Контроль доступа к файлам и защита данных

Контроль доступа к файлам

Матрица контроля доступа

Опр. Матрица контроля доступа (access control matrix) – двумерный список всех пользователей и прав их доступа к файлам в системе.

Матрица контроля доступа

User \ File	1	2	3	4	5	6	7	8	9	10
1	1	1	0	0	0	0	0	0	0	0
2	0	0	1	0	1	0	0	0	0	0
3	0	1	0	1	0	1	0	0	0	0
4	1	0	0	0	0	0	0	0	0	0
5	1	1	1	1	1	1	1	1	1	1
6	0	0	0	0	0	1	1	0	0	0
7	1	0	0	0	0	0	0	0	0	1
8	1	0	0	0	0	0	0	0	0	0
9	1	1	1	1	0	0	0	0	1	1
10	1	1	0	0	1	1	0	0	0	1

Матрица контроля доступа

- Обычно очень разрежена и имеет большой размер
- Для обозначения различных видов доступа (только для чтения, для записи и т.д.) нужно использовать специальные коды

Классы пользователей

Опр. Классы пользователей (user classes) – способ классификации, указывающий группы, или отдельных пользователей, обладающих определенными правами доступа к файлам. Данные контроля доступа могут храниться в виде части блока управления файлом, занимая незначительное дисковое пространство.

Классы пользователей

- Владелец (owner) – пользователь, создавший файл
  - Обладает неограниченным доступом к файлу
  - Может изменять права других пользователей на доступ к этому файлу
- Указанный пользователь (specified user) – пользователь, которому владелец предоставил права на доступ к файлу

Классы пользователей

- Группа (group) или проект (project) – группа пользователей, работающая над конкретным проектом
  - Члены группы могут обладать доступом к связанным с проектом файлам других членов группы
- Общедоступный (public) – файл, к которому могут обращаться все пользователи
  - Можно читать или запускать, но не изменять

Вопрос для самопроверки

- Матрицы контроля доступа пригодны для большинства систем? (Да/Нет)

Вопрос для самопроверки

- Матрицы контроля доступа пригодны для большинства систем? (Да/Нет)
- Нет. Они обычно велики по размеру и сильно разрежены, поэтому их хранение приводит к бессмысленным затратам пространства на накопителях и большому времени обращения при реализации контроля доступа.

Вопрос для самопроверки

- Должна ли система обратиться к блоку управления файлом, если там хранятся данные контроля доступа, но чтение файла запрещено? (Да/Нет)

Вопрос для самопроверки

- Должна ли система обратиться к блоку управления файлом, если там хранятся данные контроля доступа, но чтение файла запрещено? (Да/Нет)
- Да. Если данные контроля доступа к файлу хранятся в блоке управления файлом, узнать о правах доступа к файлу можно только прочитав блок управления файлом.

Контроль доступа к файлам и защита данных

Резервное копирование и восстановление

Физическое резервное копирование

Опр. Физическое резервное копирование (physical backup) – копирование каждого бита на накопителе. Попытки интерпретировать содержимое накопителя при физическом резервном копировании не предпринимаются.

Логическое резервное копирование

Опр. Логическое резервное копирование (logical backup) – методика резервного копирования, при которой копируются данные файлов и информация о директориях файловой системы, часто в стандартном сжатом формате.

Инкрементное резервное копирование

Опр. Инкрементное резервное копирование (incremental backup) – методика логического резервного копирования, при которой копируются только данные, изменившиеся со времени предыдущего резервного копирования.

Вопрос для самопроверки

- Может ли физическая копия содержать часть файловой системы? (Да/Нет)

Вопрос для самопроверки

- Может ли физическая копия содержать часть файловой системы? (Да/Нет)
- Нет. Физическая резервная копия не учитывает логическую структуру файловой системы, поэтому она не может разделить содержащиеся в ней файлы.

Вопрос для самопроверки

- Поддерживает ли физическое резервное копирование инкрементное копирование данных? (Да/Нет)

Вопрос для самопроверки

- Поддерживает ли физическое резервное копирование инкрементное копирование данных? (Да/Нет)
- Нет. Инкрементное резервное копирование это методика логического резервного копирования.

Контроль доступа к файлам и защита данных

Журнальные файловые системы

Атомарная транзакция

Опр. Атомарная транзакция (atomic transaction) – группа операций, которая не влияет на состояние системы до тех пор, пока не завершаются все операции группы.

Пр. Перевод денег с одного банковского счета на другой.

