МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

DOI 10.17223/20710410/17/8

УДК 004.94

ПОСТРОЕНИЕ ИЕРАРХИЧЕСКОГО РОЛЕВОГО УПРАВЛЕНИЯ ДОСТУПОМ

Д. Н. Колегов

Национальный исследовательский Томский государственный университет, г. Томск, Россия

E-mail: d.n.kolegov@gmail.com

Предлагается подход к построению ролевого управления доступом для компьютерных систем с иерархией сущностей, отражающей установленные организационно-управленческие отношения. Формулируются определения базовых элементов и механизмов иерархической ролевой модели, развивающей семейство моделей ролевого управления доступом *RBAC* и, в отличие от них, позволяющей использовать уровни иерархии сущностей при задании и проверке разрешённых прав доступа субъектов к сущностям на основе модели полурешётки.

Ключевые слова: *модели безопасности, ролевое управление доступом, модель RBAC, иерархия сущностей.*

Введение

Важнейшим механизмом обеспечения безопасности большинства существующих компьютерных систем (КС) является механизм логического управления доступом и информационными потоками, традиционно реализуемый в операционных системах (ОС), системах управления базами данных (СУБД) и автоматизированных системах управления (АСУ). Функционирование такого механизма КС заключается в проверке имеющихся у субъекта прав доступа к сущности и последующем разрешении или запрещении соответствующего доступа. Способ задания разрешённых прав доступа субъектов к сущностям и правил их проверки регламентируется реализуемой в КС политикой управления доступом и информационными потоками, являющейся составной частью политики безопасности КС. Традиционно в КС используются дискреционные, мандатные и ролевые виды политик управления доступом.

В настоящее время наиболее широкое развитие и распространение получил механизм ролевого управления доступом, применяемый в основном в ОС с высоким уровнем безопасности, а также системах защиты СУБД и АСУ.

Как правило, при построении и реализации ролевого механизма управления доступом используется стандартизованная Национальным институтом стандартов и технологий (NIST) США модель *RBAC* [1], разработанная на основе классических моделей ролевого управления доступом [2, 3]. Ролевое управление доступом является достаточно сложным механизмом обеспечения безопасности как с точки зрения научного обоснования свойств его безопасности, так и с учётом особенностей его практической реализации. В реальных КС, в которых одновременно могут работать сотни пользователей, структура ролей может быть очень сложной, а количество различных прав

доступа значительным, проблема реализации и администрирования системы ролевого управления доступом является чрезвычайно важной задачей [4]. Для учёта различных особенностей и условий функционирования современных КС предложено множество модификаций и расширений моделей семейства $RBAC$, как развивающих, так и дополняющих их основные положения элементами и механизмами других моделей [5 – 8].

В то же время в моделях ролевого управления доступом семейства $RBAC$, как и в других известных ролевых моделях и их расширениях, не учитываются следующие особенности функционирования современных КС, затрудняющие и делающие неэффективной реализацию ролевой политики управления доступом:

— иерархичность и распределённость компонент КС;
— наличие идентичной структуры распределённых компонент КС;
— необходимость определения одинаковых правил управления доступом для распределённых компонент КС;
— возможность использования уровней иерархии КС при задании разрешённых прав доступа субъектов к сущностям и правил их проверки;
— существование нескольких иерархий в КС и наличие различных правил управления доступом для одних тех же субъектов и сущностей в зависимости от уровня заданной иерархии;
— необходимость создания большого числа ролей для реализации политики управления доступом;
— необходимость гибкого и масштабируемого задания разрешённых прав доступа субъектов к сущностям при изменении их уровней в иерархии КС, а также при добавлении в КС новых ролей, прав доступа и сущностей.

С целью развития и адаптации моделей логического управления доступом и информационными потоками к свойствам и условиям функционирования реальных КС в работе описываются базовые элементы и механизмы модели иерархического ролевого управления доступом для компьютерных систем с иерархией сущностей, отражающей установленные организационно-управленческие отношения и позволяющей использовать уровни иерархии сущностей при задании и проверке разрешённых прав доступа субъектов к сущностям на основе модели полурешётки.

