Договор № 20072000002/58

**на оказание услуг по продлению Kaspersky Endpoint Security для бизнеса – Стандартный для ЧУЗ «РЖД-Медицина г. Калининград»**

г. Калининград «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

**Частное учреждение здравоохранения «Больница «РЖД-Медицина» города Калининград»**, именуемое в дальнейшем **«Заказчик»**, в лице Главного врача Сиглаевой Людмилы Михайловны, действующего на основании Устава, с одной стороны, и

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемое в дальнейшем **«Исполнитель»**, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, именуемые в дальнейшем «Стороны», заключили настоящий Договор о нижеследующем:

**Основание заключения договора**

Основанием для заключения настоящего договора является протокол рассмотрения и оценки заявок на участие в запросе котировок № 20072000002/58а от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2020 года комиссии по закупкам ЧУЗ «РЖД-Медицина» г. Калининград», согласно которому Поставщик признан победителем запроса котировок на **оказание услуг по продлению Kaspersky Endpoint Security для бизнеса – Стандартный для** ЧУЗ «РЖД-Медицина» г. Калининград»

# 1. Предмет договора

* 1. Заказчик поручает, а Исполнитель принимает на себя обязательства оказать **услуги по продлению Kaspersky Endpoint Security для бизнеса – Стандартный для ЧУЗ «РЖД-Медицина г. Калининград»** (в дальнейшем Услуги)в соответствии с Техническим заданием (Приложение №1) и предоставить результаты оказанных Услуг Заказчику, а Заказчик обязуется принять оказанные Услуги и оплатить их в порядке и на условиях, предусмотренных Договором.

1.2. Сроки оказания Услуг: согласно техническому заданию, с момента заключения договора и до полного исполнения Сторонами своих обязательств по договору.

1.3. Оказание Услуг осуществляется по адресам: Частное учреждение здравоохранения «Больница «РЖД-Медицина» города Калининград», г. Калининград, ул. Летняя, дом 1.

1.4. Качество оказанных Услуг и результат оказанных Услуг должны соответствовать Техническому заданию, а в части не установленной им, обязательным и обычно предъявляемым требованиям к работам соответствующего рода.

Заказчик вправе не оплачивать некачественно выполненные оказанные Услуги.

# 2. Сроки выполнения работ

2.1. Настоящий Договор вступает в силу с момента его заключения Сторонами и действует до полного исполнения Сторонами своих обязательств по настоящему Договору.

2.3. Сроки оказания Услуг могут быть изменены на основании дополнительного соглашения Сторон, оформленного в письменном виде и подписанного уполномоченными представителями обеих Сторон.

2.4. Заказчик вправе отказаться от оказания Услуг Исполнителем на любом этапе оказания Услуг.

# 3. Стоимость Услуг и порядок оплаты

3.1. Стоимость Услуг по настоящему Договору составляет: \_\_\_\_\_\_\_\_\_\_\_ руб. \_\_\_копеек (\_\_\_\_\_\_\_\_\_\_\_ рублей 00 коп.). В том числе НДС (\_\_%): \_\_\_\_\_\_\_\_\_\_\_руб. \_\_\_копеек (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_рублей \_\_\_\_ коп.).

В стоимость Услуг включены все накладные и плановые расходы и издержки Исполнителя, а также все налоги, пошлины и иные обязательные платежи.

3.2. Оплата Услуг производится Заказчиком путем перечисления денежных средств на расчетный счет Исполнителя, указанный в разделе 16 настоящего Договора, в следующем порядке:

в течение 30 банковских дней после подписания Сторонами акта сдачи-приемки оказанных Услуг, при условии отсутствия замечаний к качеству оказанных Услуг.

3.3. Заказчик считается исполнившим свои обязательства по уплате платежей в соответствии с настоящим Договором с момента списания денежных средств с расчетного счета Заказчика.

3.4. Настоящим Исполнитель подтверждает, что надлежащим образом изучил все условия оказания Услуг по настоящему Договору, и что никакие обстоятельства не могут повлиять на увеличение цены по настоящему Договору, если иное не будет согласовано Сторонами в дополнительных соглашениях к настоящему Договору. Стороны также согласовали, что у Сторон не возникает права на получение с другой Стороны процентов на сумму долга за период пользования денежными средствами.

3.5. По согласованию Сторон и в случае прекращения (расторжения) Договора между Сторонами проводится сверка расчетов с составлением акта сверки взаимных расчетов по форме, представленной Заказчиком.

# 4. Обеспечение материалами и оборудованием

# и риск случайной гибели

4.1. Оказание Услуг выполняется иждивением Исполнителя - из его материалов, его силами и средствами. Материалы должны соответствовать установленным в РФ обязательным требованиям качества и безопасности, быть допущенными для использования при оказании Услуг и обеспечивать надлежащее качество оказания Услуг.

4.2. Риск случайной гибели результата оказания Услуг, другого имущества, используемого для оказания Услуг, до окончательной приемки Заказчиком результатов оказания Услуг по настоящему Договору несет Исполнитель.

# 5. Обязательства сторон

**5.1. Заказчик вправе:**

5.1.1. Требовать от Исполнителя надлежащего и своевременного исполнения обязательств в соответствии с настоящим Договором, а также требовать своевременного устранения выявленных недостатков.

