|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ:Глава администрации города Югорска\_\_\_\_\_\_\_\_\_\_М.И. Бодак«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 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 технической защите информации**

**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.11Почтовый адрес Заказчика: 628260, Ханты-Мансийский автономный округ – Югра, г. Югорск, ул.40 лет Победы, д.11Телефон: 8 (34675) 5-00-61Адрес электронной почты: inform@ugorsk.ruОтветственное 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 администрации 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  |
| 1.
 | Наименование оператора электронной площадки | Наименование: ЗАО «Сбербанк - АСТ» |
| Адрес электронной площадки в информационно-телекоммуникационной сети «Интернет» | http://sberbank-ast.ru/ |
| 1.
 | 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 технической защите информации |
|  | 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 | Ханты-Мансийский автономный округ – Югра, г.Югорск, ул.40 лет Победы, д.11 |
|  | Сроки оказания услуг | в течение 40 дней с момента подписания муниципального контракта |
|  | Начальная (максимальная) цена контракта | 493 430 (четыреста девяносто три тысячи четыреста тридцать) 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 |
| 1.
 | 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 «12» апреля 2016 года;дата окончания предоставления разъяснений положений документации об аукционе «17» апреля 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). |
| 1.
 | 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 «19» апреля 2016 года. |
| 1.
 | Дата окончания срока рассмотрения частей заявок на участие в электронном аукционе  | «21» апреля 2016 года |
| 1.
 | Дата проведения электронного аукциона |  «25» апреля 2016 года |
| 1.
 | 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, а также конкретные показатели используемого товара, соответствующие значениям, установленным в части II «Техническое задание» настоящей документации, и указание на товарный знак (его словесное обозначение) (при наличии), знак обслуживания (при наличии), фирменное наименование (при наличии), патенты (при наличии), полезные модели (при наличии), промышленные образцы (при наличии), наименование страны происхождения товара. Участник закупки также указывает страну происхождения товара[[2]](#footnote-2) в случае, если в пункте 39 настоящего раздела предусмотрено предоставление преференций участникам закупки, заявки на участие в аукционе которых содержат предложения о поставке товаров, произведённых на территории государств – членов Евразийского экономического союза. 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: 1) Лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации по видам деятельности:
2. - контроль защищённости конфиденциальной информации от утечки по техническим каналам в: средствах и системах информатизации; технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещённых в помещениях, где она обрабатывается; помещениях со средствами (системами), подлежащими защите; помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);
3. - аттестационные испытания и аттестация на соответствие требованиям по защите информации: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
4. - проектирование в защищённом исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
5. - установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищённых технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищённых программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищённости информации).
6. Лицензирование осуществляется в соответствии с п.п. 5 п. 1 ст. 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», постановлением Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» в связи с необходимостью осуществления установки и настройки поставляемого товара (средств защиты информации).
7. 2) Лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) на следующие пункты:
8. - монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств (п.12 перечня);
9. - передачу шифровальных (криптографических) средств (п.21 перечня).
10. Лицензирование осуществляется в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Порядок лицензирования определён постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».
11. 3) Лицензию ФСБ России на осуществление работ с использованием сведений, составляющих государственную тайну;
12. 4) Лицензию ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны;

5) Лицензию ФСБ России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны, включающей в себя:- проведение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в технических средствах.1. Лицензирование осуществляется в соответствии с п.п. 3 п.1 ст. 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», постановлением Правительства РФ от 16.04.2012 № 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;
2. 6) Действующий аттестат аккредитации, зарегистрированный в Государственном реестре системы сертификации средств защиты информации по требованиям безопасности, выданный ФСТЭК России, в соответствии с положением о сертификации средств защиты информации по требованиям безопасности информации, утверждённым приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199;

**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»;- документы, подтверждающие соответствие предлагаемого товара (программного обеспечения) запретам, установленным в соответствии с Постановлением Правительства РФ от 16 ноября 2015 г. № 1236 "Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд»;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 |
| 1.
 | 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 4 934 (четыре тысячи девятьсот тридцать четыре) рубля 30 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.  |
| 1.
 | 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). |
| 1.
 | 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 24 671 (двадцать четыре тысячи шестьсот семьдесят один) рубль 50 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 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 гарантии6) 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 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. |
| 1.
 | 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 технической защите информации» |
|  | 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. |
| 1.
 | 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. |
| 1.
 | 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»: 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 технической защите информации.

**2. Используемые сокращения:**

АРМ - автоматизированное рабочее место;

ЗИС - защищенная информационная система;

НСД - несанкционированный доступ;

ПО - программное обеспечение;

ОИ - объект информатизации;

ЗОИ - защищенный объект информатизации;

СЗИ - средства защиты информации;

СКЗИ - средства криптографической защиты информации;

СВТ - средства вычислительной техники;

ОТСС - основные технические средства и системы;

ВТСС - вспомогательные технические средства и системы;

ПЭМИН - побочные электромагнитные излучения и наводки;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю России;

ФСБ России - Федеральная служба безопасности России.

**3. Общие требования:**

3.1. В соответствии с настоящим техническим заданием должна быть осуществлена поставка, установка и настройка средств защиты информации для создания защищённых объектов информатизации, а также оказаны услуги по аттестации двух объектов информатизации.

3.2. Основными целями оказания услуг являются разработка и реализация организационных и технических мер для создания условий обеспечения защиты информации при обработке в автоматизированных рабочих местах в соответствии с требованиями действующих руководящих документов ФСБ России и ФСТЭК России, а также проведение специальных проверок и специальных исследований с последующей аттестацией в соответствии с требованиями действующих руководящих документов ФСТЭК России.

 Обеспечение безопасности информации должно достигаться за счёт комплексного использования организационных и технических мер защиты информации.

3.3. Этапность реализации:

- Поставка средств защиты информации;

- Установка и настройка средств защиты информации;

- Аттестация объектов информатизации.

3.4. Место оказания услуг: г. Югорск, Ханты-Мансийский автономный округ-Югра, Тюменская область, ул.40 лет Победы, д.11.

**4. Поставка средств защиты информации:**

4.1. Исполнитель должен передать Заказчику средства защиты информации (далее товар), соответствующие количеству и характеристикам, указанным в Таблице 1.

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п/п | Наименование | Характеристики | Ед. изм. | Кол-во |
| 1 | Право на использование программного обеспечения, реализующего функции криптографического шлюза | Передача неисключительных прав на воспроизведение программного обеспечения, реализующего функции криптографического шлюза, отвечающего следующим требованиям:* совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью, представленным в настоящем техническом задании: обновление программного обеспечения, обновление справочно-ключевой информацией, управлением политиками безопасности;
* совместимо (полностью) с программным комплексом, реализующим функции криптографического клиента, представленным в настоящем техническом задании: шифрование/дешифрование направляемого/принимаемого IP-трафика;
* поддержка операционных систем:
* Microsoft Windows 2000 Professional;
* Microsoft Windows XP Home/Professional;
* Microsoft Windows Vista (вся линейка);
* Microsoft Windows 7 (вся линейка).
* наличие в составе программного обеспечения, соответствующего требованиям ФСТЭК России к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно;
* наличие сертификата ФСБ России к шифровальным (криптографическим) средствам класса КС1 (для варианта исполнения 1) и класса КС2 (для варианта исполнения 2) и возможностью использования для криптографической защиты (шифрование файлов, данных, содержащихся в областях оперативной памяти, и IP-трафика, вычисление лимитов вставки для файлов, данных, содержащихся в областях оперативной памяти, и IP трафика) информации, не содержащей сведений, составляющих государственную тайну;
* осуществление функции прокси-сервера защищённых соединений;
* встроенный межсетевой экран, соответствующий 3-ому классу по требованиям ФСТЭК России;
* предоставление функции туннелирующего сервера;
* предоставление функции сервера IP-адресов;
* криптошлюз должен использовать IP-адресацию для организации защищённых каналов связи с другими криптошлюзами и криптографическими клиентами, основанную на шестнадцатеричных идентификаторах;

программное обеспечение, реализующее функции криптографического шлюза, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью, указанном в настоящем ТЗ. | шт. | 1 |
| 2 | Право на использование программного обеспечения, реализующего функции управления защищённой сетью  | Программное обеспечение, реализующее функции управления защищённой сетью должно отвечать следующим требованиям:* состоять из центра управления сетью и ключевого удостоверяющего центра;
* совместимо (полностью) с ПО, реализующим функции криптографического шлюза и программным обеспечением, реализующим функции криптографического клиента для защиты каналов связи по классу защиты КС2, указанных в настоящем ТЗ;
* выработка ключей, соответствующих ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р34.10-2001;
* создание узлов защищенной сети (криптографические шлюзы и клиенты), удаление узлов защищенной сети, определение политик связей защищённых узлов между собой, определение политики безопасности и формирование списков прикладных задач для узлов защищенной сети;
* автоматическая рассылка справочной и ключевой информации;
* проведение автоматического обновления программного обеспечения криптошлюзов и защищённых терминальных клиентов;
* формирование симметричных ключей связи узлов (криптошлюзы и защищённые терминальные клиенты) между собой;
* формирование сертификатов электронно-цифровой подписи формата X.509 v.3;
* ведение списков отозванных сертификатов электронно-цифровой подписи;
* наличие модуля гарантированной доставки обновления справочной-ключевой информации на криптошлюзы и защищённые терминальные клиенты;
* Наличие действующего сертификата ФСБ России на соответствие требованиям к шифровальным (криптографическим средствам) класса КС2;
* поддержка операционных систем (имеющихся у Заказчика):
* Windows XP x86 (32-bit) Service Pack 3;
* Windows 2003 Server.
 | шт. | 1 |
| 3 | Право на использование программное обеспечение, реализующее функции криптографического клиента для защиты каналов связи по классу защиты КС2 | Передача неисключительных прав на воспроизведение программного обеспечения, реализующего функции криптографического клиента, отвечающего следующим требованиям:* совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью, представленным в настоящем ТЗ: обновление программного обеспечения, обновление справочно-ключевой информации, управлением политиками безопасности;
* совместимо (полностью) с программно обеспечением, реализующим целевые функции криптографического шлюза, представленным в настоящем ТЗ;
* поддержка операционных систем, использующихся у Заказчика:
* Microsoft Windows 2000 Professional;
* Microsoft Windows XP Home/Professional;
* Microsoft Windows Vista (вся линейка);
* Microsoft Windows 7 (вся линейка).
* предоставлять функции клиента службы обмена файлами и сообщениями, защищенной электронной почты с функциями шифрования писем и вложений для обмена с другими криптографическими клиентами;
* предоставлять функции контроля запускаемых в операционной системе приложений;
* предоставлять функции контентной фильтрации прикладных протоколов http, ftp;
* программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью;
* взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»);
* наличие сертификата ФСБ России на соответствие требованиям к СКЗИ по классу КС2 и на соответствие требованиям к МЭ по 4-ому классу защищенности.
 | шт | 5 |
| 4 | Комплект дистрибутивов программного обеспечения для защиты каналов связи | Исполнителем должны быть предоставлены:* Установочный комплект – от 3 до 5 шт.;
* Паспорт-формуляр;
* Специальный защитный знак (голографическая наклейка, подтверждающая принадлежность ПО к средству защиты информации).
 | шт | 1 |
| 5 | Право на использование СЗИ от НСД | Средство защиты информации должно осуществлять:- защиту серверов и рабочих станций от НСД;- контроль входа пользователей в систему, в том числе и с использованием аппаратных средств защиты;- разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;- разграничение доступа пользователей к информации;- контроль утечек информации;- регистрацию событий безопасности и аудит.Требования к совместимости с операционной и аппаратной платформами:- 32-битные операционные системы: MS Windows Server 2003 SP2, MS Windows Server 2003 R2 SP2, MS Windows Server 2008 SP2, MS Windows XP Professional SP3, MS Windows Vista SP2, MS Windows 7 SP1;- 64-битные операционные системы: MS Windows Server 2003 x64 Edition SP2, MS Windows Server 2003 R2 x64 Edition SP2, MS Windows Server 2008 x64 Edition SP2, MS Windows Server 2008 R2 x64 Edition SP1, MS Windows XP Professional x64 Edition SP2, MS Windows Vista x64 Edition SP2, MS Windows 7 x64 Edition SP1;- Active Directory/ADAM/LDS (для применения СЗИ с централизованным управлением);- наличие привода CD-ROM;- в случае совместного применения средств доверенной загрузки - наличие свободного разъёма системной шины стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В, или свободный разъем PCI-Express.Требования к функциональности: - может функционировать совместно с аппаратными и программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей;- может функционировать совместно с персональными идентификаторами (для обеспечения усиленной аутентификации пользователей);- поддерживать персональные идентификаторы iButton (при совместном использовании со средствами доверенной загрузки), eToken PRO, eToken PRO Java (в форм-факторах USB и смарт карт), Rutoken;- должно обеспечивать автоматическую блокировку автоматизированной системы при изъятии персонального идентификатора пользователя;- поддержка терминального режима работы пользователей для платформ Microsoft и Citrix, а также при использовании бездисковых рабочих станций (“тонких клиентов”);- контроль устройств:* последовательные и параллельные порты;
* локальные устройства
* сменные, логические и оптические диски;
* USB – устройства,
* устройства PCMCI,
* устройства IEEE1394,
* устройства Secure Digital;

