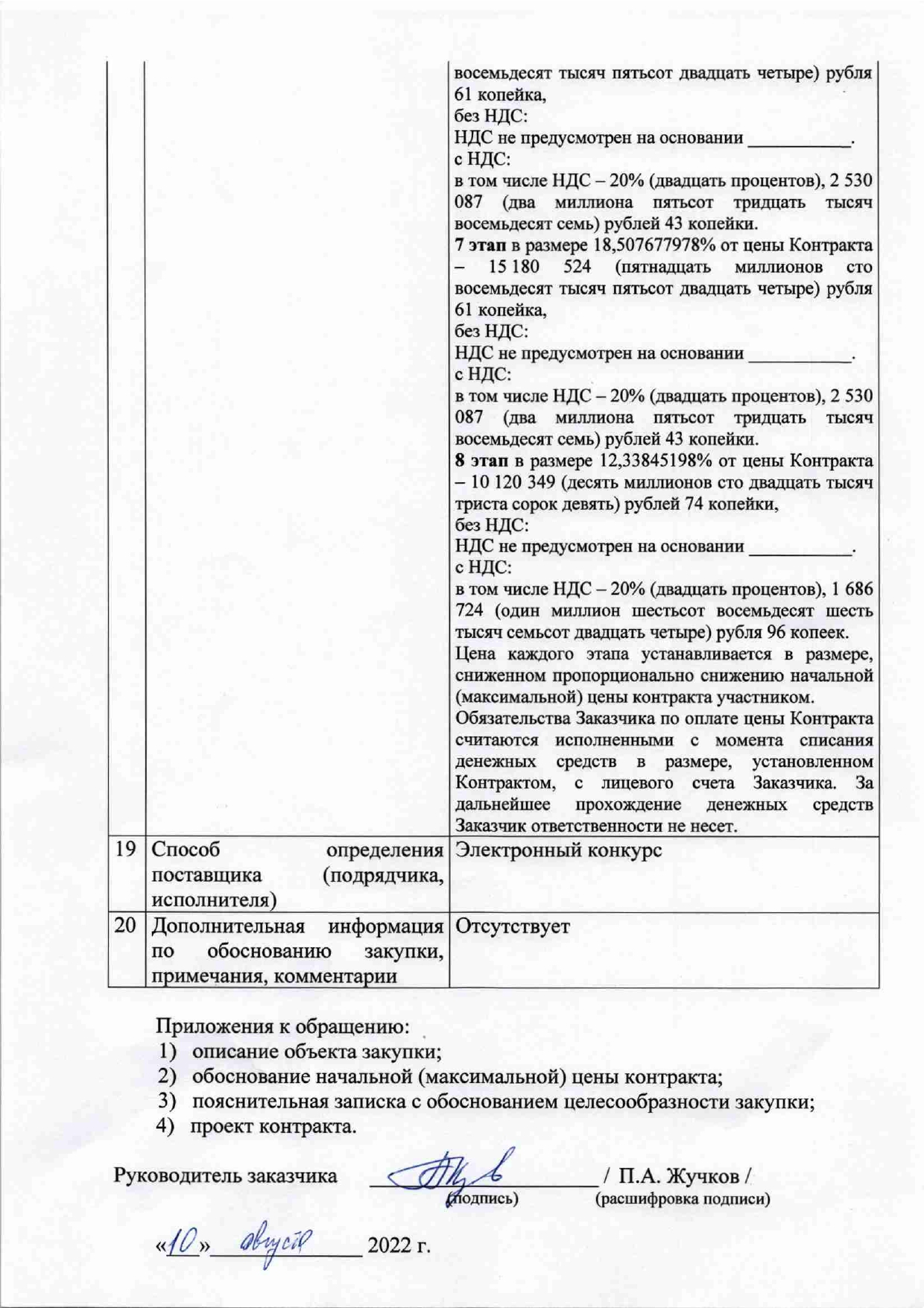


|  |  |  |
| --- | --- | --- |
|  |  | Лимиты бюджетных обязательств 2022 г. в размере 11 180 400 рублей 00 копеек  КБК: 194 0410 23.0.01.03250 242 224  Средства областного бюджета Новосибирской области в рамках реализации государственной программы Новосибирской области «Цифровая трансформация Новосибирской области»  Лимиты бюджетных обязательств 2022 г. в размере 12 568 821 рубль 45 копеек  Лимиты бюджетных обязательств 2023 г. в размере 58 273 626 рублей 73 копейки |
| 12 | Функции и полномочия Заказчика, для реализации которых осуществляется закупка (с указанием на пункты устава (положения) Заказчика) | В соответствии с Положением о министерстве цифрового развития и связи Новосибирской области, утвержденным постановлением Правительства Новосибирской области от 12.08.2019 № 314-п |
| 13 | Наименование мероприятия государственной (ведомственной) программы Новосибирской области (с указанием пункта перечня мероприятий программы и ее реквизитов) | Государственная программа Новосибирской области «Цифровая трансформация Новосибирской области»  Пункт 1.1.2.5. Сопровождение и обеспечение бесперебойного функционирования сетевой и серверной инфраструктуры ЦОД Правительства НСО  Лимиты бюджетных обязательств 2022 г. в размере 23 749 221 рубль 45 копеек  Лимиты бюджетных обязательств 2023 г. в размере 58 273 626 рублей 73 копейки |
| 14 | Сроки поставки товара, выполнения работ, оказания услуг по контракту | С 05.09.2022 по 30.11.2023 (включительно) |
| 15 | Место поставки товара, выполнения работ, оказания услуг | В соответствии с описанием объекта закупки |
| 16 | Условия поставки товара, выполнения работ, оказания услуг | В соответствии с описанием объекта закупки |
| 17 | Размер аванса по контракту | 0% (0 рублей 00 копеек) |
| 18 | Срок и порядок оплаты по контракту | Оплата оказанных по Контракту Услуг осуществляется Заказчиком на расчетный счет Исполнителя, указанный в Контракте, поэтапно. Оплата отдельного этапа исполнения Контракта производится Заказчиком в срок не более 7 (семи) рабочих дней с даты подписания Заказчиком документа о приёмке, предусмотренного п. 4.2. Контракта. Оплата производится Заказчиком на основании на основании документа о приёмке и при отсутствии у Заказчика претензий по объему и качеству оказанных Услуг, в соответствии со следующими этапами по Графику исполнения этапов по Контракту (приложение № 2):  **1 этап** в размере 0,438902096% от цены Контракта – 360 000 (триста шестьдесят тысяч) рублей 00 копеек,  без НДС:  НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  с НДС:  в том числе НДС – 20% (двадцать процентов), 60 000 (шестьдесят тысяч) рублей 00 копеек.  **2 этап** в размере 6,876132839% от цены Контракта – 5 640 000,00 (пять миллионов шестьсот сорок тысяч) рублей 00 копеек,  без НДС:  НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.  с НДС:  в том числе НДС – 20% (двадцать процентов), 940 000 (девятьсот сорок тысяч) рублей 00 копеек.  **3 этап** в размере 6,31580116% от цены Контракта – 5 180 400 (пять миллионов сто восемьдесят тысяч четыреста) рублей 00 копеек,  без НДС:  НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_.  с НДС:  в том числе НДС – 20% (двадцать процентов), 863 400 (восемьсот шестьдесят три тысячи четыреста) рублей 00 копеек.  **4 этап** в размере 15,32356133% от цены Контракта – 12 568 821 (двенадцать миллионов пятьсот шестьдесят восемь тысяч восемьсот двадцать один) рубль 45 копеек,  без НДС:  НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_.  с НДС:  в том числе НДС – 20% (двадцать процентов), 2 094 803 (два миллиона девяносто четыре тысячи восемьсот три) рубля 57 копеек.  **5 этап** в размере 21,69179462% от цены Контракта – 17 792 227 (семнадцать миллионов семьсот девяносто две тысячи двести двадцать семь) рублей 77 копеек,  без НДС:  НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_.  с НДС:  в том числе НДС – 20% (двадцать процентов), 2 965 371 (два миллиона девятьсот шестьдесят пять тысяч триста семьдесят один) рубль 30 копеек.  **6 этап** в размере 18,507677978% от цены Контракта – 15 180 524 (пятнадцать миллионов сто |



**ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ**

на оказание услуг по предоставлению выделенной инфраструктуры в центре обработки данных

1. **Основание для оказания услуг**: средства областного бюджета Новосибирской области в рамках реализации государственной программы «Цифровая трансформация Новосибирской области».
2. **Срок оказания услуг**: с 05.09.2022 по 30.11.2023 (включительно), в соответствии с графиком оказания услуг.
3. **Место оказания услуг**: г. Новосибирск, ул. Свердлова, д.14.
4. **Цель и основные задачи оказываемых услуг:** предоставление выделенной инфраструктуры в центре обработки данных Исполнителя, соответствующего требованиям Заказчика, изложенным в настоящем ООЗ.
5. **Термины и определения**

Таблица 1

|  |  |  |
| --- | --- | --- |
| 1 | ЦОД Заказчика | Центр обработки данных Правительства Новосибирской области, расположенный по адресу: г. Новосибирск, ул. Свердлова, д.14 |
| 2 | ЦОД Исполнителя | Центр обработки данных Исполнителя, соответствующий требованиям Заказчика |
| 3 | ГИС | Государственные информационные системы |
| 4 | ДГУ | Дизель-генераторная установка |
| 5 | ИБП | Источник бесперебойного питания |
| 6 | ГРЩ | Главный распределительный щит |
| 7 | РТП | Распределительная трансформаторная подстанция |
| 8 | СКУД | Система контроля и управления доступом |
| 9 | ВМ | Виртуальная машина |
| 10 | СХД | Система хранения данных |
| 11 | МЭ | Межсетевой экран |
| 12 | НСД | Несанкционированный доступ |
| 13 | ООЗ | Описание объекта закупки |
| 14 | ОС Windows | Windows 7/8/10, Windows Server 2012/2012 R2 |
| 15 | ОС Linux | Astra Linux Special Edition "Смоленск" 1.5/1.6,  Альт Линукс СПТ 8, Ubuntu 14.04 LTS Desktop/Server x64, VMware vSphere ESXi 6/6.5, CentOS 7.3/7.5, Лотос. |
| 16 | СУБД | Oracle, MS SQL, MySQL, PostgreSQL |

1. **График оказания услуг:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Этап** | **Описание** | **Результат** | **Длительность этапа** |
| **1** | Разработка и согласование документации по услуге | Разработаны и подписаны со стороны Заказчика и Исполнителя следующие документы:  1. Схема организации каналов связи от Заказчика до Исполнителя;  2. Структурная схема организации выделенной инфраструктуры, средств информационной безопасности и каналов передачи данных;  3. Перечень программного обеспечения (с указанием версий), оборудования и средств защиты информации (с указанием идентификационных (серийных) номеров и идентификаторов (маркирование средств защиты информации);  4. Форма программы и методики испытаний оказанных услуг по результатам исполнения контракта | С 05.09.2022 по 09.09.2022 (включительно) |
| **2** | 1. Организация физических каналов связи между ЦОД Заказчика и ЦОД Исполнителя;  2. Организация криптографической защиты каналов связи между ЦОД Заказчика и ЦОД Исполнителя | 1. Выполнена организация каналов связи между ЦОД Заказчика и ЦОД Исполнителя в соответствии с п. 8.2. данного ООЗ;  2. Выполнена организация криптографической защиты каналов связи между ЦОД Заказчика и ЦОД Исполнителя в соответствии с п.8.4.2. данного ООЗ | С 10.09.2022 по 23.09.2022 (включительно) |
| **3** | Организация выделенной инфраструктуры в ЦОД Исполнителя | Выполнена организация выделенной инфраструктура в ЦОД Исполнителя в соответствии с требованиями данного ООЗ в объёме согласно п.8.8. данного ООЗ | С 10.09.2022 по 30.09.2022 (включительно) |
| **4** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 01.10.2022 по 15.12.2022 (включительно) |
| **5** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 16.12.2022 по 31.03.2023 (включительно) |
| **6** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 01.04.2023 по 30.06.2023 (включительно) |
| **7** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 01.07.2023 по 30.09.2023 (включительно) |
| **8** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 01.10.2023 по 30.11.2023 (включительно) |

1. **Требования к услуге**:

В рамках оказания Услуги по предоставлению выделенной инфраструктуры в центре обработки данных с необходимым Заказчику уровнем качества Исполнитель должен обеспечить предоставление Заказчику комплексной услуги, состоящей из каналов связи, средств информационной безопасности, виртуальных и физических вычислительных ресурсов, а так же системы резервного копирования на базе имеющейся в его распоряжении (пользовании на правах собственности) инфраструктуры, отвечающих требованиям, представленным в настоящем описании объекта закупки.

Заказчику должна быть предоставлена выделенная инсталляция инфраструктуры, состоящая из вычислительных серверов, систем хранения данных, сетевого оборудования и средств информационной безопасности, в рамках которой Заказчик должен иметь возможность создания и использования виртуальных машин в требуемой конфигурации для размещения информационных систем и сервисов.

Заказчик должен иметь возможность в выделенной инфраструктуре центра обработки данных Исполнителя устанавливать любые операционные системы (из списка поддерживаемых), а внутри виртуальных машин любое совместимое программное обеспечение.

Уровень доступа Заказчика к выделенной инфраструктуре должен определяться матрицей ответственности, зафиксированной в SLA.

Услуга должна активироваться по факту выполнения инсталляционных и пусконаладочных работ, осуществляемых после подписания контракта.

Оказание услуг должно осуществляться Исполнителем собственными силами и за собственный счет на оборудовании Исполнителя, в том числе инсталляция необходимых лицензий для функционирования выделенной инфраструктуры в ЦОД Исполнителя.

Инфраструктура, предоставляемая Заказчику в ЦОДе Исполнителя, должна обеспечивать:

* Высокую доступность и бесперебойную работу приложений Заказчика;
* Надежное хранение данных Заказчика;
* Высокую доступность и отказоустойчивость всех критических бизнес-компонентов системы;
* Возможность гибкого изменения необходимого объема ресурсов для каждой виртуальной машины, как в сторону увеличения, так и в сторону уменьшения;
* Возможность удаленного подключения к инфраструктуре администраторов и сотрудников Заказчика для управления приложением и внесением корректировок с использованием VPN-подключения на основе алгоритмов шифрования ГОСТ;
* Защищенное высокоскоростное сетевое соединение с ЦОД Заказчика;
* Другие требования, указанные в настоящем описании объекта закупки.

Исполнитель в рамках оказания технической поддержки выделенной инфраструктуры и каналов связи, предоставляемых в рамках оказания услуги, должен направить Заказчику контактные данные специалистов технической поддержки (электронная почта, телефон) с градацией по уровням эскалации.

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень эскалации | Контакты | Время работы | ФИО и должность |
| Уровень 1 |  |  |  |
| Уровень 2 |  |  |  |
| Уровень 3 |  |  |  |

1. **Требования к ЦОД Исполнителя**

ЦОД Исполнителя должен находиться на территории Российской Федерации с протяженностью оптических линий связи не более 20 км от ЦОДа Заказчика, расположенного по адресу г. Новосибирск ул. Свердлова 14.

Объекты недвижимого имущества, составляющие ЦОД Исполнителя, должны быть в собственности Исполнителя.

Все элементы ЦОДа Исполнителя должны быть выполнены по уровню надежности не ниже, чем N+1, где N≥1.

* 1. **Требования к зданиям и помещениям**

В здании ЦОД Исполнителя должна быть зона погрузки/разгрузки оборудования. В случае размещения ЦОД Исполнителя не на первом этаже здания подъем оборудования необходимо обеспечить с помощью лифтов. Требования к лифтам: грузоподъемность – не менее 2 т, размеры кабины – не менее 1,1х1,5х2,2 (ШxГxВ, м). Также на пути следования оборудования не должно быть ступеней и перепадов высоты.

Несущая способность перекрытий в ЦОД Исполнителя и на пути следования оборудования должна быть не менее 1500 кг/м2.

В ЦОД Исполнителя должно быть не менее двух территориально разнесенных вводов для телекоммуникационного кабеля.

Ограждающие строительные конструкции (стены, перекрытия) машинного зала должны быть устойчивы к взлому.

* + 1. **Требования к системе кондиционирования**

Система кондиционирования должна обеспечивать следующие параметры окружающей среды в машинном зале и в электротехнических помещениях:

* температура от 23 °С до 27 °С;
* точки нормальной настройки: 25 °С;
* точность поддержания температуры: ± 2 °С;
* относительная влажность от 30% до 70%;
* точки нормальной настройки: 45% относительной влажности;
* точность поддержания относительной влажности: ± 5%;
* максимальная скорость изменения температуры в машинных залах не должна превышать: ± 5 °С в час;
* скорость изменения влажности: не более 10% в час

Температура в ЦОД Исполнителя не должна превышать 30 °С на время, отводимое на пуск и выход в рабочий режим ДГУ.

Данные мониторинга температурно-влажностного режима помещений ЦОД Исполнителя должны контролироваться диспетчерской службой Исполнителя для возможности круглосуточного контроля параметров.

* + 1. **Требования к системе пожаротушения**

Машинный зал ЦОД Исполнителя должен быть оснащен комплексом противопожарных систем, включая систему автоматического пожаротушения.

Наличие системы автоматического газового пожаротушения в помещениях машинного зала ЦОД Исполнителя, комнатах ИБП, ГРЩ и электрощитовой ЦОД. Резервный запас огнетушащего газа должен быть инсталлирован в систему и подключаться после расходования основного без проведения монтажных работ.

Система пожаротушения должна иметь на площадке резерв огнетушащего вещества не менее чем на 2 последовательных пуска и должна иметь независимый источник гарантированного электропитания, превышающий по времени автономной работы остальную систему электроснабжения ЦОД.

Все элементы инфраструктуры ЦОД Исполнителя (ГРЩ, ИБП, ДГУ, батареи, трансформаторы) должны располагаться в отдельных помещениях для исключения общего возгорания. Каждое инфраструктурное помещение должно быть оснащено системой пожарной сигнализации и необходимым типом системы пожаротушения (газовое, порошковое и т.п.).

Сигналы системы пожаротушения должны быть выведены на пульт дежурной смены. Срабатывание системы пожаротушения не должно выводить из строя размещенное и не поврежденное пожаром оборудование.

* + 1. **Требования к бесперебойному электроснабжению**

Система бесперебойного электроснабжения должны быть дублирована на всех уровнях: иметь не менее 2 вводов от независимых районных подстанций, иметь собственную РТП, обеспечивать двойное резервирование электрических линий между РТП и ИБП, иметь 2 группы ИБП на полную мощность оборудования с временем автономной работы не менее 10 минут.

Система электроснабжения должна обеспечивать действующее значение напряжения 230В/400В ± 5%, частота 50 ± 0,2 Гц, общей мощностью не менее 1500 кВт.

ЦОД Исполнителя должен иметь 2 электрических линии от ИБП до помещения щитовой ЦОД Исполнителя (по одной от каждой группы), свой электрический щит для каждой линии в помещении щитовой ЦОД, не менее 2 кабелей питания на каждую стойку от разных щитов.

Для статических ИБП время автономной работы любой из взаимно резервирующих систем ИБП на расчетную нагрузку в аварийном режиме в конфигурации N+1 (отказ одной из пары взаимно резервирующих систем ИБП) не должно превышать время, необходимое для запуска ДГУ и полного приёма им нагрузки, но не менее 10 минут.

ИБП должны размещаться в отдельном помещении с организацией доступа только для обслуживающего персонала и собственной установкой поддержания климатических параметров.

Оборудование ЦОД Исполнителя подключено к заземляющим устройствам согласно действующим нормативным документам.

Для обеспечения гарантированного электроснабжения ЦОД Исполнителя обеспечен системой гарантированного электроснабжения.

Уровень резервирования ДГУ должен быть не ниже, чем N+1, где N≥1. Хранилище дизельного топлива должно быть объемом, обеспечивающим работу всех ДГУ для обеспечения 100% критически важной нагрузки ЦОД Исполнителя в течение не менее 6 (шести) часов.

Исполнитель должен иметь действующий договор с топливными компаниями на подвоз необходимого объема топлива автоцистернами не позднее чем через 4 часа после запуска ДГУ.

* + 1. **Требования к службе безопасности**

ЦОД Исполнителя должен круглосуточно охраняться службой безопасности. Арендуемые помещения (выделенное огороженное пространство машинного зала) ЦОД Исполнителя должны быть оснащены системами контроля и управления доступа, охранного телевидения и охранной сигнализацией объекта.

* + 1. **Требования к системе контроля и управление доступом**

Двери ЦОД Исполнителя, а также всех арендуемых помещений, входящих в структуру ЦОД Исполнителя, должны быть оборудованы электронными замками и считывателями карт, подключенными к автоматизированной системе контроля и управления доступом.

Доступ в помещения ЦОД Исполнителя должен быть ограничен для обслуживающего персонала. Входные двери и двери машинного зала должны оборудоваться следующей аппаратурой:

* замками электромагнитными (электромеханическими);
* датчиками контроля двери;
* считывателями бесконтактных карт на вход и выход и/или биометрическими считывателями.

Допуск посторонних лиц в помещения ЦОД Исполнителя, в которых размещается оборудование частного контура, без сопровождения должен осуществляться на основании списка доступа. Доступ посторонних лиц в помещения ЦОД Исполнителя, не указанных в списке доступа, должен осуществляться только в сопровождении уполномоченных сотрудников Исполнителя.

Исполнитель должен осуществлять контроль за пропускным режимом.

Срок хранения записей журнала СКУД о событиях доступа должен составлять 30 календарных дней.

* + 1. **Требования к системе видеонаблюдения**

Под видеонаблюдением должны быть все двери помещений ЦОД Исполнителя, все коридоры между стойками с оборудованием, внешний периметр здания.

Телевизионная система видеонаблюдения должна обеспечивать:

* обзор всех охраняемых зон;
* непрерывную, по детекции и по расписанию мультиплексированную запись видеоинформации на жесткие диски;
* визуальное отображение происходящего в реальном масштабе времени на видеостене в помещение охраны объекта;
* создание видеоархива и его просмотр, непрерывную, по детекции и по расписанию мультиплексированную запись видеоинформации на жесткие диски;
* контроль оперативной обстановки внутри помещений с качеством, достаточным для идентификации лиц в независимости от времени суток;
* формирование архива видеозаписей текущих и тревожных событий со всех установленных видеокамер за период времени 30 дней;
* автоматический вывод изображений от соответствующих видеокамер на "тревожные" видеомониторы телевизионной системы видеоконтроля, видеостену при срабатывании охранного извещателя.
  + 1. **Требования к охранной сигнализации**

Помещения ЦОД Исполнителя должны быть оснащены системой охранной сигнализации. Охранными извещателями должно быть оборудовано:

* входные двери, двери запасных выходов, двери тамбуров эвакуационных выходов, двери лестничных площадок – извещателями "на открывание" и, для дверей со стеклянными панелями, на "разбитие" стекла;
* оконные и дверные конструкции – извещателями "на открывание" и "разбитие" стекла.

Помещения машинного зала, кроссовых, коридоров и зон помещений, входящих в структуру ЦОД Исполнителя, должны быть оборудованы пассивными инфракрасными или комбинированными (ИК+СВЧ) извещателями, в зависимости от назначения помещения и наличия помех (воздушные потоки от кондиционеров и другие помехи).

Количество датчиков должно быть определено потребностями обеспечения качественного контроля внутренних территорий данных помещений, особенно проходов между стойками с оборудованием.

Машинный зал должен защищаться двумя рубежами охранной сигнализации:

* первым рубежом охранной сигнализации блокируется дверь помещения на «открывание» и окна помещения (при наличии) на «открывание» и «разбитие». На «открывание» и «разбитие» блокируются все окна;
* вторым рубежом охранной сигнализации блокируется объем помещения на «проникновение» и движение.
  + 1. **Требования к надёжности инженерно-технических систем**

Все оказываемые услуги должны удовлетворять следующим требованиям к надежности:

Отказоустойчивость работы инфраструктуры ЦОД Исполнителя должна обеспечиваться с помощью «горячего» резервирования основных компонентов ЦОД Исполнителя, путем переключения с основных элементов на резервные, с характеристиками не ниже, чем у основных.

Ремонтные и сервисные работы на инженерной инфраструктуре, обеспечивающей работу ИТ-оборудования, должны проводиться без отключения аппаратных стоек и без снижения качественных параметров систем электроснабжения и охлаждения. Для обеспечения данного требования резервированию должны подлежать не только отдельные устройства и элементы систем, но также и каналы доставки электроснабжения и холода к аппаратным стойкам.

К ремонтным и сервисным работам, в частности, относятся:

* превентивное и плановое обслуживание;
* ремонт и замена компонентов;
* добавление или удалением элементов систем;
* тестирование компонентов и систем в целом.

Инженерно-технические системы ЦОД Исполнителя должны обеспечивать функционирование в диапазоне наружной температуры, соответствующем интервалу пиковых температур для данного региона без снижения заявленных климатических значений внутри ЦОД Исполнителя и уровня надежности инженерной инфраструктуры в целом.

В ЦОД Исполнителя круглосуточно должна присутствовать дежурная служба эксплуатации, в составе которой обязательно должно быть не менее 2-х (двух) инженеров круглосуточно.

ЦОД Исполнителя должен быть оборудован системой автоматизированного контроля и/или управления состояния инженерной инфраструктуры.

* + 1. **Требования к системе защитного заземления**

В ЦОД Исполнителя должна иметься система заземления всех элементов инженерного оборудования, имеющего металлические и токопроводящие части и корпуса в соответствии с требованиями ГОСТ Р 50571.21-2000, ГОСТ Р 50571.22-2000 и ПУЭ, 7-я редакция.

К системе защитного заземления (СЗЗ) должны быть подключены, помимо основного и дополнительного инженерного оборудования, монтажные шкафы с установленным в них оборудованием и предусмотрено заземление внешних блоков кондиционеров, системы трубопроводов и т.п.

* + 1. **Требования к системе молниезащиты технологического оборудования**

Здание ЦОД Исполнителя должно быть обеспечено молниезащитой технологического оборудования, размещенного на кровле здания, оборудования приточно-вытяжной вентиляции, чиллеров, конденсаторных блоков.

* + 1. **Требования к телекоммуникационным ресурсам ЦОД**

Факт наличия основного и резервного оптического ввода в здание ЦОД Исполнителя должен быть подтверждён исполнительной документацией по организации кабельных трасс в здании ЦОД и проектами оптических трасс операторов связи.

В ЦОДе Исполнителя должны присутствовать не менее 5 независимых на уровне активного оборудования операторов связи. Факт наличия должен подтверждаться официальными письмами о возможности подключения на территории ЦОД Исполнителя, с указанием точки подключения (машинный зал, стойка, юнит, порт).

* 1. **Требования к каналам передачи данных**

Исполнитель для организации доступа из ЦОД Заказчика к выделенной инфраструктуре ЦОД Исполнителя должен обеспечить предоставление канала передачи данных со скоростью не менее 10 Гбит/с1. Доступ должен быть организован посредством предоставления основного и резервного (независимого, прямого, волоконно-оптического) физических каналов передачи данных до ЦОД Заказчика по адресу г. Новосибирск ул. Свердлова 14, с максимальной протяженностью канала передачи данных не более 20 километров. Для обеспечения шифрования каналов связи между ЦОД Заказчика и ЦОД Исполнителя Заказчик предоставляет сертифицированные средства криптографической защиты информации и в дальнейшем их администрирует собственными силами.

Скорость обмена между виртуальными ресурсами должна быть не ниже 10 Гбит/с1.

Каналы передачи данных должны обеспечивать время отклика от инфраструктуры ЦОД Заказчика до виртуальных ресурсов, размещенных на выделенной инфраструктуре в ЦОД Исполнителя, не более 2 миллисекунд.

В целях резервирования сетевой связанности Исполнитель должен организовать подключение, путём организации отказоустойчивых кластеров из криптомаршрутизаторов, предоставляемых Заказчиком, на стороне ЦОД Заказчика и ЦОД Исполнителя по физически разнесённым каналам передачи данных.

Число потерянных пакетов на физическом канале (оптическое волокно) должно составлять не более 0,3% от общего числа пакетов (в месяц).

Доступность каналов связи должна составлять не менее 99% в отчетный период.

Формула расчета доступности услуги по предоставлению каналов связи:

Услуга по каждой точке считается недоступной в период времени:

* - с момента поступления заявки от Заказчика и до подтверждения Заказчиком восстановления услуги;
* - с момента обнаружения Исполнителем аварии на участке сети связи, через который осуществляется пропуск трафика, не имеющего альтернативного маршрута, и до момента устранения аварии;
* - с момента начала плановых работ на участке сети связи, через который осуществляется пропуск трафика, не имеющего альтернативного маршрута, и до момента завершения работ.

Доступность каналов за месяц подключения определяется по формуле:

Kд - Коэффициент доступности сети

N - Количество мест предоставления услуги

tn - Время недоступности n-ой точки подключения

- Суммарное время недоступности всех точек подключения

T - Количество минут в отчетном периоде (24×60×кол-во дней в отчетном периоде).

Техническая поддержка пользователей Услуги должна осуществляться - 24 (двадцать четыре) часа в сутки, 7 (семь) дней в неделю 365 дней в году.

Все поступающие заявки должны регистрироваться в системе учета заявок с присвоением каждой заявке уникального идентификационного номера. По требованию заказчика Исполнитель должен предоставлять статистику заявок с указанием даты регистрации, уникального идентификационного номера, содержания и текущего статуса заявки. Отчет по зарегистрированным заявкам должен предоставляться ежемесячно.

Плановые профилактические работы с закрытием одного из каналов связи должны проводиться в часы наименьшей нагрузки с извещением Заказчика не менее, чем за трое суток до начала работ. Периодичность профилактических работ – не чаще 4 (четырех) раз в течение срока действия контракта. Продолжительность проведения плановых работ не должна превышать четырех часов.

* 1. **Требования к выделенной инфраструктуре**

Услуга по предоставлению выделенной инфраструктуры в центре обработки данных должна предоставляться Исполнителем по принципу готового сервиса. Исполнитель должен предоставить Заказчику права на доступ к услуге, необходимые для точечного управления ИТ системами, при этом проведение работ, связанных с обслуживанием выделенной инфраструктуры, должны находиться в зоне ответственности Исполнителя.

Для обеспечения отказоустойчивости Исполнитель должен предусмотреть избыточность на уровне компонентов комплекса, на базе которого реализуется Услуга.

Выделенная инфраструктура должна быть защищена дополнительными средствами как информационной, так и физической безопасности, согласно требованиям к информационной безопасности настоящего описания объекта закупки.

