|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ:  Глава города Югорска  \_\_\_\_\_\_\_\_\_\_Р.З. Салахов  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2016 г. |

**ДОКУМЕНТАЦИЯ ОБ АУКЦИОНЕ В ЭЛЕКТРОННОЙ ФОРМЕ**

**среди субъектов малого предпринимательства и социально ориентированных некоммерческих организаций на право заключения муниципального контракта**

**на оказание услуг по продлению лицензий**

**на подсистему централизованной антивирусной обработки**

**2016 г.**

* 1. **СВЕДЕНИЯ О ПРОВОДИМОМ АУКЦИОНЕ В ЭЛЕКТРОННОЙ ФОРМЕ**

Настоящая документация об аукционе в электронной форме (далее по тексту также – документация об аукционе) подготовлена в соответствии с Федеральным законом от 05 апреля 2013 года №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее по тексту также – Закон о контрактной системе).

| **№**  **пункта** | **Наименование** | **Информация** |
| --- | --- | --- |
| Аукцион в электронной форме (далее по тексту также – электронный аукцион) проводит Уполномоченный орган. | | |
|  | Идентификационный код закупки: |  |
|  | Наименование Муниципального заказчика, контактная информация | Наименование: Администрация г.Югорска.  Место нахождения: 628260, Ханты-Мансийский автономный округ – Югра, г. Югорск, ул.40 лет Победы, д.11  Почтовый адрес Заказчика: 628260, Ханты-Мансийский автономный округ – Югра, г. Югорск, ул.40 лет Победы, д.11  Телефон: 8 (34675) 5-00-61  Адрес электронной почты: [inform@ugorsk.ru](mailto:inform@ugorsk.ru)  Ответственное должностное лицо: начальник отдела информационных ресурсов управления информационной политики Дергилев Олег Владимирович |
|  | Наименование уполномоченного органа (учреждения), контактная информация | Наименование: Администрация города Югорска.  Место нахождения: 628260, Ханты - Мансийский автономный округ - Югра, Тюменская обл.,  г. Югорск, ул. 40 лет Победы, 11, каб. 310.  Почтовый адрес: 628260, Ханты - Мансийский автономный округ - Югра, Тюменская обл.,  г. Югорск, ул. 40 лет Победы, 11.  Телефон: (34675) 50037 факс (34675) 50037.  Адрес электронной почты: omz@ugorsk.ru  Ответственное должностное лицо: начальник отдела муниципальных закупок управления экономической политики Захарова Наталья Борисовна. |
|  | Наименование специализированной организации, контактная информация | Не привлекается |
|  | Информация о контрактной службе заказчика, контрактном управляющем, ответственных за заключение контракта | Руководитель контрактной службы: первый заместитель главы города – директор департамента муниципальной собственности и градостроительства Голин Сергей Дмитриевич, телефон (34675) 5-00-04.  Лицо, ответственное за заключение контракта: главный специалист управления бухгалтерского учёта и отчётности Королева Наталья Борисовна, телефон: (34675) 5-00-47, адрес электронной почты: koroleva\_nb@ugorsk.ru |
|  | Наименование оператора электронной площадки | Наименование: ЗАО «Сбербанк - АСТ» |
| Адрес электронной площадки в информационно-телекоммуникационной сети «Интернет» | http://sberbank-ast.ru/ |
|  | Вид и предмет электронного аукциона | Аукцион в электронной форме среди субъектов малого предпринимательства и социально ориентированных некоммерческих организаций на право заключения муниципального контракта на оказание услуг по продлению лицензий на подсистему централизованной антивирусной обработки |
|  | Наименование и описание объекта закупки, количество поставляемого товара, объем выполняемых работ, оказываемых услуг | Указано в части II. «ТЕХНИЧЕСКОЕ ЗАДАНИЕ» настоящей документации об аукционе |
|  | Место оказания услуг | по месту нахождения Исполнителя |
|  | Сроки оказания услуг | с момента заключения муниципального контракта до 15.11.2016 года. |
|  | Начальная (максимальная) цена контракта | 137 700 (сто тридцать семь тысяч семьсот) рублей 00 копеек.  Начальная (максимальная) цена контракта включает в себя: все расходы Исполнителя, необходимые для осуществления им своих обязательств по Контракту в полном объёме и надлежащего качества, в том числе все подлежащие к уплате налоги, сборы и другие обязательные платежи, расходы на упаковку, маркировку, страхование, сертификацию, транспортные расходы по доставке товара до места поставки, затраты по хранению товара на складе Исполнителя, стоимость всех необходимых погрузочно-разгрузочных работ и иные расходы, связанные с оказанием услуг. |
|  | Обоснование начальной (максимальной) цены контракта | Содержится в части IV «Обоснование начальной (максимальной) цены контракта» |
|  | Источник финансирования | Бюджет города Югорска на 2016 год |
|  | Возможность оплаты по цене единицы работы, услуги, по цене каждой запасной части к технике, оборудованию | не предусмотрена |
|  | Сведения о валюте, используемой для формирования цены контракта и расчетов с поставщиками (исполнителями, подрядчиками) | Российский рубль |
|  | Порядок применения официального курса иностранной валюты к рублю Российской Федерации, установленного Центральным банком Российской Федерации и используемого при оплате контракта | не применяется |
|  | Единые требования к участникам закупки | В настоящем электронном аукционе, за исключением случая проведения электронного аукциона среди субъектов малого предпринимательства, социально ориентированных некоммерческих организаций может принять участие любое юридическое лицо независимо от его организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала, за исключением:- юридического лица, местом регистрации которого является государство или территория, включённые в утверждаемый в соответствии с подпунктом 1 пункта 3 статьи 284 Налогового кодекса Российской Федерации перечень государств и территорий, предоставляющих льготный налоговый режим налогообложения и (или) не предусматривающих раскрытия и предоставления информации при проведении финансовых операций (офшорные зоны) в отношении юридических лиц (далее - офшорная компания),или любое физическое лицо, в том числе зарегистрированное в качестве индивидуального предпринимателя.В случае, если электронный аукцион проводится среди субъектов малого предпринимательства, социально ориентированных некоммерческих организаций в соответствии указанием на это в пункте 7 настоящего раздела, участниками закупки могут быть только субъекты малого предпринимательства, социально ориентированные некоммерческие организации. Статус субъекта малого предпринимательства, социально ориентированной некоммерческой организации определяется в соответствии с законодательством Российской Федерации.Требования к участникам закупки: 1) соответствие требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставки товаров, выполнение работ и оказание услуг, являющихся объектом закупки;  2) непроведение ликвидации участника закупки - юридического лица и отсутствие решения арбитражного суда о признании участника закупки - юридического лица, индивидуального предпринимателя несостоятельным (банкротом) и об открытии конкурсного производства;  3) неприостановление деятельности участника закупки в порядке, установленном Кодексом Российской Федерации об административных правонарушениях, на день подачи заявки на участие в закупке;  4) отсутствие у участника закупки недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной и которые признаны безнадёжными 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 закупки по данным бухгалтерской отчётности за последний завершённый отчётный период. Участник закупки считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по такому заявлению на дату рассмотрения заявки на участие в определении поставщика (подрядчика, исполнителя) не принято;  5) отсутствие у участника закупки – физического лица либо у руководителя, членов коллегиального исполнительного органа или главного бухгалтера участника закупки – юридического лица судимости за преступления в сфере экономики (за исключением лиц, у которых такая судимость погашена или снята), а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определённые должности или заниматься определённой деятельностью, связанной с поставкой товаров, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации;  6) обладание участником закупки исключительными правами на результаты интеллектуальной деятельности, если в связи с исполнением контракта заказчик приобретает права на такие результаты, за исключением случаев заключения контрактов на создание произведений литературы или искусства, исполнения, на финансирование проката или показа национального фильма;  7) отсутствие между участником закупки и заказчиком конфликта интересов, под которым понимаются случаи, при которых руководитель заказчика, член комиссии по осуществлению закупок, руководитель контрактной службы заказчика, контрактный управляющий состоят в браке с физическими лицами, являющимися выгодоприобретателями, единоличным исполнительным органом хозяйственного общества (директором, генеральным директором, управляющим, президентом и другими), членами коллегиального исполнительного органа хозяйственного общества, руководителем (директором, генеральным директором) учреждения или унитарного предприятия либо иными органами управления юридических лиц - участников закупки, с физическими лицами, в том числе зарегистрированными в качестве индивидуального предпринимателя, - участниками закупки либо являются близкими родственниками (родственниками по прямой восходящей и нисходящей линии (родителями и детьми, дедушкой, бабушкой и внуками), полнородными и неполнородными (имеющими общих отца или мать) братьями и сёстрами), усыновителями или усыновленными указанных физических лиц. Под выгодоприобретателями для целей настоящей статьи понимаются физические лица, владеющие напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном капитале хозяйственного общества;  8) участник закупки не является офшорной компанией. |
| Требование об отсутствии сведений об участнике закупки в реестре недобросовестных поставщиков | Отсутствие в реестре недобросовестных поставщиков (подрядчиков, исполнителей) информации об участнике закупки, в том числе информации об учредителях, о членах коллегиального исполнительного органа, лице, исполняющем функции единоличного исполнительного органа участника закупки - юридического лица. |
| Дополнительные требования к участникам закупки | Не установлено |
|  | Требование о привлечении к исполнению контракта субподрядчиков, соисполнителей из числа субъектов малого предпринимательства и социально ориентированных некоммерческих организаций | Не установлено |
|  | Порядок, даты начала и окончания срока предоставления участникам закупки разъяснений положений документации об аукционе | Любой участник электронного аукциона, получивший аккредитацию на электронной площадке, вправе направить на адрес электронной площадки, на которой планируется проведение такого аукциона, запрос о даче разъяснений положений документации о таком аукционе.  При этом участник такого аукциона вправе направить не более чем три запроса о даче разъяснений положений данной документации в отношении одного такого аукциона.  В течение двух дней с даты поступления от оператора электронной площадки запроса заказчик размещает в единой информационной системе контрактной системы в сфере закупок[[1]](#footnote-1) разъяснения положений документации об электронном аукционе с указанием предмета запроса, но без указания участника такого аукциона, от которого поступил указанный запрос, при условии, что указанный запрос поступил заказчику не позднее чем за три дня до даты окончания срока подачи заявок на участие в таком аукционе.  Дата начала предоставления разъяснений положений документации об аукционе «03» июня 2016 года;  дата окончания предоставления разъяснений положений документации об аукционе «12» июня 2016 года.  Если последний день срока приходится на нерабочий день, днём окончания срока считается ближайший следующий за ним рабочий день (ст.193 Гражданского кодекса Российской Федерации). |
|  | Дата и время окончания срока подачи заявок на участие в электронном аукционе | Участник закупки, получивший аккредитацию на электронной площадке, вправе подать заявку на участие в электронном аукционе в любое время с момента размещения извещения о его проведении до 10 часов 00 минут «14» июня 2016 года. |
|  | Дата окончания срока рассмотрения частей заявок на участие в электронном аукционе | «16» июня 2016 года |
|  | Дата проведения электронного аукциона | «20» июня 2016 года |
|  | Требования к содержанию и составу заявки на участие в электронном аукционе | Заявка на участие в электронном аукционе состоит из двух частей.  Первая часть заявки на участие в электронном аукционе должна содержать следующие сведения: согласие участника аукциона на оказание услуги на условиях, предусмотренных настоящей документацией.  Вторая часть заявки на участие в электронном аукционе должна содержать следующие документы и информацию:  1) наименование, фирменное наименование (при наличии), место нахождения, почтовый адрес (для юридического лица), фамилия, имя, отчество (при наличии), паспортные данные, место жительства (для физического лица), номер контактного телефона, идентификационный номер налогоплательщика участника такого аукциона или в соответствии с законодательством соответствующего иностранного государства аналог идентификационного номера налогоплательщика участника такого аукциона (для иностранного лица), идентификационный номер налогоплательщика (при наличии) учредителей, членов коллегиального исполнительного органа, лица, исполняющего функции единоличного исполнительного органа участника такого аукциона;  2) **документы (или копии этих документов)**, подтверждающие соответствие участника аукциона следующим требованиям:   1. а) соответствие требованиям, установленным в соответствии с законодательством Российской Федерации к лицам, осуществляющим поставки товаров, выполнение работ и оказание услуг, являющихся объектом закупки, а именно: не установлено;   **а также декларация** о соответствии участника аукциона следующим требованиям:   * - непроведение ликвидации участника закупки - юридического лица и отсутствие решения арбитражного суда о признании участника закупки - юридического лица, индивидуального предпринимателя несостоятельным (банкротом) и об открытии конкурсного производства; * - неприостановление деятельности участника закупки в порядке, установленном Кодексом Российской Федерации об административных правонарушениях, на день подачи заявки на участие в закупке; * - отсутствие у участника закупки недоимки по налогам, сборам, задолженности по иным обязательным платежам в бюджеты бюджетной системы Российской Федерации (за исключением сумм, на которые предоставлены отсрочка, рассрочка, инвестиционный налоговый кредит в соответствии с законодательством Российской Федерации о налогах и сборах, которые реструктурированы в соответствии с законодательством Российской Федерации, по которым имеется вступившее в законную силу решение суда о признании обязанности заявителя по уплате этих сумм исполненной и которые признаны безнадёжными 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 закупки по данным бухгалтерской отчётности за последний завершённый отчётный период. Участник закупки считается соответствующим установленному требованию в случае, если им в установленном порядке подано заявление об обжаловании указанных недоимки, задолженности и решение по такому заявлению на дату рассмотрения заявки на участие в определении поставщика (подрядчика, исполнителя) не принято; * - отсутствие у участника закупки – физического лица либо у руководителя, членов коллегиального исполнительного органа или главного бухгалтера участника закупки – юридического лица судимости за преступления в сфере экономики (за исключением лиц, у которых такая судимость погашена или снята), а также неприменение в отношении указанных физических лиц наказания в виде лишения права занимать определённые должности или заниматься определённой деятельностью, связанной с поставкой товаров, выполнением работы, оказанием услуги, являющихся объектом осуществляемой закупки, и административного наказания в виде дисквалификации; * - обладание участником закупки исключительными правами на результаты интеллектуальной деятельности, если в связи с исполнением контракта заказчик приобретает права на такие результаты, за исключением случаев заключения контрактов на создание произведений литературы или искусства, исполнения, на финансирование проката или показа национального фильма - **не требуется;** * - отсутствие между участником закупки и заказчиком конфликта интересов, под которым понимаются случаи, при которых руководитель заказчика, член комиссии по осуществлению закупок, руководитель контрактной службы заказчика, контрактный управляющий состоят в браке с физическими лицами, являющимися выгодоприобретателями, единоличным исполнительным органом хозяйственного общества (директором, генеральным директором, управляющим, президентом и другими), членами коллегиального исполнительного органа хозяйственного общества, руководителем (директором, генеральным директором) учреждения или унитарного предприятия либо иными органами управления юридических лиц - участников закупки, с физическими лицами, в том числе зарегистрированными в качестве индивидуального предпринимателя, - участниками закупки либо являются близкими родственниками (родственниками по прямой восходящей и нисходящей линии (родителями и детьми, дедушкой, бабушкой и внуками), полнородными и неполнородными (имеющими общих отца или мать) братьями и сестрами), усыновителями или усыновленными указанных физических лиц. Под выгодоприобретателями понимаются физические лица, владеющие напрямую или косвенно (через юридическое лицо или через несколько юридических лиц) более чем десятью процентами голосующих акций хозяйственного общества либо долей, превышающей десять процентов в уставном капитале хозяйственного общества;   3) копии документов, подтверждающих соответствие товара, работы или услуги требованиям, установленным в соответствии с законодательством Российской Федерации, в случае, если в соответствии с законодательством Российской Федерации установлены требования к товару, работе или услуге - **не требуется**;  4) решение об одобрении или о совершении крупной сделки либо копия данного решения в случае, если требование о необходимости наличия данного решения для совершения крупной сделки установлено федеральными законами и иными нормативными правовыми актами Российской Федерации и (или) учредительными документами юридического лица и для участника такого аукциона заключаемый контракт или предоставление обеспечения заявки на участие в аукционе, обеспечения исполнения контракта является крупной сделкой;  5) документы, подтверждающие право участника аукциона на получение преимущества или копии этих документов - **не требуется;**  6) документы, подтверждающие соответствие участника аукциона и (или) предлагаемых им товара, работы или услуги условиям, запретам и ограничениям, или копии этих документов - **требуется:** в соответствии с Постановлением Правительства РФ от 29.12.2015 № 1457 «О перечне отдельных видов работ (услуг), выполнение (оказание) которых на территории Российской Федерации организациями, находящимися под юрисдикцией Турецкой Республики, а также организациями, контролируемыми гражданами Турецкой Республики и (или) организациями, находящимися под юрисдикцией Турецкой Республики, запрещено»;  7) **декларация** о принадлежности участника закупки к субъектам малого предпринимательства или социально ориентированным некоммерческим организациям – **требуется**. |
