**Проект**

Приложение № 3
к извещению о проведении запроса котировок

**ГОСУДАРСТВЕННЫЙ КОНТРАКТ № _____**
**на оказание услуг по приобретению программного обеспечения и проведение работ по аттестации информационных систем персональных данных и государственной информационной системы**

**Идентификационный код закупки: 18266610773176661010010042001620224 4**

г. Екатеринбург «____» _____ 2018 г.

Министерство общего и профессионального образования Свердловской области, именуемое в дальнейшем «Заказчик», в лице Заместителя Министра общего и профессионального образования Свердловской области Серковой И.А., действующей на основании Доверенности от 29.01.2018 № 07/28, с одной стороны, и _____, именуемое в дальнейшем «Исполнитель», в лице директора _____, действующего на основании Устава, с другой стороны, на основании протокола заседания Единой комиссии Министерства общего и профессионального образования Свердловской области от _____ заключили настоящий государственный контракт (далее - Контракт) о нижеследующем:

## 1. ПРЕДМЕТ ГОСУДАРСТВЕННОГО КОНТРАКТА

1.1. Исполнитель оказывает услуги по приобретению программного обеспечения и проведение работ аттестации информационных систем персональных данных и государственной информационной системы - (далее - Услуги), в соответствии со Спецификацией и Техническим заданием (Приложения № 1, 2), являющихся неотъемлемыми частями Контракта, а Государственный заказчик оплачивает оказанные услуги в порядке, определенном разделом 4 Контракта.

1.2. Срок оказания Услуг: не более чем в течение 30 (Тридцати) дней после даты заключения Государственного контракта.

1.3. Место оказания Услуг: 620075, Свердловская обл., г. Екатеринбург, ул. Малышева, 33.

## 2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1.Обязанности Государственного заказчика:

2.1.1. Осуществлять своевременную оплату оказанных Услуг.

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

2.1.3. Обеспечить беспрепятственный вход в Министерство общего и профессионального образования Свердловской области специалистов (представителей) Исполнителя.

2.2. Права Государственного 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 ассортименте, 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. 1.2. Контракта.

2.3.3. Представить Государственному заказчику гарантийный срок на оказанные Услуги не менее чем на 1 год после даты подписания Государственным заказчиком акта оказанных Услуг.

## 3. ПОРЯДОК И СРОКИ ОСУЩЕСТВЛЕНИЯ ПРИЕМКИ УСЛУГ

3.1. Сдача-приемка оказанных услуг осуществляется Государственным заказчиком в месте оказания услуг и включает в себя: контроль, проверку соответствия оказанных Услуг перечню услуг, установленных Спецификацией и Техническим заданием.

3.2. Исполнитель в день оказания услуг передает Государственному заказчику Акт оказанных услуг в 2-х экземплярах, подписанных Исполнителем, содержащий сведения об оказанных услугах.

3.3. В срок не более чем 5 (Пять) рабочих дней с момента получения 2-х экземпляров актов оказанных услуг Государственный заказчик подписывает Акт оказанных услуг и направляет его Исполнителю.

3.4. В случаях необходимости для проверки соответствия и качества оказанных Услуг требованиям Контракта Государственный заказчик может проводить экспертизу. Экспертиза Товара может проводиться Государственным 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 Товара эксперты, экспертные организации имеют право запрашивать у Государственного заказчика и Исполнителя 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 Услуга, в заключении могут содержаться предложения об устранении данных нарушений, в том числе с указанием срока их устранения.

3.6. При обнаружении несоответствия качества оказанных Услуг требованиям Контракта, а также при отрицательном экспертном заключении (при необходимости) Государственный заказчик в срок, не превышающий 5 (пяти) рабочих дней направляет Исполнителю в письменной форме мотивированный Отказ от подписания Акта оказанных Услуг и приемосдаточных документов (при наличии).

3.7. При принятии Государственным 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 Государственного заказчика о принятом решении.

3.9. Исполнитель обязан в срок не более 5 (Пяти) рабочих дней со дня 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 Государственного 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 Государственного заказчика относительно качества услуг, на основании представленного Исполнителем надлежащим образом оформленных приемо-сдаточных документов, с учетом положительного экспертного заключения (при необходимости) Государственный заказчик подписывает данные документы.

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

## 4. СТОИМОСТЬ КОНТРАКТА, ПОРЯДОК И СРОКИ ЕГО ОПЛАТЫ

4.1. Цена Контракта составляет _____ рублей (_____).

4.2. Цена Контракта является твердой, определяется на весь срок его исполнения, за исключением случаев, установленных Законом о контрактной системе и Контрактом.

4.3. В цену Контракта включены все расходы, связанные с исполнением Исполнителя всех обязательств по Контракту, в том числе на уплату налогов и других обязательных платежей.

4.4. Оплата услуг производится Государственным заказчиком, путем перечисления денежных средств на расчетный счет Исполнителя не позднее чем в течение 15 (Пятнадцати) рабочих дней с

даты подписания Государственным заказчиком акта оказанных услуг. Окончательным документом, подтверждающим исполнение Контракта, является подписанный Сторонами акт оказанных услуг.

4.5. Доставка приемосдаточных документов может осуществляется почтовой связью либо нарочно по указанному в разделе 12 Контракта адресу Государственного заказчика.

4.6. Оплата по Контракту производится Государственным заказчиком в рублях РФ в порядке безналичных перечислений денежных средств на расчетный счет Исполнителя.

4.7. Финансирование Государственного контракта производится за счет средств бюджета Свердловской области.

4.8. Датой оплаты считается дата списания денежных средств со счета Государственного заказчика.

## 5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. За каждый факт неисполнения или ненадлежащего исполнения Государственным 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 как процент цены от Контракта.

5.2. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, устанавливается штраф и устанавливается в виде фиксированной суммы, определяемой в следующем порядке:

а) 3 процента цены контракта (этапа) в случае, если цена контракта (этапа) не превышает 3 млн. 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 исполнения Исполнителем обязательств, предусмотренных Контрактом, Исполнитель обязан уплатить пеню в размере одной трехсотой действующей на дату уплаты пеней ставки рефинансирования Центрального банка Российской Федерации от цены Контракта, уменьшенной на стоимость фактически исполненных Исполнителем обязательств, начисляется за каждый день просрочки исполнения обязательства, начиная со следующего дня после истечения срока исполнения.

