УДК 621.34

С.Г. СЕМЕНОВ, канд. техн. наук

СТРУКТУРНО-ИНФОРМАЦИОННЫЕ ПОРТРЕТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ НА ПРИМЕРЕ DOS-АТАКИ

Постановка проблемы

В настоящее время в Украине практически нет отраслей, где бы ни использовались информационные системы, выполняющие телекоммуникационные, информационные и расчетные функции (обработка и обмен данными, хранение информационных ресурсов, формирование сигналов управления критическими системами, построение графиков, отчетов и др.). При этом их управление осуществляется по отдельным, заранее известным алгоритмам. Однако проведенные исследования показали наличие в большинстве информационных систем различного рода структурных и функциональных априорных неопределенностей, что предполагает использование средств моделирования нечетких данных и знаний, нечеткого логического выделения, методов теории адаптивных систем [1 – 4, 7].

Анализ литературы [2 – 5, 7, 8] показал, что существующие подходы к идентификации и моделированию информационных систем оперируют априорными данными или результатами компьютерного моделирования. Однако в условиях априорной неопределенности до настоящего времени каких-либо методов или формализованных процедур выбора структуры модели не предложено.

В работе [7] был предложен подход к построению модели информационной системы на основе структурно-информационных портретов и предложен комплексный показатель эффективности функционирования системы. Однако вопросам оценки влияния внешних факторов воздействия на состояние информационной системы и изменение характеристик структурно-информационных портретов в данной работе внимания не было уделено.

Поэтому актуальной научной задачей представляется построение и исследование наблюдаемых структурно-информационных портретов информационных систем с оценкой и выбором информативных переменных в условиях воздействия различного рода внешних факторов (в том числе и негативных).

Моделирование информационных систем в условиях априорной неопределенности

В [2] представлена динамическая модель информационной системы на основе наблюдаемого структурно-информационного портрета, учитывающая апостериорные данные о ее структурных изменениях в условиях внешних воздействий. Причинно-следственные связи в структурно-функциональном пространстве R исследуемого объекта на множестве апостериорных данных $I_{an} = \{Y(t), U(t), \chi(t), \xi(t), t \in R^t\}$ описываются с помощью выражений

$$S(t) = F_1(S, A_1, U, \chi, \xi, t, \tau), \quad (1)$$

$$Y(t) = F(S, A, U, \chi, \xi, t), \quad (2)$$

а множество динамических процессов в объектах управления задается с помощью дифференциального уравнения с одним входом и выходом [2]

$$a_0 y^{(m)} + a_1 y^{(m-1)} + \ldots + a_m y = b_0 u^{(k)} + b_1 u^{(k-1)} + \ldots + b_k u + \xi + \chi, \quad (3)$$

где $S(t) \in R^s$ – вектор внутреннего состояния объекта управления, $\tau \in \Im$ – некоторый интервал времени (временная задержка). F_1, F – внутренние нелинейные операторы, структура которых известна с точностью до векторов искомых параметров $A_1(t), A(t)$, принадлежащих ограниченной, но априори неизвестной области $G_A \subseteq R^v$. $Y(t)$ – вектор выходных параметров системы.

Исследования [1 – 4, 7] показали, что для линейного стационарного объекта управления уравнение в пространстве состояний имеет вид [2, 7]:

$$\dot{X} = AX + BU + \xi + \chi, \quad (4$$

$$Y = CX + DU + \zeta, \quad (5$$

где $X \in R^m$ – вектор состояния, $A \in R^{mxm}$ – матрица состояния, $U \in R^k$ – вектор входа, $Y \in R^n$ – вектор выхода, $B \in R^{mxk}$, $C \in R^{nxm}$, $D \in R^{nxk}$, $\zeta \in R^n$ – ненаблюдаемый вектор ошибок измерения, $\xi \in R^m$, $\chi \in R^m$ – вектора помех (ξ – контролируемые возмущения, χ – неконтролируемые шумы).

