

## ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ «ML SPACE»

### 1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГИ

- 1.1. Услуга предоставляет доступ к платформе ML Space, которая обеспечивает полный цикл ML-разработки и совместную работу команд Data Scientist. Услуга предоставляется на базе защищенной инфраструктуры облачной платформы ML Space, меры защиты которой приведены в описании Услуги.
- 1.2. Услуга состоит из следующих компонентов - сопутствующих услуг:
- ML Space Deployments<sup>1</sup> (далее – «услуга Deployments»);
  - ML Space Environments<sup>2</sup> (включая подуслугу предоставления доступа к ML Space - Spark посредством ML Space - Environments, а также подуслугу предоставления доступа к ML Space - Intel® oneAPI посредством ML Space - Environments) (далее – «услуга Environments»);
  - ML Space Data Catalog (далее – «услуга Data Catalog»);
  - ML Space AutoML (далее – «услуга AutoML»).
- 1.3. Для оказания Услуги Заказчику необходимым условием является наличие на его площадке подключения к сети Интернет, достаточного для эффективной загрузки данных на сервер, а также наличие собственных данных.
- 1.4. Для подключения к Услуге Заказчик может выбрать один или несколько типов подключения:

Табл.1. Типы подключения к Услуге

Тип подключения	Описание
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). При подключении через общий канал Интернет Заказчику предоставляется базовая защита информационных систем, размещаемых в инфраструктуре облачной платформы SberCloud, от DDoS-атак на канальном уровне.
Подключение через прямой канал связи	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).

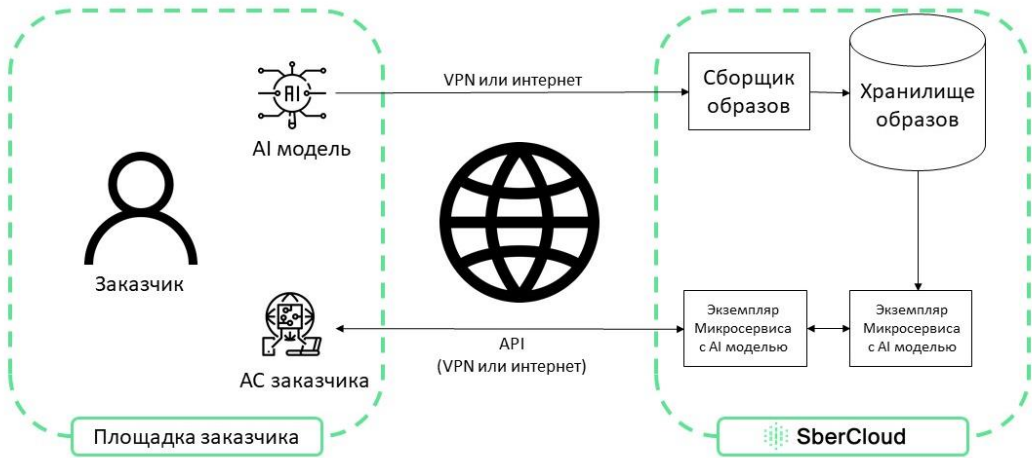
### 2. ОПИСАНИЕ УСЛУГИ DEPLOYMENTS

- 2.1. Услуга Deployments представляет собой веб-услугу для эффективной сборки Docker-образов на базе моделей Машинного и Глубокого обучения (или с другим функционалом), а также для их дальнейшего разворачивания на ресурсах SberCloud в виде микросервисов со сгенерированным API. Заказчик может разворачивать модели искусственного интеллекта на базе инфраструктуры SberCloud и услуги Deployments для дальнейшего внедрения их в функции, бизнес-процессы или микросервисы.
- 2.2. Для предоставления услуги Заказчику необходимым условием является наличие на его площадке подключения к сети Интернет, достаточного для эффективной загрузки данных, моделей или их производных (например, чекпоинтов моделей или сериализованных моделей) на сервер.
- 2.3. Заказчику для успешной реализации вывода моделей искусственного интеллекта в виде микросервисов предоставляется возможность сборки образа с любым программным обеспечением, python-библиотеками и способом взаимодействия с моделями искусственного интеллекта.
- 2.4. В рамках Услуги Заказчик может самостоятельно отслеживать и управлять состоянием развернутых моделей.

