**Техническое задание**

**по созданию системы защиты персональных данных автоматизированной информационной системы многофункционального центра предоставления государственных и муниципальных услуг в Пильнинском районе Нижегородской области**

1. Наименование объекта закупки:

**Создание системы защиты персональных данных автоматизированной информационной системы многофункционального центра предоставления государственных и муниципальных услуг в Пильнинском районе Нижегородской области**

1. Описание объекта закупки:

|  |
| --- |
| **Создание системы защиты персональных данных автоматизированной информационной системы многофункционального центра предоставления государственных и муниципальных услуг в Пильнинском районе Нижегородской области.**  **Требования к составу услуг по сопровождению объекта закупки**  Создание системы защиты персональных данных клиентского сегмента АИС МФЦ осуществляется Подрядчиком следующими этапами.  **1.Формирование требований к защите информации, содержащейся в информационной системе, разработка проекта СЗПД.**  Формирование требований к защите персональных данных, обрабатываемых в клиентском сегменте АИС МФЦ, включающее:  − обследование клиентского сегмента АИС МФЦ и условий его функционирования (проводится Подрядчиком);  − определение перечня должностных лиц (структурных подразделений), ответственных за вопросы обработки и защиты персональных данных (проводится Подрядчиком);  − уточнение (при необходимости) модели угроз безопасности персональных данных, обрабатываемых в клиентском сегменте АИС МФЦ (проводится Подрядчиком);  − определение класса защищенности сегмента системы и уровня защищенности персональных данных, обрабатываемых в клиентском сегменте АИС МФЦ (проводится ГБУ УМФЦ НО);  − определение набора базовых мер в соответствии с классом защищенности сегмента системы и уровня защищенности персональных данных, обрабатываемых в клиентском сегменте АИС МФЦ . Проведение адаптации, уточнения и дополнения набора базовых мер (при необходимости. Проводится Подрядчиком);  − разработка технического проекта системы защиты персональных данных клиентского сегмента АИС МФЦ в соответствии с требованиями настоящего технического задания, класса защищенности сегмента системы, модели угроз, включающего следующие подсистемы безопасности(проводится Подрядчиком):  - подсистема идентификации, аутентификации и управления (разграничения) доступом объектов доступа к субъектам доступа;  -подсистема регистрации и учета событий безопасности;  - подсистема обеспечения (контроля) целостности;  - подсистема межсетевого экранирования;  -подсистема криптографической защиты информации для передачи информации между центральным сегментом и периферийными сегментами АИС МФЦ ;  - подсистема антивирусной защиты;  -подсистема анализа(контроля) защищенности;  - согласование проектного решения с ГБУ УМФЦ НО и организацией, выдавшей аттестат соответствия серверного сегмента АИС МФЦ (проводится Подрядчиком).  **2. Внедрение СЗПД**  Внедрение системы защиты персональных данных (проводится Подрядчиком), включающее следующие мероприятия:  − поставка программных и (или) программно-аппаратных средств защиты информации в соответствии с проектным решением;  − установка и настройка поставленных программных и (или) программно-аппаратных средств защиты информации;  − настройка защищенного взаимодействия с серверным сегментом АИС МФЦ НО;  − проведение предварительных испытаний системы защиты.  **2.1. Поставка программных и (или) программно-аппаратных средств защиты информации**  Поставка (проводится Подрядчиком) средств защиты информации (программные и технические средства защиты информации, средства криптографической защиты информации, средства анализа защищенности) осуществляется в соответствии со спецификацией. Количество средств защиты и адреса поставки и установки определяются в п. 10 настоящего Технического задания.  **2.2. Установка и настройка поставленных программных и (или) программно-аппаратных средств защиты информации;**  Установка и настройка (проводится Подрядчиком) поставленных программных и (или) программно-аппаратных средств защиты информации производится в соответствии с документацией разработчиков средств защиты, а также требованиями, предъявляемыми к государственным ИСПДн установленного класса.  **2.3. Настройка защищенного взаимодействия с серверным сегментов АИС МФЦ НО;**  Настройка (проводится Подрядчиком) защищенного взаимодействия с серверным сегментом АИС МФЦ НО может производиться совместно с работами по установке средств защиты информации.  