РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2 525 481** (13) **C2**

(51) МПК
G06F 21/62 (2013.01)

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2012146550/08, 01.11.2012**

(24) Дата начала отсчета срока действия патента:
01.11.2012

Приоритет(ы):
(22) Дата подачи заявки: **01.11.2012**

(43) Дата публикации заявки: **10.05.2014** Бюл. № **13**

(45) Опубликовано: **20.08.2014** Бюл. № **23**

(56) Список документов, цитированных в отчете о поиске: **US 8020213 B2, 13.09.2011. US 2010/0058340 A1, 04.03.2010. Ю.С. РАКИЦКИЙ "Реализация объединения мандатного и ролевогодоступа"Высокопроизводительные параллельные вычисления на кластерных системах. Материалы XI Всероссийской конференции (Н. Новгород, 2-3 ноября 2011 г.), 2011, с. 255-257. US 2003/0225607 A1, 04.12.2003. US 2008/0034439 A1, 07.02.2008. US 7340469 B1, 04.03.2008**

Адрес для переписки:
117105, Москва, Варшавское ш., 26, Генеральному директору ОАО "НПО РусБИТех" В.Р. Ляпину

(72) Автор(ы):
Девянин Петр Николаевич (RU)

(73) Патентообладатель(и):
Открытое акционерное общество "Научно-производственное объединение Русские базовые информационные технологии" (RU), Девянин Петр Николаевич (RU)

RU 2525481 C2

(54) СПОСОБ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ПОТОКОВ В ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ С МАНДАТНЫМ И РОЛЕВЫМ УПРАВЛЕНИЕМ ДОСТУПОМ

(57) Реферат:

Изобретение относится к вычислительной технике. Технический результат заключается в предотвращении возможности использования субъектами-нарушителями защищенной информационной системы параметров ролей. Способ обеспечения безопасности информационных потоков в защищенных информационных системах с мандатным и ролевым управлением доступом, включающий представление защищенной информационной системы в рамках формальной модели безопасности логического мандатного и ролевого управления доступом и информационными потоками, в котором роли реализуют сущностями-контейнерами, к которым субъектам системы предоставляют доступы на владение, чтение или запись; каждой роли назначают уровень конфиденциальности, не превосходящий уровни конфиденциальности ролей, которым данная роль подчинена в иерархии; субъекту предоставляют доступ к роли только при условии, что он обладает к ней соответствующим эффективным правом доступа, субъекту разрешают изменять права доступа к сущностям, которыми обладает роль, только тогда, когда он обладает к роли доступом на запись; субъекту

разрешают изменять права доступа к роли только тогда, когда он обладает к ней доступом на владение. 2 з.п. ф-лы, 2 табл.

RU 2525481 C2

RUSSIAN FEDERATION

(19) **RU** (11) **2 525 481** (13) **C2**

(51) Int. Cl.
G06F 21/62 (2013.01)

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2012146550/08, 01.11.2012**

(24) Effective date for property rights:
01.11.2012

Priority:
(22) Date of filing: **01.11.2012**

(43) Application published: **10.05.2014** Bull. № **13**

(45) Date of publication: **20.08.2014** Bull. № **23**

Mail address:
117105, Moskva, Varshavskoe sh., 26, General'nomu direktoru OAO "NPO RusBITekh" V.R. Ljapinu

(72) Inventor(s):
Devjanin Petr Nikolaevich (RU)

(73) Proprietor(s):
Otkrytoe aktsionernoe obshchestvo "Nauchno-proizvodstvennoe ob"edinenie Russkie bazovye informatsionnye tekhnologii" (RU),
Devjanin Petr Nikolaevich (RU)

(54) METHOD OF SECURING INFORMATION FLOW IN SECURE INFORMATION SYSTEMS WITH MANDATORY AND ROLE-BASED ACCESS CONTROL

(57) Abstract:

FIELD: physics, computer engineering.

SUBSTANCE: invention relates to computer engineering. A method of securing information flow in secure information systems with mandatory and role-based access control, which includes presenting a secure information system within a formal security model of logic mandatory and role-based control of access and information flow in which roles are realised by substance-containers to which system subjects are granted access for ownership, reading or writing; each role is assigned a confidentiality level which does not exceed the confidentiality level of roles to which said role is subordinate in a hierarchy; a subject is granted access to a role only if the subject has the respective effective access right to said role; the subject is allowed to alter access rights to substances possessed by the role only when the subject has a write access to the role; a subject is allowed to alter the access rights to a role only when the subject has an ownership access to said role.

EFFECT: preventing secure information system violator subjects from using role parameters.

