

Описание объекта закупки

Используемые сокращения и определения

ИС	Информационная система
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
ЭВМ	Электронно-вычислительная машина
ФСТЭК	Федеральная служба по техническому и экспортному контролю Российской Федерации
УПД	Универсальный передаточный документ

1. Общие положения

1.1. Настоящее описание объекта закупки разработано с целью определения состава и содержания услуг по предоставлению неисключительных (пользовательских) прав на программное обеспечение:

- для управления идентификацией и аутентификацией в информационной системе «Реестр государственных информационных систем Кемеровской области – Кузбасса»;
- для автоматизации процессов учета и регистрации государственных информационных систем Кемеровской области – Кузбасса.

1.2. Посредством программ для ЭВМ, указанных в п. 3. настоящего Описания объекта закупки, создана единая база данных, содержащая информацию об информационных системах Заказчика, в связи с чем услуги, предусмотренные настоящим государственным контрактом, в части использования эксплуатируемых программ для ЭВМ, необходимо выполнить таким образом, чтобы обработка информации в единой базе данных и в дальнейшем осуществлялась с использованием алгоритмов, протоколов и моделей эксплуатируемых программ для ЭВМ, а также была обеспечена сохранность созданной единой базы данных.

2. Цель и правовые основания оказания услуг

2.1. Целями оказания услуг являются:

- ведение реестра государственных информационных систем, а также обеспечение процессов эксплуатации информационных систем в Кемеровской области, в соответствии с требованиями закона Кемеровской области – Кузбасса от 24.12.2019 № 151-ОЗ «О государственных информационных системах Кемеровской области – Кузбасса»;
- обеспечение выполнения требований Приказа ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений» и Приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении требований состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» в рамках информационной системы «Реестр государственных информационных систем Кемеровской области – Кузбасса» в части идентификации и аутентификации пользователей.

2.2. Правовые основания для оказания услуг:

- Федеральный закон от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»;
- Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении требований состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Закон Кемеровской области – Кузбасса от 24.12.2019 № 151-ОЗ «О государственных информационных системах Кемеровской области – Кузбасса»;
- Постановление Правительства Кемеровской области - Кузбасса от 21.04.2020 № 244 «О реестре государственных информационных систем Кемеровской области – Кузбасса»;
- Р50.1.028–2001 «Рекомендации по стандартизации. Информационные технологии поддержки жизненного цикла продукции. Методология функционального моделирования».

3. Описание эксплуатируемого Заказчиком программного обеспечения для учета государственных информационных систем и подсистемы управления идентификацией и аутентификацией пользователей

3.1. Для автоматизации процессов учета государственных информационных систем используется специализированное прикладное программное обеспечение: программа для ЭВМ «Альфа». Исключительные авторские права на программу для ЭВМ «Альфа» в целом, так и все его компоненты и модули принадлежат ООО «НПЦ «КСБ», г. Чебоксары, что подтверждается соответствующим Свидетельством о государственной регистрации программ для ЭВМ (свидетельство об официальной регистрации программы для ЭВМ в реестре российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» от 02.08.2023 №2023666532, реестровая запись №20044 от 27.11.2023).

3.2. Для управления идентификацией и аутентификацией пользователей в рамках информационной системы «Реестр государственных информационных систем Кемеровской области – Кузбасса» используется сертифицированное специализированное прикладное программное обеспечение: программа для ЭВМ «Альфа-ID» (Сертификат ФСТЭК №4576 от 22.08.2022). Исключительные авторские права на программу для ЭВМ «Альфа-ID» в целом, так и все его компоненты и модули принадлежат ООО «НПЦ «КСБ», г. Чебоксары, что подтверждается соответствующим Свидетельством о государственной регистрации программ для ЭВМ (свидетельство об официальной регистрации программы для ЭВМ в реестре российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» от 30.07.2020 №202018577, реестровая запись №7111 от 07.10.2020).

4. Состав, описание и содержание услуг, требования к документированию

4.1. Исполнитель обязан оказать услуги в составе, указанном в таблице 1.

