Математическое и компьютерное моделирование:
материалы III Международной научной конференции
(Омск, 12 ноября 2015 г.). Омск, 2015. С. 192–194. УДК 004.056

Т.М. Опарина

Омский государственный университет им. Ф.М. Достоевского, г. Омск

ИСПОЛЬЗОВАНИЕ МЕХАНИЗМА БЕЗОПАСНОСТИ DATA SECURITY POLICIES В МНОГОМЕРНОЙ СИСТЕМЕ ДАННЫХ ANALYTIC WORKSPACE MANAGER 11G ДЛЯ ОРГАНИЗАЦИИ МНОГОУРОВНЕВОГО ДОСТУПА

При проектировании разграничения прав доступа пользователей в многомерных системах существуют специальные механизмы безопасности, например, в программном продукте для создания многомерных систем Analytic workspace manager 11g от компании Oracle существует механизм безопасности Data Security Policies. Рассмотрим возможность применения данного продукта к организации многоуровневого доступа:

1. Определим некоторые понятия, используемые в многомерных базах данных. Измерения (Dimensions) – содержат набор уникальных значений, которые определяют и классифицируют данные. Они образуют края куба. Иерархии (Hierarchy) – способ организации данных на различных уровнях (Levels) агрегирования. При рассмотрении данных, аналитики используют измерения иерархий, сравнивают их на различных уровнях и делают выводы, например, о тенденциях развития продаж. Создадим хранилище данных, состоящее из трех измерений: ВРЕМЯ ПРОДАЖИ, КЛИЕНТ, ТОВАР (см. таблицу 1). Для начала необходимо определить какие данные будут относиться к определенному уровню секретности. Например, можно поддерживать следующие уровни секретности:

– общий доступ (OD);
– конфиденциально (K);
– секретно (C);
– совершенно секретно (CC).

Определим каким образом распределяются данные, в зависимости от уровня секретности (см. таблицу 1).

Таблица 1: Распределение данных, в зависимости от уровня секретности

ИЗМЕРЕНИЯ	**ВРЕМЯ ПРОДАЖИ**	**КЛИЕНТ**	**ТОВАР**
Иерархии	*КАЛЕНДАРЬ ПРОДАЖ*	*КЛИЕНТ*	*ТОВАР*
Уровни	Год (OD)	ФИО (CC)	Название товара (OD)
	Квартал (OD)	Адрес проживания (CC)	Тип товара (OD)
	Месяц (OD)	Паспортные данные (CC)	Производитель (OD)

2. В зависимости от уровня доступа пользователя необходимо обозначить к какой информации он имеет доступ. Например, если пользователь имеет уровень доступа «1», то он имеет доступ к уровню секретности «Общий доступ», а если пользователь имеет уровень доступа «2», то он имеет доступ к уровню секретности «Общий доступ» и «Совершенно секретно». Изобразим к какой информации имеет доступ пользователь в зависимости от уровня секретности (см. таблицу 2). Для назначения уровня доступа пользователя в многомерной базе данных можно использовать роль. Роль – это совокупность системных и объектных привилегий, которые сгруппированы под одним именем, чтобы облегчить администратору базы данных выдачу и отмену этих привилегий. Когда пользователю даётся роль, он получает все привилегии, связанные с ней.

Таблица 2: Связь уровня доступа к уровню секретности

Уровень доступа	**Уровень секретности**	
	Общий доступ	Совершенно секретно
«1»	+	
«2»	+	+

Создадим две роли с уровнями доступа общий доступ и секретно. Для создания роли воспользуемся командой CREATE ROLE:

– CREATE ROLE OD;

– CREATE ROLE CC.

Если пользователь имеет уровень доступа «1», то ему дается право:

GRANT OD TO USER 1.

Если пользователь имеет уровень доступа «2», то ему необходи-

мо дать следующее право:

GRANT CC TO USER 2.

Далее в программе Analytic workspace manager 11g с помощью Data Security Policy создаем следующую политику: выбираем иерархии, которые будет видеть пользователь. Для пользователя с уровнем доступа «1» в измерениях ВРЕМЯ ПРОДАЖИ и ТОВАР выбираем компоненты для общего доступа (политика POLICY1), а для пользователя с уровнем доступа «2» в измерениях ВРЕМЯ ПРОДАЖИ, КЛЕНТ и ТОВАР выбираем компоненты для совершенно секретного доступа (политика POLICY2). Затем политику POLICY1 присвоим роли OD, а политику POLICY2 присвоим роли CC.

Представленный здесь механизм позволяет администратору базы данных легко предоставить пользователям права в многомерной базе данных, в зависимости от уровня доступа пользователя.