3 cl, 2 tbl

RU 2525481 C2

RU 2525481 C2

Область техники

Изобретение относится к области защиты информационных систем, а именно к способам обеспечения безопасности информационных потоков в защищенных информационных системах с мандатным и ролевым управлением доступом.

Уровень техники

Логическое управление доступом - один из основных механизмов защиты информационных систем. В существующих информационных системах, как правило, применяется дискреционное или мандатное (полномочное) логическое управление доступом. Более перспективным является использование вместо дискреционного управления доступом ролевого, позволяющего сгруппировать права доступа (с учетом специфики их применения) в роли и в результате определить более четкие и понятные для пользователей информационных систем правила управления доступом.

Противодействие запрещенным информационным потокам (скрытым каналам), в том числе информационным потокам по памяти или по времени [ГОСТ Р 53113.1-2008, ГОСТ Р 53113.2-2009 «Защита информационных технологий и автоматизированных систем от угроз информационной безопасности, реализуемых с использованием скрытых каналов», части 1, 2] от сущностей с высоким уровнем конфиденциальности к сущностям с низким уровнем конфиденциальности - необходимое условие безопасности информационных систем, включающих механизм мандатного управления доступом. «Механическое» объединение ролевого и мандатного управления доступом без учета специфики каждого из них может негативно отразиться на безопасности полученного решения, в том числе при обеспечении защиты от запрещенных информационных потоков. Например, запрещенные информационные потоки по времени могут быть созданы кооперирующими субъектами с использованием назначения и отзыва в согласованные моменты времени прав доступа ролей.

Известна модель [Bell D.E., LaPadula L.J. Secure Computer Systems: Unified Exposition and Multics Interpretation. Bedford, Mass.: MITRE Corp., 1976. MTR-2997 Rev. 1.], в которой задаются требования к реализации в информационной системе мандатного и дискреционного управления доступом. Но в ней не рассматривается ролевое управление доступом, наличие иерархии сущностей не учитывается при управлении доступом и не предлагаются способы противодействия запрещенным информационным потокам по времени.

Известна модель [Lanawehrm E., Heitmeyer L., McLean J. A Security Model for Military Message Systems // ACM Trans. On Computer Systems. Vol.9, №3. P.198-222], в которой реализуется мандатное и дискреционное управление доступом с учетом иерархии сущностей (с применением атрибутов сущностей-контейнеров CCR - Container Clearance Required) и используются роли. Но в этой модели роли применяются только в качестве дополнения к дискреционным правам доступа, не предлагаются способы администрирования прав доступа ролей и способы противодействия запрещенным информационным потокам по времени.

Известна модель [Sandhu R. Role-Based Access Control // Advanced in Computers. Academic Press, 1998. Vol.46], в которой предлагается способ реализации мандатного и ролевого управления доступом. Для противодействия запрещенным информационным потокам по памяти в ней все роли разделяются по уровням конфиденциальности сущностей, права доступа к которым они предоставляют, и по видам доступа к ним - роли-«на чтение» и роли-«на запись», с применением соответствующих ограничений на функции текущих ролей сессий (субъектов) и прав доступа ролей. Но в данной модели не рассматриваются механизмы защиты от запрещенных информационных потоков по

времени и не предлагаются способы администрирования прав доступа ролей. Кроме того, при реализации модели без использования дополнительно дискреционного управления доступом невозможно назначение пользователям информационной системы индивидуальных прав доступа к сущностям.

Известны системы и способы, например, патенты RU 2134931 C1, H04L 9/32, G06F 12/14, опубл. 1999-08-20; RU 2434283 C1, G06F 21/20, G06F 21/22, опубл. 2011-11-20; RU 2443017 C1, G06F 21/22, G06F 12/14, опубл. 2012-02-20; US 7593942 B2, G06F 17/30, опубл. 2009-09-22; US 7831570 B2, G06F 7/00, опубл. 2010-11-09; заявка на изобретение RU 2009129744 A, G06F 13/00, опубл. 2011-02-10, ориентированные на реализацию в информационной системе мандатного управления доступом. Но в них не предлагаются способы противодействия запрещенным информационным потокам по времени, возникающим, в том числе, при использовании субъектами-нарушителями параметров ролей.

Известны системы и способы, например, патенты RU 2379754 C1, G06F 21/22 опубл. 2010-01-20; RU 2427904 C2, G06F 21/20, H04W 48/02, опубл. 2010-10-10; заявки на изобретение RU 2008148041 A, G06F 12/00, опубл. 2010-06-10; RU 2010154544 A, G06F 21/20, опубл. 2012-07-10, предназначенные для реализации управления доступом в информационных системах. Но в них не задаются требования к совместному применению мандатного и ролевого управления доступом, выполнение которых позволит назначать права доступа ролей к сущностям в соответствии с их уровнями конфиденциальности, предоставлять субъектам роли в качестве текущих в зависимости от уровней доступа субъектов и уровней конфиденциальности ролей, а также позволит предотвратить в информационной системе запрещенные информационные потоки.

