Приложение № 2
к извещению о проведении запроса котировок

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.

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 Производитель ООО «Код безопасности» Страна происхождения – Россия (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) Производитель ОАО «ИнфоТеКС» Страна происхождения – Россия (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 Производитель ООО «Код безопасности» Страна происхождения – Россия (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 Производитель ООО «Код безопасности» Страна происхождения – Россия (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 Производитель ООО «КРИПТО-ПРО» Страна происхождения – Россия (или эквивалент)	лицензия	1
6	Дистрибутив СКЗИ «КриптоПро CSP» версии 4.0 КС1 и КС2 на CD. Формуляры Производитель ООО «КРИПТО-ПРО» Страна происхождения – Россия (или эквивалент)	шт.	1
7	Сертификат технического сопровождения ПО ViPNet Client на 1 год Производитель ОАО «ИнфоТеКС» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	шт.	2

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 Производитель ООО «Код безопасности» 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 ***Должно осуществлять:*** • 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; • регистрацию событий безопасности и аудит. ***Требования к сертификации и применению в информационных системах:*** 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. СЗИ должно допускать использование в следующих информационных системах: • автоматизированные системы - до класса 1Г (включительно); • государственные информационные системы – до 1 класса защищенности (включительно); • информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно); • автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно). СЗИ должно поддерживать защиту систем терминального доступа, а также допускать применение для защиты не только физических компьютеров, но и виртуальных машин. ***Требования к операционной платформе и аппаратной части:*** • СЗИ должно функционировать на следующих платформах (должны поддерживаться и 32-, и 64-разрядные платформы): o Windows 10; o Windows 8/8.1; o Windows 7 SP1; o Windows Vista SP2; o Windows Server 2012/2012 R2; o Windows Server 2008 SP2/2008 R2 SP1. • СЗИ должно поддерживать работу и обеспечивать защиту в системах терминального доступа, построенных на базе терминальных служб сетевых ОС MS Windows или ПО Citrix. • СЗИ с централизованным управлением должно функционировать совместно с Microsoft Active Directory; • СЗИ должно обладать возможностью работы на однопроцессорных и многопроцессорных ЭВМ. • В инфраструктуре должно быть в наличии устройство, считывающее DVD (для чтения установочного диска – хотя бы на одном компьютере в информационной системе). ***Требования к функциональности СЗИ:*** СЗИ должно выполнять следующие функции по защите информации: • Контроль входа пользователей в систему и работа пользователей в системе: o проверка пароля пользователя при входе в систему; 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; ○ возможность блокировки сеанса работы пользователя при отключении персонального идентификатора; ○ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI); ○ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI); ○ возможность блокирования входа в систему локальных пользователей; ○ возможность блокирования операций вторичного входа в систему в процессе работы пользователей; ○ возможность блокировки сеанса работы пользователя по истечении интервала неактивности; ○ возможность управления политикой сложности паролей; ○ поддержка возможности входа в систему по сертификатам; ○ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей. • Избирательное (дискреционное) управление доступом: ○ возможность назначения прав доступа на файлы, каталоги, принтеры, устройства; ○ возможность наследования прав доступа для файлов, каталогов и устройств; ○ возможность установки индивидуального аудита доступа для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту. • Полномочное (мандатное) управление доступом: ○ возможность выбора уровня конфиденциальности сессии для пользователя; ○ возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам; ○ возможность изменения количества мандатных меток в системе и их названий; ○ контроль потоков конфиденциальной информации в системе; ○ возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP. • Контроль вывода конфиденциальных данных на печать: ○ возможность ограничить перечень мандатных меток информации для печати на заданном принтере; ○ теневое копирование информации, выводимой на печать; ○ автоматическая маркировка документов, выводимых на печать; ○ управление грифами (видом маркировки) при печати конфиденциальных и секретных документов. При этом должна быть возможность задать: ▪ отдельный вид грифа для каждой мандатной метки; ▪ отдельный вид маркировки для первой страницы документа; ▪ отдельный вид маркировки для последней страницы документа; ▪ вид маркировки для оборота последнего листа; ○ поддержка функции печати в файл; ○ поддержка управления запретом перенаправления принтеров в терминальных (RDP) сессиях. • Контроль аппаратной конфигурации компьютера и подключаемых устройств: ○ Должны контролироваться следующие устройства: ▪ последовательные и параллельные порты; ▪ локальные устройства; ▪ сменные, физические и оптические диски; ▪ программно реализованные диски; ▪ USB-устройства; ▪ PCMCIA-устройства; ▪ IEEE1394 (FireWire)- устройства; ▪ устройства, подключаемые по шине Secure Digital. ○ Должна быть возможность задать настройки контроля на уровне шины, класса устройства, модели устройства, экземпляра устройства. ○ Должен осуществляться контроль неизменности аппаратной конфигурации компьютера с возможностью блокировки при нарушении аппаратной

