**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

На оказание услуг по размещению ИТ-инфраструктуры в коммерческом центре обработки данных для нужд АО «Российская Национальная Перестраховочная Компания»

Данные документ описывает требования к параметрам оказания услуги и условиям, необходимым для организации её предоставления конечным Исполнителем с целью размещения виртуальных машин, резервных копий и физического сетевого оборудования АО РНПК.

**Оглавление**

[**1.** **Термины и определения** 4](#_Toc174470964)

[**2.** **Общие сведения** 4](#_Toc174470965)

[**3.** **Цели и задачи оказания услуг** 5](#_Toc174470966)

[**4.** **Требования к Исполнителю** 6](#_Toc174470967)

[**5.** **Требования к составу услуг** 6](#_Toc174470968)

[**6.** **Требования к миграции** 6](#_Toc174470969)

[**7.** **Требования к технической поддержке** 6](#_Toc174470970)

[**Приложение А. Требования к физической инфраструктуре ЦОД.** 7](#_Toc174470971)

[**Приложение Б. Требования к обеспечению вычислительными ресурсами.** 14](#_Toc174470972)

[**Приложение В. Необходимый набор сервисов и услуг.** 17](#_Toc174470973)

[**Приложение Г. Принципиальная схема ИТ-инфраструктуры Заказчика.** 21](#_Toc174470974)

[**Приложение Д. Соглашение об уровне оказания услуг.** 22](#_Toc174470975)

[**Приложение Е. Перечень виртуальных машин с указанием параметров.** 27](#_Toc174470976)

[**Приложение Ж. Требования к информационной безопасности.** 37](#_Toc174470977)

# **Термины и определения**

**«Заказчик»** – АО «Российская Национальная Перестраховочная Компания», АО РНПК.

**«Услуга»** – комплекс работ и услуг коммерческого ЦОД в рамках которых Исполнитель предоставляет Заказчику пул вычислительных мощностей с соответствующими техническими характеристиками, дисковое пространство, систему резервного копирования, систему передачи резервных копий на удалённую площадку, возможность для размещения оборудования Заказчика в стойках ЦОД, линии и каналы связи и иные цифровые и телекоммуникационные услуги по модели IaaS.

**«КЦОД»** – коммерческий центр обработки данных, выступающий в роли основного центра обработки данных Заказчика.

**«Оператор КЦОД»** – юридическое лицо, осуществляющее эксплуатацию физической и программной инфраструктуры ЦОД и осуществляющее оказание сопутствующих услуг.

**«Виртуализация»** – процесс предоставления вычислительных ресурсов Исполнителя, которые могут работать в изолированной друг от друга среде без привязки к конкретным физическим ресурсам.

**«Виртуальная память»** – энергозависимая часть компьютерной памяти, в которой временно хранятся данные и команды, необходимые процессору для выполнения им операции, имеющая возможность работать в изолированной друг от друга среде.

**«Виртуальный диск»** – совокупность ресурсов хранения данных Заказчика, имеющих возможность работать в изолированной друг от друга среде.

**«Виртуальная сеть, VLAN»** – непубличная сеть передачи данных между Виртуальными машинами Заказчика, построенная по протоколу IP (межсетевой протокол передачи данных).

**«VXLAN»** – Virtual Extensible LAN, виртуальная расширяемая локальная сеть.

**«IaaS»** – Infrastructure as a service, инфраструктура как сервис/услуга.

**«PAYG»** – pay as you go, оплата по мере использования.

**«РЦОД»** –резервный центр обработки данных Заказчика.

**«Виртуальная машина, ВМ, VM»** – размещенная на инфраструктуре Заказчика изолированная программно-аппаратная система (совокупность ресурсов Виртуальных процессоров, Виртуальной памяти, пространства Виртуального диска), эмулирующая аппаратное обеспечение и предназначенная для работы под управлением операционной системы Заказчика.

**«МСЭ»** – межсетевой экран.

**«СКС»** – структурированная кабельная сеть.

**«ЛВС»** – локальная вычислительная сеть.

**«СРК»** – система резервного копирования.

**«Техническая поддержка»** – оказание Исполнителем устных и письменных консультаций по вопросам оказания Услуги, а также устранение Инцидентов, возникающих в зоне ответственности Исполнителя в связи с оказанием Услуги.

**«Инцидент»** – любая совокупность обстоятельств, которая привела к невозможности оказания Услуги с заявленными характеристиками, сбой в работе оборудования или ПО, повлекшее ухудшение зафиксированного в SLA качества или полное / частичное прекращение предоставляемого Исполнителем сервиса.

**«Сервисный запрос»** – обращение Заказчика к Исполнителю на обслуживание / предоставление информации, на изменение отдельных параметров Услуги.

**«Запрос на изменение»** – обращение, приводящее к изменению состава и/или объема услуг, определённых в SLA или описанных в спецификации для Заказчика.

**«Запрос на предоставление информации»** – обращение, ориентированное на предоставление информации по услуге, включая отчёты по объёму трафика, сервисные отчёты, отчёты по мониторингу и т.д.

**«Технические работы»** – Аварийные и Плановые регламентные работы.

**«Влияние»** – степень воздействия Инцидента, описывающая влияние на бизнес-процессы Заказчика.

**«Время регистрации»** – параметр, определяющий скорость регистрации заявки от Заказчика в службе поддержки, вне зависимости от способа её поступления.

**«Время реакции»** – параметр, определяющий скорость назначения специалиста службы поддержки на поступившее обращение от конечного Заказчика;

**«Срочность»** – показатель, определяющий предел по времени, по истечении которого Инцидент способен оказать критичное влияние на бизнес-процессы Заказчика;

# **Общие сведения**

Заказчиком услуги является Акционерное Общество Российская Национальная Перестраховочная Компания (АО РНПК), адрес: 125047, г. Москва, ул. Гашека, дом 6 (далее по тексту Заказчик).

Функции представителя Заказчика выполняет Департамент информационных технологий и Управление внутренней и информационной безопасности АО РНПК.

Исполнитель оказания услуги выбирается в соответствии с закупочными процедурами АО РНПК.

Основанием для оказания услуг является текущее техническое задание.

Список технологических площадок Заказчика перечислен в Таблице 1.

Таблица 1. Адреса технологических площадок Заказчика.

| № | Наименование площадки | Адрес |
| --- | --- | --- |
| 1 | Основной ЦОД (текущий) | г. Москва, 1-й Дорожный проезд, дом 3 строение 2 |
| 2 | Резервный ЦОД | г. Москва, Коровинское шоссе, дом 41 |
| 3 | Офис | г. Москва, ул. Гашека, дом 6 |

# **Цели и задачи оказания услуг**

Целью оказания услуги является размещение ИТ инфраструктуры Заказчика по модели IaaS в катастрофоустойчивом исполнении с набором необходимых дополнительных услуг.

Указанная цель достигается путем реализации следующих задач:

* Предоставление пула вычислительных мощностей и дискового пространства с моделью оплаты PAYG;
* Предоставление системы резервного копирования и дискового хранилища для неё;
* Обеспечение возможности сетевой связанности с площадками Заказчика;
* Предоставление отказоустойчивого защищённого доступа в сеть Интернет;
* Размещение оборудования Заказчика в машинных залах КЦОД;
* Предоставление услуги по передаче файлов резервных копий на площадку РЦОД для обеспечения непрерывности бизнес-деятельности («Резервное копирование в облако»);
* Обеспечение защиты ИТ-инфраструктуры Заказчика;
* Предоставление технической поддержки в режиме 24\*7\*365
* Предоставление сопутствующих услуг;
* Сопровождение выделенным сервис-менеджером;

# **Требования к Исполнителю**

Предъявляемые требования заключены в следующих приложениях к настоящему техническому заданию:

* Приложение А – Требования к физической инфраструктуре ЦОД;
* Приложение Б – требования к обеспечению вычислительными ресурсами;
* Приложение Ж – требования к информационной безопасности;

# **Требования к составу услуг**

Предъявляемые требования заключены в следующих приложениях к настоящему техническому заданию:

* Приложение В – необходимый набор сервисов и услуг;
* Приложение Г – принципиальная схема организации ИТ-инфраструктуры;
* Приложение Е – перечень виртуальных машин Заказчика с указанием их параметров;

# **Требования к миграции**

При необходимости миграции из текущего ЦОД Исполнитель обязуется выполнить следующие задачи:

