Математические структуры и моделирование
2004, вып. 13, с. 140–143

УДК 681.3.053

ПОЛИТИКА БЕЗОПАСНОСТИ СУБД, ОБЕСПЕЧИВАЮЩАЯ ЗАЩИТУ ОТ ПОЛУЧЕНИЯ ИНФОРМАЦИИ ПУТЕМ ЛОГИЧЕСКИХ ВЫВОДОВ

Т.М. Опарина

In this articletechnology of a database security from reception the information from it by the way of logic conclusions is described .

Современные системы управления базами данных требуют применения сложных схем защиты данных, опирающихся на принудительный или обязательный контроль доступа к данным **(mandatory access control)**. Такой контроль доступа осуществляется с помощью специальных меток безопасности (**security labels**), каждая из которых соответствует некоторому уровню безопасности, например: несекретно, конфиденциально, секретно, совершенно секретно. Метки безопасности присваиваются данным в момент занесения их в базу данных и служат для классификации данных по уровням безопасности. Так как данные расклассифицированы по уровням безопасности метками, каждый конкретный пользователь получает ограниченный доступ к информации. Он может оперировать только с данными, находящимися на том уровне секретности, который соответствует его статусу и на уровнях ниже.

Одной из проблем возникающих при защите базы данных является получение конфиденциальной информации, путем агрегирования данных. Проблема возникает тогда, когда секретная информация получена комбинированием данных, добытых с помощью санкционированного доступа, т.е. происходит повышение уровня секретности информации. Также информацию более высоко уровня секретности можно получить с помощью проведения глубокого логического анализа. В качестве примера можно рассмотреть следующую базу данных, представленную на рис.1. Обычно каждому элементу, содержащемуся в таблице, присваивается метка, соответствующего уровня безопасности. Субъект, имеющий допуск к данным «секретные» соответственно получит доступ ко всем строкам таблицы. Изъяв данные, входящие в первую запись можно сделать следующий вывод: «Резидент Ковров А.П. собирается поехать в Англию 29.04.2004 рейсом HY663.» В итоге получаем, что данная информация скорее всего имеет наиболее высокий уровень секретности, например совершенно секретно (т.к. можно предположить что Ковров А.П. поехал в Англию для проведения какой-нибудь секретной операции).

E-mail: oparina@univer.omsk.su
Омский государственный университет

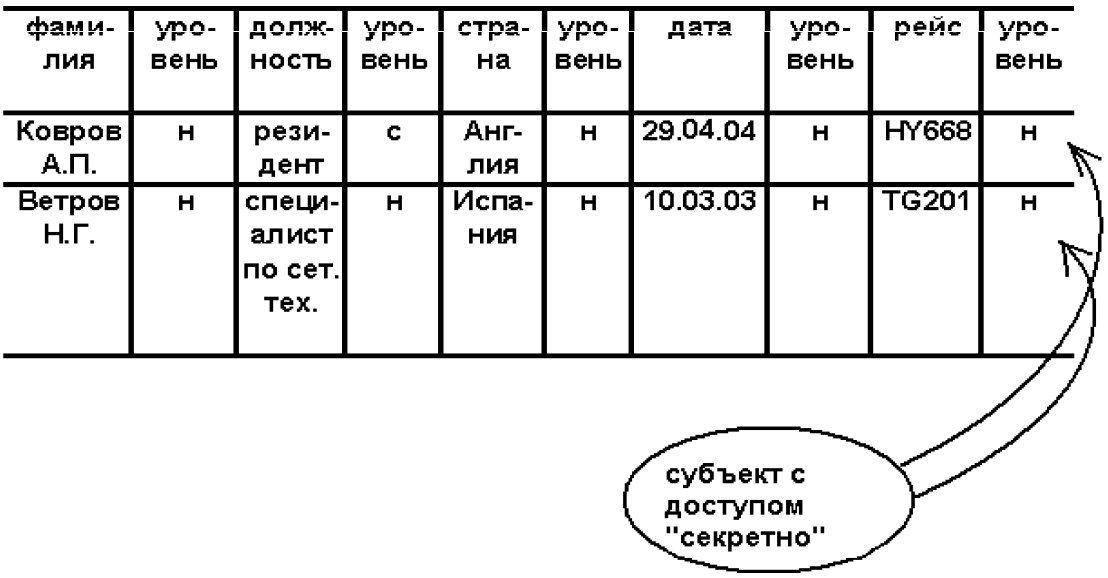

Рис. 1.

