УДК 002

АНАЛИЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ПРИМЕНЕНИИ МОДЕЛИ ОТНЕСЕНИЯ ДОКУМЕНТОВ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ К ИНФОРМАЦИОННЫМ ОБЛАСТЯМ ОТВЕТСТВЕННОСТИ ИСПОЛНИТЕЛЕЙ

Королев Игорь Дмитриевич
доктор технических наук, доцент

Поддубный Максим Игоревич
Филиал Военной академии связи (г. Краснодар), Краснодар, Россия

В данной статье проводится анализ математической модели отнесения документов автоматизированной системы к информационным областям ответственности исполнителей, позволяющий сделать вывод о реализации дискреционного разграничения доступа

Ключевые слова: ЗАЩИТА ИНФОРМАЦИИ, ДИСКРЕЦИОННАЯ ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ МАТРИЦЫ ДОСТУПОВ ХРУ

UDC 002

THE SAFETY INFORMATION ANALYSIS IN APPLYING OF DOCUMENTAL REFERENCE MODEL OF THE AUTOMATED SYSTEM IN THE INFORMATIONAL AREAS OF THE ACTOR'S LIABILITY

Korolyov Igor Dmitrievich
Dr.Sci.Tech., professor

Poddubny Maksim Igorevich
Branch of the Military Academy of connection, Krasnodar, Russia

In the given article the mathematical representation analysis of documental reference model of the automated system in the information areas of the actor's liability is made, which allows to make a conclusion of discretionary access control

Keywords: INFORMATION SECURITY, DISCRETION SECURITY POLICY, ACCESS PERMISION MATRIX OF HRU

Анализ безопасности информации при применении модели отнесения документов автоматизированной системы к информационным областям ответственности исполнителей

Обработка информации в автоматизированных системах (АС), по нашему мнению, позволит целенаправленно формировать информационные ресурсы и обеспечивать их эффективное функционирование. Однако применение АС приводит к необходимости разработки новых стратегий в области информационных технологий, учитывающих не только оперативную обработку информации, но и ее безопасность. Особенно остро проблема защиты информации стоит в организациях с распределенными информационными ресурсами [4].

Работа посвящена исследованию безопасности процесса взаимодействия должностных лиц с комплексом систем автоматизации (КСА) АС электронного документооборота.

Объектом исследования является типовая модель отнесения данных, содержащихся в документах автоматизированной системы к информационной области ответственности исполнителя (далее МОДИ)[3].

Предметом исследования – свойства МОДИ обеспечивающие безопасную обработку информации.

При повышении оперативности обработки информации нельзя пренебрегать безопасностью информации, т.к. сохранение в тайне информации конфиденциального характера имеет главенствующую роль в системах оперирующих такими сведениями.

Исследование свойств оперативности во взаимодействии со свойствами безопасности процесса взаимодействия должностных лиц с КСА АС на основе существующих моделей безопасности, обуславливает актуальность работы.

Таким образом, **целью** нашей работы является анализ свойств МОДИ обеспечивающих безопасную обработку информации.

В современных автоматизированных системах обработки информации используется несколько математических моделей безопасности:

1. Модель изолированной программной среды. Она является субъектно ориентированной. Целью моделирования является определение порядка безопасного взаимодействия субъектов системы. В рамках МОДИ нам необходимо рассматривать отнесение объектов к информационным областям ответственности субъектов, что идет в разрез с целями создания данной политики.

2. Модели безопасности информационных потоков. Данные модели, в зависимости от их представления, реализуют либо дискреционную политику безопасности (автоматная, программная модели), либо мандатную политику безопасности (вероятностная модель). Для

качественного анализа целесообразно обратиться к классическим моделям, реализующим мандатное или дискреционное разграничение доступа.

3. Мандатная политика безопасности, в классическом исполнении, описываются моделью Белла–ЛаПадула[1,5]. Однако одним из элементов указанной модели является дискреционное разграничение доступа, выраженное в матрице возможных доступов.

4. Модели, реализующие дискреционное разграничение доступа. Основой дискреционного разграничения доступа является модель Харрисона - Руззо-Ульмана (далее ХРУ) [1,5].

Таким образом, при рассмотрении математических моделей безопасности информации вАС мы неизбежно приходим к выводу о необходимости анализа МОДИ с точки зрения дискреционное разграничение доступа. При реализации в МОДИ дискреционного разграничения доступа, можно будет говорить о реализации в данной модели более сложных и надежных политик безопасности.

Исходя из поставленной цели, используя выбранный математический аппарат, определим следующие задачи исследования:

реализация функций МОДИ на основе системы ХРУ, с сохранением возможностей администрирования МОДИ и элементов системы разграничения доступа (СРД);

определить перспективы для применения существующих развитий СРД в МОДИ.

Исследовательский характер данной работы сводиться к выявлению при помощи модели ХРУ в МОДИ свойств обеспечивающих безопасную обработку информации.

