

Проект

**ГОСУДАРСТВЕННЫЙ КОНТРАКТ № _____
на оказание услуг по аттестации в области информационной безопасности**

Идентификационный код закупки: 202666107731766710100100140017490244

г. Екатеринбург

«____» _____ 2020 г.

Министерство образования и молодежной политики Свердловской области в дальнейшем «Заказчик», в лице Заместителя Министра образования и молодежной политики Свердловской Серковой И.А., действующей на основании Доверенности от 26.06.2019 № 07/21, с одной стороны, и _____, именуемое в дальнейшем «Исполнитель», в лице _____, действующего на основании Устава, с другой стороны, на основании протокола заседания Единой комиссии от _____ заключили настоящий государственный контракт (далее - Контракт) о нижеследующем:

1. ПРЕДМЕТ ГОСУДАРСТВЕННОГО КОНТРАКТА

1.1. В соответствии с условиями контракта Исполнитель оказывает услуги по аттестации в области информационной безопасности, в т. ч. поставляет Заказчику программное обеспечение (далее – Услуги, Программы соответственно) в соответствии со Спецификацией и Техническим заданием (Приложения № 1, 2), являющихся неотъемлемыми частями Контракта, а Заказчик обязуется принять и оплатить оказанные Исполнителем Услуги и возместить расходы в порядке и на условиях Контракта.

1.2. Исполнитель гарантирует наличие своего права на Программы, указанные в пункте 1.1. Контракта на основании: _____.

1.3. Срок выполнения работ (оказания Услуг): не позднее чем 90 (Девяносто) рабочих дней с даты заключения Контракта. Срок действия лицензий на Программы составляет не менее _____ год(а) с даты подписания Сторонами акта приемки оказанных услуг.

1.4. Место оказания Услуг: в соответствии с Техническим заданием (приложение № 2).

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Обязанности Заказчика:

2.1.1. Осуществлять своевременную оплату выполненных работ (оказанных Услуг).

2.1.2. Производить приемку оказанных Услуг и его оплату в порядке, предусмотренном Контрактом.

2.1.3. Обеспечить беспрепятственный вход здания расположения Заказчика специалистов (представителей) Исполнителя.

2.2. Права Заказчика:

2.2.1. В любое время осуществлять контроль и надзор за ходом, качеством и сроком исполнения Контракта, не вмешиваясь при этом в оперативно-хозяйственную деятельность Исполнителя.

2.2.2. Требовать от Исполнителя надлежащего выполнения обязательств в соответствии с условиями Контракта, а также требовать своевременного устранения выявленных недостатков.

2.3. Обязанности Исполнителя:

2.3.1. Исполнитель обязан оказать Услуги полном объеме и перечне, указанном в Спецификации (Приложение № 1) и в соответствии с техническим заданием (Приложение № 2), а также в соответствии с действующими нормами и правилами Российской Федерации, установленными для данных видов услуг.

2.3.2. Исполнитель обязан оказать услуги в срок, указанный в п. 1.3. Контракта.

2.3.3. Представить Заказчику гарантийный срок на Программы сроком на 1 год после даты подписания Сторонами акта оказанных услуг.

3. ПОРЯДОК И СРОКИ ОСУЩЕСТВЛЕНИЯ ПРИЕМКИ УСЛУГ

3.1. Сдача-приемка оказанных Услуг осуществляется Заказчиком в месте оказания услуг и включает в себя: контроль, проверку соответствия оказанных Услуг перечню услуг, установленных Спецификацией (Приложение 1) и Техническим заданием (Приложение 2).

3.2. Исполнитель в день завершения оказания услуг в полном объеме передает Заказчику Акт оказанных услуг (в 2-х экземплярах), подписанных Исполнителем, содержащий сведения об оказанных услугах, а также лицензии на право пользования Программами и соответствующие ключи активации на Программы.

3.3. В срок не более чем 2 (Двух) рабочих дней с момента получения 2-х экземпляров актов оказанных услуг Заказчик подписывает Акт оказанных услуг и направляет его Исполнителю.

3.4. В случаях необходимости для проверки соответствия и качества оказанных Услуг требованиям Контракта Заказчик может проводить экспертизу. Экспертиза Товара может проводиться Заказчиком своими силами, а в определенных законодательством случаях к проведению экспертизы обязательно привлекаются эксперты, экспертные организации на основании контрактов, заключенных 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» (далее - Закон о контрактной системе).

3.5. Для проведения экспертизы оказанных услуг эксперты, экспертные организации имеют право запрашивать у Сторон дополнительные материалы, сведения, документы, относящиеся к условиям исполнения Контракта. Результаты такой экспертизы оформляются в виде заключения.

В случае, если по результатам такой экспертизы установлены нарушения требований Контракта, не препятствующие приемке оказанных Услуг, в заключении могут содержаться предложения об устранении данных нарушений, в том числе с указанием срока их устранения.

3.6. При обнаружении несоответствия качества (объема) оказанных Услуг требованиям Контракта, а также при отрицательном экспертном заключении (при необходимости) Заказчик в срок, не превышающий 2 (Двух) рабочих дней направляет Исполнителю в письменной форме мотивированный Отказ от подписания Акта оказанных Услуг и приемосдаточных документов (при наличии).

3.7. При принятии Заказчиком решения о подписании акта оказанных Услуг или об отказе в его подписании, учитываются предложения экспертов, экспертных организаций, отраженные в заключении по результатам указанной экспертизы (при необходимости).

3.8. Исполнитель в течение 2 (Двух) рабочих дней с момента получения Отказа, указанного в п. 3.6. Контракта, проверяет обоснованность отказа от приёмки и письменно информирует Заказчика о принятом решении.

3.9. Исполнитель обязан в срок не более 2 (Двух) рабочих дней с даты истечения срока, указанного в п. 3.8. Контракта устранить недостатки.

3.10. Устранение недостатков производится за счёт Исполнителя, включая оплату всех расходов, связанных с этим.

3.11. Отказ Заказчика от принятия оказанных Услуг, не соответствующих Контракту и Техническому заданию, не освобождает Исполнителя от выполнения обязательств по Контракту.

3.12. По итогам приемки Услуг при отсутствии претензий Заказчика относительно качества услуг, на основании представленного Исполнителем надлежащим образом оформленных приемосдаточных документов, с учетом положительного экспертного заключения (при необходимости) Заказчик подписывает документы, указанные в настоящем пункте Контракта.

3.13. Обязательства Исполнителя по Контракту считаются исполненными с момента подписания Заказчиком акта оказанных услуг.

4. СТОИМОСТЬ КОНТРАКТА, ПОРЯДОК И СРОКИ ЕГО ОПЛАТЫ

4.1. Стоимость Услуги по Контракту составляет _____ (_____). НДС в размере 20% _____ (_____) / НДС не облагается на основании ст. 346.12 Налогового кодекса РФ. Аванс не предусмотрен.

4.2. Цена Контракта является твердой, определяется на весь срок его исполнения, за исключением случаев, за исключением случаев, предусмотренных п. 4.7, 4.8. Контракта.

4.3. Цена контракта включает в себя все расходы Исполнителя, связанные с оказанием услуг по заключаемому контракту по результатам данной закупки, включая стоимость затрат на приобретение материалов, транспортировку их к месту оказания услуг, уплаты налогов (в том числе НДС), сборов и других обязательных платежей.

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

4.5. Источник финансирования: за счёт средств бюджета Свердловской области.

4.6. Оплата по контракту осуществляется в рублях Российской Федерации.

4.7. Цена Контракта может быть изменена по соглашению Сторон, если по предложению Заказчика увеличивается предусмотренный Контрактом объем оказываемых услуг не более чем на 10 (Десять) процентов или уменьшается предусмотренный Контрактом объем оказываемых услуг не более чем на 10 (Десять) процентов. При этом изменение цены контракта осуществляется пропорционально дополнительному количеству объема услуг, исходя из установленной в контракте цены единицы Услуги, но не более чем на 10 (Десять) процентов цены контракта. При уменьшении предусмотренного контрактом объема Услуги Стороны контракта обязаны уменьшить цену контракта, исходя из цены единицы Услуги. Цена единицы дополнительно оказываемых услуг или цены единицы Услуги при уменьшении предусмотренного Контрактом их объема должны определяться как частное от деления первоначальной цены контракта на предусмотренное в контракте количество объема таких Услуг.