Для настройки защищенного взаимодействия с серверным сегментом АИС МФЦ НО необходимо выполнить следующие мероприятия:  1) Провести включение и регистрацию программных и программно-аппаратных средств криптографической защиты информации семейства VipNET Custom клиентского сегмента АИС МФЦ в сеть VipNET №6387 МФЦ Нижегородской области. Настроить конфигурацию ПО VipNET Клиент для подключения к АИС МФЦ. Провести настройку прав доступа клиентского ПО VipNET к ресурсам АИС МФЦ НО.  2) Провести включение и регистрацию средств защиты от НСД Dallas Lock рабочих мест клиентского сегмента АИС МФЦ НО в сервере безопасности Dallas Lock в ГБУ «Уполномоченный МФЦ» НО. Провести привязку персональных идентификаторов к учетным записям пользователей в сервере безопасности Dallas Lock в ГБУ «Уполномоченный МФЦ» НО. Организовать выдачу персональных идентификаторов пользователям под роспись в журнале.  3) Провести выдачу пользователям под роспись в журнале персональных идентификаторов для авторизации пользователей в прикладном комплексе АИС МФЦ Нижегородской области.  **2.4 Проведение предварительных испытаний системы защиты.**  На текущем этапе производится испытание работоспособности установленных средств защиты, корректность их настроек, возможность защищенного подключения к АИС МФЦ НО (проводится Подрядчиком).  **3. Аттестация**  Аттестация (проводится Подрядчиком) клиентского сегмента АИС МФЦ НО, ввод его в действие, включающая следующие этапы:  − подготовка клиентского сегмента АИС МФЦ НО к аттестации  по требованиям безопасности конфиденциальной информации, обрабатываемой в АИС МФЦ НО;  − разработка программы и методик аттестационных испытаний, аттестационных документов для клиентского сегмента АИС МФЦ НО.  Программа и методика аттестационных испытаний должна быть согласована с организацией, выдавшей аттестат соответствия серверного сегмента АИС МФЦ Нижегородской области;  − аттестация клиентского сегмента АИС МФЦ НО по требованиям безопасности конфиденциальной информации, обрабатываемой в АИС МФЦ НО (проведение аттестационных испытаний с оформлением соответствующих протоколов, подготовка заключений по результатам аттестационных испытаний, оформление и выдача аттестата соответствия клиентского сегмента АИС МФЦ НО требованиям безопасности конфиденциальной информации, обрабатываемой в АИС МФЦ НО). Срок действия аттестата соответствия должен быть не более 3 лет.  **4. Ввод в эксплуатацию СЗПД**  После выполнения всех мероприятий и получения аттестата соответствия муниципальное учреждение уведомляет официальным письмом оператора АИС МФЦ - ГБУ «Уполномоченный МФЦ» Нижегородской области о проведенных мероприятиях с предоставлением копий приказов о назначении ответственных лиц по обработке ПДн в клиентском сегменте АИС МФЦ и их контактных данных, а также копии аттестата соответствия требованиям по безопасности ИСПДн установленного класса.  ГБУ «Уполномоченный МФЦ» Нижегородской области после проверки полученных данных оформляет официальное письмо о возможности ввода в эксплуатацию клиентского сегмента АИС МФЦ соответствующего муниципального учреждения МФЦ и направляет его в адрес муниципального учреждения МФЦ.  Муниципальное учреждение МФЦ при получении письма оформляет приказ в вводе в промышленную эксплуатацию клиентского сегмента АИС МФЦ муниципального учреждения МФЦ.  **5.** **Гарантийное сопровождение**  На стадии гарантийного сопровождения (проводится Подрядчиком) системы осуществляются следующие мероприятия в соответствии с настоящим Техническим заданием.  **Требования к безопасности выполняемых работ:**  Конструкция аппаратно-программных средств защиты Системы должна обеспечивать защиту эксплуатирующего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003 и ГОСТ 12.2.007. Подключение электропитания к оборудованию Системы должно выполняться в соответствии с требованиями «Правил устройства электроустановок».  Эксплуатационная документация должна содержать указания по безопасности при эксплуатации и техническом обслуживании.  Условия эксплуатации объекта автоматизации и характеристики окружающей среды определяются в соответствии с Гигиеническими требованиями к видео-дисплейным терминалам, персональным электронно-вычислительным машинам и организации работы (Санитарные правила и нормы (СанПиН) 2.2.2/2.4.1340-03).  