и разногласия, возникающие по настоящему Контракту, подлежат досудебному урегулированию, разрешению в претензионном порядке. Срок ответа на претензию - не позднее 10 (десяти) рабочих дней с даты ее получения.

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.

* 1. Заказчик вправе принять решение об одностороннем отказе от исполнения Контракта. До принятия такого решения Заказчик вправе провести экспертизу оказанных услуг с привлечением экспертов, экспертных организаций . 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.
	2. Односторонний отказ Заказчика от исполнения контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств осуществляется Заказчиком в порядке и сроки, установленные Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
	3. 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.
	4. Заказчик обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения Контракта, в порядке и сроки, установленные Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
	5. Заказчик принимает решение об одностороннем отказе от исполнения Контракта, в случаях и порядке установленном частями 15-16 статьи 95 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
	6. Исполнитель вправе принять решения об одностороннем отказе от исполнения контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа отдельных видов обязательств. Односторонний отказ Исполнителя от исполнения контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств осуществляется Исполнителем в порядке и сроки, установленные Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
	7. Исполнитель обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения Контракта, в порядке и сроки, установленные Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
	8. 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 в силу с даты подписания муниципального контракта и действует по 16 августа 2023 г. С 17 авгутса 2023 г. обязательства Сторон по Контракту прекращаются, за исключением обязательств по возмещению убытков и выплате неустойки.

12. Прочие условия

12.1. Контракт составлен в форме электронного документа.

12.2. Все приложения к Контракту являются его неотъемной частью.

12.3. К Контракту прилагается:

- Техническое задание (Приложение №1);

- Спецификация (Приложение №2).

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 услуг, качества оказываемой услуги и иных условий Контракта.

12.6. 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.

12.7. 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.

12.8. В случае исполнения, изменения, расторжения контракта при обмене документами при применении мер ответственности и совершении иных действий в связи с нарушением поставщиком (подрядчиком, исполнителем) или заказчиком условий контракта в отношении контракта, заключенного по результатам электронных процедур, такой обмен осуществляется с использованием единой информационной системы путем направления электронных уведомлений. Такие уведомления формируются с использованием единой информационной системы, подписываются усиленной электронной подписью лица, имеющего право действовать от имени заказчика, поставщика (подрядчика, исполнителя), и размещаются в единой информационной системе без размещения на официальном сайте.

13. Адреса места нахождения, банковские реквизиты и подписи Сторон

|  |  |
| --- | --- |
| Заказчик\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"\_\_\_" \_\_\_\_\_\_ 20\_\_ г.М.П. | Исполнитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"\_\_\_" \_\_\_\_\_\_ 20\_\_ г.М.П. |

Приложение № 1

к муниципальному контракту

№ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от "\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_ 202\_\_ г.

СПЕЦИФИКАЦИЯ

Оказание услуг по продлению лицензии на подсистему централизованной антивирусной обработки

**5. Наименование, характеристика и количество поставляемого товара:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | КодОКПД2 | Наименование | Описание объекта закупки | Ед.изм. | Кол-во | Цена за ед., руб. | Сумма, руб. |
| 1 | 63.11.13.000 | Продление лицензий на подсистему централизованной антивирусной обработки. |  | место | 40 |  |  |
| Итого: цена муниципального контракта |  |

|  |  |
| --- | --- |
| ЗаказчикДиректор\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_В.И. Паньшина"\_\_\_" \_\_\_\_\_\_ 20\_\_ г.М.П. | Исполнитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"\_\_\_" \_\_\_\_\_\_ 20\_\_ г.М.П. |

Приложение № 2

к муниципальному контракту

№ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

от "\_\_\_" \_\_\_\_\_\_\_ 20\_\_ г.

**Описание объекта закупки (Техническое задание).**

1. Муниципальный заказчик:

Муниципальное казенное учреждение «Центр материально-технического и информационно- методического обеспечения».

2. Предмет муниципального контракта: оказание услуг по продлению лицензии на подсистему централизованной антивирусной обработки.

3. Срок поставки товара: с даты подписания муниципального контракта до 31.07.2023 г.

