патентообладатель Академия ФСО России. – № 2010114785/08 ; заявл. 13.04.10; опубл. 27.06.11, Бюл № 18 – 9 с. : ил.

6. Пат. 2450337 Российская федерация, МПК G06F 15/00. Способ (варианты) управления демаскирующими признаками системы связи / Е. В. Гречишников [и др.] ; заявитель и патентообладатель Академия ФСО России. – № 2011117814/08 ; заявл. 03.05.11 ; опубл. 10.05.12, Бюл. № 13. – 19 с. : ил.

Д.В. Кириллов

ПРОБЛЕМЫ АВТОМАТИЗАЦИИ УПРАВЛЕНИЯ КОНТРОЛЕМ ДОСТУПА НА ОСНОВЕ РОЛЕЙ

(Самарский государственный университет)

Для достижения цели автоматизации управления контролем доступа на основе ролей в автоматизированных системах управления предприятием (АСУП) необходимо решить задачу замыкания компонентов и отношений подсистемы реализующей политику безопасности (ПБ) и объектов и отношений уровня бизнес-логики системы (БЛ), содержащей достаточно большой объем данных о субъектах необходимых для принятия решений о назначений или отзыве полномочий, либо для выполнения других операций [1].

В простейшем случае, когда в организации используется только одна система, и управление доступом реализуется в ней же, задача с формальной точки зрения является тривиальной - необходимо обогатить систему недостающими компонентами и отношениями [2]. Простая модель данных характерная для систем, использующих ролевую политику безопасности представлена на рисунке 1.

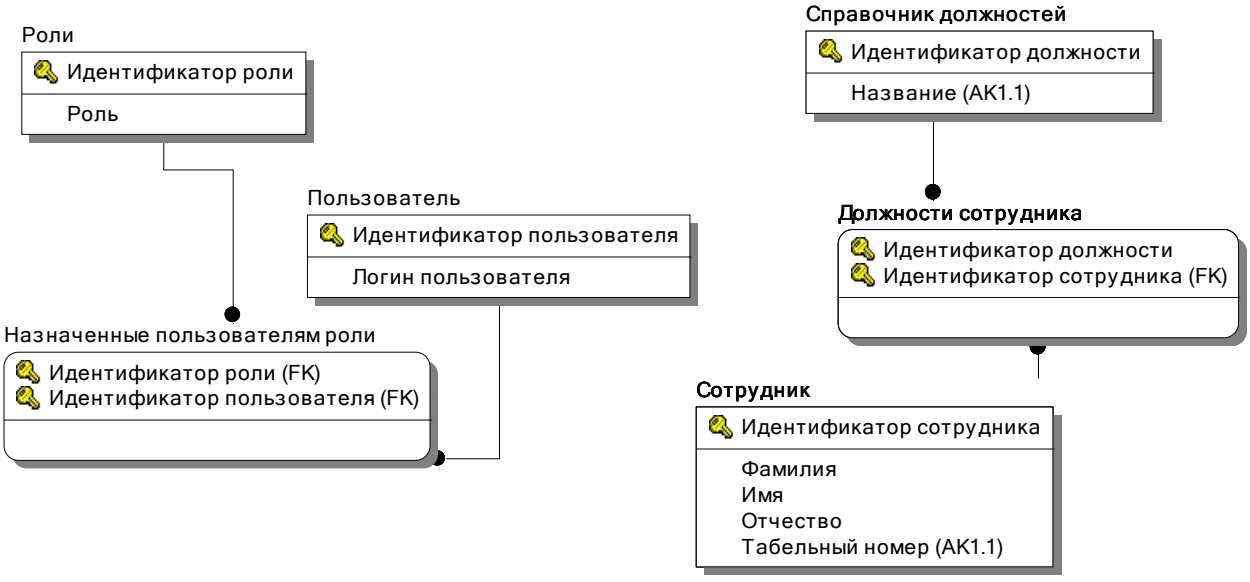

Рис. 1. Простейшая модель данных некоторых компонентов и отношений подсистемы разграничения данных
и соответствующих им объектов уровня бизнес-логики

Определим два метода связывания – атрибутное и объектное. В первом методе, обогащению подвергаются сущности представляющие компоненты и отношения подсистемы безопасности, которые уже представлены в системе путем добавления в них атрибутов-связей (логических или физических) с компонентами и отношениями уровня бизнес-логики. Результат использования такого метода на уровне моделей данных представлен на рисунке 2.

