

**ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ
УСЛУГА «ВИРТУАЛЬНЫЙ ЦОД на базе VMware»****1. НАИМЕНОВАНИЕ УСЛУГИ**

- 1.1. Наименование Услуги: Виртуальный ЦОД на базе VMware.
- 1.2. Настоящий документ содержит описание состава Услуги, ее базовой функциональности, возможных сопутствующих и дополнительных услуг, общего порядка подключения, изменения и отключения Услуги, условий предоставления и ограничений.

2. ИНФОРМАЦИЯ ОБ УСЛУГЕ**2.1. Краткое описание Услуги**

- 2.1.1 Виртуальный ЦОД на VMware (ранее и далее – Услуга), является услугой по предоставлению базовых информационно-технологических ресурсов на основе совокупности функционирующего под управлением Исполнителя серверного и сетевого оборудования, систем хранения данных и специализированного программного обеспечения. Услуга построена на основе модели обслуживания «IaaS».
- 2.1.2. В рамках Услуги Исполнитель предоставляет Заказчику Виртуальный ЦОД, имеющий в распоряжении согласованный между Исполнителем и Заказчиком набор виртуализированных вычислительных мощностей процессора (vCPU), виртуальной памяти (vRAM) и дискового пространства (vHDD), а также средства управления Виртуальным ЦОД, достаточные для создания и управления виртуальными серверами в требуемой Заказчику конфигурации в пределах выделенных виртуализированных мощностей.
- 2.1.3. Управление Виртуальным ЦОД осуществляется Заказчиком при помощи консоли Cloud Director.

2.2. Состав Услуги и основные компоненты

- 2.2.1. В состав Услуги входят:

Вычислительные ресурсы

- виртуальные процессорные ядра (vCPU);
- виртуальная оперативная память (vRAM);
- виртуальное дисковое пространство (vHDD);
- шлюз NSX Edge Gateway;
- гостевые ОС Windows и Linux;
- экземпляры ПО Microsoft.

Сетевые сервисы и компоненты

- подключение к сети интернет (в общем канале);
- один публичный IP-адрес.

Основные компоненты облачной платформы VMware

- VMware vSphere;
- VMware Cloud Director;
- VMware NSX;
- VMware vRealize Log Insight;
- VMware vRealize operations.

VMware vSphere

VMware vSphere представляет собой платформу виртуализации, обеспечивает динамическую балансировку нагрузки на серверы и системы хранения данных для достижения оптимальной производительности. Составными частями платформы VMware vSphere являются:

VMware ESXi – аппаратный гипервизор, разделяющий ресурсы физического сервера между несколькими виртуальными машинами.

VMware vCenter - централизованная платформа для управления средами VMware vSphere, помогающая автоматизировать виртуальную инфраструктуру и безопасно предоставлять к ней доступ в облаке.

VMware High Availability (HA) – механизм, позволяющий восстанавливать работоспособность виртуальных машин после аппаратного сбоя узлов виртуализации.

VMware DRS – механизм, равномерно распределяющий ВМ между всеми узлами кластера и обеспечивающий заданную производительность виртуальных машин в штатном и нештатном (в случае сбоев) режимах работы.

VMware vMotion - механизм «живой» миграции ВМ между узлами кластера для сервисного обслуживания без прерывания работы пользовательских ВМ.

VMware Cloud Director (vCD)

Cloud Director предоставляет конечным пользователям безопасные, изолированные пулы ресурсов для быстрой инициализации Виртуального ЦОД и реализует единую консоль управления.

VMware NSX

VMware NSX используется для создания программно-определяемых сетей, инкапсуляции трафика через протокол VXLAN для построения логических L2-сетей в рамках уже существующей коммутации на уровне L3. Позволяет заказчикам самостоятельно создавать выделенные сегменты сети и определять правила маршрутизации между сетями своих виртуальных ЦОД, без изменений в физической коммутации.

VMware vRealize Log Insight

VMware vRealize Log Insight – средство для сбора и анализа всех типов данных. Позволяет управлять журналами событий с помощью удобных панелей мониторинга и интеллектуальных средств анализа. Подробная визуализация рабочих процессов позволяет ускорить устранение неполадок в инфраструктуре Исполнителя.

VMware vRealize operations

VMware vRealize operations - инструмент расширенного мониторинга производительности виртуальной инфраструктуры. Собирает данные о развернутых виртуальных машинах и приложениях, включая данные об использовании процессорных ресурсов, оперативной памяти, утилизации дисковой подсистемы, длительности регистрации и производительности удаленного отображения. Опция доступна к подключению отдельно и тарифицируется дополнительно к основной Услуге.

2.3. Обеспечение защиты инфраструктуры облачной платформы SberCloud

- защита инфраструктуры облачной платформы и средств ее управления;
- защита консоли Cloud Director;
- изоляция ВЦОД.

Защита инфраструктуры облачной платформы SberCloud и средств ее управления

Защита инфраструктуры облачной платформы SberCloud и средств ее управления обеспечивается на следующих уровнях:

- на физическом уровне обеспечивается
 - размещение всего оборудования инфраструктуры в ЦОД, соответствующих требованиям надежности по категории Tier 3;
 - контроль и управление доступом к оборудованию;

– наличие системы видеонаблюдения на объектах информатизации ЦОД.

- на сетевом уровне обеспечивается защита периметров ЦОД и их сегментирование с использованием межсетевых экранов нового поколения (NGFW), осуществляющих в том числе выявление и предотвращение компьютерных атак;

- на инфраструктурном уровне обеспечивается:

- антивирусная защита инфраструктуры с использованием антивирусных средств для облачных сред;

- управление доступом к инфраструктуре с использованием средств двухфакторной аутентификации подключающихся к ней администраторов;

- контроль действий привилегированных пользователей с использованием специализированных средств;

- регулярный контроль и анализ защищенности инфраструктуры с использованием специализированных средств по выявлению уязвимостей в используемом ПО и его некорректной конфигурации, влияющей на уровень защищенности ПО, с устранением выявленных уязвимостей и/или недостатков;

- сбор и анализ событий информационной безопасности.

