Кафедра КИБЭВС

ТУСУР
Томский государственный университет систем управления и радиоэлектроники

Лекция №2

каф. КИБЭВС
И.В. Горбунов

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

Аутентификация – Проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности

Авторизация - Процесс подтверждения (проверки) прав пользователей на выполнение некоторых действий.

Злоумышленники

1. Внешние злоумышленники
2. Внутренние злоумышленники

Злоумышленники

1. Внешние злоумышленники
2. Внутренние злоумышленники
    1. Операторы
    2. Аналитики
    3. Администраторы

Операторы

Сотрудники, заполняющие БД, вводя сведения в ручную, либо выполняют задачи связанные с обработкой информации.

Работают через приложения, для которых решены проблемы связанные с разграничением доступа.

Аналитики

Сотрудники выполняющие работы связанные с получением всевозможных отчетов.

Возможности по созданию различных от четов с применением языковых средств в том числе различных запросов **(select)**

Администраторы

Сотрудники решающие вопросы жизнеобеспечения системы, ее отказо- и катастрофоустойчивости.

Проблемы обеспечения ИБ в БД

1. Управление доступом
2. Управление целостностью данных
3. Управление параллелизмом
4. Восстановление данных
5. Транзакции и восстановление
6. Откат и раскрутка транзакций
7. SQL-инъекции

Управление доступом

Управление правами доступа пользователей и приложений.

Управление целостностью данных

Нарушение целостности данных может быть вызвано рядом причин:

- сбои оборудования, физические воздействия или стихийные бедствия;
- ошибки санкционированных пользователей или умышленные действия несанкционированных пользователей;
- программные ошибки СУБД или ОС;
- ошибки в прикладных программах;
- совместное выполнение конфликтных запросов пользователей и др.

Управление параллелизмом

В системах, ориентированных на многопользовательский режим работы, возникает целый ряд новых проблем, связанных с параллельным выполнением конфликтующих запросов пользователей.

Транзакция - объединение совокупности операций, в результате которых БД из одного целостного состояния переходит в другое целостное состояние, в один логический элемент работы

Восстановление данных

Можно выделить три основных уровня восстановления:

- Оперативное восстановление, которое характеризуется возможностью восстановления на уровне отдельных транзакций при ненормальном окончании ситуации манипулирования данными (например, при ошибке в программе).
- Промежуточное восстановление .Если возникают аномалии в работе системы (системно-программные ошибки, сбои программного обеспечения, не связанные с разрушением БД), то требуется восстановить состояние всех выполняемых на момент возникновения сбоя транзакций.
- Длительное восстановление. При разрушении БД в результате дефекта на диске восстановление осуществляется с помощью копии БД. Затем воспроизводят результаты выполненных с момента снятия копии транзакций и возвращают систему в состояние на момент разрушения.

Транзакции и восстановление

Прекращение выполнения транзакции вследствие появления сбоя нарушает целостность БД . Если результаты такого выполнения транзакции потеряны, то имеется возможность их воспроизведения на момент возникновения сбоя . Таким образом, понятие транзакции играет важную роль при восстановлении. Для восстановления целостности БД транзакции должны удовлетворять следующим требованиям:

- необходимо, чтобы транзакция или выполнялась полностью, или не выполнялась совсем;
- необходимо, чтобы транзакция допускала возможность возврата в первоначальное состояние, причем, для обеспечения независимого возврата транзакции в начальное состояние монопольную блокировку необходимо осуществлять до момента завершения изменения всех объектов;
- необходимо иметь возможность воспроизведения процесса выполнения транзакции, причем, для обеспечения этого требования, совместную блокировку необходимо осуществлять до момента завершения просмотра данных всеми транзакциями.

Откат и раскрутка транзакций

Основным средством, используемым при восстановлении, является системный журнал, в котором регистрируются все изменения, вносимые в БД каждой транзакцией . Возврат транзакции в начальное состояние состоит в аннулировании всех изменений, которые осуществлены в процессе выполнения транзакции . Такую операцию называют откатом . Для воспроизведения результатов выполнения транзакции можно, используя системный журнал, восстановить значения проведенных изменений в порядке их возникновения, либо выполнить транзакцию повторно . Воспроизведение результатов выполнения транзакции с использованием системного журнала называется раскруткой . Раскрутка является достаточно сложной, но необходимой операцией механизмов восстановления современных БД .

SQL-инъекции

SQL-инъекции — встраивание вредоносного кода в запросы к базе данных — наиболее опасный вид атак. С использованием SQL-инъекций злоумышленник может не только получить закрытую информацию из базы данных, но и, при определенных условиях, внести туда изменения.

Кафедра КИБЭВС

ТУСУР
Томский государственный университет систем управления и радиоэлектроники

Спасибо за внимание!!!