5.1.2. Требовать возмещения убытков в случае нарушения сроков оказания Услуг, а также в случае их некачественного выполнения.

5.1.3. Устранять, в том числе с привлечением третьих лиц, недостатки оказанной Услуги, если Исполнитель не приступил к устранению недостатков и/или не устранил их в указанный Заказчиком срок.

**5.2. Заказчик обязуется:**

5.2.1. Оказывать содействие Исполнителю в вопросах его взаимодействия с соответствующими структурными подразделениями Заказчика при оказании Услуг на условиях, предусмотренных Договором.

5.2.2. Предоставлять Поставщику заявки на Услуги в электронном виде посредством автоматизированной системы заказов «Электронный ордер»

5.2.3. Обеспечить доступ персонала Исполнителя к месту оказания Услуг.

5.2.4. Сообщать в письменной форме Исполнителю о недостатках, обнаруженных в ходе оказания Услуг, в течение 5 (Пяти) рабочих дней после обнаружения таких недостатков.

5.2.5. Своевременно принять и оплатить надлежащим образом оказанные Услуги в порядке и на условиях, предусмотренных Договором.

5.2.6. При получении от Исполнителя уведомления о приостановлении оказания Услуг в случае, указанном в п. 5.4.4 Договора, рассмотреть вопрос о целесообразности и порядке продолжения оказания Услуг.

**5.3. Исполнитель вправе:**

5.3.1. Требовать своевременного подписания Заказчиком акта сдачи-приемки оказанных Услуг по Договору.

5.3.2. Требовать своевременной оплаты оказанных Услуг в соответствии с условиями Договора.

5.3.3. Запрашивать у Заказчика разъяснения и уточнения относительно выполнения оказания Услуг в рамках Договора.

5.3.4. Предъявить Заказчику результаты оказания Услуг к приемке досрочно, уведомив Заказчика о готовности к сдаче оказанных Услуг письменно.

**5.4. Исполнитель обязуется:**

5.4.1. В установленные сроки и надлежащим образом оказать Услуги в количестве, указанном в заявке Заказчика, направленной посредством автоматизированной системы заказов « Электронный ордер» в срок, установленный настоящим договором и представить их результат Заказчику, в соответствии с условиями Договора.

5.4.3. Обеспечить устранение недостатков, выявленных при сдаче-приемке оказания Услуг, за свой счет в кратчайшие сроки, указанные в п.6.3 настоящего Договора.

5.4.4. Приостановить оказания Услуг в случае обнаружения независящих от Исполнителя обстоятельств, которые могут оказать негативное влияние на годность результатов оказание Услуг или создать невозможность их завершения в установленный Договором срок, и незамедлительно сообщить об этом Заказчику.

5.4.5. Исполнять иные обязательства, предусмотренные действующим законодательством Российской Федерации и Договором.

5.4.6. Не передавать любую информацию, касающуюся настоящего Договора, и не раскрывать сведения, полученные в процессе исполнения Договора, третьим лицам. В случае нарушения данного условия Заказчик вправе требовать от Исполнителя компенсации всех понесенных убытков.

5.4.7. Предоставлять информацию об изменениях в составе владельцев контрагента, включая конечных бенефициаров, и (или) в исполнительных органах контрагента не позднее, чем через 5 календарных дней после таких изменений.

5.4.8. При оказании Услуг, находясь по адресу, указанному в п.1.3 настоящего договора, соблюдать режим, установленный на объекте Заказчика, правила пожарной безопасности, правила безопасности проведения работ, санитарные нормы и правила.

# 6. Порядок сдачи и приемки работ

6.1. Не позднее 10 числа месяца, следующего за отчетным Исполнитель представляет Заказчику два подписанных со стороны Исполнителя экземпляра акта сдачи-приемки оказанных Услуг, счет на оплату, а также счет-фактуру, оформленную в соответствии с действующим законодательством Российской Федерации.

6.2. Не позднее 10 (Десяти) рабочих дней с момента получения от Исполнителя документов, указанных в п. 6.1 Договора, Заказчик осуществляет приемку оказанных Услуг и направляет Исполнителю подписанный обеими Сторонами экземпляр акта сдачи-приемки оказанных Услуг, либо мотивированный отказ от принятия оказанных Услуг.

6.3. В случае представления Заказчиком мотивированного отказа от принятия оказанных Услуг, Стороны в течение 5 (Пяти) рабочих дней составляют акт о выявленных недостатках, с указанием существа выявленных недоработок Исполнителя, а также сроков и порядка их устранения.

На основании акта о выявленных недостатках Исполнитель принимает на себя обязательство устранить имеющиеся недостатки за свой счет, в том числе и в случае, когда это потребует дополнительных издержек с его стороны, в кратчайшие сроки, но не более 5 рабочих дней с даты составления акта о выявленных недостатках.

6.4. В случае досрочного оказания Услуг по Договору Заказчик вправе досрочно принять и оплатить Услуги в соответствии с условиями Договора.

6.5. В случае не подписания Заказчиком Акта сдачи-приемки Услуг и непредставления официального мотивированного отказа в соответствии с пунктом 6.3 Договора, Акт сдачи-приемки Услуг считается утвержденным Заказчиком, а Услуги по данному Акту выполненными надлежащим образом и подлежащими оплате.

