

## ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ «EVOLUTION COMPUTE»

### 1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГИ

- 1.1. Evolution Compute (далее – Услуга) – это услуга по предоставлению базовых IT-ресурсов на основе совокупности функционирующего под управлением Исполнителя серверного и сетевого оборудования, систем хранения данных и специализированного программного обеспечения. Данная Услуга позволяет Заказчику разворачивать и размещать свою IT-инфраструктуру и связанные с ней виртуальные ресурсы (виртуальные машины, системы хранения, серверы и сетевые устройства).
- 1.2. Услуга реализована на оборудовании, принадлежащем Исполнителю, и средствами системы виртуализации собственной разработки (в т. ч. на базе компонентов с открытым исходным кодом). Ресурсами Услуги являются:
- 1.2.1. Вычислительные ресурсы (1 (одна) виртуальная машина);
- 1.2.2. Иные ресурсы, в соотв. со ст. 2 настоящего Приложения.
- 1.3. В рамках Услуги Исполнитель предоставляет Заказчику возможность создать собственную виртуальную инфраструктуру на базе согласованных между Исполнителем и Заказчиком набора виртуализированных вычислительных мощностей для создания виртуальных машин (VM): виртуальных процессоров (vCPU); виртуальной памяти (vRAM); графических процессоров (GPU)<sup>1</sup>; дисковых пространств (vDisk); сетевые адаптеры и интерфейсы, а также средства управления VM. Заказчик осуществляет управление виртуальными ресурсами в пределах выделенных виртуализированных ресурсов и мощностей, а также сформированной им конфигурации.
- 1.4. Функциональные возможности:
- управление дисками;
  - изменение характеристик VM в рамках одного типа без её пересоздания;
  - поддержка нескольких сетевых интерфейсов;
  - привязка подсетей;
  - назначение публичных IP-адресов;
  - виртуальный sNAT-шлюз, группа безопасности;
  - хранение и использование публичных ключей для авторизованного доступа;
  - возможность интеграции и управления через API;
  - управление резервными копиями виртуальных машин;
  - управление пользовательскими образами;
  - возможность арендовать прерываемые виртуальные машины.
- 1.5. В состав Услуги входят:
- 1.5.1. Вычислительные ресурсы:
- инструментарий для создания VM в виде набора процессоров, оперативной памяти, графических процессоров<sup>1</sup> и возможности выбора уровня переподписки процессора;
  - виртуальные диски как средство хранения данных;
  - публичные ключи для авторизованного подключения к VM;
  - база образов с предустановленными гостевыми операционными системами, предоставляемых Исполнителем.
- 1.5.2. Сетевые функции и компоненты:
- подсети;
  - сетевые интерфейсы;
  - публичные IP-адреса с возможностью привязки к виртуальным сетевым интерфейсам;
  - виртуальный sNAT-шлюз как средство подключения к сети интернет и/или внешним сетям;
  - группы безопасности как средство управления трафиком.
- 1.6. Основные компоненты Услуги:
- IaaS контроллер;
  - кластеры SDN/виртуализации;
  - кластеры SDS;
  - средства управления (пользовательская консоль);
  - инструменты мониторинга и сбора статистики;
  - набор образов VM;
  - инструменты для работы с резервными копиями VM;
  - инструменты для работы с пользовательскими образами.
- 1.7. В целях обеспечения защиты Инфраструктуры EVO реализуются меры и механизмы защиты, описанные в таблице 1.

