

Протокол № ЗК-ДБ-89/1
вскрытия конвертов
с Заявками на участие в запросе котировок
(ОАО «Курорты Северного Кавказа»)

г. Москва

21 января 2013 г.

1. Наименование предмета запроса котировок: Заключение договора на выполнение работ по разработке системы защиты персональных данных при их обработке в информационных системах ОАО «Курорты Северного Кавказа».

2. Заказчик: Открытое акционерное общество «Курорты Северного Кавказа» (далее - ОАО «Курорты Северного Кавказа», ИНН 2632100740).

3. На процедуре вскрытия конвертов присутствовали:
 Вязовой Валерий Валерьевич, Левин Дмитрий Борисович, Топорков Сергей Владимирович, Канунников Денис Викторович, Фурин Сергей Александрович, Токарев Игорь Александрович.
 Отсутствовал: Горчев Олег Сергеевич.

На заседание Единой комиссии в качестве эксперта был приглашен: эксперт отдела информационной безопасности — Славгородский Андрей Викторович.

Кворум имеется, заседание Единой комиссии правомочно.

4. Процедура вскрытия конвертов с Заявками состоялась в 16:00 (мск) 21 января 2013 года по адресу: Российская Федерация, 119034, г. Москва, ул. Пречистенка, д. 38.

5. Извещение о проведении запроса котировок было размещено на сайте <http://www.ncsc.ru> в сети Интернет в 10:00 (мск) 29 декабря 2012 года № ЗК-ДБ-89.

6. Сведения о существенных условиях договора:

Предмет договора	Выполнение работ по разработке системы защиты персональных данных при их обработке в информационных системах ОАО «Курорты Северного Кавказа».
Максимальная цена договора	834 746 (Восемьсот тридцать четыре тысячи семьсот сорок шесть) рублей, без учета НДС. В цену договора включены все расходы исполнителя на уплату сборов, налогов (помимо НДС) и иных обязательных платежей, и является окончательной.
Наименование, перечень выполняемых работ	В соответствии с Техническим заданием (Приложение № 1) к настоящему протоколу.
Место выполнения работ	Российская Федерация, г. Москва.
Условия оплаты	Оплата осуществляется в два этапа, 30% (Тридцать) процентов в виде аванса в течение 5 (Пяти) банковских дней со дня подписания договора и 70% (Семьдесят) процентов по факту выполнения работ в течение 5 (Пяти) банковских дней на основании подписанного Акта выполненных работ.

Срок выполнения работ	не более 67 (Шестьдесят семь) календарных дней.
Финансирование	Собственные средства ОАО «Курорты Северного Кавказа»

7. До окончания указанного в извещении о проведении запроса котировок срока подачи котировочных заявок 16:00 (мск) 21 января 2013 года поступило 4 (Четыре) котировочные заявки на бумажном носителе.

8. Сведения об участниках размещения заказа, подавших котировочные заявки:

Регистрационный номер заявки участника размещения заказа	Наименование участника размещения заказа	Адрес местонахождения участника
№ ВП-13-0080 от 21 января 2013 года 13:35 (мск)	ООО «Безополис-Пато» (ИНН 7715202270)	127106, г. Москва, Алтуфьевское ш., д.27 Тел.:8-499-903-00-92
№ ВП-13-0081 от 21 января 2013 года 14:00 (мск)	ЗАО «КРОК инкорпорейтед» (ИНН 7701004101)	105082, г. Москва, ул. Большая почтовая, дом 26В, стр.2 Тел.:8-495-974-22-74
№ ВП-13-0082 от 21 января 2013 года 14:15 (мск)	ЗАО «ЛЕТА» (ИНН 7723719400)	109129, г. Москва, ул. 8-я Текстильщиков, д.11, стр.2 8-495-921-14-10
№ ВП-13-0083 от 21 января 2013 года 15:20 (мск)	ЗАО «Практика Безопасности» (ИНН 7722639014)	125315, г. Москва, ул. Часовая, д.28, корп.4 8-495-228-46-49

9. Информация по процедуре вскрытия:

Вскрытие конвертов с Заявками на участие в запросе котировок произошло в очередности поступления Заявок.

9.1 Вскрытие конверта с Заявкой на участие в запросе котировок, представленного ООО «Безополис-Пато»:

- Котировочная Заявка представлена **ООО «Безополис-Пато»**, почтовый адрес: 127106, г. Москва, Алтуфьевское ш., д.27, ИНН 7715202270;
- конверт с Заявкой запакован;
- листы Заявки не прошиты;
- стоимость выполнения работ составляет 550 000 (Пятьсот пятьдесят тысяч) рублей, без учета НДС.