# 7. Антикоррупционная оговорка

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

При исполнении своих обязательств по настоящему Договору Стороны, их аффилированные лица, работники или посредники не осуществляют действия, квалифицируемые применимым для целей настоящего Договора законодательством как дача/получение взятки, коммерческий подкуп, а также иные действия, нарушающие требования применимого законодательства и международных актов о противодействии коррупции.

7.2. В случае возникновения у Стороны подозрений, что произошло или может произойти нарушение каких-либо положений пункта 7.1 настоящего раздела, соответствующая Сторона обязуется уведомить об этом другую Сторону в письменной форме. В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений пункта 7.1 настоящего раздела другой Стороной, ее аффилированными лицами, работниками или посредниками.

Каналы уведомления Исполнителя о нарушениях каких-либо положений пункта 7.1 настоящего раздела: тел. ( )\_\_\_\_\_\_\_\_\_\_\_, электронная почта \_\_\_\_\_\_\_\_.

Каналы уведомления Заказчика о нарушениях каких-либо положений пункта 7.1 настоящего раздела: факс:(4012)601353; электронная почта: RailwayHospital@mail.ru.

Сторона, получившая уведомление о нарушении каких-либо положений пункта 7.1 настоящего раздела, обязана рассмотреть уведомление и сообщить другой Стороне об итогах его рассмотрения в течение 10 (десяти) рабочих дней с даты получения письменного уведомления.

7.3. Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений пункта 7.1 настоящего раздела с соблюдением принципов конфиденциальности и 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 факте нарушений.

7.4. В случае подтверждения факта нарушения одной Стороной положений пункта 7.1 настоящего раздела и/или неполучения другой Стороной информации об итогах рассмотрения уведомления о нарушении в соответствии с пунктом 7.2 настоящего раздела, другая Сторона имеет право расторгнуть настоящий Договор в одностороннем внесудебном порядке путем направления письменного уведомления не позднее чем за 30 (тридцать) календарных дней до даты прекращения действия настоящего Договора.

# 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 непредотвратимых при данных условиях обстоятельств, в том числе объявленной или фактической войной, гражданскими волнениями, эпидемиями, блокадами, эмбарго, пожарами, землетрясениями, наводнениями и другими природными стихийными бедствиями, изданием актов органов государственной власти.

8.2. Свидетельство, выданное торгово-промышленной палатой или иной документ, выданный 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, не позднее, чем в трехдневный срок, известить другую Сторону в письменном виде о таких обстоятельствах и их влиянии на исполнение обязательств по настоящему Договору.

В случае неисполнения Стороной обязанности, предусмотренной в настоящем пункте, она лишается права ссылаться на обстоятельства непреодолимой силы как на обстоятельство, освобождающее ее от ответственности за ненадлежащее исполнение или неисполнение обязательств по настоящему Договору.

8.4. Действие обстоятельств непреодолимой силы продлевает срок выполнения обязательств по настоящему Договору на срок действия обстоятельств непреодолимой силы.

8.5. Если обстоятельства непреодолимой силы действуют на протяжении 3 (трех) последовательных месяцев, Договор может быть расторгнут по соглашению Сторон, либо в одностороннем порядке по инициативе заинтересованной Стороны.

# 9. Конфиденциальность

1. Настоящим Стороны устанавливают режим конфиденциальности информации (коммерческая тайна) в отношении всех условий настоящего Договора, порядка и факта его исполнения. Стороны обязуются не разглашать конфиденциальную информацию, полученную ими друг от друга или ставшую известной им в ходе выполнения работ по настоящему Договору, не открывать и не разглашать в общем или в частности информацию какой-либо третьей стороне без предварительного письменного согласия другой Стороны настоящего Договора.
2. Требования п.9.1. настоящего Договора не распространяются на случаи раскрытия конфиденциальной информации по запросу уполномоченных организаций в случаях, предусмотренных законодательством Российской Федерации. Однако даже в этом случае Стороны обязаны согласовать друг с другом объем и характер предоставляемой информации.
3. Исполнитель обязуется в течение срока действия настоящего Договора и в течение 5 (пяти) лет после его прекращения обеспечить охрану полученной от Заказчика информации конфиденциального характера и не использовать эту информацию для целей, не связанных с выполнением обязательств по настоящему Договору.
4. Исполнитель обязуется обеспечить, чтобы его работники и другие привлекаемые к оказанию Услуг третьи лица также не нарушали требования конфиденциальности.

9.5. Исполнитель обязуется не передавать оригиналы или копии документов, полученных от Заказчика в связи с настоящим Договором, третьим лицам без предварительного письменного согласия Заказчика.

9.6. Исполнитель обязуется обеспечивать безопасность персональных данных при их обработке.

# 10. Ответственность сторон

10.1. Исполнитель несет ответственность перед Заказчиком за действия привлекаемых им к оказанию Услуг третьих лиц как за собственные действия.

10.2. В случае нарушения сроков оказания Услуг, предусмотренных настоящим Договором и/или Календарным планом, сроков выполнения требования Заказчика, предъявленного в соответствии с пунктом 5.1 настоящего Договора, Заказчик имеет право требовать у Исполнителя уплаты пени в размере 0,1% от стоимости Услуг, указанной в п. 3.1 настоящего Договора за каждый день просрочки.

