УДК 004.056

Т.И. Калинкина

МОДИФИЦИРОВАННАЯ МОДЕЛЬ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА

Предложена модифицированная модель мандатного разграничения доступа на основе модели Белла – ЛаПадула. Модель учитывает особенности хранения информации в базе данных. На основе этой модели разработана и реализована система мандатного разграничения доступа для СУБД Microsoft SQL Server.

***Ключевые слова**: база данных, система управления базами данных (СУБД), триггер, мандатное разграничение доступа, модель разграничения доступа, степень конфиденциальности, уровень допуска, объект доступа, субъект доступа.*

Введение. Основу современных информационных систем составляют базы данных (БД). Обеспечение защиты информации, хранимой в БД, является важной и сложной задачей. Для ее решения используются средства, встраиваемые в системы управления базами данных (СУБД). Для защиты информации в СУБД используются такие средства, как:

– идентификация, аутентификация и авторизация пользователей БД;

– средства, реализующие разграничение доступа к информации, хранимой в БД;

– аудит действий пользователей и системных программ;

– средства резервирования.

В данной работе рассматриваются средства разграничения доступа к ресурсам СУБД и БД.

Средства разграничения доступа в СУБД реализуют различные модели разграничения доступа. Основные модели разграничения доступа, используемые в современных СУБД, – это дискреционная, ролевая и мандатная (полномочная).

В базах данных часто хранится информация, имеющая разную степень конфиденциальности или ценности для ее владельца. Примером такой информации являются персональные данные. Для защиты от несанкционированного доступа к такой информации используют механизм разграничения доступа на основе мандатной модели разграничения доступа.

Мандатная модель разграничения доступа реализована в современных СУБД Oracle Database Enterprise Edition 11 и Линтер Бастион 6.0. Однако, как показали исследования, приведенные в работе, реализации мандатной модели разграничения доступа в этих СУБД не полностью учитывают особенности хранения информации в базах данных, в частности иерархическую структуру хранения информации. Отсюда возникает задача разработки модели мандатного разграничения доступа, наиболее полно учитывающей такие особенности.

Целью работы являются разработка формальной модели мандатного разграничения доступа на основе модели Белла – ЛаПадула для СУБД, учитывающей особенности хранения информации в базах данных и реализующей защиту информации от несанкционированного доступа с учетом ее степени конфиденциальности; построение на основе формальной модели мандатного разграничения доступа системы мандатного разграничения доступа для СУБД Microsoft SQL Server.

Постановка задачи. В основе мандатной модели разграничения доступа лежат уровни допуска субъектов и степень конфиденциальности объектов. Множество возможных уровней допуска и множество возможных степеней конфиденциальности для любой системы тождественны.

Каждому субъекту системы присваивается один уровень допуска, каждому объекту - одна степень конфиденциальности. В простейшем случае субъект может читать информацию только из объектов, степень конфиденциальности которых не выше уровня допуска субъекта, и записывать информацию только в объекты, степень конфиденциальности которых не ниже уровня допуска субъекта.

Из используемых в настоящее время СУБД, в которых реализован механизм мандатного разграничения доступа, две наиболее распростране-

ны: СУБД Линтер Бастион и СУБД Oracle Database Enterprise Edition. Рассмотрим реализованные в них системы мандатного разграничения доступа.

Обозначим степень конфиденциальности таблицы $f_o(o)$, а уровень допуска субъекта $f_s(s)$.

В СУБД Oracle Database Enterprise Edition мандатное разграничение доступа реализовано в подсистеме Oracle Label Security. Разграничение доступа происходит на уровне баз данных, таблиц баз данных и строк таблиц. Каждый выполняемый SQL-запрос анализируется ядром программы, и затем принимается решение о разрешении или отклонении выполнения запроса. Мандатная модель разграничения доступа СУБД Oracle Database Enterprise Edition может быть записана так:

а) $r = read$, $f_s(s) \geq f_o(o)$;

б) $r = write$, $f_s(s) = f_o(o)$.

Условие «а» соответствует ss-свойству модели Белла – ЛаПадула, условие «б» соответствует строгому *- свойству модели Белла – ЛаПадула.