Услуга по предоставлению выделенной инфраструктуры в ЦОД Исполнителя должна включать в себя ресурсы, предоставленные в пользование только Заказчику, без возможности использования этой выделенной инфраструктуры третьими лицами. Заказчик должен иметь возможность задействовать тот объем ресурсов, который необходим ему для решения текущих задач в определенный момент времени.

В ЦОД Заказчика используется платформа среды виртуализации VMware vSphere 6.7, выделенная инфраструктура Исполнителя должна быть реализована на платформе среды виртуализации, позволяющей автоматизировано мигрировать виртуальные машины из ЦОД Заказчика в ЦОД Исполнителя и в обратном направлении.

Заказчик самостоятельно через интерфейс самообслуживания, должен иметь возможность:

* создавать виртуальные машины по отдельности и в виде групп;
* управлять работой виртуальных машин (включить, выключить и перезагрузить);
* изменять конфигурацию виртуальных машин, в т.ч. конфигурацию вычислительных ресурсов, дисковую и сетевую;
* непосредственно получить доступ к консоли виртуальной машины;
* создавать копии виртуальных машин и их групп;
* монтировать ISO образы CD/DVD;
* удалять и добавлять внутренние логические сети, управлять подключением виртуальных машин к сетям;
* создавать и удалять виртуальные маршрутизаторы, управлять сервисами этих виртуальных маршрутизаторов.

Заказчик путем направления запроса в службу технической поддержки должен иметь возможность:

* получать доступ к текущим и историческим данных мониторинга производительности компонентов виртуальной инфраструктуры и виртуальных машин;
* удалять и добавлять сети на базе VLAN для частного сегмента облака (кроме сетей, использующихся для функционирования инфраструктуры);
* получать по запросу доступ к логам событий всех компонентов виртуальной инфраструктуры;
* изменять права доступа заданным группам или пользователям.

Должна быть организована возможность сохранения и выгрузки резервных копий виртуальных машин.

Должна быть обеспечена возможность создания и установки собственных и предлагаемых третьими лицами сборок виртуальных машин посредством шаблонов виртуальных машин (Virtual Appliance).

Для обеспечения отказоустойчивости и минимизации времени простоя при доступе к выделенной инфраструктуре Заказчика, Исполнитель должен:

* обеспечить подключение ресурсов выделенной инфраструктуры к сети Заказчика резервируемыми каналами связи (не менее двух);
* подключение к сети Заказчика должно использовать территориально разнесенные вводы волоконно-оптического кабеля в ЦОД.

Должна быть включена по умолчанию функция высокой доступности (High Availability), позволяющая осуществлять автоматический перенос виртуальных машин на резервный сервер в случае выхода из строя сервера в предоставляемой Заказчику выделенной инфраструктуре.

* + 1. **Требования к минимальным вычислительным ресурсам и ресурсам хранения, предоставляемым Исполнителем**

Исполнитель должен предоставить Заказчику возможность использования вычислительных ресурсов и ресурсов хранения со следующими параметрами:

|  |  |  |
| --- | --- | --- |
| **Подсистема** | **Ресурс** | **Требования** |
| Вычислители | Базовая частота vCPU | 3,1 ГГц |
| Коэффициент переподписки виртуальных ядер к физическим (pCPU:vCPU) | 1:5 |
| Система хранения данных | Тип дисков | Enterprise SSD |
| Дисковое пространство, SSD Тип 1 | 3 мс при интенсивности ввода-вывода 2 000 IOPS/TB, но не более 30 000 IOPS |
| Дисковое пространство, SATA Тип 2 | 20 мс при интенсивности ввода-вывода 200 IOPS/TB, но не более 7 000 IOPS |
| Дисковое пространство, SATA Тип 3 | 30 мс при интенсивности ввода-вывода 100 IOPS/TB, но не более 3 500 IOPS |
| Среда виртуализации и ВМ | Среда виртуализации обладает необходимым функционалом для автоматической миграции ВМ в ЦОД Заказчика в случае отказа ЦОД Исполнителя | Да |
| Максимальные параметры запускаемой ВМ | 48 ядер vCPU |
| Узлы отказоустойчивого кластера виртуализации на площадке основного ЦОД Исполнителя под задачи Заказчика | N+1 |
| Резервирование мощностей | Указанные мощности являются зарезервированными для Заказчика (Allocated pool) | Да |
| Исполнитель располагает дополнительными мощностями с показателями производительности не менее 50% от указанных для аварийного переноса выделенной инфраструктуры Заказчика в случае отказа. | Да |
| Аппаратные требования | Выделенные серверы, в т.ч. резерв N+1;  Выделенное сетевое оборудование для коммутации;  Выделенная SAN-фабрика;  Выделенные СХД;  Выделенные серверы резервного копирования;  Индивидуальный контур управления виртуализацией | ПАК состоящий из серверного и сетевого оборудования должен использоваться только для задач Заказчика |

* + 1. **Требования к системе хранения данных**

Должна быть обеспечена возможность выделения Заказчику дискового пространства трёх типов производительности согласно п.8.3.1.

Доступ к сети хранения данных каждого вычислительного узла, предоставляемого Исполнителем, должна быть не менее 16 Гбит/с.

Система хранения данных должна быть подключена не менее чем к двум независимым SAN-фабрикам, предоставляемым Исполнителем.

Общая схема организации SAN сети должна быть построена таким образом, чтобы выход из строя любого единичного компонента не приводил к остановке сервиса в целом.

* + 1. **Требования к сетевой инфраструктуре**

Сетевое коммутационное оборудование Исполнителя для оказания Услуги должно быть объединено в отказоустойчивую архитектуру при помощи технологий агрегирования для обеспечения непрерывности при проведении работ по техническому обслуживанию сетевой инфраструктуры и аварийных ситуациях на различных участках волоконно-оптических линий связи между ЦОД Заказчика и ЦОД Исполнителя.

Сетевая инфраструктура должна обеспечивать изоляцию трафика Заказчика от трафика других клиентов.

Сетевая инфраструктура ЦОД Исполнителя должна обеспечивать пропускную способность не менее 10 Гбит/сек1.

* + 1. **Требования к платформе резервного копирования**

Платформа резервного копирования должна позволять создавать Заказчику резервные копии данных. Система управления и интерфейс платформы резервного копирования должны позволять гибко настраивать частоту создания полных копий данных и копий изменений по времени. Резервные копии должны храниться на физически не зависимом от основных данных оборудовании.

Заказчику должен быть предоставлен доступ к интерфейсу управления системой. Интерфейс управления платформы резервного копирования должен содержать информацию о резервных копиях данных Заказчика, позволять Заказчику самостоятельно управлять заданиями резервного копирования и восстановления данных.

Платформа резервного копирования должна обеспечивать возможность резервного копирования ВМ на уровне образов, с возможностью копирования только изменившихся блоков, а также без установки специализированных приложений внутрь ВМ;

Платформа резервного копирования должна поддерживать передачу резервных копий, как по сети передачи, так и по сети хранения данных, включая резервное копирования ВМ напрямую с NFS хранилищ.

Платформа резервного копирования должна поддерживать механизм автоматического изменения скорости процесса резервного копирования при увеличении времени отклика на чтение на всех системах хранения с возможностью определения порогов времени отклика.

Платформа резервного копирования должна иметь механизм дедупликации и сжатия резервных копий “на лету”, возможность исключать блоки служебных файлов ОС, а также папки и файлы, указанные пользователем, для ускорения процесса резервного копирования, а также для уменьшения объема хранимых данных.

Платформа резервного копирования должна уметь использовать аппаратные снимки СХД для резервного копирования, с возможностью обеспечения целостности приложений внутри виртуальных машин. Взаимодействие должно реализовываться при помощи специализированных API на уровне СХД и без установки дополнительного программного обеспечения на них.

* + - 1. **Требования к тестированию целостности и возможности восстановления резервных копий виртуальных машин**

Платформа резервного копирования должна иметь возможность создать изолированную среду на продуктивной инфраструктуре Заказчика, с возможностью использовать ее для автоматического тестирования резервных копий или для создания тестовых зон.

Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности резервных копий ВМ. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из резервных копий и/или аппаратных снимков СХД в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри резервируемой ВМ. Должна быть возможность использовать как встроенные скрипты проверки, так и возможность использовать собственные скрипты.

* + - 1. **Требования к хранению резервных копий виртуальных машин**

Платформа резервного копирования должна иметь возможность шифровать резервные копии.

Платформа резервного копирования должна иметь возможность интегрироваться с машинами на базе ОС Linux для использования их в качестве защищенных хранилищ резервных копий, позволяющих установить настройку неизменности данных, обеспечивающую возможность защиты от удаления и изменения блоков данных резервных копий на указанный промежуток времени.

Платформа резервного копирования должна уметь передавать резервные копии между различными хранилищами с возможностью указания новой глубины хранения для резервной копии.

При передаче резервных копий между хранилищами платформа резервного копирования должна иметь возможность возобновляемой передачи резервных копий между площадками с использованием механизмов сжатия и глобальной дедупликации трафика и кэширования информации на обеих площадках на специализированных серверах.

Платформа резервного копирования должна иметь возможность формирования синтетической полной резервной копии при записи на ленту из имеющихся в дисковом хранилище резервных копий полной резервной копии и цепочки инкрементальных без создания временной синтетической полной копии на диске.

* + - 1. **Требования к восстановлению данных из резервных копий виртуальных машин**

Платформа резервного копирования должна поддерживать возможность восстановления из резервных копий даже в случае полной потери сервера резервного копирования.

Платформа резервного копирования должна поддерживать восстановление виртуальных машин как целиком, так и отдельных виртуальных дисков, и файлов конфигураций. Восстановление должно идти как по сети передачи, так и по сети хранения данных.

Платформа резервного копирования должна обеспечивать моментальный запуск виртуальных машин непосредственно из хранилища резервных копий с возможностью последующего переноса виртуальной машины на выбранное хранилище данных без прерывания работы.

Платформа резервного копирования должна обеспечивать возможность предварительного антивирусного сканирования и проверки резервных копий при восстановлении.

Платформа резервного копирования должна обеспечивать возможность до восстановления ВМ в рабочую инфраструктуру удалить данные из этой ВМ, не удаляя эти данные из резервной копии.

Платформа резервного копирования должна реализовывать гранулярное восстановление данных приложений из резервных копий, в промежуточное и/или исходное месторасположение без установки специализированного агента;

Платформа резервного копирования должна реализовывать точеное восстановление СУБД на ОС Windows и ОС Linux (с поддержкой технологии ASM), имеющихся у Заказчика, включая возможность восстановления данных до конкретной транзакции, в промежуточное и/или исходное месторасположение без установки специализированного агента.

Платформа резервного копирования должна обеспечивать возможность позволять делегировать пользователям самостоятельно восстанавливать из резервной копии объекты приложений через Web-портал.

* + 1. **Требования к функциональным возможностям репликации и аварийного восстановления виртуальных машин**

Платформа резервного копирования должна поддерживать прямую репликацию виртуальных машин без использования промежуточных резервных копий, с возможностью обеспечения создания множества точек восстановления и передачей только изменившихся блоков.

Платформа резервного копирования должна обеспечить целостность приложений внутри ВМ при репликации, без установки специализированных приложений внутрь ВМ.

Платформа резервного копирования должна обеспечивать переключение на реплицированную виртуальную машину с возможностью автоматической смены IP адреса.

Платформа резервного копирования должна обеспечивать переключение на реплицированную виртуальную машину даже при потере сервера резервного копирования.

* + - 1. **Требования к тестированию целостности и возможности восстановления реплицированных виртуальных машин**

Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности реплик ВМ. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из реплик в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри ВМ. Должна быть возможность использовать как встроенные скрипты проверки, так и возможность использовать собственные скрипты.

* + - 1. **Требования к возможности непрерывной репликации и аварийного восстановления для виртуальных машин**

Платформа резервного копирования должна поддерживать непрерывную репликацию виртуальных машин без использования снимков виртуализации, обеспечивающую минимальную потерю данных в пределах 2 секунд.

Платформа должна непрерывно реплицировать операции ввода/вывода виртуальных машин и хранить их в специальном журнале на целевом хранилище в течении нескольких часов, указанных в краткосрочной политике хранения в целях обеспечения возможности восстановления ВМ на определенный момент времени с заданным шагом.

Платформа должна обеспечивать возможность создания дополнительных точек восстановления ВМ, выходящих за пределы краткосрочной политики репликации, с учетом состояния работающих внутри приложении и обеспечения их консистентности, без установки специализированных приложений внутрь ВМ.

* 1. **Требования к средствам защиты информации.**

Выделенная Заказчику инфраструктура в ЦОД Исполнителя должна быть готова к проведению комплекса организационно-технических мероприятий, в результате внедрения которых подтвердится соответствие системы защиты информации требованиям безопасности информации в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 для размещения государственных информационных систем не ниже второго класса защищенности и информационных систем персональных данных, обрабатывающих персональные данные не ниже второго уровня защищенности.

Для обеспечения безопасности информации Исполнителем предоставляются в пользование следующие средства защиты:

* средства межсетевого экранирования и системы обнаружения вторжений (2 шт.) (п.8.4.1 данного ООЗ)
* средства защиты виртуальной инфраструктуры (1 шт.) (п 8.4.3 данного ООЗ);
* средства антивирусной защиты (30 шт.) (п. 8.4.4 данного ООЗ)
* средства доверенной загрузки (1 шт.) (п. 8.4.5 данного ООЗ)
* средства защиты от несанкционированного доступа (30 шт.) (п 8.4.6 данного ООЗ)

Средства защиты информации должны предоставляться в настроенном виде и готовыми к использованию и не должны приводить к нарушению штатного функционирования выделенной инфраструктуры.

Заказчик администрирует средства защиты информации самостоятельно.

* + 1. **Минимальные требования к используемому Исполнителем межсетевому экрану и системе обнаружения вторжений**

Межсетевой экран предоставляется в виде отказоустойчивого программно-аппаратного комплекса (2 шт.) и должен обеспечивать контроль   
8 миллионов одновременных TCP-сессий на пропускной способности канала 18 000 Мб/c.

Межсетевой экран должен регулярно получать с сервера производителя «чёрный» список ip адресов спамеров и открытых релеев.

Межсетевой экран должен регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя.

Межсетевой экран должен поддерживать следующие основные функции:

* контроль доступа пользователей в сеть и фильтрации трафика сети;
* анализ трафика сети по категориям, адресам и контенту данных;
* мониторинг действий, совершаемых пользователями при работе с сетью, а также формирование отчетности;
* предоставление возможности обновлять списки с помощью офлайн обновлений;
* контроль технологических протоколов АСУ ТП: Modbus, DNP3, MMS;
* возможность встраивания в сетевую инфраструктуру заказчика по протоколу WCCP;
* защита объектов сетевой инфраструктуры с помощью системы обнаружения вторжений (СОВ);
* контроль передаваемого трафика через межсетевой экран с помощью определения приложений L7.

Особенности реализации функций межсетевого экранирования:

1. функционал настройки средств фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение.
2. необходимо наличие события об успешной загрузке системы в журнале событий.
3. должно быть обеспечено журналирование изменения времени в консоли администрирования.
4. Необходимо наличие оповещений по SNMP при срабатывании запрещающих правил межсетевого экрана.
5. Должна обеспечиваться блокировка всего трафика при инцидентах, таких как нарушение функционирования системы. В случае если исполняемый файл из состава МСЭ изменен, весь трафик должен быть заблокирован.
6. Функционал решения должен иметь возможность запрашивать ввод пароля на разблокировку в случае несанкционированного доступа к изменениям правил МСЭ, изменениям правил оповещения, сетевым интерфейсам, добавлению учетной записи нового администратора, экспорту логов системы.
7. Фильтрация входящего и исходящего трафика должна осуществляться с одновременным обеспечением проверки на наличие вредоносного программного обеспечения.

Требования к доступности и производительности межсетевого экранирования:

* программное обеспечение должно иметь возможность быть реализованным в соответствии с методом обеспечения высокой доступности, гарантируя минимальное время простоя, и полного решения возложенных задач при выходе из строя одного из компонентов.
* программное обеспечение должно обеспечивать резервное копирование конфигураций компонентов и журналов регистрации событий с функцией исторического хранения данных с глубиной хранения не менее 12 месяцев.
* программное обеспечение должно иметь возможность масштабирования. Увеличение числа обслуживаемых пользователей и объема обрабатываемого трафика сети должно осуществляться путем подключения дополнительных программно-аппаратных компонентов.
* при наличии дополнительных узлов программное обеспечение должно позволять в любое время выводить часть узлов фильтрации из эксплуатации для обслуживания с автоматическим перераспределением нагрузки на оставшиеся узлы прозрачно для пользователей.
* должен обеспечиваться функционал настройки программно-аппаратных средств, входящих в состав, без остановки всей Системы.
* программное обеспечение должно обеспечивать функцию планового отключения для выполнения профилактических мероприятий, изменений или наращивания аппаратного обеспечения, установки обновлений на программное обеспечение.
* программное обеспечение должно предоставлять инструменты диагностирования состояния собственных компонентов.
* в программном обеспечении должна быть ролевая модель разграничения доступа. Роли должны иметь ограничения по доступу к Программному обеспечению на уровне интерфейсов, функционала, отчетов и производственных объектов.

Обеспечение следующих видов фильтрации (анализа) передаваемого контента:

* анализ передаваемых объектов по типу передаваемых объектов, в том числе определение и корректная обработка распространенных форматов файлов, применяемых в офисном ПО (DOC, DOCX, XLS, XLSX, PDF, TXT, ODT и т.д.);
* поиск и анализ регулярных выражений (ключевых слов);
* лингвистический (морфологический) анализ.
* эвристический анализ.
* автоматическое или ручное обновление компонентов с сайта производителя.

Управление доступом к средствам контентного анализа с использованием ролевой модели.

Требования к функционалу средств мониторинга и отчетности:

* протоколирование действий пользователей и администраторов
* отслеживание текущей сессии пользователя в режиме on-line, определение сервера, через который установлена сессия, подключения к серверу и разбора пользовательской сессии.

Формирование отчетности с функционалом:

* объявления пользовательских (новых) полей
* формирования запросов с использованием перекрестных запросов.

Формирование отчетности с предоставлением функционала:

* задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;
* формирования запросов к базе данных;
* задания формата отчетов;
* отправку отчетов по расписанию и по запросу администраторов;
* отключение мониторинга функционирования и формирования отчетности для конкретных пользователей/IP-адресов.
* Автоматическое или ручное обновление компонентов с сайта производителя.
* Управление доступом к средствам мониторинга и отчетности с использованием ролевой модели.
* Отправка статистической информации по протоколу NetFlow версий 5, 9, 10.

Связь с существующим окружением и интеграция

Разграничение полномочий доступа для работы и доступа пользователей в сеть должно быть реализовано на ролевой основе с использованием групп существующих доменов Active Directory.

Система должна взаимодействовать со следующими смежными системами:

* система Active Directory, в части аутентификация пользователей в Active Directory, определение принадлежности пользователей к группам Active Directory.
* системы авторизации пользователей Kerberos, NTLM, Single-sign-on в части автоматической авторизации пользователей.
* система идентификации пользователей Radius accounting, определение IP-адресов пользователей.
* система синхронизации времени, в части взаимодействия с системой синхронизации времени должна поддерживать определение точного времени.
* система доменных имен (DNS), в части взаимодействия с системой DNS должно поддерживать определение IP-адресов узлов сети по имени узла.
* система мониторинга SNMP, в части взаимодействия с системой мониторинга SNMP должно поддерживать оповещение и работу в режиме запросов состояния системы по протоколам SNMP v2 и SNMP v3.
* корпоративная почтовая система (E-mail), в части взаимодействия с корпоративной почтовой системой должно поддерживать отправку по e-mail оповещений администраторам о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
* система сбора и корреляции событий информационной безопасности, в части взаимодействия с системами сбора и корреляции событий информационной безопасности должно предоставлять механизм экспорта журнальных сообщений в режиме реального времени. Формат и детализация данных сообщений должны настраиваться.
* системы дополнительного контентного анализа, в части взаимодействия с системами дополнительного контентного анализа должно предоставлять модуль интеграции по протоколу I-CAP с указанными системами в части условий доступа на основании результатов анализа контента.

Требования к пользовательскому интерфейсу:

* программный интерфейс компонентов, включая средства управления, а также формы оповещений и уведомлений администраторов Системы и пользователей сети Интернет должен полностью поддерживать русский язык, используя кодировку текста UTF-8.
* наличие web-интерфейса для доступа к компонентам узла фильтрации Интернет-трафика, включая средства управления, полностью поддерживающего русский язык, используя кодировку текста UTF-8.

Требования к наличию отчетов:

* система должна обеспечивать формирование отчетности в табличном и графическом виде о совершаемых пользователями действиях в сети Интернет за различные периоды времени.

Дополнительные требования

* автоматическое или ручное обновление программных компонентов с сайта производителя.
* управление доступом к средствам контроля доступа в сеть Интернет и фильтрации трафика сети Интернет с использованием ролевой модели.
* протоколирование действий администраторов;
* обеспечение отказоустойчивости программно-аппаратных компонентов;
* Предоставление возможности автоматического развертывания серверов фильтрации трафика с использованием API.

Требования к происхождению

Поставляемое решение внесено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Межсетевой экран должен иметь действующий сертификат ФСТЭК России и соответствовать следующим требованиям:

- «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты» ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Д» четвертого класса защиты» ИТ.МЭ.Д4.ПЗ (ФСТЭК России, 2016);

- «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012);

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020). Четвертый уровень доверия.

* + 1. **Требования к монтажу, установке и настройке средств криптографической защиты**

Средства криптографической защиты передаются Исполнителю для их монтажа и установки в ЦОД Исполнителя силами Исполнителя. Средства криптографической защиты представляют собой интегрированные решения на базе специализированной аппаратной платформы и программного обеспечения, которое функционирует под управлением адаптированной операционной системы.

Исполнитель должен предусмотреть место размещения средств криптографической защиты с выделением необходимого места в ЦОД Исполнителя и выделением необходимой мощности питания оборудования Заказчика.

Исполнитель должен гарантировать:

исключение неконтролируемого проникновения или пребывания в месте размещения средств криптографической защиты;

системы электропитания и заземления в помещении соответствуют требованиям документа «Правила устройства электроустановок», утвержденные приказом Министерства энергетики Российской Федерации от 08.07.2004 № 204;

оборудование помещений, где эксплуатируются средства криптографической защиты средствами вентиляции и кондиционирования воздуха;

Исполнитель должен смонтировать средства криптографической защиты в выделенной инфраструктуре, осуществить ввод в эксплуатацию средств криптографической защиты с оформлением актов ввода в эксплуатацию в 2-х экземплярах – 1-ый экземпляр передается Заказчику, 2-ой экземпляр хранится у Исполнителя; произвести настройку в соответствии с технической документацией производителя средства криптографической защиты в целях организации защищенного канала связи между ЦОД Заказчика и ЦОД Исполнителя.

* + 1. **Требования к системе защиты виртуализации**

Система защиты виртуализации предоставляется в пользование в виде выделенных компьютеров для защиты от несанкционированного доступа систем гипервизора и должна осуществлять:

* аутентификацию администраторов виртуальной инфраструктуры и администраторов безопасности;
* защиту средств управления виртуальной инфраструктурой от НСД;
* защиту серверов от НСД;
* контроль целостности конфигурации виртуальных машин и их доверенную загрузку;
* мандатный принцип контроля доступа;
* регистрацию событий, связанных с информационной безопасностью;
* контроль целостности и защиту от НСД компонентов СЗИ;
* централизованное управление и мониторинг;
* создание резервной копии конфигурации СЗИ и журналов аудита;
* работу в отказоустойчивом режиме (кластер);
* синхронизация настроек безопасности между серверами СЗИ.

Требования к функциональности:

**- аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности.** Должна быть реализована модель разделения прав на управление виртуальной инфраструктурой и на управление безопасностью (для ограничения на использование привилегий суперпользователя). Должна быть возможность выделить 2 основные роли — администратор виртуальной инфраструктуры и администратор безопасности. В рамках роли администратора виртуальной инфраструктуры должна быть возможность разграничения доступа по привилегиям\типам объектов доступа. Должна быть поддержка аппаратных идентификаторов JaCarta, JaCarta2, RuToken и iButton. Доступ на управление виртуальной инфраструктурой или параметрами безопасности должен предоставляться только для аутентифицированных пользователей. Для этого в системе защиты виртуализации должна быть предусмотрена процедура аутентификации пользователей и компьютеров (рабочих мест администраторов), которая должна осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и атакам типа Man in the Middle.

Процедура аутентификации должна осуществляется с помощью отдельной программы, которую требуется запустить и ввести учетные данные до того, как осуществляется соединение с виртуальной инфраструктурой. Функционал аутентификации на рабочем месте администратора должен предоставлять возможность надежно сохранить учетные данные.

Для обеспечения защиты средств управления виртуальной инфраструктурой должен применяется функционал мандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Для этого весь управляющий трафик должен проходить через компонент системы защиты виртуализации, осуществляющий этот контроль. Правила разграничения доступа должны работать на основе меток и уровней безопасности, а также заданных ACL и параметров соединения (протоколов, портов).

Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами должен подписываться, для обеспечения защиты от атак типа Man in the Middle в процессе сетевого взаимодействия.

В системе защиты виртуализации должен присутствовать механизм блокирования любого сетевого трафика со стороны виртуальных машин к средствам управления виртуальной инфраструктурой. Тем самым должна обеспечивается защита средств управления виртуальной инфраструктурой от несанкционированного доступа со стороны скомпрометированной виртуальной машины. В системе защиты виртуализации должна быть предусмотрена возможность ограничения миграции виртуальных машин за пределы управления. В системе защиты виртуализации должен присутствовать оповещения администратора виртуальной инфраструктуры о том, что действие заблокировано СЗИ.

**- защита гипервизоров от несанкционированного доступа.** В рамках обеспечения защиты гипервизоров от несанкционированного доступа в системе защиты виртуализации должны быть реализованы следующие механизмы:

* создания списка разрешенных программ;
* контроля разграничения сети управления и сети виртуальных машин;
* настройки параметров логирования виртуальных машин;
* создания списков запрещенных устройств;
* отключения VIX API;
* запрета коммуникаций между виртуальными машинами;
* ограничения объема VMX-файла;
* контроля за использованием independent-nonpersistent дисков;
* проверки использования стандартных SSL сертификатов;
* отключения приветственной страницы;
* контроля службы виртуальной безопасности в гипервизоре;
* создания списка пользователей, которым разрешен локальный вход на виртуальный сервер;
* запретить сжатие виртуального диска;
* ограничения количества активный консольных подключений;
* блокирования подключения USB-носителей к виртуальному серверу;
* осуществления контроля и настройки правил встроенного межсетевого экрана;
* запрета клонирования и создания снимков виртуальных машин;
* очистки внешней и оперативной памяти при окончании работы с виртуальной машиной;
* ограничения доступа к конфигурационным файлам служб;
* запрета непосредственного доступа к управлению виртуального сервера;
* контроля использования протокола SSH;
* запрета операций с буфером обмена для каждой виртуальной машины;
* контроля использования CHAP для проверки подлинности при подключении iSCSI-устройств;
* создания парольных политик;
* отключения неиспользуемых протоколов, портов и функций;
* настройки безопасности виртуального коммутатора;
* запрета контроля устройств виртуального сервера со стороны виртуальных машин;
* запрета отсылки информации о производительности виртуального сервера гостевым системам;
* настройки синхронизации времени;
* запрета доступа к консоли виртуальной машины.

**- контроль целостности конфигурации виртуальных машин и доверенная загрузка.** Система защиты виртуализации должна содержать компоненты, устанавливаемые на каждый гипервизор и реализующие следующие механизмы защиты:

* контроль целостности настроек виртуальной машины перед ее загрузкой. Должен контролироваться файл \*.vmx, в котором содержится перечень устройств, доступных виртуальной машине, и ряд других критических параметров;
* контроль образа BIOS виртуальной машины. Поскольку несанкционированная подмена BIOS является угрозой безопасности, СЗИ должно контролировать целостность файла \*.nvram, в котором содержится образ BIOS виртуальной машины;
* доверенная загрузка ОС должна осуществляться путем контроля целостности загрузочного сектора виртуального диска \*.vmdk;
* контроль целостности шаблонов виртуальных машин, включая виртуальные жесткие диски.

При изменении одного из перечисленных объектов как санкционированном, так и несанкционированном, СЗИ должно предоставить администратору безопасности возможность данные изменения отменить или принять.

**- мандатный принцип контроля доступа.** В системе защиты виртуализации должен быть реализован мандатный принцип контроля доступа на основе меток конфиденциальности. Должно присутствовать два вида меток конфиденциальности: иерархические (метки) и неиерархические (категории).

Должна быть реализована возможность назначить метки на следующие субъекты, объекты, контейнеры:

* Администраторы ВИ;
* Виртуальные хосты;
* Сетевые адаптеры виртуального хоста;
* Виртуальные сети;
* Разделы хранилищ (Datastore);
* Виртуальные машины;
* Серверы управления;
* Группы объектов.

Права доступа субъектов и объектов должны проверяться на основе меток и категорий автоматически и запрещать несанкционированные действия. Субъект может получить доступ к объекту, только если выполняется условие соответствия их меток конфиденциальности. Для категорий – это совпадение хотя бы одной из категорий субъекта и объекта, для меток – это уровень иерархии субъекта должен быть равен (или выше, в зависимости от настроек СЗИ) уровню объекта.

Категории должны отличаться от меток следующими параметрами:

* Метки должны быть иерархическими, категории равноправными.
* Механизмы работы меток должны зависеть не только от пользователя, но и от его меток его текущей сессии. Категории от сессии зависеть не должны.
* Любой субъект, объект, контейнер может быть помечен несколькими категориями и только одной меткой.

Должен быть предусмотрен механизм отключения контроля мандатного доступа по типам объектов.

Должен быть предусмотрим механизм автоматизированного добавления виртуальных машин в группы объектов.

**- регистрация событий, связанных с информационной безопасностью.**

В системе защиты виртуализации должен быть реализован механизм регистрации следующих групп событий:

* аутентификации и разграничения доступа;
* попыток доступа к инфраструктуре (с указанием имени учетной записи, даты, имени компьютера или его IP-адреса)
* изменения конфигурации параметров безопасности и учетных записей администраторов инфраструктуры
* контроля целостности СЗИ, контроля целостности и доверенной загрузки виртуальных машин;
* связанных с установкой, удалением, включением, остановом и сбоем компонентов системы защиты виртуализации, а также с изменением настроек системы защиты виртуализации.

Регистрация событий на всех компонентах системы защиты виртуализации должна осуществляется в едином журнале. Для всех групп событий должны регистрироваться как факты НСД, так и правомочные действия.

