Математические структуры и моделирование
2009, вып. 20, с. 141–152

УДК 65.012.8

СОВМЕСТНАЯ РЕАЛИЗАЦИЯ МАНДАТНОГО И РОЛЕВОГО РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

С.В. Белим, Н.Ф. Богаченко, Ю.С. Ракицкий

В статье анализируется возможность совмещения ролевой и мандатной политик безопасности на основе графовой модели. С этой целью вводится понятие решеточного дерева и обобщается модель ролевого разделения доступа. Приводится простейший алгоритм мандатного разделения доступа, учитывающий концепцию ролей.

1. Введение

Необходимость совмещения различных типов разграничения доступа к информации в корпоративных сетях, как правило, обусловлена требованиями политики безопасности предприятия к хранению и обработке данных. На сегодняшний день общепринятой практикой стало использование систем управления базами данных для организации доступа к ресурсам. Все современные базы данных используют концепцию ролей для выдачи полномочий пользователям, реализуя таким образом ролевое разграничение доступа. Однако в ряде организаций, особенно связанных с защищенным документооборотом, также налагается требование использования меток безопасности и, основанного на них, мандатного разделения доступа. В рамках мандатного разделения доступа множество разрешенных доступов задается неявным образом в виде уровня конфиденциальности для объектов и уровня доверия для субъектов компьютерной системы. Решение о доступе принимается путем сопоставления уровня конфиденциальности и уровня доверия. При использовании концепции ролей задается множество разрешенных системных операций путем введения дополнительных объектов – ролей, наделенных набором разрешенных доступов. Решение о разрешении доступа принимается исходя из роли, сопоставленной субъекту.

Попытки предоставления совмещенных сервисов разграничения доступа (мандатного и ролевого) встроены в ряд систем управления базами данных. Так, например, в широко распространенной СУБД Oracle [4, стр. 54] уже в версии 7 было разработано дополнительное инструментальное средство Trusted

Омский государственный университет.
E-mail: sbelim@mail.ru

Oracle7, которое позволяло администратору кроме ролей вводить также и метки безопасности. Основным требованием мандатного разграничения доступа в данном приложении было доминирование метки пользователя над меткой строки. Начиная с версии СУБД Oracle8 этот продукт получил название Oracle Label Security. Однако оба эти продукта не получили широкой популярности в силу двух причин. Во-первых, согласование настроек двух алгоритмов приводит к большому количеству трудностей при администрировании. Во-вторых, остается неочевидным сама возможность непротиворечивого сосуществования двух принципов разграничения доступа в одной компьютерной системе.

Целью данной статьи ставится развитие модели ролевого разграничения доступа, а также доказательства принципиальной возможности построения политики безопасности, использующей концепцию ролей и мандатное разделение доступа. Также исследуются математические структуры, необходимые для моделирования политики безопасности.

2. Ролевая политика безопасности

Ролевая политика безопасности основывается на разрешении или запрещении действий в системе в целом без привязки к отдельным объектам системы. В общем случае такой подход реализуется с помощью концепции привилегий. Под привилегией понимается единица доступа к системной информации. Будем считать, что системная информация представима с помощью множества объектов $\mathbf{O}$. Роль – это именованная совокупность привилегий, то есть множество разрешенных типов доступа к системным объектам. Множество всех возможных типов доступа к системным объектам обозначим через $\mathbf{A}$. Перейдем к более строгому описанию модели ролевого разграничения доступа, приведенного в работе [6].

Определение 1. Под *привилегией* будем понимать пару (x, m), где x – системный объект ($x \in \mathbf{O}$), а m – непустое множество видов доступа ($m \subseteq \mathbf{A}$).

Определение 2. *Роль* – это именованное множество привилегий, которое в дальнейшем будем представлять в виде пары $(rname, rpset)$, где $rname$ – уникальный идентификатор, $rpset$ – множество привилегий.