Помимо этого осуществляются периодические тестирования на проникновение и аудит информационной безопасности инфраструктуры облачной платформы SberCloud с привлечением сторонних организаций. Выявленные в ходе соответствующего тестирования и/или аудита недостатки устраняются по факту их выявления.

Защита консоли Cloud Director

Защита консоли Cloud Director обеспечивается на уровне приложений с использованием специализированного межсетевого экрана уровня приложений (Web Application Firewall). Помимо этого, осуществляются регулярные сканирования консоли на наличие актуальных уязвимостей и его периодические тестирования на проникновение с привлечением сторонних организаций. Выявленные уязвимости и/или недостатки устраняются по факту их выявления.

Изоляция «Организаций» Заказчика

Изоляция «Организаций» Заказчика осуществляется на уровне облачной платформы встроенными средствами VMware Cloud и на сетевом уровне средствами VMware NSX. Помимо этого, в рамках периодических тестирований на проникновение всей инфраструктуры проводятся тестирования на возможность проникновения потенциального нарушителя из одной «Организации» в другую с преодолением используемых механизмов защиты.

2.3.1. Распределение ролей, обязанностей и ответственности Исполнителя и Заказчика в области ИБ в отношении Услуги

Распределение ролей, обязанностей и ответственности в области ИБ в отношении Услуги описано в Таблице 1.

Табл. 1. Распределение ролей, обязанностей и ответственности в области ИБ

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/ услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
Прикладной уровень и уровень операционных систем, установленных в ВМ ВЦОД Заказчика	Журналирование событий	Журналирование событий в прикладном программном обеспечении (в том числе СУБД, серверах приложений, WEB-серверах) и операционных системах, установленных в виртуальных машинах (ВМ) Заказчика.	Заказчик	Заказчик
	Управление доступом	Управление доступом к прикладному программному обеспечению (в том числе СУБД, серверам приложений, WEB-серверам) и операционным системам, установленным в ВМ Заказчика.	Заказчик	Заказчик
	Управление аутентификационной информацией	Управление аутентификационной информацией, используемой при доступе к прикладному программному обеспечению (ППО) и операционным системам (ОС), установленным в ВМ Заказчика.	Заказчик	Заказчик
	Управление уязвимостями	Контроль и анализ защищенности ОС и ППО, функционирующего в ВМ ВЦОД Заказчика, в том числе установка критических обновлений безопасности, правка конфигураций ППО, а также изменение легко-подбираемых паролей и паролей доступа по умолчанию к сервисам и компонентам ОС и ППО, обнаруженных в ходе контроля и анализа защищенности.	Заказчик	Заказчик
	Управление инцидентами ИБ	Сбор (в том числе с использованием средств SIEM) и анализ событий безопасности со всего ППО, ОС и средств защиты информации (СрЗИ), функционирующих в «Организации» (ВЦОД) Заказчика, а также мониторинг и реагирование на инциденты безопасности.	Заказчик	Заказчик
	Управление криптографией	Установка, настройка и администрирование в ВЦОД Заказчика средств криптографической защиты информации (СКЗИ) в исполнении Virtual Appliance. Настройка и администрирование размещенных в ЦОД Исполнителя программно-аппаратных СКЗИ и межсетевых экранов Заказчика.	Заказчик	Заказчик
	Установка и администрирование средств защиты	Установка, настройка и администрирование в ВМ ВЦОД Заказчика СрЗИ от несанкционированного доступа (НСД), антивирусных средств и прочих средств защиты информации, устанавливаемых в ВМ ВЦОД Заказчика.	Заказчик	Заказчик
	Управление резервированием информации	Установка и настройка в ВМ Заказчика средств резервного копирования (СРК) баз данных и прочей	Заказчик	Заказчик

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/ услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
		информации Заказчика, хранимой внутри ВМ его ВЦОД, а также администрирование указанных средств. Создание резервных копий информации Заказчика и её восстановление из резервных копий.		
	Обеспечение защиты персональных данных клиентов	Защита согласно 152-ФЗ персональных данных (ПДн) клиентов, обрабатываемых в ВМ ВЦОД Заказчика, в том числе, но не ограничиваясь защитой ПДн, обрабатываемых средствами установленных в ВМ ВЦОД Заказчика СУБД.	Заказчик	Заказчик
Уровень «Организации» и ВЦОД Заказчика	Журналирование событий	<p>Журналирование событий, связанных с функционированием объектов ВЦОД Заказчика (например, его ВМ) и действиями пользователей в консолях VMware Cloud Director и Veeam Backup&Replication, таких как:</p> <ol style="list-style-type: none"> 1. вход/выход пользователей в/из консолей; 2. создание/удаление новых учётных записей пользователей и присвоение им привилегий доступа к консолям; 3. создание/удаление ВМ; 4. запуск/останов ВМ; 5. создание клонов ВМ; 6. изменение характеристик ВМ; 7. настройка NAT/DHCP/L2VPN/L3VPN, маршрутизации, балансировщика нагрузки и/или правил межсетевого экранирования на VMware NSX Edge в «Организации» Заказчика с использованием консоли VMware Cloud Director; 8. создание/изменение задания резервного копирования с использованием консоли Veeam Backup&Replication; 9. восстановление ВМ из резервной копии с использованием консоли Veeam Backup&Replication; 10. восстановление файлов из резервной копии с использованием консоли Veeam Backup&Replication; 11. изменение дисковой политики по умолчанию для VDC; 12. включение/отключение дополнительных услуг (логирование, DFW, VPN и прочее). 	Исполнитель	Заказчик
	Администрирование «Организацией» и управление доступом к ней	Администрирование «Организацией» Заказчика с использованием консоли VMware Cloud Director.	Исполнитель (ответственность за предоставление сервиса vCD)	Заказчик

