DOI 10.17223/20710410/5/9
УДК 004.94

ДП-МОДЕЛЬ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИЧЕСКОЙ СИСТЕМЫ

Е. В. Девянина

ФГНУ «ГНТЦ „Наука“», г. Москва, Россия

E-mail: k_vitalievna@mail.ru

В статье реализуется попытка на основе семейства дискреционных ДП-моделей применить теорию формального моделирования управления доступом и информационными потоками для анализа условий безопасного функционирования компьютерных стеганографических систем.

Ключевые слова: *компьютерная безопасность, стеганография, ДП-модели.*

Большинство существующих подходов, используемых в компьютерной стеганографии [1 – 3], ориентированы либо на применение различных математических (в первую очередь вероятностных) приемов для разработки или анализа стойкости стеганографических преобразований, либо на исследование форматов файлов-контейнеров (изображений, видео, текстовых документов), используемых для сокрытия информации. В то же время стеганографические системы, как правило, реализуются программным обеспечением (ПО), являющимся частью компьютерных систем (КС). Таким образом, на безопасность стеганографической системы может оказывать влияние среда КС, в которой она функционирует.

Важнейшим компонентом обеспечения безопасности большинства существующих КС является система логического управления доступом и информационными потоками, для исследования которой используются формальные модели [4 – 6]. Следовательно, целесообразно рассмотреть подходы к применению таких моделей для анализа безопасности компьютерных стеганографических систем (КСС).

Семейство формальных моделей логического управления доступом и информационными потоками (ДП-моделей) [6, 7] предоставляет механизмы, позволяющие анализировать безопасность современных КС. Как правило, КСС функционируют в КС с дискреционным управлением доступом. Значит, в качестве основы построения формальной модели КСС (далее, сокращенно, КСС ДП-модели) следует выбрать дискреционные ДП-модели.

Заметим, что на безопасность КСС оказывают влияние следующие три фактора, которые будут взяты за основу при построении КСС ДП-модели:

— **целостность** ПО, реализующего КСС. То есть целостность сущностей, функционально ассоциированных с субъектами, реализующими стеганографические преобразования;
— **недоступность** для нарушителя параметров стеганографических преобразований. То есть недоступность данных, содержащихся в сущностях, параметрически ассоциированных с субъектами, реализующими стеганографические преобразования (сущностей, получение данных которых позволит нарушителю однозначно идентифицировать стеганографическое преобразование и осуществить обратное стеганографическое преобразование);

— **зависимость** безопасности ПО, реализующего стеганографические преобразования, от безопасности среды КСС, в которой оно функционирует. Например, зависимость от безопасности используемых в КСС операционных систем (ОС), в том числе от применяемых в ОС технологий администрирования.

Таким образом, при построении КСС ДП-модели целесообразно взять за основу ДП-модель с функционально ассоциированными с субъектами сущностями (ФАС ДП-модель), ДП-модель для политики безопасного администрирования (ПБА ДП-модель) [6] и ДП-модель с функционально и параметрически ассоциированными с субъектами сущностями (ФПАС ДП-модель) [7].

При описании КСС ДП-модели используем следующие предположения и определения.

Предположение 1. Будем считать, что КСС состоит из двух компьютеров (компьютера-источника и компьютера-приемника), удовлетворяющих следующим условиям:

— на компьютере-источнике и компьютере-приемнике функционируют доверенные субъекты «операционная система», реализующие среду для ПО, выполняющего стеганографические преобразования;
— на компьютере-источнике функционирует доверенный субъект, осуществляющий стеганографические преобразования данных из сущности-источника;
— на компьютере-приемнике функционирует доверенный субъект, осуществляющий обратное стеганографическое преобразование данных и их запись в сущность-приемник;
— передача данных между доверенными субъектами компьютера-источника и компьютера-приемника осуществляется через сущность «канал связи» (например, сеть Интернет);
— на компьютере-приемнике функционирует доверенный субъект, осуществляющий непосредственную обработку стеганографических контейнеров (таким образом, стеганографические контейнеры — видео, аудио или текстовые файлы — обрабатываются в соответствии с их содержанием, например, для просмотра).

Определение 1. *Нарушителем* в КСС является недоверенный субъект, имеющий право доступа на чтение к сущности «канал связи» (пассивный нарушитель) или имеющий права доступа на чтение и запись к сущности «канал связи» (активный нарушитель).