* На этапе формирования коммерческого предложения изучить настоящее техническое задание, произвести стоимостную оценку такой миграции и обозначить её сроки;
* Предъявить Заказчику в коммерческом предложении команду специалистов, которые будут осуществлять миграцию, и календарный план с указанием основных этапов выполнения проекта;
* После заключения договора назначить руководителя проекта по миграции, разработать декомпозированный календарный план и назначить ответственных за технологические операции;
* Разработать комплект документации согласно ГОСТ 34 в составе:
  + Отчёт о проведённом исследовании ИТ-инфраструктуры Заказчика;
  + Частное техническое задание на проведение работ по миграции;
  + Пояснительная записка, к эскизному, техническому проектам;
  + Схема функциональной структуры;
  + Программа и методика испытаний;
  + Описание комплекса технических средств;
  + Описание программного обеспечения;
  + Схема структурная комплекса технических средств;
  + Спецификация(ии) оборудования и программных продуктов;
  + Форма протокола проведения испытаний;
  + Ведомость технического проекта;
* Выполнить миграцию;
* В процессе миграции Исполнитель берёт на себя обязательства по отчуждению резервных копий у текущего КЦОД в размере 200 Tb и перемещения их в репозиторий своей площадки;
* Обеспечение всех необходимых ресурсов для выполнения миграции (оборудование, программное обеспечение, лицензии, услуги связи, работники) выполняется исключительно за счёт Исполнителя;
* При выполнении проекта миграции **допускается**:
  + Одновременная работа двух площадок (текущей и целевой);
  + Миграция некритичных ИТ-сервисов и виртуальных машин в рабочее время;
* При выполнении проекта миграции **не допускается**:
  + Простой в работе любых информационных-систем и компонент Заказчика;
  + Миграция информационных систем средней и высокой критичности в рабочее время;
  + Создание аварийных и нештатных ситуаций в момент внесения изменений в текущую инфраструктуру;

# **Требования к технической поддержке**

В рамках оказания услуг Исполнитель предоставляет техническую поддержку, администрирование и мониторинг систем ЦОДа в режиме 24\*7\*365. Исполнитель должен предоставить дату начала исполнения SLA (соглашения об уровне сервиса). SLA должен быть привязан к доступности среды, времени разрешения критичных инцидентов, времени расследования проблемы, а также временным параметрам процессов управления изменениями. SLA должно охватывать все компоненты предлагаемого решения.

Детали и параметры оказания технической поддержки зафиксированы в Приложении Д.

# **Приложение А. Требования к физической инфраструктуре ЦОД.**

1. **Общие требования к зданию КЦОД Исполнителя**
   1. Здание КЦОД Исполнителя должно располагаться в пределах Центрального федерального округа РФ.
   2. Технологическая площадка КЦОД Исполнителя должна располагаться в выделенных помещениях отдельно стоящего капитального строения с прилегающей к нему огороженной и охраняемой территорией.
   3. На технологической площадке не должно находиться имущество и оборудование и располагаться персонал или организации, не связанные с функционированием КЦОД Исполнителя.
   4. Должна предоставляться возможность круглосуточного доступа в КЦОД Исполнителя для прохода и завоза оборудования;
   5. Стены машинных залов КЦОД Исполнителя не должны соприкасаться с наружными стенами здания;
   6. В здании КЦОД Исполнителя должна быть организована зона погрузки/разгрузки оборудования. В случае размещения КЦОД Исполнителя не на первом этаже здания для подъема оборудования должен быть предусмотрен лифт.
   7. Не допускается наличие окон на наружных стенах в машинном зале;
   8. Не допускается расположение машинного зала в подвале;
   9. Нагрузочная способность на перекрытия - не менее 1200 кг на квадратный метр;
   10. Электроснабжение монтажным стойкам по территории машинного зала должен быть выполнен по потолочным лоткам над стойками с оборудованием по независимым маршрутам.
   11. Слаботочная кабельная система в машинном зале должна проходить в потолочных лотках над монтажными стойкам с активным оборудованием
   12. Магистральные трубы системы кондиционирования должны находиться в выделенных помещениях, отдельно от машинного зала с активным оборудованием, отдельно от электрощитов подачи электропитания;
   13. В машинных залах КЦОД Исполнителя должны отсутствовать трубы тепло- и водоснабжения, канализации;
2. **Требования к надежности КЦОД Исполнителя**

В КЦОД Исполнителя должны присутствовать:

* 1. промышленная система кондиционирования и вентиляции (согласно СНиП 2.04.05-86);
  2. система автоматического пожаротушения (согласно ГОСТ 12.1.004-76.ССБТ);
  3. электростатическая защита помещения (обычно полы с антистатическим покрытием, согласно ГОСТ 12.4.124-83, СН-2152-80 и СанПиН-2.2.2.542-96);
  4. Должно быть организовано круглосуточное дежурство высококвалифицированных инженеров и администраторов сети, обслуживающих инженерные системы КЦОД Исполнителя не менее двух в смену и имеющих аттестацию по электробезопасности необходимой категории.
  5. Уровень доступности КЦОД Исполнителя должен быть не менее 99,982%.

1. **Требования к телекоммуникационным ресурсам**
   1. Подтвердить факт открытости для присутствия провайдеров на площадке КЦОД Исполнителя, предоставить перечень провайдеров, которые уже предоставляют свои услуги;
   2. Исполнитель должен быть готов по требованию Заказчика предоставлять услуги связи на территории КЦОД Исполнителя;
   3. Наличие не менее 2-х независимых оптоволоконных каналов связи с московскими коммутационными центрами ММТС 9 и ММТС 10;
   4. Подтвердить возможность оказания телекоммуникационных услуг.
2. **Требования к электроснабжению**
   1. Отсутствие единой кнопки экстренного отключения электропитания ИТ нагрузки;
   2. Для системы бесперебойного электроснабжения (СБЭ) должно быть предусмотрено питание в нормальном режиме от двух независимых вводов из разных городских подстанций с устройством АВР, а при отсутствии напряжения на внешних вводах от системы гарантированного электроснабжении (СГЭ);
   3. Электропитание оборудования КЦОД Исполнителя должно быть выполнено от ИБП, построенного по системе резервирования 2N. Все энергетические системы (трансформаторы и т.п.) должны располагаться в отдельных помещениях, оборудованных системой пожаротушения, сигналы с которой выведены на пульт дежурной смены с круглосуточным режимом работы здания КЦОД Исполнителя.;
   4. Наличие действующего договора на обслуживание ИБП и ДГУ;
   5. ДГУ должны быть зарезервированы по схеме, как минимум N+1;
   6. Группа ДГУ должна:
   7. постоянно находиться в режиме ожидания и принимать всю рабочую нагрузку в течение 5 минут с момента отключения питания на внешних вводах;
   8. быть обеспечена запасом дизельного топлива с резервированием (не менее двух ёмкостей и независимых путей подвода топлива к ДГУ от каждой ёмкости);
   9. быть обеспечена запасом топлива на срок не менее 72 часов работы при полной нагрузке с возможностью дозаправки без прерывания работы, с учетом неприкосновенности резервного запаса топлива в резервной ёмкости.
   10. Мощность СГЭ должны иметь возможность выполнения роли основного источника питания.
   11. Емкости с топливом, объемом свыше 1м³, не должны располагаться в одном здании с КЦОД Исполнителя;
   12. Емкости батарей ИБП должно быть достаточно для двукратного переключения на ДГУ с учетом дополнительного запаса 5 минут, но не менее 15 минут;
   13. Исполнитель должен иметь действующий договор на поставку сезонного топлива в течении 5 часов с момента заказа.
   14. Оборудование Заказчиков должно быть обеспечено бесперебойным питанием от двух линий, каждая из которых оснащена выделенным ИБП, рассчитанным на полную мощность подключаемого оборудования;
   15. Электроснабжение каждой стойки в машинном зале должно осуществляться по двум независимым линиям, питающимся от разных трансформаторов и независимых групп ИБП.
3. **Требования к кондиционированию.**
   1. Наличие системы прецизионного кондиционирования с уровнем резервирования не ниже N+1.
   2. Система кондиционирования должна быть подключена к системе гарантированного электроснабжения, с разделением питающей сети серверного и холодильного оборудования во избежание наведения электрических помех от электромоторов в цепях питания серверов.
   3. Защита объема машинного зала от возможного вредного воздействия компонентов хладоносителя (фреоны, гликоли и т.п.) в случае разгерметизации системы кондиционирования.
   4. Охлаждение оборудования должно осуществляться через отверстия в фальшполе, удаление горячего воздуха из машинного зала должно осуществляться через объем за пространством фальшпотолка, либо с помощью других методов изоляции холодных и горячих потоков воздуха, гарантирующих отсутствие перемешивания воздуха между холодным и горячим коридорами. Должны быть организованы холодный и горячий коридоры.

КЦОД Исполнителя должен быть оборудован системой кондиционирования, способной обеспечить:

* 1. температурный режим эксплуатации оборудования от +20 до +24 градусов Цельсия, скорость изменения температуры не более 5° в час (замеры температуры производятся при включенном оборудовании на высоте 1,5м с фронтальной стороны аппаратных шкафов в различных точках аппаратного зала)
  2. режим относительной влажности воздуха от 30 % до 60 % (замеры влажности производятся при включенном оборудовании на высоте 1,5м с фронтальной стороны аппаратных шкафов в различных точках аппаратного зала).
  3. Система кондиционирования должна обеспечивать работоспособность с резервированием при температуре наружного воздуха до +39 градусов Цельсия.
  4. При пропадании внешнего питания, обеспечивать непрерывную подачу холодного воздуха в машинном зале.
  5. Данные температурно-влажностного режима помещений КЦОД Исполнителя должны быть выведены в диспетчерскую службу здания КЦОД Исполнителя для возможности круглосуточного контроля параметров.

