**УТВЕРЖДАЮ:**

Заместитель директора

по материально-техническому

обеспечению МУП «Водоканал»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Синяев

« » \_\_\_\_\_\_\_\_\_\_\_\_\_ 2025г.

**ДОКУМЕНТАЦИЯ АУКЦИОНА В ЭЛЕКТРОННОЙ ФОРМЕ,**

**УЧАСТНИКАМИ КОТОРОГО МОГУТ БЫТЬ ТОЛЬКО**

**СУБЪЕКТЫ МАЛОГО И СРЕДНЕГО ПРЕДПРИНИМАТЕЛЬСТВА**

**НА ОКАЗАНИЕ УСЛУГ ПО ПРОДЛЕНИЮ НЕИСКЛЮЧИТЕЛЬНЫХ (ЛИЦЕНЗИОННЫХ) ПРАВ ИСПОЛЬЗОВАНИЯ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

г. Йошкар-Ола

2025 г.

**СОДЕРЖАНИЕ**

**РАЗДЕЛ I. ОБЩИЕ УСЛОВИЯ ПРОВЕДЕНИЯ АУКЦИОНА В ЭЛЕКТРОННОЙ ФОРМЕ**

**РАЗДЕЛ II. ИНФОРМАЦИОННАЯ КАРТА АУКЦИОНА В ЭЛЕКТРОННОЙ**

**ФОРМЕ**

**РАЗДЕЛ III. ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**РАЗДЕЛ IV. ПРОЕКТ ДОГОВОРА**

**РАЗДЕЛ V. СВЕДЕНИЯ О НАЧАЛЬНОЙ (МАКСИМАЛЬНОЙ) ЦЕНЕ ЕДИНИЦЫ КАЖДОГО ТОВАРА, РАБОТЫ, УСЛУГИ**

**РАЗДЕЛ VI. ИНСТРУКЦИЯ ПО ЗАПОЛНЕНИЮ ЗАЯВОК НА УЧАСТИЕ В ЭЛЕКТРОННОМ АУКЦИОНЕ**

**РАЗДЕЛ I. ОБЩИЕ УСЛОВИЯ ПРОВЕДЕНИЯ АУКЦИОНА В ЭЛЕКТРОННОЙ ФОРМЕ**

**1. Общие положения**

**1.1. Публикация извещения и документации об аукционе в электронной форме на электронной торговой площадке**

1.1.1. Настоящая документация аукциона в электронной форме, участниками которого могут быть только субъекты малого и среднего предпринимательства подготовлена и разработана в соответствии с Федеральным законом от 18.07.2011 N 223-ФЗ "О закупках товаров, работ, услуг отдельными видами юридических лиц" (далее – Федеральный закон от 18.07.2011 N 223-ФЗ), Гражданским кодексом Российской Федерации, Федеральным законом от 26.07.2006 № 135-ФЗ "О защите конкуренции", Положением о закупке товаров, работ, услуг Муниципального унитарного предприятия «Водоканал» г.Йошкар-Олы» муниципального образования «Город Йошкар-Ола» (далее – Положение о закупках).

1.1.2. Проведение конкурентной закупки с участием субъектов малого и среднего предпринимательства осуществляется Заказчиком на электронной площадке, функционирующей в соответствии с едиными требованиями, предусмотренными Федеральным законом от 5 апреля 2013 года N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», и дополнительными требованиями, установленными Правительством Российской Федерации и предусматривающими:

1) требования к проведению такой конкурентной закупки в соответствии с Федеральным законом от 18.07.2011 N 223-ФЗ;

2) порядок и случаи блокирования денежных средств, внесённых участниками такой конкурентной закупки в целях обеспечения заявок на участие в такой конкурентной закупке, и прекращения данного блокирования (если требование об обеспечении заявок на участие в такой закупке установлено Заказчиком в извещении об осуществлении такой закупки, документации о конкурентной закупке);

3) порядок использования государственной информационной системы, осуществляющей фиксацию юридически значимых действий, бездействия в единой информационной системе, на электронной площадке при проведении такой закупки;

4) порядок утраты юридическим лицом статуса оператора электронной площадки для целей Федерального закона от 18.07.2011 N 223-ФЗ.

1.1.3. Публикация извещения и документации аукциона в электронной форме, участниками которого могут быть только субъекты малого и среднего предпринимательства (далее – документация о закупке, документация об аукционе в электронной форме) осуществляется на электронной торговой площадке (далее – ЭТП) http://www.rts-tender.ru (ООО «"РТС-тендер" – Электронная торговая площадка»), в единой информационной системе (далее также – ЕИС) (www.zakupki.gov.ru), на официальном сайте в соответствии с Федеральным законом от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

1.1.4. Извещение о проведении аукциона в электронной форме, участниками которого могут быть только субъекты малого и среднего предпринимательства (далее - Извещение о закупке, извещение об аукционе в электронной форме, извещение о проведении электронного аукциона) размещается заказчиком на электронной торговой площадке не менее чем за 7 (семь) календарных дней до даты окончания подачи заявок на участие в электронном аукционе.

1.1.5. Заказчик может внести изменения в извещение о проведении электронного аукциона.

1.1.6. Заказчик может отказаться от проведения электронного аукциона.

1.1.7. Заказчик несет ответственность за достоверность сведений, указанных в извещении и документации о закупке.

1.1.8. Участник закупки вправе подать заявку на участие в электронном аукционе в любой момент с момента размещения на сайте электронной площадки извещения о проведении электронного аукциона до предусмотренных документацией о закупке даты и времени окончания срока подачи заявок на участие в электронном аукционе.

1.1.9 Участнику аукциона в электронной форме (далее — электронный аукцион) для участия в аукционе в электронной форме необходимо получить аккредитацию на электронной площадке в порядке, установленном оператором электронной площадки.

1.1.10. Обмен между участником электронного аукциона, Заказчиком и оператором электронной площадки информацией, связанной с получением аккредитации на электронной площадке, осуществлением электронного аукциона, осуществляется на электронной площадке в форме электронных документов.

1.1.11. Электронные документы участника электронного аукциона, Заказчика, оператора электронной площадки должны быть подписаны усиленной квалифицированной электронной подписью (далее — электронная подпись) лица, имеющего право действовать от имени, соответственно, участника такого аукциона в электронной форме, Заказчика, оператора электронной площадки.

**1.2. Предоставление национального режима при осуществлении закупок**

1.2.1. В соответствии со статьей 3.1-4 Закона № 223-ФЗ при осуществлении закупок Заказчик предоставляет национальный режим, обеспечивающий происходящему из иностранного государства или группы иностранных государств (далее - иностранное государство) товару, работе, услуге, соответственно выполняемой, оказываемой иностранным гражданином или иностранным юридическим лицом (далее - иностранное лицо), равные условия с товаром российского происхождения, работой, услугой, соответственно выполняемой, оказываемой российским гражданином или российским юридическим лицом (далее - российское лицо), за исключением мер, принятых Правительством Российской Федерации в виде постановления Правительства РФ от 23.12.2024 № 1875 (далее – Постановление № 1875).

Если иное не предусмотрено мерами, принятыми Правительством Российской Федерации в соответствии с пунктом 1 части 2 статьи 3.1-4 Закона № 223-ФЗ, положения статьи 3.1-4 Закона № 223-ФЗ, касающиеся товара российского происхождения, работы, услуги, соответственно выполняемой, оказываемой российским лицом, применяются также в отношении товара, происходящего из иностранного государства, работы, услуги, соответственно выполняемой, оказываемой иностранным лицом, которым предоставляются равные условия с товаром российского происхождения, работой, услугой, соответственно выполняемой, оказываемой российским лицом.

1.2.2. При закупке товаров:

1.2.2.1. Если Правительством Российской Федерации установлен запрет закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, не допускаются:

• заключение договора на поставку такого товара;

• при исполнении договора замена такого товара на происходящий из иностранного государства товар, в отношении которого установлен данный запрет;

1.2.2.2. Если Правительством Российской Федерации установлено ограничение закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, не допускаются:

• заключение договора на поставку товара, происходящего из иностранного государства, если поданы заявка на участие в закупке, окончательное предложение, признанные по результатам их рассмотрения соответствующими требованиям положения о закупке, извещения и документации о конкурентной закупке (в случае проведения конкурентной закупки) и содержащие предложения о поставке товара российского происхождения;

• при исполнении договора замена товара на происходящий из иностранного государства товар, в отношении которого установлено данное ограничение, если договор предусматривает поставку товара российского происхождения;

1.2.2.3. Если Правительством Российской Федерации установлено преимущество в отношении товаров российского происхождения (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг):

• при рассмотрении, оценке, сопоставлении заявок на участие в закупке, окончательных предложений осуществляется снижение на 15 процентов ценового предложения, поданного участником закупки, предлагающим к поставке товар только российского происхождения, либо увеличение на 15 процентов ценового предложения этого участника закупки в случае подачи им предложения о размере платы, подлежащей внесению за заключение договора. Договор с участником закупки заключается без учета снижения либо увеличения ценового предложения;

• при исполнении договора допускается замена товара исключительно на товар российского происхождения, если договор предусматривает поставку товара российского происхождения.

1.2.3. При закупке работы, услуги:

1.2.3.1. Если Правительством Российской Федерации установлен запрет закупки работ, услуг, соответственно выполняемых, оказываемых иностранными лицами, не допускаются:

• заключение договора на выполнение такой работы, оказание такой услуги с подрядчиком (исполнителем), являющимся иностранным лицом;

• перемена подрядчика (исполнителя) (в случае, если эта перемена допускается гражданским законодательством), с которым заключен указанный договор, на иностранное лицо, которое зарегистрировано на территории иностранного государства, в отношении которого установлен данный запрет;

1.2.3.2. Если Правительством Российской Федерации установлено ограничение закупки работ, услуг, соответственно выполняемых, оказываемых иностранными лицами, не допускаются:

• заключение договора с участником закупки, являющимся иностранным лицом, если российским лицом поданы заявка на участие в закупке, окончательное предложение, признанные по результатам их рассмотрения соответствующими требованиям положения о закупке, извещения и документации о конкурентной закупке (в случае проведения конкурентной закупки);

• перемена подрядчика (исполнителя) (в случае, если эта перемена допускается гражданским законодательством), с которым заключен договор, на иностранное лицо, которое зарегистрировано на территории иностранного государства, в отношении которого установлено данное ограничение, если договор заключен с российским лицом;

1.2.3.3. Если Правительством Российской Федерации установлено преимущество в отношении работ, услуг, соответственно выполняемых, оказываемых российскими лицами:

• при рассмотрении, оценке, сопоставлении заявок на участие в закупке, окончательных предложений осуществляется снижение на 15 процентов ценового предложения, поданного участником закупки, являющимся российским лицом, либо увеличение на 15 процентов ценового предложения этого участника закупки в случае подачи им предложения о размере платы, подлежащей внесению за заключение с ним договора. Договор с участником закупки заключается без учета снижения либо увеличения ценового предложения;

• перемена подрядчика (исполнителя) (в случае, если эта перемена допускается гражданским законодательством), с которым заключен договор, допускается исключительно на российское лицо, если договор заключен с российским лицом.

1.2.4. Информация о запрете или об ограничении закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами, о преимуществе в отношении товаров российского происхождения (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), работ, услуг, соответственно выполняемых, оказываемых российскими лицами, в случае, если такие запрет, ограничение, преимущество установлены в соответствии с пунктом 1 части 2 статьи 3.1-4 Федерального закона №223-ФЗ в отношении товара, работы, услуги, являющихся предметом закупки указана в пункте 16 Раздела II настоящей Документации.

**1.3. Единые обязательные требования к участникам закупки.**

1.3.1. Участником закупки может является любое юридическое лицо или несколько юридических лиц, выступающих на стороне одного участника закупки, независимо от организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала, за исключением юридического лица, являющегося иностранным агентом в соответствии с Федеральным законом от 14 июля 2022 года N 255-ФЗ "О контроле за деятельностью лиц, находящихся под иностранным влиянием", либо любое физическое лицо/несколько физических лиц, выступающих на стороне одного участника закупки, в том числе индивидуальный предприниматель или несколько индивидуальных предпринимателей, выступающих на стороне одного участника закупки, за исключением физического лица, являющегося иностранным агентом в соответствии с Федеральным законом от 14 июля 2022 года N 255-ФЗ "О контроле за деятельностью лиц, находящихся под иностранным влиянием". Участник закупки для участия в конкурентной закупке подает заявку на участие в конкурентной закупке (далее при совместном упоминании - заявка на участие в закупке).

1.3.2. Заказчик осуществляет конкурентную закупку товаров, работ, услуг, участниками которой являются исключительно субъекты малого и среднего предпринимательства.

Подтверждением принадлежности участника закупки к субъектам малого и среднего предпринимательства является наличие информации о таком участнике в едином реестре субъектов малого и среднего предпринимательства. Заказчик не вправе требовать от участника закупки предоставления информации и документов, подтверждающих их принадлежность к субъектам малого и среднего предпринимательства.

1.3.3. К участникам закупки предъявляются следующие единые обязательные требования:

1) непроведение ликвидации участника конкурентной закупки с участием субъектов малого и среднего предпринимательства - юридического лица и отсутствие решения арбитражного суда о признании участника такой закупки - юридического лица или индивидуального предпринимателя несостоятельным (банкротом);

2) неприостановление деятельности участника конкурентной закупки с участием субъектов малого и среднего предпринимательства в порядке, установленном Кодексом Российской Федерации об административных правонарушениях;

3) отсутствие у участника конкурентной закупки с участием субъектов малого и среднего предпринимательства недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов участника такой закупки, по данным бухгалтерской (финансовой) отчетности за последний отчетный период. Участник такой закупки считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по данному заявлению на дату рассмотрения заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства не принято;

4) отсутствие у участника конкурентной закупки с участием субъектов малого и среднего предпринимательства - физического лица, зарегистрированного в качестве индивидуального предпринимателя, либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - участника конкурентной закупки с участием субъектов малого и среднего предпринимательства непогашенной или неснятой судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, 290, 291, 291.1 Уголовного кодекса Российской Федерации, а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся предметом осуществляемой закупки, и административного наказания в виде дисквалификации;

5) отсутствие фактов привлечения в течение двух лет до момента подачи заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства участника такой закупки - юридического лица к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях;

6) соответствие участника конкурентной закупки с участием субъектов малого и среднего предпринимательства указанным в документации о конкурентной закупке требованиям законодательства Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом закупки, если в соответствии с законодательством Российской Федерации информация и документы, подтверждающие такое соответствие, содержатся в открытых и общедоступных государственных реестрах, размещенных в информационно-телекоммуникационной сети "Интернет";

7) обладание участником конкурентной закупки с участием субъектов малого и среднего предпринимательства исключительными правами на результаты интеллектуальной деятельности, если в связи с исполнением договора заказчик приобретает права на такие результаты- *требование не установлено*;

8) обладание участником конкурентной закупки с участием субъектов малого и среднего предпринимательства правами использования результата интеллектуальной деятельности в случае использования такого результата при исполнении договора- *требование не установлено*;

1.3.4. Установлено требование об отсутствии сведений об участнике закупки в реестре недобросовестных поставщиков, предусмотренном статьёй 5 Федерального закона 223-ФЗ, и (или) в реестре недобросовестных поставщиков, предусмотренном Федеральным законом от 5 апреля 2013 года N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

**1.4. Условия участия коллективных Участников в конкурентных закупках.**

1.4.1. **Коллективный участник:** объединение (на основании договора или ином правоустанавливающем основании) поставщиков, явным образом принявшее участие в соответствующих процедурах.

Примечание. Важнейшим свойством коллективного участника является ответственность его членов (для простого товарищества – всегда солидарная, для иных форм определяется соглашением между его членами).

**Лидер коллективного участника:** лицо, являющееся одним из членов коллективного участника и представляющее интересы всех членов коллективного участника в отношениях с Организатором закупки.

1.4.2. Члены объединений, являющихся коллективными участниками закупок, должны иметь соглашение между собой (иной документ), соответствующее нормам Гражданского кодекса Российской Федерации, в котором определены права и обязанности сторон и установлен лидер коллективного участника. В случае проведения закрытых закупок к составу и лидеру коллективного участника дополнительно предъявляются требования - в случае подачи заявки коллективного участника, участником коллективного участника закупки может быть любое лицо, не приглашенное персонально, при обязательном условии, что Лидером коллективного участника может быть любое лицо, выбранное членами коллективного участника. В отдельных случаях могут быть установлены иные требования к коллективному участнику.

1.4.3. Для целей проведения конкурентной закупки лица, выступающие на стороне одного Участника, рассматриваются в качестве коллективного Участника. Особенности требований к лицам, выступающим на стороне одного Участника, предусмотрены настоящим разделом.

1.4.4. Лица, выступающие на стороне одного Участника должны иметь соглашение между собой (или иной документ), которое должно отвечать следующим требованиям:

a) соответствие нормам Гражданского кодекса Российской Федерации;

b) в соглашении должны быть четко определены права и обязанности членов коллективного Участника как в рамках участия в закупке, так и в рамках исполнения договора;

c) в соглашении должно быть приведено четкое распределение объемов, стоимости и сроков оказания услуг между членами коллективного Участника; при этом соглашением должно быть предусмотрено, что оказание услуг, требующих специальной правоспособности (к примеру, наличие лицензии), осуществляются исключительно лицами, входящими в состав коллективного Участника и обладающими необходимой правоспособностью;

d) в соглашении должен быть определен лидер, который в дальнейшем будет представлять интересы каждого из лиц, входящих в состав коллективного Участника;

е) в соглашении должен быть предусмотрен механизм установления ответственности коллективного Участника за неисполнение или ненадлежащее исполнение договора с заказчиком, в том числе объем ответственности каждого лица, входящего в состав коллективного Участника или порядок его определения, а также порядок предъявления и рассмотрения претензий заказчика;

f) соглашением должно быть предусмотрено, что договор по результатом закупки заключается с лидером согласно условиям документации о закупке.