Технические средства, входящие в состав Системы, должны удовлетворять требованиям стандартов РФ по уровням напряженности электрических полей и уровню шума на рабочих местах пользователей и обслуживающего персонала.  **Требования к функциональным и качественным характеристикам работ:**  1. Для обеспечения 2 класса защищенности в клиентских сегментах ИСПД АИС МФЦ НО Подрядчиком должны применяться:  - средства вычислительной техники не ниже 5 класса;  - средства антивирусной защиты не ниже 4 класса;  -межсетевые экраны не ниже 3 класса (при подключении к сетям международного обмена информацией).  2. Для обеспечения уровня защищенности персональных данных при их обработке в клиентском сегменте ИСПД АИС МФЦ НО необходимо выполнение следующих требований:  а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;  б) обеспечение сохранности носителей персональных данных;  в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей;  г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;  д) назначение должностного лица, ответственного за обеспечение  безопасности персональных данных в информационной системе;  е) доступ к содержанию электронного журнала сообщений был возможен исключительно для должностных лиц или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных обязанностей.  3. Организационные и технические меры защиты информации, реализуемые в клиентском сегменте ИСПД АИС МФЦ НО (в рамках ее системы защиты информации), должны обеспечивать:   * идентификацию и аутентификацию субъектов доступа и объектов  доступа; * управление доступом субъектов доступа к объектам доступа; * ограничение программной среды; * защиту машинных носителей информации; * регистрацию событий безопасности; * антивирусную защиту; * контроль (анализ) защищенности информации; * целостность информационной системы и информации; * доступность информации; * защиту технических средств; * защиту информационной системы, ее средств, систем связи и передачи данных.   В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013 г. №17 в АИС МФЦ НО должен быть реализован дополненный уточненный адаптированный базовый набор мер защиты информации.  СЗПД клиентского сегмента АИС МФЦ НО муниципального автономного учреждения «МФЦ Пильнинского района Нижегородской области» должна содержать следующие подсистемы:  − подсистема управления доступом;  − подсистема регистрации и учета;  − подсистема межсетевого экранирования;  − подсистема антивирусной защиты;  − подсистема резервного копирования;  − подсистема криптографической защиты;  − подсистема анализа защищенности.  Функции реализуются модулями используемых средств защиты информации, указанных в настоящем Технического задания.  Установленные в клиентских сегментах АИС МФЦ НО средства защиты информации должны быть подчинены системам централизованного управления серверного сегмента АИС МФЦ НО.  **Требования по техническому обучению подрядчиком персонала заказчика на подготовленных по результатам работ объектах:**  Подрядчик должен провести инструктаж персонала МАУ МФЦ по вопросам эксплуатации и администрирования программно-технических средств, использования средств защиты информации, криптографических средств и т.п. а также передать Заказчику эксплуатационную документацию от разработчиков средств защиты.  **Формы, характер и периодичность отчетов о ходе выполнения работ. Контроль качества и соблюдения сроков выполнения работ, определение соответствия выполняемых работ потребностям заказчика:**  Поставщик по результатам выполненных работ должен предоставить Заказчику комплект документов, необходимых для эксплуатации системы и отражающих текущее состояние системы при ее сдаче в постоянную эксплуатацию.  Перечень документов на систему должен соответствовать номенклатуре, приведенной в ГОСТ 34.201-89, объему документов по РД-50-34-698-90 и содержать документы в соответствии с настоящим техническим заданием.  Документация предоставляется Заказчику на бумажных и электронных носителях.  Бумажная копия комплекта документации передается в 1-м экземпляре.  Электронная копия комплекта документации передается на CD-R (DVD R) диске в 1-м экземпляре. Диск должен быть защищен от записи, иметь этикетку (подпись) с указанием изготовителя, даты изготовления, название комплекта. В корневом каталоге диска должен находиться файл содержания.  Электронные файлы проектной документации должны быть представлены в формате \*.pdf, либо в форматах с возможностью чтения в режиме просмотра средствами MS Office 2003/2007/2010/2013 в ОС Windows.  **Порядок сдачи и приемки результатов работ:**  Испытания представляют собой процесс проверки выполнения заданных функций системы, выявления и устранения недостатков в программном обеспечении, оборудовании и документации. Для проверки выполнения заданных функций системы устанавливаются следующие виды испытаний:  − предварительные испытания;  − опытная эксплуатация;  − приемочные испытания;  − аттестация системы.  Предварительные испытания системы проводят для определения ее работоспособности и решения вопроса о возможности приемки ее в опытную эксплуатацию. Предварительные испытания выполняются после проведения Исполнителем отладки и тестирования поставляемых программных и технических средств системы и представления им соответствующих документов об их готовности к испытаниям, а также после ознакомления персонала системы с документацией.  Согласование и утверждение приемочной документации выполняется в соответствии с внутренним порядком согласования и утверждения документов организации-Заказчика.  Опытную эксплуатацию системы проводят с целью определения фактических значений количественных и качественных характеристик системы и готовности персонала к работе в условиях функционирования системы, определения фактической эффективности системы, корректировки (при необходимости) документации.  Приемочные испытания системы проводят для определения соответствия ее техническому заданию, оценки качества опытной эксплуатации и решения вопроса о возможности приемки системы в постоянную эксплуатацию. Приемочным испытаниям системы должна предшествовать ее опытная эксплуатация на объекте. Испытания проводятся на технических средствах Заказчика. Допускается использовать технические средства, находящиеся на момент проверки в эксплуатации. Работы по проведению испытаний не должны оказывать влияния на функционирование серверного сегмента АИС МФЦ НО.  В соответствии с требованиями приказа ФСТЭК России от 11.02.2013 № 17 испытания проводят на стадии «Внедрение системы защиты информации информационных систем» с целью проверки соответствия создаваемой системы требованиям технического задания и на стадии «Аттестационные испытания» с целью подтверждения соответствия системы требованиям по защите информации.  Аттестация информационной системы организуется Заказчиком и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие клиентского сегмента АИС МФЦ НО требованиям по защите информации.  В качестве исходных данных, необходимых для аттестации информационной системы, используются: модели угроз безопасности информации, акт(ы) классификации информационной системы и определения требуемых уровней защищенности обрабатываемых в клиентском сегменте АИС МФЦ НО персональных данных, техническое задание на создание клиентского сегмента СЗПД, проектная и эксплуатационная документация на систему защиты клиентского сегмента АИС МФЦ НО, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей информационной системы, материалы предварительных и приемочных испытаний системы защиты информации информационной системы.  Аттестация информационной системы проводится в соответствии с программой и методиками аттестационных испытаний до начала обработки информации, подлежащей защите в информационной системе. Для проведения аттестации информационных систем применяются национальные стандарты, а также методические документы, разработанные и утвержденные  ФСТЭК России. До проведения аттестационных испытаний программа и методики аттестационных испытаний должны быть согласована с организацией, выдавшей аттестат соответствия на серверный сегмент АИС МФЦ НО.  По результатам аттестационных испытаний оформляются протоколы аттестационных испытаний, заключение о соответствии клиентского сегмента требованиям по защите информации и аттестаты соответствия (в случае положительных результатов аттестационных испытаний).  **Требования по передаче заказчику технических и иных документов по завершению и сдаче работ:**  Подрядчик передает Заказчику следующий комплект документации:  **Требования к составу комплектов проектов внутренних организационно-распорядительных документов.