9.2 Вскрытие конверта с Заявкой на участие в запросе котировок, представленного ЗАО «КРОК инкорпорейтед»:

- Котировочная Заявка представлена **ЗАО «КРОК инкорпорейтед»**, почтовый адрес: 111033, г. Москва, ул. Волочаевская, д.5, к.1, ИНН 7701004101;
- конверт с Заявкой запакован;
- все листы Заявки прошиты;
- стоимость выполнения работ составляет 793 008,48 (Семьсот девяносто три тысячи восемь) рублей 48 копеек, без учета НДС.

9.3 Вскрытие конверта с Заявкой на участие в запросе котировок, представленного ЗАО «ЛЕТА»:

- Котировочная Заявка представлена ЗАО «ЛЕТА», почтовый адрес: 109129, г. Москва, ул. 8-я Текстильщиков, д.11, стр.2, ИНН 7723719400;
- конверт с Заявкой запакован;
- все листы Заявки прошиты;
- стоимость выполнения работ составляет 820 000 (Восемьсот двадцать тысяч) рублей, без учета НДС.

9.4 **Вскрытие конверта с Заявкой на участие в запросе котировок, представленного ЗАО «Практика Безопасности»:**

- Котировочная Заявка представлена ЗАО «Практика Безопасности», почтовый адрес: 117587, г. Москва, Варшавское ш.. д.118, корп. 1, БЦ «Варшавка SKY», ИНН 7722639014;
- конверт с Заявкой запакован;
- все листы Заявки прошиты;
- стоимость выполнения работ составляет 665 000 (Шестьсот шестьдесят пять тысяч) рублей, без учета НДС.

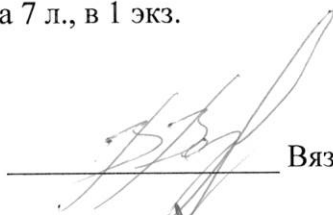
10. Настоящий протокол подлежит хранению в течение трех лет.

11. Настоящий протокол подлежит размещению на официальном сайте Заказчика <http://www.ncrc.ru> в сети Интернет.

Приложение:

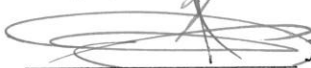
1. Техническое задание – на 7 л., в 1 экз.

Член комиссии



Вязовой Валерий Валерьевич

Член комиссии



Левин Дмитрий Борисович

Член комиссии



Топорков Сергей Владимирович

Член комиссии



Канунников Денис Викторович

Член комиссии



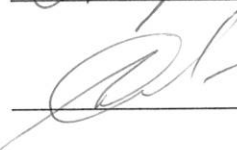
Фурин Сергей Александрович

Секретарь комиссии



Токарев Игорь Александрович

Эксперт



Славгородский Андрей Викторович

Техническое задание

Общие сведения

- 1.1. Наименование разработки: Разработка системы защиты персональных данных при их обработке в информационных системах ОАО «Курорты Северного Кавказа»
- 1.2. Наименование Заказчика: ОАО «Курорты Северного Кавказа».
- 1.3. Наименование Подрядчика.
- 1.4. Разработка ведется на основании данного технического задания, действующего законодательства в области защиты персональных данных (далее – ПДн), в том числе:
 - Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
 - Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
 - Нормативные правовые акты ФСТЭК России, ФСБ России, разработанные во исполнение Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
 - Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Руководящий документ ФСТЭК России. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утвержден Заместителем директора ФСТЭК России 15.02.2008;
 - Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;
 - ГОСТ 34.201-89 «Виды, комплектность и обозначения документов при создании автоматизированных систем»;
 - ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания»;
 - ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».
- 1.5. Сроки выполнения работ: не более 67 (Шестьдесят семь) календарных дней.
- 1.6. Порядок финансирования работ: оплата осуществляется в два этапа, 30% (Тридцать) процентов в виде аванса в течение 5 (Пяти) банковских дней со дня подписания договора и 70% (Семьдесят) процентов по факту выполнения работ в течение 5 (Пяти) банковских дней на основании подписанного Акта выполненных работ.
- 1.7. Порядок оформления и предъявления Заказчику результатов работ: по результатам работ по каждому этапу работ Подрядчик предоставляет Заказчику отчетные документы в соответствии с разделом 5 настоящего документа.