<sup>1</sup> Ранее наименование услуги ML Space Deployments – «Model Inference».

<sup>2</sup> Ранее наименование услуги ML Space Environments – «Model Training».

- 2.5. Создание, конфигурация и разворачивание моделей искусственного интеллекта осуществляется напрямую Заказчиком.
- 2.6. Хранение, использование и тарификация хранения данных осуществляется в Объектном хранилище S3 Data Catalog в рамках услуги Data Catalog.
- 2.7. На Рисунке 1 приведена общая упрощенная схема взаимодействия с услугой Deployments с удаленной площадки Заказчика (с указанием зон ответственности):



- Рисунок 1: Схема взаимодействия Заказчика с Услугами разворачивания моделей машинного и глубокого обучения на мощностях кластера ML Space Deployments.*
- 2.8. В зоне ответственности Исполнителя находится функционирование серверов с развернутыми моделями искусственного интеллекта, функционирование вычислительного кластера, Объектного хранилища S3, а также прочей инфраструктуры.

2.9. **Техническое описание решения услуги Deployments:**

Табл.2. Техническое описание решения услуги Deployments

Программная платформа	Услуга реализуется средствами веб интерфейса, внутреннего docker registry, сборщиком образов и комплексом KFServing / Knative/ISTIO/Kubernetes. С их помощью, а также программных библиотек, пользователь имеет возможность собирать и разворачивать модели искусственного интеллекта в виде микросервисов.
Аппаратная платформа	Вычисления и обсчет задач осуществляется на предоставляемой Заказчику в рамках ресурсов кластера Christofari, а также других вычислительных ресурсов и серверов SberCloud.
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.

- 2.10. Для параметров услуги Deployments устанавливаются следующие общие значения:

Табл.3. Общие значения параметров услуги Deployments

Описание	Мин. значение	Макс. значение
Количество утилизируемых в рамках вычисления задачи GPU-секунд на кластере Christofari (GPU-карт V100 и A100)	1 GPU-секунда NVIDIA Tesla V100 или A100 в конфигурации DGX-2 или DGX-A100	В соответствии с количеством свободных GPU на кластере Christofari
Количество утилизируемых в рамках вычисления задачи GPU-секунд	1 GPU-секунда	В соответствии с количеством свободных GPU
Количество утилизируемых в рамках вычисления задачи CPU-секунд	1 CPU-секунда	В соответствии с количеством свободных CPU

3. ОПИСАНИЕ УСЛУГИ ENVIRONMENTS

- 3.1. Услуга Environments предоставляет Заказчику среду разработки и рабочие окружения (включая окружения на базе docker-образов Заказчика), в том числе с Jupyter Notebook (включая услугу предоставления доступа к ML Space Spark посредством услуги Environments, а также подуслугу предоставления доступа к ML Space - Intel® oneAPI посредством ML Space – Environments (включая запуск заданий из среды GitLab), набор инструментов для хранения данных в Объектном хранилище S3 и Быстром хранилище NFS, набор инструментов для предобработки данных, а также набор

инструментов и библиотек для запуска задач по исполнению кода обучения моделей Машинного и глубокого обучения на ресурсах суперкомпьютера Christofari (а также на прочих ресурсах, доступных в SberCloud – по усмотрению Заказчика) и мониторинга процесса обучения. С помощью Услуги Заказчик может вести разработку моделей и производить ускоренную подготовку данных (в том числе при помощи преобработки данных на кластере Spark или с использованием Intel® oneAPI) и обучение моделей на больших объемах данных, благодаря мощностям суперкомпьютера и высокопроизводительным графическим ускорителям.