1.4.5. Копия соглашения между лицами, выступающими на стороне одного Участника, представляется в составе Заявки. Также часть заявки должна включать сведения о распределении объемов выполнения работ внутри коллективного Участника в произвольной форме. При подаче заявки коллективным Участником документы, требуемые в составе заявки, необходимо предоставить в отношении каждого члена коллективного Участника. При подаче заявки коллективным Участником все члены коллективного Участника должны соответствовать единым обязательным требованиям, предъявляемым к участникам конкурентной закупки.

1.4.6. Каждый член коллективного Участника должен самостоятельно отвечать требованиям, установленным к Участникам в части общей гражданской правоспособности, а также обладать специальной правоспособностью, которая требуется в соответствии с законодательством Российской Федерации для выполнения переданного ему объема оказания услуг согласно распределению объемов оказания услуг между членами коллективного Участника, указанному в соглашении.

1.4.7. В случае несоответствия какого-либо из заявленных членов коллективного Участника требованиям настоящего раздела, заявка такого коллективного Участника не допускается к дальнейшему участию в закупке.

1.4.8. Заявка на участие в конкурентной закупке подается лидером коллективного Участника от своего имени со ссылкой на то, что он представляет интересы коллективного Участника.

1.4.9. Коллективный Участник отстраняется от участия в закупке на любом этапе ее проведения, а договор с ним не подлежит подписанию, если будет установлено, что из состава коллективного участника вышло одно или несколько его лиц.

**2. Документация об аукционе в электронной форме**

**2.1. Порядок представления документации об аукционе в электронной форме**

2.1.1. В случае проведения электронного аукциона Заказчик обеспечивает размещение документации о закупке в ЕИС, на официальном сайте и на ЭТП одновременно с размещением извещения о закупке, а также на официальном сайте МУП «Водоканал»: www.vodokanal-yola.ru.

2.1.2. Размещение заказчиками в единой информационной системе информации о закупке, предоставление доступа к такой информации осуществляются без взимания платы.

2.1.3. Со дня размещения в ЕИС и на ЭТП извещения о закупке Заказчик на основании заявления любого заинтересованного лица, поданного в письменной форме, в течение двух рабочих дней со дня получения соответствующего заявления обязан предоставить такому лицу документацию о закупке в порядке, указанном в извещении о закупке. При этом документация о закупке предоставляется в письменной форме после внесения участником закупки платы за предоставление документации о закупке, если такая плата установлена Заказчиком и указание об этом содержится в извещении о закупке и в Информационной карте аукциона в электронной форме (здесь и далее ссылки относятся к настоящей Документации о закупке). Размер указанной платы не должен превышать расходы Заказчика на изготовление копии документации о закупке и доставку её лицу, подавшему указанное заявление, посредством почтовой связи.

2.1.4. Предоставление документации о закупке до размещения в ЕИС и на ЭТП извещения о закупке не допускается.

2.1.5. Если для участия в электронном аукционе иностранному лицу потребуется документация о закупке на иностранном языке, перевод на иностранный язык такое лицо осуществляет самостоятельно за свой счёт, если иного не установлено в извещении и документации о закупке.

**2.2. Разъяснение положений документации об аукционе в электронной форме**

2.2.1. Любой участник электронного аукциона, получивший аккредитацию на электронной площадке, вправе направить оператору электронной площадки с использованием программно-аппаратных средств электронной площадки, на которой планируется проведение такого электронного аукциона, запрос о даче разъяснений положений извещения о закупке и (или) документации о закупке.

2.2.2. В течение одного часа с момента поступления указанного запроса он направляется оператором электронной площадки Заказчику без указаний информации об участнике закупки, направившем данный запрос.

2.2.3. В течение 3 (трёх) рабочих дней с даты поступления указанного запроса Заказчик размещает разъяснения в единой информационной системе, на официальном сайте при условии, что указанный запрос поступил Заказчику не позднее чем за 3 (три) рабочих дня до дня окончания подачи заявок на участие в электронном аукционе.

2.2.4. В течение одного часа с момента появления в единой информационной системе разъяснений положений документации о закупке аукциона в электронной форме оператор электронной площадки размещает указанную информацию на электронной площадке и направляет уведомление об указанных разъяснениях лицу, направившему запрос о даче разъяснений положений документации о закупке по адресу электронной почты, указанному этим участником при аккредитации на электронной площадке или этим лицом при направлении запроса.

2.2.5. Разъяснения положений извещения и (или) документации о закупке не должны изменять её суть.

2.2.6. Участник имеет право подать всего три запроса на разъяснение положений извещения и (или) документации о закупке.

**2.3. Внесение изменений в извещение об аукционе в электронной форме, в документацию об аукционе в электронной форме**

2.3.1. Заказчик по собственной инициативе или в соответствии с поступившим запросом о разъяснении положений документации о закупке вправе принять решение о внесении изменений в извещение и в документацию о закупке.

2.3.2. Заказчик вправе принять решение о внесении изменений в извещение о закупке не позднее чем за 3 (три) рабочих дня до даты окончания подачи заявок на участие в электронном аукционе.

2.3.3. Изменения, вносимые в извещение и/или в документацию о закупке, о проведении аукциона в электронной форме, размещаются Заказчиком в единой информационной системе, на официальном сайте и на электронной площадке, не позднее чем в течение 3 (трёх) дней со дня принятия решения о внесении указанных изменений.

При этом срок подачи заявок на участие в электронном аукционе должен быть продлён так, чтобы с даты размещения в единой информационной системе указанных изменений до даты окончания срока подачи заявок на участие в электронном аукционе этот срок подачи заявок составлял не менее половины срока подачи заявок на участие в электронном аукционе.

2.3.4. В течение одного часа с момента размещения в единой информационной системе изменений положений документации о закупке оператор электронной площадки размещает указанную информацию на электронной площадке и направляет всем участникам закупки, подавшим заявки на участие в электронном аукционе, уведомление об указанных изменениях по адресам электронной почты, указанным этими участниками при аккредитации на электронной площадке.

2.3.5. Участники закупки должны самостоятельно отслеживать изменения, вносимые в извещения и/или в документацию о закупке. Заказчик не несёт ответственности за несвоевременное получение участником закупки информации об изменениях электронного аукциона, размещенной в единой информационной системе, на официальном сайте и на электронной площадке.

2.3.6. Изменение предмета электронного аукциона не допускается.

**2.4. Отмена аукциона в электронной форме**

2.4.1. Заказчик, разместивший в единой информационной системе извещение о проведении аукциона в электронной форме, вправе отменить проведение электронного аукциона до наступления даты и времени окончания срока подачи заявок на участие в электронном аукционе.

2.4.2. Решение об отмене электронного аукциона размещается в единой информационной системе в день принятия этого решения.

2.4.3. В течение одного часа с момента размещения в единой информационной системе извещения об отказе от осуществления электронного аукциона оператор электронной площадки размещает указанную информацию на электронной площадке.

2.4.4. По истечении срока отмены электронного аукциона и до заключения договора Заказчик вправе отменить определение поставщика (исполнителя, подрядчика) только в случае возникновения обстоятельств непреодолимой силы в соответствии с гражданским законодательством.

**3. Требования к содержанию, форме, оформлению и составу заявки на участие в электронном аукционе**

**3.1. Требования к содержанию и составу заявки на участие в электронном аукционе**

3.1.1. Заявка на участие в закупке (далее — Заявка) — комплект документов, содержащий предложение участника конкурентной закупки, направленный Заказчику по форме и в порядке, установленном документацией о закупке, с намерением принять участие в конкурентной закупке и впоследствии заключить договор на условиях, определённых документацией о закупке.

Заявка на участие в аукционе в электронной форме состоит из двух частей (такие электронные документы (две части заявки) подаются одновременно). Требования к содержанию и оформлению каждой части заявки приведены в настоящей документации.

**3.1.2. Первая часть заявки на участие в электронном аукционе должна содержать следующие информацию и документы:**

**1)** предложение участника конкурентной закупки с участием субъектов малого и среднего предпринимательства в отношении предмета закупки;

Предложение должно содержать конкретные показатели товара, соответствующие значениям, установленным документацией о закупке (Разделом III «Техническое задание» настоящей документации).

Первая часть заявки может содержать эскиз, рисунок, чертёж, фотографию, иное изображение товара, на поставку которого размещается заказ.

При этом не допускается указание в первой части заявки на участие в электронном аукционе сведений об участнике закупки и (или) о ценовом предложении.

Рекомендуемая форма первой части заявки приведена в Разделе VI «Инструкция по заполнению заявок на участие в электронном аукционе».

**3.1.3. Вторая часть заявки на участие в электронном аукционе должна содержать следующие информацию и документы:**

**1)** наименование, фирменное наименование (при наличии), адрес юридического лица в пределах места нахождения юридического лица, учредительный документ, если участником конкурентной закупки с участием субъектов малого и среднего предпринимательства является юридическое лицо;

**2)** фамилия, имя, отчество (при наличии), паспортные данные, адрес места жительства физического лица, зарегистрированного в качестве индивидуального предпринимателя, если участником конкурентной закупки с участием субъектов малого и среднего предпринимательства является индивидуальный предприниматель;

**3)** идентификационный номер налогоплательщика участника конкурентной закупки с участием субъектов малого и среднего предпринимательства или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика (для иностранного лица);

**4)** идентификационный номер налогоплательщика (при наличии) учредителей, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа юридического лица, если участником конкурентной закупки с участием субъектов малого и среднего предпринимательства является юридическое лицо, или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика таких лиц;

**5)** копия документа, подтверждающего полномочия лица действовать от имени участника конкурентной закупки с участием субъектов малого и среднего предпринимательства, за исключением случаев подписания заявки:

а) индивидуальным предпринимателем, если участником такой закупки является индивидуальный предприниматель;

б) лицом, указанным в едином государственном реестре юридических лиц в качестве лица, имеющего право без доверенности действовать от имени юридического лица (далее в настоящей главе - руководитель), если участником такой закупки является юридическое лицо;

**6)** копии документов, подтверждающих соответствие участника конкурентной закупки с участием субъектов малого и среднего предпринимательства требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом закупки, за исключением случая, если в соответствии с законодательством Российской Федерации информация и документы, подтверждающие такое соответствие, содержатся в открытых и общедоступных государственных реестрах, размещенных в информационно-телекоммуникационной сети "Интернет" (с указанием адреса сайта или страницы сайта в информационно-телекоммуникационной сети "Интернет", на которых размещены эти информация и документы) - *требование не установлено*;

**7)** копия решения о согласии на совершение крупной сделки или о последующем одобрении этой сделки, если требование о наличии указанного решения установлено законодательством Российской Федерации и для участника конкурентной закупки с участием субъектов малого и среднего предпринимательства заключение по результатам такой закупки договора либо предоставление обеспечения заявки на участие в такой закупке (если требование об обеспечении заявок установлено заказчиком в извещении об осуществлении такой закупки, документации о конкурентной закупке), обеспечения исполнения договора (если требование об обеспечении исполнения договора установлено заказчиком в извещении об осуществлении такой закупки, документации о конкурентной закупке) является крупной сделкой;

**8)** декларация, подтверждающая на дату подачи заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства *(представляется в составе заявки участником закупки с использованием программно-аппаратных средств электронной площадки)*:

а) непроведение ликвидации участника конкурентной закупки с участием субъектов малого и среднего предпринимательства - юридического лица и отсутствие решения арбитражного суда о признании участника такой закупки - юридического лица или индивидуального предпринимателя несостоятельным (банкротом);

б) неприостановление деятельности участника конкурентной закупки с участием субъектов малого и среднего предпринимательства в порядке, установленном Кодексом Российской Федерации об административных правонарушениях;

в) отсутствие у участника конкурентной закупки с участием субъектов малого и среднего предпринимательства недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов участника такой закупки, по данным бухгалтерской (финансовой) отчетности за последний отчетный период. Участник такой закупки считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по данному заявлению на дату рассмотрения заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства не принято;

г) отсутствие у участника конкурентной закупки с участием субъектов малого и среднего предпринимательства - физического лица, зарегистрированного в качестве индивидуального предпринимателя, либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - участника конкурентной закупки с участием субъектов малого и среднего предпринимательства непогашенной или неснятой судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, 290, 291, 291.1 Уголовного кодекса Российской Федерации, а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся предметом осуществляемой закупки, и административного наказания в виде дисквалификации;

д) отсутствие фактов привлечения в течение двух лет до момента подачи заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства участника такой закупки - юридического лица к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях;

е) соответствие участника конкурентной закупки с участием субъектов малого и среднего предпринимательства указанным в документации о конкурентной закупке требованиям законодательства Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом закупки, если в соответствии с законодательством Российской Федерации информация и документы, подтверждающие такое соответствие, содержатся в открытых и общедоступных государственных реестрах, размещенных в информационно-телекоммуникационной сети "Интернет" (с указанием адреса сайта или страницы сайта в информационно-телекоммуникационной сети "Интернет", на которых размещены эти информация и документы);

ж) обладание участником конкурентной закупки с участием субъектов малого и среднего предпринимательства исключительными правами на результаты интеллектуальной деятельности, если в связи с исполнением договора заказчик приобретает права на такие результаты - *требование не установлено*;

з) обладание участником конкурентной закупки с участием субъектов малого и среднего предпринимательства правами использования результата интеллектуальной деятельности в случае использования такого результата при исполнении договора - *требование не установлено*;

**9)** копии документов, подтверждающих соответствие товара, работы или услуги, являющихся предметом закупки, требованиям, установленным в соответствии с законодательством Российской Федерации, в случае, если требования к данным товару, работе или услуге установлены в соответствии с законодательством Российской Федерации и перечень таких документов предусмотрен документацией о конкурентной закупке. При этом не допускается требовать представление указанных документов, если в соответствии с законодательством Российской Федерации они передаются вместе с товаром;

**10)** **информация и документы, подтверждающие страну происхождения товаров, в отношении которых установлен запрет закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств:**

а) для подтверждения происхождения программ для электронных вычислительных машин и (или) баз данных (далее - программное обеспечение) из Российской Федерации

**- порядковый номер реестровой записи из единого реестра российских программ для электронных вычислительных машин и баз данных (далее - реестр российского программного обеспечения);**

б) для подтверждения происхождения программного обеспечения из Российской Федерации и его соответствия дополнительным требованиям к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, утвержденным постановлением Правительства Российской Федерации от 23 марта 2017 г. № 325 "Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных" (далее - дополнительные требования к программному обеспечению),

**- порядковый номер реестровой записи из реестра российского программного обеспечения, содержащей информацию о соответствии программного обеспечения дополнительным требованиям к программному обеспечению;**

в) для подтверждения происхождения программного обеспечения из государств - членов Евразийского экономического союза, за исключением Российской Федерации,

**- порядковый номер реестровой записи из единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации (далее - реестр евразийского программного обеспечения);**

г) для подтверждения происхождения программного обеспечения из государств - членов Евразийского экономического союза, за исключением Российской Федерации, и его соответствия дополнительным требованиям к программному обеспечению

**- порядковый номер реестровой записи из реестра евразийского программного обеспечения, содержащей информацию о соответствии программного обеспечения дополнительным требованиям к программному обеспечению;**

3.1.4. Документы участника закупки, должны быть подписаны усиленной квалифицированной электронной подписью (далее — электронная подпись) лица, имеющего право действовать от имени, соответственно, участника закупки.

3.1.5. В случае содержания в первой части заявки на участие в аукционе в электронной форме сведений об участнике такого аукциона и (или) о ценовом предложении данная заявка подлежит отклонению.

**4. Порядок подачи и обеспечение заявок на участие в электронном аукционе**

**4.1. Порядок, место, дата начала и дата окончания срока подачи заявок на участие в электронном аукционе**

4.1.1. Для участия в электронном аукционе участник закупки должен пройти аккредитацию на электронной торговой площадке по адресу: http://www.rts-tender.ru (ООО «"РТС-тендер" – Электронная торговая площадка»).

Субъекты малого и среднего предпринимательства получают аккредитацию на электронной площадке в порядке, установленном Федеральным законом от 5 апреля 2013 года N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

4.1.2. Участник закупки подает заявку по адресу электронной площадки «РТС-тендер» (http://www.rts-tender.ru) в соответствии с регламентом электронной площадки «РТС-тендер» с учетом требований, установленных в настоящей документации.

Для участия в электронном аукционе участник закупки подает заявку в срок и по форме, которые установлены в документации о закупке.

4.1.3. Участник закупки вправе подать только одну заявку на участие в электронном аукционе в отношении каждого предмета аукциона (лота).

4.1.4. Прием заявок на участие в электронном аукционе прекращается в день и время, указанные в извещении о закупке и Информационной карте.

4.1.5. Участник закупки, подавший заявку на участие в электронном аукционе, вправе отозвать заявку либо внести в нее изменения не позднее даты окончания срока подачи заявок, направив об этом уведомление оператору электронной площадки.

4.1.6. Участник закупки не вправе подать заявку на участие в электронном аукционе после дня и времени окончания срока подачи заявок.

4.1.7. Оператор электронной площадки обязан обеспечить конфиденциальность информации о содержании заявок на участие в электронном аукционе.

4.1.8. Подавая заявку на электронный аукцион, участник закупки подтверждает, что товары, предлагаемые им, соответствуют требованиям, изложенным в извещении и документации о закупке.

4.1.9. В случае если по окончании срока подачи заявок на участие в электронном аукционе подана только одна заявка или не подано ни одной заявки, такой аукцион признается несостоявшимся.

**4.2. Обеспечение заявок на участие в электронном аукционе**

4.2.1. В случае установления в документации о закупке требования к обеспечению заявки на участие в закупке, размер такого обеспечения не может превышать 2% начальной (максимальной) цены договора (цены лота).

4.2.2. Участие в электронном аукционе возможно при наличии на счёте участника закупки, открытом для проведения операций по обеспечению участия в закупках, денежных средств в размере не менее чем размер обеспечения заявки на участие в электронном аукционе, (если требование об обеспечении заявок установлено заказчиком в извещении о закупке и в Информационной карте).