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

4.9. Заказчик оплачивает Услуги, оказанные Исполнителем в соответствии с Контрактом, единовременным платежом в течение 15 (Пятнадцати) рабочих дней с даты подписания Сторонами Акта сдачи - приёмки оказанных услуг на основании счёта, выставленного Исполнителем.

4.10. Окончательным документом, подтверждающим исполнение Контракта, является подписанный Сторонами акт приемки оказанных Услуг.

4.11. Доставка Заказчику отчётных (исполнительных) документов по Контракту может осуществляться почтовой связью по указанному в разделе 12 Контракта адресу его местонахождения.

4.12. Сбор и доставка всех необходимых документов, подтверждающих фактическое оказание Услуг по Контракту, возлагается на Исполнителя.

4.13. Датой (днём) оплаты Контракта Стороны считают дату (день) списания денежных средств с лицевого счёта Заказчика.

4.14. В случае возникновения задолженности у какой-либо из Сторон по контракту, данная Сторона обязуется перечислить сумму задолженности другой Стороне в течение 15 (Пятнадцати) дней с даты подписания Сторонами Акта сверки взаимных расчётов.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За каждый факт неисполнения или ненадлежащего исполнения Заказчиком или Исполнителем обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), устанавливается штраф в виде фиксированной суммы, в том числе рассчитываемой в процентах от цены Контракта.

5.2. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, заключенным по результатам определения поставщика (подрядчика, исполнителя) в соответствии с пунктом 1 части 1 статьи 30 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных

и муниципальных нужд» (далее - Федеральный закон), 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.

5.3. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательства, предусмотренного Контрактом, которое не имеет стоимостного выражения, устанавливается штраф в виде фиксированной суммы, определяемой в следующем порядке:

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

5.4. За просрочку выполнения Исполнителем обязательств, предусмотренных Контрактом, Исполнитель обязан уплатить пени. Пеня начисляется за каждый день просрочки исполнения поставщиком Исполнителем обязательства, предусмотренного Контрактом, в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены контракта, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных контрактом и фактически оказанных Исполнителем.

5.5. Общая сумма начисленной неустойки (штрафов, пени) за неисполнение или ненадлежащее выполнение Исполнителем обязательств, предусмотренных контрактом, не может превышать цену Контракта.

5.6. За каждый факт неисполнения Заказчиком обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств, предусмотренных контрактом, размер штрафа устанавливается в виде фиксированной суммы, определяемой в следующем порядке:

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

5.7. Общая сумма начисленной неустойки (штрафов, пени) за ненадлежащее исполнение Заказчиком обязательств, предусмотренных Контрактом, не может превышать цену Контракта.

5.8. Оплата штрафных санкций не освобождает Стороны от выполнения своих обязательств по Контракту в полном объеме.

5.9. Истечение срока действия Контракта не исключает права Заказчика на предъявление и взыскание неустойки к Исполнителю.

5.10. Истечение срока действия Контракта также не освобождает Стороны от ответственности за неисполнение или ненадлежащее исполнение обязательств по Контракту.

5.11. В случае просрочки со стороны Исполнителя исполнения Контракта на срок более чем один месяц, Заказчик имеет право обратиться к Исполнителю с предложением о расторжении Контракта и уплате штрафных санкций, а при несогласии Исполнителя – обратиться в суд с соответствующим иском.

5.12. В случае расторжения Контракта в связи с односторонним отказом Стороны от исполнения Контракта другая Сторона вправе потребовать возмещения только фактически понесенного ущерба, непосредственно обусловленного обстоятельствами, являющимися основанием для принятия решения об одностороннем отказе от исполнения Контракта.

5.13. Исполнитель обязан возместить убытки, причиненные Заказчику в ходе исполнения контракта, в порядке, предусмотренном действующим законодательством.

5.14. Исполнителем несет перед Заказчиком ответственность за последствия неисполнения или ненадлежащего исполнения обязательств соисполнителем в соответствии с правилами п.1 ст. 313 и ст. 403 Гражданского кодекса Российской Федерации.

5.15. В случае просрочки исполнения Исполнителем обязательств, предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом, Заказчик вправе после направления требования об уплате сумм неустойки (штрафа, пени) и получения отказа (или неполучения в установленный срок ответа) Исполнителем об удовлетворении данных требований удержать сумму начисленных неустоек (штрафов, пени) одним из следующих способов:

- из денежных средств, перечисленных Исполнителем в качестве обеспечения исполнения контракта находящихся на счете Заказчика (в случае если обеспечение Контракта представлено Исполнителем в денежной форме);
- из банковской гарантии, путем направления соответствующего требования Гаранту;
- из оплаты по контракту, путем ее уменьшения на сумму начисленной неустойки (штрафа, пени);

- взыскать неустойку (штраф, пени) в порядке, установленном законодательством Российской Федерации (в судебном порядке).

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

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

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

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

5.18. Исполнителем возмещает убытки, понесенные Заказчиком в связи с возвратом целевых бюджетных средств в бюджеты бюджетной системы Российской Федерации по причине несоблюдения условий их предоставления Исполнителем вызванного неисполнением или ненадлежащим исполнением обязательств Исполнителя по Контракту.

5.19. В случае если законодательством Российской Федерации установлен иной порядок начисления штрафа, чем порядок, установленный постановлением Правительства РФ № 1042 от 30.08.2017, размер такого штрафа и порядок его начисления, устанавливается Контрактом в соответствии с законодательством Российской Федерации.

6. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ, ФОРС-МАЖОР

6.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по Контракту, если такое неисполнение явилось следствием непреодолимой силы, возникшей после его заключения. К обстоятельствам непреодолимой силы относятся: землетрясение, наводнение, иные стихийные бедствия, забастовка и другие события, препятствующие полному или частичному исполнению обязательств по Контракту. Факт наличия указанных обстоятельств должен быть подтвержден справками Торгово-промышленной палаты Российской Федерации в течение 3 (Трех) дней с момента наступления таких обстоятельств. Сторона, для которой создались такие обстоятельства, обязана незамедлительно уведомить об этом другую Сторону.

7. СРОК ДЕЙСТВИЯ, ПОРЯДОК ИЗМЕНЕНИЯ И РАСТОРЖЕНИЯ КОНТРАКТА

7.1. Контракт, вступает в силу с момента его заключения и действует до полного исполнения обязательств обеими сторонами, но не позднее 30.01.2020, при этом срок действия лицензий на поставляемые в рамках Контракта Программы составляет ____ (_____) год с даты подписания Сторонами акта приемки оказанных услуг.

7.2. Окончание действия Контракта не освобождает Стороны от надлежащего и полного исполнения обязательств, принятых на себя по условиям Контракта на момент окончания срока его действия.

7.3. Изменение существенных условий Контракта при его исполнении не допускается, за исключением их изменения по соглашению сторон и в случаях, предусмотренных статьей 95 Закона о контрактной системе.

7.3. Все изменения и дополнения к Контракту, если это допускает действующее законодательство, оформляются в письменном виде в форме дополнительного соглашения, скрепленного подписями и печатями Сторон.

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

7.5. О внесении изменений и дополнений к Контракту Стороны уведомляют друг друга не позднее, чем за 5 (Пять) рабочих дней до внесения таких изменений.

7.6. При изменении наименования, местонахождения, банковских и иных реквизитов Стороны обязаны письменно в 7 (Семидневный) срок с момента наступления таких изменений сообщить друг другу о произошедших изменениях. Риск отрицательных последствий, связанных с неисполнением данной обязанности, несет Сторона, не осуществившая соответствующее уведомление.

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

7.8. Заказчик вправе принять решение об одностороннем отказе от исполнения контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств. До принятия такого решения Заказчик вправе провести экспертизу поставленных товаров (выполненной работы, оказанной услуги) с привлечением экспертов, экспертных организаций.

7.9. Заказчик вправе отказаться от исполнения Контракта в одностороннем порядке в случаях, установленных гражданским законодательством.

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

7.11. Заказчик обязан принять решение об одностороннем отказе от исполнения контракта в случае, если в ходе исполнения контракта установлено, что Исполнитель не соответствует установленным извещением об осуществлении закупки и (или) документацией о закупке требованиям к участникам закупки или представил недостоверную информацию о своем соответствии таким требованиям, что позволило ему стать победителем аукциона в электронной форме.