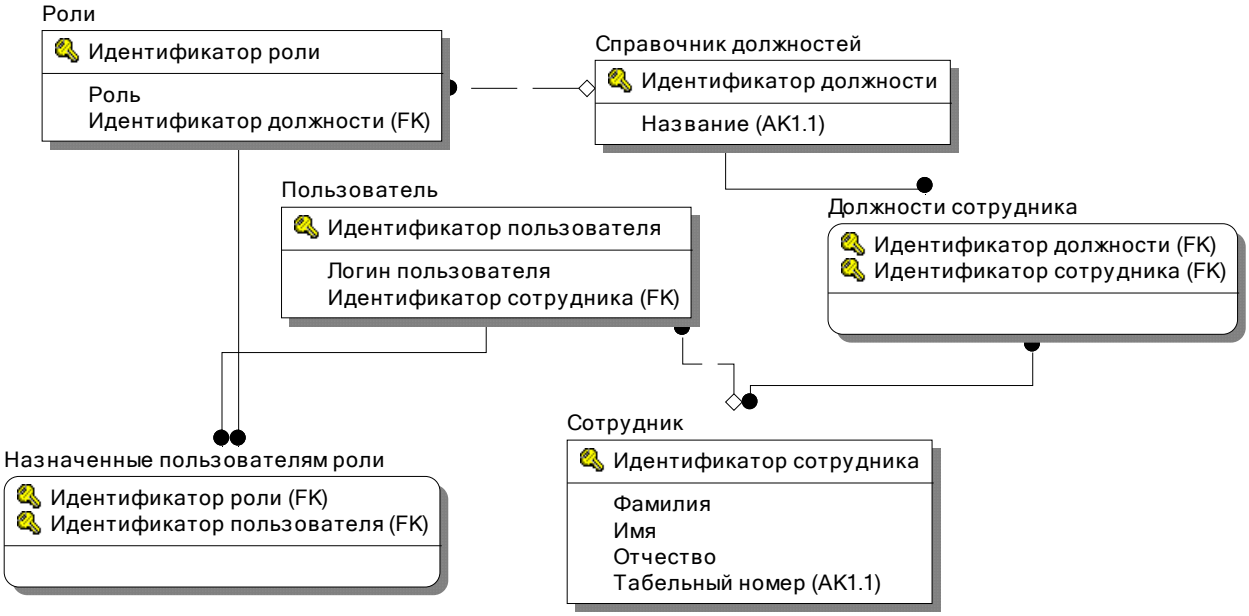

Рис. 2. Модель данных атрибутного замыкания компонентов подсистемы разграничения доступа и соответствующих им объектов бизнес-логики

Атрибутное связывание имеет ряд существенных недостатков:

1) так как зачастую требуется адаптация существующей реализации ПБ модификация существующих сущностей не допустима с точки зрения требований лицензий на использование ПО;
2) также в случае адаптации существующих механизмов разграничения доступа, аспекты реализации компонентов могут быть скрыты и не доступны для внесения прямых изменений [3];
3) в том случае, если связывание осуществляется с использованием внешних ключей между сущностями уровня бизнес-логики и уровня реализации ПБ безопасности невозможно гарантировать отсутствие проблем возникновения блокировок на компонентами и того и другого уровня;
4) возможности связывания достаточно ограничены, так как структура связей отображения должна фактически полностью повторять структуру связей между объектами уровня бизнес-логики, что на практике далеко не всегда соответствует действительности. Например, из рисунка 2 видно, что наделив сущность “Роль” атрибутом связи с сущностью “Должность”, получаем фактически отношение одна роль – одна должность, хотя в реальности у одной должности может быть более чем одна роль [4].

В случае объектного связывания, сущности представляющие компоненты и отношения подсистемы безопасности не изменяются. Вместо этого в систему вносятся новые сущности, представляющие собой отношения отображения элементов подсистемы безопасности и элементов уровня бизнес-логики (рисунок 3).