Должна быть возможность отбора событий безопасности по типу, дате и времени события, объекту\субъекту доступа.

В системе защиты виртуализации должен быть реализован механизм отправки уведомлений о событиях безопасности по протоколам SMTP и Syslog.

**- контроль целостности и защита от НСД компонентов системы защиты виртуализации.** Система защиты виртуализации должна содержать собственные механизмы контроля целостности компонентов системы защиты виртуализации. Механизмы должны действовать на всех компонентах СЗИ.

**- централизованное управление и мониторинг.** Система защиты виртуализации должна содержать Консоль управления, устанавливающуюся на рабочее место администратора безопасности со следующим функционалом:

* управление учетными записями администраторов виртуальной инфраструктуры и администраторов безопасности;
* назначение прав на доступ к защищаемым объектам;
* развертывание и настройка компонентов защиты Виртуального хостов;
* настройка правил разграничения запуска виртуальных машин и утверждение изменений параметров виртуальных машин, произведенных администраторами ВИ;
* просмотр журнала регистрации событий безопасности.
* Все изменения, произведенные администратором безопасности, должны сохраняться централизованно.

Требования по сертификации:

система защиты виртуализации должна быть сертифицирована на соответствие требованиям:

Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности,

* «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - не ниже 4 уровня доверия.

Администрирование системы защиты виртуализации осуществляется Заказчиком.

* + 1. **Требования к средствам антивирусной защиты**

Средства антивирусной защиты предоставляются в виде неисключительных (пользовательских) прав на программное обеспечение (30 шт.) и сертифицированного комплекта дистрибутивов для рабочих станций (серверов) под управлением операционных систем семейства Windows и Linux.

Общие требования для средств антивирусной защиты:

Программное средство антивирусной защиты информации включает в себя:

программные средства антивирусной защиты для рабочих станций и серверов Windows;

программные средства антивирусной защиты для рабочих станций и серверов Linux;

Программные средства антивирусной защиты для рабочих станций Windows обеспечивают реализацию следующих функциональных возможностей:

антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;

антивирусное сканирование по расписанию;

антивирусное сканирование подключаемых устройств;

эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;

нейтрализации действий активного заражения;

анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;

анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;

откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;

ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;

облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;

фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;

проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;

блокировку баннеров и всплывающих окон на загружаемых Web-страницах;

распознавания и блокировку фишинговых и небезопасных сайтов;

встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;

защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;

возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;

контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;

создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;

контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;

возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;

записи в журнал событий о записи и/или удалении файлов на съемных дисках;

контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;

защиты от атак типа BadUSB;

запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;

установки только выбранных компонентов программного средства антивирусной защиты;

централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

запуск задач по расписанию и/или сразу после запуска приложения;

гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

возможность проверки целостности антивирусной программы;

возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;

наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

наличие защищенного хранилища для отчетов о работе антивируса;

возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;

возможность интеграции с Windows Defender Security Center;

наличие поддержки Antimalware Scan Interface (AMSI);

наличие поддержки Windows Subsystem for Linux (WSL);

возможность защитить паролем восстановление объектов из резервного хранилища;

резидентного антивирусного мониторинга;

облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

проверку ресурсов доступных по SMB / NFS;

эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

антивирусное сканирование по команде пользователя или администратора и по расписанию;

антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;

проверку сообщений электронной почты в текстовом формате (Plain text);

наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);

защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;

помещение подозрительных и поврежденных объектов на карантин;

проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов;

возможность перехвата и проверки файловых операций на уровне SAMBA;

управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;

запуск задач по расписанию и/или сразу после загрузки операционной системы;

возможность экспортировать и сохранять отчеты в форматах HTML и CSV;

гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;

возможность управления через пользовательский графический интерфейс без root прав;

централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Программный интерфейс всех антивирусных средств, включая средства управления, на русском и английском языке.

Все антивирусные средства, включая средства управления, обладают контекстной справочной системой на русском и английском языке.

Требования по сертификации:

- средство антивирусной защиты должно быть сертифицировано на соответствие требованиям ФСТЭК России «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012) не ниже 2 класса защищенности.

Администрирование средств антивирусной защиты осуществляется Заказчиком.

* + 1. **Требования к средствам доверенной загрузки**

Средство доверенной загрузки должно осуществлять:

- идентификацию и аутентификацию пользователей;

- доверенную загрузку;

- контроль целостности программной и аппаратной среды;

- функции сторожевого таймера;

- ведение журнала регистрации событий

Требования к функциональности:

- идентификация пользователей (должна производиться по отчуждаемому персональному идентификатору, а аутентификация - по вводимому с клавиатуры паролю);

- должна обеспечиваться работа с паролями администратора или пользователя длиной до 127 символов;

- должна иметься возможность задавать имя пользователя длиной до 40 символов;

- СДЗ должно обеспечивать возможность регистрации до 300 пользователей на одном компьютере;

- защита от несанкционированной загрузки нештатной операционной системы (ОС);

СДЗ должно иметь возможность контролировать целостность:

- файлов и физических секторов жесткого диска;

- элементов системного реестра;

- журнала транзакций NTFS и EXT4;

- PCI-устройств;

- структур SMBIOS;

- в комплекте поставки должны быть драйверы платы, которые должны функционировать в среде следующих ОС Windows и ОС Linux имеющихся у заказчика, при этом должна обеспечиваться возможность получения случайных последовательностей с физического датчика случайных чисел платы СДЗ для ПО в ОС;

- поддержка файловых систем NTFS, FAT32, FAT16, EXT4, EXT3, EXT2;

- реализация функции сторожевого таймера посредством воздействия на механизм reset и на питание ЭВМ;

- функционирование журнала событий безопасности и его хранение в энергонезависимой памяти платы СДЗ с возможностью экспорта в виде текстового файла;

Требования по сертификации:

Средство доверенной загрузки должно быть сертифицировано на соответствие требованиям ФСТЭК России «Профиль защиты средств доверенной загрузки уровня платы расширения второго класса защиты ИТ.СДЗ.ПР2.ПЗ» (ФСТЭК России, 2013), «Требования к средствам доверенной загрузки (ФСТЭК России, 2013);

Администрирование средств доверенной загрузки осуществляется Заказчиком.

* + 1. **Требования к средствам защиты от несанкционированного доступа**

Средства защиты от НСД предоставляются в виде универсальных неисключительных прав на использование программного обеспечения (30 шт.) для установки на ПЭВМ под управлением имеющейся у Заказчика операционной системы Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Windows Server 2016, CentOS 7.7, CentOS 8.0 и сертифицированных комплектов дистрибутивов (для Windows и Linux).

СЗИ поддерживает 32- и 64-битные версии операционных систем.

Средства защиты от НСД должны осуществлять:

* контроль входа пользователей в систему, в том числе с использованием аппаратных средств защиты;
* разграничение доступа пользователей к защищаемым ресурсам (файлам, каталогам) компьютера;
* разграничение доступа пользователей к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам;
* уничтожение (затирание) содержимого файлов при их удалении;
* очистку освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств);
* контроль целостности ключевых компонентов и объектов файловой системы;
* создание замкнутой программной среды для пользователей;
* межсетевое экранирование сетевого трафика;
* регистрацию событий безопасности в журналах;
* контроль действий пользователей, связанных с доступом к файлам, устройствам и узлам вычислительной сети;
* проведение аудита действий субъектов (пользователей, процессов) с объектами файловой системы и аудита сетевых соединений.

СЗИ должно допускать использование в следующих информационных системах:

* автоматизированные системы - до класса 2Г (включительно);
* государственные информационные системы – до 2 класса защищенности (включительно);
* информационные системы персональных данных – до 2 уровня защищенности (включительно);
* автоматизированные системы управления производственными и технологическими процессами – до 2 класса защищенности (включительно).

СЗИ должно выполнять следующие функции по защите информации:

* контроль входа пользователей в систему как по логину/паролю, так и с использованием аппаратных средств усиленной аутентификации.
* совместное функционирование с программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей.
* разграничение доступа пользователей к защищаемым ресурсам (файлам, каталогам) компьютера.
* создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы, файлы загружаемых библиотек, запуск скриптов по технологии. Должна иметься возможность формирования списка исключений для ресурсов, в который входят разрешенные для запуска программы, файлы, библиотеки и скрипты.
* контроль устройств, подключаемых к шинам USB, SATA, IEEE 1394. Контролируемые устройства должны идентифицироваться по следующим параметрам: VendorID, DeviceID, серийный номер, а также у администратора должна быть дополнительная возможность задать для каждого устройства условную символьную метку для его идентификации.
* затирание освобождаемых страниц оперативной памяти, при этом должна быть предусмотрена возможность разбиения больших страниц на более мелкие непосредственно перед очисткой; затирание освобождаемых блоков на файловых системах EXT2, EXT3, EXT4 и VFAT; безопасное удаление информации на жестких дисках и внешних носителях; затирание страниц SWAP при выключении компьютера или перезагрузке операционной системы.

- функциональный самоконтроль средства защиты.

- контроль целостности критических объектов операционной системы и ресурсов файловой системы компьютера, поставленных на контроль администратором. Контроль целостности должен проводиться в автоматическом режиме при загрузке операционной системы. Также администратор должен иметь возможность вручную запустить проверку целостности защищаемых ресурсов.

- поддержка следующих режимов реакции СЗИ на нарушение целостности объектов: только регистрация события безопасности; блокировка АС в случае нарушения безопасности; восстановление из эталонного значения (для файловых объектов) и блокировка АС.

- межсетевое экранирование сетевого трафика на основе формируемых правил фильтрации на сетевом, транспортном и прикладном уровне запросов. Должна осуществляться фильтрация с учетом полей сетевых пакетов, направления трафика, сетевого интерфейса, с учетом расписания.

- регистрация событий безопасности в журнале безопасности, контроль действий пользователей: доступ к защищаемым файлам, устройствам и узлам вычислительной сети; событий вывода файлов на печать.

- аудит действий субъектов с объектами файловой системы и сетевых соединений, аудит отчуждения информации.

- аудит действий администратора при доступе к файловым объектам.

- фильтрация событий безопасности, контекстный поиск в журнале безопасности.

- автоматическое построение отчетов по результатам аудита.

- управление СЗИ: с помощью графического интерфейса и командной строки.

Требования по сертификации:

СЗИ должно соответствовать требованиям руководящих документов:

* «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности,
* «Требования к межсетевым экранам» (ФСТЭК России, 2016) – не ниже 4 класса защиты,
* «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016),
* «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - не ниже 4 уровня доверия.

Администрирование средств защиты информации от несанкционированного доступа осуществляется Заказчиком.

* 1. **Требования к исполнителю**

Исполнитель должен обеспечивать эксплуатацию и техническую поддержку предоставляемой Заказчику выделенной инфраструктуры.

Исполнитель должен назначить выделенного Сервис-Менеджера для оказания услуг по управлению технической поддержкой выделенной инфраструктуры и каналов связи, предоставляемых в рамках оказания услуги. В рамках данной услуги Сервис-Менеджер обязан:

- установить и поддерживать оперативную связь с уполномоченными представителями Заказчика для выполнения условий контракта;

- проводить измерение, отслеживание и оценку уровня услуг, оказываемых в соответствии с уровнями обслуживания;

- обеспечить координацию и управление деятельностью технического персонала, связанного с указанием услуг;

- проводить ежемесячные совещания, путем сеансов конференцсвязи или совещаний на территории Заказчика с целью:

- анализа любых проблем, которые возникают при взаимодействии со службой технической поддержки;

- согласования любых действий по результатам сеанса конференцсвязи или совещания;

- согласования сроков завершения таких действий;

- согласования сроков проведения будущих ежемесячных сеансов конференцсвязи или совещаний и предварительного согласования целей и задач сеансов конференцсвязи/совещаний.

- обеспечить подготовку отчетов в соответствии с условиями требований к документации;

- разработать и предоставить план работ по техническому обслуживанию и сопровождению на период действия договора и отслеживать его выполнение;

- быть осведомленным о запросах приоритета 1, осуществленных со стороны Заказчика в службу технической поддержки Исполнителя и отслеживать последующие действия;

- при необходимости координировать взаимодействие между техническим персоналом Заказчика и соответствующим персоналом Исполнителя.

**Исполнитель должен обладать**

1. Лицензией Роскомнадзора на осуществление деятельности в области оказания услуг связи с местом действия на территории РФ, на которой располагаются Объекты Заказчика, для следующих услуг связи, утверждённых постановлением Правительства РФ от 18.02.2005 № 87 «Об утверждении перечня наименований услуг связи, вносимых в лицензии и перечней лицензионных условий»:

* - Услуги связи по предоставлению каналов связи (п.13 постановления);
* - Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации (п.14 постановления).

1. Лицензией ФСБ России на разработку, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание 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) согласно Постановлению Правительства РФ от 16 апреля 2012 г. N 313: Предоставление юридическим и физическим лицам защищённых с использованием шифровальных (криптографических) средств каналов связи для передачи информации (п.27 постановления).
   1. **Требования к мониторингу и службе технической поддержки Исполнителя**

Для обеспечения бесперебойного и эффективного оказания услуги Исполнитель должен организовать функционирование службы технической поддержки.

Служба технической поддержки Исполнителя должна иметь утвержденный порядок управления инцидентами, в том числе и инцидентами информационной безопасности.

Служба технической поддержки Исполнителя должна быть доступна для обращения специалистов Ответственных лиц Заказчика круглосуточно без перерывов 24 (Двадцать четыре) часа в сутки, 7 (Семь) дней в неделю, 365 дней в году.

Заказчик должен иметь самостоятельную возможность получения информации об объеме используемых ресурсов.

Исполнитель предоставляет выделенный телефонный номер для регистрации заявок.

Предоставленная телефонная линия и доступ в веб-порталу должны быть доступны в формате 24х7х365.

В ЦОД, используемом Исполнителем для оказания Услуги должна функционировать собственная диспетчерская служба, контролирующая в круглосуточном режиме работу оборудования основных инженерных систем, систем жизнеобеспечения, режимы их работы, возникновения аварийных ситуаций, температурно-влажностные режимы технологических помещений, осуществляет сбор информации и отображение текущего состояния инженерных систем в режиме реального времени, хранение исторических данных, возможности их отображения и анализа.

Наличие у Исполнителя формализованных и функционирующих процессов управления инцидентами и изменениями в соответствии с методологией ITIL/ITSM.

Время реакции на инциденты должно быть гарантированным и указываться в SLA.

Служба технической поддержки Исполнителя должна информировать представителей Заказчика о проведении плановых/технологических работ, а также о возникших инцидентах и ходе работ по их устранению.

Взаимодействие Заказчика и Исполнителя должно осуществляться в рамках потребления и оказания Услуг через централизованную службу поддержки Исполнителя в соответствии с правилами взаимодействия Исполнителя и Заказчика.

Правила взаимодействия Исполнителя и Заказчика должны содержать:

* + описание способов взаимодействия со службой технической поддержки;
  + описание классификаций обращений и определение приоритетов;
  + описание требований к заполнению обращений;
  + описание статусов обращений.

Все поступающие обращения контактных лиц Заказчика должны регистрироваться в системе учета и обработки обращений Заказчика, при этом каждому обращению должен присваиваться уникальный номер, который в дальнейшем помогает идентифицировать обращение. При регистрации обращения и при изменении его статуса, контактное лицо Заказчика автоматически информируется системой посредством отправки электронных писем на адрес, указанный при регистрации контактного лица Заказчика.

Обращения должны получать приоритеты в зависимости от установленного значения срочности и влияния на бизнес-процессы.

Обращения категории «Инцидент» должны получать приоритеты в зависимости от установленного значения срочности и влияния на бизнес-процессы согласно модели, описанной в SLA.

* 1. **Требования к соглашению об уровне обслуживания (service level agreement)**

Услуга по предоставлению выделенной инфраструктуры и каналов связи в ЦОД Исполнителя должна оказываться в режиме «24х7х365» - 24 часа в сутки, 7 дней в неделю, 365 дней в году.

**Требования к параметрам оказываемой услуги:**

**- Время оказания и показатели доступности услуг.**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Услуга** | **Время предоставления** | **Уровень доступности** |
| 1. | Предоставление выделенной инфраструктуры в центре обработки данных Исполнителя | 24х7х365 - 24 часа в сутки, 7 дней в неделю, 365 дней в году | 99,982% |

**- Параметры услуги – Предоставление выделенной инфраструктуры в центре обработки данных Исполнителя.**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Метрика** | **Допустимое значение** | **Измерение** |
| 1. | Время доступа к SATA-диску на виртуальной машине | не более 30 мс при интенсивности ввода-вывода 100 IOPS/TB, но не более 3 500 IOPS | Среднее значение на интервале 20 минут по данным интерфейса управления СХД. Размер блока 4 KB, отношение количества операций чтение/запись 70/30 |
| 2. | Время доступа к SAS-диску на виртуальной машине | не более 20 мс при интенсивности ввода-вывода 200 IOPS/TB, но не более 7 000 IOPS | Среднее значение на интервале 20 минут по данным интерфейса управления СХД. Размер блока 4 KB, отношение количества операций чтение/запись 70/30 |
| 3. | Время доступа к SSD-диску на виртуальной машине | Не более 3 мс при интенсивности ввода-вывода 2 000 IOPS/TB, но не более 15 000 IOPS или 800 MB/s. | Среднее значение на интервале 20 минут по данным интерфейса управления СХД. Размер блока 4 KB, отношение количества операций чтение/запись 70/30 |
| 4. | CPU Ready | До 10%. | Среднее значение по всем ядрам, система мониторинга Исполнителя |
| 5. | RAM Swapped процент от сконфигурированной памяти VM | До 10% | Система мониторинга Исполнителя |

**- Устранение инцидентов. Приоритеты инцидентов.**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Приоритет инцидента** | **Описание** |
| Инцидент – неисправность, сбой в работе оборудования или ПО, иное событие, повлекшее ухудшение зафиксированного в SLA качества или полное / частичное прекращение предоставляемой Исполнителем услуги. | | |
| 1 | Приоритет 1 | Не доступна виртуальная машина на уровне программно-аппаратного комплекса Исполнителя |
| RAM Swapped процент от сконфигурированной памяти виртуальной машины свыше 30% |
| HDD IOPS уменьшение на 50% и более от оговоренных значений |
| Среднее время отклика SSD-диска на виртуальной машине от 10мс до 20мс |
| Среднее время отклика SAS-диска на виртуальной машине свыше 100мс |
| Среднее время отклика SATA-диска на виртуальной машине свыше 120мс |
| Процент потерянных пакетов в пределах СПД Исполнителя более 1% |
| Средняя сетевая задержка в пределах СПД Исполнителя более 20мс |
| 2 | Приоритет 2 | Отсутствие доступа к интерфейсу управления виртуальными машинами более 2 часов |
| RAM Swapped процент от сконфигурированной памяти виртуальной машины 20% - 30% |
| HDD IOPS уменьшение от 20% до 50% от оговоренных значений |
| Среднее время отклика SSD-диска на виртуальной машине от 5мс до 10мс |
| Среднее время отклика SAS-диска на виртуальной машине 40-80мс |
| Среднее время отклика SATA-диска на виртуальной машине 50-100мс |
| Процент потерянных пакетов в пределах сети передачи данных Исполнителя от 0,4% до 1% |
| Средняя сетевая задержка в пределах сети передачи данных Исполнителя от 5мс до 20мс |
| 3 | Приоритет 3 | RAM Swapped процент от сконфигурированной памяти виртуальной машины 10% - 20% |
| HDD IOPS уменьшение от 10% до 20% от оговоренных значений |
| Среднее время отклика SSD-диска на виртуальной машине от 3мс до 5мс |
| Среднее время отклика SAS-диска на виртуальной машине от 20мс до 40мс |
| Среднее время отклика SATA-диска на виртуальной машине от 30мс до 50мс |
| Процент потерянных пакетов в пределах сети передачи данных Исполнителя от 0,2% до 0,4% |

**- Решение инцидентов.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Приоритет инцидента** | **Обработка** | **Время реакции на инцидент, минут\*** | **Максимальное время решения инцидента, минут\*\*** | **Суммарное время решения инцидентов в месяц, не более, минут** |
| 1. | 1 | Круглосуточно | 5 | 120 | 120 |
| 2. | 2 | Круглосуточно | 5 | 160 | 320 |
| 3. | 3 | Круглосуточно | 5 | 310 | 930 |

*\*Принятие и регистрация обращения, классификация и приоритизация. Заказчик уведомляется соответствующим электронным письмом.*

*\*\*Время решения инцидента начинает считаться с момента уведомления Заказчика о его регистрации и присвоении идентификационного номера до момента его решения.*

- **Обработка запросов пользователей. Классификация и приоритеты запросов**.

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Классификация** | **Приоритет** | **Описание** |
| 1. | Запрос на обслуживание | 4 | Зафиксированная потребность Заказчика в обслуживании в рамках предоставляемых ему услуг (определённых в SLA или описанных в спецификации для Заказчика) или компонент, их образующих, не связанное со сбоем или отказом в IT-инфраструктуре. |
| 2. | Запрос на изменение | 5 | Запрос, приводящий к изменению состава и/или объема услуг, определённых в SLA или описанных в спецификации для Заказчика. |
| 3. | Запрос на предоставление информации | 6 | Запрос на предоставление информации по услуге, включая отчёты по объёму трафика, сервисные отчёты, отчёты по мониторингу и т.д. |

**- Обработка запросов.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Категория** | **Приоритет** | **Обработка** | **Время реакции на запрос, минут\*** | **Максимальное время решения запроса, не более часов\*\*** |
| 1. | Запрос на обслуживание | 4 | В рабочие часы\*\*\* | 20 | 12 |
| 2. | Запрос на изменение | 5 | В рабочие часы | 20 | 16\*\*\*\* |
| 3. | Запрос на предоставление информации | 6 | В рабочие часы | 20 | 72 |

*\*Принятие и регистрация обращения, классификация и приоритизация. Заказчик уведомляется соответствующим электронным письмом.*

*\*\*Время решения обращения начинает считаться с момента уведомления Заказчика о его регистрации и присвоении идентификационного номера до момента его решения.*

*\*\*\*В рабочие часы Заказчика: рабочие дни РФ с 9.00 до 18.00.*

*\*\*\*\*Время решения запроса на изменение сводится к времени расценки работ и материалов, необходимых для проведения изменений, а также ознакомлению Заказчика со сроками проводимых изменений.*

**- Проведение регламентных работ.**

| **№ п/п** | **Позиция** | **Показатели** | **Уведомление  Заказчика** | **Дополнительные условия** |
| --- | --- | --- | --- | --- |
| 1. | Проведение технологических работ | Суммарная продолжительность перерывов в работе услуги – не более 1,6 часов в год. Интервалы между перерывами – не менее 30 календарных дней. | Не менее чем за 5 календарных дня до начала перерыва | Время проведения работ согласовывается с Заказчиком |
| 2. | Проведение экстренного обновления, связанного с установкой выпускаемых производителем обновлений (upgrades) и\или корректирующих заплаток (patches) имеющих критическое значение для работоспособности, производительности, безопасности ПО | Время перерыва равно фактическому времени установки обновлений (upgrades), корректирующих заплаток (patches) и тестирования | Непосредственно перед началом работ | Предполагаемая продолжительность проведения работ сообщается Заказчику |

**- Типовые обращения/инциденты и их классификация**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Категория запроса** | **Описание** | **Условия** | **Приоритет** |
| 1. | Запрос на обслуживание | Восстановление ВМ | восстановление ВМ из резервной копии. | 4 |
| 2. | Запрос на обслуживание | Установка ОС | Развертывание образа на виртуальную машину (установка ОС) | 4 |
| 3. | Запрос на обслуживание | Изменение настоек сети | Настройка сетевой связанности, изменение параметров сети BM (IP, VPN, VLAN) | 4 |
| 4. | Запрос на обслуживание | Перемещение ВМ | Обслуживание по запросу заказчика. Операции по миграции ВМ, либо ее HDD. | 4 |
| 5. | Запрос на изменение | Изменение объектов обслуживания | Добавление или изъятие объектов обслуживания (расширить виртуальные машины, расширить параметры ВМ, новая ВМ) | 5 |
| 6. | Запрос на изменение | Изменение условий обслуживания | Изменение параметров SLA, контактных лиц со стороны Заказчика, изменение взаимодействий. | 5 |
| 7. | Запрос на предоставление информации | Предоставление отчета | Формирование внеочередного отчета с дополнительными критериями оценки | 6 |
| 8. | Запрос на предоставление информации | Предоставление отчета | Предоставление дополнительной информации о структуре дополнительных услуг и их стоимости. | 6 |

* 1. **Требования к объему вычислительных ресурсов и ресурсов хранения данных**

Общее количество ресурсов, предоставляемое в рамках оказания услуги, должно быть в объёме не менее:

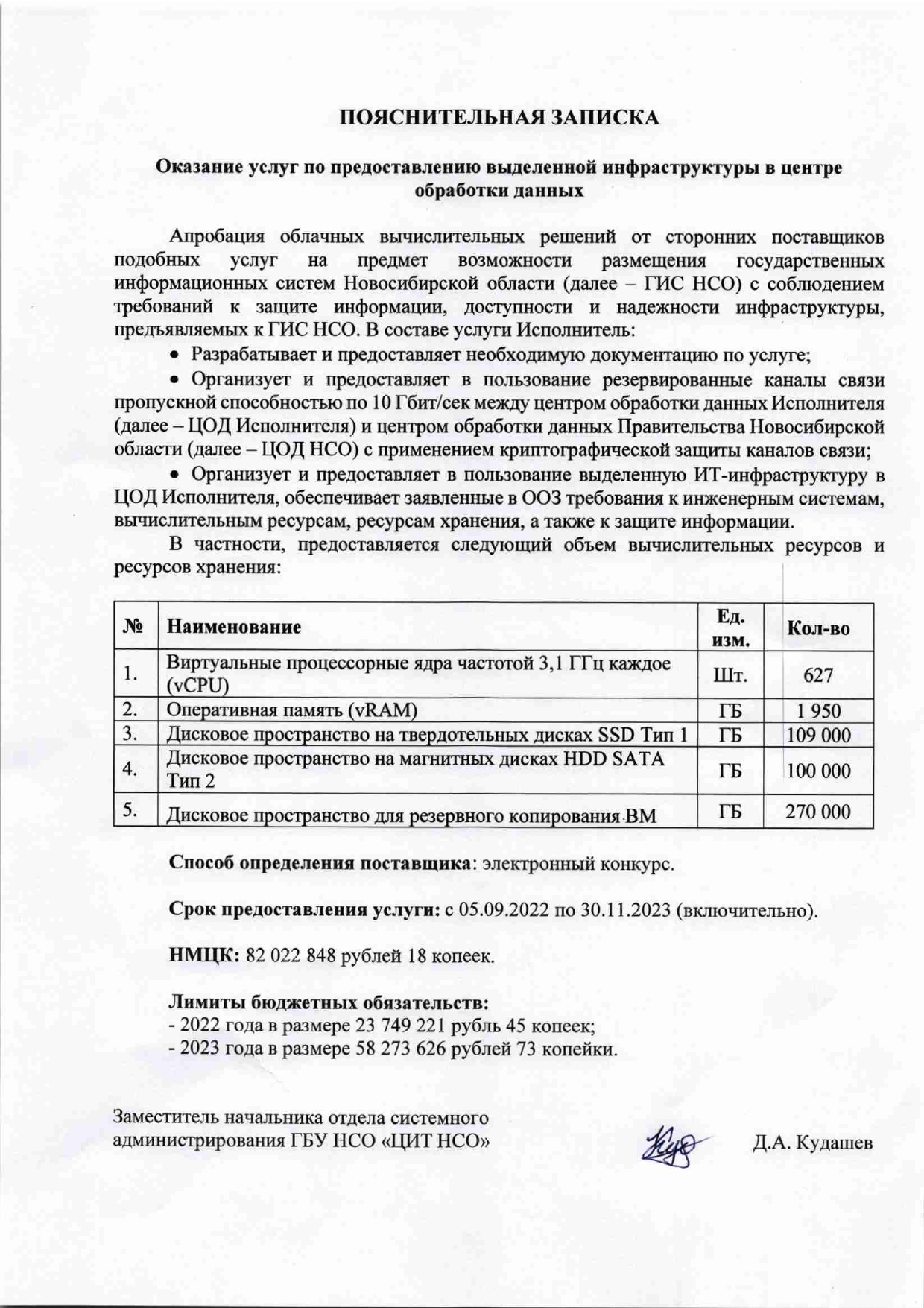
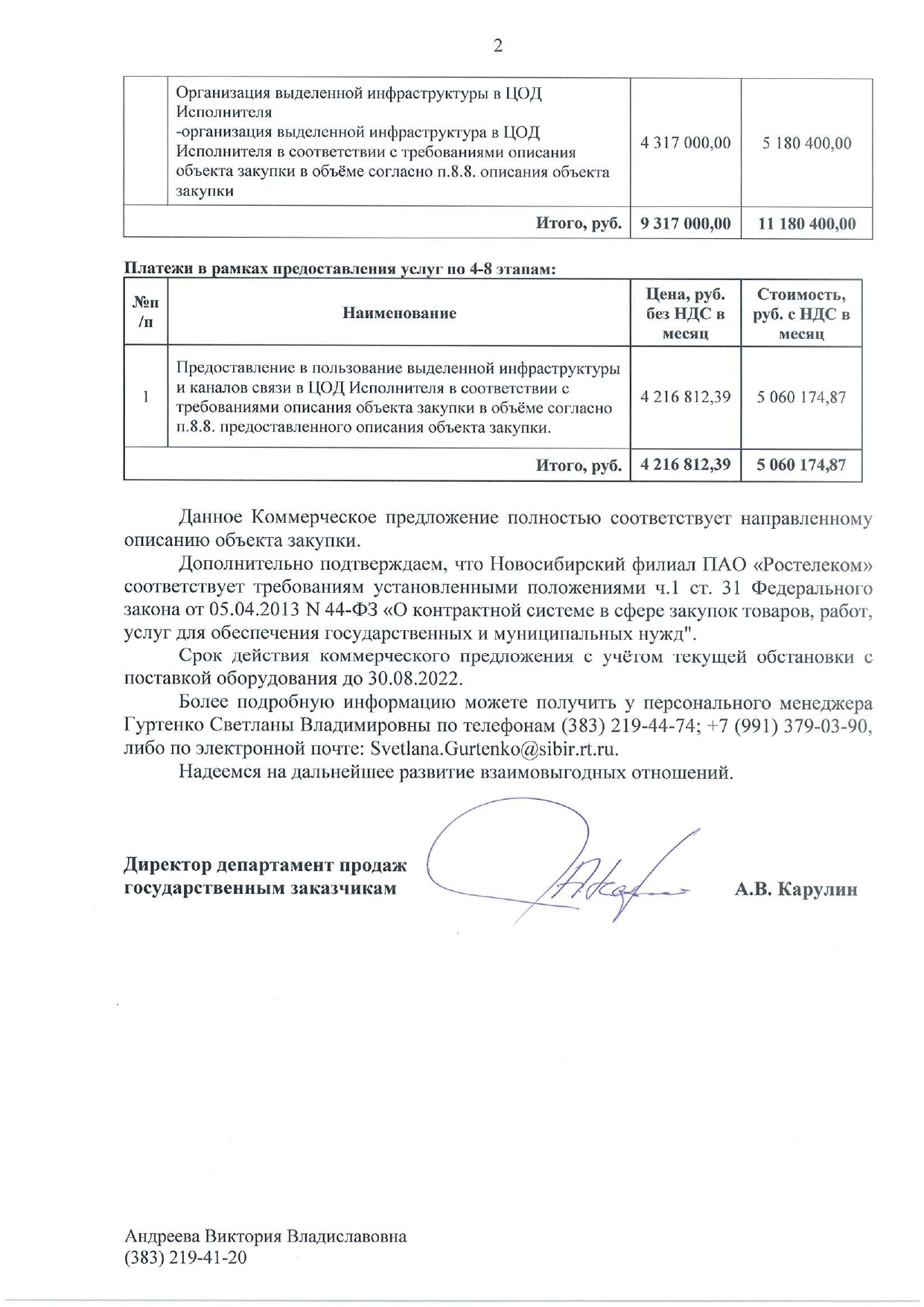
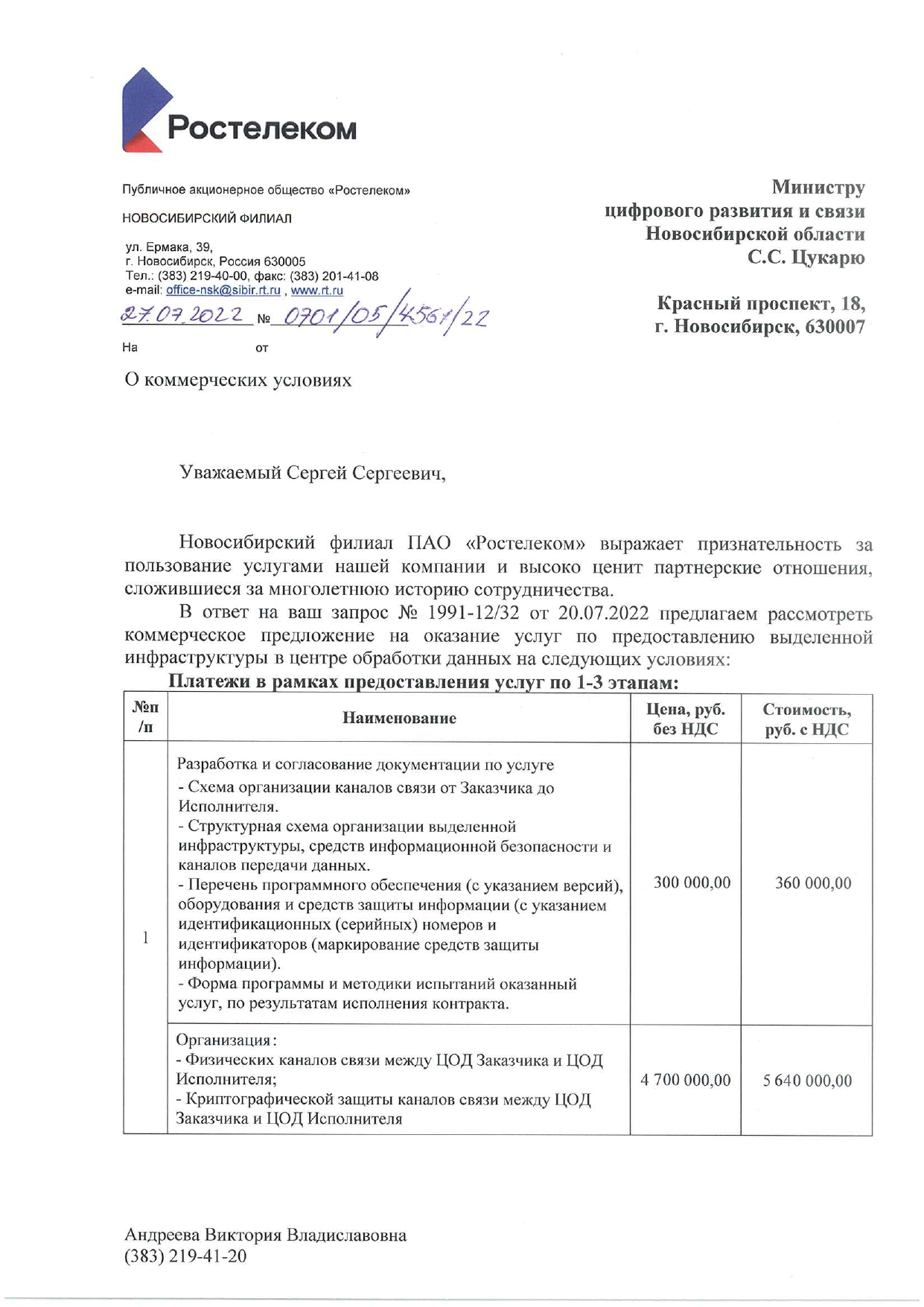
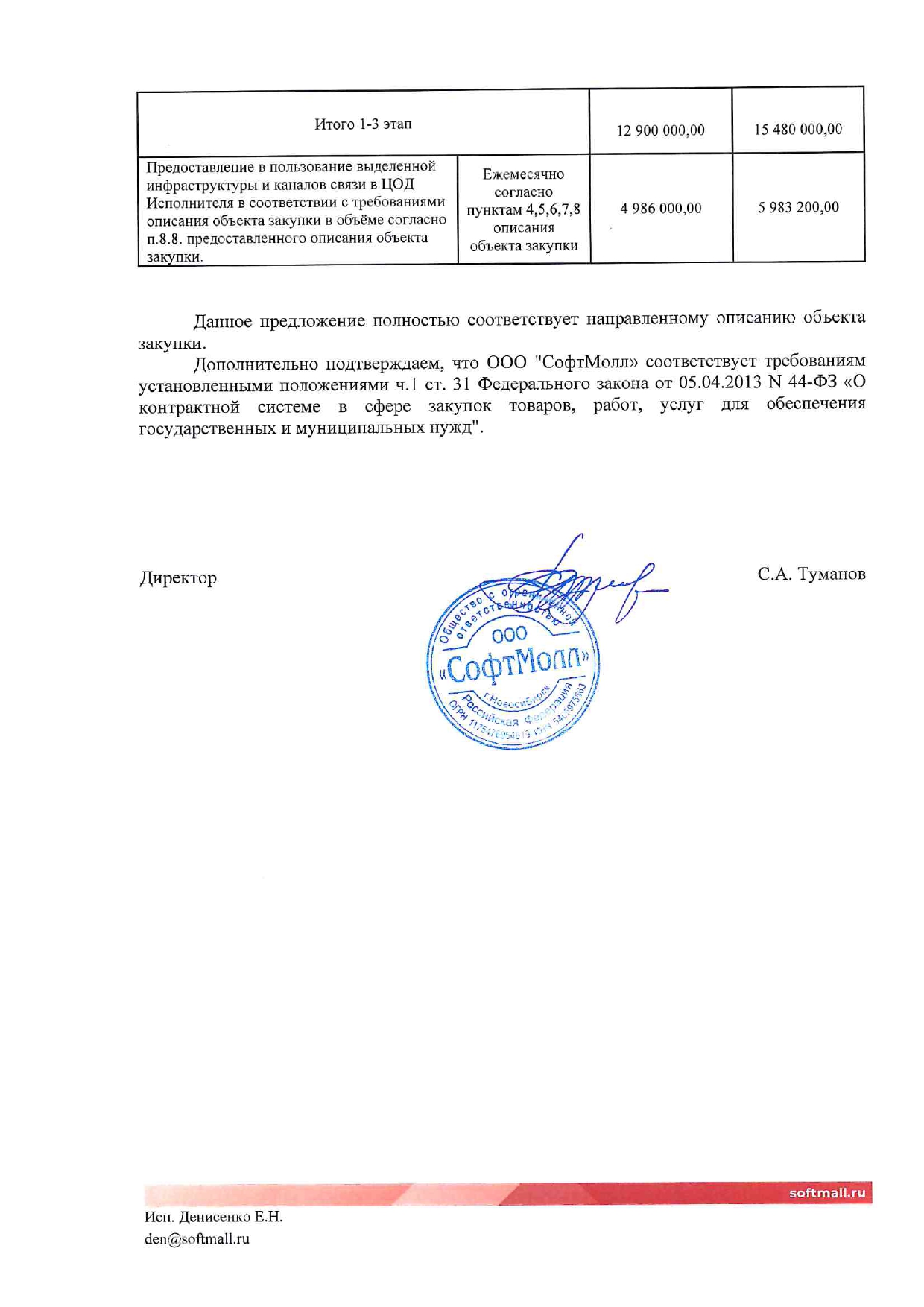
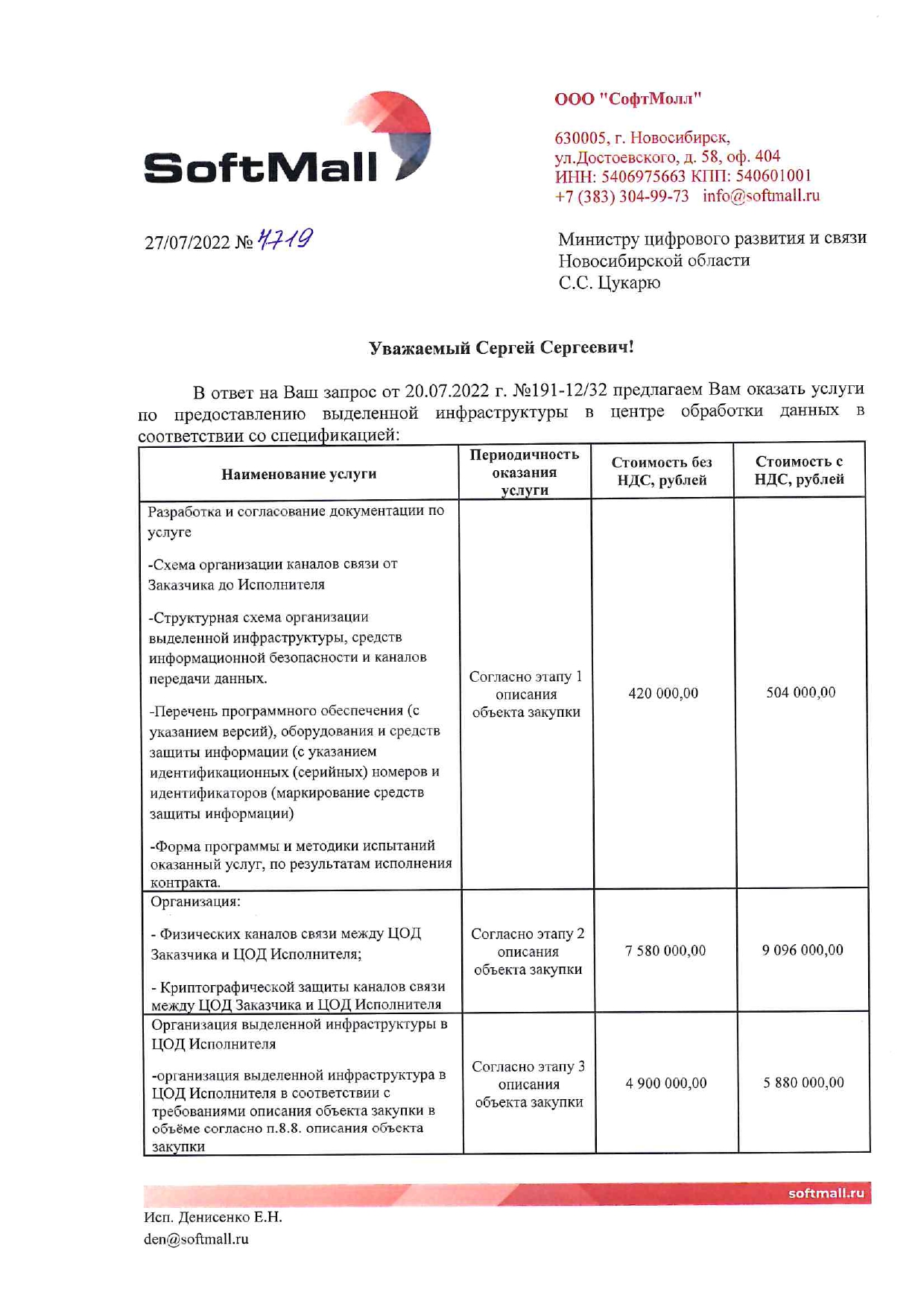
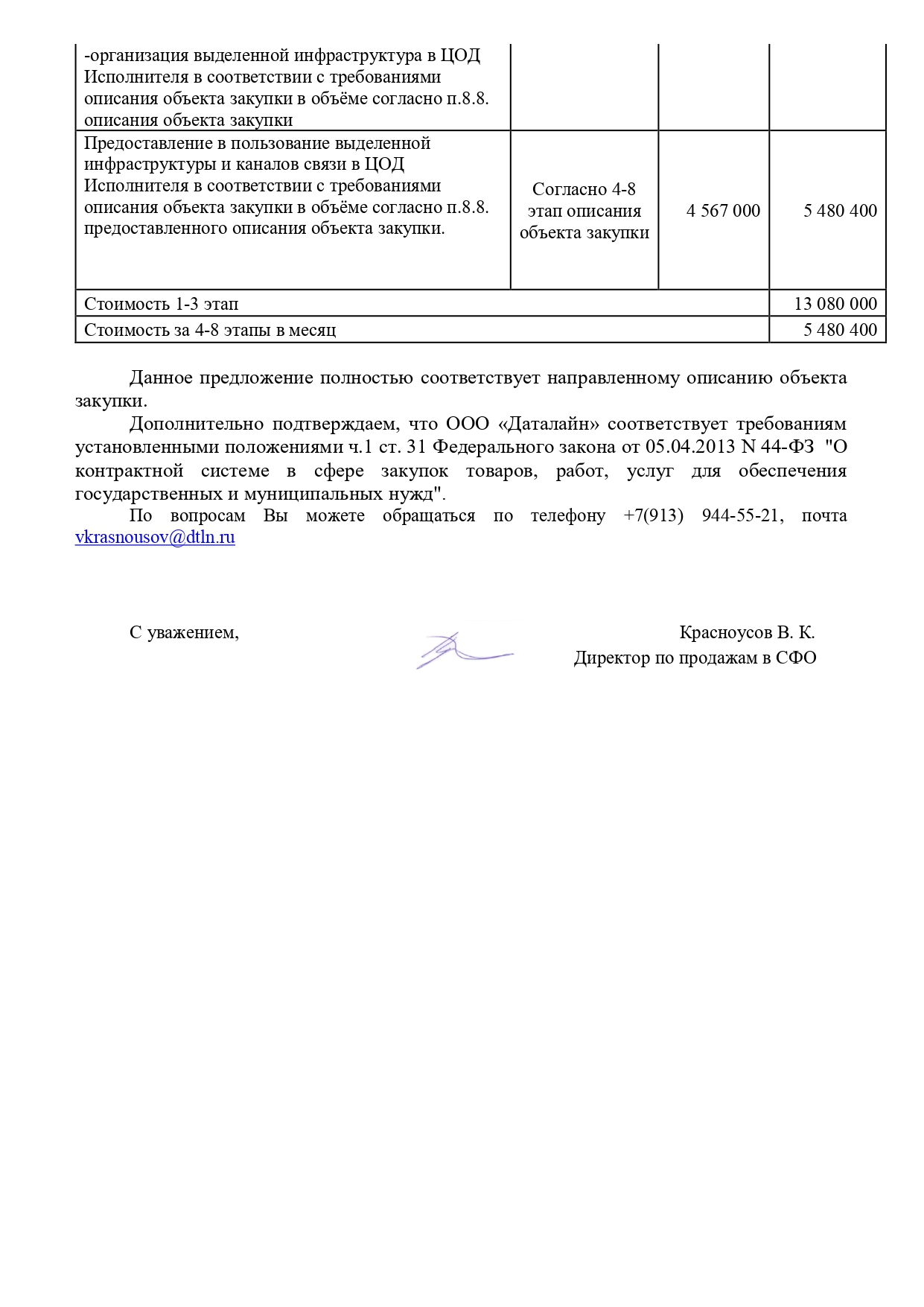
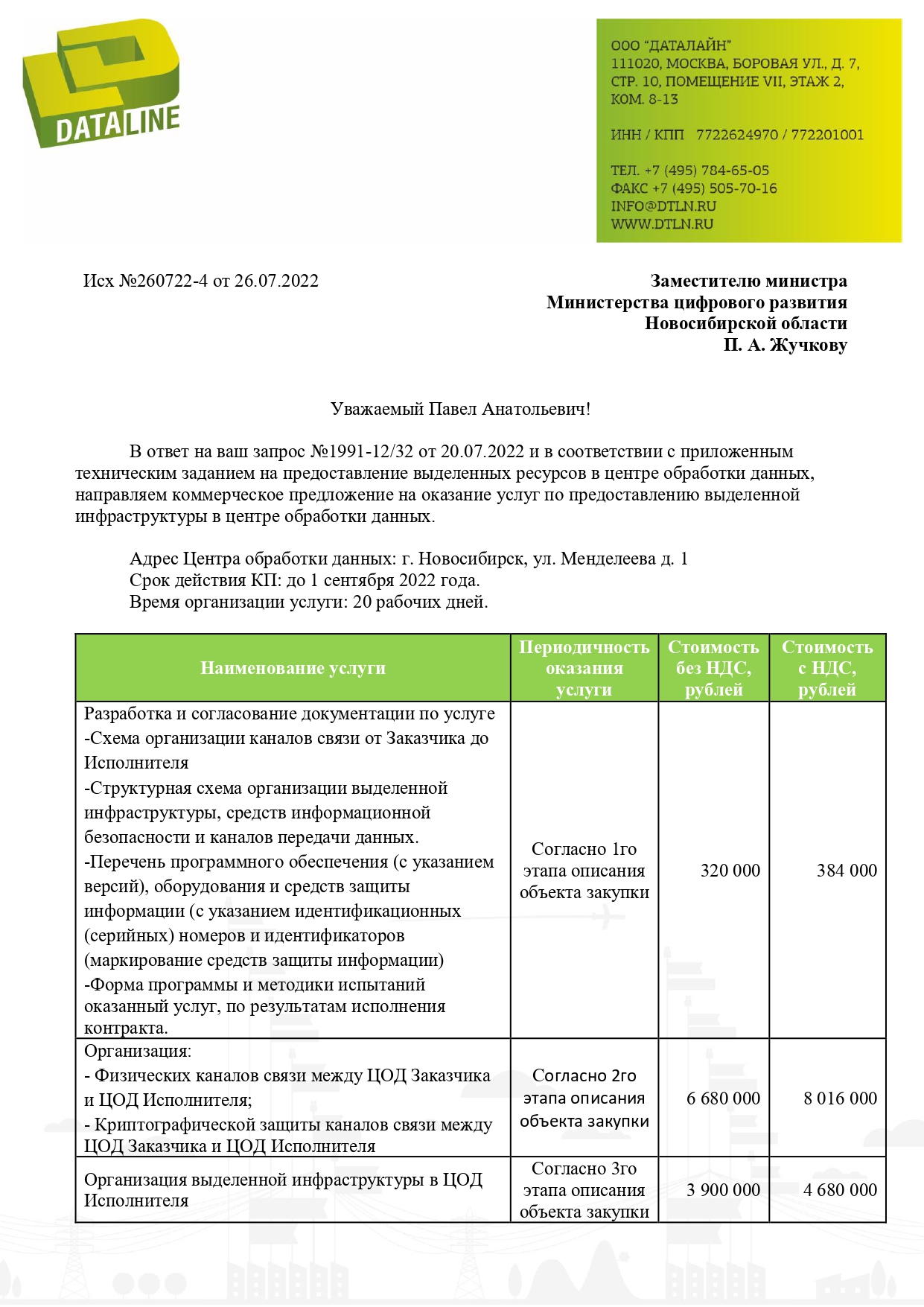
|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Ед. изм.** | **Кол-во** |
| 1. | vCPU | Шт. | 627 |
| 2. | vRAM | ГБ | 1 950 |
| 3. | HDD SSD Тип 1 | ГБ | 109 000 |
| 4. | HDD SATA Тип 2 | ГБ | 100 000 |
| 5. | Дисковое пространство для резервного копирования ВМ | ГБ | 270 000 |
| 6. | Юнит в закрытом контуре приватного облака для размещения оборудования заказчика | Шт. | 4 |

**ОБОСНОВАНИЕ НАЧАЛЬНОЙ (МАКСИМАЛЬНОЙ) ЦЕНЫ КОНТРАКТА**

В соответствии со статьей 22 Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» и Методическими рекомендациями по применению методов определения начальной (максимальной) цены контракта, цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем) начальная (максимальная) цена контракта определена Методом сопоставимых рыночных цен (анализа рынка):

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Наименование** | **Кол-во** | **Цена услуги (руб.)/источники информации о ценах** | | | **Минимальная цена за услугу (руб.)** | **Начальная (максимальная) цена контракта**  **(руб.)** |
| **Исполнитель 1**  **(письмо № 260722-4 от 26.07.2022)** | **Исполнитель 2**  **(письмо № 4719 от 27.07.2022)** | **Исполнитель 3**  **(письмо № 0701/05/4561/22 от 27.07.2022)** |
| **1.** | **Оказание услуг по предоставлению выделенной инфраструктуры в центре обработки данных, в том числе:** | **1** | **89 805 600,00** | **99 244 800,00** | **82 022 848,18** | **82 022 848,18** | **82 022 848,18** |
| 1.1. | Разработка и согласование документации по услуге (1 этап) | 1 | 384 000,00 | 504 000,00 | 360 000,00 | 360 000,00 | 360 000,00 |
| 1.2. | 1. Организация физических каналов связи между ЦОД Заказчика и ЦОД Исполнителя; 2. Организация криптографической защиты каналов связи между ЦОД Заказчика и ЦОД Исполнителя (2 этап) | 1 | 8 016 000,00 | 9 096 000,00 | 5 640 000,00 | 5 640 000,00 | 5 640 000,00 |
| 1.3. | Организация выделенной инфраструктуры в ЦОД Исполнителя (3 этап) | 1 | 4 680 000,00 | 5 880 000,00 | 5 180 400,00 | 5 180 400,00 | 5 180 400,00 |
| 1.4. | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя (4-8 этапы) | 1 | 76 725 600,00 | 83 764 800,00 | 70 842 448,18 | 70 842 448,18 | 70 842 448,18 |

Начальная (максимальная) цена контракта 82 022 848 рублей 18 копеек определена по минимальному значению вышеуказанных данных.



**Контракт**

**на оказание услуг для обеспечения нужд Новосибирской области**

г. Новосибирск «\_\_»\_\_\_\_\_\_\_20\_\_ г.

Министерство цифрового развития и связи Новосибирской области, именуемое в дальнейшем «Заказчик» для обеспечения нужд Новосибирской области, в лице министра Цукаря Сергея Сергеевича, действующего на основании Положения о министерстве, с одной стороны, и \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, именуем\_\_\_ в дальнейшем «Исполнитель», в лице \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, действующ\_\_\_ на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, с другой стороны, вместе именуемые «Стороны» и каждый в отдельности «Сторона», с соблюдением требований Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее   –  Закон о контрактной системе), при способе определения Исполнителя электронный конкурс (протокол \_\_\_\_\_\_\_ № \_\_\_\_\_\_от \_\_\_\_\_) заключили настоящий контракт (далее – Контракт) о нижеследующем:

**1. Предмет Контракта**

1.1. Предметом Контракта является оказание услуг по предоставлению выделенной инфраструктуры в центре обработки данных (далее – Услуги) по заданию Заказчика в соответствии с Описанием объекта закупки (приложение № 1 к Контракту) и на условиях, предусмотренных Контрактом.

Идентификационный код закупки: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

1.2. Оказание Услуг осуществляется Исполнителем в соответствии с законодательством Российской Федерации, требованиями иных нормативных правовых актов, регулирующих порядок предоставления такого вида Услуг, устанавливающих требования к качеству такого вида Услуг, в соответствии с условиями Контракта.

**2. Цена Контракта и порядок расчетов**

2.1. Цена Контракта составляет \_\_\_\_\_\_\_\_ (\_\_\_) рублей,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – \_\_\_\_\_% (\_\_\_ процентов), \_\_\_\_\_\_\_ (\_\_\_) рублей (далее – цена Контракта).

В случае, если Контракт заключается с юридическим лицом или физическим лицом, в том числе зарегистрированным в качестве индивидуального предпринимателя, то сумма, подлежащая уплате Заказчиком, уменьшается на размер налогов, сборов и иных обязательных платежей в бюджеты бюджетной системы Российской Федерации, связанных с оплатой Контракта, если в соответствии с законодательством Российской Федерации о налогах и сборах такие налоги, сборы и иные обязательные платежи подлежат уплате в бюджеты бюджетной системы Российской Федерации Заказчиком.

Источник финансирования: средства областного бюджета Новосибирской области в рамках государственной программы Новосибирской области «Цифровая трансформация Новосибирской области»; за счет лимитов бюджетных обязательств 2022 г. в размере 28,95439743% от цены Контракта, \_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_) рублей; за счет лимитов бюджетных обязательств 2023 г. в размере 71,04560256 % от цены Контракта, \_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_) рублей.

2.2. Цена Контракта является твердой и не может изменяться в ходе его исполнения, за исключением случаев, предусмотренных Законом о контрактной системе и Контрактом. Цена Контракта включает в себя расходы, связанные с оказанием Услуг, предусмотренных Контрактом, в полном объеме, страхование, уплату таможенных пошлин, налогов, сборов и других обязательных платежей.

2.3. Исполнитель проинформирован, что в соответствии с распоряжением Правительства Новосибирской области от 14.05.2013 № 205-рп «О мерах по повышению собираемости налогов и укреплению налоговой дисциплины», при наличии у Исполнителя недоимки по налоговым платежам в бюджеты бюджетной системы Российской Федерации, превышающей сумму 2 миллиона 250 тысяч рублей в течение 2 (двух) месяцев, информация может быть передана в Следственное управление Следственного комитета Российской Федерации по Новосибирской области.

2.4. Оплата оказанных по Контракту Услуг осуществляется Заказчиком на расчетный счет Исполнителя, указанный в Контракте, поэтапно. Оплата отдельного этапа исполнения Контракта производится Заказчиком в срок не более 7 (семи) рабочих дней с даты подписания Заказчиком документа о приёмке, предусмотренного п. 4.2. Контракта. Оплата производится Заказчиком на основании на основании документа о приёмке и при отсутствии у Заказчика претензий по объему и качеству оказанных Услуг, в соответствии со следующими этапами по Графику исполнения этапов по Контракту (приложение № 2):

**1 этап** в размере 0,438902096% от цены Контракта – 360 000 (триста шестьдесят тысяч) рублей 00 копеек,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – 20% (двадцать процентов), 60 000 (шестьдесят тысяч) рублей 00 копеек.

**2 этап** в размере 6,876132839% от цены Контракта – 5 640 000,00 (пять миллионов шестьсот сорок тысяч) рублей 00 копеек,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – 20% (двадцать процентов), 940 000 (девятьсот сорок тысяч) рублей 00 копеек.

**3 этап** в размере 6,31580116% от цены Контракта – 5 180 400 (пять миллионов сто восемьдесят тысяч четыреста) рублей 00 копеек,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – 20% (двадцать процентов), 863 400 (восемьсот шестьдесят три тысячи четыреста) рублей 00 копеек.

**4 этап** в размере 15,32356133% от цены Контракта – 12 568 821 (двенадцать миллионов пятьсот шестьдесят восемь тысяч восемьсот двадцать один) рубль 45 копеек,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – 20% (двадцать процентов), 2 094 803 (два миллиона девяносто четыре тысячи восемьсот три) рубля 57 копеек.

**5 этап** в размере 21,69179462% от цены Контракта – 17 792 227 (семнадцать миллионов семьсот девяносто две тысячи двести двадцать семь) рублей 77 копеек,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – 20% (двадцать процентов), 2 965 371 (два миллиона девятьсот шестьдесят пять тысяч триста семьдесят один) рубль 30 копеек.

**6 этап** в размере 18,507677978% от цены Контракта – 15 180 524 (пятнадцать миллионов сто восемьдесят тысяч пятьсот двадцать четыре) рубля 61 копейка,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – 20% (двадцать процентов), 2 530 087 (два миллиона пятьсот тридцать тысяч восемьдесят семь) рублей 43 копейки.

**7 этап** в размере 18,507677978% от цены Контракта – 15 180 524 (пятнадцать миллионов сто восемьдесят тысяч пятьсот двадцать четыре) рубля 61 копейка,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – 20% (двадцать процентов), 2 530 087 (два миллиона пятьсот тридцать тысяч восемьдесят семь) рублей 43 копейки.

**8 этап** в размере 12,33845198% от цены Контракта – 10 120 349 (десять миллионов сто двадцать тысяч триста сорок девять) рублей 74 копейки,

без НДС:

НДС не предусмотрен на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

с НДС:

в том числе НДС – 20% (двадцать процентов), 1 686 724 (один миллион шестьсот восемьдесят шесть тысяч семьсот двадцать четыре) рубля 96 копеек.

Цена каждого этапа устанавливается в размере, сниженном пропорционально снижению начальной (максимальной) цены контракта участником.

Обязательства Заказчика по оплате цены Контракта считаются исполненными с момента списания денежных средств в размере, установленном Контрактом, с лицевого счета Заказчика. За дальнейшее прохождение денежных средств Заказчик ответственности не несет.

**3. Порядок оказания Услуг**

3.1. Исполнитель оказывает Услуги в соответствии с Описанием объекта закупки.

3.2. Место оказания Услуг: г. Новосибирск, ул. Свердлова, д. 14.

3.3. Срок оказания Услуг Исполнителем по Контракту в полном объеме: с 05.09.2022 по 06.12.2023 (включительно).

3.4. Срок исполнения Контракта: с 05.09.2022 по 26.12.2022 (включительно).