10.3. В случае ненадлежащего выполнения Исполнителем условий настоящего Договора, несоответствия оказания Услуг обусловленным Сторонами требованиям, Заказчик имеет право требовать у Исполнителя уплаты штрафа в размере 1% от стоимости Услуг, указанной в п. 3.1 настоящего Договора.

В случае возникновения при этом у Заказчика каких-либо убытков Исполнитель возмещает такие убытки Заказчику в полном объеме на основании предоставленных Заказчиком документов, доказывающих факт возникновения и размер понесенных убытков.

10.4. Перечисленные в настоящем Договоре штрафные санкции могут быть взысканы Заказчиком путем удержания причитающихся сумм при оплате счетов Исполнителя. Если Заказчик не удержит по какой-либо причине сумму штрафных санкций, Исполнитель обязуется уплатить такую сумму по первому письменному требованию Заказчика.

Для целей расчета неустойки по настоящему Договору Стороны применяют цену Услуг в том размере, в котором такая цена оплачена или подлежит оплате по настоящему Договору с учетом НДС (если Исполнитель является плательщиком НДС).

10.5. В случаях, не предусмотренных настоящим Договором, за неисполнение или ненадлежащее исполнение своих обязательств по настоящему Договору Стороны несут ответственность в соответствии с законодательством Российской Федерации.

10.6. Уплата Исполнителем неустойки и возмещение убытков не освобождают Исполнителя от выполнения обязательств в натуре по настоящему Договору.

10.7. Обязательство по выплате неустойки у виновной Стороны наступает после получения от потерпевшей Стороны соответствующего письменного требования. Срок удовлетворения такого требования – 10 (десять) рабочих дней с даты его получения виновной Стороной.

# 11. Порядок внесения изменений, дополнений в Договор и его расторжение

11.1. В настоящий Договор могут быть внесены изменения и дополнения, которые оформляются Сторонами дополнительными соглашениями к настоящему Договору.

11.2. Стороны вправе расторгнуть настоящий Договор (отказаться от исполнения настоящего Договора) по основаниям, в порядке и с применением последствий, предусмотренных настоящим Договором и законодательством Российской Федерации. При этом Заказчик вправе в любое время расторгнуть настоящий Договор в одностороннем внесудебном порядке.

11.3. Расторжение настоящего Договора в одностороннем порядке (отказ от исполнения настоящего Договора) осуществляется путем направления одной Стороной письменного уведомления об этом другой Стороне не позднее, чем за 30 (тридцать) календарных дней до даты расторжения настоящего Договора. Настоящий Договор считается расторгнутым (прекращенным) с даты, указанной в уведомлении о расторжении настоящего Договора.

11.4. В случае расторжения настоящего Договора (отказа от исполнения настоящего Договора) по инициативе Заказчика, за исключением случаев, предусмотренных пунктом 11.5 настоящего Договора, или по причинам, за которые ни одна из Сторон не отвечает, оплате подлежат обоснованные, необходимые, фактически понесенные, документально подтвержденные Исполнителем расходы до даты получения Исполнителем уведомления о расторжении настоящего Договора или подписания соглашения о расторжении настоящего Договора.

11.5. В случае расторжения настоящего Договора (отказа от исполнения настоящего Договора) по причинам, связанным с ненадлежащим выполнением Исполнителем условий настоящего Договора, несоответствием результатов Услуг требованиям настоящего Договора, Исполнитель не вправе требовать оплаты, а также обязан вернуть полученные по настоящему Договору денежные средства и возместить доказанные фактические убытки Заказчика в течение 7 (семи) календарных дней с даты предъявления Заказчиком соответствующего требования.

11.6. Договор может быть расторгнут в случае неисполнения Исполнителем требования, предусмотренного пунктом 5.4.7. настоящего Договора.

# 12. Разрешение споров

12.1. 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.

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

12.3. Стороны установили обязательный досудебный порядок урегулирования споров, вытекающих из невыполнения (ненадлежащего выполнения) условий настоящего Договора, путем направления претензии.

12.4. Претензия составляется одной из Сторон в письменной форме, подписывается уполномоченным на то должностным лицом, с печатью организации и направляется в адрес второй Стороны ценным заказным письмом с описью вложения и уведомлением о вручении.

12.5. Срок рассмотрения претензии составляет один месяц со дня ее получения. Ответ на претензию направляется ценным заказным письмом с описью вложенных в конверт документов и уведомлением о вручении.

12.6. В случае отсутствия информации о получении Стороной-адресатом направленной ей корреспонденции по урегулированию споров и претензий в досудебном порядке, любая корреспонденция считается полученной Стороной-адресатом через 15 рабочих дней с даты ее направления по адресу, указанному Стороной-адресатом в разделе 16 настоящего Договора.

12.7. Все споры и разногласия между Сторонами, которые могут возникнуть по настоящему Договору, если они не будут разрешены путем переговоров, решаются в Арбитражном суде Калининградской области.

# 13. Права на результаты работ и переход рисков

13.1 Риск случайной гибели или повреждения результата Услуг Исполнителя переходит к Заказчику с момента подписания Сторонами Акта сдачи-приемки Услуг. До подписания Сторонами указанного Акта риск случайной гибели или повреждения результата работ несет Исполнитель.