|  | Инструкция по заполнению заявки на участие в электронном аукционе | Заявки на участие в электронном аукционе подаются только участниками закупки, получившими аккредитацию на электронной площадке.  Участник закупки вправе подать только одну заявку на участие в электронном аукционе.  Заявка на участие в электронном аукционе направляется участником закупки оператору электронной площадки в форме двух электронных документов, содержащих предусмотренные пунктом 23 настоящей документацией об аукционе части заявки. Обе части заявок на участие в электронном аукционе подаются одновременно.  Заявка на участие в электронном аукционе, подготовленная участником закупки, должна быть cоставлена на русском языке. Входящие в заявку на участие в электронном аукционе документы, оригиналы которых выданы участнику закупки третьими лицами на ином языке, могут быть представлены на этом языке при условии, что к ним будет прилагаться перевод на русский язык. В случае противоречия оригинала и перевода преимущество будет иметь перевод.  Все документы, входящие в состав заявки на участие в электронном аукционе, должны иметь чётко читаемый текст.  Сведения, содержащиеся в заявке на участие в электронном аукционе, не должны допускать двусмысленных толкований.  **Инструкция по заполнению первой части заявки на участие в открытом аукционе в электронной форме**  При подаче сведений участниками закупки должны применяться обозначения (единицы измерения, наименования показателей, технических, функциональных параметров) в соответствии с обозначениями, установленными в части II «ТЕХНИЧЕСКОЕ ЗАДАНИЕ».  В случае применения заказчиком в техническом задании слов:  **«не менее», «не ниже»** - участником предоставляется значение равное или превышающее указанное;  **«не более», «не выше»** - участником предоставляется значение равное или менее указанного;  **«менее»,** **«ниже» -** участником предоставляется значение меньше указанного;  **«более», «выше», «свыше»** - участником предоставляется значение, превышающее указанное;  **«до» -** участником предоставляется значение меньше указанного, за исключением случаев, когда указанное значение сопровождается словом «включительно» либо используется при диапазонном значении;  **«от» -** участником предоставляется указанное значение или превышающее его.  В случае применение заказчиком в техническом задании перечислений характеристик через союз **«и»,** знаки «,» **«;»,** **«/» -** участник указывает характеристики всех перечисленных значений.  В случае, если характеристика товара указана с использованием нескольких значений, требования применяются к каждому значению.  При использовании союзов **«или»,** **«либо» -** участники выбирают одно из значений. При использовании **«и (или)» -** участник предлагает несколько показателей или один (на свой выбор).  В случае применения заказчиком в техническом задании значений:  - со знаком **«-»** - участник в заявке предлагает диапазонное значение, заданное техническим заданием (включаются верхние и нижние границы диапазона);  - со словами **«диапазон может быть расширен» -** участником представляется диапазон не менее указанных значений в рамках, равных показателям верхней и нижней границы диапазона, либо значения, расширяющие границы диапазона;  - если в Техническом задании устанавливается диапазонный показатель, наименование которого сопровождается словами *«диапазон должен быть не менее от…- до»*, или *«диапазон должен быть не более от…- до…»,* участником закупки должен быть предложен товар с конкретными значениями верхнего и нижнего предела показателя, соответствующим заявленным требованиям, но без сопровождения словами *«диапазон должен быть не менее»*, *«диапазон должен быть не более»*.  - при описании диапазона предлогами **«от»** и **«до»** предельные показатели входят в диапазон;  - со знаком **«+/-»** (например - погрешность) - участник предлагает конкретное цифровое значение с указанием знака «**+/-**».  Если характеристики товара содержатся в колонке «Неизменяемое (точное) значение показателя, установленное заказчиком» – участник не вправе изменять указанные характеристики.  При перечислении нескольких показателей одной характеристики товара необходимо употреблять союз «и», знаки «;» «,».  При предоставлении участниками конкретных значений показателей необходимо исключить употребление слов и словосочетаний: «или», «либо», «и (или)», «должен быть/иметь», «должна быть/иметь», «должны быть/иметь», «может», «в основном», «и другое», «в пределах», «ориентировочно», «не более», «не менее», «не ранее», «не хуже», «не выше», «не ниже», «до», «от», «более», «менее», «выше», «ниже», «возможность» за исключением случаев, когда рядом с установленным показателем заказчиком указано «значение является неизменным» или характеристика товара указана в колонке «Неизменяемое (точное) значение показателя, установленное заказчиком».  При использовании заказчиком в части II «ТЕХНИЧЕСКОЕ ЗАДАНИЕ» вышеуказанных терминов участник предлагает цифровое значение.  Документы, предусмотренные подпунктами 5, 6 и 7 пункта 23 части I «СВЕДЕНИЯ О ПРОВОДИМОМ АУКЦИОНЕ В ЭЛЕКТРОННОЙ ФОРМЕ» документации об аукционе, предоставляются в составе второй части заявки в случае установления соответствующих преимуществ, условий, запретов и ограничений в пунктах 7, 38, 39 части I «СВЕДЕНИЯ О ПРОВОДИМОМ АУКЦИОНЕ В ЭЛЕКТРОННОЙ ФОРМЕ» документации об аукционе.  Несоблюдение указанных требований является основанием для принятия аукционной комиссией решения о признании заявки участника не соответствующей требованиям, установленным настоящей документацией об аукционе |
|  | Размер обеспечения заявок на участие в электронном аукционе | Обеспечение заявки на участие в аукционе предусмотрено в размере 1% от начальной (максимальной) цены контракта, что составляет 1 377 (одна тысяча триста семьдесят семь) рублей 00 копеек. НДС не облагается. |
|  | Реквизиты счета для внесения денежных средств в качестве обеспечения заявок на участие в электронном аукционе | Денежные средства, внесённые в качестве обеспечения заявок, при проведении электронных аукционов перечисляются на счёт оператора электронной площадки в банке. |
|  | Срок, в течение которого победитель такого аукциона или иной участник, с которым заключается контракт при уклонении победителя такого аукциона от заключения контракта, должен подписать контракт | В течение пяти дней со дня получения проекта контракта от оператора электронной площадки |
|  | Условия признания  победителя электронного аукциона или иного участника такого аукциона уклонившимися от заключения контракта | Победитель электронного аукциона признается уклонившимся от заключения контракта в случае, если в течение пяти дней со дня получения проекта контракта от оператора электронной площадки, он не направил заказчику проект контракта, подписанный лицом, имеющим право действовать от имени победителя аукциона, а также обеспечение исполнения контракта или направил протокол разногласий по истечении тринадцати дней с даты размещения в единой информационной системе протокола подведения итогов электронного аукциона или не исполнил требования, предусмотренные статьёй 37 Закона о контрактной системе (в случае снижения при проведении электронного аукциона цены контракта на двадцать пять процентов и более от начальной (максимальной) цены контракта). |
|  | Размер обеспечения исполнения контракта, срок и порядок предоставления обеспечения исполнения контракта, требования к обеспечению исполнения контракта | Размер обеспечения исполнения контракта в размере 5 % от начальной (максимальной) цены контракта составляет 6 885 (шесть тысяч восемьсот восемьдесят пять) рублей 00 копеек.Контракт заключается только после предоставления участником аукциона, с которым заключается контракт обеспечения исполнения контракта.Исполнение контракта может обеспечиваться банковской гарантией, выданной банком, соответствующей требованиям статьи 45 Закона о контрактной системе, или денежными средствами. Способ обеспечения исполнения контракта определяется участником закупки, с которым заключается контракт, самостоятельно.Срок действия банковской гарантии должен превышать срок действия контракта не менее чем на один месяц.В случае возникновения обстоятельств, препятствующих заключению контракта в установленные Законом о контрактной системе сроки, срок действия банковской гарантии продлевается на срок наличия таких обстоятельств.Обеспечение исполнения контракта должно быть предоставлено одновременно с подписанным экземпляром контракта. Положения настоящей документации об обеспечении исполнения контракта не применяются в случае:  1) заключения контракта с участником закупки, который является государственным или муниципальным казённым учреждением;  2) осуществления закупки услуги по предоставлению кредита;  3) заключения бюджетным учреждением контракта, предметом которого является выдача банковской гарантии. Требования к обеспечению исполнения контракта, предоставляемому в виде банковской гарантии, установлены в статье 45 Закона о контрактной системе, а именно: 1. Банковская гарантия должна быть безотзывной;  2. Банковская гарантия должна содержать:  1) сумму банковской гарантии, подлежащую уплате гарантом заказчику в случае ненадлежащего исполнения обязательств принципалом в соответствии со [статьёй 96](consultantplus://offline/ref=B4AD8D930238F7B31D588C7097510AC56834F4EEC87D2B5A386D307D50D128C2096D93CFFC627DD66B47G) Закона о контрактной системе;  2) обязательства принципала, надлежащее исполнение которых обеспечивается банковской гарантией;  3) обязанность гаранта уплатить заказчику неустойку в размере 0,1 процента денежной суммы, подлежащей уплате, за каждый календарный день просрочки;  4) условие, согласно которому исполнением обязательств гаранта по банковской гарантии является фактическое поступление денежных сумм на счёт, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими заказчику;  5) условие о праве заказчика на бесспорное списание денежных средств со счета гаранта, если гарантом в срок не более чем пять рабочих дней не исполнено требование заказчика об уплате денежной суммы по банковской гарантии, направленное до окончания срока действия банковской гарантии  6) срок действия банковской гарантии;  7) отлагательное условие, предусматривающее заключение договора предоставления банковской гарантии по обязательствам принципала, возникшим из контракта при его заключении, в случае предоставления банковской гарантии в качестве обеспечения исполнения контракта;  8) установленный Правительством Российской Федерации [перечень](consultantplus://offline/ref=B4AD8D930238F7B31D588C7097510AC56834F7EDCC7E2B5A386D307D50D128C2096D93CFFC637ED36B4AG) документов, предоставляемых заказчиком банку одновременно с требованием об осуществлении уплаты денежной суммы по банковской гарантии.  3. Банковская гарантия должна быть включена в реестр банковских гарантий, размещённый в единой информационной системе. Требования к обеспечению исполнения контракта, предоставляемому в виде денежных средств:денежные средства, вносимые в обеспечение исполнения контракта, должны быть перечислены в размере и по реквизитам, установленном в пункте 30 настоящей документацией об аукционе;факт внесения денежных средств в обеспечение исполнения контракта подтверждается платёжным поручением с отметкой банка об оплате (квитанцией в случае наличной формы оплаты), оригинальной выпиской из банка в случае, если перевод денежных средств осуществлялся при помощи системы «Банк-клиент»;денежные средства, вносимые в обеспечение исполнения контракта, должны быть зачислены по реквизитам счета заказчика, указанным в пункте 30 настоящей документацией об аукционе, до заключения контракта. В противном случае обеспечение исполнения контракта в виде денежных средств считается непредоставленным;денежные средства возвращаются поставщику (подрядчику, исполнителю) с которым заключён контракт, при условии надлежащего исполнения им всех своих обязательств по контракту в течение срока, установленного в Проекте контракта (часть III « ПРОЕКТ КОНТРАКТА») со дня получения заказчиком соответствующего письменного требования поставщика (подрядчика, исполнителя); денежные средства возвращаются по реквизитам, указанным поставщиком (подрядчиком, исполнителем) в письменном требовании.В случае, если по каким либо причинам обеспечение исполнения обязательств по контракту перестало быть действительным, закончило своё действие или иным образом перестало обеспечивать исполнение поставщиком (подрядчиком, исполнителем), своих обязательств по контракту, соответствующий поставщик (подрядчик, исполнитель) обязуется в течение 10 (Десяти) банковских дней предоставить заказчику иное (новое) надлежащее обеспечение исполнение обязательств по контракту уменьшенное на размер выполненных обязательств по контракту, при этом может быть изменён способ обеспечения исполнения контракта.В ходе исполнения контракта поставщик (подрядчик, исполнитель) вправе предоставить заказчику обеспечение исполнения контракта, уменьшенное на размер выполненных обязательств, предусмотренных контрактом, взамен ранее предоставленного обеспечения исполнения контракта. При этом может быть изменён способ обеспечения исполнения контракта. |
|  | Реквизиты счета для внесения обеспечения исполнения контракта (в случае, если участник закупки выбрал обеспечение исполнения контракта в виде перечисления денежных средств) | ИНН 8622002368, КПП 862201001, Депфин Югорска (Администрация г. Югорска л/с 070050000), р/с 40302810800065000006, Ф-л ЗС ПАО «Ханты-Мансийский банк Открытие», г.Ханты-Мансийск, БИК 047162782, к/с 30101810771620000782. Назначение платежа: «Обеспечение исполнения муниципального контракта по аукциону в электронной форме №\_\_\_ на оказание услуг по продлению лицензий на подсистему централизованной антивирусной обработки» |
|  | Обязательства по контракту, которые должны быть обеспечены | По контракту должны быть обеспечены обязательства исполнителя по возмещению убытков заказчика, причинённых неисполнением или ненадлежащим исполнением обязательств по контракту, а также обязанность выплаты неустойки, предусмотренной контрактом. |
|  | Снижение цены контракта без изменения предусмотренных контрактом оказываемой услуги и иных условий контракта | Допускается |
|  | Изменение количества объема услуг не более чем на 10 процентов | Не допускается |
|  | Увеличение количества поставляемого на сумму, не превышающую разницы между ценой контракта, предложенной таким участником, и начальной (максимальной) ценой контракта (ценой лота) | Не допускается |
|  | Возможность одностороннего отказа от исполнения контракта в соответствии с положениями частей 8 - 26 статьи 95 Закона о контрактной системе | Односторонний отказ от исполнения контракта допускается в соответствии с гражданским законодательством Российской Федерации. |
|  | Требование о соответствии поставляемого товара изображению товара | Не установлено |
|  | Требование о соответствии поставляемого товара образцу или макету, товара | Не установлено |
|  | Сведения о предоставлении преимуществ участникам закупки | Преимущества для субъектов малого предпринимательства, социально ориентированных некоммерческих организаций – **предоставляются.**  Преимущества, предоставляемые осуществляющим производство товаров, выполнение работ, оказание услуг учреждениям и предприятиям уголовно-исполнительной системы: **не предоставляются.** Размер \_\_\_\_\_\_\_\_\_\_\_% от цены контракта.  Преимущества, предоставляемые осуществляющим производство товаров, выполнение работ, оказание услуг организациям инвалидов: **не предоставляются.** Размер \_\_\_\_\_\_\_\_\_\_\_% от цены контракта. |
|  | Условия, запреты и ограничения допуска товаров, происходящих из иностранного государства или группы иностранных государств, работ и услуг), соответственно выполняемых и оказываемых иностранными лицами, установленные в документации об аукционе в соответствии со статьёй 14 Закона о контрактной системе: | а) В соответствии с Постановлением Правительства РФ от 29.12.2015 № 1457 «О перечне отдельных видов работ (услуг), выполнение (оказание) которых на территории Российской Федерации организациями, находящимися под юрисдикцией Турецкой Республики, а также организациями, контролируемыми гражданами Турецкой Республики и (или) организациями, находящимися под юрисдикцией Турецкой Республики, запрещено», принятого во исполнение подпункта «б» пункта 1 Указа Президента РФ от 28.11.2015 № 583»: установлено;  б) в соответствии с Постановлением Правительства РФ от 14.07.2014 № 656 «Об установлении запрета на допуск отдельных видов товаров машиностроения, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»: не установлено;  в) в соответствии с Постановлением Правительства РФ от 16 ноября 2015 г. N 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»: не установлено;  г) в соответствии с Приказом Министерства экономического развития РФ от 25 марта 2014 г. № 155 "Об условиях допуска товаров, происходящих из иностранных государств, для целей осуществления закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд": не установлено;  д) в соответствии с Постановлением Правительства РФ от 5 февраля 2015 г. № 102 «Об установлении ограничения допуска отдельных видов медицинских изделий, происходящих из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»: не установлено;  е) в соответствии с Постановлением Правительства РФ от 30 ноября 2015 г. № 1289 «Об ограничениях и условиях допуска происходящих из иностранных государств лекарственных препаратов, включённых в перечень жизненно необходимых и важнейших лекарственных препаратов, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»: не установлено;  ж) в соответствии с Постановлением Правительства РФ от 11 августа 2014 г. № 791 «Об установлении запрета на допуск товаров лёгкой промышленности, происходящих из иностранных государств, и (или) услуг по прокату таких товаров в целях осуществления закупок для обеспечения федеральных нужд, нужд субъектов Российской Федерации и муниципальных нужд»: не установлено. |
|  | Информация о банковском сопровождении контракта (в случаях, предусмотренных статьёй 35 Закона о контрактной системе) | Банковское сопровождение не предусмотрено |
|  | Антидемпинговые меры | а) Если начальная (максимальная) цена контракта составляет более чем пятнадцать миллионов рублей и участником закупки, с которым заключается контракт, предложена цена контракта, которая на 25 и более процентов ниже начальной (максимальной) цены контракта, контракт заключается только после предоставления таким участником обеспечения исполнения контракта в размере, превышающем в полтора раза размер обеспечения исполнения контракта, указанный в документации об аукционе, но не менее чем в размере аванса (если контрактом предусмотрена выплата аванса).  б) Если начальная (максимальная) цена контракта составляет пятнадцать миллионов рублей именее участником закупки, с которым заключается контракт, предложена цена контракта, которая на двадцать пять и более процентов ниже начальной (максимальной) цены контракта, контракт заключается только после предоставления таким участником обеспечения исполнения контракта в размере, превышающем в полтора раза размер обеспечения исполнения контракта, указанный в документации об аукционе, но не менее чем в размере аванса (если контрактом предусмотрена выплата аванса)., или информации, подтверждающей добросовестность такого участника на дату подачи заявки.  в) К информации, подтверждающей добросовестность участника закупки, относится информация, содержащаяся в реестре контрактов, заключённых заказчиками, и подтверждающая исполнение таким участником в течение одного года до даты подачи заявки на участие в аукционе трёх и более контрактов (при этом все контракты должны быть исполнены без применения к такому участнику неустоек (штрафов, пеней), либо в течение двух лет до даты подачи заявки на участие в аукционе четырёх и более контрактов (при этом не менее чем семьдесят пять процентов контрактов должны быть исполнены без применения к такому участнику неустоек (штрафов, пеней), либо в течение трёх лет до даты подачи заявки на участие в аукционе трёх и более контрактов (при этом все контракты должны быть исполнены без применения к такому участнику неустоек (штрафов, пеней). В этих случаях цена одного из контрактов должна составлять не менее чем двадцать процентов цены, по которой участником закупки предложено заключить контракт.  г) Информация, предусмотренная подпунктом «в» настоящего пункта документации об аукционе, предоставляется участником закупки при направлении заказчику подписанного проекта контракта. При невыполнении таким участником, признанным победителем аукциона, данного требования или признании комиссией по осуществлению закупок информации, подтверждающей добросовестность участника закупки, недостоверной контракт с таким участником не заключается, и он признается уклонившимся от заключения контракта. В этом случае решение комиссии по осуществлению закупок оформляется протоколом, который размещается в единой информационной системе и доводится до сведения всех участников аукциона не позднее рабочего дня, следующего за днём подписания указанного протокола.  д) Обеспечение, указанное в подпунктах «а» и «б» настоящего пункта документации об аукционе, предоставляется участником закупки, с которым заключается контракт, до его заключения. Участник закупки, не выполнивший данного требования, признается уклонившимся от заключения контракта. В этом случае уклонение участника закупки от заключения контракта оформляется протоколом, который размещается в единой информационной системе и доводится до сведения всех участников закупки не позднее рабочего дня, следующего за днём подписания указанного протокола.  е) Если предметом контракта является поставка товара, необходимого для нормального жизнеобеспечения (продовольствие, средства для оказания скорой, в том числе скорой специализированной, медицинской помощи в экстренной или неотложной форме, лекарственные средства, топливо), участник закупки, предложивший цену контракта, которая на двадцать пять и более процентов ниже начальной (максимальной) цены контракта, обязан представить заказчику обоснование предлагаемой цены контракта, которое может включать в себя гарантийное письмо от производителя с указанием цены и количества поставляемого товара, документы, подтверждающие наличие товара у участника закупки, иные документы и расчёты, подтверждающие возможность участника закупки осуществить поставку товара по предлагаемой цене.  ж) Обоснование, указанное в подпункте «е» настоящего пункта документации об аукционе, представляется участником закупки, с которым заключается контракт, при направлении заказчику подписанного проекта контракта. В случае невыполнения таким участником данного требования он признается уклонившимся от заключения контракта. При признании комиссией по осуществлению закупок предложенной цены контракта необоснованной контракт с таким участником не заключается и право заключения контракта переходит к участнику аукциона, который предложил такую же, как и победитель аукциона, цену контракта или предложение о цене контракта которого содержит лучшие условия по цене контракта, следующие после условий, предложенных победителем аукциона. В этих случаях решение комиссии по осуществлению закупок оформляется протоколом, который размещается в единой информационной системе и доводится до сведения всех участников аукциона не позднее рабочего дня, следующего за днём подписания указанного протокола.  з) Антидемпинговые меры не применяются в случае, если при осуществлении закупок лекарственных препаратов, которые включены в утверждённый Правительством Российской Федерации перечень жизненно необходимых и важнейших лекарственных препаратов, участником закупки, с которым заключается контракт, предложена цена всех закупаемых лекарственных препаратов, сниженная не более чем на двадцать пять процентов относительно их зарегистрированной в соответствии с законодательством об обращении лекарственных средств предельной отпускной цены. |
|  | Ограничения участия в определении поставщика (подрядчика, исполнителя) | Информация об ограничениях указана в пунктах 7, 38 и 39 настоящего раздела. |