В процессе исследования обнаружено, что в СУБД Oracle некоторые области таблиц, например названия столбцов, не контролируются системой мандатного разграничения доступа. А значит, пользователь может переместить защищаемую информацию в эти области и, таким образом, понизить ее степень конфиденциальности.

В процессе исследований была изучена реализованная в СУБД Линтер Бастион модель мандатного разграничения доступа. Реализация этой модели для таблиц и столбцов баз данных может быть записана так:

а) $r = read$;

б) $r = write, f_s(s) \geq f_o(o)$.

Эти условия не соответствуют модели Белла – ЛаПадула. Любой субъект может прочитать системную информацию о таблице, например узнать ее имя, количество в ней строк, количество столбцов и параметры файлов, в которых записана таблица, и это может способствовать успешной атаке на базу данных с целью похищения защищаемой информации. Любой субъект может модифицировать таблицу более низкой степени конфиденциальности, например изменить имя существующего столбца, записав в него некоторую конфиденциальную информацию. Это также канал утечки информации.

Видно, что любой субъект может получать информацию о таблицах, степень конфиденциальности которых выше уровня допуска субъекта. Эта информация может помочь злоумышленнику осуществить взлом базы данных.

При анализе мандатного разграничения в СУБД Линтер Бастион на уровне полей таблиц баз данных модель мандатного разграничения доступа может быть записана так:

а) $r = read, f_s(s) \geq f_o(o)$;

б) $r = write$, $f_s(s) \geq f_o(o)$.

Условие «а» соответствует ss-свойству модели Белла – ЛаПадула; условие «б» соответствует нестрогому *- свойству модели Белла – ЛаПадула. Здесь также есть канал утечки информации. Субъект может записать информацию высшей степени конфиденциальности в поле низшей степени конфиденциальности, при этом степень конфиденциальности поля остается неизменной, хотя в нем может находиться информация, относящаяся к высшей степени конфиденциальности. Возможна ситуация, когда субъект пытается записать информацию в объект, степень конфиденциальности которого выше уровня допуска субъекта. Такие действия субъекта приводят к повышению степени конфиденциальности объекта. В этом случае хранимая в нем ранее информация становится недоступной для пользователей, которым она была ранее доступна.

В результате изучения моделей мандатного разграничения доступа СУБД Oracle Database Enterprise Edition и СУБД Линтер Бастион выявлены следующие уязвимости, приводящие к нарушению защиты информации:

1. Защищаемая информация может быть перемещена в области таблиц, не контролируемые системой мандатного разграничения доступа, например в имена столбцов таблиц. Возможность помещения защищаемой информации в имена столбцов таблиц является серьезным каналом утечки информации. В имена столбцов таблиц может быть записана любая текстовая информация. Максимальная длина имени столбца в СУБД Линтер Бастион составляет 66 символов [1], в СУБД Oracle Database Enterprise Edition – 30 символов [2]. Решение этой проблемы сводится к установке ограничений на операции изменения имен столбцов таблиц и создания новых столбцов, то есть на операторы ALTER TABLE языка SQL.

2. Возможность завышения степени конфиденциальности информации. Очевидный способ решения проблемы – это установка запрета для субъектов записывать информацию в объекты низшей степени конфиденциальности. Такой запрет понижает удобность работы с СУБД, поэтому нужно также добавить возможность для

субъекта при каждом подключении к базе данных выбрать свой текущий уровень допуска, не превышающий собственный уровень допуска субъекта.

3. Возможность записи информации в поле, степень конфиденциальности которого ниже степени конфиденциальности, к которой относится данная информация. Для решения этой проблемы необходимо запретить для субъектов возможность записи информации в поля, относящиеся к низшей степени конфиденциальности, или предусмотреть автоматическое повышение степени конфиденциальности полей при записи в поля информации высшей степени конфиденциальности.

По результатам анализа реализации систем мандатного доступа в СУБД были сформулированы предварительные требования к разрабатываемой формальной модели:

1) не должны существовать области таблиц баз данных, не контролируемые системой мандатного разграничения доступа, в которые может быть скопирована защищаемая информация;

2) запись информации высшей категории конфиденциальности в таблицы низшей категории конфиденциальности необходимо запретить, чтобы избежать завышения категории конфиденциальности информации, хранимой в таблице.