Назначение и цели

2.1. Назначение:

- проведение комплекса мероприятий по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных (далее – ИСПДн);

– определение типа угроз безопасности персональных данных, актуальных для ИСПДн (под актуальными угрозами безопасности ПДн понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к ПДн при их обработке в информационной системе, результатом, которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение ПДн, а также иные неправомерные действия);

– разработка требований к системе защиты персональных данных (далее – СЗПДн) призванной обеспечить необходимый уровень защищенности ПДн при их обработке в ИСПДн.

2.2. Цели разработки СЗПДн:

- провести обследование процессов обработки ПДн и ИСПДн Заказчика, выполнить оценку степени выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и подзаконных нормативных правовых актов, а также подготовить рекомендации по составу необходимых для проведения мероприятий по организации корректной обработки и защиты ПДн;
- выполнить экспертную оценку организационно-распорядительной документации, обеспечивающей выполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и подзаконных нормативных правовых актов;
- дать рекомендации по приведению организационно-распорядительной документации в соответствие требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», руководящих и подзаконных нормативных правовых актов;
- разработать техническое задание на создание СЗПДн, соответствующее требованиям руководящих и нормативно-методических документов ФСТЭК России и ФСБ России в области защиты информации;
- разработать технико-экономическое обоснование создания СЗПДн

Характеристика объекта защиты

3.1. Объектом защиты являются ПДн, обрабатываемые в ИСПДн.

3.2. Обработка ПДн в ИСПДн осуществляется с использованием средств автоматизации.

3.3. ИСПДн включает в свой состав:

- локальную вычислительную сеть;
- автоматизированные рабочие места;
- серверное оборудование.

3.4. ИСПДн имеет подключение к сетям связи общего пользования и сетям международного информационного обмена.

3.5. По режиму обработки ПДн ИСПДн является многопользовательской.

3.6. Все технические средства ИСПДн находятся на территории Российской Федерации.

Требования к разрабатываемой СЗПДн

4.1. Разрабатываемая СЗПДн должна представлять собой единый структурный комплекс, объединяющий подсистемы информационной безопасности различного назначения:

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

- подсистема обеспечения безопасного межсетевого взаимодействия;
- подсистема антивирусной защиты;
- подсистема обнаружения вторжений;
- подсистема анализа защищенности;
- подсистема резервного копирования;
- подсистема криптографической защиты.

4.2. При разработке СЗПДн должны учитываться меры по защите ПДн, реализованные Заказчиком на момент проведения работ, а также особенности бизнес-процессов, реализующих основные виды деятельности Заказчика.

4.3. Компоненты СЗПДн должны обеспечивать возможность взаимодействия с элементами существующей ИТ-инфраструктуры Заказчика.

4.4. Компоненты СЗПДн не должны снижать производительность существующих у Заказчика информационных систем.

4.5. Разрабатываемая СЗПДн должна обеспечивать:

- возможность модернизации путем замены технического и/или программного обеспечения;
- штатное функционирование в случае одновременной работы всех пользователей Заказчика;
- восстановление настроек при сбоях в работе силами штатного обслуживающего персонала в срок не более 12 часов.

4.6. Целевое назначение СЗПДн должно сохраняться на протяжении всего срока ее эксплуатации. Срок эксплуатации СЗПДн определяется сроком устойчивой работы технических средств вычислительных комплексов, своевременным проведением работ по замене (обновлению) технических средств, по сопровождению и обновлению программного обеспечения системы (в рамках гарантийного и послегарантийного обслуживания) и его модернизации.

4.7. В составе СЗПДн должно использоваться только лицензионное программное обеспечение, кроме того должны применяться только серийно выпускаемые программные и технические средства.

4.8. В составе СЗПДн должны использоваться средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия, что подтверждается сертификатами соответствия ФСТЭК России и/или ФСБ России.

4.9. При выборе методов и способов защиты информации, входящих в состав СЗПДн, Подрядчик должен руководствоваться требованиями Постановления Правительства РФ от 01.11.2012 № 1119 и нормативных правовых актов, принятых ФСТЭК России и ФСБ России во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

4.10. Выбранные методы и способы защиты информации, в составе разрабатываемой СЗПДн, должны обеспечивать нейтрализацию актуальных угроз безопасности ПДн при их обработке в ИСПДн, которые предварительно должны быть определены Подрядчиком и зафиксированы в документе «Модель угроз безопасности ПДн при их обработке в ИСПДн» (подробнее в разделе 5 настоящего документа).

