УДК 007: 519.876.5

В.В. Лавлинский, Д.В. Сысоев, О.В. Чурко, Н.Т. Югов

Построение топологического пространства взаимодействия системы защиты информации с внешней средой

Рассматриваются оценки достижения устойчивого результата взаимодействия подсистем защиты информации и подсистемы «проникновения», а также построение топологического пространства информационной системы в целом.

Анализ взаимодействия двух систем (системы защиты информации (СЗИ) при выбранной политике безопасности и системы «проникновения» (СЗЛ)) определяет непрерывность данного процесса в реальном масштабе времени. В [3] рассматривается взаимодействие систем защиты информации и систем «проникновения» при выбранной политике безопасности, а также анализируются виды взаимодействия этих двух систем и выявляются их отношения.

В работе [3] результатом функционирования информационной системы (ИС) со встроенными средствами защиты и существующими СЗЛ является либо недостижимость защищаемой информации для системы «проникновения», либо ее доступность (достижимость) для системы СЗЛ. В первом случае будем считать, что взаимодействие нейтрально, т.е. система защиты информации при выбранной политике безопасности выполняет свои функции и ей не требуется дополнительных действий по устранению угроз безопасности информации (БИ). Во втором случае принимается, что взаимодействие систем будет конфликтно, т.е. СЗИ при выбранной политике безопасности информации не выполняет свои функции, и ей требуются дополнительные меры по устранению угроз безопасности информации.

Так же как и в [1], формально представим описание информационной системы тройкой ИС = {ИС, G, R}, ИС $\subset X(t) \times Y(t)$, $X(t) = \times \{X(t)\}_m$ — входной объект системы $Y(t) = \times \{Y(t)\}_p$ — выходной объект системы ($t \in T = [0, T]$ – время, $\times$ — символ декартова произведения); ИС = $\{СЗИ_i\}_N$ — множество элементов (подсистем), $СЗИ_i \subset X_i(t) \times Y_i(t)$, $X_i(t) = \times \{X_{ik}(t)\}$, $X_{ik}(t) = \{x_{ik}(t)\}$, $k = \overline{1, m_i}$, $Y_i(t) = \times \{Y_{ir}(t)\}$, $Y_{ir} = \{y_{ir}(t)\}$, $r = \overline{1, \rho_i}$; G = (ИС, E) — ориентированный граф с множеством вершин ИС, |ИС| = N и множеством дуг E = $\{e_{ij}\}$, |E| = M, характеризующий $\forall$ i,j $= \overline{1,N}$ наличие связей между подсистемами $СЗИ_i$ М ИС; R = < R, F > — алгебра, где $R(t) = \{R(C(t), X(t))\}_N$ ($R_i(t)$: $(C_i(t) \times X_i(t)) \rightarrow Y_i(t)$ — отображение, $C(t) = \times \{C_i(t)\}$, $C_i(t) = \{C_{in}(t)\}$, $n = \overline{1, m_i}$ — множество глобальных состояний i-й подсистемы) = множество носитель; $F(t) = \{f_1, f_2, ..., f_x\}$ — сигнатура алгебры.

Общую систему действий, формирования влияний и воздействий можно описать деревом [1], вид которого представлен на рис. 1.

В [3] были сформулированы определения, показывающие взаимодействия подсистем системы ИС, таких как СЗИ и СЗЛ.

В первом случае подсистема $СЗИ_i$ вступает в отношение безразличия $>I_6$ к подсистеме $СЗЛ_j$ (($СЗИ_i$, $СЗЛ_j$) $\in >I_6$), если система защиты информации достижима для системы «проникновения» $СЗИ_i \vec{d}\ СЗЛ_j \wedge q'_j(b_{ij}) = 0$. Подсистема $СЗЛ_j$ вступает в отношение безразличия $>I_6$ к подсистеме $СЗИ_i$ (($СЗЛ_j$, $СЗИ_i$) $\in >I_6$), если система защиты информации контрдостижима (недостижима) для системы «проникновения» $СЗИ_i \bar{d}\ СЗЛ_j \wedge q'_i(b_{ji}) = 0$. Граф этих отношений показан на рис. 2.

Подсистема $СЗИ_i$ вступает в отношение конфликта >I к подсистеме $СЗЛ_j$ (($СЗИ_i$, $СЗЛ_j$) $\in$ >I), если $СЗИ_i \vec{d}\ СЗЛ_j \wedge q'_j(b_{ij}) < 0$, и подсистема $СЗЛ_j$ вступает в отношение конфликта >I к подсистеме $СЗИ_i$ (($СЗЛ_j$, $СЗИ_i$) $\in$ >I), если $СЗИ_i \bar{d}\ СЗЛ_j \wedge q'_i(b_{ji}) < 0$. Граф этих отношений показан на рис. 3.