1. Оценка сложности применения моделей ролевого управления доступом семейства $RBAC$ для КС с иерархией сущностей

Пусть имеется организация с иерархической структурой своих подразделений, эксплуатирующая некоторую распределенную КС. В соответствии с установленными организационно-управленческими отношениями и заданной политикой безопасности КС пользователи должны иметь некоторые виды прав доступа к данным своего подразделения, определяемые их функциональными и должностными обязанностями. При этом сотрудники вышестоящего по организационно-штатной структуре подразделения должны иметь права доступа к данным нижестоящих (подчинённых) подразделений, а сотрудники нижестоящих подразделений не должны получать права доступа к данным вышестоящих подразделений. Таким образом, в соответствии с требованиями политики безопасности управления доступом предоставление прав доступа зависит от уровней сущностей в иерархии КС и полномочий пользователя.

Оценим сложность реализации ролевого управления доступом рассматриваемой КС для моделей $RBAC_0$ и $RBAC_1$. Для простоты изложения рассмотрим граничный случай, когда иерархическая структура организации представляется полным

бинарным деревом высоты H, а узлами дерева являются классы разбиения множества сущностей.

Пусть N — количество должностей пользователей КС, тогда в рамках модели $RBAC_0$ число ролей, необходимое для реализации политики управления доступом, равно $M = N(2^{H+1} - 1)$. При добавлении нового подразделения в структуру КС необходимо будет добавить N ролей. С учётом того, что в реальных КС число прав доступа и сущностей доступа, определяемых ролью, может исчисляться сотнями, применение модели $RBAC_0$ в таких КС является неэффективным и сложно реализуемым.

Использование модели $RBAC_1$ позволяет более эффективно реализовать политику управления доступом. В этом случае необходимо построить N двоичных деревьев иерархии ролей, аналогичных дереву иерархии КС, с числом вершин $2^{H+1}-1$. Применение модели $RBAC_1$ позволяет более просто организовать назначение ролей и прав доступа пользователям, но требует построения и администрирования нескольких иерархий ролей.

Неэффективным оказывается применение моделей $RBAC$ для реализации ролевого управления доступом в КС с иерархией сущностей в следующих случаях:

— переподчинение подразделений;
— добавление новых сущностей во все подчинённые подразделения;
— добавление нового или удаление существующего права доступа к идентичным сущностям для всех подчинённых подразделений.

Таким образом, подход, основанный на применении моделей семейства $RBAC$ для реализации ролевой политики управления доступом в КС с иерархией сущностей, отражающей установленные организационно-управленческие отношения, не является оптимальным.

2. Определение политики иерархического ролевого управления доступом

Пусть имеется некоторая КС с заданной на ней древовидной иерархической структурой и для каждой сущности определён её уровень иерархии. В качестве одного из атрибутов, используемых при управления доступом, рассмотрим уровень иерархии сущности и на его основе определим политику управления доступом в КС. Основная идея такой политики заключается в назначении всем сущностям уровней иерархии в соответствии со структурой КС и предоставлении субъекту права доступа к сущности только в том случае, если уровень иерархии субъекта не меньше уровня иерархии сущности. При этом на множестве иерархии сущностей должна быть задана верхняя полурешётка (далее — полурешётка).

Таким образом, политика иерархического управления доступом — это политика, соответствующая следующим основным требованиям управления доступом в КС:

1) все сущности должны быть идентифицированы;
2) задана полурешётка уровней иерархии КС;
3) для каждой сущности определён уровень её иерархии в КС, задающий ограничения на доступ субъектов к сущностям;
4) субъект обладает правом доступа к сущности КС в том и только в том случае, если уровень иерархии субъекта не меньше уровня иерархии сущности.

Политика иерархического управления доступом, основываясь только на уровнях иерархии сущностей, обладает свойством избыточности разрешённых прав доступа субъектов к сущностям. Для выполнения принципа наименьших привилегий при доступе субъектов с высоким уровнем иерархии к сущностям с низким уровнем иерархии

положения введённой политики управления доступом добавляются к положениям политики ролевого управления доступом. При этом используется механизм задания типа сущности, понимаемого как атрибут сущности, используемый при реализации некоторого метода управления доступом в качестве аналога права доступа [10]. Механизм типов сущностей позволяет сформировать роли, в которых права доступа к сущностям группируются по их типу, что позволяет задавать права доступа субъектов ко всем сущностям одного типа, в том числе к сущностям с разными уровнями иерархии по отношении к субъекту, одновременно.

