УТВЕРЖДАЮ

Главный инженер
«Курскатомэнергоремонт» -
филиал АО «Атомэнергоремонт»
_____ И.С. Жилин
«_28_» _июля_____2022 г

ТЕХНИЧЕСКОЕ ЗАДАНИЕ № 02.6/302-2022
на оказание услуг

Предмет закупки: Создание системы защиты информационной системы персональных данных и организация подключения к «Федеральному реестру сведений о документах об образовании и (или) о квалификации, документах об обучении»

Курчатов
2022

СОДЕРЖАНИЕ

РАЗДЕЛ 1. НАИМЕНОВАНИЕ ПРЕДМЕТА ЗАКУПКИ

1.1. Создание системы защиты информационной системы персональных данных и организация подключения к «Федеральному реестру сведений о документах об образовании и (или) о квалификации, документах об обучении».

РАЗДЕЛ 2. ОПИСАНИЕ УСЛУГ ИЛИ РАБОТ

Подраздел 2.1 Состав (перечень) оказываемых услуг или выполняемых работ
Создание системы защиты информационной системы персональных данных и организация подключения к «Федеральному реестру сведений о документах об образовании и (или) о квалификации, документах об обучении» включает в себя: 2.1.1 Сбор и анализ исходных данных и разработка комплекта документации; 2.1.2 Поставка СЗИ; 2.1.3 Внедрение поставляемых СЗИ; 2.1.4 Настройка подключения ИСПДн к информационным ресурсам ФИС «ФРДО»; 2.1.5 Проведение оценки эффективности реализованных мер по обеспечению безопасности ПДн, разработка подтверждающей документации. 2.1.6 Оказание услуг по техническому сопровождению сроком не менее 12 месяцев.
Подраздел 2.2 Описание оказываемых услуг или выполняемых работ
2.2.1 Сбор и анализ исходных данных и разработка комплекта документации, включает в себя разработку следующих документов: - «Акт обследования ИСПДн»; - «Модель угроз безопасности ПДн» - «Проект Акта определения уровня защищенности ПДн»; - «Техническое задание на создание системы защиты ПДн»; - «Программа и методики оценки эффективности реализованных мер по обеспечению безопасности ПДн»; - комплект шаблонов организационно-распорядительной документации. 2.2.2 Поставка средств защиты информации должна включать в себя: - Установочный комплект СЗИ Secret Net Studio 8 или эквивалент; - Право на использование комплекта СЗИ Secret Net Studio 8 или эквивалент; - Компакт-диск с дистрибутивом ПО ViPNet Client for Windows или эквивалент; - Предоставление права использования ПО ViPNet Client КС2 for Windows или эквивалент; - Компакт-диск с дистрибутивом ПО ViPNet PKI Client КС2 for Windows или эквивалент; - Предоставление права на использование ПО ViPNet PKI Client КС2 for Windows или эквивалент. 2.2.3 Внедрение поставляемых СЗИ: установка и настройка на 1 (одном) компьютере «Курскатомэнергоремонт»- филиал «Атомэнергоремонт»; 2.2.4 Настройка подключения ИСПДн к информационным ресурсам ФИС «ФРДО»; 2.2.5 Проведение оценки эффективности реализованных мер по обеспечению безопасности ПДн, разработка подтверждающей документации: - «Технический паспорт ИСПДн» - «Протокол проведения оценки эффективности реализованных мер по обеспечению безопасности ПДн»; - «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности ПДн».. 2.2.6 Оказание услуг по техническому сопровождению сроком не менее 12 месяцев.
Подраздел 2.3 Объем оказываемых услуг или выполняемых работ, либо доля оказываемых услуг или выполняемых работ в общем объеме закупки

№ п/п	Наименование услуги	Характеристики	Кол-во
1	Установочный комплект. Secret Net Studio 8 или эквивалент	Дистрибутив должен поставляться в виде CD-диска в комплекте с заверенной копией сертификата ФСТЭК России формуляром и кратким руководством. Должен иметь действующую лицензию ФСТЭК.	1
2	Лицензия на использование комплекта "Постоянная защита" Средства защиты информации Secret Net Studio 8 или эквивалент	Выполнять функции модуля защиты от несанкционированного доступа. 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:	1

