

ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГ
УСЛУГА «AI CLOUD - MODEL TRAINING»

1. НАИМЕНОВАНИЕ УСЛУГИ

- 1.1. Наименование Услуги: «AI Cloud - Model Training».
- 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

Услуга предоставляется на базе инфраструктуры облачной платформы «AI Cloud».

Услуга предоставляет Заказчику среду разработки Jupyter Notebook, набор инструментов для хранения данных в Объектном хранилище S3, а также набор инструментов и библиотек для запуска задач по исполнению кода обучения моделей машинного и глубокого обучения на ресурсах суперкомпьютера «Кристофари» и мониторинга процесса обучения.

Для оказания Услуги Заказчику необходимым условием является наличие на его площадке подключения к сети интернет, достаточного для эффективной загрузки данных на сервер, а также наличия собственных данных для обучения модели.

С помощью Услуги Заказчик может вести разработку моделей и производить ускоренное обучение моделей на больших объемах данных, благодаря мощностям суперкомпьютера и высокопроизводительным графическим ускорителям.

Заказчику для успешной реализации задачи обучения моделей на больших объемах данных предоставляется возможность загрузки и хранения данных в Объектное хранилище S3, а также возможность подключения к этому хранилищу как из Jupyter Notebook'а, так и из кластера, на котором будет вычисляться задача обучения модели.

На Рисунке 1 приведена общая упрощенная схема взаимодействия с сервисом AI Cloud - Model Training с удаленной площадки Заказчика (с указанием зон ответственности):

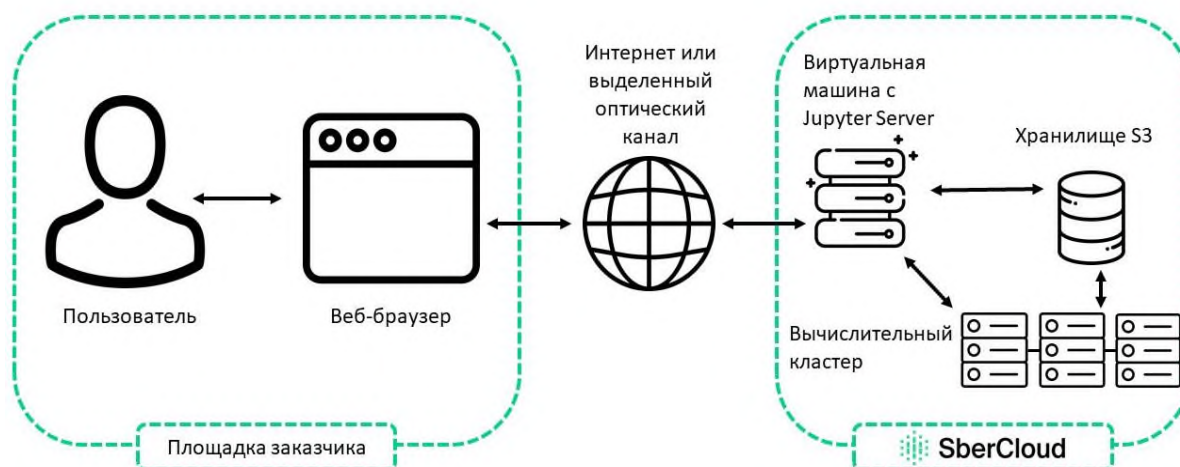


Рисунок 1 Схема взаимодействия Заказчика с Сервисом обучения моделей машинного и глубокого обучения на мощностях кластера SberCloud (AI Cloud - Model Training).

В зоне ответственности Исполнителя – функционирование серверов с развернутым Jupyter Server, а именно: функционирование вычислительного кластера, Объектного хранилища S3, сетевого подключения к ним, а также обеспечение кибербезопасности в объеме, установленном Приложением.

В рамках Услуги Заказчик может самостоятельно отслеживать состояние заданий обучения модели.

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

- Подключение через общий канал Интернет (shared) 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 (Услуга предоставляется по умолчанию).
- Подключение через прямой 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» (Услуга оплачивается отдельно).