- 3.2. 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'a, так и из кластера, на котором будет вычисляться задача обучения модели.
- 3.3. 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.
- 3.4. В рамках Услуги Заказчик может самостоятельно отслеживать состояние заданий обучения модели.
- 3.5. Хранение, использование, тарификация хранения в Объектном хранилище S3 и Быстром хранилище NFS осуществляется в рамках услуги Data Catalog. Заказчику для потребления услуги Environments предоставляется доступ к Объектному хранилищу S3 в неограниченном размере, Быстрое хранилище NFS предоставляется со стандартной квотой в каждом из регионов, предоставляемой на workspace с возможностью увеличения через обращение в Техническую поддержку.
- 3.6. Создание, конфигурация и запуск задач на обучение, сред обучения, сред Intel® oneAPI и кластеров Spark осуществляется Заказчиком через пользовательский интерфейс услуги Environments.
- 3.7. На Рисунке 2 приведена общая упрощенная схема взаимодействия с услугами Environments с удаленной площадки Заказчика (с указанием зон ответственности):

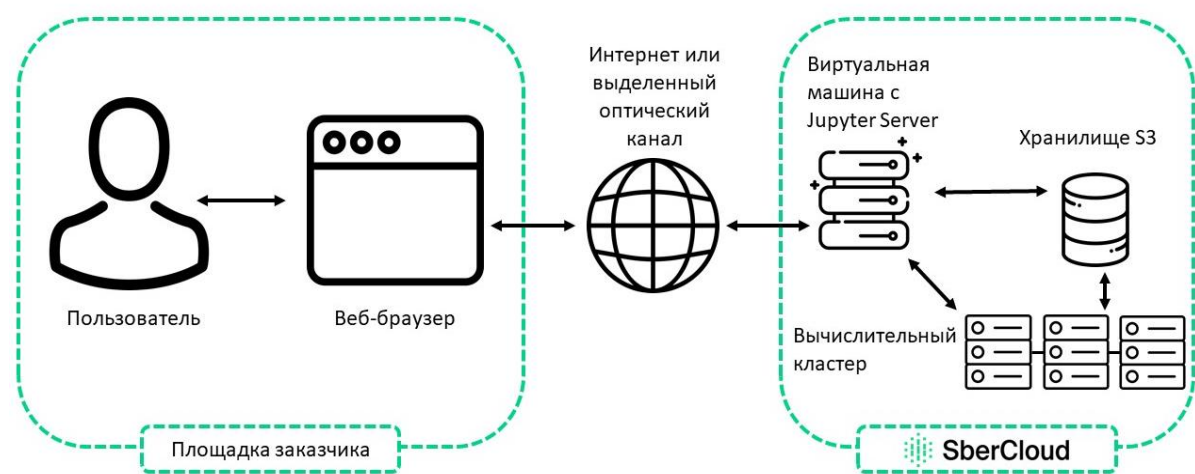


Рисунок 2: Схема взаимодействия Заказчика с услугами обучения моделей машинного и глубокого обучения ML Space Environments.

- 3.8. В зоне ответственности Исполнителя находится функционирование Серверов с развернутым Jupyter Server, кластера Spark, окружений Intel® oneAPI, функционирование вычислительного кластера, Объектного хранилища S3 и Быстрого хранилища NFS Data Catalog.
- 3.9. **Техническое описание решения услуги Environments:**

Табл.4. Техническое описание решения услуги Environments

Программная платформа	Услуга реализуется средствами Jupyter Server и Jupyter Notebook. Посредством него и программных библиотек пользователь имеет возможность запускать задачи на вычисление на кластерах.
Аппаратная платформа	Вычисления и обсчет задач осуществляется на предоставляемой Заказчику в рамках ресурсов кластера Christofari (а также на прочих ресурсах, доступных в SberCloud – по усмотрению Заказчика).
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.

