УДК 004.056.52

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ РОЛЕВОГО РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В КОРПОРАТИВНЫХ БАЗАХ ДАННЫХ

Никитин Ю.А.
Научный руководитель — профессор Саенко И.Б.
Военная академия связи, г. Санкт-Петербург

Корпоративные базы данных (КБД) характеризуются, с одной стороны, достаточно большим числом работающих с ними пользователей. С другой стороны, в КБД содержатся и подлежат обработке достаточно разнообразные по важности и конфиденциальности сведения. Это приводит к необходимости осуществлять эффективное управление разграничением доступа к информации, содержащейся в КБД, ограничивая либо запрещая работу конкретных групп пользователей с одними видами информационных объектов и полностью разрешая их работу с другими видами объектов. Для этих целей создаются и поддерживаются в актуальном состоянии системы разграничения доступа (СРД) к информации в КБД.

Проблема построения СРД к информации в КБД заключается в том, чтобы с минимальными трудозатратами определить рациональную СРД, отвечающую предъявляемым требованиям по конфиденциальности и доступности информации, используя при этом механизмы разграничения доступа, предоставляемые системами управления базами данных (СУБД). Свойства конфиденциальности и доступности информации являются взаимно антагонистическими, так как усиление одного из данных свойств неизбежно оказывает негативное влияние на другое свойство.

В настоящее время в качестве СУБД в отечественных информационных системах широко используются такие программные продукты как *Oracle*, *Informix*, *MS SQL Server*, *InterBase* и прочие. В общем случае все они обладают возможностями построения многоуровневых СРД с одновременной реализацией ролевого, дискреционного и мандатного способов доступа. При этом наибольшее распространение получили ролевой и дискреционный способы. Мандатный способ применим реже. С одной стороны, необходимость разделения конфиденциальной информации по уровням в КБД возникает редко. С другой стороны, СУБД с возможностями реализации мандатного способа являются достаточно дорогими. Поэтому далее ограничимся вопросами совместного применения ролевого и дискреционного способов доступа к информации в КБД.

Формальное представление решения по построению СРД задается в виде набора матриц доступа, элементами которых являются целые числа, определяющие права доступа конкретных пользователей или их групп к информационным объектам или их категориям. К такому же формальному представлению сводятся требования по разграничению доступа, определяемые политикой информационной безопасности. Идеальным является такой вариант построения СРД, когда реальные и требуемые матрицы доступа полностью совпадают. Однако на практике при достаточно большом количестве пользователей КБД (как правило, свыше 50) это невыполнимо. В результате возникает задача построения СРД в одном из двух возможных вариантов ее постановки: либо обеспечить максимальную конфиденциальность данных при выполнении заданных ограничений на их доступность, либо обеспечить максимальную доступность данных при выполнении заданных ограничений на их конфиденциальность.

Рассмотрим содержательную постановку данной задачи. Согласно политике безопасности, в соответствии с которой осуществляется создание СРД к информации, фиксируется некоторая требуемая схема (матрица) разграничения доступа (СхРД), отобра-

жающая требуемые разрешительные полномочия субъектов доступа относительно объектов доступа, хранимых в КБД.

Администратор безопасности имеет возможность создания некоторого множества ролей, являющихся элементами СхРД. Для каждой роли устанавливаются, с одной стороны, разрешительные полномочия по отношению к объектам доступа. С другой стороны, каждой роли сопоставляется список субъектов доступа. В этом случае каждый субъект получает разрешительные права на доступ к тем объектам, к которым имеются разрешительные полномочия данной роли. При этом один и тот же субъект может одновременно принадлежать разным ролям.

Кроме того, в дополнение к ролевому способу доступа возможна реализация дополнительной СхРД на основании дискреционного способа, когда каждому субъекту напрямую задаются дополнительные полномочия относительно объектов доступа. Дополнительная дискреционная СхРД необходима в том случае, если ролевая СхРД не смогла совпасть с требуемой. В этом случае дополнительная СхРД играет роль уточняющего компонента общей СРД.

Однако не каждая СУБД при реализации ролевой СхРД имеет возможность одновременной реализации дискреционной СхРД. Поэтому в общем случае следует полагать, что рациональная СРД создается только с использованием ролевой СхРД.

Тогда построение СРД на основе технологии ролевого разграничения доступа к информации сводится к формированию следующей постановки задачи и ее дальнейшему решению. Необходимо, исходя из заданной СхРД, найти: 1) множество ролей; 2) разрешительные полномочия по отношению к объектам доступа для каждой роли; 3) список субъектов доступа для каждой роли – такие, чтобы реальная СхРД, получаемая в результате реализации ролевого способа доступа, с одной стороны, отвечала требованиям конфиденциальности и доступности данных, а с другой стороны, имела минимальное количество ролей.

Требованию минимизации количества ролей имеется следующее обоснование. Если количество ролей равно либо больше количества объектов, то в этом случае задача имеет тривиальное решение: для каждого субъекта доступа предусмотрены одна или несколько ролей, причем каждой роли соответствует только один субъект. Положим, что количество ролей на единицу меньше, чем количество субъектов. В этом случае для одной из ролей необходимо сопоставить одновременно два субъекта и определить права ролей таким образом, чтобы реальная СхРД совпадала с требуемой. Однако в этом случае не всегда существует решение задачи, когда реальная и требуемая схемы совпадают. Если далее уменьшить количество ролей на единицу, то вероятность того, что не будет существовать реальной схемы, полностью совпадающей с требуемой, еще более возрастает. Таким образом, уменьшение количества ролей неизбежно приводит в общем случае к увеличению расхождения между требуемой СхРД и СхРД, являющейся рациональной по критериям конфиденциальности и доступности информации.

Для решения поставленной задачи построения СРД на основе технологии ролевого разграничения доступа к информации предлагается использовать метод генетических алгоритмов оптимизации.

Существенным отличием генетического алгоритма, разработанного для решения данной задачи, является обеспечение возможности учета и обработки в ходе выполнения основных генетических операций (скрещивания, мутации, селекции) хромосом переменной длины. Это существенно сокращает количество этапов эволюционного моделирования, требуемых для достижения конечной популяцией особей своего стационарного состояния и, тем самым, определения рационального решения задачи построения СРД в КБД на основе технологии ролевого разграничения доступа к информации.