Откат транзакции

Опр. Откат транзакции (rolling back a transaction) – возврат системы в состояние, в котором она пребывала до начала выполнения транзакции.

Журнальная файловая система

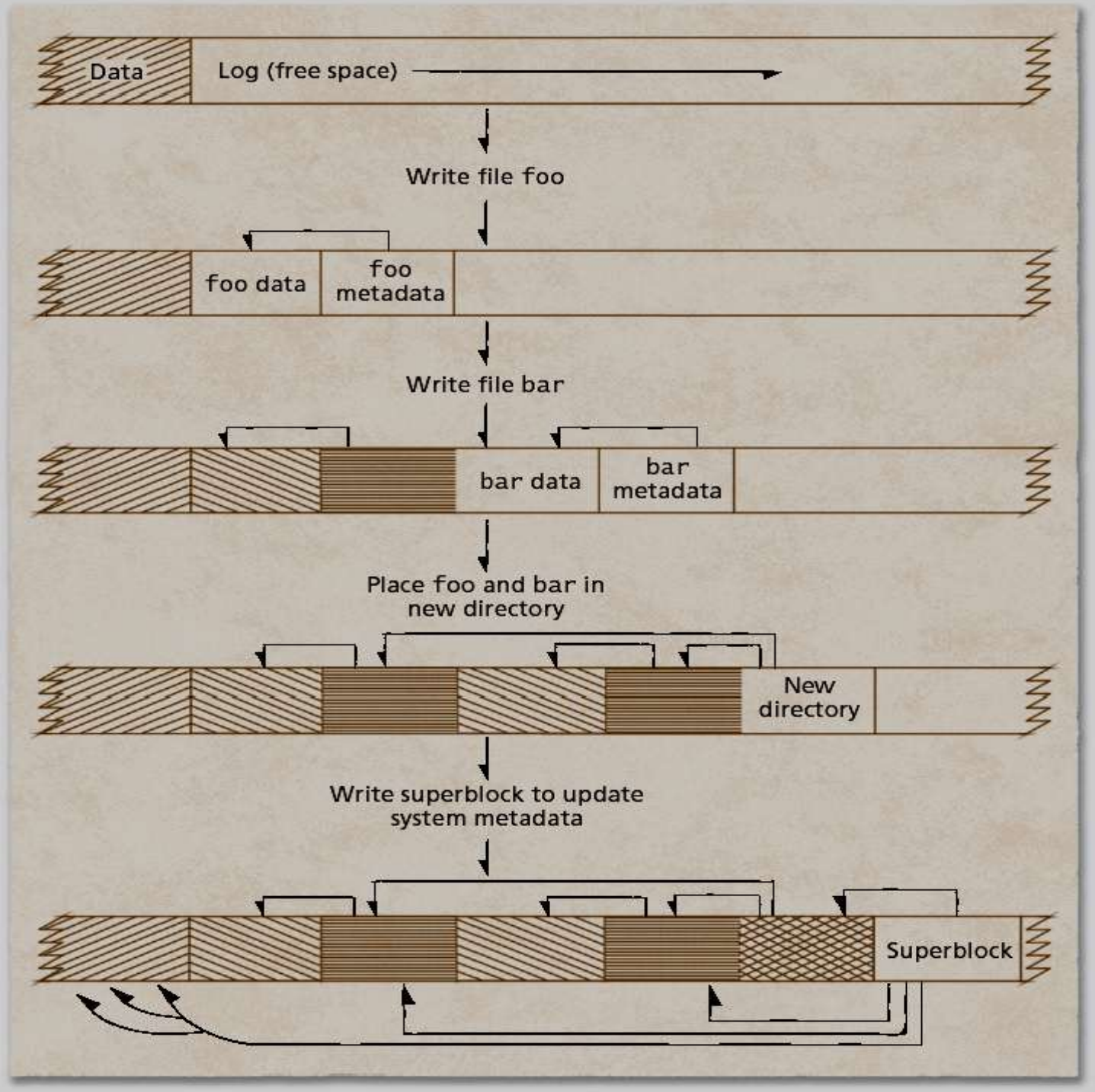
Опр. Журнальная файловая система (Log-structured File System, LFS) – файловая система, выполняющая все операции с файлами в виде транзакций, чтобы гарантировать целостность файловой системы и метаданных.

