Реляционная модель логического разграничения доступа

А. А. Иткес (МГУ имени М. В. Ломоносова, Москва)

В статье рассматривается задача управления доступом к объектам информационных систем управления наукометрической информацией. Представлена реляционная модель логического разграничения доступа к объектам таких систем, обладающая рядом важных в контексте поставленной задачи свойств, которыми не обладают другие модели логического разграничения доступа.

Ключевые слова: информационная безопасность, наукометрия, разграничение доступа, реляционная модель.

В докладе рассматривается реляционная модель логического разграничения доступа (ЛРД) к объектам информационных систем. Данная модель разрабатывалась для использования в системах управления наукометрической информацией, одной из которых является информационно-аналитическая система (ИАС) «Наука-МГУ» («ИСТИНА»). Эта и аналогичные ей системы имеют ряд свойств, аналогичных свойствам социальных сетей, а именно — множество пользователей постоянно меняется без участия администратора системы, и права доступа пользователей к объектам определяются различными видами взаимосвязей между объектами, в том числе и опосредованными. Вместе с тем, в работе [2] показано, что ранее существующие модели ЛРД, предназначенные для использования в социальных сетях, не удовлетворяют требованиям, предъявляемым к механизмам ЛРД ИАС «Наука-МГУ» («ИСТИНА»). По этой причине была разработана реляционная модель ЛРД [1], устраняющая недостатки ранее существовующих моделей.

При использовании реляционной модели ЛРД в информационной системе задаются следующие конечные множества:

- $Objects$ — множество объектов;
- $Users \subset Objects$ — множество пользователей;
- $Classes$ — множество классов;

- *Actions* — множество возможных действий над объектами;
- *Relations* — множество видов отношений между объектами;
- *Chains* — множество цепочек отношений.

В случае ИАС «Наука-МГУ» («ИСТИНА») множество *Objects* включает в себя такие объекты системы, как учетные записи научных сотрудников, статьи, журналы, научные организации и подразделения. В множестве объектов выделено множество пользователей — активных сущностей, совершающих операции над другими объектами. С каждым объектом ассоциирована метка, причисляющая его к определенному классу, и определяющая, является ли объект пользователем, или каким-либо ресурсом системы. Например, в ИАС «Наука-МГУ» («ИСТИНА») существуют классы «пользователь», «статья», «журнал», «подразделение» и другие. Множество *Actions* включает возможные действия над объектами системы. Множество *Relations* — это множество разных видов взаимосвязей (отношений) между объектами. Для ИАС «Наука-МГУ» («ИСТИНА») примерами отношений являются отношение авторства, связывающее пользователя с публикацией, отношение места работы, связывающее пользователя с организацией или подразделением, отношение, связывающее пользователя с подразделением, для которого этот пользователь является ответственным за сопровождение информации в системе и отношение, связывающее публикацию с подразделением, в котором работает один из ее авторов. Последнее отношение представляет собой пример порожденного отношения, которое автоматически возникает между двумя объектами, если существует третий объект, определенным образом связанный с ними обоими. Другие отношения, для которых информация о связанных этими отношениями объектах хранится в базе данных системы и не зависит от других отношений, называются примитивными. Такими являются представленные выше отношения авторства и места работы. Последнее из основных множеств реляционной модели ЛРД — это множество цепочек отношений, каждая из которых представляет собой правило, по которому два объекта считаются связанными определенным порожденным отношением, если существуют объекты, связанные с этими двумя объектами определенным образом. Цепочка, имеющая вид $(r_{12}, r_{23}) \to r_{13}$ означает, что объекты o_1 и o_3 считаются связанными отношением r_{13}, если существует такой объект o_2, что объекты o_1 и o_2 связаны отношением r_{12}, а объекты o_2 и o_3 связаны отношением r_{23}. Последовательность (o_1, o_2, o_3) при этом называется цепочкой объектов, соответствующей цепочке отношений $(r_{12}, r_{23}) \to r_{13}$.

С каждым из отношений в системе при использовании реляционной модели ассоциированы множества разрешенных и запрещенных действий. Если действие a является разрешенным для отношения R, то пользователь, связанный с целевым объектом отношением R, имеет право осуществлять доступ a к целевому объекту. Если действие a является запрещенным для отношения R, то пользователь, связанный с целевым объектом отношением R, не имеет право осуществлять доступ a к целевому объекту даже в том случае, если существует другое отношение, связывающее данного пользователя с данным объектом и разрешающее действие a.