	конфигурации. ○ Должна быть возможность присвоить устройствам хранения информации мандатную метку. Если метка устройства не соответствует сессии пользователя – работа с устройством хранения должна блокироваться. ○ Должен осуществляться контроль вывода информации на внешние устройства хранения с возможностью теневого копирования отчуждаемой информации. ○ В инфраструктуре виртуальных рабочих станций (VDI) должны контролироваться устройства, подключаемые к виртуальным рабочим станциям с рабочего места пользователя. ○ При терминальном подключении (RDP) должна быть возможность управления запретом подключения устройств, COM- и LPT-портов, локальных дисков и PnP-устройств. • Контроль сетевых интерфейсов: ○ Должна быть возможность включения/выключения явно заданного сетевого интерфейса или интерфейса, определяемого типом – Ethernet, WiFi, IrDA, Bluetooth, FireWire (IEEE1394). ○ Должна быть возможность управления сетевыми интерфейсами в зависимости от уровня сессии пользователя. • 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. ○ Список модулей, разрешенных для запуска, должен строиться: ▪ с помощью явного указания модулей; ▪ по информации об установленных на компьютере программах; ▪ по зависимостям исполняемых модулей; ▪ по ярлыкам в главном меню; ▪ по событиям журнала безопасности. • Контроль целостности файлов, каталогов, элементов системного реестра: ○ Должна быть возможность проведения контроля целостности, в процессе загрузки ОС, в фоновом режиме при работе пользователя. ○ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов. ○ Должна быть возможность восстановления исходного состояния контролируемого объекта. ○ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП. ○ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ. • Изоляция программных модулей и контроль доступа к буферу обмена и операциям перетаскивания (drag-and-drop) для изолированных модулей. • Автоматическое затирание удаляемой информации на локальных и сменных дисках компьютера при удалении пользователем конфиденциальной информации с возможностью настройки количества проходов затирания информации. • Автоматическое затирание оперативной памяти компьютера с возможностью настройки количества проходов затирания информации. • Затирание информации на локальных и сменных дисках по команде пользователя. • Затирание данных и имен файлов, каталогов при удалении информации. • Возможность управления запретом передачи буфера обмена в терминальную (RDP) сессию. • Функциональный контроль ключевых компонентов системы. • Регистрация событий безопасности в журнале. ○ Должна быть возможность формирования отчетов по результатам аудита. ○ Должна быть возможность поиска и фильтрации при работе с данными аудита. • Получение отчета по параметрам системы защиты. ***Требования к централизованному управлению в доменной сети:*** СЗИ должно предоставлять следующие возможности по управлению системой: • Отображение структуры доменов, организационных подразделений,

