

Библиографический список

1. Parzen, E. On estimation of a probability density function and mode / E. Parzen // Ann. Math. Statistic. 1962. Vol. 33. P. 1065–1076.

2. Епанечников, В. А. Непараметрическая оценка многомерной плотности вероятности / В. А. Епанечников // Теория вероятности и ее применения. 1969. Вып. 1. Т. 14. С. 156–161.

V. A. Lapko, S. S. Varochkin, I. A. Egorochkin

DEVELOPMENT AND RESEARCH OF NONPARAMETRIC ESTIMATION OF PROBABILITY DENSITY BASED ON THE PRINCIPLE OF TRAINING SAMPLE DECOMPOSITION ACCORDING TO ITS VOLUME

The two-level nonparametric estimation of probability density based on the principle of decomposition of training sample according to its volume is offered. This estimation is characterized by high computing efficiency due to the opportunity of parallel computing technologies use. The results of computing experiments are given.

Keywords: estimation of density probability, the big samples, asymptotic properties, research of the properties, parallel computing technologies.

УДК 004.94

Д. Н. Колегов

ДП-МОДЕЛЬ КОМПЬЮТЕРНОЙ СИСТЕМЫ С ФУНКЦИОНАЛЬНО И ПАРАМЕТРИЧЕСКИ АССОЦИИРОВАННЫМИ С СУБЪЕКТАМИ СУЩНОСТЯМИ

Вводится понятие параметрически-ассоциированной с субъектом сущности в компьютерной системе (КС) и строится расширение ФАС ДП-модели КС, охватывающее такие сущности. Формулируются и обосновываются условия получения недоверенным субъектом права доступа владения к другому субъекту в этом расширении.

Ключевые слова: компьютерная безопасность, математические модели безопасности, дискреционные модели, анализ безопасности, права доступа, информационные потоки.

Анализ безопасности компьютерных систем является одной из актуальных проблем теории компьютерной безопасности. Данная проблема возникает в связи с необходимостью использования формальных (математических) моделей для проведения оценки безопасности КС на соответствие функциональным требованиям, критериям, политикам или стандартам безопасности. Причем для разработки КС с высоким уровнем доверия к их безопасности использование математических моделей является обязательным.

Для анализа безопасности КС используются формальные модели, позволяющие анализировать условия передачи прав доступа и реализации информационных потоков в КС. Одной из таких современных моделей КС с дискреционным управлением доступа является ДП-модель с ее расширениями [1].

Дальнейшее изложение будет опираться на работу [1] с учетом всех определений, обозначений и теорем в ней.

Сущность называется функционально-ассоциированной с субъектом, если она определяет вид преобразования данных, выполняемого этим субъектом. В ДП-моделях с функционально-ассоциированными с субъектами сущностями (ФАС ДП-моделях) анализируется ситуация, когда реализация информационного потока по памяти к сущности, функционально-ассоциированной с субъек-

том, приводит к изменению вида преобразования данных, реализуемого этим субъектом.

В то же время в современных КС возможна реализация информационного потока по памяти от сущности, позволяющая получить права доступа различных субъектов КС, в том числе и доверенных. Такие сущности являются параметрически-ассоциированными с субъектами КС. Например, получение субъектом-нарушителем доступа на чтение к конфигурационному файлу или реестру, в котором хранится пароль или хэш-значение пароля субъекта КС, позволяет субъекту-нарушителю получить право доступа владения к последнему субъекту.

Кроме того, в настоящее время дополнительно к классическим угрозам нарушения конфиденциальности, целостности и доступности информации рассматривают угрозу раскрытия параметров КС – возможность идентификации параметров, функций безопасности и свойств КС, знание которых позволяет реализовать нарушение безопасности [2]. Например, чтение сообщения, выдаваемого субъектом-процессом при подключении к нему, позволяет нарушителю идентифицировать программное обеспечение (ПО), реализующее данный субъект-процесс КС, и получить права доступа последнего, используя известные уязвимые места в ПО.

Таким образом, для обеспечения возможности анализа получения субъектом права доступа владения к другому субъекту с использованием информационного потока от сущности, параметрически-ассоциированной с последним, следует построить расширение ФАС ДП-модели, охватывающее информационные потоки указанного вида и отражающее возможность получения субъектом права доступа владения к другому субъекту в современных КС. Решение этой задачи и является целью данной работы. Для этого в работе вводится определение параметрически-ассоциированных сущностей с субъектами в КС, на их основе строится ДП-модель с функционально и параметрически ассоциированными с субъектами сущностями, которая является требуемым расширением ФАС ДП-модели, и в рамках этой модели формулируются и обосновываются необходимые и достаточные условия получения субъектом права доступа владения к другому субъекту.

