

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ ОБЪЕКТНОЕ ХРАНИЛИЩЕ S3

1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГИ

- 1.1. Услуга предоставляет доступ к Объектному хранилищу - высокомасштабируемой аппаратно-программной платформе хранения данных, которая позволяет Заказчикам хранить, обрабатывать неструктурированные данные (объекты) и извлекать любые объемы данных.
- 1.2. Доступ к Объектному хранилищу предоставляется с помощью API интерфейса. Список поддерживаемых команд API Объектного хранилища S3 и их описание находятся на Портале по адресу: <https://portal.sbercloud.ru/swagger#/buckets>, а также в описании аппаратного хранилища данных, на котором работает Корзина по адресу <https://docs.sbercloud.ru/s3/ug/index.html>
- 1.3. Услуга реализована средствами аппаратно-программной платформы Исполнителя.
- 1.4. Управление Объектным хранилищем осуществляется Заказчиком посредством функционала Портала.
- 1.5. **Состав Услуги и основные компоненты.** В состав Услуги ходят следующие опции:
- Объектное хранилище S3, хранение данных;
 - Объектное хранилище S3, георепликация данных;
 - Объектное хранилище S3, исходящий трафик;
- 1.6. В целях обеспечения защиты Объектного хранилища реализовываются следующие меры и механизмы защиты:

Табл.1. Обеспечение защиты Объектного хранилища S3

Уровни защиты	Мероприятия
Защита инфраструктуры Объектного хранилища 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 периметра инфраструктуры с использованием межсетевых экранов нового поколения (NGFW), осуществляющих в том числе выявление и предотвращение компьютерных атак.
Инфраструктурный	Обеспечивается: <ul style="list-style-type: none"> - двухфакторная аутентификация администраторов инфраструктуры; - подключение администраторов инфраструктуры к средствам ее управления с использованием VPN; - контроль действий привилегированных пользователей (администраторов инфраструктуры) 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 Объектного хранилища S3 с привлечением сторонних организаций. Выявленные в ходе соответствующего тестирования и/или аудита недостатки устраняются по факту их выявления.
Защита Портала	
Приложения	Обеспечивается на уровне приложений с использованием специализированного межсетевого экрана уровня приложений.
Дополнительный	Осуществляются регулярные сканирования Портала на наличие актуальных уязвимостей. Проводятся тестирования на проникновение с привлечением сторонних организаций. Уязвимости и/или недостатки устраняются по факту их выявления.
Защита интерфейсов доступа к Объектному хранилищу	
Мероприятия	
Подключение, создание, загрузка и передача Объектов в Объектное хранилище S3 осуществляется по протоколу HTTPS (TLS v1.2, 1.3).	

Запросы на доступ к Объектам через S3 REST API проходят проверку подлинности с помощью метода Hash-based Message Authentication Code (HMAC).
Разграничение доступа к пользовательским данным Объектного хранилища
Мероприятия
Заказчику предоставляется доступ только к выделенным для него Пространству имен и Корзинам внутри него.
Для получения доступа к своей Корзине Заказчик должен авторизоваться в системе с помощью Access key/Secret key. Автоматическая Генерация ключей происходит при создании Пространства имен, кроме этого, Заказчик может самостоятельно управлять созданием ключей и разграничением прав доступа к Корзинам. Исполнитель не имеет доступа к хранящимся внутри Пространства имен данным и не производит их загрузку, обработку, изменение, удаление, копирование либо иные действия.
При уничтожении выделенного Пространства имен оно уничтожается вместе с имеющимися внутри него данными.

1.7. Типы ресурсов:

- 1.7.1. Объем хранимых данных - объем хранимых данных Заказчика на аппаратно-программной платформе Исполнителя.
- 1.7.2. Объем исходящего трафика - объем исходящего трафика Заказчика, переданного из зон доступности Исполнителя.
- 1.7.3. Объем входящих обращений к хранилищу (Requests) - объем входящих обращений Заказчика к аппаратно-программной платформе Исполнителя.

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

Табл.2. Типы подключения к сети и сетевые сервисы

Тип подключения	Описание
Подключение через общий канал Интернет (shared)	Через Интернет с подключением к общему для всех заказчиков Услуге каналу передачи данных;
Подключение через выделенный канал Direct connect	Через выделенный канал от Объектного хранилища S3 до площадки клиента (подключение по выделенному каналу осуществляется в рамках отдельной услуги «Direct connect»).
Подключение через внутреннюю сетевую инфраструктуру SberCloud без выхода в сеть Интернет.	В случае использования услуги «Виртуальный ЦОД на базе VMware» доступ к Объектному хранилищу S3 осуществляется через внутреннюю сетевую инфраструктуру SberCloud без выхода в сеть Интернет.