3.5. Сроки исполнения этапов по Контракту отражены в Графике исполнения этапов по Контракту (приложение № 2 к Контракту).

**4. Порядок сдачи и приемки оказанных Услуг**

4.1. Приемка этапа исполнения Контракта на соответствие их объема и качества требованиям, установленным в Контракте, осуществляется поэтапно комиссией, сформированной на основании приказа Заказчика, и состоящей из представителей Заказчика, подведомственного заказчику ГБУ НСО «ЦИТ НСО» и Исполнителя, в соответствии с Графиком исполнения этапов по Контракту (приложение №2).

4.2. Исполнитель в течении 5 (пяти) рабочих дней после завершения оказания Услуг, предусмотренных Контрактом, в соответствии с Графиком оказания услуг, указанным в п. 6 Приложения №1 к Контракту, формирует с использованием единой информационной системы, подписывает усиленной электронной подписью лица, имеющего право действовать от имени Исполнителя, и размещает в единой информационной системе документ о приемке, который должен содержать:

4.2.1. Идентификационный код закупки, наименование, место нахождения заказчика, наименование объекта закупки, место оказания услуги, информацию об Исполнителе, предусмотренную подпунктами "а", "г" и "е" ч. 1 ст. 43 Закона о контрактной системе, единицу измерения оказанной услуги;

4.2.2. наименование оказанной услуги;

4.2.3. наименование страны происхождения поставленного товара (при осуществлении закупки товара, в том числе поставляемого заказчику при оказании закупаемых услуг);

4.2.4. информацию о количестве поставленного товара (при осуществлении закупки товара, в том числе поставляемого заказчику при оказании закупаемых услуг);

4.2.5. информацию об объеме оказанной услуги;

4.2.6. стоимость исполненных Исполнителем обязательств, предусмотренных Контрактом, с указанием цены за единицу (при осуществлении закупки товара, в том числе поставляемого заказчику при оказании закупаемых услуг) оказанной услуги;

4.2.7. иную информацию с учетом требований, установленных в соответствии с ч. 3 ст. 5 Закона о контрактной системе.

4.3. К документу о приемке, предусмотренному пунктом 4.2 настоящего Контракта, могут прилагаться документы, которые считаются его неотъемлемой частью. При этом в случае, если информация, содержащаяся в прилагаемых документах, не соответствует информации, содержащейся в документе о приемке, приоритет имеет предусмотренная пунктом 4.2 настоящего Контракта информация, содержащаяся в документе о приемке.

4.4. Документ о приемке, подписанный Исполнителем, не позднее 1 (одного) часа с момента его размещения в единой информационной системе автоматически с использованием единой информационной системы направляется Заказчику.

Датой поступления Заказчику документа о приемке, подписанного Исполнителем, считается дата размещения такого документа в единой информационной системе в соответствии с часовой зоной, в которой расположен Заказчик.

4.5. Не позднее 10 (десяти) рабочих дней, следующих за днем поступления Заказчику документа о приемке, члены приемочной комиссии подписывают усиленными электронными подписями поступивший документ о приемке или формируют с использованием единой информационной системы, подписывают усиленными электронными подписями мотивированный отказ от подписания документа о приемке с указанием причин такого отказа.

При этом, если приемочная комиссия включает членов, не являющихся работниками Заказчика, допускается осуществлять подписание документа о приемке, составление мотивированного отказа от подписания документа о приемке, подписание такого отказа без использования усиленных электронных подписей и единой информационной системы.

4.6. После подписания членами приемочной комиссии документа о приемке или мотивированного отказа от подписания документа о приемке Заказчик подписывает документ о приемке или мотивированный отказ от подписания документа о приемке усиленной электронной подписью лица, имеющего право действовать от имени Заказчика, и размещает их в единой информационной системе.

Если члены приемочной комиссии не использовали усиленные электронные подписи и единую информационную систему, заказчик прилагает подписанные ими документы в форме электронных образов бумажных документов.

4.7. Документ о приемке, мотивированный отказ от подписания документа о приемке не позднее одного часа с момента размещения в единой информационной системе направляются автоматически с использованием единой информационной системы Исполнителю.

Датой поступления Исполнителю документа о приемке, мотивированного отказа от подписания документа о приемке считается дата размещения в соответствии с настоящим пунктом таких документа о приемке, мотивированного отказа в единой информационной системе в соответствии с часовой зоной, в которой расположен Исполнитель.

4.8. В случае получения мотивированного отказа от подписания документа о приемке Исполнитель вправе устранить причины, указанные в таком мотивированном отказе, и направить Заказчику документ о приемке в порядке, предусмотренном пунктами 4.2-4.4 настоящего Контракта.

4.9. Датой приемки оказанной услуги считается дата размещения в единой информационной системе документа о приемке, подписанного Заказчиком.

4.10. Внесение исправлений в документ о приемке, оформленный в соответствии с положениями пунктов 4.2-4.4 настоящего Контракта, осуществляется путем формирования, подписания усиленными электронными подписями лиц, имеющих право действовать от имени Исполнителя, Заказчика, и размещения в единой информационной системе исправленного документа о приемке.

4.11. Для проверки представленных Исполнителем результатов на их соответствие условиям Контракта Заказчик проводит экспертизу. Экспертиза результатов может проводиться Заказчиком своими силами или к ее проведению могут привлекаться эксперты, экспертные организации.

**5. Права и обязанности Сторон**

5.1. Заказчик вправе:

5.1.1. Требовать от Исполнителя надлежащего исполнения обязательств в соответствии с Контрактом, а также требовать своевременного устранения выявленных недостатков.

5.1.2. В случае досрочного исполнения Исполнителем обязательств по Контракту принять и оплатить Услуги в соответствии с установленным в Контракте порядком.

5.1.3. Запрашивать у Исполнителя информацию о ходе оказываемых Услуг.

5.1.4. Осуществлять контроль и надзор за качеством, порядком и сроками оказания Услуг, давать указания о способе оказания Услуг, не вмешиваясь при этом в оперативно-хозяйственную деятельность Исполнителя.

5.1.5. Отказаться от приемки результата Услуг в случаях, предусмотренных Контрактом и законодательством Российской Федерации, в том числе в случае обнаружения неустранимых недостатков.

5.1.6. Отказаться в любое время до сдачи Услуг от исполнения Контракта и потребовать возмещения ущерба, если Исполнитель не приступает своевременно к исполнению Контракта или оказывает Услуги настолько медленно, что окончание их к сроку, указанному в Контракте, становится явно невозможным.

5.1.7. Принять решение об одностороннем отказе от исполнения Контракта в соответствии с Законом о контрактной системе.

5.1.8. По соглашению с Исполнителем изменить существенные условия Контракта в случаях, установленных Законом о контрактной системе.

5.1.9. Пользоваться иными правами, установленными Контрактом и законодательством Российской Федерации.

5.2. Заказчик обязан:

5.2.1. Провести экспертизу для проверки представленных Исполнителем результатов оказанных Услуг, предусмотренных Контрактом в соответствии с п. 4.11 Контракта.

5.2.2. Сообщать в письменной форме Исполнителю о недостатках, обнаруженных в ходе оказания Услуг, в течение 2 (двух) рабочих дней после обнаружения таких недостатков. Заказчик, обнаружив при осуществлении контроля и надзора за ходом оказания Услуг отступления от условий Контракта, которые могут ухудшить качество Услуг, или иные их недостатки, должен в течение 1 (одного) календарного дня заявить об этом Исполнителю. Заказчик обязан назначить своего ответственного представителя для контроля за оказанием Исполнителем Услуг по Контракту и согласования организационных вопросов.

5.2.3. Своевременно принять и оплатить надлежащим образом оказанные Услуги в соответствии с Контрактом, включая проведение экспертизы оказанных Услуг, а также отдельных этапов исполнения Контракта в соответствии с законодательством Российской Федерации.

5.2.4. При получении от Исполнителя уведомления о приостановлении оказания Услуг в случае, указанном в [подпункте 5.4.6](#Par760) Контракта, в течение 3 (трех) рабочих дней рассмотреть вопрос о целесообразности и порядке продолжения оказания Услуг.

5.2.5. Не позднее 5 (пяти) рабочих дней с момента возникновения права требования от Исполнителя оплаты неустойки (штрафа, пени) направить Исполнителю претензионное письмо с требованием оплаты в течение 5 (пяти) рабочих дней с даты получения претензионного письма неустойки (штрафа, пени), рассчитанной в соответствии с законодательством Российской Федерации и условиями Контракта.

5.2.6. При неоплате Исполнителем неустойки (штрафа, пени) в течение 10 (десяти) рабочих дней с даты истечения срока для оплаты неустойки (штрафа, пени), указанного в претензионном письме, а также в случае полного или частичного немотивированного отказа в удовлетворении претензии либо неполучения в срок ответа на претензию направить в суд исковое заявление с требованием оплаты неустойки (штрафа, пени), рассчитанной в соответствии с законодательством Российской Федерации и условиями Контракта.

5.2.7. В течение 40 (сорока) рабочих дней с даты фактического исполнения обязательств Исполнителем принять необходимые меры по взысканию неустойки (штрафа, пени) за весь период просрочки исполнения обязательств, предусмотренных Контрактом, а именно потребовать оплаты неустойки (штрафа, пени), рассчитанной в соответствии с законодательством Российской Федерации и условиями Контракта за весь период просрочки исполнения, и в случае неоплаты Исполнителем неустойки (штрафа, пени) в течение указанного срока направить в суд исковое заявление с соответствующими требованиями.

5.2.8. При направлении в суд искового заявления с требованиями о расторжении Контракта одновременно заявлять требования об оплате неустойки (штрафа, пени), рассчитанной в соответствии с законодательством Российской Федерации и условиями Контракта.

5.2.9. В случае обеспечения исполнения Контракта в форме независимой гарантии, при неисполнении Исполнителем своих обязательств, Заказчик обязан обратиться к гаранту с требованием исполнить обязанности в соответствии с выданной гарантией.

5.2.10. Обеспечить конфиденциальность информации, представленной Исполнителем в ходе исполнения обязательств по Контракту, за исключением случаев, когда Заказчик в соответствии с законодательством Российской Федерации обязан предоставлять информацию третьим лицам.

5.2.11. Исполнять иные обязанности, предусмотренные законодательством Российской Федерации и условиями Контракта.

5.3. Исполнитель вправе:

5.3.1. Требовать своевременного подписания Заказчиком документа о приемке Услуг по Контракту на основании представленных Исполнителем документов, указанных в [п. 4.](#Par718)2 Контракта, и при условии истечения срока, указанного в [п. 4.5](#Par718) Контракта.

5.3.2. Требовать своевременной оплаты оказанных Услуг в соответствии с [условиями](#Par704) Контракта.

5.3.3. Требовать уплаты неустоек (штрафов, пеней) в случае просрочки исполнения Заказчиком обязательств, предусмотренных Контрактом, а также в иных случаях ненадлежащего исполнения Заказчиком обязательств, предусмотренных Контрактом.

5.3.4. Запрашивать у Заказчика разъяснения и уточнения относительно оказания Услуг в рамках Контракта.

5.3.5. Получать от Заказчика содействие при оказании Услуг в соответствии с условиями Контракта (с согласия Заказчика).

5.3.6. Досрочно исполнить обязательства по Контракту с согласия Заказчика.

5.3.7. Привлекать к исполнению своих обязательств по Контракту других лиц – соисполнителей, обладающих специальными знаниями, навыками, квалификацией, специальным оборудованием и т.п., по видам (содержанию) Услуг. При этом Исполнитель несет ответственность перед Заказчиком за неисполнение или ненадлежащее исполнение обязательств соисполнителей.

5.3.8. Принять решение об одностороннем отказе от исполнения Контракта в соответствии с законодательством Российской Федерации.

5.3.9. Пользоваться иными правами, установленными Контрактом и законодательством Российской Федерации.

5.4. Исполнитель обязан:

5.4.1. Своевременно и надлежащим образом исполнять обязательства в соответствии с условиями Контракта и сформировать документ о приемке в порядке, предусмотренном п. 4.2 Контракта, по итогам исполнения Контракта.

5.4.2. Своевременно представить по запросу Заказчика в сроки, указанные в таком запросе, информацию о ходе исполнения обязательств, в том числе о сложностях, возникающих при исполнении Контракта.

5.4.3. Обеспечивать соответствие результатов Услуг требованиям качества, безопасности жизни и здоровья, а также иным требованиям сертификации, безопасности (санитарным нормам и правилам, государственным стандартам и т.п.), лицензирования, установленным законодательством Российской Федерации.

Исполнитель обязан в течение срока действия Контракта представить по запросу Заказчика в течение 1 (одного) рабочего дня после дня получения указанного запроса документы, подтверждающие соответствие Услуг указанным выше требованиям.

5.4.4. Обеспечить устранение недостатков, выявленных при приемке Заказчиком Услуг и в течение гарантийного срока, за свой счет.

5.4.5. Предоставить обеспечение исполнения Контракта, обеспечение гарантийных обязательств в случаях, установленных Законом о контрактной системе и Контрактом.

5.4.6. Приостановить оказание Услуг в случае обнаружения не зависящих от Исполнителя обстоятельств, которые могут оказать негативное влияние на качество результатов оказываемых Услуг или создать невозможность их завершения в установленный Контрактом срок, и сообщить об этом Заказчику в течение 1 (одного) рабочего дня после приостановления оказания Услуг.

5.4.7. В течение 1 (одного) рабочего дня информировать Заказчика о невозможности оказать Услуги в надлежащем объеме, в предусмотренные Контрактом сроки, надлежащего качества.

5.4.8. В случае если законодательством Российской Федерации предусмотрены обязательные требования к лицам, осуществляющим определенные виды деятельности, входящие в состав услуг, оказываемых по Контракту (лицензирование, членство в саморегулируемых организациях, аккредитация и прочее), Исполнитель обязан обеспечить наличие документов, подтверждающих его соответствие, либо привлекаемых им соисполнителей, требованиям, установленным законодательством Российской Федерации, в течение всего срока исполнения Контракта. Указанные документы представляются Исполнителем по требованию Заказчика в течение 5 (пяти) рабочих дней со дня получения соответствующего требования.

5.4.9. Представить Заказчику сведения об изменении своего фактического местонахождения в срок не позднее 5 (пяти) рабочих дней со дня соответствующего изменения. В случае непредставления уведомления об изменении адреса фактическим местонахождением Исполнителя будет считаться адрес, указанный в Контракте.

5.4.10. Обеспечить конфиденциальность информации, предоставленной Заказчиком в ходе исполнения обязательств по Контракту, за исключением случаев, когда Исполнитель в соответствии с законодательством Российской Федерации обязан предоставлять информацию третьим лицам.

5.4.11. Исполнять иные обязанности, предусмотренные законодательством Российской Федерации и Контрактом.

**6. Гарантии**

6.1. Исполнитель гарантирует, что оказываемые Услуги соответствуют требованиям, установленным в Контракте, обязательным нормам и правилам, регулирующим данную деятельность (ГОСТ, ТУ), а также иным требованиям законодательства Российской Федерации, действующим на момент оказания Услуг.

6.2. Гарантийный срок на оказываемые по Контракту Услуги не установлен.

**7. Ответственность Сторон**

7.1. За неисполнение или ненадлежащее исполнение своих обязательств, установленных Контрактом, Стороны несут ответственность в соответствии с законодательством Российской Федерации и Контрактом.

Размеры неустоек (штрафов, пеней), указанные в настоящем разделе, определяются в   соответствии с Правилами определения размера штрафа, начисляемого в случае ненадлежащего исполнения заказчиком, неисполнения или ненадлежащего исполнения поставщиком (подрядчиком, исполнителем) обязательств, предусмотренных контрактом (за исключением просрочки исполнения обязательств заказчиком, поставщиком (подрядчиком, исполнителем), утвержденными постановлением Правительства Российской Федерации от 30.08.2017 № 1042 (далее – Правила), а также в соответствии с положениями статьи 34 Закона о контрактной системе.

7.2. В случае просрочки исполнения Заказчиком обязательств, предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Заказчиком обязательств, предусмотренных Контрактом, Исполнитель вправе потребовать уплаты неустоек (штрафов, пеней).

Пеня в размере 1/300 (одной трехсотой) действующей на дату уплаты пеней ключевой ставки Центрального банка Российской Федерации от не уплаченной в срок суммы начисляется за каждый день просрочки исполнения обязательства, предусмотренного Контрактом, начиная со дня, следующего после дня истечения установленного Контрактом срока исполнения обязательства.

7.3. За каждый факт неисполнения Заказчиком обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств, предусмотренных Контрактом, размер штрафа устанавливается в следующем порядке:

1000 рублей, если цена Контракта не превышает 3 млн. рублей (включительно);

5000 рублей, если цена Контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

10000 рублей, если цена Контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно).

7.4. В случае просрочки исполнения Исполнителем обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, а также в иных случаях неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, Заказчик направляет Исполнителю требование об уплате неустоек (штрафов, пеней).

Пеня начисляется за каждый день просрочки исполнения Исполнителем обязательства, предусмотренного Контрактом, начиная со дня, следующего после дня истечения установленного Контрактом срока исполнения обязательства, и устанавливается в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены отдельного этапа исполнения Контракта, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных соответствующим отдельным этапом исполнения Контракта и фактически исполненных Исполнителем обязательств, за исключением случаев, если законодательством Российской Федерации установлен иной порядок начисления пени.

7.5. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, размер штрафа устанавливается в следующем порядке:

10 процентов цены Контракта (этапа) в случае, если цена Контракта (этапа) не превышает 3 млн. рублей;

5 процентов цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 3 млн. рублей до 50 млн. рублей (включительно);

1 процент цены Контракта (этапа) в случае, если цена Контракта (этапа) составляет от 50 млн. рублей до 100 млн. рублей (включительно).

7.6. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательства, предусмотренного Контрактом, которое не имеет стоимостного выражения, размер штрафа устанавливается (при наличии в Контракте таких обязательств) в следующем порядке:

1000 рублей, если цена Контракта не превышает 3 млн. рублей;

5000 рублей, если цена Контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

10000 рублей, если цена Контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно).

7.7. За каждый факт неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, заключенным с победителем закупки (или с иным участником закупки в случаях, установленных Законом о контрактной системе), предложившим наиболее высокую цену за право заключения Контракта, размер штрафа рассчитывается в порядке, установленном Правилами, за исключением просрочки исполнения обязательств (в том числе гарантийного обязательства), предусмотренных Контрактом, и устанавливается в следующем порядке:

а) в случае, если цена Контракта не превышает начальную (максимальную) цену Контракта:

10 процентов начальной (максимальной) цены Контракта, если цена Контракта не превышает 3 млн. рублей;

5 процентов начальной (максимальной) цены Контракта, если цена Контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

1 процент начальной (максимальной) цены Контракта, если цена контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно);

б) в случае, если цена Контракта превышает начальную (максимальную) цену Контракта:

10 процентов цены Контракта, если цена контракта не превышает 3 млн. рублей;

5 процентов цены Контракта, если цена контракта составляет от 3 млн. рублей до 50 млн. рублей (включительно);

1 процент цены Контракта, если цена Контракта составляет от 50 млн. рублей до 100 млн. рублей (включительно).

7.8. Общая сумма начисленных штрафов за неисполнение или ненадлежащее исполнение Исполнителем обязательств, предусмотренных Контрактом, не может превышать цену Контракта.

Общая сумма начисленных штрафов за ненадлежащее исполнение Заказчиком обязательств, предусмотренных Контрактом, не может превышать цену Контракта.

7.9. В случае неисполнения или ненадлежащего исполнения Исполнителем обязательств, предусмотренных Контрактом, Заказчик вправе произвести оплату по Контракту за вычетом соответствующего размера неустойки (штрафа, пени) (при этом исполнение обязательства Исполнителя по перечислению неустойки (штрафа, пени) и (или) убытков в доход бюджета возлагается на Заказчика) либо осуществить удержание суммы неустойки (штрафа, пени) из обеспечения исполнения Контракта, предоставленного Исполнителем в соответствии с разделом 8 настоящего Контракта.

7.10. Уплата Стороной неустойки (штрафа, пени) не освобождает ее от исполнения обязательств по Контракту.

7.11. Сторона освобождается от уплаты неустойки (штрафа, пени), если докажет, что неисполнение или ненадлежащее исполнение обязательства, предусмотренного Контрактом, произошло по вине другой Стороны или вследствие непреодолимой силы, а именно чрезвычайных и непредотвратимых при данных условиях обстоятельств: стихийных природных явлений (землетрясений, наводнений, пожаров и т.д.), действий объективных внешних факторов (военных действий, актов органов государственной власти и управления и т.п.), подтвержденных в установленном законодательством порядке, препятствующих надлежащему исполнению обязательств по Контракту, которые возникли после заключения Контракта, на время действия этих обстоятельств, если эти обстоятельства непосредственно повлияли на исполнение Стороной своих обязательств, а также которые Сторона была не в состоянии предвидеть и предотвратить.

**8. Обеспечение исполнения Контракта**

8.1. Обеспечение исполнения Контракта предусмотрено для обеспечения исполнения Исполнителем его обязательств по Контракту, в том числе таких обязательств, как оказание Услуг надлежащего качества, соблюдения сроков оказания Услуг, оплата неустойки (штрафа, пени) за неисполнение или ненадлежащее исполнение условий Контракта, возмещение ущерба.

Обеспечение исполнения Контракта не применяется, если участник закупки, с которым заключается Контракт, является казенным учреждением.

Исполнение Контракта обеспечивается предоставлением независимой гарантии, выданной организациями, указанными в ч. 1 ст. 45 Закона о контрактной системе или внесением денежных средств на указанный Заказчиком счет, на котором в соответствии с законодательством Российской Федерации учитываются операции со средствами, поступающими Заказчику.

Способ обеспечения исполнения Контракта определяется Исполнителем самостоятельно.

8.2. Размер обеспечения исполнения Контракта составляет 30% (тридцать процентов) начальной (максимальной) цены Контракта, что составляет 24 606 854 (двадцать четыре миллиона шестьсот шесть тысяч восемьсот пятьдесят четыре) рубля 45 копеек.

При снижении цены в предложенной Исполнителем заявке на двадцать пять процентов и более по отношению к начальной (максимальной) цене Контракта Исполнитель, с которым заключается Контракт, предоставляет обеспечение исполнения Контракта с учетом положений ст. 37 Закона о контрактной системе.

8.3. В ходе исполнения Контракта Исполнитель вправе изменить способ обеспечения исполнения Контракта и (или) предоставить Заказчику взамен ранее предоставленного обеспечения исполнения Контракта новое обеспечение исполнения Контракта, размер которого может быть уменьшен в порядке и случаях, которые предусмотрены частями 7.2 и 7.3 статьи 96 Закона о контрактной системе.

8.4. Срок действия независимой гарантии определяется Исполнителем самостоятельно в соответствии с требованиями Закона о контрактной системе, при этом данный срок должен превышать срок исполнения обеспечиваемых обязательств не менее чем на один месяц, в том числе в случае его изменения в соответствии со статьей 95 Закона о контрактной системе.

8.5. В случае если по каким-либо причинам обеспечение исполнения Контракта перестало быть действительным, закончило свое действие или иным образом перестало обеспечивать исполнение Исполнителем его обязательств по Контракту, Исполнитель обязуется в течение 10 (десяти) рабочих дней с момента, когда такое обеспечение перестало действовать, предоставить Заказчику новое надлежащее обеспечение исполнения Контракта на тех же условиях и в таком же размере.

Действие указанного пункта не распространяется на случаи, если Исполнителем представлена недостоверная (поддельная) независимая гарантия.

В случае отзыва в соответствии с законодательством Российской Федерации у банка, предоставившего независимую гарантию в качестве обеспечения исполнения Контракта, лицензии на осуществление банковских операций Исполнитель обязуется предоставить новое обеспечение исполнения Контракта не позднее одного месяца со дня надлежащего уведомления Заказчиком Исполнителя о необходимости предоставить соответствующее обеспечение. Размер такого обеспечения может быть уменьшен в порядке и случаях, которые предусмотрены частями 7, 7.1, 7.2 и 7.3 статьи 96 Закона о контрактной системе. За каждый день просрочки исполнения Исполнителем обязательства, предусмотренного настоящим абзацем, начисляется пеня в размере одной трехсотой действующей на дату уплаты пени ключевой ставки Центрального банка Российской Федерации от цены Контракта, уменьшенной на сумму, пропорциональную объему обязательств, предусмотренных Контрактом и фактически исполненных Исполнителем.

8.6. Прекращение обеспечения исполнения Контракта или не соответствующее требованиям Закона о контрактной системе обеспечение исполнения Контракта по истечении срока, указанного в п. 8.5 Контракта, признается существенным нарушением Контракта Исполнителем и является основанием для расторжения Контракта по требованию Заказчика с возмещением ущерба в полном объеме.

8.7. В случае надлежащего исполнения Исполнителем обязательств по Контракту обеспечение исполнения Контракта подлежит возврату Исполнителю. Заказчик осуществляет возврат денежных средств на расчетный счет Исполнителя, указанный в Контракте, после оказания всего объема Услуг в течение 30 (тридцати) календарных дней с даты подписания Сторонами документа о приёмке, предусмотренного п. 4.2. Контракта, при отсутствии у Заказчика претензий по объему и качеству оказанных Услуг.

В случае уменьшения размера обеспечения исполнения Контракта в порядке и случаях, установленных Законом о контрактной системе, часть денежных средств, внесенная Исполнителем в качестве обеспечения исполнения контракта, по заявлению Исполнителя подлежит возврату Исполнителю в течение 30 (тридцати) дней с даты получения Заказчиком указанного заявления, при отсутствии у Заказчика претензий по объему и качеству оказанных Услуг.

8.8. Обеспечение исполнения Контракта сохраняет свою силу при изменении законодательства Российской Федерации, а также при реорганизации Исполнителя или Заказчика.

8.9. Независимая гарантия должна быть безотзывной и должна содержать сведения, указанные в Законе о контрактной системе.

Независимая гарантия, предоставленная в качестве обеспечения гарантийных обязательств, должна содержать условие об обязанности гаранта уплатить Заказчику денежную сумму по независимой гарантии не позднее 10 (десяти) рабочих дней со дня, следующего за днем получения гарантом требования Заказчика, соответствующего условиям такой независимой гарантии, при отсутствии предусмотренных Гражданским кодексом Российской Федерации оснований для отказа в удовлетворении этого требования.

8.10. Все затраты, связанные с заключением и оформлением договоров и иных документов по обеспечению исполнения Контракта, несет Исполнитель.

8.11. Исполнитель освобождается от предоставления обеспечения гарантийных обязательств в случаях, предусмотренных частью 8 статьи 96 Закона о контрактной системе.

**9. Срок исполнения, порядок изменения и расторжения Контракта**

9.1. Контракт вступает в силу со дня его подписания Сторонами, всоответствии с положениями статьи 51 Закона о контрактной системе*.*

9.2. Срок исполнения Контракта действует по 26.12.2022 (включительно). Окончание срока исполнения Контракта не освобождает Стороны от выполнения обязательств, предусмотренных Контрактом, а также от ответственности за нарушение условий Контракта.

9.3. Контракт может быть расторгнут:

по соглашению Сторон;

по решению суда;

в случае одностороннего отказа Стороны Контракта от исполнения Контракта в соответствии с гражданским законодательством.

9.4. Заказчик вправе обратиться в суд в установленном законодательством Российской Федерации порядке с требованием о расторжении Контракта в следующих случаях:

9.4.1. При существенном нарушении Контракта Исполнителем.

9.4.2. В случае просрочки исполнения обязательств по оказанию Услуг более чем на 5 (пять) календарных дней.

9.4.3. В случае неоднократного нарушения сроков оказания Услуг – более двух раз более чем на 5 (пять) календарных дней.

9.4.4. В случае существенного нарушения требований к качеству оказываемых Услуг (обнаружения неустранимых недостатков, недостатков, которые не могут быть устранены без несоразмерных расходов или затрат времени, или выявляются неоднократно, либо проявляются вновь после их устранения, и других подобных недостатков).

9.4.5. Установления факта предоставления недостоверной (поддельной) независимой гарантии или содержащихся в ней сведений, а также представление независимой гарантии, не соответствующей требованиям Закона о контрактной системе.

9.4.6. В иных случаях, предусмотренных законодательством Российской Федерации.

9.5. Заказчик обязан принять решение об одностороннем отказе от исполнения Контракта в случаях:

9.5.1. В ходе исполнения Контракта установлено, что Исполнитель перестал соответствовать установленным извещением об осуществлении закупки и (или) документацией о закупке требованиям к участникам закупки.

9.5.2. В ходе исполнения Контракта установлено, что при определении поставщика (подрядчика, исполнителя) Исполнитель представил недостоверную информацию о своем соответствии требованиям, указанным в пункте 9.5.1. настоящего Контракта, что позволило ему стать победителем определения поставщика (подрядчика, исполнителя).

9.5.3. В иных случаях, установленных частью 15 статьи 95 Закона о контрактной системе.

9.6. Заказчик вправе принять решение об одностороннем отказе от исполнения Контракта по основаниям, предусмотренным Гражданским кодексом Российской Федерации для одностороннего отказа от исполнения договора возмездного оказания услуг, договора подряда в случаях, установленных в статье 783 ГК РФ, в том числе в следующих случаях:

9.6.1. В любое время без указания причин при условии оплаты Исполнителю фактически понесенных им расходов (пункт 1 статьи 782 ГК РФ).

9.6.2. Если Исполнитель не приступает своевременно к исполнению Контракта или оказывает Услуги настолько медленно, что окончание их к сроку становится явно невозможным (пункт 2 статьи 715 ГК РФ).

9.6.3. Если во время оказания Услуг станет очевидным, что они не будут оказаны надлежащим образом, Заказчик вправе назначить Исполнителю разумный срок для устранения недостатков и при неисполнении Исполнителем в назначенный срок этого требования отказаться от исполнения Контракта (пункт 3 статьи 715 ГК РФ).

9.6.4. Если отступления от условий Контракта или иные недостатки результата Услуг в установленный Заказчиком разумный срок не были устранены Исполнителем либо являются существенными и неустранимыми (пункт 3 статьи 723 ГК РФ).

9.6.5. Если при нарушении Исполнителем конечного срока оказания Услуг, указанного в Контракте, исполнение Исполнителем Контракта утратило для Заказчика интерес (пункт 3 статьи 708 ГК РФ, пункт 2 статьи 405 ГК РФ).

9.7. Заказчик до принятия решения об одностороннем отказе от исполнения Контракта вправе провести экспертизу оказанных Услуг с привлечением экспертов, экспертных организаций.

