

## ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ «ВИРТУАЛЬНЫЙ ЦОД на базе VMware»

### 1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГИ

- 1.1. Виртуальный ЦОД на базе VMware 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.
- 1.2. Услуга построена на основе модели обслуживания «IaaS». 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. Руководство Пользователя по Услуге доступно по электронному адресу: <https://docs.sbercloud.ru/vdc-vmware/ug/>.
- 1.3. Управление Виртуальным ЦОД осуществляется Заказчиком при помощи консоли Cloud Director.
- 1.4. **Состав и основные компоненты Услуги:**

Табл.1. Состав и основные компоненты

Ресурсы	
Наименование группы	Содержание
Вычислительные ресурсы	<ul style="list-style-type: none"> <li>- виртуальные процессорные ядра (vCPU);</li> <li>- виртуальная оперативная память (vRAM);</li> <li>- виртуальное дисковое пространство (vHDD);</li> <li>- шлюз NSX Edge Gateway.</li> </ul>
Сетевые сервисы и компоненты	<ul style="list-style-type: none"> <li>- подключение к сети интернет (в общем канале);</li> <li>- один публичный IP-адрес.</li> </ul>
Основные компоненты облачной платформы VMware	<ul style="list-style-type: none"> <li>- VMware vSphere;</li> <li>- VMware Cloud Director;</li> <li>- VMware NSX;</li> <li>- VMware vRealize Log Insight;</li> <li>- VMware vRealize operations.</li> </ul>

- 1.4.1. 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.
- 1.4.2. VMware Cloud Director (vCD) предоставляет конечным пользователям безопасные, изолированные пулы ресурсов для быстрой инициализации Виртуального ЦОД и реализует единую консоль управления.
- 1.4.3. 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.
- 1.4.4. VMware vRealize Log Insight является средством 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.

1.4.5. VMware vRealize operations представляет собой инструмент расширенного мониторинга производительности виртуальной инфраструктуры, который 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. Данная опция доступна к подключению отдельно и тарифицируется дополнительно к основной Услуге.

1.5. В целях обеспечения защиты инфраструктуры облачной платформы SberCloud реализовываются следующие меры и механизмы защиты:

Табл.2. Обеспечение защиты инфраструктуры облачной платформы SberCloud

Уровни защиты	Мероприятия
<b>Защита инфраструктуры облачной платформы и средств ее управления</b>	
Физический	Обеспечивается: <ul style="list-style-type: none"> <li>– размещение всего оборудования инфраструктуры в ЦОД, соответствующих требованиям надежности по категории Tier 3;</li> <li>– контроль и управление доступом к оборудованию;</li> <li>– наличие системы видеонаблюдения на объектах информатизации ЦОД.</li> </ul>
Сетевой	Обеспечивается защита периметров ЦОД и их сегментирование с использованием межсетевых экранов нового поколения (NGFW), осуществляющих в том числе выявление и предотвращение компьютерных атак.
Инфраструктурный	Обеспечивается: <ul style="list-style-type: none"> <li>– антивирусная защита инфраструктуры с использованием антивирусных средств для облачных сред;</li> <li>– управление доступом к инфраструктуре с использованием средств двухфакторной аутентификации подключающихся к ней администраторов;</li> <li>– контроль действий привилегированных пользователей с использованием специализированных средств;</li> <li>– 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;</li> <li>– сбор и анализ событий информационной безопасности.</li> </ul>
Дополнительный	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.
<b>Защита консоли Cloud Director</b>	
Приложения	Защита с использованием специализированного межсетевого экрана уровня приложений (Web Application Firewall).
Дополнительный	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.
<b>Изоляция «Организаций» Заказчика</b>	
Облачная платформа	Осуществляется встроенными средствами VMware Cloud Director
Сетевой	Осуществляется средствами VMware NSX.
Дополнительный	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.

1.6. Распределение ролей, обязанностей и ответственности в области ИБ в отношении Услуги описано в Таблице 3.