* 1. **ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**1.** **Предмет муниципального контракта**: оказание услуг по продлению лицензий на подсистему централизованной антивирусной обработки (код ОКПД2: 63.11.13.000).

**2. Общие требования:**

2.1. Место предоставления услуг: по месту нахождения Исполнителя.

2.2. Исполнитель обеспечивает предусмотренную производителем функциональность программного обеспечения в рамках продления действующей лицензии на подсистему централизованной антивирусной обработки Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition № 1B52-150922-054449 (на 200 защищаемых объектов). Эквивалент не предусмотрен в связи с необходимостью обеспечения работы единой антивирусной сети защиты информации заказчика, а также обеспечения совместимости и взаимодействия реализованной подсистемы антивирусной обработки и программного обеспечения информационной системы Заказчика.

**3. Перечень предоставляемых услуг:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование услуг | Характеристика предоставляемых услуг | Ед.  изм. | Кол-во |
| 1 | Продление лицензий на подсистему централизованной антивирусной обработки | Состав предоставляемых услуг:  Продление действующей лицензии на антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition на срок 1 год с учётом имеющейся у Заказчика (на 200 защищаемых объектов).  Комплектация:  - ключевой файл для активации программного обеспечения;  - экземпляр лицензионного соглашения с правообладателем программного обеспечения (ЗАО «Лаборатория Касперского»). | шт | 200 |

**4. Требования к поставляемому программному обеспечению:**

4.1. Назначение подсистемы централизованной антивирусной обработки:

- Защита рабочих станций от вредоносных программ;

- Защита файловых серверов;

- Безопасность мобильных устройств;

- Управление мобильными устройствами;

- Контроль программ, устройств и веб-ресурсов.

4.2. Общие требования к программному обеспечению:

Антивирусные средства должны включать:

• программные средства антивирусной защиты для рабочих станций Windows;

• программные средства антивирусной защиты для рабочих станций Mac OS;

• программные средства антивирусной защиты для рабочих станций Linux;

• программные средства антивирусной защиты для файловых серверов Windows;

• программные средства антивирусной защиты для файловых серверов Mac OS;

• программные средства антивирусной защиты для файловых серверов Linux;

• программные средства антивирусной защиты для файловых серверов Novell Netware;

• программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows;

• программные средства антивирусной защиты для мобильных устройств (смартфонов);

• программные средства централизованного управления, мониторинга и обновления;

• обновляемые базы данных сигнатур вредоносных программ и атак;

• эксплуатационную документацию на русском языке.

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

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

4.3. Требования к программным средствам антивирусной защиты для рабочих станций Windows:

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

• Microsoft Windows XP Professional (SP3 или выше);

• Microsoft Windows Vista Business/Enterprise/Ultimate (SP2 или выше);

• Microsoft Windows Vista Business/Enterprise/Ultimate x64 (SP2 или выше);

• Microsoft Windows 7 Professional/Enterprise/Ultimate;

• Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

• Microsoft Windows 8 Professional/Enterprise;

• Microsoft Windows 8 Professional/Enterprise x64 Edition.

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:

• Резидентный антивирусный мониторинг;

• Программные средства защиты от сетевых атак;

• Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• Обнаружение скрытых процессов;

• Антивирусное сканирование по команде пользователя или администратора и по расписанию;

• Антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;

• Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем;

• Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;

• Защита электронной корреспонденции, как от вредоносных программ, так и от спама, с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента; независимо от типа протокола (в том числе MAPI, HTTP) — в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и The Bat!;

• Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP;

• Проверка скриптов — проверка скриптов, обрабатываемых в Microsoft Internet Explorer, а также WSH-скриптов (таких как Java Script, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в интернете;

• Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами;

• Запуск задач по расписанию и/или сразу после загрузки операционной системы;

• Защита от ещё не известных вредоносных программ на основе анализа их поведения и контроля изменений системного реестра, с возможностью автоматического восстановления изменённых вредоносной программой значений системного реестра;

• Автоматический контроль программ, запускаемых на компьютере пользователя, осуществляющий контроль активности программ и ограничивающий выполнение опасных действий;

• Защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;

• Проверка протокола IPv6;

• Защита от программ-маскировщиков, программ автодозвона на платные сайты;

• Блокировка баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц;

• Распознавание и блокировка фишинг-сайтов;

• Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения по пути нахождения программы, метаданным, контрольной сумме MD5;

• Осуществление контроля работы пользователя с внешними устройствами ввода/вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям;

• Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;

• Интеграция с системой обновления Windows Update для установки патчей, закрывающих обнаруженные уязвимости;

• Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

• Настройка проверки критических областей компьютера в виде отдельной задачи;

• Технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющие избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;

• Возможность установки только выбранных компонентов программного средства антивирусной защиты;

• Централизованное управление с помощью единой системы управления.