В [3] показано, что реализация моделей в пространстве состояний связана с необходимостью оценки ненаблюдаемых компонентов вектора $X(t)$ на множестве I_{an}. Однако, как показали исследования, в условиях априорной неопределенности данная задача не всегда выполнима с заданной точностью. В то же время решение о структуре модели исследуемой системы должно приниматься исходя из принципа информационной полноты анализируемых (используемых при моделировании) данных (множества $I = \{I_a, I_{an}\}$, где I_a, I_{an} – соответственно априорная и апостериорная информация об объекте исследования). Особенно это важно в условиях априорной неопределенности, характерной для функционирования информационных систем.

Используем приведенные выше предложения при моделировании информационной системы. Для этого рассмотрим систему уравнений [3]:

$$\begin{aligned} \dot{X} &= F(X, U, A, t), \\ Y &= F_Y(X, U, A_1, t), \end{aligned} \quad (6$$

где $U \in \Omega_U \subset \hat{U} \subseteq R^m$ – входной вектор системы, $Y \in \hat{Y} \subset R^n$ – выход системы, $X \in \hat{X} \subseteq R^q$ – вектор состояния, $\hat{U}, \hat{Y}, \hat{X}$ – множества входных и выходных сигналов, а также состояний системы соответственно, $\hat{Y} \subseteq \hat{X} \subseteq R^n$, $A \in R^{q \times p}$, $A_1 \in R^{n \times q}$ – матрицы параметров, $F : R^q \times R^m \times J \to R^q$ – гладкая непрерывно дифференцируемая по $\hat{X}$ и по A вектор-функция, $t \in J$, $F_Y : R^q \times R^m \times J \to R^n$ – функция, задающая способ формирования выходного вектора системы.

В состав множества I_{an} входят не сами векторы U и Y, а их наблюдаемые и вычисляемые аналоги (векторы $\tilde{U}(t)$, $\tilde{Y}(t)$, $\tilde{K}(t)$), которые получаются в результате мониторинга информационной системы и применения операторов f_U, f_Y, f_K в пространствах $\aleph, \Re, \Im$ входных и выходных векторов соответственно, а так же временном пространстве J:

$$f_U : \aleph \times J \to R^m, \; f_Y : \Re \times J \to R^n, \; f_K : \Im \times J \to R^k. \quad (7$$

Следует заметить, что указанные в (6) операторы отражают также ошибки измерения.

Операторы $f_U \in N_U$, $f_Y \in N_Y$ определены на множествах N_U, N_Y, характеризующих неопределенность процесса измерения. В зависимости от доступности процесса наблюдения множества N_U и N_Y могут иметь как нечеткую природу, так и статистическую [2, 3].

Как показали исследования [2, 3, 7], при идентификации динамических систем целесообразно использовать множество I_{an}. Используя операторы (7), получим множество наблюдений (наблюдаемое структурно-информационное множество)

$$I_{an} = I(\tilde{U},\tilde{Y}) = \left\{\tilde{U} \in R^m, \tilde{Y} \in R^n \middle| \tilde{U}(t) = f_U(U,t), \tilde{Y}(t) = f_Y(Y,t)\ \forall (t \in J)\right\}, \quad (8)$$

Представим множество (8) в виде: $I_{an} = I(\tilde{U},\tilde{Y}) = I(\tilde{U}) \cup I(\tilde{Y}) \quad \forall t \in J$.

Определим бинарное отношение Z между множествами $\tilde{U}$ и $\tilde{Y}$ системы (6): $Z \subset \tilde{U} \times \tilde{Y}$. Назовем это множество портретом системы (6) в пространстве $\aleph \times \Re$. Соответствующий фазовый портрет системы (6) представим в виде

$$Z_\phi \subset \hat{X} \setminus \hat{U} \times \hat{Y} \quad \forall U(\cdot) \in \Omega_U. \quad (9)$$

Расширенным фазовым портретом системы будем называть отображение $Z_\phi \subset \hat{X} \times \hat{U} \quad (\forall U(\cdot) \in \Omega_U) \& (\forall t \in J)$.