<sup>1</sup> Для получения доступа к Виртуальным машинам с GPU необходимо создать заявку на Заказ через Техническую поддержку. Подробнее в п. 4.1. Приложения

Таблица 1. Обеспечение защиты Инфраструктуры EVO

Уровни защиты	Мероприятия
<b>Защита Облака Cloud.ru и средств его управления</b>	
Физический	Обеспечивается: <ul style="list-style-type: none"> <li>– размещение всего оборудования инфраструктуры в ЦОД, соответствующих требованиям надежности по категории Tier 3;</li> <li>– контроль и управление доступом к оборудованию, размещенному в ЦОД (охраняемая территория ЦОД, пропускной режим, системы контроля и управления доступом, запирающие стоек);</li> <li>– наличие внешней (по периметру ЦОД) и внутренней (в машинных залах ЦОД) систем видеонаблюдения на объектах информатизации ЦОД.</li> </ul>
Сетевой	Обеспечивается защита периметров ЦОД и их сегментирование с использованием межсетевых экранов нового поколения (NGFW), осуществляющих в том числе выявление и предотвращение компьютерных атак.
Инфраструктурный	Обеспечивается: <ul style="list-style-type: none"> <li>– антивирусная защита инфраструктуры с использованием антивирусных средств для облачных сред;</li> <li>– управление доступом к инфраструктуре и учетными записями пользователей, которые имеют доступ к инфраструктуре, в том числе с использованием средств двухфакторной аутентификации;</li> <li>– контроль действий привилегированных пользователей с использованием специализированных средств;</li> <li>– регулярный контроль и анализ защищенности инфраструктуры с использованием специализированных средств по выявлению уязвимостей в используемом ПО и его некорректной конфигурации, влияющей на уровень защищенности ПО, с устранением выявленных уязвимостей и/или недостатков;</li> <li>– сбор и анализ событий в компонентах и средствах информационной безопасности.</li> </ul>
Дополнительный	Осуществляются периодические тестирования на проникновение и аудит информационной безопасности Инфраструктуры Облака Cloud.ru с привлечением сторонних организаций. Выявленные в ходе соответствующего тестирования и/или аудита недостатки устраняются по факту их выявления.
<b>Защита КУ EVO</b>	
Приложения	Защита консоли обеспечивается на уровне приложений с использованием специализированного межсетевого экрана уровня приложений (Web Application Firewall).
Дополнительный	Осуществляются регулярные сканирования консоли на наличие актуальных уязвимостей и его периодические тестирования на проникновение с привлечением сторонних организаций. Выявленные уязвимости и/или недостатки устраняются по факту их выявления.
<b>Изоляция «Организаций» Заказчика</b>	
EVO	Осуществляется на уровне Облака Cloud.ru встроенными средствами подсистемы виртуализации.
Сетевой	Осуществляется средствами SDN.
Дополнительный	В рамках периодических тестирований на проникновение всей инфраструктуры проводятся тестирования на возможность проникновения потенциального нарушителя из одной «Организации» в другую с преодолением используемых механизмов защиты.

1.8. Распределение ролей, обязанностей и ответственности в области ИБ при использовании Услуги описано в таблице 2.