4.4. Требования к программным средствам антивирусной защиты для рабочих станций и файловых серверов Mac:

Программные средства антивирусной защиты систем рабочих станций и серверов под управлением семейства ОС MAC должны функционировать на следующих версиях ОС:

Рабочие станции/ноутбуки:

• Mac OS X 10.6 (32/64 бит) - Snow Leopard;

• Mac OS X 10.5 (32 бит) – Leopard;

• Mac OS X 10.4 (32 бит) – Tiger.

Серверы:

• Mac OS X Server 10.6.

Программные средства антивирусной защиты систем рабочих станций и серверов под управлением семейства ОС MAC должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• централизованно управляться с помощью единой системы управления.

4.5. Требования к программным средствам антивирусной защиты для рабочих станций Linux:

Программные средства антивирусной защиты рабочих станций под управлением ОС Linux должны функционировать под управлением следующих платформ:

• 32-битные платформы:

 Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92);

 Fedora 9 (kernel 2.6.25);

 SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21);

 OpenSUSE Linux 11.0 (kernel 2.6.25);

 Debian GNU/Linux 4.0 r4 (kernel 2.6.24);

 Mandriva Corporate Desktop 4 (kernel 2.6.12);

 Ubuntu 8.04.1 Desktop Edition (kernel 2.6.25);

 Linux XP Enterprise Desktop 2008 (2.6.25.10-47.3.lxp2008);

 Red Hat Enterprise Linux 5.5 Desktop;

 Red Hat Enterprise Linux 6 Desktop;

 Fedora 14;

 CentOS-5.5;

 SUSE Linux Enterprise Desktop 10 SP3;

 SUSE Linux Enterprise Desktop 11 SP1;

 openSUSE Linux 11.3;

 Debian GNU/Linux 6.0.1;

 Mandriva Linux 2010;

 Ubuntu 10.04 LTS Desktop Edition.

• 64-битные платформы:

 Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92);

 Fedora 9 (kernel 2.6.25);

 SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21);

 OpenSUSE Linux 11.0 (kernel 2.6.25);

 Red Hat Enterprise Linux 5.5;

 Red Hat Enterprise Linux 6 Desktop;

 Fedora 14;

 CentOS-5.5;

 SUSE Linux Enterprise Desktop 10 SP3;

 SUSE Linux Enterprise Desktop 11 SP1;

 openSUSE Linux 11.3;

 Debian GNU/Linux 6.0.1;

 Ubuntu 10.04 LTS Desktop.

Программные средства антивирусной защиты рабочих станций под управлением ОС Linux должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверку и лечение файлов в архивах;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• помещение подозрительных и поврежденных объектов на карантин;

• возможность экспортировать и сохранять отчеты в форматах HTML и CSV;

• возможность перехвата и проверки файловых операций на уровне SAMBA;

• гибкого управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

• сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;

• возможность управление через графический интерфейс;

• централизованно управляться с помощью единой системы управления.

4.6. Требования к программным средствам антивирусной защиты для файловых серверов Windows:

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

• Microsoft Small Business Server 2011 Essentials х64 Edition;

• Microsoft Small Business Server 2011 Standard х64 Edition;

• Microsoft Windows Server 2012 Foundation х64 Edition;

• Microsoft Windows Server 2012 Essentials х64 Edition;

• Microsoft Windows Server 2012 Standard х64 Edition;

• Microsoft Windows Server 2008 R2 Standard / Enterprise х64 Edition SP0 и выше;

• Microsoft Windows Server 2008 Standard / Enterprise х64 Edition SP2 и выше;

• Microsoft Windows Server 2008 Standard / Enterprise SP2 и выше;

• Microsoft Windows Server 2003 R2 Standard / Enterprise SP2 и выше;

• Microsoft Windows Server 2003 R2 Standard х64 Edition SP2 и выше;

• Microsoft Windows Server 2003 Standard SP2;

• Microsoft Windows Server 2003 Standard х64 Edition SP2.

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• программные средства защиты от сетевых атак;

• защиту от хакерских атак, путем использования межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа;

• облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;

• обнаружение скрытых процессов;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверку и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;

• антивирусную проверку и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• защиту от еще не известных вредоносных программ, принадлежащих зарегистрированным семействам, на основе эвристического анализа;

• ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• настройки проверки критических областей сервера в качестве отдельной задачи;

• регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;

• наличием множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);

• технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, защита файлов приложения от несанкционированного доступа и изменения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющими избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;

• централизованно управляться с помощью единой системы управления.

4.7. Требования к программным средствам антивирусной защиты для файловых серверов Linux:

Программные средства антивирусной защиты серверов под управлением ОС Linux должны функционировать под управлением следующих платформ:

• 32-битные платформы:

 Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92);

 Red Hat Enterprise Linux 5.5 Server 2.6.18-186.el5;

 Red Hat Enterprise Linux 6 Server 2.6.32-71.el6.i686;

 Fedora 9 (kernel 2.6.25);

 Fedora 13 2.6.33.3-85.fc13.i686.PAE;

 CentOS-5.5 2.6.18-194.el5;

 Novel Open Enterprise Server 2 (kernel 2.6.16.46-0.12);

 Novel Open Enterprise Server 2 SP2 2.6.16.60-0.54.5-default;

 SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21);

 SUSE Linux Enterprise Server 10 SP3 2.6.16.60-0.54.5-default;

 SUSE Linux Enterprise Server 11 SP1 2.6.32.12-0.7-pae;

 OpenSUSE Linux 11.0 (kernel 2.6.25);

 OpenSUSE Linux 11.3 2.6.34-12-desktop;

 Debian GNU/Linux 4.0 r4 (kernel 2.6.24);

 Debian GNU/Linux 5.0.5 2.6.26-2-686;

 Mandriva Corporate Server 4 (kernel 2.6.12);

 Mandriva Enterprise Server 5.1 2.6.27.45-desktop-1mnb;

 Ubuntu 8.04.1 Server Edition (kernel 2.6.25);

 Ubuntu 10.04 Server Edition 2.6.32-21-generic;

 FreeBSD 7.3-RELEASE;

 FreeBSD 8.1-RELEASE.

• 64-битные платформы:

 Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92);

 Red Hat Enterprise Linux 5.5 server 2.6.18-194.el5;

 Red Hat Enterprise Linux 6 Server 2.6.32-71.el6.x86\_64;

 Fedora 9 (kernel 2.6.25);

 Fedora 13 2.6.33.3-85.fc13.x86\_64;

 CentOS-5.5 2.6.18-194.el5;

 SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21);

 SUSE Linux Enterprise Server 10 SP3 2.6.16.60-0.54.5-default;

 SUSE Linux Enterprise Server 11 SP1 2.6.32.12-0.7-default;

 Novell Open Enterprise Server 2 SP2 2.6.16.60-0.54.5-default;

 OpenSUSE Linux 11.3 2.6.34-12-desktop;

 OpenSUSE Linux 11.0 (kernel 2.6.25);

 Debian GNU/Linux 5.0.5 2.6.26-2-amd64;

 Ubuntu 10.04 Server Edition 2.6.32-21-generic;

 FreeBSD 7.3-RELEASE;

 FreeBSD 8.1-RELEASE.

Программные средства антивирусной защиты серверов под управлением ОС Linux должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверку и лечение файлов в архивах;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• помещение подозрительных и поврежденных объектов на карантин;

• формирование отчетов в форматах HTML, CSV, PDF и XLS;

• возможность перехвата и проверки файловых операций на уровне SAMBA;

• сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;

• удаленно через веб-браузер управлять антивирусом и настраивать его;

• централизованно управляться с помощью единой системы управления.

4.8. Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows:

Программные средства антивирусной защиты серверов масштаба предприятия под управлением семейства ОС Microsoft Windows и терминальных серверов должны функционировать на следующих версиях ОС:

• 32-битные платформы:

 Microsoft Windows Server 2003 Standard Edition с пакетом обновлений 1 или выше;

 Microsoft Windows Server 2003 Enterprise Edition с пакетом обновлений 1 или выше;

 Microsoft Windows Server 2003 R2 Standard Edition и выше;

 Microsoft Windows Server 2003 R2 Enterprise Edition и выше;

 Microsoft Windows Server 2008 Standard Edition;

 Microsoft Windows Server 2008 Enterprise Edition;

 Microsoft Windows Server 2008 Data Center Edition;

 Microsoft Windows Server 2008 Core Standard Edition;

 Microsoft Windows Server 2008 Core Enterprise Edition;

 Microsoft Windows Server 2008 Core Data Center Edition.

• 64-битные платформы:

 Microsoft Windows Server 2003 x64 Standard Edition;

 Microsoft Windows Server 2003 x64 Enterprise Edition;

 Microsoft Windows Server 2003 R2 Standard x64 Edition;

 Microsoft Windows Server 2003 R2 Enterprise x64 Edition;

 Microsoft Windows Server 2008 x64 Standard Edition;

 Microsoft Windows Server 2008 x64 Enterprise Edition;

 Microsoft Windows Server 2008 x64 Data Center Edition;

 Microsoft Windows Server 2008 Core x64 Standard Edition;

 Microsoft Windows Server 2008 Core x64 Enterprise Edition;

 Microsoft Windows Server 2008 Core x64 Data Center Edition;

 Microsoft Windows Server 2008 R2 Standard Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Enterprise Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Datacenter Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Core Standard Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Core Enterprise Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Core Datacenter Edition Release с пакетом обновлений SP1;

 Microsoft Windows Hyper-V Server 2008 R2 Release с пакетом обновлений SP1.

• Терминальные серверы:

 Microsoft Terminal на базе Windows 2003 Server;

 Microsoft Terminal на базе Windows Server 2008;

 Citrix Presentation Server 4.0;

 Citrix Presentation Server 4.5;

 Citrix XenApp 4.5;

 Citrix XenApp 5.0;

 Citrix XenApp 6.0.

Программные средства антивирусной защиты серверов масштаба предприятия под управлением семейства ОС Microsoft Windows и терминальных серверов должны обеспечивать реализацию следующих функциональных возможностей:

• Осуществление антивирусной проверки на серверах, выполняющих разные функции:

 Серверов терминалов и принт-серверов;

 Серверов приложений и контроллеров доменов;

 Файловых серверов.

• Возможность использования для защиты кластера серверов;

• Возможность защиты систем хранения данных EMC Celerra;

• Определение в объектах файловой системы сервера угрозы следующих типов:

 Классических вирусов;

 Сетевых червей;

 Троянских программ;

 Прочих вредоносных программ;

 Программ-реклам;

 Программ порнографического содержания;

 Потенциально опасных приложений.

• Проверка следующих объектов защищаемого сервера при доступе к ним:

 Файлов при их записи и считывании;

 Альтернативных потоков файловых систем (NTFS-streams);

 Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей.

• Предотвращение вирусных эпидемий за счет фиксации возникновения вирусных атак;

• Восстановление после заражения путем удаления всех связанных с ликвидированным вредоносным объектом записей в системных файлах и реестре ОС, что предотвращает возможные сбои в работе операционной системы;

• 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;

• Проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере;

• Помещение подозрительных и поврежденных объектов на карантин;

• При защите терминальных серверов поддержка режимов публикации рабочего стола и публикации приложений;

• Масштабируемость за счет задания количества рабочих процессов антивируса для ускорения обработки запросов к серверу при использовании многопроцессорных серверов;

• Балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: антивирусная проверка может продолжаться в фоновом режиме;

• Выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие);

• Разделение прав администраторов, основанное на стандартных механизмах ОС Microsoft Windows;

• Уведомления различными методами администраторов и пользователей о событиях в антивирусной защите. Поддержка Simple Network Management Protocol (SNMP;

• Cовместимость с системами управления дисковым пространством (Hierarchical Storage Management), позволяющая настраивать способы проверки для Offline Files;

• Оптимизация для использования на многопроцессорных серверах на базе технологии Intel Xeon™, позволяющая использовать приложение в условиях высоких нагрузок;

• Возможность управления с помощью MMC консоли;

• Централизованно управляться с помощью единой системы управления.

4.9. Требования к программным средствам антивирусной защиты смартфонов:

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

• Android 2.2 – 2.x, 4.0; Android 3 for tablets;

• iOS 4, 5;

• BlackBerry 4.5 – 6.0, 7.0; BlackBerry for tablets;

• Windows Mobile 5.0 – 6.5;

• Symbian 9.1 – 9.3, Symbian 3, Anna, Belle.

Программные средства для антивирусной защиты смартфонов должны обеспечивать следующую функциональность:

• постоянную защиту файловой системы смартфона, перехват и проверку:

• всех входящих объектов, передающихся с помощью беспроводных соединений (инфракрасный порт, Bluetooth), сообщений EMS и MMS, при синхронизации с персональным компьютером и загрузке файлов через браузер;

• файлов, открываемых на смартфоне;

• программ, устанавливаемых из интерфейса смартфона.

• проверку объектов файловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию;

• надежное изолирование зараженных объектов в карантинном хранилище;

• обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов;

• блокирование нежелательных SMS и MMS сообщений;

• шифрование наиболее важных файлов, папок и карты памяти;

• возможность скрывать важные контакты и историю общения с ними;

• осуществлять функцию «антивор», т.е. обеспечивать блокировку мобильного устройства, удаление данных, сообщений и книги контактов, получение координат местоположения, а также определение, у кого находится пропавшее устройство.

4.10. Требования к системе управления антивирусной защитой:

Программные средства управления для защищаемых рабочих станций, файловых серверов и смартфонов должны функционировать на следующих операционных системах:

Сервер администрирования:

• Microsoft Windows XP Professional SP2 и выше;

• Microsoft Windows XP Professional x64 и выше;

• Microsoft Windows Server 2003 и выше;

• Microsoft Windows Server 2003 x64 и выше;

• Microsoft Windows Vista SP1 и выше;

• Microsoft Windows Vista x64 SP1 и всеми текущими обновлениями;

• Microsoft Windows Server 2008;

• Microsoft Windows Server 2008, развернутая в режиме Server Core;

• Microsoft Windows Server 2008 x64 SP1 и всеми текущими обновлениями;

• Microsoft Windows Server 2008 R2;

• Microsoft Windows Server 2012;

• Microsoft Windows Small Business Server 2003;

• Microsoft Windows Small Business Server 2008;

• Microsoft Windows Small Business Server 2011;

• Microsoft Windows 7 Professional/Enterprise/Ultimate;

• Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

• Microsoft Windows 8;

• Microsoft Windows 8 x64.