- контроль устройств, подключаемых/отключаемых в процессе работы автоматизированной системы;- контроль неизменности аппаратной конфигурации компьютера;- управление подключениями (IrDA, WiFi, FireWire, Ethernet, Bluetooth);- контроль вывода информации на отчуждаемые носители;- теневое копирование отчуждаемой информации;- разграничение доступа к принтерам;- контроль буфера обмена Windows;- создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера;- должно обеспечивать автоматическую настройку механизмов защиты при добавлении в систему приложения, обрабатывающего конфиденциальную информацию;- возможность выбора уровня конфиденциальности сессии для пользователя; - разграничение доступа пользователей к конфиденциальным данным и приложениям;- мандатное управление доступом, включая – к устройствам;- контроль вывода конфиденциальных данных на печать, управление грифами конфиденциальности при печати конфиденциальных и секретных документов;- контроль целостности файлов, каталогов, элементов системного реестра; - возможность контроля целостности до загрузки операционной системы (при совместном применении со средствами доверенной загрузки);- функциональный контроль ключевых компонентов системы;- автоматическое затирание данных на диске при удалении конфиденциальных файлов пользователем;- регистрация событий безопасности в журнале безопасности;- возможность автоматического оповещения по электронной почте о событиях несанкционированного доступа;- возможность формирования отчетов по результатам аудита;- реакции СЗИ при нарушении целостности: * регистрацию события в журнале;
* блокировку компьютера;
* восстановление повреждённой/модифицированной информации;
* отклонение или принятие изменений;

- функциональный самоконтроль подсистем защиты.Требования к централизованному управлению в доменной сети: - централизованный мониторинг и оперативное управление рабочими станциями;- централизованный сбор и хранение журналов безопасности, регистрация событий безопасности;- аудит безопасности, формирования отчётов по результатам аудита;- возможность создания централизованной политики безопасности по использованию отчуждаемых USB носителей информации;- возможность создания централизованной политики замкнутой программной среды;- возможность интеграции с политиками безопасности Active Directory;- централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу;- должно обеспечивать создание доменов безопасности в территориально-распределённой сети, при этом предоставляется возможность делегирования административных полномочий по информационной безопасности;- возможность создания отчётов по перечню установленного ПО, сведениям о ресурсах, объектах и параметрах защищаемого компьютера.Требования по сертификации:- показатель защищенности от НСД (Гостехкомиссия России, 1999) не ниже 3-го класса защищенности. Классификация по уровню отсутствия НДВ (Гостехкомиссия России, 1999) – не ниже 2-го уровня контроля | шт | 5 |
| 6 | \*Программа для ЭВМ Kaspersky Certifiedmedia Pack Customized Russian Edition. Media Pack  | Комплектность:- CD в конверте с записанными сертифицированными приложениями;- формуляр;- заверенная копия сертификата ФСТЭК России, удостоверяющий, что антивирус соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля.- заверенная копия сертификата ФСБ России, удостоверяющая, что программное изделие соответствует требованиям ФСБ России к антивирусным средствам классов А2, Б2, В2, Г2. | шт | 1 |
| 7 | \* Дополнительный модуль для UserGate Proxy & Firewall 6.X Entensys URL Filtering (до 200 сессий на 1 год) | Способ передачи прав: электронный ключ.Программный продукт должен представлять собой возможность активировать дополнительный встроенный модуль фильтрации интернет-трафика по категориям Entensys URL-filtering в эксплуатируемом Заказчиком прокси-сервере UserGate Proxy&Firewall 6.0 до 200 сессийФункциональные характеристики:- Дополнительный модуль для UserGate Proxy & Firewall 6.X Entensys URL Filtering (до 200 сессий на 1 год) - должен позволять блокировать доступ к нежелательным ресурсам, как в отдельности, так и по категориям сайтов. Работа модуля фильтрации по категориям сайтов должна быть основана на технологии Entensys URL Filtering, в которой используется база данных, содержащая 500 млн. сайтов, разделённых на 73 категории. Администратор должен иметь возможность запрещать доступ к отдельным сайтам, к категориям сайтов, либо к тем сайтам, адреса которых содержат заданные фрагменты слов. База должна быть специально адаптирована для использования русскоязычными пользователями и содержать до 10 миллионов русскоязычных сайтов. Программный продукт должен быть совместим с операционной системой Windows Windows 7/8/2008/2012.Поставляемый программный продукт должен включать в себя Лицензию на использование лицензионной версии (неисключительные имущественные права) сроком работы 1 год с момента активации электронного ключа. | шт | 1 |

\* поставка эквивалента невозможна по причине эксплуатации Заказчиком средств антивирусной защиты и прокси-сервера UserGate Proxy & Firewall 6.X, совместимых с товарами, указанными в п.6,7 соответственно, таблицы №1 настоящего технического задания.

4.2. Исполнитель самостоятельно или через перевозчика осуществляет поставку товара по адресу Заказчика. О готовности к отгрузке товара Исполнитель сообщает не позднее, чем за 2 (два) календарных дня до дня отгрузки.

4.3. В случае использования услуг перевозчика для доставки товара Заказчику Исполнитель обязан известить Заказчика о факте передачи товара перевозчику, а также о наименовании перевозчика и реквизитах отгрузочных документов.

Заказчик в течение трёх рабочих дней с момента поставки товара обязан осуществить приёмку указанного товара по количеству и комплектности в соответствии с техническим заданием, с подписанием товарной накладной (ТОРГ-12).

В указанный период, в целях подтверждения работоспособности товара и его соответствия заявленным требованиям Заказчик вправе выполнить тестирование (пробный запуск) поставленного товара собственными силами. Товар должен иметь формуляры, комплектность товара должна соответствовать формуляру.

4.4. Программное обеспечение в составе товара должно быть передано Заказчику в соответствии с действующим законодательством с предоставлением сублицензионных договоров и актов приёма-передачи неисключительных прав. Права на использование ПО, за исключением п.7, таблицы №1, настоящего технического задания, должны быть бессрочным.

**5. Установка и настройка средств защиты информации:**

5.1. Исполнитель должен выполнить установку и настройку поставляемых в рамках настоящего ТЗ средств защиты информации (таблица №1). Средства защиты информации должны быть установлены и настроены в соответствии с требованиями следующих документов:

а) Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

б) Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

в) Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждённые 8 Центром ФСБ России от 21 февраля 2008 года №149/54-144;

г) Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённые руководством 8 Центра ФСБ России 21 февраля 2008 года №149/6/6-622;

д) Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации»;

е) Технический проект на систему защиты информации органов муниципальной власти города Югорска.

Исполнитель, по требованию Заказчика, обеспечивает настройку межсетевого взаимодействия с ЗИС (защищённая сеть управления образования администрации города Югорска сеть № 4298, защищённая сеть органов местного самоуправления г. Югорска сеть № 3901), согласно проектных решений на систему защиты информации органов муниципальной власти города Югорска. При этом взаимодействие с эксплуатирующими организациями, осуществляющими техническое сопровождение обозначенных защищённых сетей, Исполнитель осуществляет самостоятельно.

5.2. Для установки и настройки товара Заказчик:

а) Предоставляет аппаратную платформу для создания программно-аппаратного комплекса, выполняющего функции криптографического шлюза, удовлетворяющую следующим требованиям:

Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более;

Объём ОЗУ не менее 1 Гбайт;

Свободное место на жёстком диске — не менее 1 Гбайт;

Сетевой интерфейс или модем. Количество сетевых интерфейсов зависит от требований к функциональности координатора;

Операционная система — Microsoft Windows XP (32-разрядная), Server 2003 (32-разрядная), Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Server 2008 R2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Server 2012 (64-разрядная); Для операционной системы должен быть установлен самый последний пакет обновлений, накопительный пакет обновления часовых поясов KB2570791;

При использовании Internet Explorer — версия 6.0 или выше.

б) Обеспечивает свободное место для размещения предоставленной аппаратной платформы в серверном помещении.

в) Предоставляет таблицы маршрутизации для настройки сети.

г) Для настройки внешних соединений с программно-аппаратным комплексом, настраивает NAT либо предоставляет внешний IP-адрес.

д) Для монтажа сформированного программно-аппаратного комплекса, реализующего целевые функции оборудования по защите каналов связи, в СКС проводит работы по трассировке Ethernet кабелей категории 5E до места установки программно-аппаратного комплекса в серверной стойке с обеспечением доступности гарантированного источника питания переменного тока не менее 220V.

