УДК 004.056

Д.В. Кириллов

Классификация моделей делегирования полномочий в контроле доступа на основе ролей

Обсуждаются проблемы, связанные с классификацией существующих моделей делегирования полномочий. Представляется подход к классификации, основанный на выделении типичных характеристик существующих моделей.

Ключевые слова: контроль доступа на основе ролей, делегирование полномочий, модели делегирования полномочий, характеристики моделей делегирования полномочий.

Модели делегирования полномочий достаточно широко применяются для реализации принципов организационного управления в автоматизированных информационных системах, использующих в качестве механизма разграничения полномочий контроль доступа на основе ролей (КДОР) [1]. Однако зачастую возникает вопрос, какой модели отдать предпочтения для наибольшего соответствия стоящим перед предприятием задачам. Кроме того, аналогичные вопросы возникают и при синтезе новых моделей делегирования полномочий. Автором было проведено исследование существующих моделей делегирования полномочий в контексте КДОР и на основе полученных результатов были выделены некоторые общие признаки моделей, которые могут быть использованы как классификационные.

В контексте КДОР модели делегирования полномочий могут быть классифицированы по следующим характеристикам:

1) *по направлению делегирования полномочий* выделяют делегирования видов «пользователь–пользователь», «роль–роль», «пользователь–роль», «роль–пользователь»;

2) *по продолжительности делегирования полномочий* – постоянное и временное;

3) *по объему делегируемых полномочий* – полное (делегирование роли) и частичное (делегирование полномочий) делегирование;

4) *по области применения в контексте КДОР* – делегирование в «плоском» КДОР, в иерархическом КДОР (в свою очередь разделяющееся на нисходящее, восходящее и кросс-делегирование), и в КДОР с ограничениями;

5) *по возможности переделегирования полномочий* – одношаговое и многошаговое;

6) *по сохранению делегированных полномочий у делегирующего пользователя* – с сохранением и без сохранения полномочий;

7) *по механизму отзыва полномочия* подразделяется в свою очередь по видам.

Обобщенная схема классификации представлена на рис. 1.

Рассмотрим сущность каждой из использованных классификационных характеристик.

Под направленностью делегирования полномочий понимают то, кто выступает в качестве субъекта делегирующего полномочия и кто выступает в качестве субъекта делегата. Здесь возможны следующие варианты:

1) *«пользователь–пользователь»* – в этом случае пользователь, делегирующий полномочия, делегирует их некоторому конкретному пользователю;

2) *«роль–роль»* – подразумевает использование в виде предусловий, ограничивающих делегирование, отношений вида $can_delegate \subseteq ROLES \times ROLES$, т.е. для всех членов некоторой роли допускается делегировать полномочия только пользователям, ассоциированным с некоторым подмножеством множества ролей;

3) *«пользователь–роль»* – подразумевает использование в виде предусловий, ограничивающих делегирование, отношений вида $can_delegate \subseteq USERS \times ROLES$, т.е. для некоторого пользователя допускается делегировать полномочия только пользователям, ассоциированным с некоторым подмножеством множества ролей;

4) *«роль–пользователь»* – подразумевает использование в виде предусловий, ограничивающих делегирование, отношений вида $can_delegate \subseteq ROLES \times USERS$, т.е. для всех членов некоторой роли допускается делегировать полномочия только некоторым пользователям.