1. **Требования к системе пожаротушения.**
   1. Наличие автоматической системы газового пожаротушения, с использованием разрешенного к применению огнетушащего вещества, со световой и звуковой сигнализацией;
   2. Газообразный агент не должен оказывать негативного влияния на электронное оборудование после срабатывания системы.
   3. Система газового пожаротушения должна соответствовать действующим НПБ РФ.
   4. Система газового пожаротушения должна быть обеспечена гарантированным электропитанием по первой категории электроснабжения.
   5. Наличие в машинном зале датчиков раннего обнаружения задымления (газоанализаторов);
   6. Выпуск ОТВ в машинных залах и технологических помещениях (например, помещениях с ИБП) должно осуществляться секторно.
   7. Срабатывание системы пожаротушения не должно выводить из строя размещенное и не поврежденное пожаром оборудование.
   8. Аспирационная система пожарной сигнализации - система пожарной сигнализации с активным забором воздуха из зоны горячего коридора машинного зала и фильтром предварительной очистки анализируемого воздуха.
   9. Количество расчетных пожаров - не менее двух. Система пожаротушения должна обеспечивать возможность тушения любого защищаемого объема два раза подряд без необходимости промежуточного обслуживания и дозаправки.
2. **Требования к физической безопасности и контролю доступа.**
   1. Круглосуточный пропускной режим с организацией контрольно-пропускного пункта при входе в КЦОД Исполнителя и предоставлением доступа ограниченного числа лиц из числа эксплуатационного персонала ЦОД и уполномоченных представителей заказчиков;
   2. Система безопасности и автоматизированного контроля доступа с хранением истории доступа не менее 90 суток;
   3. Круглосуточно охраняемые помещения и охраняемую территорию, на которой находится КЦОД Исполнителя и обеспечивающие системы (РТП, ДГУ);
   4. Система видеонаблюдения снаружи и внутри (с полным покрытием входов/выходов, а также межрядного пространства машинного зала) КЦОД Исполнителя с хранением информации с камер не менее 6 месяцев;
   5. Система разграничения физического доступа в технологические помещения КЦОД Исполнителя на базе идентификации (магнитного пропуска)
   6. Контроль доступа со стороны персонала охраны и дежурной смены, регламент доступа;
   7. Не менее 3 периметров контроля доступа к оборудованию Заказчика с размещением физического оборудования Заказчика в выделенной стойке, закрывающейся на ключ, оборудованной сигнализацией и видеонаблюдением;
   8. охраняемый периметр территории здания размещения КЦОД Исполнителя;
   9. охраняемое здание КЦОД Исполнителя;
   10. ограничение доступа в помещения с инженерными системам КЦОД, с АРМами управления КЦОД, и в машинные залы КЦОД Исполнителя.
   11. В КЦОД Исполнителя должна быть реализована схема зонирования по типам подсистем для исключения или минимизации доступа инженерных служб в машинный зал Электрощитовые, кондиционеры, прочие инженерные подсистемы КЦОД Исполнителя должны быть вынесены в отдельные (от машинного зала) помещения КЦОД Исполнителя. Доступ в помещения КЦОД Исполнителя должен обеспечиваться системой контроля и управления доступом с идентификацией по картам-пропускам и двухфакторной аутентификацией.
   12. Физический доступ уполномоченных представителей Заказчика к расположенному в КЦОД Исполнителя физическому оборудованию Заказчика должен предоставляться круглосуточно (в режиме 24/7/365) на основании заранее утвержденных списков и принятого в КЦОД Исполнителя регламента без взимания платы.
   13. Логический доступ персонала КЦОД к системам управления виртуальными машинами, к гипервизорам, удаленным консолям управления оборудованием, СХД и АСО, должен осуществляться через систему управления привилегированными пользователями (PAM), с видеорегистрацией всех управляющих воздействий со стороны персонала.
   14. В организации, эксплуатирующей КЦОД Исполнителя должен быть введён режим коммерческой тайны в соответствии с законодательством РФ. Информационные ресурсы Заказчика, должны быть включены в Перечень защищаемой конфиденциальной информации организации, эксплуатирующей КЦОД. Со стороны организации, эксплуатирующей КЦОД, должна осуществляться охрана конфиденциальности информационных ресурсов Заказчика, как информация, составляющей коммерческую тайну организации КЦОД. Организация, эксплуатирующая КЦОД, должна соблюдать условия неразглашения информации, содержащейся в информационных ресурсах Заказчика
3. **Требования к техническому обслуживанию и поддержке**
   1. Исполнитель обязан обеспечить круглосуточный мониторинг систем обеспечения КЦОД Исполнителя (инженерных систем).
   2. Здание, в котором расположен КЦОД Исполнителя, должно быть оснащено автоматизированной системой диспетчеризации и управления.
   3. Исполнитель должен иметь в КЦОД Исполнителя диспетчерскую службу, контролирующую в круглосуточным режиме 24/7 работу оборудования основных инженерных систем, систем жизнеобеспечения, режимов их работы, возникновения аварийных ситуаций, температурно-влажностные режимы технологических помещений, факты возникновения аварийных ситуаций, осуществлять сбор информации и отображение текущего состояния инженерных систем КЦОД Исполнителя в режиме реального времени, хранение исторических данных, возможности их отображения и анализа (отчеты, графики, тренды) на АРМ диспетчера.
   4. Для обработки заявок (в том числе о недоступности услуг и/или существенном ухудшении качества предоставления услуг) должна функционировать Служба технической поддержки Исполнителя.
   5. Представители Заказчика могут отправлять заявки, контролировать ход исполнения заявок, для чего контактируют со Службой технической поддержки Исполнителя.

Исполнитель должен обеспечить присутствие дежурного инженера в КЦОД Исполнителя круглосуточно без перерывов 24 / 7 /365 (366).

1. **Требования к сертификации КЦОД Исполнителя**
   1. Для обеспечения гарантий качества и надежности предоставляемых услуг Исполнитель должен быть сертифицирован на соответствие системы управления IT-сервисами требованиям международного стандарта ISO/IEC 20000-1:2011.
   2. Процессы технического обслуживания заказчиков Исполнителя должны соответствовать стандартам системы менеджмента качества предприятия ISO 9001-2015;
   3. Система управления информационной безопасностью Исполнителя должна быть сертифицирована на соответствие требованиям ISO/IEC 27001:2013 в области действующей системы менеджмента информационной безопасности.
   4. Исполнитель должен представить действующие лицензии и документы:
   5. На деятельность по технической защите конфиденциальной информации (ФСТЭК);
   6. На оказание телематических услуг связи (РОСКОМНАДЗОР)
   7. О соответствии требованиям стандарта Tier III (Tier Certification of Design Documents; Tier Certification of Constructed Facility; Tier Certification of  Operational Sustainability)
   8. Наличие сертификата соответствия требованиям безопасности информации, предъявляемым к информационным системам класса защищенности 1Г, о защите информации предъявляемым к государственным информационным системам первого класса защищенности и на нем обеспечивается первый уровень защищенности обрабатываемых персональных данных.

# **Приложение Б. Требования к обеспечению вычислительными ресурсами.**

* + 1. КЦОД Исполнителя должен предоставить Заказчику в аренду вычислительные ресурсы в виде виртуальных машин и дискового пространства по модели IaaS, тип «collocation».
    2. Минимальный объём виртуальных ресурсов, которые необходимо выделить для размещения виртуальных машин:

Таблица 2. Параметры предоставления минимальной квоты вычислительных ресурсов.

|  |  |  |  |
| --- | --- | --- | --- |
| vCPU | RAM | HDD | Объём HDD для СРК |
| 7 THz | 13 Tb | 130 Tb | 500 Tb |

* + 1. Поставщик услуг обязан предоставить для возможности использования серверное оборудование со следующем перечнем физических процессоров:
* Intel Xeon Gold CPU 6248R 2x24 3.0 GHz
* Intel Xeon Gold 6140, 2.3GHz
* Intel Xeon E5-2660 v3, 2.6GHz
  + 1. Необходимо обеспечить отсутствие переподписки по CPU.
    2. Должна быть предоставлена возможность использования CPU pinning - закрепление определенных физических ядер за виртуальным сервером.
    3. На каждом из хостов виртуализации необходимо обеспечить запас ядер для собственных нужд гипервизора.
    4. Поставщик обеспечивает возможность заказа услуги по аренде виртуальных машин с графическим процессором A100 с преднастроенными конфигурациями:

Таблица 3. Параметры конфигураций ВМ с GPU.