Таблица 2. Распределение ролей, обязанностей и ответственности в области ИБ

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/ услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/ сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
Прикладной уровень и уровень использования услуги Заказчиком	Журналирование событий	Журналирование событий в прикладном программном обеспечении (ППО).	Заказчик	Заказчик
	Управление доступом	Управление доступом к ППО.	Заказчик	Заказчик
	Управление аутентификационной информацией	Управление аутентификационной информацией, используемой для доступа к ППО.	Заказчик	Заказчик
	Обеспечение защиты персональных данных клиентов	Защита согласно 152-ФЗ персональных данных (ПДн) клиентов, обрабатываемых в рамках использования ППО.	Заказчик и Исполнитель	Заказчик
Уровень «Организации»	Управление аутентификационной информацией	Создание/удаление новых учётных записей в составе организации заказчика.	Исполнитель	Заказчик
Инфраструктурный уровень	Мониторинг и поддержка	Мониторинг инфраструктуры Услуги, обеспечение её доступности, производительности, наличия необходимого количества оборудования, обеспечение необходимой для её работы пропускной способности сети, вычислительных мощностей.	Исполнитель	Исполнитель
	Журналирование событий	Журналирование событий в компонентах и средствах защиты информации инфраструктуры Услуги.	Исполнитель	Исполнитель
	Управление доступом	Управление доступом к сегменту управления инфраструктурой Услуги.	Исполнитель	Исполнитель
	Управление конфигурацией	Контроль и управление процессами изменения конфигурации инфраструктуры Услуги.	Исполнитель	Исполнитель
	Управление безопасностью для виртуальных и физических сетей	Защита периметров ЦОД инфраструктуры Услуги с использованием кластеров высокопроизводительных межсетевых экранов нового поколения (NGFW), обеспечивающих межсетевое экранирование и защиту от компьютерных атак инфраструктуры. Внутреннее сегментирование сетевых инфраструктур EVO с использованием NGFW и выделением в рамках ЦОД на сетевом уровне DMZ, PROD- и MGMT-сегментов инфраструктуры.	Исполнитель	Исполнитель
	Установка и администрирование средств защиты	Установка, настройка и администрирование средств защиты информации в составе инфраструктуры, в том числе: Средств антивирусной защиты. Средств контроля действий привилегированных пользователей (администраторов Cloud) класса PIM&PAM. SIEM. Средств контроля и анализа защищенности. WEB Application Firewall (WAF), используемого для защиты публикуемых КУ EVO. NGFW. Identity and access management (IAM).	Исполнитель	Исполнитель
	Обеспечение защиты персональных данных клиентов	Защита ПДн сотрудников Заказчика, имеющих доступ к КУ EVO, обрабатываемых в инфраструктуре Исполнителя.	Исполнитель	Исполнитель

Таблица 2. Распределение ролей, обязанностей и ответственности в области ИБ

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/ услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/ сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
Физический уровень	Контроль доступа	Контроль доступа в ЦОД и помещения инфраструктуры EVO (охраняемая территория ЦОД, пропускной режим, системы контроля и управления доступом, запирающие стоек).	Исполнитель	Исполнитель
	Видеонаблюдение	Наличие внешней (по периметру ЦОД) и внутренней (в машинных залах ЦОД) систем видеонаблюдения.	Исполнитель	Исполнитель
	Размещение оборудования	Предоставление электропитания, доступа к сети интернет и свободного места в стойках ЦОД. Предоставление, монтаж и коммутация оборудования (compute, network) в стойках ЦОД.	Исполнитель	Исполнитель

1.9. Типы ресурсов, требования, рекомендации и ограничения, указаны в таблице 3.