4. Место поставки:

- 628260, Тюменская обл., Ханты - Мансийский автономный округ - Югра, г. Югорск, ул. Ленина, д.29;

- 628260, Тюменская обл., Ханты - Мансийский автономный округ - Югра, г. Югорск, ул. Геологов, д.9.

5. Наименование, требования к составу и характеристики:

6. ОКПД 2: 63.11.13.000

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | КодОКПД2 | Наименование | Описание объекта закупки | Ед.изм. | Кол-во |
| 1 | 63.11.13.000 | Продление лицензий на подсистему централизованной антивирусной обработки | Предоставление неисключительного права на использование программного обеспечения 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)действующая лицензия: 280E-220620-065030-256-1492 | место | 40 |

**1. 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 / Ultimate / Enterprise Service Pack 1 и выше;

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

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

o Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise;

o Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise.

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 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;

• наличие инструмента мониторинга сети по протоколам TCP и UDP;

• возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;

• возможность установки ограничение длительности выполнения задачи;

• возможность ставить задачи проверки в очередь, если проверка уже выполняется.

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), Microsoft Small Business Server 2011 Standard (64-разрядная) поддерживается только с установленным Service Pack 1 для Microsoft Windows Server 2008 R2;

o Windows MultiPoint Server 2011 (64-разрядная);

o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;

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

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

o Windows Server 2016 Essentials / Standard / Datacenter;

o Windows Server 2019 Essentials / Standard / Datacenter;

o Windows Server 2022.

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;

• возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;

• возможность установки ограничения длительности выполнения задачи;

• возможность ставить задачи проверки в очередь, если проверка уже выполняется.

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 10.14 - 12;

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;

• возможность установки расширений из командной строки с помощью новой команды kav;

• возможность задавать исключения при проверке указанных областей на уровне перехватов файловых операций;

• возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены.

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 CentOS 6.7 и выше.

o Debian GNU/Linux 10.1 и выше.

o Debian GNU/Linux 11.

o Mageia 4.

o Red Hat Enterprise Linux 6.7 и выше.

o Альт 8 СП Рабочая Станция.

o Альт 8 СП Сервер.

o Альт Образование 10.

o Альт Рабочая Станция 10.

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

o AlmaLinux OS 8 и выше.

o AlmaLinux OS 9 и выше.

o AlterOS 7.5 и выше.

o Amazon Linux 2.

o Astra Linux Common Edition 2.12.

o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).

o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).

o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).

o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).

o CentOS 6.7 и выше.

o CentOS 7.2 и выше.

o CentOS Stream 9.

o Debian GNU/Linux 10.1 и выше.

o Debian GNU/Linux 11.

o EMIAS 1.0.

o EulerOS 2.0 SP5.

o LinuxMint 19.2 и выше.

o LinuxMint 20.3 и выше.

o openSUSE Leap 15.0 и выше.

o Oracle Linux 7.3 и выше.

o Oracle Linux 8.0 и выше.

o Red Hat Enterprise Linux 6.7 и выше.

o Red Hat Enterprise Linux 7.2 и выше.

o Red Hat Enterprise Linux 8.0 и выше.

o Red Hat Enterprise Linux 9.

o Rocky Linux 8.5 и выше.

o SUSE Linux Enterprise Server 12.5 и выше.

o SUSE Linux Enterprise Server 15 и выше.

o Ubuntu 20.04 LTS.

o Ubuntu 22.04 LTS.

o Альт 8 СП Рабочая станция.

o Альт 8 СП Сервер.

o Альт Образование 10.

o Альт Рабочая Станция 10.

o Альт Сервер 10.

o Атлант, сборка Alcyone, версия 2022.02.

o Гослинукс 7.17.

o Гослинукс 7.2.

o РЕД ОС 7.3.

o РОСА "Кобальт" 7.9.

o РОСА "Хром" 12.

o ОСОН "ОСНова".

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

o Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).

o EulerOS 2.0 SP8.

o SUSE Linux Enterprise Server 15 SP3.

o Ubuntu 20.04 LTS.

o Альт 8 СП Сервер.

o РЕД ОС 7.3.

