УДК 004.02

05.00.00 Технические науки

ПРЕДСТАВЛЕНИЕ ПОЛИТИКИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА ЧЕРЕЗ МОДЕЛЬ ХАРРИСОНА-РУЗЗО-УЛЬМАНА

Королев Игорь Дмитриевич
доктор технических наук, профессор
РИНЦ (SPIN –код: 3629-2713)

Поддубный Максим Игоревич
РИНЦ (SPIN – код: 4293-2165)

Филиал Военной академии связи (г. Краснодар), Краснодар, Россия

В защищенной автоматизированной информационной системе принятую модель разграничения доступа реализует монитор безопасности. Модели безопасности рассматриваются, как правило, в отношении системы, которая представляет собой единое целое и имеет единый монитор безопасности. Тем не менее, архитектура реальных автоматизированных информационных систем и процессы их функционирования могут характеризоваться распределенностью. Распределенная автоматизированная информационная система состоит более чем из одного локального сегмента, представляющего собой обособленную совокупность субъектов и объектов доступа. В распределенной системе локальные сегменты могут быть реализованы как на основе дискреционных, так и на основе мандатных моделей безопасности (т.е. являться разнородными). Одним из направлений обеспечения безопасности в данном случае является реализация общего монитора безопасности, обеспечивающего единую (согласованную) политику разграничения доступа. Для безопасного взаимодействия разнородных систем необходимо сведение их к единой модели. Следовательно, при объединении информационных систем неизменно становиться проблема организации их взаимодействия. При этом в системах, обрабатывающих информацию различного уровня конфиденциальности, необходимо реализовать мандатное разграничения доступа. В данной статье мандатная политика безопасности, представленная классической моделью Белла-ЛаПадула, описывается элементами классической модели Харрисона-Руззо-Ульмана. С использованием механизмов изменения матрицы доступов описывается возможность присвоения и изменение меток конфиденциальности, анализируется соблюдение свойств безопасности

UDC 004.02

Technical sciences

PRESENTATION OF MANDATORY POLICY OF ACCESS CONTROL VIA THE HARRISON-RUSSO-WILLIAM'S MODEL

Korolyov Igor Dmitrievich
Dr.Sci.Tech., professor
Russian Science Citation Index (SPIN-code: 3629-2713)
Poddubny Maksim Igorevich
Russian Science Citation Index (SPIN-code: 4293-2165)
Branch of the Military Academy of connection, Krasnodar, Russia

The accepted model of the access control is realized with the monitor of safety in the protected automated information system. Models of safety are considered, as a rule, as a system which is a single whole and has the uniform monitor of safety. Nevertheless, the architecture of the real automated information systems and processes of their functioning can be characterized by distribution. The distributed automated information system consists more than of one local segment representing isolated set of subjects and objects of access. In the distributed system local segments can be realized both on the basis of discretionary, and on the basis of mandatory models of safety (i.e. to be diverse). One of directions of a safety in this case is realization of the general monitor of the safety providing the uniform (coordinated) policy of access control. For safe interaction of patchwork systems it's necessary to bring them to a single model. Hence, while the integration of information systems the problem of their interaction becomes persistent. Thus in the systems processing the information of a various level of confidentiality, it is necessary to realize mandatory access control. In given clause the mandatory policy of the safety presented by classical model of Bell-LaPadula, is described by the elements of classical model of Harrison-Russo-William. Using the mechanisms of change of a matrix access the opportunity of assignment and change of confidentiality marks is described and the observance of safe practices within the limits of mandatory access control is analyzed. The safety of application of the given approach has been proved. The perspective direction of research has been defined

в рамках мандатного разграничения доступа. Доказывается безопасность применения данного подхода. Определяется перспективное направление исследования

Ключевые слова: БЕЗОПАСНОСТЬ ИНФОРМАЦИИ, МАНДАТНАЯ ПОЛИТИКА БЕЗОПАСНОСТИ, ДИСКРЕЦИОННАЯ ПОЛИТИКА БЕЗОПАСНОСТИ, РАЗГРАНИЧЕНИЕ ДОСТУПА

Keywords: INFORMATION SECURITY, MANDATORY SECURITY POLICY , DISCRETIONARY SECURITY POLICY, ACCESS CONTROL

ПРЕДСТАВЛЕНИЕ ПОЛИТИКИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА ЧЕРЕЗ МОДЕЛЬ ХАРРИСОНА-РУЗЗО-УЛЬМАНА

Интегральную совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает состояние защищенности информации в заданном пространстве угроз, называется политикой безопасности. Выделяют две основные (базовые) политики безопасности – дискреционная и мандатная. Формальное выражение политики безопасности (математическое, схемотехническое, алгоритмическое и т.д.) называется моделью безопасности [1].

