Извещение о проведении запроса котировок № 86 от 17.06.2019

на право заключения лицензионного договора на предоставление (передачу) прав на условиях простой (неисключительной) лицензии на использование программ для электронно-вычислительных машин (ЭВМ) для нужд НУЗ «Отделенческая больница на ст. Исакогорка ОАО «РЖД».

1	Способ закупки	Запрос котировок
2	Наименование, место нахождения, почтовый адрес, адрес электронной почты, номер контактного телефона заказчика	НУЗ «Отделенческая больница на ст. Исакогорка ОАО «РЖД», г. Архангельск ул. Тимме, д.5 , nuz-secretar@medrzd29.ru Телефон (8182) 67-30-10, (8182) 27-00-07 доб.158
3	Предмет договора	Право заключения лицензионного договора на предоставление (передачу) прав на условиях простой (неисключительной) лицензии на использование программ для электронно-вычислительных машин (ЭВМ) для нужд НУЗ «Отделенческая больница на ст. Исакогорка ОАО «РЖД». (Наименование, количество, характеристики Товара, Работ, Услуг указаны в Техническом задании (Приложение № 3 к Закупочной документации).
4	Место выполнения Работ, оказания Услуг	Место выполнения Работ, оказания Услуг: по месту нахождения Исполнителя. Место предоставления результатов работ, услуг (передачи прав на условиях простой (неисключительной) лицензии для использования программ для ЭВМ) Архангельск, ул. Тимме, д.5, в рабочие дни (с понедельника по пятницу, исключая праздничные дни) с 8.00 до 15.00.. Под рабочими днями при исполнении Договора сторонами понимаются дни недели с понедельника по пятницу, исключая приходящиеся на эти дни недели выходные и праздничные дни, установленные или перенесенные в соответствии со статьей 112 Трудового кодекса РФ.
5	Сведения о начальной (максимальной) цене Договора	Начальная максимальная цена составляет 82 040,00 (Восемьдесят две тысячи сорок) рублей 00 копеек. Начальная (максимальная) цена договора включает в себя стоимость работ и услуг, накладные и плановые расходы, все налоги и пошлины и иные обязательные платежи, а также вознаграждение исполнителя за передачу исключительных имущественных прав на результаты интеллектуальной деятельности передаваемые исполнителем заказчику по договору (Приложение № 4 к документации о проведении закупки).
6	Место, дата и время рассмотрения предложений с заявками участников и подведение итогов.	Срок подачи заявок участников закупки составляет 7 (семь) календарных дней с момента размещения Извещения о закупке на официальном сайте Заказчика. Заявки в письменной форме подаются по адресу: г. Архангельск, ул. Тимме, д.5 с 17.06.*2019 г.* с 15 ч 00 мин. по 24.06.*2019 г.* до 15 ч 00 мин. время местное. Порядок подачи заявок - в соответствии с документацией о проведение закупки Вскрытие конвертов с заявками участников: г. Архангельск, ул. Тимме, д.5 25.06.2019 г. в 12 ч. 00 мин. (время местное). Рассмотрение и оценка предложений: г. Архангельск, ул. Тимме, д.5 25.06.2019 г. в 12 ч. 10 мин. (время местное).
7	Процедура закупки проводится в соответствии с требованиями Положения о закупке товаров, работ и услуг для нужд негосударственных учреждений здравоохранения ОАО «РЖД» от 02 апреля 2018 г., размещенного на сайте заказчика.	

Приложение:

1. Документация о проведении закупки.

Должность ответственного экономист 1 категории Ершова Галина Александровна

Ф.И.О.

Приложение № 1
к Извещению 86 от 17.06.2019 г.

Документация о проведении закупки

на право заключения лицензионного договора на предоставление (передачу) прав на условиях простой (неисключительной) лицензии на использование программ для электронно-вычислительных машин (ЭВМ) для нужд НУЗ «Отделенческая больница на ст. Исакогорка ОАО «РЖД».

Общие положения

Настоящая документация о проведении закупки (закупочная документация) подготовлена в соответствии с нормативными правовыми актами:

Гражданский кодекс Российской Федерации;

Федеральный закон от 26.07.2006 № 135-ФЗ «О защите конкуренции»;

Положением о закупке товаров, работ, услуг для нужд НУЗ ОАО «РЖД», утвержденным приказом Центральной дирекции здравоохранения ОАО «РЖД» от 02.04.2018 № ЦДЗ-35.

Во всех вопросах, особо не оговоренных в тексте настоящей документации, Заказчик и Комиссия по проведению закупок товаров, выполнению работ и оказанию услуг НУЗ « Отделенческая больница на ст. Исакогорка ОАО «РЖД». (далее - Комиссия) руководствуются требованиями Положения о закупке товаров, работ, услуг для нужд НУЗ ОАО «РЖД».

Извещение и Документация о проведении закупки размещается на официальном сайте НУЗ «Отделенческая больница на ст. Исакогорка ОАО «РЖД» по адресу: www.medrzd29.ru

1. Требования к содержанию, форме, оформлению и составу заявки на участие в закупке, а также порядок, место, дата и время начала и дата, и время окончания срока подачи заявок на участие в закупке:

1.1. Место, дата и время начала и дата, и время окончания срока подачи заявок на участие в закупке установлены в Извещении.

1.2. Заявка на участие в закупке оформляется по форме Приложения № 1 к Документации и подается Заказчику в письменной форме в запечатанном конверте, не позволяющем просматривать содержание такой заявки до даты и времени вскрытия конвертов с заявками на участие в закупке.

1.3. Заявка должна содержать следующие информацию и документы:

1.3.1. предложение участника закупки в отношении объекта закупки. При этом описание участниками закупки выполняемой работы, оказываемой услуги, которые являются предметом закупки, их количественных и качественных характеристик осуществляется по форме Приложения № 2 к Документации

1.3.2. наименование, организационно-правовая форма, место нахождения, почтовый адрес участника закупки (для юридического лица), фамилия, имя, отчество, паспортные данные, место жительства участника закупки (для физического лица), номер телефона, адрес электронной почты, банковские реквизиты;

1.3.3. идентификационный номер налогоплательщика;

1.3.4. согласие участника закупки на поставку товара в соответствии с условиями, установленными Документацией.

1.3.5. предлагаемая участником закупки цена товара;

1.3.6. документы, подтверждающие соответствие участников закупки требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом договора.

Перечень документов:

1) Учредительные документы с учетом внесенных в них изменений, свидетельства о государственной регистрации учредительных документов и внесенных в них изменений;

2) Свидетельство о государственной регистрации контрагента, свидетельство о внесении в государственный реестр изменений в сведения о юридическом лице, не связанных с внесением в учредительные документы, свидетельство о постановке на учет в налоговом органе;

3) Выписка из единого государственного реестра юридических лиц, выданная регистрирующим органом не ранее чем за один месяц до предоставления документов;

4) Документы, подтверждающие полномочия лица на подписание договора, оформленные надлежащим образом (протокол (решение) уполномоченного органа управления контрагента о назначении Исполнительного органа; оригинал доверенности, если договор со стороны контрагента подписан не единоличным Исполнительным органом;

5) согласие соответствующего органа управления контрагента на совершение сделки, предусмотренной договором, в случаях, когда это определено законодательством Российской Федерации и учредительными документами контрагента);

6) Согласие контролирующих органов на совершение сделки или подтверждение уведомления соответствующих органов о совершении сделки в случаях, когда такое согласие или уведомление предусмотрено законодательством Российской Федерации;

7) Информационная справка, содержащая сведения о владельцах контрагента, включая конечных бенефициаров, с приложением подтверждающих документов;

Непредставление указанных документов в составе заявки на участие в запросе котировок в печатной форме влечет за собой отказ в допуске к участию либо признания заявки участника не соответствующей требованиям документации;

1.3.7. документ (либо заверенная участником закупки копия), подтверждающий полномочия лица, подписавшего заявку;

1.3.8. декларация о соответствии участника закупки требованиям, установленным пунктом 8 Документации (подается в письменном виде по произвольной форме).

1.4. В случае наличия в составе заявки документов и информации, текст которых не поддается прочтению, такие документы и информация считаются непредставленными.

1.5. Участник закупки может подать только одну заявку по одному лоту для участия в закупке. Если участник закупки подает более одной заявки по лоту, а ранее поданные им заявки по этому лоту не отозваны, все заявки такого участника

закупки по лоту отклоняются.
1.6. Основанием для отказа в приеме заявки является истечение срока подачи заявок, установленным Документацией.
1.7. Заказчик принимает конверты с заявками до истечения срока подачи заявок, за исключением конвертов, на которых отсутствует необходимая информация, незапечатанных и поврежденных конвертов.
1.8. По истечении срока подачи заявок конверты с заявками не принимаются. Конверт с заявкой, полученный Заказчиком по истечении срока подачи заявок по почте, не вскрывается и не возвращается.
1.9. Каждый конверт с заявкой, поступивший в установленный срок, принимается Заказчиком в соответствии с условиями, предусмотренными Документацией.
2. Требования к описанию участниками закупки выполняемых работ, оказываемых услуг, которые являются предметом закупки, их количественных и качественных характеристик: установлены в Приложении №3 к документации о проведении закупки (далее - Документация).
3. Место выполнения Работ, оказания Услуг: по месту нахождения Исполнителя.
Место предоставления результатов работ, услуг (передачи прав на условиях простой (неисключительной) лицензии для использования программ для ЭВМ) Архангельск, ул. Тимме, д.5, в рабочие дни (с понедельника по пятницу, исключая праздничные дни) с 8.00 до 15.00.
Под рабочими днями при исполнении Договора сторонами понимаются дни недели с понедельника по пятницу, исключая приходящиеся на эти дни недели выходные и праздничные дни, установленные или перенесенные в соответствии со статьей 112 Трудового кодекса РФ.
Срок выполнения работ, оказания услуг по предоставлению неисключительных лицензионных прав: в течение 5 (пяти) рабочих дней с момента подписания договора.
4. Сведения о начальной (максимальной) цене Договора указаны в Извещении.
5. Форма, срок и порядок оплаты товара: Безналичный расчет на основании счета, после заключения договора в течении 30 (тридцати) календарных дней, с момента подписания акты приемки-передачи объекта интеллектуальной собственности.
6. Начальная (максимальная) цена договора включает в себя стоимость работ и услуг, накладные и плановые расходы, все налоги и пошлины и иные обязательные платежи, а также вознаграждение исполнителя за передачу исключительных имущественных прав на результаты интеллектуальной деятельности передаваемые исполнителем заказчику по договору (Приложение № 4 к документации о проведении закупки).
7. Срок подачи заявок участников закупки составляет 7 (семь) календарных дней с момента размещения Извещения о закупке на официальном сайте Заказчика. Извещения о закупке на официальном сайте Заказчика. Заявки подаются с 17.06.*2019 г.* с 15 ч 00 мин. по 24.06.*2019 г.* до 15 ч 00 мин. время местное.
Прием заявок на участие в запросе котировок в письменной форме осуществляется по адресу: г. Архангельск, ул. Тимме д. 5, приемная главного врача, 3 этажа, в рабочие дни с 9-00 до 17-00 (местное время). Порядок подачи заявок - в соответствии с закупочной документацией.
8. Участники закупки должны отвечать следующим установленным требованиям:
- установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставку товара, являющихся предметом договора;
- не проведение ликвидации участника закупки - юридического лица и отсутствие решения арбитражного суда о признании участника закупки - юридического лица или индивидуального предпринимателя несостоятельным (банкротом) и об открытии конкурсного производства;
- не приостановление деятельности участника закупки в порядке, установленном Кодексом Российской Федерации об административных правонарушениях, на дату подачи заявки на участие в закупке;
- отсутствие у участника закупки 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). Участник закупки считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по такому заявлению на дату рассмотрения заявки на участие в определении поставщика не принято;
- отсутствие у участника закупки - физического лица либо у руководителя, членов коллегиального исполнительного органа или главного бухгалтера юридического лица - участника закупки судимости за преступления в сфере экономики (за исключением лиц, у которых такая судимость погашена или снята), 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 объектом осуществляемой закупки, и административного наказания в виде дисквалификации;
- обладание участником закупки исключительными правами на результаты интеллектуальной деятельности, если в связи с исполнением договора Заказчик приобретает права на такие результаты;
- отсутствие между участником закупки и Заказчиком конфликта интересов, под которым понимаются случаи, при которых руководитель Заказчика, член экспертной группы, член комиссии, лицо, ответственное за организацию конкурентной процедуры, состоят в браке с физическими лицами, являющимися выгодоприобретателями, единоличным исполнительным органом хозяйственного общества (директором, генеральным директором, управляющим, президентом и другими), членами коллегиального исполнительного органа хозяйственного общества, руководителем (директором, генеральным директором) учреждения или унитарного предприятия либо иными органами управления юридических лиц - участников закупки; с физическими лицами, в том числе зарегистрированными в качестве индивидуального предпринимателя, - участниками закупки либо являются близкими родственниками (родственниками по прямой восходящей и нисходящей линии (родителями и детьми, дедушкой, бабушкой и внуками), полнородными и не полнородными (имеющими общих отца или мать) братьями и сестрами), усыновителями или усыновленными указанных физических лиц.

