

Техническое задание

на оказание комплекса услуг по предоставлению вычислительных мощностей для размещения на них цифровых сервисов для вычислений, хранения и обработки данных

1. Перечень терминов и сокращений

Виртуализация	процесс предоставления вычислительных ресурсов Исполнителя, которые могут работать в изолированной друг от друга среде без привязки к конкретным физическим ресурсам
Виртуальный центр обработки данных (ВЦОД)	совокупность вычислительных ресурсов (Виртуальной оперативной памяти, Виртуального дискового пространства и Виртуальных сетей), предназначенных для создания и функционирования Виртуальных машин Заказчика
Виртуальная машина (ВМ)	размещенная на инфраструктуре Исполнителя изолированная программно-аппаратная система (совокупность ресурсов Виртуальных процессоров, Виртуальной памяти, Виртуального дискового пространства), эмулирующая аппаратное обеспечение и предназначенная для работы под управлением операционной системы Заказчика
Виртуальная память (RAM)	энергозависимая часть компьютерной памяти, в которой временно хранятся данные и команды, необходимые процессору для выполнения им операции, имеющая возможность работать в изолированной друг от друга среде
Виртуальный процессор (vCPU)	часть процессорной мощности инфраструктуры Исполнителя, выделяемой для Виртуальной машины, работающей под управлением операционной системы Заказчика
Влияние	мера воздействия Инцидента, описывающая влияние на бизнес-процессы Заказчика
ГБ	гигабайт – кратная единица измерения количества информации
Инфраструктура	совокупность инженерных и вспомогательных элементов, включающая в себя сеть связи, центр обработки данных (инженерное и вычислительное оборудование, специалистов) и систему обеспечения информационной безопасности, предназначенных для обеспечения функционирования информационной системы
Инцидент	незапланированное событие, которое привело или может привести к прерыванию предоставления услуги или к снижению ее качества, даже если оно еще не повлияло на услугу для Заказчика
Панель управления	портал в сети Интернет, с помощью которого осуществляются настройка и управление Услугой

Платформа Виртуализации	специализированное программное обеспечение, реализующее Виртуализацию на ПАК Исполнителя
Облачная платформа	инфраструктура Исполнителя, обладающая функционалом предоставления Заказчику в оперативное управление масштабируемых вычислительных мощностей и обеспечивающая в интересах Заказчика обработку, хранение и распространение информации
Платформа виртуализации	программно-аппаратный комплекс, обеспечивающий запуск и управление виртуальными машинами
СКЗИ	средство криптографической защиты информации
Техническая поддержка	оказание Исполнителем устных и письменных консультаций по вопросам оказания Услуги, а также устранение Инцидентов, возникающих в зоне ответственности Исполнителя в связи с оказанием Услуги
ТЗ	Описание объекта закупки (Техническое задание)
ФСБ России	Федеральная служба безопасности Российской Федерации
ФСТЭК России	Федеральная служба по техническому и экспортному контролю Российской Федерации
Центр обработки данных (ЦОД)	структура или группа структур, предназначенных для централизованного размещения, организации взаимодействия и эксплуатации ИС, сетевого и телекоммуникационного оборудования, обеспечивающих возможность оказания услуг в области хранения, обработки и передачи данных, а также все объекты и инфраструктуры, используемые для распределения электроэнергии и контроля среды в сочетании со средствами обеспечения требуемой устойчивости и безопасности для достижения желаемого уровня доступности оказываемых услуг
DDoS (Distributed Denial of Service)	распределённая атака типа «отказ в обслуживании»
DNS	сетевая служба разрешения доменных имен в IP-адреса
IP (Internet Protocol, Межсетевой протокол)	маршрутизируемый протокол сетевого уровня семейства TCP/IP
IP-адрес	уникальный сетевой адрес в сети передачи данных, построенный по протоколу IP (межсетевой протокол передачи данных)
VPN (Virtual Private Net)	виртуальная частная сеть
Web-интерфейс	веб-страница или совокупность веб-страниц, предоставляющая пользовательский интерфейс для взаимодействия с сервисом или устройством посредством протокола HTTP(S) и веб-браузера

Uptime Institute	международный институт по сертификации дата-центров
TIER III	стандарт надежности оборудования и инфраструктуры дата-центров от Uptime Institute, ключевой особенностью которого является отсутствие необходимости прерывать работу на время ремонта/профилактических мероприятий
Тикет-система	система обмена сообщениями между Заказчиком и Исполнителем путем отправки/получения запросов через электронную форму, расположенную в Панели управления. Применяется в том числе для оказания технической поддержки.