Таблица 3. Типы ресурсов, описания, рекомендации и ограничения

Тип ресурса: Организация	
Описание	Рекомендации и ограничения
Организация – это главная родительская сущность, которая создается в момент подключения Услуги Заказчику. Организация в первую очередь предназначена для хранения общей информации в рамках нескольких проектов Заказчика.	
Тип ресурса: Проект	
Описание	Рекомендации и ограничения
Проект – это элемент управления ресурсами в рамках организации, который позволяет распределять облачные ресурсы между проектными задачами и командами. В каждом проекте можно подключать только нужные платформы и услуги.	
Тип ресурса: Зона доступности	
Описание	Рекомендации и ограничения
Зона доступности, или иначе Availability Zone (AZ), определяет принадлежность объектов виртуальной инфраструктуры одному физическому местоположению, в котором размещаются элементы инфраструктуры Исполнителя (вычислительные и сетевые ресурсы, устройства энергообеспечения и т. д.).	Заказчику доступно несколько зон доступности для построения собственной инфраструктуры, но при этом Заказчику недоступны возможности по созданию новых и управлению конфигурацией существующих зон доступности. Создание новых и управление конфигурацией существующих зон доступности является функцией Исполнителя. Если Заказчику необходимо получить новую или изменить конфигурацию существующей зоны доступности ему следует обратиться к Исполнителю.
Тип ресурса: Виртуальная машина (VM)	
Описание	Рекомендации и ограничения
При формировании Заказа Заказчику предоставляется выбор из набора образов VM, обладающих предопределённым набором количества виртуальных процессоров (vCPU), фиксированного объёма оперативной памяти (vRAM), фиксированного количества графических процессоров (GPU) <sup>1</sup> и уровнем переподписки процессора, используя которые он может создать виртуальную машину необходимой конфигурации. Заказчику доступно создание, модификация и удаление виртуальных машин из личного кабинета Облачной платформы. VM обслуживаются физическими процессорами Intel.	В рамках одной VM Заказчик может использовать процессоры только с одинаковой частотой (обслуживаемые процессорами одного типа).
Тип ресурса: Виртуальный диск (vDisk)	
Описание	Рекомендации и ограничения
В рамках услуги предоставляется один дисковый профиль. Заказчику доступно создание, модификация и удаление дисков из КУ EVO.	
Тип ресурса: Подсеть	
Описание	Рекомендации и ограничения
Подсети обеспечивают сетевое взаимодействие виртуальных машин. Заказчику доступно создание, модификация и удаление подсетей посредством КУ EVO.	
Тип ресурса: Интерфейс	
Описание	Рекомендации и ограничения
Интерфейс – это элемент инфраструктуры, обеспечивающий подключение виртуальной машины к подсети, с точки зрения обычного персонального компьютера это сетевая карта. Интерфейс может быть один или несколько, также в рамках управления трафиком на интерфейсы могут назначаться группы безопасности. Заказчику доступно создание, модификация и удаление интерфейсов из личного кабинета Облачной платформы.	
Тип ресурса: Публичный IP-адрес	
Описание	Рекомендации и ограничения
Публичный IP-адрес (Public IP) назначается виртуальной машине или NAT-шлюзу для обеспечения доступа в интернет или другие публичные сети. Публичный IP может быть арендован Заказчиком и переназначен от одной	

VM/NAT-шлюза Заказчика на другую VM/NAT-шлюз, принадлежащую ему.	
<b>Тип ресурса: Виртуальный sNAT-шлюз</b>	
<b>Описание</b>	<b>Рекомендации и ограничения</b>
sNAT-шлюз является компонентом облачной сетевой инфраструктуры, который позволяет осуществлять трансляцию внутренних частных IP-адресов во внешнюю (публичную) сеть, например для организации доступа из сети клиента в интернет с помощью одного публичного IP-адреса. В случае использования виртуального sNAT-шлюза пользователь освобождается от необходимости арендовать и назначать публичный IP-адрес всем своим виртуальным машинам, которые получают возможность выходить в интернет через один публичный IP-адрес, арендованный и назначенный клиентом sNAT-шлюзу.	
<b>Тип ресурса: Публичный ключ</b>	
<b>Описание</b>	<b>Рекомендации и ограничения</b>
Публичные ключи – это криптографические ключи, которые используются для идентификации пользователей при их подключении с помощью безопасных протоколов (например SSH) к принадлежащим им виртуальным машинам (открытый ключ размещается на VM, а ответный приватный ключ хранится у клиента).	
<b>Тип ресурса: Группа безопасности</b>	
<b>Описание</b>	<b>Рекомендации и ограничения</b>
Группа безопасности – это компонент услуги, выполняющий функции контроля трафика виртуальных машин. Функции, поддерживаемые данным компонентом услуги, позволяют установить разрешающие правила входящего и исходящего трафика для виртуальных машин в группе безопасности. Весь трафик, который явно не разрешен правилами, запрещен.	Группа безопасности назначается интерфейсу VM. У каждого интерфейса может быть свой набор групп безопасности. В случае если VM или её интерфейсу при создании не была назначена группа, то такая VM будет добавлена в группу безопасности по умолчанию.
<b>Тип ресурса: Тегирование объектов</b>	
<b>Описание</b>	<b>Рекомендации и ограничения</b>
Теги используются для маркировки объектов и сущностей, которые клиент создаёт и использует в процессе эксплуатации инфраструктуры, построенной на облачных сервисах. Назначение тегов, или иначе меток, позволяет клиенту ускорить процесс поиска и фильтрации интересующих его объектов.	
<b>Тип ресурса: Доступ к библиотеке образов</b>	
<b>Описание</b>	<b>Рекомендации и ограничения</b>
Образ виртуальной машины – это инструмент для создания виртуальной машины с предустановленной гостевой операционной системой, которая используется для быстрого развёртывания VM и минимизации усилий со стороны Заказчика при её создании. Заказчику предоставляется определённый набор общедоступных образов, создание и конфигурирование которых выполняется Исполнителем. Развёртывание образа виртуальной машины возможно только в той зоне доступности, в которую этот образ загружен.	
<b>Тип ресурса: Резервная копия</b>	
<b>Описание</b>	<b>Рекомендации и ограничения</b>
Сервис позволяет Заказчику создавать планы резервного копирования, формирующие полные и (или) инкрементальные резервные копии. Также Сервис обеспечивает хранение и восстановление (развёртывание) данных резервных копий на платформе Evolution в облачной среде <a href="https://cloud.ru">Cloud.ru</a> .	
<b>Тип ресурса: Пользовательский образ</b>	
<b>Описание</b>	<b>Рекомендации и ограничения</b>
Сервис, предоставляющий функциональность загрузки и хранения образов виртуальных машин или операционных систем для последующего разворачивания в облачной среде Cloud.ru.	

