**III. ПРОЕКТ КОНТРАКТА**

**МУНИЦИПАЛЬНый КОНТРАКТ на оказание услуг №\_\_\_\_\_\_\_**

(ИКЗ № 203862200236886220100101190016202244)

г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_202\_\_ 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 аттестации рабочих мест отдела опеки и попечительства, а Заказчик обязуется принять и оплатить их.

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

1.3. Место оказания услуг: Администрация города Югорска, 628260, Ханты-Мансийский автономный округ – Югра, г. Югорск, ул. Ленина, д.41.

**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.

Источник финансирования: бюджет города Югорска на 2020 год (субвенция отдела опеки и попечительства).

2.2. Общая цена Контракта составляет \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_ копеек, включая налог на добавленную стоимость (\_\_ %): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ рублей \_\_ копеек / *НДС не облагается в соответствии с п. \_\_\_ ст. \_\_\_\_ Налогового кодекса Российской Федерации.[[1]](#footnote-1)*

Сумма, подлежащая уплате Исполнителю, уменьшается, на размер налогов, сборов и иных обязательных платежей в бюджеты бюджетной системы Российской Федерации, связанных с оплатой контракта, если в соответствии с законодательством Российской Федерации о налогах и сборах такие налоги, сборы и иные обязательные платежи подлежат уплате в бюджеты бюджетной системы Российской Федерации Заказчиком.

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. Расчёты по Контракту производятся 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 15 (пятнадцати) дней со дня подписания Заказчиком документа о приёмке, предусмотренного Контрактом.

2.5. В случае уменьшения Заказчику соответствующим финансовым органом 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. По согласованию с Исполнителем изменить объем услуг в соответствии с пунктом 12.6 Контракта.

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

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

3.1.5. Осуществлять иные права, предусмотренные Контрактом и (или) 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.

3.4.3. Привлекать для оказания услуг соисполнителей.

**4. Сроки оказания услуг**

4.1. Срок оказания услуг: с момента заключения муниципального контракта по 30.11.2020.

4.2. Досрочная сдача результатов услуг допускается только по согласованию с Заказчиком. В случае согласования досрочного оказания услуг Заказчик обязуется принять услуги и подписать документ о приёмке 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.

4.4. В случае, установленном в п. 4.3. Контракта акт взаимосверки признаётся документом, подтверждающим приёмку, в части фактически исполненных обязательствах по Контракту, в связи с чем взаиморасчёты между Сторонами осуществляются в срок, установленный в п. 2.4.4. Контракта.

**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 извещение (уведомление) о готовности услуг к сдаче и документ о приёмке.

5.3. Заказчик вправе создать приёмочную комиссию, в составе не менее пяти человек, для проверки соответствия качества услуг требованиям, установленным Контрактом. Проверка соответствия качества оказываемых услуг требованиям, установленным Контрактом, может также осуществляться с привлечением экспертов, экспертных организаций.

5.4. Стороны подписывают документ о приёмке в течение 3 дней со дня получения документа о приёмке.

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.

5.9. Приёмка услуг в целом оформляется документом о приёмке[[2]](#footnote-2) (актом оказанных услуг), который составляется в двух экземплярах и подписывается Заказчиком (в случае создания приёмочной комиссии подписывается всеми членами приёмочной комиссии и утверждается Заказчиком) и Исполнителем. В случае, когда оказание услуг осуществляется в интересах Исполнителя, документ о приёмке составляется в трёх экземплярах и подписывается Исполнителем, Заказчиком (в случае создания приёмочной комиссии подписывается всеми членами приёмочной комиссии и утверждается Заказчиком) и Исполнителем.

5.10. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом приёмка услуг оформляется документом о приёмке, в котором указываются: сведения о фактически исполненных обязательствах по Контракту, сумма, подлежащая оплате в соответствии с условиями настоящего 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. Документ составляется в двух экземплярах, подписывается Заказчиком (в случае создания приёмочной комиссии подписывается всеми членами приёмочной комиссии и утверждается Заказчиком) и Исполнителем. В случае, когда оказание услуг осуществляется в интересах Исполнителя, документ о приёмке составляется в трёх экземплярах и подписывается Исполнителем, Заказчиком (в случае создания приёмочной комиссии подписывается всеми членами приёмочной комиссии и утверждается Заказчиком) и Исполнителем.

5.11. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом[[3]](#footnote-3), Заказчик производит удержание неустойки (штрафа, пеней) и (или) возмещения убытков причинённых Исполнителем убытков. Удержание неустойки (штрафа, пеней) и (или) убытков производится Заказчиком на основании документа, составленного в соответствии с пунктом 5.10. Контракта, не позднее сроков установленных в пункте 2.4.4. Контракта. При этом исполнение обязательства Исполнителем по перечислению неустойки (штрафа, пени) и (или) убытков в доход бюджета возлагается на Заказчика.

**6. Обеспечение исполнения контракта, обеспечение гарантийных обязательств[[4]](#footnote-4)**

6.1. Исполнение контракта, гарантийные обязательства обеспечиваются предоставлением банковской гарантии, выданной банком и соответствующей требованиям статьи 45 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», или внесением денежных средств на указанный заказчиком счёт, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими заказчику.

Способ обеспечения исполнения контракта, гарантийных обязательств, срок действия банковской гарантии определяются в соответствии с требованиями Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» участником закупки, с которым заключается контракт, самостоятельно.

6.2. Обеспечение исполнения Контракта предоставляется Заказчику до заключения Контракта. Размер обеспечения исполнения Контракта составляет 10 384 (десять тысяч триста восемьдесят четыре) рубля 65 копеек (5% от начальной (максимальной) цены контракта).