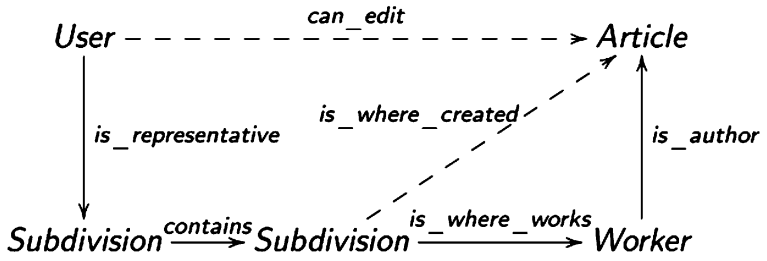

Рис. 1. Пример цепочки отношений.

Пример использования реляционной модели ЛРД представлен на рис. 1. Пусть пользователь a является ответственным за сопровождение информации в системе в рамках подразделения b, включающего в себя дочернее подразделение c, в котором работает сотрудник d, являющийся автором статьи e. Тогда пользователь a имеет право изменять атрибуты статьи e за счет существования последовательности объектов (a, b, c, d, e), связывающей пользователя с целеовй статьей следующей последовательностью отношений: «пользователь является ответственным за сопровождения информации в рамках подразделения» — «одно подразделение содержит другое» — «в подразделении работает сотрудник» — «сотрудник является автором статьи».

Кроме описанных выше элементов, реляционная модель ЛРД предусматривает возможность ассоциировать с некоторыми из объектов системы и некоторыми из пар объектов, связанных определенным отношением, набор атрибутов, которые также могут влиять на предоставление пользователю право доступа к объектам. Некоторые из цепочек отношений в системе при этом имеют соответствующие им условия, представляющие собой бесквантворные предикаты, зависящие от атрибутов объектов, соединенных отношениями, входящими в цепочку. Начальный

и конечный объект цепочки считаются связанными отношением, порождаемым цепочкой, только в том случае, если условие цепочки является истинным для объектов, входящих в цепочку.

Рассмотрим пример. В ИАС «Наука-МГУ» («ИСТИНА») пользователь, ответственный за сопровождение информации в системе в рамках подразделения, имеет право редактировать атрибуты публикаций, выполненных в подконтрольном ему подразделении. Однако, автор статьи мог сменить место работы после ее написания. Такая смена приводит к тому, что публикации данного автора оказываются связаны необходимым отношением с ответственным по подразделению, которое является новым местом работы ее автора, а не с ответственным по подразделению, в котором работа выполнялась. Логичным требованием к системе в этом случае является предоставление доступа к статье только пользователям, ответственным по подразделению, в котором фактически выполнялась работа. С этой целью реляционная модель позволяет ассоциировать с каждой публикацией атрибут, являющийся датой завершения работы над ней, а с каждой парой, состоящей из сотрудника и подразделения, являющегося местом его работы — пару атрибутов, соответствующих дате вступления сотрудника в должность и дате увольнения. При этом с цепочкой, состоящей из отношения ответственности пользователя по подразделению, отношения места работы и отношения авторства, которая порождает отношение, позволяющее пользователю редактировать атрибуты статьи, необходимо ассоцировать следующее далее условие. Предикат цепочки истиннен, если дата окончания работы над публикацией лежит в интервале между датой вступления сотрудника в должность и датой его увольнения. Если пользователь связан с целевой статьей цепочкой объектов, соответствующей данной цепочке отношений и удовлетворяющей связанному с ней условию, то он считается связанным с этой статьей отношением, дающим необходимые права доступа. В противном случае, пользователь не считается связанным с целевой статьей необходимым отношением, даже если между пользователем и статьей существует цепочка объектов, попарно связанных входящими в цепочку отношениями, однако при этом атрибуты объектов цепочки не удовлетворяют связанному с ней условию.

