Архитектура систем автоматизированного управления контролем доступа на основе ролей

Д.В. Кириллов

Самарский национальный исследовательский университет имени С.П. Королёва, 443086, Московское шоссе, 34, Самара, Россия

Аннотация

В работе рассматриваются вопросы, связанные с проектированием и разработкой систем автоматизированного управления контролем доступа на основе ролей в комплексных системах управления предприятием и представляется подход к проектированию таких систем на основе понятия замыкания подсистем управления доступом и подсистемы реализующую основную бизнес-логику системы.

Ключевые слова: контроль доступа на основе ролей; событийно-обусловленное делегирование полномочий; комплексные системы управления предприятиям

1. Введение

Предметом исследования являются автоматизированные системы особого класса – комплексные автоматизированные системы управления предприятием (КСУП). Такие системы характеризуются тем, что содержат в себе всю информацию о предприятии как объекте управления. С точки зрения управления политикой безопасности, в системах такого класса содержится вся необходимая для принятия решения о предоставлении/непредставлении доступа субъекту к выполнению тех или иных бизнес-функций. Однако, в настоящее время, возможности использования этой информации используются недостаточно – в итоге КСУП оказываются незамкнутыми относительно подсистемы разграничения доступа.

Предложенный автором событийно-обусловленный подход к делегированию и отзыву полномочий [1] в контроле доступа на основе ролей [2,3] используется как базовый для замыкания КСУП относительно подсистемы разграничения доступа и реализации, таким образом контекстно-зависимой системы разграничения доступа. Под *контекстом* в данном случае понимается совокупность бизнес-объектов системы, их состояний и атрибутов, а также информации о внутреннем состоянии системы в целом и информации о состоянии внешней по отношению к системе среды, влияющей на систему. Само понятие не замкнутости КСУП относительно подсистемы разграничения доступа можно пояснить следующим образом:

1. роли описываются в контексте понятий и существуют внутри системы КСУП, но их смысловая нагрузка формируется вне системы. Фактически, получаем роль – искусственно введенное понятие в системе.
2. пользователь также как и роль функционирует и описывается в рамках системы. Но связь между пользователем-субъектом системы и *персоной* как субъектом реального мира описывается опосредованно.
3. процессы изменения состояния самой системы и изменения отношений между компонентами подсистемы разграничения доступа параллелен;
4. субъект, осуществляющий управление системой разграничения доступа (администратор системы, офицер безопасности) является внешним субъектом по отношению к системе

2. Типовая модель КСУП в контексте контроля доступа на основе ролей

Рассмотрим схематичное представление типичной КСУП, с точки зрения исследуемых понятий (рисунок 1). Как видно из предложенной схемы, несмотря на то, что пользователи и роли также, как и бизнес-объекты присутствуют в хранилище данных КСУП их непосредственная связь с бизнес-объектами не прослеживается. С другой стороны, в идеале такая схема должна трансформироваться в архитектуру, представленную на рисунке. 2.

Неформально, сущность представленной схемы можно описать следующим образом. Для любого пользователя или роли в системе КСУП, есть некоторое отображение на множество бизнес-объектов этой системы, содержащих полную информацию об этих компонентах в контексте системы. С точки зрения бизнес-логики КСУП, непосредственно пользователь или роль это внешние субъекты, то есть для логики работы КСУП эти субъекты не имеют никакого существенного смысла. КСУП обрабатывает, хранит и предоставляет бизнес-информацию, таким образом выполняя бизнес-функции. Поэтому с ее точки зрения – эти понятия никак не влияют на ее работу. Условно говоря, если существует хотя бы один пользователь, имеющий хотя бы одну роль, включающую все функции – система с точки зрения логики реализации будет функционировать правильно.

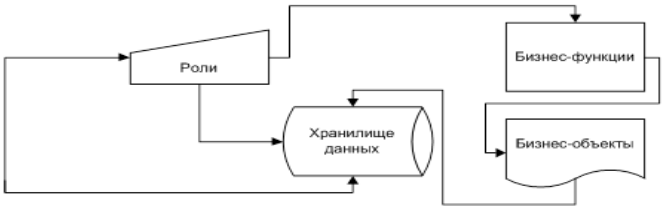

Рис. 1. Типовая архитектура современных КСУП с точки зрения подсистемы безопасности.