В основе разрабатываемой формальной модели использована модель разграничения доступа Белла – ЛаПадула. Классическая модель Белла – ЛаПадула была описана в 1975 году и в настоящее время является основной моделью, предназначенной для реализации мандатного разграничения доступа [3, 4]. В классической модели Белла – ЛаПадула анализируются условия, при выполнении которых в компьютерной системе невозможно возникновение информационных потоков от объектов высшей степени конфиденциальности к объектам низшей степени конфиденциальности. Основными элементами классической модели Белла – ЛаПадула являются:

S – множество субъектов;

O – множество объектов;

$B = \{b \subseteq S \times O \times R\}$ – множество возможных множеств текущих доступов в системе;

$R = \{read, write, append\}$ – множество видов доступа и видов прав доступа. Read – доступ на чтение, write – доступ на модификацию, append – доступ на добавление данных;

$(L, \leq)$ – решетка степеней конфиденциальности информации (например, $L = \{l_1, l_2, l_3\}$ [степень конфиденциальности 1, степень конфиденциальности 2, степень конфиденциальности 3)];

$f_s: S \to L$ – функция, задающая уровень допуска субъекта;

$f_o: O \to L$ – функция, задающая степень конфиденциальности объекта.

Система находится в безопасном состоянии, если все доступы субъектов к объектам безопасны. Доступ субъекта к объекту (s,o,r) безопасен, если выполняется, хотя бы одно из следующих условий:

а) $r = read, f_s(s) \geq f_o(o)$ – ss-свойство (свойство простой безопасности);

б) $r = append, f_s(s) \leq f_o(o)$
или $r = write, f_s(s) \leq f_o(o)$ – *-свойство.

Вместо указанного выше *-свойства в модели может быть определено строгое *-свойство следующего вида:

$r = write, f_s(s) = f_o(o)$ или

$r = append, f_s(s) = f_o(o)$.

Суть модели Белла – ЛаПадула состоит в том, что каждый субъект может читать информацию только из объектов, степень конфиденциальности которых равна или ниже уровня допуска субъекта (при использовании строгого *-свойства – только из тех объектов, степень конфиденциальности которых строго равна уровню допуска субъекта), и записывать информацию только в объекты, степень конфиденциальности которых равна или больше уровня допуска субъекта

Сформулируем окончательные требования к разрабатываемой модифицированной модели мандатного разграничения доступа. Модифицированная модель должна соответствовать следующим требованиям:

1) невозможность понижения степени конфиденциальности информации;

2) невозможность повышения степени конфиденциальности информации;

3) защита целостности информации;

4) не должны существовать области таблиц баз данных, не контролируемые системой мандатного разграничения доступа, в которые может быть скопирована защищаемая информация;

5) запись информации высшей степени конфиденциальности в таблицы низшей степени конфиденциальности необходимо запретить, чтобы избежать завышения степени конфиденциальности информации, хранимой в таблице.

Реализация данной модели мандатного раз-

граничения доступа должна обеспечивать следующие требования:

1) соответствие реализации созданной модифицированной модели мандатного разграничения доступа;

2) минимальное ухудшение производительности системы при работе механизма мандатного разграничения доступа;

3) корректность совместной работы механизма мандатного разграничения доступа и механизма дискреционного разграничения доступа в СУБД;

4) защищаемые объекты СУБД и БД: базы данных, таблицы баз данных, строки таблиц, представления, хранимые процедуры и триггеры.

Теоретические исследования. Как видно из изложенного выше, разработка модифицированной модели мандатного разграничения доступа состоит из двух основных частей: разработка формальной модели модифицированной модели мандатного разграничения доступа и ее реализация в СУБД Microsoft SQL Server.

Для реализации в формальной модели определим множество объектов доступа, множество субъектов доступа и множество операций, которые субъекты доступа могут выполнять над объектами доступа.

Объект доступа – это единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа [5]. Правила разграничения доступа – это совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа [5].

