

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ УСЛУГА ОБЪЕКТНОЕ ХРАНИЛИЩЕ S3

1. НАИМЕНОВАНИЕ УСЛУГИ

- 1.1. Наименование Услуги: «Объектное хранилище S3».
- 1.2. Настоящий документ содержит описание состава Услуги, ее базовой функциональности, возможных сопутствующих и дополнительных Услуг, общего порядка подключения, изменения и отключения Услуги, условий предоставления и ограничений.

2. ИНФОРМАЦИЯ ОБ УСЛУГЕ

2.1. Краткое описание Услуги

- 2.1.1. Объектное хранилище S3 (далее и далее – «Услуга») является услугой по предоставлению доступа к Объектному хранилищу для хранения и извлечения любых объемов данных. Доступ к Объектному хранилищу предоставляется с помощью API интерфейса Amazon S3 (далее – «S3»). Услуга реализована средствами аппаратно-программной платформы Исполнителя.
- 2.1.2. Управление Объектным хранилищем осуществляется Заказчиком при помощи Портала самообслуживания (для операций по созданию и удалению Пространств имен и Корзин), а также при помощи S3 REST API для операций над Объектами.

2.2. Состав Услуги и основные компоненты

Аппаратно-программная платформа, на базе которой реализована Услуга – это высокомасштабируемая объектная платформа хранения данных, которая позволяет Заказчикам хранить и обрабатывать неструктурированные данные как Объекты. Аппаратно-программная платформа Исполнителя обеспечивает совместимость при работе с Объектами через API интерфейса S3, а также расширяет его возможности.

2.3. Обеспечение защиты инфраструктуры

- 2.3.1. Защита Объектного хранилища S3 обеспечивается посредством:

- защиты инфраструктуры Объектного хранилища S3 и средств ее управления;
- защиты Портала управления и самообслуживания инфраструктуры;
- защиты интерфейсов доступа к Объектному хранилищу S3;
- разграничение доступа к пользовательским данным Объектного хранилища S3.

- 2.3.2. Защита инфраструктуры Объектного хранилища S3 SberCloud и средств ее управления обеспечивается средствами системы защиты информации инфраструктуры облачной платформы SberCloud на следующих уровнях:

1) на физическом уровне обеспечивается

– размещение всего оборудования инфраструктуры в ЦОД, соответствующих требованиям надежности по категории Tier 3;

– контроль и управление доступом к оборудованию;

– наличие системы видеонаблюдения в ЦОДах.

2) на сетевом уровне обеспечивается защита периметра инфраструктуры с использованием межсетевых экранов нового поколения (NGFW), осуществляющих в том числе выявление и предотвращение компьютерных атак;

3) на инфраструктурном уровне обеспечивается

- 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.

Помимо этого, 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.

2.3.1. Защита Портала управления и самообслуживания инфраструктуры

Защита Портала управления и самообслуживания инфраструктуры (<https://portal.sbercloud.ru/>) обеспечивается на уровне приложений с использованием специализированного межсетевого экрана уровня приложений (Web Application Firewall). Помимо этого, осуществляются регулярные сканирования Портала на наличие актуальных уязвимостей и его периодические тестирования на проникновение с привлечением сторонних организаций. Выявленные уязвимости и/или недостатки устраняются по факту их выявления.

2.3.2. Защита интерфейсов доступа к Объектному хранилищу S3

Подключение, создание, загрузка и передача Объектов в Объектное хранилище S3 осуществляется по протоколу HTTPS (TLS v1.2), что обеспечивает надежную защиту при передаче данных от Объектного хранилища S3 SberCloud до приложения Заказчика.

Запросы на доступ к Объектам через S3 REST API проходят проверку подлинности с помощью метода Hash-based Message Authentication Code (HMAC).

2.3.3. Разграничение доступа к пользовательским данным

Заказчику предоставляется доступ только к выделенным для него Корзинам Объектного хранилища S3. При этом на время пользования Услугой доступ к указанным областям памяти других субъектов запрещен.

Для получения доступа к своей Корзине Заказчик должен предъявить свой идентификатор (Access Key) и пароль (Security Key).