7.12. Решение Заказчика об одностороннем отказе от исполнения контракта не позднее чем в течение 3 (трех) рабочих дней с даты принятия указанного решения размещается в единой информационной системе и направляется Исполнителю по почте заказным письмом с уведомлением о вручении по адресу местонахождения Исполнителя, указанному в контракте, 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 Контракте. При невозможности получения указанных подтверждения либо информации датой такого надлежащего уведомления признается дата по истечении 13 (Тридцати) дней с даты размещения решения Заказчика об одностороннем отказе от исполнения контракта в единой информационной системе.

7.13. Решение Заказчика об одностороннем отказе от исполнения контракта вступает в силу и контракт считается расторгнутым через 10 (Десять) дней с даты надлежащего уведомления Заказчиком Исполнителя об одностороннем отказе от исполнения контракта.

7.14. 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 поставленных товаров, оказанной услуги) с привлечением экспертов, экспертных организаций. Данное правило не применяется в случае повторного нарушения Исполнителем условий контракта, которые в соответствии с гражданским законодательством являются основанием для одностороннего отказа Заказчика от исполнения Контракта.

7.15. Исполнитель вправе принять решение об одностороннем отказе от исполнения контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения отдельных видов обязательств. Решение Исполнителя об одностороннем отказе от исполнения Контракта не позднее чем в течение 3 (Трех) рабочих дней с даты принятия такого решения направляется Заказчику по почте заказным письмом с уведомлением о вручении по адресу Заказчика, указанному в контракте, а также телеграммой, либо по адресу электронной почты, либо с использованием иных средств связи и доставки, обеспечивающих фиксирование такого уведомления и получение Исполнителем 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.

7.16. Решение Исполнителя об одностороннем отказе от исполнения Контракта вступает в силу и Контракт считается расторгнутым через 10 (Десять) дней с даты надлежащего уведомления Исполнителем Заказчика об одностороннем отказе от исполнения Контракта.

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

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

7.18. Расторжение Контракта по соглашению Сторон совершается в письменной форме.

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

7.19. 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.

7.20. Заказчик вправе требовать расторжения контракта у Поставщика (подрядчика, исполнителя) в судебном порядке в следующих случаях, предусмотренных Гражданским кодексом Российской Федерации.

8. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

8.1. Споры, возникшие между Сторонами по Контракту, регулируются путем переговоров. Претензионный порядок обязателен, срок ответа на претензию – не более 10 (Десять) дней.

8.2. Все спорные вопросы и разногласия, которые могут возникнуть между Сторонами Контракта, Стороны обязуются решать путём прямых переговоров, взаимных консультаций и приложат все усилия для их урегулирования.

При невозможности разрешения споров и разногласий путём переговоров спорные вопросы разрешаются в соответствии с действующим законодательством Российской Федерации в Арбитражном суде Свердловской области.

8.3. Взаимоотношения сторон, не урегулированные Контрактом, регулируются действующим законодательством Российской Федерации.

9. ОБЕСПЕЧЕНИЕ ИСПОЛНЕНИЯ КОНТРАКТА

9.1. В целях заключения Контракта Исполнитель обязан обеспечить исполнение контракта предоставлением банковской гарантии, выданной банком и соответствующей требованиям статьи 45 Закона о контрактной системе, или внесением денежных средств на указанный Заказчиком счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими Заказчику. 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 статьей 95 Закона о контрактной системе.

9.2. Обеспечение исполнения Контракта представляется в размере 10 % от Контракта в размере: _____ (_____) рублей.

9.3. В случае, если Исполнителем предложена цена Контракта, которая на 25 (Двадцать пять) и более процентов ниже начальной (максимальной) цены контракта, Исполнитель предоставляет обеспечение исполнения Контракта в размере, превышающем в полтора раза его размер, указанный в п. 9.2. Контракта в размере _____ (_____) рублей. НДС не облагается.

9.3.1. Участник закупки, с которым заключается Контракт по результатам определения исполнителя в соответствии с пунктом 1 части 1 статьи 30 Закона о контрактной системе, освобождается от предоставления обеспечения исполнения контракта, в том числе с учетом положений статьи 37 Закона о контрактной системе, в случае предоставления таким участником закупки информации, содержащейся в реестре контрактов, заключенных заказчиками, и подтверждающей исполнение таким участником (без учета правопреемства) в течение трех лет до даты подачи заявки на участие в закупке трех контрактов, исполненных без применения к такому участнику неустоек (штрафов, пеней). Такая информация представляется участником закупки до заключения контракта в случаях, установленных настоящим Федеральным законом для предоставления обеспечения исполнения контракта. При этом сумма цен таких контрактов должна составлять не менее начальной (максимальной) цены контракта, указанной в извещении об осуществлении закупки и документации о закупке

9.4. Обеспечение исполнения контракта в виде внесения денежных средств, в том числе части этих денежных средств в случае уменьшения размера обеспечения исполнения контракта в соответствии с частями 7, 7.1 и 7.2 статьи 96 Закона о контрактной системе, возвращается Исполнителю при условии надлежащего исполнения им всех обязательств по контракту в течение 10 (Десяти) дней.

9.4. 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 изменен способ обеспечения исполнения контракта.

9.4.1. В случае, если контрактом предусмотрены отдельные этапы его исполнения и установлено требование обеспечения исполнения контракта, в ходе исполнения данного контракта размер этого обеспечения подлежит уменьшению в порядке и случаях, которые предусмотрены частями 7.2 и 7.3 статьи 96 Закона о контрактной системе.

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

9.5. Обеспечение исполнения контракта обеспечивает все обязательства Исполнителя и распространяется, в том числе, на уплату неустоек в виде штрафа, пени, предусмотренных контрактом, а также убытков, понесенных Государственным заказчиком в связи с неисполнением или ненадлежащим исполнением Исполнителем своих обязательств по Контракту, а также убытков в связи с проведением экспертизы качества оказанных услуг по Контракту, в результате которой будет установлено их ненадлежащее качество.

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

9.7. Реквизиты счета для перечисления денежных средств, в качестве обеспечения исполнения контракта:

Министерство финансов Свердловской области /Министерство образования и молодежной политики Свердловской области

ИНН 6661077317

КПП 667101001

БИК 046577001

Лицевой счет 05012261190

Расчетный счет 40302810965774000004 в Уральском ГУ Банка России

Назначение платежа: «Обеспечение контракта «Оказание услуг по аттестации в области информационной безопасности», Извещение № _____».

9.8. 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. Размер такого обеспечения может быть уменьшен в порядке и случаях, которые предусмотрены частями 7, 7.1, 7.2 и 7.3 статьи 96 Закона о контрактной системе. За каждый день просрочки исполнения Исполнителем данного обязательства начисляется пеня в размере, определенном в порядке, установленном Постановлением Правительства РФ от 30.08.2017 № 1042 «Об утверждении Правил определения размера штрафа, начисляемого в случае ненадлежащего исполнения заказчиком, неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных контрактом (за исключением просрочки исполнения обязательств заказчиком, поставщиком (подрядчиком, исполнителем), и размера пени, начисляемой за каждый день просрочки исполнения поставщиком (подрядчиком, исполнителем) обязательства, предусмотренного контрактом, о внесении изменений в постановление Правительства Российской Федерации от 15 мая 2017 г. № 570 и признании утратившим силу постановления Правительства Российской Федерации от 25 ноября 2013 г. № 1063».

10. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

10.1. Исполнитель гарантирует качество и надежность функционирования программных средств системы в течение гарантийного срока. В течение 12 месяцев после выполнения Услуг Исполнитель предоставляет гарантийное сопровождение в виде консультации технических специалистов Заказчика с использованием всех доступных средств связи (телефон, электронная почта, электронные средства online общения и т.д.). В случае наличия замечаний ФСТЭК России к подготовленному Исполнителем пакету документов по результатам создания СиЗИ, Исполнитель безвозмездно устраняет указанные замечания при условии отсутствия изменений в составе СиЗИ на АП РИС ЕГЭ Заказчика. Время Услуги линии технической поддержки Исполнителя – с 9:00 до 17:00 местного времени в рабочие дни.