4.2.3. Требование о предоставлении обеспечения в равной степени распространяется на всех участников закупки (если требование об обеспечении заявок установлено заказчиком в извещении о закупке и в Информационной карте).

4.2.4. При осуществлении конкурентной закупки с участием субъектов малого и среднего предпринимательства обеспечение заявок на участие в такой конкурентной закупке (если требование об обеспечении заявок установлено Заказчиком в извещении об осуществлении такой закупки, документации о конкурентной закупке) может предоставляться участниками такой закупки путём внесения денежных средств в соответствии с настоящим разделом или предоставления независимой гарантии. Выбор способа обеспечения заявки на участие в такой закупке осуществляется участником такой закупки.

4.2.5. Независимая гарантия, предоставляемая в качестве обеспечения заявки на участие в аукционе в электронной форме с участием субъектов малого и среднего предпринимательства, должна соответствовать следующим требованиям:

1) независимая гарантия должна быть выдана гарантом, предусмотренным частью 1 статьи 45 Федерального закона от 5 апреля 2013 года N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд";

2) независимая гарантия не может быть отозвана выдавшим ее гарантом;

3) независимая гарантия должна содержать:

а) 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;

б) перечень документов, подлежащих представлению заказчиком гаранту одновременно с требованием об уплате денежной суммы по независимой гарантии, в случае установления такого перечня Правительством Российской Федерации в соответствии с пунктом 4 части 32 статьи 3.4 Федерального закона № 223-ФЗ;

в) указание на срок действия независимой гарантии, который не может составлять менее одного месяца с даты окончания срока подачи заявок на участие в такой закупке.

4) информация о независимой гарантии должна быть включена в реестр независимых гарантий, предусмотренный частью 8 статьи 45 Федерального закона № 44-ФЗ.

Несоответствие независимой гарантии, предоставленной участником закупки с участием субъектов малого и среднего предпринимательства, требованиям, предусмотренным настоящим Разделом, является основанием для отказа в принятии ее заказчиком.

Гарант в случае просрочки исполнения обязательств по независимой гарантии, требование об уплате денежной суммы по которой соответствует условиям такой независимой гарантии и предъявлено заказчиком до окончания срока ее действия, обязан за каждый день просрочки уплатить заказчику неустойку (пени) в размере 0,1 процента денежной суммы, подлежащей уплате по такой независимой гарантии.

Независимая гарантия, предоставляемая в качестве обеспечения заявки на участие в закупке, должна быть составлена по типовой форме согласно приложению № 1 к постановлению Правительства Российской Федерации от 9 августа 2022 года № 1397 «О независимых гарантиях, предоставляемых в качестве обеспечения заявки на участие в конкурентной закупке товаров, работ, услуг в электронной форме с участием субъектов малого и среднего предпринимательства, и независимых гарантиях, предоставляемых в качестве обеспечения исполнения договора, заключаемого по результатам такой закупки, а также о внесении изменений в некоторые акты Правительства Российской Федерации» на условиях, определенных гражданским законодательством и Федеральным законом № 223-ФЗ.

4.2.6. При осуществлении аукциона в электронной форме с участием субъектов малого и среднего предпринимательства денежные средства, предназначенные для обеспечения заявки на участие в такой закупке, вносятся участником такой закупки на специальный счёт, открытый им в банке, включённый в перечень, определённый Правительством Российской Федерации в соответствии с Федеральным законом от 5 апреля 2013 года N 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее — специальный банковский счёт).

4.2.7. В течение одного часа с момента окончания срока подачи заявок на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства оператор электронной площадки направляет в банк информацию об участнике закупки и размере денежных средств, необходимом для обеспечения заявки. Банк в течение одного часа с момента получения указанной информации осуществляет блокирование при наличии на специальном банковском счете участника закупки незаблокированных денежных средств в размере обеспечения указанной заявки и информирует оператора. Блокирование денежных средств не осуществляется в случае отсутствия на специальном банковском счете участника такой закупки денежных средств в размере для обеспечения указанной заявки либо в случае приостановления операций по такому счету в соответствии с законодательством Российской Федерации, о чем оператор электронной площадки информируется в течение одного часа. В случае, если блокирование денежных средств не может быть осуществлено по основаниям, предусмотренным настоящей частью, оператор электронной площадки обязан вернуть указанную заявку подавшему ее участнику в течение одного часа с момента получения соответствующей информации от банка.

4.2.8. Участник закупки вправе распоряжаться денежными средствами, которые находятся на специальном банковском счете и в отношении которых не осуществлено блокирование.

4.2.9. В случае, уклонения или отказа участника закупки от заключения договора, и/или непредставление или представление с нарушением условий, установленных Федеральным законом №223-ФЗ и Положением о закупках, до заключения договора Заказчику обеспечения исполнения договора (в случае, если в извещении об осуществлении закупки, документации о закупке установлены требования обеспечения исполнения договора и срок его предоставления до заключения договора) денежные средства, внесенные на специальный банковский счет в качестве обеспечения заявки на участие в закупке с участием субъектов малого и среднего предпринимательства, перечисляются банком на счет заказчика, указанный в извещении о закупке с участием субъектов малого и среднего предпринимательства, в документации о такой закупке, или заказчиком предъявляется требование об уплате денежной суммы по независимой гарантии, предоставленной в качестве обеспечения заявки на участие в закупке с участием субъектов малого и среднего предпринимательства.

**5. Рассмотрение заявок на участие в электронном аукционе и проведение электронного аукциона**

**5.1. Порядок рассмотрения заявок на участие в электронном аукционе.**

5.1.1. Оператор электронной площадки в следующем порядке направляет Заказчику:

1) первые части заявок на участие в аукционе в электронной форме - не позднее дня, следующего за днем окончания срока подачи заявок на участие в конкурентной закупке с участием только субъектов малого и среднего предпринимательства, установленного извещением об осуществлении конкурентной закупки, документацией о конкурентной закупке либо уточненными извещением, документацией;

2) вторые части заявок на участие в аукционе, протокол, предусмотренный в п.5.2.4 настоящего раздела, - в сроки, установленные извещением о проведении такого аукциона, документацией о конкурентной закупке либо уточненными извещением, документацией. Указанные сроки не могут быть ранее сроков:

а) размещения заказчиком в единой информационной системе протокола, составляемого в ходе проведения такого аукциона по результатам рассмотрения первых частей заявок;

б) проведения процедуры подачи участниками аукциона в электронной форме предложений о цене договора с учетом требований п.5.2 настоящего раздела;

5.1.2 В случае, если Заказчиком принято решение об отмене конкурентной закупки с участием субъектов малого и среднего предпринимательства по одному и более предмету закупки (лоту) до наступления даты и времени окончания срока подачи заявок на участие в конкурентной закупке, оператор электронной площадки не вправе направлять Заказчику заявки участников такой конкурентной закупки. Заказчик вправе отменить конкурентную закупку.

5.1.3. Единая комиссия проверяет первые части заявок на участие в электронном аукционе на соответствие требованиям, установленным документацией о закупке в отношении товаров, работ, услуг, являющихся предметом закупки.

5.1.4. Дата окончания срока рассмотрения первых частей заявок указана Информационной карте.

5.1.5. Срок рассмотрения первых частей заявок на участие в электронном аукционе не может превышать 7 (семи) дней, со дня окончания срока подачи заявок на участие в электронном аукционе.

5.1.6. На основании результатов рассмотрения первых частей заявок на участие в электронном аукционе Единой комиссией принимается решение о допуске к участию в электронном аукционе участника закупки и о признании участника закупки, подавшего заявку на участие в электронном аукционе, участником электронного аукциона или об отказе в допуске такого участника закупки к участию в электронном аукционе.

5.1.7. В случае, если документацией о закупке предусмотрено 2 и более лота, электронный аукцион признаётся несостоявшимся только в отношении того лота, в котором принято решение об отказе в допуске к участию в электронном аукционе всех участников или о допуске к участию и о признании участником электронного аукциона только одного участника, подавшего заявку на участие в электронном аукционе в отношении этого лота.

5.1.8. На основании результатов рассмотрения первых частей заявок на участие в электронном аукционе, Единая комиссия оформляет протокол рассмотрения заявок на участие в электронном аукционе, подписывается всеми присутствующими на заседании членами Единой комиссии в день окончания рассмотрения заявок на участие в электронном аукционе. Протокол рассмотрения заявок на участие в электронном аукционе заказчик направляет оператору электронной площадки. В течение часа с момента получения указанного протокола оператор электронной площадки размещает его в единой информационной системе.

5.1.9. В течение одного рабочего дня после направления оператором электронной площадки информации, указанной в пп. 2) п. 5.1 настоящего раздела, комиссия по осуществлению закупок на основании результатов оценки заявок на участие в такой закупке присваивает каждой такой заявке порядковый номер в порядке уменьшения степени выгодности содержащихся в них условий исполнения договора. Заявке на участие в аукционе в электронной форме, в которой содержится наименьшее ценовое предложение, присваивается первый номер. В случае, если в нескольких таких заявках содержатся одинаковые ценовые предложения, меньший порядковый номер присваивается заявке, которая поступила ранее других таких заявок.

5.1.10. Единая комиссия по осуществлению закупок рассматривает вторые части заявок на участие в электронном аукционе, а также документы, направленные Заказчику оператором электронной площадки, на соответствие их требованиям, установленным документацией о закупке. Порядок отстранения и отклонения заявок на участие в электронном аукционе предусмотрен в п. 5.3 настоящего раздела.

5.1.11. Единая комиссия на основании результатов рассмотрения вторых частей заявок на участие в электронном аукционе принимает решение о соответствии или о несоответствии заявки участника электронного аукциона требованиям, установленным документацией о закупке.

5.1.12. На основании принятого решения о соответствии или о несоответствии заявки участника электронного аукциона требованиям, установленным документацией о закупке Единой комиссией, оформляется протокол, в котором фиксируются все результаты рассмотрения заявок, подписывается всеми присутствующими на заседании членами Единой комиссии.

5.1.13. В случае принятия на основании рассмотрения вторых частей заявок на участие в электронном аукционе решения о несоответствии заявок на участие в электронном аукционе требованиям, установленным документацией о закупке, в протоколе указывается обоснование принятого решения о несоответствии участника закупки положениям документации о закупке.

5.1.14. Определение победителя проводится на основании порядка подачи участниками предложений о цене договора с учётом требований, установленных настоящей документацией.

5.1.15. Заказчик составляет итоговый протокол и размещает его на электронной площадке и в единой информационной системе.

5.1.16. Протокол размещается в единой информационной системе не позднее чем через 3 (три) дня со дня подписания такого протокола.

**5.2. Порядок проведения электронного аукциона**

5.2.1. Электронный аукцион проводится на электронной площадке в день, указанный в извещении о закупке и в Информационной карте. Время начала проведения электронного аукциона устанавливается и/или оператором электронной площадки, и/или Заказчиком в соответствии с извещением и/или документацией о закупке.

5.2.2. Днём проведения электронного аукциона является рабочий день, следующий после истечения 2 (двух) дней со дня окончания срока рассмотрения первых частей заявок на участие в электронного аукционе. В электронном аукционе могут участвовать только те участники закупки, которые были допущены к участию в электронном аукционе.

5.2.3. Электронный аукцион включает в себя порядок подачи его участниками предложений о цене договора с учётом следующих требований:

1) «шаг аукциона» составляет от 0,5 процента до пяти процентов начальной (максимальной) цены договора;

2) снижение текущего минимального предложения о цене договора осуществляется на величину в пределах «шага аукциона»;

3) участник электронного аукциона не вправе подать предложение о цене договора, которое равно предложению, ранее поданному этим участником, или больше него, а также предложение о цене договора, равное нулю;

4) участник электронного аукциона не вправе подать предложение о цене договора, которое ниже, чем текущее минимальное предложение о цене договора, сниженное в пределах «шага аукциона»;

5) участник электронного аукциона не вправе подать предложение о цене договора, которое ниже, чем текущее минимальное предложение о цене договора, в том случае, если оно подано этим участником электронного аукциона.

5.2.4. В течение одного часа после окончания подачи предложений о цене договора оператор электронной площадки составляет и размещает на электронной площадке и в единой информационной системе протокол подачи предложений о цене договора, содержащие дату, время начала и окончания подачи предложений о цене договора и поступившие минимальные предложения о цене договора каждого участника аукциона в электронной форме с указанием времени их поступления.

**5.3. Основания для отстранения участников от участия в электронном аукционе**

5.3.1. Участник закупки, подавший заявку, не допускается Единой комиссией к участию в электронном аукционе в случае:

— несоответствия участника процедуры закупки обязательным требованиям, установленным документацией о закупке;

— отсутствия обязательных документов или копии документа, подтверждающего внесение денежных средств в качестве обеспечения заявки на участие в закупке, если требование обеспечения таких заявок указано в документации о закупке;

— отсутствия обязательных документов либо наличия в таких документах недостоверных сведений;

— выявления в документах, представленных участником в составе заявки, противоречивых сведений, предполагающих двоякое толкование;

— несоответствия заявки требованиям документации о закупке, в том числе наличия в таких заявках предложения о цене договора, превышающего установленную начальную (максимальную) цену договора;

5.3.2.Участник закупок отстраняется от участия в процедуре закупки, в том числе от участия в этапах закупки, в любой момент до заключения договора, если Заказчик обнаружит, что участник представил недостоверную (в том числе неполную, противоречивую) информацию, содержащуюся в документах, представленных участником в составе своей заявки, в том числе в отношении его квалификационных данных. Данные выводы могут быть основаны на документах и информации, полученной у третьих лиц, из публичных источников, иными не запрещёнными законодательством способами. Заказчик обязан зафиксировать указанную информацию на материальном носителе и направить участнику мотивированное сообщение с предложением устранить недостатки в установленные условиями процедуры закупки сроки.

5.3.3. В случае содержания в первой части заявки на участие в аукционе в электронной форме сведений об участнике такого аукциона и (или) о ценовом предложении данная заявка подлежит отклонению.

5.3.4. При осуществлении закупки товаров, работ, услуг у субъектов малого и среднего предпринимательства заказчик принимает решение об отказе в допуске к участию в закупке участника закупки или об отказе от заключения договора с участником закупки в случае отсутствия информации об участнике закупки, субподрядчике (соисполнителе) в едином реестре субъектов малого и среднего предпринимательства.

**6. Порядок заключения договора**

**6.1. Заключение договора по результатам электронного аукциона**

6.1.1. Договор по результатам электронного аукциона с участием субъектов малого и среднего предпринимательства заключается с использованием программно-аппаратных средств электронной площадки и должен быть подписан электронной подписью лица, имеющего право действовать от имени, соответственно, участника электронного аукциона, Заказчика. В случае наличия разногласий по проекту договора, направленному Заказчиком, участник такой закупки составляет протокол разногласий с указанием замечаний к положениям проекта договора, не соответствующим извещению, документации о закупке и своей заявке, с указанием соответствующих положений данных документов. Протокол разногласий направляется Заказчику с использованием программно-аппаратных средств электронной площадки. Заказчик рассматривает протокол разногласий и направляет участнику такой закупки доработанный проект договора либо повторно направляет проект договора с указанием в отдельном документе причин отказа учесть полностью или частично содержащиеся в протоколе разногласий замечания.

6.1.2. Договор по результатам конкурентной закупки с участием субъектов малого и среднего предпринимательства заключается на условиях, которые предусмотрены проектом договора, документацией о конкурентной закупке, извещением об осуществлении конкурентной закупки и заявкой участника такой закупки, с которым заключается договор.

6.1.3. Договор по результатам аукциона в электронной форме должен быть заключён не ранее чем через 10 (десять) дней и не позднее чем через 20 (двадцать) дней с даты размещения в единой информационной системе итогового протокола, составленного по результатам закупки.

В случае необходимости одобрения органом управления заказчика в соответствии с законодательством Российской Федерации заключения договора или в случае обжалования в антимонопольном органе действий (бездействия) заказчика, комиссии по осуществлению конкурентной закупки, оператора электронной площадки договор должен быть заключен не позднее чем через пять дней с даты указанного одобрения или с даты вынесения решения антимонопольного органа по результатам обжалования действий (бездействия) заказчика, комиссии по осуществлению конкурентной закупки, оператора электронной площадки.

6.1.4. При этом договор заключается только после предоставления участником электронного аукциона обеспечения исполнения договора, если такое требование было установлено в документации о закупке.

6.1.5. Договор заключается через электронную площадку путём направления Заказчиком проекта договора победителю электронного аукциона.

6.1.6. Заказчик в течение 5 (пяти) дней со дня опубликования в единой информационной системе итогового протокола о закупке направляет победителю на подпись необходимое количество экземпляров договора через оператора электронной площадки.

6.1.7. Если победитель электронного аукциона в течение 5 (пяти) дней не направит Заказчику подписанный договор либо протокол разногласия, то победитель электронного аукциона считается уклонившимся от заключения договора. По данному факту комиссия по закупке составляет протокол о признании участника закупки уклонившемся от заключения договора.

6.1.8. Если победитель электронного аукциона признан уклонившимся от заключения договора, договор может быть заключён с участником электронного аукциона, чья заявка получила второй порядковый номер по цене и условиям, предложенным вторым участником.

6.1.9. В случае уклонения участника электронного аукциона, заявке которого присвоен второй номер, от заключения договора — аукцион в электронной форме признаётся несостоявшимся.

6.1.10. Если электронный аукцион признан несостоявшимся в связи с уклонением второго участника электронного аукциона от заключения договора, Заказчик вправе осуществить закупку как у единственного поставщика (подрядчика, исполнителя).

6.1.11. В случае, если Заказчиком в Информационной карте установлено требование обеспечения исполнения договора, то такое обеспечение должно быть представлено участником в момент подписания договора. В случае непредставления обеспечения в указанный срок договор может быть расторгнут в одностороннем порядке (указанное основание расторжения договора в одностороннем порядке должно быть отражено в проекте договора, входящего в состав документации о закупке).

