

Контракт №

г. Миасс

" __ " _____ 202__ г.

Федеральное государственное бюджетное учреждение здравоохранения «Медико-санитарная часть № 92 Федерального медико-биологического агентства» (ФГБУЗ МСЧ № 92 ФМБА России), именуемое в дальнейшем «Заказчик», в лице начальника Селиванова Алексея Владимировича, действующего на основании Устава, именуемое в дальнейшем «Заказчик», с одной стороны, и _____, в лице _____, действующего на основании _____, именуемое в дальнейшем «Исполнитель», с другой стороны, а вместе именуемые в дальнейшем «Стороны», с соблюдением требований Гражданского кодекса Российской Федерации, Федерального закона от 05.04.2013 N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд", законодательства Российской Федерации, на основании протокола подведения итогов аукциона в электронной форме № _____ от _____ г., ИКЗ 261741501766074150100170060000244, заключили настоящий контракт (далее – Контракт) о нижеследующем:

1. Предмет Контракта

1.1. Настоящий контракт заключается 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» (далее – Закон о контрактной системе) по результатам проведения процедуры определения исполнителя – электронного аукциона с участником, признанным победителем по результатам проведения конкурентной процедуры, или иным участником в соответствии со статьей 83.2 Федерального закона от 05.04.2013 N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

1.2. Исполнитель обязуется продлить программное обеспечение (Касперский) Заказчику (далее - услуги) для ФГБУЗ МСЧ № 92 ФМБА России код ОКПД 2 62.01.29.000 – Оригиналы программного обеспечения прочие, согласно Спецификации (Приложение № 1 к настоящему контракту), являющейся неотъемлемой частью настоящего контракта, в срок, установленный контрактом.

1.3 Наименование, описание, характеристики, количество, оказываемых услуг оговорены сторонами в Спецификации (Приложение № 1 к настоящему контракту) и Техническом задании (Приложение № 2 к настоящему контракту), являющейся неотъемлемой частью настоящего контракта.

1.4 Место оказания услуг: 456320, Челябинская область, г. Миасс, пр-кт. Макеева, д.21.

1.5 Обязательства Исполнителя по контракту считаются исполненными при условии оказания услуг в полном объеме и надлежащего качества.

2. Срок действия контракта

2.1. Срок оказания услуг: с момента подписания контракта в течение 7 календарных дней со дня подписания Контракта.

2.2. Настоящий контракт, вступает в силу с момента подписания и действует по 30.12.2026 года, в части оплаты до полного погашения. Обязательства Сторон по Контракту прекращаются, за исключением обязательств по оплате услуг, обязательств по возмещению убытков и выплате неустойки (штрафа, пени)).

3. Порядок оказания услуг

3.1. Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

- Регламентное обновление 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.

3.2. 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.

3.3. 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 круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет.
- Web-сайт производителя АПО должен быть на русском языке, иметь специальный раздел, посвященный технической поддержке АПО, пополняемую базу знаний, а также форум пользователей программных продуктов.

3.4. По решению Заказчика для приемки оказанных услуг, может создаваться приемочная комиссия, которая состоит не менее чем из трех человек.

3.5. Для проверки предоставленных Исполнителем результатов, предусмотренных контрактом, в части их соответствия условиям контракта Заказчик проводит экспертизу на соответствие условиям Контракта своими силами или к ее проведению могут привлекаться эксперты, экспертные организации.

3.6. В случае некачественного оказания услуг Исполнитель своими силами и за свой счет обязан в течение одного рабочего дня устранить выявленные недостатки.

3.7. Факт оказания услуг оформляется путем подписания сторонами документа о приемке услуг в соответствии с разделом 6 настоящего контракта.

3.8. К закупаемому товару применяется национальный режим, предусмотренный [ст. 14](#) Федерального закона от 05.04.2013 N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

- Закупаемый товар входит в перечень, указанный в Постановлении Правительства РФ от 16.11.2015 года № 1236» Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд».

4. Порядок расчетов

4.1. Цена контракта составляет _____ (_____) рублей _____ коп.

4.2. Указанная цена контракта является твердой и определяется на весь срок исполнения контракта. Цена контракта включает все расходы, в том числе стоимость услуг, расходы на транспортировку, погрузочно-разгрузочные работы, тару, доставку до места исследования, страхование, уплату таможенных пошлин, налогов и других обязательных платежей, связанных с исполнением Контракта.

4.3. Срок оплаты заказчиком поставленного товара, составляет не более 7 (семи) рабочих дней с даты подписания заказчиком документа о приемке.

4.4. Оплата по контракту осуществляется путем перечисления денежных средств в валюте РФ (рубль) на расчетный счет Поставщика, указанный в контракте, при этом обязанности заказчика в части оплаты контракта считаются исполненными со дня списания денежных средств со счета заказчика.

4.5. Источник финансирования – **Федеральный бюджет.**

4.6. Сумма, подлежащая уплате заказчиком юридическому лицу или физическому лицу, в том числе зарегистрированному в качестве индивидуального предпринимателя, 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.

5. Права и обязанности Сторон

5.1. Заказчик обязуется:

- обеспечить своевременную приемку и оплату оказанных услуг в соответствии с условиями настоящего контракта;
- оказывать содействие Исполнителю в ходе оказания им услуг по вопросам, непосредственно связанным с предметом контракта, решение которых возможно только при участии Заказчика.

5.2. Заказчик имеет право:

- требовать от Исполнителя надлежащего исполнения обязательств по настоящему контракту и своевременного устранения выявленных недостатков;
- требовать своевременного предоставления надлежащим образом оформленной отчетной документации, подтверждающей исполнение обязанностей по настоящему контракту;
- в любое время проверять ход и качество оказания услуг, давать Исполнителю указания по оказанию услуг и требовать отчет об их исполнении, не вмешиваясь при этом в хозяйственную деятельность Исполнителя,
- привлекать экспертов, специалистов и иных лиц, обладающих необходимыми знаниями в области сертификации, стандартизации, безопасности, оценки качества и т.п., для участия в проведении экспертизы исполнения Исполнителем обязательств по настоящему контракту и представленных Исполнителем отчетных документов;
- принять решение об одностороннем отказе от исполнения контракта в соответствии с ч. 9 ст. 95 Федерального закона от 05.04.2013г. № 44-ФЗ.

5.3. Обязанности Исполнителя:

- Произвести поставку Программного Обеспечения (далее ПО) ЗАКАЗЧИКУ в соответствии с условиями настоящего Контракта, в требуемом количестве, по ценам согласно Приложения № 1 к настоящему контракту и в срок определенный в п.2. настоящего контракта.
- Оформить необходимые сопроводительные и бухгалтерские документы в виде расходной накладной, налоговой накладной, счетов-фактур, акта приемки-передачи и предоставить их ЗАКАЗЧИКУ.
- В случае поставки ПО, не отвечающих требованиям, производственный брак, или ПО, повреждено при транспортировке, обеспечить в течение 30 календарных дней его замену ПО.
- нести ответственность перед Заказчиком за надлежащее исполнение своих обязательств;

- возместить Заказчику ущерб, причиненный по вине его работников;
- сохранять конфиденциальность всей информации, полученной от Заказчика в связи с оказанием услуг, а также результатов оказания услуг.

5.4. Исполнитель вправе:

- требовать своевременной оплаты за качественно оказанные и принятые Заказчиком услуги;
- требовать своевременного подписания Заказчиком акта приема оказанных услуг при условии истечения срока, указанного в пункте 6.9. настоящего контракта;
- принять решение об одностороннем отказе от исполнения контракта в соответствии с ч. 19 ст. 95 Федерального закона от 05.04.2013г. № 44-ФЗ.

5.5. Некачественно оказанные услуги и расходы по устранению недостатков оплате Заказчиком не подлежат.

6. Порядок приемки

6.1. Исполнитель в соответствии с условиями контракта обязан предоставить заказчику результаты оказания услуги, предусмотренные контрактом и направить в адрес Заказчика документ о приемке. Документ о приемке оформляется сторонами по направленной Исполнителем форме.

6.2. Исполнитель формирует с использованием единой информационной системы, подписывает усиленной электронной подписью лица, имеющего право действовать от его имени, и размещает в единой информационной системе документ о приемке, который должен содержать:

- а) включенные в контракт в соответствии с пунктом 1 части 2 статьи 51 Федерального закона от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» идентификационный код закупки, наименование, место нахождения заказчика, наименование объекта закупки, место оказания услуги, информацию об Исполнителе, предусмотренную подпунктами "а", "г" и "е" части 1 статьи 43 Федерального закона от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», единицу измерения оказанной услуги;
- б) наименование оказанной услуги;
- в) информацию об объеме оказанной услуги;
- д) стоимость исполненных Исполнителем обязательств, предусмотренных контрактом, с указанием цены за единицу оказанной услуги;
- е) иную информацию с учетом требований, установленных в соответствии с частью 3 статьи 5 Федерального закона от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

6.3. К документу о приемке прилагаются документы, предусмотренные нормативной и технической документацией к оказанной услуге, п. 5.3. контракта, и которые считаются его неотъемлемой частью. При этом, в случае, если информация, содержащаяся в прилагаемых документах, не соответствует информации, содержащейся в документе о приемке, приоритет имеет предусмотренная 6.2. настоящего контракта и п.1 ст. 94 Федерального закона от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» информация, содержащаяся в документе о приемке.

6.4. Датой поступления заказчику документа о приемке, подписанного Исполнителем, считается дата размещения такого документа в единой информационной системе в соответствии с часовой зоной, в которой расположен заказчик.

6.5. Заказчик обязан обеспечить приемку оказанной услуги в соответствии с законодательством в сфере закупок. По решению заказчика для приемки оказанной услуги, результатов отдельного этапа исполнения контракта может создаваться приемочная комиссия, которая состоит не менее чем из пяти человек.

6.6. Приемка оказанной услуги осуществляется в порядке и в сроки, которые установлены контрактом, и оформляется документом о приемке, который подписывается заказчиком (в случае создания приемочной комиссии подписывается всеми членами приемочной комиссии и утверждается заказчиком), либо Исполнителю в те же сроки заказчиком направляется в письменной форме мотивированный отказ от подписания такого документа.