Раскрытие изобретения

Технический результат заключается в предотвращении возможности использования субъектами-нарушителями защищенной информационной системы параметров ролей, в том числе прав доступа ролей к сущностям, для реализации информационных потоков по памяти или по времени от сущностей с высоким уровнем конфиденциальности к сущностям с низким уровнем конфиденциальности информации.

Указанный результат достигается за счет того, что в способе обеспечения безопасности информационных потоков в защищенных информационных системах с мандатным и ролевым управлением доступом, включающем представление защищенной информационной системы в рамках формальной модели безопасности логического мандатного и ролевого управления доступом и информационными потоками,

роли реализуют сущностями-контейнерами, к которым субъектам системы предоставляют доступы на владение, чтение или запись;

эффективные права доступа субъектов к сущностям, в том числе к субъектам и ролям, назначают рекурсивно в соответствии с правилом: субъект обладает эффективным правом доступа к сущности только тогда, когда он обладает доступом на чтение к роли, имеющей соответствующее право доступа к сущности, и эффективными правами доступа на выполнение ко всем сущностям, которым данная сущность подчинена в иерархии;

каждой роли назначают уровень конфиденциальности, не превосходящий уровни конфиденциальности ролей, которым данная роль подчинена в иерархии;

субъекту предоставляют доступ к роли только при условии, что он обладает к ней соответствующим эффективным правом доступа, при этом доступ субъекта на чтение к роли предоставляют только тогда, когда уровень конфиденциальности роли не превосходит текущего уровня доступа субъекта, доступ субъекта на запись или на

владение к роли предоставляют только тогда, когда уровень конфиденциальности роли равен текущему уровню доступа субъекта;

субъекту разрешают изменять права доступа к сущностям или ролям, которыми обладает некоторая роль, только тогда, когда он обладает к ней доступом на запись;

субъекту разрешают изменять права доступа к роли только тогда, когда он обладает к ней доступом на владение.

Защита целостности данных, к которым в информационной системе предоставляется доступ субъектам, достигается за счет того, что информационную систему представляют в рамках формальной модели безопасности логического мандатного и ролевого управления доступом и информационными потоками и контроля целостности,

каждой роли назначают уровень целостности, не превосходящий уровни целостности ролей, которым данная роль подчинена в иерархии;

каждой роли назначают права доступа на владение или запись к сущности только тогда, когда уровень целостности сущности не выше уровня целостности роли;

субъекту предоставляют доступ к роли только тогда, когда уровень целостности роли не превосходит текущего уровня целостности субъекта.

В качестве состояния безопасности защищенной информационной системы рассматривают полное множество сущностей доступа, включающее субъекты, объекты, контейнеры и роли, и их параметров безопасности, состав и влияние которых на безопасность определяется типом и версией операционной среды защищенной информационной системы, в том числе включают такие сущности и параметры безопасности:

учетные записи доверенных и недоверенных пользователей,

элементы файловой системы, в том числе диски, каталоги, файлы, ссылки,

элементы реестра, окна графического интерфейса, COM/DCOM-объекты, сетевые интерфейсы,

процессы, потоки, демоны, драйверы, устройства, сервисы, объекты синхронизации,

списки привилегий и прав доступа ролей к сущностям, метки разделяемых контейнеров,

метки уровней доступа, конфиденциальности и целостности, CCR-метки способа доступа внутрь контейнеров; иерархии сущностей, в том числе ролей и субъектов.

Формально при реализации способа, в общем виде, информационную систему $\Sigma(G^*, OP)$ представляют множеством всех ее состояний - G^* и множеством правил преобразования состояний - OP. При этом каждое состояние информационной системы $\Sigma(G^*, OP)$ представляют кортежем (PA, A, F) и включают в его описание следующие элементы:

$E=O \cup C$ - множество сущностей (всех компонент информационной системы $\Sigma(G^*, OP)$, к которым назначают права доступа), где O - множество объектов (например, файлов), C - множество контейнеров (например, каталогов) и $O \cap C=\varnothing$;

$S \subseteq E$ - множество субъектов (например, процессов компьютеров информационной системы), функционирующих от имени учетных записей пользователей;

R - множество ролей;

$H_E: E \cup R \rightarrow 2^{E \cup R}$ - функция иерархии сущностей и ролей, удовлетворяющая условиям: если сущность или роль $e \in H_E(c)$, то $e<c$, при этом если $e \in C \cup R \cup S$, то не существует сущности-контейнера или роли $d \in C \cup R$ такой, что $e<d$, $d<c$;