Все операции по созданию, изменению (кроме изменения именования объектов) или удалению Корзин производятся Заказчиком самостоятельно через Портал (<https://portal.sbercloud.ru/>), либо через API Услуги.

Администраторы SberCloud не имеют доступа к пользовательским данным и не производят их загрузку, обработку и изменение\удаление.

2.4. **Типы ресурсов**

2.4.1. Пространство имен и Корзины

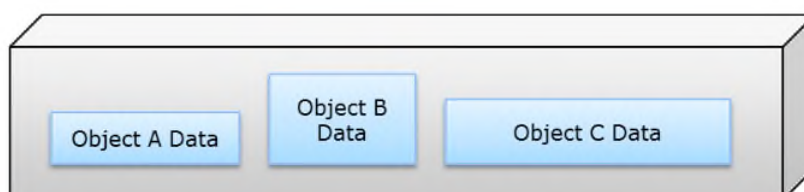
При работе с Пространством имен и Корзинами рекомендуется придерживаться следующих правил:

- Использовать префиксы в имени для группирования Корзин или Объектов – это упростит организационную структуру и позволит избежать конфликтов в наименовании (customer1.namespace1, customer1.namespace2, dev.bucket1, dev.bucket2, test.bucket1 и т.д).
- Для лучшей производительности не рекомендуется использовать более 1000 Корзин внутри одного Пространства имен.

2.4.2. Объекты

В отличие от традиционных файловых систем хранения, Объектное хранилище S3 SberCloud спроектировано таким образом, что может хранить неограниченное количество Объектов.

Внутри Объектного хранилища данные порезаны на небольшие фрагменты (chunks) и рассредоточены по дискам на нескольких нодах Объектного хранилища (серверах). Эти фрагменты могут включать в себя данные различных Объектов. Стандартный размер фрагмента для записи – 128 Мб.



2.4.3. Существует ряд особенностей при работе с Объектами разного размера:

- Небольшие Объекты_ – это Объекты размером не более 100 КВ. Запись каждого фрагмента сопряжена с рядом накладных расходов, связанных с передачей фрагмента по сети между нодами Объектного хранилища, записью на диск, журналированием, кодированием (Erasure Coding). Для того чтобы снизить эти накладные расходы при записи небольших фрагментов существует специальный механизм (box-carting). Суть механизма заключается в предварительном агрегировании множества небольших Объектов в оперативной памяти, до тех пор, пока фрагмент не достигнет размера в 2Мб, с последующей записью его на диск. Благодаря чему повышается производительность при работе с небольшими Объектами.

- Большие Объекты — это Объекты размером свыше 100 Мбайт. При работе с большими Объектами также следует придерживаться рекомендаций, которые позволят оптимизировать скорость записи/чтения.

Для работы с большими Объектами в составе S3 REST API есть вызовы, которые позволяют осуществлять доступ к составной части Объекта (multipart uploads).

2.4.4. Правила наименования

Соблюдение правил наименования является очень важным условием, которое необходимо соблюдать при создании Пространства имен (создаются системой) и Корзин (создаются Заказчиком), так как обе эти сущности могут присутствовать в DNS-имени, используемого для доступа к Объекту.

При создании Корзин нужно придерживаться следующих правил в наименовании:

- имя Корзины должно быть от 3 до 255 символов;
- для имени Корзины рекомендуется использовать строчные буквы латинского алфавита и цифры [a-z 0-9]; имя может включать символы: тире;
- имя Корзины должно начинаться и заканчиваться буквой или цифрой.

Не используйте персональную или конфиденциальную информацию в названиях Пространства имен или Корзин, так как в случае перебора имен в DNS имени можно установить действительное значение опираясь на возвращаемый код ошибки.

2.4.5. Версионность

Объектное хранилище S3 SberCloud поддерживает функцию версионности Объектов. Если эта функция активирована, то с помощью S3 REST API можно извлечь или восстановить предыдущую версию Объектов.

2.5. **Типы подключения к сети и сетевые сервисы**

Для доступа к Услуге Заказчик может выбрать тип подключения, при котором используется общий канал Интернет (shared), который 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.