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

5.6. За каждый факт неисполнения Государственным 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. За просрочку исполнения Государственным заказчиком обязательств по оплате, предусмотренных Контрактом, Государственный заказчик обязан уплатить пеню. Пеня начисляется за каждый день просрочки исполнения обязательства, предусмотренного государственным контрактом, начиная со дня, следующего после дня истечения срока, установленного пунктом 4.3 Контракта. Размер пени устанавливается в размере одной трехсотой действующей на дату уплаты пеней ставки рефинансирования Центрального банка Российской Федерации от не уплаченной в срок суммы.

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

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

5.10. Истечение срока действия Контракта не исключает права Государственного заказчика на предъявление и взыскание неустойки с Исполнителя.

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

5.12. Оплата штрафных санкций не освобождает Стороны от исполнения своих обязательств по Контракту в полном объеме.

5.13. В случае просрочки со стороны Исполнителя исполнения Контракта на срок более чем один месяц, в том числе по отдельным этапам оказания услуг, Государственный 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.

5.14. 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.

## 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 31.06.2018.

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. 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 Исполнитель 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 7 (Семь) рабочих дней до внесения таких изменений.

7.6. При изменении наименования, местонахождения, банковских и иных реквизитов Стороны обязаны письменно в 7 (семидневной) 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, в случае одностороннего отказа стороны Контракта от исполнения государственного контракта в соответствии с гражданским законодательством РФ, Законом о контрактной системе.

7.8. 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.

## 8. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

8.1. Споры, возникшие между сторонами по Контракту, регулируются путем переговоров. **Претензионный порядок обязателен**, срок ответа на претензию – 20 (Двадцать) дней.

8.2. При не достижении согласия споры передаются на рассмотрение Арбитражного суда Свердловской области.

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

## 9. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

9.1. Исполнитель гарантирует Государственному заказчику качество оказания услуг в соответствии с требованиями, предусмотренными отчетной документацией и Контрактом.

9.2. Гарантийный срок на оказанные услуги с даты подписания акта сдачи-приемки оказанных услуг составляет 1 год.

9.3. 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.

## 10. ОБЕСПЕЧЕНИЕ ИСПОЛНЕНИЯ КОНТРАКТА

10.1. Обеспечение исполнения Контракта не установлено.

## 11. ПРОЧИЕ УСЛОВИЯ

11.1. 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.

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 Государственного заказчика по номеру (343) 371-65-00, для Ответственного исполнителя по номеру 371-37-50), на E-mail Государственного заказчика – info@minobraz.ru, Ответственного исполнителя Государственного заказчика – v.bulatov@egov66.ru (соответственно) или доставлены лично по юридическим (почтовым) адресам сторон с получением под расписку соответствующим должностным лицом. Почтовый адрес указан в разделе 12 Контракта.

11.2. 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.

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

11.4. Контракт составлен в 2 (Двух) экземплярах на бумажном носителе, один из которых передается Исполнителю, а второй находится у Государственного заказчика.

15.5. Приложения:

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

## 12. ЮРИДИЧЕСКИЕ АДРЕСА И РЕКВИЗИТЫ СТОРОН

**ГОСУДАРСТВЕННЫЙ ЗАКАЗЧИК**:
Министерство общего и профессионального образования Свердловской области
Юридический / почтовый адрес: 620075,
г. Екатеринбург, ул. Малышева, д. 33
ИНН 6661077317 / КПП 666101001,
Получатель: УФК по Свердловской области (Министерство финансов СО, Министерство общего и профессионального образования СО)
л/с 02622009880,
р/счет № 40201810400000100001, лицевой счет № 03012261190,
БИК 046577001 Уральское ГУ БАНКА РОССИИ г. ЕКАТЕРИНБУРГ,

**ИСПОЛНИТЕЛЬ:**

ОКТМО 65701000
тел. (343) 371-20-08,

_____ /**И.А. Серкова** _____ / _____
М.п. М.п.

Приложение № 1
к Государственному контракту
от _____ № _____

# СПЕЦИФИКАЦИЯ

по приобретению программного обеспечения и проведение работ аттестации информационных систем персональных данных и государственной информационной системы

| | **Наименование Услуги (ПО), производитель, страна происхождения** | **Ед. измерения** | **Кол-во** | **Цена (руб.)** | **Стоимость (руб.)** |
|---|---|---|---|---|---|
| 1 | Неисключительное право на использование модулей защиты от НСД и контроля устройств средства защиты информации Secret Net Studio 8. ПО-renewal | лицензия | 3 | | |
| 2 | Передача права на использование новой версии ПО ViPNet Client 4.x (КС2) | лицензия | 2 | | |
| 3 | Неисключительное право на использование модуля обнаружения и предотвращения вторжений средства защиты информации Secret Net Studio 8, срок 1 год | лицензия | 3 | | |
| 4 | Неисключительное право на использование модуля персонального межсетевого экрана Средства защиты информации Secret Net Studio 8 | лицензия | 1 | | |
| 5 | Лицензия на обновление СКЗИ «КриптоПро CSP» до версии 4.0 на одном рабочем месте | лицензия | 1 | | |
| 6 | Дистрибутив СКЗИ «КриптоПро CSP» версии 4.0 КС1 и КС2 на CD. Формуляры | шт. | 1 | | |
| 7 | Сертификат технического сопровождения ПО ViPNet Client на 1 год | шт. | 2 | | |
| 8 | Установка и настройка ПО VipNet Client | услуга | | | |
| | Установка и настройка средства защиты информации Secret Net Studio 8 | | | | |
| 9 | Оценка эффективности принимаемых мер по обеспечению безопасности информационной системы | | | | |
| 10 | Внесение изменений в аттестационную документацию по объекту информатизации | | | | |

Всего на сумму: _____ рублей (_____).