е) Для установки и настройки программного обеспечения, реализующего функции управления защищённой сетью, предоставляет автоматизированное рабочее место с установленной операционной системой Windows XP x86 (32-bit) Service Pack 3 или Windows 2003 Server, Windows 7 Pro x86 (32-bit).

ж) Для установки и настройки, поставляемых Исполнителем товаров, на автоматизированных рабочих местах, обеспечивает предустановленную лицензионную операционную систему, а также набор необходимых офисных приложений и средства антивирусной защиты.

5.3. В рамках оказания услуг по установке, настройке оборудования и программного обеспечения Заказчик обеспечивает доступ специалистов Исполнителя к объектам информатизации и инженерным коммуникациям подразделений администрации. Доступ к ОИ и все работы осуществляются под контролем администратора информационной безопасности администрации города Югорска, который при необходимости предоставляет необходимую техническую документацию и информацию об объектах информатизации (средствах вычислительной техники, активное сетевое оборудование) и инженерных коммуникациях (СКС, слаботочные линии связи и т.п.).

**6. Аттестация объектов информатизации (ОИ) на соответствие требованиям по безопасности информации.**

6.1. Перечень подлежащих аттестации ОИ:

а) автоматизированное рабочее место на базе ПЭВМ, 3 категории, с установленными и настроенными средствами защиты информации (далее – АРМ 1);

б) автоматизированное рабочее место на базе ПЭВМ, 3 категории (далее – АРМ 2).

6.2. Основания для оказания услуг и требования по их исполнению представлены в следующей нормативной документации:

а) «Модель иностранных технических разведок на период до 2020 года (Модель ИТР-2020)» - введена в действие с 01.09.2010 приказом Федеральной службы по техническому и экспортному контролю России от 25.12.2009 № 38;

б) Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам, утверждённые решением Гостехкомиссии при Президенте Российской Федерации от 23.05.1997 № 55;

в) «Инструкция по обеспечению режима секретности в Российской Федерации» от 05.01.2004 № 3-1.

6.3. Объем и содержание оказываемых услуг по аттестации объекта информатизации АРМ 1:

6.3.1. Обследование объекта информатизации, анализ и оценка на соответствие требованиям нормативных правовых документов по защите информации, обрабатываемой на объекте информатизации. Исполнитель осуществляет:

а) анализ исходных данных;

б) проведение предварительного обследования по выявлению возможных каналов утечки информации;

в) анализ состава основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС) объекта СВТ, расположения ОТСС относительно границ контролируемой зоны и относительно ВТСС, имеющих линии связи, выходящие за границы контролируемой зоны. Выявление параллельных пробегов линий связи ОТСС с иными линиями и коммуникациями;

г) разработку программы и методики аттестационных испытаний объекта вычислительной техники;

д) корректировка организационно-распорядительной документации;

е) корректировку и согласование с Заказчиком технической и эксплуатационной документации;

ж) корректировку внутренних организационно-распорядительных и нормативных документов по безопасности информации, необходимых для реализации требований в области технической защиты информации и достаточных для аттестации объекта информатизации.

6.3.2. Подготовка и проведение аттестационных испытаний объекта информатизации на соответствие требованиям безопасности информации. Исполнитель осуществляет:

а) проверку объекта информатизации Заказчика на соответствие организационным требованиям к обеспечению безопасности информации;

б) проверку объекта информатизации Заказчика на соответствие техническим требованиям к обеспечению безопасности информации;

в) проверка объекта информатизации Заказчика на наличие технических каналов утечек информации;

г) разработка протоколов по результатам аттестационных испытаний объектов информатизации Заказчика на соответствие требованиям к обеспечению безопасности информации.

6.3.3. Требования к отчётным документам по итогам оказания услуг:

а) разработка и согласование отчётных материалов по итогам оказания услуг производится в строгом соответствии с действующими руководящими и нормативно-методическими документами ФСБ России и ФСТЭК России.

б) отчётные материалы должны быть представлены в описательной, графической (при необходимости) и табличной форме, в одном экземпляре на бумажных носителях, имеющих установленный руководящими документами гриф секретности.

в) отчётные документы должны быть исполнены без грамматических и орфографических ошибок, опечаток и описок. Официальным языком системы аттестации является русский язык, на котором оформляются все документы, используемые и выдаваемые в рамках системы аттестации.

6.3.4. Перечень отчётных документов и материалов по результатам оказанных услуг по защите информации и аттестации:

- программа-методика проведения аттестационных испытаний объекта информатизации;

- заключение о проведении специальной проверки технических средств и систем;

- акты установки сертифицированных средств защиты информации;

- предписания на эксплуатацию основных технических средств и систем;

- протоколы контроля состояния и эффективности защиты информации на соответствие требованиям по защите информации от несанкционированного доступа;

- протоколы контроля защищённости информации от утечки за счёт побочных электромагнитных излучений и наводки;

- оформление, регистрация и выдача аттестата соответствия объекта информатизации требованиям по безопасности информации.

6.4. Объем и содержание оказываемых услуг по аттестации объекта информатизации АРМ 2.

6.4.1. Обследование объекта информатизации, анализ и оценка на соответствие требованиям нормативных правовых документов по защите информации, обрабатываемой на объекте информатизации. Исполнитель осуществляет:

а) анализ исходных данных;

б) проведение предварительного обследования по выявлению возможных каналов утечки информации;

в) анализ состава основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС) объекта СВТ, расположения ОТСС относительно границ контролируемой зоны и относительно ВТСС, имеющих линии связи, выходящие за границы контролируемой зоны. Выявление параллельных пробегов линий связи ОТСС с иными линиями и коммуникациями;

г) разработку программы и методики аттестационных испытаний объекта вычислительной техники;

д) корректировка организационно-распорядительной документации;

е) корректировку и согласование с Заказчиком технической и эксплуатационной документации;

ж) корректировку внутренних организационно-распорядительных и нормативных документов по безопасности информации, необходимых для реализации требований в области технической защиты информации и достаточных для аттестации объекта информатизации.

6.4.2. Проведение специальной проверки и специальных лабораторных исследований ОТСС, следующих ОТСС:

- системный блок;

- монитор;

- клавиатура;

- манипулятор «мышь».

6.4.3. Требования к порядку оказания услуг по специальной проверки и специальных лабораторных исследованиях:

а) исполнитель должен использовать исправные и поверенные приборы, инструменты и средства измерений. Исполнитель обязан оказывать услуги с соблюдением норм и правил техники безопасности;

б) услуги должны оказываться собственными средствами Исполнителя в специально оборудованных помещениях.

в) исполнитель обязан самостоятельно провести погрузочно-разгрузочные работы и транспортировку оборудования, до технических помещений, в которых будет проводиться специальная проверка.

6.4.4. Поставка средств защиты информации.

Исполнитель должен передать Заказчику сопутствующие услугам средства защиты информации, соответствующие количеству и характеристикам, указанным в Таблице 2 настоящего технического задания.

Таблица 2

| № | Наименование СЗИ | Характеристики СЗИ | Кол-во, шт |
| --- | --- | --- | --- |
| 1 | Право на использование СЗИ от НСД | СЗИ от НСД должно быть предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (далее - АС). СЗИ от НСД должно функционировать в среде 32-разрядных операционных систем MS Windows 2000 (Server и Professional), MS Windows XP (Professional и Home Edition), MS Windows Server 2003, MS Windows Vista, MS Windows Server 2008, MS Windows 7 и устанавливаться как на автономных рабочих местах, так и на рабочих станциях и серверах локальной вычислительной сети.Количество пользователей системы должно быть не менее 6 (с учётом администратора);Дополнительные функциональные требованияВ системе защиты информации от несанкционированного доступа должны быть реализованы следующие возможности:• установка и функционирование системы защиты на компьютерах с разными файловыми системами (NTFS, FAT32);• вход в систему пользователей должен осуществляться до загрузки операционной системы только при предъявлении ими специального идентификатора (USB-ключа типа GuardantID, ruToken и пр.) и ввода пароля;• переидентификация пользователей без перезагрузки ОС при использовании однотипных идентификаторов;• одновременная работа одного пользователя с документами разных мандатных меток;• управление запуском и поддержка мандатного принципа контроля доступа для DOS-приложений и консольных приложений Win32;• создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешённых приложений;• запуск хранителя экрана и блокировка рабочей станции при удалении USB-ключа;• использование только зарегистрированных отчуждаемых носителей информации;• маркировка документов, выдаваемых на печать, независимо от печатающего их приложения;• возможность создания дополнительного идентификатора;• сокрытие логической структуры жёсткого диска при загрузке компьютера с внешнего носителя.СЗИ от НСД должно включать и обеспечивать:Поддержку современных операционных систем компании Microsoft СЗИ от НСД должна устанавливаться на автономных рабочих станциях, рабочих станциях в составе рабочей группы или домена, серверах, в том числе в составе кластера. СЗИ от НСД должна функционировать на одно- и многопроцессорных компьютерных системах на базе архитектуры x86 под управлением 32-хразрядных операционных систем Windows Vista, Windows Server 2008, Windows 7.Подсистему контроля устройствДолжна быть обеспечена возможность контроля устройств, подключённых к компьютеру путём задания дескрипторов безопасности для групп однотипных устройств.Подсистему преобразования информации на отчуждаемых носителяхДополнительный механизм защиты съёмных носителей (дискет и флэш-накопителей) путём прозрачного преобразования всей информации, записываемой на носитель. Преобразование информации должна осуществляться с применением функции гаммирования с обратной связью алгоритма криптографического преобразования по ГОСТ 28147-89.Подсистему создания и применения шаблонов настроекДанный механизм должен позволять создавать списки настроек и свободно тиражировать их на другие компьютеры.Поддержку в качестве персональных идентификаторов USB-ключей или флэш-накопителейПодсистему учёта носителей информацииДолжна существовать возможность регистрировать как отчуждаемые носители, так и отдельные тома жёстких дисков.Подсистему регистрацииВсе события СЗИ должны быть доступны для просмотра из одной программы, в т.ч. обеспечиваться функция сортировки и поиска отдельных событий СЗИ.Подсистему маркировки и учёта документов, выдаваемых на печатьПрограмма настройки маркировки документов должна позволять более гибко задавать состав и порядок информации, выводимой на печать.Подсистему управления пользователямиДолжна обеспечиваться функция работы с идентификаторами и возможность редактировать пользователей на удалённых рабочих станциях.Подсистему настройки системы защитыНастройка системы защиты должна быть реализована в виде единого центра настройки. Данное средство защиты информации должно быть сертифицирована ФСТЭК России в системе сертификации средств защиты информации по требованиям безопасности информации №РОСС RU.0001.01БИ00 и иметь действующий сертфикат соотвествия. СЗИ от НСД должно иметь сертификат ФСТЭК России, который удостоверяет, что система защиты информации является программным средством защиты от несанкционированного доступа к информации и соответствует требованиям руководящих документов Гостехкомиссии России "Средства вычислительной техники. Защита информации от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации" по 3 классу защищённости, "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств информации. Классификация по уровню контроля отсутствия недекларированных возможностей" по 2 уровню контроля. Имеющийся сертификат должен позволять использовать СЗИ от НСД при создании АС класса защищённости до 1Б включительно. | 1 |
| 2 | Устройство защиты информации по каналам побочных электромагнитных излучений и наводок на линии ВТСС, электропитания, заземления и др. токоведущие инженерные коммуникации | Спектральная плотность напряжённости электрической**.** составляющей ЭМПШ, не менее

|  |  |  |
| --- | --- | --- |
| Диапазон частот, ГГц | Вертикальная поляризация, дБ | Горизонтальная поляризация, дБ |
| Без дополнительной антенны | С дополнительной антенной | Без дополнительной антенны | С дополнительной антенной |
| От 0,01 до 0,15 | 50 | 80 | 50 | 80 |
| от 0,15 д до 1 | 45 | 70 | 40 | 70 |
| от 1 до 5 | 45 | 60 | 40 | 55 |
| от 5 до 30 | 45 | 60 | 40 | 50 |
| от 30 до 100 | 40 | 50 | 40 | 50 |
| от 100 до 1000 | 30 | 30 | 30 | 30 |
| от 1000 до 2000 | 30 | 30 | 30 | 30 |