Для любого наблюдаемого структурно-информационного множества $I(\tilde{U},\tilde{Y})$ (8) системы (6) определенного в пространстве $\aleph \times \Re$, наблюдаемые структурно-информационными портретами, называются бинарные отношения:

$$Z_i = Z_i(I_{an}) \subset I(\tilde{U}) \times I(\tilde{Y}), \quad (10)$$

$$Z_i = Z_i(I_{an}) \subset I(\tilde{U} / \tilde{Y}) \times I(\tilde{Y}). \quad (11)$$

Из (10) следует, что $Z \subseteq Z_i$ и $dom(Z_\phi) = rng(Z)$, т. е. между ними существует структурное соответствие.

Исследование информационной системы в условиях воздействия DOS-атаки

Проведем сравнительное исследование расширенного фазового и наблюдаемых структурно-информационных портретов подсистемы информационного обеспечения [7] информационной системы на примере входного трафика данных в условиях воздействия на нее Dos–атаки.

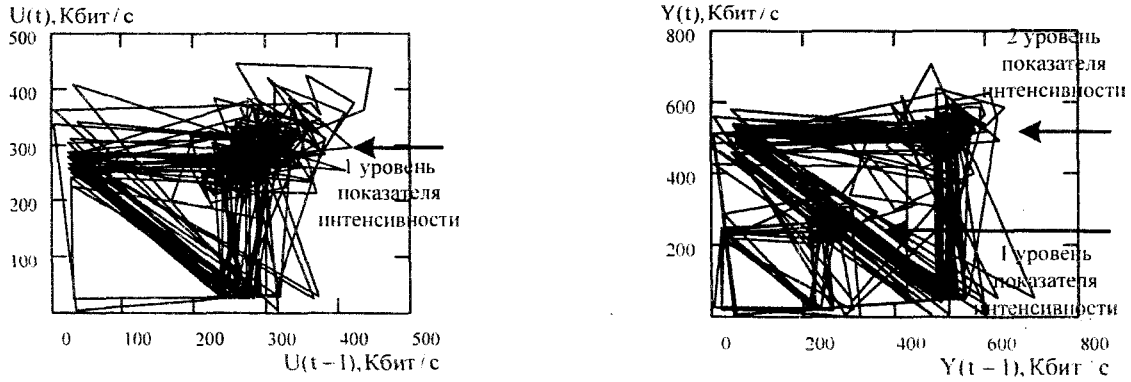
На рис. 1. представлен расширенный фазовый портрет подсистемы информационного обеспечения в условиях воздействия на подсистему информационного обеспечения Dos-атаки, при этом в качестве показателя системы выступает характеристика интенсивности входного (рис. 1, *а*) и выходного (рис. 1, *б*) трафика данных. Для наглядности графика количество отсчетов показателя интенсивности входного и выходного трафика ограничено числом 150.

Сравнивая рис. 1, *а* и 1, *б*, следует отметить изменения, характерные для исследуемого вида внешнего воздействия на информационную систему (Dos-атаку). Прежде всего, это появление второго «уровня» показателя интенсивности трафика данных (см. рис. 1), связанного с увеличением интенсивности входного потока данных. На практике именно это увеличение чаще всего приводит к деструктивным изменениям в исследуемой системе.

Использование расширенного фазового портрета в определенной степени дает картину структурных изменений в системе при воздействии внешних факторов, однако информации о внутренних свойствах системы с помощью фазовых портретов получить чаще всего невозможно. Поэтому при моделировании информационной системы целесообразно использовать и структурно-информационные портреты системы.

