

ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ (ТЕХНИЧЕСКОЕ ЗАДАНИЕ)
на оказание услуг по предоставлению вычислительных мощностей
для размещения цифровых сервисов для вычислений, хранения и
обработки данных для нужд Министерства юстиции Российской
Федерации

\

1. Общие сведения

1.1. Предмет оказываемых услуг.

Оказание услуг по предоставлению вычислительных мощностей для размещения на них Заказчиком цифровых сервисов для вычислений, хранения и обработки данных в объеме предусмотренном настоящим Техническим заданием.

1.2. Общие характеристики оказываемых услуг:

1.2.1. Срок оказываемых услуг – 6 месяцев с момента заключения государственного контракта.

1.2.2. Срок предоставления вычислительных мощностей для размещения на них Заказчиком цифровых сервисов для вычислений, хранения и обработки данных – 7 календарных дней с момента заключения государственного контракта.

1.2.3. Заказчик – Минюст России.

1.2.4. Исполнитель определяется по результатам проведения закупочных процедур.

1.2.5. Исполнитель оказывает услуги в объеме и по ценам, указанным в спецификации, исходя требований к программно-техническим компонентам ЦОД, предоставляемых Заказчику, предусмотренных разделом 8 Технического задания.

1.2.6. Заказчик самостоятельно выбирает и использует сервисы путем их заказа в Платформе. Учет выбранных и заказанных сервисов, а также лимит, ведется Платформой и определяется учетными данными Заказчика.

1.2.7. Результаты оказанных Заказчику услуг фиксируются Актом сдачи-приемки оказанных услуг в соответствии с государственным контрактом.

2. Термины и сокращения

- **Инфраструктура** - Совокупность технических и программных средств для оказания услуг Заказчику по государственному контракту
- **Серверная стойка, стойка** - конструкция для размещения и подключения технической Инфраструктуры Исполнителя для оказания услуг или для размещения серверного оборудования Заказчика.
- **Платформа** - портал самообслуживания, веб-служба (идентифицируемая уникальным веб-адресом (URL-адресом) программная система со стандартизированными интерфейсами) или личный кабинет, позволяющие удаленно использовать Сервисы платформы, управлять ими, вести их учет, в том числе, но не ограничиваясь, использовать в режиме реального времени для осуществления Заказчиком удаленных обработки, хранения и

распространения информации, а также предназначенная для общего учета Сервисов, их использования и коммуникации с Исполнителем.

- **Центр обработки данных, ЦОД** - Технологическая площадка Исполнителя, на которой размещена инфраструктура Исполнителя, обеспечивающая функционирование Платформы и Сервисов.
- **Пользовательские данные** - Информация для осуществления входа в Платформу, обрабатываемая в инфраструктуре Исполнителя.
- **Сервис платформы, Сервис** - Инфраструктура Исполнителя предоставляемая в качестве услуг, обладающая функциональностью предоставления Заказчику в оперативное управление масштабируемых вычислительных мощностей и обеспечивающая в интересах Заказчика обработку, хранение и распространение информации, а также иные функции
- **CLI** - Интерфейс управления Платформой (Command Line Interface).
- **SDK** - Средства разработки (Software Development Kit).
- **vCPU** - Виртуальный процессор (Virtual Central Processor Unit).
- **GPU** - Графические ускорители (Graphics Processing Unit) - графический процессор с повышенной производительностью для использования при сложных вычислениях.
- **RAM** - Оперативная память (Random Access Memory).
- **SLA** - Соглашение об уровне обслуживания (Service Level Agreement).
- **СУБД** - Система Управления Базами Данных.
- **IOPS** - Input/output Operations Per Second, число операций ввода/вывода, выполняемое дисковой подсистемой в секунду. Операция ввода/вывода – операция чтения или записи, выполняемая дисковой подсистемой.
- **CUDA** - Compute Unified Device Architecture - Вычислительная Унифицированная Архитектура Устройства.
- **Tensor** - Тензорные ядра, специализированные блоки графического процессора для машинного обучения, значительно повышающие скорость тренировки моделей, позволяющих решать задачи глубокого обучения.
- **DRaaS** - аварийное восстановление в облаке как сервис.