Определение 1. Политика иерархического ролевого управления доступом — это политика, соответствующая следующим основным требованиям управления доступом в КС:

1) все сущности должны быть идентифицированы;
2) задана полурешётка уровней иерархии КС и каждой сущности присвоен уровень иерархии;
3) определено множество типов сущностей и для каждой сущности указан её тип;
4) задано множество ролей, каждая из которых представляет собой некоторое множество прав доступа к сущностям определённого типа;
5) каждый субъект обладает некоторым множеством разрешённых для данного субъекта ролей;
6) субъект обладает правом доступа к сущности КС в том и только в том случае, если субъект обладает ролью, в множестве прав доступа которой имеется данное право доступа к сущности данного типа, и уровень иерархии субъекта не меньше уровня иерархии сущности.

3. Определение модели иерархического ролевого управления доступом

Определение 2. Модель, описывающую политику иерархического ролевого управления доступом, будем называть иерархической ролевой моделью управления доступом в КС и обозначать *RBAC-H*. Основными элементами данной модели являются:

— $E = O \cup C$ — множество сущностей, где O — множество объектов, C — множество контейнеров и $O \cap C = \varnothing$;
— U — множество пользователей, при этом пользователи по определению не являются сущностями ($U \cap E = \varnothing$);
— $S \subseteq E$ — множество субъект-сессий пользователей;
— T — множество типов сущностей;
— L — множество уровней иерархии сущностей;
— R_r — множество видов прав доступа;
— R — множество ролей;
— $P \subseteq (R_r \times T) \cup (R_r \times E)$ — множество прав доступа ко всем сущностям одного типа и отдельным сущностям;
— $PA : R \to 2^P$ — функция прав доступа ролей, задающая для каждой роли множество прав доступа к сущностям, при этом для каждого права доступа $p \in P$ существует роль $r \in R$, такая, что выполняется условие $p \in PA(r)$;
— $UA : U \to 2^R$ — функция авторизованных ролей пользователей, задающая для каждого пользователя множество ролей, на которые он может быть авторизован;
— $type : E \to T$ — функция типов сущностей;
— $f_e : E \to L$ — функция, задающая уровень иерархии каждой сущности;

— $user : S \to U$ — функция принадлежности субъект-сессии пользователю, задающая для каждой субъект-сессии пользователя, от имени которого она активизирована;
— $roles : S \to 2^R$ — функция, задающая для пользователя множество ролей, на которые он авторизован в текущей сессии, при этом в каждом состоянии КС для каждой субъект-сессии $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s))$.

Определение 3. Пусть X — заданное разбиение множества E в соответствии с заданной иерархией сущностей, при этом $|X| = |L|$. Доменом d сущностей множества E будем называть всякий класс из X.

Иерархией доменов назовём заданное на множестве X отношение частичного порядка $\leqslant$, удовлетворяющее следующим условиям:

— если для $d \in X$ существуют $d_1, d_2 \in X$, такие, что $d \leqslant d_1$, $d \leqslant d_2$, то $d_1 \leqslant d_2$ или $d_2 \leqslant d_1$;
— в X существует наибольший элемент.

Описанная иерархия доменов соответствует КС с иерархической древовидной структурой, отражающей организационно-управленческие отношения, и задаёт верхнюю полурешётку $(X, \leqslant)$.

Пусть L — заданное множество уровней иерархии сущностей и существует биективное отображение X на L. Определим на множестве L отношение частичного порядка $\leqslant$, где для любых $l_1, l_2 \in L$ верно: $l_1 \leqslant l_2$ тогда и только тогда, когда $d_1 \leqslant d_2$ для соответствующих $d_1, d_2 \in X$, тогда $(L, \leqslant)$ — верхняя полурешётка уровней иерархии сущностей.