6.1.12. При исполнении договора не допускается перемена поставщика (победителя закупки) (исполнителя, подрядчика), за исключением случаев, если новый поставщик (исполнитель, подрядчик) является правопреемником поставщика (исполнителя, подрядчика) по такому договору вследствие реорганизации юридического лица в форме преобразования, слияния или присоединения / при смене поставщика (подрядчика, исполнителя) по согласованию с Заказчиком на основании договора переуступки прав и обязанностей по действующему договору.

6.1.13. При заключении договора, по результатам электронного аукциона между Заказчиком и победителем могут проводиться преддоговорные переговоры (в том числе путём составления протоколов разногласий), направленные на уточнение деталей договора. При этом срок заключения договора, указанный в документации о закупке, отодвигается на срок, в течение которого проводились преддоговорные переговоры.

6.1.14. Заказчик вправе отказаться от заключения договора с участником закупки, обязанным заключить договор, в случаях:

— несоответствия участника закупки, обязанного заключить договор, требованиям, установленным в документации о закупки;

— предоставления участником закупки, обязанным заключить договор, недостоверных сведений в заявке на участие в закупке.

6.1.15. В случае отказа Заказчика от заключения договора с участником закупки, в соответствии с пунктом 6.1.14 настоящего раздела, комиссия по закупке составляет протокол об отказе от заключения договора, содержащий информацию о месте и времени его составления, о лице, с которым Заказчик отказывается заключить договор, о факте, являющемся основанием для такого отказа.

Заказчик вправе заключить договор с иным участником конкурентной закупки в порядке, установленном пунктом 6.1.8 настоящего раздела документации.

**6.2. Антидемпинговые меры**

6.2.1. Если по результатам электронного аукциона цена договора, предложенная участником закупки, с которым заключается договор, снижена на 25 (двадцать пять) и более процентов от начальной (максимальной) цены договора, победитель либо такой участник обязан предоставить Заказчику информацию, подтверждающую добросовестность такого участника, либо предоставить обеспечение исполнения договора в размере, превышающем в полтора раза размер обеспечения исполнения договора, указанный в документации о конкурентной закупке, но не менее чем в размере аванса (если договором предусмотрена выплата аванса).

 6.2.2. К информации, подтверждающей добросовестность участника закупки, относится информация, содержащаяся в реестре договоров (контрактов), заключённых Заказчиками, и подтверждающая их исполнение таким участником не менее чем за один год и (или) два года до даты подачи заявки на участие в конкурентной закупке, от двух и более договоров (контрактов), при этом все договоры (контракты) должны быть исполнены без применения к такому участнику неустоек (штрафов, пеней), заключённых по результатам конкурентных закупок. В этих случаях цена одного из договоров (контрактов) должна составлять не менее 20 (двадцати) процентов цены, по которой участником закупки предложено заключить договор в соответствии с настоящим разделом.

6.2.3. В случае неисполнения установленных требований победитель или участник закупки, с которым заключается договор, признаётся уклонившимся от заключения договора.

**6.3. Изменение договора**

6.3.1. При заключении, исполнении договора не допускается изменение его условий по сравнению с указанным в протоколе, составленном по результатам закупки, кроме случаев, предусмотренных настоящим пунктом.

6.3.2. Изменение договора в ходе его исполнения допускается по соглашению сторон.

6.3.3. Заказчик вправе изменить не более чем 10 процентов предусмотренный договором объём товаров, работ (услуг) при изменении потребности в таких товарах, работах (услугах), на выполнение, оказание которых заключён договор, или при выявлении потребности в дополнительном объёме товаров, работ (услуг), не предусмотренных договором, но связанных с работами (услугами), предусмотренными договором. Цена единицы дополнительно поставляемого товара, оказываемой услуги (работы) должна определяться как частное от деления первоначальной цены договора на предусмотренное в договоре количество такого товара, работы (услуги).

6.3.4. Заказчик вправе продлить срок действия договора (срок поставки товаров, оказание работ, услуг).

6.3.5. При исполнении договора по согласованию Заказчика с поставщиком, (подрядчиком, исполнителем) допускается поставка (использование) товара, качество, технические и функциональные характеристики (потребительские свойства) которого являются улучшенными по сравнению с таким качеством и такими характеристиками товара, указанными в договоре, при условии соблюдения положений Постановления № 1875.

**6.4. Условия расторжения договора**

6.4.1. Расторжение договора допускается по соглашению сторон, по решению суда, в случае одностороннего отказа стороны договора от исполнения договора в соответствии с гражданским законодательством.

6.4.2. Договор может быть расторгнут Заказчиком в одностороннем порядке в случае, если это было предусмотрено документацией о закупке и договором.

6.4.3. Заказчик обязан принять решение об одностороннем отказе от исполнения договора, если в ходе исполнения договора установлено, что поставщик (подрядчик, исполнитель) не соответствует установленным документацией о закупке требованиям к участникам закупки или предоставил недостоверную информацию о своём соответствии таким требованиям, что позволило ему стать победителем закупочной процедуры.

6.4.4. При расторжении договора в одностороннем порядке по вине поставщика (подрядчика, исполнителя) Заказчик обязан предъявить требование об уплате неустоек (штрафов, пеней) в связи с неисполнением или ненадлежащим исполнением обязательств, предусмотренных договором, а также обратиться к поставщику (подрядчику, исполнителю) с требованием о возмещении понесённых убытков при их наличии.

6.4.5. Расторжение договора влечёт за собой прекращение обязательств сторон договора по нему, но не освобождает от ответственности за неисполнение обязательств, которые имели место быть до расторжения договора.

6.4.6. Договор считается изменённым или расторгнутым с момента получения одной стороной уведомления другой стороны об одностороннем отказе от исполнения договора полностью или частично, если иной срок расторжения или изменения договора не предусмотрен в уведомлении либо не определён соглашением сторон.

**6.5. Обеспечение исполнения договора**

6.5.1. Если в Информационной карте, установлено требование к обеспечению исполнения договора, размер такого обеспечения:

1) не может превышать 5 процентов начальной (максимальной) цены договора (цены лота), если договором не предусмотрена выплата аванса;

2) устанавливается в размере аванса, если договором предусмотрена выплата аванса.

6.5.2. В случае установления в Информационной карте требования к обеспечению исполнения договора, такое обеспечение может предоставляться участником закупки по его выбору путём внесения денежных средств на счёт, указанный Заказчиком в Информационной карте или путём предоставления независимой гарантии.

6.5.3. При наличии в документации о закупке требования об обеспечении исполнения договора соответствующее обеспечение должно быть предоставлено участником закупки до заключения договора.

6.5.4. Независимая гарантия, предоставляемая в качестве обеспечения исполнения договора, заключаемого по результатам аукциона в электронной форме с участием субъектов малого и среднего предпринимательства, должна соответствовать следующим требованиям:

1) независимая гарантия должна быть выдана гарантом, предусмотренным частью 1 статьи 45 Федерального закона от 5 апреля 2013 года N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд";

2) независимая гарантия не может быть отозвана выдавшим ее гарантом;

3) независимая гарантия должна содержать:

а) 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;

б) перечень документов, подлежащих представлению заказчиком гаранту одновременно с требованием об уплате денежной суммы по независимой гарантии, в случае установления такого перечня Правительством Российской Федерации в соответствии с пунктом 4 части 32 статьи 3.4 Федерального закона № 223-ФЗ;

в) указание на срок ее действия, который не может составлять менее одного месяца с даты окончания предусмотренного извещением об осуществлении конкурентной закупки с участием субъектов малого и среднего предпринимательства, документацией о такой закупке срока исполнения основного обязательства;

4) независимая гарантия не должна содержать условие о представлении заказчиком гаранту судебных актов, подтверждающих неисполнение участником закупки обязательств, обеспечиваемых независимой гарантией;

5) информация о независимой гарантии должна быть включена в реестр независимых гарантий, предусмотренный частью 8 статьи 45 Федерального закона № 44-ФЗ;

Несоответствие независимой гарантии, предоставленной участником закупки с участием субъектов малого и среднего предпринимательства, требованиям, предусмотренным настоящим пунктом, является основанием для отказа в принятии ее заказчиком.

Гарант в случае просрочки исполнения обязательств по независимой гарантии, требование об уплате денежной суммы по которой соответствует условиям такой независимой гарантии и предъявлено заказчиком до окончания срока ее действия, обязан за каждый день просрочки уплатить заказчику неустойку (пени) в размере 0,1 процента денежной суммы, подлежащей уплате по такой независимой гарантии.

Правительство Российской Федерации вправе установить:

1) типовую форму независимой гарантии, предоставляемой в качестве обеспечения заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства, типовую форму независимой гарантии, предоставляемой в качестве обеспечения исполнения договора, заключаемого по результатам такой закупки;

2) форму требования об уплате денежной суммы по независимой гарантии, предоставленной в качестве обеспечения заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства, форму требования об уплате денежной суммы по независимой гарантии, предоставленной в качестве обеспечения исполнения договора, заключаемого по результатам такой закупки;

3) дополнительные требования к независимой гарантии, предоставляемой в качестве обеспечения заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства, независимой гарантии, предоставляемой в качестве обеспечения исполнения договора, заключаемого по результатам такой закупки;

4) перечень документов, представляемых заказчиком гаранту одновременно с требованием об уплате денежной суммы по независимой гарантии, предоставленной в качестве обеспечения заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства, независимой гарантии, предоставленной в качестве обеспечения исполнения договора, заключаемого по результатам такой закупки;

5) особенности порядка ведения реестра независимых гарантий, предусмотренного частью 8 статьи 45 Федерального закона от 5 апреля 2013 года N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд", для целей Федерального закона № 223-ФЗ.

6.5.5. Независимая гарантия, предоставляемая в качестве обеспечения исполнения договора, должна быть составлена по типовой форме согласно приложению № 1 к постановлению Правительства Российской Федерации от 9 августа 2022 года № 1397 «О независимых гарантиях, предоставляемых в качестве обеспечения заявки на участие в конкурентной закупке товаров, работ, услуг в электронной форме с участием субъектов малого и среднего предпринимательства, и независимых гарантиях, предоставляемых в качестве обеспечения исполнения договора, заключаемого по результатам такой закупки, а также о внесении изменений в некоторые акты Правительства Российской Федерации» на условиях, определенных гражданским законодательством и Федеральным законом № 223-ФЗ.

6.5.6. В случае, если победитель закупки или участник закупки, с которым заключается договор, в вышеуказанный срок не представил Заказчику обеспечение исполнения договора, победитель закупки или участник закупки, с которым заключается договор признаётся уклонившимся от заключения договора.

6.5.7. В случае неисполнения обязательств или ненадлежащего исполнения обязательств по договору победителем закупки или участником закупки, с которым заключается договор в случае уклонения победителя закупки от заключения договора, денежные средства, внесённые ими в качестве обеспечения исполнения договора, не возвращаются.

6.5.8. При уклонении победителя закупки или иного лица, с которым заключается договор по итогам закупки, от заключения договора или от внесения обеспечения исполнения договора, денежные средства, внесённые в качестве обеспечения заявки, не возвращаются (если требование об обеспечении заявки указано в Информационной карте).

**6.6. Признание электронного аукциона несостоявшимся и порядок заключения договора при несостоявшемся электронном аукционе**

6.6.1. Электронный аукцион признаётся несостоявшимся, если:

- по окончании срока подачи заявок на участие в электронном аукционе подана только одна заявка на участие в таком электронном аукционе;

- не подано ни одной заявки;

- на основании результатов рассмотрения заявок на участие в электронном аукционе принято решение об отказе в допуске к участию в электронном аукционе всех участников закупки, подавших заявки на участие в электронном аукционе;

- принято решение о допуске к участию в электронном аукционе, признании участником электронного аукциона только одного участника закупки, подавшего заявку на участие в электронном аукционе.

6.6.2. В случае, если документацией о закупке предусмотрено два и более лота, электронный аукцион признаётся несостоявшимся только в отношении отдельных лотов.

6.6.3. Заказчик обязан заключить договор, если электронный аукцион признан несостоявшимся по следующим основаниям:

— по окончании срока подачи заявок на участие в электронном аукционе подана только одна заявка, и она признана соответствующей требованиям документации о закупке;

— по результатам рассмотрения заявок на участие в электронном аукционе только одна заявка признана соответствующей требованиям документации о закупке;

6.6.4. Заказчик вправе заключить договор с единственным поставщиком (исполнителем, подрядчиком) или провести повторный электронный аукцион на тех же или иных условиях либо провести закупку иным способом в соответствии с Положением о закупках, если электронный аукцион был признан несостоявшимся по следующим причинам:

— по результатам рассмотрения заявок на участие в аукционе были отклонены все поданные заявки;

— по окончании срока подачи заявок на участие в аукционе в электронной форме не подано ни одной заявки.

6.6.5. При осуществлении закупки Заказчик вправе по истечении срока приёма заявок осуществить закупку без применения особенностей проведения электронного аукциона у СМСП, в случаях, если:

1) субъекты малого и среднего предпринимательства не подали заявки на участие в такой закупке;

2) заявки всех участников закупки, являющихся субъектами малого и среднего предпринимательства, отозваны или не соответствуют требованиям, предусмотренным документацией о закупке;

3) заявка, поданная единственным участником закупки, являющимся субъектом малого и среднего предпринимательства, не соответствует требованиям документации о закупке;

4) Заказчик, принял решение о том, что договор по результатам закупки не заключается.

6.6.6. Если договор по результатам закупки не заключён, Заказчик вправе отменить решение о подведении итогов закупки, принятое по результатам такой закупки, и осуществить закупку без применения особенностей проведения электронного аукциона у СМСП.

