Авторы:

Завгородний Станислав Дмитриевич

студент

Швейкин Владислав Витальевич

студент

Дмитриев Егор Андреевич

студент

Танаев Иван Владимирович

студент

ФГАОУ ВО «Самарский национальный исследовательский университет им. академика С.П. Королева»

г. Самара, Самарская область

РОЛИ И РАЗГРАНИЧЕНИЕ ДОСТУПА НА ОСНОВЕ РОЛЕЙ

Аннотация*: в данной работе рассматривается ролевая политика безопасности баз данных. В основе статьи лежат понятия о пользователях, привилегиях, ролях и сеансах. Также проводится сравнение ролевой модели с другими моделями безопасности баз данных и описание модификаций ролевой политики безопасности баз данных.*

Ключевые слова*: база данных, пользователь, роль, привилегия, сеанс.*

Основные понятия

Введем некоторые определения, которые будут использованы в работе.

Определение 1. Пользователь – это работающий с системой человек, выполняющий специальные служебные функции.

Определение 2. Роль – это абстрактная сущность, действующая в системе, с которой связан лимитированный, логически связанный набор привилегий, которые необходимы для осуществления специальной деятельности. Одним из самых распространенных примеров роли является учетная запись администратора, который наделен специальными полномочиями и может использоваться несколькими пользователями.

Определение 3. Привилегия – это на выполнение специального вида операций с несколькими или одним объектами системы.

Определение 4. Сеанс – это соответствие между пользователем и множеством ролей.

Введение

Большой интерес ролевая политика безопасности баз данных представляет в контексте решения задач защиты информации в автоматизированных системах организационного управления в связи тем, что основой модели является идея того, что данные системы принадлежат не пользователю, а организации. Такая модель направлена на упрощение и достижение формальной ясности в технологии обеспечения политики безопасности системы. Ролевая политика является сильно усовершенствованной моделью Харрисона – Руззо – Ульмана, но она не относится ни к мандатным, ни к дискреционным моделям.

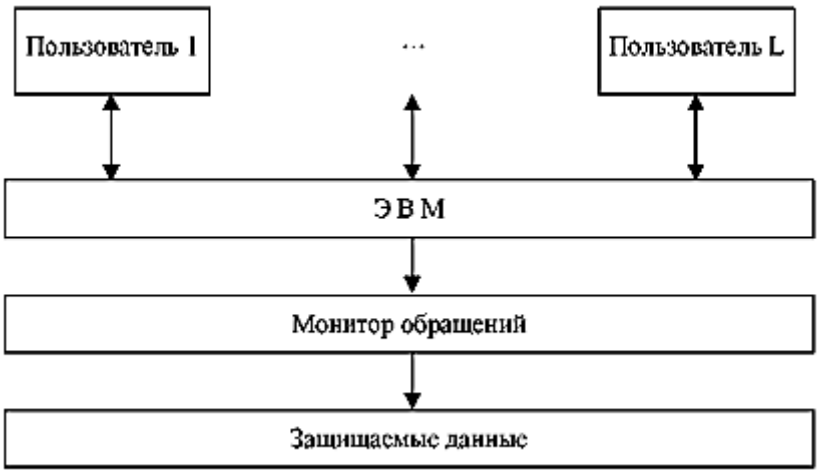

Рис. 1. Схема модели Харрисона, Руззо и Ульмана

Она определяет особый тип политики, основанный компромиссе между жесткостью правил контроля доступа, характерной для мандатных моделей, и гибкостью управления доступом, присущей дискреционным моделей. В ролевой политики управление доступом осуществляется с помощью правил, которые регламентируют назначение ролей пользователям и активацию ролей во время сеансов, а также на основе матрицы прав доступа для ролей.