Определение 2. *Нарушением безопасности* КСС является реализация субъектом-нарушителем направленного к себе информационного потока по памяти от сущности-источника или от сущности-приемника.

Определение 3. Доверенные субъекты компьютера-источника и компьютера-приемника называются *стеганографически корректными*, когда они не участвуют в реализации информационных потоков по памяти от сущности-источника или сущности-приемника к сущности «канал связи».

Определение 4. Доверенные субъекты компьютера-источника и компьютера-приемника называются *параметрически корректными*, когда они не участвуют в реализации информационных потоков по памяти от параметрически ассоциированных с ними сущностей к сущности «канал связи».

Существует ПО [1], сохраняющее в стеганографических контейнерах данные, позволяющие однозначно идентифицировать стеганографическое преобразование и осуществить обратное преобразование. Значит, не всегда доверенные субъекты, реализующие стеганографические преобразования, являются параметрически корректными. В то же время такие доверенные субъекты, как правило, не осуществляют сохранение в контейнерах или передачу по каналам связи скрываемых данных в явном, непреобразованном виде. Следовательно, стеганографическая корректность доверенных субъектов, реализующих стеганографические преобразования, является естественной для существующих КСС. Поэтому в дальнейшем будем использовать следующее предположение.

Предположение 2. Будем считать, что в рамках КСС ДП-модели все доверенные субъекты являются стеганографически корректными.

Из предположения 2 следует, что доверенные субъекты КСС не осуществляют непосредственную передачу данных, подлежащих стеганографичекому сокрытию, через сущность «канал связи». Кроме того, в соответствии с предположениями ФАС, ФПАС и ПБА ДП-моделей доверенные субъекты не реализуют информационные потоки по времени и имеют права доступа владения к сущностям, размещенным на компьютере, на котором функционирует соответствующий доверенный субъект.

В рамках предположений 1 и 2, используя элементы ФАС, ФПАС и ПБА ДП-моделей, опишем элементы КСС ДП-модели. Используем следующие обозначения:

s_{os_1}, s_{os_2} — доверенные субъекты «операционная система» компьютера-источника и компьютера-приемника соответственно;

$e_{os_1} \in [s_{os_1}]$, $e_{os_2} \in [s_{os_2}]$ — сущности, функционально ассоциированные с субъектами s_{os_1} и s_{os_2} соответственно;

e_s, e_d — сущность-источник и сущность-приемник соответственно;

s_1 — доверенный субъект, реализующий стеганографическое преобразование на компьютере-источнике, при этом по определению выполняются условия $s_1 < s_{os1}$ (субъект s_1 подчинен в иерархии сущностей субъекту s_{os_1}), $s_1 \in [s_{os_1}]$;

s_2 — доверенный субъект, реализующий обратное стеганографическое преобразование на компьютере-приемнике, при этом по определению выполняются условия $s_2 < s_{os_2}$, $s_2 \in [s_{os_2}]$;

s_3 — доверенный субъект, осуществляющий на компьютере-приемнике непосредственную обработку стеганографических контейнеров, при этом по определению выполняются условия $s_3 < s_{os_2}$, $s_3 \in [s_{os_2}]$;

$e_1 \in [s_1]$, $e_2 \in [s_2]$ — сущности, функционально ассоциированные с субъектами s_1 и s_2 соответственно (содержащиеся в сущностях данные задают стеганографическое преобразование, реализуемое субъектами);

$e_3 \in [s_3]$ — сущность, функционально ассоциированная с субъектом s_3;

$e'_1 \in]s_1[$, $e'_2 \in]s_2[$ — сущности, параметрически ассоциированные с субъектами s_1 и s_2 соответственно (содержащиеся в сущностях данные идентифицируют стеганографическое преобразование, реализуемое субъектами);

e_c — сущность «канал связи»;

s_a — недоверенный субъект-нарушитель.

Начальное состояние $G_0 = (S_0, E_0, R_0 \cup A_0 \cup F_0, H_0)$ системы $\Sigma(G^*, OP, G_0)$ зададим в соответствии с рис. 1 (показан случай активного нарушителя, в случае пассивного нарушителя субъект s_a не имеет права доступа $write_r$ к сущности e_c).