3. Требования к Инфраструктуре Исполнителя

3.1. Общие требования

- 3.1.1. Заказчику предоставляется Доступ к личному кабинету, позволяющий удаленно использовать Сервисы платформы.
- 3.1.2. Все ЦОД и оборудование в рамках Инфраструктуры Исполнителя, необходимые для оказания услуг по государственному контракту,

должны находиться в собственности или на условиях эксклюзивной аренды у Исполнителя.

- 3.1.3. ЦОД и все его инженерные системы должны соответствовать уровню надежности не ниже TIER III по классификации Uptime Institute.
- 3.1.4. В целях отказоустойчивости Сервисов должна быть возможность задействования не менее двух инженерно-независимых ЦОД, где каждый ЦОД изолирован от аппаратных и программных сбоев в другом ЦОД. Необходимость обусловлена требованиями к обеспечению полной независимости инфраструктурных площадок и реализации возможности использования технологии высокодоступного георезервирования и синхронизации данных.
- 3.1.5. Каждый 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.
- 3.1.6. В ЦОД должна быть возможность подключения не менее чем к пяти независимым телеком-провайдерам на скоростях не менее 10Гбит/с.
- 3.1.7. Каждый ЦОД должен обладать собственным охраняемым периметром, оборудованным системами наблюдения. Оператор вычислительной платформы должен иметь на объекте собственную службу физической охраны.
- 3.1.8. Каждый ЦОД должен находиться на территории Российской Федерации, из которых не менее одного ЦОД - на территории г. Москва.
- 3.1.9. Размещение всех компонентов Инфраструктуры Исполнителя 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 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», в частности ч. 4 ст. 16.

3.2. Электропитание в ЦОД

- 3.2.1. Система внешнего электроснабжения ЦОД должна включать не менее двух взаиморезервируемых вводов от городской сети. Питание ЦОД должно осуществляться от разных взаиморезервируемых распределительных трансформаторных подстанций (далее - ТП).
- 3.2.2. Система бесперебойного электроснабжения должна быть выполнена на основе взаимно резервирующих систем ИБП с уровнем надежности, определяемым не ниже, чем уровень TIER III (соответствии с классификацией Uptime Institute). Для ЦОД система бесперебойного электроснабжения должна в нормальном режиме работы получать питание от двух независимых вводов электроснабжения, при отсутствии

напряжения на внешних вводах – питание от системы гарантированного электроснабжения. Система бесперебойного электропитания для размещаемого ИТ-оборудования должна осуществляться от 1-ой особой категории электроснабжения, с резервированием по схеме 2N, или по топологии 3/2N, 4/3N, 5/4N и т.д.

- 3.2.3. Инженерные системы должны быть зарезервированы на всем своем протяжении, должны быть в наличии несколько линий распределения электропитания и резервирование охлаждения.
- 3.2.4. Расположение взаиморезервируемых линий электроснабжения должны быть выполнены в разных кабеленесущих системах, в соответствии с требованиями действующих нормативных документов.
- 3.2.5. Для обеспечения гарантированного электроснабжения, ЦОД должен быть обеспечен системой гарантированного электроснабжения с уровнем надежности, определяемым не ниже, чем уровень TIER III (соответствии с классификацией Uptime Institute). Хранилище дизельного топлива должно быть объемом, обеспечивающим работу ДГУ для обеспечения 100% критически важной нагрузки ЦОД в течение не менее 12 (двенадцати) часов. Исполнитель должен иметь не менее двух действующих договоров с топливной компанией на подвоз необходимого объема топлива автоцистернами, для обеспечения бесперебойной работы в течение 60 (шестидесяти) часов.
- 3.2.6. Система рабочего освещения предназначена для обеспечения требуемого уровня освещенности в помещениях ЦОД при повседневной эксплуатации, и должна удовлетворять следующим требованиям: Освещенность помещения машинного зала должна быть не менее 300Лк на высоте 0,8 м от уровня пола.

