|  |  |
| --- | --- |
|  | **«УТВЕРЖДАЮ»**  **Главный врач**  **ОГАУЗ «Иркутская городская**  **клиническая больница № 8»**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Ж.В. Есева/** |

**Извещение о проведении закупки**

**на оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License**

**путем запроса котировок в электронной форме, участниками которого могут являться только субъекты малого и среднего предпринимательства**

**№ 137-24**

|  |  |  |
| --- | --- | --- |
| 1. | **Способ осуществления закупки:** | Запрос котировок в электронной форме, участниками которого могут являться только субъекты малого и среднего предпринимательства |
| 2. | **Наименование Заказчика:** | ОГАУЗ «Иркутская городская клиническая больница № 8» |
| 3. | **Место нахождения Заказчика:** | 664048, г. Иркутск, ул. Ярославского, 300 |
| 4. | **Почтовый адрес Заказчика:** | 664048, г. Иркутск, ул. Ярославского, 300 |
| 5. | **Адрес электронной почты Заказчика:** | [info@gkb8.ru](mailto:info@gkb8.ru) |
| 6. | **Контактный телефон Заказчика:** | (3952) 55-14-51, (3952)50-24-90 Черных Алексей Сергеевич |
| 7. | **Предмет договора c указанием количества поставляемого товара, объема выполняемой работы, оказываемой услуги, а также краткое описание предмета закупки:** | **Предмет договора:** Оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License.  **Количество поставляемого товара, объем выполняемой работы, оказываемой услуги:**  Согласно Техническому заданию (*Приложение № 1к Извещению о проведении запроса котировок в электронной форме (далее - Извещение)*)  **Описание предмета закупки:**  Согласно Техническому заданию (*Приложение № 1 к Извещению*) |
| 8. | **Код по ОКПД2:** | 58.29.50.000 |
| 9. | **Номер позиции в плане закупок:** | 233 |
| 10. | **Источник финансирования:** | Средства территориального фонда ОМС,  Средства от приносящей доход деятельности |
| 11. | **Срок поставки товара, выполнения работы, оказания услуги** | Срок оказания услуг (включая срок передачи прав на использовании ПО):20 календарных дней с даты подписания договора. |
| 12. | **Место поставки товара, выполнения работы, оказания услуги:** | г. Иркутск, ул. Баумана 214а/1 (каб. 422) |
| 13. | **Сведения о НМЦД либо о формуле цены и максимальном значении цены договора, либо о цене единицы товара, работы, услуги, сумме цен таких единиц и максимальном значении цены договора:** | **936630 руб. (девятьсот тридцать шесть тысяч шестьсот тридцать рублей 00 копеек)** |
| 14. | **Информация о валюте, используемой для формирования НМЦД, максимального значения цены договора и расчетов с поставщиком (подрядчиком, исполнителем):** | Российский рубль |
| 15. | **Порядок применения официального курса иностранной валюты к рублю Российской Федерации, установленного Центральным банком Российской Федерации и используемого при оплате договора:** | Требование не установлено |
| 16. | **Срок предоставления Извещения:** | С даты публикации Извещения в единой информационной системе в сфере закупок (далее – ЕИС) [zakupki.gov.ru](http://www.zakupki.gov.ru) **«03» июля 2024 года по «10» июля 2024 года** до 09.00 (время иркутское) |
| 17. | **Место предоставления Извещения:** | Документация размещена в ЕИС [zakupki.gov.ru](http://www.zakupki.gov.ru)и на электронной площадке (далее – ЭП) «ТЭК - Торг» в сети «Интернет» https://www.tektorg.ru/ |
| 18. | **Порядок предоставления Извещения:** | Документация находится в открытом доступе, начиная с даты размещения настоящего извещения о проведении запроса котировок в электронной форме.  **Порядок получения документации:**  В форме электронного документа. |
| 19. | **Размер, порядок и сроки внесения платы, взимаемой Заказчиком за предоставление Извещения:** | Требование не установлено |
| 20. | **Порядок, дата начала, дата и время окончания срока подачи заявок на участие в закупке:** | **Порядок подачи заявок:**  Заявка на участие в закупке подается посредством ЭП в форме электронного документа, подписанного усиленной квалифицированной электронной подписью (далее – электронная подпись) лица, имеющего право действовать от участника закупки, по форме и в порядке, которые указаны в настоящем Извещении, до истечения срока подачи заявок в запросе котировок.  Взаимодействие между участником закупки, заказчиком, оператором ЭП осуществляется в соответствии со статьей 3.3. Закона № 223-ФЗ.  Любой участник закупки вправе подать только одну заявку на участие в закупке.  В течение одного часа с момента получения заявки на участие в закупке оператор ЭП обязан присвоить ей идентификационный номер и подтвердить в форме электронного документа, направляемого участнику закупки, подавшему данную заявку, её получение с указанием присвоенного ей идентификационного номера.  В течение одного часа с момента получения заявки на участие в закупке оператор ЭП возвращает данную заявку подавшему её участнику такой закупки в случае:  1) подачи данной заявки с нарушением требований о наличии усиленной квалифицированной электронной подписи лица, имеющего право действовать от имени участника закупки;  2) подачи одним участником закупки двух и более заявок на участие в нем при условии, что поданные ранее заявки этим участником не отозваны. В указанном случае этому участнику возвращаются все заявки на участие в такой закупке;  3) получения данной заявки после даты или времени окончания срока подачи заявок на участие в закупке;  4) подачи участником закупки заявки, содержащей предложение о цене договора, превышающей НМЦД или равной нулю, либо предложение о сумме цен единиц товара, работы, услуги, превышающей начальную сумму таких единиц или равной нулю.  Одновременно с возвратом заявки на участие в закупке оператор ЭП обязан уведомить в форме электронного документа участника такойзакупки, подавшего данную заявку, об основаниях её возврата с указанием требований Положения, которые были нарушены. Возврат заявок на участие в закупке оператором ЭП по иным основаниям не допускается.  Участник закупки, подавший заявку на участие в закупке, вправе изменить или отозвать заявку на участие в закупке в любое время до окончания срока подачи заявок на участие в закупке, направив об этом уведомление оператору ЭП посредством программно-аппаратных средств ЭП.  **Язык заявки** – русский.  **Дата начала подачи заявок:** «03» июля 2024 года  **Дата и время окончания подачи заявок:**  «10» июля 2024 года 09:00 часов (время иркутское) |
| 21. | **В соответствии с подпунктом 2 пункта 5.1 Положения, участниками закупки могут быть только субъекты малого и среднего предпринимательства:** | Подтверждением принадлежности участника закупки к субъектам малого и среднего предпринимательства является наличие информации о таком участнике закупки в едином реестре субъектов малого и среднего предпринимательства. |
| 22. | **Адрес ЭП в информационно-телекоммуникационной сети «Интернет»:** | ЭП «ТЭК - Торг» по адресу в сети Интернет: <https://www.tektorg.ru/>  *(в соответствии с Распоряжением Правительства РФ от 12.07.2018 № 1447-р «Об утверждении перечней операторов электронных площадок и специализированных электронных площадок, предусмотренных Федеральными законами от 05.04.2013 N 44-ФЗ, от 18.07.2011 N 223-ФЗ»)*  *Субъекты малого и среднего предпринимательства получают аккредитацию на электронной площадке в порядке, установленном Федеральным* [*законом*](consultantplus://offline/ref=94466BBBC5CEC69AD59E440FA04EAB744C064ABF295DF3089A7E3AFF486CE27EA080C60F4EA61F833A64D8AAFAA156E62F3EE749E8C0lEi7E) *от 5 апреля 2013 года N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".* |
| 23. | **Размер обеспечения заявок на участие в закупке, требования к обеспечению заявок на участие в закупке, в том числе условия независимой гарантии:** | Требование не установлено |
| 24. | **Размер обеспечения исполнения договора, требования к обеспечению исполнения договора, в том числе условия независимой гарантии:** | 3 % от начальной (максимальной) цены договора, что составляет:  **28098,90 руб. (двадцать восемь тысяч девяносто восемь рублей девяносто копеек)**  В случае если по результатам закупки **цена договора**, предложенная победителем, участником закупки, с которым заключается договор, **снижена на двадцать пять и более процентов от НМЦД**, такой победитель либо такой участник **обязан** до заключения договора предоставить Заказчику документы, подтверждающие обеспечение исполнения договора в размере **в полтора раза превышающем** размер обеспечения исполнения договора, указанный в Извещении, а в случае если Извещением **обеспечение** исполнения договора **не было предусмотрено**, договор заключается только **после предоставления** таким победителем, участником **обеспечения** исполнения договора в размере **пяти процентов** начальной (максимальной) цены договора, но не менее чем в размере аванса (если договором предусмотрена выплата аванса).  **Исполнение договора может обеспечиваться:**   1. **внесением денежных средств**:   Реквизиты для перечисления обеспечения исполнения договора:  ИНН 3810009342  КПП 381001001  Минфин Иркутской области (ОГАУЗ «Иркутская городская клиническая больница № 8», л/с 80303060207)  Казначейский счет 03224643250000003400  Банковский счет 40102810145370000026  Наименование банка: Отделение Иркутск//УФК по Иркутской области, г. Иркутск  БИК 012520101  КПС 0000000000000000510  КВФО 3  Код субсидии 803093000  Отраслевой код 00000000000000000  Назначение платежа: обеспечение исполнения договора № 137-24   1. **предоставлением независимой гарантии**.   Способ обеспечения исполнения договора определяется участником закупки, с которым заключается договор, самостоятельно.  В случае, если обеспечение исполнения договора осуществляется путем предоставления независимой гарантии, то такие независимые гарантии должны быть выданы банком, включенным в перечень банков, которые вправе выдавать независимые гарантии для обеспечения исполнения контрактов и соответствующих требованиям, установленным частями 1 и 1.1 статьи 45 Федерального закона № 44-ФЗ, размещенный на официальном сайте федерального органа исполнительной власти по регулированию контрактной системы в сфере закупок в информационно-телекоммуникационной сети «Интернет».  Независимая гарантия, предоставляемая в качестве обеспечения исполнения контракта, **должна быть безотзывной** и должна содержать:  1) сумму независимой гарантии, подлежащую уплате гарантом Заказчику в случае ненадлежащего исполнения обязательств принципалом;  2) перечень обязательств принципала, надлежащее исполнение которых обеспечивается независимой гарантией;  3) указание на обязанность гаранта уплатить Заказчику неустойку в размере одной десятой процента суммы, подлежащей уплате, за каждый день просрочки;  4) условие, согласно которому обязательства гаранта по независимой гарантии считаются исполненными с момента поступления денежных средств на счет Заказчика;  5) условие о сроке действия независимой гарантии (срок действия независимой гарантии, предоставленной в качестве обеспечения заявки, должен составлять не менее чем два месяца с даты окончания срока подачи заявок, срок действия независимой гарантии, предоставленной в качестве обеспечения договора, должен превышать срок действия договора не менее чем на один месяц, в случае, если договором предусматривается поставка товара с последующей отсрочкой (рассрочкой) платежа Заказчика, срок действия независимой гарантии должен превышать срок поставки товара не менее чем на один месяц);  6) отлагательное условие о том, что договор предоставления независимой гарантии заключается по обязательствам участника закупки, которые возникнут из договора при его заключении;  7) условие о праве Заказчика в случае ненадлежащего выполнения или невыполнения поставщиком (подрядчиком, исполнителем) обязательств, обеспеченных независимой гарантией, представлять на бумажном носителе или в форме электронного документа требование об уплате денежной суммы по независимой гарантии, предоставленной в качестве обеспечения исполнения договора, в размере цены договора, уменьшенном на сумму, пропорциональную объему фактически исполненных поставщиком (подрядчиком, исполнителем) обязательств, предусмотренных договором и оплаченных Заказчиком, но не превышающем размер обеспечения исполнения договора;  8) условие о праве Заказчика по передаче права требования по независимой гарантии при перемене Заказчика в случаях, предусмотренных законодательством Российской Федерации, с предварительным извещением об этом гаранта;  9) условие о том, что расходы, возникающие в связи с перечислением денежных средств гарантом по независимой гарантии, несет гарант;  10) перечень документов, которые Заказчик должен предоставить банку вместе с требованием уплатить денежные средства по независимой гарантии:  а) расчет суммы, включаемой в требование по независимой гарантии;  б) распоряжение, подтверждающее перечисление Заказчиком аванса принципалу, с отметкой банка Заказчика или федерального органа исполнительной власти, осуществляющего правоприменительные функции по кассовому обслуживанию исполнения бюджетов бюджетной системы Российской Федерации(если выплата аванса предусмотрена договором, а требование по независимой гарантии предъявлено в случае ненадлежащего исполнения принципалом обязательств по возврату аванса);  в) документ, подтверждающий полномочия лица, подписавшего требование по независимой гарантии (доверенность) (в случае, если требование по независимой гарантии подписано лицом, не указанным в Едином государственном реестре юридических лиц в качестве лица, имеющего право без доверенности действовать от имени Заказчика);  11) обязательное наличие нумерации на всех листах независимой гарантии, которые должны быть прошиты, подписаны и скреплены печатью гаранта, в случае ее оформления в письменной форме на бумажном носителе на нескольких листах.  В независимой гарантию включается условие об обязанности гаранта уплатить Заказчику (бенефициару) денежную сумму по независимой гарантии не позднее десяти рабочих дней со дня, следующего за днем получения гарантом требования Заказчика (бенефициара), соответствующего условиям такой независимой гарантии, при отсутствии предусмотренных Гражданским кодексом Российской Федерации оснований для отказа в удовлетворении этого требования.  Недопустимо включение в независимую гарантию:  1) положений о праве гаранта отказывать в удовлетворении требования Заказчика о платеже по независимой гарантии в случае непредоставления гаранту Заказчиком уведомления о нарушении поставщиком (подрядчиком, исполнителем) условий договора или расторжении договора (за исключением случаев, когда направление такого уведомления предусмотрено условиями договора или законодательством Российской Федерации);  2) требований о предоставлении Заказчиком гаранту отчета об исполнении договора;  3) требований о предоставлении Заказчиком гаранту одновременно с требованием об осуществлении уплаты денежной суммы по независимой гарантии документов, не включенных в перечень документов, которые Заказчик должен предоставить банку вместе с требованием уплатить денежные средства по независимой гарантии.  Договор заключается после предоставления участником закупки, с которым заключается договор, обеспечения исполнения договора в соответствии с Извещением и положениями второго абзаца Раздела 42 Извещения.  В случае непредоставления победителем (единственным участником) запроса котировок в электронной форме, с которым заключается договор, обеспечения исполнения договора в срок, установленный для заключения договора, такой победитель (единственный участник) считается уклонившимся от заключения договора.  В ходе исполнения договора поставщик (подрядчик, исполнитель) вправе предоставить Заказчику обеспечение исполнения договора, уменьшенное на размер выполненных обязательств, предусмотренных договором, взамен ранее предоставленного обеспечения исполнения договора. При этом, по согласованию с Заказчиком, может быть изменен способ обеспечения исполнения договора.  В случае если участником закупки является государственное или муниципальное казенное учреждение, государственное или муниципальное бюджетное учреждение, государственное или муниципальное автономное учреждение, положения настоящего раздела об обеспечении исполнения договора к такому участнику закупки не применяются. |
