ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на оказание услуги по защищенной передаче данных с актуализацией криптографического оборудования ГАУЗ «Медицинский информационно-аналитический центр» Брянской области с целью бесперебойного функционирования регионального сегмента ЕГИСЗ Брянской области.

1. Общие сведения.

1.1.Наименование услуги

Защищенная передача данных с актуализацией криптографического оборудования «Программно-аппаратный комплекс (ПАК) VipNet координатор HW1000»(далее - СКЗИ) и программного обеспечения ViPNet Administrator (КС2) для ГАУЗ «Медицинский информационно-аналитический центр» Брянской области (далее – Заказчика) с целью бесперебойного функционирования регионального сегмента Единой государственной информационной системы (ЕГИСЗ) Брянской области.

1.2.Требования к участникам размещения заказа

1.2.1.Исполнитель должен иметь:

1.2.1.1.Лицензию РОСКОМНАДЗОРА на оказание телематических услуг связи;

1.2.1.2.Лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации;

1.2.1.3.Лицензию 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 (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). Указанная лицензия должна содержать следующие виды работ:

1.2.1.3.1.Монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств или монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств информационных систем или монтаж, установка (инсталляция), наладка шифровальных (криптографических) средств телекоммуникационных систем;

1.2.1.3.2.Передача шифровальных (криптографических) средств или передача защищенных с использованием шифровальных (криптографических) средств информационных систем или передача защищенных с использованием шифровальных (криптографических) средств телекоммуникационных систем;

1.2.1.3.3.Предоставление услуг по шифрованию информации, не содержащей сведений, составляющих государственную тайну, с использованием шифровальных (криптографических) средств в интересах юридических и физических лиц, а также индивидуальных предпринимателей.

Для подтверждения этого требования Исполнитель должен предоставить заверенные копии всех вышеперечисленных лицензий.

1.3. Термины и определения

1.3.1. **РС ЕГИСЗ –** региональный сегмент (РС) Единой государственной информационной системы здравоохранения (ЕГИСЗ) Брянской области - совокупность регулярно выполняемых в режиме промышленной либо опытной эксплуатации организационно-технических и программно-технических мероприятий, обеспечивающих информационную поддержку методического и организационного обеспечения деятельности системы здравоохранения Брянской области и взаимодействие с федеральным сегментом ЕГИСЗ.

1.3.2.**Участники РС ЕГИСЗ** – медицинские организации, подведомственные департаменту здравоохранения Брянской области, обеспечивающие работу пользователей на уровне прикладных компонентов и инфраструктуры РС ЕГИСЗ Брянской области, находящейся в их ведении.

1.3.3.**ЗКСПД** - защищенная корпоративная сеть передачи данных.

1.3.4.**СКЗИ** – средство криптографической защиты информации.

1.3.5.**Инфраструктура ЗКСПД** - общесистемный технологический компонент, предназначенный для обеспечения защищенного процессного взаимодействия между прикладными компонентами РС ЕГИСЗ.

2. Цели и задачи

2.1. Целями являются:

2.1.1.Обеспечение бесперебойной работы инфраструктуры ЗКСПД на стороне Заказчика с обеспечением криптографической защиты передаваемой информации (данных);

2.1.2.Реализация «Концепции создания единой государственной информационной системы в сфере здравоохранения» в части построения и функционирование ЗКСПД в полном соответствии с методическими рекомендациями медицинским организациям по организации криптографической защиты каналов при взаимодействии в рамках Единой государственной информационной системы в сфере здравоохранения, подготовленных Министерством здравоохранения Российской Федерации.

2.1.3.Повышение эффективности информационного обмена в сфере здравоохранения;

2.1.4.Улучшение качества обслуживания населения.

2.2. Для реализации поставленных целей необходимо решить следующие задачи:

2.2.1. Осуществить передачу неисключительных лицензионных прав на обновление для актуализации предоставленного Заказчиком СКЗИ, а именно:

2.2.1.1.Провести обновление СКЗИ до актуальной версии, только для версии, имеющей действующий сертификат соответствия ФСБ России. Установка несертифицированного обновления для СКЗИ происходит только по согласованию с Заказчиком.

2.2.1.2.Выполнить конфигурирование СКЗИ для обеспечения его корректного функционирования. Всю необходимую информацию для конфигурирования СКЗИ Заказчик обязуется предоставить по требованию Исполнителю в полном объеме.

2.2.1.3.Подготовить и представить Заказчику следующий комплект документов:

-сертификат технической поддержки (пункт 2.2.1.4.);

-акт установки и ввода в эксплуатацию средства СКЗИ;

-комплект эксплуатационной документации (описание системы, руководство пользователя системы) и дистрибутив СКЗИ;

-новые сертификаты ФСТЭК и ФСБ на СКЗИ;

-формуляр на СКЗИ.

2.2.1.4. Требования к сертификату технической поддержки (далее – Сертификат ТП).

