МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

DOI 10.17223/20710410/7/2

УДК 004.94

АНАЛИЗ В РАМКАХ БАЗОВОЙ РОЛЕВОЙ ДП-МОДЕЛИ БЕЗОПАСНОСТИ СИСТЕМ С ПРОСТЫМИ ТРАЕКТОРИЯМИ ФУНКЦИОНИРОВАНИЯ[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 передачи прав доступа и реализации информационных потоков по памяти. При этом рассматриваются только простые траектории функционирования системы, 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 базовой ролевой ДП-модели (БР ДП-модели) [1, 2] рассмотрим условия передачи прав доступа и реализации информационных потоков по памяти для случая, когда на траекториях функционирования системы субъект-сессии 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;

$S \subseteq E$ — 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;

[1]Работа выполнена при поддержке гранта МД–2.2010.10.

$UA : U \to 2^R$ — 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 могут 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: $take\_role(x,r)$, $grant\_right(x,r,(y,\alpha_r))$, $create\_entity(x,r,y,z)$, $create\_first\_session(u,r,y,z)$, $create\_session(x,w,r,y,z)$, $rename\_entity(x,y,z)$, $control(x,y,z)$, $access\_own(x,y)$, $take\_access\_own(x,y,z)$, $access\_read(x,y)$, $access\_write(x,y)$, $access\_append(x,y)$, $flow(x,y,y',z)$, $find(x,y,z)$, $post(x,y,z)$, $pass(x,y,z)$, $take\_flow(x,y)$;

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

Используем следующие предположение и определения БР ДП-модели.

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.

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.

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 $(s_x, s_y, own_a) \in A_N$.

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 1–6.

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 $s_1 = x$ и $s_2, \ldots, s_m \in (N_U \cup S) \setminus \{x\}$, где $s_m = y$ и $m \geqslant 2$, такая, что для каждого i, $1 \leqslant i < m$, истинен предикат $simple\_directly\_access\_own(s_i, s_{i+1}, G)\}$. Определим функцию $island : N_U \cup S \to 2^{N_u \cup S}$, задающую для каждых субъект-сессии или недоверенного пользователя соответствующий им остров. При этом используются следующие 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 $island\_actions(x) = \{(p,r) \in P \times R : \exists y \in island(x)$ $[(y \in N_U \ \& \ (p,r) \in PA(UA(y)) \times can\_manage\_rights(AUA(y))) \vee (y \in N_S \cap S \ \&$ $\& \ (p,r) \in PA(UA(user(y))) \times can\_manage\_rights(AUA(user(y)))) \vee (y \in L_S \cap S \ \&$ $\& \ (p,r) \in PA(roles(y)) \times can\_manage\_rights(roles(y) \cap AR))]\}$.

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 соединяются 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 $r_y \in can\_manage\_rights(roles(z) \cap AR)$.

При этом используется следующее обозначение:

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

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 соединяются 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 $(w, own_r) \in \in PA(r_v)$.

При этом используется следующее обозначение:

$is\_bridge : (N_U \cup (N_S \cap S)) \times (N_U \cup S) \times (N_U \cup S) \to \{\text{true}, \text{false}\}$ — функция, для которой по определению справедливо равенство $is\_bridge(x, y, z) = \text{true}$ 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 [2] обоснованы алгоритмически проверяемые необходимые и достаточные условия истинности предиката $simple\_can\_access\_own(x, y, G_0)$.

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 $simple\_can\_access\_own(user_0(x), y, G_0)$.

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).

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 $is\_bridge(x_m, y_{m-1}, y) = \text{true}$.

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

2. Условия передачи прав доступа

В рамках БР ДП-модели рассмотрим условия передачи прав доступа с участием произвольного числа субъект-сессий для простых траекторий функционирования системы. Дадим определение.

Определение 8. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют пользователь $x \in U_0$ и право доступа к сущности $(e, \alpha) \in P_0$. Определим предикат $simple\_can\_share((e, \alpha), x, G_0)$, 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 существует субъект-сессия $s_x \in S_N$, такая, что $user_N(s_x) = x$ и выполняется условие $(e, \alpha) \in de\_facto\_rights_N(s_x)$.

Определим и обоснуем алгоритмически проверяемые необходимые и достаточные условия истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$ для случая, когда $x \in N_U$.

Теорема 2. 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 право доступа к сущности $(e, \alpha) \in P_0$. Предикат $simple\_can\_share((e, \alpha), x, G_0)$ является истинным тогда и только тогда, когда выполняется одно из условий.

1. Выполняется условие $(e, \delta) \in PA_0(UA_0(x))$, где $\delta \in \{\alpha, own_r\}$.

2. Существует субъект-сессия или недоверенный пользователь $y \in N_U \cup S_0$, истинен предикат $simple\_can\_access\_own(x, y, G_0)$ и выполняется одно из условий:

— $y \in N_U$ и $(e, \alpha) \in PA_0(UA_0(y))$;
— $y \in N_S \cap S_0$ и $(e, \alpha) \in PA_0(UA_0(user_0(y)))$;
— $y \in L_S \cap S_0$ и $(e, \alpha) \in PA_0(roles_0(y))$.

3. Существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_m \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_1, \ldots, y_m \in N_U \cup S_0$, где $m \geqslant 2$, таких, что $x_1 = x$, $y_i \in island(x_i)$, где $1 \leqslant i \leqslant m$, и выполняется одно из условий:

— $y_m \in N_U$ и $(e, own_r) \in PA_0(UA_0(y_m))$;
— $y_m \in N_S \cap S_0$ и $(e, own_r) \in PA_0(UA_0(user_0(y_m)))$;
— $y_m \in L_S \cap S_0$ и $(e, own_r) \in PA_0(roles_0(y_m))$.

При этом справедливо равенство $is\_simple\_bridge(x_m, y_{m-1}, y_m) = \text{true}$, и для каждого $2 \leqslant i \leqslant m$ справедливо равенство или $is\_bridge(x_i, y_{i-1}, y_i) = \text{true}$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = \text{true}$.

Доказательство. Докажем достаточность выполнения условий теоремы для истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$ при $x \in N_U$.

Пусть выполнено условие 1 теоремы. Тогда по предположению 1 существуют сущность $e_x \in E_0$, административная роль $ar_x \in AUA_0(x)$ и роль $r_x \in can\_manage\_rights(ar_x)$, такие, что $(e_x, execute_r) \in PA_0(UA_0(x))$. Положим

$op_1 = create\_first\_session(x, r_x, e_x, s_x)$.

По условию 1 существует роль $r_e \in UA_0(x)$, такая, что $(e, \delta) \in PA_0(r_e)$, где $\delta \in \{\alpha, own_r\}$. Тогда положим

$op_2 = take\_role(s_x, r_e)$.

Если $\delta = \alpha$, то положим $N = 2$.

Если $\delta = own_r$, то положим

$op_3 = take\_role(s_x, ar_x)$;

$op_4 = grant\_right(s_x, r_e, (e, \alpha))$;

$N = 4$.

Таким образом, существует $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$ — простая траектория без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и в состоянии G_N выполняется условие $user_N(s_x) = x$ и право доступа к сущности $(e, \alpha) \in de\_facto\_rights_N(s_x)$. Следовательно, по определению 8 предикат $simple\_can\_share((e, \alpha), x, G_0)$ является истинным.

Пусть выполнено условие 2 теоремы. Тогда существует субъект-сессия или недоверенный пользователь $y \in N_U \cup S_0$, истинен предикат $simple\_can\_access\_own(x, y, G_0)$ и по определению 3 существуют состояния $G_1, \ldots, G_M$ и правила преобразования состояний $op_1, \ldots, op_M$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_M} G_M$, где $M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, существуют субъект-сессии $s_x, s_y \in S_M$, такие, что $user_M(s_x) = x$, или $s_y = y$, или $user_M(s_y) = y$, и выполняется условие $(s_x, s_y, own_a) \in A_M$. По условию 1 теоремы возможны три случая.

