

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ «ВИРТУАЛЬНЫЙ ЦОД»

1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГИ

- 1.1. Виртуальный ЦОД 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/ug/>.
- 1.3. Управление Виртуальным ЦОД осуществляется Заказчиком при помощи KY ENT.
- 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"> виртуальные процессорные ядра (vCPU); виртуальная оперативная память (vRAM); виртуальное дисковое пространство (vHDD); Edge Gateway.
Сетевые сервисы и компоненты	<ul style="list-style-type: none"> подключение к сети интернет (в общем канале); один публичный IP-адрес.
Основные компоненты ENT	<ul style="list-style-type: none"> платформа виртуализации; KY ENT; платформа виртуализации сети (SDN).

- 1.4.1. Платформа виртуализации обеспечивает динамическую балансировку нагрузки на серверы и системы хранения данных для достижения оптимальной производительности. Составными частями платформы виртуализации являются:
- Аппаратный гипервизор – механизм, разделяющий ресурсы физического сервера между несколькими виртуальными машинами.
 - High Availability (HA) – механизм, позволяющий восстанавливать работоспособность виртуальных машин после аппаратного сбоя узлов виртуализации.
 - Сервис балансировки рабочих нагрузок – механизм, равномерно распределяющий ВМ между всеми узлами кластера и обеспечивающий заданную производительность виртуальных машин в штатном и нештатном (в случае сбоев) режимах работы.
 - Сервис онлайн миграции ВМ – механизм «живой» миграции ВМ между узлами кластера для сервисного обслуживания без прерывания работы пользовательских ВМ.
- 1.4.2. KY ENT предоставляет конечным пользователям безопасные, изолированные пулы ресурсов для быстрой инициализации Виртуального ЦОД и реализует единую консоль управления.
- 1.4.3. Платформа виртуализации сети (SDN) используется для создания программно-определяемых сетей, инкапсуляции трафика через протокол Geneve для построения логических L2-сетей в рамках уже существующей коммутации на уровне L3. Позволяет Заказчику самостоятельно создавать выделенные сегменты сети и определять правила маршрутизации между сетями своих виртуальных ЦОД, без изменений в физической коммутации.
- 1.5. В целях обеспечения защиты Инфраструктуры ENT реализовываются следующие меры и механизмы защиты:

