1. **ПРОЕКТ КОНТРАКТА**

**ГОСУДАРСТВЕННЫЙ КОНТРАКТ №** \_\_\_\_\_

Оказание услуг по предоставлению лицензий на право использовать компьютерное программное обеспечение Kaspersky Endpoint Security для бизнеса Стандартный для нужд Управления архивами Свердловской области

(ИКЗ 242666100190366700100100070015829244)

г. Екатеринбург «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2024 г.

Управление архивами Свердловской области, именуемое в дальнейшем «Заказчик», в лице Начальника Управления архивами Свердловской области Тараборина Романа Сергеевича, действующего на основании Положения, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуемый в дальнейшем «Исполнитель», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (*ИНН \_\_\_\_)*, действующего на основании \_\_\_\_\_\_\_\_\_\_, вместе именуемые «Стороны», в соответствии с Федеральным законом от 5 апреля 2013 года № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Закон о контрактной системе) и действующим законодательством Российской Федерации и по результатам проведения аукциона в электронной форме на основании (протокол от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 года)статьи 51 Закона о контрактной системе заключили настоящий государственный контракт, именуемый в дальнейшем «контракт», о нижеследующем:

1. ПРЕДМЕТ КОНТРАКТА

1.1. Исполнитель обязуется оказать услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение Kaspersky Endpoint Security для бизнеса Стандартный для нужд Управления архивами Свердловской области (далее – Услуги), в соответствии с Описанием объекта закупки (Приложение № 1), а Заказчик обязуется принять и оплатить Услуги в установленном контрактом порядке, форме и размере.

1.2. Программное обеспечение Kaspersky Endpoint Security для бизнеса – Стандартный, включено в Единый реестр российских программ для электронных вычислительных машин и баз данных:

Название: Kaspersky Endpoint Security для бизнеса Стандартный;

Сведения о правообладателях программного обеспечения: российская коммерческая организация;

Название организации: АКЦИОНЕРНОЕ ОБЩЕСТВО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»;

ИНН: 7713140469;

Сведения об основаниях возникновения исключительного права: собственная разработка;

Класс программного обеспечения по классификатору, утвержденному приказом от 22.09.2020 № 486: Средства антивирусной защиты;

Адрес страницы сайта правообладателя: <https://www.kaspersky.ru/small-to-medium-business-security/endpoint-select>;

Дата регистрации: 18 Марта 2016;

Рег. номер ПО: 205;

Решение уполномоченного органа: Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.03.2016 №112 «О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных».

Срок действия лицензии: 2 (два) года с 13.02.2024 - продление использования программного обеспечения.

1.3. Услуги, оказываемые в соответствии с контрактом, должны соответствовать требованиям законодательства Российской Федерации.

2. ЦЕНА КОНТРАКТА И ПОРЯДОК РАСЧЕТА

2.1. Цена контракта является твердой и не может изменяться в ходе его исполнения, за исключением случаев, предусмотренных п.п. 2.5, 2.6, 2.7 контракта*.*

2.2. Цена контракта (цена Услуг) составляет: \_\_\_\_\_\_\_рублей (\_\_\_\_\_ рублей \_\_ копеек), *в том числе налог на добавленную стоимость (далее - НДС) по налоговой ставке \_\_\_ (\_\_) процентов, а в случае, если контракт заключается с лицами, не являющимися в соответствии с законодательством Российской Федерации о налогах и сборах плательщиком НДС, то цена контракта НДС не облагается,* согласно Расчету стоимости услуг (Приложение № 2).

Аванс не предусмотрен.

Сумма, подлежащая уплате Заказчиком юридическому лицу или физическому лицу, в том числе зарегистрированному в качестве индивидуального предпринимателя, уменьшается на размер налогов, сборов и иных обязательных платежей в бюджеты бюджетной системы Российской Федерации, связанных с оплатой контракта, если в соответствии с законодательством Российской Федерации о налогах и сборах такие налоги, сборы и иные обязательные платежи подлежат уплате в бюджеты бюджетной системы Российской Федерации заказчиком.

Источник финансирования: бюджет Свердловской области.

2.3.Оплата по контракту осуществляется в рублях Российской Федерации.

2.4. В цену контракта включены все расходы Исполнителя, необходимые для исполнения обязательств по контракту, стоимость вознаграждения по лицензионному/сублицензионному договору, в том числе уплату налогов, сборов и других обязательных платежей для данного вида Услуг.

2.5. Цена контракта может быть снижена по соглашению Сторон без изменения предусмотренных контрактом объема Услуг, качества и иных условий исполнения контракта.

2.6. Заказчик по согласованию с Исполнителем вправе изменить не более чем на десять процентов предусмотренный контрактом объем оказанных Услуг. При этом по соглашению Сторон допускается изменение с учетом положений бюджетного законодательства Российской Федерации цены контракта пропорционально дополнительному объему оказанных Услуг исходя из установленной в контракте цены за единицу оказанных Услуг, но не более чем на десять процентов цены контракта. При уменьшении предусмотренного контрактом объема оказанных Услуг, Стороны обязаны уменьшить цену контракта исходя из цены за единицу оказанных Услуг. Цена единицы дополнительно оказываемой Услуги или цена единицы оказываемой Услуги при уменьшении предусмотренного контрактом объема оказываемых Услуг должна определяться как частное от деления первоначальной цены контракта на предусмотренный в контракте объем Услуг.

2.7. Цена может быть изменена в случаях, предусмотренных пунктом 6 статьи 161 Бюджетного кодекса Российской Федерации, при уменьшении ранее доведенных до Заказчика как получателя бюджетных средств лимитов бюджетных обязательств. При этом Заказчик в ходе исполнения контракта обеспечивает согласование новых условий контракта, в том числе цены и (или) сроков исполнения контракта и (или) объема Услуг, предусмотренных контрактом.

2.8. Оплата по контракту осуществляется Заказчиком по факту оказания Услуг на основании подписанного Сторонами документа о приемке в форме электронного документа в Единой информационной системе в сфере закупок (далее – ЕИС) путем перечисления денежных средств на банковский счет Исполнителя в течение 7 (семи) рабочих дней с даты подписания Заказчиком документа о приемке в форме электронного документа в ЕИС, за счет лимитов бюджетных обязательств 2024 года.

2.9. Направление Исполнителем в ЕИС документа о приемке, является условием оплаты. При этом ненаправление Исполнителем в ЕИС документа о приемке или направление его с нарушением формы (ненадлежащее оформление, отсутствие необходимых сведений, реквизитов), либо с неоговоренными исправлениями, является для Заказчика основанием для задержки оплаты до устранения Исполнителем указанных недостатков. В этом случае Заказчик не несёт ответственности за просрочку платежа и не возмещает убытки Исполнителя, возникшие в связи с данными обстоятельствами.