Предлагаемая математическая МОДИ разработана на основе средств алгебры конечных предикатов[2,3].

Для выполнения поставленной задачи определим элементы МОДИ, которыми будем оперировать:

$D = \{d_i\}$, где $1 \le i \le p$ – конечное множество документов поступающих исполнителю;

$Z = \{z_m\}$, где $1 \le m \le p`$ – конечное множество зон документа;

$M = \{m_a\}, 1 \le a \le n$ – конечное множество переменных в зонах документа;

$T^k = \{t_j^k\}$, где $1 \le j \le q$ – множество терминологических понятий;

$P(d_i, t_j^k) = \delta$, где $d_i \in D, t_j^k \in T^k, \delta = \{0, 1\}.$ – предикат персонификации областей ответственности исполнителей;

При реализации данной модели в ХРУ необходимо указанные элементы представить элементам системы ХРУ.

Модель ХРУ описывает дискреционную систему разграничения доступа. Элементами модели ХРУ при этом являются:

O – множество объектов системы;

S – множество субъектов системы ($S \subseteq O$);

R – множество видов прав доступа субъектов на объекты;

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

Функционирование системы рассматривается только с точки зрения изменений в матрице доступа. Возможные изменения определяются шестью видами примитивных операторов.

В результате выполнения примитивного оператора α осуществляется переход из одного состояния q = (S, O, M) в результирующее состояние q` = (S`, O`, M`). Этот переход обозначим через $q \vdash_\alpha q`$.

Т.к. система МОДИ относит новый объект в системы (документ) к области ответственности субъекта (исполнитель), следовательно, нас будут интересовать операторы:

«создать» объект o`;

«внести» право r∈Rв матрицу M.

Из примитивных операторов составляются команды. Каждая команда состоит из двух частей:

условия, при которых выполняется команда;

последовательности примитивных операторов.

Представим МОДИ в виде системы ХРУ при этом:

O = O` ∪O``, где O` = M, O``– множество объектов системы;

S = S` ∪S``, где S` = Z, S`` – множество субъектов системы (S⊆O);

R= {read, write, own, yes}– множество видов прав доступа субъектов на объекты, где право (yes) будет сигнализировать о наличии в конкретной зоне z_m некоторого признака m_a;

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

D ⊆ Oи выступает в качестве конечного множества объектов подлежащих «созданию» в СРД;

T^kвыражается в виде внесенных прав доступа yes∈ M[s`, o`];

$P(d, t^k)$– задается в виде условий команды «создания» o`;

Таким образом, команда в общем виде записывается так:

command $c(x_1, \dots, x_k)$

if $(r_1 \in M[x_{s_1}, x_{o_1}])$and ... and $(r_m \in M[x_{s_m}, x_{o_m}])$then

α_1;

. . .

α_n;

endif

end

Например: СРД состоит из 3-х субъектов 3 объектов и распределяет между 2-я субъектами поступающие документы 2-х видов определяющихся по двум различным признакам в двух зонах соответственно, на основе принципа описанного в публикации И.Д. Королева и С.В. Носенко [2].

При этом:

$O` = \{o_1, o_2\}$; $O`` = \{o_3, o_4, o_5\}$; $O = \{o_1, o_2, o_3, o_4, o_5\}$;

$S` = \{s_1, s_2\}$; $S`` = \{s_3, s_4, s_5\}$; $S = \{s_1, s_2, s_3, s_4, s_5\}$;

R = {read, write, own, yes};

$$M = \begin{bmatrix} - & o_1 & o_2 & o_3 & o_4 & o_5 \\ s_1 & yes & yes & 0 & 0 & 0 \\ s_2 & yes & yes & 0 & 0 & 0 \\ s_3 & 0 & 0 & own\ write & 0 & 0 \\ s_4 & 0 & 0 & 0 & own\ write & read \\ s_5 & 0 & 0 & 0 & read & own\ write \end{bmatrix}$$

В данную систему по условию поступают два вида документов. Каждый вид характеризуется признаками, определяющими его вид в зонах документа «подпись» и «согласование». Наличие признаков, определяющих вид документа в зонах удобно представить в виде таблиц: заявление по вопросу А (Таблица 1) и заявление по вопросу Б (Таблица 2).

Таблица 1 – Признаки определяющие заявление по запросу А

признак / Зона документа	Начальник отдела	Начальник цеха	Директор	Зам. директора
Подпись	1	0	0	0
Согласование	0	0	1	0

Таблица 2 - Признаки определяющие заявление по запросу Б

признак / Зона документа	Начальник отдела	Начальник цеха	Директор	Зам. директора
Подпись	0	1	0	0
Согласование	0	0	0	1

Система будет проверять наличие или отсутствие установленной переменной в соответствующей зоне документа, поэтому переменная может принимать на себя только одно значение, но в каждой зоне своё. Данные матрицы информативность системы позволяет свести в одну, при этом информативность не ограничена, а введение дополнительных зон и переменных осуществляется введением дополнительных o`, s` или введением дополнительных прав доступа.