Табл.2. Обеспечение защиты Инфраструктуры ENT

Уровни защиты	Мероприятия
Защита Облака Cloud и средств его управления	
Физический	Обеспечивается: <ul style="list-style-type: none"> 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.
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"> – 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.
Дополнительный	Осуществляются периодические тестирования на проникновение и аудит информационной безопасности Инфраструктуры ENT с привлечением сторонних организаций. Выявленные в ходе соответствующего тестирования и/или аудита недостатки устраняются по факту их выявления.
Защита KY ENT	
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.
Изоляция «Организаций» Заказчика	
ENT	Осуществляется встроенными средствами ENT.
Сетевой	Осуществляется средствами SDN.
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, установленными 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 КУ ENT и консоли управления резервным копированием ВМ, 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 Edge Gateway в «Организации» Заказчика с использованием KY ENT; 8. создание/изменение задания резервного копирования с использованием консоли управления резервным копированием VM; 9. восстановление VM из резервной копии с использованием консоли управления резервным копированием VM; 10. восстановление файлов из резервной копии с использованием консоли управления резервным копированием VM; 11. изменение дисковой политики по умолчанию для виртуальных ЦОД; 12. включение/отключение дополнительных услуг (логирование, DFW, VPN и прочее).		
	Администрирование «Организацией» и управление доступом к ней	Администрирование «Организацией» Заказчика с использованием KY ENT. Администрирование доступом к «Организации» Заказчика с использованием KY ENT.	Исполнитель (ответственность за предоставление сервиса ENT) 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 KY ENT необходимых виртуальных сетей в процессе администрирования ВЦОД Заказчика. Межсетевое экранирование периметра ВЦОД Заказчика с использованием Edge Gateway. Обеспечение внутреннего сегментирования (с использованием KY ENT) и внутреннего межсетевого экранирования (с использованием Edge Gateway) ВЦОД Заказчика. Настройка NAT/DHCP/L2VPN/L3VPN, маршрутизации и балансировщика нагрузки на Edge Gateway в «Организации» Заказчика с использованием KY ENT.	Исполнитель (ответственность за предоставление сервиса) Заказчик (ответственность за администрирование)	Заказчик
	Управление резервированием информации	Управление резервированием информации Заказчика с использованием консоли управления резервным копированием VM, включающее в себя: создание/изменение заданий резервного копирования информации Заказчика;	Исполнитель (ответственность за	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
	(предоставляется в рамках отдельной Услуги)	восстановление ВМ Заказчика из резервной копии; восстановление файлов Заказчика из резервной копии.	предоставление сервиса) Заказчик (ответственность за управление резервированием своей информации)	
	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 ENT, 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 и средствах защиты информации Инфраструктуры ENT.	Исполнитель	Исполнитель
	Управление доступом	Управление доступом к сегменту управления Инфраструктурой ENT, её VLAN-ам и компонентам.	Исполнитель	Исполнитель
	Управление аутентификационной информацией	Управление учётными записями AD привилегированных пользователей, имеющих доступ к сегменту управления Инфраструктурой ENT, и их вторым фактором аутентификации (аутентификаторами).	Исполнитель	Исполнитель
	Управление уязвимостями	Контроль и анализ защищенности служебных ВМ MGMT-сегмента и гипервизоров Инфраструктуры ENT.	Исполнитель	Исполнитель
	Управление инцидентами ИБ	Сбор с использованием средств SIEM с компонентов и средств защиты информации Инфраструктуры ENT 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 ENT.	Исполнитель	Исполнитель
	Управление безопасностью для виртуальных и физических сетей	Защита периметров ЦОД Инфраструктуры ENT с использованием кластеров высокопроизводительных межсетевых экранов нового поколения (NGFW), обеспечивающих межсетевое экранирование и защиту от компьютерных атак Инфраструктуры.	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
		Защита сетевой Инфраструктуры ENT (входа в облако) от DDoS-атак, направленных на переполнение канальной емкости. Внутреннее сегментирование сетевых Инфраструктур ENT с использованием NGFW и выделением в рамках ЦОД на сетевом уровне DMZ, PROD- и MGMT-сегментов Инфраструктуры.		
	Установка и администрирование средств защиты	Установка, настройка и администрирование средств защиты информации в составе Инфраструктуры ENT, в том числе: 1. средств антивирусной защиты; 2. средств контроля действий привилегированных пользователей (администраторов Cloud) класса PIM&PAM; 3. SIEM; 4. средств контроля и анализа защищенности; 5. WEB Application Firewall (WAF), используемого для защиты публикуемых КУ ENT и консоли управления резервным копированием ВМ; 6. NGFW; 7. Identity and access management (IAM).	Исполнитель	Исполнитель
	Управление резервированием информации	Резервное копирование и восстановление из образов служебных виртуальных машин Инфраструктуры Платформы ENT с использованием CPK Backup & Replication.	Исполнитель	Исполнитель
	Обеспечение защиты персональных данных клиентов	Защита ПДн сотрудников Заказчика, имеющих доступ КУ ENT и консоли управления резервным копированием ВМ, обрабатываемых в Инфраструктуре ENT.	Исполнитель	Исполнитель
Физический уровень	Контроль доступа	Контроль доступа в ЦОД и помещения Инфраструктуры ENT (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 2,6 ГГц; не менее 3,0 ГГц; не менее 3,5 ГГц ¹ . 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 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. 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 ² 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 загруженности общего канала передачи данных). Заказчику предоставляется базовая защита информационных систем, размещаемых в Инфраструктуре ENT, от DDoS-атак, направленных на истощение канальной ёмкости сетевой Инфраструктуры ENT.

¹ Технически допустимо выделять до 24/48/56 vCPU (для vCPU частотой 3,5/3,0/2,6 ГГц, соответственно) 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 Cloud.

Подробная информация по доступным подключениям приведена в Приложении № 1.ENT.6. к Договору.

1.8.1. В остальных случаях, а также по запросу, может быть предоставлена расширенная защита информационных систем Заказчика, размещаемых в Инфраструктуре ENT, 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.

1.9. Сетевые сервисы SDN.