Первый случай: выполняются условия $y \in N_U$ и $(e, \alpha) \in PA_0(UA_0(y))$. Тогда существует роль $r_y \in UA_0(y) = UA_M(user_M(s_y))$, такая, что $(e, \alpha) \in PA_0(r_y)$. Положим

$op_{M+1} = take\_role(s_y, r_y)$;

$N = M + 1$.

Второй случай: выполняются условия $y \in N_S \cap S_0$ и $(e, \alpha) \in PA_0(UA_0(user_0(y)))$. Тогда существует роль $r_y \in UA_0(user_0(y))$, такая, что $(e, \alpha) \in PA_0(r_y)$. Положим

$op_{M+1} = take\_role(y, r_y)$;

$N = M + 1$.

Третий случай: выполняется условие $y \in L_S \cap S_0$ и $(e, \alpha) \in PA_0(roles_0(y))$. Тогда положим $N = M$. Следовательно, траектория $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа и выполняется условие $(e, \alpha) \in de\_facto\_rights_N(s_x)$. Значит, по определению 8 предикат $simple\_can\_share((e, \alpha), x, G_0)$ является истинным.

Пусть выполнено условие 3 теоремы, тогда выполняются условия $m \geqslant 2$ и $is\_simple\_bridge(x_m, y_{m-1}, y_m) = \text{true}$. Выберем минимальное $2 \leqslant k \leqslant m$, такое, что справедливы равенства $is\_simple\_bridge(x_l, y_{l-1}, y_l) = \text{true}$, где $k \leqslant l \leqslant m$. Для каждого простого моста, соединяющего субъект-сессию или недоверенного пользователя y_{l-1} с субъект-сессией или недоверенным пользователем y_l через недоверенную субъект-сессию или недоверенного пользователя x_l, выполняется условие $y_l \in island(x_l)$ и существует роль $r_{y_{l-1}}$, удовлетворяющая условиям определения 6, где $k \leqslant l \leqslant m$.

По утверждению 1 и определению 3 существуют состояния $G_1, \ldots, G_M$ и правила преобразования состояний $op_1, \ldots, op_M$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_M} G_M$, где $M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и для каждого $k \leqslant l \leqslant m$ существует субъект-сессия $s_{x_l} \in S_M$, такая, что или $user_M(s_{x_l}) = x_l$, или $s_{x_l} = x_l$, существует субъект-сессия $s_{y_l} \in S_M$, такая, что $user_M(s_{y_l}) = y$ или $s_{y_l} = y_l$, и выполняется условие $(s_{x_l}, s_{y_l}, own_a) \in A_M$. Положим

$op_{M+1} = grant\_right(s_{x_m}, r_{y_{m-1}}, (e, own_r))$;

$\ldots$

$op_{M+m-k} = grant\_right(s_{x_{k+1}}, r_{y_k}, (e, own_r))$;

$op_{M+m-k+1} = grant\_right(s_{x_k}, r_{y_{k-1}}, (e, \alpha))$;

$K = M + m - k + 1$.

Возможны два случая.

Первый случай: справедливо равенство $k = 2$. По условию теоремы $y_1 \in island(x)$, следовательно, по утверждению 1 существуют состояния $G_{K+1}, \ldots, G_N$ и правила преобразования состояний $op_{K+1}, \ldots, op_N$, такие, что $G_K \vdash_{op_{K+1}} G_{K+1} \vdash_{op_{K+2}} \ldots \vdash_{op_N} G_N$, где $N \geqslant K$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, существуют субъект-сессии $s_x, s_{y_1} \in S_N$, такие, что выполняются условия:

— $user_N(s_x) = x$ или $s_x = x$;
— существует субъект-сессия $s_{y_1} \in S_N$, такая, что $user_N(s_{y_1}) = y_1$ или $s_{y_1} = y_1$;
— $(s_x, s_{y_1}, own_a) \in A_N$.

Второй случай: выполняется неравенство $k > 2$. Тогда выполняется условие $is\_bridge(x_{k-1}, y_{k-2}, y_{k-1}) = \text{true}$ и последовательность недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_{k-1} \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_1, \ldots, y_{k-1} \in N_U \cup S_0$ удовлетворяет условиям теоремы 1.

Следовательно, истинен предикат $simple\_can\_access\_own(x, y_{k-1}, G_0)$, и по определению 3 существуют состояния $G_{K+1}, \ldots, G_N$ и правила преобразования состояний $op_{K+1}, \ldots, op_N$, такие, что $G_K \vdash_{op_{K+1}} G_{K+1} \vdash_{op_{K+2}} \ldots \vdash_{op_N} G_N$, где $N \geqslant K$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, существуют субъект-сессии $s_x, s_{y_{k-1}} \in S_N$, такие, что выполняются условия:

— $user_N(s_x) = x$;
— $s_{y_{k-1}} = y_{k-1}$ или $user_N(s_{y_{k-1}}) = y_{k-1}$;
— $(s_x, s_{y_{k-1}}, own_a) \in A_N$.

Таким образом, в обоих случаях выполняется условие $(e, \alpha) \in de\_facto\_rights_N(s_x)$, и траектория $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$ является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа. Значит, по определению 8 предикат $simple\_can\_share((e, \alpha), x, G_0)$ является истинным.

Обоснована достаточность выполнения условий теоремы для истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$ при $x \in N_U$.

Докажем необходимость выполнения условий теоремы для истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$ при $x \in N_U$. По определению 8 существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует субъект-сессия $s_x \in S_N$, такая, что $user_N(s_x) = x$ и выполняется условие $(e, \alpha) \in$ $\in de\_facto\_rights_N(s_x)$.

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

Пусть $N = 0$, тогда существует недоверенная субъект-сессия $s_x \in N_S \cap S_0$, такая, что $user_0(s_x) = x$, и выполняется условие $(e, \alpha) \in de\_facto\_rights_0(s_x)$. Значит, существует роль $r \in R \cup AR$, такая, что $(e, \alpha) \in PA_0(r)$. Возможны два случая.

Первый случай: выполняется условие $r \in roles_0(s_x) \subset UA_0(x)$. Следовательно, условие 1 теоремы выполнено.

Второй случай: существует субъект-сессия $y \in S_0$, такая, что $r \in roles_0(y)$ и $(s_x, y, own_a) \in A_0$. Следовательно, по определению 3 истинен предикат $simple\_can\_access\_own(x, y, G_0)$. Таким образом, условие 2 теоремы выполнено.

Пусть $N = 1$, тогда из минимальности N следует, что выполняются условия $(e, \alpha) \notin de\_facto\_rights_0(s_x)$ и $(e, \alpha) \in de\_facto\_rights_1(s_x)$. Возможны пять случаев.

Первый случай: существует недоверенная субъект-сессия $y \in N_S \cap S_0$, такая, что либо $y = s_x$, либо $(s_x, y, own_a) \in A_0$, и существует роль $r_e \in UA_0(user_0(y))$, такая, что $(e, \alpha) \in PA_0(r_e)$ и $op_1 = take\_role(y, r_e)$. Если $y = s_x$, то выполнено условие 1 теоремы. Если $(s_x, y, own_a) \in A_0$, то по определению 3 предикат $simple\_can\_access\_own(x, y, G_0)$ является истинным. Следовательно, условие 2 теоремы выполнено.

Второй случай: существует субъект-сессия $y_1 \in S_0$, такая, что либо $y_1 = s_x$, либо $(s_x, y_1, own_a) \in A_0$, и существуют недоверенная субъект-сессия $x_2 \in N_S \cap S_0$ и роль $r_e \in roles_0(y_1)$, такие, что $((e, own_r), r_e) \in de\_facto\_actions_0(x_2)$, и $op_1 = grant\_right(x_2, r_e, (e, \alpha))$. Значит, существует субъект-сессия $y_2 \in S_0$, такая, что либо $y_2 = x_2$, либо $(x_2, y_2, own_a) \in A_0$, и выполняются условия $(e, own_r) \in PA_0(roles_0(y_2))$ и $r_e \in can\_manage\_rights(roles_0(y_2) \cap AR))$. Следова-

тельно, справедливо равенство $is\_simple\_bridge(x_2, y_1, y_2) = \text{true}$. По определению 5 выполняются условия $y_1 \in island(x)$ и $y_2 \in island(x_2)$. Положим $m = 2$. Следовательно, условие 3 теоремы выполнено.