В случае привлечения заказчиком для проведения указанной экспертизы экспертов, экспертных организаций при принятии решения о приемке или об отказе в приемке результатов отдельного этапа исполнения контракта либо оказанной услуги заказчик (приемочная комиссия) должны учитывать отраженные в заключении по результатам указанной экспертизы предложения экспертов, экспертных организаций, привлеченных для ее проведения.

6.7. Заказчик вправе не отказывать в приемке оказанной услуги в случае выявления несоответствия услуги условиям контракта, если выявленное несоответствие не препятствует приемке услуги и устранено исполнителем.

6.8. Приемка результатов оказанной услуги осуществляется в срок не позднее 20 (двадцать) рабочих дней (включая срок на проведение экспертизы и подписание документа о приемке), следующих за днем поступления документа о приемке Заказчику.

6.9. По результатам приемки оказанной услуги Заказчик (за исключением случая создания приемочной комиссии) осуществляет одно из следующих действий:

- а) подписывает усиленной электронной подписью лица, имеющего право действовать от имени заказчика, и размещает в единой информационной системе документ о приемке;
 - б) формирует с использованием единой информационной системы, подписывает усиленной электронной подписью лица, имеющего право действовать от имени заказчика, и размещает в единой информационной системе мотивированный отказ от подписания документа о приемке с указанием причин такого отказа;
- 6.10. В случае создания приемочной комиссии по результатам оказанной услуги:

- а) члены приемочной комиссии подписывают усиленными электронными подписями поступивший документ о приемке или формируют с использованием единой информационной системы, подписывают усиленными электронными подписями

мотивированный отказ от подписания документа о приемке с указанием причин такого отказа. При этом, если приемочная комиссия включает членов, не являющихся работниками заказчика, допускается осуществлять подписание документа о приемке, составление мотивированного отказа от подписания документа о приемке, подписание такого отказа без использования усиленных электронных подписей и единой информационной системы;

б) после подписания членами приемочной комиссии документа о приемке или мотивированного отказа от подписания документа о приемке заказчик подписывает документ о приемке или мотивированный отказ от подписания документа о приемке усиленной электронной подписью лица, имеющего право действовать от имени заказчика, и размещает их в единой информационной системе. Если члены приемочной комиссии не использовали усиленные электронные подписи и единую информационную систему, заказчик прилагает подписанные ими документы в форме электронных образов бумажных документов.

6.11. Внесение исправлений в документ о приемке осуществляется путем формирования, подписания усиленными электронными подписями лиц, имеющих право действовать от имени исполнителя, заказчика, и размещения в единой информационной системе исправленного документа о приемке.

6.12. В случае получения мотивированного отказа от подписания документа о приемке Исполнитель в срок, предусмотренный контрактом (п. 6.17.) вправе устранить причины, указанные в таком мотивированном отказе и направить заказчику документ о приемке в порядке, предусмотренном п.6.8. настоящего контракта.

6.13. Приемка оказанной услуги Заказчиком осуществляется в следующем порядке:

- проверка соответствия оказанных услуг, результатов отдельного этапа исполнения контракта условиям контракта, с представлением заказчику четко и правильно оформленной отчетной документации в установленной комплектности и необходимом количестве экземпляров.

- проверка соответствия услуг соответствующей нормативной документации, демонстрация результата оказанных услуг .

- определяется фактический объем оказанных услуг на соответствие его требованиям контракта.

- при проверке качества услуг проверяются свойства и характеристики ее результатов на их соответствие требованиям контракта, соответствующей нормативной документации.

- проверка соответствия услуг их безопасности требованиям нормативных правовых актов, контракта и предусмотренной им нормативной документации о свойствах и характеристиках результатов услуг, позволяющих обеспечивать защиту жизни и здоровья людей и охрану окружающей среды.

6.14. При отсутствии замечаний и разногласий по результатам приемки документ о приемке подписывается в порядке, предусмотренном контрактом.

6.15. Документ о приемке также может быть оформлен сторонами на бумажном носителе в двух экземплярах, по одному для каждой из сторон, в форме, аналогичной документу о приемке в электронном виде, либо в форме, предложенной исполнителем.

6.16. При наличии выявленных несоответствий или недостатков замечания и разногласия по результатам приемки отражаются Заказчиком в мотивированном отказе от приемки в порядке и сроки, предусмотренные контрактом.

6.17. Срок на устранение выявленных по результатам приемки несоответствий или недостатков составляет 10 (десять) рабочих дней следующих за днем поступления мотивированного отказа от приемки, а именно, за днем размещения мотивированного отказа в единой информационной системе в соответствии с часовой зоной, в которой расположен Исполнитель.

В случае устранения выявленных несоответствий или недостатков оказанной услуги, приемка производится в сроки и в порядке, предусмотренными контрактом для приемки услуги.

6.18. Датой приемки оказанной услуги считается дата размещения в единой информационной системе документа о приемке, подписанного заказчиком.

6.19. Для проверки предоставленных Исполнителем результатов, предусмотренных контрактом, в части их соответствия условиям контракта заказчик обязан провести экспертизу. Экспертиза результатов, предусмотренных контрактом, может проводиться заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации на основании контрактов, заключенных в соответствии с настоящим Федеральным законом.

Результаты такой экспертизы оформляются в виде заключения, которое подписывается экспертом, уполномоченным представителем экспертной организации и должно быть объективным, обоснованным и соответствовать законодательству Российской Федерации.

6.20. Для проведения экспертизы оказанной услуги эксперты, экспертные организации имеют право запрашивать у заказчика и Исполнителя дополнительные материалы, относящиеся к условиям исполнения контракта и отдельным этапам исполнения контракта (при наличии).

В случае, если по результатам такой экспертизы установлены нарушения требований контракта, не препятствующие приемке поставленного товара в заключении могут содержаться предложения об устранении данных нарушений, в том числе с указанием срока их устранения.

Исполнитель обязан компенсировать Заказчику все возникшие в связи с проведением экспертизы расходы, по предъявлении Заказчиком письменного требования и копии соответствующего заключения, других документов, подтверждающих затраты Заказчика.

6.21. Датой оказания услуги считается дата приемки услуги, согласно п. 6.18 настоящего контракта.

6.22. Услуга, не соответствующая требованиям, оговоренным настоящим контрактом, а также не имеющая сопроводительных документов, считается не оказанной.

6.23. Ответственный за приемку представитель Заказчика: _____ тел. (_____).

7. Ответственность сторон

7.1. Стороны несут ответственность за невыполнение или ненадлежащее выполнение условий настоящего Контракта в соответствии с законодательством Российской Федерации.

7.2. Ответственность Исполнителя:

7.2.1. За каждый факт неисполнения или ненадлежащего исполнения исполнителем обязательств, предусмотренных контрактом, заключенным по результатам определения исполнителя в соответствии с [п. 1 ч. 1 ст. 30](#) Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" (далее - Федеральный закон), за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных контрактом, размер штрафа устанавливается в размере 1 % цены контракта (этапа), но не более 5 тыс. рублей и не менее 1 тыс. рублей.

7.2.2. 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, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных контрактом размер штрафа устанавливается в размере *10 процентов начальной (максимальной) цены контракта* и составляет 20622,42 (двадцать тысяч шестьсот двадцать два рубля 42 коп).

7.2.3. За каждый факт неисполнения или ненадлежащего исполнения исполнителем обязательства, предусмотренного контрактом, которое не имеет стоимостного выражения, размер штрафа устанавливается в размере 1000 (одна тысяча) рублей.

7.2.4. 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.

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

7.3. Ответственность заказчика:

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):

7.3.1. За каждый факт неисполнения заказчиком обязательств, предусмотренных контрактом, за исключением просрочки исполнения обязательств, предусмотренных контрактом, размер штрафа устанавливается в размере 1000 (одна тысяча) руб.

7.3.2. Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного контрактом, начиная со дня, следующего после дня истечения установленного контрактом срока исполнения обязательства. Такая пеня устанавливается контрактом в размере одной трехсотой действующей на дату уплаты пеней ключевой ставки Центрального банка Российской Федерации от не уплаченной в срок суммы.

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

7.4. Уплата неустойки не освобождает стороны от исполнения обязательств, принятых на себя по контракту.

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

7.6. Заказчик имеет право удерживать суммы неисполненных Исполнителем требований об уплате неустоек (штрафов, пеней), предъявленных заказчиком в соответствии с Федеральным законом от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», из суммы, подлежащей оплате Исполнителю.

7.7. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательства, предусмотренного контрактом, заказчик вправе удерживать в свою пользу неустойку (штрафы, пени), предъявленных заказчиком в соответствии с Федеральным законом от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», из обеспечения исполнения контракта.

8. Порядок изменения и расторжения контракта

8.1. Изменение существенных условий контракта при его исполнении не допускается, за исключением их изменения по соглашению сторон:

- снижение цены контракта без изменения качества и объема услуг и иных условий контракта (ч.1 ст. 95 Федерального закона от 05.04.2013 N 44-ФЗ) ;

- увеличение или уменьшение предусмотренного контрактом объема услуг не более чем на десять процентов с пропорциональным изменением цены контракта (ч.1 ст. 95 Федеральным законом от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»).

- если при исполнении контракта изменяется срок исполнения отдельного этапа (отдельных этапов) исполнения контракта, при их наличии, в рамках срока исполнения контракта, предусмотренного при его заключении;

В иных случаях, предусмотренных ст. 95 Федеральным законом от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

8.2. Предусмотренные п.8.1. настоящего контракта изменения осуществляются при условии предоставления Исполнителем в

соответствии с Федеральным законом от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» обеспечения исполнения контракта, если такие изменения влекут возникновение новых обязательств Исполнителя, не обеспеченных ранее предоставленным обеспечением исполнения контракта, при этом:

1) размер обеспечения может быть уменьшен в порядке и случаях, предусмотренных частями 7 - 7.3 статьи 96 Федеральным законом от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

2) обеспечение исполнения контракта может быть предоставлено путем внесения соответствующих изменений в условия ранее предоставленной заказчику независимой гарантии (при наличии);

3) если обеспечение исполнения контракта осуществляется путем предоставления новой независимой гарантии, возврат заказчиком ранее предоставленной ему независимой гарантии предоставившему ее гаранту не осуществляется, взыскание по ней не производится, заказчик признается отказавшимся от своих прав по ранее предоставленной независимой гарантии, обязательство гаранта перед заказчиком по ранее предоставленной независимой гарантии прекращается с момента выдачи новой независимой гарантии;

4) если при увеличении в соответствии с настоящей статьей цены контракта обеспечение исполнения контракта осуществляется путем внесения денежных средств, исполнитель вносит на счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими заказчику, денежные средства в размере, пропорциональном стоимости новых обязательств Исполнителя.