**РАЗДЕЛ II. ИНФОРМАЦИОННАЯ КАРТА АУКЦИОНА В ЭЛЕКТРОННОЙ ФОРМЕ**

|  |  |  |
| --- | --- | --- |
| № п/п | **Наименование пункта** | **Текст пояснений** |
| 1 | Наименование заказчика, контактная информация | Муниципальное унитарное предприятие «Водоканал» г.Йошкар-Олы» муниципального образования «Город Йошкар-Ола» (сокращенное наименование – МУП «Водоканал»);  Место нахождения - 424039, Республика Марий Эл, г. Йошкар-Ола, ул. Дружбы, д. 2;  Почтовый адрес - 424039, Республика Марий Эл, г. Йошкар-Ола, ул. Дружбы, д. 2;  Адрес электронной почты - log@vod12.ru;  Номер контактного телефона - (8362) 64-57-62  Ответственное лицо за размещение закупки - Ерсулова Анна Викторовна |
| 2 | Способ осуществления закупки | Аукцион в электронной форме, участниками которого могут быть только субъекты малого и среднего предпринимательства |
| 3 | Количество лотов | 1 (один) |
| 4 | Предмет договора | Оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения |
| 5 | Классификация товаров, работ, услуг. | ОКПД2:58.29.50.000 Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение  ОКВЭД2: 58.29 Издание прочих программных продуктов |
| 6 | Адрес электронной площадки | http://www.rts-tender.ru (ООО «"РТС-тендер" – Электронная торговая площадка») |
| 7 | Место, условия и сроки (периоды) поставки товара, выполнения работ, оказания услуг | Место поставки товара: РМЭ, г. Йошкар-Ола, ул. Дружбы, д. 2;  Срок поставки товара, выполнения работ, оказания услуг: Срок оказания услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения в течение 3 рабочих дней после заключения Договора.  Условия поставки товара, выполнения работ, оказания услуг: Срок действия продления неисключительных (лицензионных) прав использования антивирусного программного обеспечения составляет 2 года. |
| 8 | Источник финансирования заказа | Собственные средства МУП «Водоканал» |
| 9 | Начальная (максимальная) цена договора (цена лота) | **596 200 (Пятьсот девяносто шесть тысяч двести) руб. 50 коп.** |
| 10 | Количество, требования к безопасности, качеству, техническим характеристикам, функциональным характеристикам (потребительским свойствам) товара, работы, услуги | 150 штук;  Описание объекта закупки представлено в Разделе III «Техническое задание» настоящей документации. |
| 11 | Валюта, использованная для формирования цены договора и расчета с поставщиками (исполнителями, подрядчиками). Порядок применения официального курса иностранной валюты к рублю РФ, установленного ЦБ и используемого при оплате заключенного договора | Российский рубль |
| 12 | Порядок формирования цены договора (цены лота) | Цена Договора включает в себя все расходы, связанные с оказанием услуг, предусмотренных Договором в полном объеме, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей, а также иные расходы, связанные с использованием Исполнителем своих обязательств по Договору. |
| 13 | Обоснование и порядок формирования начальной максимальной цены договора | Начальная (максимальная) цена договора рассчитывается методом сопоставления рыночных цен (анализа рынка) и заключается в установлении НМЦД на основании информации о рыночных ценах (далее — ценовая информация) идентичных товаров, планируемых к закупкам, а при их отсутствии — однородных товаров. В этом случае определение стоимости товаров, работ, услуг производится посредством изучения ценовых предложений, включая структуру цены, от не менее, чем трёх поставщиков (подрядчиков, исполнителей), осуществляющих такие услуги.  Сведения о начальной (максимальной) цене единицы каждого товара приведены в Разделе V «Сведения о начальной (максимальной) цене единицы каждого товара, работы, услуги» |
| 14 | Ограничение участия в закупке для участников | Установлено.  **Закупка, участниками которой являются только субъекты малого и среднего предпринимательства.**  Подтверждением принадлежности участника закупки к субъектам малого и среднего предпринимательства является наличие информации о таком участнике в едином реестре субъектов малого и среднего предпринимательства. |
| 15 | Единые обязательные требования к участникам закупки | 1) непроведение ликвидации участника конкурентной закупки с участием субъектов малого и среднего предпринимательства - юридического лица и отсутствие решения арбитражного суда о признании участника такой закупки - юридического лица или индивидуального предпринимателя несостоятельным (банкротом);  2) неприостановление деятельности участника конкурентной закупки с участием субъектов малого и среднего предпринимательства в порядке, установленном Кодексом Российской Федерации об административных правонарушениях;  3) отсутствие у участника конкурентной закупки с участием субъектов малого и среднего предпринимательства недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает двадцать пять процентов балансовой стоимости активов участника такой закупки, по данным бухгалтерской (финансовой) отчетности за последний отчетный период. Участник такой закупки считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по данному заявлению на дату рассмотрения заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства не принято;  4) отсутствие у участника конкурентной закупки с участием субъектов малого и среднего предпринимательства - физического лица, зарегистрированного в качестве индивидуального предпринимателя, либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - участника конкурентной закупки с участием субъектов малого и среднего предпринимательства непогашенной или неснятой судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, 290, 291, 291.1 Уголовного кодекса Российской Федерации, а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся предметом осуществляемой закупки, и административного наказания в виде дисквалификации;  5) отсутствие фактов привлечения в течение двух лет до момента подачи заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства участника такой закупки - юридического лица к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях;  6) соответствие участника конкурентной закупки с участием субъектов малого и среднего предпринимательства указанным в документации о конкурентной закупке требованиям законодательства Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом закупки, если в соответствии с законодательством Российской Федерации информация и документы, подтверждающие такое соответствие, содержатся в открытых и общедоступных государственных реестрах, размещенных в информационно-телекоммуникационной сети "Интернет";  7) обладание участником конкурентной закупки с участием субъектов малого и среднего предпринимательства исключительными правами на результаты интеллектуальной деятельности, если в связи с исполнением договора заказчик приобретает права на такие результаты;  8) обладание участником конкурентной закупки с участием субъектов малого и среднего предпринимательства правами использования результата интеллектуальной деятельности в случае использования такого результата при исполнении договора; |
| 15.1 | Требование об отсутствии сведений об участнике закупки в реестре недобросовестных поставщиков, предусмотренном ст. 5 Федерального закона 223-ФЗ, и (или) в реестре недобросовестных поставщиков, предусмотренном Федеральным законом от 5 апреля 2013 года N 44-ФЗ. | Установлено |
| 15.2 | Требование к участникам закупки | Участником закупки может является любое юридическое лицо или несколько юридических лиц, выступающих на стороне одного участника закупки, независимо от организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала, за исключением юридического лица, являющегося иностранным агентом в соответствии с Федеральным законом от 14 июля 2022 года N 255-ФЗ "О контроле за деятельностью лиц, находящихся под иностранным влиянием", либо любое физическое лицо/несколько физических лиц, выступающих на стороне одного участника закупки, в том числе индивидуальный предприниматель или несколько индивидуальных предпринимателей, выступающих на стороне одного участника закупки, за исключением физического лица, являющегося иностранным агентом в соответствии с Федеральным законом от 14 июля 2022 года N 255-ФЗ "О контроле за деятельностью лиц, находящихся под иностранным влиянием". Участник закупки для участия в конкурентной закупке подает заявку на участие в закупке. |
| 16 | Информация о запрете или об ограничении закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами, о преимуществе в отношении товаров российского происхождения (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), работ, услуг, соответственно выполняемых, оказываемых российскими лицами, в случае, если такие запрет, ограничение, преимущество установлены в соответствии с пунктом 1 части 2 статьи 3.1-4 Федерального закона №223-ФЗ в отношении товара, работы, услуги, являющихся предметом закупки | В соответствии с положениями Постановления Правительства РФ от 23.12.2024 № 1875 «О мерах по предоставлению национального режима при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, закупок товаров, работ, услуг отдельными видами юридических лиц» (далее также – Постановление № 1875) **установлен запрет** закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными гражданами, иностранными юридическими лицами (далее - иностранные лица), по перечню согласно приложению № 1 Постановления № 1875. |
| 16.1 | Порядок рассмотрения заявок на участие в аукционе в электронной форме | Правительством Российской Федерации установлен запрет закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств, вследствие чего не допускаются:  • заключение договора на поставку такого товара;  • при исполнении договора замена такого товара на происходящий из иностранного государства товар, в отношении которого установлен данный запрет; |
| 17 | Внесение платы за предоставление документации о закупке на бумажном носителе | Документация о закупке предоставляется бесплатно |
| 18 | Форма, сроки и порядок оплаты поставляемого товара, выполненной работы, оказанной услуги | Оплата производится по безналичному расчету путем перечисления на расчетный счет Исполнителя в течение 7 (семи) рабочих дней после продления неисключительных (лицензионных) прав использования антивирусного программного обеспечения и подписания акта приема-передачи прав ответственными лицами Исполнителя и Заказчика. |
| 19 | Размер обеспечения заявок на участие в электронном аукционе | Не требуется |
| 20 | Дата и время окончания срока предоставления участникам закупки разъяснений положений документации о закупке | Начало предоставления разъяснений участникам закупки – «18» марта 2025;  Окончание предоставления разъяснений участникам закупки – «25» марта 2025 г. в 17 час.00 мин.  В течение 3 (трёх) рабочих дней с даты поступления запроса Заказчик размещает разъяснения в единой информационной системе, при условии, что указанный запрос поступил Заказчику не позднее чем за 3 (три) рабочих дня до дня окончания подачи заявок на участие в электронном аукционе. |
| 21 | Дата начала, дата и время окончания срока подачи заявок на участие в электронном аукционе | Дата начала срока подачи заявок - **«18» марта 2025 г.**  Дата и время окончания срока подачи заявок – **«26» марта 2025 г. в 10 часов 00 минут (время московское)** |
| 22 | Дата окончания срока рассмотрения первых частей заявок на участие в электронном аукционе | **«28» марта 2025 г.** |
| 23 | Дата проведения электронного аукциона | **31.03.2025г. в 10 час. 00 мин. (время московское)** |
| 24 | Дата рассмотрения вторых частей заявок и подведения итогов | **01.04.2025г.** |
| 25 | Требования к содержанию и составу заявки | **Первая часть заявки на участие в электронном аукционе должна содержать следующие информацию и документы:**  **1)** предложение участника конкурентной закупки с участием субъектов малого и среднего предпринимательства в отношении предмета закупки;  Предложение должно содержать конкретные показатели товара, соответствующие значениям, установленным документацией о закупке (Разделом III «Техническое задание»).  Первая часть заявки может содержать эскиз, рисунок, чертёж, фотографию, иное изображение товара, на поставку которого размещается заказ.  При этом не допускается указание в первой части заявки на участие в электронном аукционе сведений об участнике закупки и (или) о ценовом предложении.  Рекомендуемая форма первой части заявки приведена в Разделе VI «Инструкция по заполнению заявок на участие в электронном аукционе».  **Вторая часть заявки на участие в электронном аукционе должна содержать следующие информацию и документы:**  **1)** наименование, фирменное наименование (при наличии), адрес юридического лица в пределах места нахождения юридического лица, учредительный документ, если участником конкурентной закупки с участием субъектов малого и среднего предпринимательства является юридическое лицо;  **2)** фамилия, имя, отчество (при наличии), паспортные данные, адрес места жительства физического лица, зарегистрированного в качестве индивидуального предпринимателя, если участником конкурентной закупки с участием субъектов малого и среднего предпринимательства является индивидуальный предприниматель;  **3)** идентификационный номер налогоплательщика участника конкурентной закупки с участием субъектов малого и среднего предпринимательства или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика (для иностранного лица);  **4)** идентификационный номер налогоплательщика (при наличии) учредителей, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа юридического лица, если участником конкурентной закупки с участием субъектов малого и среднего предпринимательства является юридическое лицо, или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика таких лиц;  **5)** копия документа, подтверждающего полномочия лица действовать от имени участника конкурентной закупки с участием субъектов малого и среднего предпринимательства, за исключением случаев подписания заявки:  а) индивидуальным предпринимателем, если участником такой закупки является индивидуальный предприниматель;  б) лицом, указанным в едином государственном реестре юридических лиц в качестве лица, имеющего право без доверенности действовать от имени юридического лица (далее в настоящей главе - руководитель), если участником такой закупки является юридическое лицо;  **6)** копии документов, подтверждающих соответствие участника конкурентной закупки с участием субъектов малого и среднего предпринимательства требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом закупки, за исключением случая, если в соответствии с законодательством Российской Федерации информация и документы, подтверждающие такое соответствие, содержатся в открытых и общедоступных государственных реестрах, размещенных в информационно-телекоммуникационной сети "Интернет" (с указанием адреса сайта или страницы сайта в информационно-телекоммуникационной сети "Интернет", на которых размещены эти информация и документы) - *требование не установлено*;  **7)** копия решения о согласии на совершение крупной сделки или о последующем одобрении этой сделки, если требование о наличии указанного решения установлено законодательством Российской Федерации и для участника конкурентной закупки с участием субъектов малого и среднего предпринимательства заключение по результатам такой закупки договора либо предоставление обеспечения заявки на участие в такой закупке (если требование об обеспечении заявок установлено заказчиком в извещении об осуществлении такой закупки, документации о конкурентной закупке), обеспечения исполнения договора (если требование об обеспечении исполнения договора установлено заказчиком в извещении об осуществлении такой закупки, документации о конкурентной закупке) является крупной сделкой;  **8)** декларация, подтверждающая на дату подачи заявки на участие в конкурентной закупке с участием субъектов малого и среднего предпринимательства соответствие участника закупки требованиям, установленным в соответствии с п.15 настоящей Информационной карты *(представляется в составе заявки участником закупки с использованием программно-аппаратных средств электронной площадки);*  **9)** копии документов, подтверждающих соответствие товара, работы или услуги, являющихся предметом закупки, требованиям, установленным в соответствии с законодательством Российской Федерации, в случае, если требования к данным товару, работе или услуге установлены в соответствии с законодательством Российской Федерации и перечень таких документов предусмотрен документацией о конкурентной закупке. При этом не допускается требовать представление указанных документов, если в соответствии с законодательством Российской Федерации они передаются вместе с товаром;  **10)** **информация и документы, подтверждающие страну происхождения товаров, в отношении которых установлен запрет закупок товаров (в том числе поставляемых при выполнении закупаемых работ, оказании закупаемых услуг), происходящих из иностранных государств:**  а) для подтверждения происхождения программ для электронных вычислительных машин и (или) баз данных (далее - программное обеспечение) из Российской Федерации  **- порядковый номер реестровой записи из единого реестра российских программ для электронных вычислительных машин и баз данных (далее - реестр российского программного обеспечения);**  б) для подтверждения происхождения программного обеспечения из Российской Федерации и его соответствия дополнительным требованиям к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, утвержденным постановлением Правительства Российской Федерации от 23 марта 2017 г. № 325 "Об утверждении дополнительных требований к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения, и внесении изменений в Правила формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных" (далее - дополнительные требования к программному обеспечению),  **- порядковый номер реестровой записи из реестра российского программного обеспечения, содержащей информацию о соответствии программного обеспечения дополнительным требованиям к программному обеспечению;**  в) для подтверждения происхождения программного обеспечения из государств - членов Евразийского экономического союза, за исключением Российской Федерации,  **- порядковый номер реестровой записи из единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации (далее - реестр евразийского программного обеспечения);**  г) для подтверждения происхождения программного обеспечения из государств - членов Евразийского экономического союза, за исключением Российской Федерации, и его соответствия дополнительным требованиям к программному обеспечению  **- порядковый номер реестровой записи из реестра евразийского программного обеспечения, содержащей информацию о соответствии программного обеспечения дополнительным требованиям к программному обеспечению;** |
| 26 | Размер обеспечения исполнения договора | 5 процентов от начальной (максимальной) цены договора – 29 810 (Двадцать девять тысяч восемьсот десять) рублей 03 копейки.  Предоставляется до момента заключения договора. Исполнение договора может обеспечиваться независимой гарантией или внесением денежных средств на счет Заказчика. Способ обеспечения исполнения договора определяется победителем электронного аукциона или иным участником, с которым заключается договор при уклонении победителя от подписания договора, самостоятельно.  В случае если предложенная участником закупки цена снижена на двадцать пять и более процентов по отношению к начальной (максимальной) цене Договора, участник закупки, с которым заключается Договор, предоставляет обеспечение исполнения Договора в размере, превышающем в полтора раза размер обеспечения исполнения Договора, что составляет 44 715 (Сорок четыре тысячи семьсот пятнадцать) рублей 05 копеек или предоставляет информацию, подтверждающую добросовестность Поставщика. |
| 27 | Реквизиты заказчика для внесения обеспечения исполнения договора | **Получатель: Муниципальное унитарное предприятие «Водоканал» г.Йошкар-Олы» муниципального образования «Город Йошкар-Ола»;**  **ИНН 1215020390**  **КПП 121501001**  **Расчетный счет 40702810300000050227**  **Банк получателя: Банк ГПБ (АО)**  **Корреспондентский счет 30101810200000000823**  **БИК 044525823**  **В назначении платежа указать:** «Средства для обеспечения исполнения Договора по объекту закупки: «Оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения». |
| 28 | Изменение договора | Изменение договора в ходе его исполнения допускается по соглашению сторон:  - Заказчик вправе изменить не более чем 10 процентов предусмотренный договором объём товаров, работ (услуг) при изменении потребности в таких товарах, работах (услугах), на выполнение, оказание которых заключён договор, или при выявлении потребности в дополнительном объёме товаров, работ (услуг), не предусмотренных договором, но связанных с работами (услугами), предусмотренными договором. Цена единицы дополнительно поставляемого товара, оказываемой услуги (работы) должна определяться как частное от деления первоначальной цены договора на предусмотренное в договоре количество такого товара, работы (услуги);  - Заказчик вправе продлить срок действия договора (срок поставки товаров, оказание работ, услуг);  - при исполнении договора по согласованию Заказчика с поставщиком, (подрядчиком, исполнителем) допускается поставка (использование) товара, качество, технические и функциональные характеристики (потребительские свойства) которого являются улучшенными по сравнению с таким качеством и такими характеристиками товара, указанными в договоре, при условии соблюдения положений Постановления № 1875. |

**РАЗДЕЛ III. ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

Заказчик заявляет продление неисключительных (лицензионных) прав антивирусного программного обеспечения на уже приобретенный и используемый программный продукт Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 100-149, сроком на 2 года. Номер лицензии 2B1E-230403-071837-1-39009. Количество рабочих мест 150 (Лицензирование количества компонентов защиты рабочих станций и файловых серверов должно быть универсальным и ограничиваться только общим количеством защищаемых объектов). Участник размещения заказа не вправе предложить эквивалент, т.к. предложение другого антивирусного программного обеспечения не обеспечит совместимости с существующим у Заказчика программным обеспечением.

Согласно закону о закупках товаров, работ, услуг отдельными видами юридических лиц, заказчик заявляет о необходимости предоставления в рамках услуги средств защиты информации, совместимых с существующим у Заказчика программным обеспечением Kaspersky Security Center.

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование | Единица измерения | Количество |
| 1 | Продление лицензии Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 100-149 Node 2 year Renewal License | шт. | 150 |

* **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 мобильных устройств (смартфонов и планшетов);
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ и атак;
* эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

* **Требования к программным средствам антивирусной защиты для рабочих станций Windows**

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:

* Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;
* Windows 8 Professional / Enterprise (32 / 64-разрядная);
* Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
* Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise/Enterprise multi-session;
* Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise

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

* + антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
  + антивирусное сканирование по расписанию;
  + антивирусное сканирование подключаемых устройств;
  + эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
  + нейтрализации действий активного заражения;
  + анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
  + анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
  + блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
  + откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
  + ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
  + облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
  + антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
  + защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
  + фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
  + проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
  + блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
  + распознавания и блокировку фишинговых и небезопасных сайтов;
  + встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
  + защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
  + защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
  + контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
  + создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
  + контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
  + управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
  + записи в журнал событий о записи и/или удалении файлов на съемных дисках;
  + назначение приоритета для правил доступа к устройствам с файловой системой;
  + контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
  + защиты от атак типа BadUSB;
  + 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;
  + возможность 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 создание 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.
* **Требования к программным средствам антивирусной защиты для серверов Windows**

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий:

* Windows Small Business Server 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;
* Windows MultiPoint Server 2011 (64-разрядная);
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая Core Mode)

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 (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.
* **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:

* macOS 11 - 13;

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;
* установки из файла .pkg через JAMF;
* 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:

* CentOS 6.7 и выше.
* Debian GNU/Linux 10.1 и выше.
* Debian GNU/Linux 11.
* Mageia 4.
* Red Hat Enterprise Linux 6.7 и выше.
* Альт 8 СП Рабочая Станция.
* Альт 8 СП Сервер.
* Альт Образование 10.
* Альт Рабочая Станция 10.

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

* AlmaLinux OS 8 и выше.
* AlmaLinux OS 9 и выше.
* AlterOS 7.5 и выше.
* Amazon Linux 2.
* Astra Linux Common Edition 2.12.
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
* Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
* CentOS 6.7 и выше.
* CentOS 7.2 и выше.
* CentOS Stream 9.
* Debian GNU/Linux 10.1 и выше.
* Debian GNU/Linux 11 и выше.
* EMIAS 1.0.
* EulerOS 2.0 SP5.
* LinuxMint 20.3 и выше.
* LinuxMint 21.1.
* openSUSE Leap 15.0 и выше.
* Oracle Linux 7.3 и выше.
* Oracle Linux 8.0 и выше.
* Oracle Linux 9.0 и выше
* Red Hat Enterprise Linux 6.7 и выше.
* Red Hat Enterprise Linux 7.2 и выше.
* Red Hat Enterprise Linux 8.0 и выше.
* Red Hat Enterprise Linux 9 и выше.
* Rocky Linux 8.5 и выше.
* Rocky Linux 9.1.
* SUSE Linux Enterprise Server 12.5 и выше.
* SUSE Linux Enterprise Server 15 и выше.
* Ubuntu 20.04 LTS.
* Ubuntu 22.04 LTS.
* Альт 8 СП Рабочая станция.
* Альт 8 СП Сервер.
* Альт Образование 10.
* Альт Рабочая Станция 10.
* Альт Сервер 10.
* Атлант, сборка Alcyone, версия 2022.02.
* Гослинукс 7.17.
* Гослинукс 7.2.
* РЕД ОС 7.3.
* РОСА "Кобальт" 7.9.
* РОСА "Хром" 12.