	серверов безопасности и защищаемых компьютеров. • Динамическое отображение состояния каждого защищаемого компьютера с учетом критичности состояния с точки зрения системы защиты. • Отображение тревог, происходящих на защищаемых компьютерах, возможность задать признак того, что тревога обработана администратором безопасности. • Разделение тревог по уровням критичности события и важности отдельных защищаемых компьютеров. • Выполнение оперативных команд для немедленного реагирования на инциденты безопасности (заблокировать работу пользователя, выключить компьютер). • Выполнение команд, специфичных для защитных подсистем. • Оперативное управление защищаемыми компьютерами, возможность централизованно изменить параметры работы защищаемого компьютера. • Возможность создавать централизованные политики безопасности, распространяемые на разные (заданные) группы защищаемых компьютеров. • Централизованный сбор журналов безопасности с защищаемых компьютеров, их хранение, возможность обработки и архивирования. • Анализ собранных журналов на наличие заданных угроз безопасности с поддержкой редактирования правил детектирования угроз. • Централизованное управление в сложной доменной сети (domain tree) должно функционировать по иерархическому принципу, при этом система должна позволять: ○ распространить настройки, заданные для сервера безопасности, на все подчиненные компьютеры (в том числе – по иерархии серверов); ○ посмотреть состояние и выполнить команду на любом компьютере, подчиненном серверу безопасности (в том числе – по иерархии серверов). • Создавать домены безопасности в территориально распределенной сети, при этом должна предоставляться возможность делегирования административных полномочий лицам, ответственным за подразделения (домены безопасности). • Создавать отчеты по ресурсам и параметрам защищаемых компьютеров, используемых в системе.
Передача права на использование новой версии ПО ViPNet Client 4.x (КС2) Производитель ОАО «ИнфоТеКС» 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: – совместимо (полностью) с программным обеспечением, реализующим функции управления защищённой сетью (ViPNet Administrator), обновления программного обеспечения, обновления справочно-ключевой информации, управление политиками безопасности; – совместимо (полностью) с программно-аппаратным комплексом, реализующим функции шифрование/дешифрование направляемого/принимаемого IP-трафика (ViPNet Coordinator HW1000); – поддержка операционных систем: • Microsoft Windows 2000 Professional; • Microsoft Windows XP Home/Professional; • Microsoft Windows Vista (вся линейка); • Microsoft Windows 7 (вся линейка) – наличие сертификата ФСБ России по классу КС1/КС2; – предоставлять функции контроля запускаемых в операционной системе приложений; – предоставлять функции контентной фильтрации прикладных протоколов http, ftp; – программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью; – взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»).
Неисключительное право на	***Должно осуществлять:***

использование модуля обнаружения и предотвращения вторжений средства защиты информации Secret Net Studio 8, срок 1 год Производитель ООО «Код безопасности» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	• контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; • обнаружение и предотвращение вторжений; • регистрацию событий безопасности и аудит. ***Требования к сертификации и применению в информационных системах:*** 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. СЗИ должно допускать использование в следующих информационных системах: • автоматизированные системы - до класса 1Г (включительно); • государственные информационные системы – до 1 класса защищенности (включительно); • информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно); • автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно). ***Требования к функциональности СЗИ:*** СЗИ должно выполнять следующие функции по защите информации: • Контроль входа пользователей в систему и работа пользователей в системе: ○ проверка пароля пользователя при входе в систему; ○ 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; ○ возможность блокировки сеанса работы пользователя при отключении персонального идентификатора; ○ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI); ○ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI); ○ возможность блокирования входа в систему локальных пользователей; ○ возможность блокирования операций вторичного входа в систему в процессе работы пользователей; ○ возможность блокировки сеанса работы пользователя по истечении интервала неактивности; ○ возможность управления политикой сложности паролей; ○ поддержка возможности входа в систему по сертификатам; ○ возможность проверки принадлежности аппаратного идентификатора в процессе управления аппаратными идентификаторами пользователей. • Контроль целостности файлов, каталогов, элементов системного реестра: ○ Должна быть возможность проведения контроля целостности в процессе загрузки ОС, в фоновом режиме при работе пользователя. ○ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов. ○ Должна быть возможность восстановления исходного состояния контролируемого объекта. ○ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП. ○ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ. • Обнаружение и предотвращение вторжений: ○ Должна обеспечиваться защита от вторжений с помощью сигнатурных и эвристических механизмов. ○ 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.