8.3. В случае уменьшения в соответствии с настоящей статьей цены контракта заказчик возвращает исполнителю денежные средства в размере, пропорциональном размеру такого уменьшения цены контракта.

8.4. В случае изменения срока исполнения контракта в соответствии с частью 27 статьи 34 Федерального закона от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» новый срок возврата заказчиком Исполнителю денежных средств, внесенных в качестве обеспечения исполнения контракта соответствует сроку, установленному п. 10.20 настоящего контракта.

8.5. При исполнении контракта (за исключением случаев, которые предусмотрены нормативными правовыми актами, принятыми в соответствии с частью 6 статьи 14 Федерального закона от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд») по согласованию заказчика с Исполнителем допускается оказание услуги, качество, технические и функциональные характеристики (потребительские свойства) которой являются улучшенными по сравнению с качеством и соответствующими техническими и функциональными характеристиками, указанными в контракте. В этом случае соответствующие изменения должны быть внесены заказчиком в реестр контрактов, заключенных заказчиком.

8.6. Расторжение контракта допускается по соглашению сторон, по решению суда.

8.7. 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, при условии, если это было предусмотрено контрактом, в том числе в случае:

-отступление исполнителя в услуге от условий контракта или иные недостатки результата оказания услуг, которые не были устранены в установленный заказчиком разумный срок, либо являются существенными и неустраняемыми ([пункт 3 статьи 723 ГК РФ](#)).

8.8. Заказчик обязан принять решение об одностороннем отказе от исполнения контракта в случаях:

1) если в ходе исполнения контракта установлено, что:

а) Исполнитель перестал соответствовать установленным извещением об осуществлении закупки требованиям к участникам закупки (за исключением требования, предусмотренного частью 1.1 (при наличии такого требования) статьи 31 Федерального закона от 05.04.2013 N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд») и (или) поставляемому товару;

б) при определении Исполнителя Исполнитель представил недостоверную информацию о своем соответствии требованиям, указанным в подпункте "а" настоящего пункта, что позволило ему стать победителем определения Исполнителя;

8.9. 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.

8.10. 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.

9. Порядок урегулирования споров

9.1. Разрешение споров в порядке исполнения настоящего контракта осуществляется путем переговоров.

9.2. Для разрешения споров, связанных с нарушением Сторонами своих обязательств по настоящему Контракту либо иным образом вытекающих из Контракта, применяется обязательный досудебный (претензионный) порядок разрешения споров. Сторона, права которой нарушены, до обращения в суд обязана предъявить другой стороне письменную претензию с изложением своих требований. При необходимости к претензии прилагаются документы, подтверждающие выявленные нарушения. Право на предъявление претензии возникает у Стороны чье право было нарушено на следующий день после его нарушения.

Претензии и иные юридически значимые сообщения могут быть направлены и будут считаться направленными надлежащим образом Сторонами друг другу одним из нижеперечисленных способов по реквизитам сторон, указанным в Контракте:

— письмом на указанный в настоящем пункте контракта электронный почтовый ящик (e-mail) – при этом подтверждением такого направления является сохраненная отправившей стороной в ее электронном почтовом ящике скан-копия претензии в формате PDF, JPEG, TIFF или PNG, а также распечатанная бумажная версия отправленного сообщения – такое письмо считается полученным адресатом на следующий календарный день после его отправки;

e-mail Заказчика _____

e-mail Исполнителя _____

— заказным или ценным письмом с описью вложения, а также курьерской доставкой, передачей лично Стороне или его уполномоченному представителю под роспись по адресу места ее нахождения, указанному в контракте в разделе «Адреса и реквизиты сторон» ;

— факсом, на указанный в настоящем пункте контракта номер

Факс Заказчика _____

Факс Исполнителя _____

Срок рассмотрения претензии – 10 (десять) календарных дней со дня ее получения.

В случае если ответ на претензию не будет получен направившей ее Стороной в течение 20 (двадцати) календарных дней со дня ее направления, либо если Стороны не придут к соглашению по возникшим претензиям и/или разногласиям, Сторона, право которой нарушено, вправе обратиться с иском в Арбитражный суд Челябинской области.

9.3. В случае не урегулирования споров и разногласий в досудебном порядке они передаются на рассмотрение в Арбитражный суд Челябинской области.

10. Обеспечение исполнения контракта

10.1. Обеспечение исполнения контракта предоставлено Исполнителем и составляет 10 (десять) % от цены контракта, что составляет ____.

Способ обеспечения исполнения контракта определяются в соответствии с требованиями Закона о контрактной системе исполнителем самостоятельно, в том числе он может быть в следующих формах:

внесения денежных средств / независимой безотзывной гарантии.

Платежные реквизиты для перечисления денежных средств для обеспечения исполнения контракта (гарантийных обязательств):

Реквизиты счета для внесения обеспечения исполнения контракта:

Получатель: **ФГБУЗ МСЧ № 92 ФМБА России**

456320 г. Миасс, пр. Макеева, 21

ИНН 7415017660 КПП 741501001

УФК по Новосибирской области (ФГБУЗ МСЧ № 92 ФМБА России,

л/с 20696Ц21050)

Казначейский счет 032 146 430 000 000 15115

Единый казначейский счет 401 028 104 453 700 000 43

ОКЦ № 1 СибГУ Банка России/УФК по Новосибирской области г. Новосибирск

БИК 015 004 950

КБК 000000000000000000510 обязательно для заполнения

Назначение платежа: обеспечение контракта, заключенного по результатам аукциона в электронной форме

10.2. В случае, если участником предоставлено обеспечение в форме независимой безотзывной гарантии, то она может быть выдана:

- банками, соответствующими требованиям, установленным Постановлением правительства РФ от 12 апреля 2018 г № 440 «О требованиях к банкам, которые вправе выдавать банковские гарантии для обеспечения заявок и исполнения контрактов», в части не противоречащей Федеральному закону №44-ФЗ от 05.04.2013 г. «О Контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», и включенный федеральным органом исполнительной власти по регулированию контрактной системы в сфере закупок в Перечень банков, соответствующих установленным требованиям;

- государственной корпорацией развития "ВЭБ.РФ";

- фондами содействия кредитованию (гарантийными фондами, фондами поручительств), являющимися участниками национальной гарантийной системы поддержки малого и среднего предпринимательства, предусмотренной Федеральным законом от 24 июля 2007 года N 209-ФЗ "О развитии малого и среднего предпринимательства в Российской Федерации" (далее - региональные гарантийные организации), соответствующими требованиям, установленным Правительством Российской Федерации, и включенными федеральным органом исполнительной власти по регулированию контрактной системы в сфере закупок в Перечень региональных гарантийных организаций (при осуществлении закупок в соответствии с пунктом 1 части 1 статьи 30 настоящего Федерального закона);

- Евразийским банком развития (если участник закупки является юридическим лицом, зарегистрированным на территории государства - члена Евразийского экономического союза, за исключением Российской Федерации, или физическим лицом, являющимся гражданином государства - члена Евразийского экономического союза, за исключением Российской Федерации).

10.3 Выданная банком независимая безотзывная гарантия должна соответствовать требованиям статьи 45 Федерального

закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и Постановления Правительства РФ от 8 ноября 2013 г. N 1005 "О банковских гарантиях, используемых для целей Федерального закона "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд", в части не противоречащей Федеральному закону №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

10.4. Если при проведении аукциона предложенная цена контракта, уменьшилась на двадцать пять и более процентов начальной (максимальной) цены контракта, Исполнитель перечисляет обеспечение исполнения контракта (безотзывной независимой гарантией или внесением денежных средств), в порядке и размере, предусмотренном разд. 11 настоящего контракта.

10.5. Контракт заключается после предоставления участником закупки, с которым заключается контракт, обеспечения исполнения контракта в соответствии с Федеральным законом №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

10.6. В случае не предоставления участником закупки, с которым заключается контракт, обеспечения исполнения контракта в срок, установленный для заключения контракта, такой участник считается уклонившимся от заключения контракта.

10.7. Заказчик в качестве обеспечения принимает независимую безотзывную гарантию, которая должна содержать:

1) сумму независимой гарантии, подлежащую уплате гарантом заказчику в случае ненадлежащего исполнения обязательств принципалом в соответствии со статьей 96 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», а также идентификационный код закупки, при осуществлении которой предоставляется такая независимая гарантия;

2) обязательства принципала, надлежащее исполнение которых обеспечивается независимой гарантией;

3) обязанность гаранта уплатить заказчику неустойку в размере 0,1 процента денежной суммы, подлежащей уплате, за каждый день просрочки;

4) условие, согласно которому исполнением обязательств гаранта по независимой гарантии является фактическое поступление денежных сумм на счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими заказчику;

5) срок действия независимой гарантии с учетом требований статьи 96 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»;

6) отлагательное условие, предусматривающее заключение договора предоставления независимой гарантии по обязательствам принципала, возникшим из контракта при его заключении, в случае предоставления независимой гарантии в качестве обеспечения исполнения контракта;

7) установленный Правительством Российской Федерации перечень документов, предоставляемых заказчиком гаранту одновременно с требованием об осуществлении уплаты денежной суммы по независимой гарантии.

10.8. В независимую гарантию включается условие об обязанности гаранта уплатить заказчику (бенефициару) денежную сумму по независимой гарантии не позднее десяти рабочих дней со дня, следующего за днем получения гарантом требования заказчика (бенефициара), соответствующего условиям такой независимой гарантии, при отсутствии предусмотренных Гражданским кодексом Российской Федерации оснований для отказа в удовлетворении этого требования.

