УТВЕРЖДЕНО
Приказ генерального директора
СООО «Белорусские облачные технологии»
№ 92/1-ОД от 17.05.2019
(в редакции приказа № 320-ОД от 13.08.2020)

ПРАВИЛА ОКАЗАНИЯ УСЛУГИ ПРЕДОСТАВЛЕНИЯ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ «ЗАЩИЩЕННАЯ ВИРТУАЛЬНАЯ ИНФРАСТРУКТУРА»

1. ОПИСАНИЕ УСЛУГИ

1. Настоящие Правила оказания услуги предоставления облачной инфраструктуры «Защищенная виртуальная инфраструктура» (далее – Правила) определяют порядок оказания данной услуги.

2. В Правилах и Договоре на оказание услуги используются следующие термины и определения:

ИТ-ресурсы – программно-аппаратные средства, размещенные в республиканском центре обработки данных, выделяемые Оператором Клиенту для размещения и хранения информации, функционирования информационных ресурсов и/или информационных систем, а также для администрирования этих информационных ресурсов и/или информационных систем.

Единая республиканская сеть передачи данных (ЕРСПД) – мультисервисная сеть электросвязи, являющаяся частью сети электросвязи общего пользования и представляющая собой комплекс взаимодействующих между собой сетей передачи данных государственных органов и организаций, а также других юридических лиц негосударственной формы собственности и индивидуальных предпринимателей, присоединяющих существующие сети к ЕРСПД в добровольном порядке, за исключением сетей передачи данных, предназначенных для обеспечения национальной безопасности, обороны и охраны правопорядка.

Информационная система (ИС) – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств.

Информационный ресурс (ИР) – организованная совокупность документированной информации, включающая базы данных, другие взаимосвязанные данные в информационных системах.

Государственные органы и организации – государственные органы, иные государственные организации, а также хозяйственные общества, в отношении которых Республика Беларусь либо административно-

территориальная единица обладает акциями (долями в уставных фондах) в размере более 50 процентов.

Согласованный уровень услуг – набор параметров и показателей достижений, на основании которых измеряется качество оказания Услуги в соответствии с Соглашением об уровне обслуживания, изложенным в настоящих Правилах.

Уполномоченный администратор – администратор информационного ресурса и/или администратор безопасности Клиента, определенные сторонами в Договоре.

Учетные данные – логин и пароль, присваиваемые Клиенту для его идентификации, позволяющие получать доступ к порталу управления виртуальной инфраструктурой vCloud Director (далее – Портал).

3. Услуга предоставления облачной инфраструктуры «Защищенная виртуальная инфраструктура» (далее – Услуга) – это услуга республиканской платформы, реализованная Оператором с помощью категории служб облачных вычислений «Инфраструктура как услуга» (IaaS) для размещения информационных систем (ИС) Клиента, относящихся к классам типовых информационных систем 5-часн, 5-гос, 3-фл, 3-юл, 3-дсп в соответствии с СТБ 34.101.30-2017 «Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация».

4. При оказании Услуги используются средства виртуализации VMware и обеспечивается информационная безопасность ИТ-ресурсов, выделенных Клиенту. Оператор использует сертифицированные средства защиты информации, обеспечивает условия для безопасного функционирования ИР/ИС, что подтверждено Аттестатом соответствия системы защиты информации информационной системы требованиям по защите информации, актуальная копия которого размещена на официальном сайте Оператора.

5. Для организации доступа к Услуге Оператор обеспечивает подключение ИТ-ресурсов, выделенных Клиенту, к каналам доступа к сети Интернет в рамках Заказа на Услугу и (или) отдельного договора, с обеспечением необходимого уровня защиты и параметров качества услуг передачи данных, определенных приложением к Правилам оказания услуг электросвязи, утвержденным постановлением Совета Министров Республики Беларусь от 17 августа 2006 г. №1055.

6. Оператор обеспечивает защиту ИТ-ресурсов, выделенных Клиенту, в соответствии с утвержденной у Оператора и согласованной с Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ) политикой информационной безопасности.

7. Объем предоставляемой Услуги выбирается Клиентом согласно установленным Тарифам Оператора. Изменение объема ИТ-ресурсов, выделенных Клиенту в рамках виртуального центра обработки данных (VDC), осуществляется в пределах технических возможностей Оператора посредством направления нового Заказа на услугу в адрес Оператора.

8. Пользуясь Услугой, Клиент может в рамках собственного VDC, создаваемого на базе выделенной виртуальной инфраструктуры, самостоятельно конфигурировать ее для размещения собственных ИР/ИС.

9. Для реализации возможности восстановления компонентов инфраструктуры, Клиенту предоставляется доступ к системе резервного копирования и восстановления. Услуги резервного копирования и восстановления реализованы на базе программного обеспечения Veeam, хранение резервных копий осуществляется на отказоустойчивом дисковом массиве. Все услуги по резервному копированию оплачиваются согласно Тарифам Оператора. Ответственность за управление процедурами резервирования возлагается на владельца ИР/ИС.