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/ услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
		Администрирование доступом к «Организации» Заказчика с использованием консоли VMware Cloud Director.	Заказчик (ответственность за администрирование «Организацией» и доступом к ней)	
	Управление аутентификационной информацией	Создание/удаление новых учётных записей в «Организации» и присвоение им привилегий доступа к «Организации» Заказчика.	Исполнитель (ответственность за предоставление сервиса) Заказчик (ответственность за управление аутентификационной информацией)	Заказчик
	Управление безопасностью и прочими настройками для виртуальных сетей	Создание, удаление и администрирование с использованием консоли VMware Cloud Director необходимых VxLAN в процессе администрирования ВЦОД Заказчика. Межсетевое экранирование периметра ВЦОД Заказчика с использованием VMware NSX Edge. Обеспечение внутреннего сегментирования (с использованием VMware Cloud Director) и внутреннего межсетевого экранирования (с использованием VMware NSX Edge) ВЦОД Заказчика. Настройка NAT/DHCP/L2VPN/L3VPN, маршрутизации и балансировщика нагрузки на VMware NSX Edge в «Организации» Заказчика с использованием консоли VMware Cloud Director.	Исполнитель (ответственность за предоставление сервиса) Заказчик (ответственность за администрирование)	Заказчик
	Управление резервированием информации	Управление резервированием информации Заказчика с использованием консоли средства резервного копирования Veeam Backup&Replication, включающее в себя: 1. создание/изменение заданий резервного копирования информации Заказчика; 2. восстановление ВМ Заказчика из резервной копии; 3. восстановление файлов Заказчика из резервной копии.	Исполнитель (ответственность за предоставление сервиса) Заказчик (ответственность за управление резервированием своей информации)	Заказчик
	Установка и использование СЗИ	Установка, администрирование, своевременное обновление и безотлагательная установка критических обновлений безопасности на используемых в ВЦОД Заказчика виртуальных средствах защиты информации в исполнениях Virtual appliance (межсетевые экраны,	Заказчик	Заказчик

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/ услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
		системы обнаружений и/или предотвращений компьютерных атак и прочее). Настройка и администрирование программно-аппаратных средств защиты информации Заказчика, в том числе средств криптографической защиты информации, размещаемых в ЦОД Исполнителя.		
	Обеспечение защиты персональных данных клиентов	Обеспечение соответствия ВЦОД в составе информационных систем персональных данных (ИСПДн) Заказчика требованиям 152-ФЗ.	Заказчик	Заказчик
Инфраструктурный уровень	Мониторинг и поддержка	Мониторинг инфраструктуры облачной платформы SberCloud, обеспечение её доступности, производительности, наличия необходимого количества оборудования, обеспечение необходимой для её работы пропускной способности сети, вычислительных мощностей и емкости систем хранения данных (СХД) инфраструктуры.	Исполнитель	Исполнитель
	Журналирование событий	Журналирование событий в компонентах облачной платформы и средствах защиты информации инфраструктуры облачной платформы SberCloud.	Исполнитель	Исполнитель
	Управление доступом	Управление доступом к сегменту управления инфраструктурой облачной платформы SberCloud, её VLAN-ам и компонентам.	Исполнитель	Исполнитель
	Управление аутентификационной информацией	Управление учётными записями AD привилегированных пользователей, имеющих доступ к сегменту управления инфраструктурой облачной платформы SberCloud, и их вторым фактором аутентификации (аутентификаторами).	Исполнитель	Исполнитель
	Управление уязвимостями	Контроль и анализ защищенности служебных VM MGMT-сегмента и ESXi-серверов инфраструктуры облачной платформы SberCloud.	Исполнитель	Исполнитель
	Управление инцидентами ИБ	Сбор с использованием средств SIEM с компонентов облачной платформы и средств защиты информации инфраструктуры облачной платформы SberCloud событий безопасности. Анализ собранных событий безопасности, а также мониторинг и реагирование на инциденты безопасности с привлечением внешнего SOC.	Исполнитель	Исполнитель
	Управление конфигурацией	Контроль и управление процессами изменения конфигурации инфраструктуры облачной платформы SberCloud	Исполнитель	Исполнитель

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/ услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
	Управление безопасностью для виртуальных и физических сетей	Защита периметров ЦОД инфраструктуры облачной платформы SberCloud с использованием кластеров высокопроизводительных межсетевых экранов нового поколения (NGFW), обеспечивающих межсетевое экранирование и защиту от компьютерных атак инфраструктуры. Защита сетевой инфраструктуры облачной платформы SberCloud (входа в облако) от DDoS-атак, направленных на переполнение канальной емкости. Внутреннее сегментирование сетевых инфраструктур облачной платформы SberCloud с использованием NGFW и выделением в рамках ЦОД на сетевом уровне DMZ, PROD- и MGMT-сегментов инфраструктуры.	Исполнитель	Исполнитель
	Установка и администрирование средств защиты	Установка, настройка и администрирование средств защиты информации в составе инфраструктуры облачной платформы SberCloud, в том числе: 1. средств антивирусной защиты; 2. средств контроля действий привилегированных пользователей (администраторов SberCloud) класса PIM&PAM; 3. SIEM; 4. средств контроля и анализа защищенности; 5. WEB Application Firewall (WAF), используемого для защиты публикуемых консолей VMware Cloud Director и Veeam Backup&Replication; 6. NGFW; 7. Identity and access management (IAM).	Исполнитель	Исполнитель
	Управление резервированием информации	Резервное копирование и восстановление из образов служебных виртуальных машин инфраструктуры облачной платформы SberCloud с использованием СРК Veeam Backup&Replication.	Исполнитель	Исполнитель
	Обеспечение защиты персональных данных клиентов	Защита ПДн сотрудников Заказчика, имеющих доступ к консолям Veeam и Cloud, обрабатываемых в инфраструктуре облачной платформы SberCloud.	Исполнитель	Исполнитель
Физический уровень	Контроль доступа	Контроль доступа в ЦОД и помещения инфраструктуры облачной платформы SberCloud (охраняемая территория ЦОД, пропускной режим, системы контроля и управления доступом, запирающие стоек).	Исполнитель	Исполнитель
	Видеонаблюдение	Наличие внешней (по периметру ЦОД) и внутренней (в машинных залах ЦОД) систем видеонаблюдения	Исполнитель	Исполнитель

