ТЕНДЕРНОЕ ЗАДАНИЕ

Предоставление ресурсов облачной инфраструктуры

Указать № и предмет конкурса (тендера)

1. Предмет конкурса: Определение наилучшего предложения и заключение договора на аренду облачной платформы (вычислительных мощностей) для разворачивания, запуска и эксплуатации произвольных сервисов АО КБ «ЮНИСТРИМ»

2. ПО виртуализации и гипервизор любой из перечисленных:
   - VMware ESX
   - Microsoft Hype-V
   - KVM

3. Для оценки рассматривается **почасовая** оплата нижеследующих типов виртуальных серверов и типов дисковых хранилищ для виртуальных серверов:

Виртуальные сервера		**Текущие потребности**	
vCPU	**RAM (GB)**	**количество**	**общее время, ч/мес**
2	4	16	8582
2	8	4	2976
2	16	1	744
4	8	20	6036
4	16	8	3000
4	32	7	2545
8	16	22	11471
8	32	3	1696
8	64	3	1697
16	32	16	7986
16	128	1	744
24	96	2	1488
32	128	2	742
40	320	2	745

Типы дисковых хранилищ	GB - текущие потребности
Без гарантии по производительности (SATA)	30 000
С гарантированной производительностью 400 IOPS	3 000
С гарантированной производительностью 1000 IOPS	5 000
С гарантированной производительностью 3000 IOPS	2 000
С гарантированной производительностью 5000 IOPS	1 000
С гарантированной производительностью 10000 IOPS	5 000

4. **Общие требования:**
   - «Облачная» платформа должна быть расположена на базе двух или более ЦОД.
   - Пользователи должны иметь возможность самостоятельного управления составом и параметрами услуг, предоставляемых на базе «Облачной» платформы.
   - «Облачная» платформа должна обладать функционалом, позволяющим интегрировать виртуальные серверы Заказчика, запущенные на ее базе, с внешним физическим оборудованием Заказчика или Провайдера, размещенным в том же ЦОД Провайдера.
   - Услуги «Облачной» платформы должны предоставляться и оплачиваться по факту использования. Гранулярность учета услуг должна быть не более 1 часа.
   - «Облачная» платформа должна предоставлять информацию о текущем денежном балансе Заказчика в режиме реального времени самостоятельно (.csv, xml, pdf, xls)
   - Услуги должны оказываться без каких-либо авансовых платежей в начале отчетного периода.
   - Необходимость в оплате какого-либо минимального объема услуг в начале отчетного периода должна отсутствовать. В случае, если Заказчик не пользовался услугами в течение отчетного периода, Провайдер на должен выставлять ему счета по итогам отчетного периода.
   - Провайдер должен обладать как минимум следующими статусами для возможности предоставления в составе услуг «облачной» платформы программных продуктов от Microsoft по схеме ежемесячной подписки на них:
     - ✓ Gold Datacenter;
     - ✓ Silver Cloud Platform.
   - Возможность доступа к графической консоли серверов, запущенных на базе «облачной» платформы, при помощи веб-браузера.
   - «Облачная» платформа должна обладать документированными программными средствами управления (API).
   - «Облачная» платформа должна иметь справочную информацию на весь функционал, доступный Заказчику.
   - Возможность автоматического перезапуска виртуальных серверов ИТ-системы на альтернативных работоспособных физических серверах в случае выхода из строя физических серверов, на которых текущие виртуальные серверы размещались до аппаратного сбоя.
   - «Облачная» платформа должна иметь средство автоматизации для управления инфраструктурой посредством API.
   - Облачная платформа должна иметь файловый сервис совместимый по программному интерфейсу с AmazonS3.