3.3. Требования к организации электроснабжения стоек

- 3.3.1. Подключение стоек осуществляется через разъем IEC 60309, степень защиты разъема IP44 (или иное по согласованию с Заказчиком). Разъем для подключения стоек должны находиться не далее 2 метра от стойки, и быть защищены автоматами соответствующего номинала.
- 3.3.2. PDU каждой стойки должны подключаться к независимым взаимно резервируемым вводам электропитания. Каждая стойка должна быть заземлена на общую шину помещения ЦОД медным проводом сечением не менее 6 мм². Каскадное заземление стоек не допускается.
- 3.3.3. При подключении новых стоек к системе электроснабжения ЦОД, допускается снижение надежности в электропитании и охлаждении до N+1 уже подключенных стоек.

3.4. Система молниезащиты и уравнивания потенциалов в ЦОД

- 3.4.1. На вводе в здание или в машинный зал должна быть предусмотрена система уравнивания потенциалов, соответствующая ГОСТ 464-79.
- 3.4.2. Для борьбы с перенапряжениями в групповой и распределительной сети, для защиты электроники от импульсов перенапряжений должно применяться устройство защиты от

импульсных перенапряжений, соответствующее ГОСТ IEC 61643-11-2013.

3.5. Система охлаждения ЦОД

- 3.5.1. Система охлаждения в серверной должна обеспечивать следующие параметры окружающей среды в холодном коридоре машинного зала:
 - о Температура от 20 °С до 28 °С.
 - о Точки нормальной настройки: 24 °С.
 - о Точность поддержания температуры: ± 4 °С.
 - о относительная влажность от 25% до 65%; с точностью $\pm 10\%$
- 3.5.2. Все элементы системы охлаждения должны быть выполнены по уровню надежности не ниже, чем TIER III (в соответствии с классификацией Uptime Institute) с резервированием по оборудованию не ниже, чем N+1. Производительность по холоду системы холодоснабжения без учета резервирования должна быть выше тепловыделения от размещаемого оборудования на Объекте. Все компоненты системы холодоснабжения должны быть запитаны по по двум взаиморезервируемым вводам.
- 3.5.3. Система кондиционирования позволяет охлаждать оборудование стойки без применения дополнительных мер со стороны Заказчика.

3.6. Система пожаротушения в ЦОД

- 3.6.1. Должна быть обеспечена работа системы автоматического газового пожаротушения в помещениях машинного зала ЦОД, комнатах ИБП, ГРЩ и электрощитовой ЦОД, резервный запас огнетушащего газа должен быть инсталлирован в систему и подключаться после расходования основного.
- 3.6.2. ЦОД должен быть оснащен системой пожарной безопасности и системой автоматического газового пожаротушения (со световой и звуковой сигнализацией), оборудован комплексом средств сверхраннего обнаружения дыма.
- 3.6.3. Системы пожарной безопасности и пожаротушения ЦОД, должны иметь необходимые сертификаты пожарной безопасности, должны быть выполнены в соответствии с требованиями действующих норм пожарной безопасности РФ.
- 3.6.4. Срабатывание системы пожаротушения не должно выводить из строя размещенное и не поврежденное пожаром оборудование.
- 3.6.5. АПС (автоматическая система пожарной сигнализации) должна быть предназначена для:
 - о обнаружения очагов пожара в контролируемых помещениях;
 - о формирования сигнала «Пожар» для оповещения дежурного персонала;
 - о формирования управляющих сигналов для систем противопожарной автоматики;

- о инженерных систем, системы оповещения и управления эвакуацией людей при пожаре;
- о контроля состояния элементов систем, управляемых от АПС;
- о отображения и протоколирования информации о событиях в системе и действиях оператора.

3.6.6. Количество пожарных извещателей, устанавливаемых в каждом помещении, должно соответствовать требованиям СП 485.1311500.2020.