Если определена роль r, то ее имя $r.rname$, а множество привилегий – $r.rpset$. Далее введем два множества: R – множество ролей системы, P – множество всех возможных привилегий. Также определим функцию, играющую важную роль в администрировании систем с ролевым разграничением доступа:

$$\Psi : R \to 2^{|P|}.$$

Данное отображение показывает привилегии заданной роли. По сути $\Psi(r) = r.rpset$. Через концепцию ролей осуществляется доступ к системной информации.

Пусть UID – множество идентификаторов пользователей, GID – множество идентификаторов групп пользователей, общее множество идентификаторов, для которых производится ролевое разграничение доступа $ID = UID \cup GID$.

Для систем с ролевым разграничением доступа важную роль играет процесс авторизации. Причем возможны два случая. Авторизация «Роль – Привилегия» включает заданную привилегию в множество привилегий данной роли, то есть, если роль r авторизована на привилегию p, то $p \in r.rpset$. Авторизация «Роль-Роль» подразумевает включение привилегий одной роли в множество привилегий другой роли. То есть, если роль r_1 авторизована на роль r_2, то $r_2.rpset \subseteq r_1.rpset$.

Авторизация «Роль-Роль» порождает бинарное *отношение* на множестве ролей. Обозначим это отношение через $r_1 \to r_2$, если роль r_1 авторизована на роль r_2.

Как показано в работе [6], функция Ψ монотонно возрастает по отношению к операции $\to$, то есть если $r_1 \to r_2$, то $\Psi(r_2) \subseteq \Psi(r_1)$.

Обозначим цепочку вида $r_i \to r_{i_1} \to \ldots \to r_{i_n} \to r_j$ через $r_i \to^+ r_j$ (при $n > 0$) и $r_i \to^* r_j$ (при $n \geqslant 0$).

Определение 3. *Ролевым путем* $p(r_i, r_j)$ между двумя ролями r_i и r_j будем называть цепочку $r_i \to^* r_j$.

Заданному отношению на множестве ролей можно сопоставить ориентированный граф, в котором дуга (r_1, r_2) существует тогда и только тогда, когда роль r_1 авторизована на роль r_2. Очевидно, что ролевой путь $p(r_i, r_j)$ изоморфен ориентированному пути в этом орграфе, ведущему из вершины r_i в вершину r_j.

Определение 4. *Тривиальным* является ролевой путь, состоящий из одной роли, то есть путь нулевой длины из вершины к самой себе.

Определение 5. Будем говорить, что роль r_i *доминирует* над ролью r_j, а роль r_j *подчиняется* роли r_i, если существует ролевой путь $p(r_i, r_j)$. Или в графовой постановке: вершина r_i *доминирует* над вершиной r_j, а вершина r_j *подчиняется* вершине r_i, если существует ориентированный путь $p(r_i, r_j)$.

Легко доказать, что отношение доминирования одной роли над другой задает *отношение частичного порядка* на множестве ролей R. Следует отметить, что возможно два различных случая, зависящих от принципа администрирования ролевой политики безопасности. В первом случае допускается существование ролей с совпадающим набором полномочий. Тогда отношения порядка между ролями нестрогое. Однако такой подход имеет смысл только как временная мера при формировании ролевой политики безопасности. В окончательно сформированной иерархии ролей существование двух ролей с совпадающими полномочиями лишено смысла. Второй случай исключает наличие двух ролей с совпадающими полномочиями. Для данного подхода отношение порядка будет строгим. В дальнейшем будем придерживаться именно второго подхода, обеспечивающего оптимальное управление ролями, но обозначать отношение доминирования роли r_i над ролью r_j как $r_i \geqslant r_j$ (или $r_j \leqslant r_i$).

3. Мандатная политика безопасности

Мандатные политики безопасности строятся основываясь на понятиях уровня секретности информации и уровня доверия к пользователю. Существуют различные подходы, позволяющие определять уровень секретности информации. Наиболее общий подход строится на основе решетки ценностей. Приведем основные определения из теории решеток [2, стр. 17], используемые в дальнейшем тексте.