2. Требования к порядку оказания услуги.

2.1. Исполнитель в течение 3 (трех) рабочих дней с даты заключения Договора обязан предоставить Заказчику копию(и) аттестата(ов) соответствия требованиям по защите информации вычислительных мощностей, предоставляемых Заказчику для размещения на них цифровых сервисов для вычислений, хранения и обработки данных в рамках оказываемой Услуги:

- классу защищенности для государственных информационных систем – не ниже второго включительно (в соответствии с требованиями Приказа ФСТЭК России № 17 от 11.02.2013);
- уровню защищенности персональных данных – не ниже четвертого включительно (в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119, приказа ФСТЭК России от 18.02.2013 № 21).

2.2. Доступ к закупаемым Услугам предоставляется через Панель управления. Аутентификационные данные для доступа к закупаемым Услугам (логин и временный пароль) предоставляются Заказчику в течение 3 рабочих дней с момента подписания договора посредством направления их на адрес электронной почты, указанный Заказчиком. Также Исполнителем может быть предоставлена возможность самостоятельной регистрации в панели управления, в данном случае доступ Заказчику предоставляется в течение одного часа с момента его регистрации.

2.3. Исполнителем должно обеспечиваться функционирование единой круглосуточной службы технической поддержки.

2.4. Исполнитель оказывает услугу на базе собственной или арендованной инфраструктуры центров обработки данных (ЦОД), соответствующей требованиям настоящего Технического задания. Все необходимые аппаратные средства и программные компоненты для оказания услуг обеспечиваются Исполнителем за свой счёт.

2.5. При необходимости Исполнитель обязан предоставить информацию о физическом размещении вычислительных ресурсов и обеспечить доступ к ним для целей аудита или проверки со стороны Заказчика и/или контролирующих органов, в пределах законодательства Российской Федерации. Доступ Заказчика для аудита возможен только в случае заблаговременного согласования с Исполнителем объема проводимого аудита и списка представителей Заказчика, направленных не позднее 72 часов до планируемой даты аудита. Исполнитель вправе обоснованно сократить запрошенный Заказчиком объем аудита.

3. Перечень нормативных правовых и нормативных технических актов.

3.1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3.2. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных».

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

3.4. Приказ Минцифры России от 01.11.2023 г. № 936 «Об утверждении требований о защите информации при предоставлении вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к информационно-телекоммуникационной сети «Интернет».

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

3.6. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (Зарегистрировано в Минюсте России 14.05.2013 № 28375).

3.7. Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состав 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».

3.8. ГОСТ Р ИСО/МЭК 27001-2021 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (утв. и введен в действие Приказом Росстандарта от 30.11.2021 № 1653-ст).

3.9. «Методический документ. Методика оценки угроз безопасности информации» (утв. ФСТЭК России 05.02.2021).

3.10. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15.02.2008).

3.11. «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014).

4. Требования к услуге

В рамках оказания комплекса услуг по предоставлению вычислительных мощностей для размещения Заказчиком цифровых сервисов, хранения и обработки данных Исполнитель обязан обеспечивать функционирование необходимой сетевой инфраструктуры. Это включает оказание услуг связи, представляющих собой Ethernet-подключение со скоростью передачи данных не менее 1 Гбит/с, без ограничения входящего и исходящего трафика, необходимые для доступа Заказчика к вычислительным ресурсам, обмена данными между компонентами виртуальной среды и взаимодействия с Панелью управления. Указанные функции сетевой связности и передачи данных являются неотъемлемой технологической частью комплексной услуги и включаются в её стоимость.

4.1. Состав услуги.

№	Наименование
1	Предоставление виртуальных машин
2	Предоставление сетевого хранилища
3	Предоставление сетевых ресурсов с защитой от атак

4	Предоставление технической поддержки
---	--------------------------------------

4.2. Предоставление виртуальных машин.