Под выгодоприобретателями в данном случае понимаются физические лица, владеющие напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном капитале хозяйственного общества.
- отсутствие сведений об участниках закупки в реестре недобросовестных поставщиков, предусмотренном статьей 5 Федерального закона «О закупках товаров, работ, услуг отдельными видами юридических лиц», и (или) в реестре недобросовестных поставщиков, предусмотренном Федеральным законом «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».
9. Участник закупки вправе направить Заказчику письменный запрос на разъяснение Документации в сроки, установленные в Документации. Запрос от юридического лица оформляется на фирменном бланке участника закупки (при наличии), заверяется уполномоченным лицом участника закупки. Запрос может быть направлен посредством почтовой связи, факсимильной связи, курьерской доставки. Запрос не может быть направлен посредством электронной почты. Запрос о разъяснении Документации, полученный от участника позднее срока, установленного в Документации, не подлежит рассмотрению. Заказчик обязан опубликовать разъяснения на официальном сайте не позднее 2 рабочих дней со дня поступления запроса на разъяснение.
Заказчик обязан письменно ответить на запрос о разъяснении документации о проведении закупки. В случае его получения не позднее, чем за 2 рабочих дня до окончания срока подачи заявок, в течение двух рабочих дней, с 10 ч 00 мин. до 17 ч 00 мин., со дня его поступления, но не позднее срока окончания подачи заявок.
10. Место, дата и время рассмотрения заявок участников закупки и подведения итогов закупки установлены в Извещении о проведение запроса котировок.
11. Критерии и сопоставление заявок участников закупки.
Критериями оценки и сопоставления заявок участников закупки являются соответствие требованиям, установленным в Документации, и наиболее низкая цена товара, предложенная участником закупки.
установленным в Документации, и наиболее низкая цена товара, предложенная участником закупки.
12. Порядок и сопоставление заявок участников закупки:
Комиссия рассматривает котировочные заявки на предмет соответствия их требованиям, указанным в запросе котировок, и сопоставляет предложения по цене договора.
В ходе рассмотрения котировочных заявок комиссия вправе потребовать от участника закупки разъяснения сведений, содержащихся в котировочных заявках, не допуская при этом изменения содержания заявки.
В случае установления недостоверности информации, содержащейся в документах, представленных участником закупки, комиссия может отстранить такого участника на любом этапе проведения.
Комиссия может отклонить котировочные заявки в случае:
1) несоответствия котировочной заявки требованиям, указанным в запросе котировок;
2) при предложении в котировочной заявке цены товаров, работ, услуг выше начальной (максимальной) цены договора (цены лота);
3) отказа от проведения запроса котировок;
4) непредставления участником закупки разъяснений положений котировочной заявки (в случае наличия требования заказчика или организатора процедуры закупки).
Отклонение котировочных заявок по иным основаниям не допускается.
Лучшей признается котировочная заявка, которая отвечает всем требованиям, установленным в запросе котировок, и содержит наиболее низкую цену товаров, работ, услуг. При наличии нескольких равнозначных котировочных заявок лучшей признается та, которая поступила раньше.
13. Процедура закупки проводится в соответствии с требованиями Положения о закупке товаров, работ и услуг для нужд негосударственных учреждений здравоохранения ОАО «РЖД», утвержденным приказом Центральной дирекции здравоохранения ОАО «РЖД» от 02.04.2018 № ЦДЗ-35, размещенного на сайте заказчика.
Право Заказчика отказаться от проведения закупки.
Заказчик вправе отказаться от проведения закупки в любое время, в том числе после подписания протокола по результатам закупки. Заказчик не несет при этом никакой ответственности перед любыми физическими и юридическими лицами, которым такое действие может принести убытки.
Уведомление об отказе от проведения закупки размещается на сайте Заказчика не позднее 3 (трех) дней со дня принятия решения об отказе от проведения закупки.
14. Участник закупки вправе изменить или отозвать свою заявку до истечения срока подачи заявок. В этом случае участники закупки не утрачивают право на предоставленное обеспечение заявки. Изменение заявки или уведомление о ее отзыве является действительным, если изменение осуществлено или уведомление получено Заказчиком до истечения срока подачи заявок.
15. Требования к обеспечению заявок на участие в закупки: не установлены. Требования к обеспечению исполнения договора: не установлены.
16. Порядок заключения договора.
По результатам рассмотрения и оценки представленных котировочных заявок участнику размещения заказа, подавшему котировочную заявку, которая отвечает всем требованиям, установленным в настоящем извещении, и в которой указана наиболее низкая стоимость по договору, признанному победителем, будет направлен для подписания проект договора.
Договор может быть заключен не ранее чем через 3 (три) рабочих дня с момента размещения на официальном сайте www.medrzd29.ru протокола подведения итогов запроса котировок. Срок заключения договора по итогам закупки не может превысить 30 дней. Если в указанный срок победитель не представит Заказчику подписанный договор, победитель будет признан уклонившимся от заключения договора.
17. Срок, в течение которого победитель закупки или иной участник закупки, с которым заключается Договор при уклонении победителя закупки от заключения Договора, должен подписать Договор:
17.1. Если победитель закупки не исполнил необходимые для заключения договора условия, Заказчик вправе заключить договор с участником закупки, предложившим в закупочной заявке такую же цену, как и победитель в проведенной закупке,

или с участником закупки, предложение о цене договора которого содержит лучшие условия по цене договора, следующие после предложенных победителем в проведенной закупке условий.

Приложение:
1) Форма котировочной заявки;
2) Анкета участника запроса котировок цен;
3) Техническое задание;
4) Проект договора.

Председатель конкурсной комиссии – главный врач О.А.Савельева

Приложение № 1
к Документации о проведении закупки

ФОРМА

КОТИРОВОЧНАЯ ЗАЯВКА

на право заключения лицензионного договора на предоставление (передачу) прав на условиях простой (неисключительной) лицензии на использование программ для электронно-вычислительных машин (ЭВМ) для нужд НУЗ «Отделенческая больница на ст. Исакогорка ОАО «РЖД».

Адрес: 163000 г. Архангельск, ул. Тимме, д.5, (для приема заявок).

Телефон: 8 (8182) 67-30-10
nuz-secretar@medrzd29.ru

Уважаемые господа!

Мы, _____
(наименование, организационно-правовая форма, **ИНН**, ОГРН, место нахождения, почтовый адрес участника закупки (для юридического лица), фамилия, имя, отчество, паспортные данные, место жительства участника закупки (для физического лица), номер телефона, адрес электронной почты, банковские реквизиты участника размещения заказа)
на основании Вашего извещения о проведении запроса котировок предлагаем поставить товар:

№ п/п	Наименование работ, услуг/ Характеристика работ, услуг	Ед. изм.	Кол-во	Цена (руб.)	Сумма (руб.)
1		шт.	1		
2		шт.	2		
Итого:					

Итого сумма договора _____ *(Указать цифрами и прописью)* руб., в том числе НДС (__%) _____рублей.

Условия исполнения договора:

Место выполнения Работ, оказания Услуг: Место выполнения Работ, оказания Услуг: по месту нахождения Исполнителя. Место предоставления результатов работ, услуг (передачи прав на условиях простой (неисключительной) лицензии для использования программ для ЭВМ) Архангельск, ул. Тимме, д.5, в рабочие дни (с понедельника по пятницу, исключая праздничные дни) с 8.00 до 15.00.

Срок выполнения работ, оказания услуг по предоставлению неисключительных лицензионных прав: в течение 5 (пяти) рабочих дней с момента подписания договора.

Стоимость Работ(услуг) составляет:

_____ (_____) рублей _____ копеек.

Стоимость Работ(услуг) включает:

Стоимость Работ по договору включает в себя стоимость работ и услуг, накладные и плановые расходы, все налоги и пошлины и иные обязательные платежи, а также вознаграждение исполнителя за передачу исключительных имущественных прав на результаты интеллектуальной деятельности передаваемые исполнителем заказчику по договору (Приложение № 4 к документации о проведении закупки).

Срок и порядок оплаты Работ(услуг):

Безналичный расчет на основании счета, после заключения договора в течении 30 (тридцати) календарных дней, с момента подписания акты приемки-передачи объекта интеллектуальной собственности.