**ПОДПИСИ СТОРОН:**

| **Государственный заказчик:** | **Исполнитель:** |
|---|---|
| **_____ /И.А. Серкова** | **_____/_____** |
| М.п. | М.п. |

Приложение № 2
к Государственному контракту
от _____ № _____

**Техническое задание**
**Приобретение программного обеспечения и проведение работ аттестации информационных систем персональных данных и государственной информационной системы**

**1. Общие сведения**

**1.1 Объекты информатизации**

Объектом информатизации являются информационные системы персональных данных и государственной информационной системы Министерства общего и профессионального образования Свердловской области (далее – учреждение).

**1.2. Состав услуг**

Услуги включают:

- поставка программного обеспечения;

- установка и настройка программного обеспечения;

проведение работ аттестации информационных систем персональных данных и государственной информационной системы.

Перечень необходимого программного обеспечения приведен в Приложении № 1.

Технические требования к поставляемому программному обеспечению приведены в Приложении № 2.

Перечень мест установки программного обеспечения приведен в Приложении № 3.

**1.3. Основание оказания услуг**

Основаниями оказания настоящих услуг являются:

- наличие в учреждении: информационных систем, в которых осуществляется обработка информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, и в частности, персональных данных;

- требования законодательства Российской Федерации в области защиты информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

**2. Назначение и цели создания системы защиты объектов информатизации**

**2.1. Назначение системы защиты**

Система защиты объектов информатизации предназначена для обеспечения выполнения требований Федерального закона РФ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»; Федерального закона РФ № 152-ФЗ от 27 июля 2006 г. «О персональных данных».

**2.2. Цели создания системы защиты объектов информатизации**

Основными целями создания системы защиты объектов информатизации являются:

- защита информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, обрабатываемой в информационных системах, от неправомерного или случайного доступа к ней, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения ее, а также от иных неправомерных действий в ее отношении за

счёт комплексного использования организационных, программных, программно-аппаратных средств и мер защиты;

- выполнение требований законодательства по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну.

**2.3. Цели аттестации объекта информатизации**

Целью аттестации объекта информатизации является оценка эффективности реализованных в рамках системы защиты мер по обеспечению безопасности информации в соответствии с национальными стандартами ограниченного распространения.

**3. Общая характеристика объектов информатизации**

В состав объекта информатизации входит 3 автоматизированных рабочих места (далее - АРМ).

**4. Требования к системе защиты объекта информатизации**

**4.1. Требования законодательства в сфере защиты информации**

Для объектов информатизации мероприятиями по защите информации, обрабатываемой на объектах информатизации, будут являться меры, соответствующие выполнению требований:

Федерального закона РФ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации»;

Федерального закона РФ № 152-ФЗ от 27.07.2006 г. «О персональных данных»;

Постановления Правительства РФ от 01.112012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Приказа Федерального агентства правительственной связи и информации при Президенте РФ от 13.06.2001 г. № 152 «Об утверждении инструкции по 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»;

Приказа ФСБ РФ от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

Приказа 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»;

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

Приказа ФСБ России от 10.07.2014 г. № 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».

**4.2. Требования к системе защиты объекта информатизации в целом**

Для реализации мероприятий по обеспечению безопасности информации, обрабатываемой на объектах информатизации, Исполнитель должен создать систему защиты информации, обрабатываемой на объектах информатизации.

**4.2.1. Требования к структуре и функционированию системы защиты объекта информатизации**

**4.2.1.1. Требования к составу**

Для создания системы необходимо построить следующие подсистемы, используя поставляемые Исполнителем программное обеспечение в соответствии с Приложениями № 1, № 2):

- подсистема управления доступом, регистрации, учета и обеспечения целостности;

- подсистема криптографической защиты информации;
- подсистема межсетевого экранирования и защиты каналов связи;
- подсистема обнаружения и предотвращения вторжений;

и др. подсистемы, необходимые для комплексной реализации требований нормативных документов, изложенных в п. 4.1.

**1) Подсистема управления доступом, регистрации, учета и обеспечения целостности**

Описываемая подсистема должна включать в себя средство управления доступом субъектов доступа к объектам доступа. Подсистема должна обеспечить выполнение политики управления доступом, разграничения прав доступа, парольной политики, контроль целостности средств защиты информации на АРМах.

Все АРМ объекта информатизации должны быть оснащены Исполнителем средствами управления доступа пользователей.

**2) Подсистема криптографической защиты информации**

Два АРМа объекта информатизации должны быть оснащены Исполнителем криптографической защитой информации.

Поставляемое программное обеспечение должно быть совместимо с программным обеспечением, используемым работниками на объекте информатизации для исполнения своих функциональных обязанностей.

**3) Подсистема межсетевого экранирования**

Описываемая подсистема должна включать в себя персональный межсетевой экран. Персональный межсетевой экран должен защищать АРМ от сетевых атак и попыток несанкционированного доступа при подключении к сети.

Все АРМ объекта информатизации должны быть оснащены Исполнителем персональным межсетевым экраном.

Поставляемое программное обеспечение должно быть совместимо с программным обеспечением, используемым работниками на объекте информатизации для исполнения своих функциональных обязанностей.

**4) Подсистема обнаружения и предотвращения вторжений**

Описываемая подсистема должна включать в себя систему обнаружения вторжений, обеспечивающую блокировку вредоносных процессов при их попытках воздействия на рабочие процессы АРМ, блокировку сетевых сканеров.

Все АРМ объекта информатизации должны быть оснащены Исполнителем средством обнаружения и предотвращения вторжений.

Поставляемое программное обеспечение должно быть совместимо с программным обеспечением, используемым работниками на объекте информатизации для исполнения своих функциональных обязанностей.

**4.2.1.2. Требования к взаимосвязи между подсистемами и компонентами, смежными подсистемами**

Смежными подсистемами являются:

- локальная вычислительная сеть;
- сеть международного информационного обмена – Интернет.

Решения по подключению смежных подсистем должны соответствовать действующим государственным стандартам в области связи и телекоммуникаций.

**4.2.2. Требования к надёжности**

Элементы системы защиты объектов информатизации должны удовлетворять условиям работы в круглосуточном режиме, а также иметь возможность восстановления в случаях сбоев.

Должна быть предусмотрена техническая поддержка сроком на один год средств криптографической защиты информации. Техническая поддержка должна включать в себя:

- консультации и ответы на вопросы по электронной почте;
- консультации по «горячей» телефонной линии.