Важным свойством реляционной модели ЛРД является возможность использовать в качестве элементов цепочек отношения, порождаемые другими цепочками. В случае, если первая цепочка содержит в качестве элемента отношение, порождаемое второй цепочкой, первая цепочка будет эквивалентна цепочке, полученной из нее заменой отноше-

ния, порождаемого второй цепочкой, на подпоследовательность отношений, составляющих вторую цепочку. Данная операция над цепочками называется расширением первой цепочки отношений второй цепочкой. Условие расширенной цепочки при этом является конъюнкцией условий исходных цепочек. Реляционная модель ЛРД позволяет выделить в отдельные цепочки фрагменты, часто встречающиеся в других цепочках, что позволяет упростить описание модели. В примере, представленном на рис. 1, цепочка, порождающая отношение *can_edit*, содержит элементы *is_representative*, *contains* и *is_where_created*. Отношение *is_where_created*, в свою очередь, порождается цепочкой, состоящей из двух отношений *is_where_works* и *is_author*. При этом механизмы реляционной модели ЛРД автоматически вставляют вторую цепочку в первую на место порожденного ею отношения. Таким образом, отношение *can_edit* порождается цепочкой из четырех элементов: *is_representative*, *contains*, *is_where_works* и *is_author*.

Из представленного примера следует, что механизм подцепочек также позволяет отнести условие, повторяющееся в нескольких цепочках, к одной общей подцепочке. Из примера очевидно, что условие «дата написания статьи лежит в диапазоне между датами встапления автора в должность и его увольнения» относится к подцепочке, порождающей отношение *is_where_created* и будет автоматически применено ко всем цепочкам, содержащим эту подцепочку. Таким образом, механизм подцепочек позволяет значительно сократить описание модели и упростить ее модификацию, устраняя дублирующиеся элементы в описании модели. Вместе с тем, использование подцепочек может привести к ситуации зацикленного порождения отношений. Этот факт означает, что модель, содержащая цепочку, которая включает в качестве элемента отношение, которое порождается этой же цепочкой, не может быть использована на практике. Кроме того модель, которая содержит две цепочки, одна из которых включает в качестве элемента отношение A и порождает отношение B, а другая включает отношение B и порождает отношение A, также является некорректной. При использовании реляционной модели ЛРД требуется провести проверку корректности набора правил прежде чем устанавливать его для использования в целевой системе. Использование именованных подцепочек отношений и атрибутов отношений между объектами отличает реляционную модель от ряда моделей, предназначенных для использования в социальных сетях, в том числе и наиболее выразительных из них [3].

В настоящее время создан прототип программного комплекса, реализующего управление доступом к объектам информационных систем на основе реляционной модели ЛРД. Данное программное средство работает следующим образом. Принимая на входе описание реляционной модели на специально разработанном языке, программа производит расширение всех цепочек отношений, пока это возможно. Множество цепочек отношений системы, таким образом, преобразуется в эквивалентное ему множество, содержащее цепочки только из примитивных отношений. Для каждой из таких цепочек генерируется SQL-запрос к СУБД, проверяющий существование цепочки объектов, связывающей заданные начальный и конечный объекты соответствующей цепочкой отношений. После этого создается программный модуль на языке Python, проверяющий возможность доступа пользователя к объекту путем последовательного анализа результатов всех ранее сгенерированных запросов к СУБД. Этот модуль может быть затем встроен в целевое WEB-приложение. Таким образом, приложение, непосредственно проверяющее доступ пользователя к объекту, не выполняет операции расширения цепочек отношений, которые уже выполнены на стадии предобработки модели. Использование этапа предобработки правил ускоряет работу механизмов реляционной модели и гарантирует корректность используемого WEB-приложением набора цепочек.

Список литературы

[1] Васенин В. А., Иткес А. А., Шапченко К. А., Бухонов В. Ю. Реляционная модель логического разграничения доступа на основе цепочек отношений // Программная инженерия. — 2015. — № 9. — С. 11–19.

[2] Васенин В. А., Иткес А. А., Шапченко К. А. О применении моделей разграничения доступа в социальных сетях к одному классу многопользовательских систем управления контентом // Программная инженерия. — 2015. — № 4. — С. 10–19.

[3] Bogaerts J., Decat M., Lagaisse B., Joosen W. Entity-Based Access Control: supporting more expressive access control policies.