**  Комплект проектов внутренних организационно-распорядительных документов, регулирующих вопросы защиты персональных данных в отношении клиентского сегмента АИС МФЦ НО, соответственно должен включать:  − приказ (форма) о проведении работ по защите персональных данных;  − проект приказа о назначении ответственного(ых) за организацию обработки и защиты персональных данных;  − перечень персональных данных (копия утвержденного документа по серверному сегменту АИС МФЦ НО);  − акт классификации АИС МФЦ НО (копия утвержденного документа по серверному сегменту АИС МФЦ НО);  − модель угроз безопасности персональным данным (копия утвержденного документа по серверному сегменту АИС МФЦ НО);  − перечень адаптированных базовых мер (копия утвержденного документа по серверному сегменту АИС МФЦ НО);  − техническое задание на систему защиты клиентского сегмента АИС МФЦ НО (копия утвержденного документа по серверному сегменту АИС МФЦ НО);  − план мероприятий по созданию и эксплуатации системы защиты персональных данных в клиентском сегменте АИС МФЦ НО.  − положение по обработке и защите персональных данных (копия утвержденного документа по серверному сегменту АИС МФЦ НО);  − приказ(форма) о назначении ответственных;  − приказ(форма) о допуске сотрудников;  − инструкции:  а) инструкция администратора системы;  б) инструкция пользователя;  − проекты(формы) журналов:  в) журнал учета средств защиты информации;  г) журнал выдачи идентификаторов;  д) журнал проведения периодического контроля(проверок);  е) журнал ознакомления с ОРД и инструктажа;  − регламенты:  ж) регламент  парольной защиты;  з) регламент доступа к ресурсам системы МФЦ;  и) регламент антивирусной защиты;  к) регламент учета СЗИ, документов и носителей;  л) регламент по модификации ПО и ТС;  м) регламент(инструкция) действий в нештатных ситуациях;  − технический паспорт ИСПДн (оригинал);  − приказ(форма) о вводе в эксплуатацию СЗПДн в ИСПДн.  **Требования к содержанию технического проекта на создание СЗПД АИС МФЦ НО**  Технический (технорабочий) проект на создание СЗПД АИС МФЦ НО должен включать:  − пояснительную записку к техническому (технорабочему) проекту;  − ведомость документов рабочего проекта;  − комплект схем;  − спецификацию программно-аппаратных средств системы защиты информации.  **Требования к содержанию эксплуатационной документации**  В состав документации должны входить документы:   1. Комплект документации на средства персональных данных клиентского сегмента АИС МФ-НО;   2. Акты приемки в опытную (промышленную) эксплуатацию клиентского сегмента АИС МФЦ НО.  **Требования к содержанию документации по аттестации**  В состав документации должны входить документы:  - программа и методика аттестационных испытаний клиентского сегмента АИС МФЦ НО;  - протоколы проведения аттестационных испытаний клиентского сегмента АИС МФЦ НО;  - заключения по результатам аттестационных испытаний клиентского сегмента АИС МФЦ НО;  - аттестат(ы) соответствия на рабочие места клиентского сегмента АИС МФЦ НО.  **К закупаемой продукции не применяется национальный режим, предусмотренный** [**ст. 14**](consultantplus://offline/ref=01521F953713F47FC44CAB93B1AB503F686BA5089D9D0508D4CFAFB86A7963C55EB9DAC75F7592DAS843I) **Федерального закона от 05.04.2013 N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд"** |
| Для создания и функционирования СЗПД Подрядчик должен передать Заказчику, выполнить работы:   1. Обследование клиентского сегмента АИС МФЦ НО 2. Разработка технического решения (проекта) системы защиты персональных данных клиентского сегмента АИС МФЦ НО 3. Разработка комплекта организационно-распорядительных документов по вопросам защиты персональных данных клиентского сегмента АИС МФЦ НО 4. Работы по установке и настройке средств защиты информации от НСД 5. Работы по установке и настройке средств криптографической защиты информации, организации защищенного взаимодействия 6. Работы по установке и настройке средств анализа защищенности 7. Аттестация клиентского сегмента АИС МФЦ НО по требования безопасности конфиденциальной информации;   Поставить, установить и настроить следующие программно-аппаратные комплексы защиты информации, совместимые по функционалу и возможности централизованного управления средствами защиты, внедренными в серверном сегменте АИС МФЦ НО:   |  |  |  | | --- | --- | --- | | **№** | **Наименование средства защиты** | **Кол-во, шт.