Подход который наиболее часто используется для разрешения данной проблемы – это тщательное проектирование модели данных и максимальное ограничение доступа пользователей к информации. Предположим, что можно запретить доступ всех пользователей обладающих уровнем доступа «секретно» к первой записи, но таким образом мы получаем существенное ограничение на выборку данных из таблицы.

Далее мы рассмотрим возможность построения модели защиты базы данных от логических выводов, которая позволяет смягчить условия на ограничение получения данных.

Проведем формальное описание политики безопасности системы, представленной на рис.1:

1. К данной системе могут осуществлять доступ субъекты (пользователи) со следующими уровнями доступа:

   $S_{\text{Н}}$ – несекретно;

   $S_{\text{К}}$ – конфиденциально;

   $S_{\text{С}}$ – секретно;

   $S_{\text{СС}}$ – совершенно секретно.

2. Информационная система состоит из объектов, которые обозначим: O_1, O_2, O_3, O_4, O_5. Данным объектам поставим в соответствие данные первой записи Ковров А.П., резидент, Англия, 29.04.04, HY668. Для рассмотрения мы не будем использовать вторую запись, т.к. ее анализ не позволит нам вывести никакой секретной информации.

3. Построим матрицу M отображающую принадлежность объектов к субъектам.

	O_1	O_2	O_3	O_4	O_5
$S_{\text{Н}}$	чт./зп.	запрет чт./зп.	чт./зп.	чт./зп.	чт./зп.
$S_{\text{К}}$	чт./зп.	запрет чт./зп.	чт./зп.	чт./зп.	чт./зп.
$S_{\text{С}}$	чт./зп.	чт./зп.	чт./зп.	чт./зп.	чт./зп.
$S_{\text{СС}}$	чт./зп.	чт./зп.	чт./зп.	чт./зп.	чт./зп.

Здесь же в реальной ситуации нужно рассмотреть и отношение субъект-субъект. Последнее необходимо для того, чтобы в область действия модели включались также отношения между субъектами [3]. Таким образом, мы сможем рассматривать возможность доверительных отношений между субъектами.

Проведем полный анализ объектов в данной системе и установим возможность получения информации более высокого уровня с помощью логических выводов на основе агрегирования данных. Логический анализ проведем, ориентируясь на известные нам факты, но возможно он не совсем соответствует анализу, который проводят соответствующие органы:

$O_1 \bigcup O_2$- секретно	$O_3 \bigcup O_5$-несекретно	$O_2 \bigcup O_3 \bigcup O_4$-секретно
$O_1 \bigcup O_3$-несекретно	$O_4 \bigcup O_5$-несекретно	$O_2 \bigcup O_3 \bigcup O_5$-секретно
$O_1 \bigcup O_4$-несекретно	$O_1 \bigcup O_2 \bigcup O_3$-сов. секретно	$O_2 \bigcup O_4 \bigcup O_5$-секретно
$O_1 \bigcup O_5$-несекретно	$O_1 \bigcup O_2 \bigcup O_4$-сов. секретно	$O_3 \bigcup O_4 \bigcup O_5$-несекретно
$O_2 \bigcup O_3$-несекретно	$O_1 \bigcup O_2 \bigcup O_5$-сов. секретно	$O_1 \bigcup O_2 \bigcup O_3 \bigcup O_4$-сов. секретно
$O_2 \bigcup O_4$-несекретно	$O_1 \bigcup O_3 \bigcup O_4$-несекретно	$O_1 \bigcup O_2 \bigcup O_3 \bigcup O_5$-сов. секретно
$O_2 \bigcup O_5$-несекретно	$O_1 \bigcup O_3 \bigcup O_5$-несекретно	$O_1 \bigcup O_2 \bigcup O_4 \bigcup O_5$-сов. секретно
$O_3 \bigcup O_4$-несекретно	$O_1 \bigcup O_4 \bigcup O_5$-несекретно	$O_1 \bigcup O_3 \bigcup O_4 \bigcup O_5$-несекретно
$O_2 \bigcup O_3 \bigcup O_4 \bigcup O_5$-сов. секретно	$O_1 \bigcup O_2 \bigcup O_3 \bigcup O_4 \bigcup O_5$-сов. секретно	