|  |  |  |  |
| --- | --- | --- | --- |
| Параметр | Единица измерения | Конфигурация 1 | Конфигурация 2 |
| Виртуальный процессор 2,6 GHz | Штука | 32 | 64 |
| Оперативная память | Гигабайт | 160 | 320 |
| Виртуальный диск SSD (производительность 30 IOPS на 1Gb) | Гигабайт | 800 | 1600 |
| GPU | штука | 1 x A100 80 Гб | 2 x A100 80 Гб |

* + 1. Для памяти RAM должна быть исключена опция memory ballooning.
    2. Для дискового пространства должны использоваться системы хранения данных на SSD-дисках. Минимальная эталонная политика производительности 0,1 IOPS на 1 Gb. Исполнителю предоставляются возможности по выбору политики дискового пространства для ВМ со следующими политиками производительности:

Таблица 4. Параметры политик производительности HDD накопителей.

|  |  |
| --- | --- |
| Имя политики | Производительность IOPS на 1 Gb |
| SAS | 0,1 |
| SSD Basic | 0,4 |
| SSD Fast | 2 |
| SSD Ultra | 10 |
| SSD Ultra Plus | 30 |

* + 1. Сеть передачи данных (LAN) и сеть хранения данных (SAN) должны быть изолированы друг от друга с гарантированной пропускной способностью (т.е. для организации этих сетей используются отдельные коммутаторы, порты на гипервизорах, соединители).
    2. 100% выделенного объёма дискового пространства должно быть доступно к заполнению без влияния на производительность диска.
    3. Поставщик услуг обязан представить эластичную инфраструктуру, которая позволяет наращивать потребляемые Заказчиком виртуальные ресурсы без простоев и без ограничений итогового количества ресурсов в любой момент времени.
    4. Оператор ЦОД должен предоставить возможность по запросу Заказчика физического размещение ВМ на разных гипервизорах.
    5. Оператор ЦОД должен предоставить возможность по запросу Заказчика закрепить виртуальную машину статически на одном гипервизоре.
    6. Все используемые для размещения одного кластера ADB компоненты инфраструктуры (гипервизоры, СХД/SDS, коммутаторы и т.д.) должны находиться в рамках одного ЦОД (обеспечение постоянного latency в рамках одной локальной сети).
    7. Все дисковые ресурсы кластера (для каждой СХД/SDS в отдельности) должны быть зарезервированы (т.е. обеспечена доступность данных при выходе из строя любого одного компонента сети хранения данных или системы хранения данных)
    8. Максимальное количество ресурсов на виртуальную машину:

Таблица 5. Требования к максимальному количеству ресурсов на 1 ВМ.

|  |  |
| --- | --- |
| vCPU | 96 |
| RAM | 1.5 Tb |
| Диск | 32 Tb |

* + 1. Конфигурация арендуемых виртуальных ресурсов должна обеспечивать одновременную непрерывную работу всех виртуальных машин, указанных в Приложении Е и предоставляться в виде отказоустойчивого пула.
    2. Сетевая связность между всеми ВМ в пуле должна быть зарезервирована (поставщику услуг необходимо обеспечивать сетевую доступность виртуальных машин без снижения требуемой производительности при выходе из строя любого одного компонента сети передачи данных, например, сетевого порта NIC, SFP-модуля, сетевого кабеля, сетевого порта коммутатора, коммутатора целиком)
    3. По запросу Заказчика оператор ЦОД должен обеспечить возможность передачи трафика между ВМ с MTU 8300 в рамках всего пула выделяемых ресурсов.
    4. Должна предоставляться возможность распределять трафик ВМ на несколько сетевых адаптеров (до 10).
    5. Должна быть реализована возможность ограничения пропускной способности виртуальной сети/адаптера произвольным значением.
    6. Оператор ЦОД должен обеспечить скорость передачи данных по LAN между ВМ в размере 10 Гбит/сек.
    7. ЛВС Заказчика должна быть соединена с ЛВС Исполнителя по резервируемому оптическому каналу со скоростью 10 Гбит/сек.
    8. Исполнитель должен обладать возможностью предоставлять доступ к услуге универсального объектного хранилища «S3 Object Storage».

# **Приложение В. Необходимый набор сервисов и услуг.**

* + 1. **Требования к возможностям управления.**
  1. КЦОД Исполнителя должен предоставить Заказчику доступ к средствам управления, позволяющим выполнять обслуживание и текущую эксплуатацию всех виртуальных машин Заказчика, использующих арендуемые вычислительные ресурсы. Средства управления должны предусматривать возможность двухфакторной аутентификации.

1. **Требования к сервису создания резервных копий.**
   1. Для всех арендуемых виртуальных ресурсов должен быть организован сервис резервного копирования, обеспечивающий создание консистентных резервных копий.
   2. Для системы резервного копирования должна быть выделена квота дискового хранилища не менее 500 Tb с возможностью дальнейшего расширения без ограничений.
   3. Исполнитель должен предоставить описание решения по резервному копированию и хранению резервных копий, порядок восстановления, предоставить SLA на услугу.
   4. Скорость записи данных виртуальных машин в репозиторий СРК должна составлять не менее 3000 гигабайт в час.
   5. Скорость восстановления данных виртуальных машин из СРК в среду виртуализации должна составлять не менее 3000 гигабайт в час.
   6. Хранилище резервных копий должно быть расположено на отдельном физическом хранилище, на котором не хранятся данные из иных систем (диски виртуальных машин, иные данные).
   7. Хранилище резервных копий должно быть реализовано в отказоустойчивом исполнении.
2. **Требования к услуге «Резервное копирование в облако» (передача резервных копий в РЦОД АО КорпСофт)**
   1. Услуга заключается в предоставлении Заказчику возможности создания резервных копий виртуальных машин Заказчика, размещенных в его собственной инфраструктуре, и хранения их в хранилище на стороне Исполнителя, а также последующего восстановления данных из резервных копий в случае сбоя и их потери.
   2. Услуга резервного копирования в облако должна обеспечить передачу файлов резервных копий в резервный ЦОД Заказчика. Адрес резервного ЦОДа указан в «Таблица 1 – Адреса технологических площадок Заказчика» технического задания.
   3. Резервные копии могут быть переданы исключительно через локальную сеть Заказчика, существующую между ЦОДами. Для этих целей Исполнитель выполняет все необходимые настройки своей инфраструктуры для интеграции сервиса с резервным ЦОД.
   4. Исполнитель обеспечивает скорость передачи копий РК по сети не ниже чем 1200 мбит/сек с возможностью изменения как в сторону увеличения, так и в сторону уменьшения по запросу Заказчика.
   5. На стороне РЦОД оператор использует Veeam Cloud Connect для приёма и сохранения копий РК.
   6. Исполнитель обеспечивает целостность передаваемых данных и несёт ответственность за их работоспособность.
3. **Обеспечение защищенного хранения персональных данных**
   1. Для всех арендуемых виртуальных машин должна быть обеспечена антивирусная защита.
   2. Требования к защите информации, отнесенной к персональным данным, аналогичны требованиям, приведенным в пункте 7.14 Приложения А.
4. **Требования к услугам по размещению оборудования Заказчика**
   1. Исполнитель должен выделить отдельный телекоммуникационный шкаф шириной 1000мм и высотой 42 юнита для размещения оборудования Заказчика, перечисленного в таблице 2.

Таблица 6. Подлежащее размещению оборудование.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Оборудование | Размеры, Rack Unit | Потребляемая мощность, Вт | Тепловыделение, BTU/h |
| 1 | Коммутатор Eltex MES5332A | 1 | 160 | Н/Д |
| 2 | Коммутатор Eltex MES5332A | 1 | 160 | Н/Д |
| 3 | Межсетевой экран UserGate E1000 | 1 | 300 | Н/Д |
| 4 | Межсетевой экран UserGate E1000 | 1 | 300 | Н/Д |
| 5 | Межсетевой экран Check Point 5600 NGTP Appliance | 1 | 90 | 240 |
| 6 | Межсетевой экран Check Point 5600 NGTP Appliance | 1 | 90 | 240 |
| 7 | Криптошлюз S-Terra VPN Gate 8000 | 1 | 160 | 136 |
| 8 | Криптошлюз S-Terra VPN Gate 3000 | 1 | 90 | 136 |
| 9 | ЦУС Континент | 1 | 40 | Н/Д |
| 10 | TLS-сервер IPCR550 | 1 | 40 | Н/Д |
| 11 | Сервер | 2 | 100 | Н/Д |
| 12 | Сервер | 2 | 100 | Н/Д |

Примечание – в таблице приводятся максимально возможные показатели.