Сервером администрирования должна использоваться одна из следующих СУБД:

• Microsoft SQL Express 2005;

• Microsoft SQL Express 2008;

• Microsoft SQL Express 2008 R2;

• Microsoft SQL Express 2012;

• Microsoft SQL Server 2005;

• Microsoft SQL Server 2008;

• Microsoft SQL Server 2008 R2;

• Microsoft SQL Server 2012;

• MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91;

• MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90.

Консоль администрирования:

• Microsoft Windows XP Professional SP2 и выше;

• Microsoft Windows XP Professional x64 и выше;

• Microsoft Windows Server 2003 и выше;

• Microsoft Windows Server 2003 x64 и выше;

• Windows Small Business Server 2003;

• Microsoft Windows Vista SP1 и выше;

• Microsoft Windows Vista x64 SP1 и всеми текущими обновлениями;

• Microsoft Windows Server 2008;

• Microsoft Windows Server 2008 x64 SP1 и всеми текущими обновлениями;

• Windows Small Business Server 2008 x64;

• Microsoft Windows Server 2008 x64 R2;

• Microsoft Windows Server 2008 x64 R2 SP1;

• Windows Small Business Server 2011 x64;

• Microsoft Windows 8;

• Microsoft Windows 8 x64;

• Microsoft Windows 7 Professional/Enterprise/Ultimate SP1;

• Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1.

Агент администрирования: программные требования должны соответствовать требованиям к программным средствам антивирусной защиты.

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:

• установка системы антивирусной защиты из единого дистрибутива;

• выбор установки в зависимости от количества защищаемых узлов;

• создание групп логической сети на основе структуры Active Directory;

• автоматическое распределение компьютеров по группам управления, в случае появления новых компьютеров в сети;

• централизованную установку/обновление/удаление программных средств антивирусной защиты, настройку, администрирование, просмотр отчетов и статистической информации по их работе;

• централизованное удаление несовместимых приложений;

• централизованное управление установкой/запуском программ на компьютерах пользователей с возможностью контроля программ по пути нахождения программы, метаданным, MD5 контрольной сумме и возможностью присвоения привилегий определенным пользователям;

• централизованное управление доступом к веб-ресурсам с компьютеров пользователей, с возможностью фильтрации по категориям и типу данных загружаемого контента, гибко задавать параметры времени действия правил и возможностью присвоения привилегий определенным пользователям;

• наличие различных методов установки антивирусных приложений: удаленный - RPC, GPO, агент администрирования, локальный - автономный пакет установки;

• удаленная установка программных средств антивирусной защиты с последней версией баз приложения;

• автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;

• автоматизированный поиск уязвимостей, в установленных приложения и операционной системе, на компьютерах пользователей;

• тестирование загруженных обновлений средствами сервера администрирования перед распространением на клиентские машины; доставку 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;

• централизованное осуществление контроля работы пользователя с внешними устройствами ввода / вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создавать доверенные устройства по их идентификатору и возможностью предоставлять привилегии, для запуска внешних устройств, определенным пользователям;

• построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;

• создание виртуальных серверов управления антивирусным приложением;

• 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;

• централизованный сбор информации и создание отчетов о состоянии антивирусной защиты;

• инвентаризация установленного ПО и оборудования на компьютерах пользователей;

• наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройку рассылки почтовых уведомлений о них;

• функция для управления мобильными устройствами сервер Exchange ActiveSync;

• функция для управления мобильными устройствами сервер iOS MDM;

• возможность отправки SMS-сообщений мобильным пользователям;

• централизованная установка приложений на управляемые мобильные устройства;

• централизованная установка сертификатов на управляемые мобильные устройства;

• централизованный сбор информации о всех установленных на клиентских компьютерах приложениях;

• интеграция с CISCO NAC и MS NAP;

• экспорта 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;

• поддержка Windows Failover Clustering;

• наличие веб-консоли управления приложением;

• наличие системы контроля возникновения вирусных эпидемий.

Требования к обновлению антивирусных баз:

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

• регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз антиспама не реже одного раза в 5 минут;

• множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;

• проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации:

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

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

Требования к технической поддержке:

Техническая поддержка антивирусного программного обеспечения должна:

• Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнёров на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет;

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

Согласовано: Работник контрактной службы: О.В.Дергилев

* 1. **ПРОЕКТ КОНТРАКТА**

**МУНИЦИПАЛЬНый КОНТРАКТ на оказание услуг**

**по продлению лицензий на подсистему централизованной антивирусной обработки**

г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_201\_\_\_ г.

Администрация города Югорска, именуемая в дальнейшем Заказчик, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуем\_\_ в дальнейшем Исполнитель, в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, вместе именуемые «Стороны», в соответствии с законодательством Российской Федерации и иными нормативными правовыми актами о контрактной системе в сфере закупок, и на основании

решения Единой комиссии по осуществлению закупок для обеспечения муниципальных нужд города Югорска (протокол\_\_\_\_\_\_\_\_\_ от \_\_\_\_\_ № \_\_\_\_\_)

*решения Заказчика от \_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_\_ об осуществлении закупки у единственного исполнителя в соответствии с пунктом \_\_\_\_\_\_\_\_ части 1 статьи 93 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»*

заключили настоящий муниципальный контракт, именуемый в дальнейшем «Контракт», о нижеследующем:

**1. Предмет контракта**

1.1. Исполнитель обязуется своевременно оказать на условиях Контракта услуги по продлению лицензий на подсистему централизованной антивирусной обработки, а Заказчик обязуется принять и оплатить их.

* 1. Состав и объем услуг определяется в Техническом задании (Приложение) к Контракту.

1.3. Место оказания услуг: по месту нахождения Исполнителя.

**2. Цена контракта и порядок расчётов**

2.1. Цена Контракта является твёрдой, не может изменяться в ходе заключения и исполнения Контракта, за исключением случаев, установленных Контрактом и (или) предусмотренных законодательством Российской Федерации.

2.2. Общая цена Контракта составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_ копеек, включая налог на добавленную стоимость (\_\_ %): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_ копеек *(НДС не облагается на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Налогового кодекса РФ и \_\_\_\_\_\_\_\_).*

Оплата по Контракту уменьшается на размер налоговых платежей, связанных с оплатой контракта, и составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_ копеек *(если Контракт заключается с физическим лицом, за исключением индивидуального предпринимателя или иного занимающегося частной практикой лица).*

2.3. В общую цену Контракта включены все расходы Исполнителя, необходимые для осуществления им своих обязательств по Контракту в полном объёме и надлежащего качества, в том числе все подлежащие к уплате налоги, сборы и другие обязательные платежи, расходы на упаковку, маркировку, страхование, сертификацию, транспортные расходы по доставке товара до места поставки, затраты по хранению товара на складе Исполнителя, стоимость всех необходимых погрузочно-разгрузочных работ и иные расходы, связанные с оказанием услуг.

2.4. Оплата по Контракту производится в следующем порядке:

2.4.1. Оплата производится в безналичном порядке путём перечисления Заказчиком денежных средств на указанный в Контракте расчётный счёт Исполнителя.

2.4.2. Оплата производится в рублях Российской Федерации.

2.4.3. Заказчик на основании выставленного Исполнителем счета перечисляет авансовый платёж в размере 30% от общей цены Контракта, что составляет \_\_\_\_\_\_\_\_\_ рублей \_\_ копеек, в течение 10 (десяти) рабочих дней со дня заключения Контракта.

2.4.4. Расчёт за оказанные услуги осуществляется в течение 10 (десяти) дней со дня подписания Заказчиком Акта об оказанных услугах.

2.4.5. В случаях, предусмотренных пунктом 2.6 Контракта, оплата оказанных услуг (части услуг) производится в течение 10 (десяти) дней со дня поступления Заказчику от Исполнителя денежных средств в счёт уплаты в полном объёме начисленной и выставленной Заказчиком неустойки (штрафа, пени) и (или) возмещения Исполнителем убытков, согласно предъявленным Заказчиком требованиям, на основании подписанных Заказчиком Актов об оказанных услугах.

2.5. В случае начисления Заказчиком Исполнителю неустойки (штрафа, пени) и (или) предъявления требования о возмещении убытков, Стороны подписывают Акт взаимосверки обязательств по Контракту, в котором, также, указываются: сведения о фактически исполненных обязательствах по Контракту, сумма, подлежащая оплате в соответствии с условиями Контракта, размер неустойки (штрафа, пени) и (или) убытков, подлежащей взысканию, основания применения и порядок расчёта неустойки (штрафа, пени) и (или) убытков, итоговая сумма, подлежащая оплате Исполнителю по Контракту.

В случае подписания Сторонами Акта взаимосверки обязательств по Контракту оплата оказанных услуг осуществляется Исполнителю за вычетом соответствующего размера неустойки (штрафа, пени) и (или) убытков согласно указанному Акту и на основании представленного Исполнителем счета.

2.6. В случае, если при начислении Заказчиком Исполнителю неустойки (штрафа, пени) и (или) предъявления требования о возмещении убытков, Стороны не подписали Акт взаимосверки обязательств по Контракту, указанный в п. 2.5 Контракта, Заказчик вправе не производить оплату по Контракту до уплаты Исполнителем начисленной и выставленной Заказчиком неустойки (штрафа, пени) и (или) до возмещения Исполнителем убытков, согласно предъявленным Заказчиком требованиям.

2.7. В случае уменьшения Заказчику соответствующими финансовыми органами в установленном порядке ранее доведённых лимитов бюджетных обязательств, приводящего к невозможности исполнения Заказчиком обязательств по Контракту, о чем Заказчик уведомляет Исполнителя, Стороны согласовывают в соответствии с законодательством Российской Федерации новые условия, в том числе по цене и (или) объёму услуг.

**3. Права и обязанности Сторон**

3.1. Заказчик имеет право:

3.1.1. Досрочно принять и оплатить услуги в соответствии с условиями Контракта.

3.1.2. Требовать возмещения неустойки и (или) убытков, причинённых по вине Исполнителя.

3.1.3. Привлекать экспертов, экспертные организации для проверки соответствия качества оказываемых услуг требованиям, установленным Контрактом.

3.1.4. Осуществлять иные права, предусмотренные Контрактом и законодательством Российской Федерации.

3.2. Заказчик обязан:

3.2.1. Обеспечить приёмку оказанных по Контракту услуг по объёму и качеству.

3.2.2. Оплатить услуги в порядке, предусмотренном Контрактом.

3.2.3. Своевременно предоставить Исполнителю информацию, необходимую для исполнения Контракта.

3.2.4. Выполнять иные обязанности, предусмотренные Контрактом.

3.3. Исполнитель обязан:

3.3.1. Оказать услуги в сроки, предусмотренные Контрактом.

3.3.2. Не предоставлять другим лицам или разглашать иным способом конфиденциальную информацию, полученную в результате исполнения обязательств по Контракту.

3.3.3. По требованию Заказчика своими средствами и за свой счёт в срок, согласованный с Заказчиком устранить допущенные по своей вине в оказанных услугах недостатки или иные отступления от условий Контракта.

3.3.4. Предоставлять своевременно достоверную информацию о ходе исполнения своих обязательств, в том числе о сложностях, возникающих при исполнении Контракта.

3.3.5. Выполнять иные обязанности, предусмотренные Контрактом.

3.4. Исполнитель вправе:

3.4.1. Требовать приёмки и оплаты услуг в объёме, порядке, сроки и на условиях, предусмотренных Контрактом.

3.4.2. По согласованию с Заказчиком досрочно оказать услуги. Заказчик вправе досрочно принять и оплатить услуги в соответствии с условиями Контракта.

**4. Сроки оказания услуг**

4.1. Срок оказания услуг: с момента заключения муниципального контракта до 15.11.2016 года.

4.2. Досрочная сдача результатов услуг допускается только по согласованию с Заказчиком. В случае согласования досрочного оказания услуг Заказчик обязуется принять услуги и подписать Акт об оказанных услугах в порядке, установленном Контрактом.

4.3. В случае, если в п. 11.1 Контракта указана дата, при наступлении которой обязательства сторон прекращаются, за исключением обязательств по оплате услуг, гарантийных обязательств, обязательств по возмещению убытков и выплате неустойки (штрафа, пени), Стороны после наступления указанной даты не вправе требовать исполнения Контракта в части оказания услуг и их приёмки. При наступлении указанной даты (в случае, если она установлена) Заказчиком в двух экземплярах составляется Акт взаимосверки обязательств по Контракту, в котором указываются сведения о прекращении действия Контракта; сведения о фактически исполненных обязательствах по Контракту; сумма, подлежащая оплате в соответствии с условиями Контракта.

Исполнитель обязан подписать Акт взаимосверки обязательств. В случае уклонения Исполнителя от подписания данного акта Заказчик проставляет в нем соответствующую отметку. Акт взаимосверки обязательств является основанием для проведения взаиморасчётов между Сторонами.

**5. Порядок сдачи и приёмки услуг**

5.1. Приёмка услуг на соответствие их объёма и качества требованиям, установленным в Контракте, производится за счёт Заказчика.

5.2. Исполнитель после оказания услуг, в срок не более 5 дней направляет в адрес Заказчика Акт об оказанных услугах.

5.3. Заказчик вправе создать приёмочную комиссию, в составе не менее пяти человек, для проверки соответствия качества услуг требованиям, установленным Контрактом. В состав такой приёмочной комиссии могут быть включены представители участников закупки, участвовавших в процедуре определения исполнителя, на основании которого заключён Контракт, но не ставших победителями. Проверка соответствия качества оказываемых услуг требованиям, установленным Контрактом, может также осуществляться с привлечением экспертов, экспертных организаций.

5.4. Стороны подписывают Акты об оказанных услугах в течение 3 дней со дня получения акта об оказанных услугах.

5.5. В случае обнаружения недостатков в объёме и качестве оказанных услуг Заказчик направляет Исполнителю уведомление в порядке, предусмотренном п. 5.7 Контракта.

5.6. В случае если Исполнитель не согласен с предъявляемой Заказчиком претензией о некачественной услуге, Исполнитель обязан самостоятельно подтвердить качество услуг заключением эксперта, экспертной организации и оригинал экспертного заключения представить Заказчику. Выбор эксперта, экспертной организации осуществляется Исполнителем и согласовывается с Заказчиком. Оплата услуг эксперта, экспертной организации, а также всех расходов для экспертизы осуществляется Исполнителем.