3.10. Для параметров услуги Environments устанавливаются следующие общие значения:

Табл.5. Общие значения параметров услуги Environments

Описание	Мин. значение	Макс. значение
Количество утилизируемых в рамках вычисления задачи GPU (по тарифу ai-standart в рамках услуги Предоставление доступа к ML Space Environments (от 1 до 8 GPU))	1 GPU	8 GPU
Количество утилизируемых в рамках вычисления задачи GPU (по тарифу ai-pro в рамках услуги Предоставление доступа к ML Space Environments (от 9 GPU))	9 GPU	В соответствии с количеством доступных GPU на момент запуска задачи на суперкомпьютере (вычислительных кластерах Christofari)
Количество утилизируемых в рамках вычисления задачи CPU	1 CPU	В соответствии с количеством доступных CPU на момент запуска задачи

#### 4. ОПИСАНИЕ УСЛУГИ DATA CATALOG

4.1. Услуга Data Catalog предоставляет Заказчику возможность совместной работы, хранения, версионирования артефактов для машинного обучения (датасетов, моделей, докер-образов, кода и др.), а также доступ к AI marketplace.

4.2. Услуга Data Catalog включает в себя:

- Файловый менеджер на основе Объектного хранилища S3 с управлением правами доступа пользователей, тегированием файлов, версионированием и архивацией файлов;
- Быстрое хранилище NFS и трансфер между Объектным хранилищем S3 и Быстрым хранилищем NFS;
- Data transfer service - коннекторы к файловым системам (HDFS, S3 (Amazon, Google Cloud Storage) и базам данных (PostgreSQL, MySQL, MS SQL, Hive, BigQuery), а также правила и история переносов;
- Docker registry - загрузка, хранение, и иные способы совместного управления контейнерами;
- Model и dataset registry - загрузка, хранение и иные способы совместного управления моделями и датасетами;
- AI marketplace - маркетплейс артефактов машинного обучения (датасетов, моделей, контейнеров, скриптов, пайплайнов и др.) DataHub, а также маркетплейс контейнеров в формате готовых AI-сервисов AI Services.

4.3. Основным хранилищем для хранения данных и обученных моделей является Объектное хранилище S3 Data Catalog. Для использования данных Data Catalog для обучения моделей через создание Окружений (Jupyter server) и Задач в Environment необходимые данные перекадываются на Быстрое хранилище NFS.

4.4. Работа с услугами осуществляется Заказчиком через пользовательский интерфейс услуги Data Catalog и главное меню платформы.

4.5. **Техническое описание решения услуги Data Catalog:**

Табл. 6. Техническое описание решения услуги Data catalog

Программная платформа	Услуга реализуется посредством интерфейса и API файлового менеджера S3, перекадчика данных с S3 на NFS, Data transfer service, registry и AI marketplace. Посредством данных модулей реализуется возможность совместной работы, хранения, версионирования артефактов и инструментов для решения задач машинного обучения (датасетов, моделей, докер-образов, кода и др.).
Аппаратная платформа	Данные из Data Catalog хранятся в Объектом хранилище S3 и Быстром хранилище NFS, используются в услугах Environments, Deployments и AutoML. Вычисления и обсчет задач осуществляется на предоставляемой Заказчику в рамках Услуги области кластера Christofari (а также на прочих ресурсах, доступных в SberCloud – по усмотрению Заказчика).
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.

4.6. Для параметров услуги Data Catalog устанавливаются следующие общие значения:

Табл. 7. Общие значения параметров услуги Data Catalog

Описание	Мин. значение	Макс. значение
Количество утилизируемых GB S3	1 GB	В соответствии с количеством доступных GB на S3
Количество утилизируемых GB NFS	1 GB	В соответствии с количеством доступных GB на NFS