Согласно основной аксиомы теории защиты информации, все вопросы безопасности информации описываются доступами субъектов к объектам [2]. Из основных критериев оценки безопасности следует, что все системы разграничения доступа (СРД) должны быть спроектированы на основе математических моделей.

В защищенной системе принятую модель разграничения доступа осуществляет монитор безопасности. Рассмотрение моделей безопасности, как правило, позиционируются в отношении системы, которая представляет из себя единое целое (монолитная система) и имеет единый монитор безопасности. Тем не менее, архитектура реальных автоматизированных информационных систем и процессы их функционирования могут характеризоваться распределенностью. Распределенной автоматизированной информационной системой

называется система, состоящая более чем из одного локального сегмента, представляющего собой обособленную совокупность субъектов и объектов доступа [2]. В распределенной системе локальные сегменты могут быть реализованы как на основе дискреционных, так и на основе мандатных моделей безопасности (т.е. являться разнородными). Одним из направлений обеспечения безопасности в данном случае является реализация общего монитора безопасности, обеспечивающего единую (согласованную) политику разграничения доступа.

Для безопасного взаимодействия разнородных систем необходимо сведение их к единой модели. Следовательно, при объединении информационных систем неизменно становиться проблема организации их взаимодействия [1].

Т. к. объединяемые автоматизированные информационные системы могут реализовывать разные политики безопасности, изучение взаимодействия разнородных моделей безопасности является **актуальной задачей**.

В моделях, реализующих мандатную политику безопасности, разграничение доступа осуществляется на основе присвоенных всем субъектам и объектам системы меток конфиденциальности. При этом ограничения не распространяются на сущности одного уровня. Для разграничения доступа в пределах одной степени конфиденциальности (доступа) применяется дискреционная политика безопасности. Из данного утверждения можно сделать вывод, что дискреционное разграничение доступа можно рассматривать, как частный случай мандатной политики безопасности информационной системы, в которой все сущности одинаковой степени конфиденциальности (уровня доступа). Следовательно, описание объединения разнородных моделей безопасности возможно приведением мандатного разграничения доступа к дискреционному. Однако, устранение негативного информационного

потока от объектов с большим уровнем конфиденциальности к меньшим - выполняется в мандатном разграничении доступа. Следовательно, для автоматизированных информационных систем, обрабатывающих информацию разного уровня конфиденциальности, приемлемым является мандатное разграничение доступа.

Для сведения разнородных моделей к мандатному разграничению доступа необходимо выразить его через модель, описывающую дискреционную политику безопасности.

Для анализа взаимодействия разнородных систем в качестве примера реализации дискреционного разграничения доступа рассмотрим классическую модель Харрисона-Руззо-Ульмана (ХРУ), мандатного – классическую модель Белла-ЛаПадула (БЛП).

Цель работы – представить классическую модель БЛП элементами классической модели ХРУ.

Объектом исследования при этом является классическая модель безопасности ХРУ.

Предметом исследования являются свойства модели ХРУ позволяющие описать мандатное разграничение доступа.

Для достижения поставленной цели определим следующие **задачи**:

представить мандатное разграничение доступа (модель БЛП) элементами модели ХРУ;

определить перспективы применения данного подхода при объединении автоматизированных информационных систем, реализующих разнородные модели безопасности;

определить дальнейшее направление исследования.

Применение механизмов изменения матрицы доступов ХРУ для описания мандатного разграничения доступов обладает **научной новизной**.