Определение 6. *Решетка* – это частично упорядоченное множество, в котором каждое двухэлементное подмножество имеет как точную верхнюю (sup), так и точную нижнюю (inf) грани, принадлежащие этому множеству.

Определение 7. Для A, B элемент $C = \sup(A, B)$ называется *точной* или *наименьшей верхней гранью*, если:

1. $A \leqslant C$, $B \leqslant C$.
2. $\forall D : A \leqslant D,\ B \leqslant D \Rightarrow\ C \leqslant D$.

Определение 8. Для A, B элемент $E = \inf(A, B)$ называется *точной* или *наибольшей нижней гранью*, если:

1. $E \leqslant A$, $E \leqslant B$.
2. $\forall D : D \leqslant A,\ D \leqslant B \Rightarrow\ D \leqslant E$.

Каждому объекту и субъекту системы сопоставляется «метка безопасности», являющаяся элементом решетки. При запросе на доступ субъекта к объекту происходит сравнение меток безопасности. Доступ разрешен, если метка безопасности субъекта доминирует над меткой безопасности объекта, в остальных случаях доступ запрещен.

В связи с тем что основные концепции ролевого доступа сформулированы в терминах теории графов, введем аналогичные понятия для мандатного разграничения доступа.

Определение 9. *Решеточным графом* будем называть ориентированный граф[1], вершины которого образуют решетку. При этом отношение порядка задается отношением доминирования на множестве вершин графа: если $\exists\, p(r_1, r_2)$, то $r_1 \geqslant r_2$. Наименьшая верхняя грань $\sup(r_1, r_2)$ определяется как ближайшая вершина, доминирующая над r_1 и r_2. Наибольшая нижняя грань $\inf(r_1, r_2)$ определяется как ближайшая вершина, подчиненная вершинам r_1 и r_2.

Определим более формально понятия *наименьшей верхней* и *наибольшей нижней* граней в контексте ориентированного графа:
$r = \sup(r_1, r_2) \Longleftrightarrow$

[1]Если исходя из контекста понятно, что речь идет об ориентированном графе, то орграф будем называть просто графом.

1. $\exists\, p(r, r_1)$ & $p(r, r_2)$, то есть r является верхней гранью.
2. Если $\exists\, p(r', r_1)$ & $p(r', r_2)$, то $\exists\, p(r', r)$, то есть r минимальна среди всех верхних граней.

$r = \inf(r_1, r_2) \Longleftrightarrow$

1. $\exists\, p(r_1, r)$ & $p(r_2, r)$, то есть r является нижней гранью.
2. Если $\exists\, p(r_1, r')$ & $p(r_2, r')$, то $\exists\, p(r, r')$, то есть r максимальна среди всех нижних граней.

Теорема 1. *Для произвольной решетки существует изоморфный ей решеточный граф.*

Доказательство. Пусть задана некоторая произвольная решетка. Сопоставим узлам решетки вершины графа G, а отношение порядка представим ориентированными дугами, направленными от «меньшей» вершины к «большей»: $r_1 \geqslant r_2 \Longleftrightarrow \exists (r_1, r_2) \in E$, где E – множество дуг графа G.

Операции взятия inf и sup для узлов решетки r_1 и r_2 дадут те же узлы, что и в случае применения этих операций к построенному графу G (так как дуга между двумя вершинами образует путь единичной длины между ними). ■

Замечание 1. Решеточный граф, изоморфный заданной решетке, неединственен. Действительно, например, графы на рисунке 1 изоморфны одной и той же решетке (M, P), где $M = \{a, b, c, d\}$ – множество узлов решетки, $P = \{(a, b), (a, c), (a, d), (b, d), (c, d)\}$ – отношение частичного порядка, заданное на M.

Определение 10. Решеточные графы G_1 и G_2 назовем *эквивалентными* ($G_1 \sim G_2$), если они изоморфны одной и той же решетке.