Таблица 1

№ п/п	Наименование	Отчетная документация
1.	Передача неисключительных (пользовательских) прав на программу для ЭВМ «Альфа», в соответствии с п. 4.2.	- Акт приема-передачи прав - Лицензионный/ сублицензионный договор
2.	Передача неисключительных (пользовательских) прав на программу для ЭВМ «Альфа-ID», в соответствии с п. 4.2.	- Акт приема-передачи прав - Лицензионный/ сублицензионный договор

4.2. С целью соблюдения требований ч.7 ст. 14 ФЗ № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Исполнитель обязан надлежащим образом с соблюдением требований действующего законодательства (ст. 1235 Гражданского кодекса Российской Федерации) предоставить права на использование ее компонентов (прикладного программного обеспечения), являющихся самостоятельным объектом интеллектуальной собственности, путем передачи (предоставления) Заказчику неисключительных прав на использование программы для ЭВМ «Альфа» и программы для ЭВМ «Альфа-ID», в составе, указанном в таблице 2.

Таблица 2

№ п/п	Наименование	Кол-во, шт.
1.	Неисключительные права на программу для ЭВМ «Альфа». Приложение «АльфаРеестр». Лицензия на получение обновлений к Серверной лицензии «Регион-42», (ID платформы 4204) Срок действия с 01.01.2027 по 30.09.2027	1
2.	Неисключительные права на программу для ЭВМ «Альфа». Приложение «АльфаКоннект». Лицензия на получение обновлений к Серверной лицензии «Регион-42» (до 10000 пользователей), (ID платформы 4204) Срок действия с 01.01.2027 по 30.09.2027	1
3.	Неисключительные права на программу для ЭВМ «Альфа-ID». Лицензия на получение обновлений к Серверной лицензии (до 10000 пользователей), (ID платформы 4208) Срок действия с 01.01.2027 по 30.09.2027	1

4.3. Исполнитель обязан обеспечить Заказчику в течение 9 (девяти) месяцев (с 01.01.2027 по 30.09.2027) расширенную гарантийную поддержку ЭВМ «Альфа» (далее – Специализированное ПО) в составе:

- информационная поддержка пользователей Специализированного ПО (по бесплатной «горячей» линии, e-mail, через онлайн-консультант) по вопросам эксплуатации Специализированного ПО на русском языке с понедельника по пятницу, с 8.30 до 17.30 часов по местному времени Заказчика;
- возможность получения обновлений Специализированного ПО, в том числе включающих:
 - исправление выявленных Заказчиком ошибок в работе Специализированного ПО;
 - изменения пользовательского функционала Специализированного ПО, связанные с повышением удобства использования программного обеспечения (перечень изменений, возможных к внесению, согласовывается с разработчиком Специализированного ПО в рабочем порядке);
 - изменения функциональных возможностей Специализированного ПО по письменным запросам Заказчика (перечень изменений, возможных к внесению, согласовывается с разработчиком Специализированного ПО в рабочем порядке);
 - актуализацию документации по установке и настройке Специализированного ПО;
 - обеспечение доступа к серверу обновлений Специализированного ПО;
- администрирование Специализированного ПО в части управления пользователями и организациями;
- оцифровка регламентов по подключению пользователей к ИС, не состоящим из нескольких подсистем, или к подсистемам, для 3 (трех) регламентов;
- обеспечение работоспособности Специализированного ПО, включающее:
 - удаленный мониторинг работоспособности Специализированного ПО и информирование Заказчика о нештатных ситуациях;

- переустановку Специализированного ПО, восстановление Специализированного ПО из резервной копии (предоставленной Заказчиком) силами разработчика (правообладателя) при выходе из строя серверного оборудования или критических сбоях в работе системного ПО Заказчика, на котором функционирует Специализированное ПО;
- удаленное обновление Специализированного ПО на мощностях Заказчика специалистами разработчика (правообладателя);
- консультации разработчика (правообладателя) в процессе отладки специалистами Заказчика совместной работы Специализированного ПО с СКЗИ Заказчика, применяемыми для подключения (при необходимости) к Специализированному ПО специалистов разработчика (правообладателя) и оказания экспертной поддержки специалистами Исполнителя и разработчика (правообладателя);
- консультации разработчика (правообладателя) в процессе отладки специалистами Заказчика совместной работы Специализированного ПО с СКЗИ Заказчика, применяемыми для подключения к Специализированному ПО удаленных пользователей;
- консультации разработчика (правообладателя) в процессе отладки специалистами Заказчика совместной работы Специализированного ПО и локальных СЗИ Заказчика, применяемых для защиты информации, обрабатываемой в Специализированном ПО;
- внесение изменений в услуги, ранее созданные в Специализированном ПО, с использованием текущих возможностей встроенного конструктора бизнес-процессов, в том числе, внесение изменений в формы генерируемых соглашений, актов по требованию Заказчика.