Классическая модель Белла-ЛаПадула состоит из следующих элементов [3]:

$O = \{o_j\}$, где $j = \overline{1,J}$ – множество объектов системы;

$S = \{s_i\}$, где $i = \overline{1,I}$ – множество субъектов системы;

$R = \{r_z\}$, где $z = \overline{1,Z}$ – множество видов прав доступа субъектов на объекты;

M – матрица доступов, строки которой соответствуют субъектам, а столбцы – объектам. M[s,o]⊆R, где R – права доступа субъекта s_i на

o

объект ;

– множество возможных множеств текущих доступов в системе, где – множество текущих доступов в системе;

$(L, \leq)$ – решетка уровней конфиденциальности, например $L = \{Un(unclussified), Sc(secret), TSc(top\ secret)\}$, где $Un < Sc < TSc$;

$(f_s, f_o, f_c) \in F = L^s \times L^o \times L^s$ – тройка функций (f_s, f_o, f_c), определяющих $f_s(s_i): S \to L$ – уровень доступа субъекта $[\![(s)]\!]_i$; $f_o(o_j): O \to L$ – уровень конфиденциальности объекта (o_j); $f_c(s_i): S \to L$ – текущий уровень доступа субъекта (s_i), при этом для любого $s_i \in S$ справедливо неравенство$f_c(s_i) \leq f_s(s_i)$;

$V = B \times M \times F$ – множество состояний системы;

– множество запросов системе;

$D = \{d_y\}$, где $y = \overline{1,y'}$ – множество ответов системы по запросам, например: $d_1 = yes,\ d_2 = no,\ d_3 = error$;

– множество действий системы, где четверка $(q'_e, d_y, v^*, v) \in w'$ означает, что система по запросу q'_e с ответом d_y перешла из состояния v в состояние v^*;

$N_0 = \{0,1,2 \ldots\}$ – множество значений времени;

В классической модели Белла-ЛаПадула рассматривается три вида запросов системе:

- запросы изменения множества текущих доступов ;

- запросы изменения функций (f_s, f_o, f_c);

- запросы изменения текущей структуры разрешения доступа в матрице M.

Безопасность системы определяется с помощью трех свойств:

ss - свойства простой безопасности, при этом:

$r \in \{execute, append\}$;

$r \in \{read, write\}$ и $f_s(s_i) \geq f_o(o_j)$.

* - свойство «звезда», при этом:

$r = execute$;

$r = append$ и $f_o(o_j) \geq f_c(s_i)$;

$r = read$ и $f_c(s_i) \geq f_o(o_j)$;

$r = write$ и $f_c(s_i) = f_o(o_j)$.

ds - свойство дискреционной безопасности, при этом:

$r \in M\{s, o\}$.

Основываясь на базовой теории безопасности [3], можно сделать вывод, что система будет безопасной, если каждый доступ в системе обладает всеми тремя свойствами одновременно.

Элементами модели ХРУ являются [2]:

$O = \{o_j\}$, где $j = \overline{1,j}$ – множество объектов системы;

$S = \{s_i\}$, где $i = \overline{1,i}$ – множество субъектов системы, где $(S \subseteq O)$;

$R = \{r_z\}$, где $z = \overline{1,z}$ – множество видов прав доступа субъектов на объекты;

M – матрица доступов, строки которой соответствуют субъектам, а

$M[S,O] \subseteq R$

столбцы – объектам. . где R – права доступа субъекта s_i на

o

объект .

- множество состояний системы ХРУ.

В результате выполнения примитивного оператора α осуществляется переход из состояния $q_g = (S,O,M)$ в результирующее состояние $q_{g+1} = (S^*,O^*,M^*)$. Указанный переход обозначается через $q_1 g \vdash_1 \alpha\, q_1(g+1)$. Функционирование системы рассматривается только с точки зрения изменений в матрице доступа. Возможные изменения определяются шестью видами примитивных операторов α. Т. к. модель БЛП не описывает администрирование системы, то для ее представления будут применяться только два из них:

«внести» право $r \in R$ в $M\,[s_i,o_j]$;

«удалить» право $r \in R$ из $M\,[s_i,o_j]$.

Из примитивных операторов составляются команды, состоящие из двух частей:

условия, при которых выполняется команда;

последовательности примитивных операторов.

Таким образом каждая команда может на основе заданных в ней условий выполнять несколько примитивных операторов. Следовательно, необходимо обеспечить выполнение всех запросов системе, реализующей модель БЛП и действия системы по ним с соблюдением всех свойств безопасности в рамках выполнения примитивных операторов в командах с определенными условиями.