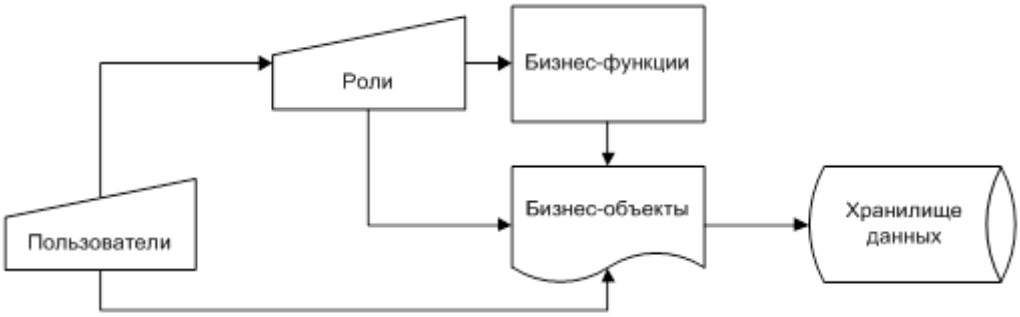

Рис. 2. Замкнутая архитектура КСУП с точки зрения подсистемы безопасности.

Особенность комплексных систем управления предприятием заключается в том, что все компоненты, реализующие политику безопасности, такие как пользователи, роли, операции и отношения между ними – имеют то или иное отображение в понятия и бизнес-объекты системы.

Например:

- пользователи в конечном итоге представляются такими сущностями как сотрудник, клиент, партнер (в зависимости от контекста системы);
- роли представляются сущностями должность, тип клиента, тип партнера и т.д.

Таким образом, используя контекстно-зависимый механизм контроля доступа, можно связать компоненты подсистемы безопасности и компоненты бизнес-логики, таким образом получив возможность замкнуть КСУП относительно реализации политики безопасности.

3. Типовая модель КСУП в контексте контроля доступа на основе ролей

Рассмотрим на примере диаграммы вариантов использования (*Use Case* диаграмма) процесс управления политикой безопасности в типовой КСУП (рисунок 3).

Как видно из схемы, администратор системы (или офицер безопасности) осуществляет управление пользователями и ролями, используя информацию о том, каким образом это требуется делать исходя из некоторой неформально представленной информации о бизнес-функциях и их связях с выполняемой бизнес- операциями. Связь ролей и бизнес-операций осуществляется в зависимости от способа реализации системы – в случае статического множества ролей, данная функция выполняется разработчиком, в случае динамического – также администратором системы.

При построении контекстно-зависимой системы разграничения доступа (КЗСРД) таким образом необходимо решить следующие задачи:

1. Реализовать механизм отображения компонентов подсистемы безопасности на компоненты бизнес-логики;
2. Реализовать механизм синхронизации изменений на уровне бизнес-логики на компоненты подсистемы безопасности.

Отображение компонентов подсистемы безопасности на компоненты бизнес-логики должно выполняться путем выполнения трех типовых операций - синхронизация пользователей, синхронизация полномочий и синхронизация ролей [4].

Синхронизация пользователей – в любой момент времени для любого пользователей из множества пользователей *имеется* один или более бизнес-объект, однозначно соответствующий этому объекту. Такими сущностями могут выступать сотрудник, клиент, партнер и т.п.