**5. Внесение изменений в аттестационную документацию по объекту информатизации**

В результате оказания услуг по аттестации необходимо внести изменения в аттестационную документацию по объекту информатизации. Исполнителем вносятся изменения в следующие документы:

- организационно-распорядительные документы, реализующие организационные мероприятия по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну,
- документ о внесении изменений в технический паспорт информационной системы.

По результатам оказания услуги Исполнителем изготавливаются следующие документы:

- протокол оценки эффективности принимаемых мер по обеспечению безопасности защищаемой информации (персональных данных) в ИС;

**6. Услуги по установке и настройке средств защиты информации**

Исполнителем оказываются услуги по установке и настройке поставляемых средств защиты информации.

Средства защиты информации настраиваются таким образом, чтобы обеспечивать выполнение всех необходимых требований федеральных законов, нормативных документов РФ, ФСТЭК России и ФСБ России к аттестации объектов информатизации.

**7. Обязательные требования к Исполнителю**

Исполнитель должен иметь следующие лицензии:

1) Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации на следующие виды работ:

- контроль защищенности конфиденциальной информации от утечки по техническим каналам;
- контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;
- проектирование в защищенном исполнении: средств и систем информатизации;

аттестационные испытания и аттестация на соответствие требованиям по защите информации;

- установка, монтаж, наладка, испытания, ремонт средств защиты информации.

2) Лицензия ФСБ России на осуществление деятельности по техническому обслуживанию шифровальных (криптографических) средств, либо лицензии ФСБ России на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств на следующие виды работ:

- передача шифровальных (криптографических) средств;
- работы по обслуживанию шифровальных (криптографических) средств, предусмотренные технической и эксплуатационной документацией на эти средства.

**8. Гарантийные обязательства**

Гарантийный срок на оказанные услуги с даты подписания акта сдачи-приемки оказанных услуг составляет 1 год.

**ПОДПИСИ СТОРОН:**

| **Государственный заказчик:** | **Исполнитель:** |
|---|---|
| _____ **/И.А. Серкова** | _____/_____ |
| М.п. | М.п. |

**Приложение № 1**
к техническому заданию

**Количество поставляемых средств защиты информации**

| № п/п | Наименование программного обеспечения и краткие характеристики | Объем поставки | |
|---|---|---|---|
| | | Единица измерения | Кол-во |
| 1 | Неисключительное право на использование модулей защиты от НСД и контроля устройств средства защиты информации Secret Net Studio 8. ПО-renewal<br>Производитель ООО «Код безопасности»<br>Страна происхождения – Россия<br>(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | лицензия | 3 |
| 2 | Передача права на использование новой версии ПО ViPNet Client 4.x (КС2)<br>Производитель ОАО «ИнфоТеКС»<br>Страна происхождения – Россия<br>(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | лицензия | 2 |
| 3 | Неисключительное право на использование модуля обнаружения и предотвращения вторжений средства защиты информации Secret Net Studio 8, срок 1 год<br>Производитель ООО «Код безопасности»<br>Страна происхождения – Россия<br>(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | лицензия | 3 |
| 4 | Неисключительное право на использование модуля персонального межсетевого экрана Средства защиты информации Secret Net Studio 8<br>Производитель ООО «Код безопасности»<br>Страна происхождения – Россия<br>(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | лицензия | 1 |
| 5 | Лицензия на обновление СКЗИ «КриптоПро CSP» до версии 4.0 на одном рабочем месте<br>Производитель ООО «КРИПТО-ПРО»<br>Страна происхождения – Россия<br>(или эквивалент) | лицензия | 1 |
| 6 | Дистрибутив СКЗИ «КриптоПро CSP» версии 4.0 КС1 и КС2 на CD. Формуляры<br>Производитель ООО «КРИПТО-ПРО»<br>Страна происхождения – Россия<br>(или эквивалент) | шт. | 1 |
| 7 | Сертификат технического сопровождения ПО ViPNet Client на 1 год<br>Производитель ОАО «ИнфоТеКС»<br>Страна происхождения – Россия<br>(эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | шт. | 2 |

**ПОДПИСИ СТОРОН:**

**Государственный заказчик:** **Исполнитель:**

_____ **/И.А. Серкова** _____/_____

М.п. М.п.

**Приложение № 2**
к техническому заданию

## Технические требования к поставляемым средствам защиты информации:

| Наименование | Технические требования |
|---|---|
| **Неисключительное право на использование модулей защиты от НСД и контроля устройств средства защиты информации Secret Net Studio 8. ПО-renewal**<br>Производитель ООО «Код безопасности»<br>Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | Обновление программного обеспечения до версии Secret Net Studio 8<br>***Должно осуществлять:***<br>• защиту серверов и рабочих станций от НСД;<br>• контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты;<br>• разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации;<br>• разграничение доступа пользователей к информации;<br>• контроль утечек информации;<br>• регистрацию событий безопасности и аудит.<br>***Требования к сертификации и применению в информационных системах:***<br>СЗИ должно соответствовать требованиям документов: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности, «Требования к средствам контроля съемных машинных носителей информации» (ФСТЭК России, 2014) не ниже 4 класса защиты, «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты» ИТ.СКН.П4.ПЗ (ФСТЭК России, 2014). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля.<br>СЗИ должно допускать использование в следующих информационных системах:<br>• автоматизированные системы - до класса 1Г (включительно);<br>• государственные информационные системы – до 1 класса защищенности (включительно);<br>• информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно);<br>• автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно).<br>СЗИ должно поддерживать защиту систем терминального доступа, а также допускать применение для защиты не только физических компьютеров, но и виртуальных машин.<br>***Требования к операционной платформе и аппаратной части:***<br>• СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы):<br>o Windows 10;<br>o Windows 8/8.1;<br>o Windows 7 SP1;<br>o Windows Vista SP2;<br>o Windows Server 2012/2012 R2;<br>o Windows Server 2008 SP2/2008 R2 SP1.<br>• СЗИ должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix.<br>• СЗИ с централизованным управлением должно функционировать совместно с Microsoft Active Directory;<br>• СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ.<br>• В инфраструктуре должно быть в наличии устройство, считывающее DVD (для чтения установочного диска – хотя бы на одном компьютере в информационной системе).<br>***Требования к функциональности СЗИ:***<br>СЗИ должно выполнять следующие функции по защите информации:<br>• Контроль входа пользователей в систему и работа пользователей в системе:<br>o проверка пароля пользователя при входе в систему;<br>o поддержка персональных идентификаторов (USB-токенов и смарт-карт) для входа в систему и разблокировки компьютера – iButton, eToken Pro (Java), Рутокен S, Рутокен ЭЦП, Рутокен Lite, Jacarta |