| 25. | **Описание предмета закупки:** | Согласно Техническому заданию (*Приложение № 1 к Извещению)* |
| 26. | **Требования к содержанию, форме, оформлению и составу заявки на участие в закупке:** | **Требования к содержанию и составу заявки на участие в закупке с участием субъектов малого и среднего предпринимательства:**  Заявка на участие в закупке с участием субъектов малого и среднего предпринимательства должна содержать информацию и документы:  1) согласие участника закупки с участием субъектов малого и среднего предпринимательства на поставку товара, выполнение работы или оказание услуги на условиях, предусмотренных Извещением о закупке *(в соответствии с Формой заявки (Приложение № 3 к Извещению))*;  2)предложение участника закупки с участием субъектов малого и среднего предпринимательства в отношении предмета закупки: описание поставляемого товара, выполняемой работы, оказываемой услуги, которые являются предметом закупки в соответствии с требованиями Извещения (*см. Приложение № 1 к Извещению*). При осуществлении закупки товара или закупки работы, услуги, для выполнения, оказания которых используется товар, конкретные показатели товара, соответствующие значениям, установленным Извещением, указание на товарный знак (его словесное обозначение) (при наличии), производителя, наименование страны происхождения поставляемого товара (включается в заявку на участие в случае отсутствия в Извещении указания на товарный знак или в случае, если участник закупки предлагает товар, который обозначен товарным знаком, отличным от товарного знака, указанного в Извещении) *(предусмотрено Формой заявки (Приложение № 3 к Извещению))*;  3) предложение о цене договора (цене лота, единицы товара, работы, услуги);  4) наименование, фирменное наименование (при наличии), адрес юридического лица в пределах места нахождения юридического лица если участником закупки с участием субъектов малого и среднего предпринимательства является юридическое лицо *(в соответствии Формой заявки (Приложение № 3 к Извещению))*;  5) фамилия, имя, отчество (при наличии), паспортные данные, адрес места жительства физического лица, зарегистрированного в качестве индивидуального предпринимателя, если участником закупки с участием субъектов малого и среднего предпринимательства является индивидуальный предприниматель *(в соответствии Формой заявки (Приложение № 3 к Извещению))*;  6) идентификационный номер налогоплательщика участника закупки с участием субъектов малого и среднего предпринимательства или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика (для иностранного лица);  7) идентификационный номер налогоплательщика (при наличии) учредителей, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа юридического лица, если участником закупки с участием субъектов малого и среднего предпринимательства является юридическое лицо, или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика таких лиц;  8) учредительный документ, если участником закупки с участием субъектов малого и среднего предпринимательства является юридическое лицо;  9) копию документа, подтверждающего полномочия лица действовать от имени участника закупки с участием субъектов малого и среднего предпринимательства, за исключением случаев подписания заявки:  а) индивидуальным предпринимателем, если участником закупки является индивидуальный предприниматель;  б) лицом, указанным в едином государственном реестре юридических лиц в качестве лица, имеющего право без доверенности действовать от имени юридического лица (далее - руководитель), если участником закупки является юридическое лицо;  10) копии документов, подтверждающих соответствие участника закупки с участием субъектов малого и среднего предпринимательства требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом закупки, установленным Заказчиком в пункте 1 Раздела 30, за исключением случая, предусмотренного пунктом 7 раздела 30 Извещения о закупке *(в составе заявки необходимо представить копию документа);*  11) копию решения о согласии на совершение крупной сделки или о последующем одобрении этой сделки, если требование о наличии указанного решения установлено законодательством Российской Федерации и для участника закупки с участием субъектов малого и среднего предпринимательства заключение по результатам закупки договора либо предоставление обеспечения заявки на участие в закупке (если требование об обеспечении заявок установлено заказчиком в извещении об осуществлении закупки), обеспечения исполнения договора (если требование об обеспечении исполнения договора установлено заказчиком в извещении об осуществлении закупки) является крупной сделкой;  12) декларацию о соответствии участника закупки с участием субъектов малого и среднего предпринимательства требованиям, установленным в соответствии с Разделом 30 Извещения *(предусмотрено Формой заявки (Приложение № 3 к Извещению);*  13) копии документов, подтверждающих соответствие товара, работы или услуги, являющихся предметом закупки, требованиям, установленным в соответствии с законодательством Российской Федерации, в случае, если требования к данным товару, работе или услуге установлены в соответствии с законодательством Российской Федерации и перечень таких документов предусмотрен извещением о закупке кроме случаев, если в соответствии с законодательством Российской Федерации они передаются вместе с товаром;  14) наименование страны происхождения поставляемого товара (при осуществлении закупки товара, в том числе поставляемого заказчику при выполнении закупаемых работ, оказании закупаемых услуг);  15) документ, подтверждающий страну происхождения товара, предусмотренный постановлением Правительства Российской Федерации от 16.09.2016 № 925, постановлением Правительства Российской Федерации от 03.12.2020 № 2013.  Оператор электронной площадки обеспечивает участнику закупки с участием субъектов малого и среднего предпринимательства возможность включения в состав заявки и направления заказчику информации и документов, указанных в настоящем разделе, посредством программно-аппаратных средств электронной площадки в случае их представления оператору при аккредитации на электронной площадке.  Оператор электронной площадки обеспечивает участнику закупки с участием субъектов малого и среднего предпринимательства возможность включения в состав заявки и направления заказчику информации и документов, указанных в настоящем разделе, посредством программно-аппаратных средств электронной площадки в случае их представления данному оператору при аккредитации на электронной площадке в порядке, установленном Федеральным законом от 5 апреля 2013 года N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".  **Требования к форме, оформлению заявки на участие в закупке:**  Заявка на участие в закупке должна содержать все сведения и информацию, установленные в Приложении № 3 к Извещению ***(рекомендуется оформлять в виде файлов с расширением (\*.doc), (\*.docx))***;  Форма предоставления сведений и документов, подлежащих обязательному включению в заявку на участие в закупке, из нижеперечисленных:  1) сведения, сформированные с помощью средств, предусмотренных программно-аппаратным комплексом ЭП;  2) сведения в электронном виде - файл в формате, обеспечивающем возможность его сохранения на технических средствах Заказчика и допускающем после сохранения возможность поиска и копирования произвольного фрагмента текста;  3) копия документа, графический вид – файл, содержащий графический образ оригинала документа, заверенный в порядке, установленном извещением о закупке.  Сведения, сформированные с помощью средств, предусмотренных программно-аппаратным комплексом ЭП и сведения в электронном виде должны совпадать, в случае несовпадения приоритетными являются сведения, составленные с помощью средств, предусмотренных программно-аппаратным комплексом ЭП.  Электронные документы, входящие в состав заявки должны иметь один из распространенных форматов документов: с расширением (\*.doc), (\*.docx), (\*.xls), (\*.xlsx), (\*.txt), (\*.pdf), (\*.jpg).  Все документы, заполняемые участником закупки по формам, содержащимся в Приложении № 3 Извещения, и представляемые участниками закупки в составе заявки на участие в закупке, должны содержать все страницы, должны быть заполнены по всем пунктам и графам, четко читаемы, и должны быть подписаны электронной подписью в соответствии с требованиями Федерального закона от 6 мая 2011 года № 63-ФЗ «Об электронной подписи».  Файлы формируются по принципу: один файл – один документ.  Допускается размещение в составе заявки документов, сохраненных в архивах, при этом размещение в составе заявки архивов, разделенных на несколько частей, открытие каждой из которых по отдельности невозможно, не допускается.  Все файлы не должны иметь защиты от их открытия, копирования их содержимого или их печати.  Файлы должны быть именованы так, чтобы из их названия ясно следовало, какой документ, требуемый в соответствии с Извещением, в каком файле находится.  Расхождение между численным и буквенным выражением предлагаемой цены договора не допускается.  Цена договора, указанная участником закупки в графе «ИТОГО (цена договора), руб.» Раздела 3. Приложения № 3 к Извещению, должна соответствовать сумме общих стоимостей по всем позициям закупаемого товара (общая стоимость по каждой позиции закупаемого товара рассчитана как произведение количества товара и цены единицы поставляемого товара по данной позиции). |
| 27. | **Требования к описанию участником закупки поставляемого товара, его функциональных характеристик (потребительских свойств), его количественных и качественных характеристик, требования к описанию участниками такой закупки выполняемой работы, оказываемой услуги, из количественных и качественных характеристик;** | Установлены в Техническом задании (*Приложение № 1 к Извещению*) и проекте договора (*Приложение № 2 к Извещению*). |
| 28. | **Обоснование начальной (максимальной) цены договора либо цены единицы товара, работы, услуги, включая информацию о расходах на перевозку, страхование, уплату таможенных пошлин, налогов и других обязательных платежей:** | **Обоснование начальной (максимальной) цены договора указано в Приложении № 4 к Извещению.**  Цена договора включает трудозатраты, затраты на средства для оказания услуг, НДС (в случае, если Исполнитель является плательщиком НДС), стоимость материалов и средств, необходимых для оказания услуг, транспортные расходы, а также расходы на страхование, уплату налогов, таможенных пошлин, сборов и другие обязательные платежи, предусмотренные договором, является твердой и определяется на весь срок исполнения договора, то есть является конечной. |
| 29. | **Форма, сроки и порядок оплаты товара, работы, услуги:** | Оплата производится за фактически оказанные услуги на основании счета и подписанного сторонами акта об оказанных услугах, путем перечисления денежных средств на расчетный счет Исполнителя в течение 7 (семи) рабочих дней с момента подписания акта за оказанные услуги. Днем оплаты является день списания денежных средств с расчетного счета Заказчика |
| 30. | **Требования к участникам закупки:** | 1) соответствие участника закупки с участием субъектов малого и среднего предпринимательства требованиям, устанавливаемым в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставки товаров, выполнение работ, оказание услуг, являющихся предметом закупки;  2) непроведение ликвидации участника закупки с участием субъектов малого и среднего предпринимательства - юридического лица и отсутствие решения арбитражного суда о признании участника закупки - юридического лица или индивидуального предпринимателя несостоятельным (банкротом);  3) неприостановление деятельности участника закупки с участием субъектов малого и среднего предпринимательства в порядке, установленном Кодексом Российской Федерации об административных правонарушениях;  4) отсутствие у участника закупки с участием субъектов малого и среднего предпринимательства недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает **двадцать пять процентов** балансовой стоимости активов участника такой закупки, по данным бухгалтерской (финансовой) отчетности за последний отчетный период. Участник закупки с участием субъектов малого и среднего предпринимательства считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по данному заявлению на дату рассмотрения заявки на участие в закупке не принято;  5) отсутствие у участника закупки с участием субъектов малого и среднего предпринимательства - физического лица, зарегистрированного в качестве индивидуального предпринимателя, либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - участника закупки с участием субъектов малого и среднего предпринимательства непогашенной или неснятой судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, [290](consultantplus://offline/ref=06DAB305DF3DF45773AC76426B0289841374F086155A83DAA68D53AB9583B2CD1031C6D7BAB0CA3B54A7F29DD6BE2005EFED15691276KAm1H), [291](consultantplus://offline/ref=06DAB305DF3DF45773AC76426B0289841374F086155A83DAA68D53AB9583B2CD1031C6D7BAB2CC3B54A7F29DD6BE2005EFED15691276KAm1H), [291.1](consultantplus://offline/ref=06DAB305DF3DF45773AC76426B0289841374F086155A83DAA68D53AB9583B2CD1031C6D7BABDC83B54A7F29DD6BE2005EFED15691276KAm1H) Уголовного кодекса Российской Федерации, а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся предметом осуществляемой закупки, и административного наказания в виде дисквалификации;  6) отсутствие фактов привлечения в течение двух лет до момента подачи заявки на участие в закупке с участием субъектов малого и среднего предпринимательства участника закупки - юридического лица к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях;  7) соответствие участника закупки с участием субъектов малого и среднего предпринимательства указанным в извещении о закупке требованиям законодательства Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом закупки, если в соответствии с законодательством Российской Федерации информация и документы, подтверждающие такое соответствие, содержатся в открытых и общедоступных государственных реестрах, размещенных в информационно-телекоммуникационной сети "Интернет" (с указанием адреса сайта или страницы сайта в информационно-телекоммуникационной сети "Интернет", на которых размещены эти информация и документы);  8) обладание участником закупки с участием субъектов малого и среднего предпринимательства исключительными правами на результаты интеллектуальной деятельности, если в связи с исполнением договора заказчик приобретает права на такие результаты;  9) обладание участником закупки с участием субъектов малого и среднего предпринимательства правами использования результата интеллектуальной деятельности в случае использования такого результата при исполнении договора.  Декларация, предусмотренная настоящим разделом, представляется в составе заявки участником закупки с участием субъектов малого и среднего предпринимательства с использованием программно-аппаратных средств электронной площадки. |
| 31. | **Требования к участникам закупки и привлекаемым ими субподрядчикам, соисполнителям и (или) изготовителям товара, являющегося предметом закупки, и перечень документов, предоставляемых участниками закупки для подтверждения их соответствия указанным требованиям, в случае закупки работ по проектированию, строительству, модернизации и ремонту особо опасных, технически сложных объектов капитального строительства и закупки товаров, работ, услуг, связанных с использованием атомной энергии:** | Требование не установлено |
