ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ДИДЖИТРЕК» (ООО «ДТ»)
Адрес: 115114, Москва г., Муниципальный Округ Замоскворечье вн. тер. г., Шлюзовая набережная, д. 8, стр. 1
ИНН: 9705200012, КПП: 770501001, ОГРН: 1237700339788
Тел.: +7 985 770-45-12, Email: info@digi-track.ru

Описание функциональных характеристик ПО «DigiTrack Confidential Computing»

г. Москва – 2026

Оглавление

1. Общие сведения

1.1. Назначение документа

Документ описывает функциональные характеристики программного обеспечения (ПО) «DigiTrack Confidential Computing»

1.2. Назначение программного обеспечения

Программное обеспечение предназначено для реализации процессов защищённого совместного обучения и исполнения моделей машинного обучения в распределённой среде без передачи исходных данных между участниками.

1.3. Область применения

ПО применяется в информационных системах организаций, осуществляющих обработку данных с ограничениями на их передачу, в том числе в рамках межорганизационного взаимодействия.

2. Функциональные характеристики программного обеспечения

Состав участников

В минимальном сценарии используются две стороны:

- **Координатор** — сторона, инициирующая процессы;
- **Партнёр данных** — сторона, владеющая локальными признаками или локальными идентификаторами.

2.1. Управление участниками взаимодействия

Программное обеспечение обеспечивает:

- регистрацию участников процесса;
- назначение ролей (координатор, участник/партнёр данных);
- управление доступом к функциям системы;
- конфигурацию параметров взаимодействия между участниками.

2.2. Загрузка, хранение и обработка данных

Программное обеспечение обеспечивает:

- загрузку наборов данных в изолированную среду выполнения;
- хранение данных на стороне участника без передачи другим участникам;
- обработку наборов признаков (фичей), используемых при обучении и исполнении моделей.

2.3. Сверка данных (определение общих объектов)

Программное обеспечение обеспечивает:

- обезличивание идентификаторов объектов;
- шифрование идентификаторов;
- выполнение процедуры сопоставления записей между участниками без раскрытия исходных данных;
- формирование множества общих объектов, используемых для последующего обучения модели.

2.4. Реализация процесса совместного обучения модели

Программное обеспечение обеспечивает:

- инициацию процесса обучения по команде координатора;
- выполнение локальных вычислений на стороне участников;
- формирование промежуточных вычислительных параметров (векторов оптимизации функции потерь);
- передачу промежуточных параметров в зашифрованном или обезличенном виде;
- агрегацию полученных параметров координатором;
- обновление параметров модели по результатам агрегации;
- итерационное выполнение процесса до достижения заданных критериев;
- формирование распределённой модели, части которой хранятся у участников.

2.5. Реализация процесса исполнения модели (скоринг)

Программное обеспечение обеспечивает:

- загрузку данных для расчёта прогнозов на стороне каждого участника;
- инициацию процесса исполнения модели координатором;
- выполнение локальных вычислений участниками;
- обмен промежуточными вычислениями в защищённом виде;
- агрегацию результатов на стороне координатора;
- формирование итоговых прогнозных значений (скоринга).

2.6. Реализация функций координатора

Программное обеспечение обеспечивает выполнение функций координатора, включая:

- запуск процессов сверки данных;
- управление процессом обучения модели;
- управление процессом исполнения модели;
- координацию обмена промежуточными вычислениями;
- агрегацию результатов вычислений;
- хранение состояния процессов и результатов.

2.7. Журналирование и контроль выполнения

Программное обеспечение обеспечивает:

- ведение журналов выполнения операций;
- фиксацию статусов процессов;
- регистрацию ошибок и исключительных ситуаций;
- хранение параметров запусков процессов.

3. Характеристики обеспечения информационной безопасности

Программное обеспечение реализует следующие функции защиты информации:

3.1. Обеспечение конфиденциальности данных

- исключение передачи исходных данных между участниками;
- использование обезличенных идентификаторов;
- выполнение вычислений в изолированных средах.

3.2. Защита каналов взаимодействия

- использование защищённых каналов связи при передаче данных;
- шифрование передаваемых промежуточных вычислений.

3.3. Защита программных артефактов

- передача контейнеров и компонентов в зашифрованном виде;
- контроль целостности передаваемых файлов с использованием криптографических хеш-функций;
- раздельная передача средств доступа (паролей, ключей).

4. Технические характеристики, влияющие на функциональность

Программное обеспечение обеспечивает:

- обработку больших объёмов данных (в том числе сотни миллионов записей);
- масштабируемость вычислительных процессов;
- выполнение длительных вычислительных операций;
- возможность возобновления процессов после сбоев.

5. Архитектурные особенности

Программное обеспечение:

- реализовано с использованием распределённой архитектуры;
- поддерживает контейнеризацию компонентов;
- обеспечивает развертывание:
    - в инфраструктуре заказчика (on-premise),

    - в облачной среде,
    - в гибридной инфраструктуре;
- функционирует в операционных системах семейства Linux.

6. Результаты функционирования программного обеспечения

В результате работы программного обеспечения формируются:

- распределённая модель машинного обучения;
- прогнозные значения (скоринг), полученные без раскрытия исходных данных;
- журналы выполнения операций и процессов.

7. Ограничения функционирования

- необходимость наличия вычислительных ресурсов у участников;
- необходимость предварительной настройки защищённых каналов связи;
- зависимость корректности результатов от качества входных данных.