10.2. Гарантийный срок на Программы составляет _____ год, который исчисляется с даты подписания Сторонами акта приемки оказанных услуг.

10.3. Если в период гарантийного срока обнаружатся недостатки или дефекты (скрытые недостатки и/или дефекты), то Исполнитель (в случае если не докажет отсутствие своей вины) обязан устранить их за свой счет и в сроки, согласованные Сторонами и зафиксированные в акте с перечнем выявленных недостатков и сроком их устранения. Гарантийный срок в этом случае соответственно продлевается на период устранения недостатков/дефектов.

11. АНТИКОРРУПЦИОННАЯ ОГОВОРКА

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

11.2. В случае возникновения у Стороны добросовестных и обоснованных подозрений, что

произошло или может произойти нарушение каких-либо положений настоящего раздела контракта, соответствующая Сторона обязуется уведомить другую Сторону в письменной форме не позднее 5 рабочих дней с момента возникновения указанных подозрений. В письменном уведомлении указываются лица, причастные к нарушению условий контракта, фактические обстоятельства дела и предоставляются материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение настоящего раздела контракта. Каналы уведомления Заказчика о нарушениях каких-либо положений настоящего раздела по эл почте: info.minobraz@egov66.ru

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

11.3. Стороны гарантируют осуществление надлежащего разбирательства по фактам нарушения положений настоящего раздела контракта с соблюдением принципов конфиденциальности и применение эффективных мер по предотвращению возможных конфликтных ситуаций. Стороны гарантируют отсутствие негативных последствий как для уведомившей Стороны в целом, так и для конкретных работников уведомившей Стороны, сообщивших о факте нарушений условий настоящего раздела контракта.

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

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

12. ПРОЧИЕ УСЛОВИЯ

12.1. Официальный документооборот в рамках Контракта осуществляется путём обмена подлинниками документов со ссылкой на его номер. Для оперативного решения вопросов допускается обмен документами посредством факсимильной связи, а также электронной почты, с обязательной досылкой (передачей) подлинного документа в течение 3 (Трёх) рабочих дней.

12.2. Все уведомления и сообщения должны направляться в письменной форме. Уведомления и сообщения будут считаться исполненными надлежащим образом, если они посланы заказным письмом, по телеграфу, телефаксу (для Заказчика по номеру (343) 3120004, E-mail: info@minobraz.ru, Ответственного исполнителя Заказчика (Леман Юрий Станиславович): по номеру (343) 371-3120004 (доб. 037), Email: – yu.leman@egov66.ru (соответственно) или доставлены лично по юридическим (почтовым) адресам сторон с получением под расписку соответствующим должностным лицом. Почтовый адрес указан в разделе 13 Контракта.

12.2. В случаях, когда документ отправляется почтой либо на электронный адрес, обязанность Стороны Контракта по обеспечению доставки документа считается выполненной в момент передачи почтовой корреспонденции в соответствующее почтовое отделение связи, и, соответственно, отправки документа на указанный Стороной электронный адрес, без уведомления о его получении.

12.3. Стороны гарантируют сохранение в тайне документации, информации, других сведений, полученных ими друг от друга в рамках Контракта и имеющих конфиденциальное содержание (служебная и коммерческая тайна, персональные данные и т.п.). Сторона, допустившая разглашение конфиденциальной информации, обязуется возместить все убытки, причиненные таким разглашением другой стороне, в полном объеме. Доказательство нарушения положений настоящей статьи возлагается на сторону, заявляющую о таком нарушении.

12.3. По всем вопросам, не урегулированным Контрактом, Стороны руководствуются законодательством Российской Федерации.

12.4. Контракт составлен в форме электронного документа, подписанного усиленными электронными подписями Сторон, а также, может быть составлен в 2 (Двух) экземплярах на бумажном носителе, один из которых передается Исполнителю, а второй находится у Заказчика.

12.5. Приложения:

Приложение № 1 «Спецификация»
Приложение № 2 «Техническое задание»

13. ЮРИДИЧЕСКИЕ АДРЕСА И РЕКВИЗИТЫ СТОРОН

ЗАКАЗЧИК:

Министерство образования и молодежной
политики Свердловской области
Юридический/почтовый адрес: 620075,
г. Екатеринбург, ул. Малышева, 33
ИНН 6661077317 /КПП 667101001
Получатель: УФК по Свердловской области
(Министерство финансов Свердловской
области, Министерство образования и
молодежной политики Свердловской области)
л/с 02622009880
р/счет № 40201810400000100001, лицевой счет
№ 03012261190
БИК 046577001 Уральское ГУ БАНКА
РОССИИ г. ЕКАТЕРИНБУРГ
ОКТМО 65701000
Тел. (343) 312-00-04
Ответственное лицо: Леман Ю.С.
тел. +7 (343) 3120004 (доб. 037)

ИСПОЛНИТЕЛЬ:

_____ / **И.А. Серкова**
М.п.

_____ / _____ /

СПЕЦИФИКАЦИЯ

на оказание услуг по аттестации в области информационной безопасности

№ п/п	Наименование	Объем поставки		Цена за ед.	Сумма (руб.)
		Единица измерения	Кол-во		
1	2	3	4	5	6
1.	Оказание услуг по аттестации в области информационной безопасности, в т.ч.:	услуга	1		
1.1.	Сертифицированный дистрибутив «Средство антивирусной защиты»	Шт.	1		
1.2.	Право на использование «Средство анализа защищенности»	Шт.	1		
1.3.	Сертифицированный дистрибутив «Средство анализа защищенности»	Шт.	1		
1.4.	Сертифицированный дистрибутив «Система защиты информации от несанкционированного доступа с модулем межсетевоего экрана»	Шт.	1		
1.5.	Право на использование «Система защиты информации от несанкционированного доступа»	Шт.	1		
1.6.	Право на использование модуля межсетевоего экрана «Системы защиты информации от несанкционированного доступа»	Шт.	1		
2.	Установка и настройка средств защиты информации	услуга	1		
3	Разработка документации: - организационно-распорядительные документы на объект информатизации; - проектные документы на объект информатизации: модель угроз безопасности информации, акт классификации, технический проект, технический паспорт на объект информатизации и проч.	услуга	1		
4	Проведение аттестационных испытаний информационной системы. Выдача аттестата соответствия	услуга	1		
				Итого	

Всего на сумму: _____ рублей (_____) рублей. НДС в размере 20 % _____ (_____) / НДС не облагается на основании ст. 346.12 Налогового кодекса РФ.

ПОДПИСИ СТОРОН:

Государственный заказчик:

Исполнитель:

_____/И.А. Серкова

_____/_____

М.п.

М.п.

Техническое задание на оказание услуг по аттестации в области информационной безопасности

1. В настоящем Техническом задании приведены описание, назначение и цели проведения Услуг по приведению в соответствие требованиям законодательства в области защиты информации ограниченного доступа, обрабатываемой на абонентском пункте региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования Министерства образования и молодежной политики Свердловской области.

Документ разработан в соответствии с ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы», ГОСТ 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении», Требованиями к защите персональных данных при их обработке в информационных системах персональных данных,¹ Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах².

2. Общие сведения

3. Наименование Услуг: оказание услуг по созданию системы защиты информации и проведению комплекса организационных и технических мероприятий (аттестационных испытаний) информационных систем на соответствие требованиям защиты информации абонентского пункта региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования Министерства образования и молодежной политики Свердловской области (далее - Услуги).

4. Заказчик: Министерство образования и молодежной политики Свердловской области

5. Юридический адрес: 620075, г. Екатеринбург, ул. Малышева, 33.

6. Требования к Исполнителю

Исполнитель должен иметь: лицензию ФСТЭК России на право осуществления деятельности по технической защите конфиденциальной информации, предусматривающую:

- услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- Услуги и услуги по аттестационным испытаниям и аттестации на соответствие требованиям по защите информации: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
- Услуги и услуги по проектированию в защищенном исполнении: средств и систем информатизации; помещений со средствами (системами) информатизации, подлежащими защите; защищаемых помещений;
- услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (технических средств защиты информации, защищенных технических средств обработки информации, технических средств контроля эффективности мер защиты информации, программных (программно-технических) средств защиты информации, защищенных программных (программно-технических) средств обработки информации, программных (программно-технических) средств контроля эффективности защиты информации).