10. Клиент вправе заказать дополнительные услуги, ресурсы и права (лицензии) на программное обеспечение (ПО) согласно установленным Тарифам Оператора.

11. Предоставляемое Оператором в рамках Услуги ПО не является отказоустойчивыми.

12. Оператор оказывает Клиенту техническую поддержку на постоянной основе в соответствии с разделом 4 «Соглашение об уровне обслуживания» настоящих Правил.

13. По запросу Клиента может оказываться расширенная техническая поддержка (в рамках дополнительных услуг), в состав которой может входить следующий набор сервисов на каждую виртуальную машину:

создание и внесение изменений в параметры виртуальных машин (далее – VM) и контейнеров (далее – vApp);

создание каталогов и шаблонов VM;

установка операционных систем VM;

загрузка шаблонов vApp клиента;

управление VM (остановка, запуск, перезарузка, копирование, перенос, удаление);

выполнение операций с виртуальными сетями, настройка и изменение параметров (Internet, DHCP, NAT, Firewall, RDP, SSH, VPN);

мониторинг состояния VM VDC Клиента (Running, Shut down, Faulty, Deleted, Restarting и т.д) – CPU Usage, Memory (RAM) Usage, Disk (HDD) Usage. Пределом (Threshold) по каждому из параметров для оповещения Клиента являются значения, которые определяются индивидуально по требованию Клиента и фиксируются в Заказе на Услугу.

2. ОСОБЕННОСТИ ОРГАНИЗАЦИИ И ОКАЗАНИЯ УСЛУГИ

14. Устные и письменные консультации по вопросам оказания Услуги (информационная поддержка) осуществляются Оператором в рабочее время по телефонам +375 17 287 11 11 и/или +375 17 287 11 49 и/или посредством электронной почты sales@becloud.by.

15. Организация, выразившая готовность заключить Договор, до его подписания обязана заключить с Оператором Соглашение о конфиденциальности (при необходимости) и заполнить опросный лист, по

формам, размещенным на сайте Оператора, а также согласовать с Оператором параметры Заказа по форме, установленной настоящими Правилами в разделе 6 «Формы документов».

16. При формировании Заказа на Услугу необходимо соблюдать и учитывать ряд правил, установленных Оператором:

максимальное количество процессоров для VM – 24 vCPU, максимальный объем vRAM 128ГБ (из расчета на одну VM);

максимально допустимое соотношение выделяемых виртуальных ресурсов для одной VM (vCPU/vRAM) – 1:N, где N<=8;

максимальный размер одного vHDD для VM – 10 ТБ;

максимальный размер vHDD для резервного копирования – не более 3-х кратного размера дискового пространства, выделенного Клиенту в рамках ресурсов vHDD.

17. Оказание Услуги в Тестовом периоде не превышает 14 дней.

18. Дата начала оказания Услуги фиксируется в Акте начала оказания Услуги.

19. В течение 5 (пяти) рабочих дней после вступления Договора в силу Оператор обеспечивает возможность использования VDC (в размере ИТ-ресурсов, запрошенных Клиентом).

20. Для исполнения п.19 уполномоченному администратору Клиента на адрес электронной почты, указанный в Договоре, с электронного адреса noreply@becloud.by Оператором передается информация о порядке и реквизитах доступа (за исключением пароля) в закодированном архиве и пароль от архива в виде SMS-сообщения - на указанный мобильный номер телефона. С момента передачи уполномоченному администратору Клиента порядка и реквизитов доступа ответственность за смену пароля, его конфиденциальность возлагается на Клиента.

21. Управление виртуальной инфраструктурой, предоставленной Клиенту, осуществляется уполномоченным администратором Клиента через Портал, который позволяет:

создавать VM и управлять ими;

создавать внутренние и маршрутизируемые (с выходом в Интернет) и изолированные сети;

устанавливать VM с операционными системами из имеющихся шаблонов и загружать образы операционных систем с самостоятельной установкой;

гибко управлять правами доступа к пулу виртуальных ресурсов;

настраивать балансировку нагрузки между сетевыми интерфейсами VM;

и другое

в соответствии с документом «Управление облачной платформой VMware vCloud Director. Руководство пользователя», подключение уполномоченного администратора Клиента к Порталу с использованием средств криптографической защиты информации осуществляется в соответствии с документом «Инструкция по подключению к vCloud Director», размещенными в разделе «Услуги» на официальном сайте Оператора.

Данные для доступа и авторизации на Портале предоставляются Клиенту после подключения Услуги в соответствии с установленной у Оператора политикой информационной безопасности.

Доступ уполномоченных администраторов Клиента к Порталу осуществляется с использованием криптографических средств защиты информации посредством браузеров Google Chrome, Mozilla Firefox, Internet Explorer.

22. Доступ уполномоченных администраторов Клиента к ИР/ИС, размещенным в предоставленном Клиенту VDC, осуществляется удаленно через организованный канал с использованием сети Интернет (в рамках Заказа на Услугу) или выделенный канал связи (с заключением договора на услуги электросвязи).