При подаче котировочной заявки в соответствии с Вашим запросом котировок, мы выражаем согласие с условиями договора, указанными в запросе котировок, а также мы берем на себя обязательства представить документы (оригиналы или заверенные копии), подтверждающие сведения, указанные в котировочной заявке, а именно;

- Учредительные документы с учетом внесенных в них изменений, свидетельства о государственной регистрации учредительных документов и внесенных в них изменений;
- Свидетельство о государственной регистрации контрагента, свидетельство о внесении в государственный реестр изменений в сведения о юридическом лице, не связанных с внесением в учредительные документы, свидетельство о постановке на учет в налоговом органе;
- Выписка из единого государственного реестра юридических лиц, выданная регистрирующим органом не ранее чем за один месяц до предоставления документов;
- Документы, подтверждающие полномочия лица на подписание договора, оформленные надлежащим образом (протокол (решение) уполномоченного органа управления контрагента о назначении Исполнительного органа; оригинал доверенности, если договор со стороны контрагента подписан не единоличным Исполнительным органом; согласие соответствующего органа управления контрагента на совершение сделки, предусмотренной договором, в случаях, когда это определено законодательством Российской Федерации и учредительными документами контрагента);
- Согласие контролирующих органов на совершение сделки или подтверждение уведомления соответствующих органов о совершении сделки в случаях, когда такое согласие или уведомление предусмотрено законодательством Российской Федерации;
- Информационная справка, содержащая сведения о владельцах контрагента, включая конечных бенефициаров, с

приложением подтверждающих документов;

Настоящей заявкой подтверждаем, что против _____
(наименование Участника размещения заказа)

- не проводится ликвидация Участника закупки – юридического лица и отсутствуют решения арбитражного суда о признании Участника закупки - юридического лица, индивидуального предпринимателя несостоятельным (банкротом) и об открытии конкурсного производства,
- не проводится приостановление деятельности Участника закупки в порядке, установленном Кодексом Российской Федерации об административных правонарушениях, на дату подачи заявки на участие в закупке,

Настоящей заявкой подтверждаем, что у _____ *(наименование Участника размещения заказа)*

- отсутствуют 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),
- у руководителя, членов коллегиального исполнительного органа или главного бухгалтера юридического лица – участника закупки отсутствуют судимости за преступления в сфере экономики (за исключением лиц, у которых такая судимость погашена или снята), 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 объектом осуществляемой закупки, и административного наказания в виде дисквалификации,
- имеются исключительные права на результаты интеллектуальной деятельности, если в связи с исполнением договора заказчик приобретает права на такие результаты,
- и заказчиком процедуры закупки отсутствует конфликт интересов, под которым понимаются случаи, при которых руководитель заказчика и, член экспертной группы, член комиссии, лицо, ответственное за организацию конкурентной процедуры, состоят в браке с физическими лицами, являющимися выгодоприобретателями, единоличным исполнительным органом хозяйственного общества (директором, генеральным директором, управляющим, президентом и другими), членами коллегиального исполнительного органа хозяйственного общества, руководителем (директором, генеральным директором) учреждения или унитарного предприятия либо иными органами управления юридических лиц - участников закупки, с физическими лицами, в том числе зарегистрированными в качестве индивидуального предпринимателя, - участниками закупки либо являются близкими родственниками (родственниками по прямой восходящей и нисходящей линии (родителями и детьми, дедушкой, бабушкой и внуками), полнородными и не полнородными (имеющими общих отца или мать) братьями и сестрами), усыновителями или усыновленными указанных физических лиц. Под выгодоприобретателями в данном случае понимаются физические лица, владеющие напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном капитале хозяйственного общества.
- отсутствуют сведения об участнике закупки в реестре недобросовестных поставщиков, предусмотренном статьей 5 Федерального закона «О закупках товаров, работ, услуг отдельными видами юридических лиц», и (или) в реестре недобросовестных поставщиков, предусмотренном Федеральным законом «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

В случае, если наши предложения будут признаны лучшими, мы берем на себя обязательства подписать договор в соответствии с требованиями Извещения и условиями наших предложений, не позднее чем через 5 (пять) календарных дней со дня публикации победителя на официальном сайте.

Сообщаем, что для оперативного уведомления нас по вопросам организационного характера и взаимодействия с Заказчиком нами уполномочен _____ *(Ф.И.О., телефон сотрудника)*

Все сведения о проведении запроса котировок просим сообщать уполномоченному лицу.

_____	_____	_____
(должность подписавшего)	(подпись) М.П.	(фамилия, инициалы)

Приложение №2
к Документации о проведении закупки

АНКЕТА УЧАСТНИКА РАЗМЕЩЕНИЯ ЗАКАЗА

1. Полное и сокращенное наименования организации и ее организационно-правовая форма *(на основании Учредительных документов установленной формы (устав, положение, учредительный договор), свидетельства о государственной регистрации, свидетельства о внесении записи в единый государственный реестр юридических лиц)* **Ф.И.О. участника размещения заказа – физического лица**	
2. Регистрационные данные: Дата, место и орган регистрации юридического лица, регистрации физического лица в качестве индивидуального предпринимателя *(на основании Свидетельства о государственной регистрации)* **Паспортные данные для участника размещения заказа – физического лица**	
3. 3.1. Номер и почтовый адрес Инспекции Федеральной налоговой службы, в которой участник размещения заказа зарегистрирован в качестве налогоплательщика	
3.2.ИНН, КПП, ОГРН, ОКПО участника размещения заказа	**ИНН** **КПП** **ОГРН** **ОКПО**
4.Юридический адрес/место жительства участника размещения заказа	**Страна Россия** **Адрес:**
5. Почтовый адрес участника размещения заказа	**Страна Россия** **Адрес:** **Телефон:** **Факс:**
6.Банковские реквизиты *(может быть несколько)*: 6.1. Наименование обслуживающего банка 6.2. Расчетный счет 6.3. Корреспондентский счет 6.4. Код БИК	
7. Сведения о выданных участнику размещения заказа лицензиях, необходимых для выполнения обязательств по контракту *(указывается лицензируемый вид деятельности, реквизиты действующей лицензии, наименование территории на которой действует лицензия)*	

Мы, нижеподписавшиеся, заверяем правильность всех данных, указанных в анкете.
Участник размещения заказа
(уполномоченный представитель) _____ (подпись) _____ (фамилия, инициалы).

Главный бухгалтер _____ (подпись) _____ (фамилия, инициалы).

М.П.
Директор _____ (подпись) _____ (фамилия, инициалы).
(должность подписавшего
(для юридического лица))

Приложение № 3
к Документации о проведении закупки

Техническое задание

на оказание услуг по предоставлению неисключительных лицензионных прав на антивирусное программное обеспечение «Kaspersky Endpoint Security для бизнеса - Стандартный» (продление с расширением).

Поставляемое программное обеспечение должно быть включено в единый реестр российских программ для электронных вычислительных машин и баз данных в соответствии со статьей 12.1. Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации

п/п	Наименование товара	Основные характеристики товара
	Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 50-99 Node 2 year Renewal License	Описание объекта закупки: Kaspersky Endpoint Security для бизнеса - Стандартный - 50-99 Node 2 year Renewal License (KL4863RAQDR) Тип ключа: для бизнеса - Стандартный Количество лицензий:1 Количество защищаемых объектов в рамках лицензии:70 Срок подписки: Срок действия лицензии - 24 (Двадцать четыре) месяца с момента активации ключа доступа Место оказания услуг: Российская Федерация. г. Архангельск, ул. Тимме 5 Срок оказания услуг по предоставлению неисключительных лицензионных прав на антивирусное программное обеспечение «Kaspersky Endpoint Security для бизнеса - Стандартный»: в течение 5 (пяти) рабочих дней с момента подписания договора 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 Linux. Программные средства антивирусной защиты для файловых серверов Windows. Программные средства антивирусной защиты для файловых серверов Linux. Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных 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 языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке. Требования к программным средствам антивирусной защиты для рабочих станций Windows: Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64; Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 и выше x86 / x64; Microsoft Windows 8 Professional /Enterprise x86 / x64; Microsoft Windows 8.1 Professional / Enterprise x86 / x64; Microsoft Windows 10 Pro / Enterprise x86 / x64; Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей: Антивирусное сканирование в режиме реального времени и по запросу. Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы. Антивирусное сканирование по расписанию. Запуск задач по расписанию и/или сразу после загрузки операционной системы. Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем. Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу. Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP — независимо от используемого почтового клиента; Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристическогоанализа, с возможностью настройки доверенных сайтов. Блокировка баннеров и всплывающих окон, загружаемых с Web- страниц. Распознавание и блокировка фишинг-сайтов. Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет пейджерами. Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения. Возможность совершить

откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных вредоносными программами файлов.
Возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам.
Автоматическое определение уровней ограничения на основании репутации программы.
Наличие механизмов защиты от атак типа BadUSB.
Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых
правил для конкретных программ.
Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных
приложений при работе в вычислительных сетях любого типа, включая беспроводные.
Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме MD5 или SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory. Осуществление 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.
Осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.).
Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory.
Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось. Запуск специальной задачи для
обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файловогопространства.
Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая
избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.
Возможность установки только выбранных компонентов программного средства антивирусной защиты.
Полно дисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On. Обязательно наличие инструментов восстановления, зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС. Должна быть реализована поддержка UEFI- систем.
Поддержка двухфакторной аутентификации при полно дисковом 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 выбранныхприложений.
Шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети
организации. Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
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 Sierra 10.12
•Mac OS X 10.11 (El Capitan)
•Mac OS X 10.10 (Yosemite)
• Mac OS X 10.9 (Mavericks)
• Mac OS X 10.8 (Mountain Lion)
• Mac OS X 10.7 (Lion)
Программные средства антивирусной защиты для рабочих станций Mac должныобеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг.
Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы. Антивирусное сканирование по команде пользователя или администратора и по расписанию.
Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
Централизованное управление всеми вышеуказанными
компонентами с помощью едином системы управления.
Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу.
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.
Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS. Автоматическое обновление антивирусных баз по расписанию.
Защита информации, передаваемой через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик).
Требования к программным средствам антивирусной защиты для рабочих станций Linux:
Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
• Red Hat® Enterprise Linux® 6.7 x86/x64
• Red Hat® Enterprise Linux® 6.8 x86/x64
• Red Hat® Enterprise Linux® 7.2 x64
• Red Hat® Enterprise Linux® 7.3 x64
• CentOS-6.7 x86/x64
• CentOS-6.8 x86/x64
• CentOS-7.2 x64
• CentOS-7.3 x64
• SUSE® Linux Enterprise Desktop 12 x64
• openSUSE® 42.2 x64
• Debian GNU/Linux 7.10 x86/x64
• Debian GNU/Linux 7.11 x86/x64
• Debian GNU/Linux 8.6 x86/x64
• Debian GNU/Linux 8.7 x86/x64
• Ubuntu 10.04 LTS x86/x64
• Ubuntu 12.04 LTS x86/x64
• Ubuntu Server 14.04 LTS x86/x64
• Ubuntu Server 16.04 LTS x86/x64
• Ubuntu Server 16.10 LTS x86/x64
• OracleLinux 7.3 x64
Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг.
Проверка ресурсов доступных по SMB / NFS Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.
Антивирусное сканирование по команде пользователя или администратора и по расписанию.
Антивирусная проверку и лечение файлов в архивах.
Запуск задач по расписанию и/или сразу после загрузки операционной системы.
Помещение подозрительных и поврежденных объектов на карантин.
Возможность экспортировать и сохранять отчеты в форматах HTML и CSV.
Возможность перехвата и проверки файловых операций на уровне SAMBA.
Гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу.
Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он
представляет информационную ценность.
Возможность управления через пользовательский графический интерфейс.
Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
Требования к программным средствам антивирусной защиты для файловых серверов Windows.
Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением
операционных систем следующих версий:
• Microsoft Windows Small Business Server 2011 Standard x64;
• Microsoft Windows Server 2008 Standard / Enterprise SP2 x86/x64;
• Microsoft Windows Server 2008 R2 Standard / Enterprise x64 SP1;
• Microsoft Windows Server 2012 Standard / Foundation x64;
• Microsoft Windows Server 2012 R2 Standard x64.
• Microsoft Windows Server 2016 x64.
Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:
Антивирусное сканирование в режиме реального времени и по запросу.
Антивирусное сканирование по команде пользователя или администратора и по расписанию.
Запуск задач по расписанию и/или сразу после загрузки операционной системы.
Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу.
Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов.
Создание сетевых правил для конкретных программ.
Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных

приложений при работе в вычислительных сетях любого типа, включая беспроводные.
Запуск специальной задачи для обнаружения уязвимостей в
приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
Антивирусная проверка и лечение файлов в
архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем.
Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
Настройки проверки критических областей сервера в качестве отдельной задачи.
Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать
антивирусное сканирование в фоновом режиме.
Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий).
Защита от удаленного несанкционированного управления
сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.
Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory.
Централизованное управление всеми вышеуказанными
компонентами с помощью единой системы управления.
Требования к программным средствам антивирусной защиты для файловых серверов Linux:
Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
• Red Hat® Enterprise Linux® 6.7 x86/x64
• Red Hat® Enterprise Linux® 6.8 x86/x64
• Red Hat® Enterprise Linux® 7.2 x64
• Red Hat® Enterprise Linux® 7.3 x64
• CentOS-6.7 x86/x64
• CentOS-6.8 x86/x64
• CentOS-7.2 x64
• CentOS-7.3 x64
• SUSE® Linux Enterprise Desktop 12 x64
• openSUSE® 42.2 x64
• Debian GNU/Linux 7.10 x86/x64
• Debian GNU/Linux 7.11 x86/x64
• Debian GNU/Linux 8.6 x86/x64
• Debian GNU/Linux 8.7 x86/x64
• Ubuntu 10.04 LTS x86/x64
• Ubuntu 12.04 LTS x86/x64
• Ubuntu Server 14.04 LTS x86/x64
• Ubuntu Server 16.04 LTS x86/x64
• Ubuntu Server 16.10 LTS x86/x64
• OracleLinux 7.3 x64
Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг.
Антивирусное сканирование по команде пользователя или администратора и по расписанию.
Проверка ресурсов доступных по SMB / NFS.
Антивирусная проверка и лечение файлов в архивах.
Запуск задач по расписанию и/или сразу после загрузки операционной системы.
Помещение подозрительных и поврежденных объектов на карантин.
Формирование отчетов в форматах HTML, CSV, PDF и XLS. Возможность перехвата и проверки файловых операций на уровне.
Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он
представляет информационную ценность.
Удаленно через веб-браузер управлять антивирусом и настраивать его.
Централизованно управляться с помощью единой системы управления.
Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows:
Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
• Microsoft Windows Server 2008
Standard/Enterprise/DataCenter/Core SP1 и выше x86/x64;
• Microsoft Windows Server 2008 R2 Core/ Standard/Enterprise/DataCenter SP1 и выше x64;
• Microsoft Windows Server 2012 Core/Standard/Essential/DataCenter/Foundation x64;
• Microsoft Windows Server 2012 R2 Core/Standard/Essential/DataCenter/Foundation x64;
• Microsoft Windows Server 2016 Core/Standard/Datacenter/Essentials x64;

• Microsoft Windows Storage Server 2008 R2 x64;
• Microsoft Windows Storage Server 2008 R2 SP2 Standard/Workgroup x64;
• Microsoft Windows Storage Server 2012 (все редакции) x64;
• Microsoft Windows Storage Server 2012 R2 (все редакции) x64;
• Microsoft Windows Storage Server 2016 x64;
• Microsoft Windows Hyper-V Server 2008 R2 SP1 x64;
• Microsoft Windows Hyper-V Server 2012 x64;
• Microsoft Windows Hyper-V Server 2012 R2 x64;
• Microsoft Windows Hyper-V Server 2016 x64.
Терминальные серверы:
• Microsoft Remote Desktop Services на базе Windows Server 2008;
• Microsoft Remote Desktop Services на базе Windows Server 2012;
• Microsoft Remote Desktop Services на базе Windows Server 2012 R2;
• Microsoft Remote Desktop Services на базе Windows Server 2012;
• Citrix XenApp 6.0/6.5/7.0/7.5 - 7.9;
• Citrix XenDeskTop 7.0/7.1/7.5/7.9.
Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:
Осуществление антивирусной проверки на серверах, выполняющих разные функции: Серверов терминалов и принт- серверов; Серверов приложений и контроллеров доменов; Файловых серверов.
Возможность использования для защиты кластера серверов. Проверка следующих объектов защищаемого сервера при доступе к ним: Файлов при их записи и считывании; Альтернативных потоков файловых систем (NTFS-streams); Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей.
Предотвращение вирусных эпидемий за счет фиксации возникновения вирусных атак.
Восстановление после заражения путем удаления всех связанных с ликвидированным вредоносным объектом записей в системных файлах и реестре ОС, что предотвращает возможные сбои в работе 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.
Контроль запуска исполняемых файлов, скриптов и пакетов MSI, а также DLL модулей и драйверов с возможностью запрета запуска недоверенных приложений.
Возможность автоматически сформировать набор правил запуска приложений на основании текущего набора ПО на одном сервере.
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.
Возможность блокировки доступа удаленного компьютера к сетевым ресурсам сервера.
Отслеживание попыток вредоносного шифрования файлов на общих сетевых папках сервера и блокирование компьютеров с которых идет такая активность.
Проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере.
Проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи.
Помещение подозрительных и поврежденных объектов на карантин.
Возможность восстановления файлов из карантина в сетевые папки.
При защите терминальных серверов поддержка режимов публикации рабочего стола и публикации приложений. Масштабируемость за счет задания количества рабочих процессов антивируса для ускорения обработки запросов к серверу при использовании многопроцессорных серверов.
Балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач:
антивирусная проверка может продолжаться в фоновом режиме.
Выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие). Наличие локальной консоли управления.
Возможность подключения к другим средствам защиты для серверов масштаба предприятия с помощью локальной консоли.
Разделение прав администраторов, основанное на стандартных механизмах ОС Microsoft Windows.
Наличие встроенных исключений для стандартных ролей сервера (Контролер домена, Сервер БД и тд). Уведомления различными методами администраторов и пользователей о событиях в антивирусной защите. Поддержка Simple Network Management Protocol (SNMP).
Поддержка технологий ReFS(Resilient file system) и CSV (Cluster Shared Volume).
Централизованно управляться с помощью единой системы управления.
Требования к программным средствам антивирусной защиты мобильных устройств:
Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:
• Android 4.0-7.1.1;
• Apple iOS 8.0— 10.0;
• Windows Phone 8.1, 10.
Решение должно централизованно управлять с помощью единой консоли управления.
Программные средства для антивирусной защиты смартфонов для ОС Android должны обеспечивать следующую функциональность:
Постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем

проверки на
репутационных облачных сервисам производителя антивирусных средств защиты.
Мгновенная проверка устанавливаемых приложений.
Проверка файловой системы устройства по требованию и по расписанию.
Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных
облачных сервисов производителя антивирусных средств защиты.
Поддержка белых списков разрешенных сайтов.
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.
Возможность получения политик безопасности через Google Cloud Messaging.
Базовая поддержка Android for Work.
Наличие возможности создания специальной оболочки для мобильных программ с целью контроля
действий программы, возможностью удаления данных и настроек
программы, добавления дополнительного пароля для старта приложения, в том числе с помощью
учетных данных Active Directory .
Возможность заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного
устройства.
Указание параметров подключения к wi-fi сетям.
Наличие возможности указания обязательных к установке приложений.
Блокирование нежелательных SMS сообщений, возможность блокировки мобильного устройства,
удаление данных, удаление данных связанных с рабочей деятельностью, получение координат
местоположения устройства, удаленного возврата к заводским настройкам (factory reset).
Постоянная проверка телефона на соответствие корпоративным политикам с возможностью
автоматической блокировки устройства, удаления данных, запрета
запуска корпоративных приложений при выявлении несоответствий.
Возможность получения текущего номера SIM-карты телефона посредством СМС, возможность
автоматической блокировки устройства при смене SIM-карты или при
включении телефона без SIM-карты.
Поддержка технологий Samsung KNOX1 и KNOX2.
Программные средства для антивирусной защиты смартфонов для ОС Apple Ios должны
обеспечивать следующую функциональность:
Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных
сервисов производителя антивирусных средств защиты.
Возможность определения местоположения устройства. Программные средства для антивирусной
защиты смартфонов для ОС Windows Phone должны обеспечивать
следующую функциональность:
Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных
сервисов производителя антивирусных средств защиты.
Возможность определения местоположения устройства. Требования к программным средствам
централизованного управления, мониторинга и обновления Программные средства
централизованного управления, мониторинга и
обновления должны функционировать на компьютерах, работающих под управлением операционных
систем следующих версий:
• Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 x86 / x64;
• Microsoft Windows 8 Professional / Enterprise x86 / x64;
• Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
• Microsoft Windows 10 Professional/Enterprise/Education x86 / x64;
• Microsoft Windows 10 RSI x86 /x64;
• Microsoft Windows 10 RS2 x86 / x64;
• Microsoft Windows Server 2008
Foundation/Standard/Enterprise/Datacenter SP1 x86 / x64;
• Microsoft Windows Server 2008;
• Microsoft Windows Server 2008 SP1 x86 / x64;
• Microsoft Windows Server 2008 R2 Core/Foundation/Standard/Enterprise/Datacenter
x64;
• Microsoft Windows Server 2008 R2 Core/Foundation/Standard/Enterprise/Datacenter
SP1 x64;
• Microsoft Windows Server 2012 Core/Foundation/Standard/Enterprise/Datacenter x64;
• Microsoft Windows Server 2012 R2
Core/Essentials/Foundation/Standard/Enterprise/Datacenterx64;
• Microsoft Windows Small Business Server 2008 Standard/Premium x64;
• Microsoft Windows Small Business Server 2011 Essentials/Premium/Standard x64.
Программные средства централизованного управления, мониторинга и обновления должны
функционировать с СУБД следующих версий:
• Microsoft SQL Express 2008/2008R2/2012/2014;
• Microsoft SQL Server 2008/2008R2/2012/2014/2016;
• Microsoft Azure SQL Database;
• MySQL 5.5, 5.6, 5.7 x86/x64;
• MySQL Enterprise 5.5, 5.6, 5.7 x86/x64.
Программные средства централизованного управления, мониторинга и обновления
должны функционировать на виртуальных платформах следующих версий:
• VMware Workstation 9.x, Workstation 10.x, 12x Pro;

• VMware vSphere 5.5, 6;
• Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1,2012, 20012 R2;
• Microsoft VirtualPC 2007(6.0.156.0);
• Parallels Desktop 7,11;
• Citrix XenServer 6.1, 6.2, 6.5, 7;
• Oracle VM VirtualBox 4.0.4-70112.
Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:
• Установка системы управления антивирусной защиты из единого дистрибутива.
• Выбор установки в зависимости от количества защищаемых узлов.
• Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.
• Возможность поиска и обнаружения компьютеров в сети по IP- адресу, имени хоста, имени домена, маске подсети.
• Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.
• Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.
• 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.
• Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности. Должна быть реализована возможность поддержки иерархии таких триггеров.
• Автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.
• 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.
• Автоматическое развертывание по требованию специализированной системы защиты для виртуальных инфраструктур на базе VMware ESXi, Microsoft Hyper-V, Citrix XenServer.
• Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне.
• 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.
• 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.
• Возможность подключения по RDP или штатными средствами из консоли управления. Пользователю должен выводиться запрос на разрешение дистанционного подключения.
• Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.
• 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 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
• Функция управления мобильными устройствами через сервер Exchange ActiveSync.
• Функция управления мобильными устройствами через сервер iOS MDM.
• Возможность отправки SMS-оповещений о заданных событиях.

• Централизованная установка приложений на управляемые мобильные устройства.
• Централизованная установка сертификатов на управляемые мобильные устройства.
• Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.
• Возможность 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 как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд.
• Наличие преднастроенных стандартных отчетов о работе системы.
• Экспорт отчетов в файлы форматов PDF и XML.
• Возможность передачи событий из базы данных в IBM Qradar и HP Arcsight или по Syslog (RFC 5424).
• 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 веб-консоли управления приложением.
• Наличие портала самообслуживания пользователей. Портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя.
• Наличие системы контроля возникновения вирусных эпидемий. Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:
• Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток.
• Множественность путей обновления, в том числе - по каналам связи и на отчуждаемых электронных носителях информации.
• Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

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.