| | |
|---|---|
| | PKI, Jacarta Gost, Jacarta PKI Flash, Jacarta Gost Flash, Esmart USB Token, Esmart, Esmart ГОСТ;<br>○ возможность блокировки сеанса работы пользователя при отключении персонального идентификатора;<br>○ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI);<br>○ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI);<br>○ возможность блокирования входа в систему локальных пользователей;<br>○ возможность блокирования операций вторичного входа в систему в процессе работы пользователей;<br>○ возможность блокировки сеанса работы пользователя по истечении интервала неактивности;<br>○ возможность управления политикой сложности паролей;<br>○ поддержка возможности входа в систему по сертификатам;<br>○ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей.<br>• Избирательное (дискреционное) управление доступом:<br>○ возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;<br>○ возможность наследования прав доступа для файлов, каталогов и устройств;<br>○ возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту.<br>• Полномочное (мандатное) управление доступом:<br>○ возможность выбора уровня конфиденциальности сессии для пользователя;<br>○ возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам;<br>○ возможность изменения количества мандатных меток в системе и их названий;<br>○ контроль потоков конфиденциальной информации в системе;<br>○ возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP.<br>• Контроль вывода конфиденциальных данных на печать:<br>○ возможность ограничить перечень мандатных меток информации для печати на заданном принтере;<br>○ теневое копирование информации, выводимой на печать;<br>○ автоматическая маркировка документов, выводимых на печать;<br>○ управление грифами (видом маркировки) при печати конфиденциальных и секретных документов. При этом должна быть возможность задать:<br>▪ отдельный вид грифа для каждой мандатной метки;<br>▪ отдельный вид маркировки для первой страницы документа;<br>▪ отдельный вид маркировки для последней страницы документа;<br>▪ вид маркировки для оборота последнего листа;<br>○ поддержка функции печати в файл;<br>○ поддержка управления запретом перенаправления принтеров в терминальных (RDP) сессиях.<br>• Контроль аппаратной конфигурации компьютера и подключаемых устройств:<br>○ Должны контролироваться следующие устройства:<br>▪ последовательные и параллельные порты;<br>▪ локальные устройства;<br>▪ сменные, физические и оптические диски;<br>▪ программно-реализованные диски;<br>▪ USB-устройства;<br>▪ PCMCIA-устройства;<br>▪ IEEE1394 (FireWire)- устройства;<br>▪ устройства, подключаемые по шине Secure Digital. |

| | |
|---|---|
| | ○ Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства.<br>○ Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной конфигурации.<br>○ Должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться.<br>○ Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации.<br>○ В инфраструктуре виртуальных рабочих станций (VDI) должны контролироваться устройства, подключаемые к виртуальным рабочим станциям с рабочего места пользователя.<br>○ При терминальном подключении (RDP) должна быть возможность управления запретом подключения устройств, COM- и LPT-портов, локальных дисков и PnP-устройств.<br>• Контроль сетевых интерфейсов:<br>○ Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394).<br>○ Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя.<br>• Создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы (EXE-модули), файлы загружаемых библиотек (DLL-модули), запуск скриптов по технологии Active Scripts.<br>○ Список модулей, разрешенных для запуска, должен строиться:<br>▪ с помощью явного указания модулей;<br>▪ по информации об установленных на компьютере программах;<br>▪ по зависимостям исполняемых модулей;<br>▪ по ярлыкам в главном меню;<br>▪ по событиям журнала безопасности.<br>• Контроль целостности файлов, каталогов, элементов системного реестра:<br>○ Должна быть возможность проведения контроля целостности, в процессе загрузки ОС, в фоновом режиме при работе пользователя.<br>○ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов.<br>○ Должна быть возможность восстановления исходного состояния контролируемого объекта.<br>○ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП.<br>○ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ.<br>• Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей.<br>• Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации.<br>• Автоматическое затирание оперативной памяти компьютера с возможностью настройки количества проходов затирания информации.<br>• Затирание информации на локальных и сменных дисках по команде пользователя.<br>• Затирание данных и имен файлов, каталогов при удалении информации.<br>• Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию.<br>• Функциональный контроль ключевых компонентов системы.<br>• Регистрация событий безопасности в журнале.<br>○ Должна быть возможность формирования отчетов по результатам аудита. |