23. Для ИС классов 5-гос, 5-частн в соответствии с СТБ 34.101.30-2017 «Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация» возможны следующие схемы организации доступа уполномоченных администраторов Клиента:

через сеть Интернет;

через сеть Интернет с использованием средств криптографической защиты информации;

через ЕРСПД на сетевом уровне (L3VPN);

через ЕРСПД на сетевом уровне (L3VPN) с использованием средств криптографической защиты информации;

с доступом к ЕРСПД на канальном уровне (L2);

с доступом к ЕРСПД на канальном уровне (L2) с использованием средств криптографической защиты информации;

24. Для ИС классов 3-фл, 3-юл, 3-дсп в соответствии с СТБ 34.101.30-2017 «Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация» возможны следующие схемы организации доступа пользователей Клиента:

через сеть Интернет с использованием средств криптографической защиты информации[1];

через ЕРСПД на сетевом уровне (L3VPN) с использованием средств криптографической защиты информации[2];

с доступом к ЕРСПД на канальном уровне (L2) с использованием средств криптографической защиты информации[2].

25. Перенос ИР и ИС Клиента на республиканскую платформу осуществляется Клиентом самостоятельно.

26. Клиент несет исключительную ответственность за организованный им доступ к ИР и/или ИС, размещенным в рамках выделенного Клиенту VDC и порядок использования ИТ-ресурсов в рамках выделенного Клиенту VDC.

27. В случае утери или компрометации реквизитов доступа Клиент обязан незамедлительно сообщить о данном факте и обратиться за получением новых реквизитов по электронному адресу vdcsupport@becloud.by. Обращение должно

[1] Для организации сетевого доступа к ИС класса 3-дсп (СТБ 34.101.30-2017) применяются выделенные программно-аппаратные средства криптографической защиты информации, предоставляемые Клиентом.

производиться с электронного адреса уполномоченного администратора Клиента, указанного в Договоре.

28. После процедуры изменения или сброса реквизитов доступа Клиент должен направить в адрес Оператора заявление на официальном бланке организации за подписью уполномоченного лица с соответствующим запросом и указанием причины изменения или сброса реквизитов доступа в рамках оказываемой Услуги (с указанием реквизитов Договора).

29. При заказе прав (лицензий) на программное обеспечение (ПО) операционной системы Microsoft Оператор передает ПО путем предоставления удаленного доступа к заказанному Клиентом ПО, размещенному на республиканской платформе, с последующей установкой ПО на виртуальную машину. Для оказания данной услуги Клиент предоставляет Оператору временный доступ к виртуальной машине. Правообладатель ПО Microsoft – компания Microsoft и его аффилированные лица не предоставляют технической поддержки в отношении заказанного Клиентом в рамках Услуги ПО.

30. При заказе прав (лицензий) на ПО антивирусной защиты VM оплата ПО производится ежемесячно (по подписочной модели – от момента оформления Заказа до момента окончания месяца, в котором производится отказ от ПО). При отказе от ПО оплата заказанного ПО производится за полный календарный месяц его использования.

31. При заказе прав (лицензий) на ПО криптографической защиты информации Оператор предоставляет Клиенту доступ к инсталляционному пакету ПО для его загрузки и инструкцию по установке. Оплата ПО производится ежемесячно (по подписочной модели – от момента оформления Заказа до момента окончания месяца, в котором производится отказ от ПО). При отказе от ПО оплата заказанного ПО производится за полный календарный месяц его использования. Дополнительно, в случае использования технологических сертификатов открытого ключа, Клиент возмещает стоимость их выпуска в РУЦ ГосСУОК.

3. ОБЯЗАННОСТИ СТОРОН

32. Клиент обязуется:

32.1. Для повышения уровня информационной безопасности выполнять следующие требования, которые могут быть дополнены положениями Политики информационной безопасности или иных локальных правовых актов Клиента:

32.1.1. для операционных систем (ОС) семейства Windows:

встроенная учетная запись с административными правами Administrator (Администратор) должна быть переименована именем, не связанным с ее назначением, должна быть отключена и предназначена только для служебного использования для настройки или обслуживания ИС и/или ИР при загрузке в «безопасном режиме»;

пароль должен соответствовать требованиям Политики информационной безопасности Клиента и сохраняться в секрете в соответствии с требованиями

локальных правовых актов Клиента, регламентирующих работу с информацией ограниченного распространения;

встроенная учетная запись Guest (Гость) должна быть отключена.