2.10. Датой оплаты контракта Стороны считают дату списания денежных средств с лицевого счета Заказчика.

2.11. По итогам исполнения Сторонами всех обязательств, предусмотренных контрактом, в течение 15 (пятнадцати) рабочих дней Стороны подписывают Акт сверки взаимных расчетов в 2 (двух) экземплярах. Заказчик должен подписать, заверить печатью и возвратить один экземпляр Акта сверки взаимных расчетов Исполнителю или предоставить мотивированные возражения по поводу достоверности содержащейся в нем информации в течение 5 (пяти) рабочих дней с даты его получения.

3. СРОК, МЕСТО И ПОРЯДОК ОКАЗАНИЯ УСЛУГ

3.1. **Срок оказания Услуг:** Услуги оказываются в течение 3 (Трех) рабочих дней с даты заключения контракта.

3.2. **Место оказания Услуг**: Передача лицензий на право использовать компьютерное программное обеспечение Kaspersky Endpoint Security для бизнеса Стандартный осуществляется по месту нахождения Управления архивами Свердловской области (г. Екатеринбург, ул. Малышева, 101, оф. 524).

3.3. **Порядок оказания Услуг:** в соответствии с Описанием объекта закупки.

4. ПРАВА И ОБЯЗАННОСТИ СТОРОН

**4.1. Заказчик вправе:**

4.1.1. Требовать от Исполнителя надлежащего исполнения обязательств в соответствии с условиями контракта.

4.1.2. Требовать от Исполнителя представления надлежащим образом оформленного документа, указанного в пункте 2.8. контракта.

4.1.3. Контролировать ход оказания Услуг Исполнителем по контракту без вмешательства в деятельность Исполнителя.

4.1.4. Требовать своевременного устранения выявленных недостатков.

4.1.5. Отказаться от оплаты Услуг, не предусмотренных контрактом, но оказанных Исполнителем.

4.1.6. Привлекать экспертов, экспертные организации для проверки соответствия качества оказанных Услуг требованиям, установленным контрактом.

4.1.7. Производить оплату контракта за вычетом соответствующего размера неустойки (штрафа, пени).

**4.2. Заказчик обязан:**

4.2.1. Создать Исполнителю необходимые условия для оказания Услуг.

4.2.2. Обеспечить приемку и оплату оказанных Услуг в соответствии с условиями контракта.

4.2.3. Требовать уплаты неустоек (штрафов, пеней) в соответствии с разделом 6 контракта.

4.2.4. Для проверки предоставленных Исполнителем результатов оказанных Услуг, предусмотренных контрактом, в части их соответствия условиям контракта, провести экспертизу оказанной Услуги. Экспертиза результатов, предусмотренных контрактом, может проводиться Заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации на основании контрактов, заключенных в соответствии с Законом о контрактной системе.

**4.3. Исполнитель вправе:**

4.3.1. Требовать приемки и своевременной оплаты оказанных Услуг в объеме, порядке, сроки и на условиях, предусмотренных контрактом.

4.3.2. Запрашивать у Заказчика разъяснения и уточнения по вопросам оказания Услуг в рамках контракта.

**4.4. Исполнитель обязан:**

4.4.1. Оказать Услуги на условиях и в сроки, предусмотренные контрактом.

4.4.2. Обеспечить соблюдение конфиденциальности информации, полученной в рамках исполнения контракта.

4.4.3. Предпринимать все возможные правовые, организационные и технические меры по предотвращению разглашения информации, которая стала известной в ходе исполнения контракта, в течение всего срока действия контракта.

4.4.4. Гарантировать Заказчику оказание Услуг по контракту без нарушения исключительных прав третьих лиц.

4.4.5. Исполнитель должен обладать законными правами на предоставление Управлению архивами Свердловской области лицензии на право использовать компьютерное программное Kaspersky Endpoint Security для бизнеса Стандартный.

4.4.6. Предоставление лицензий должно осуществляться без нарушения авторских и исключительных прав на объекты интеллектуальной собственности, в соответствии с нормами гражданского законодательства (ст.1229, ст.1233, ст.1252, ст.1253, ст.1261 и ст.1270 Гражданского кодекса Российской федерации).

4.4.7. Предоставлять Заказчику по его требованию в сроки, указанные в таком требовании, документы, относящиеся к предмету контракта.

4.4.8. Своевременно предоставлять Заказчику достоверную информацию о ходе исполнения своих обязательств, о сложностях, возникающих при исполнении контракта.

4.4.9. Представить надлежаще оформленные в соответствии с требованиями контракта и действующего законодательства документы, в полном объеме и в сроки, указанные в п. 5.3. контракта. При нарушении данного требования, Заказчик обязан применить к Исполнителю штрафные санкции в соответствии с п. 6.9. контракта.

4.4.10. В случае изменения банковских реквизитов, указанных в контракте, Исполнитель обязан в течение 3 (трех) рабочих дней в письменной форме сообщить об этом Заказчику с указанием новых реквизитов расчетного счета. В противном случае, все риски, связанные с перечислением Заказчиком денежных средств на указанный в контракте счет Исполнителя, несет Исполнитель.

4.4.11. Исполнять иные обязательства, предусмотренные действующим законодательством и контрактом.

5. ПОРЯДОК СДАЧИ И ПРИЕМКИ ОКАЗАННЫХ УСЛУГ

5.1. Приемка результатов оказанных Услуг осуществляется согласно требованиям действующего законодательства Российской Федерации, включая проведение экспертизы в соответствии с Законом о контрактной системе.

5.2. Факт оказания Услуг Исполнителем и принятия их Заказчиком подтверждается подписанием Сторонами документа о приемке в форме электронного документа в ЕИС.

5.3. Исполнитель в течение **10 (десяти)** рабочих дней с даты передачи Управлению архивами Свердловской области лицензий на право использовать компьютерное программное обеспечение «Kaspersky Endpoint Security для бизнеса Стандартный» по акту приема-передачи прав формирует, подписывает усиленной электронной подписью лица, имеющего право действовать от имени Исполнителя, и размещает в ЕИС документ о приемке.

5.4. Заказчик, в срок **не более 10 (десяти)** рабочих дней со дня получения от Исполнителя документа о приемке, и на основании результатов экспертизы, осуществляет одно из следующих действий:

а) подписывает усиленной электронной подписью лица, имеющего право действовать от имени Заказчика, и размещает в ЕИС документ о приемке;

б) формирует с использованием ЕИС, подписывает усиленной электронной подписью лица, имеющего право действовать от имени Заказчика, и размещает в ЕИС мотивированный отказ от подписания документа о приемке с указанием причин такого отказа.