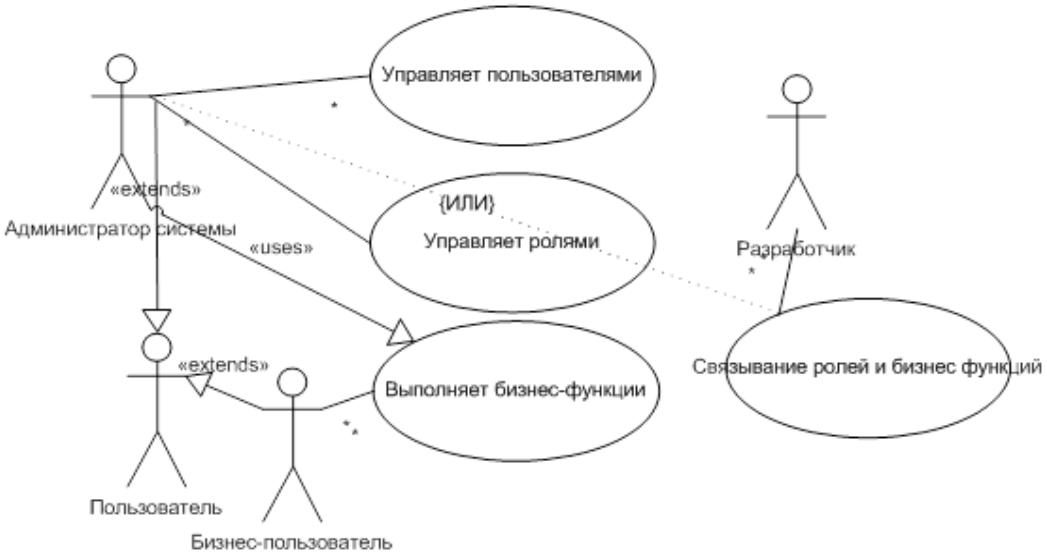

Рис. 3. Use-case диаграмма управления политикой безопасности в типовой КСУП.

Соответствие может быть достигнуто следующими путями:

- Элементы множества *U* порождаются в результате порождения соответствующей сущности бизнес-функцией, с одновременным созданием связи.
- Элементы множества *U* порождаются независимо от выполнения порождения сущности бизнес-функцией, но до тех пор, пока не будет однозначно установлено соответствие между сущностью и элементом множества *U* – данный элемент не может быть активирован. В этом случае, механизм отложенного связывания должен быть формализован и строится на основе полной и достаточной информации связанной как с элементом множества *U*, так и с сущностью создаваемой бизнес-функцией.
- Элементы множества *U* удаляются, если ассоциированная с ними сущность перестает существовать в контексте понятий бизнес-объектов
- Элементы множества *U* блокируются, если ассоциированная с ними сущность перестает быть активной в контексте понятий бизнес-объектов.

Синхронизация ролей – в любой момент времени для любого элемента множества ролей имеется один или более бизнес-объект, однозначно соответствующий этому компоненту. Такими сущностями могут выступать должности, категории должностей, сущности ассоциированные с видами партнеров, клиентов и иных контрагентов, которым предоставляется доступ к системе.

Соответствие может быть достигнуто следующими путями:

- Элементы множества ролей порождаются в результате порождения соответствующей сущности бизнес-функцией, с одновременным созданием связи. Данный способ подходит тогда, когда множество ролей формируются динамически.
- Элементы множества ролей порождаются независимо от выполнения порождения сущности бизнес-функцией. В этом случае, механизм отложенного связывания должен быть формализован и строится на основе полной и достаточной информации связанной как с элементом множества ролей, так и с сущностью создаваемой бизнес-функцией. Данный способ применим тогда, когда, либо множество ролей статичное, либо формирование и связывание ролей с бизнес-операциями происходит независимо от контекста (например, в промышленных КСУП при статическом связывании ролей с бизнес-операциями).

При втором варианте реализации существует несколько возможных вариантов задания соответствия. В простейший из них это матрица, в которой строками являются бизнес-объекты, а столбцами роли (маркер *e* означает в данном случае наличие связи, рисунок 4). В случае необходимости, данная матрица может быть представлена в более сложной древовидной структуре, что может значительно упростить формирование соответствия при наличии иерархии ролей.

	r_1	r_2	…	r_k
bo_1	E			
bo_2		e		e
…				
bo_n				e

Рис. 4. Матрица задания соответствий ролей и бизнес-объектов.