Третий случай: существуют субъект-сессии $y, z \in S_0$, такие, что $z \in [y]$ и либо $s_x = z$, либо $(s_x, z, own_a) \in A_0$, и $(e, \alpha) \in PA_0(roles_0(y))$, $op_1 = control(s_x, y, z)$.

Четвертый случай: существует субъект-сессия $y \in S_0$, такая, что $(y, own_r) \in \in de\_facto\_rights_0(s_x)$, $(e, \alpha) \in PA_0(roles_0(y))$ и $op_1 = access\_own(s_x, y)$. Значит, существует субъект-сессия $z \in S_0$, такая, что $(s_x, z, own_a) \in A_0$ и $(y, own_r) \in \in PA_0(roles_0(z))$.

Пятый случай: существуют субъект-сессии $y, z \in S_0$, такие, что $\{(s_x, z, own_a), (z, y, own_a)\} \in A_0$, и $(e, \alpha) \in PA_0(roles_0(y))$, $op_1 = take\_access\_own(s_x, z, y)$.

В третьем, четвертом и пятом случаях по определению 5 выполняется условие $y \in island(x) \setminus \{x\}$. Следовательно, по утверждению 1 истинен предикат $simple\_can\_access\_own(x, y, G_0)$, и условие 2 теоремы выполнено.

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

Из минимальности N следует, что существует недоверенная субъект-сессия $s_x \in N_S \cap S_{N-1}$, такая, что $user_{N-1}(s_x) = x$, и выполняются условия $(e, \alpha) \notin de\_facto\_rights_{N-1}(s_x)$ и $(e, \alpha) \in de\_facto\_rights_N(s_x)$. Возможны пять случаев.

Первый случай: существует недоверенная субъект-сессия $s_{y'} \in N_S \cap S_{N-1}$, такая, что либо $s_{y'} = s_x$, либо $(s_x, s_{y'}, own_a) \in A_{N-1}$, и существует роль $r_e \in UA_{N-1}(user_{N-1}(s_{y'}))$, такая, что $(e, \alpha) \in PA_{N-1}(r_e)$ и $op_N = take\_role(s_{y'}, r_e)$. Положим $y' = user_{N-1}(s_{y'})$, тогда по предположению 1 выполняется условие $r_e \in UA_0(y')$. Возможны две ситуации.

Первая ситуация: выполняется условие $(e, \alpha) \in PA_0(r_e)$. Если $s_{y'} = s_x$, то выполняется условие $(e, \alpha) \in PA_0(UA_0(x))$ и выполнено условие 1 теоремы. Если $(s_x, s_{y'}, own_a) \in A_{N-1}$, то положим $y = y'$. Тогда $(e, \alpha) \in PA_0(UA_0(y))$ и по определению 3 истинен предикат $simple\_can\_access\_own(x, y, G_0)$. Следовательно, выполнено условие 2 теоремы.

Вторая ситуация: выполняется условие $(e, \alpha) \notin PA_0(r_e)$. Если $s_{y'} = s_x$, то положим $k = 1$, $y_1 = s_{y'}$. Пусть $(s_x, s_{y'}, own_a) \in A_{N-1}$, тогда по определению 3 истинен предикат $simple\_can\_access\_own(x, y', G_0)$. Следовательно, по теореме 1 существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_k \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_1, \ldots, y_k \in N_U \cup S_0$, где $k \geqslant 1$, таких, что $x_1 = x$, $y_k = s_{y'}$, $y_i \in island(x_i)$, где $1 \leqslant i \leqslant m$, и выполняются условия:

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

При этом существуют $1 \leqslant M < N$ и недоверенная субъект-сессия $s_{x'} \in N_S \cap \cap S_{M-1}$, такие, что $((e, own_r), r_e) \in de\_facto\_actions_{M-1}(s_{x'})$ и $op_M = grant\_right(s_{x'}, r_e, (e, \alpha))$. Значит, существует субъект-сессия $s_{y''} \in S_{M-1}$, такая, что либо $s_{x'} = s_{y''}$, либо $(s_{x'}, s_{y''}, own_a) \in A_{M-1}$. При этом выполняются условия $r_e \in can\_manage\_rights(roles_{M-1}(s_{y''}) \cap AR))$ и $(e, own_r) \in PA_{M-1}(roles_{M-1}(s_{y''}))$. Положим $x' = = user_{M-1}(s_{x'}) \in N_U$. Если $s_{y''} \in N_S$, то положим $y_{k+1} = user_{M-1}(s_{y''}) \in N_U$. Тогда выполняется условие $r_e \in can\_manage\_rights(UA_0(y_{k+1}) \cap AR))$. Если $s_{y''} \in L_S$, то положим $y_{k+1} = s_{y''}$, по предположению 1 выполняются условия $y_{k+1} \in L_S \cap S_0$ и

$r_e \in can\_manage\_rights(roles_0(y_{k+1}) \cap AR)$). Значит, либо $x' = y_{k+1}$, либо истинен предикат $simple\_can\_access\_own(x', y_{k+1}, G_0)$, и по теореме 1 существует недоверенный пользователь $x_{k+1} \in N_U$, такой, что $y_{k+1} \in island(x_{k+1})$. Следовательно, по определению 6 справедливо равенство $is\_simple\_bridge(x_{k+1}, y_k, y_{k+1}) = \text{true}$. При этом так как $y_{k+1} \in island(x_{k+1})$, то возможен выбор такого x_{k+1}, что истинен предикат $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ с длиной траектории меньше N.

Значит, по предположению индукции для предиката $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ и из выполнения одного из условий

— $y_{k+1} \in N_U$ и $(e, own_r) \in PA_{M-1}(UA_{M-1}(y_{k+1}))$;
— $y_{k+1} \in L_S \cap S_0$ и $(e, own_r) \in PA_{M-1}(roles_{M-1}(y_{k+1}))$

следует, что для предиката $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ выполнено условие 1 или условие 3 теоремы.

Если для предиката $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ выполнено условие 1 теоремы, то $(e, own_r) \in PA_0(UA_0(x_{k+1}))$ и $y_{k+1} = x_{k+1}$. Положим $m = k + 1$.

Если для предиката $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ выполнено условие 3 теоремы, то существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_{k+1}, \ldots, x_m \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_{k+1}, \ldots, y_m \in N_U \cup S_0$, где $m \geqslant k + 1$, таких, что $y_i \in island(x_i)$, где $k + 1 \leqslant i \leqslant m$, и выполняется одно из условий:

— $y_m \in N_U$ и $(e, own_r) \in PA_0(UA_0(y_m))$;
— $y_m \in N_S \cap S_0$ и $(e, own_r) \in PA_0(UA_0(user_0(y_m)))$;
— $y_m \in L_S \cap S_0$ и $(e, own_r) \in PA_0(roles_0(y_m))$.

При этом справедливо равенство $is\_simple\_bridge(x_m, y_{m-1}, y_m) = \text{true}$, и для каждого $k + 2 \leqslant i \leqslant m$ справедливо равенство или $is\_bridge(x_i, y_{i-1}, y_i) = \text{true}$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = \text{true}$.

Таким образом, в первом случае во второй ситуации выполнено условие 3 теоремы.

Второй случай: существует субъект-сессия $s_{y'} \in S_{N-1}$, такая, что либо $s_{y'} = s_x$, либо $(s_x, s_{y'}, own_a) \in A_{N-1}$, и существуют недоверенная субъект-сессия $s_{x'} \in N_S \cap S_{N-1}$ и роль $r_e \in roles_{N-1}(s_{y'})$, такие, что $((e, own_r), r_e) \in de\_facto\_actions_{N-1}(s_{x'})$, и $op_N = grant\_right(s_{x'}, r_e, (e, \alpha))$. Значит, существует субъект-сессия $s_{y''} \in S_{N-1}$, такая, что либо $s_{y''} = s_{x'}$, либо $(s_{x'}, s_{y''}, own_a) \in A_{N-1}$, и выполняются условия $(e, own_r) \in PA_{N-1}(roles_{N-1}(s_{y''}))$, $r_e \in can\_manage\_rights(roles_{N-1}(s_{y''}) \cap AR)$).

