УДК 681.326

© Стюгин М.А.
Styugin M.

ПОСТАНОВКА ЗАДАЧИ ДЕЗИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

STATEMENT OF THE PROBLEM OF MISINFORMATION IN INFORMATION SYSTEMS

Аннотация. *В статье показаны информационные ограничении субъекта при исследовании объектов, имеющих функциональную структуру. На основании данных ограничений построена модель, позволяющая моделировать устойчивые субъективные представления исследователя об исследуемом объекте. Дан также ответ на вопрос, в каком случае субъект может утверждать, что его субъективная функциональная структура объекта соответствует действительной. Приведены примеры реализации данного подхода на математических моделях информационной безопасности.*

Работа поддержана грантом Президента Российской Федерации МК-1039.2013.9.

Annotation. *The article shows the limitation of the subject information in the study of objects with a functional structure. On the basis of these constraints, a model can simulate steady subjective perceptions about the object explorer. Dan is also the answer to the question in which case the subject can claim that his subjective functional structure corresponds to the actual object. The examples of this approach on mathematical models of information security.*

This work was supported by a grant from the President of the Russian Federation MK-1039.2013.9.

Ключевые слова. *Модель исследователя, информационная структура конфликта, информационный поток, дезинформация, модель черного ящика, теория графов, математическая модель информационной безопасности.*

Key words. *Model researcher, the information structure of the conflict, the flow of information, misinformation, black box model, graph theory, mathematical model of information security.*

В основном моделирование каких-либо систем затрагивает только их объективную строну. То есть модель системы строится таким образом, как если бы информация о ней была бы нам однозначно и объективно известна. Эта некая «предельная» или «идеальная» модель не всегда корректно накладывается на реальность. Особенно это важно для конфликтующих структур, где информация об объекте конфликта может являться условием его развития. Для моделирования таких процессов важно описать процесс исследования системы, как он выглядит со стороны самого исследователя, понять информационные ограничения исследователя, а также ресурс для дезинформации, который эти ограничения задают.

Базовая модель исследователя

Базовая модель исследователя с информационными ограничениями была описана в работе [1]. На рис.1 представлена модель исследователя – «черный ящик». «Черный ящик» – единственная формализованная модель исследования на сегодняшний день, поэтому ее и будем исследовать. Перебирая значения входных параметров и наблюдая значения «выхода» - функции черного ящика, мы тем самым можем определить функцию исследуемой системы. В реальных системах мы, как правило, не можем знать, что является для черного ящика входом и выходом, поэтому исследователю приходится строить гипотезы относительно функциональной структуры ящика. Такая гипотеза, по существу. есть предположение относительно множества параметров (**par`**), от которого зависит целевая функция системы f.

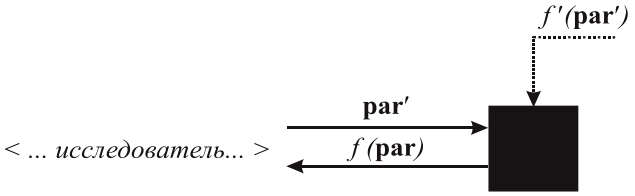

Рис.1. Модель исследователя

Имея некую гипотезу относительно функциональной структуры черного ящика – f'(**par'**) и перебирая множество входных параметров **par'**, исследователь на-

Стюгин Михаил Андреевич – кандидат технических наук, старший преподаватель, ФГБОУ ВПО «Сибирский федеральный университет», тел. (495)543-36-76.

Styugin Michael. – PhD, enior lecturer, VPO Siberian federal university, tel. (495) 543-36-76.

блюдает значение функции – $f(\mathbf{par})$. Гипотезу исследователя будем называть *стереотипной схемой.*

Несмотря на различие функций, множество их значений определено на одном множестве, так как исследователь контролирует значение одного выхода

f: $\mathbf{par} \rightarrow \mathbf{y}$; f': $\mathbf{par}' \rightarrow \mathbf{y}$; f'': $\mathbf{par}'' \rightarrow \mathbf{y}$; ...