5.5. Заказчик вправе не отказывать в приемке Услуг в случае выявления несоответствия Услуг условиям контракта, если выявленное несоответствие не препятствует приемке Услуг и устранено Исполнителем.

5.6. Датой поступления Исполнителю документа о приемке, мотивированного отказа от подписания документа о приемке, считается дата размещения документа о приемке, мотивированного отказа в ЕИС в соответствии с часовой зоной, в которой расположен Исполнитель.

5.7. Внесение исправлений в документ о приемке, осуществляется путем формирования, подписания усиленными электронными подписями лиц, имеющих право действовать от имени Исполнителя, Заказчика, и размещения в ЕИС исправленного документа о приемке.

5.8. В случае получения Исполнителем мотивированного отказа от подписания документа о приемке, Исполнитель в течение 3 (трех) рабочих дней с даты получения мотивированного отказа вправе устранить за свой счет причины, указанные в таком мотивированном отказе, и вновь направить Заказчику документ о приемке в порядке, установленном настоящим разделом контракта.

5.9. Заказчик, в течение 5 (пяти) рабочих дней с момента получения от Исполнителя документов на оказанные Услуги повторно осуществляет приемку оказанных Услуг в порядке, установленном настоящим разделом контракта.

5.10. После устранения недостатков, послуживших основанием для неподписания документа о приемке, Исполнитель и Заказчик подписывают документ о приемке в ЕИС в порядке и сроки, предусмотренные настоящим разделом.

5.11. Документ о приемке должен содержать следующую информацию:

а) Идентификационный код закупки, наименование, место нахождения Заказчика, наименование объекта закупки, место оказания Услуги, информацию об Исполнителе,

б) единицу измерения оказанной Услуги;

в) наименование оказанной Услуги;

г) информацию об объеме оказанной Услуги;

д) стоимость исполненных Исполнителем обязательств, предусмотренных контрактом, с указанием цены за единицу оказанных Услуг;

е) иную информацию с учетом требований, установленных контрактом.

5.12. К документу о приемке могут прилагаться документы, которые считаются его неотъемлемой частью. При этом в случае, если информация, содержащаяся в прилагаемых документах, не соответствует информации, содержащейся в документе о приемке, приоритет имеет информация, содержащаяся в документе о приемке.

5.13. Датой поступления Заказчику документа о приемке, подписанного Исполнителем, считается дата размещения такого документа в ЕИС в соответствии с часовой зоной, в которой расположен Заказчик.

5.14. Для проверки соответствия оказанной Услуги условиям контракта, Заказчик обязан провести экспертизу. Экспертиза может проводиться Заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации на основании контрактов, заключенных в соответствии с Законом о контрактной системе.

5.15. Для проведения экспертизы Заказчик, эксперты, экспертные организации имеют право запрашивать у Исполнителя дополнительные материалы, относящиеся к условиям исполнения контракта.

5.16. Заказчик вправе при приемке оказанных Услуг осуществлять фотосъемку и (или) видеозапись (видеосъемку) такой приемки в части ее соответствия условиям контракта.

5.17. Датой приемки оказанной Услуги считается дата размещения в ЕИС документа о приемке, подписанного Заказчиком.

6. ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. За неисполнение или ненадлежащее исполнение обязательств, предусмотренных контрактом, Стороны несут ответственность в соответствии с законодательством Российской Федерации.

6.2. В случае просрочки исполнения Заказчиком обязательств, предусмотренных контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Заказчиком обязательств, предусмотренных контрактом, Исполнитель вправе потребовать уплаты неустоек (штрафов, пеней).

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

6.4. Штрафы начисляются за ненадлежащее исполнение Заказчиком обязательств, предусмотренных контрактом, за исключением просрочки исполнения обязательств, предусмотренных контрактом.

Размер штрафа устанавливается контрактом в порядке, установленном постановлением Правительства Российской Федерации от 30.08.2017 № 1042 «Об утверждении Правил определения размера штрафа, начисляемого в случае ненадлежащего исполнения заказчиком, неисполнения или ненадлежащего исполнения поставщиком (подрядчиком, исполнителем) обязательств, предусмотренных контрактом (за исключением просрочки исполнения обязательств заказчиком, поставщиком (подрядчиком, исполнителем), о внесении изменений в постановление Правительства Российской Федерации от 15 мая 2017 г. № 570 и признании утратившим силу постановления Правительства Российской Федерации от 25 ноября 2013 г.   
№ 1063» (далее – постановление Правительства РФ от 30.08.2017 № 1042), за каждый факт неисполнения Заказчиком обязательства в размере:

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

5000 рублей, если цена контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

10000 рублей, если цена контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно);

100000 рублей, если цена контракта превышает 100 млн. рублей.

что составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

6.5. В случае просрочки исполнения Исполнителем обязательств (в том числе гарантийного обязательства), предусмотренных контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, Заказчик направляет Исполнителютребование об уплате неустоек (штрафов, пеней).

6.6. Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного контрактом, начиная со дня, следующего после дня истечения установленного контрактом срока исполнения обязательства, и устанавливается в размере одной трехсотой действующей на дату уплаты пени [ключевой ставки](http://mobileonline.garant.ru/#/document/10180094/entry/100) Центрального банка Российской Федерации от цены контракта (отдельного этапа исполнения контракта), уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных контрактом (соответствующим отдельным этапом исполнения контракта) и фактически исполненных Исполнителем, за исключением случаев, если законодательством Российской Федерации установлен иной порядок начисления пени.

6.7. Штрафы начисляются за каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных контрактом. Размер штрафа устанавливается контрактом в порядке, установленном постановлением Правительства РФ от 30.08.2017 № 1042, в размере 1 процента цены контракта, но не более 5 тыс. рублей и не менее 1 тыс. рублей, что составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей.

6.8. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, заключенным с победителем закупки (или с иным участником закупки в случаях, установленных Законом о контрактной системе), предложившим наиболее высокую цену за право заключения контракта, размер штрафа рассчитывается в порядке, установленном постановлением Правительства РФ от 30.08.2017 № 1042, за исключением просрочки исполнения обязательств, предусмотренных контрактом, и устанавливается в следующем порядке:

а) в случае, если цена контракта не превышает начальную (максимальную) цену контракта:

10 процентов начальной (максимальной) цены контракта, если цена не превышает 3 млн. рублей;

5 процентов начальной (максимальной) цены контракта, если цена контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

1 процент начальной (максимальной) цены контракта, если цена контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно);

б) в случае, если цена контракта превышает начальную (максимальную) цену контракта:

10 процентов цены контракта, если цена контракта не превышает 3 млн. рублей;

5 процентов цены контракта, если цена контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

1 процент цены контракта, если цена контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно).