Т. к. модель БЛП включает в себя дискреционную составляющую, некоторые элементы присущи также и модели ХРУ и не нуждаются в дополнительном представлении:

O – множество объектов системы, S – множество субъектов системы и M – матрица доступов, строки которой соответствуют субъектам, а столбцы – объектам. M[s,o]⊆R, где R – права доступа субъекта s_i на o

объект . При реализации дискреционного разграничения доступа в автоматизированной информационной системе матрица доступа не храниться в явном виде, поскольку очень велика. Для сокращения объема матрицы доступа используется объединение субъектов доступа в группы. Права группы предоставляются каждому субъекту группы. Ввиду большой градации в рамках СРД существуют противоречия (группе разрешен доступ, а одному субъекту группы нет), что приводит к наличию на пересечении строк и столбцов матрицы как разрешающего, так и запрещающего права доступа. При использовании дискреционного разграничения доступа автоматизированная система всегда содержит правила разрешения подобных противоречий.

В указанном подходе на практике фактически применяются как права разрешающие доступ, так и запрещающие его (активно применяется в операционных системах Windows) [5]. Исходя из этого, во множество

прав доступа включим права, разрешающие доступ всем кроме указанного и обозначим $R' \subset R$, тогда, $R = \{read', write', own', execute', append', read, write, own, execute, append\}$, при этом R' назначаются владельцем объекта и выполняют функцию дискреционного «ужесточения» модели БЛП, а R – предоставляются в соответствии со свойствами безопасности и выполняют функцию мандатного разграничения доступа. В автоматизированной системе при возникновении противоречия на запрещение и предоставление права доступа – запрещение будет являться приоритетным, т. е. ds-свойство безопасности соблюдается во всех командах.

Представим остальные элементы модели БЛП элементами модели ХРУ.

$(L, \leq)$ – в виде $S_L = \{s_a\}$, где $a_1 = Un, a_2 = Sc, a_3 = TSc$, при этом $S_L \subset S$;

для реализации $(f_s, f_o, f_c) \in F = L^s \times L^o \times L^s$ применим сегмент матрицы доступов ХРУ [4], в котором степени конфиденциальности (уровни доступа) выражены доступом (например, read) субъекта $s_a \in S_L$ к определяемому объекту (включая оставшиеся S). Данные субъекты - часть системы безопасности, не хранят в себе информацию и являются доверенными. При этом для выражения $f_c(s_i)$, в данном сегменте можно использовать еще одно право доступа из возможных (например, write), что позволит избежать расширения матрицы доступов. Однако, для упрощения понимания работы модели для каждого $\{s_i\} \in S$ зададим субъект s'_i, доступ субъекта s_a к которому выражает значение $f_c(s_i)$. Применяемый сегмент матрицы доступов будет иметь вид, представленный в таблице.

Таблица – СЕГМЕНТ МАТРИЦЫ ХРУ РЕАЛИЗУЮЩИЙ ТРОЙКУ ФУНКЦИЙ f_s, f_o, f_c.

-	s_1	s'_1	s_2	s'_2	…	s_i	s'_i	o_1	…	o_j

s_{TS}	read	0	0	0	…	0	0	read	…	r
s_S	0	read	read	0	…	read	read	0	…	r
s_U	0	0	0	read	…	0	0	0	…	r
s_1	0	0	0	0	…	0	0	0	0	r
s_2										
⋮										
s_i										

Например: в указанном случае $f_s(s_1) = TSc, f_o(o_1) = TSc, f_c(s_1) = Sc$.

V – множество состояний системы БЛП, в виде – состояний системы ХРУ;

Текущие доступы в модели ХРУ предоставляются субъектам системы в рамках прав, заданных в матрице доступов, а множество всех множеств доступов зададим аналогично БЛП .

– множество запросов системе, в виде множества команд X ;

D – множество реакций системы, реализующей модель ХРУ, предусматривает выполнение оператора α при соблюдении условий команды множества X и невыполнение в обратном случае;

W – множество действий системы, в виде примитивных операторов α. При этом действия системы описанной БЛП полностью реализуемы действиями системы описанной ХРУ, т.е. $W = Q \times D \times V^* \times V$ представим в виде $q_i g \vdash_i \alpha\, q_i(g+1)$.

Реализация мандатного разграничения доступа моделью ХРУ будет выполнена при соблюдении двух условий:

- все запросы системе реализованы;

- при выполнении действий в соответствии с запросами система остается безопасной относительно условий безопасности модели БЛП.