На рис. 2. представлены наблюдаемые структурно-информационные портреты подсистемы информационного обеспечения в условиях воздействия на нее Dos-атаки, при этом в качестве измеряемых векторов наблюдаемого структурно-информационного множества $I(\tilde{U},\tilde{Y})$ выступают интенсивность входного ($\tilde{U}$) и выходного ($\tilde{Y}$) трафика данных (рис.2, *а*), коэффициент структурности $K(t) = \dfrac{\tilde{Y}(t)}{\tilde{U}(t)}$ (рис. 2, *б*), и коэффициент пачечности

$K_n(t) = \frac{\widetilde{V}_{\max}(t)}{\widetilde{V}_{cp}(t)}$ (рис 2, *в*), где $\widetilde{V}_{\max}$ – максимальная скорость передаваемых данных, $\widetilde{V}_{cp}$ – средняя скорость передаваемых данных.



а *б*

Рис. 1

Анализ графиков на рис. 1 и 2 позволяет сделать вывод о разнородности траекторий наблюдаемых структурно-информационных портретов и траекторий на фазовой плоскости подсистемы информационного обеспечения. Это подтверждает гипотезу о том, что множества Z_ϕ и Z_i имеют различные структуры. Данная закономерность объясняется, прежде всего внутренними свойствами подсистемы информационного обеспечения и структурной сложностью информационного трафика.

Рассмотренные на рис. 2 примеры построения наблюдаемых структурно-информационных портретов иллюстрируют структуру системы в пространствах $\aleph \times \Re$ (рис. 2, *а*), $\Im \times \Re$ (рис. 2, *б*, *в*) и могут быть использованы при решении задачи структурной идентификации.

Однако, как показали исследования, на основе качественной (визуальной) информации состоянии исследуемых объектов можно сделать вывод только о стационарности (или нестационарности) системы. При этом остается нерешенным вопрос выбора информативных переменных наиболее полно описывающих состояние системы. Поэтому следующей важной научной задачей представляется задача исследования наблюдаемых структурно-информационных портретов на предмет выбора кортежа информативных векторов, наиболее полно описывающих структурные особенности системы.

Проведенные исследования [8] показали, что в теории идентификации для решения данной задачи чаще всего используются методы корреляционного анализа [2, 3, 6, 8], при этом в качестве показателя отбора применяется коэффициент взаимной корреляции.

Пусть исследуемый объект, описывается уравнением:

$$y(t) = f(t, U), \quad \{y(t) = f(t, K), y(t) = f(t, Kn)\}, \qquad (1$$

где $f(\cdot)$ – функция заданного класса.

Рассмотрим проекцию наблюдаемых структурно-информационных портретов Z_i на плоскости $\{y, u_i\}, \{y, k_i\}, \{y, kn_i\}$, где $u_i \in \aleph, k_i \in \Im, kn_i \in \Im$ – точки входных данных мониторинга в пространствах $\aleph, \Re, \Im$ (см рис. 3, *а*, *б*, *в* соответственно). Получим сужение отображений $Z_i : Z_i^{u_i} \subset Z_i\big|_{u_i \in U}$, $Z_i : Z_i^{k_i} \subset Z_i\big|_{k_i \in K}$, $Z_i : Z_i^{kn_i} \subset Z_i\big|_{kn_i \in U}$ и траектории движения системы, заданные графиками $\varphi_{u_i} : I(y) \to I(u_i \in U)$, $\varphi_{k_i} : I(y) \to I(k_i \in K)$, $\varphi_{kn_i} : I(y) \to I(kn_i \in Kn)$.