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;

• получения данных о действиях программ на компьютере пользователя;

• создание файлов трассировки при запуске программы;

• получение информации обо всех исполняемых файлах программ, установленных на компьютерах;

• проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;

• сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий.

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 2003 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

o Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

o Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше.

64-разрядных операционных систем Microsoft Windows

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

o Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

o Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

o Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;

o Microsoft Small Business Server 2008 Standard / Premium SP2 или выше;

o Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;

o Windows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;

o Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;

o Microsoft Small Business Server 2011 Essentials / Standard SP1 или выше;

o Microsoft Windows MultiPoint Server 2011 Standard / Premium;

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

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

o Microsoft MultiPoint Server 2012 Standard / Premium;

o Windows Storage Server 2012;

o Windows Hyper-V Server 2012;

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

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

o Windows Storage Server 2012 R2;

o Windows Hyper-V Server 2012 R2;

o Windows Server 2016 Essentials / Standard / Datacenter;

o Windows Server 2016 MultiPoint;

o Windows Server 2016 Core Standard / Datacenter;

o Microsoft Windows MultiPoint Server 2016;

o Windows Storage Server 2016;

o Windows Hyper-V Server 2016;

o Windows Server 2019 Essentials / Standard / Datacenter;

o Windows Server 2019 Core;

o Windows Storage Server 2019;

o Windows Hyper-V Server 2019;

o Windows Server 2022;

o Windows 10 Enterprise multi-session.

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;

• включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.

Требования к программным средствам антивирусной защиты мобильных устройств

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

o Android 5.0–13 (включая Android 12L, исключая Go Edition);

o iOS 10–16 или iPadOS 13–15;

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 на базе ОС Windows

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

o Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;

o Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;

o Microsoft Windows 11 Home 64-разрядная;

o Microsoft Windows 11 Pro 64-разрядная;

o Microsoft Windows 11 Enterprise 64-разрядная;

o Microsoft Windows 11 Education 64-разрядная;

o Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;

o Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;

o Microsoft Windows 8 Pro 32-разрядная/64-разрядная;

o Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;

o Microsoft Windows 7 Professional Service Pack 1 32-разрядная/64-разрядная;

o Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная;

o Windows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;

o Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;

o Windows Server 2012 Server Core 64-разрядная;

o Windows Server 2012 Datacenter 64-разрядная;

o Windows Server 2012 Essentials 64-разрядная;

o Windows Server 2012 Foundation 64-разрядная;

o Windows Server 2012 Standard 64-разрядная;

o Windows Server 2012 R2 Server Core 64-разрядная;

o Windows Server 2012 R2 Datacenter 64-разрядная;

o Windows Server 2012 R2 Essentials 64-разрядная;

o Windows Server 2012 R2 Foundation 64-разрядная;

o Windows Server 2012 R2 Standard 64-разрядная;

o Windows Server 2016 Datacenter (LTSB) 64-разрядная;

o Windows Server 2016 Standard (LTSB) 64-разрядная;

o Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;

o Windows Server 2019 Standard 64-разрядная;

o Windows Server 2019 Datacenter 64-разрядная;

o Windows Server 2019 Core 64-разрядная;

o Windows Server 2022 Standard 64-разрядная;

o Windows Server 2022 Datacenter 64-разрядная;

o Windows Server 2022 Core 64-разрядная;

o Windows Storage Server 2012 64-разрядная;

o Windows Storage Server 2012 R2 64-разрядная;

o Windows Storage Server 2016 64-разрядная;

o Windows Storage Server 2019 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

o VMware vSphere 6.7;

o VMware vSphere 7.0;

o VMware Workstation 16 Pro;

o Microsoft Hyper-V Server 2012 64-разрядная;

o Microsoft Hyper-V Server 2012 R2 64-разрядная;

o Microsoft Hyper-V Server 2016 64-разрядная;

o Microsoft Hyper-V Server 2019 64-разрядная;

o Microsoft Hyper-V Server 2022 64-разрядная;

o Citrix XenServer 7.1 LTSR;

o Citrix XenServer 8.x;

o Parallels Desktop 17;

o Oracle VM VirtualBox 6.x.

