Математические структуры и моделирование
2004, вып. 14, с. 123–127

УДК 681.3

Т.М. Опарина

МОДЕЛЬ АВТОМАТИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В БАЗЕ ДАННЫХ ОТ ПОЛУЧЕНИЯ ДАННЫХ С ПОМОЩЬЮ ЛОГИЧЕСКИХ ВЫВОДОВ

Хранимая информация в базе данных представляет собой большую ценность, следовательно, эту информацию нужно защищать. Практически во всех СУБД есть средства для ограничения выполнения некоторых действий определенными пользователями. Однако ни одна из них не предоставляет возможности в полном объеме ограничить получение секретной информации с помощью логических выводов при санкционированном доступе. В связи с этим пользователи, имеющие санкционированный доступ к базе данных, должны рассматриваться как потенциальный источник утечки информации.

В данной статье представлена модель, позволяющая, возможно, отчасти решить вышеописанную проблему вывода информации при многоуровневой защите.

1. Многоуровневая модель безопасности баз данных

Многоуровневая модель безопасности баз данных наиболее часто строится на основе мандатной модели Белл-ЛаПадула. В этой модели все сущности делятся на активные — субъекты и пассивные – объекты. Всем сущностям ставится в соответствие специальная метка безопасности, например: совершенно секретно, секретно, конфиденциально, несекретно. После чего в системе устанавливаются следующие правила контроля доступа:

1. Субъект имеет права доступа только к тем объектам, метка безопасности которых не выше его собственной метки безопасности.

2. Субъект имеет право заносить информацию только в те объекты, метка безопасности которых не ниже его собственной метки безопасности.

В реальной жизни первое правило не всегда может гарантировать защиту базы данных от утечки информации [2, 4]. Данное правило скорее должно звучать следующим образом:

© **2004 Т.М. Опарина**
E-mail: oparina@univer.omsk.su
Омский государственный университет