ДП-модель с функционально и параметрически ассоциированными с субъектами сущностями. *Определение 1.* Пусть $G = (S, E, R \cup A \cup F, H)$ – состояние КС $\Sigma(G^*, OP)$. Сущность $e \in E$ будем называть *параметрически-ассоциированной* с субъектом $s \in S$ в состоянии G , если чтение данных в сущности e субъектом $z \in S$ позволяет ему получить право владения к субъекту s в этом или последующих состояниях КС.

Замечание 1. Сущность $e \in E$, параметрически-ассоциированная с субъектом $s \in S$, содержит аргументы операций преобразования данных, выполняемого субъектом s в этом или последующих состояниях.

Замечание 2. В множество сущностей, параметрически-ассоциированных с субъектом $s \in S$, могут входить сущности, на которые субъект s не имеет прав доступа. Например, сущность-пароль, параметрически-ассоциированная с недоверенным субъектом-пользователем в операционной системе (ОС) семейства GNU/Linux, хранится в файле, правами доступа к которому могут обладать только доверенные субъекты-процессы данной ОС. Кроме того, возможно создание субъектов ОС, которые препятствовали бы доступу субъектов к некоторым критичным сущностям КС, несмотря на наличие необходимых прав доступа данных субъектов к этим сущностям [3].

Замечание 3. Существуют сущности, параметрически-ассоциированные с субъектом, которые не являются функционально-ассоциированными с ним. Примером такой сущности является раздел реестра ОС семейства Windows 2000/XP/2003, содержащий информацию об установленных обновлениях ОС узла. Также существуют сущности, параметрически-ассоциированные с субъектом, которые являются функционально-ассоциированными с ним. Так, зная идентификатор сессии пользователя веб-приложения, возможно получить его права доступа; с другой стороны, удаление данного идентификатора приводит к закрытию сессии пользователя.

С учетом того, что доверенные субъекты не участвуют в реализации информационных потоков по времени и в современных КС, как правило, реализация информационного потока по времени от сущности, параметрически-ассоциированной с субъектом, не приводит к получению другим субъектом права доступа владения к перво-

му, будем считать, что в КС выполняется следующее предположение.

Предположение 1. Только информационный поток по памяти от сущности, параметрически-ассоциированной с субъектом, приводит к получению другим субъектом права доступа владения к первому субъекту. Множество сущностей, параметрически-ассоциированных с субъектом, не изменяется в процессе функционирования системы.

Через $s[s \subset E]$ обозначим множество всех сущностей, параметрически-ассоциированных с субъектом s . При этом будем считать, что $s \in s[s]$.

Наличие у субъекта данных о параметрах функционирования другого субъекта КС может позволить получить первому субъекту право доступа владения ко второму субъекту. При этом первому субъекту необходимо иметь возможность реализовать информационный поток по памяти к некоторому субъекту, позволяющему получить права доступа ко второму субъекту. Например, при получении субъектом-нарушителем пароля доверенного субъекта, первому необходимо иметь возможность записи пароля в сущность-интерфейс КС. Таким образом, будем считать, что в КС выполняется следующее предположение.

Предположение 2. Если субъект реализовал информационный поток по памяти от сущности, параметрически-ассоциированной с другим субъектом, к себе, то первый субъект получает право доступа владения ко второму субъекту.

В соответствии с данными предположениями модифицируем определение ФАС ДП-модели для возможности анализа условий получения субъектом права доступа владения к другому субъекту с использованием реализации информационного потока по памяти от сущности, параметрически-ассоциированной с последним субъектом. Модифицированную ФАС ДП-модель будем называть *ДП-моделью с функционально и параметрически ассоциированными с субъектами сущностями*, или *ФПАС ДП-моделью*. Модификация состоит в добавлении к правилам преобразования состояний ФАС ДП-модели правила – $know(x, y, z)$, определяемого в следующей таблице: аргументом операции является состояние G , значением – состояние G' , параметрами – сущности x, y, z (см. таблицу).

Замечание 2. Правило $know(x, y, z)$ является монотонным, т. е. применение данного правила не приводит к удалению ребер или вершин из графа доступа.

Анализ условий получения субъектом права доступа владения к другому субъекту. Сформулируем и обоснуем условия получения субъектом права доступа владения own , к другому субъекту для случая, когда в КС $\Sigma(G^*, OP)$ используется правило преобразования состояний $know(x, y, z)$.

Определение 2. Траекторию функционирования КС $\Sigma(G^*, OP)$ будем называть *траекторией без кооперации доверенных и недоверенных субъектов для передачи прав доступа*, если при ее реализации используются монотонные правила преобразования состояний, и доверенные субъекты:

– не дают недоверенным субъектам права доступа к сущностям;

– не берут у недоверенных субъектов права доступа к сущностям;

– используя информационные потоки по памяти к сущностям, не получают право доступа владения к субъектам;

– используя информационные потоки по памяти от сущностей, не получают право доступа владения к субъектам.