Пр. NTFS Journal File System

Файловые системы Linux и Unix

Журнальная файловая система

- Данные записываются в конец журнала (log), файл которого занимает все свободное пространство накопителя
- По журналу обычно распределяются метаданные файлов, что позволяет быстро находить запрашиваемые данные
- Файловая операция завершается только после записи метаданных файла
- Операция с директорией завершается только после записи суперблока



Запись двух файлов в новую директорию в журнальной файловой системе

Вопрос для самопроверки

- LFS записывает сначала метаданные файла, а затем его данные? (Да/Нет)

Вопрос для самопроверки

- LFS записывает сначала метаданные файла, а затем его данные? (Да/Нет)
- Нет. Если система запишет сначала метаданные файла, а затем данные, и в системе возникнет отказ, то метаданные будут указывать на некорректные блоки (т.е. в блоках будут отсутствовать данные файла).

Вопрос для самопроверки

- Повышает ли кэширование производительность LFS? (Да/Нет)

Вопрос для самопроверки

- Повышает ли кэширование производительность LFS? (Да/Нет)
- Да. Поскольку измененные директории и метаданные всегда записываются в конец журнала, LFS может потребоваться просмотреть весь журнал, чтобы найти конкретный файл. Дабы уменьшить серьезность этой проблемы, LFS кэширует информацию о размещении файлов в файловой системе.

Вопрос для самопроверки

- Свойственны ли LFS проблемы фрагментации? (Да/Нет)

Вопрос для самопроверки

- Свойственны ли LFS проблемы фрагментации? (Да/Нет)
- Да. Когда в журнале больше не остается свободного места, LFS освобождает блоки для размещения новых данных, если другие блоки содержат измененные копии данных из этих блоков. При этом новые могут оказаться фрагментированными. Чтобы решить эту проблему, LFS может создавать непрерывные участки в журнале, группируя данные, что требует накладных расходов.

Контроль доступа к файлам и защита данных

Системы баз данных

База данных

Опр. База данных (database) – централизованно управляемое хранилище данных, представленных в стандартизованном формате (например, иерархические, реляционные, объектно-ориентированные базы данных).

Базы данных

- Данные можно просматривать в соответствии с определенными логическими взаимосвязями между ними
- Данные организуются по их содержанию, а не размещению, за счет чего можно уменьшить или исключить избыточность данных

Система базы данных

Опр. Система базы данных (database system) – определенный набор данных, аппаратных устройств, на которых эти данные хранятся, и программ, управляющих доступом к данным (эти программы называются системой управления базы данных, СУБД).

Реляционная модель

Опр. Реляционная модель (relational model) – предложенная Коддом модель данных, лежащая в основе большинства современных систем баз данных. Реляционная база данных – это набор связанных отношений.

Отношение

Опр. Отношение (relation) – набор строк в реляционной базе данных.