 Спектральная плотность напряжённости магнитной составляющей ЭМПШ, не менее

|  |  |  |
| --- | --- | --- |
| Диапазон частот, МГц | Без дополнительной антенны, дБ | С дополнительной антенной, дБ |
| от 0,01 до 0,15 | 30 | 30 |
| от 0,15 до 4 | 35 | 35 |
| от 4 до 10 | 40 | 40 |
| от 10 до 30 | 30 | 35 |

 Спектральная плотность напряжения помех в линиях электропитания и заземления, не менее

|  |  |  |
| --- | --- | --- |
| Диапазон частот, мГц | Без дополнительной антенны, дБ | С дополнительной антенной, дБ |
| от 0,01 до 0,04 | 25 | 25 |
| от 0,04 до 10 | 35 | 35 |
| от 10 до 100 | 35 | 45 |
| от 100 до 600 | 25 | 25 |
| от 600 до 1000 | 15 | 15 |

 | 1 |

 6.4.5. Разработка проекта организационно-распорядительной документации. Исполнитель осуществляет:

* разработку и согласование с Заказчиком технической и эксплуатационной документации;
* разработку проектов внутренних организационно-распорядительных и нормативных документов по безопасности информации, необходимых для реализации требований в области технической защиты информации и достаточных для аттестации объекта информатизации.

6.4.6. Подготовка и проведение аттестационных испытаний объекта информатизации на соответствие требованиям безопасности информации. Исполнитель осуществляет:

* проверку объекта информатизации Заказчика на соответствие организационным требованиям к обеспечению безопасности информации;
* проверку объекта информатизации Заказчика на соответствие техническим требованиям к обеспечению безопасности информации;
* проверку объекта информатизации Заказчика на наличие технических каналов утечек информации;
* разработку протоколов по результатам аттестационных испытаний объектов информатизации Заказчика на соответствие требованиям к обеспечению безопасности информации.

6.4.7. Требования к отчётным документам по итогам оказания услуг:

* разработка и согласование отчётных материалов по итогам оказания услуг производится в строгом соответствии с действующими руководящими и нормативно-методическими документами ФСБ России и ФСТЭК России;
* отчётные материалы должны быть представлены в описательной, графической (при необходимости) и табличной форме, в одном экземпляре на бумажных носителях, имеющих установленный руководящими документами гриф секретности;
* отчётные документы должны быть исполнены без грамматических и орфографических ошибок, опечаток и описок. Официальным языком системы аттестации является русский язык, на котором оформляются все документы, используемые и выдаваемые в рамках системы аттестации.

6.4.8. Перечень отчётных документов и материалов по результатам оказанных услуг по защите информации и аттестации:

* программа-методика проведения аттестационных испытаний объекта информатизации;
* заключение о проведении специальной проверки технических средств и систем;
* акты установки сертифицированных средств защиты информации;
* предписания на эксплуатацию основных технических средств и систем;
* протоколы контроля состояния и эффективности защиты информации на соответствие требованиям по защите информации от несанкционированного доступа;
* протоколы контроля защищённости информации от утечки за счёт побочных электромагнитных излучений и наводки;

- оформление, регистрация и выдача аттестата соответствия объекта информатизации требованиям по безопасности информации.

6.5. Общие условия и требования

6.5.1. Обязательным условием подписания акта сдачи-приемки оказанных услуг является выдача аттестатов соответствия требованиям по безопасности информации на ОИ сроком на 3 (три) года.

6.5.2. Требования к качеству оказываемых услуг:

Требования к качеству оказания комплекса специальных научно-технических услуг в области защиты информации содержатся в руководящих документах ФСБ России, ФСТЭК России в области защиты информации.

Организация, содержание и полнота оказываемых услуг по защите объектов информатизации от технических средств разведки должны соответствовать требованиям руководящих документов, регламентирующих данное направление защиты информации.

 6.5.3. Требования по обеспечению режима секретности и сохранения государственной тайны при оказании услуг:

* порядок сохранения государственной тайны и соблюдения режима секретности при оказании услуг на объектах должен удовлетворять требованиям «Инструкции по обеспечению режима секретности в Российской Федерации» № 3-1 от 05.01.2004, СТР и другим руководящим документам ФСТЭК России.
* стороны обязаны взять на себя обязательства строго соблюдать конфиденциальность сведений, полученных при оказании услуг, о результатах исследований, степени защищённости объектов информатизации и мероприятиях, применяемых для их защиты, а также технической, финансовой, коммерческой и другой информации и принимать все необходимые меры к предотвращению разглашения имеющихся сведений.
* передача указанной информации другим лицам может осуществляться только с согласия Заказчика, выраженного в письменной форме.
* гриф секретности отчётных документов должен соответствовать степени секретности сведений, содержащихся в документах.

 6.6. Требования по допуску аттестационной комиссии и специалистов Исполнителя на объекты информатизации:

Исполнитель обязан заблаговременно представить в режимно-секретное подразделение Заказчика утверждённый список своих специалистов для оказания услуг по защите информации и членов аттестационной комиссии для проведения аттестационных испытаний, а также список (перечень) оборудования и контрольно-измерительной аппаратуры, необходимых для оказания заявленных услуг (для заказа пропусков на внос и вынос в здание).

Каждый член аттестационной комиссии и специалист Исполнителя для получения доступа к объектам аттестации обязан постоянно иметь на руках документы, удостоверяющие личность, справку о допуске (не ниже второй формы) и предписание на выполнение задания.

6.7. Требования к контрольно-измерительной аппаратуре, инструменту и технике безопасности при оказании услуг:

Все услуги по защите информации и аттестации объектов информатизации проводятся с применением только поверенной и технически исправной контрольно-измерительной аппаратуры и инструментов (Исполнитель обязан предоставить Заказчику свидетельства о поверке аппаратуры).

Услуги по установке и настройке средств защиты информации и аттестации объектов информатизации должны быть оказаны в соответствии с требованиями в Российской Федерации норм и правил охраны труда, техники безопасности, электро-, пожаро- и взрывобезопасности, и не создавать угрозы безопасности для жизни и здоровья людей в процессе эксплуатации объектов.

6.8. Специальные требования и условия:

Заказчик в процессе оказания услуг обязан обеспечить в согласованное время доступ аттестационной комиссии исполнителя на объекты Заказчика для оказания услуг, предусмотренных техническим заданием.

Члены аттестационной комиссии в процессе оказания услуг обязаны:

* осуществлять оказание услуг с учётом действующих у Заказчика правил электробезопасности, охраны труда и техники безопасности;
* выполнять установленные требования пропускного и внутриобъектового режима.

**7. Гарантии, обеспечиваемые Исполнителем.**

 7.1. Передаваемые средства защиты информации должны отвечать санитарным и экологическим требованиям, быть неповреждёнными. В отношении средств защиты информации, для которых законодательством Российской Федерации предусмотрена обязательная сертификация, должны быть представлены соответствующие сертификаты.

Качество средств защиты информации должно соответствовать установленным в Российской Федерации государственным стандартам. Замена некачественных средств защиты информации осуществляется за счёт Исполнителя.

Исполнитель предоставляет гарантию на оборудование системы защиты информации (средства защиты информации) не менее 1 (одного) года, при этом предоставление такой гарантии осуществляется вместе с данными средствами защиты информации и срок действия гарантии устанавливается в соответствии со сроком действия гарантии производителя данных средств защиты информации, указанного в гарантийном талоне.

Исполнитель гарантирует, что все средства защиты информации, передаваемые в соответствии с условиями контракта, являются новыми, неиспользованными, при доставке и далее не будут иметь дефектов, связанных с конструкцией, материалами, либо проявляющихся в результате действий или упущения Исполнителя, при нормальном соблюдении Заказчиком правил хранения и использования средств защиты информации, установленных производителем.

Если в течение гарантийного срока будет выявлено, что средства защиты информации не соответствуют требованиям контракта, Исполнитель обязан предпринять меры по устранению нарушений указанных требований. Устранение нарушений должно быть завершено не позднее 30 (тридцати) рабочих дней с даты поступления официального уведомления от уполномоченного представителя Заказчика.

7.2. Гарантийное техническое сопровождение.

По завершению создания системы защиты информации на ОИ, Исполнителем должно быть обеспечено гарантийное техническое сопровождение в течение 1 (одного) календарного года, с даты выдачи аттестата соответствия объектов информатизации требованиям по безопасности информации.

Гарантийное техническое сопровождение включает в себя:

* консультации по эксплуатации СЗИ;
* консультации Администратора информационной безопасности Заказчика по правилам эксплуатации СЗИ.
* уточнение функций и характеристик устанавливаемых СЗИ;
* разъяснение положений технической документации по установке СЗИ;
* анализ и коррекция допущенных ошибок при эксплуатации СЗИ по телефону, e-mail и на месте расположения объекта информатизации.

**8. Требования к исполнителю.**

Исполнитель должен предоставить следующие разрешительные документы:

1) Лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации по видам деятельности:

- контроль защищённости конфиденциальной информации от утечки по техническим каналам в: средствах и системах информатизации; технических средствах (системах), не обрабатывающих конфиденциальную информацию, но размещённых в помещениях, где она обрабатывается; помещениях со средствами (системами), подлежащими защите; помещениях, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения);

 - аттестационные испытания и аттестация на соответствие требованиям по защите информации: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;

- проектирование в защищённом исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;

 - установка, монтаж, испытания, ремонт средств защиты информации (технических средств защиты информации, защищённых технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищённых программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля защищённости информации).