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

o Microsoft SQL Server 2012 Express 64-разрядная;

o Microsoft SQL Server 2014 Express 64-разрядная;

o Microsoft SQL Server 2016 Express 64-разрядная;

o Microsoft SQL Server 2017 Express 64-разрядная;

o Microsoft SQL Server 2019 Express 64-разрядная;

o Microsoft SQL Server 2014 (все редакции) 64-разрядная;

o Microsoft SQL Server 2016 (все редакции) 64-разрядная;

o Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная;

o Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная;

o Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная (требуются дополнительные действия);

o Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия);

o Microsoft Azure SQL Database;

o Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure;

o MySQL 5.7 Community 32-разрядная/64-разрядная;

o MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;

o MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная;

o MariaDB 10.5.x 32-разрядная/64-разрядная;

o MariaDB 10.4.x 32-разрядная/64-разрядная;

o MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;

o MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

o MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

o MariaDB 10.1.30 и выше 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;

• 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;

• двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;

• использования дополнительной аутентификация после изменения параметров учетной записи пользователя.

• возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами;

• возможность развернуть сервер администрирования как систему высокой доступности.

Требования к программным средствам централизованного управления, мониторинга и обновления на базе ОС Linux

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

o Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;

o Debian GNU/Linux 10.х (Buster) 32-разрядная/64-разрядная;

o Debian GNU/Linux 9.х (Stretch) 32-разрядная/64-разрядная;

o Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;

o Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная;

o CentOS 7.x 64-разрядная;

o Red Hat Enterprise Linux Server 8.x 64-разрядная;

o Red Hat Enterprise Linux Server 7.x 64-разрядная;

o SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная;

o SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная;

o Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

o Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

o Astra Linux Common Edition 2.12 64-разрядная;

o Альт Сервер 10 64-разрядная;

o Альт Сервер 9.2 64-разрядная;

o Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;

o Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная;

o Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная;

o Oracle Linux 7 64-разрядная;

o Oracle Linux 8 64-разрядная;

o РЕД ОС 7.3 Сервер 64-разрядная;

o РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

Программные средства централизованного управления, мониторинга и обновления должны поддерживать установку на следующих виртуальных платформах:

o VMware vSphere 6.7.

o VMware vSphere 7.0;

o VMware Workstation 16 Pro;

o Microsoft Hyper-V Server 2012 64-разрядная;

o Microsoft Hyper-V Server 2012 R2 64-разрядная;

o Microsoft Hyper-V Server 2016 64-разрядная;

o Microsoft Hyper-V Server 2019 64-разрядная;

o Microsoft Hyper-V Server 2022 64-разрядная;

o Citrix XenServer 7.1 LTSR;

o Citrix XenServer 8.x;

o Parallels Desktop 17;

o Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:

o Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;

o Альт Сервер 10 64-разрядная;

o Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;

o Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;

o Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;

o РЕД ОС 7.3 Сервер 64-разрядная;

o РЕД ОС 7.3 Сертифицированная редакция 64-разрядная

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

o MySQL 5.7 Community 32-разрядная/64-разрядная;

o MySQL 8.0 32-разрядная/64-разрядная;

o MariaDB 10.5.x 32-разрядная/64-разрядная;

o MariaDB 10.4.x 32-разрядная/64-разрядная;

o MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;

o MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;

o MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.

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

• централизованные установка, обновление и удаление программных средств антивирусной защиты;

• централизованная настройка, администрирование;

• просмотр отчетов и статистической информации по работе средств защиты;

• сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;

• иерархии триггеров, по которым происходит перераспределение;

• 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;

• построение графических отчетов по событиям антивирусной защиты, 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;

• наличие системы контроля возникновения вирусных эпидемий;

• управления антивирусной защитой с использованием WEB консоли;

• возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;

• возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;

• возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули.

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 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.

|  |  |
| --- | --- |
| Заказчик\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"\_\_\_" \_\_\_\_\_\_ 20\_\_ г.М.П. | Исполнитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"\_\_\_" \_\_\_\_\_\_ 20\_\_ г.М.П. |