Математические структуры и моделирование
2010, вып. 21, с. 128–132

УДК 65.012.810

ОБЪЕДИНЕНИЕ МАНДАТНЫХ ПОЛИТИК БЕЗОПАСНОСТИ

С.В. Белим, Ю.С. Ракицкий

В данной работе рассмотрен возможный подход к построению мандатной политики безопасности составного предприятия. Исследована возможность непротиворечивого объединения уровней доступа. Предложен один из возможных алгоритмов.

1. Постановка задачи

Пусть организация состоит из N отделов D_1, $D_2, \ldots, D_n$. В каждом из отделов D_i $(i = \overline{1,N})$ действует мандатная политика безопасности, построенная на решетке L_i [2]. Необходимо построить общую политику безопасности организации, непротиворечиво включающую в себя все политики безопасности отделов. Данная задача распадается на два случая:

1. Политика безопасности изначально строится для всей организации, функционирование отделов должно быть организовано в определенной степени изолированно. Причем надо учитывать, что возможна ситуация, когда в каждом отделе свои требования к политике безопасности. Если организационными мерами возможно ввести для всех отделов единую шкалу ценности информации, то задача становится тривиальной.
2. Происходит объединение нескольких организаций в единую корпорацию, при этом начальные организации приобретают статус отделов. Необходимо учитывать, что в каждой организации до объединения существовала своя политика безопасности, изменение которой может привести к невозможности дальнейшего функционирования отдела. Таким образом, необходимо построить политику безопасности корпорации, сохранив при этом политики безопасности отделов.

В обоих случаях необходимо строить общую решетку ценностей, включающую в себя решетки отделов. Дополнительно необходимо обеспечить взаимодействие между отделами свободное от утечек информации. Будем решать задачу индуктивно. Рассмотрим объединение двух отделов. Далее, рассматривая полученное объединение как один новый отдел, присоединим к нему третий отдел и так далее. Таким образом, достаточно научиться строить объединение

Омский государственный университет им. Ф.М. Достоевского.
E-mail: sbelim@omsu.ru

двух отделов, которые без потери общности можно обозначить D_1 и D_2, а соответствующие им решетки ценностей L_1 и L_2. Документы, исходящие из одного отдела в другой, должны автоматически включаться в документооборот нового отдела. Следует отметить, что пересечение решеток может быть непустым $L_1 \cap L_2 \neq \emptyset$. Если передаваемый документ имеет метку безопасности из пересечения решеток, то проблем с переклассификацией не возникает, и, как следствие, отсутствует утечка информации. Поэтому в дальнейшем будем рассматривать только ситуацию, когда входящее сообщение имеет метку безопасности, отсутствующую в данном отделе.

2. Простое решение задачи

Наиболее простым решением задачи является построение единой решетки ценностей организации как декартова произведения решеток [3] отделов:

$$L = L_1 \times L_2.$$

При таком подходе каждый документ в системе будет характеризоваться парой меток безопасности (m_1, m_2) ($m_1 \in L_1$, $m_2 \in L_2$). В первом отделе при разграничении доступа учитывается только m_1, во втором – только m_2. Проблем с переклассификацией документов при передаче между отделами не возникает, так как происходит просто переключение с одной метки на другую.

Рассмотрим пример такого объединения. Пусть в отделе D_1 действует линейная решетка ценностей $L_1 = a_1, a_2, a_3$ с тремя уровнями безопасности $(a_1 < a_2 < a_3)$, диаграмма которой приведена на рисунке 1.

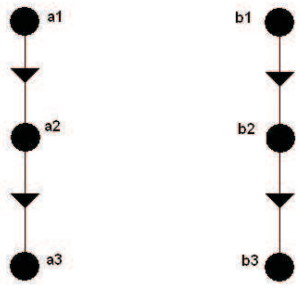

Рис. 1. Линейная решетка ценностей

Во втором отделе D_2 пусть действует линейная решетка ценностей $L_2 = b_1, b_2, b_3$ с тремя уровнями безопасности $(b_1 < b_2 < b_3)$, диаграмма которой также представлена на рисунке 1. Итоговая решетка безопасности объединенной организации будет иметь 9 меток безопасности, ее диаграмма приведена на рисунке 2.

Две метки безопасности в декартовом произведении сравнимы, если сравнимы как первая, так и вторая пара координат одновременно, причем они упорядочены одинаково.