¹ утверждено Постановлением Правительства РФ от 01.11.2012 № 1119

² утверждено приказом ФСТЭК России от 11.02.2013 № 17

7. Основания для проведения Услуг

Услуги должны осуществляться на основании и в соответствии с нормативными документами Российской Федерации в области обеспечения безопасности информации и персональных данных:

- Федеральный закон от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006г. № 152-ФЗ «О персональных данных»;
- постановление Правительства Российской Федерации от 01 ноября 2012г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказ ФСТЭК от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- приказ ФСБ России от 10 июля 2014г. № 378 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их работе 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 защищенности»;
- «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России (№ 149/7/2/6-432 от 31 марта 2015г.);
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная ФСТЭК России 15 февраля 2008г.;
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная ФСТЭК России 14 февраля 2008г.;
- ГОСТ РО 0043-003-2012 Защита информации. Аттестация объектов информатизации. Общие положения;
- ГОСТ РО 0043-004-2013 Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний;
- иные нормативно-правовые, организационно-распорядительные и нормативно-технические документы Российской Федерации в области обеспечения безопасности персональных данных.

8. Плановые сроки начала и окончания Услуг

Срок оказания Услуг: 90 (Девяносто) рабочих дней с даты заключения Государственного контракта.

9. Сведения об источниках и порядке финансирования Услуг

Источники финансирования Услуг – Бюджет Свердловской области.

10. Порядок оформления и предъявления Заказчику результатов Услуг

Разработка итоговой документации должна вестись в соответствии с ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем».

Передача документации для согласования, через открытые каналы связи без шифрования – запрещена.

Шифрование должно выполняться с помощью, предоставленного Исполнителем, веб-сервиса, который позволяет выполнять на компьютере пользователя следующие операции с электронными документами:

- зашифровать и расшифровать документ;
- шифрование и расшифрование отдельных файлов и архивов данных;
- шифрование без ограничения размера шифруемых данных;
- просмотр списка ключевых контейнеров;
- сохранение и отправка из сервиса по электронной почте пакета документов одним архивом, содержащим зашифрованный документ и инструкцию по расшифрованию документа;
- поддержка криптопровайдеров (CSP) «КриптоПро CSP», «ViPNet CSP»;
- поддержка ключевых носителей Rutoken и eToken, eSmart, JaCarta.

Веб-сервис должен корректно функционировать на операционных Windows с установленным криптопровайдером (CSP).

Результаты оказания Услуг передаются комплектом документов, который должен быть передан на бумажном носителе и в электронном виде (форматы *.docx, *.pdf, *.vsd) Заказчику. Установочные комплекты и лицензии, поставляемых средств защиты информации должны быть переданы вместе с комплектом документов.

11. Назначение и цели проведения Услуг

11.1. Назначение проведения Услуг

Задачей создания системы защиты информации (далее – СИЗИ) и проведения комплекса организационных и технических мероприятий (аттестационных испытаний) абонентском пункте региональной информационной системы обеспечения проведения государственной итоговой аттестации обучающихся, освоивших основные образовательные программы основного общего и среднего общего образования (далее – АП РИС ЕГЭ) является поддержка высокой доступности технических, программных и информационных ресурсов АП РИС ЕГЭ пользователям АП РИС ЕГЭ в соответствии с предоставленными им правами и полномочиями и проведение оценки соответствия обеспечения защиты информации ограниченного доступа (далее – ИОД), обрабатываемой на АП РИС ЕГЭ от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий.

11.2. Цели проведения Услуг

Основными целями проведения настоящих Услуг являются:

- защита ИОД, обрабатываемой на АП РИС ЕГЭ, от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа за счёт комплексного использования организационных, программных, программно-аппаратных средств и мер защиты;
- защита ИОД, передаваемой по открытым каналам связи, от утечки, искажения и подмены авторства сообщения;
- обнаружение атак и предотвращение инцидентов в области информационной безопасности;
- определение соответствия АП РИС ЕГЭ требованиям положениям и требованиям действующих нормативных правовых актов, методических документов и национальных стандартов в области защиты ИОД.

○

12. Площадки проведения Услуг (место оказания услуг)

Перечень площадок проведения Услуг перечислен в таблице 2.1.

Таблица 2.1

№ п/п	Адрес площадки	Наименование площадки
1	620075, г. Екатеринбург, ул. Малышева, 33	Министерство образования и молодежной политики Свердловской области

13. Общая характеристика объекта защиты

Объектом защиты являются ИОД, обрабатываемая на АП РИС ЕГЭ Заказчика, воздействие на которую, при возникновении инцидентов информационной безопасности, может привести к негативным последствиям.

Обработка защищаемой информации на АП РИС ЕГЭ осуществляется на 1 рабочем месте.

14. Описание информационных систем

Характеристики АП РИС ЕГЭ представлены в таблице 3.1.

Таблица 3.1

Категория обрабатываемых ПДн	Иные категории ПДн
Категория субъектов ПДн	Субъекты, не являющиеся сотрудниками оператора
Объем обрабатываемых ПДн	менее 100 000
Структура ИС	Локальная
Наличие подключения к сетям международного информационного обмена	имеющая одноточечное подключение к сетям связи международного информационного обмена
Режим обУслуги информации	Многопользовательский
Местонахождение технических средств	В пределах РФ
Трансграничная передача информация	Не осуществляется

15. Требования к системе защиты информации

15.1. Требования к системе в целом

СиЗИ Заказчика в целом должна быть совместима с используемыми программными и техническими решениями и соответствовать требованиям руководящих и нормативных документов в области защиты информационных систем.

15.2. Требования к совместимости

Применяемые средства защиты информации (далее – СЗИ) для создания СиЗИ должны быть совместимы с сетевой, канальной инфраструктурой АП РИС ЕГЭ, используемым оборудованием и программным обеспечением и не накладывать ограничений на функционирование АП РИС ЕГЭ.

15.3. Требования по надежности

СЗИ должны иметь возможность осуществления резервирования настроек, резервного копирования файлов конфигураций и восстановления в случаях сбоев.

15.4. Требования по стандартизации, унификации и сертификации

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

Комплексная защита информации и информационных ресурсов должна обеспечиваться с помощью общесистемных и специализированных, программных и аппаратно-программных СЗИ, сертифицированных ФСТЭК России и ФСБ России, включая средства криптографической защиты информации (далее – СКЗИ). Используемые СЗИ должны иметь соответствующие сертификаты ФСТЭК России и/или ФСБ России.

15.5. Требования по патентной чистоте

Программные и аппаратно-программные СЗИ, приобретаемые у сторонних организаций, должны сопровождаться документацией, подтверждающей правомочность этих организаций поставлять данную продукцию.

15.6. Требования к безопасности

Сведения, полученные Исполнителем при выполнении Услуг и не указанные в настоящем техническом задании, являются информацией ограниченного доступа.

Исполнитель Услуг обязуется:

- не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации ограниченного доступа;
- не передавать информацию ограниченного доступа о настоящих Услугах и полученных результатах третьей стороне;
- не осуществлять несанкционированный доступ к информационным ресурсам;
- не проводить незаконное копирование информации, циркулирующей или хранящейся на АП РИС ЕГЭ;
- не предпринимать манипулирование информацией, циркулирующей или хранящейся на АП РИС ЕГЭ (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию);

- не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации;
- не внедрять на АП РИС ЕГЭ программы-вирусы (загрузочные, файловые и др.);
- не устанавливать программные и аппаратные закладные устройства в технические средства АП РИС ЕГЭ;
- не устанавливать в технические средства АП РИС ЕГЭ программное обеспечение, зараженное вирусами;
- не осуществлять передачу материалов Услуг по создаваемой СиЗИ на объекте сторонним организациям, а также публикацию их в открытой печати без разрешения Заказчика.

Нарушение настоящих требований влечет за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

15.7. Перспективы развития, модернизации системы

Проектируемая и создаваемая СиЗИ должна быть масштабируемая и обеспечивать подключение новых участников безопасного информационного обмена без ухудшения функционирования (снижения степени защищённости) АП РИС ЕГЭ.

Должна быть предусмотрена возможность дальнейшего развития АП РИС ЕГЭ в следующих направлениях:

- расширение состава прикладных функций АП РИС ЕГЭ;
- интеграция АП РИС ЕГЭ с другими ИС и ресурсами.