Если Заказчиком проведена экспертиза оказанной Услуги с привлечением экспертов, экспертных организаций, решение об одностороннем отказе от исполнения Контракта может быть принято Заказчиком только при условии, что по результатам экспертизы оказанной Услуги в заключении эксперта, экспертной организации будут подтверждены нарушения условий Контракта, послужившие основанием для одностороннего отказа Заказчика от исполнения Контракта.

9.8. В случае принятия Заказчиком решения об одностороннем отказе от исполнения Контракта, заключенного по результатам проведения электронных процедур, закрытых электронных процедур, Заказчик руководствуется положениями ст. 95 Закона о контрактной системе.

9.9. Решение Заказчика об одностороннем отказе от исполнения Контракта вступает в силу и Контракт считается расторгнутым через 10 (десять) календарных дней с даты надлежащего уведомления Заказчиком Исполнителя об одностороннем отказе от исполнения Контракта.

9.10. Заказчик обязан отменить не вступившее в силу решение об одностороннем отказе от исполнения Контракта, если в течение 10 (десяти) календарных дней с даты надлежащего уведомления Исполнителя о принятом решении об одностороннем отказе от исполнения Контракта устранено нарушение условий Контракта, послужившее основанием для принятия указанного решения, а также Заказчику компенсированы затраты на проведение экспертизы в соответствии с [п. 9.7](consultantplus://offline/ref=0643D14249E6A088D2F8A516E7617D17BC269B70614D58B1FE70E6614402B47E0ECAC33A295426FCB4a3F) Контракта. Данное правило не применяется в случае повторного нарушения Исполнителем условий Контракта, которые в соответствии с законодательством Российской Федерации являются основанием для одностороннего отказа Заказчика от исполнения Контракта.

9.11.В случае отмены Заказчиком не вступившего в силу решения об одностороннем отказе от исполнения контракта, размещенного в единой информационной системе в соответствии с п.9.8 Контракта, заказчик не позднее одного дня, следующего за днем такой отмены, формирует с использованием единой информационной системы извещение об отмене решения об одностороннем отказе от исполнения контракта, подписывает его усиленной электронной подписью лица, имеющего право действовать от имени заказчика, и размещает такое извещение в единой информационной системе.

9.12. Исполнитель вправе принять решение об одностороннем отказе от исполнения Контракта в соответствии с законодательством Российской Федерации.

**10. Порядок урегулирования споров**

10.1. Все споры и разногласия, возникшие в связи с исполнением Контракта, его изменением, расторжением или признанием недействительным, Стороны будут стремиться решить путем переговоров.

10.2. В случае недостижения взаимного согласия все споры по Контракту разрешаются в Арбитражном суде Новосибирской области.

10.3. До передачи спора на разрешение Арбитражного суда Новосибирской области Стороны примут меры к его урегулированию в претензионном порядке. Претензия должна быть направлена в письменном виде. По полученной претензии Сторона обязана дать письменный ответ по существу в срок не позднее 3 (трех) рабочих дней с даты ее получения.

**11. Прочие условия**

11.1. Все уведомления Сторон, связанные с исполнением Контракта, направляются в письменной форме по почте заказным письмом с уведомлением о вручении по адресу Стороны, указанному в Контракте, или с использованием факсимильной связи, электронной почты с   последующим представлением оригинала. В случае направления уведомлений с  использованием почты датой получения уведомления признается дата получения отправляющей Стороной подтверждения о вручении второй Стороне указанного уведомления либо дата получения Стороной информации об отсутствии адресата по его адресу, указанному в Контракте. При невозможности получения указанных подтверждения либо информации датой такого надлежащего уведомления признается дата по истечении 14 (четырнадцати) календарных дней с даты направления уведомления по почте заказным письмом с уведомлением о вручении. В случае отправления уведомлений посредством факсимильной связи и электронной почты уведомления считаются полученными Стороной в день их отправки.

11.2.  Контракт заключен в электронной форме в порядке, предусмотренном статьей 51 Закона о контрактной системе.

11.3. В случае перемены Заказчика по Контракту права и обязанности Заказчика по Контракту переходят к новому заказчику в том же объеме и на тех же условиях.

11.4. При исполнении Контракта не допускается перемена Исполнителя, за исключением случаев, если новый исполнитель является правопреемником Исполнителя по Контракту вследствие реорганизации юридического лица в форме преобразования, слияния или присоединения.

11.5. Во всем, что не предусмотрено Контрактом, Стороны руководствуются законодательством Российской Федерации.

11.6. Ответственное должностное лицо Заказчика: Кудашев Дмитрий Александрович, тел.: (383) 296-99-31, e-mail: kud@nso.ru.

**12. Приложения**

12.1. Неотъемлемыми частями Контракта являются следующие приложения к Контракту:

приложение № 1 «Описание объекта закупки»;

приложение № 2 «График исполнения этапов по Контракту».

**13. Адреса, реквизиты и подписи Сторон**

|  |  |  |
| --- | --- | --- |
| Заказчик  Министерство цифрового развития и связи Новосибирской области,  Место нахождения: 630007, г. Новосибирск, ул. Красный проспект, 18  Почтовый адрес: 630007, г. Новосибирск, ул. Красный проспект, 18ИНН/КПП 5406643611/540601001  МФ и НП НСО (МИНЦИФРА НСО, л/сч 380010011)  Единый казначейский счет 40102810445370000043  Казначейский счет 03221643500000005100  СИБИРСКОЕ ГУ БАНКА РОССИИ//УФК по Новосибирской области г. Новосибирск  БИК 015004950  Эл. почта: [digit@nso.ru](mailto:digit@nso.ru) |  | Исполнитель |
|  |  |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ С.С. Цукарь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

МП (при наличии) МП (при наличии)

Приложение № 1 к Контракту

от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. №\_\_\_\_

**ОПИСАНИЕ ОБЪЕКТА ЗАКУПКИ**

на оказание услуг по предоставлению выделенной инфраструктуры в центре обработки данных

1. **Основание для оказания услуг**: средства областного бюджета Новосибирской области в рамках реализации государственной программы «Цифровая трансформация Новосибирской области».
2. **Срок оказания услуг**: с 05.09.2022 по 30.11.2023 (включительно), в соответствии с графиком оказания услуг.
3. **Место оказания услуг**: г. Новосибирск, ул. Свердлова, д.14.
4. **Цель и основные задачи оказываемых услуг:** предоставление выделенной инфраструктуры в центре обработки данных Исполнителя, соответствующего требованиям Заказчика, изложенным в настоящем ООЗ.
5. **Термины и определения**

Таблица 1

|  |  |  |
| --- | --- | --- |
| 1 | ЦОД Заказчика | Центр обработки данных Правительства Новосибирской области, расположенный по адресу: г. Новосибирск, ул. Свердлова, д.14 |
| 2 | ЦОД Исполнителя | Центр обработки данных Исполнителя, соответствующий требованиям Заказчика |
| 3 | ГИС | Государственные информационные системы |
| 4 | ДГУ | Дизель-генераторная установка |
| 5 | ИБП | Источник бесперебойного питания |
| 6 | ГРЩ | Главный распределительный щит |
| 7 | РТП | Распределительная трансформаторная подстанция |
| 8 | СКУД | Система контроля и управления доступом |
| 9 | ВМ | Виртуальная машина |
| 10 | СХД | Система хранения данных |
| 11 | МЭ | Межсетевой экран |
| 12 | НСД | Несанкционированный доступ |
| 13 | ООЗ | Описание объекта закупки |
| 14 | ОС Windows | Windows 7/8/10, Windows Server 2012/2012 R2 |
| 15 | ОС Linux | Astra Linux Special Edition "Смоленск" 1.5/1.6,  Альт Линукс СПТ 8, Ubuntu 14.04 LTS Desktop/Server x64, VMware vSphere ESXi 6/6.5, CentOS 7.3/7.5, Лотос. |
| 16 | СУБД | Oracle, MS SQL, MySQL, PostgreSQL |

1. **График оказания услуг:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Этап** | **Описание** | **Результат** | **Длительность этапа** |
| **1** | Разработка и согласование документации по услуге | Разработаны и подписаны со стороны Заказчика и Исполнителя следующие документы:  1. Схема организации каналов связи от Заказчика до Исполнителя;  2. Структурная схема организации выделенной инфраструктуры, средств информационной безопасности и каналов передачи данных;  3. Перечень программного обеспечения (с указанием версий), оборудования и средств защиты информации (с указанием идентификационных (серийных) номеров и идентификаторов (маркирование средств защиты информации);  4. Форма программы и методики испытаний оказанных услуг по результатам исполнения контракта | С 05.09.2022 по 09.09.2022 (включительно) |
| **2** | 1. Организация физических каналов связи между ЦОД Заказчика и ЦОД Исполнителя;  2. Организация криптографической защиты каналов связи между ЦОД Заказчика и ЦОД Исполнителя | 1. Выполнена организация каналов связи между ЦОД Заказчика и ЦОД Исполнителя в соответствии с п. 8.2. данного ООЗ;  2. Выполнена организация криптографической защиты каналов связи между ЦОД Заказчика и ЦОД Исполнителя в соответствии с п.8.4.2. данного ООЗ | С 10.09.2022 по 23.09.2022 (включительно) |
| **3** | Организация выделенной инфраструктуры в ЦОД Исполнителя | Выполнена организация выделенной инфраструктура в ЦОД Исполнителя в соответствии с требованиями данного ООЗ в объёме согласно п.8.8. данного ООЗ | С 10.09.2022 по 30.09.2022 (включительно) |
| **4** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 01.10.2022 по 15.12.2022 (включительно) |
| **5** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 16.12.2022 по 31.03.2023 (включительно) |
| **6** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 01.04.2023 по 30.06.2023 (включительно) |
| **7** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 01.07.2023 по 30.09.2023 (включительно) |
| **8** | Предоставление выделенной инфраструктуры и каналов связи в ЦОД Исполнителя | Заказчику предоставлена выделенная инфраструктура в ЦОД Исполнителя и каналы связи в соответствии с требованиями данного ООЗ и в объёме согласно п.8.8. данного ООЗ | С 01.10.2023 по 30.11.2023 (включительно) |

1. **Требования к услуге**:

В рамках оказания Услуги по предоставлению выделенной инфраструктуры в центре обработки данных с необходимым Заказчику уровнем качества Исполнитель должен обеспечить предоставление Заказчику комплексной услуги, состоящей из каналов связи, средств информационной безопасности, виртуальных и физических вычислительных ресурсов, а так же системы резервного копирования на базе имеющейся в его распоряжении (пользовании на правах собственности) инфраструктуры, отвечающих требованиям, представленным в настоящем описании объекта закупки.

Заказчику должна быть предоставлена выделенная инсталляция инфраструктуры, состоящая из вычислительных серверов, систем хранения данных, сетевого оборудования и средств информационной безопасности, в рамках которой Заказчик должен иметь возможность создания и использования виртуальных машин в требуемой конфигурации для размещения информационных систем и сервисов.

Заказчик должен иметь возможность в выделенной инфраструктуре центра обработки данных Исполнителя устанавливать любые операционные системы (из списка поддерживаемых), а внутри виртуальных машин любое совместимое программное обеспечение.

Уровень доступа Заказчика к выделенной инфраструктуре должен определяться матрицей ответственности, зафиксированной в SLA.

Услуга должна активироваться по факту выполнения инсталляционных и пусконаладочных работ, осуществляемых после подписания контракта.

Оказание услуг должно осуществляться Исполнителем собственными силами и за собственный счет на оборудовании Исполнителя, в том числе инсталляция необходимых лицензий для функционирования выделенной инфраструктуры в ЦОД Исполнителя.

Инфраструктура, предоставляемая Заказчику в ЦОДе Исполнителя, должна обеспечивать:

* Высокую доступность и бесперебойную работу приложений Заказчика;
* Надежное хранение данных Заказчика;
* Высокую доступность и отказоустойчивость всех критических бизнес-компонентов системы;
* Возможность гибкого изменения необходимого объема ресурсов для каждой виртуальной машины, как в сторону увеличения, так и в сторону уменьшения;
* Возможность удаленного подключения к инфраструктуре администраторов и сотрудников Заказчика для управления приложением и внесением корректировок с использованием VPN-подключения на основе алгоритмов шифрования ГОСТ;
* Защищенное высокоскоростное сетевое соединение с ЦОД Заказчика;
* Другие требования, указанные в настоящем описании объекта закупки.

Исполнитель в рамках оказания технической поддержки выделенной инфраструктуры и каналов связи, предоставляемых в рамках оказания услуги, должен направить Заказчику контактные данные специалистов технической поддержки (электронная почта, телефон) с градацией по уровням эскалации.

|  |  |  |  |
| --- | --- | --- | --- |
| Уровень эскалации | Контакты | Время работы | ФИО и должность |
| Уровень 1 |  |  |  |
| Уровень 2 |  |  |  |
| Уровень 3 |  |  |  |

1. **Требования к ЦОД Исполнителя**

ЦОД Исполнителя должен находиться на территории Российской Федерации с протяженностью оптических линий связи не более 20 км от ЦОДа Заказчика, расположенного по адресу г. Новосибирск ул. Свердлова 14.

Объекты недвижимого имущества, составляющие ЦОД Исполнителя, должны быть в собственности Исполнителя.

Все элементы ЦОДа Исполнителя должны быть выполнены по уровню надежности не ниже, чем N+1, где N≥1.

* 1. **Требования к зданиям и помещениям**

В здании ЦОД Исполнителя должна быть зона погрузки/разгрузки оборудования. В случае размещения ЦОД Исполнителя не на первом этаже здания подъем оборудования необходимо обеспечить с помощью лифтов. Требования к лифтам: грузоподъемность – не менее 2 т, размеры кабины – не менее 1,1х1,5х2,2 (ШxГxВ, м). Также на пути следования оборудования не должно быть ступеней и перепадов высоты.

Несущая способность перекрытий в ЦОД Исполнителя и на пути следования оборудования должна быть не менее 1500 кг/м2.

В ЦОД Исполнителя должно быть не менее двух территориально разнесенных вводов для телекоммуникационного кабеля.

Ограждающие строительные конструкции (стены, перекрытия) машинного зала должны быть устойчивы к взлому.

* + 1. **Требования к системе кондиционирования**

Система кондиционирования должна обеспечивать следующие параметры окружающей среды в машинном зале и в электротехнических помещениях:

* температура от 23 °С до 27 °С;
* точки нормальной настройки: 25 °С;
* точность поддержания температуры: ± 2 °С;
* относительная влажность от 30% до 70%;
* точки нормальной настройки: 45% относительной влажности;
* точность поддержания относительной влажности: ± 5%;
* максимальная скорость изменения температуры в машинных залах не должна превышать: ± 5 °С в час;
* скорость изменения влажности: не более 10% в час

Температура в ЦОД Исполнителя не должна превышать 30 °С на время, отводимое на пуск и выход в рабочий режим ДГУ.

Данные мониторинга температурно-влажностного режима помещений ЦОД Исполнителя должны контролироваться диспетчерской службой Исполнителя для возможности круглосуточного контроля параметров.

* + 1. **Требования к системе пожаротушения**

Машинный зал ЦОД Исполнителя должен быть оснащен комплексом противопожарных систем, включая систему автоматического пожаротушения.

Наличие системы автоматического газового пожаротушения в помещениях машинного зала ЦОД Исполнителя, комнатах ИБП, ГРЩ и электрощитовой ЦОД. Резервный запас огнетушащего газа должен быть инсталлирован в систему и подключаться после расходования основного без проведения монтажных работ.

Система пожаротушения должна иметь на площадке резерв огнетушащего вещества не менее чем на 2 последовательных пуска и должна иметь независимый источник гарантированного электропитания, превышающий по времени автономной работы остальную систему электроснабжения ЦОД.

Все элементы инфраструктуры ЦОД Исполнителя (ГРЩ, ИБП, ДГУ, батареи, трансформаторы) должны располагаться в отдельных помещениях для исключения общего возгорания. Каждое инфраструктурное помещение должно быть оснащено системой пожарной сигнализации и необходимым типом системы пожаротушения (газовое, порошковое и т.п.).

Сигналы системы пожаротушения должны быть выведены на пульт дежурной смены. Срабатывание системы пожаротушения не должно выводить из строя размещенное и не поврежденное пожаром оборудование.

* + 1. **Требования к бесперебойному электроснабжению**

Система бесперебойного электроснабжения должны быть дублирована на всех уровнях: иметь не менее 2 вводов от независимых районных подстанций, иметь собственную РТП, обеспечивать двойное резервирование электрических линий между РТП и ИБП, иметь 2 группы ИБП на полную мощность оборудования с временем автономной работы не менее 10 минут.

Система электроснабжения должна обеспечивать действующее значение напряжения 230В/400В ± 5%, частота 50 ± 0,2 Гц, общей мощностью не менее 1500 кВт.

ЦОД Исполнителя должен иметь 2 электрических линии от ИБП до помещения щитовой ЦОД Исполнителя (по одной от каждой группы), свой электрический щит для каждой линии в помещении щитовой ЦОД, не менее 2 кабелей питания на каждую стойку от разных щитов.

Для статических ИБП время автономной работы любой из взаимно резервирующих систем ИБП на расчетную нагрузку в аварийном режиме в конфигурации N+1 (отказ одной из пары взаимно резервирующих систем ИБП) не должно превышать время, необходимое для запуска ДГУ и полного приёма им нагрузки, но не менее 10 минут.

ИБП должны размещаться в отдельном помещении с организацией доступа только для обслуживающего персонала и собственной установкой поддержания климатических параметров.

Оборудование ЦОД Исполнителя подключено к заземляющим устройствам согласно действующим нормативным документам.

Для обеспечения гарантированного электроснабжения ЦОД Исполнителя обеспечен системой гарантированного электроснабжения.

Уровень резервирования ДГУ должен быть не ниже, чем N+1, где N≥1. Хранилище дизельного топлива должно быть объемом, обеспечивающим работу всех ДГУ для обеспечения 100% критически важной нагрузки ЦОД Исполнителя в течение не менее 6 (шести) часов.

Исполнитель должен иметь действующий договор с топливными компаниями на подвоз необходимого объема топлива автоцистернами не позднее чем через 4 часа после запуска ДГУ.

* + 1. **Требования к службе безопасности**

ЦОД Исполнителя должен круглосуточно охраняться службой безопасности. Арендуемые помещения (выделенное огороженное пространство машинного зала) ЦОД Исполнителя должны быть оснащены системами контроля и управления доступа, охранного телевидения и охранной сигнализацией объекта.

* + 1. **Требования к системе контроля и управление доступом**

Двери ЦОД Исполнителя, а также всех арендуемых помещений, входящих в структуру ЦОД Исполнителя, должны быть оборудованы электронными замками и считывателями карт, подключенными к автоматизированной системе контроля и управления доступом.

Доступ в помещения ЦОД Исполнителя должен быть ограничен для обслуживающего персонала. Входные двери и двери машинного зала должны оборудоваться следующей аппаратурой:

* замками электромагнитными (электромеханическими);
* датчиками контроля двери;
* считывателями бесконтактных карт на вход и выход и/или биометрическими считывателями.

Допуск посторонних лиц в помещения ЦОД Исполнителя, в которых размещается оборудование частного контура, без сопровождения должен осуществляться на основании списка доступа. Доступ посторонних лиц в помещения ЦОД Исполнителя, не указанных в списке доступа, должен осуществляться только в сопровождении уполномоченных сотрудников Исполнителя.

Исполнитель должен осуществлять контроль за пропускным режимом.

Срок хранения записей журнала СКУД о событиях доступа должен составлять 30 календарных дней.

* + 1. **Требования к системе видеонаблюдения**

Под видеонаблюдением должны быть все двери помещений ЦОД Исполнителя, все коридоры между стойками с оборудованием, внешний периметр здания.

Телевизионная система видеонаблюдения должна обеспечивать:

* обзор всех охраняемых зон;
* непрерывную, по детекции и по расписанию мультиплексированную запись видеоинформации на жесткие диски;
* визуальное отображение происходящего в реальном масштабе времени на видеостене в помещение охраны объекта;
* создание видеоархива и его просмотр, непрерывную, по детекции и по расписанию мультиплексированную запись видеоинформации на жесткие диски;
* контроль оперативной обстановки внутри помещений с качеством, достаточным для идентификации лиц в независимости от времени суток;
* формирование архива видеозаписей текущих и тревожных событий со всех установленных видеокамер за период времени 30 дней;
* автоматический вывод изображений от соответствующих видеокамер на "тревожные" видеомониторы телевизионной системы видеоконтроля, видеостену при срабатывании охранного извещателя.
  + 1. **Требования к охранной сигнализации**

Помещения ЦОД Исполнителя должны быть оснащены системой охранной сигнализации. Охранными извещателями должно быть оборудовано:

* входные двери, двери запасных выходов, двери тамбуров эвакуационных выходов, двери лестничных площадок – извещателями "на открывание" и, для дверей со стеклянными панелями, на "разбитие" стекла;
* оконные и дверные конструкции – извещателями "на открывание" и "разбитие" стекла.

Помещения машинного зала, кроссовых, коридоров и зон помещений, входящих в структуру ЦОД Исполнителя, должны быть оборудованы пассивными инфракрасными или комбинированными (ИК+СВЧ) извещателями, в зависимости от назначения помещения и наличия помех (воздушные потоки от кондиционеров и другие помехи).

Количество датчиков должно быть определено потребностями обеспечения качественного контроля внутренних территорий данных помещений, особенно проходов между стойками с оборудованием.

Машинный зал должен защищаться двумя рубежами охранной сигнализации:

* первым рубежом охранной сигнализации блокируется дверь помещения на «открывание» и окна помещения (при наличии) на «открывание» и «разбитие». На «открывание» и «разбитие» блокируются все окна;
* вторым рубежом охранной сигнализации блокируется объем помещения на «проникновение» и движение.
  + 1. **Требования к надёжности инженерно-технических систем**

Все оказываемые услуги должны удовлетворять следующим требованиям к надежности:

Отказоустойчивость работы инфраструктуры ЦОД Исполнителя должна обеспечиваться с помощью «горячего» резервирования основных компонентов ЦОД Исполнителя, путем переключения с основных элементов на резервные, с характеристиками не ниже, чем у основных.

Ремонтные и сервисные работы на инженерной инфраструктуре, обеспечивающей работу ИТ-оборудования, должны проводиться без отключения аппаратных стоек и без снижения качественных параметров систем электроснабжения и охлаждения. Для обеспечения данного требования резервированию должны подлежать не только отдельные устройства и элементы систем, но также и каналы доставки электроснабжения и холода к аппаратным стойкам.

К ремонтным и сервисным работам, в частности, относятся:

* превентивное и плановое обслуживание;
* ремонт и замена компонентов;
* добавление или удалением элементов систем;
* тестирование компонентов и систем в целом.

Инженерно-технические системы ЦОД Исполнителя должны обеспечивать функционирование в диапазоне наружной температуры, соответствующем интервалу пиковых температур для данного региона без снижения заявленных климатических значений внутри ЦОД Исполнителя и уровня надежности инженерной инфраструктуры в целом.

В ЦОД Исполнителя круглосуточно должна присутствовать дежурная служба эксплуатации, в составе которой обязательно должно быть не менее 2-х (двух) инженеров круглосуточно.

ЦОД Исполнителя должен быть оборудован системой автоматизированного контроля и/или управления состояния инженерной инфраструктуры.

* + 1. **Требования к системе защитного заземления**

В ЦОД Исполнителя должна иметься система заземления всех элементов инженерного оборудования, имеющего металлические и токопроводящие части и корпуса в соответствии с требованиями ГОСТ Р 50571.21-2000, ГОСТ Р 50571.22-2000 и ПУЭ, 7-я редакция.

К системе защитного заземления (СЗЗ) должны быть подключены, помимо основного и дополнительного инженерного оборудования, монтажные шкафы с установленным в них оборудованием и предусмотрено заземление внешних блоков кондиционеров, системы трубопроводов и т.п.

* + 1. **Требования к системе молниезащиты технологического оборудования**

Здание ЦОД Исполнителя должно быть обеспечено молниезащитой технологического оборудования, размещенного на кровле здания, оборудования приточно-вытяжной вентиляции, чиллеров, конденсаторных блоков.

* + 1. **Требования к телекоммуникационным ресурсам ЦОД**

Факт наличия основного и резервного оптического ввода в здание ЦОД Исполнителя должен быть подтверждён исполнительной документацией по организации кабельных трасс в здании ЦОД и проектами оптических трасс операторов связи.

В ЦОДе Исполнителя должны присутствовать не менее 5 независимых на уровне активного оборудования операторов связи. Факт наличия должен подтверждаться официальными письмами о возможности подключения на территории ЦОД Исполнителя, с указанием точки подключения (машинный зал, стойка, юнит, порт).

* 1. **Требования к каналам передачи данных**

Исполнитель для организации доступа из ЦОД Заказчика к выделенной инфраструктуре ЦОД Исполнителя должен обеспечить предоставление канала передачи данных со скоростью не менее 10 Гбит/с1. Доступ должен быть организован посредством предоставления основного и резервного (независимого, прямого, волоконно-оптического) физических каналов передачи данных до ЦОД Заказчика по адресу г. Новосибирск ул. Свердлова 14, с максимальной протяженностью канала передачи данных не более 20 километров. Для обеспечения шифрования каналов связи между ЦОД Заказчика и ЦОД Исполнителя Заказчик предоставляет сертифицированные средства криптографической защиты информации и в дальнейшем их администрирует собственными силами.

Скорость обмена между виртуальными ресурсами должна быть не ниже 10 Гбит/с1.

Каналы передачи данных должны обеспечивать время отклика от инфраструктуры ЦОД Заказчика до виртуальных ресурсов, размещенных на выделенной инфраструктуре в ЦОД Исполнителя, не более 2 миллисекунд.

В целях резервирования сетевой связанности Исполнитель должен организовать подключение, путём организации отказоустойчивых кластеров из криптомаршрутизаторов, предоставляемых Заказчиком, на стороне ЦОД Заказчика и ЦОД Исполнителя по физически разнесённым каналам передачи данных.

Число потерянных пакетов на физическом канале (оптическое волокно) должно составлять не более 0,3% от общего числа пакетов (в месяц).

Доступность каналов связи должна составлять не менее 99% в отчетный период.

Формула расчета доступности услуги по предоставлению каналов связи:

Услуга по каждой точке считается недоступной в период времени:

* - с момента поступления заявки от Заказчика и до подтверждения Заказчиком восстановления услуги;
* - с момента обнаружения Исполнителем аварии на участке сети связи, через который осуществляется пропуск трафика, не имеющего альтернативного маршрута, и до момента устранения аварии;
* - с момента начала плановых работ на участке сети связи, через который осуществляется пропуск трафика, не имеющего альтернативного маршрута, и до момента завершения работ.

Доступность каналов за месяц подключения определяется по формуле:

Kд - Коэффициент доступности сети

N - Количество мест предоставления услуги

tn - Время недоступности n-ой точки подключения

- Суммарное время недоступности всех точек подключения

T - Количество минут в отчетном периоде (24×60×кол-во дней в отчетном периоде).

Техническая поддержка пользователей Услуги должна осуществляться - 24 (двадцать четыре) часа в сутки, 7 (семь) дней в неделю 365 дней в году.

Все поступающие заявки должны регистрироваться в системе учета заявок с присвоением каждой заявке уникального идентификационного номера. По требованию заказчика Исполнитель должен предоставлять статистику заявок с указанием даты регистрации, уникального идентификационного номера, содержания и текущего статуса заявки. Отчет по зарегистрированным заявкам должен предоставляться ежемесячно.

Плановые профилактические работы с закрытием одного из каналов связи должны проводиться в часы наименьшей нагрузки с извещением Заказчика не менее, чем за трое суток до начала работ. Периодичность профилактических работ – не чаще 4 (четырех) раз в течение срока действия контракта. Продолжительность проведения плановых работ не должна превышать четырех часов.

* 1. **Требования к выделенной инфраструктуре**

Услуга по предоставлению выделенной инфраструктуры в центре обработки данных должна предоставляться Исполнителем по принципу готового сервиса. Исполнитель должен предоставить Заказчику права на доступ к услуге, необходимые для точечного управления ИТ системами, при этом проведение работ, связанных с обслуживанием выделенной инфраструктуры, должны находиться в зоне ответственности Исполнителя.

Для обеспечения отказоустойчивости Исполнитель должен предусмотреть избыточность на уровне компонентов комплекса, на базе которого реализуется Услуга.

Выделенная инфраструктура должна быть защищена дополнительными средствами как информационной, так и физической безопасности, согласно требованиям к информационной безопасности настоящего описания объекта закупки.

Услуга по предоставлению выделенной инфраструктуры в ЦОД Исполнителя должна включать в себя ресурсы, предоставленные в пользование только Заказчику, без возможности использования этой выделенной инфраструктуры третьими лицами. Заказчик должен иметь возможность задействовать тот объем ресурсов, который необходим ему для решения текущих задач в определенный момент времени.

В ЦОД Заказчика используется платформа среды виртуализации VMware vSphere 6.7, выделенная инфраструктура Исполнителя должна быть реализована на платформе среды виртуализации, позволяющей автоматизировано мигрировать виртуальные машины из ЦОД Заказчика в ЦОД Исполнителя и в обратном направлении.

Заказчик самостоятельно через интерфейс самообслуживания, должен иметь возможность:

* создавать виртуальные машины по отдельности и в виде групп;
* управлять работой виртуальных машин (включить, выключить и перезагрузить);
* изменять конфигурацию виртуальных машин, в т.ч. конфигурацию вычислительных ресурсов, дисковую и сетевую;
* непосредственно получить доступ к консоли виртуальной машины;
* создавать копии виртуальных машин и их групп;
* монтировать ISO образы CD/DVD;
* удалять и добавлять внутренние логические сети, управлять подключением виртуальных машин к сетям;
* создавать и удалять виртуальные маршрутизаторы, управлять сервисами этих виртуальных маршрутизаторов.

Заказчик путем направления запроса в службу технической поддержки должен иметь возможность:

* получать доступ к текущим и историческим данных мониторинга производительности компонентов виртуальной инфраструктуры и виртуальных машин;
* удалять и добавлять сети на базе VLAN для частного сегмента облака (кроме сетей, использующихся для функционирования инфраструктуры);
* получать по запросу доступ к логам событий всех компонентов виртуальной инфраструктуры;
* изменять права доступа заданным группам или пользователям.

Должна быть организована возможность сохранения и выгрузки резервных копий виртуальных машин.

Должна быть обеспечена возможность создания и установки собственных и предлагаемых третьими лицами сборок виртуальных машин посредством шаблонов виртуальных машин (Virtual Appliance).