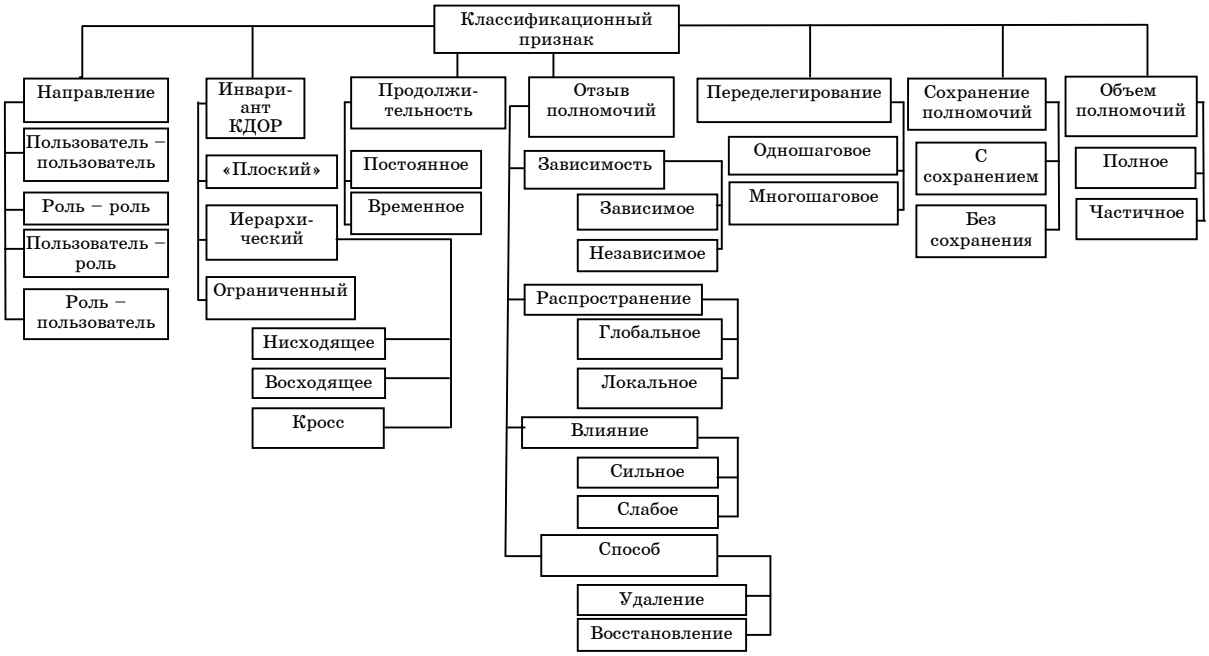

Рис. 1. Классификация моделей делегирования полномочий

Под продолжительностью делегирования подразумевается наличие или отсутствие ограничений на время делегирования полномочий. Здесь возможно два варианта:

1) Постоянное делегирование – срок, на который делегируются полномочия, не ограничивается.

2) Временное делегирование – при выполнении операции делегирования указывается временное ограничение, используемое для автоматического отзыва полномочий.

Под объемом делегирования полномочий понимается то, в каком виде осуществляется делегирование полномочий. Допустимо два варианта:

1) Полное – в этом случае делегируется часть полномочий, возможно не ассоциированных одновременно с одной и той же ролью.

2) Частичное.

По области применения в контексте КДОР подразумевается то, в контексте какого инварианта модели КДОР возможно применение данной модели делегирования полномочий, соответственно здесь возможны следующие варианты:

1) *делегирование в «плоском» КДОР* – подразумевает делегирование в контексте модели *RBAC0;*

2) *в иерархическом КДОР* – подразумевает применение в модели *RBAC1* и в свою очередь, по направленности делегирования полномочий в контексте иерархии ролей подразделяется на:

а) *нисходящее* – допускается делегирование вниз по иерархии;

б) *восходящее* – допускается делегирование вверх по иерархии;

в) *кросс-делегирование* – допускается делегирование между различными ветвями иерархии ролей;

3) *КДОР с ограничениями* – подразумевает применение в моделях *RBAC2* и *RBAC3*.

Под возможностью переделегирования полномочий понимается поддержка формирования цепочек делегирования полномочий, при которой ранее делегированные полномочия могут быть впоследствии делегированы другому пользователю или роли. Здесь возможно два варианта:

1) *Одношаговое делегирование* – не подразумевает дальнейшего делегирования ранее делегированных полномочий.

2) *Многошаговое делегирование* – подразумевает возможность переделегировать полномочия.

По возможности сохранения делегированных полномочий у делегирующего пользователя модели могут быть следующих двух видов:

1) *С сохранением* – в рамках данного вида модели пользователь, делегировавший членство в роли, сохраняет собственное членство в ней, либо, в случае частичного делегирования полномочий, сохраняет эти полномочия.

2) *Без сохранения* – в данном случае пользователь, делегировавший членство в роли, теряет свое членство в ней либо теряет полномочия в случае их делегирования.

Модели делегирования полномочий также можно классифицировать по механизму отзыва полномочий. Здесь возможно выделить следующие классификационные признаки:

По зависимости от делегировавшего пользователя – в данном случае подразумевается, наличие или отсутствие ограничения на субъектов, имеющих право на отзыв полномочий. Выделяется два возможных варианта:

1) *Зависимое* – в данном случае делегированные полномочия может отозвать только тот субъект, кто эти полномочия делегировал, либо офицер безопасности системы.

2) *Независимое* – в данном случае делегированные полномочия может отозвать любой пользователь в роли, совпадающей или старшей по отношению к роли пользователя, делегировавшего полномочия.

По распространению отзыва делегированных полномочий – в данном случае подразумевается масштаб распространения процедуры отзыва полномочий. Здесь выделяется два вида:

1) *Глобальное* – в этом случае отзываются не только полномочия в рамках заданной цепочки делегирования, но и полномочия, связанные с ними.

2) *Локальное* – в этом случае отзыв полномочий распространяется только на заданную цепочку делегирования.