# 14. Прочие условия

14.1. Заказчик приобретает право собственности на результат оказанных Услуг с момента подписания Акта сдачи-приемки Услуг. Разработанная документация может быть использована Заказчиком только в отношении тех объектов, для которых она (документация) разрабатывалась.

14.2. Все вопросы, не урегулированные настоящим Договором, регламентируются нормами действующего гражданского законодательства Российской Федерации.

14.3. Все изменения и дополнения к настоящему Договору считаются действительными, если они оформлены в виде дополнительных соглашений к Договору и подписаны обеими Сторонами.

14.4. Все уведомления, сообщения, согласования в рамках исполнения настоящего Договора могут быть направлены другой Стороне по электронному адресу, указанному в реквизитах настоящего Договора, или предусмотренные по тексту 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. Сторона, указавшая неверный электронный адрес или не указавшая его вовсе, не вправе ссылаться на несвоевременное получение уведомления, сообщения и прочей письменной документации от другой Стороны. В этом случае уведомления, сообщения и прочая переписка будут считаться принятыми к исполнению другой Стороной с даты отправки электронного письма или, если не указан электронный адрес, с даты, установленной отправителем письма/ уведомления, направленного иным способом.

**15. Налоговая оговорка.**

15.1 Поставщик гарантирует, что:

зарегистрирован в ЕГРЮЛ надлежащим образом;

его исполнительный орган находится и осуществляет функции управления по месту регистрации юридического лица, и в нем нет дисквалифицированных лиц;

располагает персоналом, имуществом и материальными ресурсами, необходимыми для выполнения своих обязательств по договору, а в случае привлечения подрядных организаций (соисполнителей) принимает все меры должной осмотрительности, чтобы подрядные организации (соисполнители) соответствовали данному требованию;

располагает лицензиями, необходимыми для осуществления деятельности и исполнения обязательств по договору, если осуществляемая по договору деятельность является лицензируемой;

является членом саморегулируемой организации, если осуществляемая по договору деятельность требует членства в саморегулируемой организации;

ведет бухгалтерский учет и составляет бухгалтерскую отчетность в соответствии с законодательством Российской Федерации и нормативными правовыми актами по бухгалтерскому учету, представляет годовую бухгалтерскую отчетность в налоговый орган;

ведет налоговый учет и составляет налоговую отчетность в соответствии с законодательством Российской Федерации, субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления, своевременно и в полном объеме представляет налоговую отчетность в налоговые органы;

не допускает искажения сведений о фактах хозяйственной жизни (совокупности таких фактов) и объектах налогообложения в первичных документах, бухгалтерском и налоговом учете, в бухгалтерской и налоговой отчетности, а также не отражает в бухгалтерском и налоговом учете, в бухгалтерской и налоговой отчетности факты хозяйственной жизни выборочно, игнорируя те из них, которые непосредственно не связаны с получением налоговой выгоды;

своевременно и в полном объеме уплачивает налоги, сборы и страховые взносы;

отражает в налоговой отчетности по НДС все суммы НДС, предъявленные Заказчику (Покупателю) – данный абзац исключается в случае освобождения от уплаты НДС при заключении договора;

лица, подписывающие от его имени первичные документы и счета-фактуры, имеют на это все необходимые полномочия и доверенности.

15.2. Если Поставщик нарушит гарантии (любую одну, несколько или все вместе), указанные в пункте 1 настоящего раздела, и это повлечет:

предъявление налоговыми органами требований к Заказчику (Покупателю) об уплате налогов, сборов, страховых взносов, штрафов, пеней, отказ в возможности признать расходы для целей налогообложения прибыли или включить НДС в состав налоговых вычетов и(или)

предъявление третьими лицами, купившими у Заказчика Услуги, имущественные права, являющиеся предметом настоящего договора, требований к Заказчику о возмещении убытков в виде начисленных по решению налогового органа налогов, сборов, страховых взносов, пеней, штрафов, а также возникших из-за отказа в возможности признать расходы для целей налогообложения прибыли или включить НДС в состав налоговых вычетов, то Поставщик обязуется возместить Заказчику убытки, который последний понес вследствие таких нарушений.

15.3.  Поставщик в соответствии со ст. 406.1. Гражданского кодекса Российской Федерации, возмещает Заказчику все убытки последнего, возникшие в случаях, указанных в пункте 2 настоящего раздела. При этом факт оспаривания или не оспаривания налоговых доначислений в налоговом органе, в том числе вышестоящем, или в суде, а также факт оспаривания или не оспаривания в суде претензий третьих лиц не влияет на обязанность Поставщика возместить имущественные потери.

# 16. Перечень приложений

16.1. К настоящему Договору прилагаются и являются его неотъемлемой частью:

1. Приложение №1 – Техническое задание.

**17. Адреса и платёжные реквизиты Сторон**

|  |  |
| --- | --- |
| **Покупатель:****Частное учреждение здравоохранения «Больница «РЖД-Медицина» города Калининград»**ОГРН 1043900824604, ИНН3908029088, КПП 390601001,ОКПО 73707902, местонахождение 236005, Калининградская область, город Калининград, улица Летняя, д.1р/с: 40703810220380004163 в Филиале №7806 банка ВТБ (публичное акционерное общество) в г. Санкт-Петербурге (Филиал №7806 Банка ВТБ (ПАО)), к/с 30101810240300000707, БИК 044030707Тел/Факс: 8 (4012) 60-13-53, 60-19-50Еmail: RailwayHospital@mail.ru | **Поставщик:** |
| Главный врач\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Сиглаева Л.М./ |  |

Приложение № 1

к Договору № 20072000002/58

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_г.