При подключении через общий канал Интернет Заказчику предоставляется базовая защита информационных систем, размещаемых в инфраструктуре облачной платформы SberCloud, от DDoS-атак на канальном уровне.

2.6. **Программная платформа**

Платформа полностью использует программно-определяемую архитектуру, что позволяет независимо масштабировать вычислительные ресурсы и ресурсы хранения.

2.7. **Аппаратная платформа**

Объектное хранилище S3 SberCloud представляет из себя легко масштабируемую программно-определяемую систему хранения данных, состоящую из серверов корпоративного уровня, базирующихся на процессорах архитектуры x86/64.

Для взаимодействия между нодами и для внешнего подключения используется высокопроизводительные сетевые коммутаторы с портами 25Gb и 100Gb (UpLink).

3. БАЗОВАЯ ФУНКЦИОНАЛЬНОСТЬ И МЕТРИКИ УСЛУГИ

3.1. Услуга Объектное хранилище S3 описана в Таблице 1.

Табл. 1. Параметры предоставляемых Услуг

Сервис	Тарифицируемые единицы	Характеристики и метрики	Допустимые значения
Объектное хранилище S3	Производительность доступа по протоколу https (размер блока – 4 Кбайт)	Производительность чтения	15000 – 24000 опер/с
		Производительность записи	1700 – 5000 опер/с
	Производительность доступа по протоколу https (размер блока – 64 Кбайт)	Производительность чтения	10000 – 15000 опер/с
		Производительность записи	2000 – 4000 опер/с
	Производительность доступа по протоколу https (размер блока – 2 Мбайт)	Производительность чтения	400 – 600 опер/с
		Производительность записи	400 – 600 опер/с
	Производительность доступа по протоколу https (размер блока – 8 Мбайт)	Производительность чтения	120 – 150 опер/с
		Производительность записи	120 – 150 опер/с
	Производительность доступа по протоколу https (размер блока – 128 Мбайт)	Производительность чтения	8 – 10 опер/с
		Производительность записи	5 – 10 опер/с
	Производительность доступа по протоколу https при смешанных операциях. Чтение (размер блока - 4Кбайт) - 80%, запись (размер блока - 64Кбайт) - 20%	Производительность чтения	1400 – 5000 опер/с
		Производительность записи	380 – 1200 опер/с
	Производительность доступа по протоколу https при смешанных операциях. Чтение (размер блока - 512Кбайт) - 80%, запись (размер блока - 2Мбайт) - 20%	Производительность чтения	1300 – 1500 опер/с
		Производительность записи	320 – 380 опер/с
Сетевые сервисы	Доступ в Интернет в общем канале	Полоса пропускания	5 Гбит/с

4. ТАРИФИКАЦИЯ УСЛУГИ

4.1. Для данной Услуги используется Динамическая тарификация (Pay as you go).

4.2. Величина ежемесячного платежа за пользование Услугой определяется в соответствии с заказанным объемом перечисленных ниже опций:

- Тарификация в соответствии с объемом хранимых данных за Отчётный период;
- Тарификация в соответствии с объемом исходящего трафика от Объектного хранилища S3 к Заказчику за Отчётный период.

4.3. Окончательная стоимость Услуги формируется на основе Тарифов, согласованных Сторонами.

4.4. Динамическая тарификация осуществляется в почасовом порядке (из расчета стоимости 1 (одного) часа), начиная с подключения Услуги.

4.5. Данные (отчёты об использовании) по динамической тарификации Заказчик может запросить у менеджера по Договору.

5. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

5.1. Возможные виды подключения / изменения / отключения Услуги:

5.1.1. Посредством совершения действий на Портале.

5.2. Возможный порядок расчётов по Услуге:

5.2.1. Предварительная оплата;

5.2.2. Постоплата (на основании отдельно заключенного письменного бланка Заказа).

5.3. Возможные способы оплаты / порядок пополнения баланса:

5.3.1. Оплата в безналичном порядке на основании выставленного Исполнителем счёта;

5.3.2. Оплата посредством электронных средств платежа.