Лицензирование осуществляется в соответствии с п.п. 5 п. 1 ст. 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», постановлением Правительства РФ от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» в связи с необходимостью осуществления установки и настройки поставляемого товара (средств защиты информации).

2) Лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) на следующие пункты:

- монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств (п.12 перечня);

- передачу шифровальных (криптографических) средств (п.21 перечня).

Лицензирование осуществляется в соответствии с Федеральным законом от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности». Порядок лицензирования определён постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 «О лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

3) Лицензию ФСБ России на осуществление работ с использованием сведений, составляющих государственную тайну;

4) Лицензию ФСТЭК России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны;

5) Лицензию ФСБ России на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны, включающей в себя:

- проведение работ по выявлению электронных устройств, предназначенных для негласного получения информации, в технических средствах.

Лицензирование осуществляется в соответствии с п.п. 3 п.1 ст. 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», постановлением Правительства РФ от 16.04.2012 № 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»;

6)Действующий аттестат аккредитации, зарегистрированный в Государственном реестре системы сертификации средств защиты информации по требованиям безопасности, выданный ФСТЭК России, в соответствии с положением о сертификации средств защиты информации по требованиям безопасности информации, утверждённым приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27 октября 1995 г. № 199.

Согласовано: Работник контрактной службы: О.В.Дергилев

* 1. **ПРОЕКТ КОНТРАКТА**

**МУНИЦИПАЛЬНый КОНТРАКТ на оказание услуг**

**по технической защите информации**

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 технической защите информации, а Заказчик обязуется принять и оплатить их.

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

1.3. Место оказания услуг: администрация города Югорска, Ханты-Мансийский автономный округ – Югра, г.Югорск, ул.40 лет Победы, д.11.

**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 \_\_\_\_\_\_\_\_).* Смета Контракта определена в Приложении 2.

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. Авансовые платежи по Контракту не предусмотрены.

2.4.4. Расчёт за оказанные услуги осуществляется в течение 10 (десяти) дней со дня подписания Заказчиком Акта об оказанных услугах и товарных накладных (форма ТОРГ12). Программное обеспечение передаётся Заказчику в соответствии с действующим законодательством с предоставлением сублицензионного договора и акта приёма-передачи неисключительных прав.

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: в течение 40 дней с момента подписания муниципального контракта.

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 следующие документы (в двух экземплярах): Акт об оказанных услугах, товарные накладные, сублицензионный договор, счёт и счёт-фактуру.

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, товарные накладные, сублицензионный договор 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 извещения является: \_\_\_\_\_\_\_\_\_. Номером факса для получения извещения является: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

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 24 671 (двадцать четыре тысячи шестьсот семьдесят один) рубль 50 копеек (5 процентов от начальной (максимальной) цены контракта).

В случае принятия антидемпинговых мер, размер обеспечения исполнения контракта составит 37 007 (тридцать семь тысяч семь) рублей 25 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 31.07.2016. 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 30.06.2016. С 01.07.2016 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 1);

- Смета Контракта (Приложение 2).

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 1

к Муниципальному контракту

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

**Техническое задание**

**1.** **Предмет муниципального контракта**: оказание услуг по технической защите информации.

**2. Используемые сокращения:**

АРМ - автоматизированное рабочее место;

ЗИС - защищенная информационная система;

НСД - несанкционированный доступ;

ПО - программное обеспечение;

ОИ - объект информатизации;

ЗОИ - защищенный объект информатизации;

СЗИ - средства защиты информации;

СКЗИ - средства криптографической защиты информации;

СВТ - средства вычислительной техники;

ОТСС - основные технические средства и системы;

ВТСС - вспомогательные технические средства и системы;

ПЭМИН - побочные электромагнитные излучения и наводки;

ФСТЭК России - Федеральная служба по техническому и экспортному контролю России;

ФСБ России - Федеральная служба безопасности России.

**3. Общие требования:**

3.1. В соответствии с настоящим техническим заданием должна быть осуществлена поставка, установка и настройка средств защиты информации для создания защищённых объектов информатизации, а также оказаны услуги по аттестации двух объектов информатизации.

3.2. Основными целями оказания услуг являются разработка и реализация организационных и технических мер для создания условий обеспечения защиты информации при обработке в автоматизированных рабочих местах в соответствии с требованиями действующих руководящих документов ФСБ России и ФСТЭК России, а также проведение специальных проверок и специальных исследований с последующей аттестацией в соответствии с требованиями действующих руководящих документов ФСТЭК России.

 Обеспечение безопасности информации должно достигаться за счёт комплексного использования организационных и технических мер защиты информации.

3.3. Этапность реализации:

- Поставка средств защиты информации;

- Установка и настройка средств защиты информации;

- Аттестация объектов информатизации.

3.4. Место оказания услуг: г. Югорск, Ханты-Мансийский автономный округ-Югра, Тюменская область, ул.40 лет Победы, д.11.

**4. Поставка средств защиты информации:**

4.1. Исполнитель должен передать Заказчику средства защиты информации (далее товар), соответствующие количеству и характеристикам, указанным в Таблице 1.

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п/п | Наименование | Характеристики | Ед. изм. | Кол-во |
| 1 | Право на использование программного обеспечения, реализующего функции криптографического шлюза | Передача неисключительных прав на воспроизведение программного обеспечения, реализующего функции криптографического шлюза, отвечающего следующим требованиям:* совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью, представленным в настоящем техническом задании: обновление программного обеспечения, обновление справочно-ключевой информацией, управлением политиками безопасности;
* совместимо (полностью) с программным комплексом, реализующим функции криптографического клиента, представленным в настоящем техническом задании: шифрование/дешифрование направляемого/принимаемого IP-трафика;
* поддержка операционных систем:
* Microsoft Windows 2000 Professional;
* Microsoft Windows XP Home/Professional;
* Microsoft Windows Vista (вся линейка);
* Microsoft Windows 7 (вся линейка).
* наличие в составе программного обеспечения, соответствующего требованиям ФСТЭК России к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно;
* осуществление функции прокси-сервера защищённых соединений;
* встроенный межсетевой экран, соответствующий 3-ому классу по требованиям ФСТЭК России;
* предоставление функции туннелирующего сервера;
* предоставление функции сервера IP-адресов;
* криптошлюз должен использовать IP-адресацию для организации защищённых каналов связи с другими криптошлюзами и криптографическими клиентами, основанную на шестнадцатеричных идентификаторах;

программное обеспечение, реализующее функции криптографического шлюза, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью. | шт. | 1 |
| 2 | Право на использование программного обеспечения, реализующего функции управления защищённой сетью  | Программное обеспечение, реализующее функции управления защищённой сетью должно отвечать следующим требованиям:* состоять из центра управления сетью и ключевого удостоверяющего центра;
* совместимо (полностью) с ПО, реализующим функции криптографического шлюза и программным обеспечением, реализующим функции криптографического клиента для защиты каналов связи по классу защиты КС2, указанных в настоящем ТЗ;
* выработка ключей, соответствующих ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р34.10-2001;
* создание узлов защищенной сети (криптографические шлюзы и клиенты), удаление узлов защищенной сети, определение политик связей защищённых узлов между собой, определение политики безопасности и формирование списков прикладных задач для узлов защищенной сети;
* автоматическая рассылка справочной и ключевой информации;
* проведение автоматического обновления программного обеспечения криптошлюзов и защищённых терминальных клиентов;
* формирование симметричных ключей связи узлов (криптошлюзы и защищённые терминальные клиенты) между собой;
* формирование сертификатов электронно-цифровой подписи формата X.509 v.3;
* ведение списков отозванных сертификатов электронно-цифровой подписи;
* наличие модуля гарантированной доставки обновления справочной-ключевой информации на криптошлюзы и защищённые терминальные клиенты;
* Наличие действующего сертификата ФСБ России на соответствие требованиям к шифровальным (криптографическим средствам) класса КС2;
* поддержка операционных систем (имеющихся у Заказчика):
* Windows XP x86 (32-bit) Service Pack 3;
* Windows 2003 Server.
 | шт. | 1 |
| 3 | Право на использование программное обеспечение, реализующее функции криптографического клиента для защиты каналов связи по классу защиты КС2 | Передача неисключительных прав на воспроизведение программного обеспечения, реализующего функции криптографического клиента, отвечающего следующим требованиям:* совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью, представленным в настоящем ТЗ: обновление программного обеспечения, обновление справочно-ключевой информации, управлением политиками безопасности;
* совместимо (полностью) с программно обеспечением, реализующим целевые функции криптографического шлюза, представленным в настоящем ТЗ;
* поддержка операционных систем, использующихся у Заказчика:
* Microsoft Windows 2000 Professional;
* Microsoft Windows XP Home/Professional;
* Microsoft Windows Vista (вся линейка);
* Microsoft Windows 7 (вся линейка).
* предоставлять функции клиента службы обмена файлами и сообщениями, защищенной электронной почты с функциями шифрования писем и вложений для обмена с другими криптографическими клиентами;
* предоставлять функции контроля запускаемых в операционной системе приложений;
* предоставлять функции контентной фильтрации прикладных протоколов http, ftp;
* программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью;
* взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»)
* наличие сертификата ФСБ России на соответствие требованиям к СКЗИ по классу КС2 и на соответствие требованиям к МЭ по 4-ому классу защищенности.
 | шт | 5 |
| 4 | Комплект дистрибутивов программного обеспечения для защиты каналов связи | Исполнителем должны быть предоставлены:* Установочный комплект – от 3 до 5 шт.;
* Паспорт-формуляр;
* Специальный защитный знак (голографическая наклейка, подтверждающая принадлежность ПО к средству защиты информации).
 | шт | 1 |
| 5 | Право на использование СЗИ от НСД | Средство защиты информации должно осуществлять:- защиту серверов и рабочих станций от НСД;- контроль входа пользователей в систему, в том числе и с использованием аппаратных средств защиты;- разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;- разграничение доступа пользователей к информации;- контроль утечек информации;- регистрацию событий безопасности и аудит.Требования к совместимости с операционной и аппаратной платформами:- 32-битные операционные системы: MS Windows Server 2003 SP2, MS Windows Server 2003 R2 SP2, MS Windows Server 2008 SP2, MS Windows XP Professional SP3, MS Windows Vista SP2, MS Windows 7 SP1;- 64-битные операционные системы: MS Windows Server 2003 x64 Edition SP2, MS Windows Server 2003 R2 x64 Edition SP2, MS Windows Server 2008 x64 Edition SP2, MS Windows Server 2008 R2 x64 Edition SP1, MS Windows XP Professional x64 Edition SP2, MS Windows Vista x64 Edition SP2, MS Windows 7 x64 Edition SP1;- Active Directory/ADAM/LDS (для применения СЗИ с централизованным управлением);- наличие привода CD-ROM;- в случае совместного применения средств доверенной загрузки - наличие свободного разъёма системной шины стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В, или свободный разъем PCI-Express.Требования к функциональности: - может функционировать совместно с аппаратными и программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей;- может функционировать совместно с персональными идентификаторами (для обеспечения усиленной аутентификации пользователей);- поддерживать персональные идентификаторы iButton (при совместном использовании со средствами доверенной загрузки), eToken PRO, eToken PRO Java (в форм-факторах USB и смарт карт), Rutoken;- должно обеспечивать автоматическую блокировку автоматизированной системы при изъятии персонального идентификатора пользователя;- поддержка терминального режима работы пользователей для платформ Microsoft и Citrix, а также при использовании бездисковых рабочих станций (“тонких клиентов”);- контроль устройств:* последовательные и параллельные порты;
* локальные устройства
* сменные, логические и оптические диски;
* USB – устройства,
* устройства PCMCI,
* устройства IEEE1394,
* устройства Secure Digital;