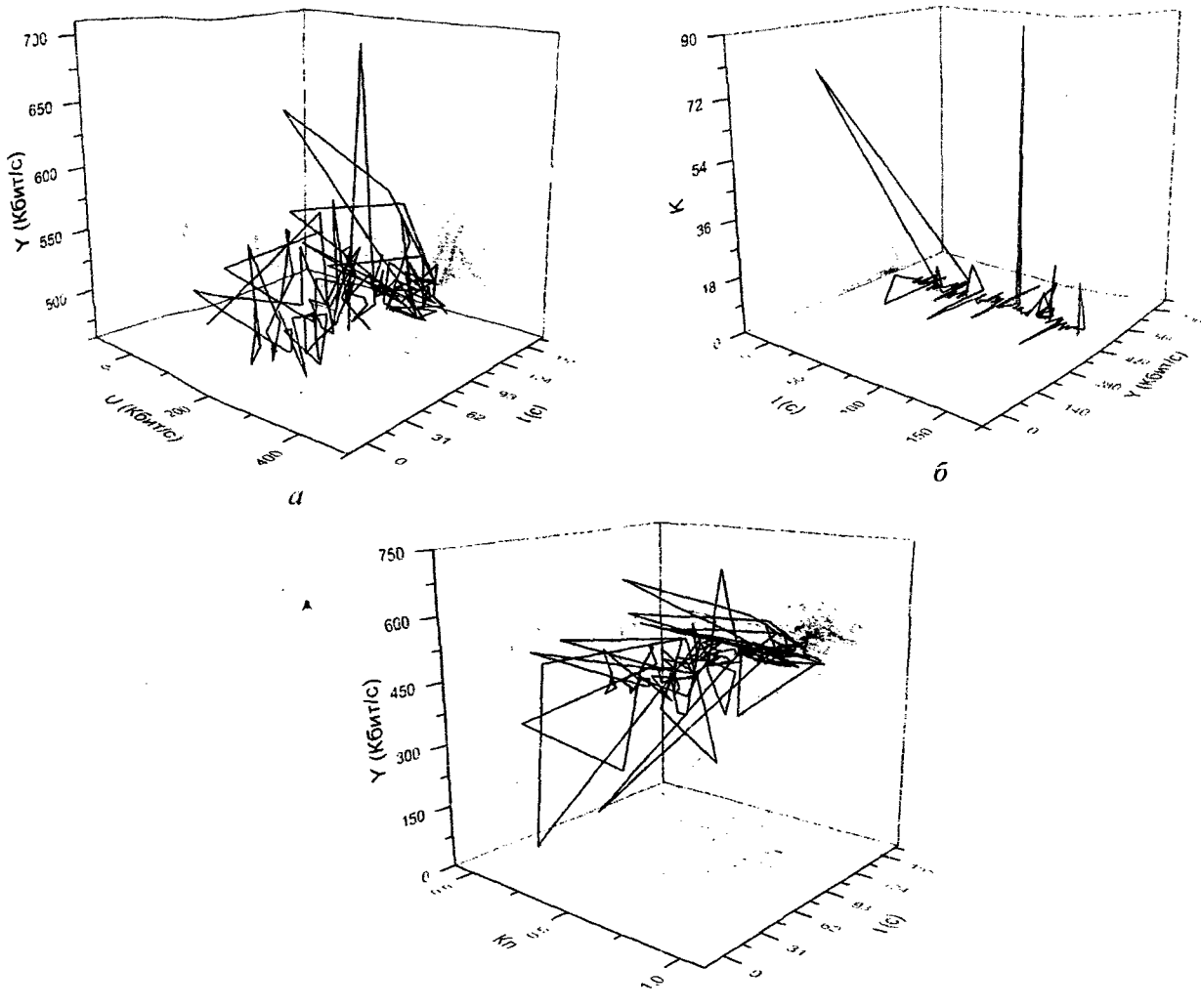


Рис. 2

Рассмотрим зависимости $u_i = u_i(y)$, $k_i = k_i(y)$ и $kn_i = kn_i(y)$, где $u_i(y)$, $k_i(y)$, $kn_i(y)$ – проекция точек u_i, k_i, kn_i на плоскости $\{y, u_i\}, \{y, k_i\}, \{y, kn_i\}$ соответственно и аппроксимируем их линейными моделями $\overline{\varphi}_{u_i}$, $\overline{\varphi}_{k_i}$, $\overline{\varphi}_{kn_i}$ (на основе полученных данных добавим линии тренда), то есть получим оценку изменений переменных $u_i(y)$, $k_i(y)$, $kn_i(y)$ в среднем:

$$\overline{\varphi}_{u_i} : u_i = u_i(y) = a_{0,i} + a_{1,i} y, \tag{13}$$

$$\overline{\varphi}_{k_i} : k_i = k_i(y) = b_{0,i} + b_{1,i} y, \tag{14}$$

$$\overline{\varphi}_{kn_i} : kn_i = kn_i(y) = c_{0,i} + c_{1,i} y, \tag{15}$$

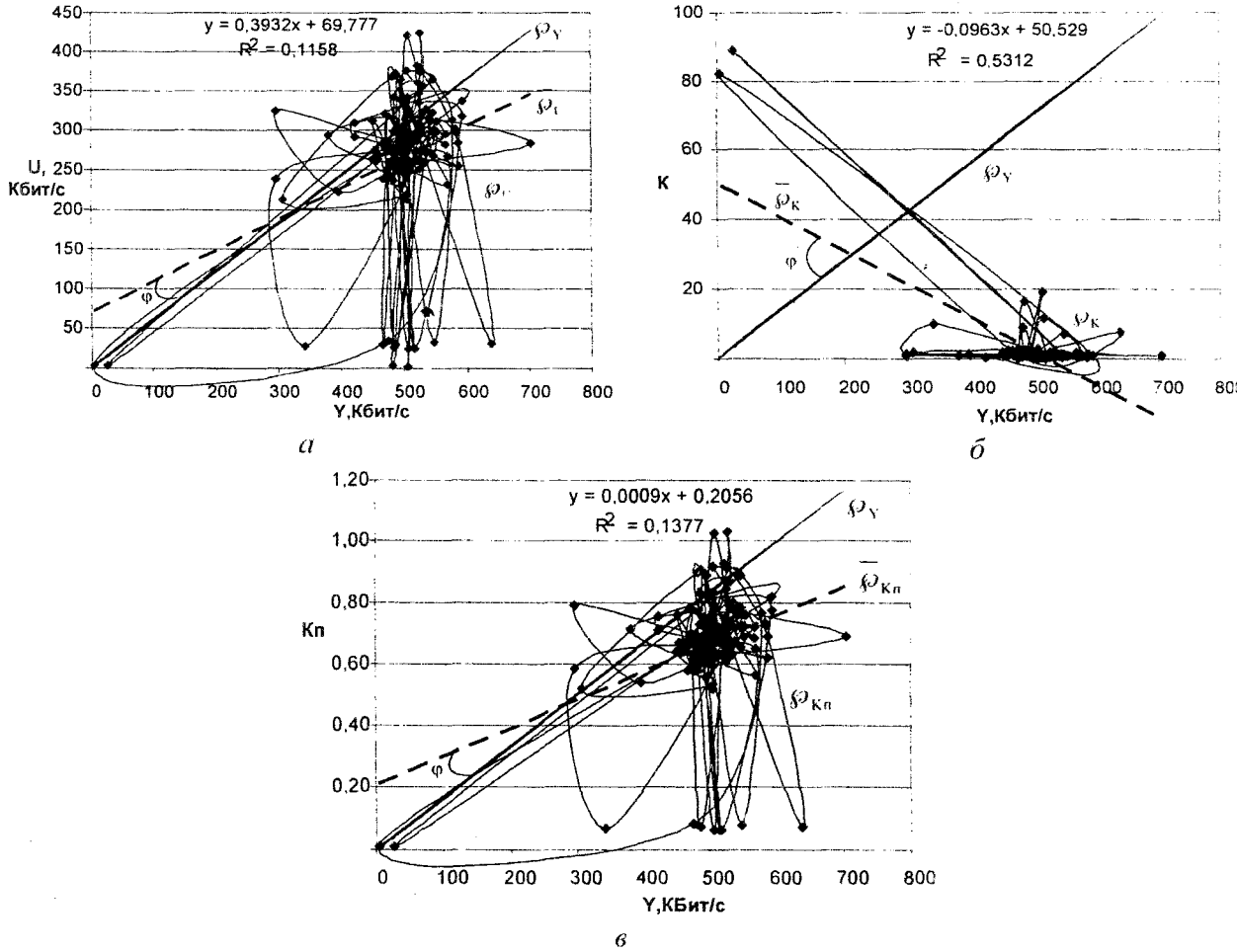
где $a_{0,i}, a_{1,i}, b_{0,i}, b_{1,i}, c_{0,i}, c_{1,i}$ – некоторые числа.