Техническое задание

**по продлению Kaspersky Endpoint Security для бизнеса – Стандартный для**

1. **Наименование и описание объекта закупки (функциональные, технические и качественные характеристики, эксплуатационные характеристики объекта закупки), объем и условия оказания услуг, требования к качеству услуг:**

 **1.1. Наименование объекта закупки:** оказание услуг по продлению лицензии Kaspersky Endpoint Security для бизнеса – Стандартный

 **1.2. Описание услуг, объем и условия оказания услуг, требования к качеству услуг:**

|  |  |
| --- | --- |
| **Наименование**  | Продление лицензии пользователя (передача неисключительных прав на использование программ для ЭВМ) ЧУЗ "РЖД-МЕДИЦИНА" Г. КАЛИНИНГРАД"№26FE-180910-144526-7-1559, лицензия на 2 года, программное обеспечение Kaspersky Endpoint Security для бизнеса – Стандартный 50-99 NodeRenewal 2 yearKL4863RAQDR \* |
| **Количество закупаемых товаров, объем работ, услуг** | Лицензия на 70 рабочих места |
| **Место поставки** | 236005, КАЛИНИНГРАДСКАЯ ОБЛ, КАЛИНИНГРАД Г, ЛЕТНЯЯ УЛ, 1 |
| **Срок (периодичность) передачи неисключительных лицензионных прав** | Поставщик передает неисключительные лицензионные права Заказчику в срок не позднее 30 (тридцати) календарных дней в полном объеме с момента заключения государственного контракта. |
| **Условия поставки товара** | Датой передачи неисключительных лицензионных прав, считается дата подписания Акта приема передачи неисключительных прав, **без претензий**. |
| **Требования по объему и сроку гарантий качества товаров** | Поставщик гарантирует работу ключа на программный продукт в течение 24 месяцев при соблюдении условий лицензионного соглашения. Гарантийные обязательства вступают в силу с момента приема передачи неисключительных прав заказчику. |

\* данное программное обеспечение (далее ПО) не сопровождается словами «или эквивалент», так как необходимо обеспечить взаимодействие указанного ПО с базами данных и другим ПО, которые используются Заказчиком.

**1.3. Технические требования к системе антивирусной защиты: KasperskyEndpointSecurity для бизнеса – Стандартный**

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

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

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

# Требования к программным средствам антивирусной защиты для рабочих станций Windows

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

* Windows 7 Home / Professional / Enterprise (32 / 64-разрядная);
* Windows 8 Professional / Enterprise (32 / 64-разрядная);
* Windows 8.1 Professional / Enterprise (32 / 64-разрядная);
* Windows 10 Home / Pro / Education / Enterprise (32 / 64-разрядная).

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

* антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
* фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
* проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
* блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
* распознавания и блокировку фишинговых и небезопасных сайтов;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
* возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (ActiveDirectory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из ActiveDirectory;
* возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (ActiveDirectory или локальных пользователей/групп), в рамках контроля устройств;
* записи в журнал событий о записи и/или удалении файлов на съемных дисках;
* контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из ActiveDirectory;
* защиты от атак типа BadUSB;
* запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после запуска приложения;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* возможность проверки целостности антивирусной программы;
* возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;
* возможностьинтеграциис Windows Defender Security Center;
* наличиеподдержки Antimalware Scan Interface (AMSI);
* наличиеподдержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.

# Требования к программным средствам антивирусной защиты для серверов Windows

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

* Windows Small Business Server 2008 Standard / Premium (64-разрядная);
* Windows Small Business Server 2011 Essentials / Standard (64-разрядная);
* Windows MultiPoint Server 2011 (64-разрядная);
* Windows Server 2008 Standard / Enterprise Service Pack 2 (64-разрядная);
* Windows Server 2008 R2 Foundation / Standard / Enterprise Service Pack 1 (64-разрядная);
* Windows Server 2012 Foundation / Essentials / Standard (64-разрядная);
* Windows Server 2012 R2 Foundation / Essentials / Standard (64-разрядная);
* WindowsServer 2016 (64-разрядная) (с ограничениями);
* WindowsServer 2019 (64-разрядная) (с ограничениями).

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

* антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (ActiveDirectory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* возможность проверки целостности антивирусной программы;
* возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;
* возможностьинтеграциис Windows Defender Security Center;
* наличиеподдержки Antimalware Scan Interface (AMSI);
* наличиеподдержки Windows Subsystem for Linux (WSL);
* возможность защитить паролем восстановление объектов из резервного хранилища.

# 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 Catalina 10.15;
* macOSMojave 10.14;
* macOSHighSierra 10.13;
* macOSSierra 10.12.