- контроль устройств, подключаемых/отключаемых в процессе работы автоматизированной системы;- контроль неизменности аппаратной конфигурации компьютера;- управление подключениями (IrDA, WiFi, FireWire, Ethernet, Bluetooth);- контроль вывода информации на отчуждаемые носители;- теневое копирование отчуждаемой информации;- разграничение доступа к принтерам;- контроль буфера обмена Windows;- создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера;- должно обеспечивать автоматическую настройку механизмов защиты при добавлении в систему приложения, обрабатывающего конфиденциальную информацию;- возможность выбора уровня конфиденциальности сессии для пользователя; - разграничение доступа пользователей к конфиденциальным данным и приложениям;- мандатное управление доступом, включая – к устройствам;- контроль вывода конфиденциальных данных на печать, управление грифами конфиденциальности при печати конфиденциальных и секретных документов;- контроль целостности файлов, каталогов, элементов системного реестра; - возможность контроля целостности до загрузки операционной системы (при совместном применении со средствами доверенной загрузки);- функциональный контроль ключевых компонентов системы;- автоматическое затирание данных на диске при удалении конфиденциальных файлов пользователем;- регистрация событий безопасности в журнале безопасности;- возможность автоматического оповещения по электронной почте о событиях несанкционированного доступа;- возможность формирования отчетов по результатам аудита;- реакции СЗИ при нарушении целостности: * регистрацию события в журнале;
* блокировку компьютера;
* восстановление повреждённой/модифицированной информации;
* отклонение или принятие изменений;

- функциональный самоконтроль подсистем защиты.Требования к централизованному управлению в доменной сети: - централизованный мониторинг и оперативное управление рабочими станциями;- централизованный сбор и хранение журналов безопасности, регистрация событий безопасности;- аудит безопасности, формирования отчётов по результатам аудита;- возможность создания централизованной политики безопасности по использованию отчуждаемых USB носителей информации;- возможность создания централизованной политики замкнутой программной среды;- возможность интеграции с политиками безопасности Active Directory;- централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу;- должно обеспечивать создание доменов безопасности в территориально-распределённой сети, при этом предоставляется возможность делегирования административных полномочий по информационной безопасности;- возможность создания отчётов по перечню установленного ПО, сведениям о ресурсах, объектах и параметрах защищаемого компьютера.Требования по сертификации:- показатель защищенности от НСД (Гостехкомиссия России, 1999) не ниже 3-го класса защищенности. Классификация по уровню отсутствия НДВ (Гостехкомиссия России, 1999) – не ниже 2-го уровня контроля | шт | 5 |
| 6 | \*Программа для ЭВМ Kaspersky Certifiedmedia Pack Customized Russian Edition. Media Pack  | Комплектность:- CD в конверте с записанными сертифицированными приложениями;- формуляр;- заверенная копия сертификата ФСТЭК России, удостоверяющий, что антивирус соответствует требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) по 4 уровню контроля.- заверенная копия сертификата ФСБ России, удостоверяющая, что программное изделие соответствует требованиям ФСБ России к антивирусным средствам классов А2, Б2, В2, Г2. | шт | 1 |
| 7 | \* Дополнительный модуль для UserGate Proxy & Firewall 6.X Entensys URL Filtering (до 200 сессий на 1 год) | Способ передачи прав: электронный ключ.Программный продукт должен представлять собой возможность активировать дополнительный встроенный модуль фильтрации интернет-трафика по категориям Entensys URL-filtering в эксплуатируемом Заказчиком прокси-сервере UserGate Proxy&Firewall 6.0 до 200 сессийФункциональные характеристики:- Дополнительный модуль для UserGate Proxy & Firewall 6.X Entensys URL Filtering (до 200 сессий на 1 год) - должен позволять блокировать доступ к нежелательным ресурсам, как в отдельности, так и по категориям сайтов. Работа модуля фильтрации по категориям сайтов должна быть основана на технологии Entensys URL Filtering, в которой используется база данных, содержащая 500 млн. сайтов, разделённых на 73 категории. Администратор должен иметь возможность запрещать доступ к отдельным сайтам, к категориям сайтов, либо к тем сайтам, адреса которых содержат заданные фрагменты слов. База должна быть специально адаптирована для использования русскоязычными пользователями и содержать до 10 миллионов русскоязычных сайтов. Программный продукт должен быть совместим с операционной системой Windows Windows 7/8/2008/2012.Поставляемый программный продукт должен включать в себя Лицензию на использование лицензионной версии (неисключительные имущественные права) сроком работы 1 год с момента активации электронного ключа. | шт | 1 |

\* поставка эквивалента невозможна по причине эксплуатации Заказчиком средств антивирусной защиты и прокси-сервера UserGate Proxy & Firewall 6.X, совместимых с товарами, указанными в п.6,7 соответственно, таблицы №1 настоящего технического задания.

4.2. Исполнитель самостоятельно или через перевозчика осуществляет поставку товара по адресу Заказчика. О готовности к отгрузке товара Исполнитель сообщает не позднее, чем за 2 (два) календарных дня до дня отгрузки.

4.3. В случае использования услуг перевозчика для доставки товара Заказчику Исполнитель обязан известить Заказчика о факте передачи товара перевозчику, а также о наименовании перевозчика и реквизитах отгрузочных документов.

Заказчик в течение трёх рабочих дней с момента поставки товара обязан осуществить приёмку указанного товара по количеству и комплектности в соответствии с техническим заданием, с подписанием товарной накладной (ТОРГ-12).

В указанный период, в целях подтверждения работоспособности товара и его соответствия заявленным требованиям Заказчик вправе выполнить тестирование (пробный запуск) поставленного товара собственными силами. Товар должен иметь формуляры, комплектность товара должна соответствовать формуляру.

4.4. Программное обеспечение в составе товара должно быть передано Заказчику в соответствии с действующим законодательством с предоставлением сублицензионных договоров и актов приёма-передачи неисключительных прав. Права на использование ПО, за исключением п.7, таблицы №1, настоящего технического задания, должны быть бессрочным.

**5. Установка и настройка средств защиты информации:**

5.1. Исполнитель должен выполнить установку и настройку поставляемых в рамках настоящего ТЗ средств защиты информации (таблица №1). Средства защиты информации должны быть установлены и настроены в соответствии с требованиями следующих документов:

а) Приказ ФСТЭК от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

б) Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

в) Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утверждённые 8 Центром ФСБ России от 21 февраля 2008 года №149/54-144;

г) Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утверждённые руководством 8 Центра ФСБ России 21 февраля 2008 года №149/6/6-622;

д) Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации»;

е) Технический проект на систему защиты информации органов муниципальной власти города Югорска.

Исполнитель, по требованию Заказчика, обеспечивает настройку межсетевого взаимодействия с ЗИС (защищённая сеть управления образования администрации города Югорска сеть № 4298, защищённая сеть органов местного самоуправления г. Югорска сеть № 3901), согласно проектных решений на систему защиты информации органов муниципальной власти города Югорска. При этом взаимодействие с эксплуатирующими организациями, осуществляющими техническое сопровождение обозначенных защищённых сетей, Исполнитель осуществляет самостоятельно.

5.2. Для установки и настройки товара Заказчик:

а) Предоставляет аппаратную платформу для создания программно-аппаратного комплекса, выполняющего функции криптографического шлюза, удовлетворяющую следующим требованиям:

Процессор — Intel Core 2 Duo или другой схожий по производительности x86-совместимый процессор с количеством ядер 2 и более;

Объём ОЗУ не менее 1 Гбайт;

Свободное место на жёстком диске — не менее 1 Гбайт;

Сетевой интерфейс или модем. Количество сетевых интерфейсов зависит от требований к функциональности координатора;

Операционная система — Microsoft Windows XP (32-разрядная), Server 2003 (32-разрядная), Vista (32/64-разрядная), Server 2008 (32/64-разрядная), Server 2008 R2 (64-разрядная), Windows 7 (32/64-разрядная), Windows 8 (32/64-разрядная), Server 2012 (64-разрядная); Для операционной системы должен быть установлен самый последний пакет обновлений, накопительный пакет обновления часовых поясов KB2570791;

При использовании Internet Explorer — версия 6.0 или выше.

б) Обеспечивает свободное место для размещения предоставленной аппаратной платформы в серверном помещении.

в) Предоставляет таблицы маршрутизации для настройки сети.

г) Для настройки внешних соединений с программно-аппаратным комплексом, настраивает NAT либо предоставляет внешний IP-адрес.

д) Для монтажа сформированного программно-аппаратного комплекса, реализующего целевые функции оборудования по защите каналов связи, в СКС проводит работы по трассировке Ethernet кабелей категории 5E до места установки программно-аппаратного комплекса в серверной стойке с обеспечением доступности гарантированного источника питания переменного тока не менее 220V.

е) Для установки и настройки программного обеспечения, реализующего функции управления защищённой сетью, предоставляет автоматизированное рабочее место с установленной операционной системой Windows XP x86 (32-bit) Service Pack 3 или Windows 2003 Server, Windows 7 Pro x86 (32-bit).

ж) Для установки и настройки, поставляемых Исполнителем товаров, на автоматизированных рабочих местах, обеспечивает предустановленную лицензионную операционную систему, а также набор необходимых офисных приложений и средства антивирусной защиты.

5.3. В рамках оказания услуг по установке, настройке оборудования и программного обеспечения Заказчик обеспечивает доступ специалистов Исполнителя к объектам информатизации и инженерным коммуникациям подразделений администрации. Доступ к ОИ и все работы осуществляются под контролем администратора информационной безопасности администрации города Югорска, который при необходимости предоставляет необходимую техническую документацию и информацию об объектах информатизации (средствах вычислительной техники, активное сетевое оборудование) и инженерных коммуникациях (СКС, слаботочные линии связи и т.п.).

**6. Аттестация объектов информатизации (ОИ) на соответствие требованиям по безопасности информации.**

6.1. Перечень подлежащих аттестации ОИ:

а) автоматизированное рабочее место на базе ПЭВМ, 3 категории, с установленными и настроенными средствами защиты информации (далее – АРМ 1);

б) автоматизированное рабочее место на базе ПЭВМ, 3 категории (далее – АРМ 2).