Аналогично модели $RBAC$ будем предполагать, что множества U, X, T, L, P, R, R_r и функции UA, PA, $type$ не изменяются с течением времени.

Определение 4. Пусть имеются множества E, S, X, U, T, P, R, R_r, функции PA, UA, $type$, $user$, $roles$ и $(L, \leqslant)$ — полурешётка уровней иерархии. Определим предикат $can\_access(s, e, p)$, истинный тогда и только тогда, когда выполняются следующие условия:

— $f_e(e) \leqslant f_e(s)$;
— $(p, type(e)) \in PA(roles(s))$.

Определение 5. Будем говорить, что в КС реализовано иерархическое ролевое управление доступом *RBAC-H*, если любая субъект-сессия $s \in S$ пользователя $user(s) \in U$ может обладать правом доступа $p \in R_r$ к сущности $e \in E$ тогда и только тогда, когда истинен предикат $can\_access(s, e, p)$.

Одним из важных механизмов семейства моделей ролевого управления доступом являются ограничения, накладываемые на множества ролей, на которые может быть авторизован пользователь или на которые он авторизуется в течение одной сессии. Основные ограничения, определённые в рамках моделей ролевого управления доступом семейства $RBAC$ [4], могут быть перенесены в предложенную модель. В то же время для большего соответствия иерархического управления доступом процедурам обработки данных, используемым в реальных КС, необходимо определить новые виды ограничений, существенные именно для данного вида управления доступом.

Определим функцию $h : E \to X$, такую, что $h(e) = d$, если $e \in d$, где $e \in E$ и $d \in X$.

Определение 6. Будем говорить, что в модели *RBAC-H* заданы ограничения на область доступа пользователя в иерархии сущностей, если выполняются следующие условия:

Условие 1. Определена функция $UD : U \to 2^X$.

Условие 2. Для любых $s \in S$, $e \in E$, $p \in R_r$ если истинен предикат $can\_access(s, e, p)$ и $user(s) = u$, то $h(e) \in UD(u)$.

Определение 7. Будем говорить, что в модели *RBAC-H* заданы ограничения на область авторизации ролей в иерархии сущностей, если выполняются следующие условия:

Условие 1. Определена функция $RD : R \to 2^X$.

Условие 2. Для любых $s \in S$, $e \in E$, $p \in R_r$ если истинен предикат $can\_access(s, e, p)$ и $r \in roles(s)$, то $h(e) \in RD(r)$.

Определение 8. Будем говорить, что в модели *RBAC-H* заданы ограничения на область авторизации ролей пользователя в иерархии сущностей, если выполняются следующие условия:

Условие 1. Определена функция $URD : U \times R \to 2^X$.

Условие 2. Для любых $s \in S$, $e \in E$, $p \in R_r$ если истинен предикат $can\_access(s, e, p)$, $user(s) = u$ и $r \in roles(s)$, то $h(e) \in URD(u, r)$.

Определение 9. Будем говорить, что в модели *RBAC-H* заданы ограничения на область применения прав доступа в иерархии сущностей, если выполняются следующие условия:

Условие 1. Определена функция $PD : P \to 2^X$.

Условие 2. Для любых $s \in S$, $e \in E$, $p \in R_r$ если истинен предикат $can\_access(s, e, p)$, то $h(e) \in PD(p)$.

Определение 10. Будем говорить, что в модели *RBAC-H* заданы ограничения на область доступа к типу сущностей в иерархии сущностей, если выполняются следующие условия:

Условие 1. Определена функция $TD : T \to 2^X$.

Условие 2. Для любых $s \in S$, $e \in E$, $p \in R_r$ если истинен предикат $can\_access(s, e, p)$, то $h(e) \in TD(type(e))$.

Общая структура элементов модели иерархического ролевого управления доступом имеет вид, представленный на рис. 1.