6.9. За каждый факт неисполнения или ненадлежащего исполнения   
Исполнителем обязательства, предусмотренного контрактом, которое не имеет стоимостного выражения, размер штрафа устанавливается в следующем порядке:

1000 рублей, если цена контракта не превышает 3 млн. рублей;

5000 рублей, если цена контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

10000 рублей, если цена контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно);

100000 рублей, если цена контракта превышает 100 млн. рублей,

что составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

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

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

6.12. Исполнитель обязан возместить убытки, причиненные Заказчику в ходе исполнения контракта, в порядке, предусмотренном законодательством Российской Федерации.

6.13. В случае просрочки исполнения Исполнителем обязательств, предусмотренных контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, Заказчик после направления требования об уплате сумм неустойки (штрафа, пени) и неполучения ответа Исполнителя (или получения ответа о несогласии с предъявленным требованием), вправе:

-удержать суммы неисполненных Исполнителем требований об уплате неустоек (штрафов, пени), предъявленных Заказчиком, из суммы, подлежащей оплате Исполнителю;

-взыскать неустойку (штраф, пени) в судебном порядке.

В случае удовлетворения Исполнителем требования об уплате неустойки (штрафа, пени), Заказчик, руководствуясь статьей 313 Гражданского кодекса Российской Федерации, перечисляет неустойку в доход бюджета Свердловской области.

Перечисление неустойки (штрафа, пени) в доход соответствующего бюджета бюджетной системы Российской Федерации производится Заказчиком платежным документом с указанием Исполнителя, за которого осуществляется перечисление неустойки (штрафа, пени) в соответствии с условиями контрактом.

6.14. Уплата неустойки (штрафа, пени) не освобождает виновную Сторону от выполнения принятых на себя обязательств по контракту.

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

6.16. В качестве подтверждения фактов неисполнения или ненадлежащего исполнения Исполнителем обязательств Заказчик вправе использовать фото или видеоматериалы.

7. ОБЕСПЕЧЕНИЕ ИСПОЛНЕНИЯ КОНТРАКТА И ОБЕСПЕЧЕНИЕ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ

7.1. В целях заключения Контракта Исполнитель обязан обеспечить исполнение Контракта (гарантийных обязательств) предоставлением независимой гарантии, соответствующей требованиям статьи 45 Закона о контрактной системе, или внесением денежных средств на указанный Заказчиком счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими Заказчику. Способ обеспечения исполнения Контракта, срок действия независимой гарантии определяются в соответствии с требованиями Закона о контрактной системе Исполнителем самостоятельно. При этом срок действия независимой гарантии должен превышать предусмотренный Контрактом срок исполнения обязательств, которые должны быть обеспечены такой гарантией, не менее чем на один месяц, в том числе в случае его изменения в соответствии со статьей 95 Закона о контрактной системе.

7.2. Обеспечение исполнения Контракта представляется в размере 5 % цены Контракта в сумме \_\_\_\_\_\_ (\_\_\_\_\_\_) рублей \_\_\_ копеек.

Участник закупки, с которым заключается Контракт по результатам определения подрядчика в соответствии с пунктом 1 части 1 статьи 30 Закона о контрактной системе, освобождается от предоставления обеспечения исполнения Контракта в случае, если он предоставил до заключения Контракта в случаях, установленных Законом о контрактной системе, информацию, содержащуюся в реестре контрактов, заключенных заказчиками,  
и подтверждающую исполнение таким участником (без учета правопреемства) в течение трех лет до даты подачи заявки на участие в закупке трех контрактов, исполненных без применения к такому участнику неустоек (штрафов, пеней). Порядок предоставления данной информации предусмотрен частью 8.1 статьи 96 Закона о контрактной системе.

7.3. В случае, если Исполнителем предложена цена Контракта, которая на двадцать пять и более процентов ниже начальной (максимальной) цены Контракта, Исполнитель предоставляет обеспечение исполнения Контракта в размере, превышающем в полтора раза размер обеспечения исполнения Контракта, указанного в извещении в сумме \_\_\_\_\_\_\_ руб. (\_\_\_\_\_\_\_\_\_\_) рублей или информацию, подтверждающую добросовестность Исполнителя, с одновременным предоставлением обеспечения исполнения Контракта в размере обеспечения исполнения Контракта, указанном в извещении.

7.4. Обеспечение исполнения Контракта в виде внесения денежных средств, в том числе части этих денежных средств в случае уменьшения размера обеспечения исполнения Контракта в соответствии с частями 7, 7.1 и 7.2 статьи 96 Закона о контрактной системе, возвращается Исполнителю при условии надлежащего исполнения им всех обязательств по Контракту  
в течение 15 (пятнадцати) дней с даты исполнения обязательств по Контракту.

7.5. В ходе исполнения Контракта Исполнитель вправе изменить способ обеспечения исполнения Контракта и (или) предоставить Заказчику взамен ранее предоставленного обеспечения исполнения Контракта новое обеспечение исполнения Контракта, размер которого может быть уменьшен в порядке и случаях, которые предусмотрены частями 7.2 и 7.3 статьи 96 Закона о контрактной системе.

7.6. Обеспечение исполнения Контракта обеспечивает все обязательства Исполнителя и распространяется, в том числе, на уплату неустоек в виде штрафа, пени, предусмотренных Контрактом, а также убытков, понесенных Заказчиком в связи с неисполнением или ненадлежащим исполнением Исполнителем своих обязательств по Контракту, а также убытков в связи с проведением экспертизы качества Услуг, в том числе лабораторных испытаний,  
в результате которой будет установлено их ненадлежащее качество.

7.7. Обеспечение исполнения Контракта удерживается Заказчиком в размере, равном сумме невыполненных обязательств, неустойки и причиненных убытков, в случаях неисполнения или ненадлежащего исполнения своих обязательств Исполнителем, включая просрочку исполнения обязательств, одностороннего отказа Исполнителя от исполнения Контракта при отсутствии нарушения условий Контракта Заказчиком.