6.2. Основания для оказания услуг и требования по их исполнению представлены в следующей нормативной документации:

а) «Модель иностранных технических разведок на период до 2020 года (Модель ИТР-2020)» - введена в действие с 01.09.2010 приказом Федеральной службы по техническому и экспортному контролю России от 25.12.2009 № 38;

б) Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам, утверждённые решением Гостехкомиссии при Президенте Российской Федерации от 23.05.1997 № 55;

в) «Инструкция по обеспечению режима секретности в Российской Федерации» от 05.01.2004 № 3-1.

6.3. Объем и содержание оказываемых услуг по аттестации объекта информатизации АРМ 1:

6.3.1. Обследование объекта информатизации, анализ и оценка на соответствие требованиям нормативных правовых документов по защите информации, обрабатываемой на объекте информатизации. Исполнитель осуществляет:

а) анализ исходных данных;

б) проведение предварительного обследования по выявлению возможных каналов утечки информации;

в) анализ состава основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС) объекта СВТ, расположения ОТСС относительно границ контролируемой зоны и относительно ВТСС, имеющих линии связи, выходящие за границы контролируемой зоны. Выявление параллельных пробегов линий связи ОТСС с иными линиями и коммуникациями;

г) разработку программы и методики аттестационных испытаний объекта вычислительной техники;

д) корректировка организационно-распорядительной документации;

е) корректировку и согласование с Заказчиком технической и эксплуатационной документации;

ж) корректировку внутренних организационно-распорядительных и нормативных документов по безопасности информации, необходимых для реализации требований в области технической защиты информации и достаточных для аттестации объекта информатизации.

6.3.2. Подготовка и проведение аттестационных испытаний объекта информатизации на соответствие требованиям безопасности информации. Исполнитель осуществляет:

а) проверку объекта информатизации Заказчика на соответствие организационным требованиям к обеспечению безопасности информации;

б) проверку объекта информатизации Заказчика на соответствие техническим требованиям к обеспечению безопасности информации;

в) проверка объекта информатизации Заказчика на наличие технических каналов утечек информации;

г) разработка протоколов по результатам аттестационных испытаний объектов информатизации Заказчика на соответствие требованиям к обеспечению безопасности информации.

6.3.3. Требования к отчётным документам по итогам оказания услуг:

а) разработка и согласование отчётных материалов по итогам оказания услуг производится в строгом соответствии с действующими руководящими и нормативно-методическими документами ФСБ России и ФСТЭК России.

б) отчётные материалы должны быть представлены в описательной, графической (при необходимости) и табличной форме, в одном экземпляре на бумажных носителях, имеющих установленный руководящими документами гриф секретности.

в) отчётные документы должны быть исполнены без грамматических и орфографических ошибок, опечаток и описок. Официальным языком системы аттестации является русский язык, на котором оформляются все документы, используемые и выдаваемые в рамках системы аттестации.

6.3.4. Перечень отчётных документов и материалов по результатам оказанных услуг по защите информации и аттестации:

- программа-методика проведения аттестационных испытаний объекта информатизации;

- заключение о проведении специальной проверки технических средств и систем;

- акты установки сертифицированных средств защиты информации;

- предписания на эксплуатацию основных технических средств и систем;

- протоколы контроля состояния и эффективности защиты информации на соответствие требованиям по защите информации от несанкционированного доступа;

- протоколы контроля защищённости информации от утечки за счёт побочных электромагнитных излучений и наводки;

- оформление, регистрация и выдача аттестата соответствия объекта информатизации требованиям по безопасности информации.

6.4. Объем и содержание оказываемых услуг по аттестации объекта информатизации АРМ 2.

6.4.1. Обследование объекта информатизации, анализ и оценка на соответствие требованиям нормативных правовых документов по защите информации, обрабатываемой на объекте информатизации. Исполнитель осуществляет:

а) анализ исходных данных;

б) проведение предварительного обследования по выявлению возможных каналов утечки информации;

в) анализ состава основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС) объекта СВТ, расположения ОТСС относительно границ контролируемой зоны и относительно ВТСС, имеющих линии связи, выходящие за границы контролируемой зоны. Выявление параллельных пробегов линий связи ОТСС с иными линиями и коммуникациями;

г) разработку программы и методики аттестационных испытаний объекта вычислительной техники;

д) корректировка организационно-распорядительной документации;

е) корректировку и согласование с Заказчиком технической и эксплуатационной документации;

ж) корректировку внутренних организационно-распорядительных и нормативных документов по безопасности информации, необходимых для реализации требований в области технической защиты информации и достаточных для аттестации объекта информатизации.

6.4.2. Проведение специальной проверки и специальных лабораторных исследований ОТСС, следующих ОТСС:

- системный блок;

- монитор;

- клавиатура;

- манипулятор «мышь».

6.4.3. Требования к порядку оказания услуг по специальной проверки и специальных лабораторных исследованиях:

а) исполнитель должен использовать исправные и поверенные приборы, инструменты и средства измерений. Исполнитель обязан оказывать услуги с соблюдением норм и правил техники безопасности;

б) услуги должны оказываться собственными средствами Исполнителя в специально оборудованных помещениях.

в) исполнитель обязан самостоятельно провести погрузочно-разгрузочные работы и транспортировку оборудования, до технических помещений, в которых будет проводиться специальная проверка.

6.4.4. Поставка средств защиты информации.

Исполнитель должен передать Заказчику сопутствующие услугам средства защиты информации, соответствующие количеству и характеристикам, указанным в Таблице 2 настоящего технического задания.

Таблица 2

| № | Наименование СЗИ | Характеристики СЗИ | Кол-во, шт |
| --- | --- | --- | --- |
| 1 | Право на использование СЗИ от НСД | СЗИ от НСД должно быть предназначено для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах (далее - АС). СЗИ от НСД должно функционировать в среде 32-разрядных операционных систем MS Windows 2000 (Server и Professional), MS Windows XP (Professional и Home Edition), MS Windows Server 2003, MS Windows Vista, MS Windows Server 2008, MS Windows 7 и устанавливаться как на автономных рабочих местах, так и на рабочих станциях и серверах локальной вычислительной сети.Количество пользователей системы должно быть не менее 6 (с учётом администратора);Дополнительные функциональные требованияВ системе защиты информации от несанкционированного доступа должны быть реализованы следующие возможности:• установка и функционирование системы защиты на компьютерах с разными файловыми системами (NTFS, FAT32);• вход в систему пользователей должен осуществляться до загрузки операционной системы только при предъявлении ими специального идентификатора (USB-ключа типа GuardantID, ruToken и пр.) и ввода пароля;• переидентификация пользователей без перезагрузки ОС при использовании однотипных идентификаторов;• одновременная работа одного пользователя с документами разных мандатных меток;• управление запуском и поддержка мандатного принципа контроля доступа для DOS-приложений и консольных приложений Win32;• создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешённых приложений;• запуск хранителя экрана и блокировка рабочей станции при удалении USB-ключа;• использование только зарегистрированных отчуждаемых носителей информации;• маркировка документов, выдаваемых на печать, независимо от печатающего их приложения;• возможность создания дополнительного идентификатора;• сокрытие логической структуры жёсткого диска при загрузке компьютера с внешнего носителя.СЗИ от НСД должно включать и обеспечивать:Поддержку современных операционных систем компании Microsoft СЗИ от НСД должна устанавливаться на автономных рабочих станциях, рабочих станциях в составе рабочей группы или домена, серверах, в том числе в составе кластера. СЗИ от НСД должна функционировать на одно- и многопроцессорных компьютерных системах на базе архитектуры x86 под управлением 32-хразрядных операционных систем Windows Vista, Windows Server 2008, Windows 7.Подсистему контроля устройствДолжна быть обеспечена возможность контроля устройств, подключённых к компьютеру путём задания дескрипторов безопасности для групп однотипных устройств.Подсистему преобразования информации на отчуждаемых носителяхДополнительный механизм защиты съёмных носителей (дискет и флэш-накопителей) путём прозрачного преобразования всей информации, записываемой на носитель. Преобразование информации должна осуществляться с применением функции гаммирования с обратной связью алгоритма криптографического преобразования по ГОСТ 28147-89.Подсистему создания и применения шаблонов настроекДанный механизм должен позволять создавать списки настроек и свободно тиражировать их на другие компьютеры.Поддержку в качестве персональных идентификаторов USB-ключей или флэш-накопителейПодсистему учёта носителей информацииДолжна существовать возможность регистрировать как отчуждаемые носители, так и отдельные тома жёстких дисков.Подсистему регистрацииВсе события СЗИ должны быть доступны для просмотра из одной программы, в т.ч. обеспечиваться функция сортировки и поиска отдельных событий СЗИ.Подсистему маркировки и учёта документов, выдаваемых на печатьПрограмма настройки маркировки документов должна позволять более гибко задавать состав и порядок информации, выводимой на печать.Подсистему управления пользователямиДолжна обеспечиваться функция работы с идентификаторами и возможность редактировать пользователей на удалённых рабочих станциях.Подсистему настройки системы защитыНастройка системы защиты должна быть реализована в виде единого центра настройки. Данное средство защиты информации должно быть сертифицирована ФСТЭК России в системе сертификации средств защиты информации по требованиям безопасности информации №РОСС RU.0001.01БИ00 и иметь действующий сертфикат соотвествия. СЗИ от НСД должно иметь сертификат ФСТЭК России, который удостоверяет, что система защиты информации является программным средством защиты от несанкционированного доступа к информации и соответствует требованиям руководящих документов Гостехкомиссии России "Средства вычислительной техники. Защита информации от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации" по 3 классу защищённости, "Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств информации. Классификация по уровню контроля отсутствия недекларированных возможностей" по 2 уровню контроля. Имеющийся сертификат должен позволять использовать СЗИ от НСД при создании АС класса защищённости до 1Б включительно. | 1 |
| 2 | Устройство защиты информации по каналам побочных электромагнитных излучений и наводок на линии ВТСС, электропитания, заземления и др. токоведущие инженерные коммуникации | Спектральная плотность напряжённости электрической**.** составляющей ЭМПШ, не менее

|  |  |  |
| --- | --- | --- |
| Диапазон частот, ГГц | Вертикальная поляризация, дБ | Горизонтальная поляризация, дБ |
| Без дополнительной антенны | С дополнительной антенной | Без дополнительной антенны | С дополнительной антенной |
| От 0,01 до 0,15 | 50 | 80 | 50 | 80 |
| от 0,15 д до 1 | 45 | 70 | 40 | 70 |
| от 1 до 5 | 45 | 60 | 40 | 55 |
| от 5 до 30 | 45 | 60 | 40 | 50 |
| от 30 до 100 | 40 | 50 | 40 | 50 |
| от 100 до 1000 | 30 | 30 | 30 | 30 |
| от 1000 до 2000 | 30 | 30 | 30 | 30 |

 Спектральная плотность напряжённости магнитной составляющей ЭМПШ, не менее

|  |  |  |
| --- | --- | --- |
| Диапазон частот, МГц | Без дополнительной антенны, дБ | С дополнительной антенной, дБ |
| от 0,01 до 0,15 | 30 | 30 |
| от 0,15 до 4 | 35 | 35 |
| от 4 до 10 | 40 | 40 |
| от 10 до 30 | 30 | 35 |

 Спектральная плотность напряжения помех в линиях электропитания и заземления, не менее

|  |  |  |
| --- | --- | --- |
| Диапазон частот, мГц | Без дополнительной антенны, дБ | С дополнительной антенной, дБ |
| от 0,01 до 0,04 | 25 | 25 |
| от 0,04 до 10 | 35 | 35 |
| от 10 до 100 | 35 | 45 |
| от 100 до 600 | 25 | 25 |
| от 600 до 1000 | 15 | 15 |

 | 1 |

 6.4.5. Разработка проекта организационно-распорядительной документации. Исполнитель осуществляет:

* разработку и согласование с Заказчиком технической и эксплуатационной документации;
* разработку проектов внутренних организационно-распорядительных и нормативных документов по безопасности информации, необходимых для реализации требований в области технической защиты информации и достаточных для аттестации объекта информатизации.