Табл. 3. 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 защиты информации (СЗИ) в исполнении Virtual Appliance. Настройка и администрирование размещенных в ЦОД Исполнителя программно-аппаратных СЗИ 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 информации Заказчика, хранимой внутри ВМ его ВЦОД, а также администрирование указанных средств. Создание резервных копий информации Заказчика и её восстановление из резервных копий.	Заказчик	Заказчик
	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	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: 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;	Исполнитель	Заказчик

Табл. 3. 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
		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).		
	Администрирование «Организацией» и управление доступом к ней	Администрирование «Организацией» Заказчика с использованием консоли VMware Cloud Director. Администрирование доступом к «Организации» Заказчика с использованием консоли VMware Cloud Director.	Исполнитель (ответственность за предоставление сервиса vCD)  Заказчик (ответственность за администрирование «Организацией» и доступом к ней)	Заказчик
	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

Табл. 3. 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
	Управление резервированием информации (предоставляется в рамках отдельной Услуги)	Управление резервированием информации Заказчика с использованием консоли средства резервного копирования Veeam Backup&Replication, включающее в себя: создание/изменение заданий резервного копирования информации Заказчика; восстановление ВМ Заказчика из резервной копии; 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, системы обнаружений и/или предотвращения компьютерных атак и прочее). Настройка и администрирование программно-аппаратных средств защиты информации Заказчика, в том числе средств криптографической защиты информации, размещаемых в ЦОД Исполнителя.	Заказчик	Заказчик
	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 ВМ 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 (в том числе с привлечением внешнего SOC).	Исполнитель	Исполнитель
	Управление конфигурацией	Контроль и управление процессами изменения конфигурации инфраструктуры облачной платформы SberCloud	Исполнитель	Исполнитель

Табл. 3. 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
	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
	Размещение оборудования	Предоставление электропитания, доступа к сети Интернет и свободного места в стойках ЦОД. Предоставление, монтаж и коммутация оборудования (compute, network и storage) в стойках ЦОД. Размещение, подключение к питанию, сети Интернет и ВЦОД Заказчика средств защиты информации Заказчика, в том числе средств криптографической защиты информации.	Исполнитель	Исполнитель

## 1.7. Типы ресурсов, требования, рекомендации и ограничения:

Табл.4. Типы ресурсов, требования, рекомендации и ограничения

Тип ресурса: виртуальные процессорные ядра (vCPU)	
Требования	Рекомендации и ограничения
При формировании Заказа Заказчику предоставляется выбор из следующих ядер: с частотой не менее 3,0 ГГц; не менее 3,5 ГГц <sup>1</sup> . vCPU обслуживаются физическими процессорами Intel.	В рамках одного Виртуального ЦОД Заказчик может использовать только vCPU с одинаковой частотой (обслуживаемые процессорами одного типа). Ограничения на количество vCPU указаны в Таблице «Параметры предоставляемых услуг» раздела 3 настоящего документа.
Тип ресурса: виртуальная оперативная память (vRAM)	
Требования	Рекомендации и ограничения
При формировании Заказа Заказчик указывает требуемый объем vRAM. 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.	Ограничения на количество vRAM указаны в Таблице «Параметры предоставляемых услуг» раздела 3 настоящего документа.
Тип ресурса: виртуальное дисковое пространство (vHDD)	
Требования	Рекомендации и ограничения
В рамках услуги предоставляется два дисковых профиля, отличающихся по скорости обмена данными (количеству операций ввода-вывода (IOPS)) и времени отклика: SATA/NLSAS и SSD. Каждый дисковый профиль соответствует своему типу дисков на системе хранения данных. В рамках одного Виртуального ЦОД можно использовать дисковые профили различного типа. <b>Важно:</b> при заказе Виртуального дискового пространства отдельно должен быть учтен требуемый объем vRAM для размещения swar-файлов виртуальных серверов. Выделенная емкость дискового пространства занимает все виртуальными машинами Заказчика (включенными и выключенными), созданными Заказчиком Snapshot, а также swar-файлами vRAM всех виртуальных машин Заказчика.	Минимальное значение для экземпляра Виртуального ЦОД – 100 Гб. Суммарный объем виртуального дискового пространства каждого дискового профиля должен быть кратен 100 Гб.