6.3. В ходе исполнения контракта Исполнитель вправе изменить способ обеспечения исполнения контракта и (или) предоставить Заказчику взамен ранее предоставленного обеспечения исполнения контракта новое обеспечение исполнения контракта, размер которого может быть уменьшен в порядке и случаях, которые предусмотрены частями 7.2 и 7.3 статьи 96 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». Исполнитель вправе изменить способ обеспечения гарантийных обязательств и (или) предоставить заказчику взамен ранее предоставленного обеспечения гарантийных обязательств новое обеспечение гарантийных обязательств.

6.4. Срок действия банковской гарантии должен превышать предусмотренный контрактом срок исполнения обязательств, которые должны быть обеспечены такой банковской гарантией, не менее чем на один месяц, в том числе в случае его изменения в соответствии со статьёй 95 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

В случае отзыва в соответствии с законодательством Российской Федерации у банка, предоставившего банковскую гарантию в качестве обеспечения исполнения Контракта, лицензии на осуществление банковских операций Исполнитель обязан предоставить новое обеспечение исполнения контракта не позднее одного месяца со дня надлежащего уведомления Заказчиком Исполнителя о необходимости предоставить соответствующее обеспечение.

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. Банковская гарантия оформляется в письменной форме на бумажном носителе или в форме электронного документа, подписанного усиленной квалифицированной электронной подписью лица, имеющего право действовать от имени банка, на условиях, определённых гражданским законодательством, Федеральным законом 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 8 ноября 2013 г. №1005 (с учётом изменений и дополнений).

6.7. Денежные средства возвращаются в полном объёме либо в части, оставшейся после удовлетворения требований Заказчика, возникших в период действия обеспечения в срок не превышающий тридцать дней с момента подписания Сторонами документов, подтверждающих надлежащее исполнение обязательств по Контракту[[5]](#footnote-5).

6.8. Предусмотренное [частями 7](https://login.consultant.ru/link/?rnd=35D11FC4BBD9CC225822D2561C3F808A&req=doc&base=LAW&n=315347&dst=1109&fld=134&date=19.06.2019) статьи 96 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» уменьшение размера обеспечения исполнения контракта осуществляется при условии отсутствия неисполненных Исполнителем требований об уплате неустоек (штрафов, пеней), предъявленных заказчиком в соответствии с Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», а также приёмки заказчиком поставленного товара, результатов отдельного этапа исполнения контракта в объёме выплаченного аванса (если контрактом предусмотрена выплата аванса).

6.9. Участник закупки, с которым заключается контракт по результатам определения поставщика в соответствии с [пунктом 1 части 1 статьи 30](https://login.consultant.ru/link/?rnd=35D11FC4BBD9CC225822D2561C3F808A&req=doc&base=LAW&n=315347&dst=101858&fld=134&date=19.06.2019) Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», освобождается от предоставления обеспечения исполнения контракта, в том числе с учётом положений [статьи 37](https://login.consultant.ru/link/?rnd=35D11FC4BBD9CC225822D2561C3F808A&req=doc&base=LAW&n=315347&dst=100437&fld=134&date=19.06.2019) Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», в случаях установленных Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

6.10. Обеспечение исполнения контракта не применяется в случаях, установленных Федеральным законом от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд».

**7. Ответственность Сторон[[6]](#footnote-6)**

7.1. Стороны несут ответственность за неисполнение и ненадлежащее исполнение Контракта, в том числе за неполное и (или) несвоевременное исполнение своих обязательств по Контракту, в соответствии с положениями Гражданского кодекса Российской Федерации, 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 30.08.2017 № 1042 (с учётом изменений и дополнений).

7.2. Размер штрафа устанавливается Контрактом в порядке, установленном пунктами 7.3 – 7.7, в виде фиксированной суммы, в том числе рассчитываемой как процент цены Контракта, или в случае, если Контрактом предусмотрены этапы исполнения Контракта, как процент этапа исполнения Контракта (далее - цена контракта (этапа)).

7.3. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, размер штрафа устанавливается следующем порядке (за исключением случаев, предусмотренных [пунктами 7.4](#P67) – 7.[7](#P81)):

а) 10 процентов цены Контракта (этапа) в случае, если цена Контракта (этапа) не превышает 3 млн. рублей;

б) 5 процентов цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 3 млн. рублей до 50 млн. рублей (включительно);

в) 1 процент цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 50 млн. рублей до 100 млн. рублей (включительно);

г) 0,5 процента цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 100 млн. рублей до 500 млн. рублей (включительно);

д) 0,4 процента цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 500 млн. рублей до 1 млрд. рублей (включительно);

е) 0,3 процента цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 1 млрд. рублей до 2 млрд. рублей (включительно);

ж) 0,25 процента цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 2 млрд. рублей до 5 млрд. рублей (включительно);

з) 0,2 процента цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 5 млрд. рублей до 10 млрд. рублей (включительно);

и) 0,1 процента цены Контракта (этапа) в случае, если цена Контракта (этапа) превышает 10 млрд. рублей.

7.4. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, заключённым по результатам определения Исполнителя в соответствии с [пунктом 1 части 1 статьи 30](consultantplus://offline/ref=D24FEE69E1B7CD8A16BB8E7671CAA689283A9F94587855EC14DDB06FAEC3FCB85E295C0AE157E7F5VF7DG) Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд», за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, размер штрафа устанавливается в размере 1 процента цены контракта (этапа), но не более 5 тыс. рублей и не менее 1 тыс. рублей.