4.11. Разрабатываемая СЗПДн должна обеспечивать:

- реализацию разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе;
- разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;
- идентификацию и проверку подлинности пользователей и обслуживающего

персонала при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

- регистрацию действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;
- локальный контроль на рабочих местах и серверах;
- анализ сетевого трафика;
- возможность контроля подключаемых внешних устройств;
- ограничение доступа в зависимости от типа съемного носителя;
- возможность разрешать копирование только на доверенные носители;
- анализ событий, зафиксированных системой;
- контроль целостности программных средств СЗПДн, обрабатываемой информации, а также неизменность программной среды
- резервирование технических средств, дублирование массивов и носителей информации;
- предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок;
- межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;
- обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;
- анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);
- защиту информации при ее передаче по каналам связи;
- использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;
- централизованное управление.

Состав и содержание работ

5.1. Требования к составу работ

5.1.1. Выполнение работ по разработке СЗПДн должно предполагать их разбиение на последовательные этапы. План работ должен состоять из следующих этапов:

- Обследование процессов обработки ПДн и ИСПДн Заказчика, изучение организационно-распорядительной документации Заказчика, анализ собранной информации и разработка отчетной документации;
- Подготовка рекомендаций по приведению организационно-распорядительной документации Заказчика в соответствие требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и подзаконных нормативных правовых актов;
- Разработка Технического задания на создание СЗПДн;
- Разработка Техничко-экономического обоснования создания СЗПДн.

5.2. Требования к содержанию и результатам работ этапа «Обследование процессов обработки ПДн и ИСПДн Заказчика, изучение организационно-распорядительной документации Заказчика, анализ собранной информации и разработка отчетной документации»

5.2.1. Сбор информации, необходимой для подготовки отчетных документов Подрядчиком, в том числе об организационной структуре Заказчика, о процессах обработки ПДн, особенностях ИТ-инфраструктуры, а также о применяемых Заказчиком мерах и средствах защиты информации, может осуществляться следующими способами:

- анкетирование;
- изучение внутренней нормативной документации Заказчика;
- интервьюирование специалистов Заказчика, задействованных в обработке ПДн;
- интервьюирование специалистов Заказчика, отвечающих за контроль и обеспечение ИТ-инфраструктуры и информационной безопасности;
- выборочные проверки средств обработки и обеспечения безопасности ПДн.

5.2.2. Вся полученная в ходе интервьюирования информация должна быть документально зафиксирована в протоколах.

5.2.3. Перечень внутренних нормативных документов Заказчика, используемых при оценке степени выполнения требований законодательства РФ в части обработки и обеспечения безопасности ПДн, должен быть зафиксирован в Отчете.

5.2.4. Отчет о результатах обследования процессов обработки ПДн должен включать в себя:

- результаты проведенных мероприятий по обследованию процессов обработки ПДн, информационных систем, используемых для обработки ПДн, и текущих мероприятий по защите, предпринимаемых Заказчиком;

- заключение о степени выполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», подзаконных актов и руководящих документов ФСТЭК России и ФСБ России;

- рекомендации по составу необходимых для проведения мероприятий по организации корректной обработки и защиты ПДн и по приведению процессов обработки ПДн в ИСПДн в соответствие требованиям законодательства РФ.

5.2.5. Подрядчиком должны быть разработаны следующие проекты документов (в качестве приложений к Отчету или в виде самостоятельных документов):

- Перечень ПДн;
- Перечень подразделений и лиц, допущенных к работе с ПДн;
- Перечень ИСПДн;
- Модели угроз безопасности ПДн при их обработке в ИСПДн обосновывающие выбор уровня защищенности ИСПДн;
- Акты определения уровней защищенности ПДн при их обработке в ИСПДн;
- Уведомление уполномоченного органа по защите прав субъектов ПДн об обработке ПДн (при необходимости).

5.2.6. Документ «Перечень ПДн» должен содержать полный перечень ПДн, обрабатываемых Заказчиком, с указанием категорий субъектов ПДн, содержания сведений, сроков хранения, целей и правовых оснований обработки ПДн.

5.2.7. В документе «Перечень подразделений и лиц, допущенных к работе с ПДн» должны быть указаны все структурные подразделения и должности работников, задействованных в процессах обработки ПДн, с указанием категорий субъектов, к ПДн которых они допущены.

5.2.8. В документе «Перечень ИСПДн» должны быть зафиксированы все ИСПДн Заказчика с указанием типов угроз безопасности ПДн, актуальных для ИСПДн, и уровней защищенности ПДн. Перечень и состав выделяемых ИСПДн предварительно согласовывается с Заказчиком.