2.2.1.4.1.Сертификат ТП – документ, оформленный в бумажном виде, содержащий информацию о полном наименовании Заказчика, уникальном идентификационном номере сертификата, полном списке продуктов с указанием версии, на которые распространяется данный Сертификат ТП, и подтверждающий право Заказчика на получение от Исполнителя технической поддержки (ТП) с момента начала оказания услуги.

2.2.1.4.2.Условия ТП должны распространяться на указанные в Сертификате ТП СКЗИ и регламентировать порядок действий Исполнителя, сроки и иные моменты, связанные с предоставлением ТП.

2.2.1.4.3.В период действия Сертификата ТП Исполнитель должен оказывать Заказчику телефонные консультации, консультации с использованием электронной почты, а так же иными согласованным с Заказчиком способами по устранению неисправностей, связанных с оказанием услуги.

2.2.2. Выполнить настройку СКЗИ Заказчика, перечисленных и размещенных по адресам, приведенным в Таблице 1.

2.2.3. Подключить СКЗИ Заказчика, перечисленные и размещенные по адресам, которые приведены в Таблице 1, к инфраструктуре ЗКСПД, в соответствии с п.3.

2.3. Критерии достижения цели

В качестве основных критериев при достижении целей, определенных в **п. 2.1.**, принимаются показатели бесперебойной передачи шифрованного трафика между информационными системами Заказчика и хотя бы одного из участников РС ЕГИСЗ.

2.4. Качество услуг.

Качество услуг определяется соответствием требованиям нормативных документов указанных в п.4 настоящего технического задания.

3. Требования для подключения к инфраструктуре ЗКСПД

Канал связи для подключения к инфраструктуре ЗКСПД должен обеспечивать круглосуточную бесперебойную возможность осуществления соединений между СКЗИ Заказчика и СКЗИ хотя бы одного из участников РС ЕГИСЗ с целью передачи шифрованной информации со скоростью не менее 10 Мб/с.

Подключение СКЗИ Заказчика к инфраструктуре ЗКСПД и предоставление возможности передачи трафика осуществляется с момента получения Исполнителем письменного уведомления от Заказчика.

4. Выполнение требований законодательства РФ при оказании услуг

Предоставляемая услуга должна соответствовать законодательству Российской Федерации в области защиты информации и удовлетворять требованиям следующих нормативно-правовых документов РФ:

-Федеральный закон РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 13.07.2015);

-Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» (ред. от 30.12.2015);

-Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

-Приказ Министерства здравоохранения и социального развития Российской Федерации от 28.04.2011 № 364 «Об утверждении Концепции создания единой государственной информационной системы в сфере здравоохранения» (ред. от 12.04.2012);Концепция региональной информатизации (утв. распоряжением Правительства РФ от 29.12.2014 № 2769-р);

- Приказ Федерального Фонда обязательного медицинского страхования от 07.04.2011 №79 «Об утверждении общих принципов построения и функционирования информационных систем и порядка информационного взаимодействия в сфере обязательного медицинского страхования» (ред. от 26.12.2013);

-Методические рекомендации по составу и техническим требованиям к сетевому телекоммуникационному оборудованию учреждений системы здравоохранения для регионального уровня единой государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним, обязательные для создания в 2011-2012 годах в рамках реализации региональных программ модернизации здравоохранения (опубликованы на официальном сайте Минздравсоцразвития РФ 29.06.2011);

-Методические рекомендации по порядку организации работ по созданию субъектом Российской Федерации в 2011-2012 годах регионального фрагмента единой государственной информационной системы в сфере здравоохранения (опубликованы на официальном сайте Минздравсоцразвития РФ 29.06.2011);

-Методические рекомендации по составу, создаваемых в 2011 - 2012 годах в рамках реализации региональных программ модернизации здравоохранения, прикладных компонентов регионального уровня единой

государственной информационной системы в сфере здравоохранения, а также функциональные требования к ним (опубликованы на официальном сайте Минздравсоцразвития РФ 29.06.2011);

-Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. от 21.07.2014);

-Приказ ФСТЭК РФ 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;

-Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости, включая «Методические рекомендации по составлению Частной модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений здравоохранения, социальной сферы, труда и занятости» (утв. Минздравсоцразвития РФ23 Л 2.2009);

-Методические рекомендации по проведению в 2011 - 2012 годах работ по информационной безопасности для регионального уровня единой государственной информационной системы в сфере здравоохранения (опубликованы на официальном сайте Минздравсоцразвития РФ 29.06.2011);

-Приказ ФСБ России от 10.07.2014 №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»;

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

Таблица 1

№ п/п	Наименование СКЗИ, адрес размещения	Кол-во СКЗИ
1.	«Программно-аппаратный комплекс (ПАК) VipNet координатор HW1000», 241050, г. Брянск, ул. Луначарского , 9а	3
2.	«Программное обеспечение ViPNet Administrator (КС2)», 241050, г. Брянск, ул. Луначарского , 9а	1