10.9. Уменьшение в соответствии с частями 7 и, при наличии этапов исполнения контракта, 7.1. статьи 96 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» размера обеспечения исполнения контракта, предоставленного в виде независимой гарантии, осуществляется заказчиком путем отказа от части своих прав по этой гарантии. При этом датой такого отказа признается дата включения предусмотренной частью 7.2 статьи 96 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» информации в соответствующий реестр контрактов, предусмотренный статьей 103 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

10.10. Запрещается включение в условия независимой гарантии требования о представлении заказчиком гаранту судебных актов, подтверждающих неисполнение принципалом обязательств, обеспечиваемых независимой гарантией.

10.11. Независимая гарантия, информация о ней и документы, предусмотренные частью 9 ст. 45 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», должны быть включены в реестр независимых гарантий, размещенный в единой информационной системе, за исключением независимых гарантий, указанных в части 8.1 ст. 45 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

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

10.13. В ходе исполнения контракта Поставщик 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 ст. 96 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конфрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и, соответственно п.п.10.9 и.10.10. настоящего контракта.

Поставщик вправе изменить способ обеспечения гарантийных обязательств (при их наличии) и (или) предоставить заказчику взамен ранее предоставленного обеспечения гарантийных обязательств новое обеспечение гарантийных обязательств.

10.14. В случае, если контрактом предусмотрены отдельные этапы его исполнения и установлено требование обеспечения исполнения контракта, в ходе исполнения данного контракта размер этого обеспечения подлежит уменьшению в порядке и случаях, которые предусмотрены частями 7.2 и 7.3 ст. 96 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конкретной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и, соответственно п.п.10.9 и.10.10. настоящего контракта.

10.15. Размер обеспечения исполнения контракта уменьшается посредством направления Заказчиком информации об исполнении Поставщиком обязательств по оказанию услуги или об исполнении им отдельного этапа исполнения контракта и стоимости исполненных обязательств для включения в соответствующий реестр контрактов, предусмотренный статьей 103 Закона о контрактной системе. Уменьшение размера обеспечения исполнения контракта производится пропорционально стоимости исполненных обязательств, приемка и оплата которых осуществлены в порядке и сроки, которые предусмотрены контрактом. В случае, если обеспечение исполнения контракта осуществляется путем предоставления независимой гарантии, требование Заказчика об уплате денежных сумм по этой гарантии может быть предъявлено в размере не более размера обеспечения исполнения контракта, рассчитанного заказчиком на основании информации об исполнении контракта, размещенной в соответствующем реестре контрактов. В случае, если обеспечение исполнения контракта осуществляется путем внесения денежных средств на счет, указанный Заказчиком, по заявлению Поставщика ему возвращаются Заказчиком в установленный в соответствии с частью 27 статьи 34 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конкретной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» контрактом срок денежные средства в сумме, на которую уменьшен размер обеспечения исполнения контракта, рассчитанный Заказчиком на основании информации об исполнении контракта, размещенной в соответствующем реестре контрактов.

10.16. Уменьшение размера обеспечения исполнения контракта осуществляется при условии отсутствия неисполненных Поставщиком требований об уплате неустоек (штрафов, пеней), предъявленных Заказчиком в соответствии с Законом о контрактной системе и настоящим контрактом, а также приемки Заказчиком оказанной услуги, результатов отдельного этапа исполнения контракта в объеме выплаченного аванса (если контрактом предусмотрена выплата аванса).

10.17. Участник закупки, с которым заключается контракт по результатам определения поставщика в соответствии с пунктом 1 части 1 статьи 30 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конкретной 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 настоящего Федерального закона, от обеспечения 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)

10.18. Обеспечение исполнения контракта, включая положения о предоставлении такого обеспечения с учетом положений статьи 37 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конкретной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» не предоставляется в случае заключения контракта с участником закупки, который является казенным учреждением.

10.19. В случае предоставления нового обеспечения исполнения контракта в соответствии с частью 30 статьи 34, пунктом 9 части 1 статьи 95, частью 7 статьи 96 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конкретной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» возврат независимой гарантии заказчиком гаранту, предоставившему указанную независимую гарантию, не осуществляется, взыскание по ней не производится.

10.20. Срок возврата заказчиком Поставщику денежных средств, внесенных в качестве обеспечения исполнения контракта (если такая форма обеспечения исполнения контракта применяется поставщиком, в том числе части этих денежных средств в случае уменьшения размера обеспечения исполнения контракта в соответствии с Законом о контрактной системе, не должен превышать тридцать дней с даты исполнения поставщиком (подрядчиком, исполнителем) обязательств, предусмотренных контрактом, а в случае установления заказчиком ограничения, предусмотренного частью 3 статьи 30 настоящего Федерального закона, такой срок не должен превышать пятнадцать дней с даты исполнения поставщиком (подрядчиком, исполнителем) обязательств, предусмотренных контрактом.

10.21. Исключение банка из перечня, предусмотренного частью 1.2 статьи 45 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конкретной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», региональной гарантийной организации из перечня, предусмотренного частью 1.7 статьи 45 Федерального закона №44-ФЗ от 05.04.2013 г. «О Конкретной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», не прекращает действия выданных гарантом и принятых заказчиками независимых гарантий и не освобождает гаранта от ответственности за неисполнение либо ненадлежащее исполнение условий таких независимых гарантий.

10.22. В случае отзыва в соответствии с законодательством Российской Федерации у банка, предоставившего независимую гарантию в качестве обеспечения исполнения контракта, лицензии на осуществление банковских операций Поставщик обязан предоставить новое обеспечение исполнения контракта не позднее одного месяца со дня надлежащего уведомления Заказчиком Поставщика о необходимости предоставить соответствующее обеспечение. Размер такого обеспечения может быть уменьшен в порядке и случаях, которые предусмотрены Законом о контрактной системе и настоящим контрактом. За каждый день просрочки исполнения Поставщиком обязательства, предусмотренного настоящим пунктом, начисляется пеня в размере, определенном в порядке, установленном в соответствии с разд. 7 настоящего контракта.

10.23. В случае, если после заключения контракта по каким либо причинам обеспечение исполнения обязательств по контракту перестало быть действительным, закончилось свое действие или иным образом перестало обеспечивать исполнение поставщиком (подрядчиком, исполнителем), своих обязательств по контракту, соответствующий поставщик (подрядчик, исполнитель) обязуется в течение 10 (Десяти) банковских дней предоставить заказчику иное (новое) надлежащее обеспечение исполнения обязательств по контракту уменьшенное на размер выполненных обязательств по контракту, при этом может быть изменен способ обеспечения исполнения контракта.

11. Антидемпинговые меры

11.1. Если участником закупки (Исполнителем), с которым заключается контракт, предложена цена контракта, которая на двадцать пять и более процентов ниже начальной (максимальной) цены контракта, контракт заключается только после предоставления таким участником обеспечения исполнения контракта, в размере, превышающем в полтора раза размер обеспечения исполнения контракта, указанный в п.10.1 настоящего контракта, что составляет _____ или предоставляет информацию, подтверждающую добросовестность такого участника в соответствии с частью 3 ст. 37 Закона о контрактной системе № 44-ФЗ с одновременным предоставлением таким участником обеспечения исполнения контракта в размере обеспечения исполнения контракта, указанном в п.10.1 настоящего контракта.

11.2. К информации, подтверждающей добросовестность участника закупки, относится информация, содержащаяся в реестре контрактов, заключенных заказчиками, и подтверждающая исполнение таким участником в течение трех лет до даты подачи заявки на участие в закупке трех контрактов (с учетом правопреемства), исполненных без применения к такому участнику неустоек (штрафов, пеней). При этом цена одного из таких контрактов должна составлять не менее чем двадцать процентов начальной (максимальной) цены контракта, указанной в извещении об осуществлении закупки и документации о закупке.

11.3. Информация, предусмотренная пунктом 11.2. настоящего контракта, предоставляется участником закупки (Поставщиком) при направлении заказчику подписанного проекта контракта. При невыполнении таким участником, признанным победителем аукциона, данного требования или признании комиссией по осуществлению закупок информации, подтверждающей добросовестность участника закупки, недостоверной контракт с таким участником не заключается, и он признается уклонившимся от заключения контракта. В этом случае решение комиссии по осуществлению закупок оформляется протоколом, который размещается в единой информационной системе и доводится до сведения всех участников аукциона не позднее рабочего дня, следующего за днем подписания указанного протокола.

11.4. Обеспечение, указанное в разд. 10 настоящего контракта, предоставляется участником закупки (Поставщиком), с которым заключается контракт, до его заключения. Участник закупки, не выполнивший данного требования, признается уклонившимся от заключения контракта.

12. Антикоррупционная оговорка

12.1. При исполнении своих обязательств по Контракту, Стороны, их аффилированные лица, работники или посредники не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам, для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или иные неправомерные цели. При исполнении своих обязательств по Контракту, Стороны, их аффилированные лица, работники или посредники не осуществляют действия, квалифицируемые применимым для целей Контракта законодательством, как дача/получение взятки, коммерческий подкуп, а также действия, нарушающие требования применимого законодательства и международных актов о противодействии легализации (отмыванию) доходов, полученных преступным путем.

12.2. В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений настоящей Статьи, соответствующая Сторона обязуется уведомить другую Сторону в письменной форме. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений настоящей Статьи контрагентом, его аффилированными лицами, работниками или посредниками выражающееся в действиях, квалифицируемых применимым законодательством, как дача или получение взятки, коммерческий подкуп, а также действиях, нарушающих требования применимого законодательства и международных актов о противодействии легализации доходов, полученных преступным путем. После письменного уведомления, соответствующая Сторона имеет право приостановить исполнение обязательств по Контракту до получения подтверждения, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение десяти рабочих дней с даты направления письменного уведомления.

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

13. Обстоятельства непреодолимой силы

13.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по контракту, если оно являлось следствием действия обстоятельств непреодолимой силы, возникших против воли и желания сторон, и которые нельзя было предвидеть или предотвратить.

13.2. Документ, выданный соответствующим компетентным органом, является достаточным подтверждением наличия или продолжительности действия непреодолимой силы.

13.3. Сторона, которая не исполняет своего обязательства вследствие действия непреодолимой силы, должна немедленно известить другую сторону о препятствии и его влияния на исполнение обязательств по контракту.