Требования к качеству и безопасности:

Антивирусные программные средства должны быть включены в единый реестр российских программ для электронных вычислительных машин и баз данных.

При поставке пакетов безопасности Сублицензиату должны быть предоставлены:
лицензионное соглашение, определяющее условия использования Сублицензиатом программного обеспечения и подтверждающее права Сублицензиата на обновление и поддержку (гарантийное сопровождение);
-лицензионный ключ официального исполнения;
- комплект документации на русском языке.
- руководство пользователя (администратора).

Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.
- регистрационная информация должна быть предоставлена в виде ключевого файла/авторизационного номера/кода активации, которая генерируется Правообладателями программного обеспечения персонально для Сублицензиата и необходима и достаточна для полнофункциональной работоспособности ПО, на материальном носителе или по согласованию с Сублицензиатом по сети Интернет на электронный почтовый адрес, указанный Сублицензиатом;

Применение эквивалента не допускается по причине необходимости обеспечения совместимости с имеющимся у Сублицензиата программным обеспечением.

Лицензиат должен являться авторизированным партнером правообладателя (Письмо / Сертификат) / Правообладателем.

Объем и сроки предоставления гарантии качества услуги:

Срок предоставления гарантии качества услуг — на весь период продления неисключительного права на использование и воспроизведение антивирусного программного обеспечения.

Предоставление обновлений программного обеспечения (регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз антиспама не реже одного раза в 5 минут; множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;
предоставление технической возможности обновления баз сигнатур по мере выявления новых версий вредоносного программного кода);
-предоставление обновления антивирусного программного обеспечения и сигнатур угроз в течение всего срока действия лицензии;
- предоставление комплекта документации;
предоставление консультаций Сублицензиату по вопросам инсталляции программного обеспечения, авторизации программного обеспечения, описанию основных функциональных возможностей

		программного обеспечения и области его применения, ответы на вопросы по описанию новых функций новых версий программного обеспечения; безвозмездное исправление по требованию Сублицензиата всех выявленных недостатков, если в процессе оказания услуги Лицензиат допустил отступление от условий контракта, ухудшившее качество услуг, в течение 5 календарных дней с момента вручения в письменном виде Сублицензиатом соответствующего требования Лицензиату. Техническая поддержка антивирусного программного обеспечения: - Должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет. - на веб-сайте производителя средств антивирусной защиты должны быть опубликованы: специальный раздел, посвящённый технической поддержке антивирусного программного обеспечения; пополняемая база знаний; форум пользователей программных продуктов. Гарантийные обязательства: Гарантийный срок на оказываемую Лицензиатом услугу (включая возможность ежедневного обновления баз данных сигнатур по средствам сети Интернет) составляет 12 (двенадцать) месяцев с момента активации ключа доступа . Требования к наличию сертификатов и лицензий: Антивирусное программное обеспечение должно иметь: • действующий на момент заключения договора сертификат соответствия ФСТЭК России, подтверждающий соответствие требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012, «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012) «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012); • действующий на момент заключения договора сертификат соответствия ФСБ России, подтверждающий обеспечение безопасности информации при инсталляции и использовании программного изделия. Требования к гарантийным обязательствам: «Лицензиат» должен гарантировать, что программное обеспечение, на неисключительные права использования которого передаются лицензии в соответствии с настоящим Техническим заданием (далее - ПО), является полностью лицензионным, правомерно введено в гражданский оборот на территории Российской Федерации и обеспечивается технической поддержкой соответствующих правообладателей (производителей), а также, что предоставляемые в соответствии с данными лицензиями неисключительные права использования программного обеспечения не нарушают каких- либо авторских прав, неимущественных и/или имущественных прав любых третьих лиц. «Лицензиат» должен гарантировать бесперебойное функционирование программного обеспечения на автоматизированных рабочих местах «Сублицензиата». «Лицензиат» должен гарантировать то, что гарантийный период, в течение которого «Лицензиат» обязуется безвозмездно (за свой счет) исправлять ошибки в программном обеспечении, которые приводят к невозможности реализации (использования) «Сублицензиатом» каких-либо функций программного обеспечения, должен составлять не менее 24 месяцев

Приложение № 4
к Документации о проведении закупки

ЛИЦЕНЗИОННЫЙ ДОГОВОР № _____ **ПРОЕКТ**

г. Архангельск «___»_____ 20__ г.

_____, именуемое в дальнейшем **«Лицензиар»** в лице _____, действующего на основании _____ с одной стороны, и **Негосударственное учреждение здравоохранения «Отделенческая больница на станции Исакогорка открытого акционерного общества "Российские железные дороги" (НУЗ "Отделенческая больница на ст. Исакогорка ОАО "РЖД")**, именуемое в дальнейшем **«Лицензиат»**, в лице главного врача Савельевой Ольги Анатольевны, действующего на основании Устава, с другой стороны, вместе именуемые «Стороны», заключили настоящий Договор о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Лицензиар обязуется предоставить Лицензиату право использования объекта интеллектуальной собственности - _____, (далее - Программное обеспечение) в порядке, предусмотренном Договором, а Лицензиат обязуется уплатить Лицензиару обусловленное Договором вознаграждение.

1.2. Лицензиар гарантирует, что является правообладателем исключительного права на Программное обеспечение.

1.3. Принадлежность исключительного права на Объект интеллектуальной собственности Лицензиару подтверждается:_____.

1.4. В целях идентификации Объекта интеллектуальной собственности Лицензиар передает Лицензиату в 1 (одном) экземпляре Программное обеспечение на материальном носителе в электронном виде по Акту приемки-передачи объекта интеллектуальной собственности на материальном носителе по форме, согласованной в Приложении № 1.

1.5. Лицензиату предоставляется право использования Программного обеспечения с сохранением за Лицензиаром права выдать лицензии другим лицам (простая (неисключительная) лицензия).

1.6. Лицензиар передает Лицензиату Программное обеспечение на материальном носителе в электронном виде, по адресу: г. Архангельск ул. Тимме д. 5, с 9 час. до 16 час., в будние дни по предварительному согласованию точного времени.

2. ПРАВА, ПЕРЕДАВАЕМЫЕ ЛИЦЕНЗИАТУ

2.1. По настоящему Договору Лицензиату предоставляется право использовать Программное обеспечение следующим способом: _____.

2.2. По настоящему Договору использование Лицензиатом Программного обеспечения допускается на территории всего мира.

2.3. Лицензиат вправе заключать сублицензионный договор без дополнительного получения письменного одобрения по каждому такому факту.

2.4. Лицензиат обязан предоставить Лицензиару, по первому требованию (требование должно быть оформлено в письменном виде), в течение 5 (пяти) рабочих дней со дня направления такого требования, отчет в письменном виде о результатах использования объекта интеллектуальной собственности или средства индивидуализации, согласно условиям настоящего Договора.

2.5. Под исключительным правом на вновь созданный объект интеллектуальной собственности Стороны понимают и признают: право Лицензиата на все результаты интеллектуальной деятельности, которые возникнут, в том числе, в процессе реализации прав по настоящему Договору. Лицензиат приобретает исключительные права в полном объеме, и вправе использовать в любой форме и любыми не противоречащими закону способами.

2.6. Исключительные права на вновь созданный объект интеллектуальной собственности – Программное обеспечение – возникают у Лицензиата с момента создания данного объекта интеллектуальной собственности.

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. Лицензиар обязуется:

3.1.1. Передать Лицензиату Программное обеспечение, свободным от прав третьих лиц, в состоянии, позволяющем его использование на условиях настоящего Договора, в течение десяти дней с момента заключения настоящего Договора.

3.1.2. Передать Лицензиату экземпляр Программного обеспечения на материальном носителе, содержащем программу для установки, а также техническую документацию к Программному обеспечению.

3.2. Лицензиар вправе:

3.2.1. В случае нарушения Лицензиатом условий (способов) использования прав на Программное обеспечение по Договору, лишить Лицензиата лицензии на использование прав на Программное обеспечение.

3.2.2. Договор предоставляет Лицензиату право на использование Программного обеспечения с сохранением за Лицензиаром права выдачи лицензий другим лицам. Лицензиат может использовать экземпляр Программного обеспечения только в пределах тех прав и теми способами, которые предусмотрены Договором.

3.3. Лицензиат обязуется:

3.3.1. Выплатить Лицензиару вознаграждение за предоставление (передачу) Лицензиату прав на использование Программного обеспечения в порядке и сроки, установленные Договором.

3.3.2. Использовать Программное обеспечение исключительно способами, предусмотренными Договором.

3.3.3. Строго придерживаться и не нарушать условий Договора, а также обеспечить конфиденциальность полученной при сотрудничестве с Лицензиаром коммерческой и технической информации.

3.4. Лицензиат вправе:

3.4.1. Предоставить право использования Программного обеспечения в соответствии с настоящим Договором другому лицу.

3.4.2. Отказаться от исполнения Договора, если Лицензиар в нарушение условий Договора отказывается передать Лицензиату право на использование Программного обеспечения по Договору.

4. ВОЗНАГРАЖДЕНИЕ И СРОК ОПЛАТЫ

4.1. Вознаграждение Лицензиара, за предоставление Лицензиату прав на использование Программного обеспечения по Договору составляет: _____(_____) рублей ___ копеек в месяц (НДС не облагается на основании пп. 26 п. 2 ст. 149 НК РФ).

4.2. Оплата по Договору осуществляется Лицензиатом в безналичной форме, путем перечисления денежных средств на расчетный счет Лицензиара в течении 30 календарных дней.

4.3. Датой исполнения обязательства Лицензиата по оплате считается дата списания денежных средств с расчетного счета Лицензиара.

4.4. Проценты на сумму оплаты по Договору не начисляются и не уплачиваются.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За невыполнение или ненадлежащее выполнение обязательств по настоящему Договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

5.2. Использование Лицензиатом Программного обеспечения способом, не предусмотренным настоящим Договором, либо по прекращении действия Договора, либо иным образом за пределами прав, предоставленных Лицензиату по Договору, влечет ответственность за нарушение исключительного права на результат интеллектуальной деятельности, установленную законодательством.

5.3. При существенном нарушении Лицензиатом обязанности уплатить Лицензиару в установленный срок вознаграждение за предоставление лицензии Лицензиар может в одностороннем порядке отказаться от настоящего Договора и потребовать возмещения убытков, причиненных расторжением такого Договора.

6. КОНФИДЕНЦИАЛЬНОСТЬ

6.1. Условия настоящего Договора и дополнительных соглашений к нему, а также все материалы и (или) сведения, принадлежащие Лицензиару в отношении Программного обеспечения, ставшие известными Лицензиату, конфиденциальны и не подлежат разглашению.

6.2. Лицензиат обязан сохранять конфиденциальность сведений, касающихся Программного обеспечения и иных прав Лицензиара, в течение всего срока действия настоящего Договора.

6.3. Лицензиар имеет право с момента заключения настоящего Договора и в течение срока его действия в любой момент потребовать от Лицензиата заключения отдельного соглашения о неразглашении конфиденциальной информации, касающейся предмета настоящего Договора, а Лицензиат обязан заключить его и соблюдать условия.