Таким образом, в КС $\Sigma(G^*, OP)$ на траекториях без кооперации доверенных и недоверенных субъектов для передачи прав доступа доверенные субъекты:

– не инициируют выполнения следующих правил преобразования состояний: $take_right(\alpha_r, u, x, e)$, $grant_right(\alpha_r, u, x, e)$, $control(u, y, z)$, $know(u, y, z)$;

– доверенные субъекты могут выполнять монотонные правила преобразования состояний: $own_take(\alpha_r, u, e)$, $create_entity(u, e, e')$, $create_subject(u, e, e')$, $rename_entity(u, e, e')$, $access_read(u, e)$, $access_write(u, e)$, $access_append(u, e)$, $find(u, e, e')$, $post(u, e, e')$, $pass(u, e, e')$ с условиями и результатами применения в соответствии с правилами преобразования БК ДП-модели, где $u \in L_s$ – доверенный субъект; $x \in N_s$ – недоверенный субъект; y – субъект, что $z[y]$ или $z \in [y]$; z, e, e' – сущности; $\alpha_r \in R_r$ – право доступа.

Определение 3. Траекторию функционирования КС $\Sigma(G^*, OP)$ будем называть траекторией без кооперации доверенных и недоверенных субъектов для передачи прав доступа и реализации информационных потоков, если она является траекторией без кооперации доверенных и недоверенных субъектов для передачи прав доступа, и при ее реализации используются следующие правила преобразования состояний:

– $take_right(\alpha_r, x, y, z)$, $grant_right(\alpha_r, x, y, z)$, $own_take(\alpha_r, x, y)$ с условиями и результатами применения в соответствии с правилами преобразования базовой ДП-модели;

– $create_entity(x, y, z)$, $create_subject(x, y, z)$, $rename_entity(x, y, z)$, $access_read(x, y)$, $access_write(x, y)$, $access_append(x, y)$, $flow(x, y, z)$, $find(x, y, z)$, $post(x, y, z)$, $pass(x, y, z)$ с условиями и результатами применения в соответствии с правилами преобразования БК ДП-модели;

– $control(x, y, z)$, $know(x, y, z)$ с условиями и результатами применения в соответствии с правилами преобразования ФАС ДП-модели и таблицы.

Определение 4. Пусть имеются $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ – состояние системы $S(G^*, OP)$, недоверенный субъект $x \in N_s \cap S_0$ и субъект $y \in S_0$, где $x \neq y$. Определим предикат $can_share_own(x, y, G_0, L_s)$, который будет истинным тогда и только тогда, когда существуют состояния $G_1, \dots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \dots, op_N$ такие, что траектория $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \dots \vdash_{op_N} G_N$ является траекторией без кооперации доверенных и недоверенных субъектов для передачи прав доступа и реализации информационных потоков, и $(x, y, own_r) \in R_N$, где $N \geq 0$.

Определение 5. Пусть имеются $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ – состояние системы $S(G^*, OP)$, недоверенный субъект $x \in N_s \cap S_0$ и субъект $y \in S_0$, где $x \neq y$. Определим предикат $directly_can_share_own(x, y, G_0, L_s)$, который будет истинным тогда и только тогда, когда существует последовательность субъектов $s_1, \dots, s_m \in S_0$, где $s_1 = x$, $s_m = y$ и $m \geq 2$, таких, что для каждого $i = 1, \dots, m-1$ выполняется одно из условий:

(1) $s_i \in N_s \cap S_0$, $s_i \in [s_{i+1}]$ или $s_i \in [s_{i+1}]$;

(2) истинен предикат $can_share(own_r, s_i, s_{i+1}, G_0, L_s)$;

(3) существует сущность $e \in [s_{i+1}]$ такая, что истинен предикат $can_write_memory(s_i, e, G_0, L_s)$;

(4) существует сущность $e \in [s_{i+1}]$ такая, что истинен предикат $can_write_memory(e, s_i, G_0, L_s)$.

Лемма. Пусть имеется $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ – состояние системы $S(G^*, OP)$, недоверенный субъект $x \in N_s \cap S_0$ и субъект $y \in S_0$, где $x \neq y$ и истинен предикат $directly_can_share_own(x, y, G_0, L_s)$. Тогда истинен предикат $can_share_own(x, y, G_0, L_s)$.

Доказательство. Пусть истинен предикат $directly_can_share_own(x, y, G_0, L_s)$, тогда по определению 5 существует последовательность субъектов $s_1, \dots, s_m \in S_0$, где $s_1 = x$, $s_m = y$ и $m \geq 2$, таких, что для каждого $i = 1, \dots, m-1$ выполняется одно из условий (1)–(4). Докажем, что для такой последовательности $s_1, \dots, s_m$ предикат $can_share_own(x, y, G_0, L_s)$ является истинным.

Проведем доказательство этого утверждения индукцией по длине m .

Пусть $m = 2$, тогда возможно четыре случая.

Первый случай: $x \in N_s \cap S_0$, $x \in [y]$ или $x \in [y]$. Если $x \in [y]$, то пусть $op_1 = control(x, y, x)$. Тогда $G_0 \vdash_{op_1} G_1$, $(x, y, own_r) \in R_1$ и предикат $can_share_own(x, y, G_0, L_s)$ истинен. Если $x \in [y]$, то пусть $op_1 = know(x, y, x)$. Тогда $G_0 \vdash_{op_1} G_1$ и $(x, y, own_r) \in R_1$ и предикат $can_share_own(x, y, G_0, L_s)$ также истинен.

Во втором случае истинен предикат $can_share(own_r, x, y, G_0, L_s)$. Следовательно, истинен предикат $can_share_own(x, y, G_0, L_s)$.

В третьем случае имеется $x \in N_s \cap S_0$, существует сущность $e \in [y]$ и истинен предикат $can_write_memory(x, e, G_0, L_s)$. Пусть $op_1 = control(x, y, e)$, тогда $G_0 \vdash_{op_1} G_1$, $(x, y, own_r) \in R_1$ и предикат $can_share_own(x, y, G_0, L_s)$ истинен.

В четвертом случае имеется $x \in N_s \cap S_0$, существует сущность $e \in [y]$ и истинен предикат $can_write_memory(e, x, G_0, L_s)$. Пусть $op_1 = know(x, y, e)$, тогда $G_0 \vdash_{op_1} G_1$, $(x, y, own_r) \in R_1$ и предикат $can_share_own(x, y, G_0, L_s)$ истинен.

Докажем индуктивный шаг. Пусть $m > 2$ и доказываемое утверждение верно для всех последовательностей субъектов длины $k < m$. Докажем, что оно верно и для всех таких последовательностей длины m .

Рассмотрим последовательность субъектов $s_1, \dots, s_m \in S_0$, где $s_1 = x$, $s_2 = z$ и $s_m = y$. Пусть $z \in N_s \cap S_0$. Тогда по предположению индукции существуют правила преобразования состояний $op_1, \dots, op_N$ такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \dots \vdash_{op_N} G_N$ и $(z, y, own_r) \in R_N$, где $N \geq 0$.

Условия и результаты применения правила $know(x, y, z)$ ФПАС ДП-модели

Правило	Исходное состояние $G = (S, E, R \cup A \cup F, H)$	Результирующее состояние $G' = (S', E', R' \cup A' \cup F', H')$
$know(x, y, z)$	$x, y \in S, z \in E, z \in [y]$ или $x = z$, или $(z, x, write_m) \in F$	$S' = S, E' = E, A' = A, H' = H$, $F' = F, R' = R \cup \{(x, y, own_r)\}$

$\dots \vdash_{opN} G_N$ и верно, что $(x, z, own_p), (z, y, own_p) \in R_N$, где $N \geq 0$. Положим $op_{N+1} = take_right(own_p, x, z, y)$. Тогда $G_{N+1} = (S_{N+1}, E_{N+1}, R_{N+1} \cup A_{N+1} \cup F_{N+1}, H_{N+1})$ и $(x, y, own_p) \in R_{N+1}$, следовательно, предикат $can_share_own(x, y, G_0, L_S)$ истинен.

Если $z \in L_S \cap S_0$, то $(z, y, own_p) \in R_0$, и по предположению индукции предикат $can_share_own(x, z, G_0, L_S)$ истинен. Следовательно, существуют правила преобразования состояний $op_1, \dots, op_N$ такие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \dots \vdash_{opN} G_N$, и $(x, z, own_p) \in R_N$, где $N \geq 0$. Аналогично получаем истинность предиката $can_share_own(x, y, G_0, L_S)$. Лемма доказана.

Теорема. Пусть имеются $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ – состояние системы $S(G^*, OP)$ и право доступа владения $(x, y, own_p) \in N_p$, где $x \in N_S \cap S_0, y \in S_0$ и $x \neq y$. Тогда предикат $can_share_own(x, y, G_0, L_S)$ является истинным, если и только если существует последовательность субъектов $s_1, \dots, s_m$ в S_0 , где $s_1 = x, s_m = y$ и $m \geq 2$, таких, что выполняется одно из следующих условий.

Условие 1. $m = 2$ и истинен предикат $directly_can_share_own(x, y, G_0, L_S)$.

Условие 2. $m > 2$ и для каждого $i = 1, \dots, m - 2$ выполняется одно из условий:

- $s_i, s_{i+1} \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(s_i, s_{i+1}, G_0, L_S)$, $directly_can_share_own(s_{i+1}, s_{i+2}, G_0, L_S)$;

- $i < m - 2, s_i, s_{i+2} \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(s_i, s_{i+1}, G_0, L_S)$, $directly_can_share_own(s_{i+1}, s_{i+2}, G_0, L_S)$;

- $i < m - 2, s_{i+1}, s_{i+2} \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(s_{i+1}, s_i, G_0, L_S)$, $directly_can_share_own(s_{i+1}, s_{i+2}, G_0, L_S)$;

- $s_{i+1} \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(s_{i+1}, s_i, G_0, L_S)$, $directly_can_share_own(s_{i+1}, s_{i+2}, G_0, L_S)$.