* 1. Всё оборудование должно быть обеспечено бесперебойным электропитанием от двух разных энергонезависимых источников.
  2. Климатические условия в помещении с оборудованием должны соответствовать требованиям производителей.
  3. Всё оборудование должно иметь возможность подключения к следующим сетям передачи данных:
* сеть виртуальных машин Заказчика;
* канал передачи данных между КЦОД Исполнителя и офисом Заказчика (г. Москва ул.Гашека 6, Ducat Place III);
* канал передачи данных между КЦОД Исполнителя и резервным центром обработки данных Заказчика (г. Москва, Коровинское шоссе дом 41);
* глобальная сеть Интернет;
  1. Оборудование Заказчика, размещённое в КЦОД, должно иметь выделенный физический оптико-волоконный канал связи для подключения к локальной сети КЦОД.
  2. Должна быть предоставлена возможность для организации L2VPN каналов связи с технологическими площадки Заказчика, указанными в таблице 1 технического защдания для организации Site-to-Site IPsec-тоннелей. Все перемычки для соединения операторского оборудования с ЛВС Заказчика и ЦОДа выполняются по оптико-волоконным линиям связи.
  3. Должно быть обеспечено присутствие следующих операторов связи: Мегафон, Билайн, МТС, Ростелеком.
  4. Должен быть обеспечен доступ для персонала Заказчика ко всему оборудованию для выполнения текущего обслуживания и эксплуатации.

1. **Требования к услугам по обеспечению сетевой доступности виртуальных машин Заказчика.**
   1. Все вычислительные ресурсы и сервисы в пределах КЦОД Исполнителя должны быть обеспечены сетевой связанностью с пропускной способностью не ниже 10 Гбит/сек.
   2. Должен быть предоставлен безлимитный отказоустойчивый канал для доступа в Интернет для виртуальных машин и оборудования Заказчика. Пропускная способность канала должна быть не менее 1 Гбит/с с возможностями расширения минимум до 2 Гбит/с.
   3. Исполнитель предоставляет услугу аренды двух независимых от провайдера Интернет блоков IP-адресов размером «/28» каждый.
   4. Исполнитель передаёт в использование Заказчику не менее 100 штук VLAN в виртуальной сети КЦОД с технической возможностью соединения этих VLAN с сетевым оборудованием Заказчика через установленный волоконно-оптический канал и возможностями дальнейшего расширения.
2. **Требования к организации Disaster Recovery**
   1. В рамках исполнения политик обеспечения непрерывности бизнес-деятельности Заказчика Исполнитель должен организовать своевременную передачу файлов резеревных копий на площадку РЦОД Заказчика.
   2. Исполнитель несёт ответственность за консистентность передаваемых данных.
   3. Исполнитель несёт ответственность за соблюдение SLA по передаче данных на удалённую площадку.
   4. Время выполнения резервных копий и их передача на удалённую площадку не должна выходить за рамки технологического окна в 8 часов.
3. **Требования к квалификации и правовому оформлению взаимоотношений**
   1. КЦОД Исполнителя должен гарантировать работоспособность сервисов и сохранность данных в течение определенного времени в случае возникновения форс-мажорных обстоятельств, препятствующих проведению платежей Заказчика за предоставляемые услуги (grace period) до 45 календарных дней.

# **Приложение Г. Принципиальная схема ИТ-инфраструктуры Заказчика.**



# **Приложение Д. Соглашение об уровне оказания услуг.**

**Уровень услуг**

Таблица 7. Приоритеты инцидентов.

|  |  |  |
| --- | --- | --- |
| № п/п | Приоритет инцидента | Описание |
| 1 | Приоритет 1 | Не доступна виртуальная машина на уровне облачной платформы Исполнителя |
| RAM Swapped процент от сконфигурированной памяти виртуальной машины свыше 30% |
| Количество MIPS на одно vCPU менее 1000 |
| HDD IOPS уменьшение на 30% и более от оговоренных значений |
| Среднее время отклика SSD-диска на виртуальной машине свыше 13 мс |
| Среднее время отклика SAS-диска на виртуальной машине свыше 100 мс |
| Процент потерянных пакетов в пределах сети передачи данных Исполнителя более 1% |
| Средняя сетевая задержка в пределах Исполнителя более 15 мс |
| 2 | Приоритет 2 | Отсутствие доступа к интерфейсу управления виртуальными машинами более 1 часа |
| RAM Swapped процент от сконфигурированной памяти виртуальной машины свыше 20% |
| Количество MIPS на одно vCPU 1200-1500 |
| HDD IOPS уменьшение от 20% до 30% от оговоренных значений |
| Среднее время отклика SAS-диска на виртуальной машине 7 до 13мс |
| Среднее время отклика SAS-диска на виртуальной машине 50-100мс |
| Процент потерянных пакетов в пределах Исполнителя от 0,4% до 1% |
| Средняя сетевая задержка в пределах Исполнителя от 10 до 15мс |
| 3 | Приоритет 3 | Отсутствие доступа к интерфейсу управления виртуальными машинами более 2 часов |
| RAM Swapped процент от сконфигурированной памяти виртуальной машины свыше 10% |
| Количество MIPS на одно vCPU 1500-1700 |
| HDD IOPS уменьшение от 10% до 20% от оговоренных значений |
| Среднее время отклика SSD-диска на виртуальной машине от 3 до 7мс |
| Среднее время отклика SAS-диска на виртуальной машине от 30мс до 50мс |
| Процент потерянных пакетов в пределах Исполнителя от 0,2% до 0,4% |
| Средняя сетевая задержка в пределах Исполнителя от 5 до 10мс |

Таблица 8. Параметры решения инцидентов.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | Приоритет инцидента | Обработка | Время реакции, мин\* | Максимальное время решения, мин\*\* | Суммарное время решения инцидентов в месяц, не более, мин | Допустимое количество инцидентов в месяц, не более шт |
| 1 | 1 | Круглосуточно | 30 | 120 | 120 | 1 |
| 2 | 2 | Круглосуточно | 90 | 240 | 480 | 2 |
| 3 | 3 | Круглосуточно | 120 | 480 | 1440 | 3 |

\*Принятие и регистрация обращения, классификация и приоритезации. 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.

Таблица 9. Классификация и приоритеты обращений типа «запрос».

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Классификация | Приоритет | Описание |
| 1 | Сервисный запрос | 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. |

Таблица 10. Параметры обработки запросов.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Категория | Приоритет | Обработка | Время реакции на запрос, минут\* | Максимальное время решения запроса, не более часов\*\* |
| 1 | Сервисный запрос | 4 | В рабочие часы\*\*\* | 60 | 24 |
| 2 | Запрос на изменение | 5 | В рабочие часы | 60 | 48 |
| 3 | Запрос на предоставление информации | 6 | В рабочие часы | 60 | 72 |

\*Принятие и регистрация обращения, классификация и приоритезация. 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 Исполнителя: рабочие дни РФ с 9.00 до 18.00.