Для обеспечения отказоустойчивости и минимизации времени простоя при доступе к выделенной инфраструктуре Заказчика, Исполнитель должен:

* обеспечить подключение ресурсов выделенной инфраструктуры к сети Заказчика резервируемыми каналами связи (не менее двух);
* подключение к сети Заказчика должно использовать территориально разнесенные вводы волоконно-оптического кабеля в ЦОД.

Должна быть включена по умолчанию функция высокой доступности (High Availability), позволяющая осуществлять автоматический перенос виртуальных машин на резервный сервер в случае выхода из строя сервера в предоставляемой Заказчику выделенной инфраструктуре.

* + 1. **Требования к минимальным вычислительным ресурсам и ресурсам хранения, предоставляемым Исполнителем**

Исполнитель должен предоставить Заказчику возможность использования вычислительных ресурсов и ресурсов хранения со следующими параметрами:

|  |  |  |
| --- | --- | --- |
| **Подсистема** | **Ресурс** | **Требования** |
| Вычислители | Базовая частота vCPU | 3,1 ГГц |
| Коэффициент переподписки виртуальных ядер к физическим (pCPU:vCPU) | 1:5 |
| Система хранения данных | Тип дисков | Enterprise SSD |
| Дисковое пространство, SSD Тип 1 | 3 мс при интенсивности ввода-вывода 2 000 IOPS/TB, но не более 30 000 IOPS |
| Дисковое пространство, SATA Тип 2 | 20 мс при интенсивности ввода-вывода 200 IOPS/TB, но не более 7 000 IOPS |
| Дисковое пространство, SATA Тип 3 | 30 мс при интенсивности ввода-вывода 100 IOPS/TB, но не более 3 500 IOPS |
| Среда виртуализации и ВМ | Среда виртуализации обладает необходимым функционалом для автоматической миграции ВМ в ЦОД Заказчика в случае отказа ЦОД Исполнителя | Да |
| Максимальные параметры запускаемой ВМ | 48 ядер vCPU |
| Узлы отказоустойчивого кластера виртуализации на площадке основного ЦОД Исполнителя под задачи Заказчика | N+1 |
| Резервирование мощностей | Указанные мощности являются зарезервированными для Заказчика (Allocated pool) | Да |
| Исполнитель располагает дополнительными мощностями с показателями производительности не менее 50% от указанных для аварийного переноса выделенной инфраструктуры Заказчика в случае отказа. | Да |
| Аппаратные требования | Выделенные серверы, в т.ч. резерв N+1;  Выделенное сетевое оборудование для коммутации;  Выделенная SAN-фабрика;  Выделенные СХД;  Выделенные серверы резервного копирования;  Индивидуальный контур управления виртуализацией | ПАК состоящий из серверного и сетевого оборудования должен использоваться только для задач Заказчика |

* + 1. **Требования к системе хранения данных**

Должна быть обеспечена возможность выделения Заказчику дискового пространства трёх типов производительности согласно п.8.3.1.

Доступ к сети хранения данных каждого вычислительного узла, предоставляемого Исполнителем, должна быть не менее 16 Гбит/с.

Система хранения данных должна быть подключена не менее чем к двум независимым SAN-фабрикам, предоставляемым Исполнителем.

Общая схема организации SAN сети должна быть построена таким образом, чтобы выход из строя любого единичного компонента не приводил к остановке сервиса в целом.

* + 1. **Требования к сетевой инфраструктуре**

Сетевое коммутационное оборудование Исполнителя для оказания Услуги должно быть объединено в отказоустойчивую архитектуру при помощи технологий агрегирования для обеспечения непрерывности при проведении работ по техническому обслуживанию сетевой инфраструктуры и аварийных ситуациях на различных участках волоконно-оптических линий связи между ЦОД Заказчика и ЦОД Исполнителя.

Сетевая инфраструктура должна обеспечивать изоляцию трафика Заказчика от трафика других клиентов.

Сетевая инфраструктура ЦОД Исполнителя должна обеспечивать пропускную способность не менее 10 Гбит/сек1.

* + 1. **Требования к платформе резервного копирования**

Платформа резервного копирования должна позволять создавать Заказчику резервные копии данных. Система управления и интерфейс платформы резервного копирования должны позволять гибко настраивать частоту создания полных копий данных и копий изменений по времени. Резервные копии должны храниться на физически не зависимом от основных данных оборудовании.

Заказчику должен быть предоставлен доступ к интерфейсу управления системой. Интерфейс управления платформы резервного копирования должен содержать информацию о резервных копиях данных Заказчика, позволять Заказчику самостоятельно управлять заданиями резервного копирования и восстановления данных.

Платформа резервного копирования должна обеспечивать возможность резервного копирования ВМ на уровне образов, с возможностью копирования только изменившихся блоков, а также без установки специализированных приложений внутрь ВМ;

Платформа резервного копирования должна поддерживать передачу резервных копий, как по сети передачи, так и по сети хранения данных, включая резервное копирования ВМ напрямую с NFS хранилищ.

Платформа резервного копирования должна поддерживать механизм автоматического изменения скорости процесса резервного копирования при увеличении времени отклика на чтение на всех системах хранения с возможностью определения порогов времени отклика.

Платформа резервного копирования должна иметь механизм дедупликации и сжатия резервных копий “на лету”, возможность исключать блоки служебных файлов ОС, а также папки и файлы, указанные пользователем, для ускорения процесса резервного копирования, а также для уменьшения объема хранимых данных.

Платформа резервного копирования должна уметь использовать аппаратные снимки СХД для резервного копирования, с возможностью обеспечения целостности приложений внутри виртуальных машин. Взаимодействие должно реализовываться при помощи специализированных API на уровне СХД и без установки дополнительного программного обеспечения на них.

* + - 1. **Требования к тестированию целостности и возможности восстановления резервных копий виртуальных машин**

Платформа резервного копирования должна иметь возможность создать изолированную среду на продуктивной инфраструктуре Заказчика, с возможностью использовать ее для автоматического тестирования резервных копий или для создания тестовых зон.

Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности резервных копий ВМ. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из резервных копий и/или аппаратных снимков СХД в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри резервируемой ВМ. Должна быть возможность использовать как встроенные скрипты проверки, так и возможность использовать собственные скрипты.

* + - 1. **Требования к хранению резервных копий виртуальных машин**

Платформа резервного копирования должна иметь возможность шифровать резервные копии.

Платформа резервного копирования должна иметь возможность интегрироваться с машинами на базе ОС Linux для использования их в качестве защищенных хранилищ резервных копий, позволяющих установить настройку неизменности данных, обеспечивающую возможность защиты от удаления и изменения блоков данных резервных копий на указанный промежуток времени.

Платформа резервного копирования должна уметь передавать резервные копии между различными хранилищами с возможностью указания новой глубины хранения для резервной копии.

При передаче резервных копий между хранилищами платформа резервного копирования должна иметь возможность возобновляемой передачи резервных копий между площадками с использованием механизмов сжатия и глобальной дедупликации трафика и кэширования информации на обеих площадках на специализированных серверах.

Платформа резервного копирования должна иметь возможность формирования синтетической полной резервной копии при записи на ленту из имеющихся в дисковом хранилище резервных копий полной резервной копии и цепочки инкрементальных без создания временной синтетической полной копии на диске.

* + - 1. **Требования к восстановлению данных из резервных копий виртуальных машин**

Платформа резервного копирования должна поддерживать возможность восстановления из резервных копий даже в случае полной потери сервера резервного копирования.

Платформа резервного копирования должна поддерживать восстановление виртуальных машин как целиком, так и отдельных виртуальных дисков, и файлов конфигураций. Восстановление должно идти как по сети передачи, так и по сети хранения данных.

Платформа резервного копирования должна обеспечивать моментальный запуск виртуальных машин непосредственно из хранилища резервных копий с возможностью последующего переноса виртуальной машины на выбранное хранилище данных без прерывания работы.

Платформа резервного копирования должна обеспечивать возможность предварительного антивирусного сканирования и проверки резервных копий при восстановлении.

Платформа резервного копирования должна обеспечивать возможность до восстановления ВМ в рабочую инфраструктуру удалить данные из этой ВМ, не удаляя эти данные из резервной копии.

Платформа резервного копирования должна реализовывать гранулярное восстановление данных приложений из резервных копий, в промежуточное и/или исходное месторасположение без установки специализированного агента;

Платформа резервного копирования должна реализовывать точеное восстановление СУБД на ОС Windows и ОС Linux (с поддержкой технологии ASM), имеющихся у Заказчика, включая возможность восстановления данных до конкретной транзакции, в промежуточное и/или исходное месторасположение без установки специализированного агента.

Платформа резервного копирования должна обеспечивать возможность позволять делегировать пользователям самостоятельно восстанавливать из резервной копии объекты приложений через Web-портал.

* + 1. **Требования к функциональным возможностям репликации и аварийного восстановления виртуальных машин**

Платформа резервного копирования должна поддерживать прямую репликацию виртуальных машин без использования промежуточных резервных копий, с возможностью обеспечения создания множества точек восстановления и передачей только изменившихся блоков.

Платформа резервного копирования должна обеспечить целостность приложений внутри ВМ при репликации, без установки специализированных приложений внутрь ВМ.

Платформа резервного копирования должна обеспечивать переключение на реплицированную виртуальную машину с возможностью автоматической смены IP адреса.

Платформа резервного копирования должна обеспечивать переключение на реплицированную виртуальную машину даже при потере сервера резервного копирования.

* + - 1. **Требования к тестированию целостности и возможности восстановления реплицированных виртуальных машин**

Платформа резервного копирования должна иметь возможность автоматического тестирования работоспособности реплик ВМ. Проверка должна осуществляться с помощью запуска связанных виртуальных машин из реплик в изолированной среде по расписанию, с возможностью тестирования работоспособности приложений и сервисов внутри ВМ. Должна быть возможность использовать как встроенные скрипты проверки, так и возможность использовать собственные скрипты.

* + - 1. **Требования к возможности непрерывной репликации и аварийного восстановления для виртуальных машин**

Платформа резервного копирования должна поддерживать непрерывную репликацию виртуальных машин без использования снимков виртуализации, обеспечивающую минимальную потерю данных в пределах 2 секунд.

Платформа должна непрерывно реплицировать операции ввода/вывода виртуальных машин и хранить их в специальном журнале на целевом хранилище в течении нескольких часов, указанных в краткосрочной политике хранения в целях обеспечения возможности восстановления ВМ на определенный момент времени с заданным шагом.

Платформа должна обеспечивать возможность создания дополнительных точек восстановления ВМ, выходящих за пределы краткосрочной политики репликации, с учетом состояния работающих внутри приложении и обеспечения их консистентности, без установки специализированных приложений внутрь ВМ.

* 1. **Требования к средствам защиты информации.**

Выделенная Заказчику инфраструктура в ЦОД Исполнителя должна быть готова к проведению комплекса организационно-технических мероприятий, в результате внедрения которых подтвердится соответствие системы защиты информации требованиям безопасности информации в соответствии с приказом ФСТЭК России от 11.02.2013 № 17 для размещения государственных информационных систем не ниже второго класса защищенности и информационных систем персональных данных, обрабатывающих персональные данные не ниже второго уровня защищенности.

Для обеспечения безопасности информации Исполнителем предоставляются в пользование следующие средства защиты:

* средства межсетевого экранирования и системы обнаружения вторжений (2 шт.) (п.8.4.1 данного ООЗ)
* средства защиты виртуальной инфраструктуры (1 шт.) (п 8.4.3 данного ООЗ);
* средства антивирусной защиты (30 шт.) (п. 8.4.4 данного ООЗ)
* средства доверенной загрузки (1 шт.) (п. 8.4.5 данного ООЗ)
* средства защиты от несанкционированного доступа (30 шт.) (п 8.4.6 данного ООЗ)

Средства защиты информации должны предоставляться в настроенном виде и готовыми к использованию и не должны приводить к нарушению штатного функционирования выделенной инфраструктуры.

Заказчик администрирует средства защиты информации самостоятельно.

* + 1. **Минимальные требования к используемому Исполнителем межсетевому экрану и системе обнаружения вторжений**

Межсетевой экран предоставляется в виде отказоустойчивого программно-аппаратного комплекса (2 шт.) и должен обеспечивать контроль   
8 миллионов одновременных TCP-сессий на пропускной способности канала 18 000 Мб/c.

Межсетевой экран должен регулярно получать с сервера производителя «чёрный» список ip адресов спамеров и открытых релеев.

Межсетевой экран должен регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя.

Межсетевой экран должен поддерживать следующие основные функции:

* контроль доступа пользователей в сеть и фильтрации трафика сети;
* анализ трафика сети по категориям, адресам и контенту данных;
* мониторинг действий, совершаемых пользователями при работе с сетью, а также формирование отчетности;
* предоставление возможности обновлять списки с помощью офлайн обновлений;
* контроль технологических протоколов АСУ ТП: Modbus, DNP3, MMS;
* возможность встраивания в сетевую инфраструктуру заказчика по протоколу WCCP;
* защита объектов сетевой инфраструктуры с помощью системы обнаружения вторжений (СОВ);
* контроль передаваемого трафика через межсетевой экран с помощью определения приложений L7.

Особенности реализации функций межсетевого экранирования:

1. функционал настройки средств фильтрации входящего и исходящего трафика должен позволять указывать в качестве фильтра маску или регулярное выражение.
2. необходимо наличие события об успешной загрузке системы в журнале событий.
3. должно быть обеспечено журналирование изменения времени в консоли администрирования.
4. Необходимо наличие оповещений по SNMP при срабатывании запрещающих правил межсетевого экрана.
5. Должна обеспечиваться блокировка всего трафика при инцидентах, таких как нарушение функционирования системы. В случае если исполняемый файл из состава МСЭ изменен, весь трафик должен быть заблокирован.
6. Функционал решения должен иметь возможность запрашивать ввод пароля на разблокировку в случае несанкционированного доступа к изменениям правил МСЭ, изменениям правил оповещения, сетевым интерфейсам, добавлению учетной записи нового администратора, экспорту логов системы.
7. Фильтрация входящего и исходящего трафика должна осуществляться с одновременным обеспечением проверки на наличие вредоносного программного обеспечения.

Требования к доступности и производительности межсетевого экранирования:

* программное обеспечение должно иметь возможность быть реализованным в соответствии с методом обеспечения высокой доступности, гарантируя минимальное время простоя, и полного решения возложенных задач при выходе из строя одного из компонентов.
* программное обеспечение должно обеспечивать резервное копирование конфигураций компонентов и журналов регистрации событий с функцией исторического хранения данных с глубиной хранения не менее 12 месяцев.
* программное обеспечение должно иметь возможность масштабирования. Увеличение числа обслуживаемых пользователей и объема обрабатываемого трафика сети должно осуществляться путем подключения дополнительных программно-аппаратных компонентов.
* при наличии дополнительных узлов программное обеспечение должно позволять в любое время выводить часть узлов фильтрации из эксплуатации для обслуживания с автоматическим перераспределением нагрузки на оставшиеся узлы прозрачно для пользователей.
* должен обеспечиваться функционал настройки программно-аппаратных средств, входящих в состав, без остановки всей Системы.
* программное обеспечение должно обеспечивать функцию планового отключения для выполнения профилактических мероприятий, изменений или наращивания аппаратного обеспечения, установки обновлений на программное обеспечение.
* программное обеспечение должно предоставлять инструменты диагностирования состояния собственных компонентов.
* в программном обеспечении должна быть ролевая модель разграничения доступа. Роли должны иметь ограничения по доступу к Программному обеспечению на уровне интерфейсов, функционала, отчетов и производственных объектов.

Обеспечение следующих видов фильтрации (анализа) передаваемого контента:

* анализ передаваемых объектов по типу передаваемых объектов, в том числе определение и корректная обработка распространенных форматов файлов, применяемых в офисном ПО (DOC, DOCX, XLS, XLSX, PDF, TXT, ODT и т.д.);
* поиск и анализ регулярных выражений (ключевых слов);
* лингвистический (морфологический) анализ.
* эвристический анализ.
* автоматическое или ручное обновление компонентов с сайта производителя.

Управление доступом к средствам контентного анализа с использованием ролевой модели.

Требования к функционалу средств мониторинга и отчетности:

* протоколирование действий пользователей и администраторов
* отслеживание текущей сессии пользователя в режиме on-line, определение сервера, через который установлена сессия, подключения к серверу и разбора пользовательской сессии.

Формирование отчетности с функционалом:

* объявления пользовательских (новых) полей
* формирования запросов с использованием перекрестных запросов.

Формирование отчетности с предоставлением функционала:

* задания фильтров по всем (любым) полям, поддерживаемым средствами мониторинга функционирования и формирования отчетности;
* формирования запросов к базе данных;
* задания формата отчетов;
* отправку отчетов по расписанию и по запросу администраторов;
* отключение мониторинга функционирования и формирования отчетности для конкретных пользователей/IP-адресов.
* Автоматическое или ручное обновление компонентов с сайта производителя.
* Управление доступом к средствам мониторинга и отчетности с использованием ролевой модели.
* Отправка статистической информации по протоколу NetFlow версий 5, 9, 10.

Связь с существующим окружением и интеграция

Разграничение полномочий доступа для работы и доступа пользователей в сеть должно быть реализовано на ролевой основе с использованием групп существующих доменов Active Directory.

Система должна взаимодействовать со следующими смежными системами:

* система Active Directory, в части аутентификация пользователей в Active Directory, определение принадлежности пользователей к группам Active Directory.
* системы авторизации пользователей Kerberos, NTLM, Single-sign-on в части автоматической авторизации пользователей.
* система идентификации пользователей Radius accounting, определение IP-адресов пользователей.
* система синхронизации времени, в части взаимодействия с системой синхронизации времени должна поддерживать определение точного времени.
* система доменных имен (DNS), в части взаимодействия с системой DNS должно поддерживать определение IP-адресов узлов сети по имени узла.
* система мониторинга SNMP, в части взаимодействия с системой мониторинга SNMP должно поддерживать оповещение и работу в режиме запросов состояния системы по протоколам SNMP v2 и SNMP v3.
* корпоративная почтовая система (E-mail), в части взаимодействия с корпоративной почтовой системой должно поддерживать отправку по e-mail оповещений администраторам о событиях в работе средств контроля доступа в сеть Интернет и фильтрации трафика сети Интернет.
* система сбора и корреляции событий информационной безопасности, в части взаимодействия с системами сбора и корреляции событий информационной безопасности должно предоставлять механизм экспорта журнальных сообщений в режиме реального времени. Формат и детализация данных сообщений должны настраиваться.
* системы дополнительного контентного анализа, в части взаимодействия с системами дополнительного контентного анализа должно предоставлять модуль интеграции по протоколу I-CAP с указанными системами в части условий доступа на основании результатов анализа контента.

Требования к пользовательскому интерфейсу:

* программный интерфейс компонентов, включая средства управления, а также формы оповещений и уведомлений администраторов Системы и пользователей сети Интернет должен полностью поддерживать русский язык, используя кодировку текста UTF-8.
* наличие web-интерфейса для доступа к компонентам узла фильтрации Интернет-трафика, включая средства управления, полностью поддерживающего русский язык, используя кодировку текста UTF-8.

Требования к наличию отчетов:

* система должна обеспечивать формирование отчетности в табличном и графическом виде о совершаемых пользователями действиях в сети Интернет за различные периоды времени.

Дополнительные требования

* автоматическое или ручное обновление программных компонентов с сайта производителя.
* управление доступом к средствам контроля доступа в сеть Интернет и фильтрации трафика сети Интернет с использованием ролевой модели.
* протоколирование действий администраторов;
* обеспечение отказоустойчивости программно-аппаратных компонентов;
* Предоставление возможности автоматического развертывания серверов фильтрации трафика с использованием API.

Требования к происхождению

Поставляемое решение внесено в Единый реестр российских программ для электронных вычислительных машин и баз данных.

Межсетевой экран должен иметь действующий сертификат ФСТЭК России и соответствовать следующим требованиям:

- «Требования к межсетевым экранам» (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» ИТ.МЭ.А4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты» ИТ.МЭ.Б4.ПЗ (ФСТЭК России, 2016), «Профиль защиты межсетевых экранов типа «Д» четвертого класса защиты» ИТ.МЭ.Д4.ПЗ (ФСТЭК России, 2016);

- «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011), «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (ФСТЭК России, 2012);

- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020). Четвертый уровень доверия.

* + 1. **Требования к монтажу, установке и настройке средств криптографической защиты**

Средства криптографической защиты передаются Исполнителю для их монтажа и установки в ЦОД Исполнителя силами Исполнителя. Средства криптографической защиты представляют собой интегрированные решения на базе специализированной аппаратной платформы и программного обеспечения, которое функционирует под управлением адаптированной операционной системы.

Исполнитель должен предусмотреть место размещения средств криптографической защиты с выделением необходимого места в ЦОД Исполнителя и выделением необходимой мощности питания оборудования Заказчика.

Исполнитель должен гарантировать:

исключение неконтролируемого проникновения или пребывания в месте размещения средств криптографической защиты;

системы электропитания и заземления в помещении соответствуют требованиям документа «Правила устройства электроустановок», утвержденные приказом Министерства энергетики Российской Федерации от 08.07.2004 № 204;

оборудование помещений, где эксплуатируются средства криптографической защиты средствами вентиляции и кондиционирования воздуха;

Исполнитель должен смонтировать средства криптографической защиты в выделенной инфраструктуре, осуществить ввод в эксплуатацию средств криптографической защиты с оформлением актов ввода в эксплуатацию в 2-х экземплярах – 1-ый экземпляр передается Заказчику, 2-ой экземпляр хранится у Исполнителя; произвести настройку в соответствии с технической документацией производителя средства криптографической защиты в целях организации защищенного канала связи между ЦОД Заказчика и ЦОД Исполнителя.

* + 1. **Требования к системе защиты виртуализации**

Система защиты виртуализации предоставляется в пользование в виде выделенных компьютеров для защиты от несанкционированного доступа систем гипервизора и должна осуществлять:

* аутентификацию администраторов виртуальной инфраструктуры и администраторов безопасности;
* защиту средств управления виртуальной инфраструктурой от НСД;
* защиту серверов от НСД;
* контроль целостности конфигурации виртуальных машин и их доверенную загрузку;
* мандатный принцип контроля доступа;
* регистрацию событий, связанных с информационной безопасностью;
* контроль целостности и защиту от НСД компонентов СЗИ;
* централизованное управление и мониторинг;
* создание резервной копии конфигурации СЗИ и журналов аудита;
* работу в отказоустойчивом режиме (кластер);
* синхронизация настроек безопасности между серверами СЗИ.

Требования к функциональности:

**- аутентификация администраторов виртуальной инфраструктуры и администраторов безопасности.** Должна быть реализована модель разделения прав на управление виртуальной инфраструктурой и на управление безопасностью (для ограничения на использование привилегий суперпользователя). Должна быть возможность выделить 2 основные роли — администратор виртуальной инфраструктуры и администратор безопасности. В рамках роли администратора виртуальной инфраструктуры должна быть возможность разграничения доступа по привилегиям\типам объектов доступа. Должна быть поддержка аппаратных идентификаторов JaCarta, JaCarta2, RuToken и iButton. Доступ на управление виртуальной инфраструктурой или параметрами безопасности должен предоставляться только для аутентифицированных пользователей. Для этого в системе защиты виртуализации должна быть предусмотрена процедура аутентификации пользователей и компьютеров (рабочих мест администраторов), которая должна осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и атакам типа Man in the Middle.

Процедура аутентификации должна осуществляется с помощью отдельной программы, которую требуется запустить и ввести учетные данные до того, как осуществляется соединение с виртуальной инфраструктурой. Функционал аутентификации на рабочем месте администратора должен предоставлять возможность надежно сохранить учетные данные.

Для обеспечения защиты средств управления виртуальной инфраструктурой должен применяется функционал мандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Для этого весь управляющий трафик должен проходить через компонент системы защиты виртуализации, осуществляющий этот контроль. Правила разграничения доступа должны работать на основе меток и уровней безопасности, а также заданных ACL и параметров соединения (протоколов, портов).

Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами должен подписываться, для обеспечения защиты от атак типа Man in the Middle в процессе сетевого взаимодействия.

В системе защиты виртуализации должен присутствовать механизм блокирования любого сетевого трафика со стороны виртуальных машин к средствам управления виртуальной инфраструктурой. Тем самым должна обеспечивается защита средств управления виртуальной инфраструктурой от несанкционированного доступа со стороны скомпрометированной виртуальной машины. В системе защиты виртуализации должна быть предусмотрена возможность ограничения миграции виртуальных машин за пределы управления. В системе защиты виртуализации должен присутствовать оповещения администратора виртуальной инфраструктуры о том, что действие заблокировано СЗИ.

**- защита гипервизоров от несанкционированного доступа.** В рамках обеспечения защиты гипервизоров от несанкционированного доступа в системе защиты виртуализации должны быть реализованы следующие механизмы:

* создания списка разрешенных программ;
* контроля разграничения сети управления и сети виртуальных машин;
* настройки параметров логирования виртуальных машин;
* создания списков запрещенных устройств;
* отключения VIX API;
* запрета коммуникаций между виртуальными машинами;
* ограничения объема VMX-файла;
* контроля за использованием independent-nonpersistent дисков;
* проверки использования стандартных SSL сертификатов;
* отключения приветственной страницы;
* контроля службы виртуальной безопасности в гипервизоре;
* создания списка пользователей, которым разрешен локальный вход на виртуальный сервер;
* запретить сжатие виртуального диска;
* ограничения количества активный консольных подключений;
* блокирования подключения USB-носителей к виртуальному серверу;
* осуществления контроля и настройки правил встроенного межсетевого экрана;
* запрета клонирования и создания снимков виртуальных машин;
* очистки внешней и оперативной памяти при окончании работы с виртуальной машиной;
* ограничения доступа к конфигурационным файлам служб;
* запрета непосредственного доступа к управлению виртуального сервера;
* контроля использования протокола SSH;
* запрета операций с буфером обмена для каждой виртуальной машины;
* контроля использования CHAP для проверки подлинности при подключении iSCSI-устройств;
* создания парольных политик;
* отключения неиспользуемых протоколов, портов и функций;
* настройки безопасности виртуального коммутатора;
* запрета контроля устройств виртуального сервера со стороны виртуальных машин;
* запрета отсылки информации о производительности виртуального сервера гостевым системам;
* настройки синхронизации времени;
* запрета доступа к консоли виртуальной машины.

**- контроль целостности конфигурации виртуальных машин и доверенная загрузка.** Система защиты виртуализации должна содержать компоненты, устанавливаемые на каждый гипервизор и реализующие следующие механизмы защиты:

* контроль целостности настроек виртуальной машины перед ее загрузкой. Должен контролироваться файл \*.vmx, в котором содержится перечень устройств, доступных виртуальной машине, и ряд других критических параметров;
* контроль образа BIOS виртуальной машины. Поскольку несанкционированная подмена BIOS является угрозой безопасности, СЗИ должно контролировать целостность файла \*.nvram, в котором содержится образ BIOS виртуальной машины;
* доверенная загрузка ОС должна осуществляться путем контроля целостности загрузочного сектора виртуального диска \*.vmdk;
* контроль целостности шаблонов виртуальных машин, включая виртуальные жесткие диски.

При изменении одного из перечисленных объектов как санкционированном, так и несанкционированном, СЗИ должно предоставить администратору безопасности возможность данные изменения отменить или принять.

**- мандатный принцип контроля доступа.** В системе защиты виртуализации должен быть реализован мандатный принцип контроля доступа на основе меток конфиденциальности. Должно присутствовать два вида меток конфиденциальности: иерархические (метки) и неиерархические (категории).

Должна быть реализована возможность назначить метки на следующие субъекты, объекты, контейнеры:

* Администраторы ВИ;
* Виртуальные хосты;
* Сетевые адаптеры виртуального хоста;
* Виртуальные сети;
* Разделы хранилищ (Datastore);
* Виртуальные машины;
* Серверы управления;
* Группы объектов.

Права доступа субъектов и объектов должны проверяться на основе меток и категорий автоматически и запрещать несанкционированные действия. Субъект может получить доступ к объекту, только если выполняется условие соответствия их меток конфиденциальности. Для категорий – это совпадение хотя бы одной из категорий субъекта и объекта, для меток – это уровень иерархии субъекта должен быть равен (или выше, в зависимости от настроек СЗИ) уровню объекта.

Категории должны отличаться от меток следующими параметрами:

* Метки должны быть иерархическими, категории равноправными.
* Механизмы работы меток должны зависеть не только от пользователя, но и от его меток его текущей сессии. Категории от сессии зависеть не должны.
* Любой субъект, объект, контейнер может быть помечен несколькими категориями и только одной меткой.

Должен быть предусмотрен механизм отключения контроля мандатного доступа по типам объектов.

Должен быть предусмотрим механизм автоматизированного добавления виртуальных машин в группы объектов.

**- регистрация событий, связанных с информационной безопасностью.**

В системе защиты виртуализации должен быть реализован механизм регистрации следующих групп событий:

* аутентификации и разграничения доступа;
* попыток доступа к инфраструктуре (с указанием имени учетной записи, даты, имени компьютера или его IP-адреса)
* изменения конфигурации параметров безопасности и учетных записей администраторов инфраструктуры
* контроля целостности СЗИ, контроля целостности и доверенной загрузки виртуальных машин;
* связанных с установкой, удалением, включением, остановом и сбоем компонентов системы защиты виртуализации, а также с изменением настроек системы защиты виртуализации.

Регистрация событий на всех компонентах системы защиты виртуализации должна осуществляется в едином журнале. Для всех групп событий должны регистрироваться как факты НСД, так и правомочные действия.

Должна быть возможность отбора событий безопасности по типу, дате и времени события, объекту\субъекту доступа.

В системе защиты виртуализации должен быть реализован механизм отправки уведомлений о событиях безопасности по протоколам SMTP и Syslog.

**- контроль целостности и защита от НСД компонентов системы защиты виртуализации.** Система защиты виртуализации должна содержать собственные механизмы контроля целостности компонентов системы защиты виртуализации. Механизмы должны действовать на всех компонентах СЗИ.

**- централизованное управление и мониторинг.** Система защиты виртуализации должна содержать Консоль управления, устанавливающуюся на рабочее место администратора безопасности со следующим функционалом:

* управление учетными записями администраторов виртуальной инфраструктуры и администраторов безопасности;
* назначение прав на доступ к защищаемым объектам;
* развертывание и настройка компонентов защиты Виртуального хостов;
* настройка правил разграничения запуска виртуальных машин и утверждение изменений параметров виртуальных машин, произведенных администраторами ВИ;
* просмотр журнала регистрации событий безопасности.
* Все изменения, произведенные администратором безопасности, должны сохраняться централизованно.

Требования по сертификации:

система защиты виртуализации должна быть сертифицирована на соответствие требованиям:

Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности,

* «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - не ниже 4 уровня доверия.