Доказательство.

Докажем достаточность выполнения условий теоремы для истинности предиката $can_share_own(x, y, G_0, L_S)$.

Если выполнено первое условие теоремы, то в соответствии с леммой предикат $can_share_own(x, y, G_0, L_S)$ является истинным.

Если выполнено второе условие теоремы, то существует последовательность субъектов $s_1, \dots, s_m$ в S_0 , где $s_1 = x, s_m = y$ и $m > 2$. Проведем доказательство индукцией по длине m последовательности субъектов.

Пусть $m = 3$. Возможны два случая.

Первый случай: $x, s_2 \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(x, s_2, G_0, L_S)$, $directly_can_share_own(s_2, y, G_0, L_S)$. Тогда в соответствии с леммой существуют состояния $G_1, \dots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \dots, op_N$ такие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \dots \vdash_{opN} G_N$ и $(x, s_2, own_p), (s_2, y, own_p) \in R_N$, где $N \geq 0$. Пусть $op_{N+1} = take_right(own_p, x, s_2, y)$ и $G_{N+1} = (S_{N+1}, E_{N+1}, R_{N+1} \cup A_{N+1} \cup F_{N+1}, H_{N+1})$. Тогда $(x, y, own_p) \in R_{N+1}$ и предикат $can_share_own(x, y, G_0, L_S)$ являются истинными.

Второй случай: $s_2 \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(s_2, x, G_0, L_S)$, $directly_can_share_own(s_2, y, G_0, L_S)$. Тогда в соответствии с леммой существуют состояния $G_1, \dots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \dots, op_N$ та-

кие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \dots \vdash_{opN} G_N$ и $(s_2, x, own_p), (s_2, y, own_p) \in R_N$, где $N \geq 0$. Пусть $op_{N+1} = grant_right(own_p, s_2, x, y)$ и $G_{N+1} = (S_{N+1}, E_{N+1}, R_{N+1} \cup A_{N+1} \cup F_{N+1}, H_{N+1})$. Тогда право $(x, y, own_p) \in R_{N+1}$ и предикат $can_share_own(x, y, G_0, L_S)$ являются истинными.

Докажем индуктивный шаг. Пусть $m > 3$ и утверждение верно для всех последовательностей субъектов длины $k < m$. Докажем, что утверждение верно для всех таких последовательностей длины m .

Пусть $s_1, \dots, s_m$ последовательность субъектов из S_0 субъектов, где $s_1 = x, s_2 = z, s_3 = w$ и $s_m = y$.

Возможно четыре случая.

Первый случай: $x, z \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(x, z, G_0, L_S)$, $directly_can_share_own(z, w, G_0, L_S)$. Тогда в соответствии с леммой существуют состояния $G_1, \dots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \dots, op_N$ такие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \dots \vdash_{opN} G_N$ и $(x, z, own_p), (z, w, own_p) \in R_N$, где $N \geq 0$. По предположению индукции существуют состояния $G_{N+1}, \dots, G_{N+K} = (S_{N+K}, E_{N+K}, R_{N+K} \cup A_{N+K} \cup F_{N+K}, H_{N+K})$ и правила преобразования состояний $op_{N+1}, \dots, op_{N+K}$ такие, что $G_{N+1} \vdash_{op(N+1)} G_{N+2} \vdash_{op(N+2)} \dots \vdash_{op(N+K)} G_{N+K}$ и $(w, y, own_p) \in R_{N+K}$, где $K \geq 0$. Положим $op_{N+K+1} = take_right(own_p, x, z, w)$, $op_{N+K+2} = take_right(own_p, x, w, y)$. Тогда $G_{N+K+1} \vdash_{op(N+K+1)} G_{N+K+2} \vdash_{op(N+K+2)} G_{N+K+2} = (S_{N+K+2}, E_{N+K+2}, R_{N+K+2} \cup A_{N+K+2} \cup F_{N+K+2}, H_{N+K+2})$ и право $(x, y, own_p) \in R_{N+K+2}$. Следовательно, предикат $can_share_own(x, y, G_0, L_S)$ истинен.