| | |
|---|---|
| | ○ Должна быть возможность поиска и фильтрации при работе с данными аудита.<br>• Получение отчета по параметрам системы защиты.<br>***Требования к централизованному управлению в доменной сети:***<br>СЗИ должно предоставлять следующие возможности по управлению системой:<br>• Отображение структуры доменов, организационных подразделений, серверов безопасности и защищаемых компьютеров.<br>• Динамическое отображение состояния каждого защищаемого компьютера с учетом критичности состояния с точки зрения системы защиты.<br>• Отображение тревог, происходящих на защищаемых компьютерах, возможность задать признак того, что тревога обработана администратором безопасности.<br>• Разделение тревог по уровням критичности события и важности отдельных защищаемых компьютеров.<br>• Выполнение оперативных команд для немедленного реагирования на инциденты безопасности (заблокировать работу пользователя, выключить компьютер).<br>• Выполнение команд, специфичных для защитных подсистем.<br>• Оперативное управление защищаемыми компьютерами, возможность централизованно изменить параметры работы защищаемого компьютера.<br>• Возможность создавать централизованные политики безопасности, распространяемые на разные (заданные) группы защищаемых компьютеров.<br>• Централизованный сбор журналов безопасности с защищаемых компьютеров, их хранение, возможность обработки и архивирования.<br>• Анализ собранных журналов на наличие заданных угроз безопасности с поддержкой редактирования правил детектирования угроз.<br>• Централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу, при этом система должна позволять:<br>○ распространить настройки, заданные для сервера безопасности, на все подчиненные компьютеры (в том числе – по иерархии серверов);<br>○ посмотреть состояние и выполнить команду на любом компьютере, подчиненном серверу безопасности (в том числе – по иерархии серверов).<br>• Создавать домены безопасности в территориально распределенной сети, при этом должна предоставляться возможность делегирования административных полномочий лицам, ответственным за подразделения (домены безопасности).<br>• Создавать отчеты по ресурсам и параметрам защищаемых компьютеров, используемых в системе. |
| **Передача права на использование новой версии ПО ViPNet Client 4.x (КС2)**<br>Производитель ОАО «ИнфоТеКС»<br>Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | Программное обеспечение, реализующее функции криптографического клиента, должно интегрироваться и расширять уже существующую систему защиты каналов связи (ViPNet сеть № 2057), построенную на базе продуктов ViPNet, а также отвечать следующим требованиям:<br>– совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью (ViPNet Administrator), обновления программного обеспечения, обновления справочно-ключевой информации, управление политиками безопасности;<br>– совместимо (полностью) с программно-аппаратным комплексом, реализующим функции шифрование/дешифрование направляемого/принимаемого IP-трафика (ViPNet Coordinator HW1000);<br>– поддержка операционных систем:<br>• Microsoft Windows 2000 Professional;<br>• Microsoft Windows XP Home/Professional;<br>• Microsoft Windows Vista (вся линейка);<br>• Microsoft Windows 7 (вся линейка)<br>– наличие сертификата ФСБ России по классу КС1/КС2;<br>– предоставлять функции контроля запускаемых в операционной системе приложений;<br>– предоставлять функции контентной фильтрации прикладных протоколов http, ftp;<br>– программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном |

| | |
|---|---|
| | обеспечении, реализующем функции управления защищённой сетью;<br>– взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»). |
| **Неисключительное право на использование модуля обнаружения и предотвращения вторжений средства защиты информации Secret Net Studio 8, срок 1 год**<br>Производитель ООО «Код безопасности»<br>Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | ***Должно осуществлять:***<br>• контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты;<br>• обнаружение и предотвращение вторжений;<br>• регистрацию событий безопасности и аудит.<br>***Требования к сертификации и применению в информационных системах:***<br>СЗИ должно соответствовать требованиям документов: «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011)» не ниже 4 класса защиты, «Профиль защиты систем обнаружения вторжений уровня узла четвертого класса защиты» ИТ.СОВ.У4.ПЗ (ФСТЭК России, 2011). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля.<br>СЗИ должно допускать использование в следующих информационных системах:<br>• автоматизированные системы - до класса 1Г (включительно);<br>• государственные информационные системы – до 1 класса защищенности (включительно);<br>• информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно);<br>• автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно).<br>***Требования к функциональности СЗИ:***<br>СЗИ должно выполнять следующие функции по защите информации:<br>• Контроль входа пользователей в систему и работа пользователей в системе:<br>o проверка пароля пользователя при входе в систему;<br>o поддержка персональных идентификаторов (USB-токенов и смарт-карт) для входа в систему и разблокировки компьютера – iButton, eToken Pro (Java), Рутокен S, Рутокен ЭЦП, Рутокен Lite, Jacarta PKI, Jacarta Gost, Jacarta PKI Flash, Jacarta Gost Flash, Esmart USB Token, Esmart, Esmart ГОСТ;<br>o возможность блокировки сеанса работы пользователя при отключении персонального идентификатора;<br>o возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI);<br>o однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI);<br>o возможность блокирования входа в систему локальных пользователей;<br>o возможность блокирования операций вторичного входа в систему в процессе работы пользователей;<br>o возможность блокировки сеанса работы пользователя по истечении интервала неактивности;<br>o возможность управления политикой сложности паролей;<br>o поддержка возможности входа в систему по сертификатам;<br>o возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей.<br>• Контроль целостности файлов, каталогов, элементов системного реестра:<br>o Должна быть возможность проведения контроля целостности в процессе загрузки ОС, в фоновом режиме при работе пользователя.<br>o Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов.<br>o Должна быть возможность восстановления исходного состояния контролируемого объекта.<br>o Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП.<br>o При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров |

| | |
|---|---|
| | операционной системы и СЗИ.<br>• Обнаружение и предотвращение вторжений:<br>o Должна обеспечиваться защита от вторжений с помощью сигнатурных и эвристических механизмов.<br>o Сигнатурные механизмы должны обеспечивать проверку HTTP-трафика на наличие заданных конструкций как для входящего, так и для исходящего сетевого трафика. При обнаружении признаков атаки прохождение подозрительных сетевых пакетов должно быть заблокировано.<br>o Эвристические механизмы должны распознавать и фиксировать следующие типы атак:<br>▪ сканирование портов;<br>▪ подделка ARP (ARP-spoofing);<br>▪ SYN-флуд;<br>▪ атаки, направленные на отказ в обслуживании (DoS);<br>▪ распределенные атаки, направленные на отказ в обслуживании (DDoS).<br>При обнаружении признаков атаки эвристическими методами должен осуществляться временный запрет на прием сетевых пакетов с IP-адреса атакующего компьютера.<br>o Должны обеспечиваться обнаружение и блокировка аномальных сетевых пакетов.<br>• Функциональный контроль ключевых компонентов системы.<br>• Регистрация событий безопасности в журнале.<br>o Должна быть возможность формирования отчетов по результатам аудита.<br>o Должна быть возможность поиска и фильтрации при работе с данными аудита. |
| **Неисключительное право на использование модуля персонального межсетевого экрана Средства защиты информации Secret Net Studio 8**<br>Производитель ООО «Код безопасности»<br>Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | ***Должно осуществлять:***<br>• контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты;<br>• аутентификацию входящих и исходящих сетевых запросов в локальной сети методами, устойчивыми к пассивному и/или активному прослушиванию сети;<br>• фильтрацию сетевых пакетов;<br>• защиту установленных сетевых соединений;<br>• регистрацию событий безопасности и аудит.<br>***Требования к сертификации и применению в информационных системах:***<br>СЗИ должно соответствовать требованиям руководящего документов: «Требования к межсетевым экранам» (ФСТЭК России, 2016) не ниже 4 класса защиты, «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016). Комплект должен соответствовать требованиям документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларируемых возможностей» (Гостехкомиссия России, 1999) – не ниже 4 уровня контроля.<br>СЗИ должно допускать использование в следующих информационных системах:<br>• автоматизированные системы - до класса 1Г (включительно);<br>• государственные информационные системы – до 1 класса защищенности (включительно);<br>• информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно);<br>• автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно).<br>***Требования к функциональности СЗИ:***<br>СЗИ должно выполнять следующие функции по защите информации:<br>• Контроль входа пользователей в систему и работа пользователей в системе:<br>o проверка пароля пользователя при входе в систему;<br>o поддержка персональных идентификаторов (USB-токенов и смарт-карт) для входа в систему и разблокировки компьютера – iButton, eToken Pro (Java), Рутокен S, Рутокен ЭЦП, Рутокен Lite, Jacarta PKI, Jacarta Gost, Jacarta PKI Flash, Jacarta Gost Flash, Esmart USB Token, Esmart, Esmart ГОСТ;<br>o возможность блокировки сеанса работы пользователя при отключении персонального идентификатора;<br>o возможность использования персональных идентификаторов для |