Наименование технологического (архитектурного) уровня	Применимые к уровню процессы/ услуги/сервисы ИБ	Описание процесса/сервиса/услуги	Ответственность за предоставление/ администрирование услуги/сервиса/ процессов	Кому предоставлен доступ к средствам предоставления услуги/сервиса/ процесса
	Размещение оборудования	<p>Предоставление электропитания, доступа к сети Интернет и свободного места в стойках ЦОД.</p> <p>Предоставление, монтаж и коммутация оборудования (compute, network и storage) в стойках ЦОД.</p> <p>Размещение, подключение к питанию, сети Интернет и ВЦОД Заказчика средств защиты информации Заказчика, в том числе средств криптографической защиты информации.</p>	Исполнитель	Исполнитель

2.4. Типы ресурсов

2.4.1. Виртуальные процессорные ядра (vCPU)

При формировании Заказа Заказчику предоставляется выбор из следующих ядер: с частотой 2,1 ГГц; 2,4 ГГц; 2,6 ГГц; 3,0 ГГц; 3,5 ГГц.¹

vCPU обслуживаются физическими процессорами Intel.

Рекомендации и ограничения:

В рамках одного Виртуального ЦОД Заказчик может использовать только vCPU с одинаковой частотой (обслуживаемые процессорами одного типа).

2.4.2. Виртуальная оперативная память (vRAM)

При формировании Заказа Заказчик указывает требуемый объем vRAM.

Важно: при формировании Заказа услуги требуемый объем vRAM должен быть дополнительно учтен в рамках заказываемого объема Виртуального дискового пространства (vHDD) выбранного профиля для размещения swar-файлов виртуальных серверов.

Рекомендации и ограничения:

Минимальное значение для экземпляра Виртуального ЦОД – 1 Гб.

2.4.3. Виртуальное дисковое пространство (vHDD)

В рамках услуги предоставляется три дисковых профиля, отличающихся по скорости обмена данными (количеству операций ввода-вывода (IOPS)) и времени отклика: SATA/NLSAS, SAS и SSD. Каждый дисковый профиль соответствует своему типу дисков на системе хранения данных.

В рамках одного Виртуального ЦОД можно использовать дисковые профили различного типа.

Важно: при заказе Виртуального дискового пространства отдельно должен быть учтен требуемый объем vRAM для размещения swar-файлов виртуальных серверов.

2.5. Типы подключения к сети

Для подключения к Услуге Заказчик может выбрать один или несколько типов подключения. Подключение через выделенный гарантированный² канал Интернет (Заказчику предоставляется отдельная полоса для доступа к Услуге, которая не разделяется с другими заказчиками) или подключение через общий канал Интернет (shared), который предполагает логическое подключение к общему для всех Заказчиков Услуги каналу передачи данных (скорость сетевого соединения для каждого Заказчика не является гарантированной и зависит от загруженности общего канала передачи данных). Доступные подключения:

- **Подключение к сервису в облаке через сеть Интернет - NAT**

Пользователи подключаются к виртуальной машине в облаке, опубликованной через IP адрес, маршрутизируемый в сети Интернет. Данный сценарий рекомендуется использовать для предоставления доступа к публичному сервису через сеть Интернет.

Ограничения:

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

- **Подключение к сервису в облаке через Site to Site VPN – L3 VPN (IPsec VPN)**

¹ Технически допустимо выделять до 256 vCPU на один виртуальный сервер. Однако для лучшей производительности рекомендуется придерживаться значений, описанных в разделе «3. Базовая функциональность и метрики Услуги».

² Заданная скорость гарантируется внутри сети Исполнителя начиная от порта пограничного маршрутизатора узла связи SberCloud.

На сетевом оборудовании Заказчика (роутер или межсетевой экран) настраивается статический IPsec-тоннель в облако, с помощью которого пользователи подключаются к виртуальным машинам в облаке на IP адреса, маршрутизируемые в рамках облачной сети Заказчика. Данный сценарий рекомендуется использовать для связи on premise сетей Заказчика с сетями в облаке как основное подключение или как резервное подключение при наличии подключения через прямой канал связи.

Ограничения:

- Требуется наличие у Заказчика сетевого оборудования с поддержкой IPsec VPN;
- В базовой конфигурации доступна организация до 512 IPsec тоннелей. Технически есть возможность расширения данного количества до 1600, 4096 или 6000 тоннелей, что потребует дополнительных трудозатрат операторов и ресурсов облака.

Подключение через прямой канал связи. Данный способ подключения позволяет обеспечить взаимодействие сетей Заказчика с сетью в облаке с помощью выделенных каналов связи стороннего провайдера. Опционально, с помощью данного сценария, к Услуге Заказчика может быть подключен альтернативный канал в сеть Интернет. Для данного подключения могут быть использованы выделенные каналы Заказчика, организованные с использованием «темной оптики». Доступные подключения:

- **L2 подключение**

Данный сценарий позволяет связать сеть клиента в облаке с on-premise сетями клиента вне облака по L2. При таком подключении, существующие виртуальные машины в инфраструктуре Заказчика будут находиться в одной L2/L3 сети с машинами в облаке, что дает возможность для реализации такого сервиса как миграция машин без смены IP адреса. Данный сценарий рекомендуется использовать только как временное подключение для миграции виртуальных машин Заказчика из on premise инфраструктуры в облако. Либо на постоянной основе при технической невозможности работы приложений Заказчика между on premise и облаком по L3.