Таблица 11. 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 |

# **Приложение Е. Перечень виртуальных машин с указанием параметров.**

Таблица 12. Перечень ВМ.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Имя виртуальной машины | Количество vCPU | Объём RAM, Gb | Объём HDD, Gb | Имя сети VLAN |
| VM-01 | 2 | 4 | 34 | VLAN-13 |
| VM-02 | 8 | 16 | 146 | VLAN-34 |
| VM-03 | 4 | 32 | 132 | VLAN-26 |
| VM-04 | 4 | 32 | 132 | VLAN-26 |
| VM-05 | 12 | 12 | 72 | VLAN-19 |
| VM-06 | 1 | 0,125 | 80 | VLAN-07 |
| VM-07 | 2 | 2 | 52 | VLAN-13 |
| VM-08 | 2 | 2 | 152 | VLAN-37 |
| VM-09 | 4 | 32 | 132 | VLAN-26 |
| VM-10 | 12 | 64 | 184 | VLAN-19 |
| VM-11 | 2 | 2 | 52 | VLAN-08 |
| VM-12 | 2 | 4 | 34 | VLAN-26 |
| VM-13 | 4 | 8 | 308 | VLAN-14 |
| VM-14 | 4 | 8 | 158 | VLAN-37 |
| VM-15 | 2 | 4 | 34 | VLAN-01 |
| VM-16 | 6 | 48 | 498 | VLAN-23 |
| VM-17 | 4 | 32 | 92 | VLAN-26 |
| VM-18 | 2 | 4 | 44 | VLAN-26 |
| VM-19 | 2 | 4 | 54 | VLAN-11 |
| VM-20 | 2 | 12 | 657 | VLAN-12 |
| VM-21 | 4 | 8 | 158 | VLAN-33 |
| VM-22 | 8 | 12 | 38 | VLAN-12 |
| VM-23 | 4 | 32 | 152 | VLAN-03 |
| VM-24 | 2 | 16 | 216 | VLAN-22 |
| VM-25 | 1 | 2 | 22 | VLAN-12 |
| VM-26 | 4 | 8 | 108 | VLAN-12 |
| VM-27 | 4 | 16 | 146 | VLAN-34 |
| VM-28 | 1 | 0,125 | 50 | VLAN-07 |
| VM-29 | 1 | 0,125 | 110 | VLAN-07 |
| VM-30 | 4 | 32 | 532 | VLAN-07 |
| VM-31 | 2 | 6 | 191 | VLAN-11 |
| VM-32 | 4 | 16 | 136 | VLAN-01 |
| VM-33 | 12 | 64 | 184 | VLAN-19 |
| VM-34 | 4 | 4 | 64 | VLAN-31 |
| VM-35 | 2 | 2 | 72 | VLAN-12 |
| VM-36 | 4 | 8 | 58 | VLAN-37 |
| VM-37 | 4 | 32 | 92 | VLAN-26 |
| VM-38 | 2 | 16 | 216 | VLAN-22 |
| VM-39 | 1 | 0,125 | 180 | VLAN-07 |
| VM-40 | 4 | 16 | 646 | VLAN-02 |
| VM-41 | 2 | 2 | 42 | VLAN-26 |
| VM-42 | 4 | 16 | 166 | VLAN-26 |
| VM-43 | 4 | 8 | 108 | VLAN-12 |
| VM-44 | 8 | 32 | 282 | VLAN-26 |
| VM-45 | 4 | 8 | 474 | VLAN-25 |
| VM-46 | 4 | 2 | 222 | VLAN-07 |
| VM-47 | 2 | 4 | 54 | VLAN-05 |
| VM-48 | 4 | 8 | 108 | VLAN-12 |
| VM-49 | 4 | 16 | 146 | VLAN-34 |
| VM-50 | 1 | 0,125 | 200 | VLAN-39 |
| VM-51 | 4 | 8 | 58 | VLAN-33 |
| VM-52 | 8 | 32 | 692 | VLAN-21 |
| VM-53 | 12 | 32 | 181 | VLAN-23 |
| VM-54 | 2 | 8 | 68 | VLAN-26 |
| VM-55 | 4 | 6 | 96 | VLAN-12 |
| VM-56 | 16 | 64 | 1021 | VLAN-28 |
| VM-57 | 4 | 32 | 182 | VLAN-02 |
| VM-58 | 12 | 64 | 144 | VLAN-19 |
| VM-59 | 4 | 8 | 108 | VLAN-12 |
| VM-60 | 6 | 12 | 112 | VLAN-35 |
| VM-61 | 4 | 32 | 92 | VLAN-26 |
| VM-62 | 4 | 16 | 496 | VLAN-02 |
| VM-63 | 2 | 22 | 317 | VLAN-11 |
| VM-64 | 16 | 64 | 334 | VLAN-36 |
| VM-65 | 8 | 32 | 482 | VLAN-01 |
| VM-66 | 1 | 0,125 | 180 | VLAN-07 |
| VM-67 | 2 | 4 | 204 | VLAN-37 |
| VM-68 | 4 | 4 | 44 | VLAN-12 |
| VM-69 | 8 | 32 | 232 | VLAN-01 |
| VM-70 | 1 | 0,125 | 50 | VLAN-39 |
| VM-71 | 4 | 16 | 2946 | VLAN-12 |
| VM-72 | 4 | 8 | 138 | VLAN-33 |
| VM-73 | 2 | 4 | 154 | VLAN-33 |
| VM-74 | 4 | 32 | 92 | VLAN-26 |
| VM-75 | 2 | 8 | 128 | VLAN-11 |
| VM-76 | 2 | 8 | 68 | VLAN-03 |
| VM-77 | 8 | 16 | 216 | VLAN-10 |
| VM-78 | 2 | 4 | 34 | VLAN-01 |
| VM-79 | 18 | 64 | 144 | VLAN-39 |
| VM-80 | 16 | 64 | 114 | VLAN-06 |
| VM-81 | 4 | 4 | 34 | VLAN-31 |
| VM-82 | 12 | 64 | 154 | VLAN-19 |
| VM-83 | 2 | 4 | 34 | VLAN-26 |
| VM-84 | 4 | 8 | 78 | VLAN-19 |
| VM-85 | 20 | 64 | 289 | VLAN-11 |
| VM-86 | 4 | 16 | 656 | VLAN-26 |
| VM-87 | 4 | 8 | 158 | VLAN-33 |
| VM-88 | 2 | 2 | 52 | VLAN-08 |
| VM-89 | 16 | 32 | 1952 | VLAN-26 |
| VM-90 | 4 | 16 | 146 | VLAN-32 |
| VM-91 | 1 | 1 | 531 | VLAN-39 |
| VM-92 | 1 | 0,125 | 150 | VLAN-39 |
| VM-93 | 4 | 8 | 58 | VLAN-33 |
| VM-94 | 16 | 32 | 1902 | VLAN-03 |
| VM-95 | 4 | 4 | 24 | VLAN-02 |
| VM-96 | 2 | 4 | 104 | VLAN-11 |
| VM-97 | 1 | 0,125 | 80 | VLAN-08 |
| VM-98 | 8 | 32 | 192 | VLAN-24 |
| VM-99 | 2 | 4 | 204 | VLAN-33 |
| VM-100 | 4 | 16 | 146 | VLAN-34 |
| VM-101 | 4 | 8 | 308 | VLAN-25 |
| VM-102 | 4 | 8 | 88 | VLAN-12 |
| VM-103 | 4 | 8 | 48 | VLAN-12 |
| VM-104 | 4 | 16 | 251 | VLAN-21 |
| VM-105 | 4 | 32 | 152 | VLAN-03 |
| VM-106 | 4 | 16 | 446 | VLAN-07 |
| VM-107 | 8 | 16 | 176 | VLAN-21 |
| VM-108 | 12 | 64 | 144 | VLAN-19 |
| VM-109 | 2 | 2 | 202 | VLAN-37 |
| VM-110 | 4 | 8 | 558 | VLAN-26 |
| VM-111 | 1 | 0,125 | 80 | VLAN-07 |
| VM-112 | 2 | 10 | 310 | VLAN-12 |
| VM-113 | 12 | 64 | 184 | VLAN-19 |
| VM-114 | 2 | 2 | 51 | VLAN-33 |
| VM-115 | 8 | 64 | 614 | VLAN-04 |
| VM-116 | 4 | 8 | 4808 | VLAN-12 |
| VM-117 | 4 | 32 | 82 | VLAN-07 |
| VM-118 | 12 | 64 | 184 | VLAN-19 |
| VM-119 | 1 | 1 | 61 | VLAN-23 |
| VM-120 | 2 | 8 | 58 | VLAN-12 |
| VM-121 | 12 | 64 | 184 | VLAN-19 |
| VM-122 | 12 | 24 | 84 | VLAN-12 |
| VM-123 | 4 | 4 | 34 | VLAN-25 |
| VM-124 | 12 | 24 | 84 | VLAN-39 |
| VM-125 | 4 | 8 | 268 | VLAN-32 |
| VM-126 | 4 | 12 | 112 | VLAN-12 |
| VM-127 | 12 | 12 | 72 | VLAN-19 |
| VM-128 | 4 | 16 | 166 | VLAN-37 |
| VM-129 | 4 | 4 | 84 | VLAN-34 |
| VM-130 | 4 | 16 | 786 | VLAN-26 |
| VM-131 | 4 | 6 | 56 | VLAN-12 |
| VM-132 | 4 | 16 | 116 | VLAN-23 |
| VM-133 | 8 | 16 | 66 | VLAN-20 |
| VM-134 | 1 | 0,125 | 300 | VLAN-39 |
| VM-135 | 4 | 32 | 232 | VLAN-22 |
| VM-136 | 10 | 64 | 4384 | VLAN-12 |
| VM-137 | 4 | 8 | 158 | VLAN-33 |
| VM-138 | 4 | 32 | 132 | VLAN-26 |
| VM-139 | 4 | 40 | 140 | VLAN-01 |
| VM-140 | 2 | 4 | 164 | VLAN-09 |
| VM-141 | 4 | 8 | 78 | VLAN-19 |
| VM-142 | 2 | 8 | 68 | VLAN-26 |
| VM-143 | 4 | 32 | 232 | VLAN-02 |
| VM-144 | 4 | 12 | 112 | VLAN-12 |
| VM-145 | 18 | 64 | 144 | VLAN-19 |
| VM-146 | 2 | 4 | 34 | VLAN-15 |
| VM-147 | 4 | 32 | 132 | VLAN-26 |
| VM-148 | 4 | 8 | 108 | VLAN-12 |
| VM-149 | 8 | 16 | 166 | VLAN-11 |
| VM-150 | 12 | 64 | 184 | VLAN-19 |
| VM-151 | 1 | 1 | 61 | VLAN-23 |
| VM-152 | 1 | 0,125 | 50 | VLAN-39 |
| VM-153 | 12 | 64 | 144 | VLAN-19 |