4.2.1. Инфраструктура должна позволять разместить 16 виртуальных машин, предоставляемых Исполнителем, со следующими параметрами:

	Виртуальный процессор, vCPU	Виртуальная память, RAM (ГБ)	Системные диски (SSD, ГБ)
BM1	4	8	300
BM2	4	10	200
BM3	4	10	200
BM4	4	8	100
BM5	4	4	10
BM6	4	4	10
BM7	4	4	10
BM8	16	8	300
BM9	4	8	2000
BM10	4	8	1000
BM11	4	4	200
BM12	2	8	1000
BM13	8	10	1000
BM14	4	4	50
BM15	2	8	50
BM16	4	8	50

4.2.2. Совокупный объём необходимых базовых ресурсов Исполнителя составляет:

- Виртуальных процессоров (vCPU) – не менее 76 шт.
- Виртуальной памяти (RAM)– не менее 114 ГБ
- Системных дисков – не менее 6480 ГБ

4.2.3. Инфраструктура должна позволять перераспределять базовые ресурсы между виртуальными машинами без превышения совокупных объёмов базовых ресурсов.

4.2.4. Общие требования к Виртуальным процессорам:

- Базовая тактовая частота ядер процессоров серверов виртуализации должна быть не менее 2.4 ГГц.
- Должна быть возможность повышения тактовой частоты ядер Виртуальных процессоров (TurboBoost) до 3.6 Ghz без ограничений по времени TurboBoost.
- Допустимый коэффициент переподписки vCPU к физическим CPU не должен превышать 2:1.
- Вычислительные ресурсы должны предоставляться на основе современных серверных процессоров выпуска не ранее 2020 года.

4.2.5. Требования к системным дискам.

Заказчику должен предоставляться доступ к дискам с низкой сетевой задержкой (latency), размещенным на хостах виртуализации вне сетевого хранилища данных и предназначенным для установки операционных систем виртуальных машин, соответствующим следующим требованиям:

- Диски должны обеспечивать низкое время доступа не более 1 мс. (миллисекунды) из операционной системы виртуальной машины.
- Размещение таких дисков может быть локальным или сетевым, при этом технология хранения должна обеспечивать минимальную задержку и высокую надёжность.

- Для обеспечения отказоустойчивости и предотвращения потери данных в случае выхода из строя диска, диски должны быть объединены в отказоустойчивую конфигурацию не ниже RAID 10 (или эквивалентную по уровню надёжности).
- Виртуальные машины должны запускаться и функционировать в случае отказа одного из физических дисков массива.

4.3. Предоставление сетевого хранилища.

Заказчику должен предоставляться доступ к сетевому хранилищу для хранения пользовательских данных, соответствующему следующим требованиям:

- Хранилище должно быть сетевым и поддерживать возможность подключения к различным виртуальным машинам, включая возможность повторного подключения (перемонтирования) в случае их перезапуска, миграции или отказа.
- Данные должны храниться в отказоустойчивой конфигурации, обеспечивающей сохранность информации при отказе оборудования.
- Решение может быть реализовано как на базе специализированного оборудования (например, отказоустойчивой СХД с внутренним резервированием), так и в виде распределённого хранилища (например, с хранением не менее трёх копий на независимых серверах, расположенных в разных стойках).
- Уровень отказоустойчивости должен исключать потерю данных при выходе из строя одного или более узлов хранения.

Минимальные требования по производительности сетевого хранилища: не менее 7000 IOPS на чтение и 4000 IOPS на запись. Необходимый объем ресурсов сетевого хранилища – не менее 4 ТБ.

4.4. Предоставление сетевых ресурсов с защитой от атак.

У каждой предоставляемой виртуальной машины должен быть как минимум 1 виртуальный сетевой адаптер.

- 4.4.1. Для каждой виртуальной машины должен быть выделен 1 статический IPv4-адрес из глобально маршрутизируемого пула («белый» IPv4-адрес).
- 4.4.2. Для каждой виртуальной машины должна быть возможность настройки дополнительных виртуальных сетевых адаптеров для обеспечения связности виртуальных машин между собой с использованием не маршрутизируемых ipv4-адресов («серые» IPv4-адреса).
- 4.4.3. Пропускная способность сетевых соединений между виртуальными машинами должна быть не ниже 5 Гбит/с без ограничения трафика.
- 4.4.4. Пропускная способность сетевого соединения виртуальных машин с сетью интернет должна быть не ниже 1 Гбит/с без ограничения трафика.
- 4.4.5. Заказчику должна быть предоставлена возможность организации L3VPN-соединения между виртуальной инфраструктурой Заказчика и внешним ЦОД, не принадлежащим Исполнителю, без ограничения используемых протоколов (IPsec, GRE, OpenVPN и др.), включая возможность туннелирования по публичному интернету или через физическое соединение. Организация (при необходимости) и администрирование такого VPN – соединения выполняется Заказчиком самостоятельно. При ограничениях на уровне Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций Исполнитель не несёт ответственность в случае невозможности организации L3VPN-соединения.
- 4.4.6. Сервис защиты ресурсов виртуальной защищённой инфраструктуры от DDoS-атак не должен тарифицироваться.