Структура ролевой политики

Ролевая модель состоит из трех компонент: модель отображения пользователь-роль, модель отображения привилегия-роль и модель отображения роль-роль. Первая из данных моделей направлена на обеспечение правильного отображения множества пользователей на множество ролей в условиях децентрализованного управления. Выдвигаемое решение основывается на использовании специальных отношений «разрешено назначить» и «разрешено отозвать». Точно такой же подход предлагается для реализации модели отображения привилегия-роль. Оба отношения являются отношениями «многие ко многим». Получается, что роль может содержать нескольких пользователей, а пользователь может быть членом сразу нескольких ролей. Аналогично одна привилегия может быть предоставлена нескольким ролям, а роль может иметь большое количество привилегий.

Для модели отображения роль-роль необходима реализация трех классов ролей: возможности, группы и универсальные роли.

Логическая структура объектов управления упрощается, если ввести иерархию ролей. Роль, которая входит в иерархию, может включать другие роли, при этом она наследует все привилегии включаемых ролей.

Рис. 2. Пример иерархии ролей

Реализуя политику безопасности организации, в основе которой лежит базовая модель, вводится механизм ограничений. С помощью них поддерживаются роли, для которых политикой безопасности не допускается одновременное отображение на определенного пользователя. Такие роли называют взаимоисключающими. Другим вариантом ограничений является ограничение на назначение

пользователя на роль – это число членов конкретной роли. Например, только один сотрудник в текущий момент может быть отображен на роль руководителя. Точно также можно ограничить число ролей, которые могут быть выполнены определенным пользователем. Такое ограничение называется количественным ограничением. При нем вводится понятие необходимых ролей, основанных на компетентности пользователей. Только пользователи, являющиеся членами определенной группы, могут быть назначены роль лиц, выполняющих операции, для которых необходима соответствующая квалификация.

Базовая ролевая модель

Базовая ролевая модель RBAC0 (от анг. Role Based Access Control) состоит из следующих компонент:

– множества пользователей U, множества ролей R, множества привилегий P и множества сеансов S;

– отношение типа «многие-ко-многим» $PA \subseteq P \times R$, представляющее собой отображение множества ролей на множество привилегий;

– отношение типа «многие-ко-многим» $UA \subseteq U \times R$, представляющее собой отображение множества пользователей на множество ролей;

– функция $user: S \to U$. Она ставит в соответствие каждому сеансу s_i только одного пользователя $user(s_i)$ (не меняется в течение времени жизни сеанса);

– функция $roles: S \to 2^R$. Она ставит в соответствие каждому сеансу s_i набор ролей $roles(s_i) \subseteq \{r \mid (user(s_i),r) \in UA\}$ (набор ролей может меняться со временем).

Из определения следует, что с сеансом s ассоциируется множество привилегий.

Естественным развитием базовой ролевой модели является модель иерархии ролей. Наиболее известная модель иерархии ролей $RBAC_1$ является стандартным расширением ролевой модели. $RBAC_1$ содержит в себе следующие компоненты:

– множества *U, R, P, S,* отношения *PA, UA* и функция *user* определены так же как в определении $RBAC_0$;

– отношение частичного порядка на R: *RH* C *R x R* называется иерархией ролей;

– модифицированная функция *roles: S -> 2^R*. Она определена следующим соотношением *roles(s_i)* C *{r| (□r' => r)[user(s_i), r']| ϵ UA}* (набор ролей может меняться со временем).

Другой модификацией базовой модели является модель $RBAC_2$, которая определяет понятие ограничений. Они являются мощным механизмом для определения высокоуровневой политики безопасности предприятия. $RBAC_2$ включает следующее множество объектов:

– все объекты модели $RBAC_0$;

– совокупность предикатов, определяющих, являются ли разрешенными значения различных компонент $RBAC_0$. В модель $RBAC_2$, включаются только разрешенные значения компонент.

Так как и иерархия ролей, и механизм ограничений являются хорошими инструментами в достижении в качественной безопасности организации, то логичным следствием развития базовой ролевой модели стало создание обобщенной модели $RBAC_3$, объединяющей модели $RBAC_1$ и $RBAC_2$, обеспечивающей механизм ограничений вместе с иерархией ролей.

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.