## 1.8. Для подключения к Услуге Заказчик может выбрать один или несколько типов подключения:

Табл.5. Типы подключения к сети и сетевые сервисы

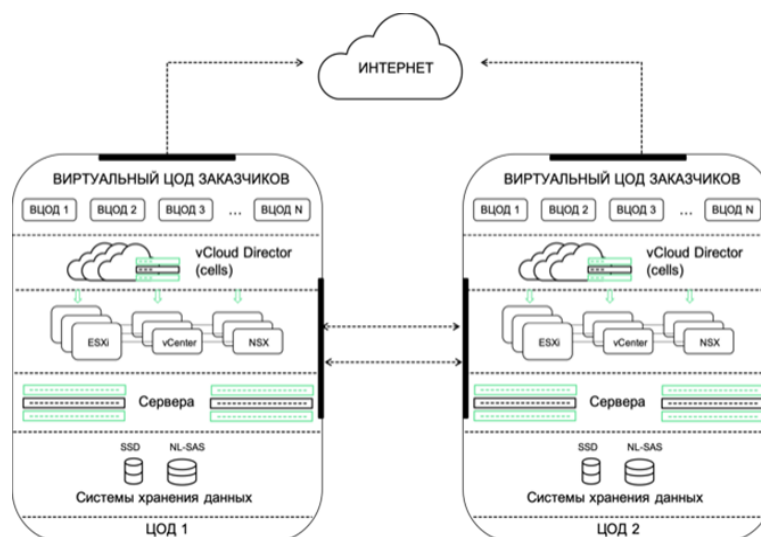
Тип подключения	Описание
Подключение через выделенный гарантированный <sup>2</sup> канал Интернет	Заказчику предоставляется отдельная полоса для доступа к Услуге, которая не разделяется с другими заказчиками.
Подключение через выделенный канал связи	Данный способ подключения позволяет обеспечить взаимодействие 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».
Подключение через общий канал Интернет	Предполагает логическое подключение к общему для всех Заказчиков Услуги каналу передачи данных (скорость сетевого соединения для каждого Заказчика не является гарантированной и зависит от загрузки общего канала передачи данных). 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.

Подробная информация по доступным подключениям приведена в Приложении № 1.6 к Договору.

<sup>1</sup> Технически допустимо выделять до 48/96 vCPU (для vCPU частотой 3,5/3,0 ГГц, соответственно) на один виртуальный сервер. Однако для лучшей производительности рекомендуется придерживаться значений, описанных в разделе «3. Базовая функциональность и метрики услуги».

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

- 1.8.1. 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.
- 1.8.2. Для обмена данными между виртуальными машинами в пределах ВЦОД используется внутреннее сетевое взаимодействие, реализованное на базе сетевого оборудования Исполнителя и средствами гипервизора VMware ESXi.
- 1.9. **Сетевые сервисы NSX:**
- 1.9.1. Виртуальный шлюз VMware NSX Edge Gateway - предоставляется по умолчанию в конфигурации Comrast, достаточной для создания небольших вычислительных сред с малым количеством сервисов, и может быть изменен в случае необходимости обработки большего количества сетевых функций.
- 1.9.2. 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.
- 1.10. **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 (в рамках Услуги доступа к программному обеспечению Microsoft) и Linux. При импорте и использовании Заказчиком собственных образов виртуальных машин, которые не имеют официальной совместимости со стороны VMware, Исполнитель не гарантирует работоспособность данных виртуальных машин, и решение возможных проблем не регулируется действующим Соглашением об уровне предоставлении Услуги.
- 1.11. **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 на рисунке ниже:



1.12. **Аппаратная платформа:**

Табл.6. Компоненты и характеристики аппаратной платформы

Компоненты	Характеристики
Серверная платформа	В качестве вычислительной платформы используются серверные решения корпоративного уровня, базирующиеся на процессорах архитектуры x86/64.
СХД	Для организации сервиса предоставления виртуальных дисков применяются системы хранения данных уровня middle-range с



	резервированием основных компонент, таких как блоки питания, контроллерные модули.
Сеть	<p>Базируется на оборудовании ведущих мировых производителей, которое обеспечивает:</p> <ul style="list-style-type: none"> <li>– высокий уровень контроля и безопасности благодаря потоковой телеметрии и упреждающему анализу на линейной скорости передачи;</li> <li>– высокую производительность приложений благодаря интеллектуальным буферам и отсутствию потери пакетов;</li> <li>– высокую производительность и масштабируемость благодаря мультискоростным портам 1/10/25/50/100G.</li> </ul> <p>Сетевая подсистема реализована с применением топологии Leaf - Spine, которая обеспечивает следующие преимущества:</p> <ul style="list-style-type: none"> <li>– предсказуемость задержек;</li> <li>– высокий уровень масштабируемости без прерывания работы сети;</li> <li>– защиту от появления петель;</li> <li>– высокий уровень автоматизации управления и поддержки.</li> </ul>

1.13. **Мониторинг.** Представляет собой дополнительный сервис для отслеживания состояния ВМ, реализованный средствами VMware vRealize Operations. 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).