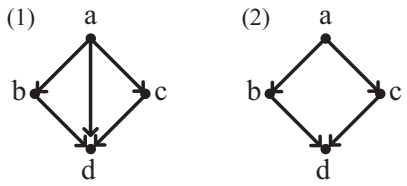

Рис. 1. Эквивалентные решеточные графы

Далее проанализируем, какими свойствами должен обладать решеточный граф и какие признаки являются достаточными условиями того, что граф решеточный.

Определение 11. Связный ориентированный граф называется *сетью*, если в нем существует единственный *источник* (вершина без входящих дуг) и единственный *сток* (вершина без исходящих дуг) [3, стр. 199].

Теорема 2. *Решеточный граф является сетью без ориентированных циклов.*

Доказательство. Пусть ориентированный граф G с множеством вершин R – решеточный.

Докажем, что в G нет ориентированных циклов. Допустим? это не так. Тогда узлы решетки, отвечающие ориентированному циклу, связаны отношением порядка: $r_i \geqslant r_{i+1} \geqslant \ldots \geqslant r_{i+n} \geqslant r_i$. По транзитивности получаем: $(r_i \geqslant r_{i+1})\&(r_{i+1} \geqslant r_i) \Rightarrow (r_i = r_{i+1})$. Но узлы решетки образуют множество, следовательно, все различны – это противоречие.

Так как граф G решеточный, то $\forall r_1, r_2 \in R\ \exists r_3 \in R : r_3 = \sup(r_1, r_2)$. По определению, $\sup(r_1, r_2)$ - это вершина, доминирующая над r_1, r_2, то есть в G существуют ориентированные пути $p(r_3, r_1)$ и $p(r_3, r_2)$. Следовательно, $\forall r_1, r_2$ существует неориентированный путь $p(r_3, r_1) \cup (r_3, r_2)$, соединяющий их, а значит, граф G связен.

Существование источника и стока следует из следующих рассуждений. Пусть, например, источника не существует, это значит, что $\forall r \in R$ найдется входящая дуга (r', r), то есть $\exists r' : r \leqslant r'$. Следовательно, $\exists \{r_i\}_{i=1}^{\infty} : r_i \leqslant r_{i+1}$. В силу конечности множества вершин $\exists i, j : (i < j)\&(r_i = r_j)$. Тогда $r_i \leqslant r_{i+1} \leqslant \ldots \leqslant r_j = r_i$. Получаем ориентированный цикл – противоречие с ранее доказанным. Существование стока доказывается аналогично.

Докажем единственность источника. Пусть это не так. Тогда существует как минимум два различных источника s_1 и s_2 ($s_1 \neq s_2$). Так как граф G решеточный, то должна существовать вершина r, из которой можно построить ориентированные пути $p(r, s_1)$ и $p(r, s_2)$. Но s_1 и s_2 – источники, следовательно, возможны лишь тривиальные пути, ведущие в эти вершины: $p(s_1, s_1)$ и $p(s_2, s_2)$. Отсюда получаем, что для существования $\sup(s_1, s_2)$ надо потребовать: $s_1 = s_2$ – это противоречие. Аналогично доказывается единственность стока. ■

Теорема 3. *Источник в решеточном графе доминирует над любой вершиной, а сток подчиняется любой вершине этого графа.*

Доказательство. Действительно, пусть s – источник. По определению решеточного графа $\forall r \in R : \exists r' = \sup(s, r)$. Следовательно, в графе найдутся ориентированные пути $p(r', r)$ и $p(r', s)$. Так как в s не входит ни одна дуга, то $r' = s$ и $\forall r \in R : \exists p(s, r)$. Аналогично доказывается, что $\forall r \in R : \exists p(r, t)$, где t – сток. ■

Утверждение, обратное к теореме 2, неверно: не любая сеть без ориентированных циклов является решеточным графом. Возможны две причины, по которым ориентированный граф не будет решеточным (частично упорядоченное множество не будет решеткой [5]):

1. Найдутся две вершины, вообще не имеющие верхней (нижней) грани.

2. Найдутся две вершины, для которых нельзя выбрать минимальную среди верхних (максимальную среди нижних) граней – они несравнимы.