В СУБД Microsoft SQL Server имеются следующие объекты доступа:

- файлы баз данных;
- базы данных;
- таблицы баз данных;
- столбцы таблиц;
- строки таблиц;
- хранимые процедуры;
- представления;
- триггеры.

В качестве объектов доступа при реализации модифицированной модели мандатного разграничения доступа выбраны таблицы, строки таблиц, представления, триггеры.

Субъект доступа – это лицо или процесс, действия которого регламентируются правилами разграничения доступа [5]. Субъектами разграничения доступа в СУБД Microsoft SQL Server являются пользователи, процессы, запускаемые пользователями, и программы. Все эти субъекты доступа в Microsoft SQL Server представлены учетными записями пользователей, поэтому можно рассматривать учетные записи пользователей как субъекты разграничения доступа в СУБД. В процессе работы субъекты доступа могут выполнять следующие действия над объектами доступа:

– над базами данных – создание (create database), удаление (drop database), изменение свойств (alter database). Вследствие ограничений СУБД Microsoft SQL Server невозможно контролировать операции переименования баз данных. Однако эти операции можно ограничить, используя системы дискреционного и ролевого разграничения доступа;

– над таблицами баз данных – создание (create table), удаление (drop table), изменение (alter table);

– над строками таблиц – выборка (select), удаление (delete), обновление (update), добавление (insert);

– над хранимыми процедурами – создание (create procedure), удаление (drop procedure), изменение (alter procedure);

– над представлениями – создание (create view), удаление (drop view), изменение (alter view);

– над триггерами – создание (create trigger), удаление (drop trigger), изменение (alter trigger).

Определим формальные операции read, write и append через операции СУБД Microsoft SQL Server. Определение этих операций приведено в таблице 1.

Таблица 1

Объект доступа	Операция read	Операция write	Операция append
База данных	–	изменение удаление	–
Таблица	–	изменение удаление	вставка
Строка в таблице или представление	выборка	удаление обновление	–
Столбец в таблице	выборка	удаление обновление	–
Хранимая процедура	–	изменение удаление	–
Представление	–	изменение удаление	–
Триггер	–	изменение удаление	–

Введем формальные обозначения для объектов доступа. Формальные обозначения для объектов доступа представлены в таблице 2.

Таблица 2

Объект	Обозначение множества объектов
База данных	B (database)
Таблица	T (table)
Строка	W (row)
Хранимая процедура	P (procedure)
Представление	V (view)
Триггер	E (trigger)

Формальная модель модифицированной модели мандатного разграничения доступа включает условия для выполнения операций над соответствующими объектами СУБД и БД, имеющими следующий вид:

1) $r = write, f_s(s) = f_o(o)\ \ \forall b \in B$;
2) $r = write, f_s(s) = f_o(t)$;
3) $r = append, f_s(s) \le f_o(t)\ \ \forall t \in T$;
4) $r = read, f_s(s) \ge f_o(r)$;
5) $r = write, f_s(s) = f_o(w)\ \ \forall w \in W$;
6) $r = write, f_s(s) = f_o(p)\ \ \forall p \in P$;
7) $r = write, f_s(s) = f_o(v)\ \ \forall v \in V$;
8) $r = write, f_s(s) = f_o(e)\ \ \forall e \in E$.

Из этих условий видно, что степень конфиденциальности строки таблицы не может быть задана ниже степени конфиденциальности таблицы, в состав которой входит эта строка, а степень конфиденциальности таблицы не может быть задана ниже степени конфиденциальности базы данных, в состав которой входит эта таблица.

Для базы данных задано лишь условие 1 для операции write. Это объясняется тем, что для базы данных определена лишь эта операция. Условие задано таким образом, что только пользователь с уровнем допуска, равным степени конфиденциальности базы данных, может выполнить операцию write над базой данных. Благодаря этому выполняется требование о невозможности записи защищаемой информации в области баз данных, не контролируемые системой мандатного разграничения доступа. В данном случае такой областью могло быть, например, имя базы данных. Однако даже это поле теперь должно контролироваться системой мандатного разграничения доступа.