7.5. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, заключённым с победителем закупки (или с иным участником закупки в случаях, установленных Федеральным [законом](consultantplus://offline/ref=D24FEE69E1B7CD8A16BB8E7671CAA689283A9F94587855EC14DDB06FAEVC73G)), предложившим наиболее высокую цену за право заключения Контракта, размер штрафа рассчитывается в порядке, установленном Правилами, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, и устанавливается в следующем порядке:

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

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

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

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

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

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

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

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

7.6. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательства, предусмотренного Контрактом, которое не имеет стоимостного выражения, размер штрафа устанавливается (при наличии в Контракте таких обязательств) в следующем порядке:

а) 1000 рублей, если цена Контракта не превышает 3 млн. рублей;

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

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

г) 100000 рублей, если цена Контракта превышает 100 млн. рублей.

7.7. В случае если в соответствии с [частью 6 статьи 30](consultantplus://offline/ref=D24FEE69E1B7CD8A16BB8E7671CAA689283A9F94587855EC14DDB06FAEC3FCB85E295C0AE157E7F7VF75G) Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» Контрактом предусмотрено условие о гражданско-правовой ответственности Исполнителей за неисполнение условия о привлечении к исполнению Контракта, соисполнителей из числа субъектов малого предпринимательства, социально ориентированных некоммерческих организаций в виде штрафа, штраф устанавливается в размере 5 процентов объёма такого привлечения, установленного контрактом.

7.8. За каждый факт неисполнения Заказчиком обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств, предусмотренных Контрактом, размер штрафа устанавливается в следующем порядке:

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

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

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

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

7.9. Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного контрактом, начиная со дня, следующего после дня истечения установленного контрактом срока исполнения обязательства, и устанавливается контрактом в размере одной трёхсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены контракта, уменьшенной на сумму, пропорциональную объёму обязательств, предусмотренных контрактом и фактически исполненных Исполнителем, за исключением случаев, если законодательством Российской Федерации установлен иной порядок начисления пени.

7.10. 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.

7.11. Пеня устанавливается Контрактом в размере одной трёхсотой действующей на дату уплаты пеней ключевой ставки Центрального банка Российской Федерации от не уплаченной в срок суммы (пункт 5 статьи 34 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»).

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

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

**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. Любые споры, разногласия и требования, возникающие из Контракта, подлежат разрешению 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 невозможно 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 трёх рабочих дней, следующих 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 трёх рабочих дней, следующих 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 по 20.12.2020.

С 21.12.2020 обязательства Сторон по Контракту прекращаются, за исключением обязательств по оплате услуг, гарантийных обязательств, обязательств по возмещению убытков и выплате неустойки.

**12. Прочие условия**

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

12.2. Все приложения к Контракту являются его неотъёмной частью.

12.3. К Контракту прилагаются:

- Техническое задание (Приложение).

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

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

12.6. Заказчик по согласованию с Исполнителем в ходе исполнения Контракта вправе изменить не более чем на десять процентов предусмотренный Контрактом объем услуг при изменении потребности в услугах, на оказание которых заключён контракт. При этом по соглашению Сторон допускается изменение с учётом положений бюджетного законодательства Российской Федерации цены Контракта пропорционально дополнительному объёму услуг исходя из установленной в Контракте цены единицы услуги, но не более чем на десять процентов цены Контракта. При уменьшении предусмотренного Контрактом объёма услуг Стороны контракта обязаны уменьшить цену Контракта исходя из цены единицы услуги.

12.7.  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.

12.8. 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:

Контрактная служба: Дергилев О.В.

Бухгалтерия: (раздел 2 Контракта) Михайлова Л.А.

Юридическое управление: Плотников Д.С.

Приложение

к Муниципальному контракту

№ \_\_\_\_ от «\_\_\_» \_\_\_\_\_\_\_ 202\_\_ г.

**Техническое задание**

**1.** **Предмет муниципального контракта**: оказание услуг по аттестации рабочих мест отдела опеки и попечительства.

**2. Используемые сокращения:**

АРМ - автоматизированное рабочее место;

ИСПДн – информационная система персональных данных;

ГИС – государственная информационная система;

МЭ – межсетевой экран;

НСД - несанкционированный доступ;

ОС – операционная система;

ПАК – программно-аппаратный комплекс;

ПДн – персональные данные;

ПО - программное обеспечение;

ПЭВМ - персональная электронно-вычислительная машина;

СЗИ – система защиты информации;

СЗПДн - система защиты информационной системы персональных данных;

СрЗИ - средство защиты информации;

СКЗИ - средства криптографической защиты информации;

ТЗ - техническое задание;

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 должны быть оказаны услуги по проведению аттестации 8 (восьми) рабочих мест отдела опеки и попечительства администрации города Югорска (создание системы защиты информации).

3.2. Цели и задачи оказания услуг:

Основной целью услуги является создание системы защиты информационной системы персональных данных администрации города Югорска.

Достижение указанной цели обеспечивается выполнением следующих задач:

1) выполнение требований нормативных правовых актов Российской Федерации, руководящих документов ФСТЭК России и ФСБ России, регламентирующих вопросы защиты персональных данных;

2) обеспечение безопасности информации и персональных данных при их обработке в ИСПДн путём нейтрализации актуальных угроз безопасности;

3) построение системы защиты информационной системы персональных данных.

3.3. Место оказания услуг: г. Югорск, Ханты-Мансийский автономный округ-Югра, Тюменская область, ул. Ленина, д.41.

3.4. Комплекс мероприятий должен соответствовать следующим нормативным правовым актам и руководящим документам:

- федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

- указ Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

- постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая ФСТЭК России 15.02.2008;

- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая ФСТЭК России 14.02.2008;

- приказ ФСБ от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости»;

- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утверждённая приказом ФАПСИ от 13.06.2001 № 152.