| 32. | **Формы, порядок, дата и время окончания срока предоставления участникам закупки разъяснений положений Извещения:** | **Формы и порядок предоставления разъяснений положений Извещения:**  Любой участник закупки вправе направить Заказчику запрос о даче разъяснений положений Извещения об осуществлении закупки.  Разъяснения положений Извещения о закупке производятся заказчиком через ЭП посредством обмена документами между заказчиком и участником закупки, направившим запрос в следующем порядке:  Участник закупки направляет через ЭП электронный документ (информацию в электронной форме, подписанную усиленной квалифицированной электронной подписью), содержащий запрос на разъяснение положений извещения о закупке, документации о закупке.  В течение трех рабочих дней с даты поступления такого запроса, Заказчик осуществляет разъяснение положений извещения и (или) документации о конкурентной закупке и, не позднее чем в течение трех дней со дня предоставления таких разъяснений, размещает их в ЕИС с указанием предмета запроса, но без указания участника такой закупки, от которого поступил указанный запрос. При этом Заказчик вправе не осуществлять такое разъяснение в случае, если указанный запрос поступил позднее, чем за три рабочих дня до даты окончания срока подачи заявок на участие в такой закупке.  **Дата и время окончания срока предоставления участникам закупки разъяснений положений Извещения о проведении закупки:**  «09» июля 2024 г. (16:00) |
| 33. | **Дата рассмотрения предложений участников закупки и подведение итогов закупки:** | «10» июля 2024 г. |
| 34. | **Условия предоставления приоритета товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами:** | Приоритет товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами предоставляется в соответствии с постановлением Правительства РФ от 16.09.2016 № 925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами» (далее – Постановление № 925).  В соответствии с пунктом 2 Постановления № 925 оценка и сопоставление заявок на участие в закупке, которые содержат предложения о поставке товаров российского происхождения, выполнении работ, оказании услуг российскими лицами, по стоимостным критериям оценки производятся по предложенной в указанных заявках цене договора, сниженной на 15 процентов, при этом договор заключается по цене договора, предложенной участником в заявке на участие в закупке.  В соответствии с пунктом 2(1) Постановления N 925 при осуществлении закупок радиоэлектронной продукции способом, победителем в котором признается лицо, предложившее наиболее низкую цену договора, оценка и сопоставление заявок на участие в закупке, которые содержат предложения о поставке радиоэлектронной продукции, включенной в единый реестр российской радиоэлектронной продукции (далее - Реестр), по стоимостным критериям оценки производятся по предложенной в указанных заявках цене договора, сниженной на 30 процентов, при этом договор заключается по цене договора, предложенной участником в заявке на участие в закупке.  Для целей установления соотношения цены предлагаемых к поставке товаров российского и иностранного происхождения, цены выполнения работ, оказания услуг российскими и иностранными лицами в случаях, предусмотренных подпунктом «г» Раздела 34 Извещения, цена единицы каждого товара, работы, услуги определяется как произведение начальной (максимальной) цены единицы товара, работы, услуги, указанной в Приложении № 1 Извещения, на коэффициент изменения начальной (максимальной) цены договора по результатам проведения закупки, определяемый как результат деления цены договора, по которой заключается договор, на начальную (максимальную) цену договора.  Отсутствие в заявке на участие в закупке указания (декларирования) страны происхождения поставляемого товара не является основанием для отклонения заявки на участие в закупке и такая заявка рассматривается как содержащая предложение о поставке иностранных товаров.  Участник закупки относится к российским или иностранным лицам на основании документов участника закупки, содержащих информацию о месте его регистрации (для юридических лиц и индивидуальных предпринимателей), на основании документов, удостоверяющих личность (для физических лиц).  Приоритет не предоставляется в случаях, если:  а) закупка признана несостоявшейся и договор заключается с единственным участником закупки;  б) в заявке на участие в закупке не содержится предложений о поставке товаров российского происхождения, выполнении работ, оказании услуг российскими лицами;  в) в заявке на участие в закупке не содержится предложений о поставке товаров иностранного происхождения, выполнении работ, оказании услуг иностранными лицами;  г) в заявке на участие в закупке, представленной участником закупки, при котором победитель закупки определяется на основе критериев оценки и сопоставления заявок на участие в закупке, указанных в документации о закупке, или победителем которой признается лицо, предложившее наиболее низкую цену договора, содержится предложение о поставке товаров российского и иностранного происхождения, выполнении работ, оказании услуг российскими и иностранными лицами, при этом стоимость товаров российского происхождения, стоимость работ, услуг, выполняемых, оказываемых российскими лицами, составляет менее 50 процентов стоимости всех предложенных таким участником товаров, работ, услуг. |
| 35. | **Требование об указании (декларировании) участником закупки в заявке на участие в закупке (в соответствующей части заявки, содержащей предложение о поставке товара) наименования страны происхождения поставляемых товаров:** | Участник закупки в заявке на участие в закупке в соответствующей части заявки, содержащей предложение о поставке товара, указывает наименование страны происхождения поставляемых товаров *(предусмотрено Формой заявки (Приложение № 3 к Извещению))*. |
| 36. | **Положение об ответственности участников закупки за предоставление недостоверных сведений о стране происхождения товара, указанного в заявке:** | Участник закупки несет ответственность за представление недостоверных сведений о стране происхождения товара, указанного в заявке на участие в закупке. |
| 37. | **Сведения о начальной (максимальной) цене единицы каждого товара, работы, услуги, являющиеся предметом закупки:** | Установлены в Техническом задании *(Приложение № 1 к Извещению)* |
| 38. | **Критерии рассмотрения и оценки заявок на участие в закупке:** | Оценка заявок на участие в закупке производится по единственному критерию – цене, с учетом приоритета товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами в соответствии с Разделом 34 Извещения. |
| 39. | **Порядок подведения итогов:** | Закупочная комиссия не рассматривает и отклоняет заявки на участие в запросе котировок в электронной форме, если:   1. Участник закупки, подавший заявку на участие в запросе котировок в электронной форме, не соответствует требованиям к участнику закупки, установленным в Извещении; 2. Заявка признана не соответствующей требованиям, установленным в Извещении; 3. Непредоставления документов и информации, определенных в Извещении либо наличия в предоставленных в составе заявки на участие в запросе котировок в электронной форме документах и информации недостоверных сведений об участнике, подавшем такую заявку, или о товарах, работах, услугах соответственно на поставку, выполнение, оказание которых проводится запрос котировок в электронной форме.   В течение одного рабочего дня после направления оператором электронной площадки Заказчику заявок на участие в закупке, закупочная комиссия на основании результатов оценки заявок на участие в закупке присваивает каждой заявке порядковый номер в порядке уменьшения степени выгодности содержащихся в них условий исполнения договора. Заявке на участие в закупке, в которой содержится наименьшее ценовое предложение, присваивается первый номер. В случае, если в нескольких заявках содержатся одинаковые по степени выгодности условия исполнения договора или одинаковые ценовые предложения, меньший порядковый номер присваивается заявке, которая поступила ранее других заявок.  Результаты рассмотрения и оценки заявок на участие в запросе котировок в электронной форме оформляются протоколом, который подписывается всеми присутствующими на заседании членами закупочной комиссии.  Протокол рассмотрения и оценки заявок на участие в запросе котировок в электронной форме, подписывается в день рассмотрения и оценки заявок (день рассмотрения единственной заявки) всеми присутствующими членами закупочной комиссии и размещается Заказчиком в ЕИС и на ЭП не позднее чем через три дня с даты подписания.  В случае, если по окончании срока подачи заявок на участие в запросе котировок в электронной форме подана только одна такая заявка или не подано ни одной такой заявки, запрос котировок в электронной форме признается несостоявшимся.  Запрос котировок в электронной форме признается несостоявшимся в случае, если по результатам рассмотрения заявок на участие в запросе котировок в электронной форме закупочной комиссией отклонены все поданные заявки на участие в запросе котировок в электронной форме или только одна такая заявка признана соответствующей всем требованиям, указанным в Извещении.  Отстранение участника закупки от участия в определении поставщика (подрядчика, исполнителя) или отказ от заключения договора с победителем определения поставщика (подрядчика, исполнителя) осуществляется в любой момент до заключения договора, если Заказчик или закупочная комиссия обнаружит, что участник закупки не соответствует требованиям, указанным в пункте 30 Извещения, или предоставил недостоверную информацию в отношении своего соответствия указанным требованиям. |
| 40. | **Срок подписания договора участником закупки:** | Договор по результатам закупки с участием субъектов малого и среднего предпринимательства заключается с использованием программно-аппаратных средств электронной площадки и должен быть подписан электронной подписью лица, имеющего право действовать от имени соответственно участника такой конкурентной закупки, заказчика. В случае наличия разногласий по проекту договора, направленному заказчиком, участник закупки составляет протокол разногласий с указанием замечаний к положениям проекта договора, не соответствующим извещению о закупке и своей заявке, с указанием соответствующих положений данных документов. Протокол разногласий направляется заказчику с использованием программно-аппаратных средств электронной площадки в порядке, указанном в настоящем разделе. Заказчик рассматривает протокол разногласий и направляет участнику закупки доработанный проект договора либо повторно направляет проект договора с указанием в отдельном документе причин отказа учесть полностью или частично содержащиеся в протоколе разногласий замечания.  Договор может быть заключен не ранее чем через десять и не позднее чем через двадцать дней с даты размещения в ЕИС протокола подведения итогов закупки. В случае необходимости одобрения органом управления Заказчика в соответствии с законодательством Российской Федерации заключения договора или в случае обжалования в антимонопольном органе действий (бездействия) Заказчика, закупочной комиссии, оператора электронной площадки договор должен быть заключен не позднее чем через пять дней с даты указанного одобрения или с даты вынесения решения антимонопольного органа по результатам обжалования действий (бездействия) Заказчика, закупочной комиссии по осуществлению конкурентной закупки, оператора электронной площадки.  В течение пяти дней с даты размещения в ЕИС протокола рассмотрения и оценки заявок на участие в закупке Заказчик размещает на ЭП без своей подписи проект договора, который составляется путем включения в проект договора, прилагаемый к Извещению, цены договора, предложенной победителем, (единственным участником), информации о товаре (товарном знаке и (или) конкретных показателях товара), предложения победителя (единственного участника) запроса котировок в электронной форме о качественных, функциональных и экологических характеристиках предмета закупки и об иных условиях исполнения договора, указанных в заявке, окончательном предложении победителя конкурентной закупки в электронной форме.  В течение пяти дней с даты размещения Заказчиком и на ЭП проекта договора победитель (единственный участник) запроса котировок в электронной форме подписывает усиленной квалифицированной электронной подписью указанный проект договора, размещает на ЭП подписанный проект договора и документ, подтверждающий предоставление обеспечения исполнения договора, если данное требование установлено в Извещении, либо размещает протокол разногласий. В случае если по результатам закупки цена договора снижена на двадцать пять процентов и более от начальной (максимальной) цены договора, победитель (единственный участник) соответствующей закупки предоставляет обеспечение исполнения договора в соответствии с положениями абзаца второго Раздела 42 Извещения.  В течение пяти дней с даты размещения Заказчиком на ЭП проекта договора победитель (единственный участник) закупки в случае наличия разногласий по проекту договора, размещенному в соответствии с настоящим разделом Извещения, размещает на ЭП протокол разногласий, подписанный усиленной квалифицированной электронной подписью лица, имеющего право действовать от имени победителя (единственного участника) такой закупки. Указанный протокол может быть размещен на ЭП в отношении соответствующего договора не более чем один раз. При этом победитель (единственный участник) запроса котировок в электронной форме, указывает в протоколе разногласий замечания к положениям проекта договора, не соответствующим Извещению и своей заявке на участие в такой закупке, с указанием соответствующих положений данных документов.  В течение трех рабочих дней с даты размещения победителем (единственным участником) запроса котировок в электронной форме на ЭП в соответствии с настоящим разделом Извещения протокола разногласий Заказчик рассматривает протокол разногласий и без своей подписи размещает на ЭП доработанный проект договора либо повторно размещает на ЭП проект договора с указанием в отдельном документе причин отказа учесть полностью или частично содержащиеся в протоколе разногласий замечания.  В течение трех рабочих дней с даты размещения Заказчиком на ЭП документов, предусмотренных предыдущим абзацем настоящего раздела Извещения, победитель (единственный участник) запроса котировок в электронной форме размещает на ЭП проект договора, подписанный усиленной квалифицированной электронной подписью лица, имеющего право действовать от имени такого победителя (единственного участника), а также документ и (или) информацию, подтверждающие предоставление обеспечения исполнения договора в соответствии с настоящим разделом Извещения, подписанные усиленной квалифицированной электронной подписью указанного лица.  В течение трех рабочих дней с даты размещения на ЭП проекта договора, подписанного усиленной квалифицированной электронной подписью лица, имеющего право действовать от имени победителя запроса котировок в электронной форме и предоставления таким победителем соответствующего требованиям абзаца второго Раздела 42 Извещения, обеспечения исполнения договора Заказчик обязан разместить на ЭП договор, подписанный усиленной квалифицированной электронной подписью лица, имеющего право действовать от имени Заказчика. Договор считается заключенным с момента размещения договора, подписанного Заказчиком. |
