Ю. С. Ракицкий, С. В. Белим

МОДЕЛЬ СОВМЕЩЕНИЯ ДВУХ МАНДАТНЫХ ПОЛИТИК БЕЗОПАСНОСТИ

Необходимость совмещения двух мандатных политик безопасности может возникнуть в системах, требующих обеспечения конфиденциальности и целостности информации одновременно. Конфиденциальность, или невозможность утечки высокоуровневой информации низкоуровневым пользователям, гарантируется при запрете потоков информации сверху вниз, т. е. уровень доверия субъекта должен доминировать над уровнем конфиденциальности объекта в решетке ценностей. Целостность информации, согласно модели Биба [1], гарантируется при отсутствии потоков снизу вверх, когда низкоуровневые пользователи не могут вносить изменения в высокоуровневые объекты. Целостность гарантируется, если разрешены только те доступы, в которых уровень субъекта не выше уровня объекта в решетке ценностей. Таким образом, попытки обеспечить конфиденциальность и целостность одновременно на одной решетке ценностей приводят к противоречащим друг другу правилам. В результате возможно перемещение информации только на одном уровне и невозможно обмениваться данными субъектам с разными уровнями полномочий. В частности, эта ситуация означает, что в операционных системах прикладные процессы не могут взаимодействовать с системными процессами и наоборот.

Данное противоречие разрешается обычно с помощью введения двух решеток ценностей: одной — для обеспечения конфиденциальности, другой — для обеспечения целостности. При этом задача администрирования системы становится весьма трудоемкой, так как каждый доступ проверяется по двум независимым правилам. Встает задача построения единой решетки ценностей, которая обеспечивает выполнимость обеих политик безопасности таким образом, чтобы при каждом доступе проверялось только одно условие.

Задача совмещения двух решеток ценностей осложняется необходимостью совпадения меток вершин решеток. Алгебраического изоморфизма соответствующих решеток недостаточно для того, чтобы безболезненно соединить две политики безопасности. Рассмотрим простой пример. Пусть имеется две линейные решетки ценностей, одна из решеток $S_1 = \{N<S<TS\}$, другая решетка $S_2 = \{S<TS<STS\}$. С точки зрения формального алгебраического подхода обе решетки изоморфны, так как представляют собой линейное упорядоченное множество из трех элементов. Формальное сопоставление по этому признаку приводит к тому, что пользователь с уровнем доступа S может читать документы уровня TS из второй организации, тогда как в своей организации ему такие документы недоступны.

Приведем некоторые утверждения, показывающие возможность непротиворечивого совмещения двух мандатных политик безопасности без утечек информации.

Теорема 1. Если решетка S_1 изоморфна некоторой подрешетке S_2 и совпадают соответствующие метки вершин, то общая политика безопасности может быть построена на основе решетки $S = S_2$ без утечки информации.

Теорема доказана авторами.

Введем два понятия, необходимых для построения общей решетки ценностей двух организаций.

$dS = \text{minus}(S_1,S_2)$

dS — максимальная общая подрешетка S_1 и S_2, т. е. подрешетка, которая входит в S_1 и S_2 с совпадающими метками вершин.

$DS = \text{maxus}(S_1,S_2)$

DS — минимальная решетка, включающая в себя S_1 и S_2 как подрешетки с сохранением меток вершин.

Задача поиска общей решетки ценностей сводится к поиску DS. В теореме 1 по сути рассматривается случай когда $dS = S_1$.

Введем дополнительное преобразование для произвольной решетки ценностей S. Будем называть операцию $Sv\{0\}$ дополнением решетки S нулевым элементом, если для любого элемента s решетки S будет выполняться $\{0\} < s$.

Теорема 2. Если $dS = 0$, то $DS = (S1v\{0\}) \times (S2v\{0\})$.

Теорема доказана авторами

Рассмотрим пример. Пусть в отделе D_1 действует линейная решетка ценностей $L_1 = a_1,a_2,a_3$ с тремя уровнями безопасности $a_1 < a_2 < a_3$. Пусть в отделе D_2 действует линейная решетка ценностей $L_2 = b_1,b_2,b_3$ с тремя уровнями безопасности $b_1 < b_2 < b_3$. Построим прямое произведение решеток $L = L_1 \times L_2$ [2]. Получим решетку с 9 уровнями безопасности. Если метка безопасности сообщения из решетки L_1 отдела D_1 не входит в решетку D_2, то ни один субъект отдела D_2 не может прочитать такое сообщение, пока ему не предоставят соответствующий доступ, т. е. новую метку безопасности из декартова произведения решеток $L_1 \times L_2$.

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 добавить в новую решетку безопасности дополнительные уровни безопасности, которые будут являться подрешетками новой решетки и имитировать работу каждого из отделов до слияния. Для этого необходимо использовать преобразование, которое будет дополнять любую решетку нулевым элементом. Возвращаясь к нашему примеру, решетка ценностей L_1 так и останется линейной, но минимальным элементом станет не a_3, а $\{0\}$. Аналогичные рассуждения можно применить и к решетке L_2. В результате получим решетки L_1^0 и L_2^0. Построение единой решетки из двух полученных нами при помощи добавления пустого элемента можно также осуществить при помощи декартова произведения $L^0 = L_1^0 \times L_2^0$. При таком подходе результирующая решетка будет состоять из 16 элементов. При этом можно заметить, что 9 элементов решетки, образующие подрешетку, являются в точности решеткой L. 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^0 можно также выделить еще 2 подрешетки, каждая из которых будет имитировать работу отделов без информационного обмена.

Теорема 3. Если $dS \neq 0$, то $DS \subset (S1v\{0\}) \times (S2v\{0\})$, т. е. меньше, чем прямое произведение решеток.

Теорема доказана авторами.

Последняя теорема показывает, что при наличии в различных решетках одинаковых меток безопасности получение объединения этих решеток через декартово произведение будет избыточным, значит, необходим алгоритм построения объединения с учетом общих меток безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Уральский университет, 2003.
2. *Биркгоф Г.* Теория решеток. М.: Наука. Главная редакция физико-математической литературы, 1984. — 568 с.