Для таблицы заданы два условия: 2 и 3. Первое условие на операцию write задано таким образом, что только пользователи с уровнем допуска, равным степени конфиденциальности таблицы, могли изменить свойства таблицы: например, удалить столбцы, добавить новые или переименовать их. Это также обеспечивает выполнение требования о невозможности записи защищаемой информации в области, не контролируемые системой мандатного разграничения доступа. Второе условие на операцию append позволяет добавлять новые строки в таблицу только тем пользователям, уровень допуска которых не выше степени конфиденциальности информации. Таким образом, пользователь не может записать в таблицу низшей степени конфиденциальности информацию, относящуюся к высшей степени конфиденциальности, повысив, таким образом, степень конфиденциальности таблицы. Благодаря этому выполняется требование о невозможности неправомерного повышения степени конфиденциальности хранящейся в базе данных информации.

Для строки таблицы заданы два условия: 4 и 5. Первое условие на операцию read позволяет читать информацию, содержащуюся в строке, только тем пользователям, уровень допуска которых не ниже степени конфиденциальности этой строки. Второе условие на операцию write позволяет записывать информацию в строку только тем пользователям, уровень допуска которых равен степени конфиденциальности строки.

Для хранимой процедуры заданы два условия: 6 и 7. Первое условие на операцию write позволяет изменять код хранимой процедуры только тем пользователям, уровень допуска которых равен степени конфиденциальности хранимой процедуры. Второе условие на операцию append позволяет запускать хранимую процедуру на выполнение только тем пользователям, уровень допуска которых равен степени конфиденциальности хранимой процедуры. Такое жесткое требование необходимо потому, что в ходе выполнения хранимой процедуры могут выполняться операции чтения и записи данных.

Для представления задано одно условие 8. Это условие позволяет изменять код представления только тем пользователям, уровень допуска которых равен степени конфиденциальности представления.

Так как в модели не предусмотрено разрешение выполнения записи данных пользователями с высшим уровнем допуска в объекты низ-

шей степени конфиденциальности (то есть условия созданной модели мандатного разграничения доступа, регламентирующие выполнение операций записи данных, соответствуют строгим *-свойствам модели Белла – ЛаПадула), то требование о необходимости повышения степени конфиденциальности объекта при записи в него информации, относящейся к высшей степени конфиденциальности, для данной модели мандатного разграничения доступа не имеет значения.

Экспериментальные исследования. Предложенная модифицированная модель мандатного разграничения доступа реализована на основе представлений, триггеров DDL и триггеров DML.

Для работы модифицированной модели мандатного разграничения доступа необходимо создать специальные таблицы. Степени конфиденциальности всех объектов базы данных, кроме строк таблиц, хранятся в специальной таблице objlevels в каждой базе данных. Метки доступа строк таблиц хранятся в самих таблицах, в столбцах rowlevel. Уровни допуска всех пользователей СУБД хранятся в таблице userlevels в базе данных master. Степени конфиденциальности триггеров уровня сервера хранятся в таблице triggerlevels в базе данных master. Также в базе данных master существует специальная таблица mac, в которой хранится служебная информация, использующаяся только триггерами системы мандатного разграничения доступа при ее работе. Из вышеперечисленных таблиц следующие должны быть созданы администратором СУБД вручную перед началом использования системы мандатного разграничения доступа в СУБД userlevels, mac, triggerlevels.

Остальные таблицы создаются автоматически триггерами системы мандатного разграничения доступа при ее работе. Столбцы rowlevel для каждой созданной пользователем таблицы и представления для каждой созданной пользователем таблицы, необходимые для доступа пользователей к таблицам, также создаются автоматически.

В таблице userlevels хранятся имена пользователей СУБД и их уровни допуска.

При работе системы мандатного разграничения доступа при создании каждой таблицы в пользовательской базе данных в этой базе данных должно быть автоматически создано представление особого вида с именем, соответствующим имени таблицы с приставкой “mac”. Принцип работы представления: из таблицы userlevels извлекается уровень допуска текущего пользователя, затем из защищаемой таблицы выбираются только те строки, значения степени конфиденциальности которых, хранящиеся в столбце rowlevel, не превышают уровня допуска текущего пользователя – в соответствии с условием 4 формальной модели модифицированной модели мандатного разграничения доступа.