У исследователя может присутствовать любая из гипотез f^x: $\mathbf{par}^x \rightarrow \mathbf{y}$, но такой функции может не существовать в действительности. То есть в рамках выбранного множества параметров $\mathbf{par}^x$ невозможно найти функциональное отображение на множество **y**. Может быть ситуация когда функциональная зависимость есть, но не равна реальной функции черного ящика $f^x \neq f$.

Множество всех возможных множеств параметров функции черного ящика составляет множество $\mathbf{S}_{\mathbf{par}}$, т.е.

$\mathbf{par}', \mathbf{par}'', \mathbf{par}''', \ldots . \in \mathbf{S}_{\mathbf{par}}$.

Множество всех возможных функций черного ящика по гипотезам исследователя

$\mathbf{F}_{\mathbf{par}} = \{ f^x(\mathbf{par}^x) : \mathbf{par}^x \in \mathbf{S}_{\mathbf{par}} \}$.

Для каждого исследователя можно определить множество параметрической видимости $\mathbf{S}_\mathbf{v} \subseteq \mathbf{S}_{\mathbf{par}}$, т.е. те параметры, которые субъект может наблюдать, и множество функциональной видимости $\mathbf{F}_\mathbf{v} \subseteq \mathbf{F}_{\mathbf{par}}$ (множество различимых для него значений функции)

$\mathbf{F}_\mathbf{v} = \{ f^x(\mathbf{par}^x) : \mathbf{par}^x \in \mathbf{S}_\mathbf{v} \}$.

Описанная модель исследователя может принадлежать одному из четырех классов.

Класс 1. $\mathbf{par}' = \mathbf{par}$, $\mathbf{par} \in \mathbf{S}_\mathbf{v}$, $\{ f(\mathbf{par}) \} \in \mathbf{F}_\mathbf{v}$.

Эта классическая модель исследования черного ящика. Для определения функциональной структуры черного ящика достаточно перебрать входные значения и сопоставить со значением функции выхода. Здесь стереотипная схема (гипотеза) исследователя соответствует действительности.

Класс 2. $\mathbf{par}' \neq \mathbf{par}$, $\mathbf{par} \in \mathbf{S}_\mathbf{v}$, $\{ f(\mathbf{par}) \} \in \mathbf{F}_\mathbf{v}$.

Неинформативная обратная связь. В силу неверной гипотезы относительно функциональной структуры системы исследователь не может найти функцию черного ящика. Здесь стереотипная схема (гипотеза) уже не соответствует действительности. Задача исследователя при данных условиях путем перебора гипотез добиться информативной обратной связи и свести тем самым систему к первому классу.

Класс 3. $\mathbf{par}' \neq \mathbf{par}$, $\mathbf{par} \notin \mathbf{S}_\mathbf{v}$, $\{ f(\mathbf{par}) \} \in \mathbf{F}_\mathbf{v}$.

Невозможно добиться информативной обратной связи от исследуемой системы. Параметры целевой функции черного ящика не входят в область параметрической видимости исследователя. Исследование в таких условиях бессмысленно. Необходимо расширить область параметрической видимости и привести тем самым модель ко второму классу.

Класс 4. $\mathbf{par}' \neq \mathbf{par}$, $\mathbf{par}' \notin \mathbf{S}_\mathbf{v}$, $\{ f'(\mathbf{par}') \} \notin \mathbf{F}_\mathbf{v}$.

Невозможность постановки задачи исследования. В такой ситуации исследователь может сопоставить с моделью черного ящика более простую функциональную структуру. Поскольку нет какого-либо диссонанса в рамках наблюдаемых величин, то и невозможна постановка задачи исследования. Перевести модель к третьему или второму классу можно только путем расширения области функциональной видимости.