3.6.7. Расстановка пожарных извещателей в помещениях должна быть принята согласно, СП 485.1311500.2020.

3.6.8. В здании Центра обработки данных, должна быть система оповещения и управления эвакуацией людей при пожаре 2 типа, что предполагает звуковой и световой способы оповещения, которая должна состоять из:

- о световые табло «ВЫХОД»;
- о звуковые оповещатели;
- о настенные звуковые оповещатели.

3.6.9. Количество звуковых оповещателей, их расстановка и мощность должны обеспечивать уровень звука во всех местах постоянного или временного пребывания людей в соответствии с СП 3.13130.2009.

3.6.10. Контроль и управление системами противопожарной защиты каждого машинного зала должен быть из помещения Центрального пожарного поста (диспетчерская), с постоянным (круглосуточным) пребыванием дежурного персонала.

3.7. Требования к системе мониторинга инфраструктуры инженерных систем ЦОД

3.7.1. Исполнитель должен обеспечить в режиме 24x7x365(6) мониторинг инфраструктуры инженерных систем своего ЦОД.

3.7.2. В ЦОД должна функционировать система мониторинга и управления, предназначенная для управления технологическими процессами, а также мониторинга состояния и, при возможности, ручного местного управления следующим инженерным оборудованием:

- о система пожарной сигнализации и газового пожаротушения;
- о система кондиционирования;
- о система гарантированного электроснабжения;
- о система бесперебойного электроснабжения.

3.7.3. Автоматизированная система мониторинга и управления ЦОД должна обеспечивать следующей функциональностью:

- о сбор информации со штатных систем управления инженерными системами;

- о получение информации о работе оборудования и различных параметрах от независимых датчиков и преобразователей;
 - о непрерывный анализ поступающей информации и выдача сигналов о выходе параметров из допустимых пределов;
 - о автоматическое управление инженерными системами в случае аварийных ситуаций;
 - о архивирование поступающей информации;
 - о протоколирование действий персонала.
- 3.7.4. Исполнитель должен обеспечить в режиме 24x7x365(6) дежурство специалистов, обслуживающих инфраструктуру и инженерные системы ЦОД.
- 3.7.5. Исполнитель должен использовать автоматизированную систему диспетчеризации и управления для сбора оперативной и статистической информации о работе инженерных систем и технологического оборудования.
- 3.7.6. Исполнитель должен обеспечить оповещение в случае сбоя в работе инженерных систем ЦОД ответственных работников Заказчика посредством электронной почты и/или иными каналами связи.

3.8. Требования по безопасности ЦОД

- 3.8.1. Круглосуточное видеонаблюдение в здании и машинном зале ЦОД с записью и хранением данных с видеокамер не менее 3-х месяцев.
- 3.8.2. 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.
- 3.8.3. Глубина хранения данных по логам системы доступа должна составлять не менее 3-х месяцев.
- 3.8.4. Круглосуточная охрана помещения ЦОД и всего комплекса здания, обеспечивающих функционирование ЦОД.

3.9. Требования к квалификации и соответствию Исполнителя и его Инфраструктуры законодательству Российской Федерации в области защиты информации

- 3.9.1. Исполнитель должен являться резидентом Российской Федерации и при осуществлении своей деятельности соблюдать все требования законодательства Российской Федерации. Инфраструктура и вычислительные мощности, должны быть размещены на территории Российской Федерации.
- 3.9.2. Исполнитель должен иметь следующие лицензии (наличие подтверждается копией):

- Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации;
- Лицензия ФСТЭК России на деятельность по разработке и производству средств защиты конфиденциальной информации;
- Лицензия Федеральной службы по надзору в сфере связи и массовых коммуникаций на услуги по предоставлению каналов связи;
- Лицензия Федеральной службы по надзору в сфере связи и массовых коммуникаций на телематические услуги связи;
- Лицензия Федеральной службы по надзору в сфере связи и массовых коммуникаций на оказание услуг связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации;
- Лицензия ФСБ России на деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