Первый случай отсекается требованием существования источника и стока в орграфе и отсутствием ориентированных циклов.

Теорема 4. *Источник в сети без ориентированных циклов доминирует над любой вершиной, а сток – подчиняется любой вершине этого графа.*

Доказательство. Пусть r – произвольная вершина сети без ориентированных циклов, s – источник, t – сток.

Будем строить ориентированный путь, начиная с вершины r и добавляя на каждом шаге по одной дуге. В силу отсутствия в сети ориентированных циклов, процесс построения пути конечен, причем последней присоединенной дугой будет дуга, ведущая в единственный сток графа. Следовательно, в сети существует по крайней мере один ориентированный путь $p(r_1, t)$. Но тогда t подчиняется вершине r.

Существование ориентированного пути $p(s, r)$ доказывается аналогично, но его построение ведется в направлении, обратном ориентации дуг. Таким образом, s доминирует над вершиной r. ■

Замечание 2. Из теоремы 4 очевидным образом следует, что в сети без ориентированных циклов для любой пары вершин существуют по крайней мере одна верхняя грань (это источник) и одна нижняя грань (это сток). Но остается открытым вопрос о возможности выбора *наименьшей* верхней (*наибольшей* нижней) граней, то есть вопрос сравнимости граней.

Вторую причину «нерешеточности» графа легко проиллюстрировать примером: граф (1) на рисунке 2 – сеть без ориентированных циклов, но она не является решеточным графом. Действительно, вершины a и b имеют две несравнимые нижние грани c и d, а еще одна нижняя грань t заведомо меньше c и d; вершины c и d имеют две несравнимые верхние грани a и b, а еще одна верхняя грань s заведомо больше a и b.

Но требование отсутствия в сети подграфов, имеющих более одного стока или источника, как у подграфа, порожденного множеством вершин $\{a, b, c, d\}$ (см. рис. 2 (1)), не является достаточным условием решеточности. Действительно, добавление вершины e (см. рис. 2 (2)) делает рассмотренную сеть решеточным графом: $\inf(a, b) = e$ (c и d по-прежнему несравнимы, но $(e \geqslant c)\&(e \geqslant d)$) и $\sup(c, d) = e$ (a и b по-прежнему несравнимы, но $(e \leqslant a)\&(e \leqslant b)$).

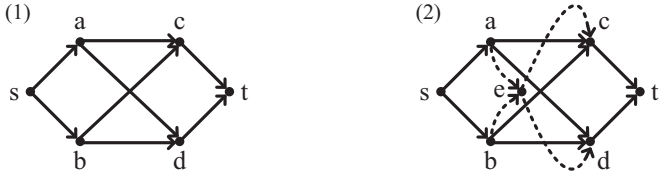

Рис. 2. Сеть, не являющаяся решеточным графом (1), и сеть, являющаяся решеточным графом (2)

Следующие теоремы дают ряд достаточных условий решеточности графа.

Теорема 5. *Пусть граф G является сетью и удаление стока превращает его в ориентированное дерево*[2]*. Тогда G – решеточный.*

Доказательство. Пусть s – источник, t – сток и $G\backslash\{t\} = T$ – дерево, полученное из исходного графа удалением стока. Если R – множество вершин графа G, то $R_T = R\backslash\{t\}$ – множество вершин дерева T и s – корень дерева.

Докажем существование наименьшей верхней грани для любой пары вершин графа G.

Пусть r_1 и r_2 ($r_1 \neq r_2$) – две произвольные вершины дерева T. По теореме о свойствах ордерева для любой его вершины существует единственный ориентированный путь, ведущий в эту вершину из корня [3, стр. 239]. Тогда $\exists\,!\; p(s, r_1)$ и $\exists\,!\; p(s, r_2)$. Так как $r_1 \neq r_2$, то эти пути не совпадают. Пусть r' – последняя, считая от s, из общих вершин этих путей. Очевидно, что все вершины, принадлежащие ориентированному пути $p(s, r')$, являются верхними гранями вершин r_1 и r_2, а r' – минимальная среди них. В силу единственности путей $p(s, r_1)$ и $p(s, r_2)$ других верхних граней у вершин r_1 и r_2 нет. Следовательно, $r' = \sup(r_1, r_2)$.