| 41. | **Порядок заключения договора в случае уклонения победителя от заключения договора:** | Победитель (единственный участник) запроса котировок в электронной форме признается уклонившимся от заключения договора в случае, если в сроки, предусмотренные Разделом 42 Извещения он не направил Заказчику проект договора, подписанный лицом, имеющим право действовать от имени такого победителя (единственного участника), или не направил протокол разногласий, или не предоставил обеспечение исполнения договора, предусмотренное Извещением, положениями абзаца второго Раздела 42 Извещения. При этом Заказчик не позднее трех дней с даты признания победителя (единственного участника) конкурентной закупки в электронной форме уклонившимся от заключения договора, составляет и размещает на ЭП протокол о признании такого победителя (единственного участника) уклонившимся от заключения договора, содержащий информацию о месте и времени его составления, о победителе, признанном уклонившимся от заключения договора, о факте, являющемся основанием для такого признания, а также реквизиты документов, подтверждающих этот факт.  В случае неисполнения требований, установленных положениями абзаца второго Раздела 42 Извещения, победитель или участник закупки, с которым заключается договор, признается уклонившимся от заключения договора.  В случае, если победитель запроса котировок в электронной форме признан уклонившимся от заключения договора, Заказчик вправе заключить договор с участником конкурентной закупки в электронной форме, заявке которого присвоен второй номер. Этот участник признается победителем такой закупки, и в проект договора, прилагаемый к Извещению, Заказчиком включаются условия исполнения данного договора, предложенные этим участником. Проект договора должен быть направлен Заказчиком этому участнику в срок, не превышающий пяти дней с даты признания победителя такой процедуры уклонившимся от заключения договора. При этом Заказчик вправе обратиться в суд с требованием о возмещении убытков, причиненных уклонением от заключения договора в части, не покрытой суммой обеспечения заявки на участие в закупке. |
| 42. | **Условия заключения и исполнения договора:** | Договор заключается только после предоставления участником закупки обеспечения исполнения договора в соответствии с требованиями Заказчика, установленными в Разделе 24 Извещения.  В случае если по результатам закупки цена договора, предложенная победителем, участником закупки, с которым заключается договор, снижена на двадцать пять и более процентов от НМЦД, такой победитель либо такой участник обязан до заключения договора предоставить Заказчику документы, подтверждающие обеспечение исполнения договора в размере в полтора раза превышающем размер обеспечения исполнения договора, указанный в Извещении, а в случае если Извещением обеспечение исполнения договора не было предусмотрено, договор заключается только после предоставления таким победителем, участником обеспечения исполнения договора в размере пяти процентов начальной (максимальной) цены договора, но не менее чем в размере аванса (если договором предусмотрена выплата аванса).  Договор заключается с победителем (единственным участником) закупки на условиях, предусмотренных Извещением и заявкой победителя закупки либо заявкой единственного участника закупки, заявка которого по результатам рассмотрения заявок на участие в закупке признана соответствующей требованиям Извещения.  Страна происхождения поставляемого товара указывается на основании сведений, содержащихся в заявке на участие в закупке, представленной участником закупки, с которым заключается договор.  В случае признания победителя закупки уклонившимся от заключения договора, договор заключается с участником закупки, который предложил такие же, как и победитель закупки условия исполнения договора или предложение которого содержит лучшие условия исполнения договора, следующие после условий, предложенных победителем закупки, который признан уклонившемся от заключения договора.  Участник закупки, признанный победителем закупки в соответствии с абзацем 3 Раздела 41 Извещения, вправе подписать проект договора или направить Заказчику протокол разногласий в сроки, предусмотренные Разделом 40 Извещения, либо отказаться от заключения договора. Одновременно с подписанным договором этот победитель обязан предоставить обеспечение исполнения договора, если требование обеспечения исполнения договора предусмотрено извещением и (или) документацией о конкурентной закупке, абзацем 2 настоящего Раздела Извещения. |
| 43. | **Порядок исполнения, изменения и расторжения договора по результатам закупки:** | Поставщик (подрядчик, исполнитель) в соответствии с условиями договора обязан своевременно предоставлять достоверную информацию о ходе исполнения своих обязательств, в том числе о сложностях, возникающих при исполнении договора, а также к установленному договором сроку представить Заказчику результаты исполнения договора, при этом Заказчик обязан обеспечить их приемку в соответствии с настоящей главой.  Для проверки предоставленных поставщиком (подрядчиком, исполнителем) результатов, предусмотренных договором, в части их соответствия условиям договора Заказчик вправе провести экспертизу. Экспертиза результатов, предусмотренных договором, может проводиться Заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации на основании договоров, заключенных в соответствии с Федеральным законом № 223-ФЗ.  Для проведения экспертизы поставленного товара, выполненной работы или оказанной услуги эксперты, экспертные организации имеют право запрашивать у Заказчика и поставщика (подрядчика, исполнителя) дополнительные материалы, относящиеся к условиям исполнения договора и отдельным этапам исполнения договора. Результаты такой экспертизы оформляются в виде заключения, которое подписывается экспертом, уполномоченным представителем экспертной организации и должно быть объективным, обоснованным и соответствовать законодательству Российской Федерации. В случае, если по результатам такой экспертизы установлены нарушения требований договора, не препятствующие приемке поставленного товара, выполненной работы или оказанной услуги, в заключении могут содержаться предложения об устранении данных нарушений, в том числе с указанием срока их устранения.  По решению Заказчика для приемки результатов договора (его отдельных этапов) может создаваться приемочная комиссия.  Приемка результатов договора (его отдельных этапов) осуществляется в порядке и сроки, установленные договором, и оформляется документом о приемке, либо в те же сроки Заказчик направляет поставщику (подрядчику, исполнителю) письменный мотивированный отказ от подписания такого документа.  Заказчик, приемочная комиссия отказывают в приемке результатов договора в случае несоответствия представленных результатов условиям договора. Допускается приемка результатов отдельного этапа исполнения договора либо поставленного товара, выполненной работы или оказанной услуги в случае выявления несоответствия этих результатов либо этих товара, работы, услуги условиям договора, если выявленное несоответствие не препятствует приемке этих результатов либо этих товара, работы, услуги и устранено поставщиком (подрядчиком, исполнителем).  При исполнении договора, заключенного с участником закупки, которому предоставлен приоритет, не допускается замена страны происхождения товаров, за исключением случая, когда в результате такой замены вместо иностранных товаров поставляются российские товары, при этом качество, технические и функциональные характеристики (потребительские свойства) таких товаров не должны уступать качеству и соответствующим техническим и функциональным характеристикам товаров, указанных в договоре.  **Случаи изменения существенных условий договора:**   1. при снижении цены договора без изменения предусмотренных договором количества товара, объема работы или услуги, качества поставляемого товара, выполняемой работы, оказываемой услуги и иных условий договора; 2. если по предложению Заказчика увеличиваются предусмотренные договором количество товара, объем работы или услуги не более чем на десять процентов или уменьшаются предусмотренные договором количество поставляемого товара, объем выполняемой работы или оказываемой услуги не более чем на десять процентов. При этом по соглашению сторон допускается изменение цены договора пропорционально дополнительному количеству товара, дополнительному объему работы или услуги исходя из установленной в договоре цены единицы товара, работы или услуги, но не более чем на десять процентов цены договора. При уменьшении предусмотренных договором количества товара, объема работы или услуги стороны договора обязаны уменьшить цену договора исходя из цены единицы товара, работы или услуги. Цена единицы дополнительно поставляемого товара или цена единицы товара при уменьшении предусмотренного договором количества поставляемого товара должна определяться как частное от деления первоначальной цены договора на предусмотренное в договоре количество такого товара;   3) изменение в соответствии с законодательством Российской Федерации регулируемых цен (тарифов) на товары, работы, услуги;  4) по согласованию сторон допускается поставка товара, выполнение работы или оказание услуги, качество, эксплуатационные, технические и функциональные характеристики (потребительские свойства) которых являются улучшенными по сравнению с качеством и соответствующими техническими и функциональными характеристиками, указанными в договоре. В этом случае соответствующие изменения должны быть внесены Заказчиком в реестр договоров, заключенных Заказчиком;  5) по согласованию сторон допускается увеличение количества поставляемого товара на сумму, не превышающую разницы между ценой договора, предложенной участником закупки с которым заключен договор, и начальной (максимальной) ценой договора. При этом цена единицы товара не должна превышать цену единицы товара, определяемую как частное от деления цены договора, указанной в заявке участника, на количество товара, указанное в документации о конкурентной закупке;  6) если исполнение заключенного договора, предметом которого является строительство, реконструкция объекта капитального строительства, выполнение работ по сохранению объектов культурного наследия (памятников истории и культуры) народов Российской Федерации, в срок, установленный договором, невозможно в случае возникновения обстоятельств непреодолимой силы, срок исполнения обязательств по такому договору может быть продлен на срок действия таких обязательств без изменения иных условий договора. Для целей настоящего пункта к обстоятельствам непреодолимой силы относятся стихийные бедствия (землетрясение, наводнение, ураган), пожар, массовые заболевания (эпидемии), забастовки, военные действия, террористические акты, диверсии, ограничения перевозок, запретительные меры государства, запрет торговых операций, в том числе с отдельными странами, вследствие принятия международных санкций;  7) если исполнение заключенного договора, предметом которого являются капитальный ремонт, снос, строительство, реконструкция объекта капитального строительства, выполнение работ по сохранению объектов культурного наследия (памятников истории и культуры) народов Российской Федерации, невозможно в срок, установленный договором, по причине возникновения независящих от воли сторон непредвиденных обстоятельств, условия и срок исполнения обязательств по такому договору могут быть изменены на срок действия таких обстоятельств, но не более двенадцати месяцев. Для целей настоящего пункта к непредвиденным обстоятельствам относятся: устранение недостатков, несоответствий в проекте, проектно-сметной документации, научно-проектной документации, выявленных в ходе проведения капитального ремонта, сноса, строительства, реконструкции объекта капитального строительства, выполнения работ по сохранению объектов культурного наследия (памятников истории и культуры) народов Российской Федерации; изъятие или перенос собственником (уполномоченной собственником организацией) неучтенных в проекте, проектно-сметной документации на выполнение работ по капитальному ремонту, сносу строительству, реконструкции объектов капитального строительства, научно-проектной документации на проведение работ по сохранению объектов культурного наследия (памятников истории и культуры) народов Российской Федерации коммуникаций, наличие принятых к производству судами исковых заявлений об оспаривании сноса, переноса и (или) переустройства расположенных в границах строительной площадки объектов капитального строительства, коммуникаций, неучтенных в проектной документации на выполнение работ по строительству, реконструкции объектов капитального строительства, научно-проектной документации на проведение работ по сохранению объектов культурного наследия (памятников истории и культуры) народов Российской Федерации;  8) в случае, если договор заключен на поставку товара, выполнение работ, оказание услуг (по цене за единицу), объем которых невозможно определить и на момент истечения срока действия договора Заказчиком осуществлена оплата за фактически поставленный товар, фактически выполненную работу, оказанную услугу, в размере меньше максимального значения цены договора, Заказчик по соглашению сторон вправе продлить срок действия договора на срок не более шести месяцев;  9) при изменении объема и (или) видов выполняемых работ по договору, предметом которого является выполнение работ по строительству, реконструкции, капитальному ремонту, сносу объекта капитального строительства, проведению работ по сохранению объектов культурного наследия. При этом допускается изменение цены договора не более чем на 10 процентов цены договора;  Расторжение договора допускается по соглашению сторон, по решению суда, в случае одностороннего отказа стороны договора от исполнения договора в соответствии с гражданским законодательством.  Договор может быть расторгнут Заказчиком в одностороннем порядке в случае, если это было предусмотрено документацией о конкурентной закупке и договором.  Заказчик обязан принять решение об одностороннем отказе от исполнения договора, если в ходе исполнения договора установлено, что поставщик (подрядчик, исполнитель) не соответствует установленным извещением о закупке требованиям к участникам закупки или предоставил недостоверную информацию о своем соответствии таким требованиям, что позволило ему стать победителем закупки.  При расторжении договора в одностороннем порядке по вине поставщика (подрядчика, исполнителя) Заказчик обязан предъявить требование об уплате неустоек (штрафов, пеней) в связи с неисполнением или ненадлежащим исполнением обязательств, предусмотренных договором, а также обратиться к поставщику (подрядчику, исполнителю) с требованием о возмещении понесенных убытков при их наличии.  Расторжение договора влечет за собой прекращение обязательств сторон по договору, но не освобождает от ответственности за неисполнение обязательств, которые имели место быть до расторжения договора.  В случае перемены Заказчика права и обязанности Заказчика, предусмотренные договором, переходят к новому Заказчику. |
| 44. | **Внесение изменений в извещение о проведении закупки:** | Заказчик вправе принять решение о внесении изменений в извещение о закупке не позднее даты и времени окончания срока подачи заявок на участие в закупке.  Изменения, внесенные в извещение о закупке, размещаются Заказчиком в ЕИС не позднее чем в течение трех дней со дня принятия решения о внесении указанных изменений, а в случае если Заказчик принял решение о внесении изменений в день окончания срока подачи заявок, изменения, внесенные в извещение о закупке, размещаются в день принятия такого решения. |
| 45. | **Отмена проведения закупки:** | Заказчик, официально разместивший в ЕИС извещение о закупке, вправе отменить ее проведение до наступления даты и времени окончания срока подачи заявок на участие в такой закупке. Решение об отмене закупки размещается в ЕИС в день принятия этого решения. |
| 46. | **Иные условия предмета закупки:** | Установлены в техническом задании, проекте договора, являющихся неотъемлемой частью Извещения. |