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

* резидентный антивирусный мониторинг;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* автоматическое обновление антивирусных баз по расписанию;
* резервное копирование зараженных файлов перед их удалением, для возможности восстановления;
* эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
* защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* проверку сетевого трафика, передаваемого через браузеры Safari, GoogleChrome и Firefox (HTTP и HTTPS трафик);
* контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

# Требования к программным средствам антивирусной защиты для рабочих станций Linux

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

* Ubuntu 16.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 и выше;
* Debian GNU / Linux 8.6- 8.х;
* Debian GNU / Linux 9.4 – 9.х;
* LinuxMint 18.2 – 18.х;
* LinuxMint 19 (последняя версия);
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* Лотос;
* Гослинукс 6.6.

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

* Ubuntu 16.04 LTS;
* Ubuntu 18.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 – 6.х;
* CentOS 7.2 – 7.х;
* Debian GNU / Linux 8.6- 8.х;
* Debian GNU / Linux 9.4 – 9.х;
* OracleLinux 7.3 и выше;
* SUSE LinuxEnterpriseServer 15;
* openSUSE 15;
* Альт Линукс СПТ 7.0.6 ;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* AmazonLinux AMI;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Micro Focus Open Enterprise Server 2018;
* AstraLinuxSpecialEdition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* AstraLinuxSpecialEdition 1.6 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* Циркон 36КТ;
* Циркон 36СТ;
* ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* ЕМИАС 1.0;
* Гослинукс 6.6;
* Лотос;
* РЕД ОС 7.2.

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

* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plaintext);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* помещение подозрительных и поврежденных объектов на карантин;
* проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов;
* возможность перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* возможность управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

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

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

**32-разрядных операционных систем Microsoft Windows**

* Windows Server® 2003 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter спакетомобновлений SP2 иливыше;
* Windows Server 2008 Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше;
* Windows Server 2008 Core / Standard / Enterprise / Datacenter спакетомобновлений SP1 иливыше.

**64-разрядныхоперационныхсистем Microsoft Windows**

* Windows Server 2003 Standard / Enterprise / Datacenter с пакетомобновлений SP2 иливыше;
* Windows Server 2003 R2 Standard / Enterprise / Datacenter с пакетомобновлений SP2 иливыше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Windows Server 2008 Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Microsoft Small Business Server 2008 Standard / Premium;
* Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* Windows Server 2008 Core Standard / Enterprise / Datacenter с пакетомобновлений SP1 иливыше;
* WindowsHyper-VServer 2008 R2 с пакетом обновлений SP1 или выше;
* Microsoft Small Business Server 2011 Essentials / Standard;
* Microsoft Windows MultiPoint™ Server 2011 Standard / Premium;
* Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 Core Foundation / Essentials / Standard / Datacenter;
* Microsoft Windows MultiPoint Server 2012 Standard / Premium;
* Windows Storage Server 2012;
* Windows Hyper-V Server 2012;
* Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
* Windows Server 2012 R2 Core Foundation / Essentials / Standard / Datacenter;
* Windows Storage Server 2012 R2;
* Windows Hyper-V Server 2012 R2;
* Windows Server 2016 Essentials / Standard / Datacenter;
* Windows Server 2016 MultiPoint;
* Windows Server 2016 Core Standard / Datacenter;
* Microsoft Windows MultiPoint Server 2016;
* Windows Storage Server 2016;
* Windows Hyper-V Server 2016;
* Windows Server 2019 Essentials / Standard / Datacenter;
* Windows Server 2019 Core;
* Windows Storage Server 2019;
* Windows Hyper-V Server 2019.

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

* антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
* защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
* непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft WindowsScriptTechnologies (или ActiveScripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
* анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* возможность проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* возможность добавлять процессы в список защищаемых;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
* настройки проверки критических областей сервера в качестве отдельной задачи;
* регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
* 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);
* ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
* возможность интеграции с SIEM системами;
* возможность указания количества рабочих процессов антивируса вручную;
* возможность отключить графический интерфейс;
* наличие удаленной и локальной консоли управления;
* управления параметрами антивируса из командной строки;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил.

**Требования к программным средствам антивирусной защиты для файловых серверов Linux**

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

* Ubuntu 16.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 и выше;
* Debian GNU / Linux 8.6 – 8.х;
* Debian GNU / Linux 9.4 - 9.х;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* Лотос;
* Гослинукс 6.6.

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

* Ubuntu 16.04 LTS;
* Ubuntu 18.04 LTS;
* Red Hat Enterprise Linux 6.7 – 6.х;
* Red Hat Enterprise Linux 7.2 – 7.х;
* CentOS 6.7 – 6.х;
* CentOS 7.2 – 7.х;
* Debian GNU / Linux 8.6 – 8.х;
* Debian GNU / Linux 9.4 - 9.х;
* OracleLinux 7.3 и выше;
* SUSE LinuxEnterpriseServer 15;
* openSUSE 15;
* Альт Линукс СПТ 7.0.6;
* Альт Линукс СПТ 8.0.0 Рабочая станция;
* Альт Линукс СПТ 8.0.0 Сервер;
* Альт Линукс 8.2 Рабочая станция;
* Альт Линукс 8.2 Рабочая станция К;
* Альт Линукс 8.2 Сервер;
* Альт Линукс 8.2 Образование;
* AmazonLinux AMI;
* LinuxMint 18.2 и выше;
* LinuxMint 19 (последняя версия);
* Micro Focus Open Enterprise Server 2018;
* AstraLinuxSpecialEdition 1.5 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* AstraLinuxSpecialEdition 1.6 (должна быть поддержка работы в обычном режиме и в режиме замкнутой программной среды);
* Циркон 36КТ;
* Циркон 36СТ;
* ОС РОСА «КОБАЛЬТ» 7.3 для клиентских систем;
* ОС РОСА «КОБАЛЬТ» 7.3 для серверных систем;
* ЕМИАС 1.0;
* Гослинукс 6.6;
* Лотос;
* РЕД ОС 7.2.