5.2.9. Анализ угроз безопасности ПДн при их обработке в ИСПДн и оценка актуальности угроз безопасности осуществляется на основании методик, приведенных в руководящих документах ФСТЭК России и ФСБ России. Результаты проведенного анализа и перечень актуальных угроз безопасности ПДн фиксируются в документе «Модель угроз безопасности ПДн при их обработке в ИСПДн».

5.2.10. Уровень защищенности ИСПДн определяется на основании анализа и оценки угроз безопасности ПДн при их обработке в ИСПДн, в соответствии с

характеристиками ИСПДн и с учетом ее особенностей. Результаты определения уровня защищенности ПДн фиксируются в документе «Акт определения уровней защищенности ПДн при их обработке в ИСПДн».

5.3. Требования к содержанию и результатам работ этапа «Подготовка рекомендаций по приведению организационно-распорядительной документации Заказчика в соответствие требованиям Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и подзаконных нормативных правовых актов»

5.3.1. Подрядчиком подготавливаются рекомендации по приведению организационно-распорядительной документации Заказчика в соответствие всем требованиям законодательства, предъявляемым к документационному обеспечению операторов ПДн.

5.3.2. В состав рекомендаций по организационно-распорядительной документации должны быть включены следующие документы:

- Политика обработки и обеспечения безопасности ПДн (разрабатывается в соответствии с п.2 ст.18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», предназначается для размещения в открытом доступе);
- Приказ об обеспечении безопасности обрабатываемых ПДн (форма приказа должна предполагать ввод в действие комплекта разработанной организационно-распорядительной документации, а также распределение ответственности за обработку и обеспечение безопасности ПДн между работниками Заказчика)
- Положение об обработке ПДн (является основным документом, определяющим правила обработки ПДн);
- Регламент обеспечения безопасности ПДн (в документе должны быть определены требования и порядок проведения мероприятий, направленных на обеспечение безопасности ПДн);
- Регламент использования средств защиты информации ПДн (в документе должен быть закреплён порядок использования средств защиты информации подразделениями Заказчика в соответствии с полномочиями);
- Регламент взаимодействия с субъектами ПДн (в документе должен быть закреплён порядок действий работников Заказчика при взаимодействии с субъектами ПДн);
- Инструкция работника по правилам обработки и обеспечения безопасности ПДн (документ должен объединять в себе все правила обработки и защиты ПДн для конечных пользователей).

5.4. Требования к содержанию и результатам работ этапа «Разработка Технического задания на создание СЗПДн»

5.4.1. Подрядчиком разрабатывается Техническое задание на создание СЗПДн, в котором определяются требования к СЗПДн Заказчика в целом и к ее отдельным подсистемам.

5.4.2. При разработке Технического задания на создание СЗПДн Подрядчиком, в том числе, должны быть учтены требования, указанные в разделе 4 настоящего документа.

5.4.3. Техническим заданием должна быть предусмотрена разработка частных технических заданий на подсистемы СЗПДн на этапе проектирования по согласованию с Заказчиком.

5.5. Требования к содержанию и результатам работ этапа «Разработка Технико-экономического обоснования создания СЗПДн»

5.5.1. Подрядчиком разрабатывается Технико-экономическое обоснование создания СЗПДн.

5.5.2. Техничко-экономическое обоснование создания СЗПДн должно содержать описание проектного решения по созданию СЗПДн, перечень предлагаемых к внедрению средств защиты информации, а также предварительный расчет стоимости предлагаемого решения.

Порядок контроля и приемки работ

6.1. Подрядчик должен письменно информировать Заказчика о готовности к сдаче результатов работ и предоставить комплект необходимой документации.

Требования к документированию

7.1. При разработке документации должны учитываться требования ГОСТ 34 серии, в частности:

- ГОСТ 34.601-90. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
- ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплексность и обозначение документов при создании автоматизированных систем.
- РД 50-34.698-90. Методические указания. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.

7.2. Комплект документации по проекту представляется Заказчику на бумажном носителе и в электронном виде в одном экземпляре.

7.3. Документация в электронном виде предоставляется Заказчику в формате:

- текстовые документы – Microsoft Word;
- схемы, рисунки и другие графические материалы - Microsoft Visio или PDF.

7.4. Документация должна быть выполнена на русском языке, за исключением общепринятых названий и оригинальных наименований программно-аппаратных средств.

Требования к гарантийному обслуживанию

8.1. Требования к объему гарантии качества работ: Подрядчик должен гарантировать Заказчику, что оказанные услуги и разработанные им документы соответствуют требованиям законодательства РФ, действующего на момент исполнения Договора.

8.2. Срок предоставления гарантии на работы: срок гарантии на работы должен быть не менее 24 месяцев.