**4. Объём и содержание оказываемых услуг**

4.1. Объектом защиты СЗИ является конфиденциальная информация, обрабатываемая в ИСПДн администрации города Югорска.

Состав объекта защиты: общее количество АРМ – 8.

Подробное описание ИСПДн представлено в таблице 1.

Таблица 1. Описание ИСПДн

|  |  |
| --- | --- |
| Уровень защищенности ИСПДн | 4 |
| Класс защищённости | К3 |
| Категории ПДн | Специальные |
| Объем обрабатываемых ПДн | Менее 100 000 субъектов |
| Наличие подключения к сетям международного информационного обмена | ИСПДн, имеющая одноточечное подключение к сетям связи международного информационного обмена |
| Режим обработки ПДн | Многопользовательский |
| Структура ИСПДн | Локальная |
| Тип актуальных угроз | 3-ий тип |

В соответствии с подпунктом 1 пункта 1 статьи 13 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», ИСПДн относятся к государственным информационным системам.

4.2. Настоящее Техническое задание предполагает выполнение следующих этапов услуги:

* + - 1. обследование информационной системы с целью определения текущего состояния обеспечения безопасности информации и определения состава и структуры системы защиты информации;
      2. формирование требований к системе защиты информации;
      3. разработка организационно-распорядительной документации по защите информации;
      4. поставка, установка и конфигурирование программных средств для обеспечения защиты персональных данных;
      5. оценка соответствия (аттестация) системы защиты информации требованиям безопасности информации.

4.3. Требования к содержанию услуги.

4.3.1. Обследование информационной системы включает в себя следующие работы:

* + - 1. Сбор сведений о ИСПДн (тип операционной системы, количество АРМ, структурная схема ИСПДн);
      2. Обследование состояния защищённости ИСПДн по требованиям безопасности информации осуществляется путём анкетирования, опроса специалистов и посещения объектов информатизации для изучения.

В ходе обследования:

- осуществляется сбор и систематизация данных об используемых основных и вспомогательных технических средствах и системах, а также каналах передачи данных;

- уточняется состав каждого выявленного объекта информатизации (ИСПДн);

- уточняется перечень информации, подлежащих защите на каждом объекте ИСПДн;

- уточняется состав защищаемой информации, обрабатываемой автоматизированным способом;

- собирается информация о защищённости ИСПДн на каждом объекте ИСПДн;

- уточняются условия расположения ИСПДн относительно границ контролируемой зоны;

- уточняются конфигурация, компоненты и топология ИСПДн, их физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

- уточняются состав технических средств и систем, предполагаемых к использованию в СЗИ, условия их расположения, общесистемные и прикладные программные средства;

- производится сбор документации, необходимой для достижения целей обследования (методы и способы сбора документации определяются Исполнителем совместно с Заказчиком), в частности: действующих политик информационной безопасности; документов, определяющих организационную структуру Заказчика; сведений об ИТ-инфраструктуре; сведений о действующей системе обеспечения информационной безопасности;

- определяется состав ИСПДн и проводится её классификация (определение уровня защищённости ПДн в ИСПДн, класса защищённости ИСПДн).

Обследование и анализ имеющейся системы защиты информации и применяемых технических мер (средства защиты информации и т.п.).

В ходе обследования:

- уточняется состав используемых средств защиты информации;

- подготавливается описание существующей системы защиты для ИСПДн;

- уточняются режимы обработки информации в ИСПДн в целом и в отдельных её компонентах.

4.3.2. Формирование требований к системе защиты персональных данных включает в себя:

* + - 1. Определение актуальных угроз безопасности персональных данных;
      2. Определение уровней защищённости персональных данных;
      3. Уточнение и дополнение базового набора мер.

Актуальные угрозы безопасности информации определяются по результатам оценки возможностей и потенциала нарушителей (внешних, внутренних), анализа возможных уязвимостей ИСПДн, а также с учётом структурно-функциональных характеристик ИСПДн.

Класс защищённости ИСПДн определяется в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Уровень защищённости персональных данных при обработке в ИСПДн определяется в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Предварительно определённый уровень защищённости ПДн в ИСПДн – УЗ 4.

Предварительно определённый класс защищённости ИСПДн – К3.

Базовый набор мер, который необходимо реализовать при создании системы защиты информации с учётом предварительно определённых уровня защищённости ПДн в ИСПДн и класса защищённости ИСПДн, приведён в таблице 2.

Таблица 2 –Базовый набор мер, который необходимо реализовать

при создании системы защиты информации в ГИС (К3, УЗ3)