**Приложение № 1**

**к Извещению о проведении закупки**

**на оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License путем запроса котировок в электронной форме, участниками которого могут являться только субъекты малого и среднего предпринимательства**

**№ 137-24**

**Техническое задание**

**на** **оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование товара, работ, услуг** | **Ед. изм.** | **Кол-во** | **Начальная (максимальная)\* цена за единицу, руб.** |
| 1 | Оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License \*\*    **Номер предыдущей лицензии 1B08-230808-072313-516-207** | Шт. | 750 | 1 248,84 |

**\* -** Устанавливается в соответствии с Постановлением Правительства РФ от 16.09.2016 № 925 «О приоритете товаров российского происхождения, работ, услуг, выполняемых, оказываемых российскими лицами, по отношению к товарам, происходящим из иностранного государства, работам, услугам, выполняемым, оказываемым иностранными лицами» для расчета приоритета товарам российского происхождения

\*\*- Эквивалент не предусмотрен в связи с тем, что программное обеспечение предназначено для использования в рамках существующей информационной инфраструктуры Заказчика и для обеспечения совместимости и работоспособности уже установленного программного обеспечения.

1. **Характеристика поставляемого товара.**

**1.1 Антивирусные средства должны включать:**

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

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

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

* 1. **Требования ку 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;
* Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise/.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
* фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
* проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
* блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
* распознавания и блокировку фишинговых и небезопасных сайтов;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
* защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
* записи в журнал событий о записи и/или удалении файлов на съемных дисках;
* назначение приоритета для правил доступа к устройствам с файловой системой;
* контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
* защиты от атак типа BadUSB;
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
* управления параметрами через доверенные программы удаленного администрирования;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуска задач по расписанию и/или сразу после запуска приложения;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверки целостности антивирусной программы;
* добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* импорта и экспорта списков правил и исключений в XML-формат;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* защитить паролем восстановление объектов из резервного хранилища;
* ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
* наличие инструмента мониторинга сети по протоколам TCP и UDP;
* возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
* возможность установки ограничение длительности выполнения задачи;
* возможность ставить задачи проверки в очередь, если проверка уже выполняется.
* запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
* восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;
* поддержка двухфакторной аутентификации при полнодисковом шифровании;
* шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);
* наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;
* шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
* возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
* возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
* поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании.
  1. **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.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверки целостности антивирусной программы;
* добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* защитить паролем восстановление объектов из резервного хранилища.
* импорта и экспорта списков правил и исключений в XML-формат;
* ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
* запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
* поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.
* возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
* возможность установки ограничения длительности выполнения задачи;
* возможность ставить задачи проверки в очередь, если проверка уже выполняется.
  1. **Требования к программным средствам антивирусной защиты для рабочих станций Mac**

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

* macOS 10.14 - 12;
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* резидентный антивирусный мониторинг;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* автоматическое обновление антивирусных баз по расписанию;
* резервное копирование зараженных файлов перед их удалением, для возможности восстановления;
* эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
* защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);
* контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault;
* возможность установки расширений из командной строки с помощью новой команды kav;
* возможность задавать исключения при проверке указанных областей на уровне перехватов файловых операций;
* возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены.
  1. **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;
* EMIAS 1.0;
* EulerOS 2.0 SP5;
* LinuxMint 19.2 и выше;
* LinuxMint 20.3 и выше№;
* openSUSE Leap 15.0 и выше;
* Oracle Linux 7.3 и выше;
* Oracle Linux 8.0 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;
* Rocky Linux 8.5 и выше;
* 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;
* ОСОН "ОСНова".
  1. **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;
* Ubuntu 20.04 LTS;
* Альт 8 СП Сервер;
* РЕД ОС 7.3.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* возможность проверки памяти ядра;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plain text);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* включения опции блокирования файлов во время проверки;
* помещение подозрительных и поврежденных объектов на карантин;
* перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
* управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
* проверки съемных дисков;
* отслеживания во входящем сетевом трафике активности, характерной для сетевых атак;
* проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым
* получения данных о действиях программ на компьютере пользователя;
* получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
* создание файлов трассировки при запуске программы;
* получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
* проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;
* сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий.
  1. **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.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
* защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
* непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
* анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* добавлять процессы в список защищаемых;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
* настройки проверки критических областей сервера в качестве отдельной задачи;
* регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
* продолжать антивирусное сканирование в фоновом режиме;
* наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
* ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
* интеграции с SIEM системами;
* указания количества рабочих процессов антивируса вручную;
* отключить графический интерфейс;
* наличие удаленной и локальной консоли управления;
* управления параметрами антивируса из командной строки;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
* включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.
* контроль устройств, в том числе сетевых карт и модемов;
* веб-контроль;
* защита от почтовых угроз (плагин для Outlook);
* защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп);
* создания специальных правил должно контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
* создания специальных правил должно работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должно иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
* осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем;
* информирование администратора о подключении внешних устройств;
* наличие механизмов автоматической генерации правил для контроля устройств и приложений;
  1. **Требования к программным средствам антивирусной защиты мобильных устройств**

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

* Android 5.0–13 (включая Android 12L, исключая Go Edition);
* iOS 10–16 или iPadOS 13–15;
  1. **В программном средстве антивирусной защиты смартфонов для ОС Android должны быть реализованы следующие функциональные возможности:**
* постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
* проверка файловой системы устройства по требованию и по расписанию;
* мгновенная проверка устанавливаемых приложений
* блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* наличие хранилища для изолирования зараженных объектов;
* обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
* блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
* поддержка белых списков разрешенных приложений;
* блокировка системных приложений, в рамках контроля запуска приложений;
* отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);
* заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
* указать параметры подключения к wi-fi сетям;
* указать обязательные к установке приложения;
* блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
* создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
* поддержка технологий Samsung KNOX1 и KNOX2.
  1. **В программном средстве защиты смартфонов для ОС Apple iOS должны быть реализованы следующие функциональные возможности:**
* удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
* отправки команды блокирования и удаления данных;
* создавать групповые политики безопасности мобильных устройств;
* удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;
* получать отчеты и статистику о работе мобильных устройств пользователей;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;
* централизованного управления с помощью единой консоли управления;
* наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.
  1. **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:

* Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 11 Home 64-разрядная;
* Microsoft Windows 11 Pro 64-разрядная;
* Microsoft Windows 11 Enterprise 64-разрядная;
* Microsoft Windows 11 Education 64-разрядная;
* Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;
* Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;
* Microsoft Windows 8 Pro 32-разрядная/64-разрядная;
* Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
* Microsoft Windows 7 Professional Service Pack 1 32-разрядная/64-разрядная;
* Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная;
* 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.
  1. **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 (требуются дополнительные действия);
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия);
* 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 10.5.x 32-разрядная/64-разрядная;
* MariaDB 10.4.x 32-разрядная/64-разрядная;
* MariaDB 10.3.22 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;
* MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
* автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
* указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* иерархии триггеров, по которым происходит перераспределение;
* тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* инвентаризация установленного ПО и оборудования на компьютерах пользователей;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер Exchange ActiveSync;
* функция управления мобильными устройствами через сервер iOS MDM;
* отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* интеграции по OpenAPI;
* управления антивирусной защитой с использованием WEB консоли;
* возможность управления развертыванием ОС Windows через консоль управления;
* наличие преднастроенных ролей пользователей средств централизованного управления;
* должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
* возможность подключения по RDP или штатными средствами из консоли управления;
* наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing);
* пользователю должен выводиться запрос на разрешение дистанционного подключения;
* наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal);
* должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
* возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС;
* возможность импортировать образ операционной системы из дистрибутивов (WIM)
* наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;
* автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры;
* поддержка функциональности управления шифрованием данных;
* возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF
* двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
* использования дополнительной аутентификация после изменения параметров учетной записи пользователя.
* возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами.
* автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
* возможность развернуть Сервер администрирования как систему высокой доступности;
* возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети.
  1. **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 11.х (Bullseye) 32-разрядная/64-разрядная;
* Debian GNU/Linux 10.х (Buster) 32-разрядная/64-разрядная;
* Debian GNU/Linux 9.х (Stretch) 32-разрядная/64-разрядная;
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
* Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная;
* CentOS 7.x 64-разрядная;
* Red Hat Enterprise Linux Server 8.x 64-разрядная;
* Red Hat Enterprise Linux Server 7.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 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Astra Linux Common Edition 2.12 64-разрядная;
* Альт Сервер 10 64-разрядная;
* Альт Сервер 9.2 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;
* 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 10.5.x 32-разрядная/64-разрядная;
* MariaDB 10.4.x 32-разрядная/64-разрядная;
* MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* иерархии триггеров, по которым происходит перераспределение;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* наличие системы контроля возникновения вирусных эпидемий;
* управления антивирусной защитой с использованием WEB консоли;
* возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
* возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
* возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули.
  1. **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.

1. **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.

1. **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.

1. **Требование к сертификации:** Программное обеспечение должно иметь сертификат соответствия требованиям безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации.
2. **Гарантийный срок:** Срок действия неисключительного права на использование и воспроизведение программного обеспечения должен составлять не менее 12 месяцев.
3. Продление неисключительных прав на антивирусное программное обеспечение должно сопровождаться оформленными в соответствии с законодательством Российской Федерации сертификатами, соглашениями, свидетельствами, подтверждающими их оригинальность.
4. Лицензиат должен предоставить документы, подтверждающие его полномочия на продление неисключительных прав антивирусного программного обеспечения и обслуживание этих программ в Российской Федерации. Если Лицензиат не является производителем антивирусного программного обеспечения, то он должен предоставить копии дистрибьюторских или дилерских соглашений, копии писем производителей продукции, предоставляющие Лицензиат право на продление неисключительных прав антивирусного программного обеспечения. Авторизация и статус могут подтверждаться сертификатами от производителей.
5. Продление неисключительных прав на антивирусное программное обеспечение должно сопровождаться информационной и технической поддержкой по вопросам лицензирования, активации, установки этого антивирусного программного продукта на период действия лицензий.
6. Лицензиат должен предоставить продление неисключительных прав на антивирусное программное обеспечение, в полном объеме.
7. Неисключительные права на использование программного обеспечения переходят к Сублицензиату с момента получения от Лицензиату ключевого файла и лицензионного соглашения (бумажный вариант) действуют в течение 1 года с момента активации ключевого файла.
8. При выявлении недостатков носителя информации, Лицензиат своими силами и средствами, безвозмездно исправляет их в указанные сроки по требованию Сублицензиата.
9. Программное обеспечение должно быть передано Заказчику в запечатанных конвертах. Программное обеспечение поставляется в упаковке, обеспечивающей его целостность и сохранность. Носитель информации и упаковка должны быть маркированы в соответствии с требованиями, предъявляемыми к маркировке данного продукта. Ключевой файл антивирусного программного обеспечения предоставляется на отдельном компакт-диске (CD, DVD), лицензионное соглашение предоставляется на бумажном носителе.
10. Форму сублицензионного договора предоставляет Исполнитель.

**Приложение № 2**

**к Извещению о проведении закупки**

**на оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License путем запроса котировок в электронной форме, участниками которого могут являться только субъекты малого и среднего предпринимательства**

**№ 137-24**

**ПРОЕКТ**

Договор № 137-24

**на оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License**

**г. Иркутск «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г.**

**Областное государственное автономное учреждение здравоохранения «Иркутская городская клиническая больница № 8»**, именуемое в дальнейшем **Заказчик,** в лице главного врача Есевой Жанны Владимировны, действующего на основании Устава, с одной стороны, и **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** именуемый в дальнейшем **Исполнитель,** в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**,** действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, в дальнейшем совместно именуемые Стороны, на основании результатов определения Исполнителя путем проведения запроса котировок в электронной форме, участниками которого могут являться только субъекты малого и среднего предпринимательства (протокол \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_ от \_\_\_\_\_\_\_\_\_\_\_\_\_), заключили настоящий Договор о нижеследующем:

1. **Предмет договора**
   1. Исполнитель обязуется осуществить оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License в количестве и по ценам, указанным в спецификации (Приложение № 1), Заказчик обязуется принять и оплатить услуги.

1.2. Место оказания Услуг: г. Иркутск, ул. Баумана 214а/1 (каб. 422)

1.3. Оказание Услуг осуществляется Исполнителем в соответствии с законодательством Российской Федерации, требованиями иных нормативных правовых актов, регулирующих порядок предоставления такого вида Услуг, устанавливающих требования к качеству такого вида Услуг, в соответствии с условиями договора.

1.4. Срок оказания услуг (включая срок передачи прав на использовании ПО): 20 календарных дней с даты подписания договора.

# Цена договора и порядок расчетов

2.1. Цена настоящего договора составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ руб. \_\_ коп. (прописью) и включает трудозатраты, затраты на средства для оказания услуг, НДС (в случае, если Исполнитель является плательщиком НДС), стоимость материалов и средств, необходимых для оказания услуг, транспортные расходы, а также расходы на страхование, уплату налогов, таможенных пошлин, сборов и другие обязательные платежи, предусмотренные настоящим договором, является твердой и определяется на весь срок исполнения договора, то есть является конечной.

2.2. Оплата производится за фактически оказанные услуги на основании счета и подписанного сторонами акта об оказанных услугах, путем перечисления денежных средств на расчетный счет Исполнителя в течение 7 (семи) рабочих дней с момента подписания акта за оказанные услуги. Днем оплаты является день списания денежных средств с расчетного счета Заказчика.

2.3. Цена договора может быть снижена без изменения предусмотренных договором количества услуг, качества поставляемого оказываемой услуги и иных условий договора по соглашению сторон.

2.4. В случае изменения потребности Заказчика предусмотренные договором объемы услуг могут быть увеличены или уменьшены, но не более чем на десять процентов. При этом по соглашению сторон допускается изменение цены договора пропорционально дополнительному объему услуг исходя из установленной в договоре цены единицы услуги, но не более чем на десять процентов цены договора. При уменьшении предусмотренных договором объема услуг стороны договора обязаны уменьшить цену договора исходя из цены единицы услуги.

2.5. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных настоящим Договором, Заказчик вправе производить оплату оказанных услуг за вычетом соответствующего размера неустойки (штрафа, пени), предусмотренных разделом 6 настоящего Договора.

1. **Обязанности Сторон**

**3.1. Исполнитель обязан:**

3.1.1. Своевременно и надлежащим образом оказать услуги в соответствии со спецификацией (Приложение № 1 к договору).

3.1.2. Представить по письменному запросу Заказчика в сроки, указанные в таком запросе, информацию о ходе исполнения обязательств, в том числе о сложностях, возникающих при исполнении договора.

3.1.3. Обеспечивать соответствие оказываемых услуг требованиям качества, безопасности (санитарным нормам и правилам, государственным стандартам, техническим регламентам, а также иным требованиям), в случае, если данные требования установлены законодательством Российской Федерации.

3.1.4. Исполнитель обязан в течение срока действия договора предоставить по запросу Заказчика в течение одного рабочего дня после дня получения указанного запроса документы, подтверждающие соответствие указанным выше требованиям.