Альтернативным вариантом является задание правил определения соответствия, в том случае если эти правила достаточны и непротиворечивы для определения соответствия (например, в качестве способа заданий правил может использоваться язык описания правил *СОДОП)*.

В предлагаемом подходе к реализации контекстно-зависимой КСУП предполагается использование обоих вариантов – первый вариант используется при формировании постоянной иерархии ролей, второй подход используется для формирования временных ролей и при использовании событийно-обусловленного делегирования и отзыва полномочий.

Связывание бизнес-функций с ролями осуществляется в результате специального процесса получившего название *инжиниринг ролей*. Данный процесс фактически заключается в формализации политики безопасности в терминах конкретной КСУП. В зависимости от того используется статическое или динамическое множество ролей бизнес-функции связываются с ролями либо фиксировано либо гибко. В первом случае, внесение изменений в множество связанных с той или иной ролью бизнес-функций может осуществляться только путем изменения функционала самих бизнес функций, во втором случае изменять множество функций связанных с той или иной ролью можно без изменения функционала самой системы.

В предлагаемом варианте реализации КЗСРД предполагается динамическое связывание бизнес-функций с ролями. Для этого предлагается использование параметрическое связывание бизнес-операций на основании атрибутов бизнес-сушностей (по аналогии с атрибутивной моделью КДОР), с возможностью задания условий на параметры бизнес-функций с использованием языка описания правил и условий *СОДОП*.

Кроме механизма явного связывания компонентов подсистемы безопасности с бизнес-субъектами на уровне отношений назначения пользователь-роль для КЗСРД необходимо реализовать механизм неявного связывания, что и характеризует такие системы. Под неявным связыванием понимается наличие таких формальных условий, по которым в некоторый момент времени некоторому пользователю предоставляется доступ не на основании назначенных ему ролей, а исходя из этих условий и текущего состояния системы КСУП.

Для реализации этого механизма предлагается механизм *СОДОП,* который в отличии от контекстно-зависимой модели КДОР реализуется на базе стандартной модели КДОР и соответственно может применяться в любых системах, реализующих КДОР. В отличии от других моделей делегирования полномочий, СОДОП позволяет реализовывать неявный процесс делегирования без непосредственного привлечения субъекта делегирующего полномочия. Кроме того, применение СОДОП для решения поставленных задач не требует внесения изменений в основную иерархию ролей.

3. Заключение

Таким образом, заключая проведенный анализ исследуемой предметной области, можно сделать следующие выводы:

1. Контекстно-зависимая система разграничения доступа позволяет замкнуть КСУП относительно подсистемы безопасности;
2. КЗСРД реализует функции отображения и синхронизации компонентов подсистемы разграничения доступом и бизнес-объектов;

3. КЗСРД позволяет задавать условия предоставления доступа пользователям исходя из описанных условий, текущего состояния системы (контекста) и свойств компонентов подсистемы безопасности без изменения текущей структуры и иерархии ролей;

4. КЗСРД может быть реализована либо на базе стандартного функционала КДОР практически любой КСУП либо самостоятельно.

Литература

[1] Кириллов, Д.В. Методика построения пространства решений в модели автоматизированного управления доступом на основе ролей / Д.В. Кириллов // Ползуновский вестник. – 2014. № 2. – С. 242-247.

[2] Sandhu, R. Role-based access control models / R. Sandhu, E. Coyne, H. Feinstein, C.Youman // IEEE Computer. – 1996. Vol. 29(2). – P. 38-47.

[3] Sandhu, R. The NIST Model for Role-Based Access Control: Towards a unified standart / Sandhu, R., Kuhn R., Ferraiolo D / Proceedings of the fifth ACM workshop on Role-based access control ACM Workshop on Role-Based Access Control. – 2000. 1 – P. 47-63. DOI: 10.1145/344287.344301.

[4] Кириллов, Д.В. Основные принципы событийно-обусловленного делегирования и отзыва полномочий в системах контроля доступа на основе ролей / Д.В. Кириллов // Вестник Уфимского государственного авиационного технического университета. – 2012. №1 – С. 218-225.