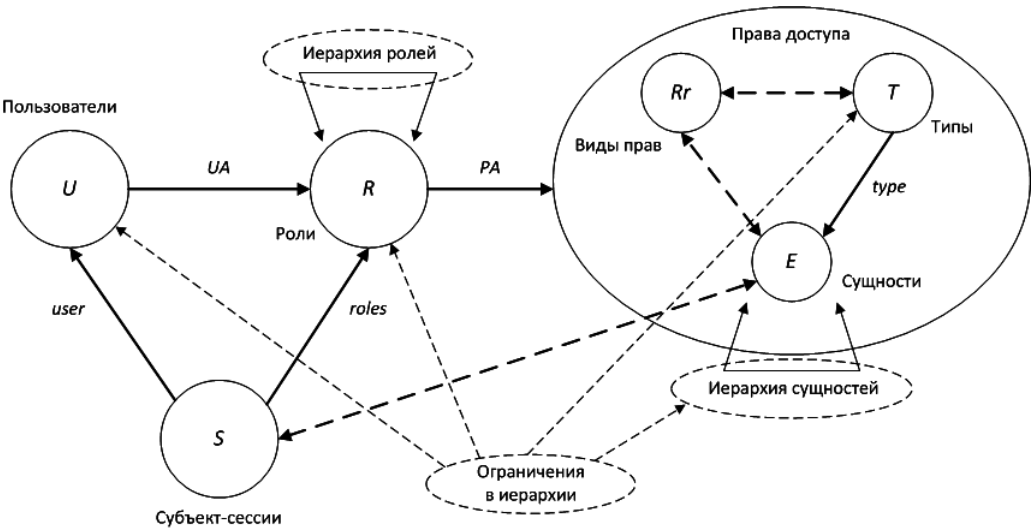

Рис. 1. Структура элементов иерархической ролевой модели *RBAC-H*

Заключение

Предложено описание базовых элементов иерархической ролевой модели управления доступом *RBAC-H*, ориентированной на КС с иерархией сущностей, отражающей установленные организационно-управленческие отношения. Добавление атрибутов иерархии и типов сущностей к элементам моделей *RBAC* позволяет адаптировать последние к условиям функционирования реальных КС, а также существенно упростить реализацию и администрирование систем ролевого управления доступом.

ЛИТЕРАТУРА

1. National Institute of Standards and Technology. Role Based Access Control (RBAC) and Role Based Security [Электронный ресурс]. Режим доступа: `http://csrc.nist.gov/groups/SNS/rbac`.
2. *Ferraiolo D. F. and Kuhn D. R.* Role Based Access Controls // Proc. 15th National Computer Security Conference, Baltimore, October 1992. P. 554–563.
3. *Sandhu R. S., Coyne E. J., Feinstein H. L., and Youman C. E.* Role-Based Access Control Models // IEEE Computer. 1996. No. 29(2). P. 38–47.
4. *Девянин П. Н.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011. 320 с.
5. *Kuhn D. R., Coyne E. J., and Weil T. R.* Adding attributes to role-based access control // IEEE Computer. 2010. No. 43(6). P. 79–81.
6. *Sandhu R. S. and Al-Kahtani MA.* A Model for Attribute-Based User-Role Assignment // Proc. 18th Annual Computer Security Applications Conference (ACSAC'02), Las Vegas, December 09–13, 2002. P. 353.
7. *Joshi J., Bertino E. A, Latif U., and Ghafoor A.* A Generalized Temporal Role-Based Access Control Model // IEEE Trans. Knowledge and Data Engineering. 2005. No. 17(1). P. 4–23.
8. *Bertion E., Catania B., and Damiani M. L.* GEO-RBAC: A Spatially Aware RBAC // Proc. 10th ACM Symposium on Access Control Models and Technologies (SACMAT'05), Stockholm, Sweeden, June 2005. P. 29–37.
9. *Thomas R. K.* Team-based Access Control (TMAC): A Primitive for Applying Role-based Access Controls in Collaborative Environments // Proc. Second ACM Workshop on Role-based Access Control (RBAC'97), Fairfax, Virginia, USA, November 1997. P. 13–19.
10. *Девянин П. Н.* Формирование словаря терминов теории моделирования безопасности управления доступом и информационными потоками в компьютерных системах // Прикладная дискретная математика. 2011. № 2. С. 17–39.