3.1.5. Обеспечить устранение недостатков и дефектов, выявленных при приемке результатов оказанных услуг, за свой счет.

3.1.6. Приостановить оказание услуг в случае обнаружения независящих от Исполнителя обстоятельств, которые могут оказать негативное влияние на годность или прочность результатов оказываемых услуг или создать невозможность их завершения в установленный договором срок, и сообщить об этом Заказчику в течение одного рабочего дня после приостановления оказания услуг.

3.1.7. В течение 1 (одного) рабочего дня информировать Заказчика о невозможности оказать услуги в надлежащем объеме, в предусмотренные договором сроки, надлежащего качества с указанием причин.

**3.2. Заказчик обязан:**

3.2.1. Обеспечить своевременную приемку оказанных услуг и провести экспертизу для проверки предоставленных Исполнителем результатов оказанных услуг, предусмотренных договором в части их соответствия условиям договора.

3.2.2. Сообщать в письменной форме Исполнителю о недостатках, обнаруженных в ходе оказания услуг, в течение 2 (двух) рабочих дней после обнаружения таких недостатков.

3.2.3. Своевременно принять и оплатить надлежащим образом оказанные услуги в соответствии с договором.

3.2.4. При получении от Исполнителя уведомления о приостановлении оказания услуг в случае, указанном в подпункте 3.1.6. договора, рассмотреть вопрос о целесообразности и порядке продолжения оказания услуг. Решение о продолжении оказания Услуг при необходимости корректировки сроков оказания услуг принимается Заказчиком и Исполнителем совместно и оформляется дополнительным соглашением к договору.

1. **Порядок приемки услуг.**

4.1. Приемка услуг по настоящему Договору оформляется актом об оказании услуг. По решению Заказчика для приемки результатов оказания услуг по Договору (его отдельных этапов) может создаваться приемочная комиссия. Исполнитель в соответствии с условиями Договора обязан своевременно предоставлять достоверную информацию о ходе исполнения своих обязательств, в том числе о сложностях, возникающих при исполнении Договора, а также к установленному Договором сроку представить Заказчику результаты оказания услуг при исполнении Договора, при этом Заказчик обязан обеспечить их приемку. Для проверки предоставленных Исполнителем результатов оказания услуг, предусмотренных Договором, в части их соответствия условиям Договора Заказчик вправе провести экспертизу. Экспертиза результатов оказания услуг, предусмотренных Договором, может проводиться Заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации на основании Договоров, заключенных в соответствии с Федеральным законом от 18.07.2011 № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц». Для проведения экспертизы оказанных услуг эксперты, экспертные организации имеют право запрашивать у Заказчика и Исполнителя дополнительные материалы, относящиеся к условиям исполнения Договора и отдельным этапам исполнения Договора. Результаты такой экспертизы оформляются в виде заключения, которое подписывается экспертом, уполномоченным представителем экспертной организации и должно быть объективным, обоснованным и соответствовать законодательству Российской Федерации. В случае, если по результатам такой экспертизы установлены нарушения требований Договора, не препятствующие приемке оказанных услуг, в заключении могут содержаться предложения об устранении данных нарушений, в том числе с указанием срока их устранения.

4.2. Заказчик в течение 5 (пяти) рабочих дней с момента получения от Исполнителя акта об оказании услуг обязан принять услуги и направить Исполнителю подписанный акт об оказании услуг или мотивированный отказ от их приемки. Заказчик, приемочная комиссия отказывают в приемке результатов договора в случае несоответствия представленных результатов условиям договора. Допускается приемка результатов отдельного этапа исполнения договора либо поставленного товара, выполненной работы или оказанной услуги в случае выявления несоответствия этих результатов либо этих товара, работы, услуги условиям договора, если выявленное несоответствие не препятствует приемке этих результатов либо этих товара, работы, услуги и устранено поставщиком (подрядчиком, исполнителем).

Допускается приемка услуг, качество, технические и функциональные характеристики (потребительские свойства) которых являются улучшенными по сравнению с качеством и соответствующими техническими и функциональными характеристиками, указанными в Извещении.

4.3. В случае мотивированного отказа Заказчика от приёмки услуг Сторонами составляется акт выявленных недостатков с перечнем выявленных недостатков и сроками их устранения. При этом указанные в акте недостатки Исполнитель обязан устранить своими силами и за счет собственных средств, после чего сдать работы Заказчику в порядке, предусмотренном настоящим разделом Договора.

1. **Ответственность сторон**

5.1. За неисполнение или ненадлежащее исполнение своих обязательств по настоящему договору, Стороны несут ответственность в соответствии с действующим законодательством РФ и настоящим договором.

5.2. За ненадлежащее исполнение или неисполнение обязательств, предусмотренных пп. 3.1.1., 3.1.3., 3.1.5., 3.1.6. настоящего договора, Исполнитель обязан уплатить штраф в размере 1% от стоимости невыполненных или ненадлежаще выполненных обязательств.

5.3. В случае нарушения сроков оплаты, предусмотренных п. 2.2. настоящего договора, Заказчик уплачивает Исполнителю пеню в размере одной трехсотой действующей на день уплаты пени ключевой ставки ЦБ РФ за каждый день просрочки исполнения обязательства, начиная со дня, следующего после дня истечения сроков, установленных п. 2.2. настоящего договора, до момента полного исполнения обязательства.

5.4. В случае нарушения Исполнителем сроков, предусмотренных пп. 1.4., 3.1.2, 3.1.4., 3.1.7. настоящего Договора, Исполнитель уплачивает Заказчику неустойку в размере 0,1% от стоимости невыполненных обязательств за каждый день просрочки до момента полного исполнения обязательств, начиная со дня, следующего после дня истечения сроков, установленных соответствующими пунктами раздела 3 настоящего Договора.

5.5. Уплата неустойки не освобождает Исполнителя от выполнения своих обязательств по настоящему договору.

**6. Обеспечение исполнения договора**

6.1. Размер обеспечения исполнения договора составляет \_\_\_\_\_\_\_\_\_\_\_ рублей.

6.2. Исполнение Договора обеспечивается предоставлением независимой гарантии или внесением денежных средств на счет Заказчика. Способ обеспечения исполнения Договора определяется Исполнителем самостоятельно.

6.3. В случае если исполнение обязательств Исполнителя по настоящему Договору обеспечивается внесением денежных средств, то Заказчик возвращает Исполнителю обеспечение исполнения Договора в течение 30 (тридцати) календарных дней с момента получения соответствующего письменного требования Заказчиком при условии выполнения Исполнителем обязательств по Договору.

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

6.5. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств по Договору обеспечение исполнения договора переходит Заказчику в размере неисполненных обязательств.

6.6. Обеспечение исполнения договора сохраняет свою силу при изменении законодательства Российской Федерации, а также при реорганизации Исполнителя или Заказчика.

6.7. Все затраты, связанные с заключением и оформлением договоров и иных документов по обеспечению исполнения Договора, несет Исполнитель.

**7. Действие непреодолимой силы**

7.1. Стороны, не исполнившие или ненадлежащим образом исполнившие обязательства по настоящему договору, освобождаются от ответственности, если докажут, что надлежащее исполнение обязательств по настоящему договору оказалось невозможным вследствие наступления обстоятельств непреодолимой силы. При этом сроки выполнения обязательств по настоящему договору соразмерно продлеваются на срок действия указанных обстоятельств.

7.2. Каждая из сторон обязана письменно сообщить о наступлении обстоятельств непреодолимой силы не позднее 10 (десяти) рабочих дней с начала их действия.

7.3. Не уведомление либо несвоевременное уведомление о наступлении обстоятельств непреодолимой силы не дает Сторонам право ссылаться при невозможности выполнить свои обязанности по настоящему договору на наступление таких обстоятельств.

**8. Рассмотрение споров**

8.1. Все споры или разногласия, возникшие между сторонами по настоящему договору и в связи с ним, разрешаются путем переговоров между ними.

8.2. В случае невозможности разрешения споров или разногласий путем переговоров, они подлежат рассмотрению в Арбитражном суде Иркутской области в установленном законодательством РФ порядке.

**9. Срок действия договора.**

9.1. Договор вступает в силу с момента подписания его Сторонами и действует до полного исполнения сторонами обязательств по настоящему договору.

**10. Прочие условия**

10.1. Взаимоотношения Сторон, не урегулированные настоящим Договором, регулируются действующим законодательством.

10.2. Настоящий Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

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

10.4. Заказчик обязан принять решение об одностороннем отказе от исполнения договора, если в ходе исполнения договора установлено, что Исполнитель не соответствует установленным документацией о закупке требованиям к участникам закупки или предоставил недостоверную информацию о своем соответствии таким требованиям, что позволило ему стать победителем закупки.

10.5. При расторжении договора в одностороннем порядке по вине Исполнителя Заказчик обязан предъявить требование об уплате неустоек (штрафов, пеней) в связи с неисполнением или ненадлежащим исполнением обязательств, предусмотренных договором, а также обратиться к Исполнителю с требованием о возмещении понесенных убытков при их наличии.

10.6. Расторжение договора влечет за собой прекращение обязательств сторон по договору, но не освобождает от ответственности за неисполнение обязательств, которые имели место быть до расторжения договора.

10.7. К настоящему Договору прилагается и является его неотъемлемой частью

*- Спецификация (Приложение № 1)*

*- Техническое задание (Приложение № 2)*

**11. Юридические адреса, банковские реквизиты и подписи сторон:**

|  |  |
| --- | --- |
| **Заказчик:**  **ОГАУЗ «ИГКБ № 8»**  **Адрес:** 664048, г. Иркутск, ул. Ярославского, 300  **Телефон** 55-14-51, 50-24-90,50-07-38  ИНН 3810009342  КПП 381001001  Минфин Иркутской области (ОГАУЗ «Иркутская городская клиническая больница № 8», л/с 80303090207, л/с 80303050207)  Казначейский счет 03224643250000003400  Банковский счет 40102810145370000026  Наименование банка: Отделение Иркутск//УФК по Иркутской области, г. Иркутск  БИК 012520101  [info@gkb8.ru](mailto:info@gkb8.ru)  **Главный врач**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Ж.В. Есева/**  **М.П.** | **Исполнитель:**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/**  **М.П.** |

Приложение № 1

к договору № 137-24  
от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**СПЕЦИФИКАЦИЯ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование услуг** | **Характеристика услуг** | **Ед.изм.** | **Кол-во** | **Цена за ед., руб.** | **Сумма с НДС, руб.** |
| 1 | Оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License  **Номер предыдущей лицензии 1B08-220725-075536-563-1978** | Указаны в Техническом задании (Приложение № 2) | Шт. | 750 |  |  |
|  | ИТОГО (цена договора): | | |  | | |
|  | В т.ч. НДС (если участник закупки является плательщиком НДС) | | |  | | |

|  |  |  |
| --- | --- | --- |
| Заказчик:  ОГАУЗ «ИГКБ № 8»  Главный врач  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Ж.В. Есева/  М.П. |  | Исполнитель:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_ /  М.П. |

Приложение № 2

к договору № 137-24  
от \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**Техническое задание**

**на оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License**

1. **Характеристика поставляемого товара.**

**1.1 Антивирусные средства должны включать:**

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

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

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

* 1. **Требования ку 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;
* Windows 11 Home / Pro / Pro для рабочих станций / Education / Enterprise/.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика, передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;
* фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;
* проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;
* блокировку баннеров и всплывающих окон на загружаемых Web-страницах;
* распознавания и блокировку фишинговых и небезопасных сайтов;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;
* защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;
* записи в журнал событий о записи и/или удалении файлов на съемных дисках;
* назначение приоритета для правил доступа к устройствам с файловой системой;
* контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;
* защиты от атак типа BadUSB;
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;
* управления параметрами через доверенные программы удаленного администрирования;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуска задач по расписанию и/или сразу после запуска приложения;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверки целостности антивирусной программы;
* добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* импорта и экспорта списков правил и исключений в XML-формат;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* защитить паролем восстановление объектов из резервного хранилища;
* ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
* наличие инструмента мониторинга сети по протоколам TCP и UDP;
* возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
* возможность установки ограничение длительности выполнения задачи;
* возможность ставить задачи проверки в очередь, если проверка уже выполняется.
* запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.
* полнодисковое шифрование с созданием специального загрузочного агента и поддержкой технологии Single Sign On, поддержка UEFI-систем;
* восстановления зашифрованного содержимого в случае сбоев загрузочного агента или файлов ОС, поддержка UEFI-систем;
* поддержка двухфакторной аутентификации при полнодисковом шифровании;
* шифрование файлов с возможностью гибкого указания шифруемого контента (по местоположению, по расширению, по создающему файл приложению);
* наличие механизмов ограничения доступа к зашифрованным файлам со стороны выбранных приложений, а также наличие технологии, позволяющей расшифровывать файлы за пределами организации с помощью пароля;
* шифрование данных на съемных носителях с возможностью задания режима работы, позволяющего шифровать и расшифровывать файлы за пределами сети организации;
* возможность формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий)
* возможность создавать служебную учетную запись агента аутентификации при шифровании диска;
* поддержка стороннего поставщика учетных данных ADSelfService Plus для работы SSO при полнодисковом шифровании.
  1. **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.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* антивирусное сканирование в режиме реального времени и по запросу из контекстного меню объекта;
* антивирусное сканирование по расписанию;
* антивирусное сканирование подключаемых устройств;
* эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;
* нейтрализации действий активного заражения;
* анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;
* анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;
* откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;
* облачной защиты от новых угроз, позволяющая приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусной проверки и лечения файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;
* встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;
* защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;
* защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля, позволяющая избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;
* установки только выбранных компонентов программного средства антивирусной защиты;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверки целостности антивирусной программы;
* добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;
* наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;
* наличие защищенного хранилища для отчетов о работе антивируса;
* включения и выключения графического интерфейса антивируса, а также наличие упрощенной версии графического интерфейса, с минимальным набором возможностей;
* интеграции с Windows Defender Security Center;
* наличие поддержки Antimalware Scan Interface (AMSI);
* наличие поддержки Windows Subsystem for Linux (WSL);
* защитить паролем восстановление объектов из резервного хранилища.
* импорта и экспорта списков правил и исключений в XML-формат;
* ограничения сетевого трафика в том случае, если подключение к интернету является лимитным;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;
* формирования шаблона поведения программ и блокировки их действий, при отклонении от шаблона поведения (адаптивный контроль аномалий);
* запуск специальной задачи для обнаружения и закрытия уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;
* поддержка компонентов Защита от веб-угроз, Защита от почтовых угроз, Веб-Контроль и Контроль устройств для компьютеров под управлением операционной системы Windows для серверов.
* возобновление задачи проверки после перезагрузки с того же места, где проверка была прервана;
* возможность установки ограничения длительности выполнения задачи;
* возможность ставить задачи проверки в очередь, если проверка уже выполняется.
  1. **Требования к программным средствам антивирусной защиты для рабочих станций Mac**

