УДК 004.02

ПРИМЕНЕНИЕ СЕГМЕНТА МАТРИЦЫ ДОСТУПОВ ХРУ В АНАЛИЗЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ, РЕАЛИЗУЮЩИХ МАНДАТНОЕ РАЗГРАНИЧЕНИЕ ДОСТУПА

Королев Игорь Дмитриевич
доктор технических наук, профессор

Поддубный Максим Игоревич

Носенко Сергей Владимирович
Филиал Военной академии связи (г. Краснодар), Краснодар, Россия

В данной статье рассматривается применение механизма изменения матрицы доступов ХРУ при анализе безопасности информационной системы, реализующей мандатное разграничение доступа на примере анализа безопасности информации при применении способа автоматической классификации формализованных документов в системе электронного документооборота

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

UDC 004.02

THE USAGE OF HRU SEGMENT MATRIX ACCESS IN THE ANALYSIS OF INFORMATION SECURITY SYSTEMS WHICH MAKE MANDATORY ACCESS CONTROL

Korolyov Igor Dmitrievich
Dr.Sci.Tech., professor

Poddubny Maksim Igorevich

Nosenko Sergey Vladimirovich
Branch of the Military Academy of connection, Krasnodar, Russia

In this article we consider the usage of HRU access matrix changing system allowing for information security system which makes mandatory access control in case of information security analysis by using an automatic classification of formalized documents in the system of electronic document management

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

Модель мандатного разграничения доступа обеспечивает информационную безопасность с помощью присвоения всем сущностям системы уровней конфиденциальности (доступа). Данные уровни или метки определяют все возможные доступы между ними. Однако из этого следует, что мандатное управление доступом не различает сущностей одного уровня доступа, и на их взаимодействия ограничения не распространяются. Поэтому мандатная модель, как правило, применяется обязательно совместно с дискреционной, которая используется для контроля за взаимодействиями между сущностями одного уровня и установки дополнительных ограничений, усиливающих мандатную модель.

Применение мандатного разграничения совместно с дискреционным реализовано в классической модели Белла-ЛаПадула. Исходя из того, что

данная модель не описывает конкретных действий системы при запросах, а лишь задает условия ее работы, обеспечивающие безопасность системы, механизмы реализации действий системы могут быть различными, но отвечающими требованиям безопасности[2].

Одним из таких запросов является запрос на изменение текущей структуры разрешения доступа в матрице M (дискреционной части модели). Действия системы по данному запросу должны осуществляться на основе механизма, реализующего изменение матрицы возможных доступов, исключающее утечку прав доступа. Данный механизм представлен в классической модели Харрисона-Руззо-Ульмана (ХРУ) [2]. Следовательно, возможно применение модели ХРУ для реализации действий системы по запросу на изменение матрицы прав доступа M.

Применение механизма модели ХРУ при анализе безопасности информационной системы, реализующей мандатное разграничение доступа, обладает **научной новизной.**

Применим данный подход при анализе информационной безопасности системы, обеспечивающей мандатное разграничение доступа на примере способа автоматической классификации формализованных документов в системе электронного документооборота (способа классификации) [4].

Способ классификации в автоматическом режиме по заранее определенным признакам определяет области информационной ответственности того или иного исполнителя, к которой относится поступающий в систему документ. Преимущество данного способа по сравнению с известными – возможность реализовать классификацию с учетом любых значений реквизитов. Реквизиты формализованного документа, содержащего сведения конфиденциального характера, строго определены [6]. Следовательно, способ классификации способен в автоматическом режиме присваивать уровни конфиденциальности

поступившим документам. Таким образом, способ классификации предоставляет право доступа к поступившему документу одним субъектам информационной системы и запрещает другим, т.е. принимает на себя часть функций системы разграничения доступа (СРД). Разграничение доступа, обеспечиваемое на основе уровней конфиденциальности объектов и уровней доступа субъектов информационных систем, является мандатным [2]. Согласно требованиям основных критериев оценки безопасности компьютерных систем, СРД должны строиться на основе математических моделей. С использованием математических моделей должно быть теоретически обосновано соответствие системы защиты требованиям заданной политики безопасности [2].

Свойство безопасности является основным в любых информационных системах, имеющих уровни конфиденциальности. Следовательно, анализ способа классификации на предмет соответствия моделям безопасности информационных систем является **актуальной задачей**.