#### 1.14. **Предоставление доступа к программному обеспечению Microsoft и Red Hat**

1.14.1. 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 (раздел 10 Договора), стоимость определяется в соответствующем бланке Заказа на основании Тарифов, установленных в Приложении 7.А.

1.14.2. В рамках предоставления доступа к программному обеспечению Microsoft Исполнитель предоставляет доступ к дистрибутивам продуктов Microsoft и предоставляет лицензию для активации данных продуктов. Техническая поддержка по продуктам Microsoft не включена в стоимость услуги и приобретается Заказчиком самостоятельно.

1.14.3. Базой для применения тарифа и расчета ежемесячного платежа за использование Windows Server является наибольшее число одновременно работавших виртуальных машин с Windows Server за расчетный период.

1.14.4. В случае индексации цен на лицензии Windows Server со стороны Microsoft, Исполнитель имеет право на индексацию Тарифа в одностороннем порядке на соответствующую величину с уведомлением Заказчика в срок не менее чем за 30 (тридцать) дней до даты изменения Тарифа. К уведомлению Заказчика Исполнитель прикладывает скан-копию соответствующего письма-уведомления от Microsoft. В случае необходимости Стороны подписывают Дополнительное соглашение о внесении изменений в Приложение № 7.А.

1.14.5. Подробная информация по условиям и ограничениям использования программного обеспечения Microsoft и Red Hat приведена в Приложении № 9 к Договору.

1.15. **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 в документации по ссылке <https://docs.sbercloud.ru/bitnami/ug/> в разделе «Ограничения и особенности». В рамках предоставляемого сервиса гарантируется успешное развертывание приложения из шаблона, при этом его дальнейшая настройка и поддержка производится Заказчиком.

1.16. **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 и оплачивается Заказчиком отдельно.

- 1.17. **Именованiе «Организаций» Заказчика.** Для корректной обработки обращений Заказчика именованiе «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.

## 2. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И МЕТРИКИ УСЛУГИ

2.1. Услуга Виртуальный ЦОД на базе VMware описана в Таблице 7:

Табл.7. Параметры предоставляемых Услуг

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Вычисления	Виртуальный процессор 3,5 ГГц, VMware (шт.)	Базовая частота процессора vCPU	Не менее 3,5 ГГц
		Host CPU Ready time	Менее 5%
		Рекомендуемое кол-во vCPU 3,5 ГГц на Виртуальный сервер (шт.)	1 - 24 шт.
		Допустимый объем vRAM на виртуальный сервер с vCPU 3,5 ГГц	1 – 384 Гб
		RAM Swapped	0%
	Виртуальный процессор 3,0 ГГц, VMware (шт.)	Базовая частота процессора vCPU	Не менее 3,0 ГГц
		Host CPU Ready time	Менее 5%
		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
		RAM Swapped	0%
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
		Допустимый объем одного виртуального жесткого диска SSD на виртуальный сервер	1 – 4096 Гб
		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
		Допустимый объем одного виртуального жесткого диска SATA на виртуальный сервер	1 – 4096 Гб
		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 %
	Виртуальный шлюз (шт.)	Средняя сетевая задержка в пределах сети передачи данных SberCloud	0 мс - 5 мс
		Пропускная способность	Не более 10 Гб/с

Табл.7. Параметры предоставляемых Услуг

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Гостевая ОС	Доступ к шаблону гостевой ОС Windows server: <ul style="list-style-type: none"> <li>• VM размером 4 и менее vCPU: VM (шт.)/ календарный мес<sup>3</sup>.</li> <li>• VM размером более 4 vCPU: vCPU (шт.)/ календарный мес<sup>3</sup>.</li> </ul>	Шаблоны гостевых ОС MS Windows Server	Windows Server 2016 Windows Server 2019 Windows Server 2022
	Доступ к шаблону гостевой ОС Red Hat Enterprise Linux: <ul style="list-style-type: none"> <li>• VM размером 24 и менее vCPU: VM тип SVG (шт.)/ календарный мес<sup>3</sup>.</li> <li>• VM размером более 24 vCPU: VM тип LVG (шт.)/ календарный мес<sup>3</sup>.</li> </ul>	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"> <li>• VM размером 1–12 vCPU: VM (шт.)/ календарный мес.<sup>3 4</sup></li> </ul>	Шаблоны ПО 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"> <li>• Пользователь (шт.)/календарный месяц<sup>3</sup>.</li> </ul>	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)
ПО	Доступ к экземплярам ПО Microsoft (SQL Server Enterprise Core, SQL Server Standard Core, SQL Server Web Edition, Windows Server Datacenter, Windows Server Standard): <ul style="list-style-type: none"> <li>• Два виртуальных/физических ядра (шт.)/ календарный месяц<sup>3</sup>.</li> </ul>	Экземпляры ПО Microsoft (SQL Server Enterprise Core, SQL Server Standard Core, SQL Server Web Edition, Windows Server Datacenter, Windows Server Standard).	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).