1.10. Для подключения к Услуге Заказчик может выбрать один или несколько типов подключения:

Таблица 4. Типы подключения к сети и сетевые сервисы

Тип подключения	Описание
Подключение через выделенный гарантированный канал Интернет	Заказчику предоставляется отдельная полоса для доступа к Услуге, которая не разделяется с другими Заказчиками
Подключение через общий канал Интернет (shared)	Предполагает логическое подключение к общему для всех Заказчиков Услуге каналу передачи данных (скорость сетевого соединения для каждого Заказчика не является гарантированной и зависит от загруженности общего канала передачи данных). Заказчику предоставляется базовая защита информационных систем, размещаемых в Инфраструктуре Облака Cloud.ru, от DDoS-атак, направленных на исчерпание канальной ёмкости сетевой Инфраструктуры Облака Cloud.ru. В остальных случаях, а также по запросу может быть предоставлена расширенная защита информационных систем Заказчика, размещаемых в Инфраструктуре Облака Cloud.ru, от DDoS-атак на всех уровнях до L7 включительно в виде отдельной тарифицируемой услуги. При этом для обмена данными между виртуальными машинами в пределах проекта клиента используется внутреннее сетевое взаимодействие, реализованное на базе сетевого оборудования Исполнителя и средствами гипервизора.

1.11. Подключение к сервису в Облаке Cloud.ru через сеть Интернет (NAT):

1.11.1. Пользователи подключаются к виртуальной машине в Облаке Cloud.ru через назначенный ей публичный IP-адрес, маршрутизируемый в сети Интернет. Данный сценарий рекомендуется использовать для предоставления доступа к публичному сервису через сеть Интернет.

1.11.2. Ограничения:

- один публичный IP-адрес на устройство (VM и/или виртуальный sNAT-шлюз) – для публикации нескольких приложений с одинаковыми портами TCP (80, 443 и т. д.) требуется выделение дополнительных публичных IP-адресов;
- для приложений с динамически выделяемыми портами (FTP, SIP, H.323 и т. д.) могут возникнуть проблемы с недоступностью сервиса - необходимо фиксировать диапазон динамически выделяемых портов в настройках приложения и прописывать их в правилах DNAT. Альтернативный вариант – выделять один публичный IP-адрес на сервис и настраивать правило Static DNAT.

1.12. В рамках базового набора предоставляемых функций, входящих в Услугу, и для каждого случая развёртывания виртуальной инфраструктуры в рамках EVO предоставляются следующие функциональные блоки:

- маршрутизация (Routing);
- преобразование адреса (NAT);
- динамическое распределение адресов DHCP.