«Структура» черного ящика

У черного ящика по определению не может быть структуры. Однако в ходе исследования мы можем разделить один черный ящик на несколько, определив структуру их взаимодействия.

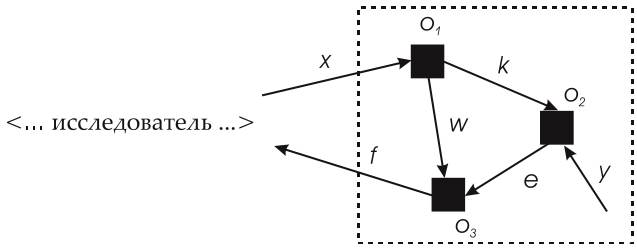

Рис.2. Структура информационных потоков

Здесь исследователь разбил черный ящик на структуру из трех объектов, каждый из которых представляет функциональный ящик, состоящий из входов и выходов. Объект O_1 имеет два выхода, т.е. его можно нормализовать, разбив на два независимых объекта с входами хи выходами ki w.

Функции объектов системы:

k(x), w(x), e(k,y), f(w,e).

Результирующая функция системы:

f(w(x),e(k(x)),y).

Здесь x и y – параметры, подаваемые на вход системы, т.е. $y \in \mathbf{par}$. При этом y, хоть и внесен исследователем в систему, но не является параметром, наблюдаемым им, т.е. $y \notin \mathbf{S}_\mathbf{v}$ и, соответственно, $\mathbf{par} \notin \mathbf{S}_\mathbf{v}$. Поскольку у системы присутствуют входные параметры, которые не входят во множество параметрической видимости, то система тем самым переходит к 3-му классу исследования, описанному выше. В данном классе субъект не может добиться информативной обратной связи от исследуемой системы. Однако отличие схемы на рис.2 от схемы на рис. 1 заключается как раз в том, что отсутствие информативной обратной связи не исключает возможность что-то узнать о системе. То есть относительно топологии и свойств информационных потоков в такой си-

стеме информативная обратная связь иногда будет присутствовать.

Для определения условий наличия информативной обратной связи необходимо разделить субъективный и объективный взгляд на систему. В случае одного черного ящика (рис.1) такое разделение осуществлялось по множеству параметров **par`** (субъективное) и **par** (объективное). В случае схемы со множеством объектов этого недостаточно, так как необходимо также разделить субъективный взгляд на объекты (их может не быть на самом деле) и информационные потоки между ними.

Таким образом мы получаем субъективную и объективную схему информационных потоков (рис.3).

Если далее объект o_3 делает аналогичные отображения, то на множестве значений функции, которую наблюдает исследователь можно определить отношение эквивалентности. То есть до исследователя доходит функция, значения которой можно разделить по двум множествам, одно из которых может быть неразличимым, т.е. не входит в область функциональной видимости $\mathbf{F_v}$. (рис.4)

Такие информационные потоки назовем «ортогональными» в силу того, что у них разные множества определения параметров и функций. Ортогональные потоки в системе всегда можно разделить, вводя дублирующие объекты. Таким образом мы получим систему с неортогональными потоками (рис. 5).