4.4. Исполнитель обязан обеспечить Заказчику расширенную гарантийную поддержку программы для ЭВМ «Альфа-ID» в течение 9 (девяти) месяцев (с 01.01.2027 по 30.09.2027), с момента подписания акта приема-передачи прав на программу для ЭВМ «Альфа-ID», в составе:

- прием обращений и оказание консультаций по эксплуатации основного функционала программы для ЭВМ «Альфа-ID» (в объеме эксплуатационной документации) по электронной почте с понедельника по пятницу (за исключением нерабочих праздничных дней) с 8:00 до 18:00 (по местному времени Заказчика);
- рекомендации по процессу установки и настройки программы для ЭВМ «Альфа-ID» (в объеме эксплуатационной документации);
- оказание консультаций в процессе самостоятельного обновления Заказчиком программы для ЭВМ «Альфа-ID»;
- решение инцидентов, связанных с работоспособностью программы для ЭВМ «Альфа-ID», с понедельника по пятницу (за исключением нерабочих праздничных дней) с 8:00 до 18:00 (по московскому времени);
- обеспечение доступа к серверу обновлений программы для ЭВМ «Альфа-ID»;
- информирование о доступных обновлениях программы для ЭВМ «Альфа-ID» (по запросу);
- прием предложений по улучшению программы для ЭВМ «Альфа-ID»;
- предоставление обновлений (hotfix), устраняющих дефекты, выявленные программе для ЭВМ «Альфа-ID»;
- осуществление технического сопровождения по местному времени (UTC +7).

4.5. Исполнитель обязан предоставить Заказчику установочный комплект сертифицированного программного изделия (программа для ЭВМ «Альфа-ID»), в составе:

- Инсталляционный комплект;
- Формуляр;
- Руководство пользователя;
- Руководство администратора;
- Заверенная копия сертификата соответствия ФСТЭК России.

5. Требования к Исполнителю

Исполнитель должен обладать необходимыми объемами лицензионных прав и полномочий для предоставления Заказчику неисключительных (пользовательских) прав на использование программы для ЭВМ «Альфа» и программы для ЭВМ «Альфа-ID». Для подтверждения данного требования Исполнителем предоставляются заверенные копии следующих документов:

- Свидетельство об официальной регистрации программы для ЭВМ «Альфа» и программы для ЭВМ «Альфа-ID», выданное в установленном законом порядке Федеральной службой по интеллектуальной собственности, патентам и товарным знакам, в случае если Исполнитель является Правообладателем (Разработчиком) программы для ЭВМ «Альфа» и программы для ЭВМ «Альфа-ID»;
- Лицензионный договор (Сублицензионный договор) с разработчиком (Правообладателем) программы для ЭВМ «Альфа» и программы для ЭВМ «Альфа-ID» с полномочиями Исполнителя на передачу третьим лицам неисключительных (пользовательских) прав на использование программы для ЭВМ «Альфа» и программы для ЭВМ «Альфа-ID» в объеме и способами, предусмотренными условиями настоящего описания объекта закупки, в случае если Исполнитель не является разработчиком (Правообладателем) программы для ЭВМ «Альфа» и программы для ЭВМ «Альфа-ID».