		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.	
3	Лицензия на использование модуля антивируса по технологии Касперского Средства защиты информации Secret Net Studio 8 или эквивалент	Выполнение функции антивирусного клиента. Антивирусная защита должна обеспечиваться автоматическая проверка наличия вредоносных программ по типовым сигнатурам и с помощью эвристического анализа. Должно обеспечиваться сканирование локальных дисков, подключаемых дисков, отчуждаемых носителей, в том числе по команде и по расписанию. Должна быть возможность указать расписание запуска антивирусных проверок с возможностью выбора ежечасного запуска, запуска в заданное время ежедневно, запуска в заданный день недели и время еженедельно или по событиям запуска СЗИ и событию успешного обновления баз. Профили антивирусного сканирования должны поддерживать настройку следующих параметров: - название и описание; - уровень эвристического анализа; - проверка или пропуск архивов; - пропуск файлов больше заданного размера; - проверка файлов только с заданным перечнем расширений; - действия с обнаруженными вредоносными объектами – лечение, удаление, помещение в карантин; - объекты сканирования, включая возможность указать проверку исполняемых процессов в оперативной памяти, проверку	1

		загрузочных секторов, проверку локальных, съемных и сетевых дисков и перечень проверяемых директорий. Должно обеспечиваться удаление вредоносного программного обеспечения и его блокировка (перемещение в карантин). Должно обеспечиваться восстановление файлов из карантина по команде администратора. Должен поддерживаться список файлов и директорий, исключаемых из проверки (белый список). Должна обеспечиваться возможность обновления баз данных признаков компьютерных вирусов (антивирусных баз), в том числе с доступом к серверу обновлений через прокси-сервер. Должен обеспечиваться контроль целостности антивирусных баз и защита от их подмены при загрузке с сервера обновлений. Должна обеспечиваться возможность развертывания зеркала сервера обновлений в локальной сети. Должна быть реализована возможность обновления антивирусных баз со съемных носителей и по локальной сети, без доступа к серверу обновлений. Должны быть: - 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.	
4	Компакт-диск с дистрибутивом ПО ViPNet Client for Windows 4.x или эквивалент	Дистрибутив должен поставляться в виде CD-диска в комплекте с заверенными копиями сертификатов ФСТЭК, ФСБ России, формуляром и кратким руководством. Должен иметь действующую лицензию ФСТЭК.	1
5	Предоставление права использования ПО ViPNet Client for Windows 4.x (КС2) или эквивалент	Программное обеспечение, реализующее функции криптографического клиента должно отвечать следующим требованиям: - полностью совместимо с программным обеспечением, реализующим функции управления защищённой сетью: обновление программного обеспечения, обновление справочно-ключевой информации, управлением политиками безопасности; - полностью совместимо с программным комплексом, реализующим функции	1

		криптографического шлюза, представленным в настоящем запросе котировок: шифрование/дешифрование направляемого/принимаемого IP-трафика; - поддержка операционных систем: Windows 8 (32/64-разрядная); Windows 8.1 (32/64-разрядная); Windows Server 2008 R2 (64-разрядная); Windows Server 2012 (64-разрядная); Windows Server 2012 R2 (64-разрядная); Windows 10 (32/64 разрядная); Windows Server 2016 (64-разрядная). - наличие в составе программного обеспечения, соответствующего требованиям ФСТЭК России к межсетевым экранам по 3 классу, отсутствию недекларируемых возможностей по 3 уровню, иметь ОУД не ниже 4+ и возможностью использования в АС до класса 1В включительно; - наличие сертификата ФСБ России по классу КС2 (КС3); - иметь встроенный персональный экран, соответствующий 3-му классу по требованиям ФСТЭК России; - предоставлять функции клиента службы обмена файлами и сообщениями, защищенной электронной почты с функциями шифрования писем и вложений для обмена с другими криптографическими клиентами; - предоставлять функции контроля запускаемых в операционной системе приложений; - предоставлять функции контентной фильтрации прикладных протоколов http, ftp; - программное обеспечение, реализующее функции криптографического клиента, должно шифровать каждый IP-пакет на уникальном ключе, основанном на паре симметричных ключей связи с другими криптографическими шлюзами и клиентами, выработанных в программном обеспечении, реализующем функции управления защищённой сетью; - взаимодействие с другими криптографическими клиентами с использованием технологии «клиент-клиент» (без использования криптографического шлюза»).	
6	Предоставление права на использование ПО ViPNet PKI Client КС2 for Windows 1.x Базовая лицензия. Бессрочная. или эквивалент	В качестве средства защиты информации для защиты файлов и данных с помощью шифрования и электронной подписи должен использоваться программный комплекс (ПК), отвечающий следующим требованиям:	1