14. Прочие условия

14.1. Любые изменения и дополнения по контракту вступают в силу и становятся его неотъемлемыми частями, только если они совершены в письменной форме, подписаны обеими сторонами и содержат ссылку на контракт.

14.2. Стороны обязуются незамедлительно информировать друг друга о возникших затруднениях, которые могут привести к невыполнению отдельных условий контракта, для согласования и принятия необходимых мер.

14.3. Стороны обязаны извещать друг друга об изменениях своего адреса, номеров телефонов, иных реквизитов в срок не позднее 3 (трех) дней с момента начала действия таких изменений.

14.4. Поставщик не вправе без предварительного письменного согласия заказчика передавать свои права по контракту третьим лицам.

14.5. Во всем остальном, что не предусмотрено контрактом, стороны руководствуются действующим законодательством РФ.

14.6. Настоящий Контракт заключается в форме электронного документа и подписывается Сторонами настоящего контракта усиленной электронной подписью.

ИСПОЛНИТЕЛЬ:

15. Адреса и реквизиты сторон

ЗАКАЗЧИК:

ФГБУЗ МСЧ № 92 ФМБА России

456320 г. Миасс, пр. Макеева, 21

ИНН 7415017660 КПП 741501001

456320 г. Миасс, пр. Макеева, 21

ИНН 7415017660 КПП 741501001

**УФК по Новосибирской области (ФГБУЗ МСЧ № 92
ФМБА России, л/с 20696Ц21050)**

Казначейский счет 032 146 430 000 000 15115

Единый казначейский счет 401 028 104 453 700 000 43

**ОКЦ № 1 СибГУ Банка России/УФК по Новосибирской
области г. Новосибирск**

БИК 015 004 950

Тел./факс: 8/3513/54-51-32

e-mail: 545132@mail.ru

Начальник _____ Селиванов А.В.

Спецификация **

№ п/п	Наименование услуг	Ед. измерения	Общее количество	Цена	НДС %	Цена с НДС	Сумма НДС	Стоимость	Страна происхождения
1	Продление лицензии антивирусной защиты (рабочие станции / файловые сервера/почтовые сервера/интернет-шлюзы) Kaspersky Total Security для бизнеса.	шт	65						

**Заполняется по итогам аукциона

Итого: _____ руб. (_____ руб. _____ коп.), в том числе НДС _____ руб. (_____ руб. _____ коп.)/НДС не предусмотрен

Заказчик _____ Исполнитель _____ (_____)

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

В связи с тем, что, ЗАКАЗЧИКОМ В НАСТОЯЩЕЕ ВРЕМЯ ИСПОЛЬЗУЕТСЯ АНТИВИРУСНАЯ ЗАЩИТА Kaspersky Total Security для бизнеса., в соответствии с п.1 ч.1 ст. 33 ФЗ № 44-ФЗ в описании объекта закупки содержится **КОНКРЕТНОЕ НАИМЕНОВАНИЕ П.О. с целью НЕЦЕЛЕСООБРАЗНОСТИ И НЕЭФФЕКТИВНОСТИ ПЕРЕУСТАНОВКИ НА ВСЕХ РАБОЧИХ СТАНЦИЯХ ЗАКАЗЧИКА.**

Антивирусное программное обеспечение должно предоставлять Заказчику защиту информации корпоративной сети не менее, чем на **12** месяцев на **65** защищаемых объектов. Лицензирование количества компонентов защиты рабочих станций и файловых серверов должно быть универсальным и ограничиваться только общим количеством защищаемых объектов. Антивирусное программное обеспечение должно производить шифрование данных, включать модуль системного администрирования, защиты почтовых серверов и защиты интернет-шлюзов.

№ п/п	Наименование	Единица измерения	Количество
1.	Продление лицензии антивирусной защиты (рабочие станции / файловые сервера/почтовые сервера/интернет-шлюзы) Kaspersky Total Security для бизнеса.	шт.	65

Общие требования

Общие требования

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 серверов масштаба предприятия и терминальных серверов Windows.
- » программные средства антивирусной защиты для мобильных устройств (смартфонов и планшетов);
- » программные средства антивирусной защиты веб-трафика;
- » программные средства антивирусной защиты и фильтрации спама с помощью отдельного сервера
- » программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux;
- » программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange;
- » 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/Enterprise multi-session;
- o Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise

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

- антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
- антивирусное сканирование по расписанию;
- антивирусное сканирование подключаемых устройств;
- эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
- нейтрализации действий активного заражения;
- анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
- анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
- блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
- откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
- ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
- облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
- антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
- защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
- фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
- проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, с возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
- блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
- распознавания и блокировку фишинговых и небезопасных сайтов;
- встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
- защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
- 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 MTP устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
- записи в журнал событий о записи и/или удалении файлов на съемных дисках;
- 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;
- 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;
- установки ограничение длительности выполнения задачи;
- ставить задачи проверки в очередь, если проверка уже выполняется;
- наличие функции Анти-Бриджинг для запрета рабочей станции одновременно устанавливать сетевые соединения по разным каналам передачи информации (проводной и беспроводной) для предотвращения создания сетевых мостов;
- обновление без перезагрузки системы;
- настройки прав доступа (чтение / запись) для портативных устройств (MTP), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам;
- настроить доступ пользователей к мобильным устройствам в приложении Android Debug Bridge (ADB);
- заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;
- настроить права печати для пользователей;
- наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;
- наличие совместимости с Azure WVD;
- настроить доступ пользователей к мобильным устройствам в приложении iTunes;
- запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

- полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
- восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;
- поддержка двухфакторной аутентификации при полнодисковом шифровании;
- шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);
- наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;
- шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
- возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
- возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
- поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании;
- возможность настроить исключения и ограничить доступ ко всем Bluetooth-устройствам кроме устройств ввода;
- возможность обновления приложения без перезагрузки операционной системы;
- возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО;
- возможность запретить внешнее управление службами приложения;
- возможность выбирать предустановленные исключения из проверки и доверенные приложения.

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 Web Server 2008 R2 Service Pack 1 и выше;
- o Windows Server 2012 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
- o Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (включая режим Server Core);
- o Windows Server 2016 Essentials / Standard / Datacenter (включая режим Server Core);
- o Windows Server 2019 Essentials / Standard / Datacenter (включая режим Server Core);
- o Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая режим Server Core).
- o Windows Server 2025 Standard / Datacenter.

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;
- 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;
- создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
- формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
- запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
- поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.
- 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;
- обновление без перезагрузки системы;
- настройки прав доступа (чтение / запись) для портативных устройств (МТР), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам;

- заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;
- настроить права печати для пользователей;
- наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;
- наличие совместимости с Azure WVD;
- возможность обновления приложения без перезагрузки операционной системы;
- возможность ограничить потребление ресурсов процессора для задачи поиска вредоносного ПО.
- возможность запретить внешнее управление службами приложения.
- возможность использования предустановленных исключений из проверки и доверенных приложений, предназначенных для быстрой настройки доверенной зоны для работы приложения на SQL-серверах, Microsoft Exchange-серверах и System Center Configuration Manager.

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:

- о macOS 12 - 15;

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.
- централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault;
- 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;
- ограничивать загрузку процессора приложением при выполнении задач поиска вредоносного ПО;
- включения облачного режима и использования облегченной версии баз вредоносного ПО, для снижения нагрузки на ресурсы операционной системы;
- пропускать сканирование системного тома, доступного только для чтения, во время выполнения задач проверки по требованию;
- анализировать активность приложений в операционной системе с использованием шаблонов опасного поведения (BSS);
- установки из файла .pkg через JAMF;

- автоматическое сканирование внешних дисков при их подключении;
- поддержки клиентских сертификатов.

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 Debian GNU/Linux 11.0 и выше.
- o Debian GNU/Linux 12.0 и выше.
- o Mageia 4.
- o Альт 8 СП Рабочая Станция (8.4).
- o Альт 8 СП Сервер (8.4).

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 9.0 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.10015-01 (очередное обновление 1.8)
- o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
- o Astra Linux Special Edition РУСБ.10015-03 (очередное обновление 7.6).
- o Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7).
- o CentOS 7.2 и выше.
- o CentOS Stream 8.
- o CentOS Stream 9.
- o Debian GNU/Linux 11.0 и выше.
- o Debian GNU/Linux 12.0 и выше.
- o EMIAS 1.0 и выше.
- o EulerOS 2.0 SP10.
- o Fedora Linux 41.
- o Kylin 10.
- o Linux Mint 21.1 и выше.
- o Linux Mint 22.0 и выше.
- o Mostech 12.
- o openSUSE Leap 15.0 и выше.
- o Oracle Linux 7.3 и выше.
- o Oracle Linux 8.0 и выше.
- o Oracle Linux 9.0 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 9.0 и выше.
- o Rocky Linux 8.5 и выше.
- o Rocky Linux 9.0 и выше.
- o SberLinux 9.0.1.
- o SberOS 3.3.3.
- o SUSE Linux Enterprise Server 12.5 и выше.
- o SUSE Linux Enterprise Server 15 и выше.
- o Ubuntu 22.04 LTS.

- o Ubuntu 24.04 LTS.
- o Альт 8 СП Рабочая станция (8.4).
- o Альт 8 СП Сервер (8.4).
- o Альт Образование 10.1.
- o Альт СП Рабочая Станция релиз 10.
- o Альт СП Рабочая Станция релиз 10.1.
- o Альт СП Сервер релиз 10.
- o Альт СП Сервер релиз 10.1.
- o Атлант, сборка Alcyone, версия 2022.02.
- o Гослинукс 7.17.
- o Гослинукс 7.2.
- o М ОС 12 Сервер.
- o МОС ОС 15.4 Арбат.
- o МСВСФЕРА АРМ 9.2 и выше.
- o МСВСФЕРА СЕРВЕР 9.2 и выше.
- o ОС МЭШ 12 Для всех пользователей (без телеметрии и без поддержки ДИТ).
- o ОС МЭШ 12 Для московских школ для интерактивных панелей (с телеметрией и поддержкой ДИТ).
- o ОС МЭШ 12 Для московских школ для компьютеров и ноутбуков (с телеметрией и поддержкой ДИТ).
- o ОСнова 2.9 и выше.
- o РЕД ОС 7.3.
- o РЕД ОС 8.0.
- o РОСА "Кобальт" 7.9.
- o РОСА "Хром" 12.
- o СинтезМ-Клиент 8.6.
- o СинтезМ-Сервер 8.6.