$R_r=\{read_r, write_r, execute_r, own_r\}$ - множество видов прав доступа, при этом $read_r$ - право доступа на чтение, $write_r$ - право доступа на запись, $execute_r$- право доступа на

выполнение, own_r- право доступа на владение;

$R_a=\{read_a, write_a, own_a\}$ - множество видов доступа, при этом $read_a$ - доступ на чтение, $write_a$ - доступ на запись, own_a- доступ на владение;

$Rf=\{write_m, write_t\}$ - множество видов информационных потоков (по памяти и по времени соответственно);

$P \subseteq (E \cup R)\times R_r$ - множеств прав доступа к сущностям и ролям;

$A \subseteq S\times(E \cup R)\times R_a$ - множество доступов субъектов к сущностям и ролям;

$F \subseteq (E \cup R)\times(E \cup R)\times R_f$ - множество информационных потоков (используют для обоснования достижения технического результата);

$PA:R\rightarrow 2^P$ - функция прав доступа к сущностям и ролям ролей, при этом для каждого права доступа $p \in P$ существует роль $r \in R$ такая, что выполняется условие $p \in PA(r)$;

$(LC, \leq)$ - решетка многоуровневой безопасности уровней конфиденциальности (как правило, декартово произведение линейной шкалы уровней конфиденциальности данных и множества всех подмножеств конечного множества неиерархических категорий данных);

$f_e:E \cup R\rightarrow LC$ - функция, задающая уровень конфиденциальности для каждой сущности или роли;

$f_s:S\rightarrow LC$ - функция, задающая для каждого субъекта его текущий уровень доступа;

$(LI, \leq)$ - линейная шкала двух уровней целостности данных, где $LI=\{i\_low, i\_high\}$, $i\_low<i\_high$;

$i_e:E \cup R\rightarrow LI$ - функция, задающая уровень целостности для каждой сущности или роли;

$i_s:S\rightarrow LI$ - функция, задающая для каждого субъекта его текущий уровень целостности;

execute_container: $S\times(E \cup R)\rightarrow\{true, false\}$ - функция доступа субъектов к сущностям или ролям в контейнерах такая, что для субъекта $s \in S$ и сущности или роли $e \in E \cup R$ справедливо равенство execute_container(s, e) = true тогда и только тогда, когда существует последовательность сущностей или ролей $e_1, \ldots, e_n \in E \cup R$, где $n\geq 1$, $e = e_n$, удовлетворяющих следующим условиям: не существует сущности-контейнера или роли $e_0 \in E \cup R$ такой, что $e_1 \in H_E(e_0)$; $e_i \in H_E(e_{i-1})$, где $1<i\leq n$; существует $r_i \in R$ такая, что $(s, r_i, read_a) \in A$ и $(e_i\ execute_r) \in PA(r_i)$, $f_e(e_i)\leq f_s(s)$ и $i_e(e_i)\leq i_s(s)$, где $1\leq i<n$.

В каждом состоянии информационной системы $\Sigma(G^*, OP)$ обеспечивают выполнение следующих условий:

у каждой роли есть права доступа $execute_{r'}$- ко всем ролям: для каждых двух ролей $r, r' \in R$ выполняется условие $(r, execute_r) \in PA(r')$;

уровень конфиденциальности сущности или роли, входящей в состав сущности-контейнера или роли, соответственно, не превосходит ее уровня конфиденциальности: для сущностей или ролей $e, e' \in E \cup R$, если $e\leq e'$, то $f_e(e)\leq fe(e')$;

уровень целостности сущности или роли, входящей в состав сущности-контейнера или роли, соответственно, не превосходит ее уровня целостности: для сущностей или ролей $e, e' \in E \cup R$, если $e\leq e'$, то $f_e(e)\leq f_e(e')$;

роль может содержать права доступа на владение или запись к сущностям или ролям с не выше, чем у нее уровнем целостности: для роли $r \in R$ и сущности или роли $e \in E \cup R$, если $(e, \alpha_r) \in PA(r)$, то $i_e(e)\leq i_e(r)$, где $\alpha_r \in \{own_r, write_r\}$.

В информационной системы $\Sigma(G^*, OP)$ реализуют, как минимум, следующие правила

преобразования состояний («де-юре» правила), условия применения которых в текущем состоянии и результаты применения в последующем состоянии системы заданы в таблице 1.