32.1.2. для ОС семейства Linux:

должен быть запрещен вход в ОС от имени учетной записи суперпользователя (root);

должна быть настроена авторизация пользователей с применением логина/пароля или сертификатов открытых ключей (по возможности контейнер с личным ключом пользователя должен быть защищен);

32.1.3. персонифицировать все учетные записи так, чтобы они позволяли однозначно идентифицировать субъекта, взаимодействующего с системным и прикладным программным обеспечением, установленным на ИТ-ресурсах Клиента;

32.1.4. настроить ограничение доступа к администрированию (административной части) ИС и/или ИР Клиента со стороны Клиента (третьих лиц, допущенных Клиентом) по сетевым (IP) адресам и портам протоколов транспортного уровня;

32.1.5. на ИС и/или ИР Клиента настроить и обеспечить функционирование средств аудита, обеспечивающие достаточный для проведения расследования инцидентов информационной безопасности уровень журналирования;

32.1.6. осуществлять работу с ИС и/или ИР Клиента (уполномоченного персонала Клиента (или уполномоченной Клиентом организации)) только с правами, принадлежащими роли «Пользователь» и предоставлением прав доступа к локальным каталогам, файлам, ветвям реестра, необходимым для нормальной работы с ИС и/или ИР в рамках предоставленных ему полномочий (привилегий).

32.1.7. использовать пароли, удовлетворяющие следующим критериям:

при первом входе в ОС должно производиться изменение временного пароля;

пароль должен состоять не менее чем из двенадцати символов;

в составе пароля должна применяться комбинация, состоящая из цифр, букв верхнего и нижнего регистра, спецсимволов;

пароль должен храниться в секрете;

не допускается передача пароля другим сотрудникам, а также посторонним лицам;

должно производиться изменение паролей при подозрении на их компрометацию;

пароль должен изменяться через регулярные промежутки времени (не реже 180 дней);

недопустимо использование предыдущих паролей за последние 12 месяцев.

32.2. выполнять рекомендации Оператора по обеспечению технических характеристик оборудования для рабочего места уполномоченного администратора Услуги и к рабочим местам персонала Клиента;

32.3. незамедлительно информировать Оператора об отклонениях от Согласованного уровня Услуг или же о другом обнаруженном событии, которое способно нарушить процесс оказания Услуг;

32.4. обеспечивать сохранность и конфиденциальность полученной от Оператора информации по исполнению Договора;

32.5. предпринять все меры, необходимые для подготовки собственной инфраструктуры к эффективному использованию Услуг, в том числе обеспечить функционирование средств защиты информации ИС и/или ИР;

32.6. выполнять обновление системного и прикладного ПО, программных средств защиты информации, используемых в ИС и/или ИР Клиента;

32.7. выполнять резервное копирование ИС и/или ИР в соответствии с принятой у Клиента политикой резервного копирования;

32.8. проверять возможность восстановления из резервных копий;

32.9. выполнять восстановление данных своими силами и за свой счет;

32.10. обеспечивать целостность своих ИС и/или ИР;

32.11. нести ответственность за управление безопасностью своих ИС и/или ИР (в том числе, в случаях привлечения для этой цели третьих лиц);

32.12. предоставлять запрашиваемую Оператором информацию об использовании Услуги в целях улучшения качества оказания Услуги Оператором;

32.13. обеспечить функционирование системы защиты информации, ведение и анализ журнала аудита и событий безопасности в части ИС и/или ИР Клиента. В случае инцидента, связанного с безопасностью информации Клиент, установив факт инцидента, незамедлительно уведомляет Оператора об инциденте на адрес электронной почты службы технической поддержки Оператора vdcsupport@becloud.by и дополнительно телефонным звонком на номер +375 (29) 249-38-89. Оператор и Клиент согласуют меры, которые необходимо предпринять для снижения воздействия инцидента и для его устранения;

32.14. обеспечить принятие необходимых мер по устранению инцидентов, влекущих несанкционированное использование ИС и/или ИР Клиента и/или связанных с подозрительной активностью со стороны ИС и/или ИР Клиента и выполнять рекомендации Оператора.

32.15. предоставлять по запросу Оператора журналы аудита в рамках решения инцидентов информационной безопасности;

32.16. использовать Услугу на условиях и с ограничениями Лицензионных соглашений правообладателей заказанного ПО;

32.17. в случае, если в рамках потребления Услуги Клиент заказывает и использует программное обеспечение Microsoft, правообладателем которого является компания Microsoft, руководствоваться правилами и ограничениями, определенными в актуальной версии документа «ServiceProviderUseRights», размещенного в открытом доступе в сети Интернет по адресу https://www.microsoft.com/ru-ru/Licensing/product-licensing/products. Клиент несет ответственность за использование ПО в соответствии с установленными

правилами и самостоятельно должен отслеживать обновления версий документа «ServiceProviderUseRights».

32.18.предоставить касающиеся Клиента сведения о его наименовании и реквизитах (в отношении Клиентов – юридических лиц) Правообладателю и его аффилированным лицам;

32.19.не удалять, не изменять или не скрывать любые уведомления об авторских правах, товарные знаки или другие уведомления об имущественных правах, содержащиеся в ПО;

32.20.не вскрывать технологии, не производить декомпиляцию и дизассемблирование компьютерных программ за исключением случаев, прямо предусмотренных законодательством Республики Беларусь;

32.21.не использовать Услугу для размещения в сети Интернет, а также для передачи через сеть Интернет любой информации, хранение и распространение которой запрещено в соответствии с законодательством;

32.22.не использовать Услугу для публикации, передачи, запроса и использования информации или ПО, которые заведомо содержат в себе вирусы или иное вредоносное программные компоненты, в том числе позволяющие получать чужие пароли либо наносить иной вред пользователям сети Интернет;

32.23.не использовать Услугу для осуществления несанкционированного доступа к ресурсам сети Интернет иди других сетей;

32.24.не проводить и не принимать участие в проведении сетевых атак и сетевого взлома.