| VM-154 | 4 | 4 | 34 | VLAN-30 |
| VM-155 | 2 | 2 | 52 | VLAN-08 |
| VM-156 | 4 | 4 | 154 | VLAN-37 |
| VM-157 | 2 | 2 | 32 | VLAN-12 |
| VM-158 | 4 | 18 | 2058 | VLAN-03 |
| VM-159 | 4 | 4 | 34 | VLAN-25 |
| VM-160 | 1 | 0,125 | 150 | VLAN-39 |
| VM-161 | 4 | 8 | 157 | VLAN-33 |
| VM-162 | 1 | 0,125 | 215 | VLAN-39 |
| VM-163 | 12 | 64 | 184 | VLAN-19 |
| VM-164 | 2 | 2 | 52 | VLAN-20 |
| VM-165 | 8 | 48 | 158 | VLAN-19 |
| VM-166 | 1 | 1 | 61 | VLAN-23 |
| VM-167 | 4 | 16 | 146 | VLAN-32 |
| VM-168 | 2 | 4 | 54 | VLAN-12 |
| VM-169 | 1 | 1 | 301 | VLAN-23 |
| VM-170 | 12 | 64 | 184 | VLAN-19 |
| VM-171 | 4 | 32 | 132 | VLAN-26 |
| VM-172 | 4 | 8 | 68 | VLAN-14 |
| VM-173 | 1 | 1 | 101 | VLAN-23 |
| VM-174 | 4 | 32 | 132 | VLAN-38 |
| VM-175 | 2 | 4 | 34 | VLAN-26 |
| VM-176 | 2 | 4 | 6889 | VLAN-19 |
| VM-177 | 4 | 10 | 110 | VLAN-12 |
| VM-178 | 4 | 6 | 96 | VLAN-19 |
| VM-179 | 8 | 32 | 532 | VLAN-24 |
| VM-180 | 12 | 32 | 5443 | VLAN-11 |
| VM-181 | 2 | 4 | 54 | VLAN-11 |
| VM-182 | 2 | 2 | 50 | VLAN-37 |
| VM-183 | 4 | 8 | 208 | VLAN-35 |
| VM-184 | 12 | 64 | 184 | VLAN-19 |
| VM-185 | 12 | 64 | 144 | VLAN-19 |
| VM-186 | 4 | 0,125 | 235 | VLAN-06 |
| VM-187 | 8 | 32 | 682 | VLAN-26 |
| VM-188 | 2 | 4 | 184 | VLAN-16 |
| VM-189 | 6 | 16 | 236 | VLAN-20 |
| VM-190 | 4 | 32 | 1134 | VLAN-26 |
| VM-191 | 8 | 16 | 116 | VLAN-19 |
| VM-192 | 2 | 4 | 54 | VLAN-12 |
| VM-193 | 4 | 16 | 246 | VLAN-01 |
| VM-194 | 4 | 32 | 92 | VLAN-26 |
| VM-195 | 4 | 16 | 66 | VLAN-07 |
| VM-196 | 4 | 32 | 132 | VLAN-26 |
| VM-197 | 4 | 12 | 112 | VLAN-12 |
| VM-198 | 20 | 48 | 398 | VLAN-29 |
| VM-199 | 2 | 2 | 52 | VLAN-20 |
| VM-200 | 4 | 8 | 68 | VLAN-19 |
| VM-201 | 4 | 8 | 168 | VLAN-23 |
| VM-202 | 12 | 40 | 600 | VLAN-39 |
| VM-203 | 8 | 16 | 176 | VLAN-21 |
| VM-204 | 36 | 96 | 951 | VLAN-18 |
| VM-205 | 4 | 32 | 332 | VLAN-38 |
| VM-206 | 2 | 8 | 68 | VLAN-19 |
| VM-207 | 4 | 16 | 96 | VLAN-07 |
| VM-208 | 2 | 4 | 154 | VLAN-37 |
| VM-209 | 2 | 4 | 64 | VLAN-11 |
| VM-210 | 4 | 16 | 836 | VLAN-01 |
| VM-211 | 4 | 32 | 152 | VLAN-03 |
| VM-212 | 4 | 8 | 158 | VLAN-37 |
| VM-213 | 4 | 8 | 58 | VLAN-33 |
| VM-214 | 4 | 32 | 132 | VLAN-26 |
| VM-215 | 2 | 4 | 84 | VLAN-34 |
| VM-216 | 4 | 16 | 191 | VLAN-02 |
| VM-217 | 4 | 8 | 58 | VLAN-20 |
| VM-218 | 4 | 8 | 68 | VLAN-19 |
| VM-219 | 4 | 16 | 106 | VLAN-19 |
| VM-220 | 4 | 8 | 88 | VLAN-34 |
| VM-221 | 1 | 1 | 51 | VLAN-23 |
| VM-222 | 2 | 4 | 44 | VLAN-12 |
| VM-223 | 4 | 8 | 58 | VLAN-37 |
| VM-224 | 4 | 16 | 146 | VLAN-32 |
| VM-225 | 16 | 64 | 334 | VLAN-06 |
| VM-226 | 2 | 6 | 126 | VLAN-11 |
| VM-227 | 4 | 4 | 34 | VLAN-25 |
| VM-228 | 12 | 24 | 84 | VLAN-39 |
| VM-229 | 1 | 1 | 601 | VLAN-23 |
| VM-230 | 12 | 32 | 182 | VLAN-23 |
| VM-231 | 2 | 12 | 12912 | VLAN-11 |
| VM-232 | 2 | 16 | 216 | VLAN-22 |
| VM-233 | 4 | 8 | 58 | VLAN-37 |
| VM-234 | 12 | 48 | 608 | VLAN-25 |
| VM-235 | 2 | 4 | 34 | VLAN-12 |
| VM-236 | 4 | 8 | 58 | VLAN-35 |
| VM-237 | 2 | 4 | 24 | VLAN-26 |
| VM-238 | 2 | 2 | 52 | VLAN-20 |
| VM-239 | 2 | 2 | 52 | VLAN-20 |
| VM-240 | 36 | 116 | 376 | VLAN-27 |
| VM-241 | 4 | 32 | 132 | VLAN-26 |
| VM-242 | 4 | 8 | 158 | VLAN-37 |
| VM-243 | 8 | 16 | 146 | VLAN-32 |
| VM-244 | 8 | 0,125 | 80 | VLAN-06 |
| VM-245 | 2 | 4 | 84 | VLAN-32 |
| VM-246 | 4 | 8 | 158 | VLAN-37 |
| VM-247 | 1 | 0,125 | 8 | VLAN-39 |
| VM-248 | 4 | 0,125 | 730 | VLAN-14 |
| VM-249 | 10 | 8 | 2056 | VLAN-14 |
| VM-250 | 4 | 4 | 34 | VLAN-30 |
| VM-251 | 4 | 4 | 164 | VLAN-19 |
| VM-252 | 2 | 2 | 52 | VLAN-20 |
| VM-253 | 2 | 16 | 216 | VLAN-22 |
| VM-254 | 2 | 4 | 134 | VLAN-11 |
| VM-255 | 2 | 4 | 204 | VLAN-37 |
| VM-256 | 4 | 48 | 238 | VLAN-03 |
| VM-257 | 12 | 32 | 182 | VLAN-23 |
| VM-258 | 2 | 4 | 34 | VLAN-12 |
| VM-259 | 8 | 32 | 432 | VLAN-26 |
| VM-260 | 4 | 16 | 165 | VLAN-33 |
| VM-261 | 8 | 40 | 335 | VLAN-02 |
| VM-262 | 8 | 16 | 176 | VLAN-21 |
| VM-263 | 8 | 32 | 1256 | VLAN-11 |
| VM-264 | 4 | 8 | 138 | VLAN-34 |
| VM-265 | 12 | 32 | 5443 | VLAN-11 |
| VM-266 | 8 | 42 | 220 | VLAN-17 |
| VM-267 | 2 | 4 | 34 | VLAN-03 |
| VM-268 | 2 | 5 | 80 | VLAN-11 |
| VM-269 | 4 | 8 | 408 | VLAN-12 |
| VM-270 | 2 | 4 | 204 | VLAN-33 |
| VM-271 | 4 | 8 | 158 | VLAN-33 |
| VM-272 | 1 | 0,125 | 100 | VLAN-39 |
| VM-273 | 12 | 64 | 614 | VLAN-27 |
| VM-274 | 4 | 8 | 68 | VLAN-19 |
| VM-275 | 4 | 16 | 366 | VLAN-02 |
| VM-276 | 4 | 32 | 82 | VLAN-07 |
| VM-277 | 2 | 2 | 52 | VLAN-20 |
| VM-278 | 4 | 4 | 84 | VLAN-32 |
| VM-279 | 4 | 16 | 451 | VLAN-02 |
| VM-280 | 8 | 64 | 394 | VLAN-01 |
| VM-281 | 4 | 24 | 104 | VLAN-19 |
| VM-282 | 2 | 4 | 1664 | VLAN-24 |
| VM-283 | 4 | 32 | 232 | VLAN-22 |
| VM-284 | 4 | 8 | 88 | VLAN-32 |
| VM-285 | 4 | 8 | 108 | VLAN-39 |
| VM-286 | 4 | 4 | 59 | VLAN-07 |
| VM-287 | 18 | 64 | 144 | VLAN-19 |
| VM-288 | 8 | 128 | 288 | VLAN-24 |
| VM-289 | 2 | 2 | 152 | VLAN-13 |
| VM-290 | 4 | 48 | 168 | VLAN-03 |
| VM-291 | 4 | 32 | 232 | VLAN-02 |
| VM-292 | 4 | 16 | 46 | VLAN-20 |
| VM-293 | 1 | 2 | 37 | VLAN-10 |
| VM-294 | 2 | 4 | 34 | VLAN-01 |
| VM-295 | 4 | 4 | 154 | VLAN-33 |
| VM-296 | 2 | 4 | 204 | VLAN-11 |
| VM-297 | 1 | 0,125 | 30 | VLAN-39 |
| VM-298 | 12 | 64 | 154 | VLAN-19 |
| VM-299 | 8 | 7,8125 | 408 | VLAN-11 |
| VM-300 | 4 | 16 | 166 | VLAN-29 |
| VM-301 | 2 | 14 | 884 | VLAN-02 |
| VM-302 | 2 | 4 | 34 | VLAN-19 |
| VM-303 | 1 | 1 | 101 | VLAN-23 |
| VM-304 | 2 | 4 | 34 | VLAN-26 |
| VM-305 | 2 | 4 | 34 | VLAN-02 |
| VM-306 | 8 | 32 | 282 | VLAN-07 |
| VM-307 | 4 | 16 | 146 | VLAN-02 |
| VM-308 | 4 | 32 | 332 | VLAN-38 |
| VM-309 | 4 | 32 | 92 | VLAN-26 |
| VM-310 | 8 | 32 | 352 | VLAN-24 |
| VM-311 | 4 | 32 | 152 | VLAN-03 |
| VM-312 | 16 | 64 | 1044 | VLAN-36 |