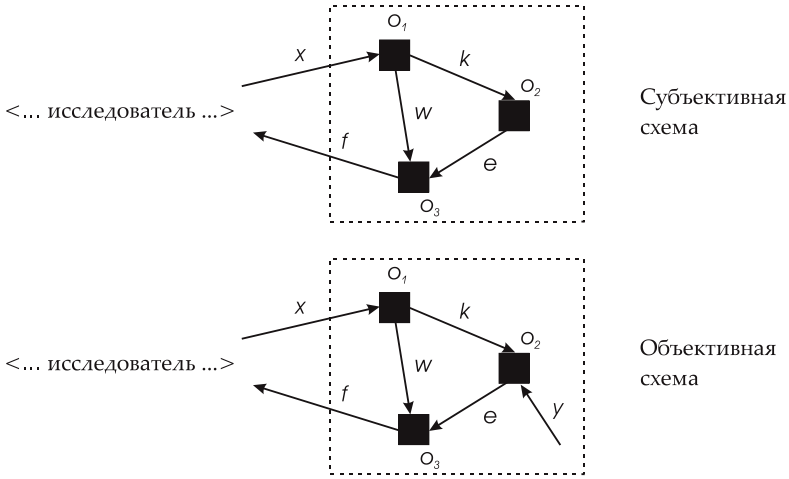

Рис.3. Субъективная и объективная схема информационных потоков

В схеме, представленной на рисунке, в объективной системе есть вход *y* для объекта O_2, а в субъективной схеме его нет. Получит ли исследователь информативную обратную связь от системы? Это зависит от свойств функций и топологии сети информационных потоков.

Исходя из описанных в работе [2] свойств модели исследователя, мы можем получить информативную обратную связь, если сможем ввести по неизвестным входным параметрам – отношение эквивалентности на множестве значений функции, наблюдаемой исследователем.

Для представленной выше схемы эти значения будут выглядеть следующим образом:

F_{o2}: $\mathbf{K}\times\mathbf{Y} \rightarrow \mathbf{E}_1\times\mathbf{E}_2$.

И можно представить данную функцию как композицию

F_{o2}^{K}: $\mathbf{K} \rightarrow \mathbf{E}_1$;

F_{o2}^{Y}: $\mathbf{Y} \rightarrow \mathbf{E}_2$;

$F_{o2} = F_{o2}^{K} \circ F_{o2}^{Y}$.

На множестве значений функции F_{o2} можно определить отношение эквивалентности

$F_{o2}^{\equiv}$: $\mathbf{E}_1\times\mathbf{E}_2 \rightarrow \forall\ \mathbf{E}_1\times\mathbf{E}_2$;

$\forall e_1 \in \mathbf{E}_1;\ e_2 \in \mathbf{E}_2;\ e_3 \in \mathbf{E}_2 \Rightarrow (e_1, e_2) = (e_1, e_3)$.

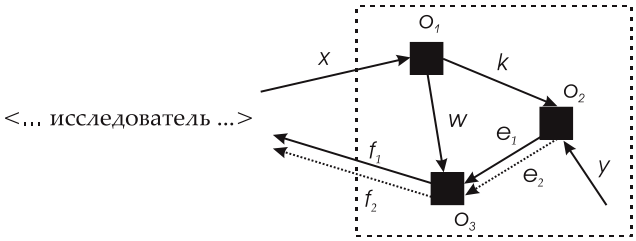

Рис.4. Ортогональные информационные потоки

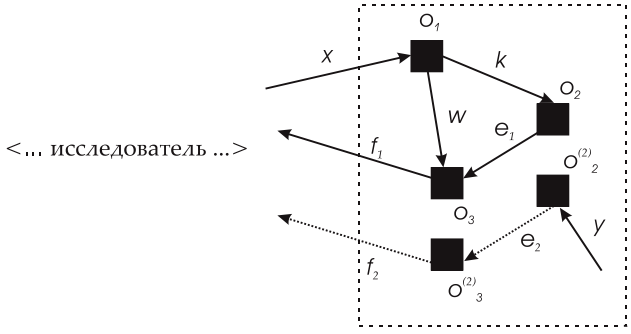

Рис.5. Разделение ортогональных потоков

В полученной системе исследователь может получить точную информативную обратную связь по верхней части схемы информационных потоков. При этом он мо-

жет никак не наблюдать функциональную реакцию нижней части схемы. Это происходит в силу уже доказанного в работе [1] утверждения, что при ограничении множества функциональной видимости субъект всегда может сопоставить с системой более простую модель и убедиться в ее истинности.