## 5. ОПИСАНИЕ УСЛУГИ AUTOML

- 5.1. Услуга AutoML предоставляет возможность проведения автоматического обучения моделей Машинного обучения посредством взаимодействия с графическим интерфейсом пользователя для задания набора исходных данных, определения задачи обучения, задания дополнительных параметров обучения и запуска задачи обучения. Обучение производится на ресурсах Исполнителя. Полученные модели Машинного обучения могут быть развернуты на ресурсах, доступных в SberCloud, либо выгружены Заказчиком для использования в собственных приложениях.
- 5.2. С помощью услуги AutoML Заказчик может вести разработку моделей без наличия специальных знаний в области Машинного обучения, получать метрики и отчеты, характеризующие полученную модель, отслеживать логи обучения, получить итоговую сериализованную модель, готовую для развертывания на ресурсах Исполнителя либо для использования в собственных приложениях.
- 5.3. Заказчику для успешной реализации задачи обучения моделей предоставляется возможность загрузки и хранения данных в Объектное хранилище S3 Data Catalog, а также возможность подключения к этому хранилищу из графического интерфейса пользователя.
- 5.4. Хранение, использование и тарификация хранения и использования данных в Объектном хранилище S3 осуществляется в рамках услуги Data Catalog.
- 5.5. Потребление и управление услугой осуществляется Заказчиком через пользовательский интерфейс услуги AutoML.
- 5.6. **Техническое описание решения услуги AutoML:**

Табл.8. Техническое описание решения услуги AutoML

Программная платформа	Услуга реализуется средствами веб интерфейса и средств платформы ML Space. Посредством них и программных библиотек пользователь имеет возможность задать параметры задачи обучения, указать расположение обучающего датасета и запустить автоматическое обучение модели.
Аппаратная платформа	Обсчет задач автоматического машинного обучения осуществляется на предоставляемой Заказчику в рамках ресурсов кластера Christofari (а также на прочих ресурсах, доступных в SberCloud – по усмотрению Заказчика).
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.

- 5.7. Для параметров услуги AutoML устанавливаются следующие общие значения:

Табл.9. Общие значения параметров услуги AutoML

Описание	Мин. значение	Макс. значение
Количество утилизируемых в рамках вычисления задачи GPU	1 GPU	16 GPU
Количество утилизируемых в рамках вычисления задачи CPU	1 CPU	Доступный на момент времени объем CPU (не более 48)

## 6. РАСПРЕДЕЛЕНИЕ РОЛЕЙ, ОБЯЗАННОСТЕЙ И ОТВЕТСТВЕННОСТИ ИСПОЛНИТЕЛЯ И ЗАКАЗЧИКА В ОБЛАСТИ ИБ В ОТНОШЕНИИ УСЛУГИ ML SPACE. ЗАЩИТА ОБЛАЧНОЙ ПЛАТФОРМЫ ML SPACE

- 6.1. Распределение ролей, обязанностей и ответственности в области ИБ в отношении Услуги описано в Таблице 10.

Табл. 10. 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.	Заказчик	Заказчик
Уровень «Организации» Заказчика, его Jupyter Notebook-ов и контейнеров.	Журналирование событий	Журналирование и мониторинг (с использованием KY ML Space ) основных событий, связанных с ходом обучения моделей AI на платформе .	Исполнитель	Заказчик
	Администрирование «Организацией» и управление доступом	Администрирование «Организацией» Заказчика с использованием Портала управления и самообслуживания Исполнителя. Заказ услуги, 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 с использованием KY ML Space и Jupyter Notebook-ам, созданными 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. Удаление данных Заказчика, обрабатывавшихся в контейнерах в ходе обучения его моделей.	Исполнитель	Исполнитель
Инфраструктурный уровень	Мониторинг и поддержка	Мониторинг инфраструктуры облачной платформы , 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