5. **Требования к предоставляемым вычислительным ресурсам:**
   - Выделение вычислительных ресурсов (виртуальные ядра, оперативная память) должно осуществляться гарантированным образом, исключающим возможность взаимного влияния виртуальных серверов Заказчика, размещенных на одном физическом узле, друг на друга.
   - «Облачная» платформа должна иметь возможность создания крупных виртуальных машин (далее –ВМ) с ресурсами до 40 vCPU 320Gb RAM.
   - «Облачная» платформа гарантировано должна предоставлять возможность выделение не менее: **Процессоров - 560vCPU, Оперативной памяти - 2TB, дисковое пространство - 50TB**
   - «Облачная» платформа должна предоставлять возможность изменения объема вычислительных ресурсов без пересоздания ВМ.
   - Гарантированное размещения ВМ на разных физических узлах должно быть доступно в «Облачной» платформе.
   - «Облачная» платформа должна предоставлять возможность выбора ЦОД при запуске ВМ.
   - Логическое деление ВМ на группы с опцией раздельного биллинга должно быть доступно в «Облачной» платформе.
   - «Облачная» платформа должна предоставлять возможность запуска ВМ с драйверами для поддержки устаревших операционных систем.
   - «Облачная» платформа должна предоставлять возможность запуска ВМ с ОС Windows/Linux.
   - «Облачная» платформа должна предоставлять возможность создания виртуальных дисков разной производительности (SAS, SSD, Flash) через веб-интерфейс управления и через API.
   - «Облачная» платформа должна предоставлять возможность изменения производительности дисков «на лету».
   - Дисковые ресурсы должны быть доступны с гарантиями по IOPS на диск.
   - В «Облачной» платформе должны быть доступны диски повышенной производительности для размещения высоконагруженных баз данных с гарантированной производительностью не менее 100 000 IOPS на диск.
   - «Облачная» платформа должна предоставлять возможность по миграции данных между дисковыми ресурсами разной производительности «на лету» без остановки в предоставлении сервиса.
   - «Облачная» платформа должна позволять организовывать изолированные сетевые окружения, не доступные для других Заказчиков «Облачной» платформы.
   - Изолированные сетевые окружения «Облачной» платформы должны позволять управлять сетевой адресацией и маршрутизацией ИТ-инфраструктуры Заказчика.
   - «Облачная» платформа должна обладать функционалом по подключению внешних выделенных каналов связи Заказчиков.
   - Возможность назначения или удаления внешних IP-адресов виртуальным серверам при помощи «облачной» платформы.
   - «Облачная» платформа должна предоставлять возможность внешнего отказоустойчивого подключения на скорости до 40 Гбит/с.
   - Облачная» платформа должна иметь встроенные DNS, DHCP сервисы
   - Облачная» платформа должна предоставлять возможность IPSec VPN соединения.

- «Облачная» платформа должна предоставлять внешнее сетевое подключение, агрегированное из соединений не менее, чем от четырех независимых операторов связи
- «Облачная» платформа должна размещаться территориально распределено на двух ЦОД Провайдера, связанных между собой двумя независимыми оптическими трассами
- «Облачная» платформа должна обеспечивать внутреннее сетевое подключение по протоколу Infiniband между серверами и СХД с пропускной способностью не менее 56 Гбит/с

6. Требования к мониторингу:

- «Облачная» платформа должна предоставлять возможность настройки триггеров на метрики нагрузки CPU, сетей, производительности дисковых ресурсов с возможностью отправку уведомления по электронной почте.
- «Облачная» платформа должна предоставлять возможность мониторинга основных параметров ВМ:
  - ✓ загрузка vCPU, %;
  - ✓ загрузка сети, получено/передано МБ/сек;
  - ✓ загрузка сети, получено/передано сетевых пакетов/сек;
  - ✓ диск операции чтения/записи, IOPS;
  - ✓ диск чтение/запись, КБ/сек.

7. Требования к информационной безопасности:

- Возможность разделения информационной среды Заказчика в рамках «Облачной» платформы на несколько независимых виртуальных сетей.
- Возможность управления доступом к виртуальным сетям по различным портам и протоколам при помощи бесплатного встроенного межсетевого экрана.
- Возможность объединения серверов виртуальной платформы в одну виртуальную частную сеть (VPN) с физическими или виртуальными серверами Заказчика, расположенными на удаленной площадке или ЦОД Заказчика.
- Доступ к функциям программного управления (API) «Облачной» платформой должен быть предоставлен таким способом, чтобы не допускать компрометации системы безопасности даже при использовании небезопасных транспортных протоколов.
- Для доступа к функциям программного управления (API) «Облачной» платформой должен применяться протокол HTTPS. Сертификаты должны быть подписаны доверенными центрами сертификатов.
- Доступ к виртуальным Linux\UNIX серверам должен осуществляться посредством протокола SSH с использованием беспарольной аутентификацией по ключам. Виртуальная платформа должна предоставлять возможность управления ключами аутентификации (создание и удаление), а также обеспечивать доступный из виртуальной машины механизм для доставки публичных ключей в виртуальную машину в процессе её загрузки.
- Возможность организации защищенного доступа к серверам ИТ-системы с использованием IPsec VPN соединения.
- Наличие встроенного в виртуальную платформу межсетевого экрана, настраиваемого отдельно для каждой виртуальной сети, а также виртуальных сетей изолированных облачных окружений.
- Наличие результатов теста на проникновение со сроком исполнения не

более 1 года.