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

* Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
* EulerOS 2.0 SP8.
* SUSE Linux Enterprise Server 15 SP3 и выше.
* Ubuntu 20.04 LTS.
* Альт 8 СП.
* РЕД ОС 7.3.

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

* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* возможность проверки памяти ядра;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plain text);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* включения опции блокирования файлов во время проверки;
* помещение подозрительных и поврежденных объектов на карантин;
* перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
* управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
* проверки съемных дисков;
* отслеживания во входящем сетевом трафике активности, характерной для сетевых атак;
* проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым
* получения данных о действиях программ на компьютере пользователя;
* 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.
* **Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows**

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

32-разрядных операционных систем Microsoft Windows

* Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше.

64-разрядных операционных систем Microsoft Windows

* Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Microsoft Small Business Server 2008 Standard / Premium SP2 или выше;
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
* Microsoft Small Business Server 2011 Essentials / Standard SP1 или выше;
* Microsoft Windows MultiPoint Server 2011 Standard / Premium;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
* Microsoft MultiPoint Server 2012 Standard / Premium;
* Windows Storage Server 2012;
* Windows Hyper-V Server 2012;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
* Windows Storage Server 2012 R2;
* Windows Hyper-V Server 2012 R2;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2016 MultiPoint;
* Windows Server 2016 Core Standard / Datacenter;
* Microsoft Windows MultiPoint Server 2016;
* Windows Storage Server 2016;
* Windows Hyper-V Server 2016;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2019 Core;
* Windows Storage Server 2019;
* Windows Hyper-V Server 2019;
* Windows Server 2022;
* Windows 10 Enterprise multi-session.

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

* антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
* защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
* непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
* анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* добавлять процессы в список защищаемых;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
* настройки проверки критических областей сервера в качестве отдельной задачи;
* регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
* продолжать антивирусное сканирование в фоновом режиме;
* наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
* ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
* интеграции с SIEM системами;
* указания количества рабочих процессов антивируса вручную;
* отключить графический интерфейс;
* наличие удаленной и локальной консоли управления;
* управления параметрами антивируса из командной строки;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
* включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.
* контроль устройств, в том числе сетевых карт и модемов;
* веб-контроль;
* защита от почтовых угроз (плагин для Outlook);
* защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления;
* 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);
* создания специальных правил должно контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
* создания специальных правил должно работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должно иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
* осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем;
* информирование администратора о подключении внешних устройств;
* наличие механизмов автоматической генерации правил для контроля устройств и приложений;
* **Требования к программным средствам антивирусной защиты мобильных устройств**

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

* Android 5.0–13 (включая Android 12L, исключая Go Edition);
* iOS 10–16 или iPadOS 13–15;

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

* постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
* проверка файловой системы устройства по требованию и по расписанию;
* мгновенная проверка устанавливаемых приложений
* блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* наличие хранилища для изолирования зараженных объектов;
* обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
* блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
* поддержка белых списков разрешенных приложений;
* блокировка системных приложений, в рамках контроля запуска приложений;
* отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);
* заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
* указать параметры подключения к wi-fi сетям;
* указать обязательные к установке приложения;
* блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
* создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
* поддержка технологий Samsung KNOX1 и KNOX2;
* 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 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:

* Windows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;
* Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
* Windows Server 2012 Server Core 64-разрядная;
* Windows Server 2012 Datacenter 64-разрядная;
* Windows Server 2012 Essentials 64-разрядная;
* Windows Server 2012 Foundation 64-разрядная;
* Windows Server 2012 Standard 64-разрядная;
* Windows Server 2012 R2 Server Core 64-разрядная;
* Windows Server 2012 R2 Datacenter 64-разрядная;
* Windows Server 2012 R2 Essentials 64-разрядная;
* Windows Server 2012 R2 Foundation 64-разрядная;
* Windows Server 2012 R2 Standard 64-разрядная;
* Windows Server 2016 Datacenter (LTSB) 64-разрядная;
* Windows Server 2016 Standard (LTSB) 64-разрядная;
* Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
* Windows Server 2019 Standard 64-разрядная;
* Windows Server 2019 Datacenter 64-разрядная;
* Windows Server 2019 Core 64-разрядная;
* Windows Server 2022 Standard 64-разрядная;
* Windows Server 2022 Datacenter 64-разрядная;
* Windows Server 2022 Core 64-разрядная;
* Windows Storage Server 2012 64-разрядная;
* Windows Storage Server 2012 R2 64-разрядная;
* Windows Storage Server 2016 64-разрядная;
* Windows Storage Server 2019 64-разрядная.

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

* VMware vSphere 6.7;
* VMware vSphere 7.0;
* VMware Workstation 16 Pro;
* Microsoft Hyper-V Server 2012 64-разрядная;
* Microsoft Hyper-V Server 2012 R2 64-разрядная;
* Microsoft Hyper-V Server 2016 64-разрядная;
* Microsoft Hyper-V Server 2019 64-разрядная;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 17;
* Oracle VM VirtualBox 6.x.

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

* Microsoft SQL Server 2012 Express 64-разрядная.
* Microsoft SQL Server 2014 Express 64-разрядная.
* Microsoft SQL Server 2016 Express 64-разрядная.
* Microsoft SQL Server 2017 Express 64-разрядная.
* Microsoft SQL Server 2019 Express 64-разрядная.
* Microsoft SQL Server 2014 (все редакции) 64-разрядная.
* Microsoft SQL Server 2016 (все редакции) 64-разрядная.
* Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная.
* Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная.
* Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная.
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная.
* Microsoft Azure SQL Database.
* Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure.
* MySQL 5.7 Community 32-разрядная/64-разрядная.
* MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
* MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* PostgreSQL 13.x 64-разрядная.
* PostgreSQL 14.х 64-разрядная.
* Postgres Pro 13.x (все редакции).
* Postgres Pro 14.x (все редакции).

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

* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
* автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
* указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* иерархии триггеров, по которым происходит перераспределение;
* тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* инвентаризация установленного ПО и оборудования на компьютерах пользователей;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер Exchange ActiveSync;
* функция управления мобильными устройствами через сервер iOS MDM;
* отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* интеграции по OpenAPI;
* управления антивирусной защитой с использованием WEB консоли;
* 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.
* **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:

* Debian GNU/Linux 9.х (Stretch) 32-разрядная/64-разрядная.
* Debian GNU/Linux 10.х (Buster) 32-разрядная/64-разрядная.
* Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная.
* Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная.
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная.
* Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
* CentOS 7.x 64-разрядная.
* Red Hat Enterprise Linux Server 7.x 64-разрядная.
* Red Hat Enterprise Linux Server 8.x 64-разрядная.
* Red Hat Enterprise Linux Server 9.x 64-разрядная.
* SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
* SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
* Astra Linux Special Edition RUSB.10015-01 (обновление 1.6) 64-разрядная.
* Astra Linux Special Edition RUSB.10015-01 (обновление 1.7) 64-разрядная.
* Astra Linux Common Edition (обновление 2.12) 64-разрядная.
* Альт Сервер 9.2 64-разрядная.
* Альт Сервер 10 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная.
* Oracle Linux 7 64-разрядная.
* Oracle Linux 8 64-разрядная.
* Oracle Linux 9 64-разрядная.
* РЕД ОС 7.3 Сервер 64-разрядная.
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

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

* VMware vSphere 6.7.
* VMware vSphere 7.0;
* VMware Workstation 16 Pro;
* Microsoft Hyper-V Server 2012 64-разрядная;
* Microsoft Hyper-V Server 2012 R2 64-разрядная;
* Microsoft Hyper-V Server 2016 64-разрядная;
* Microsoft Hyper-V Server 2019 64-разрядная;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 17;
* Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
* Альт Сервер 10 64-разрядная;
* Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
* РЕД ОС 7.3 Сервер 64-разрядная;
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная

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

* MySQL 5.7 Community 32-разрядная/64-разрядная.
* MySQL 8.0 32-разрядная/64-разрядная.
* MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* PostgreSQL 13.х 64-разрядная.
* PostgreSQL 14.х 64-разрядная.
* Postgres Pro 13.х (все редакции) 64-разрядная.
* Postgres Pro 14.х (все редакции) 64-разрядная.

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

* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* иерархии триггеров, по которым происходит перераспределение;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* наличие системы контроля возникновения вирусных эпидемий;
* управления антивирусной защитой с использованием WEB консоли;
* возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
* возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
* возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули;
* выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных.
* **Требования к обновлению антивирусных баз**

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

* + создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;
  + множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
  + проверку целостности и подлинности обновлений средствами электронной цифровой подписи.
* **Требования к эксплуатационной документации**

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

* «Руководство пользователя (администратора)»

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

* **Требования к технической поддержке**

Техническая поддержка антивирусного программного обеспечения должна:

* Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по электронной почте и через Интернет.
* Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

**РАЗДЕЛ IV.ПРОЕКТ ДОГОВОРА**

**Договор № \_\_\_\_\_\_\_**

**на оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения**

г. Йошкар-Ола «\_\_\_» \_\_\_\_\_\_\_\_ 2025 г.

Муниципальное унитарное предприятие «Водоканал» г. Йошкар-Олы» муниципального образования «Город Йошкар-Ола», именуемое в дальнейшем «Заказчик», в лице \_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_, с одной стороны и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем «Исполнитель», в лице \_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, в дальнейшем вместе именуемые «Стороны», и каждый в отдельности «Сторона», с соблюдением требований Гражданского кодекса Российской Федерации, Федерального закона от 18.07.2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (далее – Закон № 223-ФЗ), Положения о закупке товаров, работ, услуг Муниципального унитарного предприятия «Водоканал» г. Йошкар-Олы» муниципального образования «Город Йошкар-Ола» от 05.09.2018г. (в редакции от 23.12.2024 г., далее по тексту «Положение») и на условиях, предусмотренных извещением об осуществлении закупки, документацией о закупке, заявкой, на основании результатов аукциона в электронной форме (Протокол № \_\_\_\_\_\_от \_\_\_\_\_),заключили настоящий договор (далее по тексту - «Договор») о нижеследующем:

**1. ПРЕДМЕТ ДОГОВОРА**

1.1. Исполнитель обязуется качественно, в установленный настоящим Договором срок и в пределах установленной настоящим Договором цены на оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения оказать услуги и сдать результат Заказчику, а Заказчик обязуется принять результат надлежащим образом оказанных услуг и оплатить их.

1.2. Услуги оказываются в соответствии с Техническим заданием, являющемся неотъемлемой частью настоящего Договора (Приложение № 1 к настоящему Договору).

**2. ЦЕНА ДОГОВОРА**

2.1. Цена Договора составляет: \_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей \_\_ коп., в том числе НДС\_\_\_\_ (либо НДС не облагается).

2.2. Валютой для установления цены Договора и расчетов с Исполнителем является рубль Российской Федерации.

2.3. Источник финансирования Договора – собственные средства МУП «Водоканал».

2.4. Цена Договора включает в себя все расходы, связанные с оказанием услуг, предусмотренных Договором в полном объеме, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей, а также иные расходы, связанные с использованием Исполнителем своих обязательств по Договору.

2.5. Цена Договора является твердой, определяется на весь срок исполнения Договора и не может изменяться в ходе его исполнения, за исключением их изменения по соглашению сторон с учетом положений законодательства Российской Федерации в следующих случаях:

2.5.1. при снижении цены Договора без изменения предусмотренных Договором объема оказанных услуг, качества оказанных услуг и иных условий Договора;

2.5.2. если по предложению Заказчика увеличиваются предусмотренные Договором объем оказанных услуг не более чем, на десять процентов или уменьшаются предусмотренные Договором объем оказанных услуг не более, чем на десять процентов. При этом по соглашению сторон допускается изменение с учетом  
положений бюджетного законодательства Российской Федерации цены Договора пропорционально дополнительному объему услуг исходя из установленной в Договоре цены единицы услуги, но не более, чем на десять процентов цены Договора. При уменьшении предусмотренных Договором объема услуг стороны Договора обязаны уменьшить цену Договора исходя из цены единицы.

2.5.3. при исполнении Договора не допускается перемена Исполнителя, за исключением случая, если новый Исполнитель является правопреемником Исполнителя по такому Договору вследствие реорганизации юридического лица в форме преобразования, слияния или присоединения;

2.5.4. в случае перемены Заказчика права и обязанности Заказчика, предусмотренные Договором, переходят к новому Заказчику;

2.5.5. при исполнении Договора по согласованию Сторон допускается оказание услуг, качество, технически и функциональные характеристики которой являются улучшенными по сравнению с качеством и соответствующими техническими и функциональными характеристиками, указанными в Договоре. В этом случае соответствующие изменения должны быть оформлены дополнительным соглашением.

**3. ПОРЯДОК РАСЧЕТОВ**

3.1. Оплата по настоящему Договору осуществляется по цене, установленной п. 2.1 настоящего Договора.

3.2. Оплата производится по безналичному расчету путем перечисления на расчетный счет Исполнителя в течение 7 (семи) рабочих дней после продления неисключительных (лицензионных) прав использования антивирусного программного обеспечения и подписания акта приема-передачи прав ответственными лицами Исполнителя и Заказчика.

3.3. Обязательство Заказчика по оплате за оказанные услуги считается исполненным с момента списания денежных средств со счета Заказчика.

**4. ПРАВА И ОБЯЗАННОСТИ СТОРОН**

**4.1.** **Исполнитель обязан:**

4.1.1. Качественно оказать все услуги в объеме и в сроки, предусмотренные настоящим Договором и Приложением № 1, сдать результаты таких услуг Заказчику.

4.1.2. Своевременно предоставлять достоверную информацию о ходе исполнения своих обязательств, в том числе о сложностях, возникающих при исполнении Договора.

4.1.3. Предоставить Заказчику в качестве обеспечения надлежащего исполнения обязательств по настоящему Договору обеспечение исполнения обязательств по Договору в соответствии с разделом 8 настоящего Договора.

4.1.4. Немедленно письменно предупредить Заказчика при обнаружении обстоятельств, которые создают невозможность завершения услуги в срок, установленный настоящим Договором.

4.1.5. Незамедлительно в письменной форме предупредить Заказчика о возможных неблагоприятных последствиях, выявленных в ходе оказания услуг.

4.1.6. Устранять дефекты оказанных услуг за свой счет в течение гарантийного срока на оказанные услуги. Устранение дефектов производится в течение 10 (десяти) дней с момента заявления о них Заказчиком. Все расходы, связанные с устранением дефектов несет Исполнитель;

4.1.7. Для приемки оказанных услуг передать Заказчику 2 (два) экземпляра актов о сдаче-приемке оказанных услуг, счёт и счет-фактуру;

4.1.8. Участвовать в сдаче-приемке оказанных услуг в соответствии с разделом 5 настоящего Договора;

4.1.9. Нести риск случайной гибели или случайного повреждения материалов при оказании услуг и в течение гарантийного срока;

**4.2. Исполнитель гарантирует, что на момент заключения настоящего Договора:**

4.2.1. В отношении него не проводится процедура ликвидации, отсутствует решение арбитражного суда о признании его банкротом и об открытии конкурсного производства, деятельность не приостановлена в порядке, предусмотренном Кодексом Российской Федерации об административных правонарушениях, а также, что размер задолженности по начисленным налогам, сборам и иным обязательным платежам в бюджеты любого уровня или государственные внебюджетные фонды за прошедший календарный год не превышает 25% балансовой стоимости активов по данным бухгалтерской отчетности за последний завершенный отчетный период.

4.2.2. Не обременен обязательствами имущественного характера, способными помешать исполнению обязательств, по настоящему Договору.

4.2.3. За последние два года не нарушал договорных обязательств и не причинял ущерба (либо погасил причиненный ущерб) по аналогичным Договорам.

**4.3.** З**аказчик вправе**:

4.3.1. Требовать от Исполнителя представления надлежащим образом оформленной отчетной документации и материалов, подтверждающих исполнение обязательств в соответствии с техническим заданием, и настоящим Договором.

4.3.2. В случае досрочного исполнения Исполнителем обязательств по настоящему Договору принять и оплатить услуги в соответствии с установленным в Договоре порядком.

4.3.3. Запрашивать у Исполнителя информацию о ходе и состоянии исполнения обязательств Исполнителя по настоящему Договору.

**4.4. Заказчик обязан:**

4.4.1. Письменно заявить Исполнителю в течение 3 (трех) суток об обнаружении отступлений от требований технического задания (Приложение №1 к настоящему Договору), которые могут ухудшать качество услуг или вызвать иные недостатки;

4.4.2. Принять оказанные услуги в соответствии с разделом 5 настоящего Договора и, при отсутствии претензий относительно качества и других характеристик оказанных услуг и использованных материалов, подписать акты сдачи-приемки оказанных услуг и передать один экземпляр Исполнителю;

4.4.3. Оплатить оказанные услуги в соответствии с условиями настоящего Договора.

**5. ПОРЯДОК СДАЧИ-ПРИЕМКИ ОКАЗАННЫХ УСЛУГ**

5.1. Приемка оказанных услуг осуществляется комиссионно, в присутствии полномочных представителей со стороны Заказчика и Исполнителя, в соответствии с Техническим заданием.

5.2. В случае если на любых стадиях оказания услуг будут обнаружены некачественно оказаны услуги, Заказчик составляет акт, а Исполнитель обязан своими силами и без увеличения цены Договора в кратчайший срок переделать эти услуги для обеспечения их надлежащего качества и сдачи Заказчику.

5.3. Заказчик обладает полномочиями периодически давать указания:

5.3.1. Удалить или оказать заново любую услугу, которая была оказана ненадлежащим образом.

5.4. При исполнении Договора по согласованию Заказчика с Исполнителем допускается применение товара (материала), качество, технические и функциональные характеристики (потребительские свойства) которого являются улучшенными по сравнению с таким качеством и такими характеристиками товара (материала), указанными в Техническом задании.