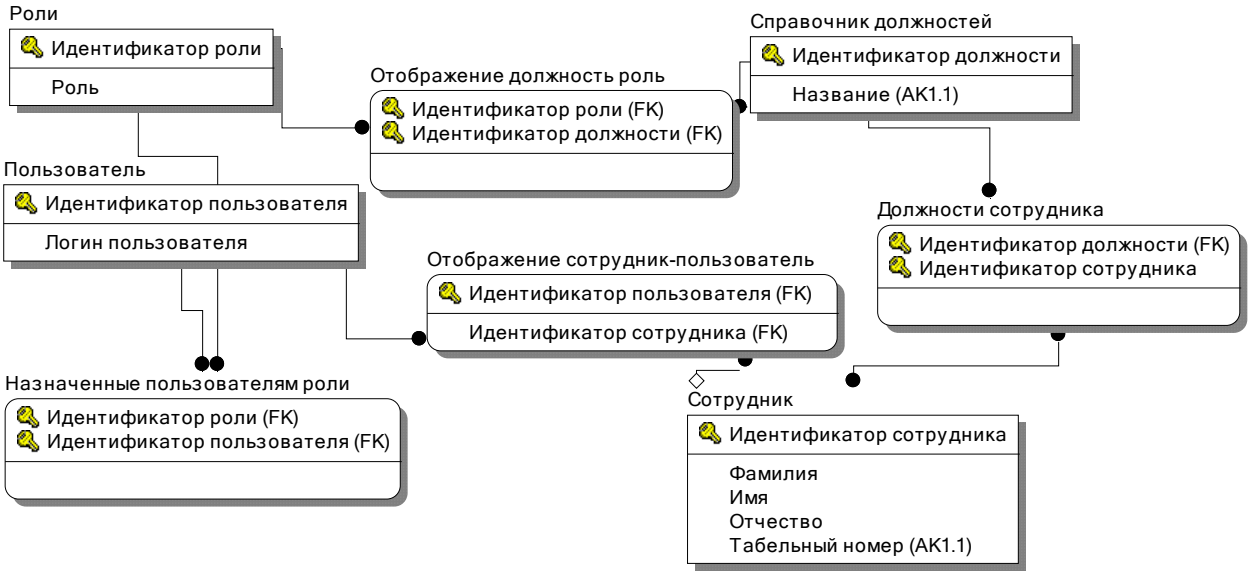

Рис. 3. Модель данных объектного замыкания компонентов подсистемы разграничения доступа и соответствующих им объектов бизнес-логики

Объектное связывание исключает недостатки связанные с ограниченностью влияния на процесс связывания с использованием атрибутного связывания, так как при его использовании не модифицируются существующие объекты и отношения, что соответственно полностью исключает прямое влияние на компоненты уровней бизнес-логики и подсистемы разграничения доступа.

Другим важным аспектом процесса замыкания уровня подсистемы разграничения доступа и уровня бизнес-логики является выбор способа реализации процесса связывания. Здесь возможно два варианта – синхронный и асинхронный.

В случае синхронного процесса порождающее событие на уровне бизнес-логики одновременно порождает событие на уровне подсистемы безопасности, фактически реакция на оба события выполняется в рамках одной транзакции. Плюсом здесь является то, что фактически система осуществит переход состояния один раз, то есть в следующий момент времени после подтверждения транзакции компоненты и отношения подсистемы безопасности будут предположительно находиться в адекватном состоянии в соответствии с описанными правилами. Минусы здесь также очевидны:

1) ошибка или невозможность выполнения транзакции на уровне подсистемы безопасности, вызовет невозможность подтверждения транзакции на уровне бизнес-логики;
2) в случае, если правила отображения имеют достаточно сложную форму, и их вычисление достаточно трудоемко, то время выполнения транзакции на уровне бизнес-логики может значительно возрасти [5];

3) с технической точки зрения возможности применения условий могут быть ограничены в связи с особенностями функционирования системы.

Асинхронная обработка предполагает, что процессы генерации событий по изменению состояний компонентов и отношений уровня БЛ и их отображения на уровень ПБ не зависят друг от друга, то есть выполняются в разных транзакциях. В этом случае, либо существует независимый процесс, отслеживающий состояние требуемых объектов и их отношений, либо над этими объектами реализуются нотификаторы (объекты генерирующие сообщения о событиях по изменению состояния объектов). И в том и другом случае, дальнейшая обработка таких событий никак не влияет на объекты уровня БЛ [6,7].

Таким образом, наиболее эффективным способом реализации механизма замыкания уровня реализации ПБ и уровня реализации БЛ является асинхронное объектное связывание.

Литература

1. Кириллов Д.В. Основные принципы событийно-обусловленного делегирования полномочий в системах контроля доступа на основе ролей// Вестник УГАТУ. 2009 т.1(30), с. 218-225.

2. Кириллов Д.В. Классификация моделей делегирования полномочий в контроле доступа на основе ролей// Доклады Томского государственного университета систем управления и радиоэлектроники, 2010, № 1(21), с. 146-150.

3. Кириллов Д.В. Особенности механизма обработки событий в СОДОП// Материалы Зимней школы аспирантов и молодых ученых УГАТУ, Уфа, 2009.

4. Ahmed Ali, Zhang Ning A Context-Risk-Aware Access Control Model for Ubiquituos Enviroments // Proceedings of the International Multiconference on Computer Science and Informational Technologies. - Wisla, Poland :, 2008. - стр. 775-782.

5. Al-Kahtani Mahammad A. A model for Attribute-Based User-Role Assigment // Proceedings of the 18th Annual Computer Security Applications Conference. - Washington, DC, USA : IEEE Computer Society, 2002.

6. Kumar A.N., Karnik N. и Chaftle G. Context sensivity in Role-Based Access // ACM SiGOPS Operating system review. - July 2002 г.. - Т. 36. - стр. 53-66.

7. Кириллов Д.В. Классификация моделей делегирования полномочий в контроле доступа на основе ролей// Доклады ТУСУРа, № 1 (21), часть 1, июнь 2010. с. 146 – 149