15.8. Требования к эргономике и технической эстетике

Разрабатываемая СиЗИ не должна вносить значительных задержек в Услугу пользователей АП РИС ЕГЭ.

Программные СЗИ должны обладать интуитивно-понятным интерфейсом управления, иметь документацию на русском языке. Регламент работы пользователей в части СЗИ, а также порядок реагирования на события информационной безопасности должны быть описаны в эксплуатационной документации.

15.9. Требования к регламенту обслуживания

Регламентные проверки технических СЗИ должны проводиться в соответствии с требованиями производителя, указанными в эксплуатационной документации к техническим средствам.

15.10. Требования руководящих документов

В СиЗИ должны быть реализованы меры защиты информации, установленные для соответствующего уровня защищенности ПДн, обрабатываемых на АП РИС ЕГЭ, в соответствии с требованиями приказа ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

В СиЗИ должны быть реализованы организационные и технические меры по обеспечению безопасности ПДн необходимые для выполнения установленных приказом ФСБ России от 10 июля 2014г. № 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 защищенности» требований для соответствующего уровня защищенности ПДн, обрабатываемых на АП РИС ЕГЭ.

15.11. Требования к видам обеспечения

16. Требования к программному и техническому обеспечению

Меры по обеспечению безопасности реализуются в том числе посредством применения на АП РИС ЕГЭ СЗИ. Технические характеристики поставляемых СЗИ, приведены в таблице 4.1.

Таблица 4.1

№ п/п	Наименование	Характеристики
1.	Медиа-комплект Kaspersky Стандартный Certified	Требования к поставке: Поставка САВ должна включать в себя:

№ п/п	Наименование	Характеристики
	Media Pack версии 11* (или эквивалент), Лицензия на использование программы не мене 1 года.	<ul style="list-style-type: none"> • фирменную коробку; • CD\DVD-диск в фирменном конверте, на котором записаны дистрибутивы сертифицированных ФСТЭК России продуктов; • заверенные копии сертификатов ФСТЭК России; • формуляр с голографической наклейкой, в котором содержатся эталонные значения контрольных сумм сертифицированных ФСТЭК России продуктов САВ. <p>Требования к сертификации и применению в информационных системах: Средство антивирусной защиты должно иметь сертификат соответствия ФСТЭК России на соответствие требованиям документов «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Б второго класса защиты. ИТ.САВ3.Б2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа В второго класса защиты. ИТ.САВ3.В2.ПЗ» (ФСТЭК России, 2012), «Профиль защиты средств антивирусной защиты типа Г второго класса защиты. ИТ.САВ3.Г2.ПЗ» (ФСТЭК России, 2012)</p>
2.	Средство анализа защищенности ПО RedCheck (эли эквивалент), Лицензия на использование программы для localhost не мене 3 лет	<p>Требования к функционалу: Средство анализа защищенности должно обеспечивать:</p> <ul style="list-style-type: none"> • Аудит обновлений системного и прикладного ПО. • Аудит уязвимостей системного и прикладного ПО. • Аудит конфигураций безопасности. • Аудит конфигураций безопасности серверов приложений: <ul style="list-style-type: none"> ○ Apache HTTP Server; ○ Nginix; ○ IIS; ○ .NET Framework; ○ Apache Tomcat; ○ PHP. • Аудит конфигураций безопасности СУБД Microsoft SQL Server. • Инвентаризацию программного и аппаратного обеспечения. <ul style="list-style-type: none"> ○ Аппаратное обеспечение: <ul style="list-style-type: none"> ○ Список CPU; ○ Материнская плата; ○ BIOS; ○ Слоты памяти; ○ Видео контроллеры; ○ Сетевые адаптеры; ○ Физические диски; ○ Логические диски; ○ Приводы чтения лазерных дисков; ○ USB-устройства. ○ Программное обеспечение: <ul style="list-style-type: none"> ○ Операционная система; ○ Службы; ○ Установленное ПО; ○ Переменные среды; ○ Локальные группы; ○ Локальные пользователи; ○ Общие папки. • Контроль целостности заданных файлов (каталогов). • Идентификацию открытых портов и сервисов. • Подбор паролей. • Документирование результатов. • Режимы сканирования и платформы для сканирования. • Поддержка следующих режимов сканирования: <ul style="list-style-type: none"> ○ А агент; ○ AL безагент; ○ RE WinRM; ○ NMAP безагентский режим сканирования с использованием NMAP. <p>Требования к сертификации: Программный комплекс должен иметь сертификат соответствия ФСТЭК России на соответствие требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля</p>

№ п/п	Наименование	Характеристики
		отсутствия не декларированных возможностей» по 4 уровню контроля и технических условий или более высокого уровня.
3.	Система защиты информации от несанкционированного доступа с модулем межсетевого экрана - Dallas Lock 8.0-К Базовый (или эквивалент), Лицензия на использование программы не мене 1 года.	<p>Должно осуществлять:</p> <ul style="list-style-type: none"> • защиту серверов и рабочих станций от НСД; • контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; • разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации; • разграничение доступа пользователей к информации; • контроль утечек информации; • аутентификацию входящих и исходящих сетевых запросов в локальной сети методами, устойчивыми к пассивному и/или активному прослушиванию сети; • фильтрацию сетевых пакетов; • защиту установленных сетевых соединений; • регистрацию событий безопасности и аудит. <p>Требования к функциональности:</p> <ul style="list-style-type: none"> ○ Регистрацию различных пользователей: локальных, доменных, сетевых. Определение количества одновременных сеансов для пользователя. Возможность ограничения количества терминальных сессий на одном компьютере. ○ Идентификацию и проверку подлинности пользователей при входе в операционную систему. Возможность двухфакторной идентификации по паролю и аппаратному идентификатору. Возможность записи авторизационных данных в идентификатор. Возможность определить принадлежность аппаратного идентификатора конкретному пользователю. Поддержку входа в ОС по сертификату смарт-карты, выданному удостоверяющим центром Windows. ○ Возможность автоматического выбора аппаратного идентификатора в окне авторизации при входе в операционную систему. ○ Возможность настройки принудительной двухфакторной аутентификации для учётной записи с правами администратора и/или пользователя. ○ Возможность средствами СЗИ НСД выполнить настройку периода действия учётной записи. ○ Возможность настройки предупреждения пользователя до входа в систему о том, что в информационной системе реализованы меры по обеспечению безопасности информации. ○ Возможность при создании учётной записи выбрать тип учётной записи (внутренний, внешний, системный, приложение, гостевой, временный). ○ Реализацию настроек сложности паролей и механизм генерации пароля, соответствующего настройкам. ○ Должен быть реализован независимый от механизмов ОС механизм разграничения прав доступа к объектам файловой системы, к запуску программ и к печати документов. Разграничения должны касаться доступа к объектам файловой системы (FAT и NTFS), реестру, сети, съёмным носителям информации. Разграничения должны касаться всех пользователей – локальных, сетевых, доменных, терминальных. ○ Должен выполняться контроль аппаратной конфигурации компьютера и следующих подключаемых устройств: <ul style="list-style-type: none"> • Android-устройств; • iOS-устройств; • Bluetooth-устройств; • DVD- и CD-ROM-дисководов; • устройств HID, MTD, PCMCIA, IEEE 1394, Secure Digital; • USB-контроллеров; • беспроводных устройств (Wireless Communication Devices); • биометрических устройств; • дисководов магнитных дисков; • звуковых, видео- и игровых устройств; • инфракрасных устройств (IrDA); • контроллеров магнитных дисков; • ленточных накопителей; • модемов;