По способу отзыва полномочий – в данном случае подразумевается то, каким образом отзываются полномочия. Выделяется два вида:

1) *Восстановление* – в данном случае полномочия, отзываемые у пользователя или роли, восстанавливаются у делегировавших их пользователей или ролей.

2) *Удаление* – в данном случае, отозванные полномочия не восстанавливаются у пользователей или ролей, делегировавших полномочия.

Модели могут комбинировать различные характеристики, и в данном случае образуется так называемая матрица возможностей конкретной модели, дополняемая также некоторыми характеристиками, такими как возможность использования правил делегирования, атрибутов компонентов, возможность реакции на возникновение событий. Все эти показатели будут использованы далее при сравнении моделей.

В результате рассмотрения моделей делегирования полномочий КДОР [2–5], был произведен сравнительный анализ их классификационных характеристик, а также некоторых дополнительных особенностей, оказывающих влияние на их область применимости и функциональные задачи, которые могут быть решены с их использованием. В таблице представлены полученные результаты анализа.

Результаты сравнительного анализа моделей делегирования

По делегированию	RBDM	ABDM	PBDM	AbiBDM	PRBDM	RDM2000	ABDMx	PCBDM	AGBDM
Направление	П–П	П–П, П–Р	П–Р	П–Р	П–Р	П–П, П–Р	П–П, П–Р	П–П, П–Р	П–П, П–Р
Инвариант КДОР	0,1	0,1	0,1	0,1,2,3	0,1,2,3	0,1,2,3	0,1,2,3	0,1,2,3	0,1,2,3
Продолжительность делегирования	П, В	П, В	В	В	В	В	В	В	В
Переделегирование	–	–	–	+	+	+	+	+	+
Сохранение полномочий	+	+	+	+	+/–	+	+	+/–	+/–
Объем полномочий	П	Ч	Ч	Ч	Ч	Ч	Ч	Ч	Ч
Классификация по отзыву									
Зависимость	–	–	–	–	+	+	+	+	+
Распространение	Л	Л	Л	Л	Л	Г	Л	Л	Л
Влияние	СЛ	СЛ	СЛ	СЛ	СЛ	СЛ	СИЛ	СИЛ	СЛ
Способ	У	У	У	У	У	У/В	У/В	В	В
Дополнительные характеристики									
Поддержка атрибутов	–	П	–	П, Р	–	–	П,Р	П,Р	–
Поддержка событий	–	–	–	–	–	–	–	–	–
Поддержка правил	–	–	–	–	–	+	–	–	–
Многоуровневые роли	–	–	–	–	–	–	–	+	–
Дополнительные условия делегирования	–	+	+	+	+	+	+	+	+

По результатам анализа моделей можно сделать следующие выводы:

1) Все рассмотренные модели реализуются на основе стандартных инвариантов модели КДОР и не используют возможности, связанные с использованием расширенных моделей, а именно поддержки механизма событий, сведений о контексте и окружении системы и т.д.;

2) Применение моделей делегирования в реальных АС по сути ограничено базовыми моделями RBDM0 и RBDM1. О реализации остальных моделей автору не удалось найти каких-либо сведений.

3) Тем не менее некоторые модели могут использоваться в качестве основы для разработки более функциональной модели, решающей поставленные задачи.

Литература

1. Role-based access control models / R. Sandhu, E. Coyne, H. Feinstein, and C Youman // IEEEComputer. – 1996. – № 29 (2). – P. 38–47.

2. Barka E. A role-based delegation model and some extensions / E. Barka, R. Sandhu // Proceedings of Sixteenth Annual Computer Security Applications Conference (ACSAC' 00). – 2000. – P. 168–177.

3. A role-based delegation model using role hierarchy supporting restricted permission inheritance / JongSoon Park, YoungLok Lee, HyungHyo Lee, and BongNam Noh. // Proceedings of the International Conference on Security and Management, SAM '03. – Las Vegas, Nevada, USA: CSREA Press, 2003. – P. 294–302.

4. Role-based cascaded delegation / Roberto Tamassia, Danfeng Yao, and William H. Winsborough // Proceedings of the 9th ACM Symposium on Access Control Models and Technologies. – Yorktown Heights, New York, USA, 2004. – P. 146–155.

Кириллов Денис Викторович
Ст. преп. каф. безопасности информационных систем, зав. сектором разработки и поддержки ИАИС Самарского государственного университета, г. Самара
Тел.: (846) 278-09-16
Эл. адрес: kirillov@ssu.samara.ru

D.V. Kirillov

A classification of role-based delegation models.

Classifications problems of existing role-based delegation models in context of role-based access control are discussed. Presenting approach on classification based on distinguishing of the most useful characteristics of delegation models.

Keywords: role-based access control, delegation, delegation models, characteristics of delegation models.