Второй случай: $x, w \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(x, z, G_0, L_S)$, $directly_can_share_own(w, z, G_0, L_S)$. Тогда в соответствии с леммой существуют состояния $G_1, \dots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \dots, op_N$ такие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \dots \vdash_{opN} G_N$ и права $(x, z, own_p), (w, z, own_p) \in R_N$, где $N \geq 0$. По предположению индукции существуют состояния $G_{N+1}, \dots, G_{N+K} = (S_{N+K}, E_{N+K}, R_{N+K} \cup A_{N+K} \cup F_{N+K}, H_{N+K})$ и правила преобразования состояний $op_{N+1}, \dots, op_{N+K}$ такие, что $G_{N+1} \vdash_{op(N+1)} G_{N+2} \vdash_{op(N+2)} \dots \vdash_{op(N+K)} G_{N+K}$ и $(w, y, own_p) \in R_{N+K}$, где $K \geq 0$. Положим $op_{N+K+1} = grant_right(own_p, w, z, y)$, $op_{N+K+2} = take_right(own_p, x, z, y)$. Тогда $G_{N+K+1} \vdash_{op(N+K+1)} G_{N+K+2} \vdash_{op(N+K+2)} G_{N+K+2} = (S_{N+K+2}, E_{N+K+2}, R_{N+K+2} \cup A_{N+K+2} \cup F_{N+K+2}, H_{N+K+2})$ и $(x, y, own_p) \in R_{N+K+2}$. Следовательно, предикат $can_share_own(x, y, G_0, L_S)$ истинен.

Третий случай: $w, z \in N_S \cap S_0$ и истинны предикаты $directly_can_share_own(z, x, G_0, L_S)$, $directly_can_share_own(w, z, G_0, L_S)$. Тогда в соответствии с леммой существуют состояния $G_1, \dots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \dots, op_N$ такие, что $G_0 \vdash_{op1} G_1 \vdash_{op2} \dots \vdash_{opN} G_N$ и $(z, x, own_p), (w, z, own_p) \in R_N$, где $N \geq 0$. По предположению индукции существуют состояния $G_{N+1}, \dots, G_{N+K} = (S_{N+K}, E_{N+K}, R_{N+K} \cup A_{N+K} \cup F_{N+K}, H_{N+K})$ и правила преобразования состояний $op_{N+1}, \dots, op_{N+K}$ такие, что $G_{N+1} \vdash_{op(N+1)} G_{N+2} \vdash_{op(N+2)} \dots \vdash_{op(N+K)} G_{N+K}$ и $(w, y, own_p) \in R_{N+K}$, где $K \geq 0$. Положим $op_{N+K+1} = grant_right(own_p, w, z, y)$, $op_{N+K+2} = grant_right(own_p, z, x, y)$.

Тогда $G_{N+K+1} \vdash_{op(N+K+1)} G_{N+K+2} \vdash_{op(N+K+2)} G_{N+K+2} = (S_{N+K+2}, E_{N+K+2}, R_{N+K+2} \cup A_{N+K+2} \cup F_{N+K+2}, H_{N+K+2})$ и $(x, y, own_p) \in R_{N+K+2}$. Следовательно, предикат $can_share_own(x, y, G_0, L_S)$ истинен.

Четвертый случай: $z \in N_s \cap S_0$ и истинны предикаты $directly_can_share_own(z, x, G_0, L_s)$, $directly_can_share_own(z, w, G_0, L_s)$. Тогда в соответствии с леммой существуют состояния $G_1, \dots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и правила преобразования состояний $op_1, \dots, op_N$ такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \dots \vdash_{op_N} G_N$ и $(z, x, own_p), (z, w, own_p) \in R_N$, где $N \geq 0$. По предположению индукции существуют состояния $G_{N+1}, \dots, G_{N+K} = (S_{N+K}, E_{N+K}, R_{N+K} \cup A_{N+K} \cup F_{N+K}, H_{N+K})$ и правила преобразования состояний $op_{N+1}, \dots, op_{N+K}$ такие, что $G_{N+1} \vdash_{op_{N+1}} G_{N+2} \vdash_{op_{N+2}} \dots \vdash_{op_{N+K}} G_{N+K}$ и $(w, y, own_p) \in R_{N+K}$, где $K \geq 0$. Положим $op_{N+K+1} = take_right(own_p, z, w, y)$, $op_{N+K+2} = grant_right(own_p, z, x, y)$. Тогда $G_{N+K} \vdash_{op_{N+K+1}} G_{N+K+1} \vdash_{op_{N+K+2}} G_{N+K+2} = (S_{N+K+2}, E_{N+K+2}, R_{N+K+2} \cup A_{N+K+2} \cup F_{N+K+2}, H_{N+K+2})$ и $(x, y, own_p) \in R_{N+K+2}$. Следовательно, предикат $can_share_own(x, y, G_0, L_s)$ истинен.

Индуктивный шаг доказан, и доказательство достаточности выполнения условий теоремы для истинности предиката $can_share_own(x, y, G_0, L_s)$ закончено.

Докажем необходимость выполнения условий теоремы для истинности этого предиката.