# **Приложение Ж. Требования к информационной безопасности.**

В соответствии с требованиями Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» АО РНПК является субъектом критической информационной инфраструктуры и информационные системы АО РНПК согласно Постановлению Правительства РФ от 08.02.2018 № 127 включены в реестр значимых объектов критической информационной инфраструктуры Российской Федерации. Информационным системам АО РНПК присвоена 3 категория значимости.

Для обеспечения обеспечения безопасности значимых объектов критической информационной инфраструктуры АО РНПК должны обеспечиваться принятие организационных и технических мер в соответствии с установленными Требованиями Федеральной службы по техническому и экспортному контролю. Такие требованиями указаны в Приказе ФСТЭК России от 25.12.2017 №239. Исполнитель ЦОДа обязан реализовать следующие меры обеспечения безопасности значимого объекта:

* + 1. **Идентификация и аутентификация (ИАФ), включая:**
* Регламентацию правил и процедур идентификации и аутентификации;
* Идентификацию и аутентификацию пользователей и инициируемых ими процессов;
* Идентификацию и аутентификацию устройств;
* Управление идентификаторами;
* Управление средствами аутентификации;
* Идентификацию и аутентификацию внешних пользователей;
* Защиту аутентификационной информации при передаче.
  + 1. **Управление доступом (УПД), включая:**
* Регламентацию правил и процедур управления доступом;
* Управление учетными записями пользователей;
* Реализацию модели управления доступом;
* Блокирование сеанса доступа пользователя при неактивности;
* Управление действиями пользователей до идентификации и аутентификации;
* Реализация защищенного удаленного доступа;
* Контроль доступа из внешних информационных (автоматизированных) систем.
  + 1. **Защита машинных носителей информации (ЗНИ), включая:**
* Регламентация правил и процедур защиты машинных носителей информации;
* Учет машинных носителей информации;
* Управление физическим доступом к машинным носителям информации;
* Контроль перемещения машинных носителей информации за пределы контролируемой зоны;
* Исключение возможности несанкционированного чтения информации на машинных носителях информации;
* Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации;
* Контроль ввода (вывода) информации на съемные машинные носители информации;
* Контроль подключения съемных машинных носителей информации;
* Уничтожение (стирание) информации на машинных носителях информации.
  + 1. **Аудит безопасности (АУД), включая:**
* Регламентация правил и процедур аудита безопасности;
* Инвентаризация информационных ресурсов;
* Анализ уязвимостей и их устранение;
* Генерирование временных меток и (или) синхронизация системного времени;
* Регистрация событий безопасности;
* Контроль и анализ сетевого трафика,
* Защита информации о событиях безопасности;
* Мониторинг безопасности;
* Реагирование на сбои при регистрации событий безопасности;
* Проведение внутренних аудитов.
  + 1. **Антивирусная защита (АВЗ), включая:**
* Регламентация правил и процедур антивирусной защиты;
* Реализация антивирусной защиты;
* Антивирусная защита электронной почты и иных сервисов;
* Обновление базы данных признаков вредоносных компьютерных программ (вирусов).
  + 1. **Предотвращение вторжений (компьютерных атак) (СОВ), включая:**
* Регламентация правил и процедур предотвращения вторжений (компьютерных атак);
* Обнаружение и предотвращение компьютерных атак.
  + 1. **Обеспечение целостности (ОЦЛ), включая:**
* Регламентация правил и процедур обеспечения целостности;
* Контроль целостности программного обеспечения;
* Контроль целостности информации.
  + 1. **Обеспечение доступности (ОДТ), включая:**
* Регламентация правил и процедур обеспечения доступности;
* Использование отказоустойчивых технических средств;
* Резервирование средств и систем;
* Контроль безотказного функционирования средств и систем;
* Резервное копирование информации;
* Обеспечение возможности восстановления информации;
* Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях;
* Контроль предоставляемых вычислительных ресурсов и каналов связи.

1. **Защита технических средств и систем (ЗТС), включая:**

* Регламентация правил и процедур защиты технических средств и систем;
* Защита информации от утечки по техническим каналам;
* Организация контролируемой зоны;
* Управление физическим доступом;
* Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;
* Защита от внешних воздействий;
* Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации.

1. **Защита информационной (автоматизированной) системы и ее компонентов (ЗИС), включая:**

* Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов;
* Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями;
* Защита периметра информационной (автоматизированной) системы;
* Эшелонированная защита информационной (автоматизированной) системы;
* Организация демилитаризованной зоны;
* Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы;
* Защита информации при ее передаче по каналам связи;
* Защита неизменяемых данных;
* Защита информации от утечек;
* Обеспечение доверенных канала, маршрута;
* Обеспечение подлинности сетевых соединений;
* Запрет несанкционированной удаленной активации периферийных устройств;
* Защита от угроз отказа в обслуживании (DOS, DDOS-атак);
* Управление сетевыми соединениями;
* Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.

1. **Реагирование на компьютерные инциденты (ИНЦ), включая:**

* Регламентация правил и процедур реагирования на компьютерные инциденты;
* Выявление компьютерных инцидентов;
* Информирование о компьютерных инцидентах;
* Анализ компьютерных инцидентов;
* Устранение последствий компьютерных инцидентов;
* Принятие мер по предотвращению повторного возникновения компьютерных инцидентов;
* Хранение и защита информации о компьютерных инцидентах.

1. **Планирование мероприятий по обеспечению безопасности (ПЛН), включая:**

* Регламентация правил и процедур планирования мероприятий по обеспечению защиты информации;
* Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации;
* Контроль выполнения мероприятий по обеспечению защиты информации.

1. **Обеспечение действий в нештатных ситуациях (ДНС), включая:**

* Регламентация правил и процедур обеспечения действий в нештатных ситуациях;
* Разработка плана действий в нештатных ситуациях;
* Обучение и отработка действий персонала в нештатных ситуациях;
* Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций;
* Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций;
* Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций;
* Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения.

1. **Защита среды виртуализации**

* Организационные и технические меры, применяемые для защиты среды виртуализации:
  + идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа;
  + сегментация и межсетевое экранирование вычислительных сетей.
* Меры по защите среды виртуализации должны обеспечивать:
  + организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации;
  + организацию и контроль информационного взаимодействия и изоляции виртуальных машин;
  + организацию защиты образов виртуальных машин;
  + регистрацию событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации.
* Разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности;
* Разграничение и контроль осуществления одновременного доступа виртуальных машин к системе хранения данных в пределах контура безопасности;
* Идентификация и аутентификация пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам;
* Реализация необходимых методов предоставления доступа к виртуальным машинам, обеспечивающих возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине;
* Обеспечение возможности принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной;
* Контроль и протоколирование доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных с реализацией двухфакторной аутентификации;
* Размещение средств защиты информации, используемых для организации контроля и протоколирования доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных на физических СВТ;
* Размещение серверных и пользовательских компонентов АС на разных виртуальных машинах.