		ПК должен обеспечивать выполнение следующих функций: - шифрование, формирование и проверку ЭП файлов; - шифрование, формирование и проверку ЭП данных, передаваемых браузерами - поддержание в актуальном состоянии CRL, необходимых для работы с сертификатами; - контроль подтверждения права пользователя на использование ПК; - управление сертификатами, используемыми для работы с ПК; - обеспечение регистрации передаваемых ПК сведений о произошедших событиях. Должен функционировать под управлением следующих ОС: Windows 8 (32/64-разрядная); Windows 8.1 (32/64-разрядная); Windows Server 2008 (32/64-разрядная); Microsoft Windows Server 2008 R2 (64-разрядная); Windows Server 2012 (32/64-разрядная); Windows Server 2012 R2 (64-разрядная). Должен поддерживать работу в следующих виртуальных средах: Microsoft Hyper-V; VMWare Workstation; VMWare Player; VMWare vSphere ESXi; VirtualBox. Обеспечивать создание ключей ЭП и ключей проверки ЭП, создание ЭП и проверку ЭП в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012. Обеспечивать хэширование данных в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012. Обеспечивать имитозащиту данных в соответствии с алгоритмом ГОСТ 28147-89 (в режиме выработки имитовставки). Обеспечивать шифрование данных в соответствии с ГОСТ 28147-89. Обеспечивать реализацию функций средства ЭП (создание ключа ЭП, создание ЭП, создание ключа проверки ЭП, проверка ЭП) в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи». Должен соответствовать требованиям ФСБ России к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, и требованиям к средствам электронной подписи, установленным для классов КС1 (для исполнения 1), КС2 (для исполнения 2) и КС3 (для исполнения 3).	

7	Оказание услуг по техническому сопровождению средств криптографической защиты информации сроком 12 месяцев	На первой линии технической поддержки выступает служба технической поддержки Производителя. Должно включать в себя: - Приём обращений и консультирование по электронной почте в рабочие дни с 1:00 до 20:00 - Приём обращений и консультирование по телефону горячей линии в рабочие дни с 1:00 до 20:00 Должно обеспечиваться: 1) Консультирование при установке Продуктов: 2) Рекомендации по настройке продукта в объеме эксплуатационной документации 3) Диагностика с целью установления факта ошибки в работе программного продукта. Выявленная ошибка, в зависимости от сложности, устраняется в процессе диагностики или в последующих обновлениях ПО. Консультирование при эксплуатации ИТКС, в составе которой есть Продукты: 4) Рекомендации по «тонкой» настройке продукта после знакомства с особенностями ИТКС Пользователя	1

Подраздел 2.4 Код ОКПД 2
62.09.20.120 – Услуги по установке программного обеспечения.

РАЗДЕЛ 3. ТРЕБОВАНИЯ К УСЛУГАМ

Подраздел 3.1 Общие требования
3.1.1 Отчетные документы должны быть представлены на бумажных носителях и/или электронном виде (для проектов документов, по согласованию с Заказчиком) в одном экземпляре. 3.1.2 Исполнитель работ должен не менее чем за 5 рабочих дней представить Заказчику утвержденный перечень своих специалистов, участвующих в проведении работ. 3.1.3 Исполнитель при проведении работ обязан обеспечить соблюдение требований правил внутреннего распорядка и пропускного (внутриобъектового) режима. 3.1.4 Место оказания услуг находится в здании «Курскатомэнергоремонт» - филиал АО «Атомэнергоремонт» по адресу: 307250, Курская область, г. Курчатов, промышленная зона Промзона, зд. 1, стр. 1, «Курскатомэнергоремонт» - филиал АО «Атомэнергоремонт». 3.1.5 Исполнитель должен соответствовать требованиям, установленным в соответствии с статьей 12 Федерального закона от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности» (https://docs.cntd.ru/document/902276657) к лицам, осуществляющим оказание услуг, являющихся объектом закупки, а именно: - наличие собственной действующей лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств,

информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), при условии наличия в данной действующей лицензии работ (услуг), предусмотренных пунктами «12», «20», «21», «28» Перечня оказываемых услуг и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, утверждённого постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313 (https://rg.ru/documents/2012/04/24/shifry-site-dok.html).