Т. к. все элементы модели БЛП сведены к множествам S, O и R, все запросы системе (рассматриваемые в БЛП) реализуемы:

- запрос изменения матрицы возможных доступов M осуществляется в рамках модели ХРУ всеми примитивными операторами α, но для осуществления дискреционной функции будут применяться права доступа R';

- запрос на изменение тройки функций f_s, f_o, f_c выполняется примитивными операторами «внести» право $r \in R$ в $M[s_a, o_j]$, «удалить» право $r \in R$ из $M[s_a, o_j]$;

- запросы изменения множества текущих доступов реализуется в объеме прав доступа в матрице M, устанавливаемых примитивными операторами «внести» право $r \in R$ в $M[s_i, o_j]$, «удалить» право $r \in R$ из $M[s_i, o_j]$.

При этом система будет безопасной лишь в том случае, если все команды формируемые в ней по запросам будут безопасны. Выполнение данного условия можно доказать проверкой соблюдения свойств безопасности каждой командой. Доказательство становиться разрешимой задачей, если запросы системе будут выполняться командами, являющимися универсальными (выполняют весь спектр запросов, не изменяясь в условиях и примитивных операторах).

Запрос на изменение матрицы возможных доступов M является дискреционной составляющей и не требует дополнительного анализа [4].

Представим остальные запросы командой модели ХРУ.

Запрос на изменение тройки функций f_s, f_o, f_c необходимо рассматривать в виде двух видов команд:

команда на изменение $f_o(o_j)$ ($f_s(s_i)$) присваивает заданному объекту системы определенную администратором степень конфиденциальности. Рассмотрим присвоение на примере метки – TSc.

$command$ «присвоить метку конфиденциальности TSc» (s_1, s_{TSc}, o_j):

$if\ \ (read \in M[s_{Sc}, o_j])\ then$

«удалить» право *read* из $M[s_{Sc}, o_j]$;

«внести» право *read* в $M[s_{TSc}, o_j]$;

endif

$if\ \ (read \in M[s_{Un}, o_j])\ then$

«удалить» право *read* из $M[s_{Un}, o_j]$;

«внести» право *read* в $M[s_{TSc}, o_j]$;

endif

end.

В данном случае присвоением уровней конфиденциальности (доступа) в системе занимается специально выделенный доверенный субъект (администратор). Представленная команда «присвоить уровень конфиденциальности TSc» универсальна, т. к. в качестве o_j, могут выступать любые субъекты и объекты системы. Неформально выполнение представленной команды можно описать так: проверяется уровень конфиденциальности объекта, исключая TSc, т. к. в этом случае исходное состояние совпадет с последующим. При выполнении условия удаляется текущая метка конфиденциальности и присваивается – TSc. Аналогично составляются команды на присвоение метки Sc и Un.

Т. к. субъект s_1 (администратор) и множество субъектов S_L (элементы описанного сегмента матрицы ХРУ – часть системы безопасности) являются доверенными субъектами, команда на изменение функций f_s, f_o безопасна. Запрос же на изменение функции f_c неразрывно связан с запросом на изменение множества текущих доступов, и будет рассматриваться совместно с ним.

Запрос на изменение текущих доступов рассмотрим на примере

предоставления права доступа read субъекту s_i на объект .

Доступы предоставляются субъекту s_i в рамках прав доступа $M[s,o] \subseteq R$. Следовательно, если соблюдаются требования безопасности при предоставлении прав доступа, текущие доступы, реализующие данное право, также будут безопасны. Условия команды формируются путем проверки всех возможных комбинаций прав доступа субъектов множества S_L на объекты основания команды. Удалив условия, нарушающие свойства безопасности, обеспечим безопасную реализацию мандатного разграничения доступа при предоставлении права чтения. Следует особо отметить, что система, реализующая мандатное разграничение доступа, в рамках свойств безопасности может вести себя по-разному [1]. Для доказательства корректности выражения БЛП элементами ХРУ установим: для предоставления доступа текущий уровень субъекта $f_c(s_i)$ принимает необходимое значение, но $f_c(s_i) \leq f_s(s_i)$, доступы, нарушающие свойства безопасности, при изменении текущего доступа субъекта $f_c(s_i)$ удаляются. Описанное действие системы будет выражено командой:

command «предоставить доступ read» (s_i, s'_i, o_j):

if $(read \in M[s_{TSc}, s_i])$ *and* $(read \in M[s_{TSc}, o_j])$ *and* $(read \in M[s_{TSc}, s'_i])$ *then*