Ограничения:

- Сценарий не может быть развернут силами клиента из Cloud Director GUI. Для разворачивания требуется участие операторов облачного провайдера;
- Максимальная возможная производительность подключения – 10 Гб/с;
- Для максимальной утилизации подключения значение MTU на всем пути следования трафика должно быть установлено не менее 9000 байт.

При подключении через общий канал Интернет Заказчику предоставляется базовая защита информационных систем, размещаемых в инфраструктуре облачной платформы SberCloud, от DDoS-атак, направленных на исчерпание канальной ёмкости сетевой инфраструктуры облачной платформы SberCloud.

В остальных случаях, а также по запросу может быть предоставлена расширенная защита информационных систем Заказчика, размещаемых в инфраструктуре облачной платформы SberCloud, от DDoS-атак на всех уровнях до L7 включительно в виде отдельной тарифицируемой услуги.

Для обмена данными между виртуальными машинами в пределах ВЦОД используется внутреннее сетевое взаимодействие, реализованное на базе сетевого оборудования Исполнителя и средствами гипервизора VMware ESXi.

2.6. Сетевые сервисы NSX

Виртуальный шлюз VMware NSX Edge Gateway предоставляется по умолчанию в конфигурации Compact, достаточной для создания небольших вычислительных сред с малым количеством сервисов, и может быть изменен в случае необходимости обработки большего количества сетевых функций. Ознакомиться с возможными конфигурациями и предельными значениями по эксплуатации виртуального шлюза VMware NSX Edge Gateway можно на официальном сайте по ссылке <https://configmax.vmware.com/guest?vmwareproduct=NSX>

Программный шлюз Edge Gateway предоставляет следующие сетевые сервисы:

- межсетевое экранирование (Firewall);
- маршрутизация (Routing);
- преобразование адреса (NAT);
- виртуальные частные сети (VPN) IPSec;

- динамическое распределение адресов DHCP.

Развертывание виртуального шлюза возможно в отказоустойчивой конфигурации (HA), при этом создается дополнительный шлюз в режиме ожидания, который перенимает на себя нагрузку в случае выхода из строя основного шлюза Edge Gateway.

2.7. Шаблоны ВМ и образы ОС

В рамках Услуги Заказчик может самостоятельно выполнить импорт/экспорт собственного образа ВМ в ВЦОД. Возможный вариант работы с образами ВМ: Заказчик самостоятельно осуществляет импорт/экспорт образов виртуальных машин, используя консоль управления Cloud Director.

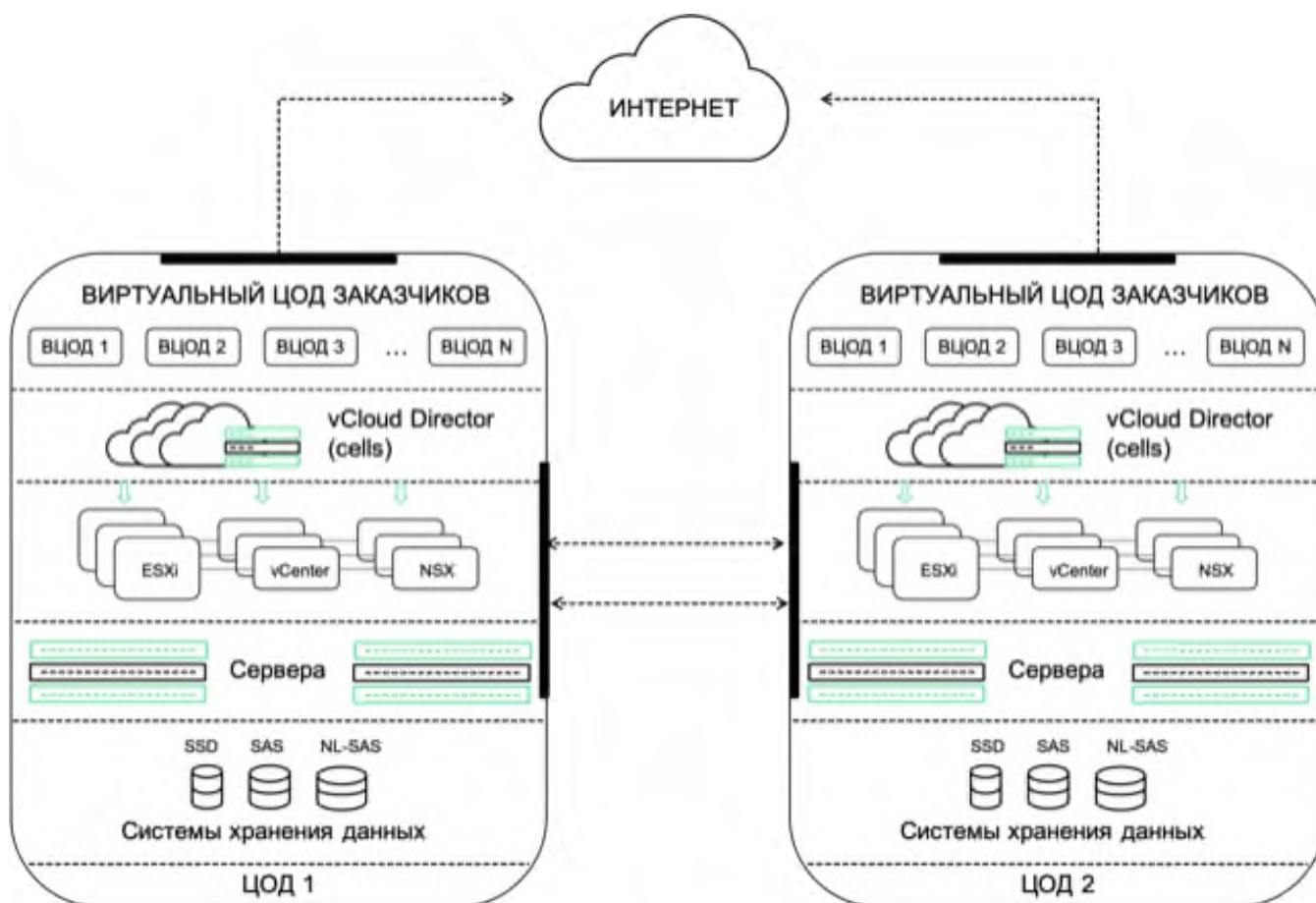
Дополнительно Заказчику предоставляется доступ к каталогу с шаблонами ВМ с предустановленными наиболее популярными версиями операционных систем Windows и Linux.