Таблица 1

«Де-юре» правила преобразования состояний информационной системы $\Sigma(G^*, OP)$

Правило	Исходное состояние G = (PA, A, F)	Результирующее состояние G'=(PA',A', F')
access_own(x, y)	$x \in S$, $y \in E \cup R$, существует $r \in R$:$(x, r, read_a) \in A$, $(y, own_r) \in PA(r)$, $f_e(y)=f_s(x)$, $i_e(y) \le i_s(x)$ и execute_container(x, y)= true	PA'=PA, F'=F, $A'=A \cup \{(x, y, own_a)\}$
access_write(x, y)	$x \in S$, $y \in E \cup R$, существует $r \in R$:$(x, r, read_a) \in A$, $(y, write_r) \in PA(r)$, $f_c(y)=f_s(x)$, $i_e(y) \le i_s(x)$ и execute_container(x, y)= true	PA'-PA, F'=F, $A'=A \cup \{(x, y, write_a)\}$
access read(x, y)	$x \in S$, $y \in E \cup R$, существует $r \in R$:$(x, r, read_a) \in A$, $(y, read_r) \in PA(r)$, $f_e(y) \le f_s(x)$, execute_container(x, y)=true, если $y \in R$, то $i_e(y) \le i_s(x)$	PA'=PA, F'=F, $A'=A \cup \{(x, y, read_a)\}$
delete_access(x, y, α_a)	$x \in S$, $y \in E \cup R$, $(x, y, \alpha_a) \in A$	PA'=PA, F'=F, $A'=A\setminus\{(x, y, \alpha_a)\}$
grant_rights(x, r, y, α_r)	$x \in S$, $y \in E \cup R$, $r \in R$, $(x, r, write_a) \in A$, $(x, y, own_a) \in A$, если $\alpha_r \in \{own_r, write_r\}$, то $i_e(y) \le i_c(r)$	A'=A, F'=F, PA'(r)=PA(r) $\cup$ {(y, α_r)} и для r' $\in R \setminus \{r\}$ выполняется равенство PA'(r')=PA (r')
remove_rights(x, r, y, a_r)	$x \in S$, $y \in E \cup R$, $r \in R$, $(x, r, write_a) \in A$, $(x, y, OWtl_a) \in A$	A'=A, F'=F, PA'(r)=PA(r) $\setminus$ {(y, a_r)}, и для r' $\in R \setminus \{r\}$ выполняется равенство PA'(r')=PA (r')

Для обоснования достижения технического результата используют, как минимум, следующие правила преобразования состояний («де-факто» правила) информационной системы $\Sigma(G^*, OP)$, условия применения которых в текущем состоянии и получаемые в результате их применения информационные потоки в последующем состоянии системы заданы в таблице 2.

Таблица 2

«Де-факто» правила преобразования состояний информационной системы $\Sigma(G^*, OP)$

Правило	Исходное состояние G=(PA, A, F)	Результирующее состояние G'=(PA', A', F')
flow_memory_access (x, y, α_a)	$x \in S$, $y \in E$, $(x, y, \alpha_a) \in A$, где $\alpha_a \in \{read_a, write_a\}$	PA'=PA, A'=A, [если $\alpha_a=read_a$, то F'=F $\cup$ {(y, x, $write_m$)}], [если $\alpha_a=write_a$, то F'=F $\cup$ {(x, y, $write_m$)}]
flow_time_access(x, y)	$x \in S$, $y \in E \cup R$, $(x, y, \alpha_a) \in A$, где $\alpha_a \in R_a$	PA'=PA, A'=A, [если $\in_a \in \{own_a, write_a\}$, то F'=F $\cup$ {(x, y, write,), (y, x, $write_t$)}],, [если $\alpha_a=read_a$, то F'=F $\cup$ {(y, x, $write_t$)}]
take_flow(x, y)	$x, y \in S$, $x \ne y$, $(x, y, own_a) \in A$	PA'=PA, A'=A, F'=F $\cup$ {(x, e, α): (y, e, α) $\in$ F, $e \in E \cup R$ и $\alpha \in \{write_m, write_t\}$}
find(x, y, z)	$x, y \in S$, $z \in E \cup R$, $x \ne z$, (x, y, α_f), $(y, z, \beta_f) \in F$, где $\alpha_f, \beta_f \in \{write_m, write_t\}$	PA'=PA, A'=A, если $write_t \in \{\alpha_f, \beta_f\}$ и $z \in E$, то F'=F $\cup$ {(x, z, $write_m$)}, иначе F'=F $\cup$ {(x, z, $write_t$)}
post(x, y, z)	$x, z \in S$, $y \in E \cup R$, $x \ne z$, $(x, y, \alpha_f) \in F$, где $\alpha_f \in \{write_m, write_t\}$, и $(z, y, \beta_a) \in A$, где $\beta_a \in R_a$	PA'=PA, A'=A, если $\alpha_f=write_m$, $\beta_a=read_a$ и $y \in E$, то F'=F $\cup$ {(x, z, $write_m$)}, иначе F'=F $\cup$ {(x, z, $write_t$)}
pass(x, y, z)	$y \in S$, $x, z \in E \cup R$, $x \ne z$, $(y, x, \alpha_a) \in A$, где $\alpha_a \in \{read_a, own_a\}$, и $(y, z, \beta_f) \in F$, где $\beta_f \in \{write_m, write_t\}$	PA'=PA, A'=A, если $\alpha_a=read_a$, $\beta_f=write_m$ и $x, z \in E$, то F'=F $\cup$ {(x, z, $write_m$)}, иначе F'=F $\cup$ {(x, z, $write_t$)}