| | |
|---|---|
| | входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI);<br>○ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI);<br>○ возможность блокирования входа в систему локальных пользователей;<br>○ возможность блокирования операций вторичного входа в систему в процессе работы пользователей;<br>○ возможность блокировки сеанса работы пользователя по истечении интервала неактивности;<br>○ возможность управления политикой сложности паролей;<br>○ поддержка возможности входа в систему по сертификатам;<br>○ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей.<br>• Контроль целостности файлов, каталогов, элементов системного реестра:<br>○ Должна быть возможность проведения контроля целостности в процессе загрузки ОС, в фоновом режиме при работе пользователя.<br>○ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов.<br>○ Должна быть возможность восстановления исходного состояния контролируемого объекта.<br>○ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП.<br>○ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ.<br>• Защита сетевого взаимодействия и фильтрация трафика:<br>○ Должны быть механизмы аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.<br>○ Должны удостоверяться субъекты доступа (пользователи и компьютеры) и защищаемые объекты (компьютеры).<br>○ Механизмы должны быть защищены от прослушивания, попыток подбора и перехвата паролей, подмены защищаемых объектов, подмены MAC- и IP-адресов.<br>○ Должны быть предусмотрены механизмы защиты установленных сетевых соединений между субъектами доступа (пользователями и компьютерами) и защищаемыми объектами (серверами и информационными системами) на основе открытых стандартов протоколов семейства IPsec, которые позволяют контролировать аутентичность и целостность передаваемых данных.<br>○ Должна быть предусмотрена настройка режима защиты сетевого взаимодействия, при этом должны быть предусмотрены следующие режимы защиты:<br>▪ соединение без защиты;<br>▪ маркируется каждый пакет;<br>▪ подписывается заголовок каждого пакета;<br>▪ подписывается каждый пакет целиком.<br>○ Должна быть возможность ограничивать сетевые соединения по правилам фильтрации:<br>▪ на уровне отдельных протоколов из стека TCP/IP;<br>▪ на уровне параметров протоколов стека TCP/IP;<br>▪ на уровне параметров служебных протоколов стека TCP/IP;<br>▪ на уровне периодов времени;<br>▪ на уровне пользователей или групп пользователей;<br>▪ на уровне параметров прикладных протоколов;<br>▪ на уровне исполняемого файла/процесса;<br>▪ на уровне сетевого адаптера.<br>○ Должна быть возможность осуществлять фильтрацию команд, параметров и последовательностей команд, а также обеспечивать блокировку мобильного кода.<br>○ Должен быть предусмотрен выбор действий для определения реакции системы на срабатывание правил фильтрации:<br>▪ регистрация информации в журнале; |

| | |
|---|---|
| | ▪ звуковая сигнализация;<br>▪ запуск программы или сценария.<br>• Функциональный контроль ключевых компонентов системы.<br>• Регистрация событий безопасности в журнале.<br>o Должна быть возможность формирования отчетов по результатам аудита.<br>o Должна быть возможность поиска и фильтрации при работе с данными аудита. |
| **Лицензия на обновление СКЗИ «КриптоПро CSP» до версии 4.0 на одном рабочем месте**<br>Производитель ООО «КРИПТО-ПРО»<br>Страна происхождения – Россия (или эквивалент) | **1. Требования к реализации криптографических стандартов**<br>Применяемое средство криптографической защиты информации (средство электронной подписи) должно обеспечивать применение ЭП и шифрования в соответствии с нормами действующего законодательства Российской Федерации и осуществлять выполнение следующих основных функций:<br>• генерацию и управление ключевой информацией;<br>• формирование электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012;<br>• подтверждение подлинности электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001и ГОСТ Р 34.10-2012;<br>• подсчет значения хеш-функции в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012;<br>• шифрование и расшифрование данных в соответствии с ГОСТ 28147-89;<br>• формирование закрытых и открытых ключей электронной подписи и шифрования;<br>• идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений;<br>• реализацию набора протоколов IPsec в соответствии с особенностями использования отечественных криптографических алгоритмов.<br>**2. Требования к сертификации**<br>Средство электронной подписи (средство криптографической защиты информации) должно быть сертифицировано ФСБ России, в качестве:<br>– Средства квалифицированной электронной подписи в соответствии с Требованиями ФСБ России к средствам электронной подписи;<br>– Средства криптографической защиты информации в соответствии с требованиями ФСБ России к шифровальным (криптографическим) средствам защиты конфиденциальной информации.<br>**3. Требования к реализации программного интерфейса встраивания**<br>Средство криптографической защиты информации (средство электронной подписи) должно соответствовать криптографическому интерфейсу компании Microsoft - Cryptographic Service Provider (CSP).<br>Встраивание средства криптографической защиты информации (средства электронной подписи) в прикладную информационную систему должно предусматривать возможность:<br>• Применения в операционных системах семейства Microsoft Windows интерфейса функций CryptoAPI и CAPICOM;<br>• Поддержки стандарта XML DSign при формировании электронной подписи в XML документах;<br>• Непосредственного вызова функций средства криптографической защиты информации (средства электронной подписи);<br>• Применения в стандартном прикладном программном обеспечении операционных систем семейства Microsoft Windows (MS Outlook Express; MS IE; MS IIS; MS Office Word, Excel, Outlook, InfoPath и т.д.) без использования дополнительных программных средств интеграции.<br>**4. Требования к составу**<br>В состав средства криптографической защиты информации (средства электронной подписи) должно входить средство сетевой аутентификации, обеспечивающее реализацию сетевого протокола SSL/TLS с использованием российских криптографических стандартов ЭП, подсчета хеш-функции и шифрования. |