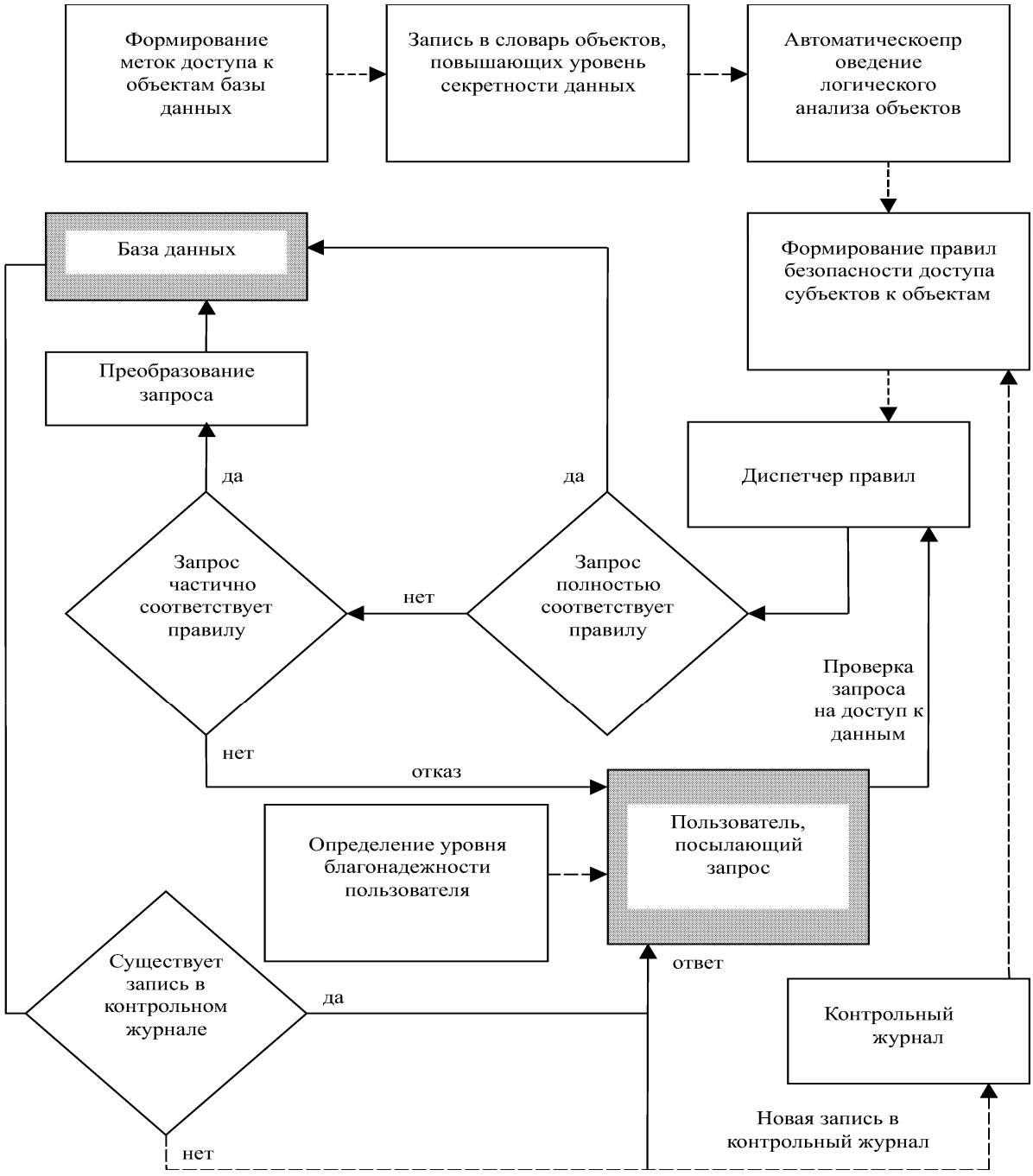

Рис. 1. Модель защиты БД от получения данных с помощью логических выводов.

Субъект имеет права доступа только к тем объектам, анализ которых не позволяет получить данные, метка безопасности которых выше его собственной метки безопасности.

2. Модель защиты СУБД от логических выводов

В представленной модели на рис.1 система обработки информации использует две основные сущности: субъекты (множество пользователей или групп пользователей) и объекты (база данных с полями и записями). Каждому пользователю или группе пользователей присваивается уровень благонадежности доступа, а объектам соответствующие метки секретности. Метки имеют составную организацию, состоящую из трех частей:

- уровень – иерархический компонент, определяющий «значимость», который может принимать значение конфиденциально, секретно, и т.п.;
- категория – компонент, определяющий принадлежность данных к определенному проекту или отделу;
- группа – иерархический компонент, который задает подмножество лиц, имеющих доступ к документу.

В табл.1 приведен пример значений, которые могут принимать метки.

Таблица 1.

Уровень	Категория	Группа
секретно	конструкторский отдел	руководители проекта
конфиденциально	конструкторский отдел	техники

Какие-либо ограничения на количество уровней отсутствуют. Метка может состоять также и из одной части – уровня. На самом деле число объектов в базе данных, влияющих на повышение уровня секретности, невелико. При проектировании политики безопасности СУБД выделяются все атрибуты, которые могут содержать такие объекты и заносятся в *словарь объектов* для последующего логического анализа. В дальнейшем при добавлении новых записей в таблицы базы данных объекты, влияющие на повышение уровня безопасности, будут вноситься в словарь. Встроенная система *контрольного журнала* представляет собой набор таблиц и позволяет отмечать следующие действия пользователей:

- идентификатор или имя пользователя;
- группа пользователя;
- идентификатор терминала;
- имя отношения, к которому происходит обращение;
- выполняемая операция;

- дата.

При помощи журнала происходит фиксирование доступа ко всем таблицам на выполнение следующих операций *select, delete, insert* или *update*. Для каждого пользователя контроль выполняется на уровне операции – одна запись создается для одной операции. Если операция выполняется повторно, то запись данного действия в журнал не делается. Данные журнала контроля впоследствии применяются для формирования правила безопасности доступа пользователей к объектам. В таблице 2 перечислены некоторые пункты операций контроля, которые разделены в зависимости от того, используется или нет ролевая политика доступа пользователей к объектам в системе. Такое разделение необходимо для того, чтобы предотвратить возможность обмена информацией между пользователями одной группы.