Рассмотрим теперь пару вершин (r, t), где r – произвольная вершина дерева T. По теореме 4 сток t подчиняется вершине r, то есть существует ориентированный путь $p(r, t)$. Следовательно, $\sup(r, t) = r$.

Докажем теперь существование наибольшей нижней грани для любой пары вершин графа G.

Рассмотрим сначала две произвольные вершины r_1 и r_2 ($r_1 \neq r_2$) дерева T. Возможны два случая: либо не существует ориентированного пути, связывающего эти две вершины, либо он единственен.

В первом случае, двигаясь из этих вершин по направлению дуг, построим ориентированные пути $p(r_1, \widetilde{r_1})$ и $p(r_2, \widetilde{r_2})$, где $\widetilde{r_1}$ и $\widetilde{r_2}$ – листья. Эти пути могут быть не единственны, но все они не имеют общих вершин (иначе в свободном дереве $\widetilde{T}$, полученном из T отменой ориентации ребер, был бы цикл, что противоречит теореме о свойствах ордерева [3, стр. 239]). В графе G существуют дуги $(\widetilde{r_1}, t)$ и $(\widetilde{r_2}, t)$. Следовательно, в графе G ориентированные пути $p(r_1, t) = p(r_1, \widetilde{r_1}) \cup (\widetilde{r_1}, t)$ и $p(r_2, t) = p(r_2, \widetilde{r_2}) \cup (\widetilde{r_2}, t)$ имеют лишь одну общую вершину t. Тогда $\inf(r_1, r_2) = t$.

Во втором случае существование наибольшей нижней грани очевидно, ею будет та из вершин r_1, r_2, которая является конечной в существующем между этими вершинами ориентированном пути.

Существование наибольшей нижней грани для двух вершин, одна из которых является стоком (пусть это вершины r и t), следует из существования по крайней мере одного ориентированного пути $p(r, t)$ (см. теорему 4). ■

Теорема 6. *Пусть граф G является сетью, а удаление источника и инвертирование всех дуг превращает его в дерево. Тогда G – решеточный.*

[2] В дальнейшем ориентированное дерево будем называть просто деревом, а неориентированное – *свободным* деревом.

Доказательство. Если инвертировать все дуги сети G, то мы получим сеть $\widehat{G}$, в которой источник и сток поменялись местами. Для графа $\widehat{G}$ справедлива теорема 5. Но тогда исходный граф G также будет решеточным, так как вершина r_1 доминирует над вершиной r_2 в графе $\widehat{G}$ тогда и только тогда, когда вершина r_2 доминирует над вершиной r_1 в графе G. ■

4. Древовидная иерархия ролей

Рассмотрим ситуацию, когда в компьютерной системе кроме ролевой политики безопасности необходимо реализовать также мандатную политику безопасности на основе некоторой решетки L. Основная проблема, возникающая в этом случае, состоит в построении правил доступа, удовлетворяющих обеим политикам безопасности и не противоречащих друг другу. В первую очередь рассмотрим иерархию ролей, образующую дерево.

Теорема 7. *Пусть в компьютерной системе действуют ролевая политика безопасности на основе дерева ролей T и мандатная политика безопасности на основе решетки L, тогда в компьютерной системе может быть построена непротиворечивая политика безопасности, включающая в себя разграничения обеих политик безопасности.*

Доказательство. Очевидно, что в дереве присутствует роль, доминирующая над всеми остальными ролями – корень дерева (назовем ее максимальной ролью – $MaxRole$). Добавим к дереву T вершину $MinRole$, не обладающую никакими привилегиями, и соединим дугами все листья дерева T с вершиной $MinRole$ (добавленные дуги ориентируем от листьев дерева T к $MinRole$), тем самым построим граф TM. Очевидно, что вершина $MaxRole$ является источником, вершина $MinRole$ – стоком, а граф TM – сетью. Согласно теореме 5, TM – решеточный граф, то тесть его вершины образуют решетку.