Найдем среднеквадратическое отклонение для переменных u_i, k_i, kn_i:

$$\sigma_{u_i}\{\sigma_{k_i}, \sigma_{kn_i}\} = \sqrt{\frac{1}{n}\sum_{j=1}^{n}\left[\begin{matrix} u_i(t_j)\{k_i(t_j), kn_i(t_j)\} - \\ - M\{u_i, k_i, kn_i\} \end{matrix}\right]^2}. \tag{16}$$

$$\sigma_{u_i(y)}\left\{\sigma_{k_i(y)},\sigma_{kn_i(y)}\right\}=\sqrt{\frac{1}{n}\sum_{j=1}^{n}\left[\begin{array}{l}u_i(t_j)\left\{k_i(t_j),kn_i(t_j)\right\}-\\-u_i(y_j)\left\{k_i(y_j),kn_i(y_j)\right\}\end{array}\right]^2}, \quad (17)$$

где $t_j \in J$ – дискретный момент получения данных эксперимента ($j=\overline{1,n}$); $M\{u_i, k_i, kn_i\}$ – математическое ожидание случайных величин u_i, k_i, kn_i; $u_i(y_j)$ – оценка математического ожидания, полученная с помощью модели (13) – (15).



а *б* *в*

Рис. 3

Для оценки степени связности переменных $u_i\{k_i, kn_i\}$ и y определим характеристики:

$$\varpi_{u_i\{k_i,kn_i\}}=\frac{a_{1,i}\left\{b_{1,i},c_{1,i}\right\}-1}{1+a_{1,i}\left\{b_{1,i},c_{1,i}\right\}}, \quad (18)$$

$$\kappa_{\gamma_{u_i}}=\frac{\sigma_{u_i}\left\{\sigma_{k_i},\sigma_{kn_i}\right\}}{\sigma_{u_i(y)}\left\{\sigma_{k_i(y)},\sigma_{kn_i(y)}\right\}}, \quad (19)$$

где $\varpi_{u_i\{k_i,kn_i\}}=tg\varphi$ – угол между прямыми γ_y и $\gamma_{u_i}\left\{\gamma_{k_i},\gamma_{kn_i}\right\}$.

Характеристика ϖ отражает влияние переменных u_i, k_i, kn_i на переменную y в (12). Величина $\kappa_{\gamma_{u_i}}$ характеризует степень взаимосвязи переменных u_i, k_i, kn_i и y.

Пусть $\hbar_{y,u_i}$, $\hbar_{y,k_i}$, $\hbar_{y,kn_i}$ – коэффициенты связности переменных y с u_i, k_i, kn_i соответственно:

$$\hbar_{y,u_i\{k_i,kn_i\}} = \mathrm{sgn}(\varpi_{u_i\{k_i,kn_i\}})\kappa_{\gamma_{u_i\{k_i,kn_i\}}},$$

где $\mathrm{sgn}(\varpi_{u_i\{k_i,kn_i\}})$ – функция направления:

$$\mathrm{sgn}(\varpi_{u_i\{k_i,kn_i\}}) = \begin{cases} 1, \varpi > 0 \\ -1, \varpi < 0 \end{cases}.$$

Проведенные исследования [2, 3, 7] показали, что для любого $\hbar_{y,u_i\{k_i,kn_i\}}$ справедливо

$$\hbar_{y,u_i\{k_i,kn_i\}} = g_{y,u_i\{k_i,kn_i\}}, \qquad (20)$$

где $g_{y,u_i\{k_i,kn_i\}}$ – коэффициент взаимной корреляции между y и u_i, k_i, kn_i.