1.9.1. Платформа виртуализации сети реализует программно-определяемую облачную сеть, а также программный подход к созданию и эксплуатации сетевых сервисов.

1.9.2. Платформа виртуализации сети включает в себя следующие компоненты:

- виртуальные сети для организации сетевой связности виртуальных машин;
- клиентские шлюзы Edge Gateway³.

1.9.3. Клиентский шлюз Edge Gateway предоставляет следующие сервисы:

- маршрутизация (Routing);
- пограничное межсетевое экранирование (Firewall);
- преобразование сетевых адресов (NAT);
- виртуальные частные сети (VPN) на базе IPsec;
- динамическое распределение сетевых адресов (DHCP).

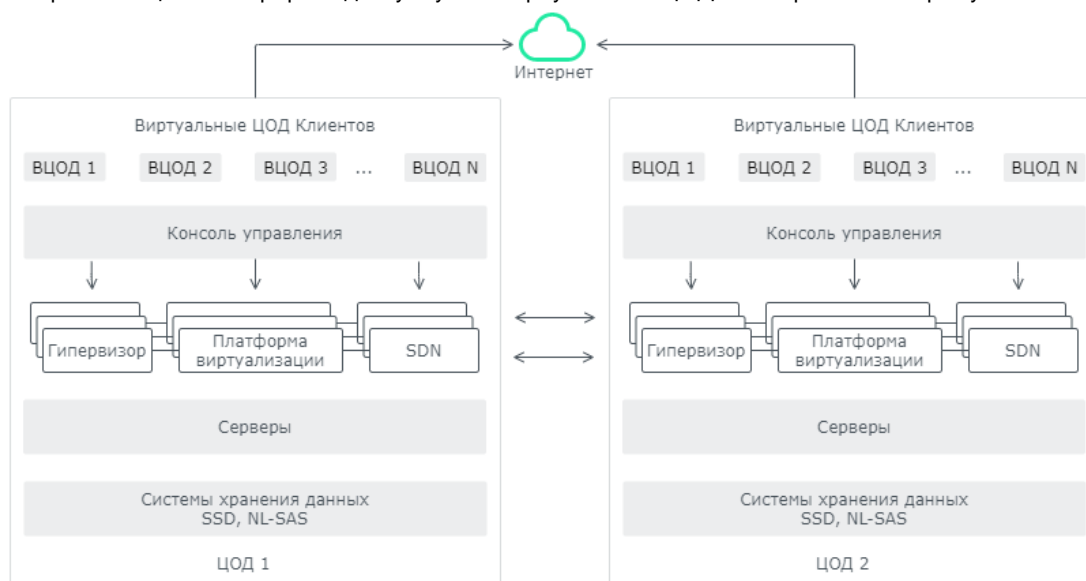
1.9.4. Клиентские шлюзы Edge Gateway разворачиваются в режиме высокой доступности. Активный шлюз обрабатывает сетевой трафик, в случае выхода его из строя трафик автоматически переключается на резервный шлюз, находящийся в режиме ожидания.

1.9.5. При построении сложной сетевой архитектуры, например, организации динамической маршрутизации BGP с локальной сетевой инфраструктурой Заказчика, необходимо использовать пограничные шлюзы Edge Gateway T0. В зависимости от требований к пропускной способности доступа в и из Интернета, а также специфической настройки сетевых сервисов могут быть развернуты Виртуальный Edge Gateway T0 или Выделенный сервер Edge Gateway T0 для повышенной производительности.

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 КУ ENT. За дополнительную плату Заказчику предоставляется доступ к каталогу с шаблонами ВМ с предустановленными наиболее популярными версиями операционных систем. При импорте и использовании Заказчиком собственных образов виртуальных машин, которые не имеют официальной совместимости со стороны поставщика платформы виртуализации, Исполнитель не гарантирует работоспособность данных виртуальных машин, и решение возможных проблем не регулируется действующим Соглашением об уровне предоставлении Услуги.

1.11. **Программная платформа.** В качестве инструмента реализации ENT используется КУ ENT. Устойчивость к отказам вычислительных узлов реализована средствами платформы виртуализации на базе технологии High Availability (HA).

Схема реализации платформы для услуги «Виртуальный ЦОД» изображена на рисунке ниже:



³ Отдельно не тарифицируются, их стоимость включена в стоимость предоставленных ресурсов и опций Услуги.