№ п/п	Наименование	Характеристики
		<ul style="list-style-type: none"> • переносных устройств; • портов (COM и LPT); • сенсоров; • сетевых адаптеров; • сканеров и цифровых фотоаппаратов; • принтеров; • съемных носителей информации (CD-ROM, FDD, USB-Flash-накопителей). <ul style="list-style-type: none"> ○ Для предотвращения утечки информации с использованием съемных носителей информации СЗИ НСД должна позволять разграничивать доступ, как к отдельным типам носителей, так и к конкретным экземплярам. ○ Должно обеспечиваться преобразование информации: <ul style="list-style-type: none"> • на съемных носителях информации, для создания доверенной среды при Услуге со съемными носителями; • при Услуге с виртуальными дисками (преобразование выполняется незаметно для пользователя); • при создании преобразованных файлов-контейнеров, используемых для хранения информации на внешних носителях или для передачи по различным каналам связи. ○ Должна выполняться блокировка виртуальных дисков с преобразованной информацией при отключении аппаратного идентификатора. ○ Должна быть обеспечена возможность работы с преобразованными файлами-контейнерами на компьютерах, где программное обеспечение СЗИ НСД не установлено. ○ Сохранение теневых копий файлов, записываемых на съемные носители. ○ В соответствии с требованиями к СЗИ НСД должен использоваться дискреционный принцип контроля доступа: <ul style="list-style-type: none"> ○ обеспечивает доступ к защищаемым объектам (дискам, каталогам, файлам) в соответствии со списками пользователей (групп) и их правами доступа (матрица доступа). ○ Возможность ограничивать средствами СЗИ НСД круг доступных сетевых ресурсов (с точностью до отдельных удаленных рабочих станций и отдельных папок общего доступа). ○ Регистрация и учет (аудит) действий пользователей независимыми от ОС средствами (включение ПЭВМ, вход/выход пользователей, доступ к ресурсам, запуск/остановка процессов, администрирование). Должны вестись непрерывные журналы (т. е. новые записи не должны затирать более старые) с возможностью сортировки и архивации записей. ○ Расширенные возможности аудита печати: печать документов с возможностью добавления штампа (произвольного или по ГОСТу), возможность сохранения теневых копий распечатываемых документов, разграничение доступа пользователей к печати и нанесению штампов. ○ Возможность организации замкнутой программной среды (ЗПС) и различные способы ее настройки. ○ Возможность разграничения доступа к буферу обмена. ○ Возможность локального и удаленного администрирования (управление учетными записями, политиками безопасности, правами доступа, аудитом, просмотр журналов). ○ Возможность контроля целостности программно-аппаратной среды (в том числе отдельных веток реестра, каталогов) при загрузке ПЭВМ, по команде администратора и по расписанию. А также контроль целостности файлов при доступе и блокировка входа в ОС при выявлении изменений. Возможность восстановления объекта доступа (файла, ветки реестра) в случае обнаружения нарушения его целостности. ○ Очистку остаточной информации (освобождаемого дискового пространства, зачистку определенных файлов и папок по команде пользователя), а также возможность полной зачистки дисков и разделов. Запрет смены пользователей без перезагрузки. ○ Выполнение регистрации действий по зачистке остаточной информации. ○ Возможность самодиагностики основного функционала СЗИ НСД с возможностью сохранения отчета. ○ Возможность сохранения конфигурации для последующего восстановления СЗИ НСД. ○ Ведение двух копий программных средств защиты информации и

№ п/п	Наименование	Характеристики
		<p>возможность возврата к настройкам по умолчанию.</p> <ul style="list-style-type: none"> ○ Возможность настройки репликации серверов безопасности. ○ Централизованное управление защищенными рабочими станциями при помощи специального модуля. С помощью этого модуля должно осуществляться централизованное управление учетными записями пользователей, политиками, правами пользователей, преобразованными съемными носителями информации. Должна поддерживаться многоуровневая иерархия групп компьютеров и наследование установленных параметров. Также этим модулем должен осуществляться периодический сбор журналов со всех защищенных рабочих станций. Возможность блокировки компьютера, завершения сеанса работы пользователя по команде администратора. ○ Возможность нотификации о наличии обновлений для СЗИ НСД на сервере компании. ○ Возможность сигнализации администратору безопасности о ситуациях несанкционированного доступа на клиентских рабочих станциях: <ul style="list-style-type: none"> • нарушение контроля целостности объекта; • попытка работы после блокировки при нарушении целостности; • попытка входа на клиентскую рабочую станцию с неправильным паролем; • блокировка пользователя после многократного ввода неправильного пароля; • СЗИ НСД на клиенте не отвечает (возможная причина – несанкционированная деактивация системы защиты); • клиент недоступен долгое время (с возможностью задания периода времени); • попытки монтирования и попытка работы с запрещенными для пользователей на клиенте устройствами. ○ Блокировка доступа к файлам по расширению. ○ Возможность настройки всех параметров СЗИ НСД из единой консоли администрирования. ○ Возможность создания отчета по назначенным правам, формирование паспорта программного обеспечения, установленного на ПЭВМ, формирование паспорта аппаратной части ПЭВМ. ○ Возможность построения иерархии управления при помощи специального модуля – менеджера, управляющего несколькими модулями централизованного управления. ○ Возможность использования механизма удаленной установки и обновления СЗИ НСД средствами модуля централизованного управления самой СЗИ или средствами групповых политик Active Directory. ○ Возможность визуализации сети защищаемых компьютеров. ○ Возможность подключения к модулям администрирования пользователя с ограниченными правами (права только на просмотр настроек; только на просмотр журналов аудита; полные права с возможностью делегирования). ○ Возможность выполнять синхронизацию времени между сервером безопасности и клиентами. ○ Интеграцию с SIEM-системами. <p>Реализация СЗИ НСД должна быть полностью программной, но с возможностью подключения аппаратных средств считывания индивидуальных идентификаторов пользователей, включая идентификаторы: USB-Flash-накопители, Touch Memory (iButton), eToken Pro/Java (USB-ключи и смарт-карты), USB-ключи Rutoken, JaCarta ГОСТ/PKI (USB-ключи и смарт-карты), карты HID Proximity.</p> <ul style="list-style-type: none"> ○ Защита сетевого взаимодействия и фильтрации трафика: <ul style="list-style-type: none"> • Должна быть возможность ограничивать сетевые соединения по правилам фильтрации: <ul style="list-style-type: none"> • сетевого трафика • служебных протоколов • входного и выходного сетевого интерфейса • любых значимых полей сетевых пакетов. • на транспортном уровне запросов на установление виртуальных соединений • на прикладном уровне запросов к прикладным сервисам. • регистрируемых событий межсетевого экрана с учетом даты/времени. • Должно быть реализовано разграничение сетевого доступа пользователей

№ п/п	Наименование	Характеристики
		<p>к узлам сети.</p> <ul style="list-style-type: none"> • Должно быть реализовано разграничение доступа к сети для приложений. • Должна быть реализована возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети. • При удаленных запросах на доступ администратора идентификация и аутентификация обеспечивается методами, устойчивыми к пассивному и активному перехвату информации. • Возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации. • Должна быть реализована локальная сигнализация попыток нарушения правил фильтрации. <p>Требования к операционной платформе и аппаратной части:</p> <ul style="list-style-type: none"> • СЗИ НСД должна представлять собой программный комплекс средств защиты информации в операционных системах семейства Windows с возможностью подключения аппаратных идентификаторов. • СЗИ НСД должна быть предназначена для ПЭВМ типа IBM PC под управлением операционных систем Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, Windows 10, Windows Server 2012 R2 в многопользовательском режиме их эксплуатации. • СЗИ НСД должна поддерживать 32- и 64-битные версии операционных систем. <p>СЗИ НСД должна быть предназначена для использования на персональных компьютерах, портативных компьютерах (ноутбуках, планшетах), серверах (в том числе контроллерах домена и терминального доступа), также поддерживать виртуальные среды и технологию Windows To Go.</p> <p>Требования к сертификации:</p> <ul style="list-style-type: none"> • СЗИ НСД должна быть сертифицирована по требованиям документов: Требования к МЭ, Профиль защиты МЭ (В четвертого класса защиты.ИТ.МЭ.В4.П3), Требования к СКН, Профиль защиты СКН (контроля подключения съемных машинных носителей информации четвертого класса защиты.ИТ.СКН.П4.П3), РД СВТ (5).

17. Требования к метрологическому обеспечению

Тестирование (диагностика) СЗИ должно проводиться посредством специальной контрольной аппаратуры, тестовых средств и специализированного программного (аппаратно-программного) обеспечения, обладающего соответствующими сертификатами ФСТЭК России, подтверждающими соответствие используемых программных (аппаратно-программных) средств требованиям, предъявляемым к средствам контроля защищенности информации.

18. Требования к методическому обеспечению

В целях формирования и закрепления организационных мер защиты ИОД, как неотъемлемых мер обеспечения безопасности ИОД, необходимо разработать комплект проектов организационно-распорядительных документов.