6. Требования в части поддержки отечественного программного обеспечения

Для надежности Программы для ЭВМ, в срок не более 30 (тридцати) рабочих дней после выхода официального релиза, должно быть обеспечено своевременное тестирование и совместимость:

- работоспособности Программы для ЭВМ с официальными релизами и версиями ядер операционных систем на базе Astra Linux (поддержка как графических, так и командных интерфейсов для эффективного

взаимодействия с системными ресурсами) с дальнейшим обновлением. В случае несовместимости Программы для ЭВМ с отдельными компонентами, входящими в состав официального релиза операционной системы, необходимо провести всесторонний анализ всех установленных библиотек и программных модулей, определить, какие именно версии или компоненты обладают необходимыми функциями, и осуществить доработку Программы для ЭВМ для ее стабильной работы с обновленной операционной системой;

- системы антивирусной защиты информации Dr.Web имеющей действующий сертификат соответствия ФСТЭК России, включая регулярные обновления, которые должны обеспечивать высокий уровень защиты от угроз и уязвимостей (без нарушения производительности компонентов Программы для ЭВМ);

- системы защиты информации от несанкционированного доступа Secret Net Studio для Linux/Secret Net LSP, имеющей действующий сертификат соответствия ФСТЭК России, которая должна включать в себя механизмы шифрования данных и аутентификации пользователей (стабильная и безопасная среда для работы пользователей, минимизируя риски потерь и несанкционированного доступа к информации).

Результатом тестирования должен быть протокол тестирования обновлений.

7. Требования к контролю, хранению, обновлению и восстановлению данных

В Программе для ЭВМ должна поддерживаться логическая целостность данных, то есть изменения должны носить характер транзакционно-ориентированных, выполняющихся в целом от начала до конца либо, в случае сбоя, не выполняющихся совсем.

Должна обеспечиваться сохранность и целостность данных Программы для ЭВМ, выполнение комплекса мер по резервному копированию данных. Средства резервного копирования предоставляет Заказчик. В целях обеспечения безопасности данных и защиты конфиденциальной информации запрещено резервное копирование Программы для ЭВМ на собственные мощности Исполнителя без согласования с Заказчиком.

Исполнитель обязан обрабатывать запросы на устранение уязвимостей в ПО по запросу Заказчика и/или оператора ЦОД.

8. Требования к защите информации Исполнителем

Доступ осуществляется по защищенной сети передачи данных. Доступ к вычислительным мощностям предоставляется при условии наличия у Исполнителя необходимых технических и программных средств для защиты информации для подключения к сети Заказчика. Подключение к защищенной сети Заказчика, а также приобретение необходимых лицензий и дистрибутивов выполняются за счет Исполнителя.

Средства криптографической защиты информации необходимо использовать не ниже класса КСЗ с действующим сертификатом ФСБ России:

- Программный комплекс ViPNet Client (версия не ниже 4.5) для сети № 2301;
- Программный комплекс ViPNet Client 5 for Linux для сети № 2301;
- Средство криптографической защиты информации «Континент-АП» (версия не ниже 4);
- Программно-аппаратный комплекс ViPNet Coordinator HW 5;
- Аппаратно-программный комплекс шифрования «Континент» (версия не ниже 3.9).

Использование операционных систем, не имеющих действующей технической поддержки производителя, запрещено.

Обмен или передача первичной ключевой информации осуществляется на физическом носителе и личном присутствии, по месту расположения администратора сети Оператора Центра обработки данных информационных систем Кемеровской области – Кузбасса, в соответствии с приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну». Исполнитель должен учитывать длительность получения первичной ключевой информации при подключении.

Исполнитель обязан в течение трех рабочих дней с момента заключения контракта начать процедуру выполнения требований информационной безопасности, а также подачу заявок на подключение к Центру обработки данных информационных систем Кемеровской области – Кузбасса.

Порядок подключения к Центру обработки данных информационных систем Кемеровской области – Кузбасса при выполнении требований государственных контрактов размещены на сайте <https://ris.kemobl.ru> в разделе «Документы», наименование документа «Порядок подключения разработчиков к ЦОДу».

Для удаленного оказания услуг Исполнитель обязан подключиться к защищенной сети передачи данных (сеть ViPNet № 2301 или «Континент») оператора центра обработки данных информационных систем Кемеровской области – Кузбасса (далее – оператор ЦОД) с соблюдением требований законодательства Российской Федерации. Оператор ЦОД – Министерство цифрового развития связи Кузбасса.

Для подключения к защищенной сети передачи данных оператора ЦОД, Исполнитель заключает соответствующие соглашения по типовой форме через информационную систему «Реестр государственных информационных систем Кемеровской области – Кузбасса» (ris.kemobl.ru).