- наличие собственной действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, при условии наличия в данной действующей лицензии работ (услуг), предусмотренных подпунктами «б», «е», «г», «д» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79.

3.1.6 Исполнитель обязан представлять Заказчику по его требованию необходимую документацию, относящуюся к оказанию услуги.

3.1.7 При оказании услуг необходимо руководствоваться требованиями действующих законодательных актов и нормативно-методических документов РФ.

3.1.8 Срок предоставления услуг: в течении 50 (пятидесяти) рабочих дней с момента заключения договора.

3.1.9 Общие требования к оформлению предоставляемой документации:

Язык оформления документации – русский, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств импортного производства.

Документы должны быть оформлены Исполнителем в соответствии с требованиями оформленный в соответствии с требованиями «ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам» (https://docs.cntd.ru/document/1200001260).

С целью надлежащего исполнения Сторонами своих обязательств, состав, объем, наименования, требования к содержанию документации могут быть скорректированы Сторонами в ходе оказания услуг.

Комплект документации оформляется Исполнителем на бумажных носителях и передается Заказчику нарочно или направляется почтовым отправлением, за исключением комплекта шаблонов организационно-распорядительной документации

Комплект шаблонов организационно-распорядительной документации оформляется Исполнителем в электронном виде, редактируемом формате и предоставляется Заказчику посредством отправки на электронную почту, предоставляемую Заказчиком или опубликованную им на официальном сайте (в случае непредоставления).

Подраздел 3.2 Требования к качеству оказываемых услуг или выполняемых работ

3.2.1 Услуги должны быть оказаны в соответствии с требованиями следующих нормативных и правовых актов Российской Федерации в области обеспечения информационной безопасности:

– Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных» (https://docs.cntd.ru/document/901990046).

– Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (https://docs.cntd.ru/document/901990051);

– Федеральный закон от 04 мая 2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (https://docs.cntd.ru/document/902276657);

– Постановление Правительства Российской Федерации от 01 ноября 2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»(https://docs.cntd.ru/document/902377706)

– Постановление Правительства Российской Федерации от 16 апреля 2012 №313 «Об

утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)» (https://base.garant.ru/70164728/);

– Постановление Правительства РФ от 03 февраля 2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (https://fstec.ru/litsenzionnaya-deyatelnost/tekhnicheskaya-zashchita-informatsii/75-postanovleniya/225-postanovlenie-pravitelstva-rossijskoj-federatsii-ot-3-fevralya-2012-g-n-79);

– «Специальные требования и рекомендации по технической защите конфиденциальной информации», утвержденные Приказом Гостехкомиссии России от 30 августа 2002 № 282 (https://bit.ly/3zBz4yC);

– Приказ ФСБ России от 10 июня 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 защищённости» (https://base.garant.ru/70727118/);

– Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" (https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21);

– ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам (https://docs.cntd.ru/document/1200001260)

3.2.2 Исполнитель должен соответствовать требованиям, установленным в соответствии с статьей 12 Федерального закона от 04.05.2011 №99-ФЗ «О лицензировании отдельных видов деятельности»(https://docs.cntd.ru/document/902276657) к лицам, осуществляющим оказание услуг, являющихся объектом закупки, а именно:

– наличие собственной действующей лицензии ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищённых с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), при условии наличия в данной действующей лицензии работ (услуг), предусмотренных пунктами «12», «20», «21», «28» Перечня оказываемых услуг и оказываемых услуг, составляющих лицензируемую деятельность в отношении шифровальных (криптографических) средств, утверждённого постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313.

- наличие собственной действующей лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, при условии наличия в данной