5.7. Обо всех нарушениях условий Контракта об объёме и качестве услуг Заказчик извещает Исполнителя не позднее трёх рабочих дней с даты обнаружения указанных нарушений. Уведомление о невыполнении или ненадлежащем выполнении Исполнителем обязательств по Контракту составляется Заказчиком в письменной форме и направляется Исполнителю по почте, факсу, электронной почте либо нарочным. Адресом электронной почты для получения уведомления является: inform@ugorsk.ru. Номером факса для получения уведомления является: 8 (34675) 50061.

5.8. Исполнитель в установленный в уведомлении (п. 5.7) срок обязан устранить все допущенные нарушения. Если Исполнитель в установленный срок не устранит нарушения, Заказчик вправе предъявить Исполнителю требование о возмещении своих расходов на устранение недостатков услуг, в случае, если устранение нарушений потребует больших временных затрат, в связи с чем Заказчик утрачивает интерес к Контракту.

**6. Обеспечение исполнения контракта\***

6.1. Способами обеспечения исполнения Контракта являются банковская гарантия, выданная банком и соответствующая требованиям п. 6.6. Контракта, или внесение денежных средств на указанный Заказчиком счёт, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими Заказчику. Способ обеспечения исполнения контракта определяется Исполнителем самостоятельно.

6.2. Обеспечение исполнения Контракта предоставляется Заказчику до заключения Контракта. Размер обеспечения исполнения Контракта составляет 6 885 (шесть тысяч восемьсот восемьдесят пять) рублей 00 копеек (5 процентов от начальной (максимальной) цены контракта).

В случае принятия антидемпинговых мер, обеспечение исполнения контракта составит 10327 (десять тысяч триста двадцать семь) рублей 50 копеек (7,5 процентов от начальной (максимальной) цены контракта).

6.3. В ходе исполнения Контракта Исполнитель вправе предоставить Заказчику обеспечение исполнения Контракта, уменьшенное на размер выполненных обязательств, предусмотренных Контрактом, взамен ранее предоставленного обеспечения исполнения Контракта. При этом может быть изменён способ обеспечения исполнения Контракта.

6.4. Срок действия обеспечения исполнения Контракта в форме банковской гарантии – до 15.12.2016. Срок действия указанного обеспечения может быть прекращён до наступления указанного срока в случае досрочного исполнения Исполнителем всех своих обязательств по Контракту.

6.5. По Контракту должны быть обеспечены обязательства Исполнителя в том числе, по возмещению убытков Заказчика, причинённых неисполнением или ненадлежащим исполнением, просрочкой исполнения обязательств по Контракту, а также обязанность по выплате неустойки (штрафа, пени), возврату аванса и иных долгов, возникших у Исполнителя перед Заказчиком.

6.6. Требования к обеспечению исполнения Контракта, предоставляемому в виде банковской гарантии:

Банковская гарантия оформляется в письменной форме на бумажном носителе или в форме электронного документа, подписанного усиленной неквалифицированной электронной подписью лица, имеющего право действовать от имени банка, на условиях, определённых гражданским законодательством и статьёй 45 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», с учётом требований установленных постановлением Правительства Российской Федерации от 08.11. 2013 № 1005 «О банковских гарантиях, используемых для целей Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

6.7. Денежные средства возвращаются в полном объёме (либо в части, оставшейся после удовлетворения требований Заказчика, возникших в период действия обеспечения) в течение десяти дней с момента подписания Сторонами документов, подтверждающих надлежащее исполнение обязательств по Контракту в полном объёме.

\* Положения раздела 6 настоящего Контракта об обеспечении исполнения контракта не применяются в случае:

1) заключения контракта с участником закупки, который является государственным или муниципальным казанным учреждением;

2) осуществления закупки услуги по предоставлению кредита;

3) заключение бюджетным учреждением контракта, предметом которого является выдача банковской гарантии.

**7. Ответственность Сторон**

7.1. Стороны несут ответственность за неисполнение и ненадлежащее исполнение Контракта, в том числе за неполное и (или) несвоевременное исполнение своих обязательств по Контракту.

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

7.3. Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного Контрактом, и устанавливается в размере одной трёхсотой действующей на дату уплаты пени ставки рефинансирования Центрального банка Российской Федерации от цены контракта, уменьшенной на сумму, пропорциональную объёму обязательств, предусмотренных контрактом и фактически исполненных Исполнителем, и определяется по формуле П = (Ц - В) x С (где Ц - цена контракта; В – стоимость фактически исполненного в установленный срок Исполнителем обязательства по контракту, определяемая на основании документа о приёмке товаров, результатов оказания услуг, в том числе отдельных этапов исполнения контрактов; С - размер ставки).

Размер ставки определяется по формуле С = СЦБ х ДП (где СЦБ – размер ставки рефинансирования, установленной Центральным банком Российской Федерации на дату уплаты пени, определяемый с учётом коэффициента К; ДП - количество дней просрочки).

Коэффициент К определяется по формуле К =ДП/ДК х 100% (где ДП - количество дней просрочки; ДК - срок исполнения обязательства по контракту (количество дней).

При К, равном 0 - 50 процентам, размер ставки определяется за каждый день просрочки и равным 0,01 ставки рефинансирования, установленной Центральным банком Российской Федерации на дату уплаты пени.

При К, равном 50 - 100 процентам, размер ставки определяется за каждый день просрочки и принимается равным 0,02 ставки рефинансирования, установленной Центральным банком Российской Федерации на дату уплаты пени.

При К, равном 100 процентам и более, размер ставки определяется за каждый день просрочки и принимается равным 0,03 ставки рефинансирования, установленной Центральным банком Российской Федерации на дату уплаты пени.

7.4. Штрафы начисляются за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных Контрактом*.* При этом штрафы не применяются в случае просрочки исполнения Исполнителем обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом. Размер штрафа устанавливается в сумме (10 процентов от цены Контракта, определённой в порядке, установленном постановлением Правительства Российской Федерации от 25.11.2013 № 1063).

7.5. Неустойка (штраф, пени) носит штрафной характер. При невыполнении обязательств по Контракту, кроме уплаты неустойки (штрафа, пени), Исполнитель возмещает в полном объёме понесённые Заказчиком убытки.

7.6. Исполнитель освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного Контрактом, произошло вследствие непреодолимой силы или по вине Заказчика.

7.7. В случае начисления Заказчиком Исполнителю неустойки (штрафа, пени) и (или) убытков, Заказчик направляет Исполнителю требование оплатить неустойку (штраф, пени) и (или) понесённые Заказчиком убытки, с указанием порядка и сроков соответствующей оплаты, но не более 5 дней со дня направления требования. В случае, если Исполнитель в добровольном порядке в установленный Заказчиком срок не оплатил неустойку (штраф, пени) и (или) убытки, Заказчик вправе уменьшить размер оплаты по Контракту на сумму начисленной неустойки (штрафа, пени) и (или) убытков в порядке, предусмотренном п. 2.5 Контракта. При этом исполнение обязательства Исполнителя по перечислению неустойки (штрафа, пени) и (или) убытков в доход бюджета возлагается на Заказчика.\*

7.8. В случае просрочки исполнения Заказчиком обязательств, предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Заказчиком обязательств, предусмотренных Контрактом, Исполнитель вправе потребовать уплаты неустоек (штрафов, пеней). Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного Контрактом, начиная со дня, следующего после дня истечения установленного Контрактом срока исполнения обязательства.

7.9. Пеня устанавливается Контрактом в размере одной трёхсотой действующей на дату уплаты пеней ставки рефинансирования Центрального банка Российской Федерации от не уплаченной в срок суммы.

7.10. Штрафы начисляются за неисполнение или ненадлежащее исполнение Заказчиком обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств, предусмотренных Контрактом. Размер штрафа составляет (2,5 процента от цены Контракта, определённой в порядке, установленном постановлением Правительства Российской Федерации от 25.11.2013 № 1063).

7.11. Заказчик освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного контрактом, произошло вследствие непреодолимой силы или по вине Исполнителя.

\* Последнее предложение п. 7.7 включается в случае, если заказчиком выступает получатель бюджетных средств. В гражданско-правовых договорах бюджетного учреждения данный пункт исключается (письмо Минфина России от 26.12.2011 № 02-11-00/5959).

**8. Форс-мажорные обстоятельства**

8.1. Стороны освобождаются от ответственности за частичное или полное невыполнение обязательств по Контракту, если оно явилось следствием обстоятельств непреодолимой силы (форс-мажор), а именно: пожара, наводнения, землетрясения, войны, военных действий, блокады, эмбарго, общих забастовок, запрещающих (либо ограничивающих) актов властей, и если эти обстоятельства непосредственно повлияли на исполнение Контракта.

8.2. Сторона, для которой создалась невозможность выполнения обязательств по Контракту, обязана немедленно (в течение 3 (трёх) дней) известить другую Сторону о наступлении и прекращении вышеуказанных обстоятельств. Несвоевременное извещение об этих обстоятельствах лишает, соответствующую Сторону права ссылается на них в будущем.

8.3. Обязанность доказать наличие обстоятельств непреодолимой силы лежит на Стороне Контракта, не выполнившей свои обязательства по Контракту.

Доказательством наличия вышеуказанных обстоятельств и их продолжительности будут служить документы Торгово-промышленной палаты Ханты-Мансийского автономного округа - Югры, или иной торгово-промышленной палаты, где имели место обстоятельства непреодолимой силы.

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

**9. Порядок разрешения споров**

9.1. Заказчик и Исполнитель должны приложить все усилия, чтобы путём прямых переговоров разрешить к обоюдному удовлетворению Сторон все противоречия или спорные вопросы, возникающие между ними в рамках Контракта.

9.2. При недостижении взаимоприемлемого решения Стороны вправе передать спорный вопрос на разрешение в судебном порядке в Арбитражном суде Ханты-Мансийского автономного округа – Югры.

**10. Расторжение Контракта**

10.1. Расторжение Контракта допускается по соглашению Сторон, по решению суда, а также в случае одностороннего отказа Стороны Контракта от исполнения Контракта в соответствии с гражданским законодательством.

10.2. Расторжение Контракта по соглашению Сторон совершается в письменной форме и возможно в случае наступления условий, при которых для одной из Сторон или обеих Сторон дальнейшее исполнение обязательств по Контракту не возможно либо возникает нецелесообразность исполнения Контракта.

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

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

10.5. Заказчик вправе принять решение об одностороннем отказе от исполнения Контракта. До принятия такого решения Заказчик вправе провести экспертизу оказанных услуг с привлечением экспертов, экспертных организаций.

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

10.7. Решение Заказчика об одностороннем отказе от исполнения Контракта в течение одного рабочего дня, следующего за датой принятия указанного решения, размещается в единой информационной системе и направляется Исполнителю по почте заказным письмом с уведомлением о вручении по адресу Исполнителя, указанному в разделе 13 Контракта, а также телеграммой, либо посредством факсимильной связи, либо по адресу электронной почты, либо с использованием иных средств связи и доставки, обеспечивающих фиксирование такого уведомления и получение Заказчиком подтверждения о его вручении Исполнителю. Выполнение Заказчиком вышеуказанных требований считается надлежащим уведомлением Исполнителя об одностороннем отказе от исполнения Контракта. Датой такого надлежащего уведомления признается дата получения Заказчиком подтверждения о вручении Исполнителю указанного уведомления либо дата получения Заказчиком информации об отсутствии Исполнителя по его адресу, указанному в разделе 13 Контракта. При невозможности получения указанных подтверждения либо информации датой такого надлежащего уведомления признается дата по истечении тридцати дней с даты размещения решения Заказчика об одностороннем отказе от исполнения Контракта в единой информационной системе.

10.8. Решение Заказчика об одностороннем отказе от исполнения Контракта вступает в силу и Контракт считается расторгнутым через десять дней с даты надлежащего уведомления Заказчиком Исполнителя об одностороннем отказе от исполнения Контракта.

10.9. Заказчик обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения Контракта, если в течение десятидневного срока с даты надлежащего уведомления Исполнителя о принятом решении об одностороннем отказе от исполнения Контракта устранено нарушение условий Контракта, послужившее основанием для принятия указанного решения, а также Заказчику компенсированы затраты на проведение экспертизы, предусмотренной п. 10.5 Контракта. Данное правило не применяется в случае повторного нарушения Исполнителем условий Контракта, которые в соответствии с гражданским законодательством являются основанием для одностороннего отказа Заказчика от исполнения Контракта.

10.10. Заказчик принимает решение об одностороннем отказе от исполнения Контракта, если в ходе исполнения Контракта будет установлено, что Исполнитель не соответствует установленным документацией о закупке требованиям к участникам закупки или предоставил недостоверную информацию о своём соответствии таким требованиям, что позволило ему стать победителем определения Исполнителя.

10.11. Исполнитель вправе принять решение об одностороннем отказе от исполнения Контракта в соответствии с гражданским законодательством. Такое решение в течение одного рабочего дня, следующего за датой его принятия, направляется Заказчику по почте заказным письмом с уведомлением о вручении по адресу Заказчика, указанному в разделе 13 Контракта, а также телеграммой, либо посредством факсимильной связи, либо по адресу электронной почты, либо с использованием иных средств связи и доставки, обеспечивающих фиксирование такого уведомления и получение Заказчиком подтверждения о его вручении Заказчику. Выполнение Исполнителем вышеуказанных требований считается надлежащим уведомлением Заказчика об одностороннем отказе от исполнения Контракта. Датой такого надлежащего уведомления признается дата получения Исполнителем подтверждения о вручении Заказчику указанного уведомления.

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

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

10.14. При расторжении Контракта в связи с односторонним отказом Стороны Контракта от исполнения Контракта другая Сторона Контракта вправе потребовать возмещения только фактически понесённого ущерба, непосредственно обусловленного обстоятельствами, являющимися основанием для принятия решения об одностороннем отказе от исполнения Контракта.

**11.Срок действия Контракта**

11.1. Контракт вступает в силу со дня подписания его Сторонами и действует до 15.11.2016. С 16.11.2016 обязательства Сторон по Контракту прекращаются, за исключением обязательств по оплате услуг, гарантийных обязательств, обязательств по возмещению убытков и выплате неустойки.

**12. Прочие условия**

12.1. Контракт составлен в форме электронного документа. После заключения Контракта Стороны вправе изготовить копию Контракта на бумажном носителе в 2 (двух) экземплярах, имеющих одинаковую юридическую силу, по одному для Заказчика и Исполнителя.

12.2. Все приложения к Контракту являются его неотъёмной частью.

12.3. К Контракту прилагаются:

- Техническое задание (Приложение).

