Безопасность баз данных

Топорец Александр Юрьевич

План

- Простейшая модель безопасности БД
- Модель многоуровневой безопасности баз данных
- Многоэкземплярность
- Тайные каналы
- Безопасные среды распределенных баз данных

Безопасность

От кого или чего мы защищаем наши данные?

- Защита от аппаратных сбоев
- Защита от ошибок пользователя
- Защита от несанкционированного доступа

Простейшая модель безопасности БД

Проверка полномочий основана на том, что для каждого пользователя или процесса информационной системы устанавливается набор санкционированных действий, которые он может выполнять по отношению к определенным объектам.

Проверка подлинности означает достоверное подтверждение того, что пользователь или процесс, пытающийся выполнить санкционированные действия, действительно является тем, за кого он себя выдает.

Модель многоуровневой безопасности БД

Многоуровневая безопасность означает, что, во-первых, в вычислительной системе хранится информация, относящаяся к разным классам безопасности, и, во-вторых, часть пользователей не имеет доступа к информации, относящейся к высшему классу безопасности.

Модель многоуровневой безопасности БД

Объекты подвергаются ***классификации***, а каждый субъект причисляется к одному из уровней (классу) доступа, который состоит из двух компонентов: иерархический компонент; некоторое множество неиерархических категорий.

В военных ведомствах США применяется следующая иерархия классов:

- совершенно секретно;
- секретно;
- конфиденциально;
- без грифа секретности.

Модель многоуровневой безопасности БД

Добавление свойства секретности приводит к появлению множественных значений, представляющих собой нечто подобное повторяющимся группам. (нарушение требований первой нормальной формы)

Фамилия	Класс	Звание	Класс	Специальность	Класс	Класс кортежа
Джонс	Н	Сержант Капитан	Н С	Программист	Н	?
Мартин	Н	Майор	Н	Оркестрант Разведчик	Н С	?

Многоэкземплярность

Многоэкземплярность – в рамках одного отношения может существовать множество кортежей с одним и тем же значением первичного ключа.

Фамилия	Класс	Звание	Класс	Специальность	Класс	Класс кортежа
Джонс	Н	Сержант	Н	Программист	Н	Н
Джонс	Н	Капитан	С	Программист	Н	С
Мартин	Н	Майор	Н	Оркестрант	Н	Н
Мартин	Н	Майор	Н	Разведчик	С	С

Маскирование объектов

Маскирование объектов – маскирование неопределенным значением значений объектов недоступных из соображений безопасности.

Фамилия	Класс	Звание	Класс	Специальность	Класс	Класс кортежа
Джонс	H	Сержант	H	Программист	H	H
Джонс	H	?	?	Программист	H	?
Мартин	H	Майор	H	Оркестрант	H	H
Мартин	H	Майор	H	?	?	?

Тайные каналы

Тайный канал – это средство, с помощью которого субъекты, обладающие высоким уровнем допуска, могут предоставлять информацию субъектам с более низким уровнем допуска.

- Тайные каналы памяти
- Тайные каналы хронометража

Безопасные среды распределенных баз данных

Раздельная внутренняя архитектура безопасных распределенных СУБД

Псевдомногоуровневый внутренний интерфейс для архитектуры безопасной распределенной СУБД

Данные без грифа секретности	Копия данных без грифа секретности, только для чтения	Копия данных без грифа секретности, только для чтения
	Секретные данные	Копия секретных данных, только для чтения Сов. Секретные данные

Топорец Александр Юрьевич
email: 4sale@mail.ru
www: www.stoporets.narod.ru