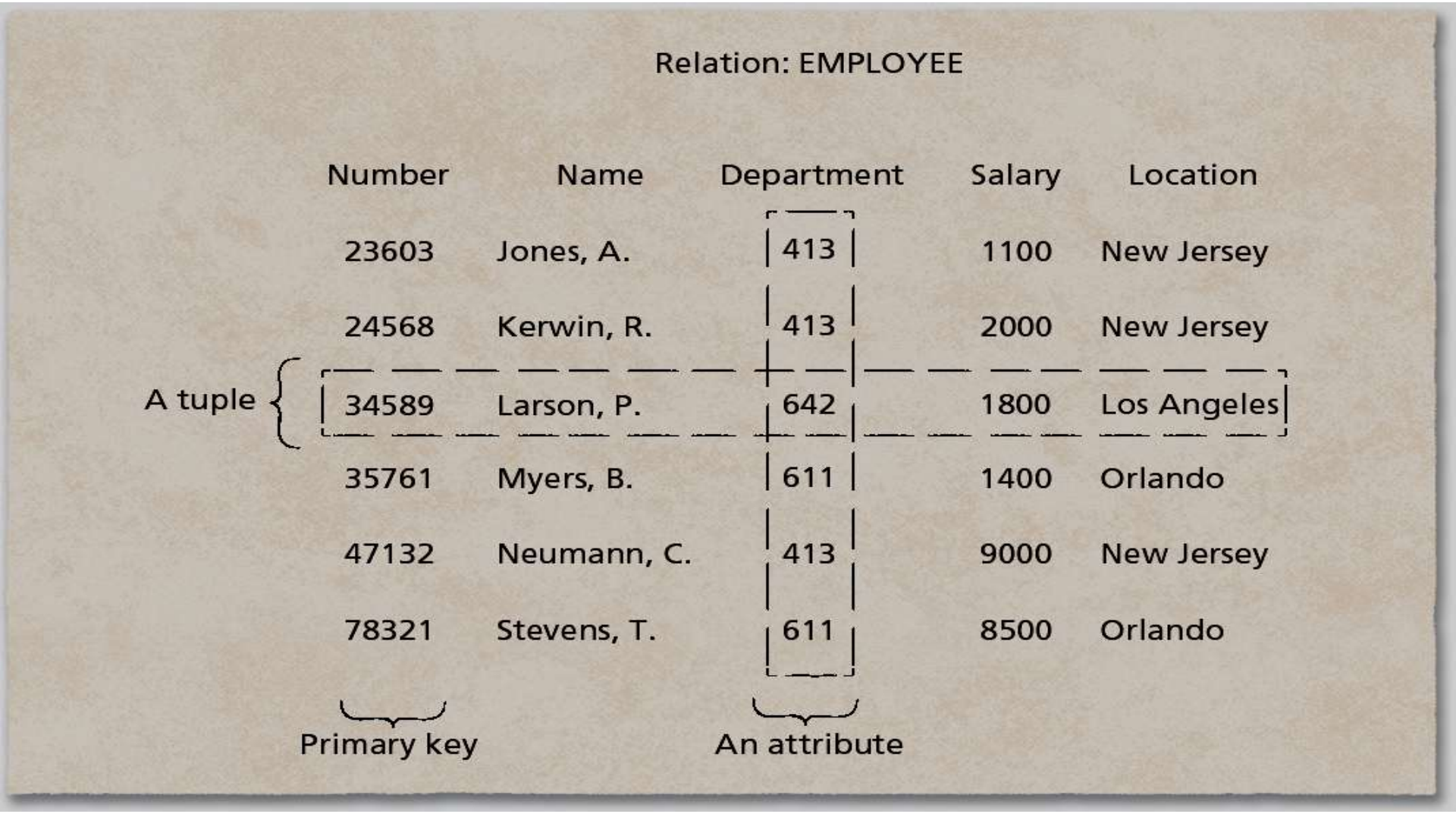
Строка

Опр. Строка (row, tuple) – элемент отношения, сочетание всех атрибутов одного объекта.

Первичный ключ

Опр. Первичный ключ (primary key) – в реляционной базе данных – сочетание атрибутов, позволяющее однозначно идентифицировать строку.

Отношение в реляционной базе данных



Преимущества реляционной модели баз данных

- Табличное представление, используемое в реляционной модели, просто реализуется в системах баз данных
- Реляционную модель можно воспринимать как универсальную форму представления баз данных
- Контроль доступа к данным элементарен: важные данные просто разносятся по разным отношениям, доступ к которым контролируется

Операционные системы и системы баз данных

- Различные службы операционных систем поддерживают системы баз данных:
  - Файловая система
  - Служба планирования
  - Менеджер процессов
  - Менеджер межпроцессного взаимодействия
  - Контроль целостности данных
  - Виртуальная память

Операционные системы и системы баз данных

- Большинство этих служб не оптимизировано специально для нужд СУБД
- Для поддержки СУБД, располагающих собственными оптимизированными службами, лучше всего использовать минимизированные операционные системы

Операционные системы и системы баз данных

- Поддержка баз данных в современных системах получает все большее распространение
- Возможно в скором будущем системы баз данных заменят файловые системы

Вопрос для самопроверки

- Базы данных уменьшают избыточность данных по сравнению с обычными файловыми системами? (Да/Нет)

Вопрос для самопроверки

- Базы данных уменьшают избыточность данных по сравнению с обычными файловыми системами? (Да/Нет)
- Да. Системы баз данных организуют данные по их содержимому, и никакие две записи не содержат одинаковую информацию. Например в базе данных может храниться одна копия информации о покупателе, к которой множество приложений может обращаться с помощью запросов.

Вопрос для самопроверки

- Значения каждого атрибута должны быть уникальными для всех строк отношения? (Да/Нет)

Вопрос для самопроверки

- Значения каждого атрибута должны быть уникальными для всех строк отношения? (Да/Нет)
- Нет. Одно и то же значение атрибута может содержаться во множестве строк отношения.

Вопрос для самопроверки

- Число операционных систем, прямо поддерживающих системы баз данных будет расти? (Да/Нет)

Вопрос для самопроверки

- Число операционных систем, прямо поддерживающих системы баз данных будет расти? (Да/Нет)
- Да. Многие операционные системы будут использовать базы данных как основное средство хранения пользовательских данных.