4. Общие требования к Платформе, а также к доступу и управлению

- 4.1.1. Платформа должна обеспечивать централизованный доступ ко всем Сервисам и функциям Платформы.
- 4.1.2. Наличие следующих средств доступа и управления у Платформы:
 - WEB интерфейс;
 - Программный интерфейс (API).
- 4.1.3. Наличие у Платформы многопользовательского доступа с возможностью назначения прав и полномочий в соответствии со следующим разграничением ролей:
 - «Наблюдатель», обладающая разрешениями на чтение к ресурсам;
 - «Администратор», обладающая всеми разрешениями роли «Наблюдатель» и разрешениями на все операции для управления ресурсом Сервисов, кроме назначения ролей другим пользователям;
 - «Администратор пользователей», обладающая доступом к управлению пользователями и без доступа к операциям для управления ресурсом Сервисов. Первого Администратора пользователей создает Владелец;

- «Владелец», обладающая всеми разрешениями на Платформе. Владелец может выполнять любые операции с Сервисами и ресурсами в них, в том числе выдавать доступ к Платформе другим пользователям: назначать им роли и отнимать их.
- 4.1.4. Доступ к WEB интерфейсу Платформы должен осуществляться с применением двухфакторной аутентификации.
- 4.1.5. Платформа должна предоставлять возможность разграничения доступа по ролям уровня самой Платформы проекта, с уровнем доступа к вычислительным ресурсам.
- 4.1.6. Платформа обеспечивает возможность создания системы разграничения доступа к виртуальной среде Сервисов с использованием проектов.
- 4.1.7. Платформа должна предоставлять интерфейс для отображения информации об объектах Сервисов.
- 4.1.8. Платформа должна предоставлять интерфейс для управления ресурсами и объектами Сервисов.
- 4.1.9. Платформа должна предоставлять интерфейс для управления жизненным циклом внутренних доступов пользователей.
- 4.1.10. Платформа должна предоставлять интерфейс для управления жизненным циклом проектов (создание, изменение, удаление, управление квотами) Сервисов.
- 4.1.11. Платформа должна предоставлять интерфейс для управления ресурсными квотами Сервисов.
- 4.1.12. Платформа должна предоставлять интерфейс для отображения информации о проекте (ресурсы, квоты, тарифы, и пр.) Сервисов.
- 4.1.13. Сервисы в случае, если они предполагают взаимное использование реализуемой функциональности и механизмов, должны иметь прямую интеграцию между собой, позволяющую осуществлять централизованное конфигурирование и сопряжение Сервисов через Платформу.
- 4.1.14. Платформа должна иметь функциональность по формированию сводного отчета об использованных ресурсах Сервисов и детализацию расходов с разбиением по:
 - «Проектам» - совокупности Сервисов, объединённых под одной учетной записью «Владельца»;
 - Отдельным Сервисам.

5. Функциональные требования к возможностям Сервисов

- 5.1. Сервисы предоставления облачных вычислительных мощностей должны обеспечивать Заказчику самостоятельное гибкое изменение объема потребляемых вычислительных ресурсов.
- 5.2. Сервисы предоставления облачных вычислительных мощностей должны обеспечивать единство управления вычислительными ресурсами, не допускается размещение части ресурсов на нескольких гетерогенных платформах и/или гипервизорах.
- 5.3. Сервисы предоставления облачных вычислительных мощностей должны обладать функциональностью непрерывного мониторинга работы виртуальных машин и инфраструктуры. В случае нарушения работоспособности сообщать информацию через портал управления ресурсами, в котором Заказчик должен иметь возможность настройки уведомлений по электронной почте. Сбор метрики в рамках мониторинга должен осуществляться в автоматическом

режиме, а также позволять осуществлять визуализацию собранных метрик в виде чартов/графиков/дашбордов, доступных к просмотру из Платформы.