Рассмотрим теперь ситуацию, приведенную выше на рис.3, с той позиции, что все потоки в ней уже являются неортогональными. В таком случае информационные потоки могут быть итеративными и неитеративными. Под неитеративной системой мы подразумеваем такую, в которой информационные потоки существуют непрерывно, меняя значение входов черных ящиков. Для неитеративной системы любой неконтролируемый вход приведет к тому, что мы никогда не сможем получить информативной обратной связи.

В итеративной системе мы всегда можем предположить, что на нескольких экспериментах значения одного или нескольких входов объекта может оставаться постоянным. Таким образом, по другим информационным потокам мы можем получить информативную обратную связь.

Подавляющее большинство всех технических и информационых систем являются итеративными. Мы можем их исследовать, не прибегая к знанию значений всех входов.

В исследовании таких структур можно выделить два ключевых вопроса, важных с прикладной точки зрения:

1. Какие субъективные схемы являются для исследователя устойчивыми.

2. Как на основании субъективной схемы можно говорить о ее соответствии объективной системе

Анализ устойчивости структур

Описанную выше схему можно представить в виде ориентированного графа

$\Gamma=(O\cup\{s\}, M)$,

где O– множество объектов в системе (черных ящиков), s–субъект (исследователь); M– множество ребер графа (информационных потоков).

В системе задан объективный граф Г и субъективный граф Γ_s. Для приведенной на рис.3 схемы построим соответствующие графы (рис. 6).

$\Gamma=(O\cup\subseteq\{s\}, M)$ – объективный граф;

$\Gamma_s=(O_s\cup\{s\}, M_s)$ – субъективный граф.

Субъективный граф не всегда является устойчивой структурой. Субъект может обнаружить несоответствие отправляемых данных и получаемой обратной связи от системы. В некоторых случаях он может не получать вообще никакой обратной связи, а в некоторых ее не ждать.

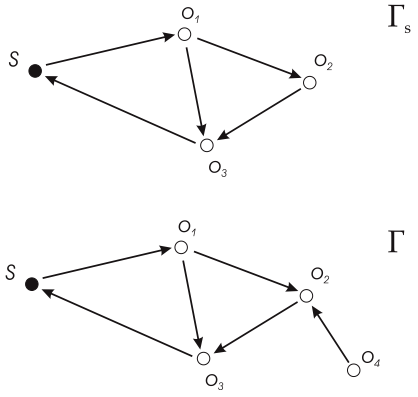

Рис.6. Субъективный и объективный граф информационных потоков

Правило 1. Структуры без обратной связи всегда устойчивы.

То есть если в рамках субъективного графа субъект не имеет обратной связи по каким-либо объектам или не имеет способов воздействия на них, то такая структура всегда является устойчивой.

Субъективный граф, показанный на рис.7, является устойчивым, так как, не имеет обратной связи ни по одному объекту. Субъект может воздействовать на объекты o_1и o_2, но не может получать от них информации. Может получать информацию от объекта o_3, но не может на него воздействовать.

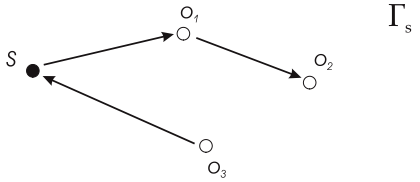

Рис.7. Структура без обратной связи

Обратная связь в графе есть если есть сильная связность (путь в одну и другую сторону) субъекта и вершин в графе. Наблюдая несоответствие обратной связи субъект может корректировать свой субъективный граф.

Определение 1. Назовем кольцом обратной связи Γ_s^k *совокупность ребер* M_s^k *сильносвязных вершин* $O_s^k\subseteq O_s$ *в графе* Γ_s *с субъектом s.*

Правило 2. Если вычитание из субъективного кольца обратной связи Γ_s^k *объективного кольца обратной связи* Γ^k *составляет непустое множество, то такая структура является неустойчивой.*

Пример неустойчивой структуры в графе приведен на рис.8.

