Innostage
центр
разработок

ОПИСАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ХРАНЕНИЯ ИСХОДНОГО ТЕКСТА И ОБЪЕКТНОГО КОДА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, СРЕДСТВ ОБРАБОТКИ КОДА

ПРОГРАММНЫЙ ПРОДУКТ
«Защита ИИ. AIDR»
версия 1.0

2026 г.

Оглавление

1. Аннотация.....2
2. Технические средства хранения и компиляции исходного кода 2
3. Описание технологии хранения исходного текста и объектного кода 2
4. Описание технологии компиляции исходного кода 3

1. Аннотация

Настоящий документ разработан в рамках исполнения требований Постановления Правительства Российской Федерации от 16.11.2015 №1236 «Об утверждении Правил формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств – членов Евразийского экономического союза, за исключением Российской Федерации» и содержит описание технических средств хранения исходного текста и объектного кода программного обеспечения, а также технических средств компиляции исходного текста в объектный код программного обеспечения.

2. Технические средства хранения и компиляции исходного кода

Настоящий документ относится к программному продукту «Защита ИИ. AIDR», далее – Программный продукт, Система.

Все технические средства хранения исходного текста и объектного кода программного обеспечения, а также технические средства компиляции исходного текста в объектный код программного обеспечения содержатся на физических серверах ЦОД, расположенных на территории Российской Федерации.

При обращении к серверам трансграничной передачи данных не осуществляется.

3. Описание технологии хранения исходного текста и объектного кода

Для хранения исходного текста и объектного кода Программного продукта используется система Git.

Git – распределенная система контроля версий, которая используется для хранения исходного кода.

Репозиторий Git представляет собой каталог файловой системы, в котором находятся файлы конфигурации репозитория, файлы журналов, хранящие операции, выполняемые над репозиторием, индекс, описывающий расположение файлов, и хранилище, содержащее собственно файлы.

В репозитории Git создаются коммиты, которые позволяют сделать снимок изменений файлов. Коммит состоит из указателя коммита, Email и имя автора, описания коммита, дерева изменений, указателя на текущую версию проекта.

Ветка – это последовательность коммитов, в которой ведется параллельная разработка функционала. Основная ветка называется master.

Процесс интеграции коммитов одной ветки в другую называется слияние (объединение) веток. Слияние в пределах разных файлов осуществляется автоматически, а в пределах одного файла – стандартным трехпанельным сравнением файлов.

Конфликты слияния возникают, когда идет объединение веток с конкурирующими коммитами (была изменена одна и та же строка в файле или когда некий файл удален в одной ветке и отредактирован в другой). Во время конфликта необходимо решить, какие изменения включить в окончательное слияние и объявить конфликт как решенный.

4. Описание технологии компиляции исходного кода

В качестве технических средств компиляции кода Программного продукта используются следующие программные продукты:

- Python 3.12 – интерпретируемый язык программирования, на котором реализованы сервисы платформы. Исходный код выполняется в среде CPython с использованием виртуального окружения (venv) для изоляции зависимостей.
- Docker – платформа контейнеризации, обеспечивающая упаковку приложений со всеми зависимостями в изолированные контейнеры. Контейнеры гарантируют воспроизводимость окружения на любой машине (разработка, тестирование, production).
- Docker Compose – инструмент оркестрации многоконтейнерных приложений. Позволяет декларативно описывать сервисы (Guardrails AI, LLM-Guard, AngryScan, PostgreSQL), их сети, тома и зависимости в файле docker-compose.yml.
- FastAPI – асинхронный веб-фреймворк для Python, используемый для построения REST API сервисов валидации контента. Предоставляет автоматическую генерацию OpenAPI-документации и валидацию запросов через Pydantic.
- Transformers (Hugging Face) – библиотека для работы с предобученными ML-моделями (BERT, RuBERT). Используется для загрузки и инференса моделей детекции токсичности, jailbreak-атак и классификации тем.GitLab Runner – программное обеспечение, осуществляющее автоматизированный запуск заданий CI/CD. Компиляция и сборка проектов осуществляется средствами GitLab CI/CD согласно заранее подготовленной конфигурации.
- Docker – программное обеспечение для контейнеризации приложений, используемое для создания изолированной среды, в которой происходит сборка и тестирование Программного продукта.
- GitLab Runner – программное обеспечение, осуществляющее автоматизированный запуск заданий CI/CD. Компиляция и сборка проектов осуществляется средствами GitLab CI/CD согласно заранее подготовленной конфигурации.
- Docker – программное обеспечение для контейнеризации приложений, используемое для создания изолированной среды, в которой происходит сборка и тестирование Программного продукта.

В процессе работы задания по сборке и развёртыванию осуществляется запуск команды docker compose build, которая собирает образы всех сервисов, устанавливает Python-зависимости из requirements.txt и предзагружает ML-модели в кэш. Для offline-развёртывания собранный образ сохраняется через docker save.