| | |
|---|---|
| | Сертификат соответствия ФСБ России должен распространяться на данное средство сетевой аутентификации, реализующее протокол SSL/TLS и входящее в состав СКЗИ.<br>В состав средства криптографической защиты информации (средства электронной подписи) должно входить библиотеки IKE, ESP, AH, обеспечивающие реализацию набора протоколов IPsec с использованием отечественных криптографических алгоритмов.<br>**5. Функциональные требования**<br>Средство криптографической защиты информации (средство электронной подписи) должно предоставлять программный интерфейс для выполнения следующих основных функций:<br>• формирование и подтверждение подлинности ЭП;<br>• подсчет значения хеш-функции данных;<br>• шифрование и расшифрование данных;<br>• формирование закрытых и открытых ключей подписи и шифрования.<br><br>Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать выполнение следующих сервисных функций:<br>• установка личных сертификатов открытых ключей с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом;<br>• копирование и удаление закрытых ключей;<br>• установка, изменение и удаление пароля на доступ к закрытому ключу.<br>**6. Требования к общесистемному программному обеспечению**<br>Средство криптографической защиты информации (средство электронной подписи) должно включать варианты исполнений, функционирующих в среде следующих операционных систем:<br><u>Windows:</u><br>Включает программно-аппаратные среды:<br>– Windows XP/Vista/7/8/8.1/10/Server 2003/2008 ( x86, x64);<br>**7. Требования к поддерживаемым ключевым носителям**<br>Средство криптографической защиты информации (средство электронной подписи) должно поддерживать следующие носители:<br>• Смарт-карты Оскар, Магистра;<br>• Электронные идентификаторы Touch-Memory DS1995, DS1996;<br>• Электронные идентификаторы Rutoken;<br>• Электронные идентификаторы eToken, Jacarta;<br>• Электронные идентификаторы ESMART Token;<br>• Смарткарты Athena IDProtect, INPASPOT, Cha cardOS, Cha JCOP, MPCOS-Gemalto;<br>• Сменный Flash-носитель;<br>• Жесткий диск ПЭВМ.<br>Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать возможность разработки программных библиотек поддержки произвольных типов перезаписываемых носителей.<br>**8. Требования к поддерживаемым стандартным приложениям и службам операционных систем**<br>Средство криптографической защиты информации (средство электронной подписи) должно поддерживаться следующими стандартными приложениями и службами операционных систем:<br>• Microsoft Certification Authority из состава Windows 2008/2008R2/2012/2012R2;<br>• Электронная почта - MS Outlook из состава Microsoft Office.<br>• Microsoft Word, Excel, Info Path из состава Microsoft Office.<br>• Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode.<br>• Службы терминалов для 2008/2008R2/2012/2012R2 (включая |

| | |
|---|---|
| | шлюз служб терминалов) с обеспечением доступа к Службе по протоколу TLS.<br>• Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer – web-сервер IIS, TLS-сервер, TLS-клиент (IE).<br>• SQL-сервер.<br>• ISA/TMG сервер.<br>• Сервер терминалов и клиент (RDP).<br>Данное средство должно обеспечивать возможность реализации сетевой аутентификации в домене MS Windows (на основе Winlogon) с использованием реализованных данным средством российских криптоалгоритмов<br>Данное средство должно обеспечивать возможность шифрования данных на жестком диске компьютера с использованием реализованных данным средством российских криптоалгоритмов, работающего под операционными системами семейства Windows, посредством расширения стандартного функционала Microsoft Encrypt File System (Microsoft EFS). |
| **Дистрибутив СКЗИ «КриптоПро CSP» версии 4.0 КС1 и КС2 на CD. Формуляры**<br>Производитель ООО «КРИПТО-ПРО»<br>Страна происхождения – Россия (или эквивалент) | Компакт-диск с дистрибутивом программного обеспечения и формуляром. |
| **Сертификат технического сопровождения ПО ViPNet Client на 1 год**<br>Производитель ОАО «ИнфоТеКС»<br>Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением) | ***Сертификат включает в себя:***<br>Оказание технических консультаций сертифицированными специалистами, с привлечением специалистов производителя сертифицированных средств защиты информации (ОАО «ИнфоТеКС»), на которые предоставляются права пользования по вопросам функционирования средств защиты по телефону горячей линии в течение рабочего дня (с 09:00 до 18:00, с понедельника по пятницу) и электронной почте.<br>Поставка сертификата технического сопровождения производителя ОАО «ИнфоТеКС», сроком действия не менее 1 года |

**ПОДПИСИ СТОРОН:**

**Государственный заказчик:** **Исполнитель:**

_____ **/И.А. Серкова** _____/_____

М.п. М.п.

**Приложение № 3**
к техническому заданию

**Перечень конечных пользователей и адреса установки средств защиты информации**

| № п/п | Наименование учреждения | Адрес установки |
|---|---|---|
| 1 | Министерство общего и профессионального образования Свердловской области; 3 (Три) рабочих места | г. Екатеринбург, ул. Малышева, 33 |

**ПОДПИСИ СТОРОН:**

**Государственный заказчик:** **Исполнитель:**

**_____ /И.А. Серкова** _____/_____

М.п. М.п.