** | |  | ПАК АМДЗ «Соболь» (сертификат ФСБ России) версии 3.0 (артикул - kb-sobol-specia-3.0 k12 v1) | не менее 5 | |  | Ключ активации сервиса прямой технической поддержки уровня "Расширенный" для ПАК "Соболь" | не менее 5 | |  | СЗИ от НСД «Dallas Lock» в. 8.0-К для подключения к серверу безопасности (в комплекте с дистрибутивом) | не менее 5 | |  | Антивирусное ПО Kapersky Endpoint Security для Бизнеса Стандартный (лицензия, 1 год) | не менее 5 | |  | Дистрибутив антивирусного ПО Kapersky MediaKIT, сертификат ФСТЭК России). | не менее 1 | |  | Аппаратный идентификатор eToken Pro Java 72К cert, сертификат ФСТЭК. | не менее 7 | |  | Комплект документации для сертифицированных электронных ключей и смарт-карт eToken eToken артикул Media-kit/CERT-1883 | не менее 1 | |  | ПАК VipNET Координатор HW100C (сеть 6387) | не менее 1 | |  | Сертификат технической поддержки VipNET координатор HW100C сроком 1 год | не менее 1 | |  | СКЗИ VipNET Client (КС3, сеть 6387) | не менее 5 | |  | Дистрибутив VipNET Client (КС3) | не менее 5 | |  | Сертификат технической поддержки VipNET Client сроком 1 год | не менее 5 | |  | Предоставление прав на использование XSpider 7.8, лицензия на 6 хостов, гарантийные обязательства в течение 1 года | не менее 1 | |

2.3. Требования к гарантийному сроку товара, работы, услуги и (или) объему предоставления гарантий его качества, к гарантийному обслуживанию товара, к расходам на эксплуатацию товара, к обязательности осуществления монтажа и наладки товара, к обучению лиц, осуществляющих использование и обслуживание товара (устанавливаются заказчиком при необходимости):

|  |
| --- |
| На стадии гарантийного сопровождения (проводится Подрядчиком) системы осуществляются следующие мероприятия:  − гарантийное обслуживание поставляемого оборудования и средств защиты информации в соответствии с гарантийными обязательствами разработчиков оборудования и средств защиты информации, но не менее 1 (одного) года;  − техническая поддержка поставляемого оборудования и средств защиты информации сроком не менее 1(одного) года, включающая:  \* обновление антивирусных и сигнатурных баз (при наличии);  \* консультации по продуктам и ответы на вопросы клиентов по электронной почте и по «горячей» телефонной линии;  \* возможность обновления версии продукта в течение срока действия технической поддержки. |
| На стадии гарантийного сопровождения (проводится Подрядчиком) системы осуществляются следующие мероприятия:  − гарантийное обслуживание поставляемого оборудования и средств защиты информации в соответствии с гарантийными обязательствами разработчиков оборудования и средств защиты информации, но не менее 1 (одного) года;  − техническая поддержка поставляемого оборудования и средств защиты информации сроком не менее 1(одного) года, включающая:  \* обновление антивирусных и сигнатурных баз (при наличии);  \* консультации по продуктам и ответы на вопросы клиентов по электронной почте и по «горячей» телефонной линии;  \* возможность обновления версии продукта в течение срока действия технической поддержки. |

1. Место выполнения работ: **Нижегородская область, р. п. Пильна, ул. Урицкого, д. 14**
2. Срок выполнения работ: в течения трех рабочих дней с момента заключения муниципального контракта.
3. Начальная (максимальная) цена контракта: **500 000 (пятьсот тысяч) рублей 00 копеек.**
4. Обоснование начальной (максимальной) цены контракта: **начальная (максимальная) цена контракта определена по методу сопоставимых цен (анализа рынка).**
5. Порядок формирования цены контракта: **цена контракта включает в себя стоимость товара, расходы на доставку (в т. ч. НДС, если облагается), сборов, таможенных пошлин и других платежей, являющихся обязательными в силу закона.**
6. Источник финансирования: средства федерального бюджета.
7. Порядок оплаты: **Оплата осуществляется в безналичном порядке. Авансовые платежи не предусмотрены. Оплату выполненной работы заказчик производит в течение 5 (пяти) рабочих дней с даты подписания акта выполненных работ по Контракту.**
8. Информация о валюте, используемой для формирования цены контракта и расчетов с исполнителем: **российский рубль.**
9. Информация о возможности заказчика изменить условия контракта в соответствии с ч. 1 ст. 95 Федерального закона от 05.04.2013 г. № 44-ФЗ: **предусмотрено.**
10. Информация о возможности одностороннего отказа от исполнения контракта: **предусмотрено.**
11. Информация о возможности заказчика заключить контракт с несколькими участниками закупки (*в случаях, предусмотренных ч. 10 ст. 34 Федерального закона от 05.04.2013 г. № 44-ФЗ*): **не предусмотрено.**
12. Требование о соответствии поставляемого товара изображению товара, образцу или макету товара *(выбрать, подчеркнуть)*, на поставку которого осуществляется закупка: **не предусмотрено.**

# Директор МАУ «МФЦ Пильнинского района»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Сурханова Н.Н./

# М. п.