| **Условное обозначение и номер меры** | **Содержание мер по обеспечению безопасности персональных данных** |
| --- | --- |
|
|  |
| I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ) | |
| ИАФ.1 | Идентификация и аутентификация пользователей, являющихся работниками оператора |
| ИАФ.3 | Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов |
| ИАФ.4 | Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации |
| ИАФ.5 | Защита обратной связи при вводе аутентификационной информации |
| ИАФ.6 | Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей) |
| II. Управление доступом субъектов доступа к объектам доступа (УПД) | |
| УПД.1 | Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей |
| УПД.2 | Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа |
| УПД.3 | Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами |
| УПД.4 | Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы |
| УПД.5 | Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы |
| УПД.6 | Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) |
| УПД.10 | Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу |
| УПД.11 | Разрешение (запрет) действий пользователей, разрешённых до идентификации и аутентификации |
| УПД.13 | Реализация защищённого удалённого доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети |
| УПД.14 | Регламентация и контроль использования в информационной системе технологий беспроводного доступа |
| УПД.15 | Регламентация и контроль использования в информационной системе мобильных технических средств |
| УПД.16 | Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) |
| III. Ограничение программной среды (ОПС) | |
| ОПС.3 | Установка (инсталляция) только разрешённого к использованию программного обеспечения и (или) его компонентов |
| IV. Защита машинных носителей информации (ЗНИ) | |
| ЗНИ.1 | Учет машинных носителей информации |
| ЗНИ.2 | Управление доступом к машинным носителям информации |
| ЗНИ.8 | Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) |
| V. Регистрация событий безопасности (РСБ) | |
| РСБ.1 | Определение событий безопасности, подлежащих регистрации, и сроков их хранения |
| РСБ.2 | Определение состава и содержания информации о событиях безопасности, подлежащих регистрации |
| РСБ.3 | Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения |
| РСБ.4 | Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объёма (ёмкости) памяти |
| РСБ.5 | Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них |
| РСБ.6 | Генерирование временных меток и (или) синхронизация системного времени в информационной системе |
| РСБ.7 | Защита информации о событиях безопасности |
| VI. Антивирусная защита (АВЗ) | |
| АВЗ.1 | Реализация антивирусной защиты |
| АВЗ.2 | Обновление базы данных признаков вредоносных компьютерных программ (вирусов) |
| VIII. Контроль (анализ) защищённости персональных данных (АНЗ) | |
| АНЗ.1 | Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей |
| АНЗ.2 | Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации |
| АНЗ.3 | Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации |
| АНЗ.4 | Контроль состава технических средств, программного обеспечения и средств защиты информации |
| АНЗ.5 | Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе |
| IX. Обеспечение целостности информационной системы и информации (ОЦЛ) | |
| ОЦЛ.3 | Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций |
| XI. Защита среды виртуализации (ЗСВ) | |
| ЗСВ.1 | Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации |
| ЗСВ.2 | Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин |
| ЗСВ.3 | Регистрация событий безопасности в виртуальной инфраструктуре |
| ЗСВ.9 | Реализация и управление антивирусной защитой в виртуальной инфраструктуре |
| ЗСВ.10 | Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей |
| XII. Защита технических средств (ЗТС) | |
| ЗТС.2 | Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования |
| ЗТС.3 | Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены |
| ЗТС.4 | Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр |
| XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС) | |
| ЗИС.3 | Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи |
| ЗИС.5 | Запрет несанкционированной удалённой активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удалённо, и оповещение пользователей об активации таких устройств |
| ЗИС.20 | Защита беспроводных соединений, применяемых в информационной системе |
| ЗИС.30 | Защита мобильных технических средств, применяемых в информационной системе |
| XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ) | |
| УКФ.1 | Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных |
| УКФ.2 | Управление изменениями конфигурации информационной системы и системы защиты персональных данных |
| УКФ.3 | Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных |
| УКФ.4 | Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных |

Актуальные угрозы безопасности информации определяются по результатам оценки возможностей и потенциала нарушителей (внешних, внутренних), анализа возможных уязвимостей информационной системы персональных данных, возможных последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности), а также с учётом структурно-функциональных характеристик ИСПДн.

В рамках данного этапа исполнитель производит анализ уязвимостей ИСПДн, сертифицированным ФСТЭК России сканером безопасности.

Требования к системе защиты информации определяются для ИСПДн с учётом адаптированного базового состава мер по защите информации в зависимости от уровня защищённости ПДн при их обработке в ИСПДн, класса защищённости ИСПДн и актуальных угроз безопасности информации и должны учитывать выявленные на данном этапе уязвимости ИСПДн.

Состав конкретных мер по защите информации определяется на основе адаптации и уточнения базового набора мер по обеспечению безопасности информации, с учётом структурно-функциональных характеристик, информационных технологий, особенностей функционирования ИСПДн (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн).

При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности информации, а также с учётом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер разрабатываются иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности информации. При этом должны быть оценены достаточность и актуальность компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

Результаты работ по формированию требований к системе защиты информации отражаются в следующих документах:

- Акт определения уровня защищённости ПДн при их обработке в ИСПДн;

- Акт классификации ИСПДн;

- Уточнённый состав мер по защите информации для реализации в системе защиты информации ИСПДн;

- Частное техническое задание на создание системы защиты информации;

- Модель угроз и нарушителя безопасности информации и персональных данных в ИСПДн.

4.3.3. Поставка программных средств, оборудования и товара для обеспечения защиты персональных данных.

Исполнителем поставляются программные средства для обеспечения защиты персональных данных в соответствии с таблицей 3.