Если $s_{y'} = s_x$, то положим $k = 1$, $y_1 = s_{y'}$. Пусть $(s_x, s_{y'}, own_a) \in A_{N-1}$, тогда по определению 3 истинен предикат $simple\_can\_access\_own(x, s_{y'}, G_0)$. Следовательно, по теореме 1 существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_k \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_1, \ldots, y_k \in N_U \cup S_0$, где $k \geqslant 1$, таких, что $x_1 = x$, $y_k = s_{y'}$, $y_i \in island(x_i)$, где $1 \leqslant i \leqslant m$, и выполняются условия:

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

Положим $x' = user_{N-1}(s_{x'}) \in N_U$. Если $s_{y''} \in N_S$, то положим $y_{k+1} = user_{N-1}(s_{y''}) \in N_U$. Тогда выполняется условие $r_e \in can\_manage\_rights(UA_0(y_{k+1}) \cap AR))$. Если $s_{y''} \in L_S$, то положим $y_{k+1} = s_{y''}$, по предположению 1 выполняются условия $y_{k+1} \in L_S \cap S_0$ и $r_e \in can\_manage\_rights(roles_0(y_{k+1}) \cap AR))$. Значит, либо $x' = y_{k+1}$,

либо истинен предикат $simple\_can\_access\_own(x', y_{k+1}, G_0)$, и по теореме 1 существует недоверенный пользователь $x_{k+1} \in N_U$, такой, что $y_{k+1} \in island(x_{k+1})$. Следовательно, по определению 6 справедливо равенство $is\_simple\_bridge(x_{k+1}, y_k, y_{k+1})$. При этом так как $y_{k+1} \in island(x_{k+1})$, то возможен выбор такого x_{k+1}, что истинен предикат $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ с длиной траектории меньше N.

Значит, по предположению индукции для предиката $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ и из выполнения одного из условий

— $y_{k+1} \in N_U$ и $(e, own_r) \in PA_{N-1}(UA_{N-1}(y_{k+1}))$;
— $y_{k+1} \in L_S \cap S_0$ и $(e, own_r) \in PA_{N-1}(roles_{N-1}(y_{k+1}))$

следует, что для предиката $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ выполнено условие 1 или условие 3 теоремы.

Если для предиката $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ выполнено условие 1 теоремы, то $(e, own_r) \in PA_0(UA_0(x_{k+1}))$ и $y_{k+1} = x_{k+1}$. Положим $m = k + 1$.

Если для предиката $simple\_can\_share((e, own_r), x_{k+1}, G_0)$ выполнено условие 3 теоремы, то существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_{k+1}, \ldots, x_m \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_{k+1}, \ldots, y_m \in N_U \cap S_0$, где $m \geqslant k + 1$, таких, что $y_i \in island(x_i)$, где $k + 1 \leqslant i \leqslant m$, и выполняется одно из условий:

— $y_m \in N_U$ и $(e, own_r) \in PA_0(UA_0(y_m))$;
— $y_m \in N_S \cap S_0$ и $(e, own_r) \in PA_0(UA_0(user_0(y_m)))$;
— $y_m \in L_S \cap S_0$ и $(e, own_r) \in PA_0(roles_0(y_m))$.

При этом справедливо равенство $is\_simple\_bridge(x_m, y_{m-1}, y_m) = \text{true}$ и для каждого $k + 2 \leqslant i \leqslant m$ справедливо равенство или $is\_bridge(x_i, y_{i-1}, y_i) = \text{true}$, или $is\_simple\_bridge(x_i, y_{i-1}, y_i) = \text{true}$.

Таким образом, во втором случае выполнено условие 3 теоремы.

Третий случай: существуют субъект-сессии $s_{y'}, s_z \in S_{N-1}$, такие, что $s_z \in [s_{y'}]$ и либо $s_x = s_z$, либо $(s_x, s_z, own_a) \in A_{N-1}$, и $(e, \alpha) \in PA_{N-1}(roles_{N-1}(s_{y'}))$, $op_N = control(s_x, s_{y'}, s_z)$.

Четвертый случай: существует субъект-сессия $s_{y'} \in S_{N-1}$, такая, что $(s_{y'}, own_r) \in de\_facto\_rights_{N-1}(s_x)$, $(e, \alpha) \in PA_{N-1}(roles_{N-1}(s_{y'}))$ и $op_N = access\_own(s_x, s_{y'})$.

Пятый случай: существуют субъект-сессии $s_{y'}, s_z \in S_{N-1}$, такие, что $\{(s_x, s_z, own_a), (s_z, s_{y'}, own_a)\} \subset A_{N-1}$, и $(e, \alpha) \in PA_{N-1}(roles_0(s_{y'}))$, $op_N = take\_access\_own(s_x, s_z, s_{y'})$.

Таким образом, в третьем, четвертом и пятом случае существует роль $r_e \in UA_{N-1}(user_{N-1}(s_{y'}))$, такая, что $(e, \alpha) \in PA_{N-1}(r_e)$. При этом, если $s_{y'} \in N_S$, то положим $y' = user_{N-1}(s_{y'})$, если $s_{y'} \in L_S$, то $y' = s_{y'}$ и по предположению 1 $y' \in L_S \cap S_0$. Значит, истинен предикат $simple\_can\_access\_own(x, y', G_0)$, и выполнение условия 2 или 3 теоремы обосновывается аналогично первому случаю.

Следовательно, доказан шаг индукции при длине траектории, равной N. Доказательство необходимости выполнения условия теоремы для истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$ при $x \in N_U$ выполнено.

Теорема доказана. ■

Определим и обоснуем алгоритмически проверяемые необходимые и достаточные условия истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$ для случая, когда $x \in L_U$.

Теорема 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 доверенный пользователь $x \in L_U$ и право доступа

к сущности $(e, \alpha) \in P_0$. Предикат $simple\_can\_share((e, \alpha), x, G_0)$ является истинным тогда и только тогда, когда существует доверенная субъект-сессия $s_x \in L_S \cap S_0$, такая, что $user_0(s_x) = x$ и выполняется одно из следующих условий:

1. Выполняется условие $(e, \alpha) \in PA_0(roles_0(s_x))$.

2. Существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_1, \ldots, x_m \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_1, \ldots, y_m \in N_U \cup S_0$, где $m \geqslant 1$, таких, что $y_i \in island(x_i)$, где $1 \leqslant i \leqslant m$, и выполняется одно из условий:

— $y_m \in N_U$ и $(e, own_r) \in PA_0(UA_0(y_m))$;
— $y_m \in N_S \cap S_0$ и $(e, own_r) \in PA_0(UA_0(user_0(y_m)))$;
— $y_m \in L_S \cap S_0$ и $(e, own_r) \in PA_0(roles_0(y_m))$.

При этом справедливо равенство $is\_simple\_bridge(x_1, s_x, y_1) = \text{true}$ и для каждого $2 \leqslant i \leqslant m$ справедливо равенство $is\_simple\_bridge(x_i, y_{i-1}, y_i) = \text{true}$.

Доказательство. Докажем достаточность выполнения условий теоремы для истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$ при $x \in L_U$.

Пусть выполнено условие 1 теоремы. Тогда по определению 8 предикат $simple\_can\_share((e, \alpha), x, G_0)$ является истинным.

Пусть выполнено условие 2 теоремы. Докажем истинность предиката $simple\_can\_share((e, \alpha), x, G_0)$ индукцией по длине m последовательностей субъект-сессий или недоверенных пользователей.

