1. **Определение СУБД**

Система управления базами данных (СУБД) – это набор программ, которые управляют структурой БД и контролируют доступ к данным, хранящимся в БД. СУБД служит посредником между пользователем и БД. Сама структура БД хранится в виде набора файлов, и единственный способ получить доступ к данным в этих файлах – через СУБД.

1. **Функции администратора СУБД**

Функции администратора:

• инсталляция СУБД - является функцией только системного администратора;

• управление памятью - Администратор должен обеспечить такое выделение памяти, чтобы с одной стороны, ее было достаточно для хранения и эффективного доступа к данным, а с другой - минимальное количество выделенной памяти оставалось неиспользованным;

• управление разделением данных между пользователями - Администратор, имея исчерпывающее представление о дисциплинах разделения, применяемых СУБД, выступает в роли консультанта прикладных программистов, сводя к минимуму взаимное блокирование приложениями друг друга;

• копирование и восстановление БД - Копирование и восстановление являются необходимыми для гарантирования сохранности данных даже при полном крахе системы;

• управление безопасностью в системе - Оно состоит в регистрации пользователей в системе, выделении пользователям привилегий и бюджетов;

• передача данных между СУБД и другими системами - .Данные, хранящиеся в БД, могут потребоваться для использования в других БД, работающих в другой инсталляции, или в приложениях, не зависящих от СУБД;

• управление производительностью - включает в себя три аспекта: настройку параметров функционирования самой СУБД, отдельных БД и отдельных приложений.

1. **Мандатное управление доступом. Средства мандатной защиты в СУБД**

Мандатное управление доступом (mandatory access control) — это разграничение доступа субъектов к объектам данных, основанное на характеризуемой меткой конфиденциальности информации, которая содержится в объектах, и на официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

При этом подходе с каждым зарегистрированным в системе пользователем ( субъектом ) и каждым защищаемым объектом системы связывается мандат, определяющий действия, которые может выполнять данный субъект над данным объектом

1. **Основные уровни восстановления БД**

1. Оперативное восстановление. Характеризуется возможностью восстановления на уровне отдельного логического элемента работы при аномальном окончании управления данны­ми (ошибка в программе, ошибка в аргументе и т.д.).

2. Промежуточное восстановление .Если возникают аномалии в системе (системно-программные ошибки, сбой аппаратного обеспечения не связанный с разрушением базы данных), то требуется восстановить состояние всех выполняемых логических эле­ментов работы на момент возникновения сбоя.

3. Длительное восстановление. При разрушении базы данных в результате дефекта на диске осущест­вляют восстановление с помощью копии базы данных. Затем воспроизводят результаты выполненных с момента снятия копии логических элементов ра­боты и возвращают систему в состояние на момент разрушения.

1. **Концепция и реализация механизма ролей БД**

Когда в организации работает множество пользователей, они, как правило, разбиваются на группы. Например, несколько бухгалтеров с одинаковыми правами. Чтобы не терять время на создание одинаковых прав для нескольких пользователей, для примера, в InterBase имеется механизм ролей. При пользовании этим механизмом, существует четыре последовательности действий:

1. Создать роль.

2. Присвоить этой роли необходимые права.

3. Назначить нужным пользователям эту роль.

4. При соединении с БД указать не только имя пользователя и пароль, но и его роль.

1. **Преимущества создания резервных копий БД встроенными средствами СУБД**

Использование встроенных механизмов InterBase имеет следующие преимущества:

* InterBase позволяет осуществлять резервное копирование БД параллельно с работой других пользователей.
* Во время резервного копирования InterBase считывает каждую запись из таблиц, параллельно занимаясь «сборкой мусора», поэтому в резервной копии не останется устаревших версий записей.
* Оставшиеся данные переупаковываются, то есть, резервная копия не будет содержать тех «дырок», что были в базе данных. Можно сказать, что данные дефрагментируются.
* Индексы пересчитываются, что приводит к оптимизации работы базы данных.
* Созданная резервная копия может быть использована для миграции базы на другие серверы (InterBase новых версий, Firebird или Yaffil), а также при восстановлении позволяет исправить некоторые параметры БД, например, размер страниц.

1. **Назначение утилиты gsec в InterBase**

GSEC – это утилита командной строки, обеспечивающая интерфейс к базе данных безопасности. Вы должны иметь права SYSDBA или суперпользователя (root для Unix), чтобы использовать GSEC. Данную утилиту можно использовать в интерактивном режиме или режиме командной строки.

di[splay] Показывает информацию обо всех пользователях из базы ISC4.GDB

di[splay] name Показывает информацию о пользователе name

a[dd] name -pw passwd [option argument option argument ...] Добавляет пользователя с именем name, паролем passwd и дополнительной информацией

mo[dify] name [options] Изменяет атрибуты пользователя

de[lete] name Удаляет информацию о пользователе с именем name из ISC4.GDB

h[elp] Показывает синтаксис команд GSEC

q[uit] Завершает сеанс

1. **Основные рекомендации по ремонту БД**

* Прежде всего, отключите от базы всех пользователей, не позволяйте им вносить изменения в БД
* Сделайте копию рабочей базы данных средствами файловой. Все попытки восстановления делайте с полученной копией, не трогая оригинал.
* Проведите полную проверку (gfix –v –full ). Если выводятся сообщения об ошибках контрольных сумм, можно добавить переключатель –i, чтобы игнорировать эти ошибки.
* Далее можно попытаться исправить разрушенные данные, помечая их как недоступные: gfix –mend –full –ignore
* После этого вновь выполните проверку на наличие разрушенных структур , как в № 3, но без –i.
* Затем попробуйте снова выполнить резервное копирование утилитой gbak, например: gbak –b –v –i
* Если это удалось, то все хорошо. Иначе попробуйте сделать еще одно резервное копирование, добавив параметр –g (не собирать мусор). Если разрушения связаны с повисшими limboтранзакциями, то –limbo.
* В большинстве случаев, такие меры позволяют сделать нормальную резервную копию. Попробуйте восстановить ее командой gbak –create –v