действующей лицензии работ (услуг), предусмотренных подпунктами «б», «е», «г», «д» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утверждённого постановлением Правительства Российской Федерации от 03 февраля 2012 г. № 79.
Подраздел 3.3 Требования к гарантийным обязательствам оказываемых услуг или выполняемых работ
3.3.1 Исполнитель при оказании услуг гарантирует соблюдение требований настоящего Технического задания, условий Договора, действующего законодательства и действующих законов РФ. 3.3.2 На все поставляемые СЗИ должны распространяться обязательства гарантийного обслуживания, предоставляемые Производителем. 3.3.3 Исполнитель должен обеспечить соблюдение правил действующего внутреннего трудового распорядка, контрольно-пропускного режима, внутренних положений и инструкций, действующих на объекте информатизации Заказчика.
Подраздел 3.4 Требования к конфиденциальности
3.4.1 Все сведения о составе и характеристиках объектов информатизации конечных пользователей и Заказчика являются конфиденциальной информацией. 3.4.2 Стороны обязуются обеспечить конфиденциальность полученной друг от друга информации и не допускать ее разглашения. 3.4.3 Конфиденциальная информация, передаваемая Исполнителю, в лице его сотрудников, на бумажном или машинном носителе, должна быть помечена реквизитами, позволяющими идентифицировать ее как конфиденциальную. 3.4.4 Сторона, получающая конфиденциальную информацию, должна обеспечить защиту этой информации от несанкционированного использования, распространения или публикации. 3.4.5 Исполнитель принимает меры по ограничению круга лиц, привлекаемых для оказания услуг на объекте Заказчика.
Подраздел 3.5 Требования к безопасности оказания услуг или выполнения работ и безопасности результата оказанных услуг или выполняемых работ
3.5.1 Исполнитель обязуется: – не проводить противозаконные действия по сбору, использованию и передаче третьей стороне информации, циркулирующей и хранящейся на объектах информатизации Заказчика; – не осуществлять несанкционированный доступ к информационным ресурсам объектов информатизации Заказчика; – не проводить незаконное копирование информации, циркулирующей или хранящейся на объектах информатизации Заказчика; – не предпринимать манипулирование информацией, циркулирующей или хранящейся на объектах информатизации (фальсифицировать, модифицировать, подделывать, блокировать, уничтожать или искажать информацию); – не нарушать технологию сбора, накопления, хранения, обработки, преобразования, отображения и передачи информации, в результате чего может быть осуществлено искажение, потеря или незаконное использование информации; – не внедрять на объектах информатизации программы-вирусы (загрузочные, файловые и др.); – не устанавливать программные и аппаратные закладные устройства в технические средства объектов информатизации Заказчика; – не устанавливать в технические средства объектов информатизации программное обеспечение, зараженное вирусами. 3.5.2 Нарушение настоящих требований влечёт за собою гражданско-правовую, административную или уголовную ответственность в соответствии с законом Российской Федерации.
Подраздел 3.6 Специальные требования

Не установлены.
Подраздел 3.7 Требования к сроку выполнения услуг или работ
Срок предоставления услуг: в течении 50 (пятидесяти) рабочих дней с момента заключения договора.

РАЗДЕЛ 4. РЕЗУЛЬТАТ ОКАЗАННЫХ УСЛУГ

Подраздел 4.1 Описание конечного результата оказанных услуг или выполняемых работ
4.1.1. Результатом сбора и анализа исходных данных и разработки комплекта документации является; – обследование ИСПДн; – определение актуальных угроз безопасности ПДн; – разработка рекомендаций по определению уровня защищенности ПДн; – формирование требований к СЗПДн; – разработка комплекта организационно-распорядительной документации: «Акта обследования информационной системы персональных данных»; «Модель угроз безопасности персональных данных» «проекта Акта определения уровня защищенности персональных данных»; «Техническое задание на создание системы защиты персональных данных»; «Программа и методики оценки эффективности реализованных мер по обеспечению безопасности персональных данных»; комплекта шаблонов организационно-распорядительной документации. 4.1.2 Поставка СЗИ: результатом поставки СЗИ является заверенные сторонами Акт оказанных услуг, фиксирующие факт поставки. 4.1.3 Результатом внедрения поставляемых СЗИ является - установка поставляемых СЗИ в соответствии с требованиями эксплуатационной документации; – настройка поставляемых СЗИ в объеме достаточном для успешного проведения оценки эффективности системы защиты ПДн; – разработка «Технический паспорт информационной системы персональных данных». – корректно функционирующая СЗПДн; 4.1.4 Настройка подключения ИСПДн к информационным ресурсам ФИС «ФРДО»; В рамках организации подключения ИСПДн к ФИС «ФРДО» Исполнитель обеспечивает: проведение оценки эффективности реализованных мер по обеспечению безопасности ПДн; настройку подключения ИСПДн к информационным ресурсам ФИС «ФРДО». 4.1.5 Результатом настройки подключения ИСПДн к информационным ресурсам ФИС «ФРДО» является доступ к порталам ФИС «ФРДО» до момента авторизации пользователем. 4.1.6 Проведение оценки эффективности реализованных мер по обеспечению безопасности ПДн, разработка подтверждающей документации. 4.1.7 В рамках проведения оценки эффективности реализованных мер по обеспечению безопасности ПДн Исполнителем проводятся комплексные испытания ИСПДн в реальных условиях эксплуатации путем проверки фактического выполнения установленных требований на различных этапах технологического процесса обработки ПДн. 4.1.8 Результатом оценки эффективности реализованных мер по обеспечению безопасности ПДн является следующая документация: – «Протокол проведения оценки эффективности реализованных мер по обеспечению безопасности персональных данных»; – «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности персональных данных». 4.1.9 Срок действия «Заключение по результатам оценки эффективности реализованных мер по обеспечению безопасности персональных данных»: 3 года.