Комплект организационно-распорядительных документов определен в таблице 4.2.

Таблица 4.2

№ п/п	Наименование документа
1	Приказ о создании комиссии по защите информации ограниченного доступа, обрабатываемой в информационных системах
2	Перечень персональных данных, обрабатываемых в информационных системах
3	Приказ о защите информации
4	Инструкция ответственного за организацию обработки персональных данных
5	Инструкция ответственного за защиту информации в информационных системах
6	Инструкция администратора информационных систем

№ п/п	Наименование документа
7	Инструкция по эксплуатации информационных системах
8	Порядок обращения со съемными машинными носителями информации ограниченного доступа
9	Приказ об обращении со средствами криптографической защиты информации
10	Приказ о разрешительной системе доступа: Приложение 1: Положение о разрешительной системе доступа; Приложение 2: Матрица доступа субъектов информационной системы
11	Регламент проведения внутреннего контроля соответствия обработки информации ограниченного доступа требованиям к защите информации ограниченного доступа
12	Регламент реагирования на инциденты информационной безопасности
13	Журнал учета съемных машинных носителей информации ограниченного доступа
14	Журнал учета лиц, имеющих доступ к обработке информации ограниченного доступа
15	Журнал учета ознакомления пользователей с правилами работы шифровальных (криптографических) средств
16	Журнал поэкземплярного учета шифровальных (криптографических) средств защиты информации
17	Приказ о допуске к Услуге со средствами криптографической защиты информации
18	Заключение о подготовке и допуске к самостоятельной Услуге со средствами криптографической защиты информации
19	Журнал учета ключей от режимных помещений, карт для доступа в режимные помещения, ключей от хранилищ, личных печатей от хранилищ
20	Положение об обеспечении безопасности информации ограниченного доступа
21	Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания технических средств, выполнения профилактических Услуг, установки и модификации аппаратных и программных средств обработки информации
22	Приказ о проведении испытаний системы защиты информации
23	Акт определения класса защищенности информационных системах
24	Акт определения уровня защищенности персональных данных при их обработки в информационных системах
25	Правила доступа в помещения

19. Требования к предоставляемым материалам (документам)

Разработка документации должна вестись в соответствии с ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначения документов при создании автоматизированных систем».

Подготавливаемая в рамках оказания услуг документация должна соответствовать требованиям следующих профильных стандартов на разработка технической документации АП РИС ЕГЭ:

- ГОСТ 19.301-79 «Единая система программной документации. Программа и методика испытаний. Требования к содержанию и оформлению»;
- ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»;
- ГОСТ 34.003-90 «Автоматизированные системы. Термины и определения»;
- ГОСТ 34.602-89 «Техническое задание на создание автоматизированной системы»;
- ГОСТ 34.201-89 «Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем»;
- ГОСТ 2.105-95 «Единая система конструкторской документации. Общие требования к текстовым документам»;
- ГОСТ 2.106-96 «Единая система конструкторской документации. Текстовые документы».

20. Состав и содержание Услуги по созданию системы защиты информации

Состав и содержание Услуг по этапам внедрения СиЗИ и проведения аттестационных испытаний, определены в таблице 5.1.

Таблица 5.1

№ п/п	Наименование Услуг	Отчетный документ
1.	Поставка СЗИ, указанных в таблице 4.1 настоящего Технического задания	Акт сдачи-приемки СЗИ
2.	Установка и настройка СЗИ	Акт установки и настройки СЗИ
3.	Разработка организационно-распорядительной документации по защите информации	Комплект организационно-распорядительных документов определен в таблице 4.2 настоящего Технического задания
4.	Разработка «Модели угроз» и технической документации на информационную систему	Описание информационной системы; Модель угроз безопасности информации; Частная модель угроз безопасности персональных данных, обрабатываемых в информационной системе и защищаемых с использованием сертифицированных средств криптографической защиты информации Техническое задание на создание системы защиты информации; Технический проект на создание системы защиты информации; Технический паспорт информационной системы
5.	Проведение аттестационных испытаний информационной системы. Выдача аттестата соответствия	Программа и методики аттестационных испытаний; Протокол проведения аттестационных испытаний; Заключение по результатам аттестационных испытаний; Аттестат соответствия (в случае успешного прохождения аттестационных испытаний)

21. Порядок проведения аттестационных испытаний

Аттестация АП РИС ЕГЭ должна быть проведена Исполнителем в соответствии с ГОСТ РО 0043–003–2012, ГОСТ РО 0043–004–2013 и включать проведение комплекса организационных и технических мероприятий (аттестационных испытаний) по требованиям безопасности информации путем:

- проведения анализа и оценки исходных данных об аттестуемом объекте информатизации (полное и точное наименование объекта информатизации и его назначение, сведения об организационно-режимных мерах защиты, принятых на объекте информатизации, перечень сертифицированной продукции, используемой в целях защиты информации, наличие и характер взаимодействия с другими объектами информатизации), анализа организационной структуры объекта информатизации (проверку условий размещения, монтажа и эксплуатации технических средств, изучение технологического процесса обработки, передачи и хранения информации, анализ информационных потоков, определение состава использованных для обработки, передачи и хранения информации технических средств);
- проведения комплексных испытаний АП РИС ЕГЭ в соответствии с разработанной программой и методиками аттестационных испытаний;
- оформления отчетной документации – протоколов аттестационных испытаний АП РИС ЕГЭ, заключений по результатам аттестационных испытаний на соответствие АП РИС ЕГЭ требованиям безопасности информации.

При наличии положительного заключения по результатам аттестационных испытаний Исполнитель должен оформить аттестат соответствия требованиям по безопасности информации на АП РИС ЕГЭ.

22. Порядок оказания услуг

Перед проведением Услуг Исполнителем должны быть определены условия соблюдения конфиденциальности при выполнении Услуг.

Все Услуги необходимо проводить в согласованное со специалистами Заказчика время, не нарушая основную рабочую деятельность.

Исполнитель обязуется оказать Услуги своими силами и средствами, с помощью своего оборудования и материалов. Исполнитель может привлекать соисполнителей только по согласованию с Заказчиком.

23. Требования к сопровождению

Исполнитель должен гарантировать качество и надежность функционирования программных средств системы в течение гарантийного срока.

В течение 12 месяцев после выполнения Услуг Исполнитель предоставляет гарантийное сопровождение в виде консультации технических специалистов Заказчика с использованием всех доступных средств связи (телефон, электронная почта, электронные средства online общения и т.д.). В случае наличия замечаний ФСТЭК России к подготовленному Исполнителем пакету документов по результатам создания СиЗИ, Исполнитель безвозмездно устраняет указанные замечания при условии отсутствия изменений в составе СиЗИ на АП РИС ЕГЭ Заказчика.

Время Услуги линии технической поддержки Исполнителя – с 9:00 до 17:00 местного времени в рабочие дни.

24. Спецификация поставляемых средств защиты информации и перечня Услуг

№ п/п	Наименование, виды и перечень (содержание и объемы) услуг	Объем поставки	
		Единицы измерения	Количество
1	Поставка средств защиты информации		
1.1.	Сертифицированный дистрибутив «Средство антивирусной защиты»	шт.	1
1.2.	Право на использование «Средство анализа защищенности»	шт.	1
1.3.	Сертифицированный дистрибутив «Средство анализа защищенности»	шт.	1
1.4.	Сертифицированный дистрибутив «Система защиты информации от несанкционированного доступа с модулем межсетевого экрана»	шт.	1
1.5.	Право на использование «Система защиты информации от несанкционированного доступа»	шт.	1
1.6.	Право на использование модуля межсетевого экрана «Системы защиты информации от несанкционированного доступа»	шт.	1
2	Установка и настройка средств защиты информации	Услуга	1
3	Разработка документации: - организационно-распорядительные документы на объект информатизации; - проектные документы на объект информатизации: модель угроз безопасности информации, акт классификации, технический проект, технический паспорт на объект информатизации и проч.	Услуга	1
4	Проведение аттестационных испытаний информационной системы. Выдача аттестата соответствия	Услуга	1

ПОДПИСИ СТОРОН:

Заказчик:

_____/ **И.А. Серкова**
М.п.

Исполнитель:

_____/_____
М.п.