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

* macOS 10.14 - 12;
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* резидентный антивирусный мониторинг;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* автоматическое обновление антивирусных баз по расписанию;
* резервное копирование зараженных файлов перед их удалением, для возможности восстановления;
* эвристический анализатор, позволяющий распознавать и блокировать ранее неизвестные вредоносные программы;
* защита от сетевых атак с использованием системы обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* проверку сетевого трафика, передаваемого через браузеры Safari, Google Chrome и Firefox (HTTP и HTTPS трафик);
* контроль работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к определенным ресурсам или категорий ресурсов, созданных и динамически обновляемых производителем
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления с возможностью управлять шифрованием FileVault;
* возможность установки расширений из командной строки с помощью новой команды kav;
* возможность задавать исключения при проверке указанных областей на уровне перехватов файловых операций;
* возможность автоматически отслеживать появление прав полного доступа к диску и выполнять установку необходимых системных расширений, как только права будут предоставлены.
  1. **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;
* EMIAS 1.0;
* EulerOS 2.0 SP5;
* LinuxMint 19.2 и выше;
* LinuxMint 20.3 и выше№;
* openSUSE Leap 15.0 и выше;
* Oracle Linux 7.3 и выше;
* Oracle Linux 8.0 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;
* Rocky Linux 8.5 и выше;
* 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;
* ОСОН "ОСНова".
  1. **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;
* Ubuntu 20.04 LTS;
* Альт 8 СП Сервер;
* РЕД ОС 7.3.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* резидентного антивирусного мониторинга;
* облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;
* проверку ресурсов доступных по SMB / NFS;
* возможность проверки памяти ядра;
* эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;
* проверку сообщений электронной почты в текстовом формате (Plain text);
* наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);
* защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;
* включения опции блокирования файлов во время проверки;
* помещение подозрительных и поврежденных объектов на карантин;
* перехвата и проверки файловых операций на уровне SAMBA;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* экспортировать и сохранять отчеты в форматах HTML и CSV;
* гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;
* сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;
* управления через пользовательский графический интерфейс без root прав;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления или веб-консоли;
* управления доступом пользователей к установленным или подключенным к компьютеру устройствам по типам устройства и шинам подключения;
* проверки съемных дисков;
* отслеживания во входящем сетевом трафике активности, характерной для сетевых атак;
* проверки трафика, поступающего на компьютер пользователя по протоколам HTTP/HTTPS и FTP, а также возможность устанавливать принадлежность веб-адресов к вредоносным или фишинговым
* получения данных о действиях программ на компьютере пользователя;
* получения информации обо всех исполняемых файлах программ, хранящихся на компьютерах (задача Инвентаризация);
* создание файлов трассировки при запуске программы;
* получение информации обо всех исполняемых файлах программ, установленных на компьютерах;
* проверку объектов автозапуска, загрузочные секторы, память процессов и память ядра;
* сохранение резервных копий файлов перед лечением или удалением и восстановление файлов из резервных копий.
  1. **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.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* антивирусное сканирование в режиме реального времени и по запросу на серверах, выполняющих разные функции: серверов терминалов, принт-серверов, серверов приложений и контроллеров доменов, файловых серверов;
* антивирусное сканирование по команде пользователя или администратора и по расписанию;
* запуск задач по расписанию и/или сразу после загрузки операционной системы;
* облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;
* антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB;
* защита файлов, альтернативных потоков файловых систем (NTFS-streams), загрузочной записи, загрузочных секторов локальных и съемных дисков;
* непрерывное отслеживание попыток выполнения на защищаемом сервере скриптов VBScript и JScript, созданных по технологиям Microsoft Windows Script Technologies (или Active Scripting), проверка программного кода скриптов и автоматически запрещение выполнение тех из них, которые признаются опасными.
* анализ обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;
* проверки контейнеров Microsoft Windows;
* защиты от эксплуатирования уязвимостей в памяти процессов;
* должна быть возможность автоматически завершать скомпрометированные процессы, при этом критические системные процессы не должны завершаться;
* добавлять процессы в список защищаемых;
* ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;
* проверка собственных модулей на возможное нарушение их целостности посредством отдельной задачи;
* настройки проверки критических областей сервера в качестве отдельной задачи;
* регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач;
* продолжать антивирусное сканирование в фоновом режиме;
* наличие множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);
* ролевой доступ к параметрам приложения и службе с помощью списков разрешений, позволяющий избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей, а также запрещающий или разрешающий управление антивирусом;
* интеграции с SIEM системами;
* указания количества рабочих процессов антивируса вручную;
* отключить графический интерфейс;
* наличие удаленной и локальной консоли управления;
* управления параметрами антивируса из командной строки;
* централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;
* управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;
* защита от сетевых угроз обеспечивающая анализ входящего трафика на наличие признаков сетевых атак;
* включение или выключение защиты процессов программы от внешних угроз (по умолчанию функция включена). При включенной функции программа защищает собственные процессы, а также процессы Агента администрирования от вмешательства сторонних процессов.
* контроль устройств, в том числе сетевых карт и модемов;
* веб-контроль;
* защита от почтовых угроз (плагин для Outlook);
* защищать HTTP и HTTPS трафик от вирусов и фишинга, с проверкой ссылок базам вредоносных веб-адресов и возможностью проверки валидности сертификатов веб-серверов, перехват трафика должен осуществляться с помощью драйвера перехвата или же с помощью его перенаправления;
* создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или же для определенных групп пользователей (Active Directory или локальных пользователей/групп);
* создания специальных правил должно контролировать приложения по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме;
* создания специальных правил должно работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки, должно иметь возможность создания списка доверенных пакетов обновлений, которые могут изменять и запускать вложенные в них файлы;
* осуществление контроля работы пользователя с внешними устройствами ввода/вывода, с возможностью создания списка доверенных устройств и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;
* осуществление контроля работы с сетью Интернет, в том числе включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории заранее созданной и динамически обновляемой производителем;
* информирование администратора о подключении внешних устройств;
* наличие механизмов автоматической генерации правил для контроля устройств и приложений;
  1. **Требования к программным средствам антивирусной защиты мобильных устройств**

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

* Android 5.0–13 (включая Android 12L, исключая Go Edition);
* iOS 10–16 или iPadOS 13–15;
  1. **В программном средстве антивирусной защиты смартфонов для ОС Android должны быть реализованы следующие функциональные возможности:**
* постоянная антивирусная защита файловой системы смартфона, с дополнительным уровнем проверки с использованием облачного репутационного сервиса производителя антивирусных средств защиты;
* проверка файловой системы устройства по требованию и по расписанию;
* мгновенная проверка устанавливаемых приложений
* блокировки вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты;
* наличие хранилища для изолирования зараженных объектов;
* обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов, по расписанию;
* блокировка запуска указанных приложений, в том числе с помощью заранее заданных категорий приложений;
* поддержка белых списков разрешенных приложений;
* блокировка системных приложений, в рамках контроля запуска приложений;
* отправки команд и push уведомлений через сервис Firebase Cloud Messaging (FCM);
* заблокировать wi-fi и bluetooth модули, а также использование камеры мобильного устройства;
* указать параметры подключения к wi-fi сетям;
* указать обязательные к установке приложения;
* блокировки мобильного устройства, удаление данных, удаление данных связанных с рабочей деятельностью, получение координат местоположения устройства, удаленного возврата к заводским настройкам (factory reset);
* создания списка правил на основе которых будет осуществляться проверка мобильного устройства на соответствие корпоративным политикам с возможностью автоматической блокировки устройства, удаления данных, запрета запуска корпоративных приложений при выявлении несоответствий;
* поддержка технологий Samsung KNOX1 и KNOX2.
  1. **В программном средстве защиты смартфонов для ОС Apple iOS должны быть реализованы следующие функциональные возможности:**
* удаленной настройки параметров iOS MDM-устройств с помощью групповых политик;
* отправки команды блокирования и удаления данных;
* создавать групповые политики безопасности мобильных устройств;
* удаленно настраивать конфигурационные параметры устройств, подключенных по протоколу Exchange ActiveSync\ iOS MDM;
* получать отчеты и статистику о работе мобильных устройств пользователей;
* блокировка вредоносных и фишинговых сайтов на основе вердиктов репутационных облачных сервисов производителя антивирусных средств защиты, при использовании supervised mode;
* централизованного управления с помощью единой консоли управления;
* наличие компонента, который позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.
  1. **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:

* Microsoft Windows 10 Enterprise 2015 LTSB 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 2016 LTSB 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 2019 LTSC 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 19H1 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций 19H1 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 19H1 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 19H1 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 19H2 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro для рабочих станций 19H2 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 19H2 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 19H2 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 20H1 (May 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 20H2 (October 2020 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 21H1 (May 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Home 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Pro 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Enterprise 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 10 Education 21H2 (October 2021 Update) 32-разрядная/64-разрядная;
* Microsoft Windows 11 Home 64-разрядная;
* Microsoft Windows 11 Pro 64-разрядная;
* Microsoft Windows 11 Enterprise 64-разрядная;
* Microsoft Windows 11 Education 64-разрядная;
* Microsoft Windows 8.1 Pro 32-разрядная/64-разрядная;
* Microsoft Windows 8.1 Enterprise 32-разрядная/64-разрядная;
* Microsoft Windows 8 Pro 32-разрядная/64-разрядная;
* Microsoft Windows 8 Enterprise 32-разрядная/64-разрядная;
* Microsoft Windows 7 Professional Service Pack 1 32-разрядная/64-разрядная;
* Microsoft Windows 7 Enterprise/Ultimate Service Pack 1 32-разрядная/64-разрядная;
* 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.
  1. **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 (требуются дополнительные действия);
* Microsoft SQL Server 2019 (все редакции) для Linux 64-разрядная (требуются дополнительные действия);
* 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 10.5.x 32-разрядная/64-разрядная;
* MariaDB 10.4.x 32-разрядная/64-разрядная;
* MariaDB 10.3.22 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;
* MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* выбор архитектуры установки централизованного средства управления, мониторинга и обновления в зависимости от количества защищаемых узлов;
* чтения информации из Active Directory, с целью получения данных об учетных записях компьютеров и пользователей в организации;
* настройки правил переноса обнаруженных компьютеров по ip-адресу, типу ОС, нахождению в OU AD;
* автоматическое распределение учетных записей компьютеров по группам управления, в случае появления новых компьютеров в сети; Возможность настройки правил переноса по ip-адресу, типу ОС, нахождению в OU AD;
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* централизованное удаление (ручное и автоматическое) несовместимых приложений средствами центра управления;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* наличие различных методов установки антивирусных агентов: для удаленной установки - RPC, GPO, средствами системы управления, для локальной установки – возможность создать автономный пакет установки;
* указания в политиках безопасности специальных триггеров, которые переопределяют настройки антивирусного решения в зависимости от учетной записи, под которой пользователь вошел в систему, текущего IPv4-адреса, а также от того, в каком OU находится компьютер или в какой группе безопасности;
* иерархии триггеров, по которым происходит перераспределение;
* тестирование загруженных обновлений средствами ПО централизованного управления перед распространением на клиентские машины;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* инвентаризация установленного ПО и оборудования на компьютерах пользователей;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* функция управления мобильными устройствами через сервер Exchange ActiveSync;
* функция управления мобильными устройствами через сервер iOS MDM;
* отправки SMS-оповещений о заданных событиях;
* централизованная установка сертификатов на управляемые мобильные устройства;
* указания любого компьютера организации центром ретрансляции обновлений для снижения сетевой нагрузки на систему управления;
* указания любого компьютера организации центром пересылки событий антивирусных агентов, выбранной группы клиентских компьютеров, серверу централизованного управления для снижения сетевой нагрузки на систему управления;
* построение графических отчетов по событиям антивирусной защиты, данным инвентаризации, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* поддержка Windows Failover Clustering;
* поддержка интеграции с Windows сервисом Certificate Authority;
* наличие портала самообслуживания пользователей;
* портал самообслуживания должен обеспечивать возможность подключения пользователей с целью установки агента управления на мобильное устройство, просмотр мобильных устройств, отправки команд блокировки, поиска устройства и удаления данных на мобильном устройстве пользователя;
* наличие системы контроля возникновения вирусных эпидемий;
* установки в облачной инфраструктуре Microsoft Azure и Google Cloud;
* интеграции по OpenAPI;
* управления антивирусной защитой с использованием WEB консоли;
* возможность управления развертыванием ОС Windows через консоль управления;
* наличие преднастроенных ролей пользователей средств централизованного управления;
* должна быть реализована возможность создавать специализированные роли с конкретно указанным набором полномочий для привязки к учетным записям пользователей;
* возможность подключения по RDP или штатными средствами из консоли управления;
* наличие возможности совместного подключения к рабочему столу Windows (Windows Desktop Sharing);
* пользователю должен выводиться запрос на разрешение дистанционного подключения;
* наличие инструментов работы с образами ОС: Создание образа целевой ОС на основе физической или виртуальной машины, установка образа на выбранные администратором компьютеры, в том числе на "голое железо" (bare metal);
* должна быть обеспечена возможность добавления наборов драйверов в ранее созданный образ;
* возможность запускать скрипты или устанавливать дополнительное ПО в автоматическом режиме после установки ОС;
* возможность импортировать образ операционной системы из дистрибутивов (WIM)
* наличие системы контроля лицензий стороннего ПО, установленного на компьютере с возможностью оповещения администратора о нарушении пользования лицензией или превышении срока действия лицензии;
* автоматическое создание установочных пакетов для сторонних приложений (Adobe Reader, Mozilla Firefox, 7-zip и др.) и автоматическая централизованная установка этих пакетов приложений на компьютеры;
* поддержка функциональности управления шифрованием данных;
* возможность интеграции с SIEM системами и передача событий в формате syslog или CEF\ LEEF
* двухэтапная проверка для снижения риска несанкционированного доступа к Консоли администрирования;
* использования дополнительной аутентификация после изменения параметров учетной записи пользователя.
* возможность работать с IPv6 и IPv4-адресами и опрашивать сети, в которых есть устройства с IPv6-адресами.
* автоматизированный поиск и закрытие уязвимостей в установленных приложениях и операционной системе на компьютерах пользователей;
* возможность развернуть Сервер администрирования как систему высокой доступности;
* возможность устанавливать обновления и закрывать уязвимости программ сторонних производителей (кроме программ Microsoft) в изолированной сети.
  1. **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 11.х (Bullseye) 32-разрядная/64-разрядная;
* Debian GNU/Linux 10.х (Buster) 32-разрядная/64-разрядная;
* Debian GNU/Linux 9.х (Stretch) 32-разрядная/64-разрядная;
* Ubuntu Server 20.04 LTS (Focal Fossa) 64-разрядная;
* Ubuntu Server 18.04 LTS (Bionic Beaver) 64-разрядная;
* CentOS 7.x 64-разрядная;
* Red Hat Enterprise Linux Server 8.x 64-разрядная;
* Red Hat Enterprise Linux Server 7.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 1.7 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Astra Linux Special Edition 1.6 (включая режим замкнутой программной среды и мандатный режим) 64-разрядная;
* Astra Linux Common Edition 2.12 64-разрядная;
* Альт Сервер 10 64-разрядная;
* Альт Сервер 9.2 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;
* 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 10.5.x 32-разрядная/64-разрядная;
* MariaDB 10.4.x 32-разрядная/64-разрядная;
* MariaDB 10.3.22 и выше 32-разрядная/64-разрядная;
* MariaDB Server 10.3 32-разрядная/64-разрядная с подсистемой хранилища InnoDB;
* MariaDB 10.1.30 и выше 32-разрядная/64-разрядная.
  1. **В программном средстве антивирусной защиты должны быть реализованы следующие функциональные возможности:**
* централизованные установка, обновление и удаление программных средств антивирусной защиты;
* централизованная настройка, администрирование;
* просмотр отчетов и статистической информации по работе средств защиты;
* сохранение истории изменений политик и задач, возможность выполнить откат к предыдущим версиям;
* иерархии триггеров, по которым происходит перераспределение;
* доставка обновлений на рабочие места пользователей сразу после их получения;
* распознавание в сети виртуальных машин и распределение баланса нагрузки запускаемых задач между ними в случае, если эти машины находятся на одном физическом сервере;
* построение многоуровневой системы управления с возможностью настройки прав администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;
* создание иерархии серверов администрирования произвольного уровня и возможность централизованного управления всей иерархией с верхнего уровня;
* поддержка мультиарендности (multi-tenancy) для серверов управления;
* обновление программных средств и антивирусных баз из разных источников, как по каналам связи, так и на машинных носителях информации;
* доступ к облачным серверам производителя антивирусного ПО через сервер управления;
* автоматическое распространение лицензии на клиентские компьютеры;
* наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройки рассылки почтовых уведомлений о них;
* построение графических отчетов по событиям антивирусной защиты, данным лицензирования установленных программ;
* наличие преднастроенных стандартных отчетов о работе системы;
* экспорт отчетов в файлы форматов PDF и XML;
* централизованное управление объектами резервных хранилищ и карантинов по всем ресурсам сети, на которых установлено антивирусное программное обеспечение;
* создание внутренних учетных записей для аутентификации на сервере управления;
* создание резервной копии системы управления встроенными средствами системы управления;
* наличие системы контроля возникновения вирусных эпидемий;
* управления антивирусной защитой с использованием WEB консоли;
* возможность обновлять и распространять антивирусные базы и программные модули на управляемых устройствах как через сервер администрирования, так и через точки распространения для снижения нагрузки на сервер администрирования и оптимизации трафика данных в корпоративной сети;
* возможность с помощью задачи проверки обновлений проверять загружаемые обновления на работоспособность и наличие ошибок перед тем, как установить эти обновления на управляемые устройства;
* возможность использовать функцию файлов различий, чтобы загружать антивирусные базы и программные модули.
  1. **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.