4.4.7. Сервис защиты должен на сетевом и транспортном уровне (L3, L4) обеспечивать защиту от типов атак:

- атак с отражением на основе UDP (DNS, NTP, memcache и пр.);
- атак с использованием фрагментированного IP трафика;
- TCP SYN/RST/PSH flood;
- различных типов UDP flood;
- различных типов ICMP flood.

4.4.8. Должен производиться централизованный сбор событий безопасности с сервисов провайдера и анализ журналов событий. Исполнитель предоставляет инструмент для централизованного сбора и анализа журналов событий с возможностью экспорта журналов событий безопасности с возможностью осуществления хранения в сервисах провайдера. По требованию Заказчику должна предоставляться выгрузка (экспорт) журналов событий безопасности за указанный период. Срок хранения журналов должен составлять не менее 12 месяцев. Состав журнала событий безопасности определяется Исполнителем и может не содержать информацию о служебной инфраструктуре.

4.4.9. На серверах платформ должно постоянно проводиться обнаружение вторжений и контроль изменений конфигураций. Результаты мониторинга должны быть доступны Заказчику. Исполнитель вправе подтвердить обнаружение вторжений и контроль изменений конфигураций путем предоставления Заказчику соответствующих актов оценки эффективности, заключений, сертификатов и аттестатов.

4.4.10. Облачная платформа должна включать как минимум одно промышленное решение (встроенное или наложенное) по обеспечению кибербезопасности и устранению интернет-угроз, включающее в себя функционал: межсетевой экран, маршрутизацию, шлюзовой антивирус, систему обнаружения и предотвращения вторжений (СОВ), систему контентной фильтрации, модуль мониторинга и статистики, систему управления трафиком и контролем доступа в интернет. Организация (при необходимости) и эксплуатация VPN – соединений осуществляется Заказчиком на арендованных вычислительных ресурсах и не обслуживается Исполнителем.

4.4.11. При работе с Облачной Платформой предполагается хранение и обработка персональных данных. Пользовательские данные не должны передаваться третьим лицам без согласия Заказчика, полученного в письменном виде.

4.5. Предоставление технической поддержки.

4.5.1. Исполнитель обязан оказывать круглосуточную техническую поддержку в режиме 24x7x365 (24 часа в сутки, 7 дней в неделю, 365 дней в году).

4.5.2. Техническая поддержка Исполнителя должна предоставлять следующую информацию:

- контактный номер телефона «горячей линии»;
- адрес электронной почты технической поддержки;
- номер инцидента, зарегистрированного в системе обработки обращений Исполнителя (тикет-система);
- время возникновения и описание инцидента;
- действия Исполнителя по устранению инцидента.

4.5.3. Время реакции (период времени между регистрацией Исполнителем, поступившего обращения Заказчика и, до первой обратной связи от Исполнителя) на инциденты:

Приоритет	Время реакции	Пример инцидента
Критический	≤ 15 мин	Полная недоступность облачной инфраструктуры
Значительный	≤ 15 мин	Снижение качества предоставления Услуги
Умеренный	≤ 15 мин	Незначительное или низкое влияние на Сервисы Заказчика
Низкий	≤ 15 мин	Консультации, рекомендации

4.5.4. Техническая поддержка должна включать:

- Консультации по сервисам и функциональным возможностям Облачной платформы;
- Предоставление документации по Облачной платформе;
- Консультации по вопросам, связанным с биллингом, настройкой бюджетирования проектов Заказчика на базе Облачной платформы;
- Диагностику ошибок в работе сервисов Облачной платформы и решение выявленных проблем;
- Восстановление доступа в Панель управления Облачной платформы;
- Круглосуточную службу мониторинга состояния всей инфраструктуры ВЦОД, включая каналы передачи данных;
- Круглосуточное нахождение в здании ЦОД сотрудников поддержки, способных выполнить работы (услуги) по ремонту и восстановлению оборудования.