Объектом исследования является способ автоматической классификации формализованных документов в системе электронного документооборота [4].

Предметом исследования являются свойства способа автоматической классификации формализованных документов в системе электронного документооборота, обеспечивающие безопасную обработку информации.

Определим следующие **задачи исследования**:

Представить способ классификации в виде математической модели Белла-ЛаПадула;

применить в качестве механизма изменения матрицы доступов модели Белла-ЛаПадула модель ХРУ.

Исследовательский характер заключается в применении в модели Белла-ЛаПадула механизма изменения матрицы доступа, свойственного модели ХРУ.

Анализируемый способ классификации разработан на основе средств алгебры конечных предикатов[1].

Для выполнения поставленной задачи определим элементы, которыми будем оперировать:

$O' = \{o'_j\}$, где $j = \overline{1, j'}$; O' – множество документов поступающих в автоматизированную систему, при этом $O' \subseteq O$, где O–множество объектов автоматизированной системы (АС).

$Z_{рек} = \{z_a\}$, где $a = \overline{1, a'}$– множество реквизитов документа;

$L_{кс} = \{l_g\}$, где $g = \overline{1, g'}$ –множество ключевых слов;

$T = \{t_h\}$, где $h = \overline{1, h'}$ – множество характеристик текста;

$V' = \{v'_k\}$, где $k = \overline{1, k'}$ – множество форм документа;

$U = \{u_p\}$, где $p = \overline{1, p'}$ множество информационных областей АС;

$W = \{w_e\}$, где $e = \overline{1, e'}$ множество значимых слов в тексте документа определенной информационной области, обладающих определенным весом.

Проанализировав правила построения предикатов, с помощью которых осуществляется автоматическая классификация поступающих в автоматизированную систему документов [4], основные этапы работы системы можно описать следующим образом:

- в зависимости от признаков документа и слов, применяемых в данном признаке, определяются реквизиты документа: $P_{рек}(Z_{рек}, T, L_{пр})$;

- по словам в реквизитах определяется форма поступившего документа $P_{ф}(V', Z_{рек}, L_{рек})$;

- после однозначного определения реквизитов и формы документа выбираются заранее определенные информационные области, в которых производится определение значимых слов и их «взвешивание»[4];

- веса, полученные в указанных областях, сравниваются с заданными значениями, после чего определяется область информационной ответственности с учетом реквизитов, обозначающих степень конфиденциальности документа [6]: $P(U, W, V')$.

Выразим все этапы работы способа классификации одним предикатом $P(U, W, L_{\text{рек}}, T, L_{\text{пр}})$, где $L_{\text{рек}}$ – множество слов реквизита поступившего документа; $L_{\text{пр}}$ – множество ключевых слов признака документа, при этом $L_{\text{рек}} \subseteq L_{\text{кс}}$ и $L_{\text{пр}} \subseteq L_{\text{кс}}$.

Для анализа безопасности информации при применении способа классификации необходимо указанные элементы представить элементами классической модели Белла-ЛаПадула.

Элементами модели Белла-ЛаПадула являются:

$O = \{\text{o}_\text{j}\}$, где $j = \overline{1, \text{j}'}$ – множество объектов системы;

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

$R = \{read, write, execute, append\}$ – множество видов прав доступа субъектов s_i на объектыo_j;

M – матрица доступов, строки которой соответствуют субъектам, а столбцы – объектам. $\text{M}[s, o] \subseteq R$, где R – права доступа субъекта s_i на объект o_j;

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

$(L, \leq)$ – решетка уровней конфиденциальности, например: $L = \{U(unclussified), C(confidential), S(secret), TS(top\ secret)\}$,
где $U < C < S < TS$;

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

$V = B \times M \times F = \{v_\gamma\}$, где $\gamma = \overline{1, \gamma'}$- множество состояний системы;

$Q = \{q_\beta\}$, где $\beta = \overline{1, \beta'}$ – множество запросов системе;

D=$\{d_\lambda\}$, где $\lambda = \overline{1, \lambda'}$ – множество ответов системы по запросам, например: $D = \{yes, no, error\}$;

$W' = Q \times D \times V \times V$ – множество действий системы, где четверка $(q_\beta, d_\lambda, v^*_{\gamma+1}, v_\gamma) \in W'$означает, что система по запросу q_βс ответом d_λ перешла из состояния v_γ в состояние$v^*_{\gamma+1}$;

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

X – множество функций x:$N_0 \rightarrow Q$, задающих все возможные последовательности запросов к системе;

Y – множество функций y:$N_0 \rightarrow D$, задающих все возможные последовательности ответов системы по запросам;

Z – множество функций z: $N_0 \rightarrow V$, задающих все возможные последовательности состояний системы.