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

- o Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
- o CentOS Stream 9.
- o EulerOS 2.0 SP10.
- o SUSE Linux Enterprise Server 15.
- o Ubuntu 22.04 LTS.
- o Альт СП Рабочая Станция релиз 10.
- o Альт СП Сервер релиз 10.
- o РЕД ОС 7.3.
- o РЕД ОС 8.0.

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 проверку 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 информации о проверенных и не измененных после проверки файлах);
- 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;
- получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
- 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;
- исключения процессов из проверки памяти процессов в общих параметрах программы;
- оптимизировать проверку журналов работы программ с помощью параметра SkipPlainTextFiles;
- исключения трафика из проверки программой;
- использовать формат JSON для запросов и вывода информации, а также для экспорта и импорта параметров программы и параметров задач;
- установки и работы на устройствах с операционными системами для архитектуры Arm;
- работать в режиме информирования пользователя в случае обнаружения угроз или при обнаружении попытки доступа к устройству;
- возможность управлять запуском приложений на защищаемых устройствах с помощью правил контроля в режимах списка запрещенных или разрешенных приложений;
- автоматический перезапуск приложения при обновлении;
- возможность задать ограничение на использование ресурсов процессора;
- возможность в автоматическом режиме выключить компоненты защиты и задачи проверки при запуске приложения после установки;
- уведомления пользователя о работе компонентов и задач в графическом пользовательском интерфейсе;
- возможность читать память процессов, не останавливая их (ядра Linux начиная с версии 3.4);
- возможность управлять доступом пользователей к веб-ресурсам;
- возможность управлять запуском приложений на защищаемых устройствах;
- функция мониторинга стабильности собственной работы приложения.

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 и выше (включая Android 12L, исключая Go Edition);
- o iOS 15 и выше или iPadOS 15 и выше;

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;
- указать разрешенные версии приложений при создании правил Контроля приложений для Android-устройств.

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.
- запретить изменение настроек Bluetooth для iOS MDM-устройств.

Требования к системе защиты веб-трафика

- Система должна поставляться в виде
 - o ISO-образа, с предустановленной операционной системой, прокси-сервером и средствами защиты и контроля трафика
 - o RPM- или DEB- пакета, содержащего дистрибутив программы для защиты и контроля трафика
- Система должна поддерживать установку и работу на следующих операционных системах:
 - o Red Hat Enterprise Linux версии 7.7, 8.
 - o Ubuntu 18.04.3 LTS.
 - o Debian 9.11, 10.1.
 - o SUSE Linux Enterprise Server 15 SP1.
 - o CentOS версии 7.7.
 - o Альт Сервер 10.
- Система должна поддерживать установку на физический и виртуальный сервер, для работы в виртуальной среде должна поддерживать установку на следующие гипервизоры:
 - o VMware ESXi 6.5 Update 3.
 - o VMware ESXi 6.7 Update 3.
 - o VMware ESXi 7.0 Update 3.

- o VMware ESXi 8.0 Update 3.
- o Microsoft Hyper-V Server 2016.
- o Microsoft Hyper-V Server 2019.
- o Windows Server 2019 Standard с установленной ролью Hyper-V.
- o Windows Server 2022 Standard с установленной ролью Hyper-V.

Система защиты веб-трафика должна обеспечивать защиту пользователей корпоративной сети при работе с веб-ресурсами: удалять вредоносные программы и другие программы, представляющие угрозу, из потока данных, поступающего в корпоративную сеть из интернета по протоколам HTTP(S) и FTP, блокировать зараженные и фишинговые веб-сайты, а также контролировать доступ к веб-ресурсам на основании категорий веб-ресурсов и типов контента и обеспечивать следующие функциональные возможности:

- выполнять антивирусную проверку объектов, передаваемых через прокси-сервер.
- лечить обнаруженные зараженные объекты и, если лечение невозможно, запрещать доступ к объекту.
- обнаруживать и лечить вирусы в любых типах файлов и вложений.
- блокировать вредоносные и фишинговые веб-сайты.
- использовать дополнительный уровень проверки на основе репутационных облачных сервисов производителя антивирусных средств защиты для обеспечения более высокой скорости реакции на угрозы, не дожидаясь обновления баз программы, а также снижения вероятности ложных срабатываний.
- осуществлять контроль и защиту SSL-шифрованного сетевого трафика при замене сертификата на стороне встроенного или внешнего прокси-сервера.
- настраивать правила доступа и защиты на основании следующих критериев:
 - o Категория веб-сайта
 - o URL ресурса
 - o Имя файла
 - o Тип файла
 - o Размер файла
 - o MIME-тип
 - o Хеш-сумма файла (MD5, SHA256)
 - o Направление трафика
 - o HTTP-метод
 - o HTTP Content-Length
 - o LDAP-запись
 - o User-agent
 - o IP-адрес или маска подсети
- настраивать приоритет выполнения прав доступа и защиты
- выполнять контроль доступа пользователей к Интернет-ресурсам на основании категорий веб-сайтов и типов контента, определенных производителем средства защиты.
- поддержка в качестве фильтра URL-адресов масок и регулярных выражений.
- осуществлять контроль использования пользователями только определенного типа веб-обозревателя (блокирование запрещенных в управляемых организациях браузер-клиентов).
- осуществлять настройку временного расписания правил контроля доступа пользователей к Интернет-ресурсам.
- интегрироваться с Microsoft Active Directory для назначения ролей пользователям управляющей консоли.
- обеспечивать возможность интеграции с несколькими доменами Microsoft Active Directory.
- обеспечивать поддержку NTLM- и Kerberos-аутентификации для службы единого входа (Single Sign-On).
- осуществлять поддержку рабочих областей для выделенных групп на основании сетевых адресов, масок подсетей, LDAP-записей.
- настраивать индивидуальные правила обработки и проверки трафика для рабочих областей, а также права доступа для администраторов этих организаций.
- возможность настраивать внешний вид страницы блокировки отдельно для каждой рабочей области
- настраивать вид веб-страницы, информирующей пользователя о блокировке Интернет-ресурса.
- вести статистику работы, включающую в себя помимо прочего информацию о выполнении и результатах антивирусной проверки, ошибках в работе приложения и предупреждениях.
- позволять экспортировать журналы событий программы в формат CSV.
- расследовать инциденты доступа в интернет с помощью поиска и просмотра событий.
- карточка события помимо прочего должна включать в себя:
 - o URL
 - o протокол

- o домен
- o результат детектирования технологиями защиты
- o время наступления события
- o имя пользователя
- o User Agent пользователя
- o IP-адрес пользователя
- o категорию, к которой относится веб-ресурс
- публиковать события программы в систему корреляции событий (SIEM) по протоколу Syslog. При этом информация о каждом событии должна передаваться как отдельное syslog-сообщение в формате CEF.
- обеспечивать возможность сбора диагностической информации о программе через веб-интерфейс
- настраивать параметры программы и управлять программой через веб-интерфейс
- поддерживать возможность импортировать и экспортировать значения параметров программы
- получать статистику работы программы по протоколу SNMP, включать и отключать отправку SNMP-ловушек
- осуществлять мониторинг состояния работы программы, сетевого трафика, обрабатываемого программой, количества проверенных и обнаруженных объектов, последних и наиболее часто встречающихся угроз, заблокированных пользователей и URL-адресов через web-интерфейс программы
- обновлять антивирусные базы, как с сайта компании – производителя (по защищенному и незащищенному http-протоколу), так и из настраиваемых ресурсов (HTTP- и FTP-серверов) по расписанию или по требованию.
- настраивать параметры прокси-сервера через веб-интерфейс программы (при развертывании из iso-файла)
- возможность группировать созданные правила доступа и защиты
- создавать правила обхода для веб-ресурсов, не требующих обработки механизмами защиты и контроля доступа
- возможность задать правила защиты по умолчанию
- возможности управления встроенным прокси-сервером через веб интерфейс программы
- подключение доверенных балансировщиков нагрузки с поддержкой заголовков PROXY protocol и HTTP Forwarded
- аутентификация пользователей на прокси сервере с использованием Kerberos и NTLM
- возможность осуществлять дешифрацию HTTPS трафика с использованием самоподписанного или корпоративного сертификата
- возможность создавать правила дешифрации трафика, в том числе для исключения ресурсов по IP и доменным именам из правил дешифрации
- возможность добавления отпечатков доверенных сертификатов в хранилище системы
- возможность управления форматом хранения журнала работы прокси-сервера
- возможность кластеризации решения
- возможность централизованного управления и мониторинга серверов системы, собранных в кластер
- должна поддерживаться возможность интеграции с системами типа «песочница» для отправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования
- возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF.

Требования к программным средствам антивирусной защиты и фильтрации спама с помощью отдельного сервера

Система должна поставляться в виде:

- o ISO-образа, с предустановленной операционной системой, почтовым-сервером и средствами защиты почтового трафика
- o виртуального почтового шлюза (OVA-шаблона) с предустановленной операционной системой, почтовым-сервером и средствами защиты почтового трафика

Система должна поддерживать установку на физический и виртуальный сервер, для работы в виртуальной среде должна поддерживать установку на следующие гипервизоры:

- o VMware ESXi 7.0 Update 3.

- o VMware ESXi 8.0 Update 3.
- o Microsoft Hyper-V Server 2019.
- o Windows Server 2019 Standard с установленной ролью Hyper-V.
- o Windows Server 2022 Standard с установленной ролью Hyper-V.
- o РЕД Виртуализация 7.3.0.
- o ПК СВ "Брест" 3.3.1 (для РЕД ОС).