Таким образом, в способе использован классический для теории моделирования безопасности управления доступом и информационными потоками подход, заключающийся в следующем: предполагается, что проверка безопасности защищенной информационной системы должна осуществляться после того, как доверенные (привилегированные, административные субъекты, являющиеся частью подсистемы безопасности, чью функциональность можно верифицировать) субъекты выполнили свои задачи по изменению параметров функционирования системы. При этом требуется удостовериться, что дальнейшее функционирование системы под воздействием недоверенных, часто рассматриваемых как нарушители, субъектов будет безопасным,

т.е. не приведет к созданию запрещенных информационных потоков. В результате достижение технического результата обосновывают следующим образом:

задают начальное состояние $G_0=(PA_0, A_0, F_0)$ информационной системы $\Sigma(G^*, OP)$, в котором отсутствуют доступы субъектов к сущностям или ролям и отсутствуют информационные потоки ($A_0=\varnothing$, $F_0=\varnothing$);

с применением математической логики и теории множеств доказывают невозможность перехода информационной системы $\Sigma(G^*, OP)$ из начального состояния $G_0=(PA_0, A_0, F_0)$ в результате применения произвольной конечной последовательности «де-юре» или «де-факто» правил $op_1, \ldots, op_N$, заданных в таблицах 1 и 2, соответственно, в состояние $G_N=(PA_N, A_N, F_N)$, где $G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N$, $N>0$, в котором существуют (во множестве F_N) запрещенные информационные потоки по памяти или по времени от сущностей или ролей с высоким уровнем конфиденциальности к сущностям или ролям с низким уровнем конфиденциальности (информационный поток вида $(x, y, write_m)$ или $(x, y, write_t)$, где $x, y \in E \cup R$ и $f_e(x)>f_e(y)$).

Осуществление изобретения

При применении способа для описания каждого состояния информационной системы $\Sigma(G^*, OP)$, в том числе ее начального состояния $G_0=(PA_0, A_0, F_0)$:

используют виды прав доступа $read_r$, $write_r$, $execute_r$, own_r и виды доступов $read_a$, $write_a$, own_a, соответственно (традиционно в защищенных информационных системах, например, в операционных системах семейства Linux, рассматривают три вида прав доступа к сущностям: на чтение, на запись и на выполнение или на использование контейнера - каталога, а также при управлении доступом к сущностям учитывают наличие у них владельцев, имеющих права передавать другим, субъектам права доступа к сущностям); применительно к ролям: право доступа own_r - владелец роли, $read_r$ - право получать роль как текущую, просматривать ее параметры, $write_r$ - право изменять множество прав доступа роли, execute - право обращаться к ролям, подчиненным данной роли в иерархии ролей; доступ own_a - владение (изменение параметров) роли, $read_a$ - получение субъектом роли как текущей, $write_a$ - доступ на изменение прав доступа роли или состава ролей, подчиненных ей в иерархии;

для предотвращения возможности использования прав доступа ролей при создании запрещенных информационных потоков роли реализуют сущностями-контейнерами (например, в операционных системах создают «виртуальную» иерархическую файловую систему, каждый элемент которой является ролью, а иерархия ее элементов соответствует иерархии ролей) и задают уровни конфиденциальности ролей (например, в операционных системах для этого используют расширенные атрибуты элементов файловой системы);

все компоненты защищенной информационной системы (субъекты, сущности и роли) разделяют на два непересекающихся множества, влияющих на целостность и безопасность системы или нет, и присваивают им соответствующие уровни целостности i_high и i_low (здесь преимущества мандатного контроля целостности аналогичны преимуществам мандатного управления доступом в сравнении с дискреционным управлением доступом, т.е. его внедрение обеспечивает большую ясность правил разделения компонент системы на критичные и некритичные с точки зрения ее целостности; его реализация с помощью ролей более понятна для пользователей и администраторов защищенной информационной системы, кроме того, требуемый для пользователя текущий уровень целостности субъекта, функционирующего от его имени,

непосредственно зависит от выполняемой пользователем в системе функции - роли; в операционных системах для задания уровней целостности используют, например, расширенные атрибуты элементов файловой системы);

использованную в формальном описании информационной системы $\Sigma(G^*, OP)$ функцию execute_container непосредственно в информационной системе не реализуют, так как ее значение при каждом доступе субъекта к сущности вычисляют при последовательной проверке прав доступа к сущностям-контейнерам, содержащим данную сущность, начиная с корневой сущности-контейнера (в операционных системах семейства Linux, например, с сущности-контейнера «/»).

При применении способа в защищенной информационной системе $\Sigma(G^*, OP)$ реализуют «де-юре» правило преобразования состояний (например, в операционных системах в функции монитора ссылок, выполняющей проверку прав доступа при доступе субъектов к сущностям):

в правилах access_own(x, y), access_write(x, y) и access_read(x, y) проверяют наличие в текущем состоянии системы у субъекта x доступа на чтение к некоторой роли r, содержащей соответствующее право доступа к сущности или роли y, а также истинность функции execute_container(x, y); кроме того, в правилах access_own(x, y) и access_write(x, y) проверяют, что уровень конфиденциальности y равен текущему уровню доступа x, а уровень целостности y не превосходит текущего уровня целостности x, в правиле access_read(x, y) проверяют, что уровень конфиденциальности y не превосходит текущего уровня доступа x, и случае, когда y является ролью, что уровень целостности y не превосходит текущего уровня целостности x; в случае успешной проверки в последующем состоянии системы предоставляют x соответствующий доступ к y;

в правиле delete_access(x, y, α_a) проверяют, что в текущем состоянии системы у субъекта x имеется доступ α_a к сущности или роли y, и в случае успешной проверки в последующем состоянии системы отзывают у x доступ oc_a к y;

в правиле grant_rights(x, r, y, α_r) проверяют наличие в текущем состоянии системы у субъекта x доступа на запись к роли r и доступа владения к сущности или роли y, кроме того, если право доступа α_r является правом доступа на владение или запись, то проверяют, что уровень целостности y не превосходит уровня целостности r, в случае успешной проверки в последующем состоянии системы предоставляют r право доступа α_r к y;

в правиле remove_rights(x, r, y, α_r) проверяют наличие в текущем состоянии системы у субъекта x доступа на запись к роли r и доступа владения к сущности или роли y, и в случае успешной проверки в последующем состоянии системы отзывают у r право доступа α_r к y.

При обосновании невозможности реализации в защищенной информационной системе $\Sigma(G^*, OP)$ запрещенных информационных потоков кроме «де-юре» правил используют «де-факто» правила преобразования состояний системы:

в правиле flow_memory_access(x, y, α_a) проверяют наличие в текущем состоянии системы у субъекта x доступа на чтение или запись α_a к сущности или роли y, и в случае успешной проверки в последующем состоянии системы включают во множество информационных потоков F информационный поток по памяти либо от y к x (во множество F добавляют элемент (x, y, $write_m$)), когда доступ α_a является доступом на чтение, либо от x к y, когда доступ α_a является доступом на запись;

в правиле flow_time_access(x, y) проверяют наличие в текущем состоянии системы у

субъекта x любого доступа α_a к сущности или роли y, и в случае успешной проверки в последующем состоянии системы включают во множество информационных потоков F информационный поток по времени от y к x (во множество F добавляют элемент (y, x, $write_t$)), и если доступ α_a является доступом на владение или запись, то также включают во множество F информационный поток по времени от x к y;

в правиле take_flow(x, y) проверяют наличие в текущем состоянии системы у субъекта x доступа владения к субъекту y, и в случае успешной проверки в последующем состоянии системы включают во множество информационных потоков F информационные потоки от x ко всем сущностям, к которым соответствующий информационный поток имел y;

в правиле find(x, y, z) проверяют наличие в текущем состоянии системы информационных потоков от субъекта x к субъекту y и от него к сущности или роли z, и в случае успешной проверки в последующем состоянии системы включают во множество информационных потоков F информационный поток от x к z по памяти, если оба существующих информационных потока являются информационными потоками по памяти, иначе включают информационный поток по времени;

в правиле post(x, y, z) проверяют наличие в текущем состоянии системы информационного потока от субъекта x к сущности или роли y и любого доступа субъекта z к y, и в случае успешной проверки в последующем состоянии системы включают во множество информационных потоков F информационный поток от x к z по памяти, если существующий информационный поток является информационным потоком по памяти, а доступ - доступ на чтение, иначе включают информационный поток по времени;

в правиле pass(x, y, z) проверяют наличие в текущем состоянии системы информационного потока от субъекта y к сущности или роли z и доступа на чтение или владение y к сущности или роли x, и в случае успешной проверки в последующем состоянии системы включают во множество информационных потоков F информационный поток от x к z по памяти, если существующий информационный поток является информационным потоком по памяти, а доступ - доступ на чтение, иначе включают информационный поток по времени.