Тогда возможно получить декартово произведение решетки, построенной на вершинах графа TM, и решетки L. Как показано в [1, стр. 21], декартово произведение решеток есть решетка.

На основании полученной решетки можно построить мандатную политику безопасности. С другой стороны, из элементов решетки возможно построить решеточный граф (см. теорему 1). Такой граф может задавать ролевую политику безопасности. ■

5. Произвольная иерархия ролей

Перейдем теперь к рассмотрению иерархии ролей, образующей произвольный ориентированный граф G.

Определение 12. *Допустимым преобразованием* ориентированного графа ролей G назовем следующий процесс: если в G имеется более одного стока, то добавляется роль, не обладающая никакими привилегиями, и дуги, ведущие от стоков графа G к новой роли.

Очевидно, что, с одной стороны, такое преобразование превращают граф ролей в сеть (в случае единственности источника), а с другой – изменения ролевой политики безопасности несущественны.

Теорема 8. *Если граф иерархии ролей является решеточным либо его можно с помощью допустимого преобразования расширить до решеточного, то ролевая политика безопасности допускает непротиворечивое совмещение с мандатной политикой безопасности.*

Доказательство. Расширим, если это необходимо, граф иерархии ролей до решеточного графа, обозначим его GM. Мандатная политика безопасности задается решеткой L. Тогда можно взять декартово произведение решетки, построенной на вершинах решеточного графа GM, и решетки L. Согласно [1, стр. 21], такое декартово произведение, обозначим его через $GM \times L$, является решеткой.

Поскольку $GM \times L$ – решетка, то она может задавать мандатную политику безопасности. С другой стороны, на основании решетки $GM \times L$ можно построить решеточный граф (см. теорему 1), который будет задавать ролевую политику безопасности. ■

6. Пример совмещения ролевой и мандатной политик безопасности

Доказательство теоремы 8 является конструктивным. В качестве иллюстрации предложенного алгоритма объединим ролевую политику безопасности, представленную на рисунке 3, и мандатную политику безопасности, построенную на линейном множестве из трех элементов.

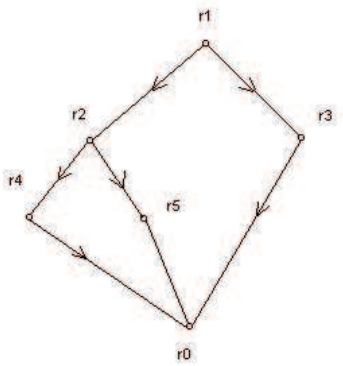

Рис. 3. Ролевая политика безопасности

Ролевая политика задается шестью ролями, одна из которых (r_0) является «пустой», то есть не обладающей какими-либо привилегиями и подчиненной любой другой роли. Очевидно, что заданная политика безопасности соответствует условиям теоремы 5. Следовательно, граф, представленный на рисунке 3, является решеточным.

Пусть мандатная политика безопасности задается решеткой L, элементами которой являются узлы l_1, l_2, l_3, причем отношение порядка задано таким образом, что $l_1 \geqslant l_2 \geqslant l_3$.

Согласно теореме 8, возможно непротиворечивое совмещение заданных политик безопасности. Для этого необходимо построить решетку $R \times L$, являющуюся декартовым произведением решеток R и L, где R – решетка, определяемая решеточным графом, представленным на рисунке 3.

Элементами решетки $L \times R$ являются пары (r_i, l_j), при $i = 0, \ldots, 5$ и $j = 1, \ldots, 3$. При этом отношение порядка задается следующим образом: $(r_i, l_j) \geqslant (r_k, l_m)$, если $r_i \geqslant r_k$ и $l_j \geqslant l_m$. Заметим, что узлы r_2 и r_3, r_4 и r_5, r_3 и r_4, r_3 и r_5 попарно несравнимы. Решеточный граф, изоморфный решетке $R \times L$, представлен на рисунке 4.