Табл. 10. 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
	Журналирование событий	Журналирование событий в компонентах облачной платформы и средствах защиты информации инфраструктуры облачной платформы .	Исполнитель	Исполнитель
	Управление доступом	Управление доступом к сегменту управления инфраструктурой облачной платформы, и компонентам.	Исполнитель	Исполнитель
	Управление аутентификационной информацией	Управление учётными записями AD привилегированных пользователей (администраторов) SberCloud, имеющих доступ к сегменту управления инфраструктурой облачной платформы , и их вторыми факторами аутентификации (аутентификаторами).	Исполнитель	Исполнитель
	Управление уязвимостями	Контроль и анализ защищенности служебных VM MGMT-сегмента, кластера Kubernetes и хостовых машин инфраструктуры облачной платформы .	Исполнитель	Исполнитель
	Управление инцидентами ИБ	Сбор с использованием средств SIEM с компонентов облачной платформы, кластера Kubernetes и средств защиты информации инфраструктуры облачной платформы 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 конфигурации инфраструктуры облачной платформы .	Исполнитель	Исполнитель
	Управление безопасностью для виртуальных и физических сетей	Защита периметров ЦОД инфраструктуры облачной платформы с использованием кластеров высокопроизводительных межсетевых экранов нового поколения (NGFW), обеспечивающих межсетевое экранирование и защиту от компьютерных атак инфраструктуры. Защита сетевой инфраструктуры облачной платформы (входа в облако) от DDoS-атак, направленных на переполнение канальной емкости. Внутреннее сегментирование сетевых инфраструктур облачной платформы 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 KY ML Space и объектному хранилищу S3 из состава ML Space 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 , 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;	Исполнитель	Исполнитель

Табл. 10. 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
		5. WEB Application Firewall (WAF), используемого для защиты публикуемой КУ ML Space; 6. NGFW.		
	Управление резервированием информации	Резервное копирование и восстановление из образов служебных виртуальных машин инфраструктуры облачной платформы с использованием СРК Veeam Backup&Replication.	Исполнитель	Исполнитель
	Защита ПДн	Соответствие инфраструктуры облачной платформы требованиям безопасности информации, предъявляемым к информационным системам персональных данных при обеспечении второго уровня защищенности персональных данных.	Исполнитель	Исполнитель
Физический уровень	Контроль доступа	Контроль доступа в ЦОД и помещения инфраструктуры облачной платформы (охраняемая территория ЦОД, пропускной режим, системы контроля и управления доступом, запирающие стойки).	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 в стойках ЦОД.	Исполнитель	Исполнитель



- 6.2. В целях обеспечения кибербезопасности инфраструктуры облачной платформы ML Space реализовываются следующие меры и механизмы защиты:

Табл.11. Обеспечение защиты инфраструктуры облачной платформы ML Space

Уровни защиты	Мероприятия
<b>Защита инфраструктуры облачной платформы и средств ее управления</b>	
Физический	Обеспечивается: <ul style="list-style-type: none"> <li>– размещение всего оборудования инфраструктуры в ЦОД, соответствующих требованиям надежности по категории Tier 3;</li> <li>– контроль и управление доступом к оборудованию;</li> <li>– наличие системы видеонаблюдения на объектах информатизации ЦОД.</li> </ul>
Сетевой	Обеспечивается защита периметров ЦОД и их сегментирование с использованием межсетевых экранов нового поколения (NGFW), осуществляющих в том числе выявление и предотвращение компьютерных атак.
Инфраструктурный	Обеспечивается: <ul style="list-style-type: none"> <li>– антивирусная защита инфраструктуры с использованием антивирусных средств для облачных сред;</li> <li>– управление доступом к инфраструктуре с использованием средств двухфакторной аутентификации подключающихся к ней администраторов;</li> <li>– контроль действий привилегированных пользователей с использованием специализированных средств;</li> <li>– 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;</li> <li>– сбор и анализ событий информационной безопасности.</li> </ul>
Дополнительный	Осуществляются периодические тестирования на проникновение и аудит информационной безопасности инфраструктуры облачной платформы ML Space с привлечением сторонних организаций. Выявленные в ходе соответствующего тестирования и/или аудита недостатки устраняются по факту их выявления.
<b>Защита KY ML Space</b>	
Приложения	Защита с использованием специализированного межсетевого экрана уровня приложений (Web Application Firewall)
Дополнительный	Осуществляются регулярные сканирования консоли на наличие актуальных уязвимостей и его периодические тестирования на проникновение с привлечением сторонних организаций. Выявленные уязвимости и/или недостатки устраняются по факту их выявления.
<b>Очистка пользовательских данных</b>	
Облачная платформа	Перед выделением и предоставлением доступа к ML Space и 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 ML Space 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.

