Автор:

Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный исследовательский

университет им. академика С.П. Королева»

г. Самара, Самарская область

ДИСКРЕЦИОННАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА

Аннотация: *в данной статье автором рассматривается разграничение доступа при помощи дискреционной модели, а также особенности её реализации.*

Ключевые слова: *информационная безопасность, привилегия, доступ, модель, администратор, матрица, Oracle.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. СУБД (система управления базами данных) – программно-аппаратный комплекс, позволяющий управлять и манипулировать базами данных.

Определение 2. Привилегия – некоторый поддерживаемый системой признак, который определяет, может ли конкретный пользователь выполнить конкретную операцию.

Наиболее простая одноуровневая модель безопасности данных основана на дискреционном (избирательном) принципе разграничения доступа, при котором управление доступом субъектов к объектам осуществляется при помощи списков управления доступом или матрицы доступа. Каждая пара (субъект – объект) должна иметь явно заданное и недвусмысленное перечисление допустимых типов доступа (читать, писать, исполнять и т. д.).

Важной стороной моделей безопасности является управление доступом. Как правило, выделяют два подхода:

– добровольное управление доступом;

– принудительное управление доступом.

Добровольное управление основывается на понятии владения объектами. Обычно субъект, который создал объект, является и его владельцем. Во многих системах право на владение тем или иным объектом может передаваться. Таким образом, добровольное управление доступом позволяет реализовать полностью децентрализованный принцип организации и управления механизмом разграничения доступа. Преимуществом данного подхода является гибкость настройки системы разграничения доступа в информационной системе на определённую совокупность пользователей и ресурсов. Но такой подход затрудняет контроль и аудит состояния безопасности данных в системе.

Принудительное управление доступом предусматривает наличие централизованного администрирования доступом. В систему вводится специальный достоверный субъект (администратор), который имеет право устанавливать права владения для всех остальных субъектов системы. Таким образом изменять матрицу доступа имеет право только администратор системы.

Особенностью принудительного способа является более жёсткое централизованное управление, но вместе с тем он обладает менее гибким и менее точным механизмом настройки системы разграничения доступа, так как владельцы объектов (ресурсов) имеют более полное представление о конфиденциальности и содержимом, чем администратор системы.

На практике, как правило, используется комбинированный способ управления доступом, когда владельцы объектов устанавливают часть полномочий, но общий контроль осуществляет администратор системы.

Реализация дискреционной модели управления доступом в СУБД Oracle

Высокий уровень безопасности данных должен быть обеспечен без уменьшения функциональных возможностей СУБД и без существенного усложнения работы пользователя в системе.

Разграничение доступа в Oracle основывается в большинстве случаев на избирательной модели управления доступом. Администратор создаёт пользователей и устанавливает привилегии на доступ к конкретным объектам и выполнение

операций. С другой стороны пользователь должен иметь возможность управлять доступом к объекту, который он создал. Решение этой задачи состоит в реализации концепции права доступа или привилегии. В языке SQL, который используется в большинстве современных СУБД, предоставляются командой GRANT, а отменяются командой REVOKE. Для того чтобы предоставить кому-либо доступ к базе данных Oracle, администратор должен обеспечить доступность базы данных, создать в ней соответствующего пользователе и предоставить пользователю определённые привилегии на доступ к объектам базы. Контроль правомерности доступа осуществляется при помощи механизма аутентификации.

В заключении следует отметить, что в СУБД Oracle реализована принцип наименьших привилегий. Пользователь имеет доступ к объекту базы данных только в том случае, если ему это явно разрешено.

Список литературы

1. Смирнов С.Н. Безопасность систем баз данных. – М.: Гелиос АРВ, 2007. – 352 с.

2. Дейт К.Дж. Введение в системы баз данных. – 8-е изд. – М.: Вильямс, 2005. – 1328 с.