где $O_1 \bigcup O_2$, $O_1 \bigcup O_3$ и т.д. логическое объединение объектов, т.е. объединение $O_1 \bigcup O_2$ будет аналогично фразе «Ковров А.П. - резидент».

Очевидно, что можно определить все варианты доступа субъектов к объектам с запретом на выборку данных, анализ которых даст нам информацию более секретную, т.е. имеем, что для:

- субъектам $S_{\text{Н}}$ и $S_{\text{К}}$ можно разрешить доступ к группе объектов O_1, O_3, O_4, O_5;
- субъекту $S_{\text{С}}$ можно разрешить доступ к группам объектов O_2, O_3, O_4 или O_2, O_3, O_5 или O_2, O_4, O_5 или O_1, O_3, O_4, O_5 (но обязательно только к одной из этих групп объектов или только к комбинации объектов, состоящей из входящих внутрь объектов одной группы);
- субъекту $S_{\text{СС}}$ можно разрешить доступ к группе объектов O_1, O_2, O_3, O_4, O_5.

Тогда при попытке доступа выполняются следующие действия:

1. Проверяется, является ли субъект собственником объекта, если нет, то доступ отклоняется. Если субъект имеет права на объект, то осуществляется переход ко второму шагу алгоритма.

2. Сравниваются вхождения объектов в группы объектов, разрешенные на использование субъекту данного уровня доступа. Если субъект уже имел выборку объектов, то происходит проверка на возможность выполнения элементарной операции, составляющей команду пользователя (например, если в приведенном выше примере пользователь S_C уже имел доступ к объектам O_2, O_3, то теперь ему можно дать привилегии только на объект O_4 или O_5. Далее после изъятия, допустим O_4, доступ к другим объектам (кроме O_2, O_3, O_4) запрещается для предотвращения получения более секретных данных).

Мы думаем, что наибольшую сложность при построении такой политики безопасности вызывает анализ информации, содержащейся в СУБД на выявление смысловой взаимосвязи между объектами, которая как раз, и позволит определить, при сочетании каких объектов произойдет получение данных более высокого уровня секретности. Здесь существенным фактором может сыграть выявление смысловой единицы, которая и влияет на получение таких данных (в нашем случае – это должность, имеющая значение «резидент»). При проектировании СУБД необходимо учитывать проведение логического анализа для упрощения которого, нужно разбить одну таблицу на несколько с небольшим количеством смысловых единиц, хотя это несколько усложнит модель данных и последующую ее обработку.

В заключение скажем, что такой подход можно реализовать, используя любой процедурный язык, расширяющий возможности языка структурированных запросов SQL, который присутствует во многих коммерческих СУБД. Отметим также, что при изменении данных, входящих в группу объектов доступ к которым происходил, потребуется автоматическое изменение привилегий доступа на исходные.

Хочется заметить необходимость проведения анализа данных, содержащихся в СУБД, иначе этот анализ могут провести за нас лица, не имеющие на то полномочий.

Литература

1. Вьюкова Н.И., Галатенко В.А. *Информационная безопасность систем управления базами данных.*
   – http://www.tts.tomsk.su/personal/~sas/DBMS/96_1/sourse/dbms_sec.htm
2. Саймон А.Р. *Стратегические технологии баз данных: менеджмент на 2000 год Пер. с англ. / Под ред. и с предисл. М.Р. Когаловского.* М.: Финансы и статистика, 1999 г.
3. Зегжда Д.П., Ивашко А.М. *Основы безопасности информационных систем* М.: Горячая линия - Телеком, 2000 г.