7.8. Реквизиты счета Заказчика для перечисления денежных средств в качестве обеспечения исполнения Контракта:

Наименование получателя:

Министерство финансов Свердловской области (Управление архивами Свердловской области л/с 05024260420)

счет 03222643650000006200

в Уральское ГУ Банка России//УФК по Свердловской области г. Екатеринбург

ИНН 6661001903

КПП 667001001

БИК 016577551

ЕКС 40102810645370000054

Назначение платежа: «Обеспечение исполнения Контракта по закупке извещение   
№ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

7.9. В случае отзыва в соответствии с законодательством Российской Федерации у банка, предоставившего независимую гарантию в качестве обеспечения исполнения Контракта, лицензии на осуществление банковских операций Исполнитель обязан предоставить новое обеспечение исполнения Контракта не позднее одного месяца со дня надлежащего уведомления Заказчиком Исполнителя о необходимости предоставить соответствующее обеспечение. Размер такого обеспечения может быть уменьшен в порядке и случаях, которые предусмотрены частями 7, 7.1, 7.2 и 7.3 статьи 96 Закона о контрактной системе. За каждый день просрочки исполнения Исполнителем данного обязательства начисляется пеня в размере, определённом  
в порядке, установленном в соответствии с законодательством Российской Федерации.

7.10. Обеспечение гарантийных обязательств **не предусмотрено.**

8. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ (форс-мажор)

8.1. Стороны освобождаются от ответственности за частичное или полное невыполнение обязательств по контракту, если оно явилось следствием обстоятельств непреодолимой силы (форс-мажор), а именно: стихийные бедствия (землетрясение, наводнение, ураган), пожар, массовые заболевания (эпидемии), забастовки, военные действия, террористические акты, диверсии, ограничения перевозок, запретительные меры государств, запрет торговых операций, в том числе с отдельными странами, вследствие принятия международных санкций и другие, не зависящие от воли Сторон контракта, обстоятельства.

8.2. Сторона, для которой создалась невозможность выполнения обязательств по контракту, обязана немедленно (в течение 3 (трех) дней) известить другую сторону о наступлении и прекращении вышеуказанных обстоятельств и подтвердить данные обстоятельства документами уполномоченной организации. Несвоевременное извещение об этих обстоятельствах лишает соответствующую Сторону права ссылаться на них в будущем.

8.3. Обязанность доказать наличие обстоятельств непреодолимой силы лежит на той Стороне контракта, которая не выполнила свои обязательства по контракту.

8.4. Если обстоятельства и их последствия будут длиться более 1 (одного) месяца, то Стороны вправе расторгнуть контракт. В этом случае ни одна из Сторон не имеет права потребовать от другой Стороны возмещения убытков.

8.5. Неуведомление или несвоевременное уведомление о наступлении обстоятельств непреодолимой силы лишает права любую из Сторон ссылаться на эти обстоятельства как на основание, освобождающее ее от ответственности за невыполнение обязательств, по отношению к другой Стороне.

9. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

9.1. Все разногласия и споры, которые могут возникнуть при исполнении контракта, подлежат предварительному разрешению путем переговоров, в том числе в претензионном порядке.

9.2. В претензии перечисляются допущенные при исполнении контракта нарушения со ссылкой на соответствующие положения контракта или его приложений, отражаются стоимостная оценка ответственности (неустойки), а также действия, которые должны быть произведены Стороной для устранения нарушений.

9.3. В случае обмена документами при применении мер ответственности и совершении иных действий в связи с нарушением Исполнителем или Заказчиком условий контракта в отношении контракта, заключенного по результатам электронных процедур, такой обмен осуществляется с использованием ЕИС путем направления электронных уведомлений. Такие уведомления формируются с использованием ЕИС, подписываются усиленной электронной подписью лица, имеющего право действовать от имени Заказчика, Исполнителя, и размещаются в ЕИС без размещения на официальном сайте.

9.4. В случае, если объем претензионной переписки, предусмотренной п. 9.3 контракта превысит объемы, допустимые функционалом ЕИС в соответствии с законодательством, дальнейший обмен документами может осуществляться посредством направления заказных писем по адресам, указанным в разделе 14, или направления электронных документов, подписанных электронными подписями, на адрес электронной почты, указанный в разделе 14.

9.5. Срок рассмотрения претензий не может превышать 10 (десять) рабочих дней с момента их получения. Датой надлежащего уведомления является дата размещения Стороной уведомления в соответствии с часовой зоной. Десятидневный срок отсчитывается со дня, следующего за днем надлежащего извещения

9.6. При неурегулировании Сторонами спора в досудебном порядке, спор подлежит рассмотрению Арбитражным судом Свердловской области.

10. УСЛОВИЯ И ПОРЯДОК РАСТОРЖЕНИЯ КОНТРАКТА

10.1. Расторжение контракта допускается по соглашению Сторон, по решению суда, а также, в случае одностороннего отказа Стороны контракта от исполнения контракта, в соответствии с Законом о контрактной системе, Гражданским кодексом Российской Федерации.

10.2. Заказчик вправе принять решение об одностороннем отказе от исполнения контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств. До принятия такого решения Заказчик вправе провести экспертизу оказанной Услугис привлечением экспертов, экспертных организаций.

Заказчик вправе отказаться от исполнения контракта в одностороннем порядке в следующих случаях:

– Исполнитель нарушил сроки оказания Услуг (п. 2 ст. 405, п. 3 ст. 708 ГК РФ);

– Исполнитель не приступил своевременно к исполнению контракта или оказывает Услуги настолько медленно, что окончание их к сроку становится невозможным (п. 2 ст. 715 ГК РФ);

– Исполнитель не устранил недостатки в установленный Заказчиком разумный срок (п. 3 ст. 715 и п. 3 ст. 723 ГК РФ);

– Недостатки оказанных Услуг являются существенными и неустранимыми (п. 3 ст. 723 ГК РФ);

– Заказчик не согласен на существенное увеличение приблизительной цены, связанное с необходимостью оказания дополнительных Услуг (п. 5 ст. 709 ГК РФ);

– в иных случаях, установленных гражданским законодательством.

Если Заказчиком проведена экспертиза оказанной Услуги с привлечением экспертов, экспертных организаций, решение об одностороннем отказе от исполнения контракта может быть принято Заказчиком только при условии, что по результатам экспертизы оказанной Услуги в заключении эксперта, экспертной организации будут подтверждены нарушения условий контракта, послужившие основанием для одностороннего отказа Заказчика от исполнения контракта.