12.4. В случае изменения наименования, адреса места нахождения или банковских реквизитов Стороны, она письменно извещает об этом другую Сторону в течение 3 рабочих дней с даты такого изменения.

12.5. По согласованию Сторон в ходе исполнения Контракта допускается снижение цены Контракта без изменения предусмотренных Контрактом объёма работы, качества выполняемой работы и иных условий Контракта.

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

12.7. В случае перемены Заказчика по контракту права и обязанности Заказчика по такому контракту переходят к новому заказчику в том же объёме и на тех же условиях.

**13. Адреса места нахождения, банковские реквизиты и подписи Сторон**

|  |  |
| --- | --- |
| Заказчик  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_ 20\_\_ г.  М.П. | Исполнитель  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_ 20\_\_ г.  М.П. |

Согласовано:

Работник контрактной службы: Дергилев О.В.

Главный бухгалтер: Михайлова Л.А.

Юридическое управление: Соломыкин В.А.

Приложение

к Муниципальному контракту

№ \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_ 201\_\_ г.

**Техническое задание**

**1.** **Предмет муниципального контракта**: оказание услуг по продлению лицензий на подсистему централизованной антивирусной обработки (код ОКПД2: 63.11.13.000).

**2. Общие требования:**

2.1. Место предоставления услуг: по месту нахождения Исполнителя.

2.2. Исполнитель обеспечивает предусмотренную производителем функциональность программного обеспечения в рамках продления действующей лицензии на подсистему централизованной антивирусной обработки Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition № 1B08-140912-051232 (на 200 защищаемых объектов).

**3. Перечень предоставляемых услуг:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Наименование услуг | Характеристика предоставляемых услуг | Ед.  изм. | Кол-во |
| 1 | Продление лицензий на подсистему централизованной антивирусной обработки | Состав предоставляемых услуг:  Продление действующей лицензии на антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition на срок 1 год с учётом имеющейся у Заказчика лицензии (на 200 защищаемых объектов).  Комплектация:  - ключевой файл для активации программного обеспечения;  - экземпляр лицензионного соглашения с правообладателем программного обеспечения (ЗАО «Лаборатория Касперского»). | шт | 200 |

**4. Требования к поставляемому программному обеспечению:**

4.1. Назначение подсистемы централизованной антивирусной обработки:

- Защита рабочих станций от вредоносных программ;

- Защита файловых серверов;

- Безопасность мобильных устройств;

- Управление мобильными устройствами;

- Контроль программ, устройств и веб-ресурсов.

4.2. Общие требования к программному обеспечению:

Антивирусные средства должны включать:

• программные средства антивирусной защиты для рабочих станций Windows;

• программные средства антивирусной защиты для рабочих станций Mac OS;

• программные средства антивирусной защиты для рабочих станций Linux;

• программные средства антивирусной защиты для файловых серверов Windows;

• программные средства антивирусной защиты для файловых серверов Mac OS;

• программные средства антивирусной защиты для файловых серверов Linux;

• программные средства антивирусной защиты для файловых серверов Novell Netware;

• программные средства антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows;

• программные средства антивирусной защиты для мобильных устройств (смартфонов);

• программные средства централизованного управления, мониторинга и обновления;

• обновляемые базы данных сигнатур вредоносных программ и атак;

• эксплуатационную документацию на русском языке.

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

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

4.3. Требования к программным средствам антивирусной защиты для рабочих станций Windows:

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

• Microsoft Windows XP Professional (SP3 или выше);

• Microsoft Windows Vista Business/Enterprise/Ultimate (SP2 или выше);

• Microsoft Windows Vista Business/Enterprise/Ultimate x64 (SP2 или выше);

• Microsoft Windows 7 Professional/Enterprise/Ultimate;

• Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

• Microsoft Windows 8 Professional/Enterprise;

• Microsoft Windows 8 Professional/Enterprise x64 Edition.

Программные средства антивирусной защиты для рабочих станций Windows должны обеспечивать реализацию следующих функциональных возможностей:

• Резидентный антивирусный мониторинг;

• Программные средства защиты от сетевых атак;

• Эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• Обнаружение скрытых процессов;

• Антивирусное сканирование по команде пользователя или администратора и по расписанию;

• Антивирусная проверка и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;

• Антивирусная проверка и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем;

• Облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;

• Защита электронной корреспонденции, как от вредоносных программ, так и от спама, с проверкой трафика на следующих протоколах: IMAP, SMTP, POP3 — независимо от используемого почтового клиента; независимо от типа протокола (в том числе MAPI, HTTP) — в рамках работы плагинов, встроенных в почтовые программы Microsoft Office Outlook и The Bat!;

• Защита веб-трафика — проверка объектов, поступающих на компьютер пользователя по протоколам HTTP, FTP;

• Проверка скриптов — проверка скриптов, обрабатываемых в Microsoft Internet Explorer, а также WSH-скриптов (таких как Java Script, Visual Basic Script и др.), запускаемых при работе пользователя на компьютере, в том числе и в интернете;

• Проверка трафика ICQ и MSN, для обеспечения безопасности работы с интернет-пейджерами;

• Запуск задач по расписанию и/или сразу после загрузки операционной системы;

• Защита от ещё не известных вредоносных программ на основе анализа их поведения и контроля изменений системного реестра, с возможностью автоматического восстановления изменённых вредоносной программой значений системного реестра;

• Автоматический контроль программ, запускаемых на компьютере пользователя, осуществляющий контроль активности программ и ограничивающий выполнение опасных действий;

• Защита от хакерских атак с использованием межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа, включая беспроводные;

• Проверка протокола IPv6;

• Защита от программ-маскировщиков, программ автодозвона на платные сайты;

• Блокировка баннеров, всплывающих окон, вредоносных сценариев, загружаемых с Web-страниц;

• Распознавание и блокировка фишинг-сайтов;

• Наличие компонента, дающего возможность создания специальных правил, запрещающих установку и/или запуск программ. Компонент должен контролировать приложения по пути нахождения программы, метаданным, контрольной сумме MD5;

• Осуществление контроля работы пользователя с внешними устройствами ввода/вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям;

• Ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• Запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям;

• Интеграция с системой обновления Windows Update для установки патчей, закрывающих обнаруженные уязвимости;

• Гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

• Настройка проверки критических областей компьютера в виде отдельной задачи;

• Технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющие избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;

• Возможность установки только выбранных компонентов программного средства антивирусной защиты;

• Централизованное управление с помощью единой системы управления.

4.4. Требования к программным средствам антивирусной защиты для рабочих станций и файловых серверов Mac:

Программные средства антивирусной защиты систем рабочих станций и серверов под управлением семейства ОС MAC должны функционировать на следующих версиях ОС:

Рабочие станции/ноутбуки:

• Mac OS X 10.6 (32/64 бит) - Snow Leopard;

• Mac OS X 10.5 (32 бит) – Leopard;

• Mac OS X 10.4 (32 бит) – Tiger.

Серверы:

• Mac OS X Server 10.6.

Программные средства антивирусной защиты систем рабочих станций и серверов под управлением семейства ОС MAC должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• централизованно управляться с помощью единой системы управления.

4.5. Требования к программным средствам антивирусной защиты для рабочих станций Linux:

Программные средства антивирусной защиты рабочих станций под управлением ОС Linux должны функционировать под управлением следующих платформ:

• 32-битные платформы:

 Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92);

 Fedora 9 (kernel 2.6.25);

 SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21);

 OpenSUSE Linux 11.0 (kernel 2.6.25);

 Debian GNU/Linux 4.0 r4 (kernel 2.6.24);

 Mandriva Corporate Desktop 4 (kernel 2.6.12);

 Ubuntu 8.04.1 Desktop Edition (kernel 2.6.25);

 Linux XP Enterprise Desktop 2008 (2.6.25.10-47.3.lxp2008);

 Red Hat Enterprise Linux 5.5 Desktop;

 Red Hat Enterprise Linux 6 Desktop;

 Fedora 14;

 CentOS-5.5;

 SUSE Linux Enterprise Desktop 10 SP3;

 SUSE Linux Enterprise Desktop 11 SP1;

 openSUSE Linux 11.3;

 Debian GNU/Linux 6.0.1;

 Mandriva Linux 2010;

 Ubuntu 10.04 LTS Desktop Edition.

• 64-битные платформы:

 Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92);

 Fedora 9 (kernel 2.6.25);

 SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21);

 OpenSUSE Linux 11.0 (kernel 2.6.25);

 Red Hat Enterprise Linux 5.5;

 Red Hat Enterprise Linux 6 Desktop;

 Fedora 14;

 CentOS-5.5;

 SUSE Linux Enterprise Desktop 10 SP3;

 SUSE Linux Enterprise Desktop 11 SP1;

 openSUSE Linux 11.3;

 Debian GNU/Linux 6.0.1;

 Ubuntu 10.04 LTS Desktop.

Программные средства антивирусной защиты рабочих станций под управлением ОС Linux должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверку и лечение файлов в архивах;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• помещение подозрительных и поврежденных объектов на карантин;

• возможность экспортировать и сохранять отчеты в форматах HTML и CSV;

• возможность перехвата и проверки файловых операций на уровне SAMBA;

• гибкого управления использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

• сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;

• возможность управление через графический интерфейс;

• централизованно управляться с помощью единой системы управления.

4.6. Требования к программным средствам антивирусной защиты для файловых серверов Windows:

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

• Microsoft Small Business Server 2011 Essentials х64 Edition;

• Microsoft Small Business Server 2011 Standard х64 Edition;

• Microsoft Windows Server 2012 Foundation х64 Edition;

• Microsoft Windows Server 2012 Essentials х64 Edition;

• Microsoft Windows Server 2012 Standard х64 Edition;

• Microsoft Windows Server 2008 R2 Standard / Enterprise х64 Edition SP0 и выше;

• Microsoft Windows Server 2008 Standard / Enterprise х64 Edition SP2 и выше;

• Microsoft Windows Server 2008 Standard / Enterprise SP2 и выше;

• Microsoft Windows Server 2003 R2 Standard / Enterprise SP2 и выше;

• Microsoft Windows Server 2003 R2 Standard х64 Edition SP2 и выше;

• Microsoft Windows Server 2003 Standard SP2;

• Microsoft Windows Server 2003 Standard х64 Edition SP2.

Программные средства антивирусной защиты для файловых серверов Windows должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

• программные средства защиты от сетевых атак;

• защиту от хакерских атак, путем использования межсетевого экрана с системой обнаружения и предотвращения вторжений (IDS/IPS) и правилами сетевой активности для наиболее популярных приложений при работе в вычислительных сетях любого типа;

• облачная защита от новых угроз, позволяющая приложению в режиме реального времени обращаться к специальным сайтам производителя, для получения вердикта по запускаемой программе или файлу;

• обнаружение скрытых процессов;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверку и лечение файлов, упакованных программами типа PKLITE, LZEXE, DIET, EXEPACK и пр.;

• антивирусную проверку и лечение файлов в архивах форматов RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, в том числе и защищенных паролем;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• защиту от еще не известных вредоносных программ, принадлежащих зарегистрированным семействам, на основе эвристического анализа;

• ускорения процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

• настройки проверки критических областей сервера в качестве отдельной задачи;

• регулировки распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: возможность продолжать антивирусное сканирование в фоновом режиме;

• наличием множественных путей уведомления администраторов о важных произошедших событиях (почтовое сообщение, звуковое оповещение, всплывающее окно, запись в журнал событий);

• технологии самозащиты приложения, защиты от удаленного несанкционированного управления сервисом приложения, защита файлов приложения от несанкционированного доступа и изменения, а также защиты доступа к параметрам приложения с помощью пароля, позволяющими избежать отключения защиты со стороны вредоносных программ, злоумышленников или неквалифицированных пользователей;

• централизованно управляться с помощью единой системы управления.

4.7. Требования к программным средствам антивирусной защиты для файловых серверов Linux:

Программные средства антивирусной защиты серверов под управлением ОС Linux должны функционировать под управлением следующих платформ:

• 32-битные платформы:

 Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92);

 Red Hat Enterprise Linux 5.5 Server 2.6.18-186.el5;

 Red Hat Enterprise Linux 6 Server 2.6.32-71.el6.i686;

 Fedora 9 (kernel 2.6.25);

 Fedora 13 2.6.33.3-85.fc13.i686.PAE;

 CentOS-5.5 2.6.18-194.el5;

 Novel Open Enterprise Server 2 (kernel 2.6.16.46-0.12);

 Novel Open Enterprise Server 2 SP2 2.6.16.60-0.54.5-default;

 SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21);

 SUSE Linux Enterprise Server 10 SP3 2.6.16.60-0.54.5-default;

 SUSE Linux Enterprise Server 11 SP1 2.6.32.12-0.7-pae;

 OpenSUSE Linux 11.0 (kernel 2.6.25);

 OpenSUSE Linux 11.3 2.6.34-12-desktop;

 Debian GNU/Linux 4.0 r4 (kernel 2.6.24);

 Debian GNU/Linux 5.0.5 2.6.26-2-686;

 Mandriva Corporate Server 4 (kernel 2.6.12);

 Mandriva Enterprise Server 5.1 2.6.27.45-desktop-1mnb;

 Ubuntu 8.04.1 Server Edition (kernel 2.6.25);

 Ubuntu 10.04 Server Edition 2.6.32-21-generic;

 FreeBSD 7.3-RELEASE;

 FreeBSD 8.1-RELEASE.

• 64-битные платформы:

 Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92);

 Red Hat Enterprise Linux 5.5 server 2.6.18-194.el5;

 Red Hat Enterprise Linux 6 Server 2.6.32-71.el6.x86\_64;

 Fedora 9 (kernel 2.6.25);

 Fedora 13 2.6.33.3-85.fc13.x86\_64;

 CentOS-5.5 2.6.18-194.el5;

 SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21);

 SUSE Linux Enterprise Server 10 SP3 2.6.16.60-0.54.5-default;

 SUSE Linux Enterprise Server 11 SP1 2.6.32.12-0.7-default;

 Novell Open Enterprise Server 2 SP2 2.6.16.60-0.54.5-default;

 OpenSUSE Linux 11.3 2.6.34-12-desktop;

 OpenSUSE Linux 11.0 (kernel 2.6.25);

 Debian GNU/Linux 5.0.5 2.6.26-2-amd64;

 Ubuntu 10.04 Server Edition 2.6.32-21-generic;

 FreeBSD 7.3-RELEASE;

 FreeBSD 8.1-RELEASE.