Таблица 3

Требования к поставляемым программным средствам

для обеспечения защиты персональных данных

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Параметры требований к программным средствам для обеспечения защиты персональных данных** | **Требования к программным средствам для обеспечения защиты персональных данных** |
|  | Передача неисключительных прав на использование средства защиты информации от несанкционированного доступа (для платформ Windows) | Средство защиты информации (ПО) от несанкционированного доступа должно иметь следующие характеристики:  1. Для применения на ПК под управлением операционных систем Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 в многопользовательском режиме их эксплуатации и поддержкой 32-х/64-х битных версий.  2. Сертификация по требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по не менее чем 5 классу защиты от НСД для СВТ и по не менее, чем по 4 классу защиты.  3. Обеспечивать:  - возможность настройки всех параметров из единой консоли администрирования;  - разграничение прав пользователей при работе на ПЭВМ. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), доступа к сети, доступа к сменным накопителям. Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных.  - блокировку файлов по расширению;  - генерация сложных паролей;  - возможность ограничивать его средствами, круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станция и отдельных папок общего доступа);  - аудит действий пользователей, независимыми от ОС средствами (вход/выход, доступ к ресурсам, запуск процессов, печать документов, управление учётными записями и политиками безопасности). Должны вестись непрерывные журналы (т.е. новые записи не должны затирать более старые);  - возможность локального и удалённого администрирования (управление пользователями, политиками безопасности, правами доступа, аудитом; просмотр журналов);  - возможность регистрации доменных учётных записей с помощью маски (\*\\*);  - возможность периодического контроля целостности файлов и программно-аппаратной среды, а также контроля по команде администратора и по расписанию.  - очистку остаточной информации (принудительная зачистка определённых файлов и папок);  - возможность организации режима замкнутой программной среды;  - возможность самодиагностики основного функционала;  - ведение двух копий программных средств защиты информации;  - возможность создания отчёта по назначенным правам;  - возможность ограничивать круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станций и отдельных папок общего доступа);  - преобразование данных в файл-контейнер для хранения их на внешних носителях либо для передачи по различным каналам связи. Возможность использования встроенного алгоритма преобразования ГОСТ 28147-89, либо подключение внешнего криптопровайдера, в том числе сертифицированного;  - удалённое администрирование;  - централизованное управление защищёнными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учётными записями пользователей, политиками, правами пользователей. Также этим модулем должен осуществляться периодический сбор журналов со всех защищённых рабочих станций;  - возможность построения иерархии управления при помощи специального модуля - менеджера, управляющего несколькими модулями централизованное управления;  - установка должна производиться локально, с помощью модуля централизованного управления, средствами групповых политик AD;  - сигнализация попыток несанкционированного доступа и его деактивации. Отправка сообщений о попытках несанкционированного доступа на почту;  - должно быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы Touch Memory (iButton), eTokenPro/Java(в том числе смарт-карты eToken), Rutoken, Rutoken ЭЦП.  У поставляемой системы защиты информации срок действия лицензии должен быть - «бессрочно».  Права на средство защиты информации от несанкционированного доступа передаются с сопутствующими дистрибутивами на физическом носителе. Физический носитель имеет формуляр, в котором указаны специальные учётные номера ФСТЭК России.  Комплект поставки:  - формуляр;  - копия сертификата соответствия ФСТЭК России;  - краткое руководство пользователя;  - верифицированный дистрибутив (компакт диск).  **Количество – 5 шт.** |
|  | Передача неисключительных прав на использование средства защиты информации от несанкционированного доступа с модулем межсетевого экранирования (для платформ Windows) | Средство защиты информации (ПО) от несанкционированного доступа должно иметь следующие характеристики:  1. Для применения на ПК под управлением операционных систем Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 в многопользовательском режиме их эксплуатации и поддержкой 32-х/64-х битных версий.  2. Сертификация по требованиям Руководящих документов (РД) ФСТЭК России (Гостехкомиссии России) по не менее чем 5 классу защиты от НСД для СВТ и по не менее, чем по 4 классу защиты.  3. Обеспечивать:  - возможность настройки всех параметров из единой консоли администрирования;  - разграничение прав пользователей при работе на ПЭВМ. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), доступа к сети, доступа к сменным накопителям. Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных.  - блокировку файлов по расширению;  - генерация сложных паролей;  - возможность ограничивать его средствами, круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станция и отдельных папок общего доступа);  - аудит действий пользователей, независимыми от ОС средствами (вход/выход, доступ к ресурсам, запуск процессов, печать документов, управление учётными записями и политиками безопасности). Должны вестись непрерывные журналы (т.е. новые записи не должны затирать более старые);  - возможность локального и удалённого администрирования (управление пользователями, политиками безопасности, правами доступа, аудитом; просмотр журналов);  - возможность регистрации доменных учётных записей с помощью маски (\*\\*);  - возможность периодического контроля целостности файлов и программно-аппаратной среды, а также контроля по команде администратора и по расписанию.  - очистку остаточной информации (принудительная зачистка определённых файлов и папок);  - возможность организации режима замкнутой программной среды;  - возможность самодиагностики основного функционала;  - ведение двух копий программных средств защиты информации;  - возможность создания отчёта по назначенным правам;  - возможность ограничивать круг доступных сетевых ресурсов (с точностью до отдельных удалённых рабочих станций и отдельных папок общего доступа);  - преобразование данных в файл-контейнер для хранения их на внешних носителях либо для передачи по различным каналам связи. Возможность использования встроенного алгоритма преобразования ГОСТ 28147-89, либо подключение внешнего криптопровайдера, в том числе сертифицированного;  - удалённое администрирование;  - централизованное управление защищёнными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учётными записями пользователей, политиками, правами пользователей. Также этим модулем должен осуществляться периодический сбор журналов со всех защищённых рабочих станций;  - возможность построения иерархии управления при помощи специального модуля - менеджера, управляющего несколькими модулями централизованное управления;  - установка должна производиться локально, с помощью модуля централизованного управления, средствами групповых политик AD;  - сигнализация попыток несанкционированного доступа и его деактивации. Отправка сообщений о попытках несанкционированного доступа на почту;  - должно быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы Touch Memory (iButton), eTokenPro/Java(в том числе смарт-карты eToken), Rutoken, Rutoken ЭЦП;  - фильтрация сетевого трафика;  - работа правил исключения;  - разделение сетей на доверенные и не доверенные согласно профилям;  - контроль сетевых соединений;  - сбор и отображение статистической информации о функционировании МЭ;  - удалённое и централизованное управление;  - обеспечение защиты от атак на сетевые протоколы на различных уровнях модели OSI;  - осуществление перехвата вызова функций ОС сторонними приложениями с возможностью гибкой настройки ограничения доступа к системным функциям для не доверенных приложений.  У поставляемой системы защиты информации срок действия лицензии должен быть - «бессрочно».  Права на средство защиты информации от несанкционированного доступа передаются с сопутствующими дистрибутивами на физическом носителе. Физический носитель имеет формуляр, в котором указаны специальные учётные номера ФСТЭК России.  Комплект поставки:  - формуляр;  - копия сертификата соответствия ФСТЭК России;  - краткое руководство пользователя;  - верифицированный дистрибутив (компакт диск).  **Количество – 3 шт.** |