Для проверки работоспособности реализованной модифицированной модели мандатного разграничения доступа была разработана специальная тестовая база данных.

В соответствии с правилами, реализованными в модифицированной модели мандатного разграничения доступа, пользователем были выполнены операции над объектами базы данных. Результаты экспериментов показали правильность реализации условий для выполнения операций над соответствующими объектами СУБД и БД. Также были выполнены проверки требований об отсутствии таких областей таблиц баз данных, в которые возможно записать любые данные независимо от уровня допуска пользователя и степени конфиденциальности таблицы. Результаты показали, что записать данные в имена столбцов таблицы невозможно, если уровень допуска пользователя не равен степени конфиденциальности таблицы, т.е. требование выполнено.

Для вычисления степени ухудшения производительности СУБД при использовании системы мандатного разграничения доступа на основе модифицированной модели необходимо сравнить время в миллисекундах выполнения некоторых операций в СУБД, в которой не используется разработанная система мандатного разграничения доступа, с временем их выполнения в СУБД, в которой используется разработанная система мандатного разграничения доступа. Наиболее часто производимые при работе СУБД операции – это операции чтения, изменения и удаления данных из таблиц и представлений, поэтому наибольшего замедления системы необходимо ожидать именно при выполнении этих операций.

Конфигурация персонального компьютера, на котором запущена СУБД Microsoft SQL Server, использованная для проведения измерений процессор AMD Athlon, мощность 1.30 ГГц, оперативная память 256 МБ.

В результате экспериментов было получены следующие результаты. При выполнении оператора insert время выполнения запроса увеличивается на 4,33 % (для 1000 строк), при выполнении оператора select – на 2,35 % (для 1.000.000 строк), при выполнении оператора update – на 8,92 % (для 100.000 строк), а при выполнении оператора delete – на 15,92 % (для 1.000.000 строк). Таким образом, степень ухудшения производительности системы невелика.

Выводы. Разработана формальная модель мандатного разграничения доступа, являющаяся адаптацией модели Белла – ЛаПадула для баз данных. В модели Белла – ЛаПадула определяется общий подход к построению систем, реализующих мандатную политику безопасности. В разработанной формальной модели мандатного разграничения доступа учитываются структура хранения информации в базах данных, объекты доступа баз данных, операции, совершаемые субъектами доступа над объектами доступа баз данных. Предложенная модель реализует требования безопасности мандатной модели разграничения доступа и требования безопасности, сформулированные в данной работе.

На основе модифицированной модели реализована система мандатного разграничения доступа для СУБД Microsoft SQL Server. Система мандатного разграничения доступа контролирует операции работы с базами данных, таблицами баз данных, строками таблиц, хранимыми процедурам, представлениями и триггерами.

Разработанная формальная модель мандатного разграничения доступа и реализация на ее основе системы мандатного разграничения доступа позволяют повысить защищенность информации, хранимой в базах данных, за счет ликвидации каналов утечки информации, позволяющих создавать потоки информации от объектов с большей степенью конфиденциальности к объектам с меньшей степенью конфиденциальности.

Ухудшение производительности в процессе функционирования системы мандатного разграничения доступа на основе модифицированной модели мандатного разграничения доступа несущественное.

К достоинствам данной модели можно отнести простоту ее установки для администраторов и прозрачность ее работы для пользователей СУБД Microsoft SQL Server. Кроме того, реализация этой модели не затрагивает системных таблиц СУБД Microsoft SQL Server, что не требует пересертификации СУБД Microsoft SQL Server при использовании ее в автоматизированных системах.

Библиографический список

1. Основные характеристики СУБД Линтер Бастион (с Интернет-сайта http://www.linter.ru/);

2. Database Object Names and Qualifiers - Oracle® Database SQL Language Reference 11g Release 2 (11.2) (с Интернет-сайта http://www.oracle.com/);

3. *Девянин П.Н.* Модели безопасности компьютерных систем: учеб. пособие для студ. высш. учеб. заведений / Петр Николаевич Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.

4. Looking Back at the Bell-La Padula Model (David Elliot Bell, Reston VA, 20191, December 7, 2005);

5. Руководящий документ Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения».