Введение. Основные характеристики средств, методов и механизмов обеспечения безопасности баз данных

План:

1. Основные характеристики методов безопасности баз данных
2. Организация и поддержание логической структуры данных
3. Интерфейс ввода данных СУБД

Исследования по проблемам защиты компьютерной информации, проведенные в конце 70-хначале 80-х годов, развитые впоследствии в различных приложениях и закрепленные в соответствующих стандартах, определяют в качестве составных элементов понятия ***безопасности информации*** - три компонента:

- ***конфиденциальность*** (защита от несанкционированного доступа);
- ***целостность*** (защита от несанкционированного изменения информации);
- ***доступность*** (защита от несанкционированного удержания информации и ресурсов, от разрушения, работоспособности).

Составляющим безопасности информации противостоят соответствующие ***угрозы***. Под ***угрозой безопасности информации*** **понимается** ***осуществляемое или потенциально осуществимое воздействие на компьютерную систему, которое прямо или косвенно может нанести ущерб безопасности информации*****.** Угрозы реализуют или пытаются реализовать ***нарушители*** информационной безопасности.

Формализованное описание или представление ***комплекса возможностей нарушителя по реализации тех или иных угроз безопасности информации*** **называют** ***моделью нарушителя (злоумышленника).***

Относящиеся к обеспечению безопасности баз данных (БД) приведены ниже:

– *доступ к информации (access to information)* - ознакомление с информацией, ее обработка (в частности, копирование), модификация, уничтожение;

– *субъект доступа (access subject)* - лицо или процесс, действия которого регламентируются правилами разграничения доступа;

– *объект доступа (access object)* - единица информации автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа;

– *правила разграничения доступа (security policy)* - совокупность правил, регламентирующих права субъектов доступа к объектам доступа;

– *санкционированный доступ (authorized access to information)* - доступ к информации, который не нарушает правил разграничения доступа;

– *несанкционированный доступ (unauthorized access to information)* - доступ к информации, который нарушает правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

– *уровень полномочий субъекта доступа (subject privilege)* - совокупность прав доступа субъекта доступа (для краткости в дальнейшем мы будем использовать термин «привилегия»);
– *нарушитель правил разграничения доступа (security policy violator)* - субъект доступа, который осуществляет несанкционированный доступ к информации;
– ***модель нарушителя правил разграничения доступа (security policy violator model)*** - абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа;
– ***целостность информации (information integrity)*** — способность средства вычислительной техники (в рассматриваемом случае - информационной системы в целом) обеспечить неизменность информации в условиях случайного и (или) преднамеренного искажения (разрушения);
– ***метка конфиденциальности (sensitivity label)*** - элемент информации, характеризующий конфиденциальность объекта;
– ***многоуровневая защита (multilevel secure)*** - защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней конфиденциальности.

Основная особенность СУБД как вида программного обеспечения. Будучи по природе ***прикладным программным обеспечением,*** т.е. предназначенным для решения конкретных прикладных задач, СУБД изначально выполняли и ***системные функции*** — расширяли возможности файловых систем ***системного программного обеспечения.*** В общем плане можно выделить следующие ***функции***, реализуемые *СУБД:*

- ***организация и поддержание логической структуры данных (схемы базы данных);***
- ***организация и поддержание физической структуры данных во внешней памяти;***
- ***организация доступа к данным и их обработка в оперативной и внешней памяти.***

Организация и поддержание логической структуры данных (схемы базы данных) обеспечивается средствами ***модели организации данных***. В обиходе просто «модель данных».

Модель данных определяется способом организации данных, ограничениями целостности и множеством операций, допустимых над объектами организации данных. Соответственно, модель данных разделяют на три составляющие — ***структурную, целостную*** **и** ***манипуляционную.***

Три основные модели организации данных:

- ***иерархическая;***
- ***сетевая;***
- ***реляционная.***

Модель организации данных, по сути, определяет ***внутренний информационный язык*** автоматизированного банка данных, реализующего автоматизированную информационную систему.

Модели данных, поддерживаемые СУБД, довольно часто используются в качестве критерия для классификации СУБД. Исходя из этого, различают ***иерархические СУБД\ сетевые СУБД*** и ***реляционные СУБД.***

Другой важной функцией СУБД является ***организация и поддержание физической структуры данных во внешней памяти***. Эта функция включает организацию и поддержание внутренней структуры файлов базы данных, иногда называемой ***форматом файлов базы данных,*** а также создание и поддержание специальных структур (индексы, страницы) для эффективного и упорядоченного доступа к данным. В этом плане эта функция тесно связана с третьей функцией СУБД - организацией доступа к данным.

Организация доступа к данным и их обработка в оперативной и внешней памяти осуществляется через реализацию процессов, получивших название - транзакций. ***Транзакцией называют последовательную совокупность операций, имеющую отдельное смысловое значение по отношению к текущему состоянию базы данных.***

Транзакция по удалению отдельной записи в базе данных последовательно включает определение страницы файла данных, содержащей указанную запись;

считывание и пересылку, соответствующей страницы, в буфер оперативной памяти; собственно, удаление записи в буфере ОЗУ;

проверку ограничений целостности по связям и другим параметрам после удаления и, наконец, «выталкивание» и фиксацию в файле базы данных нового состояния, соответствующей страницы данных.