- 5.4. Сервисы предоставления облачных вычислительных мощностей должны предоставлять возможность группировки облачных ресурсов в проекты по типу ресурса или группе целевых пользователей для возможности централизованного управления облачными ресурсами и управления правами доступа на уровне проектов. Сервис должен сопровождаться публичной документацией.
- 5.5. Инфраструктура виртуализации в Сервисах предоставления облачных вычислительных мощностей должна быть построена по схеме N+1, т.е. должна сохраняться полноценная работоспособность при отказе одного узла виртуализации.
- 5.6. Должна быть возможность получения в Платформе аналитической информации в виде графиков. Графики должны отображать значения считанной по метрикам информации с момента ее создания по настоящий момент времени (на момент просмотра графика).
- 5.7. Сервисы предоставления облачных вычислительных мощностей должны обладать разнообразными инструментами управления с авторизацией: графический интерфейс (GUI), CLI, API, SDK (Python, Node.js.) для автоматизации базовых операций. Все инструменты сопровождаются публичной документацией и примерами использования.
- 5.8. Сервисы предоставления облачных вычислительных мощностей должны предоставлять возможность Заказчику создавать виртуальные машины через веб-консоль, инструменты командной строки, terraform, API.
- 5.9. Сервисы предоставления облачных вычислительных мощностей должны предоставлять возможность Заказчику самостоятельно делать мгновенные снимки диска виртуальной машины (snapshot). Созданные снимки должны быть автоматически доступны во всех ЦОД. Данная возможность не заменяет собой резервного копирования на уровне Исполнителя.
- 5.10. Сервисы предоставления облачных вычислительных мощностей должны иметь возможность гибкой настройки количества и объемов виртуальных жестких дисков, подключенных виртуальной машине.
- 5.11. Исполнитель должен предоставить доступ к публичной документации с описанием технических особенностей Сервисов.
- 5.12. Сервисы предоставления облачных вычислительных мощностей должны обеспечивать запуск виртуальных машин на других узлах платформы виртуализации, при выходе из строя одного из них.

6. Требования к составу и характеристикам Сервисов

6.1. Сервис «Облачные серверы»

- 6.1.1. Сервис для предоставления масштабируемых облачных вычислительных мощностей в виде виртуальных машин, используемых для вычислительных ресурсов, обработки и хранения данных Заказчика.

- 6.1.2. Платформа виртуализации должна быть зарегистрирована в едином реестре российских программ для электронных вычислительных машин и баз данных, созданного в соответствии со статьей 12.1 Федерального закона «Об информации, информационных технологиях и о защите информации».
- 6.1.3. Сервиса должен быть реализован как выделенный сегмент облачной платформы соответствующий требованиям по информационной безопасности, предъявляемым для размещения информационных систем персональных данных и государственных информационных систем (приказ ФСТЭК России № 117 от 11.04.2025г., приказу ФСТЭК России № 21 от 18.02.2013г. (подтверждается аттестатом соответствия):
- государственные информационные системы (ГИС) до первого класса защищенности (К1) включительно;
 - информационные системы персональных данных (ИСПДн) до первого уровня защищенности (УЗ-1) включительно;
 - автоматизированные системы (АС) в защищенном исполнении класса 1Г.
 - Правилам применения мер обеспечения информационной безопасности при использовании облачных служб ISO/IEC 27017;
- 6.1.4. Платформа, на которой предоставляются сервисы виртуализации, должна обеспечивать запуск виртуальных машин на других узлах платформы виртуализации, при выходе из строя одного из них.
- 6.1.5. Заказчику должна быть предоставлена возможность самостоятельного мониторинга текущего состояния виртуальных машин, доступ к их консоли, возможность управления выключением/включением/перезагрузкой.
- 6.1.6. Заказчику должны быть предоставлена возможность изменения параметров вычислительных ресурсов под каждую конкретную виртуальную машину.
- 6.1.7. Хранение данных виртуальных машин (виртуальных дисков, снимков и пр.) должна осуществляться в программно-определяемой системе хранения данных платформы виртуализации, данные должны храниться не менее чем в 3 копиях, на независимых друг от друга серверах, расположенных в разных стойках.
- 6.1.8. Платформы должна предоставить Заказчику возможность:
- Создания/удаления ВМ;
 - Изменения характеристик ВМ в части CPU, RAM, а также дискового пространства;
 - Выбора ОС для создаваемых ВМ - 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.
- 6.1.9. Платформа обеспечивает отслеживание информации следующих типов:
- Метрики состояния ВМ;
 - Загруженность процессора;