Пусть истинен предикат $can_share_own(x, y, G_0, L_s)$. Тогда по определению 4 существуют состояния $G_1, \dots, G_N = (S_N, E_N, R_N \cup A_N \cup F_N, H_N)$ и последовательности правил преобразования состояний $op_1, \dots, op_N$ такие, что $G_0 \vdash_{op_1} G_1 \vdash_{op_2} \dots \vdash_{op_N} G_N$ и $(x, y, own_p) \in R_N$, где $N \geq 0$. Выберем среди последовательностей правил преобразований ту, у которой длина N является минимальной. В этом случае $(x, y, own_p) \notin R_{N-1}$. Проведем доказательство индукцией по числу N .

Пусть $N = 0$, тогда $(x, y, own_p) \in R_0$ и условие 1 теоремы выполнено.

Пусть $N = 1$, тогда $x \in N_s \cap S_0$, $y \in S_0$, $(x, y, own_p) \notin R_0$ и существует правило преобразования состояний op_1 такое, что $G_0 \vdash_{op_1} G_1$ и $(x, y, own_p) \in R_1$. Из определения правил преобразования состояний в [1] и таблицы следует, что возможны шесть случаев:

- $x \in [y]$ и $op_1 = control(x, y, x)$;
- $x \in [y]$ и $op_1 = know(x, y, x)$;
- существует сущность $e \in [y]$ такая, что $(x, e, write_m) \in F_0$ и $op_1 = control(x, y, e)$;
- существует сущность $e \in [y]$ такая, что $(e, x, write_m) \in F_0$ и $op_1 = know(x, y, e)$;
- существует $z \in N_s \cap S_0$, что $(x, z, own_p), (z, z, own_p) \in R_0$ и $op_1 = take_right(own_p, x, z, y)$;
- существует $z \in N_s \cap S_0$, что $(z, x, own_p), (x, z, own_p) \in R_0$ и $op_1 = grant_right(own_p, z, x, y)$.

Все шесть случаев соответствуют условиям 1 и 2 теоремы.

Пусть $N > 1$ и утверждение теоремы верно для всех последовательностей правил преобразований состояний длины $l < N$. Тогда $x \in N_s \cap S_0$, $y \in S_0$, $(x, y, own_p) \notin R_{N-1}$ и существует правило преобразования состояний op_N такое, что $G_{N-1} \vdash_{op_N} G_N$ и $(x, y, own_p) \in R_N$.

Из определения правил преобразования состояний, предположений о том, что множество сущностей, функционально и параметрически ассоциированных с субъектом не меняется, и минимальности N следует, что выполняется хотя бы одно из условий:

- существует сущность $e \in [y]$ такая, что $(x, e, write_m) \in F_{N-1}$ и $op_N = control(x, y, e)$;

- существует сущность $e \in [y]$ такая, что $(e, x, write_m) \in F_{N-1}$ и $op_N = know(x, y, e)$;

- существует $z \in N_s \cap S_0$, что $(x, z, own_p), (z, y, own_p) \in R_{N-1}$ и $op_N = take_right(own_p, x, z, y)$;

- существует $z \in N_s \cap S_0$, что $(z, x, own_p), (z, y, own_p) \in R_{N-1}$ и $op_N = grant_right(own_p, z, x, y)$.

Если выполнено первое или второе условие, то выполнено первое условие теоремы.

Рассмотрим случай выполнения третьего условия, когда $(x, z, own_p), (z, y, own_p) \in R_{N-1}$ и $op_N = take_right(\alpha, x, z, y)$. Доказательство для случая выполнения четвертого условия проводится аналогично доказательству для случая выполнения третьего условия.

Так как длина N минимальна, то в последовательности преобразований состояний $op_1, \dots, op_N$ не используются правила вида $create_entity(x, y, z)$ и $create_subject(x, y, z)$. Следовательно, $z \in S_0$ и истинны предикаты $can_share_own(x, z, G_0, L_s)$ и $can_share_own(z, y, G_0, L_s)$ с длинами последовательностей преобразований состояний меньше N . По предположению индукции возможны четыре случая.

Первый случай: истинны предикаты $directly_can_share_own(x, z, G_0, L_s)$ и $directly_can_share_own(z, y, G_0, L_s)$, и, следовательно, второе условие теоремы выполнено.

Второй случай: истинен предикат $directly_can_share_own(x, z, G_0, L_s)$ и существует последовательность субъектов $s_1, \dots, s_m$ в S_0 , где $s_1 = z, s_m = y$ и $m \geq 2$ таких, что выполняется условие 2. Следовательно, существует последовательность субъектов $s_1, \dots, s_{m+1}$ в S_0 , где $s_1 = x, s_2 = z, s_{m+1} = y$ таких, что выполняется условие 2 теоремы.

Третий случай: истинен предикат $directly_can_share_own(z, y, G_0, L_s)$ и существует последовательность субъектов $s_1, \dots, s_m$ в S_0 , где $s_1 = x, s_m = z$ и $m \geq 2$ таких, что выполняется условие 2. Следовательно, существует последовательность субъектов $s_1, \dots, s_{m+1}$ в S_0 , где $s_1 = x, s_m = z, s_{m+1} = y$ таких, что выполняется условие 2 теоремы.