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

запросы изменения множества текущих доступов $B_{\text{тек}}$;

запросы изменения функций f;

запросы изменения текущей структуры разрешения доступа в матрице M.

Система является безопасной, если соблюдаются свойства безопасности – ss, *, ds[2].

Следовательно, функции способа классификации должны реализоваться в рамках указанных обращений, не нарушая свойств безопасности системы. Следует особо отметить, что система мандатного разграничения доступа в данном случае не описывает принципов безопасного администрирования. Т.к. администрирование описывается другими моделями и требует отдельного исследования, в работе оно рассматриваться не будет (будем считать его безопасным, чем возведем в ранг ограничений).

Система разграничения доступа является статичной, следовательно, необходимо рассматривать последовательность состояний системы. Исходя из представленного описания реализации способа классификации, разделим анализ на два этапа.

1. Анализ безопасности информации при определении области информационной ответственности исполнителей $\mathrm{M}[s, o] \subseteq R$, где R– правадоступасубъекта s_i на объект o_j.

2. Изменение уровня конфиденциальности объекта соответственно степени конфиденциальности поступившего документа.

Для удобства понимания работы системы представим каждый этап отдельным запросом системы, и, как следствие, отдельным состоянием:

v_0– Документ o'_1поступает в АС. К объекту не имеет доступа ни один субъект кроме s_1администратора. Начальное состояние является безопасным.

v_1 – запрос на изменение M (реализует 1-й этап);

v_2 – запрос на изменение $f_o(o'_1)$(реализует 2-й этап).

На первом этапе производится запрос на изменение матрицы доступов M. Представим необходимые элементы способа классификации элементами модели Белла-ЛаПадула,

где $u_p \in U$в виде $s_u \in S$;

$w_e \in W$в виде $o_w \in O$;

$l_\mu \in L_{\text{рек}}$ в виде $o_{l_{\text{рек}}} \in O$;

$t_h \in T$в виде $o_t \in O$;

$l_{\text{пр}} \in L$в виде $o_{l_{\text{пр}}} \in O$.

Для реализации запроса применим сегмент матрицы доступов ХРУ [7].

Предикат $P(U, W, L_{\text{рек}}, T, L_{\text{пр}})$ представим в виде условий команды «определить информационную область», а выбор субъектов, к области информационной ответственности которых относится поступивший документ, – в виде срабатывания одного из примитивных операторов «внести» право доступа к объекту заданного субъекта [2]. Все документы, относящиеся к области информационной ответственности, будут однозначно определены указанным предикатом. Каждая область ответственности выражена своим предикатом, которые вместе составляют систему, обеспечивающую гарантированное отнесение поступившего документа к одной из них [3].

Кроме того, для реализации второго этапа в зависимости от реквизитов, обозначающих степень конфиденциальности поступившего документа, необходимо создать признак «узнаваемый» системой. По данному признаку система присвоит одну из предусмотренных меток конфиденциальности. В качестве указанного признака введем в сегмент матрицы доступов ХРУ объект $o_\tau \in O$, наличие права доступа к которому различных субъектов сигнализирует системе о степени конфиденциальности поступившего документа. При этом для установки данного признака в «исходное положение» все команды «определить информационную область» (независимо от условий), должны начинаться с выполнения примитивного оператора «удалить право» всех субъектов s_i к объекту o_τ.

$s_1 \in S$– доверенный субъект, который производит запросы к системе (например, администратор), реализующие функции способа классификации.

Схематично сегмент описан в таблице 1, при этом наличие или отсутствие права доступа субъекта s_uк объектам, представляющим элементы способа классификации, будет представлять собой наличие или отсутствие условий для определения области информационной ответственности.