7. РАЗРЕШЕНИЕ СПОРОВ

7.1. Все споры, возникающие при исполнении настоящего Договора, решаются Сторонами путем переговоров, которые могут проводиться в том числе, путем отправления писем по почте, обмена факсимильными сообщениями.

7.2. Если Стороны не придут к соглашению путем переговоров, все споры рассматриваются в претензионном порядке. Срок рассмотрения претензии – три недели с даты получения претензии.

7.3. В случае если споры не урегулированы Сторонами путем переговоров и в претензионном порядке, то они передаются заинтересованной Стороной в Арбитражный суд _____.

8. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

8.1. Ни одна из Сторон не несет ответственности перед другой Стороной за неисполнение или ненадлежащее исполнение обязательств по настоящему Договору, обусловленное действием обстоятельств непреодолимой силы, то есть чрезвычайных и не предотвратимых обстоятельств, в том числе в условиях объявленной или фактической войны, гражданскими волнениями, эпидемиями, блокадами, эмбарго, пожарами, землетрясениями, наводнениями и другими природными стихийными бедствиями, а также изданием актов государственных органов.

8.2. Свидетельство, выданное торгово-промышленной палатой или иным компетентным органом, является достаточным подтверждением наличия и продолжительности действия обстоятельств непреодолимой силы.

8.3. Сторона, которая не исполняет свои обязательства вследствие действия обстоятельств непреодолимой силы, должна, по возможности, в трехдневный срок известить другую Сторону о таких обстоятельствах и их влиянии на исполнение обязательств по настоящему Договору.

8.4. Если обстоятельства непреодолимой силы действуют на протяжении 3 (трех) последовательных месяцев для обеих сторон, настоящий Договор может быть расторгнут по инициативе любой из сторон, при этом инициирующая сторона обязана произвести расчеты с другой стороной по фактически исполненному до наступления форс-мажорных обстоятельств после прекращения форс-мажорных обстоятельств.

9.АНТИКОРРУПЦИОННАЯ ОГОВОРКА

9.1. 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, а также не оказывают, не предлагают оказать и не разрешают оказание каких-либо услуг, прямо или косвенно, любым лицам для оказания влияния на действия или решения этих лиц с целью получения каких-либо неправомерных преимуществ или для достижения иных неправомерных целей.

9.2. 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 взятки, получение взятки, коммерческий подкуп, а также иные действия, нарушающие требования применимого законодательства Российской Федерации и международных правовых актов в сфере предупреждения и противодействия коррупции.

9.3. В случае возникновения у одной из Сторон подозрений, что произошло или могло произойти нарушение каких-либо положений пунктов 9.1, 9.2 настоящего Договора, эта Сторона обязуется уведомить о возникновении таких подозрений другую Сторону в письменной форме. В тексте уведомления Сторона обязана сослаться на известные ей факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений пунктов 9.1, 9.2 настоящего Договора другой Стороной, её аффилированными лицами, работниками или посредниками.

9.3.1.Каналы уведомления Лицензиата о нарушениях каких-либо положений пунктов 9.1,9.2 настоящего раздела:

- факс:(8182) 67-30-10;

- электронная почта: nuz-secretar@medrzd29.ru;

Каналы уведомления Лицензиара о нарушениях каких-либо положений пунктов 9.1,9.2 настоящего раздела: _____.

9.4. Сторона, получившая уведомление о нарушениях пунктов 9.1, 9.2 настоящего Договора, обязана рассмотреть такое уведомление и сообщить другой Стороне о результатах его рассмотрения в течение 10 (десяти) рабочих дней с даты получения письменного уведомления.

9.5. Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений пунктов 9.1, 9.2 настоящего Договора с соблюдением принципов конфиденциальности, а так же применение эффективных мер по предотвращению возможных конфликтных ситуаций. Стороны гарантируют отсутствие негативных последствий как для уведомившей Стороны в целом, так и для конкретных работников уведомившей Стороны, сообщивших о выявленных фактах нарушения положений пунктов 9.1, 9.2 настоящего Договора.

9.6. В случае подтверждения факта нарушения одной из Сторон положений пунктов 9.1, 9.2 настоящего Договора, другая Сторона имеет право расторгнуть настоящий Договор в одностороннем внесудебном порядке путём направления письменного уведомления не позднее, чем за 15 (пятнадцать) календарных дней до предполагаемой даты прекращения действия настоящего Договора.

9.7. В случае неполучения Стороной, направившей уведомление о нарушении положений пунктов 9.1, 9.2 настоящего Договора, информации о результатах рассмотрения такого уведомления в установленный пунктом 9.4 настоящего Договора срок, другая Сторона имеет право расторгнуть настоящий Договор в одностороннем внесудебном порядке путём направления письменного уведомления не позднее, чем за 1 (один) календарный месяц до предполагаемой даты прекращения действия настоящего Договора.

10. СРОК ДЕЙСТВИЯ ДОГОВОРА

10.1. Договор вступает в силу с момента его подписания и действует 24 месяца.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Во всем остальном, что не предусмотрено настоящим Договором, Стороны будут руководствоваться действующим законодательством Российской Федерации.

11.2. Любые изменения и дополнения к настоящему Договору действительны при условии, если они совершены в письменной форме и подписаны Сторонами или надлежаще уполномоченными на то представителями Сторон.

11.3. Стороны обязуются своевременно извещать друг друга об изменении своих реквизитов.

11.4 Все уведомления, сообщения, согласования в рамках исполнения настоящего Договора могут быть направлены другой стороне по электронному адресу, указанному в реквизитах настоящего договора. Документы, направляемые в отсканированном виде, содержащие печать и подпись стороны, в последующем должны быть направлены в оригинале по адресу указанному получателем в реквизитах договора. В любом из случаев, срок получения такого документа, письма, уведомления, начинает течь с момента направления электронного сообщения. Сторона, указавшая неверный электронный адрес или не указавшая его вообще, не вправе ссылаться на несвоевременное получение уведомления, сообщения и прочей письменной документации от другой стороны. В этом случае, уведомления, сообщения и прочая переписка будет считаться принятыми к исполнению другой стороной с даты отправления электронного письма.

11.5. Все уведомления и сообщения в рамках настоящего Договора должны направляться Сторонами друг другу в письменной форме.

11.6. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, из которых один находится у Лицензиара, второй - у Лицензиата.

11.7. К Договору прилагаются:

- Спецификация (Приложение № 1)
- Техническое задание (Приложение № 2)
- Акт приемки-передачи объекта интеллектуальной собственности на материальном

12. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

Лицензиат: НУЗ «Отделенческая больница на ст. Исакогорка ОАО «РЖД» Юридический адрес:163060, г. Архангельск, ул. Тимме, дом 5. Почтовый адрес: 163060, г. Архангельск, ул. Тимме, дом 5. Телефон: (8182) 67-30-10 ИНН 2901126556 КПП 290101001 ОГРН 1042900020239 р/сч 40703810810390000004 в Филиале № 7806 ВТБ (ПАО) г. Санкт-Петербург БИК 044030707 к/сч 30101810240300000707	**Лицензиар:** Юридический адрес: Почтовый адрес: Телефон: ИНН КПП ОГРН р/сч БИК к/сч
Главный врач _____/ О.А Савельева / E-mail: nuz-secretar@medrzd29.ru	_____/_____ / E-mail:

Приложение №1

к договору № от «___» _____ 201_г.

Спецификация

№ п/п	Наименование Товара/Страна происхождения	Ед. изм.	Кол-во	НДС,%. /НДС не облагается	Цена за ед. с НДС, руб.	Сумма НДС, руб.	Стоимость вкл. НДС, руб.
1							
ИТОГО:							

Итого по Спецификации - _____ (_____) *рублей* ___ *копеек, в том числе НДС* ___% - _____ (_____) *рублей* _____ *копеек /или НДС не облагается*

.

от Лицензиат

_____ /О.А. Савельева/

от Лицензиар

_____/_____/

Приложение № 2
к Договору № _____
от «___»_____2019 г.

Техническое задание

на оказание услуг по предоставлению неисключительных лицензионных прав на антивирусное программное обеспечение «Kaspersky Endpoint Security для бизнеса - Стандартный» (продление с расширением).

Поставляемое программное обеспечение должно быть включено в единый реестр российских программ для электронных вычислительных машин и баз данных в соответствии со статьей 12.1. Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации

п/п	Наименование товара	Основные характеристики товара
	Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition. 50-99 Node 2 year Renewal License	Описание объекта закупки: Kaspersky Endpoint Security для бизнеса - Стандартный - 50-99 Node 2 year Renewal License (KL4863RAQDR) Тип ключа: для бизнеса - Стандартный Количество лицензий:1 Количество защищаемых объектов в рамках лицензии:70 Срок подписки: Срок действия лицензии - 24 (Двадцать четыре) месяца с момента активации ключа доступа Место оказания услуг: Российская Федерация. г. Архангельск, ул. Тимме 5 Срок оказания услуг по предоставлению неисключительных лицензионных прав на антивирусное программное обеспечение «Kaspersky Endpoint Security для бизнеса - Стандартный»: в течение 5 (пяти) рабочих дней с момента подписания договора 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 Linux. Программные средства антивирусной защиты для файловых серверов Windows. Программные средства антивирусной защиты для файловых серверов Linux. Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных 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 языке. Все антивирусные средства, включая средства управления, должны обладать контекстной справочной системой на русском языке. Требования к программным средствам антивирусной защиты для рабочих станций Windows: Программные средства антивирусной защиты для рабочих станций Windows должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий: Microsoft Windows 7 Professional / Enterprise /Ultimate x86 / x64; Microsoft Windows 7 Professional / Enterprise /Ultimate SP1 и выше x86 / x64; Microsoft Windows 8 Professional /Enterprise x86 / x64; Microsoft Windows 8.1 Professional / Enterprise x86 / x64; Microsoft Windows 10 Pro / Enterprise x86 / x64; Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей: Антивирусное сканирование в режиме реального времени и по запросу. Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы. Антивирусное сканирование по расписанию. Запуск задач по расписанию и/или сразу после загрузки операционной системы. Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем. Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу. Защита электронной корреспонденции от вредоносных программ с проверкой входящего и исходящего трафика на следующих протоколах: IMAP, SMTP, POP3, MAPI, NNTP — независимо от используемого почтового клиента; Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP, в том числе с помощью эвристическогоанализа, с возможностью настройки доверенных сайтов. Блокировка баннеров и всплывающих окон, загружаемых с Web- страниц. Распознавание и блокировка фишинг-сайтов.

Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет пейджерами.
Возможность определения аномального поведения приложения с помощью анализа последовательности действий этого приложения. Возможность совершить
откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных вредоносными программами файлов.
Возможность ограничения привилегий исполняемых программ таких как запись в реестр, доступ к файлам и папкам.
Автоматическое определение уровней ограничения на основании репутации программы.
Наличие механизмов защиты от атак типа BadUSB.
Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов. Создание сетевых
правил для конкретных программ.
Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных
приложений при работе в вычислительных сетях любого типа, включая беспроводные.
Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме MD5 или SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory. Осуществление 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.
Осуществление контроля работы пользователя с сетью Интернет, в том числе явный запрет или разрешение доступа к ресурсам определенного характера, а также возможность блокировки определенного типа информации (аудио, видео и др.).
Программное средство должно позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory.
Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось. Запуск специальной задачи для
обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файловогопространства.
Защита от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая
избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.
Возможность установки только выбранных компонентов программного средства антивирусной защиты.
Полно дисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On. Обязательно наличие инструментов восстановления, зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС. Должна быть реализована поддержка UEFI- систем.
Поддержка двухфакторной аутентификации при полно дисковом 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 выбранныхприложений.
Шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети
организации. Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
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 Sierra 10.12
•Mac OS X 10.11 (El Capitan)
•Mac OS X 10.10 (Yosemite)
• Mac OS X 10.9 (Mavericks)
• Mac OS X 10.8 (Mountain Lion)
• Mac OS X 10.7 (Lion)
Программные средства антивирусной защиты для рабочих станций Mac должныобеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг.
Эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы. Антивирусное сканирование по команде пользователя или администратора и по расписанию.
Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
Централизованное управление всеми вышеуказанными
компонентами с помощью едином системы управления.
Облачная защита от новых угроз, позволяющая приложению в режиме реального времени

обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу.
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.
Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, HTTPS. Автоматическое обновление антивирусных баз по расписанию.
Защита информации, передаваемой через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик).
Требования к программным средствам антивирусной защиты для рабочих станций Linux:
Программные средства антивирусной защиты для рабочих станций Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
• Red Hat® Enterprise Linux® 6.7 x86/x64
• Red Hat® Enterprise Linux® 6.8 x86/x64
• Red Hat® Enterprise Linux® 7.2 x64
• Red Hat® Enterprise Linux® 7.3 x64
• CentOS-6.7 x86/x64
• CentOS-6.8 x86/x64
• CentOS-7.2 x64
• CentOS-7.3 x64
• SUSE® Linux Enterprise Desktop 12 x64
• openSUSE® 42.2 x64
• Debian GNU/Linux 7.10 x86/x64
• Debian GNU/Linux 7.11 x86/x64
• Debian GNU/Linux 8.6 x86/x64
• Debian GNU/Linux 8.7 x86/x64
• Ubuntu 10.04 LTS x86/x64
• Ubuntu 12.04 LTS x86/x64
• Ubuntu Server 14.04 LTS x86/x64
• Ubuntu Server 16.04 LTS x86/x64
• Ubuntu Server 16.10 LTS x86/x64
• OracleLinux 7.3 x64
Программные средства антивирусной защиты для рабочих станций Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг.
Проверка ресурсов доступных по SMB / NFS Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы.
Антивирусное сканирование по команде пользователя или администратора и по расписанию.
Антивирусная проверку и лечение файлов в архивах.
Запуск задач по расписанию и/или сразу после загрузки операционной системы.
Помещение подозрительных и поврежденных объектов на карантин.
Возможность экспортировать и сохранять отчеты в форматах HTML и CSV.
Возможность перехвата и проверки файловых операций на уровне SAMBA.
Гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства.
Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу.
Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он
представляет информационную ценность.
Возможность управления через пользовательский графический интерфейс.
Централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
Требования к программным средствам антивирусной защиты для файловых серверов Windows.
Программные средства антивирусной защиты для файловых серверов Windows должны функционировать на компьютерах, работающих под управлением
операционных систем следующих версий:
• Microsoft Windows Small Business Server 2011 Standard x64;
• Microsoft Windows Server 2008 Standard / Enterprise SP2 x86/x64;
• Microsoft Windows Server 2008 R2 Standard / Enterprise x64 SP1;
• Microsoft Windows Server 2012 Standard / Foundation x64;
• Microsoft Windows Server 2012 R2 Standard x64.
• Microsoft Windows Server 2016 x64.
Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:
Антивирусное сканирование в режиме реального времени и по запросу.
Антивирусное сканирование по команде пользователя или администратора и по расписанию.
Запуск задач по расписанию и/или сразу после загрузки операционной системы.
Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу.

Наличие встроенного сетевого экрана, позволяющего задавать сетевые пакетные правила для определенных протоколов (TCP, UDP) и портов.
Создание сетевых правил для конкретных программ.
Защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных
приложений при работе в вычислительных сетях любого типа, включая беспроводные.
Запуск специальной задачи для обнаружения уязвимостей в
приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
Антивирусная проверка и лечение файлов в
архивах форматов RAR, ARJ, ZIP, CAB в том числе и защищенных паролем.
Ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось.
Настройки проверки критических областей сервера в качестве отдельной задачи.
Регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать
антивирусное сканирование в фоновом режиме.
Наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий).
Защита от удаленного несанкционированного управления
сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей.
Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения как по пути нахождения программы, метаданным, контрольной сумме SHA256, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, а также обеспечивать возможность исключения из правил для определенных пользователей из Active Directory.
Централизованное управление всеми вышеуказанными
компонентами с помощью единой системы управления.
Требования к программным средствам антивирусной защиты для файловых серверов Linux:
Программные средства антивирусной защиты для файловых серверов Linux должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
• Red Hat® Enterprise Linux® 6.7 x86/x64
• Red Hat® Enterprise Linux® 6.8 x86/x64
• Red Hat® Enterprise Linux® 7.2 x64
• Red Hat® Enterprise Linux® 7.3 x64
• CentOS-6.7 x86/x64
• CentOS-6.8 x86/x64
• CentOS-7.2 x64
• CentOS-7.3 x64
• SUSE® Linux Enterprise Desktop 12 x64
• openSUSE® 42.2 x64
• Debian GNU/Linux 7.10 x86/x64
• Debian GNU/Linux 7.11 x86/x64
• Debian GNU/Linux 8.6 x86/x64
• Debian GNU/Linux 8.7 x86/x64
• Ubuntu 10.04 LTS x86/x64
• Ubuntu 12.04 LTS x86/x64
• Ubuntu Server 14.04 LTS x86/x64
• Ubuntu Server 16.04 LTS x86/x64
• Ubuntu Server 16.10 LTS x86/x64
• OracleLinux 7.3 x64
Программные средства антивирусной защиты для файловых серверов Linux должны обеспечивать реализацию следующих функциональных возможностей:
Резидентный антивирусный мониторинг.
Антивирусное сканирование по команде пользователя или администратора и по расписанию.
Проверка ресурсов доступных по SMB / NFS.
Антивирусная проверка и лечение файлов в архивах.
Запуск задач по расписанию и/или сразу после загрузки операционной системы.
Помещение подозрительных и поврежденных объектов на карантин.
Формирование отчетов в форматах HTML, CSV, PDF и XLS. Возможность перехвата и проверки файловых операций на уровне.
Сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он
представляет информационную ценность.
Удаленно через веб-браузер управлять антивирусом и настраивать его.
Централизованно управляться с помощью единой системы управления.
Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows:
Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны функционировать на компьютерах, работающих под

управлением операционных систем следующих версий:
• Microsoft Windows Server 2008
Standard/Enterprise/DataCenter/Core SP1 и выше x86/x64;
• Microsoft Windows Server 2008 R2 Core/ Standard/Enterprise/DataCenter SP1 и выше x64;
• Microsoft Windows Server 2012 Core/Standard/Essential/DataCenter/Foundation x64;
• Microsoft Windows Server 2012 R2 Core/Standard/Essential/DataCenter/Foundation x64;
• Microsoft Windows Server 2016 Core/Standard/Datacenter/Essentials x64;
• Microsoft Windows Storage Server 2008 R2 x64;
• Microsoft Windows Storage Server 2008 R2 SP2 Standard/Workgroup x64;
• Microsoft Windows Storage Server 2012 (все редакции) x64;
• Microsoft Windows Storage Server 2012 R2 (все редакции) x64;
• Microsoft Windows Storage Server 2016 x64;
• Microsoft Windows Hyper-V Server 2008 R2 SP1 x64;
• Microsoft Windows Hyper-V Server 2012 x64;
• Microsoft Windows Hyper-V Server 2012 R2 x64;
• Microsoft Windows Hyper-V Server 2016 x64.
Терминальные серверы:
• Microsoft Remote Desktop Services на базе Windows Server 2008;
• Microsoft Remote Desktop Services на базе Windows Server 2012;
• Microsoft Remote Desktop Services на базе Windows Server 2012 R2;
• Microsoft Remote Desktop Services на базе Windows Server 2012;
• Citrix XenApp 6.0/6.5/7.0/7.5 - 7.9;
• Citrix XenDeskTop 7.0/7.1/7.5/7.9.
Программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:
Осуществление антивирусной проверки на серверах, выполняющих разные функции: Серверов терминалов и принт- серверов; Серверов приложений и контроллеров доменов; Файловых серверов.
Возможность использования для защиты кластера серверов. Проверка следующих объектов защищаемого сервера при доступе к ним: Файлов при их записи и считывании;
Альтернативных потоков файловых систем (NTFS-streams); Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей.
Предотвращение вирусных эпидемий за счет фиксации возникновения вирусных атак.
Восстановление после заражения путем удаления всех связанных с ликвидированным вредоносным объектом записей в системных файлах и реестре ОС, что предотвращает возможные сбои в работе 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.
Контроль запуска исполняемых файлов, скриптов и пакетов MSI, а также DLL модулей и драйверов с возможностью запрета запуска недоверенных приложений.
Возможность автоматически сформировать набор правил запуска приложений на основании текущего набора ПО на одном сервере.
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.
Возможность блокировки доступа удаленного компьютера к сетевым ресурсам сервера.
Отслеживание попыток вредоносного шифрования файлов на общих сетевых папках сервера и блокирование компьютеров с которых идет такая активность.
Проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере.
Проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи.
Помещение подозрительных и поврежденных объектов на карантин.
Возможность восстановления файлов из карантина в сетевые папки.
При защите терминальных серверов поддержка режимов публикации рабочего стола и публикации приложений. Масштабируемость за счет задания количества рабочих процессов антивируса для ускорения обработки запросов к серверу при использовании многопроцессорных серверов.
Балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: антивирусная проверка может продолжаться в фоновом режиме.
Выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие). Наличие локальной консоли управления. Возможность подключения к другим средствам защиты для серверов масштаба предприятия с помощью локальной консоли.
Разделение прав администраторов, основанное на стандартных механизмах ОС Microsoft Windows.
Наличие встроенных исключений для стандартных ролей сервера (Контролер домена, Сервер БД и тд). Уведомления различными методами администраторов и пользователей о событиях в антивирусной защите. Поддержка Simple Network Management Protocol (SNMP).
Поддержка технологий ReFS(Resilient file system) и CSV (Cluster Shared Volume).