Администрирование системы защиты виртуализации осуществляется Заказчиком.

* + 1. **Требования к средствам антивирусной защиты**

Средства антивирусной защиты предоставляются в виде неисключительных (пользовательских) прав на программное обеспечение (30 шт.) и сертифицированного комплекта дистрибутивов для рабочих станций (серверов) под управлением операционных систем семейства Windows и Linux.

Общие требования для средств антивирусной защиты:

Программное средство антивирусной защиты информации включает в себя:

программные средства антивирусной защиты для рабочих станций и серверов Windows;

программные средства антивирусной защиты для рабочих станций и серверов Linux;

Программные средства антивирусной защиты для рабочих станций Windows обеспечивают реализацию следующих функциональных возможностей:

антивирусное сканирования в режиме реального времени и по запросу из контекстного меню объекта;

антивирусное сканирование по расписанию;

антивирусное сканирование подключаемых устройств;

эвристического анализатора, позволяющего распознавать и блокировать ранее неизвестные вредоносные программы;

нейтрализации действий активного заражения;

анализа поведения приложения и производимых им действий в системе для выявления и его вредоносной активности и обнаружения несанкционированных действий;

анализа обращений к общим папкам и файлам для выявления попыток шифрования защищаемых ресурсов доступных по сети;

блокировка действий вредоносных программ, которые используют уязвимости в программном обеспечении в том числе защита памяти системных процессов;

откат действий вредоносного программного обеспечения при лечении, в том числе, восстановление зашифрованных, вредоносными программами, файлов;

ограничения привилегий (запись в реестр, доступ к файлам, папкам и другим процессам, обращение к планировщику задач, доступ к устройствам, изменение прав на объекты и т.д.) для процессов и приложений, динамически обновляемые настраиваемые списки приложений с определением уровня доверия;

облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

антивирусной проверки и лечения файлов в архивах следующих форматов: RAR, ARJ, ZIP, CAB, LHA, JAR, ICE;

защиты электронной почты от вредоносных программ с проверкой входящего и исходящего трафика передающегося по следующим протоколам: IMAP, SMTP, POP3, MAPI, NNTP;

фильтра почтовых вложений с возможностью переименования или удаления заданных типов файлов;

проверку сетевого трафика, поступающего на компьютер пользователя по протоколам HTTPS (SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2), HTTP, FTP, в том числе с помощью эвристического анализа, c возможностью настройки доверенных ресурсов и работой в режиме блокировки или статистики;

блокировку баннеров и всплывающих окон на загружаемых Web-страницах;

распознавания и блокировку фишинговых и небезопасных сайтов;

встроенного сетевого экрана, позволяющего создавать сетевые пакетные правила и сетевые правила для программ, с возможностью категоризации сетевых сегментов;

защиты от сетевых атак с использованием правил сетевого экрана для приложений и портов в вычислительных сетях любого типа;

возможность защиты от сетевых угроз, которые используют уязвимости в ARP-протоколе для подделки MAC-адреса устройства;

контроль сетевых подключений типа сетевой мост, с возможностью блокировки одновременной установки нескольких сетевых подключений;

создания специальных правил, запрещающих или разрешающих установку и/или запуск программ для всех или для определенных групп пользователей (Active Directory или локальных пользователей/групп), компонент должен контролировать приложения как по пути нахождения программы, метаданным, сертификату или его отпечатку, контрольной сумме, так и по заранее заданным категориям приложений, предоставляемым производителем программного обеспечения, компонент должен работать в режиме черного или белого списка, а также в режиме сбора статистики или блокировки;

контроля работы пользователя с внешними устройствами ввода/вывода по типу устройства и/или используемой шине, с возможностью создания списка доверенных устройств по их идентификатору и возможностью предоставления привилегий для использования внешних устройств определенным пользователям из Active Directory;

возможность управления МТР устройствами и настройки правил доступа к устройствам этого типа для всех или для групп пользователей (Active Directory или локальных пользователей/групп), в рамках контроля устройств;

записи в журнал событий о записи и/или удалении файлов на съемных дисках;

контроля работы пользователя с сетью Интернет, в том числе добавления, редактирования категорий, включение явного запрета или разрешения доступа к ресурсам определенного содержания, категории созданной и динамически обновляемой производителем, а также типа информации (аудио, видео и др.), позволять вводить временные интервалы контроля, а также назначать его только определенным пользователям из Active Directory;

защиты от атак типа BadUSB;

запуск специальной задачи для обнаружения уязвимостей в приложениях, установленных на компьютере, с возможностью предоставления отчета по обнаруженным уязвимостям.

защиты от удаленного несанкционированного управления сервисом приложения, а также защита доступа к параметрам приложения с помощью пароля;

установки только выбранных компонентов программного средства антивирусной защиты;

централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления;

запуск задач по расписанию и/или сразу после запуска приложения;

гибкое управление использованием ресурсов компьютера для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

ускорение процесса сканирования за счет пропуска объектов, состояние которых со времени прошлой проверки не изменилось;

возможность проверки целостности антивирусной программы;

возможность добавления исключений из антивирусной проверки по контрольной сумме файл, маске имени/директории или по наличию у файла доверенной цифровой подписи;

наличие у антивируса защищенного хранилища для удаленных зараженных файлов, с возможностью их восстановления;

наличие защищенного хранилища для отчетов о работе антивируса;

возможность включения и выключения графического интерфейса антивируса, а также наличие прощенной версии графического интерфейса, с минимальным набором возможностей;

возможность интеграции с Windows Defender Security Center;

наличие поддержки Antimalware Scan Interface (AMSI);

наличие поддержки Windows Subsystem for Linux (WSL);

возможность защитить паролем восстановление объектов из резервного хранилища;

резидентного антивирусного мониторинга;

облачной защиты от новых угроз, позволяющей приложению в режиме реального времени обращаться к специальным ресурсам производителя, для получения вердикта по запускаемой программе или файлу;

проверку ресурсов доступных по SMB / NFS;

эвристический анализатор, позволяющий более эффективно распознавать и блокировать ранее неизвестные вредоносные программы;

антивирусное сканирование по команде пользователя или администратора и по расписанию;

антивирусную проверка файлов в архивах zip; .7z\*; .7-z; .rar; .iso; .cab; .jar; .bz;.bz2;. tbz;.tbz2; .gz;.tgz; .arj.;

проверку сообщений электронной почты в текстовом формате (Plain text);

наличие механизмов оптимизации проверки файлов (исключения, доверенные процессы, лимит времени проверки, лимит размера проверяемого файла, механизм кеширования информация о проверенных и не измененных после проверки файлов);

защиту файлов в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования;

помещение подозрительных и поврежденных объектов на карантин;

проверку почтовых баз приложений Microsoft Outlook на наличие вредоносных объектов;

возможность перехвата и проверки файловых операций на уровне SAMBA;

управление сетевым экраном операционной системы, с возможностью восстановления исходного состояния правил;

запуск задач по расписанию и/или сразу после загрузки операционной системы;

возможность экспортировать и сохранять отчеты в форматах HTML и CSV;

гибкое управление использованием ресурсов ПК для обеспечения комфортной работы пользователей при выполнении сканирования файлового пространства;

сохранение копии зараженного объекта в резервном хранилище перед лечением и удалением в целях возможного восстановления объекта по требованию, если он представляет информационную ценность;

возможность управления через пользовательский графический интерфейс без root прав;

централизованное управление всеми вышеуказанными компонентами с помощью единой системы управления.

Программный интерфейс всех антивирусных средств, включая средства управления, на русском и английском языке.

Все антивирусные средства, включая средства управления, обладают контекстной справочной системой на русском и английском языке.

Требования по сертификации:

- средство антивирусной защиты должно быть сертифицировано на соответствие требованиям ФСТЭК России «Требования к средствам антивирусной защиты» (ФСТЭК России, 2012) не ниже 2 класса защищенности.

Администрирование средств антивирусной защиты осуществляется Заказчиком.

* + 1. **Требования к средствам доверенной загрузки**

Средство доверенной загрузки должно осуществлять:

- идентификацию и аутентификацию пользователей;

- доверенную загрузку;

- контроль целостности программной и аппаратной среды;

- функции сторожевого таймера;

- ведение журнала регистрации событий

Требования к функциональности:

- идентификация пользователей (должна производиться по отчуждаемому персональному идентификатору, а аутентификация - по вводимому с клавиатуры паролю);

- должна обеспечиваться работа с паролями администратора или пользователя длиной до 127 символов;

- должна иметься возможность задавать имя пользователя длиной до 40 символов;

- СДЗ должно обеспечивать возможность регистрации до 300 пользователей на одном компьютере;

- защита от несанкционированной загрузки нештатной операционной системы (ОС);

СДЗ должно иметь возможность контролировать целостность:

- файлов и физических секторов жесткого диска;

- элементов системного реестра;

- журнала транзакций NTFS и EXT4;

- PCI-устройств;

- структур SMBIOS;

- в комплекте поставки должны быть драйверы платы, которые должны функционировать в среде следующих ОС Windows и ОС Linux имеющихся у заказчика, при этом должна обеспечиваться возможность получения случайных последовательностей с физического датчика случайных чисел платы СДЗ для ПО в ОС;

- поддержка файловых систем NTFS, FAT32, FAT16, EXT4, EXT3, EXT2;

- реализация функции сторожевого таймера посредством воздействия на механизм reset и на питание ЭВМ;

- функционирование журнала событий безопасности и его хранение в энергонезависимой памяти платы СДЗ с возможностью экспорта в виде текстового файла;

Требования по сертификации:

Средство доверенной загрузки должно быть сертифицировано на соответствие требованиям ФСТЭК России «Профиль защиты средств доверенной загрузки уровня платы расширения второго класса защиты ИТ.СДЗ.ПР2.ПЗ» (ФСТЭК России, 2013), «Требования к средствам доверенной загрузки (ФСТЭК России, 2013);

Администрирование средств доверенной загрузки осуществляется Заказчиком.

* + 1. **Требования к средствам защиты от несанкционированного доступа**

Средства защиты от НСД предоставляются в виде универсальных неисключительных прав на использование программного обеспечения (30 шт.) для установки на ПЭВМ под управлением имеющейся у Заказчика операционной системы Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2 Windows Server 2016, CentOS 7.7, CentOS 8.0 и сертифицированных комплектов дистрибутивов (для Windows и Linux).

СЗИ поддерживает 32- и 64-битные версии операционных систем.

Средства защиты от НСД должны осуществлять:

* контроль входа пользователей в систему, в том числе с использованием аппаратных средств защиты;
* разграничение доступа пользователей к защищаемым ресурсам (файлам, каталогам) компьютера;
* разграничение доступа пользователей к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам;
* уничтожение (затирание) содержимого файлов при их удалении;
* очистку освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств);
* контроль целостности ключевых компонентов и объектов файловой системы;
* создание замкнутой программной среды для пользователей;
* межсетевое экранирование сетевого трафика;
* регистрацию событий безопасности в журналах;
* контроль действий пользователей, связанных с доступом к файлам, устройствам и узлам вычислительной сети;
* проведение аудита действий субъектов (пользователей, процессов) с объектами файловой системы и аудита сетевых соединений.

СЗИ должно допускать использование в следующих информационных системах:

* автоматизированные системы - до класса 2Г (включительно);
* государственные информационные системы – до 2 класса защищенности (включительно);
* информационные системы персональных данных – до 2 уровня защищенности (включительно);
* автоматизированные системы управления производственными и технологическими процессами – до 2 класса защищенности (включительно).

СЗИ должно выполнять следующие функции по защите информации:

* контроль входа пользователей в систему как по логину/паролю, так и с использованием аппаратных средств усиленной аутентификации.
* совместное функционирование с программно-аппаратными средствами доверенной загрузки для обеспечения защиты компьютера от несанкционированной загрузки автоматизированной системы с внешних носителей.
* разграничение доступа пользователей к защищаемым ресурсам (файлам, каталогам) компьютера.
* создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера. При этом должны контролироваться исполняемые файлы, файлы загружаемых библиотек, запуск скриптов по технологии. Должна иметься возможность формирования списка исключений для ресурсов, в который входят разрешенные для запуска программы, файлы, библиотеки и скрипты.
* контроль устройств, подключаемых к шинам USB, SATA, IEEE 1394. Контролируемые устройства должны идентифицироваться по следующим параметрам: VendorID, DeviceID, серийный номер, а также у администратора должна быть дополнительная возможность задать для каждого устройства условную символьную метку для его идентификации.
* затирание освобождаемых страниц оперативной памяти, при этом должна быть предусмотрена возможность разбиения больших страниц на более мелкие непосредственно перед очисткой; затирание освобождаемых блоков на файловых системах EXT2, EXT3, EXT4 и VFAT; безопасное удаление информации на жестких дисках и внешних носителях; затирание страниц SWAP при выключении компьютера или перезагрузке операционной системы.

- функциональный самоконтроль средства защиты.

- контроль целостности критических объектов операционной системы и ресурсов файловой системы компьютера, поставленных на контроль администратором. Контроль целостности должен проводиться в автоматическом режиме при загрузке операционной системы. Также администратор должен иметь возможность вручную запустить проверку целостности защищаемых ресурсов.

- поддержка следующих режимов реакции СЗИ на нарушение целостности объектов: только регистрация события безопасности; блокировка АС в случае нарушения безопасности; восстановление из эталонного значения (для файловых объектов) и блокировка АС.

- межсетевое экранирование сетевого трафика на основе формируемых правил фильтрации на сетевом, транспортном и прикладном уровне запросов. Должна осуществляться фильтрация с учетом полей сетевых пакетов, направления трафика, сетевого интерфейса, с учетом расписания.

- регистрация событий безопасности в журнале безопасности, контроль действий пользователей: доступ к защищаемым файлам, устройствам и узлам вычислительной сети; событий вывода файлов на печать.

- аудит действий субъектов с объектами файловой системы и сетевых соединений, аудит отчуждения информации.

- аудит действий администратора при доступе к файловым объектам.

- фильтрация событий безопасности, контекстный поиск в журнале безопасности.

- автоматическое построение отчетов по результатам аудита.

- управление СЗИ: с помощью графического интерфейса и командной строки.

Требования по сертификации:

СЗИ должно соответствовать требованиям руководящих документов:

* «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности,
* «Требования к межсетевым экранам» (ФСТЭК России, 2016) – не ниже 4 класса защиты,
* «Профиль защиты межсетевых экранов типа «В» четвертого класса защиты. ИТ.МЭ.В4.ПЗ» (ФСТЭК России, 2016),
* «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - не ниже 4 уровня доверия.

Администрирование средств защиты информации от несанкционированного доступа осуществляется Заказчиком.

* 1. **Требования к исполнителю**

Исполнитель должен обеспечивать эксплуатацию и техническую поддержку предоставляемой Заказчику выделенной инфраструктуры.

Исполнитель должен назначить выделенного Сервис-Менеджера для оказания услуг по управлению технической поддержкой выделенной инфраструктуры и каналов связи, предоставляемых в рамках оказания услуги. В рамках данной услуги Сервис-Менеджер обязан:

- установить и поддерживать оперативную связь с уполномоченными представителями Заказчика для выполнения условий контракта;

- проводить измерение, отслеживание и оценку уровня услуг, оказываемых в соответствии с уровнями обслуживания;

- обеспечить координацию и управление деятельностью технического персонала, связанного с указанием услуг;

- проводить ежемесячные совещания, путем сеансов конференцсвязи или совещаний на территории Заказчика с целью:

- анализа любых проблем, которые возникают при взаимодействии со службой технической поддержки;

- согласования любых действий по результатам сеанса конференцсвязи или совещания;

- согласования сроков завершения таких действий;

- согласования сроков проведения будущих ежемесячных сеансов конференцсвязи или совещаний и предварительного согласования целей и задач сеансов конференцсвязи/совещаний.

- обеспечить подготовку отчетов в соответствии с условиями требований к документации;

- разработать и предоставить план работ по техническому обслуживанию и сопровождению на период действия договора и отслеживать его выполнение;

- быть осведомленным о запросах приоритета 1, осуществленных со стороны Заказчика в службу технической поддержки Исполнителя и отслеживать последующие действия;

- при необходимости координировать взаимодействие между техническим персоналом Заказчика и соответствующим персоналом Исполнителя.

**Исполнитель должен обладать**

1. Лицензией Роскомнадзора на осуществление деятельности в области оказания услуг связи с местом действия на территории РФ, на которой располагаются Объекты Заказчика, для следующих услуг связи, утверждённых постановлением Правительства РФ от 18.02.2005 № 87 «Об утверждении перечня наименований услуг связи, вносимых в лицензии и перечней лицензионных условий»:

* - Услуги связи по предоставлению каналов связи (п.13 постановления);
* - Услуги связи по передаче данных, за исключением услуг связи по передаче данных для целей передачи голосовой информации (п.14 постановления).

1. Лицензией ФСБ России на разработку, производство, распространение шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, техническое обслуживание 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) согласно Постановлению Правительства РФ от 16 апреля 2012 г. N 313: Предоставление юридическим и физическим лицам защищённых с использованием шифровальных (криптографических) средств каналов связи для передачи информации (п.27 постановления).
   1. **Требования к мониторингу и службе технической поддержки Исполнителя**

Для обеспечения бесперебойного и эффективного оказания услуги Исполнитель должен организовать функционирование службы технической поддержки.

Служба технической поддержки Исполнителя должна иметь утвержденный порядок управления инцидентами, в том числе и инцидентами информационной безопасности.

Служба технической поддержки Исполнителя должна быть доступна для обращения специалистов Ответственных лиц Заказчика круглосуточно без перерывов 24 (Двадцать четыре) часа в сутки, 7 (Семь) дней в неделю, 365 дней в году.

Заказчик должен иметь самостоятельную возможность получения информации об объеме используемых ресурсов.

Исполнитель предоставляет выделенный телефонный номер для регистрации заявок.

Предоставленная телефонная линия и доступ в веб-порталу должны быть доступны в формате 24х7х365.

В ЦОД, используемом Исполнителем для оказания Услуги должна функционировать собственная диспетчерская служба, контролирующая в круглосуточном режиме работу оборудования основных инженерных систем, систем жизнеобеспечения, режимы их работы, возникновения аварийных ситуаций, температурно-влажностные режимы технологических помещений, осуществляет сбор информации и отображение текущего состояния инженерных систем в режиме реального времени, хранение исторических данных, возможности их отображения и анализа.

Наличие у Исполнителя формализованных и функционирующих процессов управления инцидентами и изменениями в соответствии с методологией ITIL/ITSM.

Время реакции на инциденты должно быть гарантированным и указываться в SLA.

Служба технической поддержки Исполнителя должна информировать представителей Заказчика о проведении плановых/технологических работ, а также о возникших инцидентах и ходе работ по их устранению.

Взаимодействие Заказчика и Исполнителя должно осуществляться в рамках потребления и оказания Услуг через централизованную службу поддержки Исполнителя в соответствии с правилами взаимодействия Исполнителя и Заказчика.

Правила взаимодействия Исполнителя и Заказчика должны содержать:

* + описание способов взаимодействия со службой технической поддержки;
  + описание классификаций обращений и определение приоритетов;
  + описание требований к заполнению обращений;
  + описание статусов обращений.

Все поступающие обращения контактных лиц Заказчика должны регистрироваться в системе учета и обработки обращений Заказчика, при этом каждому обращению должен присваиваться уникальный номер, который в дальнейшем помогает идентифицировать обращение. При регистрации обращения и при изменении его статуса, контактное лицо Заказчика автоматически информируется системой посредством отправки электронных писем на адрес, указанный при регистрации контактного лица Заказчика.

Обращения должны получать приоритеты в зависимости от установленного значения срочности и влияния на бизнес-процессы.

Обращения категории «Инцидент» должны получать приоритеты в зависимости от установленного значения срочности и влияния на бизнес-процессы согласно модели, описанной в SLA.

* 1. **Требования к соглашению об уровне обслуживания (service level agreement)**

Услуга по предоставлению выделенной инфраструктуры и каналов связи в ЦОД Исполнителя должна оказываться в режиме «24х7х365» - 24 часа в сутки, 7 дней в неделю, 365 дней в году.

**Требования к параметрам оказываемой услуги:**

**- Время оказания и показатели доступности услуг.**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Услуга** | **Время предоставления** | **Уровень доступности** |
| 1. | Предоставление выделенной инфраструктуры в центре обработки данных Исполнителя | 24х7х365 - 24 часа в сутки, 7 дней в неделю, 365 дней в году | 99,982% |

**- Параметры услуги – Предоставление выделенной инфраструктуры в центре обработки данных Исполнителя.**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Метрика** | **Допустимое значение** | **Измерение** |
| 1. | Время доступа к SATA-диску на виртуальной машине | не более 30 мс при интенсивности ввода-вывода 100 IOPS/TB, но не более 3 500 IOPS | Среднее значение на интервале 20 минут по данным интерфейса управления СХД. Размер блока 4 KB, отношение количества операций чтение/запись 70/30 |
| 2. | Время доступа к SAS-диску на виртуальной машине | не более 20 мс при интенсивности ввода-вывода 200 IOPS/TB, но не более 7 000 IOPS | Среднее значение на интервале 20 минут по данным интерфейса управления СХД. Размер блока 4 KB, отношение количества операций чтение/запись 70/30 |
| 3. | Время доступа к SSD-диску на виртуальной машине | Не более 3 мс при интенсивности ввода-вывода 2 000 IOPS/TB, но не более 15 000 IOPS или 800 MB/s. | Среднее значение на интервале 20 минут по данным интерфейса управления СХД. Размер блока 4 KB, отношение количества операций чтение/запись 70/30 |
| 4. | CPU Ready | До 10%. | Среднее значение по всем ядрам, система мониторинга Исполнителя |
| 5. | RAM Swapped процент от сконфигурированной памяти VM | До 10% | Система мониторинга Исполнителя |

**- Устранение инцидентов. Приоритеты инцидентов.**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Приоритет инцидента** | **Описание** |
| Инцидент – неисправность, сбой в работе оборудования или ПО, иное событие, повлекшее ухудшение зафиксированного в SLA качества или полное / частичное прекращение предоставляемой Исполнителем услуги. | | |
| 1 | Приоритет 1 | Не доступна виртуальная машина на уровне программно-аппаратного комплекса Исполнителя |
| RAM Swapped процент от сконфигурированной памяти виртуальной машины свыше 30% |
| HDD IOPS уменьшение на 50% и более от оговоренных значений |
| Среднее время отклика SSD-диска на виртуальной машине от 10мс до 20мс |
| Среднее время отклика SAS-диска на виртуальной машине свыше 100мс |
| Среднее время отклика SATA-диска на виртуальной машине свыше 120мс |
| Процент потерянных пакетов в пределах СПД Исполнителя более 1% |
| Средняя сетевая задержка в пределах СПД Исполнителя более 20мс |
| 2 | Приоритет 2 | Отсутствие доступа к интерфейсу управления виртуальными машинами более 2 часов |
| RAM Swapped процент от сконфигурированной памяти виртуальной машины 20% - 30% |
| HDD IOPS уменьшение от 20% до 50% от оговоренных значений |
| Среднее время отклика SSD-диска на виртуальной машине от 5мс до 10мс |
| Среднее время отклика SAS-диска на виртуальной машине 40-80мс |
| Среднее время отклика SATA-диска на виртуальной машине 50-100мс |
| Процент потерянных пакетов в пределах сети передачи данных Исполнителя от 0,4% до 1% |
| Средняя сетевая задержка в пределах сети передачи данных Исполнителя от 5мс до 20мс |
| 3 | Приоритет 3 | RAM Swapped процент от сконфигурированной памяти виртуальной машины 10% - 20% |
| HDD IOPS уменьшение от 10% до 20% от оговоренных значений |
| Среднее время отклика SSD-диска на виртуальной машине от 3мс до 5мс |
| Среднее время отклика SAS-диска на виртуальной машине от 20мс до 40мс |
| Среднее время отклика SATA-диска на виртуальной машине от 30мс до 50мс |
| Процент потерянных пакетов в пределах сети передачи данных Исполнителя от 0,2% до 0,4% |

**- Решение инцидентов.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Приоритет инцидента** | **Обработка** | **Время реакции на инцидент, минут\*** | **Максимальное время решения инцидента, минут\*\*** | **Суммарное время решения инцидентов в месяц, не более, минут** |
| 1. | 1 | Круглосуточно | 5 | 120 | 120 |
| 2. | 2 | Круглосуточно | 5 | 160 | 320 |
| 3. | 3 | Круглосуточно | 5 | 310 | 930 |

*\*Принятие и регистрация обращения, классификация и приоритизация. Заказчик уведомляется соответствующим электронным письмом.*

*\*\*Время решения инцидента начинает считаться с момента уведомления Заказчика о его регистрации и присвоении идентификационного номера до момента его решения.*

- **Обработка запросов пользователей. Классификация и приоритеты запросов**.

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Классификация** | **Приоритет** | **Описание** |
| 1. | Запрос на обслуживание | 4 | Зафиксированная потребность Заказчика в обслуживании в рамках предоставляемых ему услуг (определённых в SLA или описанных в спецификации для Заказчика) или компонент, их образующих, не связанное со сбоем или отказом в IT-инфраструктуре. |
| 2. | Запрос на изменение | 5 | Запрос, приводящий к изменению состава и/или объема услуг, определённых в SLA или описанных в спецификации для Заказчика. |
| 3. | Запрос на предоставление информации | 6 | Запрос на предоставление информации по услуге, включая отчёты по объёму трафика, сервисные отчёты, отчёты по мониторингу и т.д. |

**- Обработка запросов.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Категория** | **Приоритет** | **Обработка** | **Время реакции на запрос, минут\*** | **Максимальное время решения запроса, не более часов\*\*** |
| 1. | Запрос на обслуживание | 4 | В рабочие часы\*\*\* | 20 | 12 |
| 2. | Запрос на изменение | 5 | В рабочие часы | 20 | 16\*\*\*\* |
| 3. | Запрос на предоставление информации | 6 | В рабочие часы | 20 | 72 |

*\*Принятие и регистрация обращения, классификация и приоритизация. Заказчик уведомляется соответствующим электронным письмом.*

*\*\*Время решения обращения начинает считаться с момента уведомления Заказчика о его регистрации и присвоении идентификационного номера до момента его решения.*

*\*\*\*В рабочие часы Заказчика: рабочие дни РФ с 9.00 до 18.00.*

*\*\*\*\*Время решения запроса на изменение сводится к времени расценки работ и материалов, необходимых для проведения изменений, а также ознакомлению Заказчика со сроками проводимых изменений.*

**- Проведение регламентных работ.**

| **№ п/п** | **Позиция** | **Показатели** | **Уведомление  Заказчика** | **Дополнительные условия** |
| --- | --- | --- | --- | --- |
| 1. | Проведение технологических работ | Суммарная продолжительность перерывов в работе услуги – не более 1,6 часов в год. Интервалы между перерывами – не менее 30 календарных дней. | Не менее чем за 5 календарных дня до начала перерыва | Время проведения работ согласовывается с Заказчиком |
| 2. | Проведение экстренного обновления, связанного с установкой выпускаемых производителем обновлений (upgrades) и\или корректирующих заплаток (patches) имеющих критическое значение для работоспособности, производительности, безопасности ПО | Время перерыва равно фактическому времени установки обновлений (upgrades), корректирующих заплаток (patches) и тестирования | Непосредственно перед началом работ | Предполагаемая продолжительность проведения работ сообщается Заказчику |

**- Типовые обращения/инциденты и их классификация**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **Категория запроса** | **Описание** | **Условия** | **Приоритет** |
| 1. | Запрос на обслуживание | Восстановление ВМ | восстановление ВМ из резервной копии. | 4 |
| 2. | Запрос на обслуживание | Установка ОС | Развертывание образа на виртуальную машину (установка ОС) | 4 |
| 3. | Запрос на обслуживание | Изменение настоек сети | Настройка сетевой связанности, изменение параметров сети BM (IP, VPN, VLAN) | 4 |
| 4. | Запрос на обслуживание | Перемещение ВМ | Обслуживание по запросу заказчика. Операции по миграции ВМ, либо ее HDD. | 4 |
| 5. | Запрос на изменение | Изменение объектов обслуживания | Добавление или изъятие объектов обслуживания (расширить виртуальные машины, расширить параметры ВМ, новая ВМ) | 5 |
| 6. | Запрос на изменение | Изменение условий обслуживания | Изменение параметров SLA, контактных лиц со стороны Заказчика, изменение взаимодействий. | 5 |
| 7. | Запрос на предоставление информации | Предоставление отчета | Формирование внеочередного отчета с дополнительными критериями оценки | 6 |
| 8. | Запрос на предоставление информации | Предоставление отчета | Предоставление дополнительной информации о структуре дополнительных услуг и их стоимости. | 6 |

* 1. **Требования к объему вычислительных ресурсов и ресурсов хранения данных**

Общее количество ресурсов, предоставляемое в рамках оказания услуги, должно быть в объёме не менее:

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Наименование** | **Ед. изм.** | **Кол-во** |
| 1. | vCPU | Шт. | 627 |
| 2. | vRAM | ГБ | 1 950 |
| 3. | HDD SSD Тип 1 | ГБ | 109 000 |
| 4. | HDD SATA Тип 2 | ГБ | 100 000 |
| 5. | Дисковое пространство для резервного копирования ВМ | ГБ | 270 000 |
| 6. | Юнит в закрытом контуре приватного облака для размещения оборудования заказчика | Шт. | 4 |

|  |  |
| --- | --- |
| Заказчик: | Поставщик: |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ С.С. Цукарь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

МП (при наличии) МП (при наличии)

Приложение № 2 к Контракту

от «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ г. №\_\_\_\_

**ГРАФИК ИСПОЛНЕНИЯ ЭТАПОВ ПО КОНТРАКТУ**

|  |  |
| --- | --- |
| Наименование этапа | Срок исполнения этапов Контракта |
| Этап 1 | С 05.09.2022 по 16.09.2022 (включительно) |
| Этап 2 | С 10.09.2022 по 30.09.2022 (включительно) |
| Этап 3 | С 10.09.2022 по 07.10.2022 (включительно) |
| Этап 4 | С 01.10.2022 по 22.12.2022 (включительно) |
| Этап 5 | С 16.12.2022 по 07.04.2023 (включительно) |
| Этап 6 | С 01.04.2023 по 07.07.2023 (включительно) |
| Этап 7 | С 01.07.2023 по 06.10.2023 (включительно) |
| Этап 8 | С 01.10.2023 по 07.12.2023 (включительно) |

Заказчик Исполнитель

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ С.С. Цукарь \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г. «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

МП (при наличии) МП (при наличии)