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 midrange с резервированием основных компонент, таких как блоки питания, контроллерные модули.
Сеть	Базируется на оборудовании ведущих мировых производителей, которое обеспечивает: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – предсказуемость задержек; – высокий уровень масштабируемости без прерывания работы сети; – защиту от появления петель; – высокий уровень автоматизации управления и поддержки.

1.13. **Предоставление доступа к программному обеспечению.**

1.13.1. Исполнитель предлагает Заказчику доступ к программному обеспечению, перечень которого Заказчик может запросить у ответственного лица Исполнителя (раздел 10 Договора), стоимость определяется в соответствующем бланке Заказа на основании Тарифов, установленных в Приложении № 7.А.

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

1.13.3. Базой для применения тарифа и расчета ежемесячного платежа за использование Серверной операционной системой является наибольшее число одновременно работавших виртуальных машин с данной операционной системой за расчетный период.

1.13.4. В случае индексации цен на лицензии со стороны производителя ПО, 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 производителя ПО. В случае необходимости Стороны подписывают Дополнительное соглашение о внесении изменений в Приложение № 7.А.

1.13.5. Подробная информация по условиям и ограничениям использования программного обеспечения приведена в Приложении № 8. к Договору.

1.14. **Предоставление доступа к каталогу готовых приложений для бизнеса.** Исполнитель предоставляет Заказчику доступ к каталогу приложений. В данном каталоге размещаются предварительно настроенные шаблоны приложений открытого программного обеспечения. С перечнем доступных шаблонов Заказчик может ознакомиться в документации по ссылке <https://docs.sbercloud.ru/applications/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.

1.15. **Предоставление доступа к опции Распределенный межсетевой экран.** Исполнитель предоставляет Заказчику доступ к сетевому сервису виртуального шлюза – 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.

1.16. **Соответствие 152-ФЗ.** В рамках услуги «Соответствие 152-ФЗ» Заказчик может получить экспертную помощь по приведению собственной ИСПДн в соответствие с требованиями законодательства в области защиты персональных данных, предусмотренными Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». В результате Заказчик может снять риски санкций со стороны государственных регуляторов, а также снизить риски утечки и других инцидентов информационной безопасности в ИСПДн.

- 1.17. **Threat Detection and Response (TDR).** В рамках Услуги TDR Заказчик может решить задачи по обеспечению круглосуточного мониторинга информационной безопасности облачной инфраструктуры, оперативной реакции на инциденты ИБ, проведению расследований при обнаружении продвинутых атак и повышения защищенности инфраструктуры. Услуга предоставляется Исполнителем в партнерстве с ООО «Безопасная информационная среда» (ООО «БИЗон»). Доступ к услуге предоставляется на основании подписанного бланка Заказа и оплачивается Заказчиком отдельно.
- 1.18. **Именованние «Организаций» Заказчика.** Для корректной обработки обращений Заказчика именованние «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.
- 1.19. **Шифрование виртуальных машин.** Услуга обеспечивает возможность шифрования конфигурационных файлов данных и дисков ВМ, предоставлении доступа к шаблонам гостевых ОС с возможностью хранения ключей шифрования в vTPM. С помощью консоли управления Заказчик может самостоятельно создавать новые шифрованные ВМ, либо зашифровывать существующие ВМ. Стоимость Услуги формируется в зависимости от максимального объёма дискового пространства, выделенных для ВМ с активированной опцией «Шифрование ВМ» в течение Отчётного периода (календарного месяца). Услуга подключается посредством подписания Заказа.
- 1.20. **ГОСТ-VPN на базе VipNet** является услугой по предоставлению Заказчику защищенного канала связи с использованием средств криптографической защиты информации для подключения информационных систем, размещаемых в инфраструктуре Заказчика, к информационным системам, размещенным в Облаке Cloud.

2. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И МЕТРИКИ УСЛУГИ

2.1. Услуга Виртуальный ЦОД описана в Таблице 7:

Табл.7. Параметры предоставляемых Услуг

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Вычисления	Виртуальный процессор 3,5 ГГц, (шт.)	Базовая частота процессора vCPU	Не менее 3,5 ГГц
		Host CPU Ready time	Менее 5%
		Рекомендуемое кол-во vCPU на Виртуальный сервер (шт.)	1 - 12 шт.
		Допустимый объем vRAM на виртуальный сервер	1 – 384 Гб
		RAM Swapped	0%
	Виртуальный процессор 3,0 ГГц, (шт.)	Базовая частота процессора vCPU	Не менее 3,0 ГГц
		Host CPU Ready time	Менее 5%
		Рекомендуемое кол-во vCPU на Виртуальный сервер (шт.)	1 - 24 шт.
		Допустимый объем vRAM на виртуальный сервер	1 - 768 Гб
		RAM Swapped	0%
	Виртуальный процессор 2,6 ГГц, (шт.)	Базовая частота процессора vCPU	Не менее 2,6 ГГц
		Host CPU Ready time	Менее 5%
		Рекомендуемое кол-во vCPU на Виртуальный сервер (шт.)	1 - 28 шт.
		Допустимый объем vRAM на виртуальный сервер	1 - 768 Гб
		RAM Swapped	0%
Хранилище данных	Виртуальный жесткий диск SSD, (Гб)	HDD IOPS. Эталонные значения ⁴	5000 IOPS/1 ТБ ⁵
		Среднее время доступа к SSD Storage на виртуальной машине ²	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, (Гб)	HDD IOPS. Эталонные значения ⁴	100 IOPS/1 ТБ ⁵
		Среднее время доступа к SATA Storage на виртуальной машине ²	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

⁴ Параметры гарантируются при размере блока до 8 Кб, произвольное чтение/запись с профилем 70/30.

⁵ 1 ТБ = 1000 Гб

Табл.7. Параметры предоставляемых Услуг

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Сетевые сервисы	Доступ в Интернет в общем канале	Полоса пропускания	Не тарифицируется: не более 100 Мб/с на Виртуальный ЦОД
	Пропускная способность на виртуальный сервер	Средняя сетевая задержка в пределах сети передачи данных Cloud	0 мс - 5 мс
		Процент потерянных пакетов в пределах сети передачи данных Cloud	0% - 0,2 %
	Виртуальный шлюз (шт.)	Средняя сетевая задержка в пределах сети передачи данных Cloud	0 мс - 5 мс
		Пропускная способность	Не более 5 Гб/с
Гостевая ОС	Доступ к шаблону Серверная операционная система: <ul style="list-style-type: none"> • VM размером 4 и менее vCPU: VM (шт.)/ календарный мес⁶. • VM размером более 4 vCPU: vCPU (шт.)/ календарный мес³. 	Шаблоны Серверной операционной системы	Серверная операционная система 2016 Серверная операционная система 2019 Серверная операционная система 2022
ПО	Доступ к шаблону ПО Серверная СУБД: <ul style="list-style-type: none"> • VM размером 1–12 vCPU: VM (шт.)/ календарный мес.⁷ 	Шаблоны ПО Серверная СУБД	Серверная СУБД 2017 Enterprise Серверная СУБД 2019 Enterprise
ПО	Доступ к экземплярам ПО (Серверная СУБД Enterprise Core, Серверная СУБД Standard Core, Серверная СУБД Web Edition, Серверная операционная система: Datacenter, Серверная операционная система: Standard): <ul style="list-style-type: none"> • Два виртуальных/физических ядра (шт.)/ календарный месяц³. 	Экземпляры ПО (SQL ServerСерверная СУБД Enterprise Core, Серверная СУБД SQL Server Standard Core, Серверная СУБД SQL Server Web Edition, Серверная операционная система: Datacenter, Серверная операционная система: Standard).	Поддерживаемые версии ПО (Серверная СУБД Enterprise Core, Серверная СУБД Standard Core, Серверная СУБД Web Edition, Серверная операционная система: Datacenter, Серверная операционная система: Standard).

⁶ Минимальный период тарификации – календарный месяц. Начало использования, начиная с первой минуты, или продолжение использования Услуги в Отчётном периоде предполагает списание стоимости за полный календарный месяц. Неполный календарный месяц использования Услуги, начиная с первой минуты, округляется до полного календарного месяца пользования Услугой.

⁷ При использовании большего количества vCPU в составе экземпляра VM, пропорционально увеличивается количество доступных лицензий для оплаты (с шагом в 12 vCPU).

3. ТАРИФИКАЦИЯ УСЛУГИ

- 3.1. Услуга предоставляет на выбор два типа тарификации: Динамическая тарификация (Pay as you go, далее – PAYG) и Статическая тарификация (Allocation).
- 3.2. Динамическая тарификация (Pay as you go).
- 3.2.1. Динамическая тарификация предполагает оплату пула ресурсов, указанных ниже, по факту их потребления Заказчиком в течение Отчётного периода:
- Виртуальный процессор 2,6 ГГц, PAYG⁸;
 - Виртуальный процессор 3,0 ГГц, PAYG⁸;
 - Виртуальная память, PAYG^{8,9};
 - Виртуальный жесткий диск SATA, PAYG;
 - Виртуальный жесткий диск SSD, PAYG.
- 3.2.2. Динамическая тарификация осуществляется в почасовом режиме (из расчета стоимости одного часа), начиная с первой минуты пользования Услугой. Время учитывается с дискретностью до целого часа, то есть неполный час работы виртуальной машины считается как целый. Тарифицируется сумма соответствующих ресурсов для всех ВМ. Виртуальный процессор и виртуальная память тарифицируются с момента старта ВМ и до момента ее остановки. Виртуальный жесткий диск тарифицируется с момента создания ВМ и до её удаления. Снимки (Snapshots), swap-файлы, шаблоны ВМ и ISO-образы тарифицируются как Виртуальный жесткий диск. Для каждой ВМ учитываются максимальные значения ресурсов за каждый час.
- 3.3. Статическая тарификация (Allocation).
- 3.3.1. Величина ежемесячного платежа за пользование Услугой определяется в соответствии с заказанным объёмом перечисленных ниже ресурсов и опций:
- Виртуальный процессор 2,6 ГГц;
 - Виртуальный процессор 3,0 ГГц;
 - Виртуальный процессор 3,5 ГГц;
 - Виртуальная память⁹;
 - Виртуальный жесткий диск SATA;
 - Виртуальный жесткий диск SSD;
 - Предоставление публичного IP адреса;
 - Виртуальный EDGE Gateway T0;
 - Выделенный сервер EDGE Gateway T0;
 - Опция Распределенный межсетевой экран;
 - Доступ к шаблону Серверная операционная система³;
 - Доступ к шаблону ПО Серверная СУБД ³;
 - Доступ к прочим экземплярам ПО (перечень доступного ПО приведен в Приложении № 7.А.);
 - Виртуальный жесткий диск SATA для зашифрованных ВМ;
 - Виртуальный жесткий диск SSD для зашифрованных ВМ.
- 3.3.2. Методика расчётов потребляемых процессорных ресурсов и оперативной памяти предполагает тарификацию суммы значений предоставленных ресурсов за Отчётный период в соответствии с Тарифом. Счет выставляется на основе суммы значений.
- 3.3.3. Методика расчёта потребляемого дискового пространства предполагает оплату за весь предоставленный Заказчику объём ресурсов дискового пространства каждого типа.
- 3.3.4. Методика расчёта по опции «Распределенный межсетевой экран» предполагает тарификацию суммы значений оперативной памяти, предоставленной Заказчику в рамках его виртуального ЦОД в Отчётный период.

4. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

- 4.1. Возможные виды подключения / изменения / отключения Услуг:
- 4.1.1. Посредством подписания Заказа (с учётом п. 4.6. настоящего Приложения);
- 4.1.2. Посредством совершения действий в Личном кабинете.
- 4.2. Возможный порядок расчётов 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.

⁸ Ресурсы тарифицируются в период работы виртуальной машины.

⁹ Объём Виртуальной памяти (vRAM) должен быть дополнительно учтен при заказе Виртуального дискового пространства для хранения swap-файлов виртуальных серверов в соответствии с параметрами, указанными в разделе «Тип ресурса: виртуальная оперативная память (vRAM)» Таблицы 4.

- 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 должен быть направлен Исполнителю не позднее, чем за 3 (Три) рабочих дня до даты начала оказания Услуги;
 - 4.6.2. В течение 1 (Одного) рабочего дня 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);
 - 4.6.3. В случае согласования Сторонами Заказа Услуга 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.