Таблица 2.

Пользователь	**Группа пользователей (при ролевой политике доступа)**
Просмотр списка записей, соответсвующих данному пользователю.	Просмотр списка записей, соответсвующих данному пользователю.
Проверка существования идентичной записи у данного пользователя.	Проверка существования идентичной записи у пользователя, входящего в аналогичную группу.
Внесение записи в журнал, если идентичная запись у данного пользователя не найдена.	Внесение записи в журнал, если идентичная запись у данной группы не найдена.

Диспетчер правил представляет собой инструмент, в котором хранятся правила для управления контролем доступа к объектам в СУБД. Диспетчер правил значительно упрощает дальнейшее администрирование. Структура правила формируется администратором только один раз. Затем происходит формирование правила, обеспечивающее более сильную безопасность. Каждый раз, когда пользователь пытается что-нибудь извлечь из базы данных, происходит проверка доступа к этим данным. Контроль доступа к данным основывается на модификации запросов, что позволяет реализовать правила защиты, связанные с конкретными объектами и пользователями (рис. 2). Если SQL–запрос лишь частично соответствует правилу, то запрос пользователя к таблицам базы данных модифицируется, при более жестком условии. Благодаря этому достигается дополнительная гибкость, поскольку возвращаются только те объекты для каждого пользователя, каждой группы пользователей, объединение которых не несет более секретную информацию.

3. Заключение

Представленный здесь механизм позволяет:

– сопоставлять метки, присвоенные фрагментам данных, с меткой прав доступа пользователя;

– проводить автоматический анализ объектов на повышение уровня секретности;

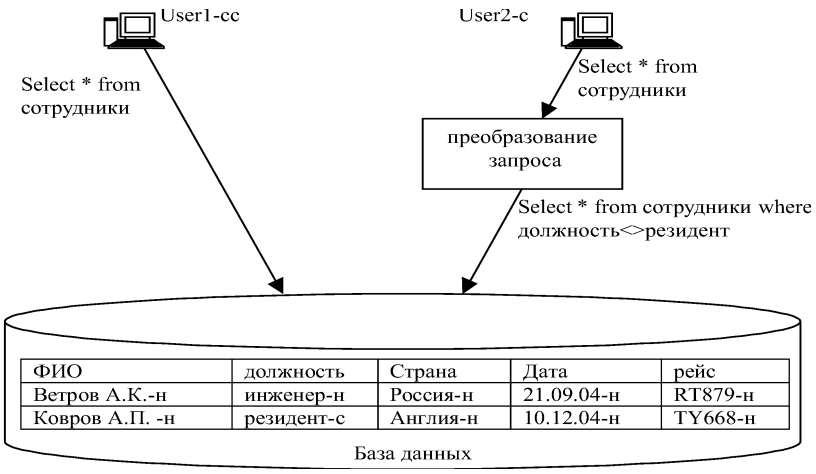

Рис. 2. Оба пользователя изначально имеют права доступа ко всем объектам базы данных, так как им присвоены уровни сс - «совершенно секретно» и с - «секретно», но если пользователь с доступом «секретно» извлечет всю информацию, то произойдет повышение уровня секретности (вся полученная информация в совокупности будет иметь уровень «совершенно секретно»), таким образом, необходимо преобразование запроса.

– задавать правила администратором базы данных при проектировании политики безопасности;

– автоматически формировать все последующие правила в базе данных, используя анализ объектов и журнал контроля;

– фиксировать все новые попытки выборки или модификации данных в базе данных в контрольный журнал;

– разделять данные на различные категории доступа в одной базе данных.

Литература

1. Марлен Терьо, Аарон Ньюмен. *ORACLE руководство по безопасности.* М. :Лори, 2004.
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.
3. Зегжда Д.П., Ивашко А.М. *Основы безопасности информационных систем* М.: Горячая линия-Телеком, 2000.
4. Опарина Т.М. *Политика безопасности СУБД, обеспечивающая защиту от получения информации путем логических выводов*//Математические структуры и моделирование/ Под ред. А.К. Гуца. Омск: ОмГУ. 2004. Вып.13.