Для организации подключения удаленных рабочих мест Исполнителя, на автоматизированных местах должны быть выполнены все требования по обеспечению защиты информации в государственных информационных системах в соответствии с законодательством Российской Федерации. Исполнителем подается заявка оператору ЦОД с указанием следующих данных:

- фамилия, имя, отчество (при наличии) пользователя (ей) автоматизированного рабочего места;
- должность;

- контактный номер телефона;
- адрес электронной почты;
- скан-копия согласия на обработку персональных данных;
- адрес размещения автоматизированного рабочего места;
- номер, дата и наименование государственного контракта;
- МАС-адрес автоматизированного рабочего места;
- инвентарный номер (в соответствии с бухгалтерским учетом Исполнителя);
- наименование сопровождаемой информационной системы;
- IP адрес(а) серверных мощностей, на которых будет/размещена информационная система;
- номер порта(ов) доступа;
- наименование протокола доступа;
- документ, подтверждающий установку средств защиты информации с указанием версии и номера

сертификата ФСТЭК России и/или ФСБ России: средства криптографической защиты информации, средство межсетевого экранирования, средство защиты информации от несанкционированного действия, средство антивирусной защиты информации на указанное автоматизированное рабочее место;

- сканированная копия утвержденной политики информационной безопасности организации – Исполнителя;
- сканированная копия утвержденного плана реагирования на компьютерные инциденты организации – Исполнителя;

Исполнителя;

- сканированная копия утвержденного регламента действий работников организации – Исполнителя в случае нештатных ситуаций.

- подтверждение и дата результатов внутренних (внешних) аудитов информационной безопасности;
- подтверждение и дата результатов тестирования на проникновение инфраструктуры.

Политика информационной безопасности организации – Исполнителя, план реагирования на компьютерные инциденты организации – Исполнителя и регламент действий работников организации – Исполнителя в случае нештатных ситуаций должны быть утверждены с учетом требований действующего законодательства Российской Федерации в области информационных технологий и информационной безопасности, а также с учетом требований федерального органа исполнительной власти в области обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

Внутренний (внешний) аудит информационной безопасности и тестирование на проникновение информационной инфраструктуры Исполнителя проводится с учетом требований действующего законодательства Российской Федерации в области информационных технологий и информационной безопасности, а также с учетом требований федерального органа исполнительной власти в области обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации. Указанные работы рекомендуется проводить не реже 1 раза в календарный год, а также внепланово, при возникновении инцидентов информационной безопасности в информационной инфраструктуре Исполнителя. Оператор ЦОД имеет право запросить документы, подтверждающие результаты проведенного аудита и тестирования.

Поддача заявки осуществляется через информационную систему «Реестр государственных информационных систем Кемеровской области – Кузбасса» (ris.kemobl.ru), услуга «Подключение организации к инфраструктуре Центра обработки данных информационных систем Кемеровской области – Кузбасса».

После проверки предоставленных документов оператором ЦОД не позднее 5-ти рабочих дней создаются учетные данные для доступа и передаются по электронной почте, указанной в заявке.

В случае изменения, увольнения состава работников Исполнителя, осуществляющих удаленный доступ к информационной инфраструктуре Заказчика, необходимо уведомить оператора ЦОД о фактах таких изменений в течении 1 календарного дня через информационную систему «Реестр государственных информационных систем Кемеровской области – Кузбасса» (ris.kemobl.ru) по заявке «Закрытие учетных записей пользователей в инфраструктуре Центра обработки данных информационных систем Кемеровской области - Кузбасса».

В случае невозможности выполнить требования на автоматизированных рабочих местах Исполнителя, оказание услуг осуществляется без использования дистанционных технологий, по месту нахождения Заказчика.

Подключение работников Исполнителя к информационной инфраструктуре Заказчика в нерабочее время производится исключительно по предварительной договоренности между сторонами. Согласование должно осуществляться Исполнителем за 24 часа до предполагаемого начала работ в рабочие дни.

В случае необходимости оказания услуг вне установленного рабочего времени по инициативе Заказчика, все виды работ и сроки их выполнения доводятся до Исполнителя не позднее чем за час до начала предполагаемых работ. При этом начало работ не должно превышать одного часа с момента поступления обращения (заявки) Заказчика.