2.2. Обеспечение защиты инфраструктуры облачной платформы «AI Cloud»

В целях обеспечения кибербезопасности инфраструктуры облачной платформы «AI Cloud» реализовываются следующие меры и механизмы защиты:

- защита инфраструктуры облачной платформы и средств ее управления;
- защита консоли управления «AI Cloud»;
- очистка пользовательских данных.

2.3. Защита инфраструктуры облачной платформы и средств ее управления

Защита инфраструктуры облачной платформы «AI Cloud» и средств ее управления обеспечивается на следующих уровнях:

- 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 на объектах информатизации ЦОД.
- на сетевом уровне обеспечивается защита периметра инфраструктуры и ее сегментирование с использованием межсетевых экранов нового поколения (NGFW), осуществляющих в том числе выявление и предотвращение компьютерных атак;
- на инфраструктурном уровне обеспечивается:
 - 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.

Помимо этого, осуществляются периодические тестирования на проникновение и аудит информационной безопасности инфраструктуры облачной платформы «AI Cloud» с привлечением сторонних организаций. Выявленные в ходе соответствующего тестирования и/или аудита недостатки устраняются по факту их выявления.

2.4. **Защита консоли управления «AI Cloud»**

Защита консоли управления «AI Cloud» обеспечивается на уровне приложений с использованием специализированного межсетевого экрана уровня приложений (Web Application Firewall). Помимо этого осуществляются регулярные сканирования консоли на наличие актуальных уязвимостей и периодические тестирования на проникновение с привлечением сторонних организаций. Выявленные уязвимости и/или недостатки устраняются по факту их выявления.

2.5. **Распределение ролей, обязанностей и ответственности Исполнителя и Заказчика в области ИБ в отношении Услуги**

Распределение ролей, обязанностей и ответственности в области ИБ в отношении Услуги описано в Таблице 1.

Табл. 1. 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 обучаемых моделей AI	Журналирование событий	Журналирование событий, связанных с деталями хода обучения моделей AI средствами самой модели.	Заказчик	Заказчик
	Управление резервированием информации	Резервирование с использованием соответствующих облачных сервисов или на ресурсах инфраструктуры Заказчика с использованием средств резервного копирования Заказчика его данных, используемых для обучения моделей, а также самих моделей, перед их загрузкой на объектное хранилище S3 из состава инфраструктуры облачной платформы AI Cloud.	Заказчик	Заказчик
Уровень «Организации» Заказчика, его Jupyter Notebook-ов и контейнеров.	Журналирование событий	Журналирование и мониторинг (с использованием консоли управления AI Cloud) основных событий, связанных с ходом обучения моделей AI на платформе AI Cloud.	Исполнитель	Заказчик
	Администрирование «Организацией» и управление доступом	Администрирование «Организацией» Заказчика с использованием Портала управления и самообслуживания Исполнителя. Заказ услуги «Model Training», создание/удаление Jupyter Notebook-ов в рамках «Организации». Предоставление сотрудникам Заказчика доступа только к Jupyter Notebook-ам его «Организации».	Исполнитель (ответственность за предоставление сервиса) Заказчик (ответственность за администрирование)	Заказчик
	Управление аутентификационной информацией	Создание/удаление с использованием Портала управления и самообслуживания Исполнителя учётных записей пользователей «Организации» (тенанта) и присвоение им привилегий доступа (в том числе по доступу к услуге «Model Training» с использованием консоли управления AI Cloud и Jupyter Notebook-ам, созданным в рамках «Организации»).	Исполнитель (ответственность за предоставление сервиса) Заказчик (ответственность за управление аутентификационной информацией)	Заказчик
	Защита данных	Обработка данных Заказчика только в рамках его Jupyter Notebook-ов и контейнеров.	Исполнитель	Исполнитель