	○ Эвристические механизмы должны распознавать и фиксировать следующие типы атак: ▪ сканирование портов; ▪ подделка ARP (ARP-spoofing); ▪ SYN-флуд; ▪ атаки, направленные на отказ в обслуживании (DoS); ▪ распределенные атаки, направленные на отказ в обслуживании (DDoS). При обнаружении признаков атаки эвристическими методами должен осуществляться временный запрет на прием сетевых пакетов с IP-адреса атакующего компьютера. ○ Должны обеспечиваться обнаружение и блокировка аномальных сетевых пакетов. • Функциональный контроль ключевых компонентов системы. • Регистрация событий безопасности в журнале. ○ Должна быть возможность формирования отчетов по результатам аудита. ○ 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 Производитель ООО «Код безопасности» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже имеющимся программным обеспечением)	***Должно осуществлять:*** • контроль входа пользователей в систему, в том числе с использованием дополнительных аппаратных средств защиты; • 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. ***Требования к сертификации и применению в информационных системах:*** 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. СЗИ должно допускать использование в следующих информационных системах: • автоматизированные системы - до класса 1Г (включительно); • государственные информационные системы – до 1 класса защищенности (включительно); • информационные системы персональных данных – до 1 уровня защищенности персональных данных (включительно); • автоматизированные системы управления производственными и технологическими процессами – до 1 класса защищенности (включительно). ***Требования к функциональности СЗИ:*** СЗИ должно выполнять следующие функции по защите информации: • Контроль входа пользователей в систему и работа пользователей в системе: ○ проверка пароля пользователя при входе в систему; ○ 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; ○ возможность блокировки сеанса работы пользователя при отключении персонального идентификатора; ○ возможность использования персональных идентификаторов для входа в систему и разблокировки в системах терминального доступа и инфраструктуре виртуальных рабочих станций (VDI); ○ однократное указание учетных данных пользователей при доступе к терминальному серверу и инфраструктуре виртуальных рабочих станций (VDI); ○ возможность блокирования входа в систему локальных пользователей; ○ возможность блокирования операций вторичного входа в систему в процессе работы пользователей; ○ возможность блокировки сеанса работы пользователя по истечении интервала неактивности; ○ возможность управления политикой сложности паролей; ○ поддержка возможности входа в систему по сертификатам; ○ возможность проверки принадлежности аппаратного идентификатора в

	процессе управления аппаратными идентификаторами пользователей. • Контроль целостности файлов, каталогов, элементов системного реестра: ○ Должна быть возможность проведения контроля целостности в процессе загрузки ОС, в фоновом режиме при работе пользователя. ○ Должна быть возможность блокировки компьютера при обнаружении нарушения целостности контролируемых объектов. ○ Должна быть возможность восстановления исходного состояния контролируемого объекта. ○ Должна быть возможность контроля исполняемых файлов по встроенной ЭЦП, чтобы избежать дополнительных перерасчетов контрольных сумм при обновлении ПО со встроенной ЭЦП. ○ При установке системы должны формироваться задания контроля целостности, обеспечивающие контроль ключевых параметров операционной системы и СЗИ. • Защита сетевого взаимодействия и фильтрация трафика: ○ Должны быть механизмы аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети. ○ Должны удостоверяться субъекты доступа (пользователи и компьютеры) и защищаемые объекты (компьютеры). ○ Механизмы должны быть защищены от прослушивания, попыток подбора и перехвата паролей, подмены защищаемых объектов, подмены MAC- и IP-адресов. ○ 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. ○ Должна быть предусмотрена настройка режима защиты сетевого взаимодействия, при этом должны быть предусмотрены следующие режимы защиты: ▪ соединение без защиты; ▪ маркируется каждый пакет; ▪ подписывается заголовок каждого пакета; ▪ подписывается каждый пакет целиком. ○ Должна быть возможность ограничивать сетевые соединения по правилам фильтрации: ▪ на уровне отдельных протоколов из стека TCP/IP; ▪ на уровне параметров протоколов стека TCP/IP; ▪ на уровне параметров служебных протоколов стека TCP/IP; ▪ на уровне периодов времени; ▪ на уровне пользователей или групп пользователей; ▪ на уровне параметров прикладных протоколов; ▪ на уровне исполняемого файла/процесса; ▪ на уровне сетевого адаптера. ○ Должна быть возможность осуществлять фильтрацию команд, параметров и последовательностей команд, а также обеспечивать блокировку мобильного кода. ○ Должен быть предусмотрен выбор действий для определения реакции системы на срабатывание правил фильтрации: ▪ регистрация информации в журнале; ▪ звуковая сигнализация; ▪ запуск программы или сценария. • Функциональный контроль ключевых компонентов системы. • Регистрация событий безопасности в журнале. ○ Должна быть возможность формирования отчетов по результатам аудита. ○ 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 Производитель ООО «КРИПТО-ПРО» Страна происхождения – Россия (или эквивалент)	**1. Требования к реализации криптографических стандартов** 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: • генерацию и управление ключевой информацией; • формирование электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012; • подтверждение подлинности электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001и ГОСТ Р 34.10-2012;