<sup>3</sup> 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.

<sup>4</sup> При использовании большого количества vCPU в составе экземпляра VM, пропорционально увеличивается количество доступных лицензий для оплаты (с шагом в 12 vCPU).

### 3. ТАРИФИКАЦИЯ УСЛУГИ

- 3.1. Тарификация Услуги статическая (Allocation).
- 3.2. Величина ежемесячного платежа за пользование услугой определяется в соответствии с заказанным объемом перечисленных ниже ресурсов и опций:
- Виртуальный процессор 3,0 ГГц, VMware;
  - Виртуальный процессор 3,5 ГГц, VMware;
  - Виртуальная память, VMware<sup>5</sup>;
  - Виртуальный жесткий диск SATA, 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;
  - Доступ к шаблону гостевой ОС MS Windows Server<sup>3</sup>;
  - Доступ к шаблону гостевой ОС Red Hat Enterprise Linux Server<sup>3</sup>;
  - Доступ к шаблону ПО MS SQL Server<sup>3</sup>;
  - 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).
- 3.3. Методика расчетов потребляемых процессорных ресурсов и оперативной памяти предполагает тарификацию суммы значений предоставленных ресурсов за Отчетный период (один месяц) в соответствии с тарифом. Счет выставляется на основе суммы значений.
- 3.4. Методика расчета потребляемого дискового пространства предполагает оплату за весь предоставленный Заказчику объем ресурсов дискового пространства каждого типа.
- 3.5. Методика расчета по опциям доступ к расширенным сетевым сервисам NSX и панель мониторинга VMware vRealize Operations предполагает тарификацию суммы значений оперативной памяти, предоставленной Заказчику в рамках его виртуального ЦОД в Отчетный период (один месяц).

### 4. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

- 4.1. **Возможные виды подключения / изменения / отключения Услуг:**
- 4.1.1. посредством подписания Заказа (с учетом п. 4.6. настоящего Приложения).
- 4.2. **Возможный порядок расчетов по Услуге:**
- 4.2.1. постоплата.
- 4.3. **Возможные способы оплаты / порядок пополнения баланса:**
- 4.3.1. оплата в безналичном порядке на основании выставленного Исполнителем счёта.
- 4.4. Заказчик самостоятельно несет ответственность за работоспособность программного обеспечения, устанавливаемого на ВМ.
- 4.5. Во избежание деградации производительности, переутилизации ресурсов хранения и повышения риска нарушения целостности диска при консолидации, Исполнитель оставляет за собой право проводить регламентные работы по удалению созданных Заказчиком SnapShot старше 7 (Семи) дней. Перед удалением SnapShot Исполнитель обязуется уведомить Заказчика по электронной почте, указанной в Договоре: за 5 (Пять) дней до удаления и за 1 (Один) день до удаления.
- 4.6. Стороны установили следующий порядок заказа Услуги по настоящему Приложению:
- 4.6.1. Заказ на подключение Услуги по настоящему Приложению должен быть направлен Исполнителю не позднее, чем за 6 (шесть) рабочих дней до даты начала оказания Услуги;
- 4.6.2. В течение 3 (трех) рабочих дней Исполнитель или его уполномоченный представитель обязуется рассмотреть Заказ на Услугу и направить лицу, направившему Заказ, ответ (подписанный со своей стороны Заказ или отказ в предоставлении Услуги с обоснованием причины);

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

- 4.6.3. В случае согласования Сторонами Заказа Услуга по такому Заказу предоставляется в дату начала оказания Услуги, зафиксированную в Заказе, с 10:00 по московскому времени.
- 4.7. Заказчик самостоятельно несет ответственность за сохранность данных и принимает самостоятельно меры по их сохранению при отказе от Услуги. При отказе от Услуги Исполнитель вправе удалить данные Заказчика по истечении 5 (пяти) рабочих дней после отказа от Услуги.