2.8. Программная платформа

Услуга реализована на базе платформы виртуализации VMware vSphere. В качестве инструмента реализации облачной инфраструктуры используется VMware Cloud Director.

Устойчивость к отказам вычислительных узлов реализована средствами платформы виртуализации VMware vSphere на базе технологии vSphere High Availability (HA).

Схема реализации платформы для услуги «Виртуальный ЦОД (VDC)» изображена ниже:



2.9. Аппаратная платформа

Серверная платформа

В качестве вычислительной платформы используются серверные решения корпоративного уровня, базирующиеся на процессорах архитектуры x86/64.

СХД Система хранения данных

Для организации сервиса предоставления виртуальных дисков применяются системы хранения данных уровня middle-range с резервированием основных компонент, таких как блоки питания, контроллерные модули.

Сеть

Сеть базируется на оборудовании ведущих мировых производителей, которое обеспечивает:

- высокий уровень контроля и безопасности благодаря потоковой телеметрии и упреждающему анализу на линейной скорости передачи;
- высокую производительность приложений благодаря интеллектуальным буферам и отсутствию потери пакетов;
- высокую производительность и масштабируемость благодаря мультискоростным портам 1/10/25/50/100G.

Сетевая подсистема реализована с применением топологии Leaf - Spine, которая обеспечивает следующие преимущества:

- предсказуемость задержек;
- высокий уровень масштабируемости без прерывания работы сети;
- высокий уровень автоматизации управления и поддержки;
- защита от появления петель.

2.10. Мониторинг

Мониторинг – дополнительный сервис для отслеживания состояния ВМ, реализованный средствами VMware vRealize Operations Advanced. VMware vRealize Operations собирает информацию с различных источников и использует продвинутые алгоритмы аналитики для изучения и распознавания нормального поведения каждого объекта мониторинга. При помощи консоли и генерируемых отчетов Заказчик получает все детали для анализа и принятия осознанного решения в следующих областях:

- поиск и устранение проблем с производительностью;
- состояние виртуальной инфраструктуры и предупреждение о возможных проблемах;
- прогнозирование и управление утилизацией инфраструктуры.

vRealize Operations является дополнительной опцией, которая может быть подключена при создании нового или уже к существующему ВЦОД.

Доступ к функциональности расширенного мониторинга осуществляется через консоль vRealize Operations (ссылка на консоль предоставляется отдельно).

2.11. Предоставление доступа к программному обеспечению Microsoft и Red Hat

В рамках партнерских соглашений Microsoft SPLA и Red Hat CCSP Исполнитель предлагает Заказчику доступ к программному обеспечению Microsoft и Red Hat. Перечень такого программного обеспечения Заказчик может запросить у ответственного лица Исполнителя (п. 10.13 Договора), стоимость определяется в соответствующем бланке Заказа.

2.12. Предоставление доступа к каталогу шаблонов Bitnami

В рамках партнерской программы VMware Cloud Provider Managed Services Provider Исполнитель предоставляет Заказчику доступ к каталогу шаблонов Bitnami. Bitnami – сервис, который предоставляет предварительно настроенные шаблоны приложений открытого программного обеспечения. С перечнем доступных шаблонов Заказчик может ознакомиться на сайте Исполнителя по ссылке <https://sbercloud.ru/vmwarebitnami>. В рамках предоставляемого сервиса гарантируется успешное развертывание приложения из шаблона, при этом его дальнейшая настройка и поддержка производится Заказчиком. Доступ к сервису предоставляется на основании подписанного бланка Заказа.

2.13. Предоставление доступа к расширенным сетевым сервисам NSX – L2VPN и Distributed Firewall

В рамках партнерской программы VMware Cloud Provider Program Исполнитель предоставляет Заказчику доступ к расширенным сетевым сервисам виртуального шлюза NSX Data Center SP Professional – L2VPN и

распределенному межсетевому экрану (Distributed firewall) для виртуальных серверов и приложений, запускаемых на физическом оборудовании Исполнителя. Доступ к сервису предоставляется на основании подписанного бланка Заказа.

2.14. Именованное «Организаций» Заказчика

Для корректной обработки обращений Заказчика именованное «Организаций» выполняется операторами Исполнителя и имеет унифицированный формат вида <Название «Организации» Заказчика> - <Порядковый номер «Организации заказчика»>. По согласованию с Исполнителем возможно изменение названия «организации» Заказчика через соответствующий запрос в службу поддержки Исполнителя.

3. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И МЕТРИКИ УСЛУГИ

Услуга Виртуальный ЦОД на базе VMware описана в Таблице 2.