Неустойчивые структуры разрушаются, образуя

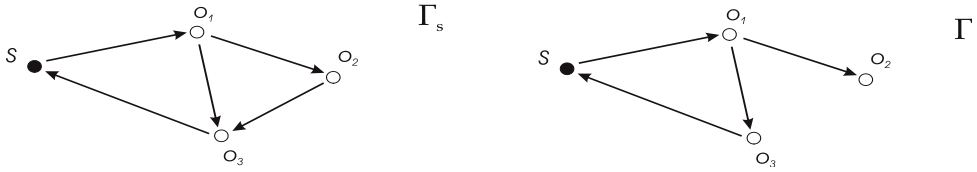

Рис.8. Неустойчивый субъективный граф по правилу 2

новый граф.

Определение 2. Преобразование графа информационных потоков с неустойчивой структурой к устойчивому графу называется приведением, а полученный граф приведенным.

Правило 3. Неустойчивый граф Γ_s по правилу 2, приводится к устойчивому графу Γ_s^* по формуле

$$\Gamma_s^* = \Gamma_s \setminus (\Gamma_s^k \setminus (\Gamma^k) = (O_s \setminus O_s^k \setminus O^k) \cup \{s\}, M_s \setminus (M_s^k \setminus O^k)) = (O_s^*) \cup \{s\}, M_s^*. \quad (1)$$

Далее будем рассматривать только итерационные системы. Для субъективных графов итерационных систем можно вывести еще одно правило неустойчивости и получения приведенных графов.

Правило 4. Существует информационный поток к одному из объектов кольца обратной связи субъективного и объективного графа(Γ_s^k является устойчивым), который присутствует в объективном графе, но отсутствующий в субъективном, т.е. $\exists (o_1, o_2) \in M, (o_1, o_2) \notin M_s$, $o_2 \in O_s^k$, $o_2 \in O^k$. *Такой граф является неустойчивым.*

Пример неустойчивого графа по правилу 4 показан на рис.9.

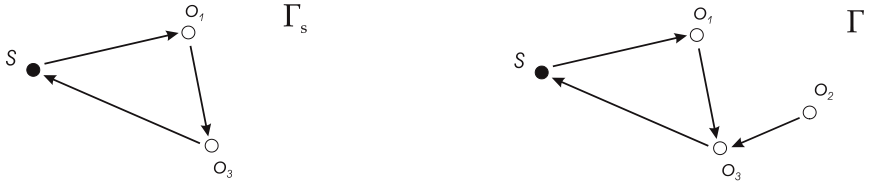

Рис. 9. Неустойчивый граф по правилу 4

Правило 5.Для неустойчивого графа по правилу 4 приведенный граф строится по следующему принципу:

$$\Gamma_{add} = \{(o_i, o_j) \mid (o_i, o_j) \in M, (o_i, o_j) \notin M_s, o_j \in O_s^k, o_j \in O^k\};$$
$$\Gamma_s^* = \Gamma_s \cup \Gamma_{add}. \quad (2)$$

Теорема 1. Последовательным применением преобразований (1) и (2) к любому субъективному графу информационных потоков мы получаем приведенный (устойчивый) граф.

Теорема 2. Граф, не содержащий сильносвязных вершин с вершиной {s}, всегда устойчив.

Оценка объективности системы

В реальных конфликтах мы можем анализировать только субъективные информационные потоки, так как сами являемся участниками системы, находимся внутри нее. Отсюда достаточно важно решить задачу оценки для исследователя, на сколько его субъективный граф соответствует объективному.

В общем случае эта задача не имеет решений, однако при введении определенных ограничений может быть решена.

Теорема 3. Если все объекты (вершины графа) в системе являются общим правилом и Γ_s^k приведенного графа субъекта Γ_s^* содержит все вершины, то $\Gamma_s^* = \Gamma$.