10.3. Заказчик обязан принять решение об одностороннем отказе от исполнения контракта если в ходе исполнения контракта установлено, что:

а) Исполнитель и (или) оказываемая Услуга перестали соответствовать установленным извещением об осуществлении закупки и (или) документацией о закупке (если Законом о контрактной системе предусмотрена документация о закупке) требованиям к участникам закупки (за исключением требования, предусмотренного частью 1.1 (при наличии такого требования) статьи 31 настоящего Федерального закона) и (или) оказываемой Услуге;

б) при определении исполнителя Исполнитель представил недостоверную информацию о своем соответствии и (или) соответствии оказываемой Услуги требованиям, указанным в подпункте «а» настоящего пункта, что позволило ему стать победителем определения исполнителя;

10.4. В случае принятия Заказчиком решения об одностороннем отказе от исполнения контракта:

1) Заказчик с использованием ЕИС формирует решение об одностороннем отказе от исполнения контракта, подписывает его усиленной электронной подписью лица, имеющего право действовать от имени Заказчика, и размещает такое решение в ЕИС.

2) решение об одностороннем отказе от исполнения контракта не позднее одного часа с момента его размещения в ЕИС в соответствии с подпунктом 1 настоящего пункта автоматически с использованием ЕИС направляется Исполнителю. Датой поступления Исполнителю решения об одностороннем отказе от исполнения контракта считается дата размещения в соответствии с настоящим пунктом такого решения в ЕИС в соответствии с часовой зоной, в которой расположен Исполнитель;

3) поступление решения об одностороннем отказе от исполнения контракта в соответствии с подпунктом 2 настоящего пункта считается надлежащим уведомлением Исполнителя об одностороннем отказе от исполнения контракта.

10.5. Решение Заказчика об одностороннем отказе от исполнения контракта вступает в силу и контракт считается расторгнутым через десять дней с даты надлежащего уведомления Заказчиком Исполнителя об одностороннем отказе от исполнения контракта.

10.6. Заказчик обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения контракта, если в течение десятидневного срока с даты надлежащего уведомления Исполнителя о принятом решении об одностороннем отказе от исполнения контракта устранено нарушение условий контракта, послужившее основанием для принятия указанного решения, а также Заказчику компенсированы затраты на проведение экспертизы оказанной услуги, с привлечением экспертов, экспертных организаций. Данное правило не применяется в случае повторного нарушения Исполнителем условий контракта, которые в соответствии с гражданским законодательством являются основанием для одностороннего отказа Заказчиком от исполнения контракта.

10.7. Исполнитель вправе принять решение об одностороннем отказе от исполнения контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств.

В случае принятия Исполнителем предусмотренного частью 19 статьи 95 Закона о контрактной системе решения об одностороннем отказе от исполнения контракта, Исполнитель направляет такое решение Заказчику в следующем порядке:

1) Исполнитель с использованием ЕИС формирует решение об одностороннем отказе от исполнения контракта, подписывает его усиленной электронной подписью лица, имеющего право действовать от имени Исполнителя, и размещает такое решение в ЕИС. В случаях, предусмотренных частью 5 статьи 103 Закона о контрактной системе, такое решение не размещается на официальном сайте;

2) решение об одностороннем отказе от исполнения контракта не позднее одного часа с момента его размещения в ЕИС в соответствии с пунктом 1 настоящей части автоматически с использованием ЕИС направляется Заказчику. Датой поступления Заказчику решения об одностороннем отказе от исполнения контракта считается дата размещения в соответствии с настоящим пунктом такого решения в ЕИС в соответствии с часовой зоной, в которой расположен Заказчик;

3) поступление решения об одностороннем отказе от исполнения контракта в соответствии с пунктом 2 настоящей части считается надлежащим уведомлением Заказчика об одностороннем отказе от исполнения контракта.

Решение Исполнителя об одностороннем отказе от исполнения контракта вступает в силу и контракт считается расторгнутым через десять дней с даты надлежащего уведомления Исполнителем Заказчика об одностороннем отказе от исполнения контракта.

Исполнитель обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения контракта, если в течение десятидневного срока с даты надлежащего уведомления Заказчика о принятом решении об одностороннем отказе от исполнения контракта устранены нарушения условий контракта, послужившие основанием для принятия указанного решения.

10.8. При расторжении контракта в связи с односторонним отказом стороны контракта от исполнения контракта другая Сторона контракта вправе потребовать возмещения только фактически понесенного ущерба, непосредственно обусловленного обстоятельствами, являющимися основанием для принятия решения об одностороннем отказе от исполнения контракта.

10.9. Расторжение контракта по соглашению Сторон совершается в письменной форме.

В случае расторжения контракта по соглашению Сторон Исполнитель возвращает Заказчику все денежные средства, перечисленные для исполнения обязательств по контракту, а Заказчик оплачивает расходы (издержки) Исполнителя за фактически исполненные обязательства по контракту.

10.10. Требование о расторжении контракта может быть заявлено Стороной в суд только после получения отказа другой Стороны на предложение расторгнуть контракт либо неполучения ответа в течение 10 (десяти) дней с даты получения предложения о расторжении контракта.

11. СРОК ДЕЙСТВИЯ КОНТРАКТА

11.1. Контракт вступает в силу с даты его подписания обеими Сторонами, определенной в соответствии со статьей 51 Закона о контрактной системе, и действует до 29 марта 2024 года, а в части оплаты (выплаты неустойки, возмещения убытков) – до полного исполнения Сторонами своих обязательств по контракту.

12. АНТИКОРРУПЦИОННАЯ ОГОВОРКА

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

12.2. В случае возникновения у Стороны добросовестных и обоснованных подозрений, что произошло или может произойти нарушение каких-либо положений настоящего раздела контракта, соответствующая Сторона обязуется уведомить другую Сторону в письменной форме не позднее 5 (пяти) рабочих дней с момента возникновения указанных подозрений. В письменном уведомлении указываются лица, причастные к нарушению условий контракта, фактические обстоятельства дела и предоставляются материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение настоящего раздела контракта.

Каналы уведомления Исполнителя о нарушениях каких-либо положений настоящего раздела: на адрес электронной почты, указанный в контракте, официальный сайт \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (при наличии).

Каналы уведомления Заказчика о нарушениях каких-либо положений настоящего раздела: на адрес электронной почты, указанный в контракте, официальный сайт oirc.midural.ru.

Сторона, получившая письменное уведомление о нарушении положений настоящего раздела контракта, обязана в течение 10 (десяти) рабочих дней с даты его получения, рассмотреть его и в течение 5 (пяти) рабочих дней с даты окончания рассмотрения, сообщить уведомившей Стороне об итогах его рассмотрения.

12.3. Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений настоящего раздела контракта 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 условий настоящего раздела контракта.

12.4. В случае подтверждения факта нарушений одной Стороной положений настоящего раздела и/или неполучения другой Стороной информации об итогах рассмотрения письменного уведомления о нарушении условий настоящего раздела контракта, другая Сторона имеет право расторгнуть настоящий контракт в судебном порядке.