В рамках оперативного взаимодействия между Заказчиком, Исполнителем и оператором ЦОД заключается порядок взаимодействия с определением контактов ответственных лиц по обеспечению информационной безопасности, не персонализированные каналы для оперативного взаимодействия (резервные каналы взаимодействия).

Исполнитель обязан:

- уведомлять Заказчика и оператора ЦОД о наступлении в его инфраструктуре компьютерных инцидентов;
- обрабатывать запрос на устранение уязвимостей в ПО по запросу Заказчика и/или оператора ЦОД.

Дополнительно Исполнитель должен реализовать следующие базовые меры по информационной безопасности в собственной инфраструктуре:

- двухфакторная аутентификация пользователей;
- антивирусная защита автоматизированных рабочих мест и серверов;

- защищенное удаленное подключение с использованием средств криптографической защиты информации;
- защита почтовых сервисов от фишинга;
- защищенный обмен файлами и информацией через файловое хранилище;
- обеспечение процесса управления уязвимостями;
- реализация парольной политики (длина пароля должна быть не менее 15 символов, пароль должен содержать буквы верхнего и нижнего регистра (А-Я, AZ, а-я, a-z), специальные символы (!, », №, %, *, /), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов).

Пароли от учетной записи Исполнителя и учетной записи Заказчика должны отличаться.

При осуществлении удаленного подключения к информационной инфраструктуре Заказчика Исполнитель организует запись всех действий своих пользователей удалённых рабочих мест. Рекомендуемый срок хранения журналов событий не менее 1 года. В случае возникновения инцидента предоставлять указанные журналы Заказчику.

Для обеспечения выявления и реагирования на события информационной безопасности (многократные попытки аутентификации, сетевое сканирование, несанкционированные подключения), инициируемые информационной инфраструктурой Исполнителя и учетными записями, с которых осуществляется удаленный доступ интегрировать (по возможности) включение информационной инфраструктуры Исполнителя в контур мониторинга информационной безопасности Заказчика (при наличии технической возможности).

Заказчик имеет право производить периодические проверки в сроки согласованные с Исполнителем на предмет возникновения нештатных ситуаций или инцидентов информационной безопасности путем имитации указанных событий (проведение тренировок).

Использование Исполнителем программного обеспечения для удаленного управления автоматизированным рабочим местом (например, TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin, LiteManager, Удаленный рабочий стол Chrome, Microsoft Remote Assistance, Microsoft Remote Desktop) запрещается.

Для доступа к информационной инфраструктуре Заказчика Исполнитель должен использовать средства вычислительной техники, которые не используются в личных целях и к которым применяются корпоративные меры по информационной безопасности.

В случае привлечения субподрядной организации для сопровождения информационной инфраструктуры Заказчика все требования, предусмотренные настоящим разделом, подлежат выполнению.

Уточняющая информация по взаимодействию в рамках требований к защите информации Исполнителем размещена на официальном сайте оператора ЦОД (digital42.ru), в разделе «Деятельность», подразделе «Информационная безопасность».

9. Требования к конфиденциальности информации

Исполнитель обязан соблюдать конфиденциальность информации, ставшей ему известной в ходе исполнения Контракта, не передавать третьим лицам и не раскрывать публично конфиденциальную информацию без согласия Заказчика, а также соблюдать требования к защите указанной информации, предусмотренные действующим законодательством.

К конфиденциальной информации относится любая информация в бумажной или электронной форме, предоставленная Заказчиком Исполнителю в процессе исполнения обязательств по Контракту.

К конфиденциальной информации не относится информация, которая отнесена законодательством Российской Федерации к категории открытой и раскрытие которой вменено в обязанность Заказчику или Исполнителю.

Исполнитель имеет право предоставлять доступ к конфиденциальной информации своим сотрудникам для выполнения ими своих трудовых обязанностей при условии соблюдения ее конфиденциальности.

Исполнитель не несет ответственности за разглашение полученной конфиденциальной информации, если она:

- на момент раскрытия была общеизвестной;
- была самостоятельно разработана Исполнителем;
- раскрыта государственным органам в соответствии с действующим законодательством Российской Федерации;
- предоставлена Заказчиком третьей стороне до момента подписания Контракта.