Подраздел 4.2 Требования по приемке услуг или выполняемых работ
4.2.1 По окончании оказания услуг Исполнитель должен предоставить Заказчику следующие основные документы: – акт сдачи-приемки услуг; – счет на оплату.
Подраздел 4.3 Требования по передаче заказчику технических и иных документов (оформление результатов оказанных услуг или выполняемых работ)
В соответствии с п. 2.2 настоящего технического задания.

РАЗДЕЛ 5. ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБУЧЕНИЮ ПЕРСОНАЛА ЗАКАЗЧИКА

Не установлены.

РАЗДЕЛ 6. ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

№ п/п	Сокращение	Расшифровка сокращения
1	АРМ	Автоматизированное рабочее место
2	ИСПДн	Информационная система персональных данных
3	ИС	Информационная система
4	ОС	Операционная система
5	ФИС «ФРДО»	Федеральная информационная система «Федеральный реестр сведений документов об образовании и (или) о квалификации, документах об обучении».
6	ПДн	Персональные данные, обрабатываемые в информационной системе персональных данных Заказчика
7	ПО	Программное обеспечение
8	СЗИ	Средство защиты информации
9	СЗПДн	Система защиты персональных данных, обрабатываемых в информационной системе персональных данных
10	ТЗ	Техническое задание
11	ФСТЭК	Федеральная служба по техническому и экспортному контролю

РАЗДЕЛ 7. ПЕРЕЧЕНЬ ПРИЛОЖЕНИЙ

Номер приложения	Наименование приложения	Номер страницы
-	-	-

Информационно-справочный документ / Служебная переписка
Краткое содержание: Согласование ТЗ «Создание системы защиты информационной системы персональных данных и организация подключения к «Федеральному реестру с...
Номер проекта документа: 31/71134-ПРОЕКТ от 27.07.2022
Регистрационный номер: 31-22-02/37400-ВН от 28.07.2022
Исполнитель: Баринова Екатерина Сергеевна, +7(47131)52200 вн. 222, АО "Атомэнергоремонт"
Данные в отчете отображены по часовому поясу: АО "Атомэнергоремонт" (UTC+3:00 Волгоград, Москва, Санкт-Петербург)

Визирование документа

Версия документа	Этап процесса	Дата и время	Организация	Подразделение сотрудника	Должность	ФИО	Виза
2	(Подписание)	28.07.2022 16:14:35	АО "Атомэнергоремонт"	АО "Атомэнергоремонт"	Главный инженер	Жилин Игорь Станиславович	Подписано
2	(Согласование)	28.07.2022 14:28:03	АО "Атомэнергоремонт"	АО "Атомэнергоремонт"	Ведущий инженер	Никулин Иван Николаевич	Согласовано
2	(Согласование)	27.07.2022 16:34:38	АО "Атомэнергоремонт"	АО "Атомэнергоремонт"	Руководитель службы подготовки персонала	Теняков Александр Семенович	Согласовано
2	(Согласование)	27.07.2022 15:10:08	АО "Атомэнергоремонт"	АО "Атомэнергоремонт"	Ведущий инженер-программист	Камынин Максим Сергеевич	Согласовано
2	(Согласование)	27.07.2022 14:43:09	АО "Атомэнергоремонт"	АО "Атомэнергоремонт"	Начальник отдела	Малышенкова Екатерина Владимировна	Согласовано
2	(Согласование)	27.07.2022 14:01:35	АО "Атомэнергоремонт"	АО "Атомэнергоремонт"	Заместитель главного инженера по подготовке производства	Квятковский Владислав Валентинович	Согласовано
2	(Согласование)	27.07.2022 13:57:58	АО "Атомэнергоремонт"	АО "Атомэнергоремонт"	Начальник отдела	Глазунова Юлия Александровна	Согласовано