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

- 6.1.10. Исполнитель должен обеспечить возможность использования балансировщиков нагрузки для балансировки трафика на определенные порты виртуальных машин Заказчика.
- 6.1.11. В качестве процессора узлов виртуализации должны использоваться процессоры AMD EPYC 9274F (24x4.05 ГГц SMT), либо аналог.
- 6.1.12. Допустимый коэффициент переподписки CPU не должен превышать 1:1.
- 6.1.13. ЛВС должна обеспечить возможность связи ВМ друг с другом и с дисковыми подсистемами с пропускной способностью не менее 5 Гбит/с.
- 6.1.14. Заказчику должна быть предоставлена возможность организовать связность по технологии L3VPN с каким-либо ЦОД-ом, не принадлежащим Исполнителю.
- 6.1.15. Должна быть возможность осуществлять резервное копирование виртуальных машин.
- 6.1.16. Возможность создания резервных копий и восстановления виртуальных машин без использования специализированных агентов средствами самой платформы виртуализации.
- 6.1.17. Возможность создания облачных серверов на выделенном хосте
- 6.1.18. Сервис должен предоставлять возможность работы не менее чем с 6 типами дисков:

- Локальный SSD-диск - быстрый диск, подключаемый напрямую к серверу вычислений через интерфейс PCIe по NVMe-протоколу;
- Сетевой базовый HDD-диск — стандартный сетевой диск, сетевое блочное хранилище на HDD-накопителе, не менее 320 IOPS;
- Сетевой базовый SSD-диск - стандартный сетевой диск, сетевое блочное хранилище на SSD-накопителе, не менее 640 IOPS;
- Сетевой универсальный SSD-диск - сетевой диск, сетевое блочное хранилище на SSD-накопителе, не менее 7000 IOPS;
- Сетевой универсальный SSD-диск с конфигурируемым значением IOPS - сетевой диск, сетевое блочное хранилище на SSD-накопителе с возможностью выбора необходимого значения IOPS в диапазоне от 2000 до 16000 IOPS
- Сетевой быстрый SSD-диск - сетевой диск, сетевое блочное хранилище на SSD-накопителе, не менее 25000 IOPS;

- 6.1.19. Сервис должен 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.

6.2. Дополнительные услуги и сервисы

- 6.2.1. В рамках оказания услуг должны предоставляться:

- 6.2.1.1. Сертифицированный ФСТЭК Межсетевой экран (МЭ) - программно-аппаратный или программный комплекс, использующийся для фильтрации сетевого трафика и построения VPN-туннелей, должен предусматривать возможность выбора аппаратного или виртуального решения,

- сертифицированного или несертифицированного ФСТЭК, с возможностью кластеризации. Тип МЭ - Usergate VE250 (8 Гбит/с, IPS - 1,3 Гбит/с, SSL VPN - 0,3 Гбит/с), либо аналог.
- 6.2.1.2. ГОСТ-VPN - сервис предоставления технической возможности организации защищенного канала связи с использованием криптографических алгоритмов ГОСТ на базе сертифицированного ФСБ средства криптографической защиты информации (СКЗИ) класса КСЗ между площадкой Исполнителя и Заказчика. Сервис предоставляет возможность организации и настройки одного Межсетевого взаимодействия между Сетью ViPNet Исполнителя и Сетью ViPNet Заказчика. Пропускная способность защищенного канала связи - не ниже 100 Мбит/сек. Реализация должна быть осуществлена на базе оборудования соответствующего требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КСЗ (иметь сертификат соответствия), а также находиться в периметре контролируемой зоны Исполнителя.
- 6.2.1.3. Предоставление доступа к программному обеспечению двухфакторной аутентификация «Мультифактор» с сертификатом ФСТЭК, или аналог.