Пусть $m = 1$. Тогда по условию теоремы справедливо равенство $is\_simple\_bridge(x_1, s_x, y_1) = \text{true}$, и по определению 6 $y_1 \in island(x_1)$ и существует роль $r_e \in roles_0(s_x)$, такая, что выполняется одно из условий:

— $y_1 \in N_U$ и $(e, own_r) \in PA_0(UA_0(y_1))$ и $r_e \in can\_manage\_rights(AUA_0(y_1))$;
— $y_1 \in N_S \cap S_0$ и $(e, own_r) \in PA_0(UA_0(user_0(y_1)))$ и $r_e \in can\_manage\_rights(AUA_0(user_0(y_1)))$;
— $y_1 \in L_S \cap S_0$ и $(e, own_r) \in PA_0(roles_0(y_1))$ и $r_e \in can\_manage\_rights(roles_0(y_1) \cap \cap AR)$.

По утверждению следствия 1 существуют состояния $G_0, \ldots, G_M$ и правила преобразования состояний $op_0, \ldots, op_M$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_M} G_M$, где $M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует недоверенная субъект-сессия $s_{x_1} \in N_S \cap S_M$, такая, что либо $user_M(s_{x_1}) = x_1$, либо $s_{x_1} = x_1$, и в состоянии G_M выполняется условие $island\_actions(x_1) = island\_actions(s_{x_1}) \in de\_facto\_actions_M(s_{x_1})$. Значит, выполняется условие $((e, own_r), r_e) \in de\_facto\_actions_M(s_{x_1})$. Положим

$op_{M+1} = grant\_right(s_{x_1}, r_e, (e, \alpha))$.

Тогда в состоянии G_{M+1}, таком, что $G_M \vdash_{op_{M+1}} G_{M+1}$, выполняется условие $(e, \alpha) \in PA_{M+1}(r_e) \in PA_{M+1}(roles_{M+1}(s_x))$. Так как траектория $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \ldots \vdash_{op_{M+1}} G_{M+1}$ является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, то по определению 8 является истинным предикат $simple\_can\_share((e, \alpha), x, G_0)$.

Заметим, что при $m = 1$ условие $s_x \in L_S \cap S_0$ не является существенным, т. е. передача прав доступа возможна в случае, когда $s_x \in N_S \cap S_0$.

Пусть $m > 1$ и утверждение верно для всех последовательностей длины $l < m$. Докажем достаточность условий теоремы при длине последовательности, равной m.

С учетом сделанного замечания и из предположения индукции следует, что существуют состояния $G_0, \ldots, G_M$ и правила преобразования состояний $op_0, \ldots, op_M$, такие,

что $G_0 \vdash_{op_1} \ldots \vdash_{op_M} G_M$, где $M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует субъект-сессия $s_{y_1} \in S_M$, такая, что либо $user_M(s_{y_1}) = y_1$, либо $s_{y_1} = y_1$, и в состоянии G_M выполняется условие $(e, \alpha) \in PA_M(roles_M(s_{y_1}))$. При этом по условию теоремы и по определению 6 справедливо равенство $is\_simple\_bridge(x_1, s_x, s_{y_1}) = \text{true}$. Выполняя рассуждения, аналогичные использованным при обосновании случая $m = 1$, получаем, что предикат $simple\_can\_share((e, \alpha), x, G_0)$ является истинным.

Таким образом, для $x \in L_U$ доказана достаточность выполнения условий теоремы для истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$.

Докажем для $x \in L_U$ необходимость выполнения условий теоремы для истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$.

Пусть истинен предикат $simple\_can\_share((e, \alpha), x, G_0)$. Тогда по определению 8 существуют состояния $G_1, \ldots, G_N = (PA_N, user_N, roles_N, A_N, F_N, H_{E_N})$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует субъект-сессия $s_x \in S_N$, такая, что $user_N(s_x) = x$ и выполняется условие $(e, \alpha) \in de\_facto\_rights_N(s_x)$. Так как $x \in L_U$, то по предположению 1 и по определениям 1 и 2 выполняются условия $s_x \in L_S \cap S_0$ и $(e, \alpha) \in PA_N(rolesN(s_x))$.

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

Пусть $N = 0$, тогда $(e, \alpha) \in PA_0(roles_0(s_x))$. Следовательно, выполнено условие 1 теоремы.

Пусть $N = 1$, тогда из минимальности N следует, что $(e, \alpha) \notin PA_0(roles_0(s_x))$. Тогда существуют недоверенная субъект-сессия $x_1 \in N_S \cap S_0$ и роль $r_e \in roles_0(s_x)$, такие, что $((e, own_r), r_e) \in de\_facto\_actions_0(x_1)$, и $op_1 = grant\_right(x_1, r_e, (e, \alpha))$. Значит, существует субъект-сессия $y_1 \in S_0$, такая, что либо $y_1 = x_1$, либо $(x_1, y_1, own_a) \in A_0$, и выполняются условия $(e, own_r) \in PA_0(roles_0(y_1))$ и $r_e \in can\_manage\_rights(roles_0(y_1) \cap AR))$. Следовательно, справедливо равенство $is\_simple\_bridge(x_1, s_x, y_1) = \text{true}$. По определению 5 выполняется условие $y_1 \in island(x_1)$. Положим $m = 1$. Следовательно, условие 2 теоремы выполнено.

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

Тогда существуют недоверенная субъект-сессия $s_{x'} \in N_S \cap S_{N-1}$ и роль $r_e \in roles_{N-1}(s_x)$, такие, что $((e, own_r), r_e) \in de\_facto\_actions_{N-1}(s_{x'})$, и $op_N = grant\_right(s_{x'}, r_e, (e, \alpha))$. Значит, существует субъект-сессия $s_{y'} \in S_{N-1}$, такая, что либо $s_{y'} = s_{x'}$, либо $(s_{x'}, s_{y'}, own_a) \in A_{N-1}$, и выполняются условия $(e, own_r) \in PA_{N-1}(roles_{N-1}(s_{y'}))$, $r_e \in can\_manage\_rights(roles_{N-1}(s_{y'}) \cap AR))$.

Положим $x' = user_{N-1}(s_{x'}) \in N_U$. Если $s_{y'} \in N_S$, то положим $y_1 = user_{N-1}(s_{y'}) \in N_U$. Тогда выполняется условие $r_e \in can\_manage\_rights(UA_0(y_1) \cap AR))$. Если $s_{y'} \in L_S$, то положим $y_1 = s_{y'}$, по предположению 1 выполняются условия $y_1 \in L_S \cap S_0$ и $r_e \in can\_manage\_rights(roles_0(y_1) \cap AR))$. Значит, либо $x' = y_1$, либо истинен предикат $simple\_can\_access\_own(x', y_1, G_0)$, и по теореме 1 существует недоверенный пользователь $x_1 \in N_U$, такой, что $y_1 \in island(x_1)$. Следовательно, по определению 6 справедливо равенство $is\_simple\_bridge(x_1, s_x, y_1)$.

Если выполняется одно из условий:

— $y_1 \in N_U$ и $(e, own_r) \in PA_0(UA_0(y_1))$;

— $y_1 \in N_S \cap S_0$ и $(e, own_r) \in PA_0(UA_0(user_0(y_1)))$;
— $y_1 \in L_S \cap S_0$ и $(e, own_r) \in PA_0(roles_0(y_1))$,

то положим $m = 1$, и условие 2 теоремы выполнено.

Пусть ни одно из данных условий не выполняется, тогда заметим, что доверенность субъект-сессии s_x не является существенной при получении принадлежащей ей ролью r_e права доступа (e, α). Следовательно, так как $(e, own_r) \in PA_{N-1}(roles_{N-1}(s_{y'}))$, где либо $y_1 \in N_U$ и $y_1 = user_{N-1}(s_{y'})$, либо $y_1 = s_{y'} \in L_S \cap S_0$, то, многократно повторяя выполненные рассуждения, получаем, что существуют последовательности недоверенных субъект-сессий или недоверенных пользователей $x_2, \ldots, x_m \in N_U \cup (N_S \cap S_0)$, субъект-сессий или недоверенных пользователей $y_2, \ldots, y_m \in N_U \cup S_0$, где $m \geqslant 2$, таких, что $y_i \in island(x_i)$, где $2 \leqslant i \leqslant m$, и выполняется одно из условий:

— $y_m \in N_U$ и $(e, own_r) \in PA_0(UA_0(y_m))$;
— $y_m \in N_S \cap S_0$ и $(e, own_r) \in PA_0(UA_0(user_0(y_m)))$;
— $y_m \in L_S \cap S_0$ и $(e, own_r) \in PA_0(roles_0(y_m))$.