Программные средства антивирусной защиты и фильтрации спама должны обеспечивать реализацию следующих функциональных возможностей:

- поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
- проверка входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговых рассылок), удаление выявленных сообщений, помещение копии сообщений в карантин;
- наличие общего карантина сообщений;
- управление карантинном из веб-интерфейса;
- детектирование вредоносных и фишинговых ссылок в теле письма;
- наличие эвристических методов детектирования;
- возможность использования репутационных облачных сервисов;
- возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
- наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
- обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов, блокировать отдельные файлы внутри архивов;
- выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений, определять формат и тип вложения, независимо от его расширения, удалять сообщения, содержащие вложения определенного формата или с определенным именем или сообщения, размер которых превышает допустимый, помещать копии сообщений в хранилище;
- сохранять резервные копии сообщений в карантине по результатам их обработки модулями защиты;
- сохранять сообщения из карантина в файл и пересылать сообщения получателям;
- возможность развертывания кластерной архитектуры почтовых серверов с возможностью централизованного управления для масштабирования решения (как горизонтально, так и вертикально);
- интеграции со службами каталогов Active Directory и Open LDAP.
- возможность отправки ловушек по протоколу SNMP;
- обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей;
- отправлять уведомления пользователям о результатах проверки их сообщений модулями программы;
- поддерживать работу персонального карантина на основе LDAP-записей;
- доступ к персональному карантину должен осуществляться на основе учетных записей LDAP;
- отправлять уведомления пользователям о состоянии персонального карантина, уведомления должны содержать список последних сообщений в карантине;
- настройки расписания отправки уведомлений;
- возможность почтовой рассылки с информацией о последних полученных письмах, помещенных в персональное хранилище пользователя.
- обновлять базы программы с серверов обновлений и пользовательских ресурсов (HTTP- и FTP-серверов) по расписанию и по требованию;
- отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования;
- осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC;
- возможность для каждого статуса проверок SPF и DMARC задать отдельное действие над сообщением и настроить уведомления по результатам каждой проверки;

- осуществлять проверку подлинности отправителей сообщений с помощью технологии сопоставления доменов отправителя;
- возможность публиковать события, происходящие во время работы приложения, в SIEM-систему по протоколу Syslog.
- подписывать исходящие сообщения электронной почты с помощью технологии DKIM;
- добавлять предупреждения о небезопасном вложении к входящим сообщениям в теме письма;
- просматривать журнал событий, аудита в веб интерфейсе программы и загружать его на жесткий диск;
- фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
- проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
- проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
- выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
- перенос в карантин зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка;
- использование регулярных выражений при создании правил фильтрации;
- в правилах фильтрации сообщений электронной почты указывать пользователей и группы пользователей из Microsoft Active Directory и generic LDAP;
- наличие встроенных ролей администратора и специалиста поддержки;
- возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем зараженные и подозрительные объекты;
- управление работой программы должно осуществляться как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Mozilla Firefox версии 127.0.2. или выше, Google Chrome версии 129.0.6668 или выше, Microsoft Edge версии 129.0.2792 или выше;
- должна поддерживаться возможность интеграции с системами типа «песочница» для отправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования;
- возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF;
- обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга считать сообщение спамом.
- возможность управления маршрутизацией почтового трафика через веб-интерфейс;
- осуществлять быструю настройку MTA с помощью мастера быстрой настройки;
- настраивать режимы TLS-шифрования сообщений для ситуаций, когда система принимает сообщения от другого сервера (действует как Сервер) или пересылает сообщения на другой сервер (действует как Клиент), а также настраивать параметры TLS для отдельных доменов.

Требования к программным средствам антивирусной защиты и фильтрации спама для почтовых серверов, установленных на операционную систему семейства Linux

Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать на компьютерах, работающих под управлением 64-битных операционных систем следующих версий:

- o CentOS 6.9.
- o CentOS 7.4.
- o Red Hat Enterprise Linux 7.4.
- o Ubuntu Server 14.04.5 LTS.
- o Ubuntu Server 16.04.4 LTS.
- o Debian GNU / Linux 9.3.
- o FreeBSD 11.1.
- o Astra Linux SE 1.5. Только при отключенном механизме мандатного разграничения доступа и отключенном механизме создания замкнутой программной среды.

- o Astra Linux SE 1.6. Только при отключенном механизме мандатного разграничения доступа и отключенном механизме создания замкнутой программной среды.
- o Alt Linux 7.0.5.
- o Rocky Linux 8.7.

Программные средства антивирусной защиты и фильтрации спама для почтовых серверов Linux должны функционировать совместно с почтовыми системами следующих версий:

- o Exim-4.86 до 4.92.
- o Postfix-2.6 и выше.
- o Sendmail-8.14 и выше.
- o Qmail-1.03 и выше.

Программные средства антивирусной защиты и фильтрации спама должны обеспечивать реализацию следующих функциональных возможностей:

- поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
- проверка входящего потока почтовых сообщений на наличие спама, потенциального спама, массовых рассылок (в том числе маркетинговых рассылок), удаление выявленных сообщений, помещение копии сообщений в карантин;
- наличие общего карантина сообщений;
- управление карантинном из веб-интерфейса;
- детектирование вредоносных и фишинговых ссылок в теле письма;
- наличие эвристических методов детектирования;
- возможность использования репутационных облачных сервисов;
- возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
- наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
- обнаруживать, блокировать и лечить зараженные почтовые сообщения и зараженные вложения, удалять сообщения и вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие макросы во вложении (например, файлы форматов Microsoft Office с макросами), удалять сообщения или вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие зашифрованные объекты, удалять сообщения или вложения, помещать копии сообщений в карантин;
- обнаруживать и блокировать сообщения, содержащие архивы, распознавать типы файлов внутри архивов, блокировать отдельные файлы внутри архивов;
- выполнять контентную фильтрацию сообщений по имени, размеру и типу вложений, определять формат и тип вложения, независимо от его расширения, удалять сообщения, содержащие вложения определенного формата или с определенным именем или сообщения, размер которых превышает допустимый, помещать копии сообщений в хранилище;
- сохранять резервные копии сообщений в карантине по результатам их обработки модулями защиты;
- сохранять сообщения из карантина в файл и пересылать сообщения получателям;
- интеграции со службами каталогов Active Directory и Open LDAP;
- возможность отправки ловушек по протоколу SNMP;
- обрабатывать почтовые сообщения согласно правилам, заданным для групп отправителей и получателей;
- отправлять уведомления пользователям о результатах проверки их сообщений модулями программы;
- поддерживать работу персонального карантина на основе LDAP-записей;
- доступ к персональному карантину должен осуществляться на основе учетных записей LDAP;
- отправлять уведомления пользователям о состоянии персонального карантина, уведомления должны содержать список последних сообщений в карантине;
- настройки расписания отправки уведомлений;
- обновлять базы программы с серверов обновлений "Лаборатории Касперского" и пользовательских ресурсов (HTTP- и FTP-серверов) по расписанию и по требованию;
- отправлять и получать сообщения по защищенному каналу TLS/SSL, осуществлять управление ключами шифрования;
- осуществлять проверку подлинности отправителей сообщений с помощью технологий SPF, DKIM и DMARC;
- добавлять предупреждения о небезопасном вложении к входящим сообщениям в тему письма;
- просматривать журнал событий, аудита в веб интерфейсе программы;

- фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
- проверка с помощью сервиса SPAM URI Realtime Blocklists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
- проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
- выявление подозрительных, поврежденных и защищенных паролем файлов, а также файлов, в результате проверки которых произошла ошибка;
- перенос в карантин зараженных, подозрительных и поврежденных объектов почтового трафика, определять защищенные паролем файлы, а также файлы, в результате проверки которых произошла ошибка;
- использование регулярных выражений при создании правил фильтрации;
- в правилах фильтрации сообщений электронной почты указывать пользователей и группы пользователей из Microsoft Active Directory и generic LDAP;
- наличие встроенных ролей администратора и специалиста поддержки;
- возможность уведомления отправителя, получателя и администратора сервера о почтовом сообщении, содержащем зараженные и подозрительные объекты;
- управление работой программы должно осуществляться как стандартными средствами операционной системы с помощью командной строки, так и через специальный веб-интерфейс, работающий на браузерах: Internet Explorer, Mozilla Firefox, Google Chrome;
- должна поддерживаться возможность интеграции с системами типа «песочница» для отправки файлов, полученных системой защиты веб-трафика для анализа, а также для получения результатов сканирования
- возможность формировать отчеты за выбранный период (сутки, неделя, месяц, год) в формате PDF;
- обнаруживать сообщения с Юникод-спуфингом. В случае обнаружения Юникод-спуфинга считает сообщение спамом.

Требования к программным средствам антивирусной защиты и фильтрации спама для серверов Microsoft Exchange

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- o Microsoft Windows Server 2022 Standard или Datacenter;
- o Microsoft Windows Server 2019 Standard или Datacenter;
- o Microsoft Windows Server 2016 Standard или Datacenter.

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны функционировать с программным обеспечением Microsoft Exchange Server следующих версий:

- o Microsoft Exchange Server 2019, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
- o Microsoft Exchange Server 2016, развернутый как минимум в одной из следующих ролей: Почтовый ящик или Пограничный транспорт.
- o Microsoft Exchange Server 2013 SP1, развернутый как минимум в одной из следующих ролей: Почтовый ящик, Пограничный транспорт или Сервер клиентского доступа (CAS).

Консоль управления программными средствами антивирусной защиты для серверов Microsoft Exchange должна быть реализована с использованием Microsoft Management Console и должна функционировать на компьютерах, работающих под управлением операционных систем следующих версий:

- o Microsoft Windows Server 2022 Standard или Datacenter;
- o Microsoft Windows Server 2019 Standard или Datacenter;
- o Microsoft Windows Server 2016 Standard или Datacenter;
- o Операционные системы Microsoft Windows Server в режиме Core.
- o Microsoft Windows 11 (x64);
- o Microsoft Windows 10 (x64).

Для установки любого компонента программы (Сервера безопасности или Консоли управления) требуется пакет обновлений Microsoft Windows KB2999226.