33. Оператор обязуется:

33.1. использовать при оказании Услуги оборудование, размещенное на территории Республики Беларусь;

33.2. при оказании Услуги применять средства защиты информации, прошедшие подтверждение соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY) в форме сертификации или декларирования соответствия;

33.3. предоставлять Клиентам IP-адреса из подсетей, специально выделенных для этих целей Оператором;

33.4. обновлять заказанное у Оператора ПО, используемое для оказания Услуги, в соответствии с порядком, установленным у Оператора;

33.5. ежегодно осуществлять внутренний аудит собственных систем защиты информации;

33.6. обеспечить доступность ИС и/или ИР Клиента, размещенных на ИТ-ресурсах Оператора, в сети Интернет в течение срока действия Договора;

33.7. обеспечивать информационную безопасность ИТ-ресурсов, выделенных Клиенту:

защиту от распределенных атак, направленных на нарушение доступности («AntiDDoS»). Порог противодействия – 40 Гбит/с;

защиту от сетевых вторжений («Intrusion Prevention System»);

фильтрацию трафика от вредоносного программного обеспечения («потоковый антивирус»);

ограничивать доступ к сети Интернет в соответствии со списками ограниченного доступа, формируемыми РУП «БелГИЭ»;

предоставлять ресурсы хранения данных для осуществления еженедельного резервного копирования ИС и/или ИР Клиента в соответствии с Тарифами Оператора;

предоставлять доступ к сервису точного (эталонного) времени Оператора (обеспечивать возможность синхронизации времени ИТ-ресурсов, выделенных Клиенту, со средой виртуализации, синхронизированной с источником точного (эталонного) времени Национального эталона времени и частоты Республики Беларусь республиканского унитарного предприятия «Белорусский государственный институт метрологии»).

34. В рамках оказываемых Услуг Оператор:

34.1. обеспечивает изоляцию ИС и/или ИР Клиента от ИС и/или ИР Оператора и третьих лиц;

34.2. в соответствии с политикой информационной безопасности осуществляет непрерывный мониторинг предоставленной инфраструктуры, телекоммуникационного оборудования, средств защиты информации Оператора, связанных с оказанием Услуги;

34.3. На основании отдельных Заказов Клиента в соответствии с Тарифами Оператора предоставить Клиенту следующие сервисы безопасности:

защита от атак на веб-приложения с использованием технологии инспекции SSL/TLS-соединений[2];

34.4. предоставление системы обработки DNS-запросов пользователей с исключением прямого использования иностранных DNS-серверов;в случае регистрации инцидента, связанного с безопасностью информации, Оператор:

34.5. установив факт инцидента, незамедлительно уведомляет определенных Договором Уполномоченных администраторов Клиента. Оператор и Клиент согласуют меры, которые необходимо предпринять для снижения воздействия инцидента и для его устранения;

проводит информирование Оперативно-аналитического центра при Президенте Республики Беларусь об обнаружении инцидентов информационной безопасности, зарегистрированных в рамках оказания Услуги.

35. Оператор не несет ответственность за:

35.1. изменения, произведенные Клиентом при настройке средств защиты ИС и/или ИР Клиента;

35.2. целостность информации Клиента;

35.3. настройку средств аудита, мониторинг и хранение журналов аудита системного и прикладного ПО, используемого Клиентом, а также средств защиты информации Клиента.

35.4. получение доступа третьими лицами к ИС и/или ИР Клиента и/или административной части ИС и/или ИР в связи с обстоятельствами, за которые Оператор не отвечает (неприменение средств защиты информации, передача

[2] В случае заказа такой услуги Клиент обязан предоставить Оператору цепочку сертификатов (корневого и подчиненных удостоверяющих центров), а также сертификат (открытую и закрытую часть ключа) для защиты от атак на веб-приложения с использованием технологии инспекции SSL/TLS-соединений.

учетных данных, использование стандартных имен учетных записей, «слабых» паролей и т.п.), уязвимостей ПО Клиента.

4. СОГЛАШЕНИЕ ОБ УРОВНЕ ОБСЛУЖИВАНИЯ

36. Определение доступности услуги

36.1. Доступность (availability) – свойство нахождения в состоянии готовности и пригодности для использования по запросу авторизированного логического объекта.

36.2. Услуга считается доступной, если ее эксплуатационные характеристики соответствуют гарантированным Оператором параметрам.