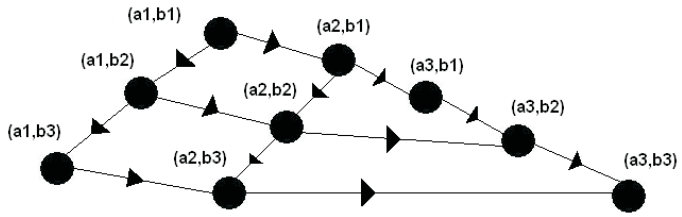

Рис. 2. Итоговая решетка безопасности объединенной организации

3. Возможности оптимизации решения

Проблема, возникающая при построении простого решения, заключается в обеспечении безопасности. Если метка безопасности сообщения из решетки L_1 отдела D_1 не входит в решетку D_2, то это означает, что ни один субъект отдела D_2 не может прочитать такое сообщение, пока ему не предоставят соответствующий доступ, то есть новую метку безопасности из декартова произведения решеток L_1 и L_2. При этом возникает ситуация, когда возможно отсутствие обмена между некоторыми субъектами из различных отделов, а это означает что ни одна из новых меток безопасности, полученных из декартова произведения решеток, им не подходит. Иначе будет возникать утечка информации, поскольку в полученной новой решетке самый низкий уровень a_3, b_3 предполагает доступ к информации каждого из отделов. Для того чтобы избежать подобной ситуации, необходимо дополнить новую решетку безопасности дополнительными уровнями безопасности, которые будут являться подрешетками новой решетки и имитировать работу каждого из отделов до слияния. Для этого необходимо ввести элементарное преобразование, которое будет дополнять любую решетку пустым элементом, или нулевым элементом. Возвращаясь к нашему примеру, решетка ценностей L_1 так и останется линейной, но минимальным элементом станет не a_3, а $\varnothing$. Аналогичные рассуждения можно применить и к решетке L_2. В результате получим решетки $L_1 \cup \varnothing = L_1^{\varnothing}$ и $L_2 \cup \varnothing = L_2^{\varnothing}$, диаграммы которых приведены на рисунке 3.

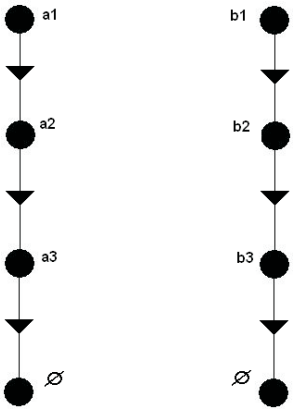

Рис. 3. Решетки $L_1 \cup \varnothing = L_1^{\varnothing}$ и $L_2 \cup \varnothing = L_2^{\varnothing}$

В случае если решетка ценностей не будет являться линейной, то, по определению решетки, для любых двух элементов существует наименьшая точная нижняя грань, то есть в любой решетке есть наименьший элемент. Это означает, что можно добавить пустой элемент, причем свойства решетки при этом не нарушатся. Пример такого дополнения изображен на рисунке 4.

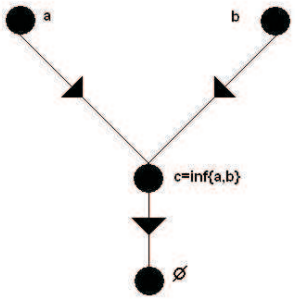

Рис. 4. Пример дополнения нелинейной решетки нулевым элементом

Построение единой решетки из двух полученных нами при помощи добавления пустого элемента можно также осуществить при помощи декартова произведения

$$L^{\varnothing} = L_1^{\varnothing} \times L_2^{\varnothing}.$$

При таком подходе результирующая решетка, диаграмма которой изображена на рисунке 5, будет состоять из 16-ти элементов. При этом можно заметить, что 9 элементов решетки $L^{\varnothing}$, образующие подрешетку, являются в точности решеткой L, диаграмма которой представлена на рисунке 1. Можно говорить о том, что решетка L является инструментом обеспечения информационного обмена между отделами D_1 и D_2, причем этот информационный обмен будет безопасным, поскольку для каждого вида взаимодействия предусмотрен специальный уровень безопасности. Кроме того, в решетке $L^{\varnothing}$ можно также выделить еще 2 подрешетки, каждая из которых будет имитировать работу отделов без информационного обмена. Диаграмма решетки $L^{\varnothing}$ представлена на рисунке 5.

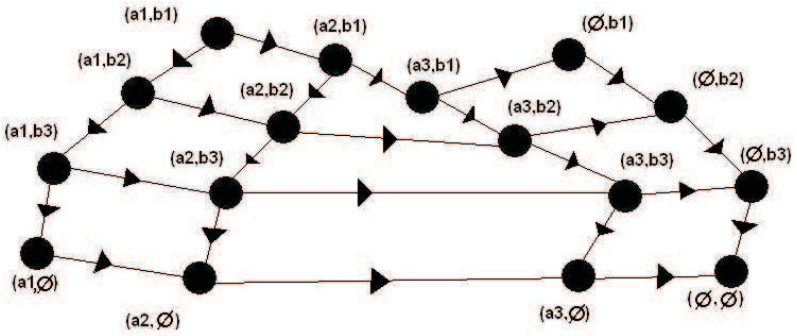

Рис. 5. Решетка $L^{\varnothing}$

4. Заключение

Таким образом, для построения общей политики безопасности организации, непротиворечиво включающей в себя все политики безопасности отделов, в случае объединения нескольких организаций в единую корпорацию необходимо дополнить каждую решетку, задающую мандатную политику безопасности для каждого из отделов, пустым элементом, после чего построить декартово произведение всех таких решеток. Это позволит получить непротиворечивую мандатную политику безопасности с отсутствием утечек информации.

Литература

1. Gyori I. *Some mathematical aspects of modelling cell population dynamics* // Computers and Math. Appl. 1990. V.20. N. 4. 6. P.127–138.
2. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах. Уральский университет, 2003.
3. Биркгоф Г. Теория решеток / Г. Биркгоф. М.:Наука. Главная редакция физико-математической литературы, 1984. 568 с.