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

* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;.tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plaintext);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* помещение подозрительных и поврежденных объектов на карантин;
* проверку почтовых баз приложений Microsoft Outlook
* возможность перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* возможность экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию;
* возможность управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами 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 4.4– 10.0;
* AppleiOS 10.0 – 12.

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

* постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
* проверка файловой системы устройства по требованию и по расписанию;
* мгновенная проверка устанавливаемых приложений
* 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, в рамках контроля запуска приложений;
* возможность отправки команд и push уведомлений через сервис FirebaseCloudMessaging (FCM);
* базовая поддержка AndroidforWork;
* возможность заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
* возможность указать параметры подключения к wi-fi сетям;
* возможность указать обязательные к установке приложения;
* возможность блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factoryreset);
* возможность создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
* поддержка технологий Samsung KNOX1 и KNOX2.

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

* возможность удаленной настройки параметров iOSMDM-устройств с помощью групповых политик;
* возможность отправки команды блокирования и удаления данных;
* возможность создавать групповые политики безопасности мобильных устройств;
* удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу ExchangeActiveSync\ iOSMDM;
* получать отчеты и статистику о работе мобильных устройств пользователей;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervisedmode;
* возможность централизованного управления с помощью единой консоли управления.

# 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 32-разрядная / 64-разрядная;
* Microsoft Windows 8 32 разрядная / 64-разрядная;
* Microsoft Windows 8;1 32-разрядная / 64-разрядная;
* Microsoft Windows 10 32-разрядная / 64-разрядная;
* Windows Server 2008, 2008 R232-разрядная / 64-разрядная;
* Windows Server 2012, 2012 R264-разрядная;
* Windows Server 2016 64-разрядная;
* WindowsServer 2019 Standard, Datacenter.

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

* VMware vSphere 5.5, 6;
* VMware Workstation 12.x Pro;
* Microsoft Hyper-V Server 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;
* Microsoft Virtual PC 2007 (6.0.156.0);
* Citrix XenServer 6.2, 6.5, 7;
* Parallels Desktop 11 для Mac;
* OracleVMVirtualBox 4.0.4-70112 (поддерживаются гостевые операционные системы Windows).

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

* Microsoft SQL Server 2008 Express 32-разрядная;
* Microsoft SQL 2008 R2 Express 64-разрядная;
* Microsoft SQL 2012 Express, 2014 Express 64-разрядная;
* MicrosoftSQLServer 2008 (все редакции) 32-разрядная / 64-разрядная;
* MicrosoftSQLServer 2008 R2 (все редакции) 64-разрядная;
* Microsoft SQL Server 2008 R2 Service Pack 2 64-разрядная;
* MicrosoftSQLServer 2012 (все редакции) 64-разрядная;
* MicrosoftSQLServer 2014 (все редакции) 64-разрядная;
* MicrosoftSQLServer 2016 (все редакции) 64-разрядная;
* Microsoft SQL Server 2017 (для Windows) 64-разрядная;
* Microsoft Azure SQL Database;
* MySQL 5.5 32-разрядная / 64-разрядная (не поддерживаются версии MySQL 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5);
* MySQL Enterprise 5.5 32-разрядная / 64-разрядная;
* MySQL 5.6 32-разрядная / 64-разрядная;
* MySQL Enterprise 5.6 32-разрядная / 64-разрядная;
* MySQL 5.7 32-разрядная / 64-разрядная;
* MySQLEnterprise 5.7 32-разрядная / 64-разрядная.

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

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

# Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

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

# Требования к эксплуатационной документации

Эксплуатационная документация для всех программных продуктов антивирусной защиты, включая средства управления, должна включать документы, подготовленные в соответствии с требованиями государственных стандартов, на русском языке, в том числе «Руководство пользователя (администратора)».

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

# Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

• Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнеров на всей территории Российской Федерации по телефону, электронной почте и через Интернет.

• Web-сайт производителя антивирусного решения должен быть на русском языке, иметь специальный раздел, посвящённый технической поддержке антивирусного решения, пополняемую базу знаний, а также форум пользователей программных продуктов.

|  |
| --- |
|  |

|  |  |  |
| --- | --- | --- |
| **От Заказчика** |  | **От Исполнителя** |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_/ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_/ |

Приложение № 2

к Договору № 20072000002/57

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г.

Спецификация

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование услуги:  | Техническое описание  | Ед. изм. | Кол-во | Цена за ед, руб. | Сумма, руб. |
| 1 |  |  |  |  |  |  |
| Итого: |  |

Стоимость Услуг составляет - \_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_ копеек, в том числе НДС \_\_\_% - \_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) рублей \_\_\_\_\_ копеек /или НДС не облагается

|  |  |  |
| --- | --- | --- |
| **От Заказчика** |  | **От Исполнителя** |
|  |  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_/ |  | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_/ |