5.5.По фактически оказанным услугам Исполнитель направляет в адрес Заказчика 2 (два) экземпляра актов о сдаче-приемке оказанных услуг, счет на оплату, счет – фактуру.

5.6. Заказчик в течение 3 (трех) рабочих дней проверяет совместно с Исполнителем качество и объемы оказанных услуг и затем:

а) либо принимает услуги и подписывает акт сдачи-приемки оказанных услуг для последующей оплаты;

б) либо при наличии замечаний Заказчика к представленному акту сдачи-приемки оказанных услуг возвращает их Исполнителю для внесения изменений в соответствии с результатами приемки;

в) либо направляет Исполнителю в письменном виде мотивированный отказ принять услуги и подписать акт сдачи-приемки оказанных услуг.

5.7. При наличии замечаний Заказчика по качеству оказанных услуг Исполнитель устраняет выявленные недостатки в течение 7 рабочих дней и предоставляет на подпись Заказчику исправленный и подписанный Исполнителем акт сдачи-приемки оказанных услуг.

5.8. При возникновении между Заказчиком и Исполнителем спора по поводу недостатков оказанных услуг или их причин по требованию любой из Сторон должна быть назначена экспертиза. Расходы по экспертизе несет Исполнитель, за исключением случаев, когда экспертизой установлено отсутствие нарушений Исполнителем Договора или причинной связи между действиями Исполнителя и обнаруженными недостатками.

5.9. Риск случайной гибели или случайного повреждения объекта, составляющего предмет настоящего Договора, до приемки этого объекта Заказчиком несет Исполнитель.

5.10. Для проверки соответствия качества оказанных Исполнителем услуг требованиям, установленным настоящим Договором, Заказчик вправе привлекать независимых экспертов.

5.11. Заказчик обязан в пятидневный срок со дня получения актов подписать их или направить Исполнителю мотивированный отказ в приемке услуг.

5.12. В случае мотивированного отказа заказчика принять услуги, составляется акт с перечнем замечаний и согласованными Сторонами сроками их устранения.

5.13. До приемки оказанных услуг, оговоренного Сторонами в заявке, риск повреждения объекта несет Исполнитель.

5.14. Услуги считаются принятыми с момента подписания сторонами акта сдачи-приемки оказания услуг.

**6. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА**

6.1. Исполнитель гарантирует качество и безопасность в соответствии с действующими стандартами, обязательных для данных услуг, оформленных в соответствии с законодательством Российской Федерации, устранение всех недостатков и дефектов, выявленных в гарантийный период.

6.2. Гарантийный срок начинает исчисляться с момента оказания услуг Исполнителем.

6.3. Срок действия продления неисключительных (лицензионных) прав использования антивирусного программного обеспечения составляет 2 года.

6.4. В случае если в течение гарантийного срока Заказчиком будут обнаружены некачественно оказанные услуги, то Исполнитель своими силами и за свой счет, без увеличения общей стоимости услуг обязан в срок, установленный Заказчиком, переделать эти услуги для обеспечения их надлежащего качества.

6.5. Наличие дефектов, выявленных в течение гарантийного срока, устанавливается двухсторонним актом, который подписывается Заказчиком и Исполнителем.

6.6. Для участия в составлении акта согласования порядка и сроков устранения дефектов по гарантийным обязательствам, Заказчик официально уведомляет Исполнителя о предстоящем обследовании Заказчик обязан направить своего представителя не позднее 5 дней со дня получения письменного извещения Заказчика, и направить Заказчику информацию о дате и времени планируемого выхода.

6.7. В случае если Исполнитель не устранил дефекты в установленные сроки, Заказчик имеет право устранить дефекты своими силами или силами третьих лиц за счет Исполнителя, взыскав при этом с Исполнителя убытки в размере стоимости услуг по устранению недостатков.

1. **ОТВЕТСТВЕННОСТЬ СТОРОН**

7.1. При нарушении условий Договора Стороны несут ответственность в соответствии с ГК РФ и настоящим Договором.

7.2. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Договором, заключенным по результатам определения Исполнителя с участием субъектов малого предпринимательства, социально ориентированных некоммерческих организаций в закупках, в соответствии с Положением, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Договором, размер штрафа устанавливается в размере 1 процента цены Договора, но не более 5 тыс. рублей и не менее 1 тыс. рублей.

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

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

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

7.4. За каждый день просрочки исполнения Исполнителем обязательства, предусмотренного Договором, начисляется пеня в размере одной трехсотой действующей на дату уплаты пени ставки рефинансирования Центрального банка Российской Федерации от цены Договора, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных Договором и фактически исполненных Исполнителем.

7.5. Общая сумма начисленных штрафов за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных Договором, не может превышать цену Договора.

7.6. Общая сумма начисленных штрафов за ненадлежащее исполнение Заказчиком обязательств, предусмотренных Договором, не может превышать цену Договора.

**8. ОБЕСПЕЧЕНИЕ ИСПОЛНЕНИЯ ДОГОВОРА**

8.1. Обеспечение исполнения настоящего Договора предоставляется Исполнителем на сумму: 29 810 (Двадцать девять тысяч восемьсот десять) рублей 03 копейки, что составляет 5% от начальной (максимальной) цены Договора, указанной в извещении об осуществлении закупки. Обеспечение исполнения Договора предоставляется Заказчику до заключения Договора.

8.2. В случае если предложенная в заявке участника закупки цена снижена на двадцать пять и более процентов по отношению к начальной (максимальной) цене Договора, участник закупки, с которым заключается Договор, предоставляет обеспечение исполнения Договора в размере, превышающем в полтора раза размер обеспечения исполнения договора, указанный в документации о проведении электронного аукциона в сумме: 44 715 (Сорок четыре тысячи семьсот пятнадцать) рублей 05 копеек или информацию, подтверждающую добросовестность Исполнителя на дату подачи заявки.

8.3. Если обеспечение исполнения Договора представляется в виде передачи Заказчику в залог денежных средств, Исполнитель, с которым заключается Договор, перечисляет сумму залога денежных средств, указанную в п. 8.\_\_ настоящего Договора, на счёт Заказчика по указанным реквизитам:

МУП «Водоканал»

ИНН 1215020390

КПП 121501001

Расчетный счет 40702810300000050227

Банк получателя: ГПБ (АО)

Корреспондентский счет 30101810200000000823

БИК 044525823

В поле «назначение платежа» обязательно указать: «Средства для обеспечения исполнения Договора по объекту закупки: «Оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения».

Обеспечение исполнения Договора перечисляется единовременно одной суммой на расчетный счет Заказчика. Перечисление обеспечения исполнения Договора по частям или третьими лицами за Исполнителя не допускается. Внесение денежных средств в качестве обеспечения исполнения Договора подтверждается платежным поручением с отметкой банка об оплате.

8.4. Обеспечение должно распространяться на все обязательства Исполнителя по Договору, в том числе по возмещению убытков, а также уплате неустоек.

8.5. В случае если Исполнителем в качестве обеспечения исполнения Договора выбрана независимая гарантия, данная гарантия должна соответствовать требованиям «Положения о независимой гарантии, предоставляемой в качестве обеспечения заявки на участие в конкурентной закупке товаров, работ, услуг в электронной форме с участием субъектов малого и среднего предпринимательства, и к независимой гарантии, предоставляемой в качестве обеспечения исполнения договора, заключаемого при осуществлении закупки» утвержденное Постановлением Правительства Российской Федерации от 9 августа 2022 г. N 1397.

8.6. Исполнитель обязан предоставить Заказчику оригинал независимой гарантии в течение пяти дней с момента заключения Договора.

8.7. Срок действия независимой гарантии должен превышать срок действия Договора не менее, чем на один месяц.

8.8. В случае возникновения обстоятельств, препятствующих заключению Договора в установленные Федеральным законом сроки, срок действия независимой гарантии продлевается на срок наличия таких обстоятельств.

8.9. В случае если по каким-либо причинам обеспечение исполнения настоящего Договора перестало быть действительным, закончило свое действие или иным образом перестало обеспечивать исполнение Исполнителем своих обязательств по настоящему Договору, Исполнитель обязуется в течение 10 (Десяти) рабочих дней с момента, когда соответствующее обеспечение исполнения Договора перестало действовать, предоставить Заказчику иное (новое) надлежащее обеспечение исполнения Договора на тех же условиях, которые указаны в настоящем разделе Договора.

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

8.11. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств по Договору обеспечение исполнения Договора переходит Заказчику в размере неисполненных обязательств. Все затраты, связанные с заключением и оформлением договоров и иных документов по обеспечению исполнения Договора, несет Исполнитель.

8.12. Денежные средства, внесенные в качестве обеспечения исполнения Договора, возвращаются Исполнителю в течение 30 (Тридцати) дней с даты подписания последнего акта сдачи-приемки услуг, а в случае расторжения Договора - в течение 30 (Тридцати) дней с даты подписания Соглашения о расторжении, после предоставления Заказчику необходимых документов, подтверждающих оказание услуг в полном объеме, на основании письменного заявления Исполнителя направленного в адрес Заказчика, с указание банковских реквизитов для перечисления.

**9. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ**

9.1. Стороны освобождаются от ответственности за полное или частичное неисполнение своих обязательств по настоящему Договору, в случае если оно явилось следствием обстоятельств непреодолимой силы, а именно стихийных бедствий, диверсий, военных действий, изменений законодательства, препятствующих надлежащему исполнению обязательств по настоящему Договору, а также других чрезвычайных обстоятельств, которые возникли после заключения настоящего Договора и непосредственно повлияли на исполнение Сторонами своих обязательств, и которые Стороны были не в состоянии предвидеть и предотвратить. Данные обстоятельства подтверждаются справкой компетентного учреждения или органа государственной власти.

9.2. При наступлении таких обстоятельств срок исполнения обязательств по настоящему Договору отодвигается соразмерно времени действия данных обстоятельств постольку, поскольку эти обстоятельства значительно влияют на исполнение настоящего Договора в срок.

9.3. Сторона, для которой надлежащее исполнение обязательств оказалось невозможным вследствие возникновения обстоятельств непреодолимой силы, обязана в течение 5 (пяти) календарных дней с даты возникновения таких обстоятельств уведомить в письменной форме другую Сторону об их возникновении, виде и возможной продолжительности действия.

9.4. Если обстоятельства, указанные в п. 9.1 настоящего Договора, будут длиться более 2 (двух) календарных месяцев с даты соответствующего уведомления, каждая из Сторон вправе расторгнуть настоящий Договор без требования возмещения убытков, понесенных в связи с наступлением таких обстоятельств.

**10. СРОКИ ОКАЗАНИЯ УСЛУГ**

10.1. Срок оказания услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения в течение 3 рабочих дней после заключения Договора.

Срок действия продления неисключительных (лицензионных) прав использования антивирусного программного обеспечения составляет 2 года.

Место оказания услуг: г. Йошкар-Ола, ул. Дружбы, д.2.

10.2. Исполнитель, по согласованию с Заказчиком, вправе оказать услуги досрочно.

10.3. Настоящий Договор может быть расторгнут:

- по соглашению Сторон;

- в судебном порядке;

- в связи с односторонним отказом Заказчика от исполнения Договора по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств.

**11. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРОВ**

11.1. Стороны принимают все меры к тому, чтобы любые спорные вопросы, разногласия, либо претензии, касающиеся исполнения настоящего Договора, были урегулированы путем переговоров, с оформлением совместного протокола урегулирования споров.

11.2. В случае невыполнения Сторонами своих обязательств и не достижения взаимного согласия споры по настоящему Договору разрешаются в Арбитражном суде Республики Марий Эл. До передачи спора на разрешение в судебный орган, Стороны принимают меры к его урегулированию в претензионном порядке. Претензия должна быть рассмотрена и по ней должен быть дан письменный ответ по существу Стороной, которой адресована претензия, в срок не позднее 10 (десяти) календарных дней с даты ее получения.

11.3. К отношениям Сторон по настоящему Договору и в связи с ним, применяется законодательство Российской Федерации.

**12. АНТИКОРРУПЦИОННАЯ ОГОВОРКА**

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

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

12.3. В случае возникновения у стороны обоснованных подозрений, что произошло или может произойти нарушение каких-либо положений настоящего раздела, соответствующая сторона обязуется уведомить другую сторону в письменной форме. После письменного уведомления, соответствующая сторона обязана направить подтверждение, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение десяти рабочих дней с даты направления письменного уведомления.

12.4. В письменном уведомлении сторона обязана сослаться на обоснованные факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений настоящего раздела 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.

12.5. В случае нарушения одной стороной обязательств воздерживаться от запрещенных в настоящем разделе Договора действий и/или неполучения другой стороной в установленный настоящим Договором срок подтверждения, что нарушения не произошло или не произойдет, другая сторона имеет право направить обоснованные факты или предоставить материалы в компетентные органы, в соответствии с применимым законодательством.

**13. ПРОЧИЕ УСЛОВИЯ**

13.1 Настоящий Договор вступает в действие с момента его подписания Сторонами и действует до полного исполнения Сторонами своих обязательств.

13.2 Настоящий Договор подписывается Сторонами на бумажном носителе в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

13.3. Все уведомления Сторон, связанные с исполнением настоящего Договора, направляются в письменной форме по почте заказным письмом по фактическому адресу Стороны, указанному в настоящем Договоре, а также могут быть направлены с использованием факсимильной связи, электронной почты с последующим предоставлением оригинала или в электронно-цифровой форме, подписанные в таком случае квалифицированной электронной подписью. В случае направления уведомлений с использованием почты уведомления считаются полученными Стороной в день фактического получения, подтвержденного отметкой почты. В случае отправления уведомлений посредством факсимильной связи и электронной почты уведомления считаются полученными Стороной в день их отправки.

13.4. Во всем, что не предусмотрено настоящим Договором, Стороны руководствуются действующим законодательством Российской Федерации.

13.5. Вопросы, не урегулированные Договором, регламентируются нормами действующего законодательства Российской Федерации.

13.6. Изменение существенных условий Договора при его исполнении не допускается, за исключением их изменения по соглашению сторон в случаях предусмотренных Положением и действующим законодательством РФ.

13.7. Выполнение в полном объёме обязательств, предусмотренных настоящим Договором, Заказчиком и Исполнителем является основанием для регистрации сведений об исполнении Договора в Реестре Договоров в порядке, предусмотренном федеральным законодательством РФ.

13.8. Приложения к настоящему Договору, являющиеся его неотъемлемыми частями:

Приложение № 1 - Техническое задание

**14. МЕСТОНАХОЖДЕНИЕ И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН**

|  |  |
| --- | --- |
| **Заказчик:**  МУП «Водоканал»  ИНН/КПП:1215020390/121501001  Адрес:424039, Республика Марий Эл,  г. Йошкар-Ола, ул. Дружбы, д.2  р/с 40702810300000050227  Банк ГПБ (АО)  БИК 044525823,  к/с 30101810200000000823  ОКПО 03220481,  Тел. (8362) 41-84-49  E-mail: ito@vod12.ru  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. | **Исполнитель:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **/**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  М.П. |

Приложение № 1 к Договору на Оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения

от \_\_\_\_\_\_\_\_\_\_№ \_\_\_\_\_\_\_\_

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Наименование:** Оказание услуг по продлению неисключительных (лицензионных) прав использования антивирусного программного обеспечения.

Заказчик заявляет ***продление*** неисключительных (лицензионных) прав антивирусного программного обеспечения на уже приобретенный и используемый программный продукт Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 100-149, сроком на 2 года. Номер лицензии 2B1E-230403-071837-1-39009. Количество рабочих мест 150 (Лицензирование количества компонентов защиты рабочих станций и файловых серверов должно быть универсальным и ограничиваться только общим количеством защищаемых объектов). Участник размещения заказа не вправе предложить эквивалент, т.к. предложение другого антивирусного программного обеспечения не обеспечит совместимости с существующим у Заказчика программным обеспечением.

Согласно закону о закупках товаров, работ, услуг отдельными видами юридических лиц, заказчик заявляет о необходимости предоставления в рамках услуги средств защиты информации, совместимых с существующим у Заказчика программным обеспечением Kaspersky Security Center.

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование | Единица измерения | Количество |
| 1 | Продление лицензии Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 100-149 Node 2 year Renewal License | шт. | 150 |

**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 мобильных устройств (смартфонов и планшетов);
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ и атак;
* эксплуатационную документацию на русском языке.

Программный интерфейс всех антивирусных средств, включая средства управления, должен быть на русском и английском языке.

Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском и английском языке.

**Требования к программным средствам антивирусной защиты для рабочих станций Windows**

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для рабочих станций следующих версий:

* Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1 и выше;
* Windows 8 Professional / Enterprise (32 / 64-разрядная);
* Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
* Windows 10 Home / Pro / Pro для рабочих станций / Education / Enterprise/Enterprise multi-session;
* Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise

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

* + антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
  + антивирусное сканирование по расписанию;
  + антивирусное сканирование подключаемых устройств;
  + эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
  + нейтрализации действий активного заражения;
  + анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
  + анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
  + блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
  + откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
  + ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
  + облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
  + антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
  + защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
  + фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
  + проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
  + блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
  + распознавания и блокировку фишинговых и небезопасных сайтов;
  + встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
  + защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
  + защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
  + контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
  + создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
  + контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
  + управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
  + записи в журнал событий о записи и/или удалении файлов на съемных дисках;
  + назначение приоритета для правил доступа к устройствам с файловой системой;
  + контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
  + защиты от атак типа BadUSB;
  + 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;
  + возможность 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 создание 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.

**Требования к программным средствам антивирусной защиты для серверов Windows**

Программные средства антивирусной защиты должны функционировать на компьютерах, работающих под управлением операционной системы для файловых серверов следующих версий:

* Windows Small Business Server 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;
* Windows MultiPoint Server 2011 (64-разрядная);
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1 и выше;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (включая Core Mode)

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 (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.