«внести» право *read* в $M[s_i, o_j]$;

endif

if $(read \in M[s_{TSc}, s_i])$ *and* $(read \in M[s_{TSc}, o_j])$ *and* $(read \in M[s_{Sc}, s'_i])$ *then*

«внести» право *read* в $M[s_i, o_j]$;

«удалить» право *read* из $M[s_{Sc}, s'_i]$;

«внести» право *read* в $M[s_{TSc}, s'_i]$;

«удалить» право append из $M\ s_i$ ко всем O-Sc;

«удалить» право write из $M\ s_i$ ко всем O-Sc;

endif

$if\ (read \in M[s_{TSc}, s_i])\ and\ (read \in M[s_{TSc}, o_j])\ and\ (read \in M[s_{Un}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

«удалить» право *read* из $M[s_{Un}, s'_i]$;

«внести» право *read* в $M[s_{TSc}, s'_i]$;

«удалить» право *append* из $M\ \ s_i$ ко всем O-Sc, Un;

«удалить» право *write* из $M\ \ s_i$ ко всем O-Un;

endif

$if\ (read \in M[s_{TSc}, s_i])\ and\ (read \in M[s_{Sc}, o_j])\ and\ (read \in M[s_{TSc}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

endif

$if\ (read \in M[s_{TSc}, s_i])\ and\ (read \in M[s_{Sc}, o_j])\ and\ (read \in M[s_{Sc}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

endif

$if\ (read \in M[s_{TSc}, s_i])\ and\ (read \in M[s_{Sc}, o_j])\ and\ (read \in M[s_{Un}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

«удалить» право *read* из $M[s_{Un}, s'_i]$;

«внести» право *read* в $M[s_{Sc}, s'_i]$;

«удалить» право *append* из $M\ \ s_i$ ко всем O-Un;

«удалить» право *write* из $M\ \ s_i$ ко всем O-Un;

endif

$if\ (read \in M[s_{TSc}, s_i])\ and\ (read \in M[s_{Un}, o_j])\ and\ (read \in M[s_{TSc}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

endif

$if\ (read \in M[s_{TSc}, s_i])\ and\ (read \in M[s_{Un}, o_j])\ and\ (read \in M[s_{Sc}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

endif

$if\ (read \in M[s_{TSc}, s_i])\ and\ (read \in M[s_{Un}, o_j])\ and\ (read \in M[s_{Un}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

endif

$if\ (read \in M[s_{Sc}, s_i])\ and\ (read \in M[s_{Sc}, o_j])\ and\ (read \in M[s_{Sc}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

endif

$if\ (read \in M[s_{Sc}, s_i])\ and\ (read \in M[s_{Sc}, o_j])\ and\ (read \in M[s_{Un}, s'_i])\ then$

«внести» право *read* в $M[s_i, o_j]$;

«удалить» право *read* из $M[s_{Un}, s'_i]$;

«внести» право *read* в $M[s_{Sc}, s'_i]$;

«удалить» право *append* из $M\ \ s_i$ ко всем O-Un;

«удалить» право *write* из $M\ \ s_i$ ко всем O-Un;

endif

$if\ \ (read \in M[s_{Sc}, s_i])\ and\ (read\ \ \in M[s_{Un}, o_j])\ and\ (read \in M[s_{Sc}, s'_i])then$

«внести» право *read* в $M[s_i, o_j]$;

endif

$if\ \ (read \in M[s_{Sc}, s_i])\ and\ (read\ \ \in M[s_{Un}, o_j])\ and\ (read \in M[s_{Un}, s'_i])then$

«внести» право *read* в $M[s_i, o_j]$;

endif

$if\ \ (read \in M[s_{Un}, s_i])\ and\ (read\ \ \in M[s_{Un}, o_j])\ and\ (read \in M[s_{Un}, s'_i])then$

«внести» право *read* в $M[s_i, o_j]$;

endif

end.