	• подсчет значения хеш-функции в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012; • шифрование и расшифрование данных в соответствии с ГОСТ 28147-89; • формирование закрытых и открытых ключей электронной подписи и шифрования; • идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений; • реализацию набора протоколов IPsec в соответствии с особенностями использования отечественных криптографических алгоритмов. **2. Требования к сертификации** Средство электронной подписи (средство криптографической защиты информации) должно быть сертифицировано ФСБ России, в качестве: – Средства квалифицированной электронной подписи в соответствии с Требованиями ФСБ России к средствам электронной подписи; – Средства криптографической защиты информации в соответствии с требованиями ФСБ России к шифровальным (криптографическим) средствам защиты конфиденциальной информации. **3. Требования к реализации программного интерфейса встраивания** Средство криптографической защиты информации (средство электронной подписи) должно соответствовать криптографическому интерфейсу компании Microsoft - Cryptographic Service Provider (CSP). Встраивание средства криптографической защиты информации (средства электронной подписи) в прикладную информационную систему должно предусматривать возможность: • Применения в операционных системах семейства Microsoft Windows интерфейса функций CryptoAPI и CAPICOM; • Поддержки стандарта XML DSign при формировании электронной подписи в XML документах; • Непосредственного вызова функций средства криптографической защиты информации (средства электронной подписи); • 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. **4. Требования к составу** 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. 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. **5. Функциональные требования** Средство криптографической защиты информации (средство электронной подписи) должно предоставлять программный интерфейс для выполнения следующих основных функций: • формирование и подтверждение подлинности ЭП; • подсчет значения хеш-функции данных; • шифрование и расшифрование данных; • формирование закрытых и открытых ключей подписи и шифрования. Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать выполнение следующих сервисных функций: • установка личных сертификатов открытых ключей с обеспечением связи сертификата открытого ключа с соответствующим указанному сертификату закрытым ключом; • копирование и удаление закрытых ключей; • установка, изменение и удаление пароля на доступ к закрытому ключу. **6. Требования к общесистемному программному обеспечению** Средство криптографической защиты информации (средство электронной подписи) должно включать варианты исполнений, функционирующих в среде следующих

	операционных систем: Windows: Включает программно-аппаратные среды: – Windows XP/Vista/7/8/8.1/10/Server 2003/2008 (x86, x64); **7. Требования к поддерживаемым ключевым носителям** Средство криптографической защиты информации (средство электронной подписи) должно поддерживать следующие носители: • Смарт-карты Оскар, Магистра; • Электронные идентификаторы Touch-Memory DS1995, DS1996; • Электронные идентификаторы Rutoken; • Электронные идентификаторы eToken, Jacarta; • Электронные идентификаторы ESMART Token; • Смарткарты Athena IDProtect, INPASPOT, Cha cardOS, Cha JCOP, MPCOS-Gemalto; • Сменный Flash-носитель; • Жесткий диск ПЭВМ. Средство криптографической защиты информации (средство электронной подписи) должно обеспечивать возможность разработки программных библиотек поддержки произвольных типов перезаписываемых носителей. **8. Требования к поддерживаемым стандартным приложениям и службам операционных систем** Средство криптографической защиты информации (средство электронной подписи) должно поддерживаться следующими стандартными приложениями и службами операционных систем: • Microsoft Certification Authority из состава Windows 2008/2008R2/2012/2012R2; • Электронная почта - MS Outlook из состава Microsoft Office. • Microsoft Word, Excel, Info Path из состава Microsoft Office. • Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode. • Службы терминалов для 2008/2008R2/2012/2012R2 (включая шлюз служб терминалов) с обеспечением доступа к Службе по протоколу TLS. • Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer – web-сервер IIS, TLS-сервер, TLS-клиент (IE). • SQL-сервер. • ISA/TMG сервер. • Сервер терминалов и клиент (RDP). Данное средство должно обеспечивать возможность реализации сетевой аутентификации в домене MS Windows (на основе Winlogon) с использованием реализованных данным средством российских криптоалгоритмов 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 Производитель ООО «КРИПТО-ПРО» Страна происхождения – Россия (или эквивалент)	Компакт-диск с дистрибутивом программного обеспечения и формуляром.
Сертификат технического сопровождения ПО ViPNet Client на 1 год Производитель ОАО «ИнфоТеКС» Страна происхождения – Россия (эквивалент не допускается в связи с необходимостью совместимости с уже	***Сертификат включает в себя:*** 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. Поставка сертификата технического сопровождения производителя ОАО «ИнфоТеКС», сроком действия не менее 1 года

имеющимся программным обеспечением)	

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