Приложение А – Техническое задание

**Министерство образования Иркутской области**

Государственное бюджетное профессиональное образовательное учреждение

Иркутской области

«Иркутский авиационный техникум»

(ГБПОУИО «ИАТ»)

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**РАСПРЕДЕЛЕНИЕ ДОСТУПА К БАЗЕ ДАННЫХ**

|  |  |  |
| --- | --- | --- |
| Руководитель: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) | (О.Н. Касьяненко) |
| Руководитель от предприятия:  М.П. | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) | (О.Д. Мухина) |
| Студент: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) | (И.А. Горбунов) |

Иркутск 2024

**1 Наименование проекта**

Наименование работы: распределение доступа к базе данных.

Исполнитель: студент иркутского авиационного техникума, группы БД-20-2, Горбунов И. А.

**2 Определение данных для ограничения доступа**

Доступ необходимо ограничить для следующих данных:

* + Пользователи. (ID, логин, пароль, роль).
  + Рейсы. (ID, дата финиша, дата старта, место старта, место финиша, ID водителя, номер машины).
  + Грузы. (ID, Тип груза, вес груза).
  + Роли. (ID, название).

То есть таблицы: «users», «cruises», «loads», «roles», которые имеют связь по внешним ключам между собой.

**3 Требования к целостности данных**

Требования к целостности данных таковы:

* + 1. Уникальность данных: каждая запись в базе данных должна быть уникальной, чтобы избежать дублирования информации.
    2. Согласованность данных: данные в базе данных должны быть согласованными и точными, чтобы избежать противоречий и ошибок.
    3. Ограничения целостности: использование ограничений целостности, таких как уникальные ключи, внешние ключи и проверочные ограничения, для обеспечения правильности данных.
    4. Актуальность данных: данные должны быть актуальными и обновленными, чтобы предоставлять точную информацию пользователям.
    5. Безопасность данных: обеспечение защиты данных от несанкционированного доступа, изменений и удалений.
    6. Резервное копирование данных: регулярное создание резервных копий данных для предотвращения потери информации в случае сбоев или аварий.

**4 Распределение ролей**

Наборы правил доступа для пользователей могут быть следующие:

user1 – SELECT

user2 – SELECT, INSERT, UPDATE

user3 – SELECT, UPDATE, DELETE

user4 – INSERT, UPDATE

user5 - DELETE