Анализ реальных систем

Применение описанной выше модели можно рассмотреть на системах информационной безопасности. Возьмем, например, классическую дискреционную модель разграничения доступа Харрисона-Руззо-Ульмана в моделях информационной безопасности[3].

В ней определены:

O – множество объектов системы;

S – множество субъектов системы ($S \subseteq O$);

R – множество видов прав доступа субъектов к объектам;

T – матрица доступов, строки которой соответствуют субъектам, а столбцы соответствуют объектам $T[s, o] \subseteq R$.

В результате выполнения примитивного оператора α осуществляется переход системы из состояния $q=(S,O,T)$ в состояние $q'=(S',O',T')$. Данный переход обозначается $q \mapsto_\alpha q'$.

В нашем случае необходимо разделить субъективные и объективные состояния системы

$\forall s_i \in S \exists\ q_{si} = (S_{si}, O_{si}, T_{si})$.

У каждого субъекта в графе, определенном состоянием $q_{si}=(S_{si}, O_{si}, T_{si})$, можно выделить область дезинформации (ложные объекты и доступы) и невидимую область (то, чего он не видит в объективной матрице доступов).

Область дезинформации: $q_{si}^{dez}=(S_{si}|S, O_{si}|O, T_{si}|T)$.

Невидимая область: $q_{si}^{inv}=(S\backslash S_{si}, O|O_{si}, T\backslash T_{si})$.

Модель Харрисона-Руззо-Ульмана (ХРУ) используется для анализа безопасного состояния систем в зависимости от возможности перехода в такое состояние q', при котором в соответствующих ячейках матрицы появляются недопустимые права доступа.

Если мы вводим субъективные состояния системы, то система ХРУ не может осуществлять переходы, если их нет в субъективных матрицах ни одного из субъектов. Таким образом, начальное состояние системы, в которой присутствуют N субъектов, мы можем выразить в следующем виде:

$$q_0=(S_{s1}\cup...\cup S_{sN}\cap S, O_{s1}\cup...\cup O_{sN}\cap O, T_{s1}\cup...\cup T_{sN}\cap T).$$

Из этой формулы видно, что если система, в которой анализируются только объективные состояния автомата ХРУ небезопасна, то это не значит, что с учетом субъективных состояний автомата ХРУ мы получим также небезопасную систему. Это дает возможность получить безопасную систему за счет корректировки субъективных матриц доступа.

Если мы введем отображение матрицы доступа на множество информационных потоков, описанных выше $I: M\rightarrow T$, то сможем ответить на вопросы:

- как можно дезинформировать субъектов в системе чтобы получить устойчивые субъективные графы доступа?
- в каком случае на основании собственного субъективного графа доступов мы можем прийти к построению объективного графа доступов?

Выводы

Приведенная модель исследователя позволяет решать задачу дезинформации в системах, чтобы сделать из безопасными. Помимо приведенного примера с моделью Харрисона-Руззо-Ульмана, аналогичные дополнения можно сделать и для других моделей информационной безопасности, таких как Take-Grant, мандатного и ролевого управления доступом [4].

Модель может также применяться при моделировании конфликтных систем, например, построения исходных платежных матриц теоретико-игровых моделей.

Литература

1. Стюгин МА. Методы защиты от исследования систем / МА. Стюгин // Информационные войны. – № 4. – 2009. – С. 23-29.

2. Стюгин МА. Защита систем от исследования. Методы и модели построения защищенных систем и управления информацией в конфликте. 2011. – 132 с.

3. Harrison M., Ruzzo W., Ullman J. Protection in operating system // Communication of ACM. 1976. №19 (8). P 461-471

4. Bell D.E., LaPadula L.J. Secure Conputer Systems: Unified Exposition and Multics Interpretation. – Bedford, Mass.: MITRE Corp., 1976.

Материал поступил в редакцию 19. 05. 2014 г.