1.13. Программная Платформа. Услуга реализована на базе платформы виртуализации разработанной и реализованной на основе решений с открытым исходным кодом доработанными Исполнителем для использования в целях развёртывания инфраструктуры Заказчика. В качестве инструмента реализации и поддержки работы облачной инфраструктуры используется программный контроллер собственной разработки.

Устойчивость к отказам вычислительных узлов реализована собственными программными средствами, входящими в состав платформы виртуализации, на базе технологии High Availability (HA).

1.14. Аппаратная Платформа

Таблица 5. Компоненты и характеристики аппаратной платформы

Компоненты	Характеристики
Вычислительные ресурсы	В качестве вычислительных ресурсов используются серверные решения корпоративного уровня, базирующиеся на процессорах архитектуры x86/64.
СХД	Для организации функций предоставления виртуальных дисков применяются системы хранения данных, построенные на программно-определяемом хранилище (SDS) собственной разработки.

Сеть	<p>Сеть построена на оборудовании ведущих мировых производителей, которое обеспечивает:</p> <ul style="list-style-type: none"> <li>– высокий уровень контроля и безопасности благодаря потоковой телеметрии и упреждающему анализу показателей работы сети (например, линейной скорости передачи данных, задержки и т. д.);</li> <li>– высокую производительность приложений благодаря интеллектуальным буферам и отсутствию потери пакетов;</li> <li>– высокую производительность и масштабируемость благодаря использованию высокоскоростных портов с различной пропускной способностью 1/10/25/50/100G.</li> </ul> <p>Сетевая подсистема реализована с применением технологий, которые обеспечивают следующие преимущества:</p> <ul style="list-style-type: none"> <li>– предсказуемость задержек;</li> <li>– высокий уровень масштабируемости без прерывания работы сети;</li> <li>– высокий уровень автоматизации управления и поддержки;</li> <li>– защита от появления сетевых петель.</li> </ul>
------	--

## 2. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И РЕСУРСЫ УСЛУГИ

### 2.1. Параметры Услуги (доступные Ресурсы Услуги)<sup>7</sup>.

Таблица 7. Параметры предоставляемой Услуги (Ресурсы Услуги)

Услуга	Тарифицируемый ресурс	Характеристики
Вычислительные Ресурсы	Виртуальная машина (шт.)	Количество vCPU на виртуальную машину (шт.)
		Объём vRAM на виртуальную машину (ГБ)
		Количество GPU на виртуальную машину (шт.)
		Время работы (час)
Хранилище данных	Виртуальный жесткий диск SSD (ГБ)	IOPS (эталонное значение)
		Среднее время доступа к vSSD на виртуальной машине (мс)
		Шаг увеличения размера vSSD в допустимом диапазоне (ГБ)
	Виртуальный жесткий диск HDD (ГБ)	IOPS (эталонное значение)
		Среднее время доступа к vHDD на виртуальной машине (мс)
		Шаг увеличения размера vHDD в допустимом диапазоне (ГБ)
Сеть	Публичный IP-адрес (шт.)	Длительность аренды (час)
		Длительность назначения на интерфейс виртуальной машины (час)
	Виртуальный NAT-шлюз (шт.)	Время работы Приватного sNAT-шлюза (час)
		Время работы Публичного sNAT-шлюза (час)
		Исходящий трафик (МБ) <sup>2</sup>
		Входящий трафик (МБ) <sup>3</sup>
Резервная копия	Объем резервной копии (ГБ)	Время хранения (час)
Пользовательский образ	Объем пользовательского образа (ГБ)	Время хранения (час)

## 3. ТАРИФИКАЦИЯ УСЛУГИ

3.1. Для данной Услуги используется Динамическая тарификация (Pay as you go), предполагающая оплату пула ресурсов, указанных выше, по факту их потребления Заказчиком в течение Отчетного периода.