Четвертый случай: существуют последовательности субъектов $s_1, \dots, s_m$ и $s'_1, \dots, s'_n$ в S_0 , где $s_1 = x, s_m = s'_1 = z, s'_n = y$ и $m, n \geq 2$, для которых выполняется условие 2. Следовательно, существует последовательность субъектов $s_1, \dots, s_{m+n-1}$ в S_0 , где $s_1 = x, s_{m+n-1} = y$ таких, что выполняется условие 2 теоремы.

Индуктивный шаг доказан, и доказательство необходимости выполнения условия теоремы для истинности предиката $can_share_own(x, y, G_0, L_s)$ закончено. Теорема доказана.

Таким образом, в работе введено понятие сущности, параметрически-ассоциированной с субъектом. Для обеспечения возможности анализа получения субъектом права доступа владения к другому субъекту с использованием информационных потоков по памяти как от сущностей, параметрически-ассоциированных с субъектом, так и к сущностям, функционально-ассоциированных с субъектом, построена ФПАС ДП-модель, являющаяся расширением ФАС ДП-модели. Данное расширение дополнительно содержит правило преобразования состояний $know()$, отражающее возможность получения в реальных КС субъектом права доступа владения к другому субъекту с использованием реализации информацион-

ного потока по памяти от сущности, параметрически-ассоциированной с последним. В рамках ФПАС ДП-модели сформулированы и обоснованы условия получения недоверенным субъектом права доступа владения к другому субъекту КС.

Библиографический список

1. Девянин, П. Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах / П. Н. Девянин. М. : Радио и связь, 2006.

2. Девянин, П. Н. Модели безопасности компьютерных систем : учеб. пособие для студ. высш. учеб. заведений / П. Н. Девянин. М. : Академия, 2005.

3. Качанов, М. А. Расширение функциональности системы безопасности ядра Linux на основе подмены системных вызовов / М. А. Качанов, Д. Н. Колегов // Прикладная дискретная математика. 2008. № 2. С. 76–80.

D. N. Kolegov

DP-MODEL OF THE COMPUTER SYSTEM WITH FUNCTIONAL AND PARAMETRIC ASSOCIATES WITH SUBJECT ENTITIES

The definition of parametric-associates with subject entities in computer system is proposed. The extension of DP-model of the computer system with functional-associates with subjects entities is constructed. In this extension the conditions that can access its own right to another subject are formulated and established.

Keywords: computer security, mathematical models of security, discretionary models, security analysis, access rights, information flows.

УДК 62 – 506.1

И. В. Ковалев, М. В. Карасева, В. О. Лесков

ИНФОРМАЦИОННО-ТЕРМИНОЛОГИЧЕСКИЙ БАЗИС КАК СОВОКУПНОСТЬ ЛЕКСИЧЕСКИ СВЯЗАННЫХ КОМПОНЕНТОВ

Рассмотрены вопросы реорганизации структуры базисного информационного компонента мультилингвистической адаптивно-обучающей технологии для применения методики обучения иностранной лексике посредством построения внутриязыковых ассоциативных полей.

Ключевые слова: мультилингвистическая адаптивно-обучающая технология, информационно-терминологический базис, частотные словари, внутриязыковые ассоциативные поля.

В работе [1] были сформулированы основные положения методики обучения иностранным языкам, которая обеспечивает организованное построение групп ассоциативных связей между лексемами целевого языка непосредственно в процессе обучения. Данная методика развивается, опираясь на мультилингвистическую адаптивно-обучающую технологию (МЛ-технологии), поэтому структуру языкового материала, который она будет использовать, рационально разрабатывалась, отталкиваясь от информационно-терминологического базиса (ИТБ) МЛ-технологии [2].

Также, в работе [1] было предложено использование ИТБ как совокупности лексически связанных компонентов (ЛС-компонентов). В соотнесении с МЛ-технологией такой подход вызывает ряд вопросов и требует более подробного описания.

Итак, от грамотно разработанной и соответствующим образом описанной структуры ИТБ, в данном случае, будет зависеть возможность и целесообразность применения настоящей методики обучения в рамках МЛ-технологии.

Информационно-терминологическое обеспечение МЛ-технологии. Информационно-терминологическая база МЛ-технологии строится на основе результатов анализа языкового материала. Под языковым материалом здесь следует понимать некоторое множество текстов интересующей разработчика предметной области изучаемого языка [3]. Размер языкового материала может варьироваться в зависимости от средств анализа, наличия оригинальных текстов и необходимого количества терминов.

Основу построения информационно-терминологической базы составляют частотные словари, по данным которых определяется приоритетность изучения тех или иных терминов. Использование таких словарей, полученных путем анализа языкового материала, качественно улучшает процесс обучения иностранной лексике [4].

В работе [2] была разработана структура информационно-терминологической базы МЛ-технологии с учетом частотных характеристик ее элементов.