Программные средства антивирусной защиты и фильтрации спама для серверов Microsoft Exchange должны обеспечивать реализацию следующих функциональных возможностей:

- совместимость с DAG в Microsoft Exchange;
- поиск и удаление по требованию всех типов вирусов, червей, троянских и других вредоносных программ в потоке входящих и исходящих почтовых сообщений, включая вложения;
- поиск и удаление в режиме реального времени всех типов вирусов, червей, троянских и других вредоносных программ в хранящихся на сервере Microsoft Exchange (в том числе в общих папках) сообщениях, включая вложения;
- наличие эвристических методов детектирования;
- проверка почтовых хранилищ и общих папок на сервере, в фоновом режиме для гарантированной обработки всех объектов с использованием самой актуальной версии антивирусных баз без заметного увеличения нагрузки на сервер;
- возможность лечить зараженные архивы;
- возможность выявления и удаления не только однозначно вредоносных, но и потенциально опасных приложений, таких как: рекламные программы, программы-сборщики информации, программы автоматического дозвона на платные сайты и другие утилиты, которые могут использоваться злоумышленниками в своих целях;
- возможность детектирования вредоносных и фишинговых ссылок в теле письма;
- сохранение копий изменяемых сообщений в резервном хранилище, что позволяет восстановить важную информацию в случае некорректного лечения объекта;
- набор параметров поиска для удобства нахождения объекта в резервном хранилище;
- дополнительный уровень проверки с помощью репутационных облачных сервисов;
- возможность интеграции с приватным репутационным сервисом, который позволяет осуществлять проверку, не отправляя данные за пределы организации;
- наличие компонента защиты, позволяющего распаковывать и анализировать составные файлы на предмет аномалий для блокировки угроз;
- возможность проверять текст в сообщениях и в темах сообщений электронной почты на наличие запрещенных слов.
- проверка различных параметров письма, таких как адреса отправителей и получателей, размер письма, а также поля заголовка сообщения;
- защита от спуфинга (подделка адреса отправителя с целью сокрытия истинного автора сообщения электронной почты).
- фильтрация или исключение из фильтрации сообщения по адресу отправителя письма (e-mail и/или IP-адрес) на основе собственных «черных» и «белых» списков;
- проверка наличия IP-адреса отправителя в списках DNS-based realtime blackhole list (DNSBL);
- проверка IP-адреса отправителя на соответствие списку разрешенных адресов для домена с помощью технологии Sender Policy Framework (SPF);
- проверка с помощью сервиса SPAM URI Realtime Block lists (SURBL) адресов и ссылок на сайты, присутствующих в теле письма;
- использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и файлов вложений);
- возможность использовать роли пользователей/администраторов для разграничения доступа к настройкам безопасности;
- аудит изменения параметров программы по событиям в журнале событий Windows;
- мониторинг состояния программы, получение статистики работы программы и управление белыми и черными списками адресов Анти-Спама с помощью команд в среде Windows PowerShell;
- использование контентной фильтрации (анализ содержимого самого письма, включая заголовок Subject и имён файлов);
- возможность фильтрации файлов Microsoft Office, содержащих макросы;
- возможность проверки и удаления сообщений, являющихся спамом или содержащих фишинговые и вредоносные ссылки;
- проверка графических вложений на совпадение с известными сигнатурами спам-сообщений;
- создание отчетов по работе системы защиты;
- возможность автоматической рассылки отчетов администраторам по расписанию;
- возможность обновления антивирусных баз как с сайтов производителя, так и с внутренних сетевых ресурсов организации;

- возможность фоновой проверки почтовых ящиков и общих папок с использованием Exchange Web Services;
- детальные отчеты в формате HTML;
- наличие возможности отправки отчетов и уведомлений на указанные адреса электронной почты;
- мониторинг работы программы с помощью System Center - Operations Manager;
- интеграция с Active Directory;
- централизованный просмотр состояния защиты;
- возможность распределять роли администраторов системы.

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 Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64-разрядная.
- o Windows Server 2016 Standard/Datacenter/Essentials/Server Core (варианты установки) (LTSC) 64-разрядная.
- o Windows Server 2019 Standard/Datacenter/Core 64-разрядная.
- o Windows Server 2022 Standard/Datacenter/Core 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 Citrix XenServer 7.1 LTSR.
- o Citrix XenServer 8.x.
- o Parallels Desktop 18.
- o Oracle VM VirtualBox 7.x.

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

- o Microsoft SQL Server 2016 (все редакции) 64-разрядная.
- o Microsoft SQL Server 2017 (все редакции) для Windows/Linux 64-разрядная.
- o Microsoft SQL Server 2019 (все редакции) для Windows/Linux 64-разрядная (требуется дополнительные действия).
- o Microsoft SQL Server 2022 (все редакции) для Windows/Linux 64-разрядная.
- o MySQL 5.7 Community 32-разрядная/64-разрядная.
- o MySQL 8.0 Community 32-разрядная/64-разрядная.
- o MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
- o MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- o PostgreSQL 13.x 64-разрядная.
- o PostgreSQL 14.x 64-разрядная.
- o PostgreSQL 15.x 64-разрядная.
- o Postgres Pro 13.x Windows/Linux 64-разрядная.
- o Postgres Pro 14.x Windows/Linux 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 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 карантин 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;

- возможность управления развертыванием ОС Windows через консоль управления;
- наличие преднастроенных ролей пользователей средств централизованного управления;
- должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
- возможность подключения по RDP или штатными средствами из консоли управления;
- наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing);
- пользователю должен выводиться запрос на разрешение дистанционного подключения;
- наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal);
- должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
- возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС;
- возможность импортировать образ операционной системы из дистрибутивов (WIM)
- наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;
- автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры;
- поддержка функциональности управления шифрованием данных;
- возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\LEEF
- 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.
- автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
- возможность развернуть Сервер администрирования как систему высокой доступности;
- возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети;
- удаленная диагностика клиентских устройств на базе Windows и Linux (получение трассировок, журналов событий, дампов, остановка и запуск приложений);
- возможность отозвать права локального администратора учетных записей на управляемых устройствах с операционной системой Linux;
- возможность изменить пароль локальной учетной записи на управляемых устройствах с операционной системой Linux.

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.x (Bullseye) 64-разрядная.
- o Debian GNU/Linux 12 (Bookworm) 64-разрядная.
- o Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
- o Ubuntu Server 24.04 LTS (Noble Numbat) 64-разрядная.
- o CentOS Stream 9 64-разрядная.
- o Red Hat Enterprise Linux Server 7.x 64-разрядная.
- o Red Hat Enterprise Linux Server 8.x 64-разрядная.
- o Red Hat Enterprise Linux Server 9.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 РУСБ.10015-01 (очередное обновление 1.6) 64-разрядная.
- o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7) 64-разрядная.
- o Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8) 64-разрядная.

- o Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6) 64-разрядная.
- o Astra Linux Special Edition РУСБ.10015-17 (очередное обновление 1.7.3) 64-разрядная.
- o Astra Linux Special Edition РУСБ.10015-03 (обновление 7.6) 64-разрядная.
- o Astra Linux Special Edition РУСБ.10015-37 (очередное обновление 7.7) 64-разрядная.
- o Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
- o Альт СП Сервер 10 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 Альт СП Рабочая станция 10 64-разрядная.
- o Oracle Linux 7 64-разрядная.
- o Oracle Linux 8 64-разрядная.
- o Oracle Linux 9 64-разрядная.
- o Platform V SberLinux OS Server (SLO) 8.9.2 64-разрядная.
- o РЕД ОС 7.3 Сервер 64-разрядная.
- o РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.
- o РЕД ОС 8 64-разрядная.
- o РОСА "КОБАЛЬТ" 7.9 64-разрядная.
- o МОС (Moscow Electronic School) 12 Сервер 64-разрядная.
- o Mostech Server 64-разрядная.
- o МосОС 15.4 Arbat 64-разрядная.

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

- o VMware vSphere 6.7.0.
- o VMware vSphere 7.0.3.
- o Citrix XenServer 7.x.
- o Citrix XenServer 8.2.
- o Parallels Desktop 18.
- o Oracle VM VirtualBox 7.0.12.
- o Kernel-based Virtual Machine (все поддерживаемые ОС Linux).

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

- 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 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
- o MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
- o MariaDB 10.4 (сборка 10.4.20 и выше) 32-разрядная/64-разрядная.
- o MariaDB 10.5 (сборка 10.5.27 и выше) 32-разрядная/64-разрядная.
- o MariaDB 10.6 (сборка 10.6.20 и выше) 32-разрядная/64-разрядная.
- o MariaDB 10.11 (сборка 10.11.10 и выше) 32-разрядная/64-разрядная.
- o MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
- o PostgreSQL 13.x 64-разрядная.
- o PostgreSQL 14.x 64-разрядная.
- o PostgreSQL 15.x 64-разрядная.
- o PostgreSQL 15.x 64-разрядная (кластер Corosync/Pacemaker).
- o PostgreSQL 16.x 64-разрядная.
- o PostgreSQL 17 64-разрядная.
- o Postgres Pro 13.x (все редакции) 64-разрядная.
- o Postgres Pro 14.x (все редакции) 64-разрядная.
- o Postgres Pro 15.x (все редакции) 64-разрядная.
- o Postgres Pro 15.x 64-разрядная (кластер Corosync/Pacemaker).
- o Postgres Pro 16.x (все редакции) 64-разрядная.

- o Postgres Pro 16.x Enterprise 64-разрядная (кластер Built-in High Availability).
- o Postgres Pro 17 (все редакции) 64-разрядная.
- o Postgres Pro 17 Enterprise 64-разрядная (кластер Built-in High Availability).
- o Platform V Pangolin 5.4.0 64-разрядная.
- o Jato 4 64-разрядная.

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

- централизованная 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 предустановленных стандартных отчетов о работе системы;
- экспорт отчетов в файлы форматов PDF и XML;
- централизованное управление объектами резервных хранилищ и карантинных 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;
- выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных;
- экспорт и импорт выборок событий;
- получение информации о программах, установленных на управляемые устройства;
- возможность поиска устройств по контроллерам доменов Microsoft Active Directory и Samba;
- возможность автоматизированного переноса данных с сервера администрирования под управлением ОС Windows на сервер администрирования под управлением ОС Linux;
- возможность удаленной диагностики управляемых устройств;
- поддержка кластерной технологии;
- возможность централизованного удаления несовместимого ПО с управляемых устройств;
- возможность централизованной перезагрузки управляемых устройств.

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, посвященный технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.