УДК 62.529

И.А. Бойченко, В.Г. Сарайкин

ИНТЕГРИРОВАННАЯ МОДЕЛЬ ПОЛИТИК БЕЗОПАСНОСТИ В СУБД

Для обеспечения санкционированного доступа пользователей СУБД к информационным объектам предложена интегрированная модель политик безопасности.

Ключевые слова: СУБД, отраслевые информационно-аналитические системы, модели, метки безопасности.

Современный этап развития лесопромышленного комплекса характеризуется его информатизацией, социально-экономические последствия которой определяют приоритетные направления научных исследований в области разработки информационно-аналитических и торговых систем. Эти направления ориентированы на создание эффективного инструментария, способного помочь пользователю в принятии корректных управленческих и регулирующих решений любой сложности и уровня, в различных сферах деятельности, локального и глобального масштабов. Основой такого инструментария служит «коллективный разум», или коллективные знания, хранящиеся в распределенных компьютерных системах и поддерживаемые современными системами управления базами данных (СУБД) и базами знаний.

Ярким примером отраслевой информационно-аналитической системы является глобальная информационно-аналитическая торговая система лесопромышленного комплекса (ГИАТС), разработанная при участии специалистов ОАО «Рослеспром», Государственного научного центра лесопромышленного комплекса, авторов данной статьи и др.

Защита ресурсов указанной информационной системы, как и других аналогичных систем, является недостаточно изученной и крайне сложной задачей. Традиционно технологии безопасности баз данных всегда отстают от других областей, таких, как сети и телекоммуникации.

С целью восполнения указанного пробела для обеспечения санкционированного доступа пользователей СУБД к информационным объектам нами предложены интегрированная модель политик безопасности на основе моделей HRU (Харрисон-Руззо-Ульман) и BLP (Белла-Ла Падула) и их модификаций и организация меток безопасности объектов, соответствующие дискреционным и мандатным моделям контроля доступа, действующим совместно. Приоритет указанных предложений подтвержден патентом РФ.

Для подобного класса систем использована модель $Q(\mathrm{CMS}) = \{(E, R, V, D)\}$ – информационная система с контролируемым пространством памяти, определяемая следующими составляющими.

Элементы доверенной среды:

конечные наборы исходных субъектов $S_0 = \{s_1, \ldots, s_N\}$ и объектов $O_0 = \{o_1, \ldots, o_M\}$, где $S_0 \subseteq O_0$;

набор типов объектов $V = \{v_1, \ldots, v_g\}$;

конечный набор прав доступа $R_l = [\, r_{ij}^{l} \,]$ – матрицы прав i-й сущности по отношению к j-й сущности для l-го действия, где $l = 1, \ldots, K$; $i = 1, \ldots, M$; $j = 1, \ldots, N$;

исходная матрица R, содержащая права доступа субъектов к объектам, и ее начальное состояние R_0;

конечный набор команд $F = \{f(e_1 : v_1, \ldots, e_s : v_s)\}$, включающий условия выполнения команд и их интерпретацию в терминах элементарных операций;

множество действий над сущностями $D = \{d_1, \ldots, d_K\}$.

Функции изменения состояния:

функция уровней безопасности $G : SUO \to L$ (ставит в соответствие каждому объекту и субъекту уровень безопасности из множества L;

функция управления уровнями $G : SUO \to P(S)$ (где $P(S)$ – множество всех подмножеств субъектов S, которым позволено изменять уровень безопасности для заданного объекта или субъекта;

функция перехода $T : (Q \times D) \to Q$, которая в ходе выполнения действия переводит систему из одного состояния в другое (система, находящаяся в состоянии $q \in Q$, при получении запроса $d \in D$ переходит в следующее состояние $q^* = T(q, d)$.

Модель системы $F(q_0, D, T)$ состоит из начального состояния q_0, множества действий D и функции перехода T.