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
		Удаление данных Заказчика, обрабатывавшихся в контейнерах в ходе обучения его моделей.		
Инфраструктурный уровень	Мониторинг и поддержка	Мониторинг инфраструктуры облачной платформы AI Cloud, 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 облачной платформы и средствах защиты информации инфраструктуры облачной платформы AI Cloud.	Исполнитель	Исполнитель
	Управление доступом	Управление доступом к сегменту управления инфраструктурой облачной платформы AI Cloud, её VLAN-ам и компонентам.	Исполнитель	Исполнитель
	Управление аутентификационной информацией	Управление учётными записями AD привилегированных пользователей (администраторов) SberCloud, имеющих доступ к сегменту управления инфраструктурой облачной платформы AI Cloud, и их вторыми факторами аутентификации (аутентификаторами).	Исполнитель	Исполнитель
	Управление уязвимостями	Контроль и анализ защищенности служебных ВМ MGMT-сегмента, кластера Kubernetes и хостовых машин инфраструктуры облачной платформы AI Cloud.	Исполнитель	Исполнитель
	Управление инцидентами ИБ	Сбор с использованием средств SIEM с компонентов облачной платформы, кластера Kubernetes и средств защиты информации инфраструктуры облачной платформы AI Cloud событий безопасности. Анализ собранных событий безопасности, а также мониторинг и реагирование на инциденты безопасности с привлечением внешнего SOC.	Исполнитель	Исполнитель
	Управление конфигурацией	Контроль и управление процессами изменения	Исполнитель	Исполнитель

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
		конфигурации инфраструктуры облачной платформы AI Cloud.		
	Управление безопасностью для виртуальных и физических сетей	Защита периметров ЦОД инфраструктуры облачной платформы AI Cloud с использованием кластеров высокопроизводительных межсетевых экранов нового поколения (NGFW), обеспечивающих межсетевое экранирование и защиту от компьютерных атак инфраструктуры. Защита сетевой инфраструктуры облачной платформы AI Cloud (входа в облако) от DDoS-атак, направленных на переполнение канальной емкости. Внутреннее сегментирование сетевых инфраструктур облачной платформы AI Cloud с использованием NGFW и выделением в рамках ЦОД на сетевом уровне DMZ, PROD- и MGMT-сегментов инфраструктуры.	Исполнитель	Исполнитель
	Управление защитой передаваемых данных	Обеспечение подключения клиентов к консоли управления AI Cloud и объектному хранилищу S3 из состава AI Cloud по защищенному протоколу HTTPS на базе протокола TLS не ниже v1.2.	Исполнитель	Исполнитель
	Установка и администрирование средств защиты	Установка, настройка и администрирование средств защиты информации в составе инфраструктуры облачной платформы AI Cloud, в том числе: 1. средств антивирусной защиты; 2. средств контроля действий привилегированных пользователей (администраторов SberCloud) класса PIM&PAM; 3.SIEM; 4. средств контроля и анализа защищенности; 5. WEB Application Firewall (WAF), используемого для защиты публикуемой консоли управления AI Cloud; 6. NGFW.	Исполнитель	Исполнитель
	Управление резервированием информации	Резервное копирование и восстановление из образов служебных виртуальных машин инфраструктуры облачной платформы AI Cloud	Исполнитель	Исполнитель

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
		с использованием СРК Veeam Backup&Replication.		
	Защита ПДн	Соответствие инфраструктуры облачной платформы AI Cloud требованиям 152-ФЗ по первому уровню защищенности (У31).	Исполнитель	Исполнитель
Физический уровень	Контроль доступа	Контроль доступа в ЦОД и помещения инфраструктуры облачной платформы AI Cloud (охраняемая территория ЦОД, пропускной режим, системы контроля и управления доступом, запирание 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, места в стойках ЦОД под оборудование (compute, network и storage), а также монтаж и коммутация оборудования инфраструктуры облачной платформы AI Cloud в стойках ЦОД.	Исполнитель	Исполнитель

2.6. Очистка пользовательских данных

Перед выделением и предоставлением доступа в «AI Cloud» к местам памяти для временного хранения и обработки данных под очередную задачу (произведения вычислений, обучения модели и т.п.) осуществляется полная очистка пользовательских данных, ранее хранимых в указанных областях памяти в ходе выполнения предыдущих задач.