3.2. Величина ежемесячного платежа за пользование Услугой определяется в соответствии с фактическим потреблением Ресурсов (п. 2.1. Приложения)

Окончательная стоимость Услуги в Отчётном периоде формируется на основании объёма потребленных Ресурсов и в соответствии с Тарифами, установленными в Приложении №7.EVO.1.

Посекундная тарификация, осуществляющаяся в почасовом порядке (из расчета стоимости 1 (одного) часа), начиная с первой секунды использования.

<sup>2</sup> Исходящий трафик, который был обработан sNAT-шлюзом на внешнем интерфейсе (публичном IP-адресе)

<sup>3</sup> Входящий трафик, который был обработан sNAT-шлюзом на внешнем интерфейсе (публичном IP-адресе)

#### 4. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

- 4.1. Возможные виды подключения / изменения / отключения Услуги:
- В отношении Виртуальных машин с GPU –в порядке, установленном п.4.4. Приложения.
  - В отношении иных типов ресурсов Услуги - совершение действий в Консоли Управления EVO.
- 4.2. Возможный порядок расчётов по Услуге:  
Предоплата<sup>4</sup>;  
Постоплата<sup>5</sup>;
- 4.3. Возможные способы оплаты / порядок пополнения Баланса:
- оплата в безналичном порядке на основании выставленного Исполнителем счёта;
  - оплата посредством электронных средств платежа.
- 4.4. Стороны установили следующий порядок Заказа Виртуальных машин с GPU по Приложению:
- 4.4.1. Подключение Услуги осуществляется Исполнителем на основании Запроса на изменение (ЗНИ)<sup>6</sup> через службу технической поддержки Исполнителя. Запрос должен быть направлен не позднее, чем за 6 (шесть) рабочих дней до желаемой даты начала потребления Услуги;
- 4.4.2. В течение 3 (трех) рабочих дней Исполнитель обязуется рассмотреть ЗНИ на подключение Услуги и направить ответ (информацию о подключении Услуги или отказ в её предоставлении Услуги);
- 4.4.3. В случае согласования Сторонами Заказа Услуги она предоставляется в дату начала её оказания (в соответствии с информацией в ЗНИ) с 10:00 по московскому времени.

#### 5. УРОВЕНЬ ПРЕДОСТАВЛЕНИЯ УСЛУГИ (SLA)

- 5.1. В соответствии с пп. 1.1.4 Приложения №2.EVO.0 вносятся следующие уточнения в уровень предоставления Услуги, действующий в отношении Услуг EVO по умолчанию.
- 5.1.1. Показатель Доступности Услуги<sup>7</sup> и Размеры компенсаций Заказчику за нарушение Доступности Услуг (п. 2.1.2. Приложения №2.EVO.0 к Договору) указаны в Таблице 2:

Таблица 2. Компенсации за нарушение целевых показателей Доступности Услуги

Доступность Ресурса за Отчётный период	Размер компенсации от стоимости Ресурса за Отчетный период
≥ 99,95 %	Компенсация не предоставляется
<99,95 %	10%
< 95,0 %	25%
< 90,0 %	50%

- 5.2. SLA не предоставляется на прерываемые виртуальные машины
- 5.3. Не учитывается как Время недоступности Услуги недоступность, связанная с нарушениями Заказчиком требований, установленных п. 1.8 Приложения, относящихся к его Зоне ответственности.
- 5.4. Для Услуги устанавливаются следующие особенности определения уровня Доступности:
- 5.4.1. Доступность рассчитывается отдельно для каждого Ресурса Услуги (п. 1.2. Приложения);
- 5.4.2. Недоступностью Услуги является:
- Невозможность подключиться/совершить авторизованный доступ к ВМ (п. 1.2.1. Приложения) в течение 5 (пяти) и более минут по причинам, зависящим от Cloud.ru<sup>7</sup>;
  - В отношении иных Ресурсов (п. 1.2.2. приложения) – невозможность обратиться к Ресурсу любыми способами, предусмотренными **Услугой**<sup>7</sup>, в течение 5 (пяти) и более минут по причинам, зависящим от Cloud.ru
- 5.4.3. Компенсация выплачивается пропорционально объёму недоступных Ресурсов Услуги, т.е. Компенсация за нарушение целевых показателей Доступности Услуги рассчитывается согласно количеству недоступных Ресурсов.
- 5.5. Во всем остальном в части предоставления Услуг применимы положения Приложения №2.EVO.0.