36.3. Значение доступности Услуги (SA – Service Availability) – это отношение количества минут в Отчетном периоде, в течение которых Услуга была доступна, к общему количеству минут в Отчетном периоде, выраженное в процентах.

37. Уровень доступности

37.1. Значение SA доступности инфраструктуры (вычислительные машины, системы хранения данных) в Отчетном периоде – 99,5%.

37.2. Перерывы предоставления доступа к Услуге квалифицируются как предоставление доступа к Услуге в штатном режиме и не включаются во время недоступности Услуги, если такие перерывы явились следствием:

изменения Клиентом настроек ПО, прямо или косвенно влияющих на доступ к Услуге, производимые без согласования с Оператором;

любых задержек, прерываний, при условии, что все вышеперечисленные события произошли не по вине Оператора;

нарушения Клиентом условий Договора с Оператором в части обеспечения условий, необходимых для доступа к Услуге, в том числе условий оплаты;

неработоспособности или несовместимости ПО, устанавливаемого Клиентом на защищенный виртуальный сервер;

доступа третьих лиц к учетным данным Клиента, произошедшего по вине Клиента;

обстоятельств непреодолимой силы, определенных согласно условий Договора.

37.3. В случае проведения работ по обслуживанию Оператор имеет право на прерывание доступа к Услуге, предварительно уведомив об этом Клиента. Данные перерывы не квалифицируются в качестве отсутствия доступа к Услуге.

38. Работы по обслуживанию

38.1. Для поддержания Согласованного уровня услуг Оператор проводит работы по обслуживанию. Тип работ по обслуживанию, период их выполнения и продолжительность, а также и обязательства Оператора по уведомлению Клиента определены в нижеприведенной таблице:

Тип работ по обслуживанию	Период проведения работ	Уведомление Клиента
Плановые работы по обслуживанию, не	Рабочее время*	Без уведомления Клиента

способные оказать влияние на доступность или функциональность Услуги		
Плановые работы по обслуживанию, способные оказать влияние на доступность или функциональность Услуги	Круглосуточно, по возможности вне рабочего времени*	Не позднее чем за 24 часа до начала работ и не позднее 1 часа после окончания работ
Аварийно-восстановительные работы по восстановлению доступности или функциональности Услуги	Осуществляются круглосуточно	Не позднее 1 часа после возникновения аварийно-восстановительных работ и не позднее 1 часа после окончания работ

*Рабочим временем считается период с 9:00 до 18:00 в будние дни.

5. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

39. Классификация инцидентов

39.1. Инцидентом, сопутствующим Услуге, считается любое незапланированное событие, которое сказалось либо могло сказаться на доступности Услуги или качестве ее предоставления.

39.2. Оператор и Клиент будут взаимодействовать для предотвращения инцидентов и оперативного устранения их с тем, чтобы свести к минимуму их воздействие на Услуги. При установлении приоритетности в устранении инцидента будут учитываться установленные на этот счет правила.

39.3. Приоритетность устранения инцидентов представлена в таблице

Приоритет	Описание инцидента	Период работ по устранению инцидента
Высокий	Инцидент считается «Высокий» в случаях: полного прерывания оказания Услуги (недоступность Услуги)	Круглосуточно
Средний	Инцидент считается «Средний» в случаях: существенного ухудшения ключевых показателей качества Услуги; нештатные ситуации, которые оказывают существенное влияние на	Круглосуточно

	предоставление Услуги и способные привести к инциденту высокой степени воздействия (Critical)	
Низкий	Инцидент считается «Низкий» в случаях: возникновения проблем, которые не оказывают влияния или оказывают несущественное влияние на предоставление Услуги и не способные привести к инциденту высокой степени воздействия (Critical)	Рабочее время

40. Уведомление об инцидентах и их устранение

40.1. Любой инцидент, сопутствующий Услугам, доводится Клиентом до сведения Оператора направлением информации о инциденте (далее Заявки) на адрес электронной почты службы технической поддержки Оператора vdcsupport@becloud.by и дополнительно телефонным звонком на номер +375 (29) 249-38-89. Оператор оказывает техническую поддержку исключительно по Заявке Клиента и только от уполномоченного представителя Клиента, указанного в разделе Договора «Контактные данные Сторон».

40.2. Оператор отреагирует на инциденты, о которых уведомил Клиент, в соответствии правилами, указанными ниже. Устранение инцидентов будет осуществляться в режиме 24×7×365(366) в соответствии с принципом «наилучшее усилие», согласно которому Оператор приложит все старания для того, чтобы оказывать Услуги на самом возможно высоком уровне.

40.3. Время реагирования в зависимости от их приоритетности в таблице ниже:

Приоритетность инцидента	Время реагирования Оператора
Высокий	1 час
Средний	2 часа
Низкий	4 часа

40.4. Оператор может связаться с лицом, уведомившем об инциденте, для уточнения информации, предоставленной Клиентом.

40.5. Оператор определит причину инцидента и меры, которые необходимо предпринять для устранения инцидента. На всем протяжении устранения инцидента Оператор будет предоставлять Клиенту информацию о прогрессе, достигнутом в устранении инцидента.