## 7. ТАРИФИКАЦИЯ УСЛУГИ

- 7.1. **Возможные виды тарификации услуги Deployments:**
- 7.1.1. Динамическая тарификация (Pay as you go).
- 7.1.2. Стоимость Услуги формируется в зависимости от количества GPU/CPU, на которых происходило вычисление запросов к API микросервисов с моделями, а также самого времени, в течение которого вычислялись запросы к API микросервисов с моделями искусственного интеллекта и объема зарезервированного Заказчиком Объектного хранилища S3.
- 7.1.3. Момент начала списания денежных средств – с момента начала вычисления запроса к API микроуслуги (для каждого запроса) или же со старта вычислительного пода.
- 7.1.4. Момент окончания списания денежных средств – с момента окончания вычисления запроса (для каждого запроса) или же с момента завершения работы вычислительного пода.
- 7.2. **Возможные виды тарификации услуги Environments:**
- 7.2.1. Динамическая тарификация (Pay as you go).

- 7.2.2. Стоимость Услуги формируется в зависимости от количества и конфигураций GPU/CPU, на которых происходило вычисление задачи, времени, в течение которого вычислялась задача.
- 7.2.3. Момент начала списания денежных средств – с момента запуска обучения модели/с момента аллокации GPU/CPU под выбранное окружение (определяется Заказчиком через пользовательский интерфейс услуги Environments).
- 7.3. **Возможные виды тарификации услуги Data Catalog:**
  - 7.3.1. Динамическая тарификация (Pay as you go).
  - 7.3.2. Стоимость Услуги формируется в зависимости от объема используемого Заказчиком Объектного хранилища S3 и Быстрого хранилища NFS (количества GB/мес).
  - 7.3.3. Момент начала списания денежных средств – с использования более чем 1 GB (определяется Заказчиком через пользовательский интерфейс услуги Data Catalog).
- 7.4. **Возможные виды тарификации услуги AutoML:**
  - 7.4.1. Динамическая тарификация (Pay as you go).
  - 7.4.2. Стоимость Услуги формируется в зависимости от количества и конфигураций GPU или CPU на которых происходило обучение модели, времени, в течение которого обучалась модель.
  - 7.4.3. Момент начала списания денежных средств – с момента запуска обучения модели.

## **8. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ**

- 8.1. **Возможные виды подключения / изменения / отключения Услуг:**
  - 8.1.1. посредством подписания Заказа;
  - 8.1.2. посредством совершения действий на Портале и KY ML Space.
- 8.2. **Возможный порядок расчётов по Услуге:**
  - 8.2.1. предварительная оплата;
  - 8.2.2. постоплата (на основании отдельно заключенного дополнительного соглашения к Договору).
- 8.3. **Возможные способы оплаты / порядок пополнения баланса:**
  - 8.3.1. оплата в безналичном порядке на основании выставленного Исполнителем счёта;
  - 8.3.2. оплата посредством электронных средств платежа.
- 8.4. В связи с характером потребления Услуги, а также объёмами, которые она может достигнуть в Отчётный период, Стороны установили, что в случае заключения с Заказчиком соглашения о применении постоплаты (пп. 8.2.2. 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.
- 8.5. Исполнитель обязуется не включать в состав Результатов работ программное обеспечение, используемое на основании открытой лицензии, условия которой требуют от пользователя раскрытия исходного кода модифицированного ПО, либо ограничивают право пользователя запрещать третьим лицам использование модифицированного ПО.