Автор:

Швейкин Владислав Витальевич

студент

ФГАОУ ВО «Самарский национальный исследовательский

университет им. академика С.П. Королева»

г. Самара, Самарская область

РОЛЕВАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА В СУБД

Аннотация: *в данной работе исследователем рассматривается вопрос преимуществ и особенностей разграничения доступа на основе ролей. В статье также обоснованы определения понятий «СУБД», «привилегия», «информационная система».*

Ключевые слова: *ролевая модель, СУБД, роль, привилегия, ограничение, информационная безопасность.*

Основные определения

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

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

3. Информационная система – система, предназначенная для хранения, поиска и обработки информации, и соответствующие организационные ресурсы, которые обеспечивают и распространяют информацию.

Введение

На сегодняшний день помимо традиционных моделей дискреционного и мандатного доступа особое внимание уделяется моделям доступа, в основе которых лежит понятие роли. Особенно ролевой подход наиболее часто используется в автоматизированных системах организационного управления, в которых для пользователей чётко определены их должностные полномочия и обязанности.

Модель направлена на упрощение и обеспечение формальной ясности в технологии обеспечения политики безопасности системы.

Управление доступом на основе ролей

Ролевая модель представляет собой особый тип политики, в основе которого лежит компромисс между гибкостью управления доступом, присущей дискреционным моделям, и жёсткостью правил контроля доступом, характерной для мандатных моделей. В ролевой модели доступа понятие субъекта можно разделить на две части: пользователь – лицо, которое использует действующую систему для выполнения конкретной задачи. Роль – совокупность прав доступа (привилегий) на объекты информационной системы, необходимых для выполнения определённых операций.

Ролевая модель включает три компоненты: модель отображения пользователь – роль, модель отображения привилегия – роль, модель отображения роль – роль.

Стоит так же отметить, что существует понятие иерархии ролей. Роль, входящая в иерархию, может включать в себя другие роли, наследуя привилегии включаемых ролей.

Администрирование ролевой моделью доступа включает много аспектов. Так как привилегии не назначаются администратором непосредственно пользователям, а приобретаются ими через роль, которая ему предписывается при выполнении некоторой функции технологического процесса, то управление индивидуальными правами пользователя сводится к назначению ему ролей.

Модель отображения пользователь – роль направлена на обеспечение корректного соответствия множества пользователей множеству ролей в условиях отсутствия централизованного управления. Возможным решением является поддержка специальных отношений «разрешено-назначить» и «разрешено-отозвать». Для реализации модели отображения привилегия – роль можно применить аналогичный подход. Модель отображения роль – роль основывается на трёх классах ролей: возможности, группы, универсальные роли.

Базовая модель

В основе базовой модели лежат следующие составляющие:

1. S – субъект (множество пользователей).

2. R – рабочая функция или название, которое определяется на уровне авторизации (множество ролей).

3. P – утверждения режима доступа к ресурсу (Множество привилегий).

4. SE – соответствие между S, R и/или P (Сеанс).

5. SA – назначение субъекта.

6. PA – функция, которая каждой роли ставит в соответствие множество прав доступа. При этом $\forall p \in P \ \exists r \in R : p \in PA(r)$.

7. Один субъект может обладать несколькими ролями.

8. Несколько субъектов могут иметь одну роль.

9. Одна роль может иметь несколько разрешений.

10. Несколько ролей могут обладать одинаковыми привилегиями.

Предполагается, что каждый пользователь и каждая привилегия связаны хотя бы одной ролью.

Для определения критерия безопасности в ролевой модели доступа используется следующее правило: Система безопасна, если любой пользователь системы, который работает в сеансе s, может осуществлять действия, требующие полномочия p только в том случае, если $p \in P(s)$

Заключение

В заключение следует отметить, что развитие децентрализованных моделей разграничения доступа, построенных на основе ролей, представляется важным и своевременным направлением совершенствования уровня информационной безопасности СУБД.

Список литературы

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

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

3. Ferraiolo D.F., Kuhn D R. (October 1992). «Role Based Access Control». 15th National Computer Security Conference: 554–563.