Программные средства антивирусной защиты серверов под управлением ОС Linux должны обеспечивать реализацию следующих функциональных возможностей:

• резидентный антивирусный мониторинг;

• антивирусное сканирование по команде пользователя или администратора и по расписанию;

• антивирусную проверку и лечение файлов в архивах;

• запуск задач по расписанию и/или сразу после загрузки операционной системы;

• помещение подозрительных и поврежденных объектов на карантин;

• формирование отчетов в форматах HTML, CSV, PDF и XLS;

• возможность перехвата и проверки файловых операций на уровне SAMBA;

• сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;

• удаленно через веб-браузер управлять антивирусом и настраивать его;

• централизованно управляться с помощью единой системы управления.

4.8. Требования к программным средствам антивирусной защиты для серверов масштаба предприятия и терминальных серверов Windows:

Программные средства антивирусной защиты серверов масштаба предприятия под управлением семейства ОС Microsoft Windows и терминальных серверов должны функционировать на следующих версиях ОС:

• 32-битные платформы:

 Microsoft Windows Server 2003 Standard Edition с пакетом обновлений 1 или выше;

 Microsoft Windows Server 2003 Enterprise Edition с пакетом обновлений 1 или выше;

 Microsoft Windows Server 2003 R2 Standard Edition и выше;

 Microsoft Windows Server 2003 R2 Enterprise Edition и выше;

 Microsoft Windows Server 2008 Standard Edition;

 Microsoft Windows Server 2008 Enterprise Edition;

 Microsoft Windows Server 2008 Data Center Edition;

 Microsoft Windows Server 2008 Core Standard Edition;

 Microsoft Windows Server 2008 Core Enterprise Edition;

 Microsoft Windows Server 2008 Core Data Center Edition.

• 64-битные платформы:

 Microsoft Windows Server 2003 x64 Standard Edition;

 Microsoft Windows Server 2003 x64 Enterprise Edition;

 Microsoft Windows Server 2003 R2 Standard x64 Edition;

 Microsoft Windows Server 2003 R2 Enterprise x64 Edition;

 Microsoft Windows Server 2008 x64 Standard Edition;

 Microsoft Windows Server 2008 x64 Enterprise Edition;

 Microsoft Windows Server 2008 x64 Data Center Edition;

 Microsoft Windows Server 2008 Core x64 Standard Edition;

 Microsoft Windows Server 2008 Core x64 Enterprise Edition;

 Microsoft Windows Server 2008 Core x64 Data Center Edition;

 Microsoft Windows Server 2008 R2 Standard Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Enterprise Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Datacenter Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Core Standard Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Core Enterprise Edition Release с пакетом обновлений SP1;

 Microsoft Windows Server 2008 R2 Core Datacenter Edition Release с пакетом обновлений SP1;

 Microsoft Windows Hyper-V Server 2008 R2 Release с пакетом обновлений SP1.

• Терминальные серверы:

 Microsoft Terminal на базе Windows 2003 Server;

 Microsoft Terminal на базе Windows Server 2008;

 Citrix Presentation Server 4.0;

 Citrix Presentation Server 4.5;

 Citrix XenApp 4.5;

 Citrix XenApp 5.0;

 Citrix XenApp 6.0.

Программные средства антивирусной защиты серверов масштаба предприятия под управлением семейства ОС Microsoft Windows и терминальных серверов должны обеспечивать реализацию следующих функциональных возможностей:

• Осуществление антивирусной проверки на серверах, выполняющих разные функции:

 Серверов терминалов и принт-серверов;

 Серверов приложений и контроллеров доменов;

 Файловых серверов.

• Возможность использования для защиты кластера серверов;

• Возможность защиты систем хранения данных EMC Celerra;

• Определение в объектах файловой системы сервера угрозы следующих типов:

 Классических вирусов;

 Сетевых червей;

 Троянских программ;

 Прочих вредоносных программ;

 Программ-реклам;

 Программ порнографического содержания;

 Потенциально опасных приложений.

• Проверка следующих объектов защищаемого сервера при доступе к ним:

 Файлов при их записи и считывании;

 Альтернативных потоков файловых систем (NTFS-streams);

 Главной загрузочной записи и загрузочных секторов локальных жестких дисков и съемных носителей.

• Предотвращение вирусных эпидемий за счет фиксации возникновения вирусных атак;

• Восстановление после заражения путем удаления всех связанных с ликвидированным вредоносным объектом записей в системных файлах и реестре ОС, что предотвращает возможные сбои в работе операционной системы;

• 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;

• Проверка по требованию, заключающаяся в однократной полной или выборочной проверке на наличие угроз объектов на сервере;

• Помещение подозрительных и поврежденных объектов на карантин;

• При защите терминальных серверов поддержка режимов публикации рабочего стола и публикации приложений;

• Масштабируемость за счет задания количества рабочих процессов антивируса для ускорения обработки запросов к серверу при использовании многопроцессорных серверов;

• Балансировка загрузки путем регулирования распределения ресурсов сервера между антивирусом и другими приложениями в зависимости от приоритетности задач: антивирусная проверка может продолжаться в фоновом режиме;

• Выбор доверенных процессов путем исключения из проверки безопасных процессов, работа которых может замедляться при антивирусной проверке (процесс резервного копирования данных, программы дефрагментации жесткого диска и другие);

• Разделение прав администраторов, основанное на стандартных механизмах ОС Microsoft Windows;

• Уведомления различными методами администраторов и пользователей о событиях в антивирусной защите. Поддержка Simple Network Management Protocol (SNMP;

• Cовместимость с системами управления дисковым пространством (Hierarchical Storage Management), позволяющая настраивать способы проверки для Offline Files;

• Оптимизация для использования на многопроцессорных серверах на базе технологии Intel Xeon™, позволяющая использовать приложение в условиях высоких нагрузок;

• Возможность управления с помощью MMC консоли;

• Централизованно управляться с помощью единой системы управления.

4.9. Требования к программным средствам антивирусной защиты смартфонов:

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

• Android 2.2 – 2.x, 4.0; Android 3 for tablets;

• iOS 4, 5;

• BlackBerry 4.5 – 6.0, 7.0; BlackBerry for tablets;

• Windows Mobile 5.0 – 6.5;

• Symbian 9.1 – 9.3, Symbian 3, Anna, Belle.

Программные средства для антивирусной защиты смартфонов должны обеспечивать следующую функциональность:

• постоянную защиту файловой системы смартфона, перехват и проверку:

• всех входящих объектов, передающихся с помощью беспроводных соединений (инфракрасный порт, Bluetooth), сообщений EMS и MMS, при синхронизации с персональным компьютером и загрузке файлов через браузер;

• файлов, открываемых на смартфоне;

• программ, устанавливаемых из интерфейса смартфона.

• проверку объектов файловой системы, находящихся на смартфоне или на подключенных картах расширения памяти, по требованию пользователя и по расписанию;

• надежное изолирование зараженных объектов в карантинном хранилище;

• обновление антивирусных баз, используемых при поиске вредоносных программ и удалении опасных объектов;

• блокирование нежелательных SMS и MMS сообщений;

• шифрование наиболее важных файлов, папок и карты памяти;

• возможность скрывать важные контакты и историю общения с ними;

• осуществлять функцию «антивор», т.е. обеспечивать блокировку мобильного устройства, удаление данных, сообщений и книги контактов, получение координат местоположения, а также определение, у кого находится пропавшее устройство.

4.10. Требования к системе управления антивирусной защитой:

Программные средства управления для защищаемых рабочих станций, файловых серверов и смартфонов должны функционировать на следующих операционных системах:

Сервер администрирования:

• Microsoft Windows XP Professional SP2 и выше;

• Microsoft Windows XP Professional x64 и выше;

• Microsoft Windows Server 2003 и выше;

• Microsoft Windows Server 2003 x64 и выше;

• Microsoft Windows Vista SP1 и выше;

• Microsoft Windows Vista x64 SP1 и всеми текущими обновлениями;

• Microsoft Windows Server 2008;

• Microsoft Windows Server 2008, развернутая в режиме Server Core;

• Microsoft Windows Server 2008 x64 SP1 и всеми текущими обновлениями;

• Microsoft Windows Server 2008 R2;

• Microsoft Windows Server 2012;

• Microsoft Windows Small Business Server 2003;

• Microsoft Windows Small Business Server 2008;

• Microsoft Windows Small Business Server 2011;

• Microsoft Windows 7 Professional/Enterprise/Ultimate;

• Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

• Microsoft Windows 8;

• Microsoft Windows 8 x64.

Сервером администрирования должна использоваться одна из следующих СУБД:

• Microsoft SQL Express 2005;

• Microsoft SQL Express 2008;

• Microsoft SQL Express 2008 R2;

• Microsoft SQL Express 2012;

• Microsoft SQL Server 2005;

• Microsoft SQL Server 2008;

• Microsoft SQL Server 2008 R2;

• Microsoft SQL Server 2012;

• MySQL 5.0.67, 5.0.77, 5.0.85, 5.0.87(SP1), 5.0.91;

• MySQL Enterprise 5.0.60(SP1), 5.0.70, 5.0.82(SP1), 5.0.90.

Консоль администрирования:

• Microsoft Windows XP Professional SP2 и выше;

• Microsoft Windows XP Professional x64 и выше;

• Microsoft Windows Server 2003 и выше;

• Microsoft Windows Server 2003 x64 и выше;

• Windows Small Business Server 2003;

• Microsoft Windows Vista SP1 и выше;

• Microsoft Windows Vista x64 SP1 и всеми текущими обновлениями;

• Microsoft Windows Server 2008;

• Microsoft Windows Server 2008 x64 SP1 и всеми текущими обновлениями;

• Windows Small Business Server 2008 x64;

• Microsoft Windows Server 2008 x64 R2;

• Microsoft Windows Server 2008 x64 R2 SP1;

• Windows Small Business Server 2011 x64;

• Microsoft Windows 8;

• Microsoft Windows 8 x64;

• Microsoft Windows 7 Professional/Enterprise/Ultimate SP1;

• Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1.

Агент администрирования: программные требования должны соответствовать требованиям к программным средствам антивирусной защиты.

Программные средства управления для всех защищаемых ресурсов должны обеспечивать реализацию следующих функциональных возможностей:

• установка системы антивирусной защиты из единого дистрибутива;

• выбор установки в зависимости от количества защищаемых узлов;

• создание групп логической сети на основе структуры Active Directory;

• автоматическое распределение компьютеров по группам управления, в случае появления новых компьютеров в сети;

• централизованную установку/обновление/удаление программных средств антивирусной защиты, настройку, администрирование, просмотр отчетов и статистической информации по их работе;

• централизованное удаление несовместимых приложений;

• централизованное управление установкой/запуском программ на компьютерах пользователей с возможностью контроля программ по пути нахождения программы, метаданным, MD5 контрольной сумме и возможностью присвоения привилегий определенным пользователям;

• централизованное управление доступом к веб-ресурсам с компьютеров пользователей, с возможностью фильтрации по категориям и типу данных загружаемого контента, гибко задавать параметры времени действия правил и возможностью присвоения привилегий определенным пользователям;

• наличие различных методов установки антивирусных приложений: удаленный - RPC, GPO, агент администрирования, локальный - автономный пакет установки;

• удаленная установка программных средств антивирусной защиты с последней версией баз приложения;

• автоматизированное обновление программных средств антивирусной защиты и антивирусных баз;

• автоматизированный поиск уязвимостей, в установленных приложения и операционной системе, на компьютерах пользователей;

• тестирование загруженных обновлений средствами сервера администрирования перед распространением на клиентские машины; доставку 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;

• централизованное осуществление контроля работы пользователя с внешними устройствами ввода / вывода, позволяя ограничивать доступ к внешним USB-носителям, мультимедийным устройствам и другим устройствам хранения данных, с возможностью создавать доверенные устройства по их идентификатору и возможностью предоставлять привилегии, для запуска внешних устройств, определенным пользователям;

• построение многоуровневой системы управления с возможностью настройки ролей администраторов и операторов, а также форм предоставляемой отчетности на каждом уровне;

• создание виртуальных серверов управления антивирусным приложением;

• 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;

• централизованный сбор информации и создание отчетов о состоянии антивирусной защиты;

• инвентаризация установленного ПО и оборудования на компьютерах пользователей;

• наличие механизма оповещения о событиях в работе установленных приложений антивирусной защиты и настройку рассылки почтовых уведомлений о них;

• функция для управления мобильными устройствами сервер Exchange ActiveSync;

• функция для управления мобильными устройствами сервер iOS MDM;

• возможность отправки SMS-сообщений мобильным пользователям;

• централизованная установка приложений на управляемые мобильные устройства;

• централизованная установка сертификатов на управляемые мобильные устройства;

• централизованный сбор информации о всех установленных на клиентских компьютерах приложениях;

• интеграция с CISCO NAC и MS NAP;

• экспорта 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;

• поддержка Windows Failover Clustering;

• наличие веб-консоли управления приложением;

• наличие системы контроля возникновения вирусных эпидемий.

Требования к обновлению антивирусных баз:

Обновляемые антивирусные базы данных должны обеспечивать реализацию следующих функциональных возможностей:

• регламентное обновление антивирусных баз не реже 24 раз в течение календарных суток, а баз антиспама не реже одного раза в 5 минут;

• множественность путей обновления, в том числе – по каналам связи и на отчуждаемых электронных носителях информации;

• проверку целостности и подлинности обновлений средствами электронной цифровой подписи.

Требования к эксплуатационной документации:

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

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

Требования к технической поддержке:

Техническая поддержка антивирусного программного обеспечения должна:

• Предоставляться на русском языке сертифицированными специалистами производителя средств антивирусной защиты и его партнёров на всей территории Российской Федерации круглосуточно без праздников и выходных по телефону, электронной почте и через Интернет;

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

|  |  |
| --- | --- |
| **Заказчик**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_ 20\_\_ г.  М.П. | **Исполнитель**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_» \_\_\_\_\_\_ 20\_\_ г.  М.П. |

1. *Единая информационная система контрактной системы в сфере закупок (единая информационная система, ЕИС) - совокупность информации, указанной в части 3 статьи 4 Закона о контрактной системе и содержащейся в базах данных, информационных технологий и технических средств, обеспечивающих формирование, обработку, хранение такой информации, а также ее предоставление с использованием официального сайта единой информационной системы в информационно-телекоммуникационной сети «Интернет». До ввода в эксплуатацию ЕИС информация размещается на сайте ‑ www.zakupki.gov.ru.* [↑](#footnote-ref-1)