12.5. Стороны информируют в письменной форме Департамент противодействия коррупции и контроля Свердловской области о случаях коррупционных нарушений не позднее 5 (пяти) рабочих дней с момента подтверждения факта соответствующего нарушения.

13. ПРОЧИЕ УСЛОВИЯ

13.1. При исполнении контракта не допускается перемена Исполнителя, за исключением случаев, если новый Исполнитель является правопреемником Исполнителя по контракту, вследствие реорганизации юридического лица в форме преобразования, слияния или присоединения.

13.2. В случае перемены Заказчика по контракту права и обязанности Заказчика по контракту переходят к новому Заказчику в том же объеме и на тех же условиях.

13.3. Изменение положений Контракта допускается в случаях, предусмотренных действующим законодательством Российской Федерации.

Изменения оформляются в письменном виде путем подписания Сторонами дополнительного соглашения к контракту. Все дополнительные соглашения являются неотъемлемой частью контракта.

13.4. Во всем, что не оговорено в контракте, Стороны руководствуются действующим законодательством Российской Федерации.

13.5. Все приложения к контракту являются его неотъемлемой частью.

13.6. К контракту прилагаются:

- Приложение № 1. Описание объекта закупки – на 15 л.;

- Приложение № 2. Спецификация – на 1 л.

14. АДРЕСА МЕСТ НАХОЖДЕНИЯ,

**БАНКОВСКИЕ РЕКВИЗИТЫ И ПОДПИСИ СТОРОН**

|  |  |  |
| --- | --- | --- |
| **Заказчик:**  Управление архивами  Свердловской области  620004 г. Екатеринбург, ул. Малышева, 101  Тел. (343) 356-18-46, 356-18-35  Факс (343) 356-18-00  e-mail: uprarchives@egov66.ru  ИНН 6661001903 КПП 667001001  р/с 03221643650000006200  Наименование Банка получателя:  УРАЛЬСКОЕ ГУ БАНКА РОССИИ//УФК  по Свердловской области г. Екатеринбург  БИК 016577551  Корреспондентский счет Банка получателя: 40102810645370000054  Наименование получателя: Министерство финансов Свердловской области (Управление архивами Свердловской области), л/с 03024260420)  ОКПО 00073424, ОКОПФ 75204,  ОКФС 13, ОКТМО 65701000001  Должность:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |  | **Исполнитель:**  полное наименование организации - поставщика (с указанием ее организационно-правовой формы) или фамилия, имя и отчество (при наличии) поставщика - физического лица, в том числе зарегистрированного в качестве индивидуального предпринимателя  ИНН \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  КПП (при наличии) \_\_\_\_\_\_\_\_\_\_\_\_\_\_  Адрес местонахождения: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Тел.: (\_\_) \_\_\_\_\_\_\_\_\_\_\_\_\_\_  Факс: (\_\_) \_\_\_\_\_\_\_\_\_\_\_\_\_\_  е-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Банковские реквизиты:  р/с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  к/с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  БИК \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ОКТМО \_\_\_\_\_\_\_\_\_\_\_\_\_\_  ОКПО\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Идентификационного номера налогоплательщика, лица имеющего право без доверенности действовать от имени юридического лица, либо действующего в качестве руководителя юридического лица  (ФИО\_ИНН)  Должность:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |

Приложение № 1 к контракту

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_2024 года № \_\_\_\_\_\_\_\_\_\_

**ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ**

на оказание услуг по предоставлению лицензий на право использовать компьютерное программное обеспечение Kaspersky Endpoint Security для бизнеса Стандартный для нужд Управления архивами Свердловской области

**Объект закупки:** услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение [Kaspersky Endpoint Security для бизнеса Стандартный](https://reestr.minsvyaz.ru/reestr/65177/) для нужд Управления архивами Свердловской области

1. **Общие сведения**

**Код ОКПД2: 58.29.50.000** - Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение.

Программное обеспечение Kaspersky Endpoint Security для бизнеса – Стандартный, включено в Единый реестр российских программ для электронных вычислительных машин и баз данных:

Название: Kaspersky Endpoint Security для бизнеса Стандартный;

Сведения о правообладателях программного обеспечения: российская коммерческая организация;

Название организации: АКЦИОНЕРНОЕ ОБЩЕСТВО «ЛАБОРАТОРИЯ КАСПЕРСКОГО»;

ИНН: 7713140469;

Сведения об основаниях возникновения исключительного права: собственная разработка;

Класс программного обеспечения по классификатору, утвержденному приказом от 22.09.2020 № 486: Средства антивирусной защиты;

Адрес страницы сайта правообладателя: <https://www.kaspersky.ru/small-to-medium-business-security/endpoint-select>;

Дата регистрации: 18 Марта 2016;

Рег. номер ПО: 205;

Решение уполномоченного органа: Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 18.03.2016 №112 «О включении сведений о программном обеспечении в единый реестр российских программ для электронных вычислительных машин и баз данных».

1. **Описание объекта закупки**

Управлению архивами Свердловской области предоставляются лицензии на право использовать компьютерное программное обеспечение [Kaspersky Endpoint Security для бизнеса Стандартный](https://reestr.minsvyaz.ru/reestr/65177/) (простые (неисключительные) лицензии) сроком на (два) года с 13.02.2024 - продление использования программного обеспечения.

Установочный дистрибутив программного обеспечения не требуется.

Количество защищаемых объектов - 50 шт.

1. **Способы и объемы использования программного обеспечения**

Компьютерное программное обеспечение Kaspersky Endpoint Security для бизнеса Стандартный планируется использовать на автоматизированных рабочих местах, с операционной системой Windows, Linux на территории Свердловской области путем воспроизведения (пп.1 п.2 ст.1270 ГК).

1. **Требования к технической безопасности**

Техническая безопасность определяется соблюдением исполнителем конфиденциальности информации, полученной от Управления архивами Свердловской области в рамках исполнения государственного контракта. Исполнитель должен предпринимать все возможные правовые, организационные и технические меры по предотвращению разглашения информации, которая стала известной в ходе исполнения государственного контракта, в течение всего срока действия государственного контракта.

1. **Результат оказания услуг**

Фактом окончания оказания услуг является подписанный Исполнителем и Управлением архивами Свердловской области акт приема-передачи лицензий на право использовать компьютерное программное обеспечение Kaspersky Endpoint Security для бизнеса Стандартный и переданные Исполнителем Управлению архивами Свердловской области Код активации[[1]](#footnote-1) и Лицензионный Сертификат[[2]](#footnote-2).