Программное обеспечение передаётся Заказчику в соответствии с действующим законодательством с предоставлением сублицензионного договора и актов приёма-передачи неисключительных прав.

Исполнитель осуществляет поставку средств защиты информации по адресу: 628260, Ханты-Мансийский Автономный округ - Югра, город Югорск, улица 40 лет Победы, 11. В случае использования услуг перевозчика для доставки Исполнитель обязан известить Заказчика о факте передачи средств защиты информации перевозчику, а также о наименовании перевозчика и реквизитах отгрузочных документов.

4.3.4. Установка и настройка средств защиты информации осуществляется Исполнителем в соответствии с решениями, изложенными в техническом задании на систему защиты информационных систем персональных данных.

При установке и настройке СрЗИ должна производиться их интеграция с имеющимися средствами защиты информации. Настройка СрЗИ должна обеспечить функционирование подсистемы защиты от несанкционированного доступа, межсетевого экранирования и антивирусной защиты.

Настроенные средства защиты не должны нарушать функционирование защищаемых информационных систем персональных данных. В целях снижения вероятности возникновения ошибок и нарушения работы ИСПДн, настройка СрЗИ должна производиться последовательно в несколько этапов.

Настройка СрЗИ должна быть произведена для соответствующего уровня защищённости персональных данных и в соответствии с матрицей доступа пользователей к защищаемым ресурсам.

Результаты работ по установке и настройке средств защиты информации отражаются в следующих документах:

– акт установки и настройки средств защиты информации.

Установка и настройка программных СЗИ от НСД не должна существенно нарушать рабочий процесс Заказчика. Время прекращения функционирования не должно превышать 1,5 часа для АРМ, 1 час для серверов.

4.3.5. Разработка организационно-распорядительной документации по защите информации.

Разработка внутренних нормативных и организационно-распорядительных документов по защите информации с обеспечением доступа к онлайн-сервису по разработке, корректировке и поддержанию в актуальном состоянии организационной распорядительной документации по защите информации сроком на не менее 12 месяцев, с внесением информации в онлайн-сервис для формирования комплекта организационно-распорядительной документации по защите информации.

Онлайн-сервис должен обеспечивать выполнение следующих функций:

- предоставление возможности прохождения электронного согласования разрабатываемых документов специалистами Заказчика, с возможностью выбора маршрута согласуемого документа – последовательно/параллельно;

- двухфакторная аутентификация пользователей с применением связки логин – пароль, а также электронной подписи;

- защита подключения к сервису с использованием сертифицированного криптопровайдера;

- формирование актуального пакета нормативной распорядительной документации по защите персональных данных, систем согласно законодательству Российской Федерации;

- наличие функционала, позволяющего автоматизировать подготовку внутренних распорядительных документов;

- наличие инструментария для планирования мероприятий по защите информации с уведомлением пользователя о приближении запланированного мероприятия через сервис и на электронную почту;

- ведение в электронном виде (в режиме онлайн) всех журналов, формы которых присутствуют в формируемом пакете документов, с возможностью выгрузки журналов целиком, а также заданного интервала записей;

- ведение версионности (истории изменений) документов, с возможностью восстановления электронного документа из резервной копии;

- хранение подписанных электронной подписью документов;

- уведомление должностного лица, использующего онлайн-сервис, об обновлениях системы, изменениях законодательства, возможных перерывах в работе онлайн-сервиса, в связи с внесением изменений, а также внесение соответствующих изменений в анкеты и шаблоны документов онлайн-сервиса;

- выгрузка документов в форматах \*.doc и \*.pdf;

- выгрузка всего пакета документов в едином файле-архиве.

Исполнителем производится аудит информационных систем персональных данных, вносится необходимая информация в программное обеспечение для автоматизации формирования и актуализации внутренней документации. Исполнитель выгружает пакет организационно-распорядительной документации по защите информации (далее – ОРД) из программного обеспечения для автоматизации формирования и актуализации внутренней документации. В случае необходимости Исполнителем вносятся правки в ОРД с учётом технологии обработки персональных данных Заказчиком. ОРД согласовываются и утверждаются Заказчиком.

Вся организационно-распорядительная документация должна соответствовать единой технологии обработки информации. Организационно-распорядительная документация должна создавать условия для обеспечения защиты информации от угроз несанкционированного доступа, инсайдерских угроз, угроз хищения носителей информации. ОРД должны предусматривать выполнение требований к составу и содержанию организационных мер защиты информационных систем персональных данных.

Вся организационно-распорядительная документация должна соответствовать единой технологии обработки информации. ОРД должна создавать условия для обеспечения защиты информации от угроз несанкционированного доступа, инсайдерских угроз, угроз хищения носителей информации. ОРД должны предусматривать выполнение требований к составу и содержанию организационных мер защиты ИСПДн.