7. Требования к технической поддержке

В рамках оказания услуг по государственному контракту Исполнитель обязан оказывать круглосуточную техническую поддержку в режиме 24x7x365 (24 часа в сутки, 7 дней в неделю).

В рамках техподдержки предоставляется следующая информация:

- Контактный номер телефона «горячей линии»;
- Адрес электронной почты технической поддержки;
- По запросу номер заявки по инциденту, в котором указывается время и описание инцидента;
- По запросу информирование Заказчика по основным этапам работ по устранению инцидента.

Время реакции¹ на инциденты:

Приоритет	Время реакции	Пример инцидента
Критический	15 мин	Недоступность инфраструктуры
Значительный	15 мин	Снижение качества предоставления Сервисов
Умеренный	15 мин	Незначительное или низкое влияние на

¹ период времени между регистрацией Исполнителем обращения Заказчика и первой обратной связью от Исполнителя.

		Сервисы Заказчика
Низкий	15 мин	Консультации, рекомендации

Исполнитель гарантирует устранение инцидентов в течение установленного времени реакции в 99% случаев от общего числа зарегистрированных инцидентов за период оказания услуг.

Исполнитель ежемесячно не позднее 15 числа предоставляет Заказчику отчет об оказанных услугах с указанием их состава и периода предоставления за отчетный период. Статистика обращений (тикетов) Исполнителя с детализацией времени реакции и решения должны отображаться в личном кабинете Заказчика.

Техническая поддержка должна включать:

- Консультации по сервисам и функциональным возможностям Сервисов;
- Предоставление документации по Сервисам;
- Консультации по вопросам, связанным с биллингом, настройка бюджетирования проектов Заказчика на базе Сервисов;
- Диагностика ошибок в работе Сервисов и решение выявленных проблем;
- Восстановление доступа в Платформу и консоль управления Сервисами;
- Круглосуточную службу мониторинга состояния всей инфраструктуры ЦОД, включая каналы передачи данных;
- Круглосуточное нахождение в здании ЦОД сотрудников поддержки, способных выполнить работы (услуги) по ремонту и восстановлению оборудования.

8. Требования к программно-техническим компонентам ЦОД:

№ п.п	Наименование	Ед. изм.	Кол-во ед. изм.*
1.1.	Оперативная память (RAM)	ГБ	1372
1.2.	Процессорные ядра (vCPU)	ядро	336
1.3.	Сетевой универсальный SSD-диск	ГБ	2800
1.4.	Графическая карта (GPU) RTX 6000 Pro, 96 ГБ	шт.	7
1.5.	Предоставление доступа к программному обеспечению Astra Linux 1.8 Воронеж	шт.	7
1.6.	Сертифицированный межсетевой экран UserGate VE250	шт.	2
1.7.	Сервис ГОСТ-VPN на базе 2xViPNet HW100 (в кластерном исполнении)	шт.	1
1.8.	Предоставление доступа к программному	шт.	5

	обеспечению «Мультифактор» (Двухфакторная аутентификация)		
--	---	--	--

* Указан максимальный возможный объем вычислительных ресурсов, доступность которых Исполнитель обязан обеспечить Заказчику для самостоятельного заказа.

** С учетом N+1 отказоустойчивости хостов облака.

Все результаты произведенных вычислений, отчеты и иные данные, созданные Заказчиком по государственному контракту, принадлежат Заказчику.

Виртуальные машины, предоставляемые с использованием графических процессоров (GPU), должны передаваться Заказчику полностью настроенными для эксплуатации: с предустановленными, работоспособными и совместимыми с используемой операционной системой версиями драйверов GPU и сопутствующего программного обеспечения (включая CUDA и иные компоненты, необходимые для работы вычислительных нагрузок Заказчика), обеспечивающими корректное определение и доступность GPU средствами операционной системы.