При этом справедливо равенство $is\_simple\_bridge(x_2, y_1, y_2) = \text{true}$, и для каждого $3 \leqslant i \leqslant m$ справедливо равенство $is\_simple\_bridge(x_i, y_{i-1}, y_i) = \text{true}$.

Таким образом, выполнено условие 2 теоремы. Следовательно, доказан шаг индукции при длине траектории, равной N.

Доказательство необходимости выполнения условия теоремы для истинности предиката $simple\_can\_share((e, \alpha), x, G_0)$ при $x \in L_U$ выполнено.

Теорема доказана. ■

3. Условия реализации информационных потоков по памяти

В рамках БР ДП-модели рассмотрим условия реализации информационных потоков по памяти с участием произвольного числа субъект-сессий для простых траекторий функционирования системы. Дадим определение.

Определение 9. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют сущности или недоверенные пользователи $x, y \in N_U \cup E_0$, где $x \neq y$. Определим предикат $simple\_can\_write\_memory(x, y, G_0)$, 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 $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и выполняется условие $(x', y', write_m) \in F_N$, где верно следующее:

— если $x \in E_0$, то $x' = x$; если $x \in N_U$, то $x' \in S_N$ и $user_N(x') = x$;
— если $y \in E_0$, то $y' = y$; если $y \in N_U$, то $y' \in S_N$ и $user_N(y') = y$.

Так как недоверенный пользователь может создать субъект-сессию, то в отличие от дискреционных или мандатных ДП-моделей в рамках БР ДП-модели он может являться источником или приемником информационного потока. С учетом условий функционирования существующих и перспективных КС будем считать, что в дальнейшем выполняется следующее предположение.

Предположение 2. У каждой доверенной субъект-сессии всегда имеется роль, обладающая правами доступа на чтение и запись к некоторой сущности. У каждого недоверенного пользователя имеется авторизованная роль, обладающая правами доступа на чтение и запись к некоторой сущности.

Обоснуем необходимые и достаточные условия истинности предиката $simple\_can\_write\_memory(x, y, G_0)$.

Теорема 4. Пусть $G_0 = (PA_0, user_0, roles_0, A_0, F_0, H_{E_0})$ — состояние системы $\Sigma(G^*, OP)$, в котором существуют сущности или недоверенные пользователи $x, y \in N_U \cup E_0$, где $x \neq y$. Предикат $simple\_can\_write\_memory(x, y, G_0)$ истинен тогда и только тогда, когда существует последовательность недоверенных пользователей или сущностей $e_1, \ldots, e_m \in N_U \cup E_0$, где $e_1 = x$, $e_m = y$ и $m \geqslant 2$, таких, что выполняется одно из условий.

1. $m = 2$ и $(x', y', write_m) \in F_0$, где выполняются условия:

— если $x \in E_0$, то $x' = x$; если $x \in N_U$, то $x' \in S_0$ и $user_0(x') = x$;
— если $y \in E_0$, то $y' = y$; если $y \in N_U$, то $y' \in S_0$ и $user_0(y') = y$.

2. Для каждого $i = 1, \ldots, m-1$ выполняется одно из условий:

— $e_i \in N_U \cup S_0$, $e_{i+1} \in N_U \cup E_0$ и $(e'_i, e'_{i+1}, write_m) \in F_0$, где верно следующее:
  - если $e_i \in S_0$, то $e'_i = e_i$; если $e_i \in N_U$, то $e'_i \in S_0$ и $user_0(e'_i) = e_i$;
  - если $e_{i+1} \in E_0$, то $e'_{i+1} = e_{i+1}$; если $e_{i+1} \in N_U$, то $e'_{i+1} \in S_0$ и $user_0(e'_{i+1}) = e_{i+1}$;
— $e_i \in N_U \cup S_0, e_{i+1} \in E_0 \setminus S_0$ и истинен предикат $simple\_can\_share((e_{i+1}, \alpha), e'_i, G_0)$, где $\alpha \in \{write_r, append_r\}$, и верно следующее:
  - если $e_i \in N_U$, то $e'_i = e_i$;
  - если $e_i \in S_0$, то $e'_i = user_0(e_i)$;
— $e_{i+1} \in N_U \cup S_0, e_i \in E_0 \setminus S_0$ и истинен предикат $simple\_can\_share((e_i, read_r), e'_{i+1}, G_0)$, где верно следующее:
  - если $e_{i+1} \in N_U$, то $e'_{i+1} = e_{i+1}$;
  - если $e_{i+1} \in S_0$, то $e'_{i+1} = user_0(e_{i+1})$;
— $e_i \in N_U \cup (N_S \cap S_0)$, $e_{i+1} \in N_U \cup S_0$ и истинен $simple\_can\_access\_own(e'_i, e_{i+1}, G_0)$, где верно следующее:
  - если $e_i \in N_U$, то $e'_i = e_i$;
  - если $e_i \in N_S \cap S_0$, то $e'_i = user_0(e_i)$;
— $e_{i+1} \in N_U \cup (N_S \cap S_0)$, $e_i \in N_U \cup S_0$ и истинен предикат $simple\_can\_access\_own(e'_{i+1}, e_i, G_0)$, где верно следующее:
  - если $e_{i+1} \in N_U$, то $e'_{i+1} = e_{i+1}$;
  - если $e_{i+1} \in N_S \cap S_0$, то $e'_{i+1} = user_0(e_{i+1})$.

Доказательство. Докажем достаточность выполнения условий теоремы для истинности предиката $simple\_can\_write\_memory(x, y, G_0)$.

Пусть выполнено условие 1 теоремы. Тогда по определению 9 предикат $simple\_can\_write\_memory(x, y, G_0)$ является истинным.

Пусть выполнено условие 2 теоремы. Тогда осуществим доказательство индукцией по длине m последовательности недоверенных пользователей или сущностей.

Пусть $m = 2$. Возможны пять случаев.

Первый случай: $x \in N_U \cup S_0$, $y \in N_U \cup E_0$ и $(x', y', write_m) \in F_0$, где выполняются условия:

— если $x \in S_0$, то $x' = x$; если $x \in N_U$, то $x' \in S_0$ и $user_0(x') = x$;
— если $y \in E_0$, то $y' = y$; если $y \in N_U$, то $y' \in S_0$ и $user_0(y') = y$.

Следовательно, по определению 9 предикат $simple\_can\_write\_memory(x, y, G_0)$ является истинным.

Второй случай: $x \in N_U \cup S_0, y \in E_0 \setminus S_0$ и истинен предикат $simple\_can\_share((y, \alpha), x', G_0)$, где $\alpha \in \{write_r, append_r\}$, и верно следующее:

— если $x \in N_U$, то $x' = x$;
— если $x \in S_0$, то $x' = user_0(x)$.

Тогда по определению 8 существуют состояния $G_1, \ldots, G_M$ и правила преобразования состояний $op_1, \ldots, op_M$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_M} G_M$, где $M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует субъект-сессия $s_x \in S_M$, такая, что $user_M(s_x) = x'$ и выполняется условие $(y, \alpha) \in de\_facto\_rights_M(s_x)$, где $\alpha \in \{write_r, append_r\}$. Если $\alpha = write_r$, то положим

$op_{M+1} = access\_write(s_x, y)$;

$N = M + 1$.

Если $\alpha = append_r$, то положим

$op_{M+1} = access\_append(s_x, y)$;

$N = M + 1$.

Таким образом, существует $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$ — простая траектория без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и в состоянии G_N выполняется условие $(s_x, y, write_m) \in F_N$, где $user_M(s_x) = x$, либо $s_x = x$. Следовательно, по определению 9 предикат $simple\_can\_write\_memory(x, y, G_0)$ является истинным.

В третьем случае: $y \in N_U \cup S_0$, $x \in E_0 \setminus S_0$ и истинен предикат $simple\_can\_share((x, read_r), y', G_0)$, где верно следующее:

— если $y \in N_U$, то $y' = y$;

— если $y \in S_0$, то $y' = user_0(y)$,

истинность предиката $simple\_can\_write\_memory(x, y, G_0)$ обосновывается аналогично второму случаю.