Централизованно управляться с помощью единой системы управления.
Требования к программным средствам антивирусной защиты мобильных устройств:
Программные средства для антивирусной защиты смартфонов должны функционировать под управлением следующих мобильных ОС:
• Android 4.0-7.1.1;
• Apple iOS 8.0— 10.0;
• Windows Phone 8.1, 10.
Решение должно централизованно управлять с помощью единой консоли управления.
Программные средства для антивирусной защиты смартфонов для ОС Android должны обеспечивать следующую функциональность:
Постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки на
репутационных облачных сервисам производителя антивирусных средств защиты.
Мгновенная проверка устанавливаемых приложений.
Проверка файловой системы устройства по требованию и по расписанию.
Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты.
Поддержка белых списков разрешенных сайтов.
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.
Возможность получения политик безопасности через Google Cloud Messaging.
Базовая поддержка Android for Work.
Наличие возможности создания специальной оболочки для мобильных программ с целью контроля действий программы, возможностью удаления данных и настроек
программы, добавления дополнительного пароля для старта приложения, в том числе с помощью учетных данных Active Directory .
Возможность заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства.
Указание параметров подключения к wi-fi сетям.
Наличие возможности указания обязательных к установке приложений.
Блокирование нежелательных SMS сообщений, возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset).
Постоянная проверка телефона на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета
запуска корпоративных приложений при выявлении несоответствий.
Возможность получения текущего номера SIM-карты телефона посредством СМС, возможность автоматической блокировки устройства при смене SIM-карты или при включении телефона без SIM-карты.
Поддержка технологий Samsung KNOX1 и KNOX2.
Программные средства для антивирусной защиты смартфонов для ОС Apple Ios должны обеспечивать следующую функциональность:
Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты.
Возможность определения местоположения устройства. Программные средства для антивирусной защиты смартфонов для ОС Windows Phone должны обеспечивать следующую функциональность:
Блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты.
Возможность определения местоположения устройства. Требования к программным средствам централизованного управления, мониторинга и обновления Программные средства централизованного управления, мониторинга и
обновления должны функционировать на компьютерах, работающих под управлением операционных систем следующих версий:
• Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 x86 / x64;
• Microsoft Windows 8 Professional / Enterprise x86 / x64;
• Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
• Microsoft Windows 10 Professional/Enterprise/Education x86 / x64;
• Microsoft Windows 10 RSI x86 /x64;
• Microsoft Windows 10 RS2 x86 / x64;
• Microsoft Windows Server 2008
Foundation/Standard/Enterprise/Datacenter SP1 x86 / x64;
• Microsoft Windows Server 2008;
• Microsoft Windows Server 2008 SP1 x86 / x64;
• Microsoft Windows Server 2008 R2 Core/Foundation/Standard/Enterprise/Datacenter x64;
• Microsoft Windows Server 2008 R2 Core/Foundation/Standard/Enterprise/Datacenter SP1 x64;
• Microsoft Windows Server 2012 Core/Foundation/Standard/Enterprise/Datacenter x64;
• Microsoft Windows Server 2012 R2

Core/Essentials/Foundation/Standard/Enterprise/Datacenterx64;
• Microsoft Windows Small Business Server 2008 Standard/Premium x64;
• Microsoft Windows Small Business Server 2011 Essentials/Premium/Standard x64.
Программные средства централизованного управления, мониторинга и обновления должны функционировать с СУБД следующих версий:
• Microsoft SQL Express 2008/2008R2/2012/2014;
• Microsoft SQL Server 2008/2008R2/2012/2014/2016;
• Microsoft Azure SQL Database;
• MySQL 5.5, 5.6, 5.7 x86/x64;
• MySQL Enterprise 5.5, 5.6, 5.7 x86/x64.
Программные средства централизованного управления, мониторинга и обновления должны функционировать на виртуальных платформах следующих версий:
• VMware Workstation 9.x, Workstation 10.x, 12x Pro;
• VMware vSphere 5.5, 6;
• Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1,2012, 20012 R2;
• Microsoft VirtualPC 2007(6.0.156.0);
• Parallels Desktop 7,11;
• Citrix XenServer 6.1, 6.2, 6.5, 7;
• Oracle VM VirtualBox 4.0.4-70112.
Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:
• Установка системы управления антивирусной защиты из единого дистрибутива.
• Выбор установки в зависимости от количества защищаемых узлов.
• Возможность чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации.
• Возможность поиска и обнаружения компьютеров в сети по IP- адресу, имени хоста, имени домена, маске подсети.
• Автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети. Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD.
• Централизованные установка, обновление и удаление программных средств антивирусной защиты. Централизованная настройка, администрирование, просмотр отчетов и статистической информации по их работе.
• 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.
• Возможность указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от УЗ, под которой пользователь вошел в систему, текущего ip-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности. Должна быть реализована возможность поддержки иерархии таких триггеров.
• Автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей.
• 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.
• Автоматическое развертывание по требованию специализированной системы защиты для виртуальных инфраструктур на базе VMware ESXi, Microsoft Hyper-V, Citrix XenServer.
• Построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне.
• 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.
• 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.
• Возможность подключения по RDP или штатными средствами из консоли управления. Пользователю должен выводиться запрос на разрешение дистанционного подключения.
• Наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них.
• 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 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
• Функция управления мобильными устройствами через сервер Exchange ActiveSync.
• Функция управления мобильными устройствами через сервер iOS MDM.
• Возможность отправки SMS-оповещений о заданных событиях.
• Централизованная установка приложений на управляемые мобильные устройства.
• Централизованная установка сертификатов на управляемые мобильные устройства.
• Возможность указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления.
• Возможность 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 как по событиям антивирусной защиты, так и по данным инвентаризации, лицензирования и тд.
• Наличие преднастроенных стандартных отчетов о работе системы.
• Экспорт отчетов в файлы форматов PDF и XML.
• Возможность передачи событий из базы данных в IBM Qradar и HP Arcsight или по Syslog (RFC 5424).
• 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 веб-консоли управления приложением.
• Наличие портала самообслуживания пользователей. Портал самообслуживания должен обеспечивать возможность подключения пользователей с целью: Установки агента управления на мобильное устройство, просмотр мобильных устройств, отправка команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя.
• Наличие системы контроля возникновения вирусных эпидемий. Требования к обновлению антивирусных баз
Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:
• Регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток.
• Множественность путей обновления, в том числе - по каналам связи и на отчуждаемых электронных носителях информации.
• Проверку целостности и подлинности обновлений средствами электронной цифровой подписи.
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.
Требования к качеству и безопасности:
Антивирусные программные средства должны быть включены в единый реестр российских программ для электронных вычислительных машин и баз данных.
При поставке пакетов безопасности Сублицензиату должны быть предоставлены:
лицензионное соглашение, определяющее условия использования Сублицензиатом программного обеспечения и подтверждающее права Сублицензиата на обновление и поддержку (гарантийное сопровождение);
-лицензионный ключ официального исполнения;
- комплект документации на русском языке.
- руководство пользователя (администратора).
Документация, поставляемая с антивирусными средствами, должна детально описывать процесс установки, настройки и эксплуатации соответствующего средства антивирусной защиты.
- регистрационная информация должна быть предоставлена в виде ключевого файла/авторизационного номера/кода активации, которая генерируется Правообладателями программного обеспечения персонально для лицензиата и необходима и достаточна для полнофункциональной работоспособности ПО, на материальном носителе или по согласованию с лицензиатом по сети Интернет на электронный почтовый адрес, указанный лицензиатом;
Применение эквивалента не допускается по причине необходимости обеспечения совместимости с имеющимся у лицензиата программным обеспечением.
Лицензиар должен являться авторизированным партнером правообладателя (Письмо /

		Сертификат) / Правообладателем. Объем и сроки предоставления гарантии качества услуги: Срок предоставления гарантии качества услуг — на весь период продления неисключительного права на использование и воспроизведение антивирусного программного обеспечения. Предоставление обновлений программного обеспечения (регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз антиспама не реже одного раза в 5 минут; множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации; предоставление технической возможности обновления баз сигнатур по мере выявления новых версий вредоносного программного кода); -предоставление обновления антивирусного программного обеспечения и сигнатур угроз в течение всего срока действия лицензии; - предоставление комплекта документации; предоставление консультаций лицензиату по вопросам инсталляции программного обеспечения, авторизации программного обеспечения, описанию основных функциональных возможностей программного обеспечения и области его применения, ответы на вопросы по описанию новых функций новых версий программного обеспечения; безвозмездное исправление по требованию лицензиата всех выявленных недостатков, если в процессе оказания услуги Лицензиар допустил отступление от условий контракта, ухудшившее качество услуг, в течение 5 календарных дней с момента вручения в письменном виде лицензиатом соответствующего требования Лицензиару. Техническая поддержка антивирусного программного обеспечения: - Должна предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет. - на веб-сайте производителя средств антивирусной защиты должны быть опубликованы: специальный раздел, посвящённый технической поддержке антивирусного программного обеспечения; пополняемая база знаний; форум пользователей программных продуктов. Гарантийные обязательства: Гарантийный срок на оказываемую Лицензиаром услугу (включая возможность ежедневного обновления баз данных сигнатур по средствам сети Интернет) составляет 12 (двенадцать) месяцев с момента активации ключа доступа . Требования к наличию сертификатов и лицензий: Антивирусное программное обеспечение должно иметь: • действующий на момент заключения договора сертификат соответствия ФСТЭК России, подтверждающий соответствие требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012, «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВЗ.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВЗ.В2.ПЗ» (ФСТЭК России, 2012) «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВЗ.Г2.ПЗ» (ФСТЭК России, 2012); • действующий на момент заключения договора сертификат соответствия ФСБ России, подтверждающий обеспечение безопасности информации при инсталляции и использовании программного изделия. Требования к гарантийным обязательствам: «Лицензиар» должен гарантировать, что программное обеспечение, на неисключительные права использования которого передаются лицензии в соответствии с настоящим Техническим заданием (далее - ПО), является полностью лицензионным, правомерно введено в гражданский оборот на территории Российской Федерации и обеспечивается технической поддержкой соответствующих правообладателей (производителей), а также, что предоставляемые в соответствии с данными лицензиями неисключительные права использования программного обеспечения не нарушают каких- либо авторских прав, неимущественных и/или имущественных прав любых третьих лиц. «Лицензиар» должен гарантировать бесперебойное функционирование программного обеспечения на автоматизированных рабочих местах «лицензиата». «Лицензиар» должен гарантировать то, что гарантийный период, в течение которого «Лицензиар» обязуется безвозмездно (за свой счет) исправлять ошибки в программном обеспечении, которые приводят к невозможности реализации (использования) «лицензиатом» каких-либо функций программного обеспечения, должен составлять не менее 24 месяцев

от Лицензиата

от Лицензиара

_____ /О.А. Савельева/

_____ /_____/

Приложение № 3

№ ___ от "__" _____ 20___ г.

АКТ ПРИЕМКИ-ПЕРЕДАЧИ
ОБЪЕКТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ
НА МАТЕРИАЛЬНОМ НОСИТЕЛЕ

г. Архангельск "__" _____ 20__ г.

_____, именуемое в дальнейшем **«Лицензиар»** в лице _____, действующего на основании _____ с одной стороны, и **Негосударственное учреждение здравоохранения «Отделенческая больница на станции Исакогорка открытого акционерного общества "Российские железные дороги" (НУЗ "Отделенческая больница на ст. Исакогорка ОАО "РЖД")**, именуемое в дальнейшем **«Лицензиат»**, в лице главного врача Савельевой Ольги Анатольевны, действующего на основании Устава, с другой стороны, вместе именуемые «Стороны»составили настоящий акт приемки-передачи объекта интеллектуальной собственности на материальном носителе (далее - Акт) к договору о предоставлении права использования программного обеспечения № ___ от "___" _____ 20__ г. (далее - Договор) о нижеследующем:

1.Лицензиар передает объект интеллектуальной собственности: программы _____на материальном носителе в электронном виде _____ в количестве_____ экземпляр, а Лицензиат принимает объект интеллектуальной собственности на материальном носителе.

2. Лицензиар передает Лицензиату исключительные права на объект интеллектуальной собственности: программы _____ _____ в объеме, указанном в пункте 2.5 Договора.

3. Индивидуальная характеристика объекта интеллектуальной собственности: программное обеспечение.

4. Материальный носитель объекта интеллектуальной собственности осмотрен Лицензиатом и принят в исправном состоянии.

5. Акт составлен в двух экземплярах, по одному для Правообладателя и Приобретателя.

от Лицензиат

_____ /О.А. Савельева/

от Лицензиар

_____ /_____/