Производные составляющие доверенной среды для групповых субъектов:

групповые субъекты – множество непустых подмножеств S, которое обозначим $\check{S} = P(S)\backslash\{\varnothing\}$;

права групповых субъектов $\check{R}$;

функции уровня безопасности объектов $G : SUO \to L$, для групповых субъектов получим $\breve{G}^{L} : \check{S} \to L$ ($\breve{G}^{L}(\check{s})$– наибольшая нижняя граница множества $\mathrm{Max}L\{G(s) \mid s \in \check{s}\}$) и $\breve{G}^{H} : \check{S} \to L$ ($\breve{G}^{H}(\check{s})$ – наименьшая верхняя граница множества $\mathrm{Min}H\{G(s) \mid s \in \check{s}\}$);

функция перехода, которая определяет следующее состояние системы после выполнения определенным субъектом некоторого запроса, как $\check{T}$: $(Q \times D) \to Q$, где $\check{T}(q, d) = q^*$; при этом в описании состояния $q = ((G, \breve{G}^{H}, \breve{G}^{L}), \check{R})$ и $q^* = (G^*, \breve{G}^{*H}, \breve{G}^{*L})^*, \check{R}^*)$ участвуют три функции уровня безопасности: G – для объектов, $\breve{G}^{H}$ и $\breve{G}^{L}$ – наименьшая верхняя и наибольшая нижняя границы для групповых субъектов.

Обеспечиваемый критерий безопасности для совместного доступа мандатной модели формулируется следующим образом.

Система $F(q_0, D, \check{T})$ безопасна тогда и только тогда, когда:

– начальное состояние q_0 безопасно;

– функция перехода $\check{T}$ такова, что для любого состояния q, достижимого из q_0 путем применения конечной последовательности действий из D, таких, что $\check{T}(q, d) = q^*$, $q = ((G, \breve{G}^H, \breve{G}^L), \check{R})$ и $q^* = (G^*, \breve{G}^{*H}, \breve{G}^{*L})^*, \check{R}^*)$ для каждого $\forall \check{s} \in \check{S}$, $\forall o \in O$ выполняются следующие условия:

если $d(\text{read}) \in \check{R}^*[\check{s}, o]$ и $d(\text{read}) \notin \check{R}^*[\check{s}, o]$, то $\breve{G}^{*L}(\check{s}) \geq G^*(o)$;

если $d(\text{read}) \in \check{R}[\check{s}, o]$ и $\breve{G}^{*L}(\check{s}) < G^*(o)$, то $d(\text{read}) \notin \check{R}^*[\check{s}, o]$;

если $d(\text{write}) \in \check{R}^*[\check{s}, o]$ и $d(\text{write}) \notin \check{R}[\check{s}, o]$, то $G^*(o) \geq \breve{G}^{*H}(\check{s})$;

если $d(\text{write}) \in \check{R}[\check{s}, o]$ и $G^*(o) < \breve{G}^{*H}(\check{s})$, то $d(\text{write}) \notin \check{R}^*[\check{s}, o]$.

В классической дискреционной модели используют следующие базовые элементарные операции, определяющие переход из одного состояния в другое, отличающееся от исходного, по крайней мере, одним компонентом.

1) Создание права M-й сущности по отношению к N-й сущности для K-го действия:

$$r_{MN}^K = p_1(s \in S, o \in O); \quad O' = O; \quad S' = S; \quad v'(o) = v(o) \ (o \in O);$$

$$R_l'[r_{ij}^l] = R_l[r_{ij}^l] \ (i \neq M) \ \forall (j \neq N) \ \forall (l \neq K); \ R_l'[r_{ij}] = R_l[r_{ij}] \cup \{r_{MN}^K\}.$$

2) Удаление права у M-й сущности по отношению к N-й сущности для K-го действия:

$$r_{MN}^K = p_2(s \in S, o \in O); \quad O' = O; \quad S' = S; \quad v'(o) = v(o) \ (o \in O);$$

$$R_l'[r_{ij}^l] = R_l[r_{ij}^l] \ (i \neq M) \ \forall (j \neq N) \ \forall (l \neq K); \quad R_l'[r_{ij}] = R_l[r_{ij}] \setminus \{r_{MN}^K\}.$$