1.9. Техническое описание Услуги:

Табл. 3. Техническое описание

Компонент	Описание
Программная платформа	Платформа полностью использует программно-определяемую архитектуру, что позволяет независимо масштабировать вычислительные ресурсы и ресурсы хранения.
Аппаратная платформа	Объектное хранилище представляет из себя легко масштабируемую программно-определяемую систему хранения данных, состоящую из серверов корпоративного уровня, базирующихся на процессорах архитектуры x86/64.
Георепликация данных	Услуга позволяет хранить данные в нескольких зонах доступности, которые размещаются в географически распределенных дата-центрах. Инфраструктура, которая находится в каждом из дата-центров, называется зоной доступности. Каждая зона изолирована от остальных, за счет этого достигается защита от аппаратных и программных сбоев в других зонах доступности. Заказчик может разместить информацию в одной зоне доступности (одном дата-центре) или в нескольких (в разных дата-центрах) с возможностью георепликации данных. При подключении георепликации, информация реплицируется между двумя зонами доступности, Заказчик самостоятельно выбирает зоны доступности, между которыми будет организована георепликация.
Пространство имен и Корзины	Данные Заказчика хранятся в Пространстве имен. При создании Пространства имен Заказчик выбирает одну из нескольких зон доступности, в которой будет расположено Пространство имен. Каждая зона доступности изолирована от остальных, оснащена независимыми системами электроснабжения, охлаждения и сетевого взаимодействия, за счёт чего достигается защита от аппаратных и программных сбоев. Пользователи Пространства

	<p>имен с соответствующими привилегиями могут создавать Корзины и объекты внутри них, используя API.</p> <p>Пространство имен объединяет в себе Корзины. При создании Пространства имен Заказчик может задать настройки по умолчанию для Корзин, которые будут автоматически применяться к создаваемым в Пространстве Корзинам. Заказчик может изменить настройки по умолчанию. В рамках Пространства имен Заказчик может выставлять настройки и правила, которые будут распространяться на все Корзины в рамках Пространства имен. За счет изолирования Корзин пользователей с помощью Пространств имен не создаются конфликты между названиями Корзин разных пользователей.</p> <p>Для каждой Корзины можно выбрать класс хранения и настройки. Класс хранения выбирает Заказчик при создании Корзины. Допустимы следующие Классы хранения:</p> <ul style="list-style-type: none"> • Стандартный; • Холодный.
Объекты	<p>Объект вместе с описывающими его метаданными хранятся в паре как один объект. Такой подход позволяет совершать быстрый поиск Объектов по их метаданным. Метаданные позволяют структурировать объекты по их атрибутам.</p>

- 1.10. **Мониторинг.** Система предоставляет возможность просматривать статистику по потреблению в личном кабинете Заказчика на Портале, для мониторинга доступны:
- объем исходящего трафика;
 - объем входящего трафика;
 - объем заполненного пространства хранилища.
- 1.11. **Требования к инфраструктуре Заказчика:**
- наличие доступа в Интернет;
 - поддержка протокола S3 API.
- 1.12. **Технические особенности и ограничения:**
- 1.12.1. Услуга ограничивается перечнем поддерживаемых API запросов. Весь список запросов описан на веб сайте по адресу: <https://docs.sbercloud.ru>.
- 1.12.2. Скорость сетевого соединения для каждого Заказчика, в случае подключения через Интернет, не является гарантированной и зависит от утилизации общего интернет-канала в зоне доступности Услуги.
- 1.12.3. Производительность (количество операций чтения/записи/удаления объектов в секунду) Услуги для каждого Заказчика не является гарантированной и зависит от общей утилизации объектного хранилища в зоне доступности Услуги.
- 1.12.4. Производительность (количество операций чтения/записи/удаления объектов в секунду) Услуги зависит от размера и количества объектов, передаваемых за единицу времени в зону доступности Услуги.
- 1.12.5. Производительность (количество операций чтения/записи/удаления объектов в секунду) Услуги зависит от используемого для взаимодействия с объектным хранилищем оборудования, ПО, его настроек и скорости доступа в интернет в зоне ответственности Заказчика.
- 1.12.6. При подключении опции георепликации, производительность операций записи может незначительно отличаться от заявленных, так как для обеспечения консистентности данных требуется подтверждение о записи объектов со всех зон доступности услуги, участвующих в георепликации.

2. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И МЕТРИКИ УСЛУГИ

- 2.1. Функциональные метрики Услуги описаны в Таблице 4.

Табл.4. Параметры предоставляемых услуг

Услуга	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Объектное хранилище S3, хранение данных	ГБ	Объем хранимых данных Заказчика на аппаратно-программной платформе Исполнителя.	Нет
Объектное хранилище S3, георепликация данных	ГБ	Хранение данных в двух географически распределенных зонах доступности.	Две зоны доступности
Объектное хранилище S3, исходящий трафик	ГБ	Объем исходящего трафика Заказчика, переданного из зон доступности Исполнителя.	Нет

3. ТАРИФИКАЦИЯ УСЛУГИ

- 3.1. Для данной Услуги используется Динамическая тарификация (Pay as you go).
- 3.2. Динамическая тарификация осуществляется ежемесячно, начиная с момента подключения Услуги. Величина ежемесячного платежа за пользование Услугой определяется в соответствии с Тарифами.

4. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

- 4.1. **Возможные виды подключения / изменения / отключения Услуги:**
- 4.2. посредством подписания Заказа;
- 4.2.1. посредством совершения действий на Портале.
- 4.3. **Возможный порядок расчётов по Услуге:**
- 4.3.1. постоплата.
- 4.4. **Возможные способы оплаты / порядок пополнения баланса:**
- 4.4.1. в безналичном порядке на основании выставленного Исполнителем счёта;
- 4.4.2. посредством электронных средств платежа.