1. **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.

1. **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.

1. **Требование к сертификации:** Программное обеспечение должно иметь сертификат соответствия требованиям безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации
2. **Гарантийный срок:** Срок действия неисключительного права на использование и воспроизведение программного обеспечения должен составлять не менее 12 месяцев.
3. Продление неисключительных прав на антивирусное программное обеспечение должно сопровождаться оформленными в соответствии с законодательством Российской Федерации сертификатами, соглашениями, свидетельствами, подтверждающими их оригинальность.
4. Лицензиат должен предоставить документы, подтверждающие его полномочия на продление неисключительных прав антивирусного программного обеспечения и обслуживание этих программ в Российской Федерации. Если Лицензиат не является производителем антивирусного программного обеспечения, то он должен предоставить копии дистрибьюторских или дилерских соглашений, копии писем производителей продукции, предоставляющие Лицензиат право на продление неисключительных прав антивирусного программного обеспечения. Авторизация и статус могут подтверждаться сертификатами от производителей.
5. Продление неисключительных прав на антивирусное программное обеспечение должно сопровождаться информационной и технической поддержкой по вопросам лицензирования, активации, установки этого антивирусного программного продукта на период действия лицензий.
6. Лицензиат должен предоставить продление неисключительных прав на антивирусное программное обеспечение, в полном объеме.
7. Неисключительные права на использование программного обеспечения переходят к Сублицензиату с момента получения от Лицензиата ключевого файла и лицензионного соглашения (бумажный вариант) действуют в течение 1 года с момента активации ключевого файла.
8. При выявлении недостатков носителя информации, Лицензиат своими силами и средствами, безвозмездно исправляет их в указанные сроки по требованию Сублицензиата.
9. Программное обеспечение должно быть передано Заказчику в запечатанных конвертах. Программное обеспечение поставляется в упаковке, обеспечивающей его целостность и сохранность. Носитель информации и упаковка должны быть маркированы в соответствии с требованиями, предъявляемыми к маркировке данного продукта. Ключевой файл антивирусного программного обеспечения предоставляется на отдельном компакт-диске (CD, DVD), лицензионное соглашение предоставляется на бумажном носителе.
10. Форму сублицензионного договора предоставляет Исполнитель.

|  |  |  |
| --- | --- | --- |
| Заказчик:  ОГАУЗ «ИГКБ № 8»  Главный врач  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Ж.В. Есева/  М.П. |  | Исполнитель:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_ /  М.П. |

**Приложение № 3**

**к Извещению о проведении закупки**

**на оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License путем запроса котировок в электронной форме, участниками которого могут являться только субъекты малого и среднего предпринимательства**

**№ 137-24**

**ФОРМА ЗАЯВКИ УЧАСТНИКА ЗАПРОСА КОТИРОВОК В ЭЛЕКТРОННОЙ ФОРМЕ**

**Раздел 1.** **Форма Заявки**

*На бланке организации*

*Дата, исх. Номер*

Заказчику:

*ОГАУЗ «Иркутская городская*

*клиническая больница № 8»*

Заявка на участие в запросе котировок в электронной форме,

участниками которого могут являться только субъекты малого и среднего предпринимательства

на оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License

Изучив извещение о проведении запроса котировок в электронной форме, участниками которого могут являться только субъекты малого и среднего предпринимательства, на оказание услуг по продлению неисключительных прав на использование и воспроизведение антивирусного программного обеспечения Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition. 500-999 Node 1 year Renewal License, выразив согласие участника закупки выполнять установленные в извещении о закупке требования и условия, *(полное наименование участника закупки с указанием организационно-правовой формы, фамилия, имя, отчество участника закупки физического лица)* в лице *(должность, ФИО),* действующего на основании *(Устава, доверенности №\_\_ от \_\_)*предлагает заключить договор в соответствии с настоящей заявкой и приложениями к заявке, проектом договора, являющимися неотъемлемыми частями к извещению о закупке, на общую сумму \_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_) руб. \_\_коп., в том числе НДС (если участник закупки является плательщиком НДС).

Настоящим подтверждаем, что:

- в отношении *(наименование организации или Ф.И.О. участника закупки)* не проводится ликвидация участника закупки - юридического лица и отсутствует решение арбитражного суда о признании участника закупки - юридического лица или индивидуального предпринимателя несостоятельным (банкротом);

- деятельность *(наименование организации или Ф.И.О. участника закупки)* не приостановлена в порядке, установленном Кодексом Российской Федерации об административных правонарушениях на дату подачи заявки на участие в закупке;

- у *(наименование организации или Ф.И.О. участника закупки)* отсутствуют недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной или которые признаны безнадежными к взысканию в соответствии с законодательством Российской Федерации о налогах и сборах) за прошедший календарный год, размер которых превышает **двадцать пять процентов** балансовой стоимости активов участника такой закупки, по данным бухгалтерской (финансовой) отчетности за последний отчетный период.[[1]](#footnote-1);

- у *(наименование организации или Ф.И.О. участника закупки)* - физического лица, зарегистрированного в качестве индивидуального предпринимателя, либо у руководителя, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа, или главного бухгалтера юридического лица - участника закупки непогашенной или неснятой судимости за преступления в сфере экономики и (или) преступления, предусмотренные статьями 289, [290](consultantplus://offline/ref=06DAB305DF3DF45773AC76426B0289841374F086155A83DAA68D53AB9583B2CD1031C6D7BAB0CA3B54A7F29DD6BE2005EFED15691276KAm1H), [291](consultantplus://offline/ref=06DAB305DF3DF45773AC76426B0289841374F086155A83DAA68D53AB9583B2CD1031C6D7BAB2CC3B54A7F29DD6BE2005EFED15691276KAm1H), [291.1](consultantplus://offline/ref=06DAB305DF3DF45773AC76426B0289841374F086155A83DAA68D53AB9583B2CD1031C6D7BABDC83B54A7F29DD6BE2005EFED15691276KAm1H) Уголовного кодекса Российской Федерации, а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определенные должности или заниматься определенной деятельностью, которые связаны с поставкой товара, выполнением работы, оказанием услуги, являющихся предметом осуществляемой закупки, и административного наказания в виде дисквалификации;

- у*(наименование организации или Ф.И.О. участника закупки)* отсутствуют факты привлечения в течение двух лет до момента подачи заявки на участие в закупке участника закупки - юридического лица к административной ответственности за совершение административного правонарушения, предусмотренного статьей 19.28 Кодекса Российской Федерации об административных правонарушениях;

- *(наименование организации или Ф.И.О. участника закупки)* соответствует указанным в извещении о закупке требованиям законодательства Российской Федерации к лицам, осуществляющим поставку товара, выполнение работы, оказание услуги, являющихся предметом закупки, если в соответствии с законодательством Российской Федерации информация и документы, подтверждающие такое соответствие, содержатся в открытых и общедоступных государственных реестрах, размещенных в информационно-телекоммуникационной сети "Интернет" (*при наличии такой информации* у*казать адрес сайта или страницы сайта в информационно-телекоммуникационной сети "Интернет", на которых размещены эти информация и документы*);

- *(наименование организации или Ф.И.О. участника закупки)* обладает исключительными правами на результаты интеллектуальной деятельности, если в связи с исполнением договора заказчик приобретает права на такие результаты;

- *(наименование организации или Ф.И.О. участника закупки)* обладает правами использования результата интеллектуальной деятельности в случае использования такого результата при исполнении договора.

**Раздел 2. Анкета участника запроса котировок**

|  |  |
| --- | --- |
| **1. Полное и сокращенное наименования организации и ее организационно-правовая форма:**  *(на основании Учредительных документов установленной формы (устав, положение и др.), свидетельства о государственной регистрации, свидетельства о внесении записи в единый государственный реестр юридических лиц, сертификата об инкорпорации или выписки из торгового реестра страны регистрации участника)*  **Ф.И.О. участника закупки – физического лица/физического лица, зарегистрированного в качестве индивидуального предпринимателя:**  **паспортные данные (для физического лица):** |  |
| **Фирменное наименование (при наличии)** |  |
| **2. ИНН, КПП, ОГРН, ОКПО *Участника****(или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика участника закупки (для иностранного лица)***:** |  |
| **3. ИНН** (при наличии) **учредителей**, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа участника закупки: |  |
| **4. Адрес юридического лица в пределах места нахождения юридического лица (адрес места жительства физического лица, зарегистрированного в качестве индивидуального предпринимателя):** |  |
| **5. Банковские реквизиты:** |  |
| 5.1. Наименование обслуживающего банка: |  |
| 5.2. Расчетный счет: |  |
| 5.3. Корреспондентский счет: |  |
| 5.4. Код БИК: |  |
| **6. Контактное лицо участника закупки, номер контактного телефона, электронной почты, факса участника закупки:** |  |

**Раздел 3. Описание поставляемого товара, работ, услуг:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п.** | **Наименование услуг** | **Характеристика услуг** | **Ед. изм.** | **Кол-во** | **Страна происхождения** | **Цена за ед., руб.** | **Сумма с НДС, руб.** |
|  |  |  |  |  |  |  |  |
|  | ИТОГО (цена договора): | | | |  | | |
|  | В т.ч. НДС (если участник закупки является плательщиком НДС) | | | |  | | |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

*(должность) (ФИО)*

1. Участник закупки с участием субъектов малого и среднего предпринимательства считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по данному заявлению на дату рассмотрения заявки на участие в закупке не принято [↑](#footnote-ref-1)