**Министерство образования Иркутской области**

Государственное бюджетное профессиональное образовательное учреждение Иркутской области

«Иркутский авиационный техникум»

(ГБПОУИО «ИАТ»)

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ НА РАСПРЕДЕЛЕНИЕ ДОСТУПА К БАЗЕ ДАННЫХ**

|  |  |  |
| --- | --- | --- |
| Руководитель: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) | (С.Н. Касьяненко) |
| Студент: | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, дата) | (К.А. Беднарж) |

Иркутск 2023

Общие требования:

Реализация должна соответствовать требованиям ГОСТ Р 51907-2002 "Информационные технологии. Методическое обеспечение. Требования к защите информации в автоматизированных системах".

Должны быть реализованы механизмы аутентификации пользователей.

Доступ к базе данных и таблицам должен быть ограничен и базироваться на ролях пользователей.

Распределение доступа к базе данных:

* Не менее 5 пользователей должны иметь доступ к базе данных.
* Каждый пользователь должен иметь уникальное имя пользователя и пароль для входа в систему.
* Разработать набор ролей пользователей, определяющих их доступ к различным функциональным возможностям базы данных.
* Распределение доступа к таблице:
* Определить таблицу, к которой будет осуществляться доступ.
* Назначить права доступа на чтение и запись к таблице различным пользователям в соответствии с их ролями.
* Реализовать механизм отслеживания и регистрации изменений данных в таблице для каждого пользователя.

Мониторинг и аудит:

* Разработать механизм мониторинга и аудита действий пользователей в базе данных.
* Вести журналы аудита для анализа действий пользователей и выявления возможных нарушений безопасности.
* Использование шифрования:
* Применить методы шифрования для защиты конфиденциальных данных, передаваемых и хранимых в базе данных.
* Обеспечить безопасное хранение паролей пользователей и других конфиденциальных данных.
* Документация и обучение:
* Предоставить документацию по использованию системы доступа к базе данных.
* Провести обучение пользователей по работе с системой и правилам безопасности.

Оценка безопасности:

Провести оценку безопасности разработанной системы доступа к базе данных с использованием современных методов тестирования на проникновение.

Этапы реализации проекта:

* Анализ требований и составление технического задания.
* Разработка архитектуры системы доступа к базе данных.
* Настройка пользователей, ролей и прав доступа.
* Тестирование функциональности и безопасности системы.
* Внедрение системы и обучение пользователей.
* Проведение аудита системы и корректировка возможных недочетов.
* Сопровождение и поддержка системы после внедрения.

**ПРИЛОЖЕНИЕ А – ПРИМЕРЫ КОММАНД**

\*Создание ролей

* CREATE ROLE admin;
* CREATE ROLE manager;
* CREATE ROLE analyst;
* CREATE ROLE operator;
* CREATE ROLE guest;

\*Назначение прав доступа

* GRANT ALL PRIVILEGES ON example\_database.\* TO admin;
* GRANT SELECT, INSERT, UPDATE, DELETE ON example\_database.
* users TO manager;
* GRANT SELECT ON example\_database.products TO manager,
* analyst, guest;
* GRANT SELECT, INSERT, UPDATE, DELETE ON example\_database.
* orders TO manager, operator;
* GRANT SELECT ON example\_database.invoices TO analyst,
* operator;

\*Создание пользователей и паролей

* CREATE USER ‘admin\_user'@'%' IDENTIFIED BY
* "admin\_password' ;
* CREATE USER 'manager\_user'@'%' IDENTIFIED BY
* "manager\_password' ;

\* Назначение ролей пользователей

* GRANT admin TO ‘admin\_user'@'%';
* GRANT manager TO 'manager\_user'@'%';