6.4.6. Подготовка и проведение аттестационных испытаний объекта информатизации на соответствие требованиям безопасности информации. Исполнитель осуществляет:

* проверку объекта информатизации Заказчика на соответствие организационным требованиям к обеспечению безопасности информации;
* проверку объекта информатизации Заказчика на соответствие техническим требованиям к обеспечению безопасности информации;
* проверку объекта информатизации Заказчика на наличие технических каналов утечек информации;
* разработку протоколов по результатам аттестационных испытаний объектов информатизации Заказчика на соответствие требованиям к обеспечению безопасности информации.

6.4.7. Требования к отчётным документам по итогам оказания услуг:

* разработка и согласование отчётных материалов по итогам оказания услуг производится в строгом соответствии с действующими руководящими и нормативно-методическими документами ФСБ России и ФСТЭК России;
* отчётные материалы должны быть представлены в описательной, графической (при необходимости) и табличной форме, в одном экземпляре на бумажных носителях, имеющих установленный руководящими документами гриф секретности;
* отчётные документы должны быть исполнены без грамматических и орфографических ошибок, опечаток и описок. Официальным языком системы аттестации является русский язык, на котором оформляются все документы, используемые и выдаваемые в рамках системы аттестации.

6.4.8. Перечень отчётных документов и материалов по результатам оказанных услуг по защите информации и аттестации:

* программа-методика проведения аттестационных испытаний объекта информатизации;
* заключение о проведении специальной проверки технических средств и систем;
* акты установки сертифицированных средств защиты информации;
* предписания на эксплуатацию основных технических средств и систем;
* протоколы контроля состояния и эффективности защиты информации на соответствие требованиям по защите информации от несанкционированного доступа;
* протоколы контроля защищённости информации от утечки за счёт побочных электромагнитных излучений и наводки;

- оформление, регистрация и выдача аттестата соответствия объекта информатизации требованиям по безопасности информации.

6.5. Общие условия и требования

6.5.1. Обязательным условием подписания акта сдачи-приемки оказанных услуг является выдача аттестатов соответствия требованиям по безопасности информации на ОИ сроком на 3 (три) года.

6.5.2. Требования к качеству оказываемых услуг:

Требования к качеству оказания комплекса специальных научно-технических услуг в области защиты информации содержатся в руководящих документах ФСБ России, ФСТЭК России в области защиты информации.

Организация, содержание и полнота оказываемых услуг по защите объектов информатизации от технических средств разведки должны соответствовать требованиям руководящих документов, регламентирующих данное направление защиты информации.

 6.5.3. Требования по обеспечению режима секретности и сохранения государственной тайны при оказании услуг:

* порядок сохранения государственной тайны и соблюдения режима секретности при оказании услуг на объектах должен удовлетворять требованиям «Инструкции по обеспечению режима секретности в Российской Федерации» № 3-1 от 05.01.2004, СТР и другим руководящим документам ФСТЭК России.
* стороны обязаны взять на себя обязательства строго соблюдать конфиденциальность сведений, полученных при оказании услуг, о результатах исследований, степени защищённости объектов информатизации и мероприятиях, применяемых для их защиты, а также технической, финансовой, коммерческой и другой информации и принимать все необходимые меры к предотвращению разглашения имеющихся сведений.
* передача указанной информации другим лицам может осуществляться только с согласия Заказчика, выраженного в письменной форме.
* гриф секретности отчётных документов должен соответствовать степени секретности сведений, содержащихся в документах.

 6.6. Требования по допуску аттестационной комиссии и специалистов Исполнителя на объекты информатизации:

Исполнитель обязан заблаговременно представить в режимно-секретное подразделение Заказчика утверждённый список своих специалистов для оказания услуг по защите информации и членов аттестационной комиссии для проведения аттестационных испытаний, а также список (перечень) оборудования и контрольно-измерительной аппаратуры, необходимых для оказания заявленных услуг (для заказа пропусков на внос и вынос в здание).

Каждый член аттестационной комиссии и специалист Исполнителя для получения доступа к объектам аттестации обязан постоянно иметь на руках документы, удостоверяющие личность, справку о допуске (не ниже второй формы) и предписание на выполнение задания.

6.7. Требования к контрольно-измерительной аппаратуре, инструменту и технике безопасности при оказании услуг:

Все услуги по защите информации и аттестации объектов информатизации проводятся с применением только поверенной и технически исправной контрольно-измерительной аппаратуры и инструментов (Исполнитель обязан предоставить Заказчику свидетельства о поверке аппаратуры).

Услуги по установке и настройке средств защиты информации и аттестации объектов информатизации должны быть оказаны в соответствии с требованиями в Российской Федерации норм и правил охраны труда, техники безопасности, электро-, пожаро- и взрывобезопасности, и не создавать угрозы безопасности для жизни и здоровья людей в процессе эксплуатации объектов.

6.8. Специальные требования и условия:

Заказчик в процессе оказания услуг обязан обеспечить в согласованное время доступ аттестационной комиссии исполнителя на объекты Заказчика для оказания услуг, предусмотренных техническим заданием.

Члены аттестационной комиссии в процессе оказания услуг обязаны:

* осуществлять оказание услуг с учётом действующих у Заказчика правил электробезопасности, охраны труда и техники безопасности;
* выполнять установленные требования пропускного и внутриобъектового режима.

**7. Гарантии, обеспечиваемые Исполнителем.**

 7.1. Передаваемые средства защиты информации должны отвечать санитарным и экологическим требованиям, быть неповреждёнными. В отношении средств защиты информации, для которых законодательством Российской Федерации предусмотрена обязательная сертификация, должны быть представлены соответствующие сертификаты.

Качество средств защиты информации должно соответствовать установленным в Российской Федерации государственным стандартам. Замена некачественных средств защиты информации осуществляется за счёт Исполнителя.

Исполнитель предоставляет гарантию на оборудование системы защиты информации (средства защиты информации) не менее 1 (одного) года, при этом предоставление такой гарантии осуществляется вместе с данными средствами защиты информации и срок действия гарантии устанавливается в соответствии со сроком действия гарантии производителя данных средств защиты информации, указанного в гарантийном талоне.

Исполнитель гарантирует, что все средства защиты информации, передаваемые в соответствии с условиями контракта, являются новыми, неиспользованными, при доставке и далее не будут иметь дефектов, связанных с конструкцией, материалами, либо проявляющихся в результате действий или упущения Исполнителя, при нормальном соблюдении Заказчиком правил хранения и использования средств защиты информации, установленных производителем.

Если в течение гарантийного срока будет выявлено, что средства защиты информации не соответствуют требованиям контракта, Исполнитель обязан предпринять меры по устранению нарушений указанных требований. Устранение нарушений должно быть завершено не позднее 30 (тридцати) рабочих дней с даты поступления официального уведомления от уполномоченного представителя Заказчика.

7.2. Гарантийное техническое сопровождение.

По завершению создания системы защиты информации на ОИ, Исполнителем должно быть обеспечено гарантийное техническое сопровождение в течение 1 (одного) календарного года, с даты выдачи аттестата соответствия объектов информатизации требованиям по безопасности информации.

Гарантийное техническое сопровождение включает в себя:

* консультации по эксплуатации СЗИ;
* консультации Администратора информационной безопасности Заказчика по правилам эксплуатации СЗИ.
* уточнение функций и характеристик устанавливаемых СЗИ;
* разъяснение положений технической документации по установке СЗИ;
* анализ и коррекция допущенных ошибок при эксплуатации СЗИ по телефону, e-mail и на месте расположения объекта информатизации.

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

Приложение 2

к Муниципальному контракту

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

Смета контракта

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование товара/услуги | Кол-во, шт. | Цена, руб. | Сумма (с НДС), руб. | в т.ч. НДС, руб |
| 1 | Право на использование программного обеспечения, реализующего функции криптографического шлюза | 1 |  |  |  |
| 2 | Право на использование программного обеспечения, реализующего функции управления защищённой сетью | 1 |  |  |  |
| 3 | Право на использование программное обеспечение, реализующее функции криптографического клиента для защиты каналов связи по классу защиты КС2 | 5 |  |  |  |
| 4 | Комплект дистрибутивов программного обеспечения для защиты каналов связи | 1 |  |  |  |
| 5 | Право на использование СЗИ от НСД | 5 |  |  |  |
| 6 | Программа для ЭВМ Kaspersky Certifiedmedia Pack Customized Russian Edition. Media Pack | 1 |  |  |  |
| 7 | Неисключительное право на программный продукт Дополнительный модуль для UserGate Proxy & Firewall 6.X Entensys URL Filtering (до 200 сессий на 1 год) | 1 |  |  |  |
| 8 | Право на использование СЗИ от НСД | 1 |  |  |  |
| 9 | Устройство защиты информации по каналам побочных электромагнитных излучений и наводок на линии ВТСС, электропитания, заземления и др. токоведущие инженерные коммуникации | 1 |  |  |  |
| 10 | Услуги по технической защите информации |  |  |  |  |

|  |  |
| --- | --- |
| **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)
2. *Наименование страны происхождения товаров указывается в соответствии с Общероссийским классификатором стран мира ОК (МК (ИСО 3166) 004-97) 025-2001 (Постановление Госстандарта России от 14.12.2001 №529-ст «О принятии и введении в действие общероссийского классификатора стран мира»). Понятие страны происхождения товара регламентируется положениями части 1 статьи 58 Таможенного кодекса Таможенного Союза.* [↑](#footnote-ref-2)