4.3.6. Оценка соответствия (аттестация) системы защиты информации требованиям безопасности информации

Аттестация информационной системы организуется Заказчиком и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации требованиям по защите информации.

Исполнителем разрабатывается программа и методика аттестационных испытаний для ИСПДн (далее – Программа-методика). Программа-методика определяет цели, задачи, методы, условия, объем, порядок и методику проведения оценки соответствия принимаемых мер по обеспечению безопасности информации в ИСПДн на соответствие требованиям законодательства по безопасности информации. Программа-методика согласовывается с Заказчиком.

В соответствии с Программой-методикой Исполнителем выполняется оценка соответствия принимаемых мер по обеспечению безопасности информации требованиям безопасности информации для ИСПДн. По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии информационной системы требованиям по защите информации и аттестат соответствия в случае положительных результатов аттестационных испытаний.

По результатам выполнения работ Исполнителем готовятся и передаются Заказчику следующие документы:

- программа и методика проведения аттестационных испытаний по требованиям безопасности информации ИСПДн;

- протокол аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации;

- заключение по результатам аттестационных испытаний ИСПДн на соответствие требованиям безопасности информации;

- аттестат соответствия требованиям по безопасности информации ИСПДн (при положительном заключении по результатам аттестационных испытаний).

**5. Дополнительные требования.**

5.1. Требования к Исполнителю.

В соответствии с Федеральным законом от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности», постановлением Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» для выполнения работ по защите информации, Исполнителю требуется лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации на следующие работы и услуги:

1) работы и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации: средств и систем информатизации;

2) работы и услуги по проектированию в защищённом исполнении: средств и систем автоматизации;

3) услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации: программных (программно-технических) средств защиты информации.

5.2. Требования к надёжности.

Средства защиты, используемые при построении СЗИ, должны обеспечивать необходимый уровень защиты информации, не снижая при этом надёжности технологий обработки информации (в т.ч. времени выполнения технологических операций) и не оказывая существенного влияния на производительность средств вычислительной техники, входящих в состав ИСПДн.

При отказе одной или нескольких компонент СЗИ должна сохранять возможность функционирования.

5.3. Требования к безопасности.

Все оборудование, входящее в состав СЗИ, должно соответствовать действующим отечественным и международным стандартам в области безопасности.

При эксплуатации, обслуживании и ремонте технических средств СЗИ необходимо соблюдать правила техники безопасности для работ (услуг), связанных с эксплуатацией электрооборудования (до 1000 В).

В ходе оказания услуг Исполнитель обязан обеспечить сохранение целостности и доступности конфиденциальной информации, в том числе персональных данных, доступ к которым получен в ходе оказания услуг, предусмотренных данным техническим заданием.

Оказание услуг, предусмотренных данным техническим заданием, осуществляется только при личном прибытии представителей Исполнителя на объекты информатизации Заказчика и осуществляется под непосредственным контролем назначенных должностных лиц, ответственных за обеспечение безопасности информации. Использование технологий удалённого доступа не допускается.

5.4. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗ ИСПДн.

К эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗИ предъявляются следующие требования:

- СЗИ эксплуатируется круглосуточно за исключением времени технического обслуживания;

- обработка информации обеспечивается в реальном режиме времени;

- питание электроэнергией технических средств защиты информации осуществляется от однофазной сети переменного тока напряжением 220 В и частотой 50 Гц;

- для всех технических и программных средств должна быть предусмотрена техническая поддержка с возможностью её продления.

5.5. Требования к стандартизации и унификации.

Услуга должна проводиться с соблюдением действующих государственных стандартов в соответствии с областью их распространения.

Решения по использованию технических средств и ПО в СЗ ИС должны обеспечивать использование однотипных компонентов в целях снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов и удобства эксплуатации.

Услуга должна обеспечивать совместимость технических средств и ПО СЗ ИС с техническими средствами и программным обеспечением, используемыми в ИСПДн Заказчика.

5.6. Требования по обеспечению конфиденциальности.

В период оказания услуги и после её окончания Исполнитель обязан не разглашать и не использовать конфиденциальную информацию, принадлежащую Заказчику, которая может стать ему известной в ходе оказания услуги. Исполнитель несёт ответственность за соблюдение этого требования в соответствии с законодательством Российской Федерации.

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

1. В случае если Исполнитель не является плательщиком НДС, Заказчик указывает: «НДС не облагается». [↑](#footnote-ref-1)
2. Заказчик вправе дополнительно расшифровать, какие документы будут подтверждать приёмку услуг, сделав на них ссылку в п. 5.9. Контракта. [↑](#footnote-ref-2)
3. Письмо ФАС России от 10.12.2015 №АЦ/70978/15, Письма Минэкономразвития России от 10.03.2016 №ОГ-Д28-3630, от 02.10.2015 №ОГ-Д28-12800, от 21.09.2015 №Д28и-2829. [↑](#footnote-ref-3)
4. Обеспечение гарантийных обязательств устанавливается Заказчиком самостоятельно, в случае установленном в соответствии с частью 4 статьи 33 Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» требований к их предоставлению. [↑](#footnote-ref-4)
5. В случае установления заказчиком ограничения, предусмотренного частью 3 статьи 30 Федерального закона № 44-ФЗ, такой срок не должен превышать пятнадцать дней с момента подписания Сторонами документов, подтверждающих надлежащее исполнение обязательств по Контракту)**.** [↑](#footnote-ref-5)
6. Если законодательством Российской Федерации установлен иной порядок начисления штрафа, чем порядок, предусмотренный Правилами, размер такого штрафа и порядок его начисления устанавливается контрактом в соответствии с законодательством Российской Федерации. [↑](#footnote-ref-6)