Четвертый случай: $x \in N_U \cup (N_S \cap S_0)$, $y \in N_U \cup S_0$ и истинен $simple\_can\_access\_own(x', y, G_0)$, где верно следующее:

— если $x \in N_U$, то $x' = x$;

— если $x \in N_S \cap S_0$, то $x' = user_0(x)$.

Тогда по определению 3 существуют состояния $G_1, \ldots, G_M$ и правила преобразования состояний $op_1, \ldots, op_M$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_M} G_M$, где $M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существуют субъект-сессии $s_x, s_y \in S_M$, такие, что $user_M(s_x) = x'$, или $s_y = y$, или $user_M(s_y) = y$ и выполняется условие $(s_x, s_y, own_a) \in A_M$.

Если $s_y \in L_S \cap S_M$, то по предположению 2 существуют роль $r \in roles_M(s_y)$ и сущность $e \in E_M$, такие, что $\{(e, read_r), (e, write_r)\} \subset PA_M(r)$. Положим

$op_{M+1} = access\_write(s_y, e)$;

$op_{M+2} = take\_flow(s_x, s_y)$;

$op_{M+3} = post(s_x, e, s_y)$;

$N = M + 3$.

Если $s_y \in N_S \cap S_M$, то по предположению 2 существуют роль $r \in UA_M(user_M(s_y))$ и сущность $e \in E_M$, такие, что $\{(e, read_r), (e, write_r)\} \subset PA_M(r)$. Положим

$op_{M+1} = take\_role(s_y, r)$;

$op_{M+2} = access\_write(s_y, e)$;

$op_{M+3} = take\_flow(s_x, s_y)$;

$op_{M+4} = post(s_x, e, s_y)$;

$N = M + 4$.

Таким образом, существует $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$ — простая траектория без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и в состоянии G_N выполняется условие $(s_x, s_y, write_m) \in F_N$, где верно следующее:

— или $s_x = x$, или $user_M(s_x) = x$;
— или $s_y = y$, или $user_N(s_y) = y$.

Следовательно, по определению 9 предикат $simple\_can\_write\_memory(x, y, G_0)$ является истинным.

В пятом случае: $y \in N_U \cup (N_S \cap S_0)$, $x \in N_U \cup S_0$ и истинен $simple\_can\_access\_own(y', x, G_0)$, где верно следующее:

— если $y \in N_U$, то $y' = y$;
— если $y \in N_S \cap S_0$, то $y' = user_0(y)$,

истинность предиката $simple\_can\_write\_memory(x, y, G_0)$ обосновывается аналогично четвертому случаю.

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

По условию теоремы существует последовательность недоверенных пользователей или сущностей $e_1, \ldots, e_m \in N_U \cup E_0$, где $e_1 = x$, $e_m = y$, таких, что выполняется условие 2. Возможны четыре случая.

Первый случай: $x \in N_U \cup S_0$, $e_{m-1} \in N_U \cup S_0$. Тогда по предположению индукции истинны предикаты $simple\_can\_write\_memory(x, e_{m-1}, G_0)$ и $simple\_can\_write\_memory(e_{m-1}, y, G_0)$, и по определению 9 существуют состояния $G_1, \ldots, G_M$ и правила преобразования состояний $op_1, \ldots, op_M$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_M} G_M$, где $M \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и выполняется условие $(x', e'_{m-1}, write_m) \in F_M$ и $(e'_{m-1}, y', write_m) \in F_M$, где выполняются условия:

— если $x \in S_0$, то $x' = x$; если $x \in N_U$, то $x' \in S_M$ и $user_M(x') = x$;
— если $e_{m-1} \in S_0$, то $e'_{m-1} = e_{m-1}$; если $e'_{m-1} \in N_U$, то $e'_{m-1} \in S_M$ и $user_M(e'_{m-1}) = e_{m-1}$;
— если $y \in E_0$, то $y' = y$; если $y \in N_U$, то $y' \in S_M$ и $user_M(y') = y$.

Положим

$op_{M+1} = find(x', e'_{m-1}, y')$;

$N = M + 1$.

Таким образом, существует $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$ — простая траектория без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и в состоянии G_N выполняется условие $(x', y', write_m) \in F_N$. Следовательно, по определению 9 предикат $simple\_can\_write\_memory(x, y, G_0)$ является истинным.

Второй случай: $x \in N_U \cup S_0$, $e_{m-1} \in E_0 \setminus S_0$. Тогда по предположению индукции истинен предикат $simple\_can\_write\_memory(x, e_{m-1}, G_0)$ и по определению 9 существуют состояния $G_1, \ldots, G_K$ и правила преобразования состояний $op_1, \ldots, op_K$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_K} G_K$, где $K \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и выполняется условие $(x', e'_{m-1}, write_m) \in F_K$, где, если $x \in S_0$, то $x' = x$; если $x \in N_U$, то $x' \in S_K$ и $user_K(x') = x$.

Кроме того, по условию теоремы $y \in N_U \cup S_0$ и выполняется одно из условий:

— $y \in S_0$ и $(e_{m-1}, read_r) \in PA_0(roles_0(y))$;
— $y \in N_U$ и истинен предикат $simple\_can\_share((e_{m-1}, read_r), y, G_0)$;
— $y \in N_S \cap S_0$ и истинен предикат $simple\_can\_share((e_{m-1}, read_r), user_0(y), G_0)$.

При выполнении первого условия положим $y' = y$ и $M = K$. При выполнении второго или третьего условия по определению 8 существуют состояния $G_{K+1}, \ldots, G_M$ и правила преобразования состояний $op_{K+1}, \ldots, op_M$, такие, что $G_K \vdash_{op_{K+1}} G_{K+1} \vdash_{op_{K+2}}$

$\ldots \vdash_{op_M} G_M$, где $M \geqslant K$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и существует субъект-сессия $y' \in S_M$, такая, что или $y' = y$, или $user_M(y') = y$, и выполняется условие $(e_{m-1}, read_r) \in de\_facto\_rights_M(y')$. Положим

$op_{M+1} = post(x', e'_{m-1}, y')$;

$N = M + 1$.

Таким образом, существует $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$ — простая траектория без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и в состоянии G_N выполняется условие $(x', y', write_m) \in F_N$. Следовательно, по определению 9 предикат $simple\_can\_write\_memory(x, y, G_0)$ является истинным.

Индуктивный шаг в третьем случае: $x \in E_0 \setminus S_0$, $e_{m-1} \in N_U \cup S_0$, обосновывается аналогично второму случаю.

Четвертый случай: $x, e_{m-1} \in E_0 \setminus S_0$. Тогда по условию теоремы $m \geqslant 4$ и $e_{m-2}, y \in \in N_U \cup S_0$. Далее индуктивный шаг обосновывается аналогично второму случаю.

Таким образом, доказана достаточность выполнения условий теоремы для истинности предиката $simple\_can\_write\_memory(x, y, G_0)$.

Докажем необходимость выполнения условий теоремы для истинности предиката $simple\_can\_write\_memory(x, y, G_0)$. По определению 9 существуют состояния $G_1, \ldots, G_N$ и правила преобразования состояний $op_1, \ldots, op_N$, такие, что $G_0 \vdash_{op_1} \ldots \vdash_{op_N} G_N$, где $N \geqslant 0$, является простой траекторией без кооперации доверенных и недоверенных субъект-сессий для передачи прав доступа, и выполняется условие $(x', y', write_m) \in F_N$, где верно следующее:

— если $x \in E_0$, то $x' = x$; если $x \in N_U$, то $x' \in S_N$ и $user_N(x') = x$;
— если $y \in E_0$, то $y' = y$; если $y \in N_U$, то $y' \in S_N$ и $user_N(y') = y$.

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

Пусть $N = 0$, тогда $(x', y', write_m) \in F_0$ и выполнено условие 1 теоремы.