4.5.5. Уровень обслуживания:

- Согласованное время работоспособности услуг (СВР) – 24 x 7;
- Согласованное время поддержки услуг (СВП) – 24 x 7;
- Расчётный период доступности – 12 месяцев с даты начала оказания услуг, определяемой по договору.
- Процент доступности за расчётный период – не менее 99,98 %
- Параметры компенсаций за нарушение уровня обслуживания указаны в разделе 7 Договора.

4.5.6. Гарантированное время восстановления Исполнителем предоставляемой услуги с момента обращения Заказчика в службу технической поддержки Исполнителя:

- Для Сетевого хранилища, подключаемого к виртуальным машинам — не более 30 минут.
- Для виртуальных машин, использующих Системные диски — не более 60 минут (в случае отказа должна быть обеспечена возможность переноса нагрузки и повторное подключение хранилища).

4.5.7. В случае невозможности восстановления услуги в пределах указанного времени, Исполнитель обязан предоставить Заказчику временную замену (виртуальную машину с аналогичными параметрами) или иное решение, обеспечивающее продолжение работы.

4.5.8. Информация о типах подключенных дисков, их характеристиках и схемах резервирования должна быть доступна Заказчику в Панели управления (личном кабинете) или по запросу.

5. Общие требования к Облачной платформе, а также к доступу и управлению.

5.1. Заказчику для оказания услуг должна быть предоставлена Платформа виртуализации, которая обеспечивает изоляцию вычислительных процессов и аппаратных ресурсов друг от друга.

5.2. Платформа виртуализации должна быть зарегистрирована в едином реестре российских программ для электронных вычислительных машин и баз данных, созданном в соответствии со статьей 12.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5.3. Управление платформой виртуализации должно осуществляться с помощью:

- Web-интерфейса (Панель управления);
- программно-аппаратных средств API.

5.4. Доступ к Панели управления должен осуществляться с применением двухфакторной аутентификации (например, OTP, SMS).

5.5. Платформа, на которой предоставляются сервисы виртуализации, должна обеспечивать запуск виртуальных машин на других узлах платформы виртуализации, при выходе из строя одного из них.

5.6. Заказчику должна быть предоставлена возможность самостоятельного мониторинга текущего состояния виртуальных машин, доступ к их консоли, возможность управления выключением/включением/перезагрузкой.

5.7. Заказчику должна быть предоставлена возможность самостоятельного управления маршрутизацией и фильтрацией трафика между Виртуальными машинами/ Виртуальными машинами и сетью Интернет.

5.8. Заказчику должна быть предоставлена возможность изменения параметров вычислительных ресурсов под каждую конкретную виртуальную машину.

5.9. Хранение данных виртуальных машин (виртуальных дисков, снимков и пр.) должна осуществляться в программно-определяемой системе хранения данных Платформы виртуализации.

5.10. Управление платформой виртуализации должно включать в себя возможность выполнения следующих функций:

- Создания/удаления VM;
- Изменения характеристик VM в части CPU, RAM, а также дискового пространства;
- Выбора ОС для создаваемых VM - Linux/Windows;
- Загрузка собственных образов ОС;
- Выбора дополнительных услуг;
- Просмотра технической и финансовой информации для отслеживания потребляемых мощностей и прогнозирования финансовых расходов;
- Снятия снапшотов виртуальных машин.

5.11. Панель управления должна предоставлять возможность разграничения доступа по ролям уровня аккаунта и проекта, с уровнем доступа к вычислительным ресурсам.

5.12. Панель управления должна обеспечивать отслеживание информации следующих типов:

- Метрики состояния VM;
- Загруженность процессора;

- Использование дискового пространства;
- Сетевой трафик (входящий и исходящий).

5.13. Должна быть предусмотрена возможность создания резервных копий виртуальных машин и восстановления из них средствами самой платформы виртуализации, без необходимости установки специализированных агентов внутри виртуальных машин.

5.14. Механизмы резервного копирования должны обеспечивать масштабируемость: при увеличении количества виртуальных машин объём, скорость и частота резервного копирования должны автоматически или оперативно масштабироваться, без снижения производительности и без необходимости ручной настройки для каждой новой виртуальной машины.

5.15. Решение по резервному копированию должно поддерживать централизованное управление заданиями резервного копирования, хранение копий в отказоустойчивом хранилище, настройку расписаний и политики хранения.

5.16. Облачная платформа должна включать в себя возможность предлагать готовые и протестированные образы ОС: Ubuntu, Oracle Linux, CentOS, Debian, Fedora CoreOS, Fedora, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Astra Linux.