Утверждение 1. Пусть в рамках КСС ДП-модели задана система $\Sigma(G^*, OP, G_0)$ и выполнены предположения 1 и 2. Предикат $can\_write\_memory(e_s, s_a, G_0)$ или пре-

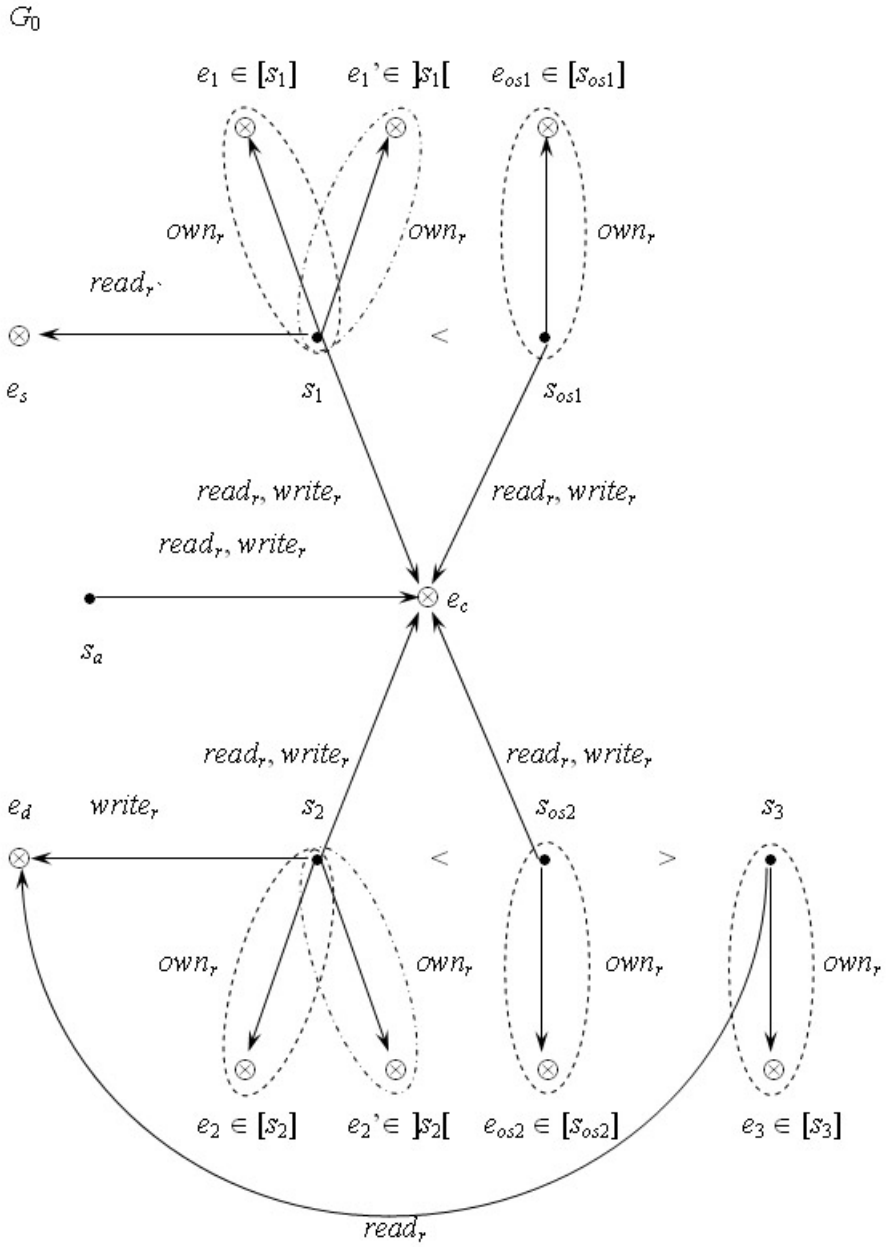

Рис. 1. Начальное состояние системы в рамках КСС ДП-модели

дикат $can\_write\_memory(e_d, s_a, G_0)$ является истинным (происходит нарушение безопасности КСС) тогда и только тогда, когда выполняется одно из следующих трех условий:

Условие 1. Субъект-нарушитель s_a является пассивным или активным, и доверенный субъект s_1 или s_2 является параметрически некорректным.

Условие 2. Субъект-нарушитель s_a является активным, и хотя бы один из доверенных субъектов s_1, s_2, s_{os_1} и s_{os_2} является некорректным (в соответствии с определением, заданным в рамках ФАС ДП-модели) относительно сущности e_c.

