Тема 32. Рассмотрение вопросов, связанных с аудитом базы данных, аудиторским журналом. Установка опций, включение и отключение аудита. Очистка и уменьшение размеров журнала.

Аудит базы данных - это процесс проверки и анализа базы данных с целью выявления возможных проблем, угроз безопасности или несоответствий требованиям. Аудит может включать проверку структуры базы данных, проверку целостности данных, проверку прав доступа пользователей, проверку на наличие уязвимостей и многое другое.

Аудиторский журнал - это журнал, в котором регистрируются все действия, выполняемые с базой данных. Он позволяет отслеживать изменения в данных, выявлять ошибки и предотвращать несанкционированный доступ к данным.

**Установка опций** аудита может быть выполнена с помощью команды SET GLOBAL audit\_options = <опции>; в SQL. Например, для включения аудита INSERT, UPDATE и DELETE для таблицы users, можно выполнить следующую команду:

SET GLOBAL audit\_options = ‘all\_priv,delete,insert,update’;

Это активирует аудит всех привилегированных команд, а также команд удаления, вставки и обновления для всех таблиц в базе данных. Чтобы активировать аудит только для определенной таблицы, необходимо указать имя таблицы в команде. Например:

mysql> SET GLOBAL audit\_options = ‘table\_name,insert’;

**Включение и отключение аудита** может быть выполнено с помощью команды FLUSH LOGS или SET GLOBAL log\_bin = {0|1}.

Если log\_bin установлен в 0, то все изменения, внесенные в таблицы, не будут записываться в журнал. Если же log\_bin установлен в 1, то все изменения будут записываться в журнал и сохраняться на диске.

Чтобы включить журнал аудита, нужно выполнить следующую команду:

mysql> SET GLOBAL log\_bin=1;

Это включит запись всех изменений, внесенных в таблицы, в журнал аудита.

Чтобы отключить журнал аудита, нужно выполнить следующую команду:

mysql> SET GLOBAL log\_bin=0;

**Очистка и уменьшение размеров аудиторского журнала** могут быть выполнены с помощью команды PURGE BINARY LOGS. Эта команда удаляет старые записи из журнала аудита, оставляя только самые последние записи.

Например, следующая команда удалит все записи, кроме последних 100:

PURGE BINARY LOGS BEFORE NOW() LIMIT 100;