3) Создание M-й сущности – субъекта типа $v_g (s \notin S)$:

$$O' = O \cup \{s_M\}; \ S' = S \cup \{s_M\}; \ v'(o) = v(o) \ (o \in O); \ v'(s) = v_g;$$

$$R_l'[r_{ij}^l] = R_l[r_{ij}^l] \quad (o, s) \in S \times O; \ R'_l[r_{Mj}] = p_4.$$

4) Удаление M-й сущности – субъекта $(s \in S)$:

$$O' = O \setminus \{s_M\}; \ S' = S \setminus \{s_M\}; \ v'(o) = v(o) \quad (o \in O); \ v'(s) \text{ – не определено};$$

$$R_l'[r_{ij}^l] = R_l[r_{ij}^l] \quad (o, s) \in S' \times O; \ R'_l[r_{Mj}] = p_4.$$

5) Создание M-й сущности – объекта типа $v_g (o \notin O)$:

$$O' = O \cup \{s_M\}; \quad S' = S \cup \{s_M\}; \quad v'(o) = v(o) \ (o \in O'); \quad v'(o) = v_g;$$

$$R_l'[r_{ij}^l] = R_l[r_{ij}^l] \ (o, s) \in S \times O; \ R'_l[r_{Mj}] = p_4.$$

6) Удаление M-й сущности – объекта $(o \in O \setminus S)$:

$$O' = O \setminus \{o_M\}; \quad S' = S; \ v'(o) = v(o) \ (o \in O'); \quad v'(o) \text{ – не определено};$$

$$R_l'[r_{ij}^l] = R_l[r_{ij}^l] \ (o, s) \in S' \times O'; \ R'_l[r_{Mj}] = p_4.$$

Сформулируем критерий безопасности данной дискреционной модели.

Для заданной системы начальное состояние $F_0 = (S_0, O_0, V_0, R_0)$ является безопасным относительно права r, если не существует применимой к F_0

последовательности команд, в результате которой право r будет занесено в ячейку матрицы R, в которой оно отсутствовало в состоянии F_0.

Указанная задача является разрешимой в следующих случаях:

команды $f(e_1 : v_1, \quad , e_s : v_s)$ являются монооперационными, т.е. состоят не более чем из одной элементарной операции;

команды $f(e_1 : v_1, \quad , e_s : v_s)$ являются ациклическими и монотонными, т.е. граф создания сущностей не содержит циклов и операций удаления (2, 4, 6);

команды $f(e_1 : v_1, \quad , e_s : v_s)$ не содержат операций создания (3, 5).

Состояние системы изменяется с помощью команд из множества F, состоящего из набора условий и операций, составляющих команду. Команды имеют формат:

command $f(e_1 : v_1, \quad , e_s : v_s)$

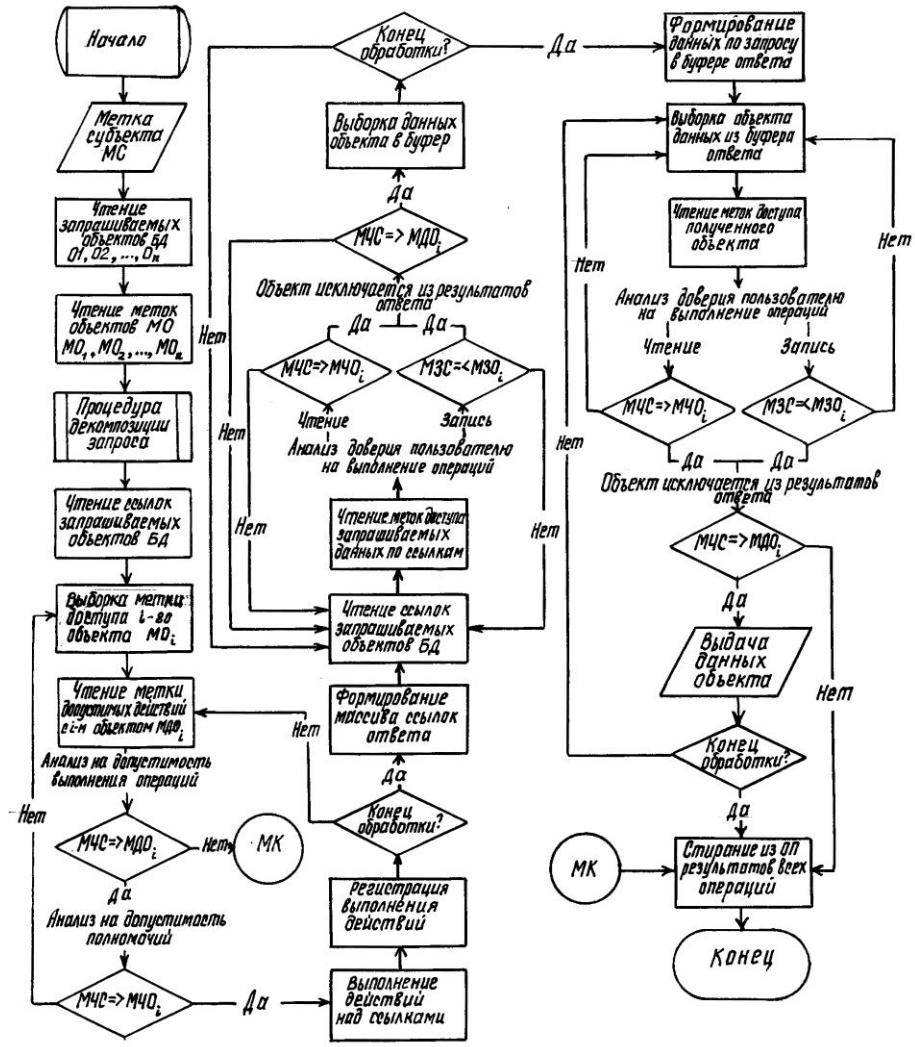
if p_1 in $R_1[r_{ij}]$ and (условия выполнения команды)

then

$c_1, c_2, \ldots c_G$, (операции, составляющие команду), где всем параметрам приписывается определенный тип.

Перед выполнением команды происходит проверка типов фактических параметров, если они не совпадают с указанными в определении, команда не выполняется. Фактически, введение контроля типов для параметров команд приводит к неявному введению дополнительных условий, так как команды могут быть осуществлены только при совпадении типов параметров.

Для обеспечения санкционированного доступа пользователя СУБД к информационным объектам автоматизированной системы предложен способ организации меток объектов, соответствующий модели мандатной политики безопасности. На рисунке приведен укрупненный алгоритм процедуры контроля и управления доступом (процедура МАСО).



Укрупненный алгоритм процедуры контроля и управления доступом (Метка объекта МО включает: группу субъекта, который внес данный объект; уровень доступа на чтение – МЧО; уровень доступа на запись – МЗО. Метка субъекта МС включает: группу, к которой принадлежит субъект; максимальный уровень доступной субъекту информации – МЧС; минимальный уровень объекта, который может быть создан данным субъектом – МЗС

Предложен способ дополнительного структурирования пользователей с введением группы доступа (группы субъекта); иерархии по уровням доступа (десять уровней от 1 до 10); иерархии по уровням доверия (десять уровней от 1 до 10).

Группа субъекта (допущенного до работы пользователя) указывает на его принадлежность к группе субъектов по доступу (принадлежность к группе людей, объединенных одними функциями). Группа назначается субъекту в со-

ответствии с правилами политики безопасности, при этом возможно перемещение субъекта из одной группы в другую.