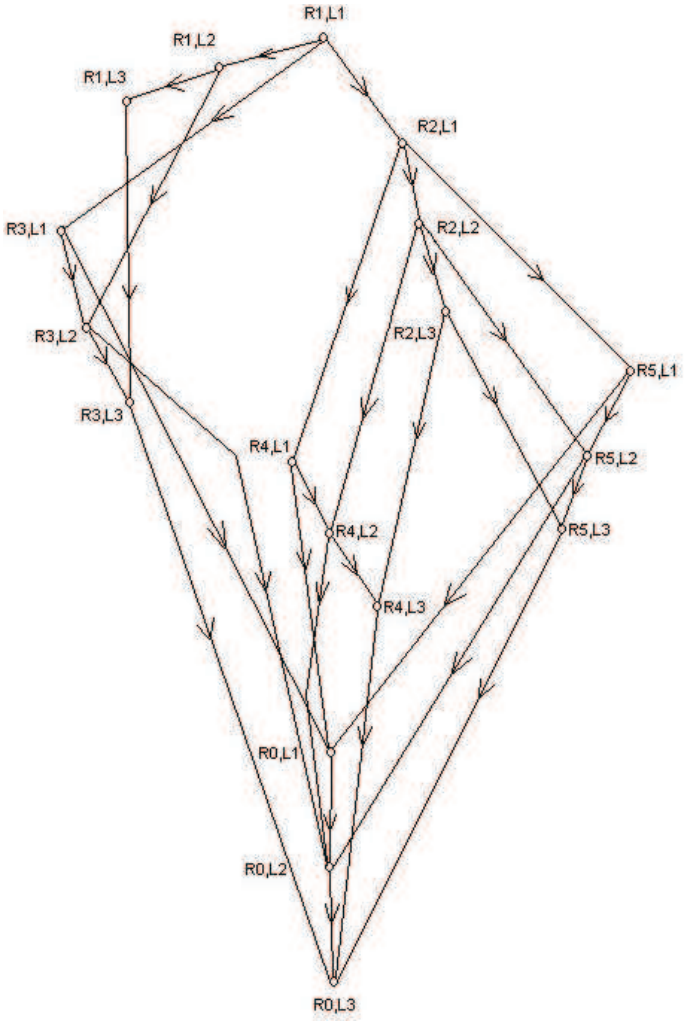

Рис. 4. Совмещение ролевой и мандатной политик безопасности

На полученной решетке $R \times L$ можно задать мандатную политику безопасности. В свою очередь, на полученном ориентированном графе (см. рис. 4) можно построить ролевую политику безопасности.

7. Заключение

Таким образом, возможно создание политики безопасности предприятия, включающей в себя мандатное и ролевое разграничение доступа. Причем результат объединения этих двух подходов может быть представлен как в виде концепции, основанной на метках безопасности, так и в виде иерархии ролей.

Литература

1. Биркгоф, Г. Теория решеток / Г. Биркгоф. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 568 с.
2. Гретцер, Г. Общая теория решеток / Г. Гретцер. / Под редакцией Д.М. Смирнова. – М.: Мир, 1981. – 456 с.
3. Новиков, Ф.А. Дискретная математика для программистов / Ф.А. Новиков. – СПб.: Питер, 2001. – 304 с.
4. Терьо, М. Oracle. Руководство по безопасности / М. Терьо, А. Ньюмен. – М.: Издательство «ЛОРИ», 2004. – 560 с.
5. Решетки [Электронный ресурс]. – Режим доступа: http://www.eltech.ru/misc/LGA_2007_FINAL/Allpage/Section8/Part8112.htm (09.10.2009).
6. Nyanchama, M. Access Rights Administration in Role-Based Security Systems / M. Nyanchama, S.L. Osborn // Database Security VIII: Status & Prospects, Biskup, Morgenstern and Landwehr, eds. North-Holland. – 1994. – C. 37-56.