Таблица 1 – Сегмент матрицы доступов, реализующий 1-й этап

-	o_w	…	$o_{w'}$	$o_{l_{\text{рек}}}$	…	$o_{l'_{\text{рек}}}$	o_t	…	$o_{t'}$	$o_{l_{\text{пр}}}$	…	$o_{l'_{\text{пр}}}$	o_τ
s_u	read	…	0	0	…	0	read	…	0	0	…	read	0
⋮	0	…	0	read	…	read	0	…	0	0	…	0	0
$s_{u'}$	0	…	read	0	…	0	0	…	read	0	…	0	0
s_1	0	0	0	0	0	0	0	0	0	0	0	0	0

Предикат P реализовывается в команде «определить информационную область». Команда в общем виде записывается так:

$command$«определить информационную область» (s_1, s_2, o'_1):

$if\ (own \in M[s_1, o'_1])and\ (read \in M[s_u, o_w])and$ …

$and\ \left(read \in M\left[s_u, o_{l'_{\text{пр}}}\right]\right) then$

«удалить» право $read$из$M[s_u, o_\tau]$;

⋮

«внести» право на чтение $read$ в $M[s_2, o'_1]$;

endif

if $\left(read \in \text{M}\left[s_{\text{u}}, \text{o}_{\text{l}_{\text{рек}}}\right]\right)$ and … and $\left(read \in \text{M}\left[s_u, \text{o}_{\text{l}_{\text{пр}}}\right]\right)$ then

«внести» право на чтение readв$M[s_u, o_\tau]$;

endif

end.

Таким образом, на первом этапе система по запросу q_1 перешла из безопасного состояния v_0 в состояние v_1, т.е. $(q_1, d_1, v_1, v_0) \in W$. Так как сегмент является недоступным для субъектов системы, а все изменения матрицы прав доступа не выходят на данном этапе за его рамки, следовательно, свойства безопасности системы (sd, ss, *) не нарушены, то есть v_1также безопасно[1].

Условия команды, в результате выполнения которых срабатывают примитивные операторы, для удобства понимания разделим на два «типа». Первый – «удаляет» права доступа к объекту o_τ (признак конфиденциальности предыдущего документа) и предоставляет право доступа субъектам соответствующей зоны информационной ответственности, второй – предоставляет право доступа к объекту o_τ на основе степени конфиденциальности поступившего документа. Количество условий каждого типа в команде будет равно количеству «видов» документов, поступающих в информационную систему и применяемых степеней конфиденциальности в системе соответственно. В данной команде представлен один «вид» документа, относящийся к области информационной ответственностиs_u, в которую входит один субъект s_2, имеющий право ознакомления (только чтение) с поступившим документом, и определяется одна степень конфиденциальности поступившего документа. При наличии большего количества условий, согласно заданных систем предикатов, лежащих в их основе, совпадение будет лишь одно, т.е. зона ответственности и степень конфиденциальности будут определены однозначно [5].

На втором этапе производится запрос изменения функций f. При поступлении данного обращения система проверяет условия, наличие соответствующих прав субъекта, сделавшего запрос (в нашем случае это доверенный субъект s_1), наличие прав доступа к объекту o_τ, определяемых

системой как соответствующая отметка конфиденциальности. По запросу изменения система совершает действие$(q_2, d_2, v_2, v_1) \in W$, где $f_o^*(o'_1) = L$ (в соответствии со степенью конфиденциальности поступившего документа).

Так как на данном этапе не рассматриваются элементы (s_i, o_j, r_{so}), а метка конфиденциальности однозначно определена в состоянии v_1, состояние системы v_2 будет безопасным.

Результатом обоих этапов является состояние системы $v_2 = B_2 \times M_2 \times F_2$, которое относится к начальному состоянию следующим образом:

$B_2 = B;$

$M_2 = M[s_2, o'_1] \cup \{read\}$;

$f_o^*(o'_1) = L$ (в соответствии со степенью конфиденциальности поступившего документа).

Внесение права доступа к объекту o_τ рассматривать нет необходимости, т.к. оно будет удалено при запуске следующей команды «определить информационную область». Это сравнение наглядно показывает, что этапы способа классификации выполнены в полном объеме, авсе промежуточные состояния системы безопасны.

Выводы:

1. Применение механизма изменения матрицы доступов ХРУ в модели Белла-ЛаПадула позволяет анализировать действие системы по запросу изменения текущей структуры разрешения доступа в матрице М.

2. Способ автоматической классификации формализованных документов в системе электронного документооборота может обеспечивать безопасную обработку информации в рамках мандатного разграничения доступа.