Табл. 2. Параметры предоставляемых Услуг

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Вычисления	Виртуальный процессор 3,5 ГГц, VMware (шт.)	Базовая частота процессора vCPU	3,5 ГГц
		Рекомендуемое кол-во vCPU 3,5 ГГц на Виртуальный сервер (шт.)	1 - 8 шт.
		Допустимый объем vRAM на виртуальный сервер с vCPU 3,5 ГГц	1 – 384 Гб
	Виртуальный процессор 3,0 ГГц, VMware (шт.)	Базовая частота процессора vCPU	3,0 ГГц
		Рекомендуемое кол-во vCPU 3,0 ГГц на Виртуальный сервер (шт.)	1 - 48 шт.
		Допустимый объем vRAM на виртуальный сервер с vCPU 3,0 ГГц	1 - 768 Гб
	Виртуальный процессор 2,6 ГГц, VMware (шт.)	Базовая частота процессора vCPU	2,6 ГГц
		Рекомендуемое кол-во vCPU 2,6 ГГц на Виртуальный сервер (шт.)	1 – 28 шт.
		Допустимый объем vRAM на виртуальный сервер с vCPU 2,6 ГГц	1 – 768 Гб
	Виртуальный процессор 2,4 ГГц, VMware (шт.)	Базовая частота процессора vCPU	2,4 ГГц
		Рекомендуемое кол-во vCPU 2,4 ГГц на Виртуальный сервер (шт.)	1 - 40 шт.
		Допустимый объем vRAM на виртуальный сервер с vCPU 2,4 ГГц	1 – 768 Гб
	Виртуальный процессор 2,1 ГГц, VMware (шт.)	Базовая частота процессора vCPU	2,1 ГГц
		Рекомендуемое кол-во vCPU 2,1 ГГц на Виртуальный сервер (шт.)	1 – 44 шт.
		Допустимый объем vRAM на виртуальный сервер с vCPU 2,1 ГГц	1 – 768 Гб

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Хранилище данных	Виртуальный жесткий диск SSD, VMware (Гб)	HDD IOPS. Эталонные значения	2000 IOPS/1 000GB
		Среднее время доступа к SSD Storage на виртуальной машине	0 мс - 5 мс
		Шаг увеличения размера виртуального диска в допустимом диапазоне	1 Гб
	Виртуальный жесткий диск SAS, VMware (Гб)	HDD IOPS. Эталонные значения	500 IOPS/1 000GB
		Среднее время доступа к SAS Storage на виртуальной машине	0 мс - 25 мс
		Шаг увеличения размера виртуального диска в допустимом диапазоне	1 Гб
	Виртуальный жесткий диск SATA, VMware (Гб)	HDD IOPS. Эталонные значения	100 IOPS/1 000GB
		Среднее время доступа к SATA Storage на виртуальной машине	0 мс - 30 мс
		Шаг увеличения размера виртуального диска в допустимом диапазоне	1 Гб
Сетевые сервисы	Доступ в Интернет в общем канале	Полоса пропускания	Не тарифицируется: не более 100 Мб/с на Виртуальный ЦОД на базе VMware
	Пропускная способность на виртуальный сервер	Средняя сетевая задержка в пределах сети передачи данных SberCloud	0 мс - 5 мс
		Процент потерянных пакетов в пределах сети передачи данных SberCloud	0% - 0,2 %
	Публичный IP (шт.)	Процент потерянных пакетов в пределах сети передачи данных SberCloud	0% - 0,2 %
		Средняя сетевая задержка в пределах сети передачи данных SberCloud	0 мс - 5 мс
		Полоса пропускания	По значениям услуги «Сеть внешняя»

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
	Виртуальный шлюз (шт.)	Средняя сетевая задержка в пределах сети передачи данных SberCloud	0 мс - 5 мс
		Пропускная способность	Не более 10 Гб/с
Гостевая ОС	Доступ к шаблону гостевой ОС MS Windows server: <ul style="list-style-type: none"> ■ ВМ размером 4 и менее vCPU: ВМ (шт.)/ календарный мес.³ ■ ВМ размером более 4 vCPU: vCPU (шт.)/ календарный мес.³ 	Шаблоны гостевых ОС Windows server	Windows server 2012
			Windows server 2016
			Windows server 2019
	Доступ к шаблону гостевой ОС Red Hat Enterprise Linux: <ul style="list-style-type: none"> ■ ВМ размером 24 и менее vCPU: ВМ тип SVG (шт.)/календарный мес.³ ■ ВМ размером более 24 vCPU: ВМ тип LVG (шт.)/календарный мес.³ 	Шаблоны гостевых ОС Red Hat Enterprise Linux	Red Hat Enterprise Linux 7
			Red Hat Enterprise Linux 8
ПО	Доступ к шаблону ПО MS SQL server: <ul style="list-style-type: none"> ■ ВМ размером 1-12 vCPU: ВМ (шт.)/календарный мес^{3 4}. 	Шаблоны ПО MS SQL Server	SQL Server 2017 Enterprise Edition
			SQL Server 2019 Enterprise Edition
ПО	Доступ к экземплярам ПО Microsoft (Exchange, Office, Productivity Suite, Project, SharePoint, Skype for Business Server, SQL Server Standard Edition, Visio, Windows Remote Desktop Services, Windows Rights Management Services): <ul style="list-style-type: none"> ■ Пользователь (шт.)/календарный месяц³. 	Экземпляры ПО Microsoft (Exchange, Office, Productivity Suite, Project, SharePoint, Skype for Business Server, SQL Server Standard Edition, Visio, Windows Remote Desktop Services, Windows Rights Management Services)	Поддерживаемые версии ПО Microsoft в рамках MS SPLA программы (Exchange, Office, Productivity Suite, Project, SharePoint, Skype for Business Server, SQL Server Standard Edition, Visio, Windows Remote Desktop Services, Windows Rights Management Services)

³ Минимальный период тарификации – календарный месяц. Начало использования, начиная с первой минуты, или продолжение использования Услуги в отчетном периоде предполагает списание стоимости за полный календарный месяц. Неполный календарный месяц использования Услуги, начиная с первой минуты, округляется до полного календарного месяца пользования Услугой.