40.6. Ответственные лица Оператора могут ходатайствовать о привлечении к устранению инцидента ответственных лиц Клиента с целью оперативного снижения степени воздействия инцидента и его устранения.

40.7. В случае, если Клиент не согласен с уровнем устранения инцидента, он может ходатайствовать о повторном открытии инцидента. В противном случае инцидент считается закрытым.

40.8. Все инциденты, о которых уведомил Клиент, регистрируются. Оператор использует информацию о произошедших инцидентах с целью улучшения качества оказываемых Услуг и не допущения их повторения.

6. ФОРМЫ ДОКУМЕНТОВ

Форма

ЗАКАЗ №_____ от «_____»_____20_ г.
к Договору № __ оказания услуги предоставления облачной инфраструктуры
«Защищенная виртуальная инфраструктура»
от «___» _____ 20_ г.

(ОБЩАЯ ЧАСТЬ)

Наименование клиента:
Тип заказа: (новая услуга, изменение услуги)
Дата начала оказания услуг: __.__.20__

1. Объем ИТ-ресурсов, запрашиваемых Клиентом

№	Наименование позиции	Кол-во, ед.	Цена за ед., без НДС, руб./мес.	Стоимость без НДС, руб.	Скидка, %	Стоимость со скидкой, без НДС, руб.
1.	Виртуальное процессорное ядро (vCPU), ядер					
2.	Оперативная память (vRAM), ГБ					
3.	Система хранения данных на базе SSD, ГБ					
	Дополнительные ресурсы, услуги, лицензии					
4.	Лицензия на ПО Veeam BackUp & Replication, ед.					
5.	Система хранения данных на базе NL SAS для резервного копирования, ГБ					
6.	Лицензии на программные средства криптографической защиты информации					
6.1.	Для доступа к средствам управления виртуальной инфраструктурой Клиента (указать наименование), ед.					
6.2.	Для установки в виртуальной					

	инфраструктуре Клиента (IaaS) (указать наименование), ед.					
6.3.	Для установки на площадке Клиента (указать наименование), ед.					
9	Лицензия на ПО антивирусной защиты (Kaspersky/ESET/VBA), ед.					
10	IP-адрес(-а)					
11	Доступ к программному обеспечению (указать наименование ПО), ед.					
	…					
	Ежемесячная плата, бел. руб.					
	Сумма НДС*, 20%, руб.					
	Ежемесячная плата с учетом НДС*, руб.					
	Дополнительные разовые услуги, бел. руб.					
	Сумма НДС*, 20%, руб.					
	Дополнительные разовые услуги с учетом НДС*, руб.					
	Оплата за период с _____ по _____: сумма без НДС _____, сумма НДС* _____, всего с НДС _____					

**При наличии*

Оператор
СООО «Белорусские облачные технологии»
220030, Республика Беларусь,
г. Минск, ул. К.Маркса, 29, пом.2,
УНП 191772685
р/с BY59SLAN30121684600170000000
в ЗАО «Банк ВТБ», SLANBY22
г. Минск, ул. Московская, д.14

_____/ /
М.П.

Клиент

_____/ /
М.П.

Форма

ЗАКАЗ №_____ от «_____»_____20_ г.

к Договору № __ оказания услуги предоставления облачной инфраструктуры «Защищенная виртуальная инфраструктура» от «___» _____ 20__ г.

(ТЕХНИЧЕСКАЯ ЧАСТЬ)

1. Клиент является:

государственным органом и иной государственной организацией, подчиненной (подотчетной) Президенту Республики Беларусь, Совету Республики и Палате представителей Национального собрания Республики Беларусь, Конституционному Суду Республики Беларусь, Верховному Суду Республики Беларусь, Аппарату Совета Министров Республики Беларусь, республиканским органам государственного управления и иным государственным организациям, подчиненным Правительству Республики Беларусь, местным исполнительным и распорядительным органам, судам;	☐
организацией, подчиненной (входящим в состав, систему) государственных органов и организаций, указанным в абзаце первом настоящего пункта; иной государственной организацией, определяемой ОАЦ для оказания ей интернет-услуг уполномоченным поставщиком интернет-услуг.	☐
органом, осуществляющим оперативно-розыскную деятельность	☐
иной государственной организацией	☐
организацией с иной формой собственности	☐

2. При предоставлении доступа к сети Интернет необходимо обеспечить дополнительную защиту информационных ресурсов Клиента (требуемое отметить):

☐ обеспечить защиту от атак на веб-приложения с использованием технологии инспекции SSL/TLS соединений[3];

☐ предоставить систему обработки DNS-запросов пользователей с исключением прямого использования иностранных DNS-серверов.

[3] В случае использования интернет-ресурсом Клиента протокола HTTPS (SSL/TLS-соединений) Клиент обязан предоставить Оператору цепочку сертификатов (корневого и подчиненных удостоверяющих центров), а также сертификат интернет-ресурса Клиента (открытую и закрытую часть ключа) для защиты от атак на веб-приложения с использованием технологии инспекции SSL/TLS-соединений.