Представив зоны документа и переменные в них в виде таблицы, мы получили наглядное отображение сегмента дискреционной модели безопасности, отвечающего за реализацию функций МОДИ. (Таблица 3)

Таблица 3– Сегмент ХРУ, реализующий функции МОДИ

значение перемен -ной / Зона документа	m_1 (o_1)	m_2 (o_2)
z_1 (s_1)	Начальник отдела	Начальник цеха
z_2 (s_2)	Директор	Зам. директора

В систему поступает документ подписанный начальником отдела и согласованных с начальником цеха.

При поступлении в АС электронного документа активируются команды на определение принадлежности его к области ответственности субъекта по переменным относящихся к зонам документа, а именно их сравнению с имеющимися в матрице доступов. В данном случае это:

command "принять документ" (s_3, o_6)
if (yes ∈ M[s_1, o_1])and (yes ∈ M[s_1, o_2])then
«создать» объектo_6;
«внести» право ownв M [s_3, o_6];
«внести» право readв M [s_4, o_6];
endif
end

command "принять документ" (s_3, o_6)
if (yes ∈ M[s_2, o_1])and (yes ∈ M[s_2, o_2])then
«создать» объект o_6;
«внести» право ownв M [s_3, o_6];
«внести» право readв M [s_5, o_6];

endif

end

В результате документ будет добавлен в область ответственности исполнителя s_4с предоставлением ему права чтения данного документа и администратор s_3оставляет право владения документом. При этом в данной системе пользователь s_3, являясь администратором сети рассматривается как доверенный субъект (т.е. используя свои должностные обязанности, не нарушает политики безопасности организации).

В результате система безопасности по одной из команд перейдет в состояние$q` \neq q$,в данном случае система будет иметь вид:

$O` = \{o_1, o_2\}$; $O`` = \{o_3, o_4, o_5\}$; $O = \{o_1, o_2, o_3, o_4, o_5, o_6\}$;

$S` = \{s_1, s_2\}$; $S`` = \{s_3, s_4, s_5\}$; $S = \{s_1, s_2, s_3, s_4, s_5\}$;

R = {read, write, own, yes};

$$M = \begin{bmatrix} - & o_1 & o_2 & o_3 & o_4 & o_5 & o_6 \\ s_1 & yes & yes & 0 & 0 & 0 & 0 \\ s_2 & yes & yes & 0 & 0 & 0 & 0 \\ s_3 & 0 & 0 & own\ write & 0 & 0 & own \\ s_4 & 0 & 0 & 0 & own\ write & read & read \\ s_5 & 0 & 0 & 0 & read & own\ write & 0 \end{bmatrix}$$

Используя результаты исследования И.Д. Королева и С.В. Носенко при создании МОДИ [2]можно утверждать, что при задании зон документа, переменных, терминологических понятий и предикатов в системе в соответствии с правилами построения МОДИ, каждый документ будет однозначно относиться к области ответственности только одного исполнителя. Другими словами подходить под условия только одной

команды запускаемой при поступлении документа. Согласно принципам функционирования системы ХРУ, команда выполняется только в том случае, если выполняются все ее условия. Таким образом, из запускаемых команд будет выполнено не более одной команды.

Очевидно, что в данной модели безопасности может быть реализованы любые реакции системы на «условия» при поступлении документа, определяемые политикой безопасности организации. Т.к. команды активируются автоматически и являются неизменными при поступлении документа любого вида, следовательно, в роли субъекта s_3может выступать автоматический программный модуль, идентифицированный в системе.

Выводы:

1. Модель МОДИ реализует дискреционную политику разграничения доступа.

2. Модель МОДИ может быть реализована на базе существующих программно – аппаратных комплексов реализующих дискреционное разграничение доступа, что существенно снизит расходы на внедрение.

3. Реализация в классической модели ХРУ позволяет говорить об открывающейся перспективе применения различных ее развитий с целью повышения уровня безопасности системы.

Список литературы:

1. Девянин П.Н. Модели безопасности компьютерных систем: Учеб.пособие для студ. высш. учеб. заведений / П.Н. Девянин – М.: Издательский центр «Академия», 2005 – 144 с.
2. 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.
3. 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.

4. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности/ В.Ю. Скиба, В.А. Курбатов – СПб. Питер, 2008. – 320с.
5. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие /П.Б. Хорев – М.: Форум, 2009. –352 с.

References

1. 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.

2. 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.

3. 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.

4. Skiba V.Ju., Kurbatov V.A. Rukovodstvo po zashhite ot vnutrennih ugroz informacionnoj bezopasnosti/ V.Ju. Skiba, V.A. Kurbatov – SPb. Piter, 2008. – 320s.

5. Horev P.B. Programmno-apparatnaja zashhita informacii: uchebnoe posobie /P.B. Horev – M.: Forum, 2009. –352 s.