⁴ При использовании большего количества vCPU в составе экземпляра ВМ, пропорционально увеличивается количество квантов услуги для оплаты (с шагом в 12 vCPU).

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
ПО	<p>Доступ к экземплярам ПО Microsoft (SQL Server Enterprise Core, SQL Server Standard Core, SQL Server Web Edition, Windows Server Datacenter, Windows Server Standard):</p> <ul style="list-style-type: none"> Два физических ядра (шт.)/ календарный месяц³. 	<p>Экземпляры ПО Microsoft (SQL Server Enterprise Core, SQL Server Standard Core, SQL Server Web Edition, Windows Server Datacenter, Windows Server Standard):</p>	<p>Поддерживаемые версии ПО Microsoft в рамках MS SPLA программы (SQL Server Enterprise Core, SQL Server Standard Core, SQL Server Web Edition, Windows Server Datacenter, Windows Server Standard).</p>
ПО	<p>Доступ к экземплярам ПО Microsoft (SharePoint Hosting, Windows Server Essentials):</p> <ul style="list-style-type: none"> Физический процессор (шт.)/ календарный месяц³. 	<p>Экземпляры ПО Microsoft (SharePoint Hosting, Windows Server Essentials)</p>	<p>Поддерживаемые версии ПО Microsoft в рамках MS SPLA программы (SharePoint Hosting, Windows Server Essentials).</p>

4. ТАРИФИКАЦИЯ УСЛУГИ

4.1. Статическая тарификация (Allocation).

Величина ежемесячного платежа за пользование услугой определяется в соответствии с заказанным объёмом перечисленных ниже ресурсов и опций:

- Виртуальный процессор 2,1 ГГц, VMware;
- Виртуальный процессор 2,4 ГГц, VMware;
- Виртуальный процессор 2,6 ГГц, VMware;
- Виртуальный процессор 3,0 ГГц, VMware;
- Виртуальный процессор 3,5 ГГц, VMware;
- Виртуальная память, VMware⁵;
- Виртуальный жесткий диск SATA, VMware;
- Виртуальный жесткий диск SAS, VMware;
- Виртуальный жесткий диск SSD, VMware;
- Предоставление публичного IP адреса;
- Сетевой шлюз NSX Edge Compact;
- Сетевой шлюз NSX Edge Large;
- Сетевой шлюз NSX Edge Quad-Large;
- Сетевой шлюз NSX Edge X-large;
- Доступ к расширенным сетевым сервисам NSX – L2VPN и Distributed Firewall;
- Панель мониторинга VMware vRealize Operations Advanced;
- Доступ к гостевой ОС MS Windows Server³;
- Доступ к гостевой ОС Red Hat Enterprise Linux Server³;
- Доступ к каталогу шаблонов Bitnami;
- Доступ к шаблону ПО MS SQL Server³;
- Доступ к экземплярам ПО Microsoft (Exchange, Office, Productivity Suite, Project, SharePoint, Skype for Business Server, SQL Server, Visio, Windows Remote Desktop Services, Windows Rights Management Services, Windows Server)³.

Методика расчётов потребляемых процессорных ресурсов и оперативной памяти предполагает тарификацию суммы значений выбранных ресурсов за отчётный период (один месяц) в соответствии с тарифом. На основе суммы значений выставляется счёт.

Методика расчёта потребляемого дискового пространства предполагает оплату за выбранный Заказчиком объём ресурсов дискового пространства.

4.2. Динамическая тарификация (Pay as you go).

Величина ежемесячного платежа за пользование Услугой определяется в соответствии с потребленным объёмом перечисленных ниже ресурсов и опций:

- Виртуальный процессор 2,1 ГГц, VMware;
- Виртуальный процессор 2,4 ГГц, VMware;
- Виртуальный процессор 2,6 ГГц, VMware;
- Виртуальный процессор 3,0 ГГц, VMware;
- Виртуальный процессор 3,5 ГГц, VMware;
- Виртуальная память, VMware⁵;
- Виртуальный жесткий диск SATA, VMware;

⁵ Объем Виртуальной памяти (vRAM) должен быть дополнительно учтен при заказе Виртуального дискового пространства для хранения swar-файлов виртуальных серверов в соответствии с пунктом 2.4.2 настоящего приложения.

- Виртуальный жесткий диск SAS, VMware;
- Виртуальный жесткий диск SSD, VMware;
- Сетевой шлюз NSX Edge Compact;
- Сетевой шлюз NSX Edge Large;
- Сетевой шлюз NSX Edge Quad-Large;
- Сетевой шлюз NSX Edge X-large;
- Доступ к расширенным сетевым сервисам NSX – L2VPN и Distributed Firewall;
- Панель мониторинга VMware vRealize Operations Advanced;
- Доступ к каталогу шаблонов Bitnami³;

Динамическая тарификация осуществляется в почасовом порядке (из расчета стоимости 1 (одного) часа), начиная с первой минуты использования. Стороны установили, что для удобства расчётов неполные часы использования Услуги, начиная с первой минуты, округляются до полного часа пользования Услугой.

Методика расчёта потребляемого дискового пространства предполагает оплату за выбранный Заказчиком объём ресурсов дискового пространства.

Данные (отчёты об использовании) по динамической тарификации Заказчик может запросить у менеджера по Договору.

5. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

5.1. Возможные виды подключения / изменения / отключения Услуг:

5.1.1. Посредством подписания Заказа.

5.2. Возможный порядок расчётов по Услуге:

5.2.1. Предварительная оплата.

5.2.2. Постоплата.

5.3. Возможные способы оплаты / порядок пополнения баланса:

5.3.1. Оплата в безналичном порядке на основании выставленного Исполнителем счёта.