

**ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ  
 «ВИРТУАЛЬНЫЕ РАБОЧИЕ МЕСТА (VDI)»**

**1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГИ**

- 1.1. Услуга предоставляется на базе платформы виртуализации рабочих мест, состоящей из совокупности базовых информационно-технологических ресурсов и функционирующей под управлением Исполнителя серверного и сетевого оборудования, систем хранения данных и специализированного программного обеспечения.
- 1.2. В рамках Услуги Исполнитель предоставляет Заказчику виртуальные рабочие места с определенными характеристиками процессора (vCPU), виртуальной памяти (vRAM), дискового пространства (vSSD) и виртуального графического процессора (vGPU), а также средства управления виртуальными рабочими местами, достаточные для создания и управления конфигурациями.
- 1.3. Управление виртуальными рабочими местами осуществляется Заказчиком при помощи консоли управления виртуальными рабочими местами и Консоли Управления Облаком VMware (далее - КУ VMware).
- 1.4. Состав и основные компоненты Услуги:

Табл.1. Состав и основные компоненты

Ресурсы	
Наименование группы	Содержание
Виртуальные рабочие места	<ul style="list-style-type: none"> <li>- виртуальные процессорные ядра (vCPU);</li> <li>- виртуальная оперативная память (vRAM);</li> <li>- виртуальное дисковое пространство (vSSD);</li> <li>- виртуальные графические процессорные ядра (vGPU)</li> </ul>
Сетевые сервисы	<ul style="list-style-type: none"> <li>- подключение к сети Интернет на гарантированной скорости;</li> <li>- один публичный IP-адрес</li> </ul>
Платформа виртуализации рабочих мест	<ul style="list-style-type: none"> <li>- консоль управления виртуальными рабочими местами;</li> <li>- платформа виртуализации (на базе услуги Виртуальный ЦОД);</li> <li>- КУ VMware;</li> <li>- платформа виртуализации сети (SDN)</li> </ul>

- 1.4.1. Описание платформы виртуализации (на базе услуги Виртуальный ЦОД) содержится в п. 1.4.1. Приложения № 1. VMW.1.1. к Договору.
- 1.4.2. Платформа виртуализации рабочих мест представляет собой выделенный набор компонентов управления инфраструктурой виртуальных рабочих мест:
  - Консоль управления виртуальными рабочими местами и брокер подключений позволяет автоматизировать развёртывание и управление изолированными пулами виртуальных рабочих мест.
  - Пограничный шлюз доступа (Unified Access Gateway) позволяет обеспечить безопасный доступ к рабочим местам в Облаке Cloud.ru.
- 1.4.3. КУ VMware предоставляет конечным пользователям возможность безопасно работать с изолированными пулами ресурсов для управления образами виртуальных машин и виртуальными маршрутизаторами.
- 1.4.4. Описание платформы виртуализации сети (SDN) содержится в п. 1.4.3. Приложения № 1. VMW.1.1. к Договору.
- 1.5. Описание мер и механизмов защиты Инфраструктуры платформы Облако VMware (далее-Инфраструктура VMW) описано в п. 1.5. Приложения № 1. VMW.1.1. к Договору.

Дополнительно к указанному в п. 1.5 Приложения № 1. VMW.1.1. к Договору, в отношении группы «Платформа виртуализации рабочих мест» используются следующие уровни защиты:

Табл.2. Обеспечение защиты Инфраструктуры VMW

Уровни защиты	Мероприятия
<b>Изоляция «Организаций» Заказчика</b>	
Платформа виртуализации рабочих мест	Осуществляется с помощью изоляции предоставленного набора компонентов каждого Заказчика

- 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 Заказчика	Журналирование событий	Журналирование событий в прикладном программном обеспечении и операционных системах, установленных в виртуальных машинах (ВМ) Заказчика	Заказчик	Заказчик
	Управление доступом	Управление доступом к прикладному программному обеспечению 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 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) на ВМ Заказчика, а также мониторинг и реагирование на инциденты безопасности	Заказчик	Заказчик
	Установка и администрирование средств защиты	Установка, настройка и администрирование в ВМ Заказчика СрЗИ от несанкционированного доступа (НСД), антивирусных средств и прочих средств защиты информации, устанавливаемых в ВМ 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 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 Заказчика, в том числе, но не ограничиваясь защитой ПДн, обрабатываемых средствами установленных в ВМ Заказчика	Заказчик	Заказчик
Уровень «Организации» и ВЦОД Заказчика	Журналирование событий	<p>Журналирование событий, связанных с функционированием объектов Заказчика (например, его виртуальное рабочее место и действиями пользователей на КУ VMware и платформе виртуализации рабочих мест таких как:</p> <ol style="list-style-type: none"> <li>1. вход/выход пользователей в/из консолей;</li> <li>2. создание/удаление новых учётных записей пользователей и присвоение им привилегий доступа к консолям;</li> <li>3. Подключение/отключение к виртуальным рабочим местам;</li> <li>4. создание/удаление виртуального рабочего места;</li> <li>5. запуск/останов виртуального рабочего места;</li> <li>6. создание клонов виртуального рабочего места;</li> <li>7. изменение характеристик виртуального рабочего места;</li> <li>8. настройка NAT/DHCP/L2VPN/L3VPN, маршрутизации, балансировщика нагрузки и/или правил межсетевого экранирования на SDN в «Организации» Заказчика с использованием КУ VMware;</li> <li>9. изменение дисковой политики по умолчанию для VDC;</li> <li>10. включение/отключение дополнительных услуг (логирование, DFW, VPN и прочее)</li> </ol>	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
	Администрирование «Организацией» и управление доступом к ней	Администрирование «Организацией» Заказчика с использованием КУ VMware и консоли управления виртуальными рабочими местами. Администрирование доступом к «Организации» Заказчика с использованием КУ VMware и консоли управления виртуальными рабочими местами	Исполнитель (ответственность за предоставление сервиса vCD консоли управления виртуальными рабочими местами)  Заказчик (ответственность за администрирование «Организацией» и доступом к ней)	Заказчик
	Работа с ПО AppVolume	Пакетирование приложений в наборы, которые можно подключить к своим BPM	Исполнитель (ответственность за предоставление компонента)  Заказчик (за создание и поддержку ПО установленное и настроенное самостоятельно)	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 КУ VMware, необходимых VxLAN в процессе администрирования Заказчика. Межсетевое экранирования периметра Заказчика с использованием SDN. Обеспечение внутреннего сегментирования (с использованием КУ VMware) и внутреннего межсетевого экранирования (с использованием SDN) Заказчика. Настройка NAT/DHCP/L2VPN/L3VPN, маршрутизации и балансировщика нагрузки на SDN в «Организации» Заказчика с использованием КУ VMware.	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 пулами виртуальных рабочих мест	Создание, удаление Золотого образа с использованием КУ VMware. Создание, удаление пулов рабочих столов с использованием консоли управления виртуальными рабочими местами. Предоставление доступа к виртуальным рабочим местам конечным пользователям	Заказчик	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 VMW, 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 VMW	Исполнитель	Исполнитель
	Управление доступом	Управление доступом к сегменту управления Инфраструктурой VMW, её VLAN-ам и компонентам	Исполнитель	Исполнитель
	Управление аутентификационной информацией	Управление учётными записями AD привилегированных пользователей, имеющих доступ к сегменту управления Инфраструктурой Cloud.ru, и их вторым фактором аутентификации (аутентификаторами).	Исполнитель	Исполнитель
	Управление уязвимостями	Контроль и анализ защищенности служебных VM MGMT-сегмента и серверов с гипервизорами для Инфраструктуры VMW	Исполнитель	Исполнитель
	Управление инцидентами ИБ	Сбор с использованием средств SIEM с компонентов и средств защиты информации инфраструктуры VMW 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 VMW	Исполнитель	Исполнитель
	Управление безопасностью виртуальных физических сетей для и	Защита периметров ЦОД Инфраструктуры VMW с использованием кластеров высокопроизводительных межсетевых экранов нового поколения (NGFW), обеспечивающих межсетевое экранирование и защиту от компьютерных атак Инфраструктуры. Защита сетевой Инфраструктуры VMW (входа в облако) от DDoS-атак, направленных на переполнение канальной емкости.	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
		Внутреннее сегментирование сетевых Инфраструктур VMW 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 VMW, в том числе: 1. средств антивирусной защиты; 2. средств контроля действий привилегированных пользователей (администраторов Cloud.ru) класса PIM&PAM; 3. SIEM; 4. средств контроля и анализа защищенности; 5. WEB Application Firewall (WAF), используемого для защиты публикуемых КУ VMware 6. NGFW; 7. Identity and access management (IAM)	Исполнитель	Исполнитель
	Обеспечение защиты персональных данных клиентов	Защита ПДн сотрудников Заказчика, имеющих доступ к КУ VMware, обрабатываемых в Инфраструктуре VMW	Исполнитель	Исполнитель
Физический уровень	Контроль доступа	Контроль доступа в ЦОД и помещения Инфраструктуры VMW (охраняемая территория ЦОД, пропускной режим, системы контроля и управления доступом, запирающие стоеки)	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. Для подключения к Услуге Заказчик может выбрать один или несколько типов подключения:

Табл.4. Типы подключения к сети и сетевые сервисы

Тип подключения	Описание
Подключение через сеть Интернет	Для качественного изображения и скорости загрузки данных полоса пропускания в расчете на одно виртуальное рабочее место Заказчика должна составлять не менее 2 Мбит/с. Полоса пропускания рассчитывается Заказчиком самостоятельно исходя из количества виртуальных рабочих мест
Подключение через выделенный канал связи	Способ подключения, позволяющий гарантировать параметры канала связи. Выделенный канал связи состоит из двух частей: <ol style="list-style-type: none"> <li>1. Канал связи от инфраструктуры Заказчика к узлу связи Cloud.ru, расположенному на ММТС-9, ММТС-10</li> <li>2. От ММТС-9, ММТС-10 до Инфраструктуры</li> </ol>

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

1.7.1. Для обмена данными между виртуальными рабочими местами используется внутреннее сетевое взаимодействие, реализованное на базе сетевого оборудования Исполнителя и средствами гипервизора.

1.8. Описание сетевых сервисов SDN содержится в п. 1.9. Приложения № 1. VMW.1.1. к Договору.

1.9. Шаблоны виртуальных рабочих мест и образы ОС.

В рамках Услуги Заказчик может самостоятельно выполнить импорт/экспорт собственного образа виртуального рабочего места. Возможный вариант работы с образами виртуального рабочего места: Заказчик самостоятельно осуществляет импорт/экспорт образов виртуальных рабочих мест, используя КУ VMware. За дополнительную плату Заказчику предоставляется доступ к каталогу с шаблонами виртуального рабочего места с предустановленными операционными системами. При импорте и использовании Заказчиком собственных образов виртуальных машин, которые не имеют официальной совместимости и отличаются согласованных конфигураций, Исполнитель не гарантирует работоспособность данных виртуальных рабочих мест, и решение возможных проблем не регулируется действующим Соглашением об уровне предоставлении Услуги.

1.10. Аутентификация и политики доступа.

Оказание услуги возможно только при предоставлении Заказчиком доступа к каталогу Active Directory и серверам DNS. Active Directory используется для управления Заказчиком доступом пользователей к развёрнутым виртуальным рабочим местам, политиками (Group Policy) и регистрации виртуальных рабочих мест. При отсутствии у Заказчика Active Directory или невозможности организации канала связи, инфраструктура Active Directory может быть размещена на ресурсах услуги «Виртуальный ЦОД», предоставленных Заказчику. Заказчик в каталоге Active Directory создаёт техническую учётную запись с минимальным набором привилегий, необходимым для предоставления услуги. Указанные привилегии можно назначать на специально созданный Organization Unit и не распространять на весь каталог. В Organization Unit автоматически будут создаваться объекты типа «Компьютер» для регистрации созданных виртуальных рабочих мест. Минимально необходимый набор указан в Таблице 5. На сервере DNS Заказчик выполняет настройку «Условная пересылка DNS» (Conditional Forwarder) для перенаправления DNS запросов к домену Исполнителя на определённые DNS серверы.

Табл.5. Привилегии Active Directory для технической учётной записи

Привилегии технической учётной записи в Active Directory запись		
Название	Ответственность за предоставление	Кому предоставлен доступ
List Content	Заказчик	Исполнитель
Read All Properties	Заказчик	Исполнитель
Write All Properties	Заказчик	Исполнитель
Read Permissions	Заказчик	Исполнитель
Reset Password	Заказчик	Исполнитель
Create Computer Objects	Заказчик	Исполнитель
Delete Computer Objects	Заказчик	Исполнитель

1.11. Сетевая связанность.

Сетевой доступ к каталогу Active Directory и DNS обеспечивается Заказчиком и может быть организован с помощью L2VPN/L3VPN или выделенного канала связи.

1.12. **Программная платформа.** Услуга реализована на базе платформы виртуализации. В качестве инструмента реализации облачной инфраструктуры и формирования золотых образов используется КУ VMware. Для создания и управления виртуальными рабочими столами используется консоль управления виртуальными рабочими местами.

Отказоустойчивость вычислительных узлов реализована средствами платформы виртуализации на базе технологии High Availability (HA).

1.13. 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 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>

1.14. Предоставление доступа к программному обеспечению осуществляется в соответствии с условиями и порядком, предусмотренными в пункте 1.13. Приложения № 1. VMW.1.1. к Договору.

## 2. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И МЕТРИКИ УСЛУГИ

2.1. Услуга Виртуальное рабочее место описана в Таблице 7:

Табл.7. Параметры предоставляемых Услуг

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Вычисления	Виртуальный процессор (шт.)	Базовая частота процессора vCPU	Не менее 2, 6 ГГц
		Host CPU Ready time	Менее 5%
		Рекомендуемое кол-во vCPU на BPM (шт.)	1 - 16 шт.
	Виртуальный память (Гб.)	RAM Swapped	0%
		Допустимый объем vRAM на BPM (Гб.)	1 - 64 Гб
	Видеопамять (Гб.)	Тип видеокарты	T4, A40, V100
Хранилище данных	Виртуальный жесткий диск SSD (Гб)	SSD IOPS. Эталонные значения	5000 IOPS/1 ТБ
		Среднее время доступа к SSD Storage на виртуальной машине	0 мс - 5 мс
		Допустимый объем одного виртуального жесткого диска SSD на BPM	1 – 4096 Гб
		Шаг увеличения размера виртуального диска в допустимом диапазоне	1 Гб
Сетевые сервисы	Через сеть Интернет	Полоса пропускания	10-1000 Мбит/с
	Выделенный канал связи	Описание подключения см. в п.1.3.2. Приложения № 1. VMW.6. к Договору.	См. п. 1.3.2. Приложения № 1. VMW.6. к Договору.
	Пропускная способность на виртуальный сервер	Средняя сетевая задержка в пределах сети передачи данных Cloud.ru	0 мс - 5 мс
		Процент потерянных пакетов в пределах сети передачи данных Cloud.ru	0% - 0,2 %
	Виртуальный шлюз (шт.)	Средняя сетевая задержка в пределах сети передачи данных Cloud.ru	0 мс - 5 мс
Пропускная способность		Не более 5 Гб/с	
Гостевая ОС	Доступ к шаблону Серверная операционная система: Виртуальное рабочее место размером 4 и менее vCPU; Виртуальное рабочее место (шт.)/ календарный месяц <sup>3</sup> ; Виртуальное рабочее место размером более 4 vCPU; vCPU (шт.)/ календарный месяц <sup>3</sup> .	Шаблоны Серверной операционной системы	Серверная операционная система 2019 Серверная операционная система 2022 иные гостевые ОС, доступные для заказа в Личном кабинете

<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.