#### 6. ПОЛЬЗОВАТЕЛЬСКИЕ ОБРАЗЫ

<sup>4</sup> Является способом по умолчанию для физических лиц, присоединившихся к условиям Договора/Оферте путём акцепта (п. 1.5. Договора/Оферты)

<sup>5</sup> Является способом по умолчанию для юридических лиц

<sup>6</sup> См. Приложение № 2.0. к Договору

<sup>7</sup> Перечень доступных параметров Услуги размещен на сайте в разделе Тарифы <https://cloud.ru/documents/tariffs/evolution/evolution-compute?source-platform=Evolution>

<sup>7</sup> при условии, что настройки ВМ и сами запросы к ней и её Ресурсам составлены корректно

- 6.1. Пользовательские образы — это виртуальные дисковые образы, создаваемые и загружаемые Заказчиком в инфраструктуру Исполнителя для последующего развёртывания в рамках предоставляемой услуги IaaS.
- 6.2. Объём ответственности Заказчика за пользовательские образы включает, но не ограничивается следующим:
- размещение в образе программного обеспечения, данных, конфигураций и иных артефактов;
  - соответствие содержимого образа требованиям действующего законодательства РФ (в частности, о персональных данных, об интеллектуальной собственности, о недопустимости распространения вредоносного кода и т.п.) и Договора;
  - обеспечение надлежащего уровня защиты персональных данных, содержащихся в образе, а также иных конфиденциальных сведений;
  - управление доступом к образу (создание, изменение, удаление) и контроль за использованием образа в рамках своих проектов;
  - выполнение всех требований по журналированию, аудиту, реагированию на инциденты, связанных с пользовательским образом.
- 6.3. Исполнитель **не несёт ответственности** за любые нарушения, возникшие в результате размещения в пользовательском образе, в т.ч. в связи с:
- незаконным или вредоносным программным обеспечением, используемым Заказчиком;
  - нарушением прав третьих лиц (в т.ч. прав авторов и правообладателей);
  - утечкой, потерей или несанкционированным доступом к персональным данным и/или конфиденциальной информации, содержащимся в образе;
  - недоступностью или некорректной работой сервисов, построенных на основе такого образа, если причина связана с содержимым образа.
- 6.4. Нарушения, связанные с пользовательским образом, Заказчик обязан незамедлительно и самостоятельно устранить, и при необходимости, предоставить Исполнителю подтверждающие документы (отчёты сканирования, результаты аудита и т.п.).

## **7. ПЕРЫВАЕМЫЕ ВИРТУАЛЬНЫЕ МАШИНЫ**

- 7.1. Прерываемые виртуальные машины — это виртуальные машины, которые могут быть удалены в следующих случаях:
- В течение 24 часов или меньше с момента запуска виртуальной машины;
  - В любой момент, если требуется высвободить ресурсы для запуска стандартной виртуальной машины.
- 6.6. Создание прерываемых виртуальных машин доступно только в случае наличия свободных ресурсов;
- 6.7. Для создания прерываемых виртуальных машин используется ограниченный набор конфигураций;
- 6.8. Отказоустойчивость прерываемой виртуальной машины не гарантируется;
- 6.9. Тип виртуальной машины выбирается при создании виртуальной машины;
- 6.10. В случае автоматического удаления прерываемой виртуальной машины загрузочный диск удаляется вместе с ней, внешние диски остаются доступны и за них взимается стоимость согласно Тарифам.