Введена возможность организации до 250 индексированных групп с номерами от 1 до 250.

Данным (объектам) присваивается метка группы пользователей (субъектов), которые их сформировали. Данные, принадлежащие одной группе пользователей, не доступны пользователям другой группы.

Однако группа может доверить другой группе работу со своими данными.

Уровень доступа субъекта задается при его создании (администратором безопасности) или изменяется позже. Он определяет: какие данные (по уровню конфиденциальности) доступны субъекту, а какие нет. Все данные с уровнем конфиденциальности более высоким, чем уровень доступа конкретного субъекта, скрываются.

Уровень доверия субъекта определяется в соответствии с правилами действующей политики безопасности и обозначает важность (т.е. конфиденциальность) данных, вносимых субъектом. СУБД не должна позволять субъекту вносить информацию в объект с низким (чем уровень доверия субъекта) уровнем конфиденциальности.

Этот уровень призван защитить пользователей с высоким уровнем доверия от случайного (или намеренного) присвоения секретным данным низкого уровня конфиденциальности. Любая вносимая (изменяемая) этим субъектом информация уже будет иметь минимальный «гриф» или уровень конфиденциальности. Его информация может быть только более (не менее) защищенной.

В доверенной среде СУБД «ЛИНТЕР» обеспечена возможность совместной реализации дискреционной и мандатной политик безопасности.

При этом действуют два глобальных правила:

доступ к объектам, поддерживаемым и дискреционной, и мандатной политиками безопасности, должен быть санкционирован ими обеими;

субъект не может ни получить доступ к объекту, к которому применены две политики безопасности, ни управлять доступом к этому объекту, если он не имеет доступа к нему в одной из политик безопасности.

В этом отношении среди пользователей выделяется только уполномоченный администратор безопасности, который может изменять метки доступа пользователей (но не данные и их метки).

В дискреционном контроле доступа для каждой пары субъект–объект можно задать явное и недвусмысленное перечисление возможных действий субъекта:

SELECT – чтение данных объекта;

INSERT – добавление новых данных в объект;

DELETE – удаление некоторых/всех данных объекта;

UPDATE – изменение данных объекта;

ALTER – изменение физической / логической структуры базовой таблицы;

INDEX – создание/удаление индексов на столбцы базовой таблицы;

ALL – все возможные действия, т.е. все предыдущие действия вместе взятые.

В профессиональных базах данных (БД), где много (тысячи) субъектов и объектов, очень сложно определять возможности (или права) каждого субъекта при работе с каждым объектом. Для упрощения этой процедуры реализуется аппарат ролей. С помощью аппарата ролей можно строить не только иерархические взаимоотношения пользователей (старший – подчиненный), но и вообще произвольную структуру доступа. Предусмотрена следующая схема построения ролей:

создать роль (значит стать ее владельцем) может только субъект Dba-категории (администратор БД);

назначить/изъять роль может только ее владелец/создатель.

Таким образом, могут присутствовать две схемы передачи прав: прямая и косвенная, через аппарат ролей. Причем обе эти схемы можно использовать в совокупности.

В мандатном методе контроля управление доступом строится на основе меток конфиденциальности или меток безопасности. Эти метки хранятся вместе с объектом и играют важную роль при разрешении (допуске) субъектов к информации помеченного объекта.

В результате применения меток безопасности объектов получается гибкая система разделения полномочий субъектов при администрировании данных и прав доступа в СУБД. Для этого в автоматизированной системе присутствуют две независимые категории администраторов – администратор БД и администратор прав доступа. С помощью комбинированных средств и методов контроля, разделенных во времени и пространстве независимых процедур установки параметров безопасности, обеспечивается эффективная защита данных.

ДальНИИЛХ
Поступила 15.12.02

I.A. Boichenko. V.G. Sarajkin

Integrated Model of Security Policy in Database Management System

An integrated security policy model has been proposed for ensuring an authorized access of database management system users to the informational objects.