### 3. ТАРИФИКАЦИЯ УСЛУГИ

3.1. Тарификация Услуги статическая (Allocation).

3.2. Величина ежемесячного платежа за пользование Услугой определяется в соответствии с заказанным объёмом перечисленных ниже ресурсов и опций. Доступные ресурсы и опции перечислены в Таблице 8.

Табл.8. Конфигурации виртуальных рабочих мест

Наименование ресурса	Единицы измерения	Кратность заказа
Виртуальный процессор (vCPU)	Шт	2
Виртуальная память (vRAM)	Гб	2
Виртуальный жесткий диск (vSSD)	Гб	10
Тарифный план Linux	Шт	1
Тарифный план Стандарт	Шт	1
Тарифный план Продвинутой	Шт	1
Предоставление доступа к шаблону Серверная операционная система	Шт	1

3.3. Работы по настройке и администрированию Услуги не входят в тарифный план и оплачиваются отдельно в составе услуги Managed Services<sup>1</sup>.

3.4. Для каждой конфигурации виртуального рабочего места доступны четыре варианта тарифного плана: Linux, Стандарт, Расширенный, Продвинутой. Описание тарифных планов представлено в Таблице 9.

Табл.9. Конфигурации виртуальных рабочих мест

Компоненты	Тарифный план		
	Linux	Стандарт	Продвинутой
Параллельный пользователь (CCU)	Да	Да	Да
Именованный пользователь	Нет	Нет	Да
Рабочий стол и приложения			
Виртуальные рабочие столы с Операционной системой	Нет	Да	Да
Виртуальные рабочие столы ОС Linux	Да	Нет	Да
Приложения, размещенные на Linux	Нет	Нет	Да
Удаленный физический доступ к ПК с Операционной системой	Нет	Да	Да
Приложения, размещенные на виртуальных машинах с Операционной системой	Нет	Нет	Да
Управление			
Rest API	Нет	Нет	Да
Мгновенные клоны для непостоянных рабочих столов (доступны для 8.x)	Да	Да	Да
Полные клоны для постоянных рабочих столов	Да	Да	Да
Профиль пользователя и персонализация	Да	Да	Нет
Стандарт, Профиль пользователя, персонализация и интеллектуальные политики	Нет	Нет	Да
Глобальный уровень прав с архитектурой Cloud Pod	Да	Да	Да
Инструмент справочной службы	Нет	Нет	Да
Доступ пользователей и протоколы			
Протоколы Blast Extreme, PCoIP, RDP	Да	Да	Да
Инструменты для совместной работы			
Организация совместных сессий в рамках одного виртуального рабочего места	Нет	Нет	Да

<sup>1</sup> См. подробнее Приложение № 11 к Договору.

Оптимизированное видео и аудио для Microsoft Teams	Нет	Нет	Да
--	-----	-----	----

- 3.5. Методика расчётов потребляемых ресурсов предполагает тарификацию суммы значений предоставленных виртуальных рабочих мест за Отчетный период в соответствии с Тарифом. Счет выставляется на основе суммы значений.

#### **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 обязуется соблюдать согласованное с Исполнителем количество виртуальных рабочих мест и их конфигурацию указанное в Бланке заказа. В случае, если Заказчик изменил ранее согласованное количество рабочих мест или конфигурацию, Исполнитель не несет ответственности за их работоспособность и вправе отключить виртуальные рабочие места, предоставленные Заказчику.
- 4.5. Заказчик самостоятельно несет ответственность за работоспособность программного обеспечения, устанавливаемого на виртуальные рабочие места.
- 4.6. Стороны установили следующий порядок Заказа Услуги:
- 4.6.1. Заказ на подключение Услуги должен быть направлен Исполнителю не позднее, чем за 3 (три) рабочих дней 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 по такому Заказу предоставляется в дату начала оказания Услуги, зафиксированную в Заказе, с 10:00 по московскому времени.
- 4.7. Заказчик 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.