Пусть $N = 1$, тогда из минимальности N следует, что $x', y' \in E_0$, $(x', y', write_m) \notin F_0$ и $(x', y', write_m) \in F_1$. Возможны семь случаев.

Первый случай: $y' \in S_0$ и $op_1 = access\_read(y', x)$, где $x' = x \in E_0 \setminus S_0$. Тогда $(x, read_r) \in de\_facto\_rights_0(y')$ и по определению 8 истинен предикат $simple\_can\_share((x, read_r), user_0(y'), G_0)$. Положим $m = 2$. Следовательно, условие 2 теоремы выполнено.

Во втором случае: $x' \in S_0$ и $op_1 = access\_write(x', y)$, и третьем случае: $x' \in S_0$ и $op_1 = access\_append(x', y)$, где $y' = y \in E_0 \setminus S_0$, выполнение условий теоремы обосновывается аналогично первому случаю.

Четвертый случай: $x' \in S_0$ и существует субъект-сессия $e_2 \in S_0$, такая, что $op_1 = find(x', e_2, y')$. Тогда $(x', e_2, write_m) \in F_0$, и или $(e_2, y', write_m) \in F_0$, или $y' = y \in E_0 \setminus S_0$, $(y, \beta) \in de\_facto\_rights_0(e_2)$, где $\beta \in \{write_r, append_r\}$. Значит, либо $(e_2, y', write_m) \in F_0$, либо $y' = y \in E_0 \setminus S_0$, $(y, \beta) \in de\_facto\_rights_0(e_2)$ и по определению 8 истинен предикат $simple\_can\_share((y, \beta), user_0(e_2), G_0)$. Положим $m = 3$. Следовательно, условие 2 теоремы выполнено.

В пятом случае: существует субъект-сессия $e_2 \in S_0$, такая, что $op_1 = pass(x', e_2, y')$, и шестом случае: $x', y' \in S_0$ и существует сущность $e_2 \in E_0$, такая, что $op_1 = post(x', e_2, y')$, выполнение условий теоремы обосновывается аналогично четвертому случаю.

Седьмой случай: $x' \in N_S \cap S_0$ и существует субъект-сессия $e_2 \in S_0$, такая, что $op_1 = take\_flow(x', e_2)$. Тогда $(x', e_2, own_a) \in A_0$ и $(e_2, y', write_m) \in F_0$. Следовательно, по определению 3 истинен предикат $simple\_can\_access\_own(user_0(x'), e_2, G_0)$. Положим $m = 3$. Следовательно, условие 2 теоремы выполнено.

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

Из минимальности N следует, что выполняется условие $(x', y', write_m) \notin F_{N-1}$. Возможны семь случаев.

Первый случай: $y' \in S_{N-1}$ и $op_N = access\_read(y', x)$, где $x' = x \in E_0 \setminus S_0$. Тогда $(x, read_r) \in de\_facto\_rights_{N-1}(y')$. Если $y' \in L_S \cap S_{N-1}$, то по предположению 1 выполняются условия $y = y' \in L_S \cap S_0$ и по определению 8 истинен предикат $simple\_can\_share((x, read_r), user_0(y), G_0)$. Если $y' \in N_S \cap S_{N-1}$, то либо $y = user_{N-1}(y')$ и по определению 8 истинен предикат $simple\_can\_share((x, read_r), y, G_0)$, либо $y = y' \in N_S \cap S_0$ и по определению 8 истинен предикат $simple\_can\_share((x, read_r), user_0(y), G_0)$. Положим $m = 2$. Следовательно, условие 2 теоремы выполнено.

Во втором случае: $x' \in S_{N-1}$ и $op_N = access\_write(x', y)$, и третьем случае: $x' \in S_{N-1}$ и $op_N = access\_append(x', y)$, где $y' = y \in E_0 \setminus S_0$, выполнение условий теоремы обосновывается аналогично первому случаю.

Четвертый случай: $x' \in S_{N-1}$ и существует субъект-сессия $s' \in S_{N-1}$, такая, что $op_N = find(x', s', y')$. Тогда $(x', s', write_m) \in F_{N-1}$, и или $(s', y', write_m) \in F_{N-1}$, или $y' = y \in E_0 \setminus S_0$, $(y, \beta) \in de\_facto\_rights_{N-1}(s')$, где $\beta \in \{write_r, append_r\}$.

Так как $(x', s', write_m) \in F_{N-1}$, то истинен предикат $simple\_can\_write\_memory(x, s, G_0)$ с длиной траектории меньше N, где либо $s = s' \in S_0$, либо $s = user_{N-1}(s') \in N_U$. По предположению индукции существует последовательность недоверенных пользователей или сущностей $e_1, \ldots, e_k \in N_U \cup E_0$, где $e_1 = x$, $e_k = s$ и $k \geqslant 2$, удовлетворяющих условию 1 или 2 теоремы.

Если $(s', y', write_m) \in F_{N-1}$, то аналогично существует последовательность недоверенных пользователей или сущностей $e_k, \ldots, e_m \in N_U \cup E_0$, где $e_k = s$, $e_m = y$ и $m - k \geqslant 1$, удовлетворяющих условию 1 или 2 теоремы, где либо $s = s' \in S_0$, либо $s = user_{N-1}(s') \in N_U$.

Если $y' = y \in E_0 \setminus S_0$, $(y, \beta) \in de\_facto\_rights_{N-1}(s')$, где $\beta \in \{write_r, append_r\}$, то по определению 8 истинен предикат $simple\_can\_share((y, \beta), s, G_0)$, где $s = user_{N-1}(s')$. Положим $m = k + 1$, $e_m = y$.

Таким образом, в четвертом случае существует последовательность недоверенных пользователей или сущностей $e_1, \ldots, e_m \in N_U \cup E_0$, где $e_1 = x$, $e_m = y$ и $m \geqslant 2$, удовлетворяющих условию 2 теоремы.

В пятом случае: существует субъект-сессия $s' \in S_{N-1}$, такая, что $op_N = pass(x', s', y')$, выполнение условий теоремы обосновывается аналогично четвертому случаю.

Шестой случай: $x', y' \in S_{N-1}$ и существует сущность $e \in E_{N-1}$, такая, что $op_N = post(x', e, y')$. Из минимальности N и предположения 2 следует, что $e \in E_0$. Значит, выполнение условий теоремы обосновывается аналогично четвертому случаю.

Седьмой случай: $x' \in N_S \cap S_{N-1}$ и существует субъект-сессия $s' \in S_{N-1}$, такая, что $op_N = take\_flow(x', s')$. Тогда $(x', s', own_a) \in A_{N-1}$ и $(s', y', write_m) \in F_{N-1}$. Если $s' \in S_0$, то положим $s = s'$; если $s' \notin S_0$, то положим $s = user_{N-1}(s') \in N_U$. Следовательно, либо $x = user_{N-1}(x')$ и по определению 3 истинен предикат $simple\_can\_access\_own(x, s, G_0)$, либо $x = x' \in N_S \cap S_0$ и по определению 3 исти-

нен предикат $simple\_can\_access\_own(user_0(x), s, G_0)$. Далее обоснование выполнения условий теоремы осуществляется аналогично четвертому случаю.

Значит, доказан шаг индукции при длине траектории, равной N. Доказательство необходимости выполнения условия теоремы для истинности предиката $simple\_can\_write\_memory(x, y, G_0)$ выполнено.

Теорема доказана. ■

Таким образом, в рамках БР ДП-модели для систем с простыми траекториями функционирования обоснованы необходимые и достаточные условия передачи прав доступа или реализации информационных потоков по памяти. В дальнейшем с применением техники доказательства теорем 1–4 планируется описать и обосновать условия передачи прав доступа, реализации информационных потоков по памяти и по времени для произвольных траекторий функционирования систем.

ЛИТЕРАТУРА

1. *Девянин П. Н.* Базовая ролевая ДП-модель // Прикладная дискретная математика. 2008. № 1(1). С. 64–70.
2. *Девянин П. Н.* Анализ условий получения доступа владения в рамках базовой ролевой ДП-модели без информационных потоков по памяти // Прикладная дискретная математика. 2009. № 3(5). С. 69–84.