Т. к. все условия различны, соблюдение возможно лишь одного из них. Если в запрос не подпадает ни под одно из заданных условий, то он противоречит свойствам безопасности, и выполнен не будет. Особое внимание необходимо обратить на оператор «удалить» право из $M\ \ s_i$ ко всем O-Un (Sc, TSc). В данном случае система должна проверить все объекты обладающие определенной степенью конфиденциальности на предмет наличия права доступа, противоречащего свойствам безопасности, и удалить его. Т. к. в этом случае объекты в основании команды будут меняться, то одним примитивным оператором это выполнить невозможно. Следовательно, необходимо производить запуск дополнительной команды по поиску и удалению прав доступа, нарушающих свойства безопасности системы, а указанный примитивный оператор будет выполнять лишь «флаговую» функцию (т. е. сигнализировать системе имеющимися средствами о необходимости запуска команды). Например:

command «удалить» право *write* из $M\ \ s_i$ ко всем O-Un» (s_i, s_{Un}, o_j):

$if \ \ (read \in M[s_{Un}, o_j])\ and\ (write \in M[s_i, o_j])then$

«удалить» право write из $M[s_i, o_j]$;

endif

end.

При этом в основание команды подставляются попеременно все объекты множества О. Из условий наглядно видно, что право записи субъекта s_i во все объекты имеющие степень конфиденциальности Un будет удалено.

Т. к. все условия команды обладают свойствами безопасности, а все исключенные условия создают угрозу, то команда безопасна.

Аналогично строятся универсальные команды для предоставления остальных заданных в системе прав доступов. Т. к. любой запрос может быть представлен универсальными и соблюдающими свойства безопасности командами, представление является безопасным.

Выводы:

1. Через модель ХРУ возможно выразить политику МРД, при этом полученная модель будет безопасной.

2. Данный подход применим при анализе безопасности информации при объединении автоматизированных информационных систем, реализующих разнородные модели безопасности.

3. Если обозначить полученное развитие модели ХРУ, как активное состояние, то дальнейшим направлением исследования будет являться создание алгоритма безопасного автоматического перехода системы в активное состояние и обратно.

Список литературы:

1. Гайдамакин Н.А. Теоретические основы компьютерной безопасности: Учеб. пособие / Н.А. Гайдамакин – Екатеринбург 2008 – 212 с.
2. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений / П.Н. Девянин – М.: Издательский центр «Академия», 2005 – 144 с.
3. Девянин П.Н. Модели безопасности компьютерных систем: Учеб.пособие для студ. высш. учеб. заведений. 2-е издание / П.Н. Девянин – М.: Горячия линия –

Телеком, 2013 – 337 с.
4. Поддубный М.И. Применение сегмента матрицы доступов ХРУ в анализе информационной безопасности систем, реализующих мандатное разграничение доступа / Королев И.Д., Поддубный М.И., Носенко С.В. //Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №07(101). – IDA [article ID]: 1011407042. – Режим доступа: http://ej.kubagro.ru/2014/07/pdf/119.pdf, 0,813 у.п.л.
5. Проскурин В.Г. Защита в операционных системах: Учеб.пособие для высш. учеб. заведений / В.Г. Проскурин, С.В. Крутов, И.В. Мацкевич – М.: «Радио и связь», 2000 – 168 с.

References

1. Gajdamakin N.A. Teoreticheskie osnovy komp'juternoj bezopasnosti: Ucheb. posobie / N.A. Gajdamakin – Ekaterinburg 2008 – 212 s.
2. Devjanin P.N. Modeli bezopasnosti komp'juternyh sistem: Ucheb. posobie dlja stud. vyssh. ucheb. zavedenij / P.N. Devjanin – M.: Izdatel'skij centr «Akademija», 2005 – 144 s.
3. Devjanin P.N. Modeli bezopasnosti komp'juternyh sistem: Ucheb.posobie dlja stud. vyssh. ucheb. zavedenij. 2-e izdanie / P.N. Devjanin – M.: Gorjachija linija – Telekom, 2013 – 337 s.
4. Poddubnyj M.I. Primenenie segmenta matricy dostupov HRU v analize informacionnoj bezopasnosti sistem, realizujushhih mandatnoe razgranichenie dostupa / Korolev I.D., Poddubnyj M.I., Nosenko S.V. //Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №07(101). – IDA [article ID]: 1011407042. – Rezhim dostupa: http://ej.kubagro.ru/2014/07/pdf/119.pdf, 0,813 u.p.l.
5. Proskurin V.G. Zashhita v operacionnyh sistemah: Ucheb.posobie dlja vyssh. ucheb. zavedenij / V.G. Proskurin, S.V. Krutov, I.V. Mackevich – M.: «Radio i svjaz'», 2000 – 168 s.