Пользователям «AI Cloud» предоставляется доступ только к выделенным для них областям памяти контейнера и объектного хранилища (S3). При этом на время пользования Услугой доступ к указанным областям памяти других субъектов запрещен.

2.7. Условия хранения данных в Объектном хранилище S3

Хранение, использование и тарификация хранения и использования данных в Объектном хранилище S3 осуществляется в рамках соответствующей Услуги по Договору (Приложение № 1.7. к Договору).

Условия использования Заказчиком Объектного хранилища S3 для цели потребления Услуги:

- Заказчику для потребления Услуги AI Cloud - Model Training требуется доступ к Объектному хранилищу S3 в размере, необходимом для хранения данных обучаемой модели.
- Для того, чтобы воспользоваться услугой доступа к Объектному хранилищу S3 Заказчику необходимо в Личном кабинете активировать доступ к ней посредством проставления «галочки» в соответствующем поле «Требуется S3 хранилище».
- Объём потреблённой в течение Отчётного периода услуги Объектное хранилище S3 рассчитывается Исполнителем в соответствии с данными АСИ.
- Стоимость Услуги Объектное хранилище S3 определена в Приложении № 7 к Договору.
- Оплата Услуги Объектное хранилище S3 осуществляется Заказчиком в порядке постоплаты на основании выставленного Исполнителем счёта и при условии подписанного Сторонами Акта. Акт и счёт выставляются в порядке, установленном ст. 4 Договора.

2.8. Использование сервиса AI Cloud - Model Training

Создание, конфигурация и запуск задач на обучение осуществляется напрямую Заказчиком.

2.9. Техническое описание решения

2.9.1. Программная платформа

Услуга реализуется средствами Jupyter Server и Jupyter Notebook. Посредством него и программных библиотек пользователь имеет возможность запускать задачи на вычисление на кластере.

2.9.2. Аппаратная платформа

Вычисления и обсчет задач осуществляется на предоставляемой Заказчику в рамках Услуги области кластера (суперкомпьютера) Кристофари.

2.9.3. Технические особенности и ограничения

Скорость загрузки данных на площадку Исполнителя ограничена пропускной способностью канала доступа в Интернет из инфраструктуры Заказчика до облака SberCloud, а также скоростью чтения данных с СХД Исполнителя.

Общие значения параметров Услуги AI Cloud - Model Training

Описание	Мин. значение	Макс. значение
Количество утилизируемых в рамках вычисления задачи GPU	1 GPU	В соответствии с количеством свободных GPU, отображаемом в Личном кабинете

3. ТАРИФИКАЦИЯ УСЛУГИ

3.1. Возможные виды тарификации Услуги:

3.1.1. Динамическая тарификация (Pay as you go).

- 3.2. Стоимость Услуги формируется в зависимости от количества GPU, на которых происходило вычисление задачи, времени, в течение которого вычислялась задача, объема зарезервированного Заказчиком Объектного хранилища S3.
- 3.3. Момент начала списания денежных средств – с момента запуска обучения модели.

4. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ

- 4.1. Возможные виды подключения / изменения / отключения Услуги:
 - 4.1.1. Посредством подписания Заказа;
 - 4.1.2. Посредством совершения действий на Портале.
- 4.2. Возможный порядок расчётов по Услуге:
 - 4.2.1. Предварительная оплата;
 - 4.2.2. Постоплата (на основании отдельно заключенного письменного бланка Заказа).
- 4.3. Возможные способы оплаты / порядок пополнения баланса:
 - 4.3.1. Оплата в безналичном порядке на основании выставленного Исполнителем счёта;
 - 4.3.2. Оплата посредством электронных средств платежа.
- 4.4. В связи с характером потребления Услуги, а также объёмов, которых она может достигнуть в Отчётный период, Стороны установили, что в случае заключения с Заказчиком соглашения о применении Постоплаты (пп. 4.2.2. настоящего Приложения) Заказчик выбирает лимит в пределах Отчётного периода, по достижении которого Услуги оказываются на основании соответствующего обращения уполномоченного лица в Контактный Центр и, по требованию Исполнителя, предоставления гарантийного письма.