3. Однозначное определение зоны информационной ответственности исполнителей и степени конфиденциальности поступившего документа позволяет применять способ автоматической классификации формализованных документов в системе электронного документооборота в СРД.

Список литературы:

1. Бондаренко М.Ф., Шабанов-Кушнаренко Ю.П. Об алгебре конечных предикатов. [Текст]// Научно-технический журнал «Бионика интеллекта». ХНУРЭ, г. Харьков, Украина – 2011 № 3(77).

2. 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.

3. Королев И.Д. Подходы к оперативной идентификации формализованных электронных документов в автоматизированных делопроизводствах / И.Д. Королев, С.В. Носенко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2013. – №08(092). – IDA [article ID]: 0921308074. – Режим доступа: http://ej.kubagro.ru/2013/08/pdf/74.pdf, 0,875 у.п.л.

4. Носенко С.В. Автоматическая классификация формализованных документов в системе электронного документооборота/ С.В. Носенко, И.Д. Королев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2014. – №02(096). – IDA [article ID]: 0961402042. – Режим доступа: http://ej.kubagro.ru/2014/02/pdf/42.pdf.

5. Носенко С.В. Математическая модель отнесения документов автоматизированной системы к информационным областям ответственности исполнителей / С.В. Носенко, И.Д. Королев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2013. – №08(092). – IDA [article ID]: 0921308057. – Режим доступа: http://ej.kubagro.ru/2013/08/pdf/57.pdf, 0,625 у.п.л.

6. О государственной тайне: Закон РФ № 5485-1 от 21.07.1993 г., (в ред. от 21.12.2013 г.) // Собрание законодательства РФ. 23.12.2013. № 51. Ст. 6697

7. Поддубный М.И. Анализ безопасности информации при применении модели отнесения документов автоматизированной системы к информационным областям ответственности исполнителей /М.И. Поддубный, И.Д. Королев // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2013. – №09(093). – IDA [article ID]: 0931309042. – Режим доступа: http://ej.kubagro.ru/2013/09/pdf/42.pdf

References

1. Bondarenko M.F., Shabanov-Kushnarenko Ju.P. Ob algebre konechnyh predikatov. [Tekst]// Nauchno-tehnicheskij zhurnal «Bionika intellekta». HNURJe, g. Har'kov, Ukraina – 2011 № 3(77).

2. 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.

3. Korolev I.D. Podhody k operativnoj identifikacii formalizovannyh jelektronnyh dokumentov v avtomatizirovannyh deloproizvodstvah / I.D. Korolev, S.V. Nosenko // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2013. – №08(092). – IDA [article ID]: 0921308074. – Rezhim dostupa: http://ej.kubagro.ru/2013/08/pdf/74.pdf, 0,875 u.p.l.

4. Nosenko S.V. Avtomaticheskaja klassifikacija formalizovannyh dokumentov v sisteme jelektronnogo dokumentooborota/ S.V. Nosenko, I.D. Korolev // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2014. – №02(096). – IDA [article ID]: 0961402042. – Rezhim dostupa: http://ej.kubagro.ru/2014/02/pdf/42.pdf.

5. Nosenko S.V. Matematicheskaja model' otnesenija dokumentov avtomatizirovannoj sistemy k informacionnym oblastjam otvetstvennosti ispolnitelej / S.V. Nosenko, I.D. Korolev // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2013. – №08(092). – IDA [article ID]: 0921308057. – Rezhim dostupa: http://ej.kubagro.ru/2013/08/pdf/57.pdf, 0,625 u.p.l.

6. O gosudarstvennoj tajne: Zakon RF № 5485-1 ot 21.07.1993 g., (v red. ot 21.12.2013 g.) // Sobranie zakonodatel'stva RF. 23.12.2013. № 51. St. 6697

7. Poddubnyj M.I. Analiz bezopasnosti informacii pri primenenii modeli otnesenija dokumentov avtomatizirovannoj sistemy k informacionnym oblastjam otvetstvennosti ispolnitelej /M.I. Poddubnyj, I.D. Korolev // Politematicheskij setevoj jelektronnyj nauchnyj zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta (Nauchnyj zhurnal KubGAU) [Jelektronnyj resurs]. – Krasnodar: KubGAU, 2013. – №09(093). – IDA [article ID]: 0931309042. – Rezhim dostupa: http://ej.kubagro.ru/2013/09/pdf/42.pdf