1. **Срок оказания услуг**

Услуги оказываются в течение 3 (трех) рабочих дней с даты заключения государственного контракта.

1. **Место оказания услуг**

Передача лицензий на право использовать компьютерное программное обеспечение Kaspersky Endpoint Security для бизнеса Стандартный осуществляется по месту нахождения Управления архивами Свердловской области (г. Екатеринбург, ул. Малышева, 101, оф. 524).

|  |  |  |
| --- | --- | --- |
| **Заказчик:**  Должность:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |  | **Исполнитель:**  Должность:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |

Приложение

к описанию объекта закупки

# Общие требования

Антивирусные средства должны включать:

* программные средства антивирусной защиты для рабочих станций Windows;
* программные средства антивирусной защиты для рабочих станций и серверов Linux;
* программные средства антивирусной защиты для файловых серверов Windows;
* программные средства централизованного управления, мониторинга и обновления;
* обновляемые базы данных сигнатур вредоносных программ и атак;
* эксплуатационную документацию на русском языке.

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

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

# 

# Требования к программным средствам антивирусной защиты для рабочих станций Windows

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

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

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

* + антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
  + антивирусное сканирование по расписанию;
  + антивирусное сканирование подключаемых устройств;
  + эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
  + нейтрализации действий активного заражения;
  + анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
  + анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
  + блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
  + откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
  + ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
  + облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
  + антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
  + защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
  + фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
  + проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
  + блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
  + распознавания и блокировку фишинговых и небезопасных сайтов;
  + встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
  + защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
  + защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
  + контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
  + создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
  + контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
  + управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
  + записи в журнал событий о записи и/или удалении файлов на съемных дисках;
  + назначение приоритета для правил доступа к устройствам с файловой системой;
  + контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
  + защиты от атак типа BadUSB;
  + запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
  + защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
  + управления параметрами через доверенные программы удаленного администрирования;
  + установки только выбранных компонентов программного средства антивирусной защиты;
  + централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
  + запуска задач по расписанию и/или сразу после запуска приложения;
  + гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
  + ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
  + проверки целостности антивирусной программы;
  + добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
  + импорта и экспорта списков правил и исключений в XML-формат;
  + наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
  + наличие защищенного хранилища для отчетов о работе антивируса;
  + включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
  + интеграции с Windows Defender Security Center;
  + наличие поддержки Antimalware Scan Interface (AMSI);
  + наличие поддержки Windows Subsystem for Linux (WSL);
  + защитить паролем восстановление объектов из резервного хранилища;
  + ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
  + наличие инструмента мониторинга сети по протоколам TCP и UDP;
  + возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
  + установки ограничение длительности выполнения задачи;
  + ставить задачи проверки в очередь, если проверка уже выполняется;
  + наличие функции Анти-Бриджинг для запрета рабочей станции одновременно устанавливать сетевые соединения по разным каналам передачи информации (проводной и беспроводной) для предотвращения создание сетевых мостов;
  + обновление без перезагрузки системы;
  + настройки прав доступа (чтение / запись) для портативных устройств (MTP), выбирать пользователей или группу пользователей, которые имеют доступ к устройствам, а также задавать расписание доступа к устройствам;
  + настроить доступ пользователей к мобильным устройствам в приложении Android Debug Bridge (ADB);
  + заряжать мобильное устройство, подключив устройство к компьютеру через USB, даже если доступ к мобильному устройству запрещен;
  + настроить права печати для пользователей;
  + наличие поддержки протокола WPA3 для контроля подключения к сетям Wi-Fi;
  + наличие совместимости с Azure WVD;
  + настроить доступ пользователей к мобильным устройствам в приложении iTunes.

# Требования к программным средствам антивирусной защиты для серверов Windows

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

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

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

* антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверки целостности антивирусной программы;
* добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* защитить паролем восстановление объектов из резервного хранилища.
* импорта и экспорта списков правил и исключений в XML-формат;
* ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
* возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
* установки ограничения длительности выполнения задачи;
* ставить задачи проверки в очередь, если проверка уже выполняется;
* обновления без перезагрузки системы;

# 

# 

# Требования к программным средствам антивирусной защиты для рабочих станций и серверов Linux

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

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

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

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

Поддерживаемые 64-битные операционные системы для архитектуры ARM:

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

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

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

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

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

32-разрядных операционных систем Microsoft Windows

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

64-разрядных операционных систем Microsoft Windows

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

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

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

# 

# 

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

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

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

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

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

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

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

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

* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
* автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
* указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* иерархии триггеров, по которым происходит перераспределение;
* тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* инвентаризация установленного ПО и оборудования на компьютерах пользователей;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер Exchange ActiveSync;
* функция управления мобильными устройствами через сервер iOS MDM;
* отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* интеграции по OpenAPI;
* управления антивирусной защитой с использованием WEB консоли;
* двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
* использования дополнительной аутентификация после изменения параметров учетной записи пользователя.
* возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами;
* возможность развернуть сервер администрирования как систему высокой доступности.

# 

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

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

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

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

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

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

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

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

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

# 

# Требования к обновлению антивирусных баз

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

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

# 

# Требования к эксплуатационной документации

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

* «Руководство пользователя (администратора)»

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

# Требования к технической поддержке

Техническая поддержка антивирусного программного обеспечения должна:

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

Приложение № 2 к контракту

от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 года № \_\_\_\_\_\_\_

**Спецификация**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/п | Наименование | Ед.  изм. | Кол-во | Цена за ед.,  руб. | Итого,  в руб. |
| 1 | Услуги по предоставлению лицензий на право использовать компьютерное программное обеспечение Kaspersky Endpoint Security для бизнеса Стандартный для нужд Управления архивами Свердловской области | Условная единица | 50 |  |  |
|  | Итого: | | |  |  |

Итого\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_) рублей), *в том числе налог на добавленную стоимость (далее - НДС) по налоговой ставке \_\_\_ (\_\_) процентов, а в случае, если контракт заключается с лицами, не являющимися в соответствии с законодательством Российской Федерации о налогах и сборах плательщиком НДС, то цена контракта НДС не облагается.*

|  |  |  |
| --- | --- | --- |
| **Заказчик:**  Должность:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |  | **Исполнитель:**  Должность:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ |

1. Код активации — уникальный набор символов, с помощью которого может быть выполнена активация ПО. [↑](#footnote-ref-1)
2. Лицензионный Сертификат — документ, передаваемый Управлению архивами Свердловской области вместе с кодом активации и содержащий информацию о предоставляемой лицензии. [↑](#footnote-ref-2)