Обоснование невозможности реализации в защищенной информационной системе $\Sigma(G^*, OP)$ запрещенных информационных потоков по памяти или по времени от сущностей или ролей с высоким уровнем конфиденциальности к сущностям или ролям с низким уровнем конфиденциальности осуществляют без использования правил преобразования состояний системы delete_access(x, y, α_a) и remove_rights(x, r, y, α_r) («немонотонных» правил, применение которых приводит к удалению из состояния его элементов - доступов субъектов к сущностям или прав доступа ролей), так как наличие этих правил не добавляет дополнительных возможностей по созданию запрещенных информационных потоков. Обоснование осуществляют от противного, предполагая возможность реализации запрещенного информационного потока по времени в результате применения к начальному состоянию системы $G_0=(PA_0, A_0, F_0)$ некоторой последовательности «де-юре» или «де-факто» правил преобразования состояний, используя при этом математическую индукцию по длине этой последовательности.

Таким образом, при применении описанного способа в защищенной информационной системе реализуют единый механизм мандатного и ролевого управления доступом, и в результате предотвращают возможность использования субъектами-нарушителями параметров ролей для создания запрещенных информационных потоков по памяти

или по времени от сущностей с высоким уровнем конфиденциальности к сущностям с низким уровнем конфиденциальности информации.

Формула изобретения

1. Способ обеспечения безопасности информационных потоков в защищенных информационных системах с мандатным и ролевым управлением доступом, включающий представление защищенной информационной системы в рамках формальной модели безопасности логического мандатного и ролевого управления доступом и информационными потоками, отличающийся тем, что роли реализуют сущностями-контейнерами, к которым субъектам системы предоставляют доступы на владение, чтение или запись; эффективные права доступа субъектов к сущностям, в том числе к субъектам и ролям, назначают рекурсивно в соответствии с правилом: субъект обладает эффективным правом доступа к сущности только тогда, когда он обладает доступом на чтение к роли, имеющей соответствующее право доступа к сущности, и эффективными правами доступа на выполнение ко всем сущностям, которым данная сущность подчинена в иерархии; каждой роли назначают уровень конфиденциальности, не превосходящий уровни конфиденциальности ролей, которым данная роль подчинена в иерархии; субъекту предоставляют доступ к роли только при условии, что он обладает к ней соответствующим эффективным правом доступа, при этом доступ субъекта на чтение к роли предоставляют только тогда, когда уровень конфиденциальности роли не превосходит текущего уровня доступа субъекта, доступ субъекта на запись или на владение к роли предоставляют только тогда, когда уровень конфиденциальности роли равен текущему уровню доступа субъекта; субъекту разрешают изменять права доступа к сущностям, которыми обладает роль, только тогда, когда он обладает к роли доступом на запись; субъекту разрешают изменять права доступа к роли только тогда, когда он обладает к ней доступом на владение.

2. Способ по п.1, отличающийся тем, что информационную систему представляют в рамках формальной модели безопасности логического мандатного и ролевого управления доступом и информационными потоками и контроля целостности, каждой роли назначают уровень целостности, не превосходящий уровни целостности ролей, которым данная роль подчинена в иерархии; каждой роли назначают права доступа на владение или запись к сущности только тогда, когда уровень целостности сущности не выше уровня целостности роли; субъекту предоставляют доступ к роли только тогда, когда уровень целостности роли не превосходит текущего уровня целостности субъекта.

3. Способ по п.1 или 2, отличающийся тем, что в качестве состояния безопасности защищенной информационной системы рассматривают полное множество сущностей доступа, включающее субъекты, объекты, контейнеры и роли, и их параметров безопасности, состав и влияние которых на безопасность определяется типом и версией операционной среды защищенной информационной системы, в том числе включают такие сущности и параметры безопасности: учетные записи доверенных и недоверенных пользователей; элементы файловой системы, в том числе диски, каталоги, файлы, ссылки; элементы реестра, окна графического интерфейса, COM/DCOM-объекты, сетевые интерфейсы; процессы, потоки, демоны, драйверы, устройства, сервисы, объекты синхронизации; списки привилегий и прав доступа ролей к сущностям, метки разделяемых контейнеров; метки уровней доступа, конфиденциальности и целостности, CCR-метки способа доступа внутрь контейнеров; иерархии сущностей, в том числе ролей и субъектов.