В таблице представлены значения коэффициентов $\hbar_{y,u_i\{k_i,kn_i\}}$, $g_{y,u_i\{k_i,kn_i\}}$ и $\varpi_{u_i\{k_i,kn_i\}}$ для случаев использования наблюдаемых структурно-информационных портретов подсистемы информационного обеспечения в условиях воздействия на нее Dos-атаки (см. рис. 3).

	$\hbar_{y,u_i\{k_i,kn_i\}}$	$g_{y,u_i\{k_i,kn_i\}}$	$\varpi_{u_i\{k_i,kn_i\}}$
u_i	0.319	0.319	0.972
k_i	0.02	0.02	0.961
kn_i	-0.004	-0.004	-0.659

Из результатов эксперимента, приведенных в таблице, видно, что g_{y,u_i} имеет наибольшее значение, и, следовательно, переменную u_i целесообразно использовать в качестве информативной переменной при структурной идентификации и моделировании информационной системы.

Выводы

Таким образом, в результате проведенных исследований предложен подход к моделированию информационной системы в условиях априорной неопределенности. Такой подход позволит повысить точность структурной идентификации системы в условиях воздействия на нее различного рода помех.

Построены и исследованы расширенный фазовый и наблюдаемые структурно-информационные портреты информационной системы в условиях воздействия на нее Dos-атаки. На их примерах показано возникновение структурных изменений (характерных для подсистемы информационного обеспечения в целом).

Проведена оценка характеристик наблюдаемых структурно-информационных портретов информационной системы в условиях воздействия Dos–атаки. Выявлено, что при структурной идентификации и моделировании информационной системы в качестве информативной переменной целесообразно использовать переменную u_i.

Список литературы: 1. *Городецкий А.Я.* Информационные системы. Вероятностные модели и статистические решения : Учеб. пособие / А.Я.Городецкий. – СПб : Изд-во СПбГПУ, 2003. – 326 с. 2. *Карабутов Н.Н.* Адаптивная идентификация систем: Информационный синтез / Н.Н.Карабутов. – М. : КомКнига, 2006. – 384 с. 3. *Карабутов Н.Н.* Структурная идентификация систем: анализ динамических структур / Н.Н.Карабутов. – М. : МГИУ, 2008. – 160 с. 4. *Киричков В.Н.* Построение адаптивных моделей динамических объектов по данным эксперимента / В.Н. Киричков, А.Н. Сильвестров. – К. : Вища шк., 1985. – 68 с. 5. *Кузнецов А.А.* Метод структурной идентификации информационных пото-

ков в телекоммуникационных сетях на основе BDS-тестирования / А.А.Кузнецов, С.Г.Семен С.Н.Симоненко, Е.В.Мелешко // Наука і техніка Повітряних Сил Збройних Сил України. – 2010 Вип. 2 (4). – Х. : ХУПС. – С. 131 – 137. 6. *Кузнецов Д.Ф.* Численное моделирование стохастическ дифференциальных уравнений и стохастических интегралов / Д.Ф. Кузнецов. – СПб. : Наука, 199 463 с. 7. *Семенов С.Г.* Структурно-функциональный анализ современных информационных систе разработкой комплексного показателя эффективности их функционирования / С.Г. Семенов // Зб. ук. праць. Системи обробки інформації. – Х. : ХУ ПС, 2011. – Вип. 2(92). – С.145-150. 8. *Семенов С* Сравнительные исследования методов идентификации трафика в телекоммуникационной сети повышения оперативности передачи данных / С.Г.Семенов, Е.В.Мелешко // Прикладная радиоэле троника. – 2010. – Т. 9, №3. – С.444-448.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 05.09.2