Оператор	**Клиент**
СООО «Белорусские облачные технологии» 220030, Республика Беларусь, г. Минск, ул. К.Маркса, 29, пом.2, УНП 191772685 р/с BY59SLAN30121684600170000000 в ЗАО «Банк ВТБ», SLANBY22 г. Минск, ул. Московская, д.14	
_____/ /	_____/ /
М.П.	М.П.

Форма

Акт начала оказания Услуг

к Договору № __ оказания услуги предоставления облачной инфраструктуры «Защищенная виртуальная инфраструктура» от «___» _____ 20__ г.

г. Минск «___» _____ 20_ г.

В соответствии с Договором № __ оказания услуги предоставления облачной инфраструктуры «Защищенная виртуальная инфраструктура» от «___» _____ 20__ г., настоящим Актом начала оказания Услуг удостоверяем, что:

1. Дата начала оказания Услуг – _____ г.
2. Стороны друг к другу претензий не имеют.

Настоящий Акт составлен на русском языке в двух экземплярах, каждый из которых имеет одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

В УДОСТОВЕРЕНИЕ всего изложенного настоящий Акт начала оказания Услуг подписан и скреплен подписями должным образом уполномоченных представителей обеих Сторон.

Оператор **СООО «Белорусские облачные технологии»** 220030, Республика Беларусь, г. Минск, ул. К. Маркса, 29, пом.2, УНП 191772685 р/с BY59SLAN30121684600170000000 в ЗАО «Банк ВТБ», SLANBY22 г. Минск, ул. Московская, д.14	**Клиент**
_____/ /	_____/ /
М.П.	М.П.

Форма

Акт сдачи-приемки оказанных услуг

к Договору № __ оказания услуги предоставления облачной инфраструктуры «Защищенная виртуальная инфраструктура» от «___» _____ 20_ г.

г. Минск «___» _____ 20_ г.

В соответствии с Договором № __ оказания услуги предоставления облачной инфраструктуры «Защищенная виртуальная инфраструктура» от «___» _____ 20_ г., и настоящим Актом сдачи-приемки оказанных Услуг Стороны удостоверяют, что:

1. Оператор предоставил Клиенту Услуги в соответствии с таблицей:

№ п/п	Заказ (№, дата)	Период оказания Услуги	Стоимость без НДС, бел. руб.
1.			
2.			
Итого стоимость, бел.руб.			
Сумма НДС при ставке 20%, бел.руб.			
Всего с НДС, бел.руб.			

Итого оказано услуг на сумму: _____ (_____), с учетом НДС при ставке 20%,

в том числе НДС составляет: _____(_____).

2. Услуги оказаны в полном объеме. Клиент не имеет претензий к Оператору по качеству оказанных услуг.

3. Настоящий Акт составлен каждой Стороной на русском языке единолично в соответствии с постановлением Министерства финансов Республики Беларусь от 12.02.2018 № 13 «О единоличном составлении первичных учетных документов и признании утратившим силу постановления Министерства финансов Республики Беларусь от 21.12.2015 № 58» и имеет одинаковую юридическую силу для каждой из Сторон.

4. Подписание Акта каждой Стороной единолично свидетельствует о сдаче-приемке оказанных услуг и является основанием для оплаты.

Оператор
СООО «Белорусские облачные технологии»
220030, Республика Беларусь,
г. Минск, ул. К. Маркса, 29, пом.2,
УНП 191772685
р/с BY59SLAN30121684600170000000
в ЗАО «Банк ВТБ», SLANBY22
г. Минск, ул. Московская, д.14

_____/ /
М.П.

Форма

Акт сверки технических перерывов при оказании Услуг

к Договору № __ оказания услуги предоставления облачной инфраструктуры «Защищенная виртуальная инфраструктура» от «___» _____ 20_ г.

г. Минск «___» _____ 20_ г.

СООО «Белорусские облачные технологии», именуемое в дальнейшем «Оператор», в лице _____, действующего на основании _____, и

_____, именуемое в дальнейшем «Клиент», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», а каждое по отдельности «Сторона», удостоверяют нижеследующее:

1. Настоящим подтверждаем факт перерыва предоставления услуги:

№	Наименование услуги	Дата и время начала перерыва	Дата и время окончания перерыва	Общее время перерыва	Причина перерыва

2. Настоящий Акт является основанием для перерасчета стоимости оказания Услуг.
3. Настоящий Акт составлен в двух экземплярах, по одному для каждой Стороны.

Оператор
СООО «Белорусские облачные технологии»
220030, Республика Беларусь,
г. Минск, ул. К. Маркса, 29, пом.2,
УНП 191772685
р/с BY59SLAN30121684600170000000
в ЗАО «Банк ВТБ», SLANBY22
г. Минск, ул. Московская, д.14

_____/ /
М.П.

Клиент

_____/ /
М.П.