5.17. Облачная платформа должна позволять Заказчику загружать собственные образы ОС общим объёмом не менее 20 Гбайт.

5.18. Должен быть обеспечен многопользовательский доступ с возможностью назначения прав и полномочий в соответствии со следующим правами ролей:

- «Наблюдатель», обладающая разрешениями на чтение к ресурсам;
- «Администратор», обладающая всеми разрешениями роли «Наблюдатель» и разрешениями на все операции для управления ресурсом, кроме назначения ролей другим пользователям;
- «Администратор пользователей», обладающая доступом к управлению пользователями и без доступа к операциям для управления ресурсом. Первого Администратора пользователей создает Владелец;
- «Владелец», обладающая всеми разрешениями на ресурс. Владелец может выполнять любые операции с облачной платформой и ресурсами в нём, в том числе выдавать доступ к облачной платформе другим пользователям: назначать им роли и отнимать их.

Допустимо отличие наименования обозначенных ролей от требуемых, но разграничение прав должно соответствовать указанным требованиям.

5.19. Облачная платформа должна обеспечивать возможность создания системы разграничения доступа к виртуальной среде с использованием проектов.

5.20. Панель управления должна предоставлять интерфейс для:

- отображения информации об объектах облачной инфраструктуры;
- управления ресурсами облачной инфраструктуры;
- управления жизненным циклом внутренних учетных записей пользователей облака;
- управления жизненным циклом проектов (создание, изменение, удаление, управление квотами);
- управления ресурсными квотами;
- отображения информации о проекте (ресурсы, квоты, тарифы, баланс и пр.).

5.21. Сервисы Облачной платформы, предполагающие взаимное использование реализуемого функционала и механизмов, должны иметь прямую интеграцию между собой, позволяющую осуществлять централизованное конфигурирование и сопряжение сервисов через Панель управления.

5.22. Облачная платформа должна иметь функционал по формированию сводного отчета об использованных ресурсах и детализацию расходов.

6. Требования к ЦОД

6.1. Общие требования.

6.1.1. ЦОД и все его инженерные системы должны соответствовать уровню надежности не ниже TIER III по классификации Uptime Institute или ГОСТ Р 58811-2020 «Центры обработки данных. Инженерная инфраструктура. Стадии создания» и ГОСТ Р 58812-2020 «Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация».

6.1.2. ЦОД и оборудование в рамках Инфраструктуры Исполнителя, необходимые для оказания услуги по Договору, должны находиться в собственности или в аренде на условиях, обеспечивающих исключительное пользование им без права управления и распоряжения со стороны третьих лиц.

6.1.3. ЦОД должен быть обеспечен зарезервированными каналами связи с пропускной способностью (пропускной способностью, обеспечиваемой в случае выхода из строя любого из каналов связи) не менее 10Гбит/с. Внешние каналы связи должны быть независимы на уровне оборудования, физических кабельных трасс и канализаций. Должна быть возможность кроссировки с сетевым оборудованием в основных точках обмена трафиком. В ЦОД должны быть организованы не менее двух независимых кабельных вводов.

6.1.4. В ЦОД должна быть возможность подключения не менее чем к четырем независимым телеком-провайдерам на скоростях не менее 10Гбит/с.

6.1.5. ЦОД должен обладать собственным охраняемым периметром, оборудованным системами наблюдения. Оператор вычислительной платформы должен иметь на объекте собственную службу физической охраны.

6.1.6. Размещение всех компонентов инфраструктуры Исполнителя должно осуществляться на территории Российской Федерации в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (в частности ч. 5 ст. 18) и Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в частности ч. 4 ст. 16).

6.1.7. Физическая инфраструктура ЦОД, на которой развернута Облачная платформа, должна соответствовать требованиям, предъявляемым к объектам информатизации при защите государственной информационной системы на соответствие классу защищенности для государственных информационных систем – не ниже второго включительно (в соответствии с требованиями Приказа ФСТЭК России № 17 от 11.02.2013); а также уровню защищенности персональных данных – не ниже четвертого включительно (в соответствии с требованиями постановления Правительства РФ от 01.11.2012 № 1119 от 01.11.2012, Приказа ФСТЭК России от 18.02.2013 № 21 от 18.02.2013), в том числе в части электроснабжения, охлаждения, противопожарной защиты, физической и организационной безопасности.