**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:

* macOS 11 - 13;

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;
* установки из файла .pkg через JAMF;
* 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:

* CentOS 6.7 и выше.
* Debian GNU/Linux 10.1 и выше.
* Debian GNU/Linux 11.
* Mageia 4.
* Red Hat Enterprise Linux 6.7 и выше.
* Альт 8 СП Рабочая Станция.
* Альт 8 СП Сервер.
* Альт Образование 10.
* Альт Рабочая Станция 10.

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

* AlmaLinux OS 8 и выше.
* AlmaLinux OS 9 и выше.
* AlterOS 7.5 и выше.
* Amazon Linux 2.
* Astra Linux Common Edition 2.12.
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.5).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.6).
* Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.7).
* Astra Linux Special Edition РУСБ.10015-16 (исполнение 1) (очередное обновление 1.6).
* CentOS 6.7 и выше.
* CentOS 7.2 и выше.
* CentOS Stream 9.
* Debian GNU/Linux 10.1 и выше.
* Debian GNU/Linux 11 и выше.
* EMIAS 1.0.
* EulerOS 2.0 SP5.
* LinuxMint 20.3 и выше.
* LinuxMint 21.1.
* openSUSE Leap 15.0 и выше.
* Oracle Linux 7.3 и выше.
* Oracle Linux 8.0 и выше.
* Oracle Linux 9.0 и выше
* Red Hat Enterprise Linux 6.7 и выше.
* Red Hat Enterprise Linux 7.2 и выше.
* Red Hat Enterprise Linux 8.0 и выше.
* Red Hat Enterprise Linux 9 и выше.
* Rocky Linux 8.5 и выше.
* Rocky Linux 9.1.
* SUSE Linux Enterprise Server 12.5 и выше.
* SUSE Linux Enterprise Server 15 и выше.
* Ubuntu 20.04 LTS.
* Ubuntu 22.04 LTS.
* Альт 8 СП Рабочая станция.
* Альт 8 СП Сервер.
* Альт Образование 10.
* Альт Рабочая Станция 10.
* Альт Сервер 10.
* Атлант, сборка Alcyone, версия 2022.02.
* Гослинукс 7.17.
* Гослинукс 7.2.
* РЕД ОС 7.3.
* РОСА "Кобальт" 7.9.
* РОСА "Хром" 12.

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

* Astra Linux Special Edition РУСБ.10152-02 (очередное обновление 4.7).
* EulerOS 2.0 SP8.
* SUSE Linux Enterprise Server 15 SP3 и выше.
* Ubuntu 20.04 LTS.
* Альт 8 СП.
* РЕД ОС 7.3.

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

* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* возможность проверки памяти ядра;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plain text);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* включения опции блокирования файлов во время проверки;
* помещение подозрительных и поврежденных объектов на карантин;
* перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
* управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
* проверки съемных дисков;
* отслеживания во входящем сетевом трафике активности, характерной для сетевых атак;
* проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым
* получения данных о действиях программ на компьютере пользователя;
* 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.

**Требования к программным средствам антивирусной защиты файловых серверов, серверов масштаба предприятия, терминальных серверов Windows**

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

32-разрядных операционных систем Microsoft Windows

* Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше.

64-разрядных операционных систем Microsoft Windows

* Windows Server 2003 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетом обновлений SP2 или выше;
* Microsoft Small Business Server 2008 Standard / Premium SP2 или выше;
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Server 2008 R2 Core Standard / Enterprise / Datacenter с пакетом обновлений SP1 или выше;
* Windows Hyper-V Server 2008 R2 с пакетом обновлений SP1 или выше;
* Microsoft Small Business Server 2011 Essentials / Standard SP1 или выше;
* Microsoft Windows MultiPoint Server 2011 Standard / Premium;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
* Microsoft MultiPoint Server 2012 Standard / Premium;
* Windows Storage Server 2012;
* Windows Hyper-V Server 2012;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
* Windows Storage Server 2012 R2;
* Windows Hyper-V Server 2012 R2;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2016 MultiPoint;
* Windows Server 2016 Core Standard / Datacenter;
* Microsoft Windows MultiPoint Server 2016;
* Windows Storage Server 2016;
* Windows Hyper-V Server 2016;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2019 Core;
* Windows Storage Server 2019;
* Windows Hyper-V Server 2019;
* Windows Server 2022;
* Windows 10 Enterprise multi-session.

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

* антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
* защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
* непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
* анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* добавлять процессы в список защищаемых;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
* настройки проверки критических областей сервера в качестве отдельной задачи;
* регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
* продолжать антивирусное сканирование в фоновом режиме;
* наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
* ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
* интеграции с SIEM системами;
* указания количества рабочих процессов антивируса вручную;
* отключить графический интерфейс;
* наличие удаленной и локальной консоли управления;
* управления параметрами антивируса из командной строки;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
* включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.
* контроль устройств, в том числе сетевых карт и модемов;
* веб-контроль;
* защита от почтовых угроз (плагин для Outlook);
* защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления;
* 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);
* создания специальных правил должно контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
* создания специальных правил должно работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должно иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
* осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем;
* информирование администратора о подключении внешних устройств;
* наличие механизмов автоматической генерации правил для контроля устройств и приложений;

**Требования к программным средствам антивирусной защиты мобильных устройств**

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

* Android 5.0–13 (включая Android 12L, исключая Go Edition);
* iOS 10–16 или iPadOS 13–15;

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

* постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
* проверка файловой системы устройства по требованию и по расписанию;
* мгновенная проверка устанавливаемых приложений
* блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* наличие хранилища для изолирования зараженных объектов;
* обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
* блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
* поддержка белых списков разрешенных приложений;
* блокировка системных приложений, в рамках контроля запуска приложений;
* отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);
* заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
* указать параметры подключения к wi-fi сетям;
* указать обязательные к установке приложения;
* блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
* создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
* поддержка технологий Samsung KNOX1 и KNOX2;
* 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 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:

* Windows Server 2008 R2 with Standard Service Pack 1 и выше 64-разрядная;
* Windows Server 2008 R2 Service Pack 1 (все редакции) 64-разрядная;
* Windows Server 2012 Server Core 64-разрядная;
* Windows Server 2012 Datacenter 64-разрядная;
* Windows Server 2012 Essentials 64-разрядная;
* Windows Server 2012 Foundation 64-разрядная;
* Windows Server 2012 Standard 64-разрядная;
* Windows Server 2012 R2 Server Core 64-разрядная;
* Windows Server 2012 R2 Datacenter 64-разрядная;
* Windows Server 2012 R2 Essentials 64-разрядная;
* Windows Server 2012 R2 Foundation 64-разрядная;
* Windows Server 2012 R2 Standard 64-разрядная;
* Windows Server 2016 Datacenter (LTSB) 64-разрядная;
* Windows Server 2016 Standard (LTSB) 64-разрядная;
* Windows Server 2016 (вариант установки Server Core) (LTSB) 64-разрядная;
* Windows Server 2019 Standard 64-разрядная;
* Windows Server 2019 Datacenter 64-разрядная;
* Windows Server 2019 Core 64-разрядная;
* Windows Server 2022 Standard 64-разрядная;
* Windows Server 2022 Datacenter 64-разрядная;
* Windows Server 2022 Core 64-разрядная;
* Windows Storage Server 2012 64-разрядная;
* Windows Storage Server 2012 R2 64-разрядная;
* Windows Storage Server 2016 64-разрядная;
* Windows Storage Server 2019 64-разрядная.

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

* VMware vSphere 6.7;
* VMware vSphere 7.0;
* VMware Workstation 16 Pro;
* Microsoft Hyper-V Server 2012 64-разрядная;
* Microsoft Hyper-V Server 2012 R2 64-разрядная;
* Microsoft Hyper-V Server 2016 64-разрядная;
* Microsoft Hyper-V Server 2019 64-разрядная;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 17;
* Oracle VM VirtualBox 6.x.

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

* Microsoft SQL Server 2012 Express 64-разрядная.
* Microsoft SQL Server 2014 Express 64-разрядная.
* Microsoft SQL Server 2016 Express 64-разрядная.
* Microsoft SQL Server 2017 Express 64-разрядная.
* Microsoft SQL Server 2019 Express 64-разрядная.
* Microsoft SQL Server 2014 (все редакции) 64-разрядная.
* Microsoft SQL Server 2016 (все редакции) 64-разрядная.
* Microsoft SQL Server 2017 (все редакции) для Windows 64-разрядная.
* Microsoft SQL Server 2017 (все редакции) для Linux 64-разрядная.
* Microsoft SQL Server 2019 (все редакции) для Windows 64-разрядная.
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная.
* Microsoft Azure SQL Database.
* Все версии SQL-серверов, поддерживаемые в облачных платформах Amazon RDS и Microsoft Azure.
* MySQL 5.7 Community 32-разрядная/64-разрядная.
* MySQL Standard Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
* MySQL Enterprise Edition 8.0 (релиз 8.0.20 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* PostgreSQL 13.x 64-разрядная.
* PostgreSQL 14.х 64-разрядная.
* Postgres Pro 13.x (все редакции).
* Postgres Pro 14.x (все редакции).

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

* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
* автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
* указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* иерархии триггеров, по которым происходит перераспределение;
* тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* инвентаризация установленного ПО и оборудования на компьютерах пользователей;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер Exchange ActiveSync;
* функция управления мобильными устройствами через сервер iOS MDM;
* отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* интеграции по OpenAPI;
* управления антивирусной защитой с использованием WEB консоли;
* 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.

**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:

* Debian GNU/Linux 9.х (Stretch) 32-разрядная/64-разрядная.
* Debian GNU/Linux 10.х (Buster) 32-разрядная/64-разрядная.
* Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная.
* Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная.
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная.
* Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64-разрядная.
* CentOS 7.x 64-разрядная.
* Red Hat Enterprise Linux Server 7.x 64-разрядная.
* Red Hat Enterprise Linux Server 8.x 64-разрядная.
* Red Hat Enterprise Linux Server 9.x 64-разрядная.
* SUSE Linux Enterprise Server 12 (все пакеты обновлений) 64-разрядная.
* SUSE Linux Enterprise Server 15 (все пакеты обновлений) 64-разрядная.
* Astra Linux Special Edition RUSB.10015-01 (обновление 1.6) 64-разрядная.
* Astra Linux Special Edition RUSB.10015-01 (обновление 1.7) 64-разрядная.
* Astra Linux Common Edition (обновление 2.12) 64-разрядная.
* Альт Сервер 9.2 64-разрядная.
* Альт Сервер 10 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-02) 64-разрядная.
* Альт 8 СП Сервер (ЛКНВ.11100-03) 64-разрядная.
* Oracle Linux 7 64-разрядная.
* Oracle Linux 8 64-разрядная.
* Oracle Linux 9 64-разрядная.
* РЕД ОС 7.3 Сервер 64-разрядная.
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная.

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

* VMware vSphere 6.7.
* VMware vSphere 7.0;
* VMware Workstation 16 Pro;
* Microsoft Hyper-V Server 2012 64-разрядная;
* Microsoft Hyper-V Server 2012 R2 64-разрядная;
* Microsoft Hyper-V Server 2016 64-разрядная;
* Microsoft Hyper-V Server 2019 64-разрядная;
* Microsoft Hyper-V Server 2022 64-разрядная;
* Citrix XenServer 7.1 LTSR;
* Citrix XenServer 8.x;
* Parallels Desktop 17;
* Виртуальная машина на основе Kernel. Поддерживает следующие операционные системы:
* Альт 8 СП Сервер (ЛКНВ.11100-01) 64-разрядная;
* Альт Сервер 10 64-разрядная;
* Astra Linux Special Edition 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Debian GNU/Linux 11.х (Bullseye) 32-разрядная/64-разрядная;
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
* РЕД ОС 7.3 Сервер 64-разрядная;
* РЕД ОС 7.3 Сертифицированная редакция 64-разрядная

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

* MySQL 5.7 Community 32-разрядная/64-разрядная.
* MySQL 8.0 32-разрядная/64-разрядная.
* MariaDB 10.1 (сборка 10.1.30 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.3 (сборка 10.3.22 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.4 (сборка 10.4.26 и выше) 32-разрядная/64-разрядная.
* MariaDB 10.5 (сборка 10.5.17 и выше) 32-разрядная/64-разрядная.
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* MariaDB Galera Cluster 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB.
* PostgreSQL 13.х 64-разрядная.
* PostgreSQL 14.х 64-разрядная.
* Postgres Pro 13.х (все редакции) 64-разрядная.
* Postgres Pro 14.х (все редакции) 64-разрядная.

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

* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* иерархии триггеров, по которым происходит перераспределение;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* наличие системы контроля возникновения вирусных эпидемий;
* управления антивирусной защитой с использованием WEB консоли;
* возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
* возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
* возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули;
* выступать в качестве главного Сервера и управлять Серверами с операционными системами Linux или Windows в качестве подчиненных.

**Требования к обновлению антивирусных баз**

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

* + создания правил обновления антивирусных баз не реже 24 раз в течение календарных суток;
  + множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
  + проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

**Требования к эксплуатационной документации**

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе:

* «Руководство пользователя (администратора)»

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.

**Требования к технической поддержке**

Техническая поддержка антивирусного программного обеспечения должна:

* Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по электронной почте и через Интернет.
* Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

**РАЗДЕЛ V. СВЕДЕНИЯ О НАЧАЛЬНОЙ (МАКСИМАЛЬНОЙ) ЦЕНЕ ЕДИНИЦЫ КАЖДОГО ТОВАРА, РАБОТЫ, УСЛУГИ**

**Начальная (максимальная) цена договора рассчитывается методом сопоставления рыночных цен (анализа рынка) и заключается в установлении НМЦД на основании информации о рыночных ценах (далее — ценовая информация) идентичных товаров, планируемых к закупкам, а при их отсутствии — однородных товаров. В этом случае определение стоимости товаров, работ, услуг производится посредством изучения ценовых предложений, включая структуру цены, от не менее, чем трёх поставщиков (подрядчиков, исполнителей), осуществляющих такие услуги.**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование товара  (работ, услуг) | Единица измерения | Кол-во | Информация о ценах товаров, работ, услуг, содержащаяся в рекламе, каталогах, описаниях товаров и в других предложениях, обращенных к неопределенному кругу лиц | | | Средняя арифметическая цена за единицу <ц> | НМЦД рынка = SЦi / N  НМЦД рынка — НМЦД, определяемая методом сопоставимых рыночных цен (анализа рынка); N — количество значений, используемых в расчёте; i — номер источника ценовой информации; SЦi — сумма товаров, работ, услуг Цi Цi — цена единицы товара, работы, услуги, представленная в источнике с номером (i) |
| Коммерческое предложение №1 | Коммерческое предложение №2 | Коммерческое предложение № 3 |  |  |
| 1 | 'Kaspersky Endpoint Security для бизнеса –  Расширенный Russian Edition. 100-149 Node 2 year  Renewal License | шт | 150 | 4013,89 | 3974,94 | 3935,19 | 3974,67 | 596 200,50 |
| **596 200,50** | | | | | | | | | |

Цена Товара включает в себя стоимость Товара, доставку, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей. Проведенные исследования позволяют определить начальную максимальную цену договора в сумме 596 200 (Пятьсот девяносто шесть тысяч двести) руб. 50 коп НДС не облагается.

**РАЗДЕЛ VI. ИНСТРУКЦИЯ ПО ЗАПОЛНЕНИЮ ЗАЯВОК НА УЧАСТИЕ В ЭЛЕКТРОННОМ АУКЦИОНЕ**

Заявка на участие в электронном аукционе направляется участником закупки оператору электронной площадки в форме двух электронных документов, содержащих сведения, предусмотренные пунктами 3.1.2. и 3.1.3. Раздела I «Общие условия проведения аукциона в электронной форме». Указанные электронные документы подаются одновременно.

При подготовке заявки на участие в электронном аукционе участниками закупки должны приниматься общепринятые обозначения и наименования в соответствии с требованиями действующих нормативных документов.

Сведения, содержащиеся в заявках участников закупки, должны быть достоверными и не должны допускать двусмысленных толкований.

При этом не допускается указание в первой части заявки на участие в электронном аукционе сведений об участнике закупки и (или) о ценовом предложении.

Заявку на участие в электронном аукционе участник закупки составляет, руководствуясь данной документацией о закупке, в соответствии с требованиями Информационной карты.

Участнику закупки в первой части своей заявки на участие в электронном аукционе на товары, для которых установлены заказчиком требования к их характеристикам необходимо предоставить конкретное предложение (т.е. не допускающее двусмысленного толкования, в отсутствии слов «эквивалент», «аналог», «превышать»).

В случае проведения закупки на поставку товара либо закупки на выполнение работ (оказания услуг) с использованием товара участнику необходимо указать конкретные показатели предлагаемого им товара в соответствии с требованиями Заказчика руководствуясь следующей инструкцией с определениями знаков и обозначений:

* слова «не менее» означают что, участнику следует предоставить в заявке конкретный показатель, более указанного значения или равный ему;
* слова *«*не более*»* означают что, участнику следует предоставить в заявке конкретный показатель, менее указанного значения или равный ему;
* слова «не выше» означают что, участнику следует предоставить в заявке конкретный показатель, не более указанного значения;
* слова «не ниже» означают что, участнику следует предоставить в заявке конкретный показатель, не менее указанного значения;
* слова «не менее …, не более …» означают что, участнику следует предоставить в заявке одно числовое значение показателя товара, входящее в установленный заказчиком интервал;
* символ «тире» или «дефис», установленный между значениями, означает что, участнику следует предоставить в заявке конкретный показатель из предоставленного диапазона, включая крайние значения.

В случае, когда предлагаемый товар не может иметь конкретное значение параметра (конкретный показатель) в соответствии со сведениями, предоставляемыми производителями таких товаров, участником закупки указывается диапазон значений.

*Рекомендуемая форма первой части заявки*

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование поставляемого товара | Показатели, позволяющие определить соответствие закупаемых товаров установленным Заказчиком требованиям.  *(участник аукциона должен указать конкретные показатели предлагаемого для поставки товара)* |
| 1 | 2 | 3 |
| 1 |  |  |
| … |  |  |