Условие 3. Субъект-нарушитель s_a является активным, и доверенный субъект s_3 является некорректным относительно сущности e_d.

Доказательство. Доказательство необходимости выполнения условий утверждения является достаточно трудоемким и проводится аналогично обоснованию необ-

ходимых условий истинности предиката $can\_write\_memory(x, y, G_0)$, выполненному в рамках ФПАС ДП-модели [7].

Доказательство достаточности выполнения условий утверждения является конструктивным. В качестве примера приведем обоснование истинности предиката $can\_write\_memory(e_s, s_a, G_0)$ при выполнении условия 1 утверждения. Пусть доверенный субъект s_1 является параметрически некорректным. Тогда положим:

$op_1 = post(s_1, e_c, s_a)$ — субъект s_1 через сущность e_c реализует информационный поток по памяти к субъекту-нарушителю s_a;

$op_2 = own\_take(read_r, s_1, e'_1)$ — субъект s_1, пользуясь правом доступа владения к сущности e'_1, получает к ней право доступа на чтение;

$op_3 = pass(e'_1, s_1, s_a)$ — субъект s_1, являясь параметрически некорректным, реализует информационный поток по памяти от сущности e'_1 к субъекту-нарушителю s_a;

$op_4 = know(s_a, s_1)$ — субъект-нарушитель s_a, пользуясь информационным потоком по памяти от сущности e'_1, параметрически ассоциированной с субъектом s_1, получает к нему право доступа владения;

$op_5 = take\_right(read_r, s_a, s_1, e_s)$ — субъект-нарушитель s_a берет у субъекта s_1 право доступа на чтение к сущности-источнику e_s;

$op_6 = access\_read(s_a, e_s)$ — субъект-нарушитель s_a получает доступ на чтение к сущности-источнику e_s и реализует от нее к себе информационный поток по памяти.

Следовательно, существует траектория $G_0 \vdash_{op_1} \ldots \vdash_{op_6} G_6 = (S_6, E_6, R_6 \cup A_6 \cup \cup F_6, H_6)$, такая, что выполняется условие $(e_s, s_a, write_m) \in F_6$. Значит, предикат $can\_write\_memory(e_s, s_a, G_0)$ является истинным. ■

Поясним смысл приведенных выше условий.

Условие 1 соответствует случаю, когда субъекты, реализующие стеганографические преобразования, передают в канал связи данные, позволяющие однозначно идентифицировать стеганографические преобразования.

При выполнении условия 2 доверенные субъекты КСС содержат уязвимости реализации, позволяющие активному субъекту-нарушителю, модифицировав данные, передаваемые по каналу связи, изменить содержание сущностей, функционально ассоциированных с доверенными субъектами, и получить над ними контроль.

В случае, когда выполняется условие 3, доверенный субъект, осуществляющий на компьютере-приемнике непосредственную обработку стеганографических контейнеров, содержит уязвимость реализации, позволяющую активному субъекту-нарушителю, модифицировав данные, передаваемые по каналу связи, изменить содержание сущностей, функционально ассоциированных с доверенным субъектом, и получить контроль над доверенными субъектами компьютера-приемника.

Доказательство утверждения показывает, что в рамках КСС ДП-модели возможен анализ безопасности КС, реализующих стеганографические преобразования данных и их передачу по каналам связи. Кроме того, возможно дальнейшее развитие КСС ДП-модели с целью более детального описания свойств и условий функционирования ПО, реализующего стеганографические преобразования, правил управления доступом, параметров администрирования и конфигурирования ОС, используемых в КСС.

ЛИТЕРАТУРА

1. *Аграновский А. В., Девянин П. Н., Хади Р. А., Черемушкин А. В.* Основы компьютерной стеганографии: Учеб. пособие для вузов. М.: Радио и связь, 2003. 152 с.
2. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: СОЛОН-Пресс, 2002. 272 с.

3. *Коханович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2002. 288 с.

4. *Bishop M.* Computer Security: art and science. ISBN 0-201-44099-7, 2002. 1084 p.

5. *Девянин П. Н.* Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр «Академия», 2005. 144 с.

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

7. *Колегов Д. Н.* ДП-модель компьютерной системы с функционально и параметрически ассоциированными с субъектами сущностями // Вестник Сибирского государственного аэрокосмического университета им. акад. М. Ф. Решетнева. 2009. Вып. 1(22). Часть 1. С. 49–54.