- Наличие у участника тендера документов, подтверждающих соответствие предлагаемого решения следующим требованиям:

a. Требования законодательства РФ в области защиты информации – Федеральные законы 149-ФЗ («Об информации, информационных технологиях и о защите информации»), 152-ФЗ («О персональных данных»), 242-ФЗ («О внесении изменений в отдельные законодательные акты РФ по вопросам осуществления государственного контроля (надзора) и муниципального контроля»), 161-ФЗ («О национальной платежной системе») и др.;
b. Положение ЦБ РФ №382-П по защите информации при обеспечении переводов денежных средств;
c. Требования ФСТЭК России и ФСБ России в области защиты информации – содержащие меры по защите персональных данных приказ ФСТЭК России №21 и Приказ ФСБ России №378, методические документы и разъяснения регуляторов; Соответствие требованиям, которые предъявляются для обеспечения до 3-го уровня защищенности ПДн включительно, подтверждающееся наличием аттестата соответствия требованиям защиты информации, установленным ФСТЭК России
d. Требования Центрального Банка РФ (ЦБ) в области защиты информации – отраслевой стандарт по обеспечению информационной безопасности (СТО БР ИББС) и рекомендации в области стандартизации (РС БР ИББС),
e. Требования ФСТЭК России и ФСБ России к лицензиатам по деятельности в области защиты информации;

8. Требования к сертификации «Облачной» платформы:

- Система учета потребляемых ресурсов должна иметь сертификат соответствия Россвязи.
- Наличие актуального сертификата на Облачную платформу PCI DSS

9. Требования к центру обработки данных:

- Провайдер должен иметь собственный датацентр, предназначенный для размещения оборудования и ИТ-систем Заказчиков.
- ЦОД Провайдера должен обладать следующими действующими сертификатами от международной аттестационной организации Uptime Institute:
  - ✓ Tier III Certification of Design Documents
  - ✓ Tier III Certification of Constructed Facility
  - ✓ Tier III Gold Certification of Operational Sustainability
- Провайдер должн иметь собственную круглосуточную (24x7) «горячую линию» и формализованные процессы обработки запросов Заказчика на сервисное обслуживание.
- Здание, в котором находится ЦОД Провайдера, должно находиться в собственности компании-претендента.
- Система бесперебойного электроснабжения, дублированная на всех уровнях: не менее 2 вводов от независимых районных подстанций, собственная РТП, двойное резервирование электрических линий между РТП и ИБП, 2 группы ИБП на полную мощность оборудования с временем автономной работы не менее 15 минут, 2 электрических линии от ИБП до помещения ЦОД (по одной от каждой группы), свой электрический щит для каждой линии в помещении ЦОД, не менее 2 кабелей питания на каждую стойку от разных щитов.
- ИБП должны размещаться в отдельном помещении с организацией доступа только для обслуживающего персонала и собственной установкой поддержания

климатических параметров.

- Система гарантированного электроснабжения (дизель-генератор) на полную мощность оборудования (включая инженерные системы ЦОД), запас топлива не менее чем на 5 часов работы на полную мощность с возможностью дозаправки топлива без прерывания работы ДГУ.
- Система кондиционирования с уровнем резервирования не ниже N+1.
- Система автоматического газового пожаротушения в помещениях машинного зала ЦОД, комнатах ИБП и ГРЩ.
- Круглосуточное видеонаблюдение в здании и машинном зале ЦОД с записью и хранением данных с видеокамер не менее 1 месяца.
- Система контроля доступа в помещение ЦОД с электронным журналированием прохода посетителей, не менее 3 периметров доступа – на входе в здание, на входе в часть здания, где расположены помещения ЦОД и вспомогательные помещения (комната ИБП и т.д.), и на входе в машинный зал ЦОД. Проходы каждого из периметров должны контролироваться видеокамерами и иметь возрастающую селективность доступа. Контроль доступа должен осуществляться при помощи электронной системы (электронные карты или система биометрического контроля).
- Круглосуточная охрана помещения ЦОД и всего комплекса зданий Провайдера, обеспечивающих функционирование ЦОД.
- Круглосуточная служба мониторинга состояния всей инфраструктуры ЦОД, включая каналы передачи данных.
- Хранение запчастей под сервисные контракты на складе в непосредственной близости от ЦОД.
- Круглосуточное нахождение в здании ЦОД сотрудников сервисной поддержки Провайдера, способных выполнить работы по ремонту и восстановлению оборудования.

10. Компании-участники должны предоставить по запросу следующие документы: решение о назначении (избрании) единоличного исполнительного органа юридического лица, действующего в настоящее время; приказ о вступлении в должность единоличного исполнительного органа юридического лица (генерального директора); бухгалтерский баланс за последний отчетный период с отметкой налогового органа; отчет о финансовых результатах за последний отчетный период с отметкой налогового органа.

11. Компании-участники конкурса должны присутствовать на рынке облачных провайдеров не менее 5 (Пяти) лет.

12. Компании-участники должны предоставить по запросу не менее 3(Трёх) положительных отзывов от клиентов по аналогичным конкурсам.

13. Для получения разъяснений по вопросам, связанным с предметом тендера просьба отправлять запрос на адрес: tender@unistream.com