МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

DOI 10.17223/20710410/5/8

УДК 004.94

АНАЛИЗ УСЛОВИЙ ПОЛУЧЕНИЯ ДОСТУПА ВЛАДЕНИЯ В РАМКАХ БАЗОВОЙ РОЛЕВОЙ ДП-МОДЕЛИ БЕЗ ИНФОРМАЦИОННЫХ ПОТОКОВ ПО ПАМЯТИ[1]

П. Н. Девянин

Институт криптографии, связи и информатики, г. Москва, Россия

E-mail: peter_devyanin@hotmail.com

В рамках базовой ролевой ДП-модели анализируются условия получения недоверенными субъект-сессиями доступа владения к доверенным субъект-сессиям. При этом рассматривается случай, когда взаимодействует произвольное число субъект-сессий, и они не получают доступа владения друг к другу с использованием информационных потоков по памяти к функционально ассоциированным с субъект-сессиями сущностям.

Ключевые слова: *компьютерная безопасность, ролевая модель, ДП-модели.*

1. Основные элементы базовой ролевой ДП-модели

На основе семейства ролевых моделей $RBAC$ [1 – 3] и семейства ДП-моделей компьютерных систем (КС) с дискреционным или мандатным управлением доступом [4] построена базовая ролевая ДП-модель (БР ДП-модель) [5, 6]. Эта модель ориентирована на анализ в КС с ролевым управлением доступом условий передачи прав доступа ролей и реализации информационных потоков по памяти и по времени.

В настоящее время в рамках БР ДП-модели не удалось завершить исследования КС с ролевым управлением доступом, на условия функционирования которых не наложено ограничений. В связи с этим в [5, 6] с применением БР ДП-модели выполнен анализ необходимых и достаточных условий передачи прав доступа для случая, когда в системе существуют только две субъект-сессии двух пользователей.

Рассмотрим БР ДП-модель, в которой взаимодействует произвольное число субъект-сессий, и они не получают доступа владения друг к другу с использованием информационных потоков по памяти к функционально ассоциированным с субъект-сессиями сущностям.

Основными элементами БР ДП-модели являются:

$E = O \cup C$ — множество сущностей, где O — множество объектов, C — множество контейнеров и $O \cap C = \varnothing$;

U — множество пользователей;

L_U — множество доверенных пользователей;

N_U — множество недоверенных пользователей;

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы. Результаты работы докладывались на Международной конференции с элементами научной школы для молодёжи, г. Омск, 7–12 сентября 2009 г.

$S \subseteq E$ — множество субъект-сессий пользователей;

L_S — множество доверенных субъект-сессий;

N_S — множество недоверенных субъект-сессий;

R — множество ролей;

AR — множество административных ролей;

$R_r = \{read_r, write_r, append_r, execute_r, own_r\}$ — множество видов прав доступа;

$R_a = \{read_a, write_a, append_a, own_a\}$ — множество видов доступа;

$R_f = \{write_m, write_t\}$ — множество видов информационных потоков;

$A \subseteq S \times E \times R_a$ — множество доступов субъект-сессий к сущностям;

$F \subseteq E \times E \times R_f$ — множество информационных потоков между сущностями;

$P \subset E \times R_r$ — множество прав доступа к сущностям;

$UA : U \to 2^R$ — функция авторизованных ролей пользователей;

$AUA : U \to 2^{AR}$ — функция авторизованных административных ролей пользователей;

$PA : R \to 2^P$ — функция прав доступа ролей;

$user : S \to U$ — функция принадлежности субъект-сессии пользователю;

$roles : S \to 2^R \cup 2^{AR}$ — функция текущих ролей субъект-сессий;

$can\_manage\_rights : AR \to 2^R$ — функция администрирования прав доступа ролей;

$H_E : E \to 2^E$ — функция иерархии сущностей;

$H_R : R \to 2^R$ — функция иерархии ролей;

$H_{AR} : AR \to 2^{AR}$ — функция иерархии административных ролей;

$G = (PA, user, roles, A, F, H_E)$ — состояние системы;

$\Sigma(G^*, OP)$ — система, при этом G^* — множество всех возможных состояний, OP — множество правил преобразования состояний;

$G \vdash_{op} G'$ — переход системы $\Sigma(G^*, OP)$ из состояния G в состояние G' с использованием правила преобразования состояний $op \in OP$;

$\Sigma(G^*, OP, G_0)$ — система $\Sigma(G^*, OP)$ с начальным состоянием G_0;

$[s] \subset E \cup U$ — множество сущностей, функционально ассоциированных с субъект-сессией s (при этом по определению выполняется условие $s \in [s]$), и пользователей, каждый из которых может создать субъект-сессию, являющуюся функционально ассоциированной сущностью с субъект-сессией s;

$fa : U \times E \to 2^E \cup 2^U$ — функция, задающая множества сущностей, функционально ассоциированных с субъект-сессией, при ее создании пользователем (или от имени пользователя другой субъект-сессией) из сущности. При этом если пользователь $u \in U$ или субъект-сессия от имени пользователя u не может создать из сущности $e \in E$ новую субъект-сессию, то по определению $fa(u, e) = \varnothing$. Кроме того, если для пользователя $u \in U$ и сущности $e \in E$ существует пользователь $x \in U$, такой, что выполняется условие $x \in fa(u, e)$, то по определению будем считать, что пользователь x может создать субъект-сессию, которая будет являться функционально ассоциированной сущностью с субъект-сессией, создаваемой пользователем u из сущности e. По определению выполняется условие: для каждой субъект-сессии $s \in S$ существует единственная сущность $e_s \in E$, такая, что справедливо равенство $fa(user(s), e_s) = [s]$;

$y(E) \subset L_S \times E$ — множество пар вида (доверенная субъект-сессия, сущность), относительно которых корректна доверенная субъект-сессия y;

$de\_facto\_roles : S \to 2^{R \cup AR}$ — функция фактических текущих ролей субъект-сессий, при этом по определению в каждом состоянии системы $G = (PA, user, roles, A, F, H_E)$ для каждой субъект-сессии $s_1 \in S$ выполняется равенство:

$de\_facto\_roles(s_1) = roles(s_1) \cup \{r \in R \cup AR : \exists s_2 \in S\ [(s_1, s_2, own_a) \in A\ \&\ \&\ r \in roles(s_2)]\}$;

$de\_facto\_rights : S \to 2^P$ — функция фактических текущих прав доступа субъект-сессий, при этом по определению в каждом состоянии системы $G = (PA, user, roles, A, F, H_E)$ для каждой субъект-сессии $s \in S$ выполняется равенство:

$de\_facto\_rights(s) = \{p \in P : \exists r \in de\_facto\_roles(s)\ [p \in PA(r)]\}$;

$de\_facto\_actions : S \to 2^P \times 2^R$ — функция фактических возможных действий субъект-сессий, при этом по определению в каждом состоянии системы $G = (PA, user, roles, A, F, H_E)$ для каждой субъект-сессии $s_1 \in S$ выполняется равенство:

$de\_facto\_actions(s_1) = (PA(roles(s_1)) \times can\_manage\_rights(roles(s_1) \cap AR)) \cup \cup\{(p, r) \in P \times R : \exists s_2 \in S\ \exists (s_1, s_2, own_a) \in A\ [r \in can\_manage\_rights(roles(s_2) \cap AR)\ \&\ \&\ p \in PA(roles(s_2))]\}$.

В БР ДП-модели определены следующие правила преобразования состояний:

— монотонные: $take\_role(x, r)$, $grant\_right(x, r, (y, \alpha_r))$, $create\_entity(x, r, y, z)$, $create\_first\_session(u, r, y, z)$, $create\_session(x, w, r, y, z)$, $rename\_entity(x, y, z)$, $control(x, y, z)$, $access\_own(x, y)$, $take\_access\_own(x, y, z)$, $access\_read(x, y)$, $access\_write(x, y)$, $access\_append(x, y)$, $flow(x, y, y', z)$, $find(x, y, z)$, $post(x, y, z)$, $pass(x, y, z)$, $take\_flow(x, y)$;

— и немонотонные: $remove\_role(x, r)$, $remove\_right(x, r, (y, \alpha_r))$, $delete\_entity(x, y, z)$.

По аналогии с базовой ДП-моделью может быть доказано, что в рамках БР ДП-модели при анализе условий передачи прав доступа, реализации информационных потоков по памяти или по времени можно обойтись применением только монотонных правил преобразования состояний.

2. Условия получения права доступа владения

2.1. Вспомогательные предложения

С целью описания в рамках БР ДП-модели условий получения недоверенной субъект-сессией доступа владения к доверенной субъект-сессии рассмотрим случай, когда взаимодействует произвольное число субъект-сессий, и они не получают доступа владения друг к другу с использованием информационных потоков по памяти к функционально ассоциированным с субъект-сессиями сущностям.

Используем следующие определение и предположение БР ДП-модели.

Определение 1. Назовем траекторию функционирования системы $\Sigma(G^*, OP)$ траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, если при ее реализации используются только монотонные правила преобразования состояний, и доверенные субъект-сессии:

— не берут роли в множество текущих ролей;

— не дают другим ролям права доступа к сущностям;

— не получают доступа владения к субъект-сессиям.

Предположение 1. Каждые пользователь или субъект-сессия системы $\Sigma(G^*, OP)$ вне зависимости от имеющихся у них авторизованных ролей являются либо доверенными, либо недоверенными. Доверенные пользователи или субъект-сессии не создают новых субъект-сессий. Каждые недоверенный пользователь или субъект-сессия могут создать только недоверенную субъект-сессию.

Дадим определения.

Определение 2. Траекторию без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, назовем простой, если при ее реализации для $0 \leqslant i \leqslant N$ каждое правило op_i не является правилом вида $control(x, y, z)$, использующим для получения доступа владения субъект-сессией x к субъект-сессии y информационный поток по памяти $(x, z, write_m)$, где $z \in [y]$.

Определение 3. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенный пользователь $x \in N_U$ и субъект-сессия или недоверенный пользователь $y \in N_U \cup S_0$, такие, что $x \neq y$. Определим предикат $simple\_can\_access\_own(x, y, G_0)$, который будет истинным тогда и только тогда, когда существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существуют субъект-сессии s_x, $s_y \in S_N$, такие, что $user_N(s_x) = x$, или $s_y = y$, или $user_N(s_y) = y$ и выполняется условие $(s_x, s_y, own_a) \in A_N$.

Для упрощения записи алгоритмически проверяемых необходимых и достаточных условий истинности предиката $simple\_can\_access\_own(x, y, G_0)$ используем следующие определения.

Определение 4. Пусть $G = (PA, user, roles, A, F, H_E)$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют субъект-сессии или недоверенные пользователи $x, y \in N_U \cup S$. Определим предикат $simple\_directly\_access\_own(x, y, G)$, который будет истинным тогда и только тогда, когда или $x = y$, или выполняется одно из следующих условий:

1. Если $y \in N_U$ и $x \in N_U$, то существуют сущность $e_y \in E$ и роль $r_y \in R$, такие, что $(e_y, execute_r) \in PA(UA(y))$, $r_y \in can\_manage\_rights(AUA(y))$ и выполняется одно из условий:

— $r_y \in UA(x)$;
— $x \in fa(y, e_y)$.

2. Если $y \in N_U$ и $x \in N_S \cap S$, то существуют сущность $e_y \in E$ и роль $r_y \in R$, такие, что $(e_y, execute_r) \in PA(UA(y))$, $r_y \in can\_manage\_rights(AUA(y))$ и выполняется одно из условий:

— $r_y \in UA(user(x))$;
— $x \in fa(y, e_y)$.

3. Если $y \in N_U$ и $x \in L_S \cap S$, то существуют сущность $e_y \in E$ и роль $r_y \in R$, такие, что $(e_y, execute_r) \in PA(UA(y))$, $r_y \in can\_manage\_rights(AUA(y))$ и выполняется одно из условий:

— $r_y \in roles(x)$;
— $x \in fa(y, e_y)$.

4. Если $y \in S$ и $x \in N_U$, то выполняется одно из условий:

— $(y, own_r) \in PA(UA(x))$;
— $x \in [y]$.

5. Если $y \in S$ и $x \in N_S \cap S$, то выполняется одно из условий:

— $(y, own_r) \in PA(UA(user(x)))$;
— $x \in [y]$;
— $(x, y, own_a) \in A$.

6. Если $y \in S$ и $x \in L_S \cap S$, то выполняется одно из условий:
— $(y, own_r) \in PA(roles(x))$;
— $x \in [y]$;
— $(x, y, own_a) \in A$.

Определение 5. Пусть $G = (PA, user, roles, A, F, H_E)$ — состояние системы $\Sigma(G^*, OP)$, в котором существует субъект-сессия или недоверенный пользователь $x \in N_U \cup S$. Назовем множество $X \subset N_U \cup S$ островом субъект-сессии или недоверенного пользователя x, если $X = \{x\} \cup \{y \in (N_U \cup S) \setminus \{x\}$: существует последовательность $s_1 s_2 \dots s_m$, где $s_1 = x$, $s_2, \dots, s_m \in (N_U \cup S) \setminus \{x\}$, $s_m = y$ и $m \geqslant 2$, такая, что для каждого i, $1 \leqslant i < m$, истинен предикат $simple\_directly\_access\_own(s_i, s_{i+1}, G)\}$ и $s_{i+1} \neq x$. Определим функцию $island : N_U \cup S \to 2^{N_u \cup S}$, задающую для каждых субъект-сессии или недоверенного пользователя соответствующий им остров.

В отличие от островов в классической модели *Take-Grant* острова в БР ДП-модели задаются для каждых субъект-сессии или недоверенного пользователя в отдельности и могут пересекаться.

Из определения 5 следует, что если существуют субъект-сессия или недоверенные пользователи x и y, такие, что $y \in island(x)$, то $island(y) \subseteq island(x)$.

Утверждение 1. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенный пользователь или недоверенная субъект-сессия $x \in N_U \cup (N_S \cap S_0)$ и субъект-сессия или недоверенный пользователь $y \in island(x) \setminus \{x\}$. Тогда справедливо одно из предложений:
— если $x \in N_U$, то истинен предикат $simple\_can\_access\_own(x, y, G_0)$;
— если $x \in N_S \cap S_0$, то истинен предикат $simple\_can\_access\_own(user_0(x), y, G_0)$.

Доказательство. Пусть выполнены условия утверждения. Тогда по определению 5 в $N_U \cup S$ существует последовательность $s_1 s_2 \dots s_m$, где $m \geqslant 2$, $s_1 = x$, $s_m = y$ и для каждого $i = 1, \dots, m-1$ истинен предикат $simple\_directly\_access\_own(s_i, s_{i+1}, G_0)$ и $s_{i+1} \neq x$. Докажем утверждение индукцией по длине m этой последовательности.

Пусть $m = 2$. Тогда справедливо неравенство $x \neq y$, истинен предикат $simple\_directly\_access\_own(x, y, G_0)$ и по определению 4 истинен предикат $directly\_access\_own(x, y, G_0)$ [6]. Следовательно (см. утверждение 2 и определение 13 в [6]), существуют состояния $G_1, \dots, G_N$ и правила преобразования состояний $op_1, \dots, op_N$, такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \dots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существуют субъект-сессии $s_x, s_y \in S_N$, такие, что $(s_x, s_y, own_a) \in A_N$ и выполняется одно из условий:
— $user_N(s_x) = x, user_N(s_y) = y$;
— $user_N(s_x) = x$, $s_y = y$;
— $s_x = x$, $user_N(s_y) = y$;
— $s_x = x$, $s_y = y$.

Тем самым в случае $m = 2$ утверждение доказано.

Предположим (предположение индукции), что таким образом утверждение доказано всегда, когда $2 \leqslant m \leqslant l$ для некоторого $l \geqslant 2$, и докажем его (шаг индукции), когда $m = l + 1$.

Итак, пусть $m = l + 1$ и $z = s_{m-1}$. Тогда $x \in N_U \cup (N_S \cap S_0)$ и $z \in (N_U \cup S_0) \setminus \{x\}$. Рассмотрим случай, когда выполняются условия $x \in N_S \cap S_0$, $z \in S_0$. Иные случаи

рассматриваются аналогично. Так как по определению 5 $z \in island(x) \setminus \{x\}$, то по предположению индукции существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа и $(x, z, own_a) \in A_N$. Если $z = y$, то шаг индукции обоснован. Пусть поэтому $z \neq y$. Возможны два случая.

П е р в ы й с л у ч а й: $z \in N_S \cap S_0$. Тогда по определению 5 $y \in island(z) \setminus \{z\}$, истинен предикат $simple\_directly\_access\_own(z, y, G_0)$ и по предположению индукции существуют состояния $G_{N+1}, \ldots, G_K$ и правила преобразования состояний $op_{N+1}, \ldots, op_K$, такие, что $G_N \vdash_{op_{N+1}} G_{N+1} \vdash_{op_{N+2}} \ldots \vdash_{op_K} G_K$, где $K \geqslant N$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа и $(z, y, own_a) \in A_K$. Положим $op_{K+1} = take\_access\_own(x, z, y)$. Тогда $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_{K+1}} G_{K+1}$ является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, выполняется условие $(x, y, own_a) \in A_{K+1}$, и по определению 3 шаг индукции обоснован.

В т о р о й с л у ч а й: $z \in L_S \cap S_0$. Тогда истинен предикат $simple\_directly\_access\_own(z, y, G_0)$ и выполняется условие 6 определения 4.

Если $(y, own_r) \in PA(roles_0(z))$, то $(y, own_r) \in de\_facto\_rights(x)$ и тогда пусть $op_{N+1} = access\_own(x, y)$. Если $z \in [y]$, то положим $op_{N+1} = control(x, y, z)$. Наконец, если $(z, y, own_a) \in A_0$, то пусть $op_{N+1} = take\_access\_own(x, z, y)$.

Таким образом, $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_{N+1}} G_{N+1}$ является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, выполняется условие $(x, y, own_a) \in A_{N+1}$, и по определению 3 шаг индукции обоснован.

Утверждение доказано. ■

Введём обозначения:

$island\_roles : N_U \cup (N_S \cap S) \to 2^R \cup 2^{AR}$ — функция, задающая для каждых недоверенного пользователя или недоверенной субъект-сессии $x \in N_U \cup (N_S \cap S)$ роли, которыми обладают все субъект-сессии или недоверенные пользователи, принадлежащие острову x. При этом по определению справедливо равенство $island\_roles(x) = \{r \in R \cup AR : \exists y \in island(x)\ [(y \in N_U \,\&\, r \in UA(y) \cup AUA(y)) \vee (y \in N_S \cap S \,\&\, r \in UA(user(y)) \cup AUA(user(y))) \vee (y \in L_S \cap S \,\&\, r \in roles(y))]\}$;

$island\_rights : N_U \cup (N_S \cap S) \to 2^P$ — функция, задающая для каждых недоверенного пользователя или недоверенной субъект-сессии $x \in N_U \cup (N_S \cap S)$ права доступа, которыми обладают все субъект-сессии или недоверенные пользователи, принадлежащие острову x. При этом по определению справедливо равенство $island\_rights(x) = \{p \in P : \exists r \in island\_roles(x)\ [p \in PA(r)]\}$;

$island\_actions : N_U \cup (N_S \cap S) \to 2^P \times 2^R$ — функция, задающая для каждых недоверенного пользователя или недоверенной субъект-сессии $x \in N_U \cup \cup (N_S \cap S)$ возможные действия, которыми обладают все субъект-сессии или недоверенные пользователи, принадлежащие острову x. При этом по определению справедливо равенство $island\_actions(x) = \{(p, r) \in P \times R : \exists y \in island(x)\ [(y \in N_U \,\&\, (p, r) \in PA(UA(y)) \times can\_manage\_rights(AUA(y))) \vee (y \in N_S \cap S \,\&\, (p, r) \in PA(UA(user(y))) \times can\_manage\_rights(AUA(user(y)))) \vee (y \in L_S \cap S \,\&\, (p, r) \in PA(roles(y)) \times can\_manage\_rights(roles(y) \cap AR))]\}$.

Следствие 1. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенный пользователь или недоверенная

субъект-сессия $x \in N_U \cup (N_S \cap S_0)$. Тогда существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует недоверенная субъект-сессия $s_x \in N_S \cap S_N$, такая, что либо $user_N(s_x) = x$, либо $s_x = x$ и выполняются условия:

— $island\_roles(x) = island\_roles(s_x) \subset de\_facto\_roles_N(s_x)$ (множество фактических ролей субъект-сессии s_x включает все роли субъект-сессий или пользователей, принадлежащих ее острову);

— $island\_rights(x) = island\_rights(s_x) \subset de\_facto\_rights_N(s_x)$ (множество фактических прав доступа субъект-сессии s_x включает все права доступа субъект-сессий или пользователей, принадлежащих ее острову);

— $island\_actions(x) = island\_actions(s_x) \subset de\_facto\_actions_N(s_x)$ (множество фактических возможных действий субъект-сессии s_x включает все возможные действия субъект-сессий или пользователей, принадлежащих ее острову).

Доказательство. Если $x \in N_U$, то по предположению 1 недоверенный пользователь x может создать недоверенную субъект-сессию s_x, такую, что $user(s_x) = x$. При этом из определений функций *island_ roles*, *island_ rights*, *island_ actions* следует, что справедливы равенства $island\_roles(x) = island\_roles(s_x)$, $island\_rights(x) = = island\_rights(s_x)$, $island\_actions(x) = island\_actions(s_x)$. Если $x \in N_S \cap S_0$, то положим $s_x = x$.

Из утверждения 1 следует, что существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа. При этом выполняются условия:

— если $y \in (island(x) \backslash \{x\}) \cap N_U$, то существует субъект-сессия $s_y \in S_N$, такая, что $user_N(s_y) = y$ и $(s_x, s_y, own_a) \in A_N$;

— если $y \in (island(x) \backslash \{x\}) \cap S_0$, то $(s_x, s_y, own_a) \in A_N$.

Таким образом, в состоянии G_N выполняются условия:

— $island\_roles(x) = island\_roles(s_x) \subset de\_facto\_roles_N(s_x)$;

— $island\_rights(x) = island\_rights(s_x) \subset de\_facto\_rights_N(s_x)$;

— $island\_actions(x) = island\_actions(s_x) \subset de\_facto\_actions_N(s_x)$.

Утверждение следствия доказано. ■

2.2. Основная теорема

Дадим необходимые определения.

Определение 6. Пусть $G = (PA, user, roles, A, F, H_E)$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенная субъект-сессия или недоверенный пользователь $x \in N_U \cup (N_S \cap S)$ и субъект-сессии или недоверенные пользователи $y, z \in N_U \cup S$. Будем говорить, что субъект-сессия или недоверенный пользователь y соединяется простым мостом с субъект-сессией или недоверенным пользователем z через недоверенную субъект-сессию или недоверенного пользователя x, если $z \in island(x)$ и существует роль $r_y \in R$, такая, что выполняются следующие два условия.

1. Или $y \in N_U$ и $r_y \in UA(y)$, или $y \in N_S \cap S$ и $r_y \in UA(user(y))$, или $y \in L_S \cap S$ и $r_y \in roles(y)$.

2. Или $z \in N_U$ и $r_y \in can\_manage\_rights(AUA(z))$, или $z \in N_S \cap S$ и $r_y \in can\_manage\_rights(AUA(user(z)))$, или $z \in L_S \cap S$ и $r_y \in can\_manage\_rights(roles(z) \cap AR)$.

Определение 7. Пусть $G = (PA, user, roles, A, F, H_E)$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенная субъект-сессия или недоверенный пользователь $x \in N_U \cup (N_S \cap S)$ и субъект-сессии или недоверенные пользователи $y, z \in N_U \cup S$. Будем говорить, что субъект-сессия или недоверенный пользователь y соединяется мостом с субъект-сессией или недоверенным пользователем z через недоверенную субъект-сессию или недоверенного пользователя x, когда существуют субъект-сессии или недоверенные пользователи $v, w \in N_U \cup S$ и роли $r_v, r_y \in R$, такие, что $v, w, z \in island(x)$, $w, z \in island(v)$, $z \in island(w)$ и выполняются следующие условия.

1. Или $y \in N_U$ и $r_y \in UA(y)$, или $y \in N_S \cap S$ и $r_y \in UA(user(y))$, или $y \in L_S \cap S$ и $r_y \in roles(y)$.

2. Или $v \in N_U$ и $r_v \in UA(v)$, $r_y \in can\_manage\_rights(AUA(v))$, или $v \in N_S \cap S$ и $r_v \in UA(user(v))$, $r_y \in can\_manage\_rights(AUA(user(v)))$, или $v \in L_S \cap S$ и $r_v \in roles(v)$, $r_y \in can\_manage\_rights(roles(v) \cap AR)$.

3. Или $w \in N_U$ и $r_v \in can\_manage\_rights(AUA(w))$, или $w \in S$ и $(w, own_r) \in \in PA(r_v)$.

Введём обозначения:

$is\_simple\_bridge : (N_U \cup (N_S \cap S)) \times (N_U \cup S) \times (N_U \cup S) \to \{true, false\}$ — функция, для которой по определению справедливо равенство $is\_simple\_bridge(x, y, z) = true$ тогда и только тогда, когда y соединен простым мостом с z через x, где $x \in N_U \cup \cup (N_S \cap S)$, $y, z \in N_U \cup S$;

$is\_bridge : (N_U \cup (N_S \cap S)) \times (N_U \cup S) \times (N_U \cup S) \to \{true, false\}$ — функция, для которой по определению справедливо равенство $is\_bridge(x, y, z) = true$ тогда и только тогда, когда y соединен мостом с z через x, где $x \in N_U \cup (N_S \cap S)$, $y, z \in N_U \cup S$.

В отличие от мостов в классической модели *Take-Grant* мосты в БР ДП-модели являются ориентированными. То есть в БР ДП-модели, если субъект-сессия или недоверенный пользователь y соединяется мостом или простым мостом с субъект-сессией или недоверенным пользователем z, то не обязательно z соединяется мостом с y.

Пусть $G = (PA, user, roles, A, F, H_E)$ — состояние системы $\Sigma(G^*, OP)$. В дополнение к обозначениям, введенным при определении графа доступов в базовой ДП-модели, используем следующие обозначения (см. рис. 1):

- вершины из множества $U \cup S$ (соответствующие пользователям и субъект-сессиям) в графе доступов будут обозначаться «•»;
- вершины из множества $R \cup AR$ (соответствующие ролям и административным ролям) в графе доступов будут обозначаться «∗»;
- если для роли $r \in R \cup AR$ и права доступа $(e, \alpha) \in P$ выполняется условие $(e, \alpha) \in \in PA(r)$, то в графе доступов r соединена с e ребром вида рис. 1, *а*, помеченным α;
- если для недоверенного пользователя $x \in N_U$ и роли $r \in R \cup AR$ выполняется условие $r \in UA(x)$ или $r \in AUA(x)$, то в графе доступов x соединен с r ребром вида рис. 1, *б*, помеченным UA или AUA соответственно;
- если для недоверенной субъект-сессии $x \in N_S \cap S$ и роли $r \in R \cup AR$ выполняется условие $r \in UA(user(x))$ или $r \in AUA(user(x))$, то в графе доступов x соединен с r ребром вида рис. 1, *в*, помеченным UA или AUA соответственно;
- если для доверенной субъект-сессии $x \in L_S \cap S$ и роли $r \in R \cup AR$ выполняется условие $r \in roles(x)$, то в графе доступов x соединен с r ребром вида рис. 1, *г*, помеченным *roles*;

— если для административной роли $ar \in AR$ и роли $r \in R$ выполняется условие $r \in can\_manage\_rights(ar)$, то в графе доступов ar соединена с r ребром вида рис. 1, *д*, помеченным cmr;
— если для субъект-сессий или недоверенных пользователей $x, y \in N_U \cup S$ выполняется условие $y \in island(x)$, то в графе доступов x соединен с y ребром вида рис. 1, *е*, помеченным *island*.

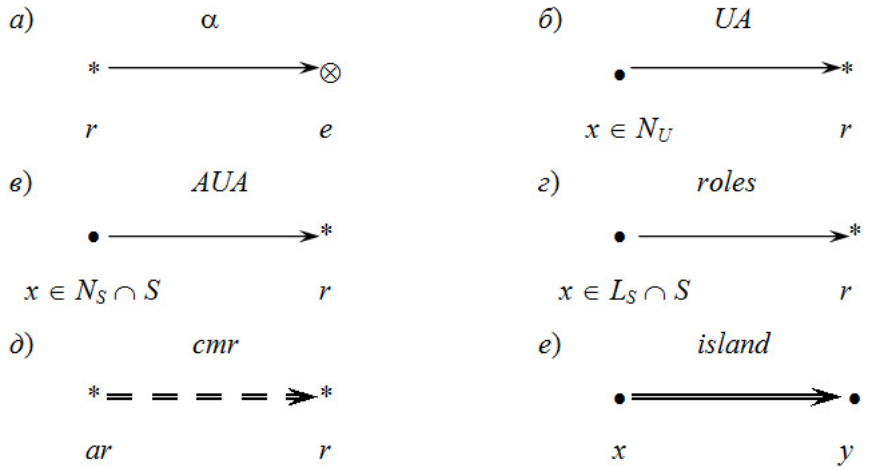

Рис. 1. Обозначения ребер в графе доступов

Пример 1. Пусть $G = (PA, user, roles, A, F, H_E)$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенная субъект-сессия или недоверенный пользователь $x \in N_U \cup (N_S \cap S)$ и субъект-сессии или недоверенные пользователи $y, z \in N_U \cup S$. С использованием введенных обозначений приведены примеры простого моста (рис. 2, *а*) и моста (рис. 2, *б*), соединяющих y с z через x.

При этом в состоянии, представленном на рис. 2, *а*, выполняется условие $is\_simple\_bridge(x, y, z) = true$, а в состоянии, представленном на рис. 2, *б*, — условие $is\_bridge(x, y, z) = true$.

Сформулируем и обоснуем алгоритмически проверяемые необходимые и достаточные условия истинности предиката $simple\_can\_access\_own(x, y, G_0)$.

Теорема 1. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют недоверенный пользователь $x \in N_U$ и субъект-сессия или недоверенный пользователь $y \in N_U \cup S_0$, такие, что $x \neq y$. Предикат $simple\_can\_access\_own(x, y, G_0)$ является истинным тогда и только тогда, когда существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_m \in N_U \cup (N_S \cap S_0)$ и субъект-сессий или недоверенных пользователей $y_1, \ldots, y_m \in N_U \cup S_0$, где $m \geqslant 1$, таких, что $x_1 = x$, $y_m = y$, $y_i \in island(x_i)$ для $1 \leqslant i \leqslant m$ и выполняются следующие условия.

1. Если $m \geqslant 2$, то справедливо равенство $is\_bridge(x_m, y_{m-1}, y) = true$.

2. Если $m \geqslant 3$, то для каждого i, $2 \leqslant i < m$, или $is\_bridge(x_i, y_{i-1}, y_i) = true$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = true$.

Доказательство. Докажем достаточность выполнения условий теоремы для истинности предиката $simple\_can\_access\_own(x, y, G_0)$. Применим индукцию по длине m последовательностей субъект-сессий или недоверенных пользователей.

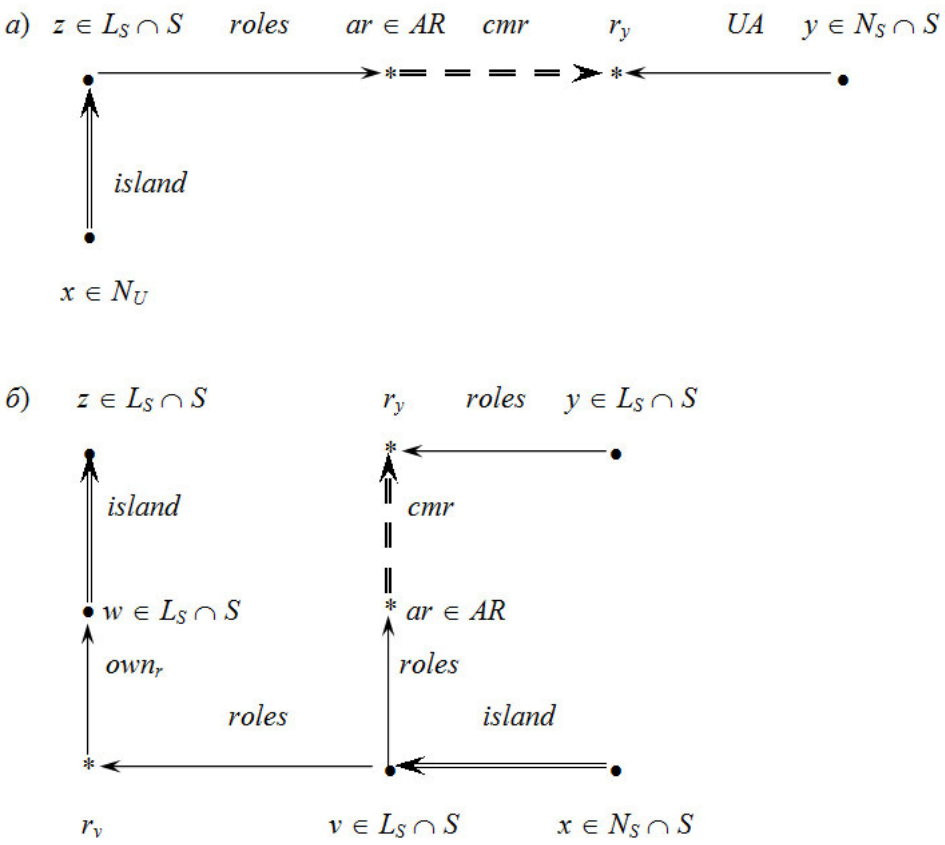

Рис. 2. Примеры мостов: простой мост ($а$); мост ($б$)

Пусть $m = 1$, тогда по условию $y \in island(x)$. Следовательно, по утверждению 1 предикат $simple\_can\_access\_own(x, y, G_0)$ является истинным.

Пусть $m = 2$, тогда по условию $is\_bridge(x_2, y_1, y) = true$, $y_1 \in island(x)$, $y \in island(x_2)$. Значит, по определению 7 существуют субъект-сессии или недоверенные пользователи $v, w \in N_U \cup S_0$ и роли $r_v, r_{y_1} \in R$, такие, что $v, w \in island(x_2)$, $w, y \in island(v)$, $y \in island(w)$ и выполняются следующие условия:

— или $y_1 \in N_U$ и $r_{y_1} \in UA_0(y_1)$, или $y_1 \in N_S \cap S_0$ и $r_{y_1} \in UA_0(user_0(y_1))$, или $y_1 \in L_S \cap S_0$ и $r_{y_1} \in roles_0(y_1)$;
— или $v \in N_U$ и $r_v \in UA_0(v)$, $r_{y_1} \in can\_manage\_rights(AUA_0(v))$, или $v \in N_S \cap S_0$ и $r_v \in UA_0(user_0(v))$, $r_{y_1} \in can\_manage\_rights(AUA_0(user_0(v)))$, или $v \in L_S \cap S_0$ и $r_v \in roles_0(v)$, $r_{y_1} \in can\_manage\_rights(roles_0(v) \cap AR)$;
— или $w \in N_U$ и $r_v \in can\_manage\_rights(AUA_0(w))$, или $w \in S_0$ и $(w, own_r) \in PA_0(r_v)$.

Пример выполнения условий теоремы для случая $m = 2$ приведен на рис. 3.

Если $w \in N_U$ и $r_v \in can\_manage\_rights(AUA_0(w))$, то по предположению 1 существует сущность $e_w \in E_0$, такая, что $(e_w, execute_r) \in PA_0(UA_0(w))$. Положим в этом случае $op_1 = create\_first\_session(w, r_v, e_w, s_w)$ и $M = 1$. Если же $w \in S_0$, то положим $s_w = w$ и $M = 0$.

Таким образом, выполняются условия $(s_w, own_r) \in PA_M(r_v)$, $s_w \in island(x_2)$, $s_w \in island(v)$, $y \in island(s_w)$ и $((s_w, own_r), r_{y_1}) \in island\_actions(x_2)$.

По утверждению следствия 1 существуют состояния $G_{M+1}, \ldots, G_L$ и правила преобразования состояний $op_{M+1}, \ldots, op_L$, такие, что $G_M \vdash_{op_{M+1}} G_{M+1} \vdash_{op_{M+2}} \ldots \vdash_{op_L} G_L$, где $L - M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных

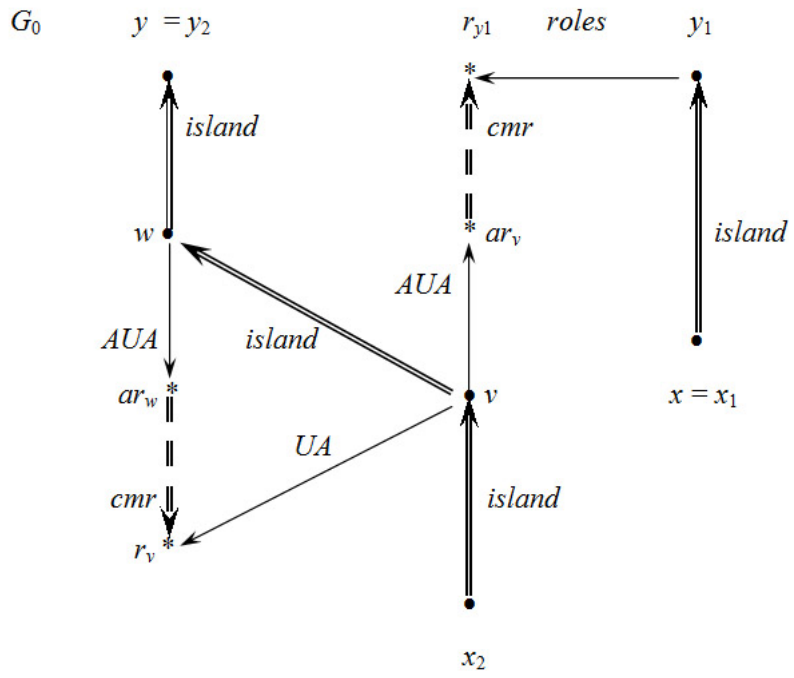

Рис. 3. Пример выполнения условий теоремы для случая $m = 2$

субъект-сессий для передачи прав доступа, и существует недоверенная субъект-сессия $s_{x_2} \in N_S \cap S_L$, такая, что либо $user_L(s_{x_2}) = x_2$, либо $s_{x_2} = x_2$, и в состоянии G_L выполняется условие $island\_actions(x_2) = island\_actions(s_{x_2}) \subset de\_facto\_actions_L(s_{x_2})$. Следовательно, выполняется условие $((s_w, own_r), r_{y_1}) \in de\_facto\_actions_L(s_{x_2})$. Положим $op_{L+1} = grant\_right(s_{x_2}, r_{y_1}, (s_w, own_r))$.

Значит, в состоянии G_{L+1}, таком, что $G_L \vdash_{op_{L+1}} G_{L+1}$, выполняются условия $(s_w, own_r) \in PA(r_{y_1})$ и $y \in island(x)$. Таким образом, по утверждению 1 истинен предикат $simple\_can\_access\_own(x, y, G_{L+1})$. Так как траектория $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_{L+1}} G_{L+1}$ является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, то по определению 3 является истинным предикат $simple\_can\_access\_own(x, y, G_0)$.

Пусть $m > 2$ и утверждение верно для всех последовательностей длины $l < m$. Докажем достаточность условий теоремы при длине последовательности, равной m.

По условию теоремы существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_m \in N_U \cup (N_S \cap S_0)$ и субъект-сессий или недоверенных пользователей $y_1, \ldots, y_m \in N_U \cup S_0$, таких, что $x_1 = x$, $y_m = y$, $y_i \in island(x_i)$, где $1 \leqslant i \leqslant m$, и

— справедливо равенство $is\_bridge(x_m, y_{m-1}, y) = true$;
— для каждого i, $2 \leqslant i < m$, или $is\_bridge(x_i, y_{i-1}, y_i) = true$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = true$.

По предположению индукции истинен предикат $simple\_can\_access\_own(x_2, y, G_0)$. Используя технику доказательства, примененную для случая $m = 2$, получаем, что существуют состояния $G_1, \ldots, G_M$ и правила преобразования состояний $op_1, \ldots, op_M$, такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_M} G_M$, где $M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует роль $r_{y_2} \in R$, такая, что выполняются следующие условия:

— или $y_2 \in N_U$ и $r_{y_2} \in UA_0(y_2)$, или $y_2 \in N_S \cap S_0$ и $r_{y_2} \in UA_0(user_0(y_2))$, или $y_2 \in L_S \cap S_0$ и $r_{y_2} \in roles_0(y_2)$;
— $(y, own_r) \in PA_M(r_{y_2})$.

Если выполняется условие $is\_bridge(x_2, y_1, y_2) = true$, то по аналогии с рассмотренным случаем для $m = 2$ получаем, что является истинным предикат $simple\_can\_access\_own(x, y, G_0)$.

Пусть выполняется условие $is\_simple\_bridge(x_2, y_1, y_2) = true$ (рис. 4).

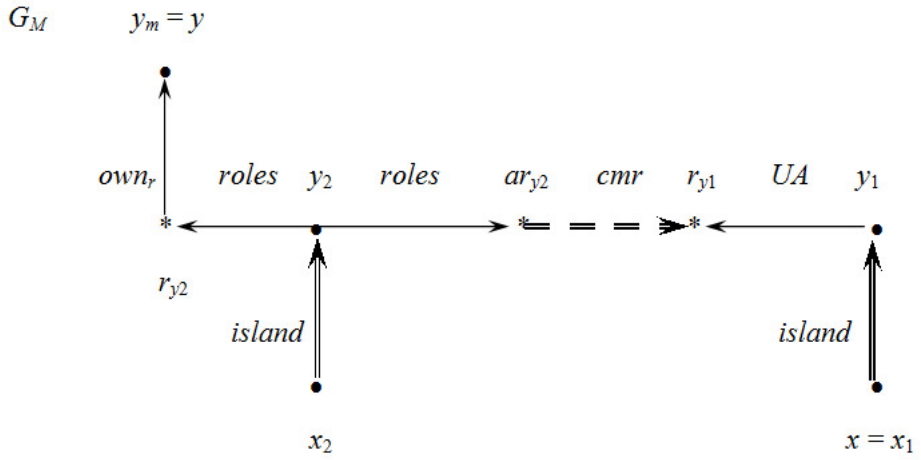

Рис. 4. Пример выполнения условия $is\_simple\_bridge(x_2, y_1, y_2) = true$

Так как $(y, own_r) \in PA_M(r_{y_2})$, $y_2 \in island(x_2)$ и $((y, own_r), r_{y_1}) \in island\_actions(x_2)$, то по утверждению следствия 1 существуют состояния $G_{M+1}, \ldots, G_L$ и правила преобразования состояний $op_{M+1}, \ldots, op_L$, такие, что $G_M \vdash_{op_{M+1}} G_{M+1} \vdash_{op_{M+2}} \ldots \vdash_{op_L} G_L$, где $L - M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует недоверенная субъект-сессия $s_{x_2} \in N_S \cap S_L$, такая, что либо $user_L(s_{x_2}) = x_2$, либо $s_{x_2} = x_2$ и в состоянии G_L выполняется условие $island\_actions(x_2) = island\_actions(s_{x_2}) \subset \subset de\_facto\_actions_L(s_{x_2})$. Следовательно, $((y, own_r), r_{y_1}) \in de\_facto\_actions_L(s_{x_2})$. Положим $op_{L+1} = grant\_right(s_{x_2}, r_{y_1}, (y, own_r))$.

Значит, в состоянии G_{L+1}, таком, что $G_L \vdash_{op_{L+1}} G_{L+1}$, выполняются условия $(y, own_r) \in PA(r_{y_1})$ и $y \in island(x)$. Таким образом, по утверждению 1 истинен предикат $simple\_can\_access\_own(x, y, G_{L+1})$. Так как траектория $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_{L+1}} G_{L+1}$ является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, то по определению 3 является истинным предикат $simple\_can\_access\_own(x, y, G_0)$. Индуктивный шаг доказан.

Обоснована достаточность выполнения условий теоремы для истинности предиката $simple\_can\_access\_own(x, y, G_0)$.

Докажем необходимость выполнения условий теоремы для истинности предиката $simple\_can\_access\_own(x, y, G_0)$. По определению 3 существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существуют субъект-сессии $s_x, s_y \in S_N$, такие, что $user_N(s_x) = x$, или $s_y = y$, или $user_N(s_y) = y$ и выполняется условие $(s_x, s_y, own_a) \in A_N$.

Среди всех траекторий выберем ту, у которой длина N является минимальной. Проведем доказательство индукцией по длине траекторий N.

Пусть $N = 0$, тогда $(s_x, s_y, own_a) \in A_0$. По определению 4 истинен предикат $simple\_directly\_access\_own(x, y, G_0)$ и $y \in island(x)$. Положим $m = 1$. Следовательно, выполнены условия теоремы.

Пусть $N = 1$, тогда из минимальности N следует, что $(s_x, s_y, own_a) \notin A_0$. Возможны три случая.

П е р в ы й с л у ч а й: $op_1 = control(s_x, s_y, s_z)$, где $s_z \in E_0$ и $s_z \in [s_y]$. При этом либо $s_x = s_z$, либо $s_z \in S_0$ и $(s_x, s_z, own_a) \in A_0$.

В т о р о й с л у ч а й: $op_1 = take\_access\_own(s_x, s_z, s_y)$ и $\{(s_x, s_z, own_a), (s_z, s_y, own_a)\} \subset A_0$.

Т р е т и й с л у ч а й: $op_1 = access\_own(s_x, s_y)$ и $(s_y, own_r) \in de\_facto\_rights_0(s_x)$. Значит, существует $s_z \in S_0$, такая, что $(s_x, s_z, own_a) \in A_0$ и $(s_y, own_r) \in PA_0(roles_0(s_z))$.

Таким образом, в каждом из трех случаев по определению 5 выполняется условие $y \in island(x)$. Положим $m = 1$. Следовательно, выполнены условия теоремы.

Пусть $N > 1$ и утверждение теоремы верно для всех траекторий длины $l < N$. Докажем, что при длине траектории N, если истинен предикат $simple\_can\_access\_own(x, y, G_0)$, то выполняются условия теоремы.

Из минимальности N следует, что $(s_x, s_y, own_a) \notin A_{N-1}$. Возможны три случая.

П е р в ы й с л у ч а й: $op_N = control(s_x, s_y, s_z)$, где $s_z \in E_{N-1}$ и $s_z \in [s_y]$. При этом либо $s_x = s_z$, либо $s_z \in S_{N-1}$ и $(s_x, s_z, own_a) \in A_{N-1}$. Если $s_x = s_z$, то по определению 5 выполняется условие $y \in island(x)$. Положим $m = 1$. Следовательно, выполнены условия теоремы. Пусть $s_x \neq s_z$, тогда положим $z = user_{N-1}(s_z)$. Возможны две ситуации.

Первая ситуация: $s_z \notin S_0$. Тогда по предположению 1 $z \in N_U$, по определению 5 истинен предикат $simple\_directly\_access\_own(z, y, G_0)$ и истинен предикат $simple\_can\_access\_own(x, z, G_0)$ с длиной траектории меньше N. Следовательно, по предположению индукции существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_m \in N_U \cup (N_S \cap S_0)$ и субъект-сессий или недоверенных пользователей $y_1, \ldots, y_m \in N_U \cup S_0$, где $m \geqslant 1$, таких, что $x_1 = x$, $y_m = z$, $y_i \in island(x_i)$, где $1 \leqslant i \leqslant m$, и

— если $m \geqslant 2$, то справедливо равенство $is\_bridge(x_m, y_{m-1}, z) = true$;
— если $m \geqslant 3$, то для каждого i, $2 \leqslant i < m$, или $is\_bridge(x_i, y_{i-1}, y_i) = true$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = true$.

Если $m = 1$, то по определению 5 выполняется условие $y \in island(x)$. Если $m \geqslant 2$, то по определениям 5 и 7 справедливо равенство $is\_bridge(x_m, y_{m-1}, y) = true$. Следовательно, условия теоремы выполнены.

Вторая ситуация: $s_z \in S_0$. По определению 5 истинен предикат $simple\_directly\_access\_own(s_z, y, G_0)$ и истинен предикат $simple\_can\_access\_own(x, s_z, G_0)$ с длиной траектории меньше N. Далее аналогично обоснованию в первой ситуации получаем, что условия теоремы выполнены.

В т о р о й с л у ч а й: $op_N = take\_access\_own(s_x, s_z, s_y)$ и $\{(s_x, s_z, own_a), (s_z, s_y, own_a)\} \subset A_{N-1}$. Положим $z = user_{N-1}(s_z)$. Возможны две ситуации.

Первая ситуация: $s_z \notin S_0$ или $s_z \in N_S \cap S_0$. Тогда по предположению 1 выполняется условие $z \in N_U$ и истинны предикаты $simple\_can\_access\_own(x, z, G_0)$ и $simple\_can\_access\_own(z, y, G_0)$ с длиной траекторий меньше N. Следовательно, по предположению индукции существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x'_1, \ldots, x'_n, x''_1, \ldots, x''_k \in N_U \cup (N_S \cap S_0)$ и субъект-

сессий или недоверенных пользователей $y'_1, \ldots, y'_n, y''_1, \ldots, y''_k \in N_U \cup S_0$, где $1 \leqslant n$, $1 \leqslant k$, таких, что $x'_1 = x$, $x''_1 = y'_n = z$, $y''_k = y$, $y'_i \in island(x'_i)$, где $1 \leqslant i \leqslant n$, $y''_i \in island(x''_i)$, где $1 \leqslant i \leqslant k$, и

— если $n \geqslant 2$, то справедливо равенство $is\_bridge(x'_n, y'_{n-1}, z) = true$;
— если $k \geqslant 2$, то справедливо равенство $is\_bridge(x''_k, y''_{k-1}, y) = true$;
— если $n \geqslant 3$, то для каждого i, $2 \leqslant i < n$, или $is\_bridge(x'_i, y'_{i-1}, y'_i) = true$, или $is\_simple\_bridge(x'_i, y'_{i-1}, y'_i) = true$;
— если $k \geqslant 3$, то для каждого i, $2 \leqslant i < k$, или $is\_bridge(x''_i, y''_{i-1}, y''_i) = true$, или $is\_simple\_bridge(x''_i, y''_{i-1}, y''_i) = true$.

Положим: $m = n + k - 1$; $x_i = x'_i$, где $1 \leqslant i \leqslant n$; $x_{n+i-1} = x''_i$, где $2 \leqslant i \leqslant k$; $y_i = y'_i$, где $1 \leqslant i < n$; $y_{n+i-1} = y''_i$, где $1 \leqslant i \leqslant k$. Тогда условия теоремы выполнены.

Вторая ситуация: $s_z \in L_S \cap S_0$. Тогда по определению 3 выполняется условие $(s_z, s_y, own_a) \in A_0$ и истинен предикат $simple\_can\_access\_own(x, s_z, G_0)$ с длиной траектории меньше N. Следовательно, по определению 5 истинен предикат $simple\_directly\_access\_own(s_z, y, G_0)$, и аналогично первому случаю получаем, что условия теоремы выполнены.

Третий случай: $op_N = access\_own(s_x, s_y)$ и выполняется условие $(s_y, own_r) \in$ $\in de\_facto\_rights_{N-1}(s_x)$. Значит, существует $s_z \in S_{N-1}$, такая, что либо $s_x = s_z$ и $(s_y, own_r) \in PA_{N-1}(roles_{N-1}(s_x))$, либо $s_x \neq s_z$, $(s_x, s_z, own_a) \in A_{N-1}$ и $(s_y, own_r) \in$ $\in PA_{N-1}(roles_{N-1}(s_z))$.

Если $s_x = s_z$ и $(s_y, own_r) \in PA_{N-1}(roles_{N-1}(s_x))$, то по определению 5 выполняется условие $y \in island(x)$. Положим $m = 1$. Следовательно, выполнены условия теоремы.

Пусть $s_x \neq s_z$. Тогда $(s_x, s_z, own_a) \in A_{N-1}$ и истинен предикат $simple\_can\_access\_$-$own(x, s_z, G_0)$ с длиной траектории меньше N. Следовательно, по предположению индукции существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_n \in N_U \cup (N_S \cap S_0)$ и субъект-сессий или недоверенных пользователей $y_1, \ldots, y_n \in N_U \cup S_0$, где $n \geqslant 1$, таких, что $x_1 = x$, $y_n = s_z$, $y_i \in island(x_i)$, где $1 \leqslant i \leqslant n$, и

— если $n \geqslant 2$, то справедливо равенство $is\_bridge(x_n, y_{n-1}, s_z) = true$;
— если $n \geqslant 3$, то для каждого $2 \leqslant i < n$ справедливо равенство или $is\_bridge(x_i, y_{i-1}, y_i) = true$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = true$.

Если либо $s_z \in L_S \cap S_0$ и $(s_y, own_r) \in PA_0(roles_0(s_z))$, либо $z \in N_U$ и $(s_y, own_r) \in$ $\in PA_0(UA_0(z))$, то по определению 7 $is\_bridge(x_n, y_{n-1}, y) = true$. Положим $m = n$. Следовательно, выполнены условия теоремы.

Пусть либо $s_z \in L_S \cap S_0$ и $(s_y, own_r) \notin PA_0(roles_0(s_z))$, либо $z \in N_U$ и $(s_y, own_r) \notin$ $PA_0(UA_0(z))$. Тогда если $s_z \in L_S \cap S_0$, то по определениям 1 и 2 имеет место $r_y \in roles_0(s_z)$. Если $z \in N_U$, то $r_y \in UA_0(z)$. Тогда существует такое M, что $1 \leqslant M < N$ и выполняется одно из следующих трех условий.

Первое условие: $y \in N_U$ и $op_M = create\_first\_session(y, r_y, e_y, s_y)$, где $e_y \in E_{M-1}$ и $r_y \in can\_manage\_rights(AUA_0(y))$. Таким образом, по определению 7 $is\_bridge(x_n, y_{n-1}, y) = true$. Положим $m = n$. Следовательно, выполнены условия теоремы.

Второе условие: $op_M = create\_session(s'_x, s'_y, r_y, e_y, s_y)$, где по предположению 1, определениям 1 и 2 существуют недоверенные субъект-сессии $s'_x, s'_y \in N_S \cap S_{M-1}$, такие, что $y = user_M(s_y) = user_M(s'_y)$, $r_y \in can\_manage\_rights(roles_{M-1}(s'_y) \cap AR)$, $e_y \in E_{M-1}$ и либо $s'_x = s'_y$, либо $(s'_x, s'_y, own_a) \in A_{M-1}$. Следовательно,

$r_y \in can\_manage\_rights(AUA_0(y))$. Таким образом, по определению 7 $is\_bridge(x_n, y_{n-1}, y) = true$. Положим $m = n$. Следовательно, выполнены условия теоремы.

Третье условие: $op_M = grant\_right(s'_x, r_y, (s_y, own_r))$, где по определениям 1 и 2 существует недоверенная субъект-сессия $s'_x \in N_S \cap S_{M-1}$, такая, что $((s_y, own_r), r_y) \in \in de\_facto\_actions_{M-1}(s'_x)$. Следовательно, возможны две ситуации.

Первая ситуация: выполняются условия $(s_y, own_r) \in PA_0(UA_0(user_{M-1}(s'_x)))$ и $r_y \in can\_manage\_rights(AUA_0(user_{M-1}(s'_x)))$, тогда положим $m = n + 1$, $x_m = user_{M-1}(s'_x)$, $y_m = y$. При этом по определению 7 $is\_bridge(x_m, s_z, y) = true$. Следовательно, выполнены условия теоремы.

Вторая ситуация: существует субъект-сессия $s'_y \in S_{M-1}$, такая, что $(s_y, own_r) \in \in PA_{M-1}(roles_{M-1}(s'_y))$, $r_y \in can\_manage\_rights(roles_{M-1}(s'_y) \cap AR)$ и $(s'_x, s'_y, own_a) \in \in A_{M-1}$. Положим $x' = user_{M-1}(s'_x)$. Если $s'_y \in L_S \cap S_0$, то положим $y' = = s'_y$, при этом выполняется условие $r_y \in can\_manage\_rights(roles_0(y') \cap AR)$. Если $s'_y \in N_S \cap S_{M-1}$, то положим $y' = user_{M-1}(s'_y)$, при этом выполняется условие $r_y \in can\_manage\_rights(AUA_0(y'))$. Следовательно, истинен предикат $simple\_can\_access\_own(x', y', G_0)$ с длиной траектории меньше $M - 1$. По предположению индукции существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_{n+1}, \ldots, x_{n+k} \in N_U \cup (N_S \cap S_0)$ и субъект-сессий или недоверенных пользователей $y_{n+1}, \ldots, y_{n+k} \in N_U \cup S_0$, где $k \geqslant 1$, таких, что $x_{n+1} = x'$, $y_{n+k} = y'$, $y_i \in island(x_i)$, где $n + 1 \leqslant i \leqslant n + k$, и

— если $k \geqslant 2$, то справедливо равенство $is\_bridge(x_{n+k}, y_{n+k-1}, y') = true$;
— если $k \geqslant 3$, то для каждого i, $n + 2 \leqslant i < n + k$, или $is\_bridge(x_i, y_{i-1}, y_i) = true$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = true$;
— выполняется условие $is\_simple\_bridge(x_{n+1}, y_n, y_{n+1}) = true$, где $y_n = s_z$.

Если либо $y' \in L_S \cap S_0$ и $(s_y, own_r) \in PA_0(roles_0(y'))$, либо $y' \in N_U$ и $(s_y, own_r) \in \in PA_0(UA_0(y'))$, то $is\_bridge(x_{n+k}, y_{n+k-1}, y) = true$. Положим $m = n + k$. Следовательно, выполнены условия теоремы.

Пусть ни $y' \in L_S \cap S_0$ и $(s_y, own_r) \in PA_0(roles_0(y'))$, ни $y' \in N_U$ и $(s_y, own_r) \in \in PA_0(UA_0(y'))$. Тогда так как $(s_y, own_r) \in PA_{M-1}(roles_{M-1}(y'))$, то, повторяя (если потребуется) многократно рассуждения, приведённые для третьего случая, получаем, что условия теоремы выполнены.

Следовательно, доказан шаг индукции при длине траектории, равной N. Доказательство необходимости условий теоремы для истинности предиката $simple\_can\_access\_own(x, y, G_0)$ закончено.

Теорема доказана. ■

Таким образом, в рамках БР ДП-модели обосновываются необходимые и достаточные условия получения субъект-сессией, функционирующей от имени недоверенного пользователя, доступа владения к другой субъект-сессии для случая, когда в системе взаимодействует произвольное число субъект-сессий, и они не используют информационные потоки по памяти.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр «Академия», 2005. 144 с.
2. *Bishop M.* Computer Security: art and science. ISBN 0-201-44099-7, 2002. 1084 p.
3. *Sandhu R.* Role-Based Access Control // Advanced in Computers. Academic Press, 1998. V. 46.

4. *Девянин П. Н.* Анализ безопасности управления доступом и информационными потоками в компьютерных системах. М.: Радио и связь, 2006. 176 с.

5. *Девянин П. Н.* О разработке моделей безопасности информационных потоков в компьютерных системах с ролевым управлением доступом // Материалы Третьей Междунар. научн. конф. по проблемам безопасности и противодействия терроризму. МГУ им. Ломоносова. 25–27 октября 2007 г. М.: МЦНМО, 2008. С. 261–265.

6. *Девянин П. Н.* Базовая ролевая ДП-модель // Прикладная дискретная математика. 2008. № 1(1). С. 64-70.