Рассмотрим бинарные отношения элементов множества ИС. Для этого выберем произвольный элемент ($СЗИ_i$, $СЗЛ_j$) $\in ИС^2 = ИС \times ИС$. Действие D_{ij} элемента $СЗИ_i$ на $СЗЛ_j$ возможно лишь при наличии отношения достижимости $СЗИ_i \vec{d}\ СЗЛ_j$ (аналогично и для действия D_{ji} — наличие отношения контрдостижимости $СЗИ_i \bar{d}\ СЗЛ_j$ и взаимного действия — наличие отношения взаимной достижимости $СЗИ_i \vec{d}\ СЗЛ_j = \{СЗИ_i \vec{d}\ СЗЛ_j \wedge СЗИ_i \bar{d}\ СЗЛ_j\}$).

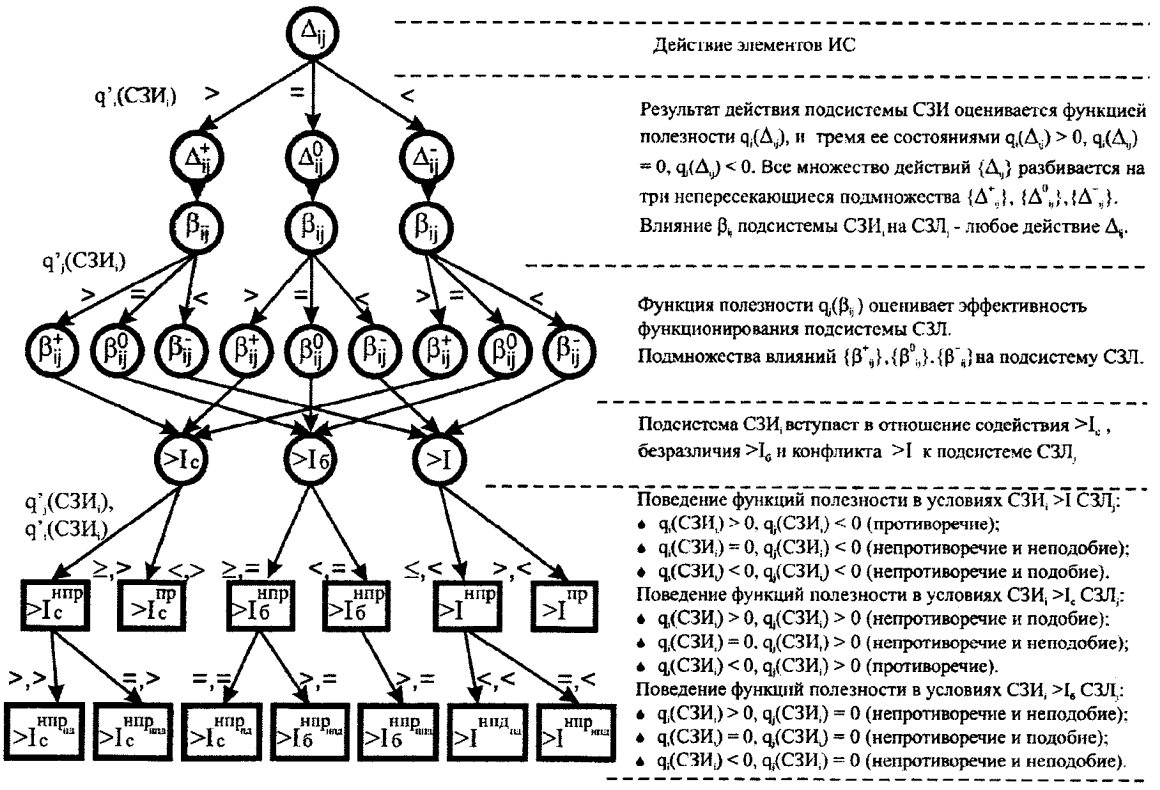

Рис. 1. Граф — дерево системы действий

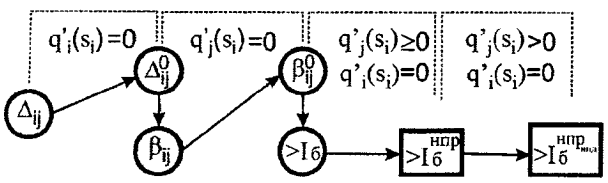

Рис. 2. Граф действий при $СЗИ_i \vec{d}\ СЗЛ_j$

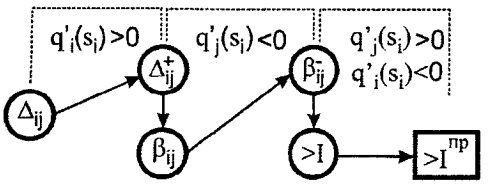

Рис. 3. Граф действий при $СЗИ_i \vec{d}\ СЗЛ_j$

Тогда можно говорить и об отношениях: $СЗИ_i \vec{\vec{d}}\ СЗЛ_j$ — вершина СЗЛ$_j$ не достижима из вершины СЗИ$_i$; $СЗИ_i \vec{\vec{d}}\ СЗЛ_j$ — вершина СЗИ$_i$ не достижима из вершины СЗЛ$_j$; $СЗИ_i \vec{\vec{d}}\ СЗЛ_j$ — вершина СЗЛ$_j$ не достижима из вершины СЗИ$_i$ и вершина СЗИ$_i$ не достижима из вершины СЗЛ$_j$.

Определение 1. Подсистемы СЗИ$_i$ и СЗЛ$_j$ вступают в отношение:

• взаимоконфликта ((СЗИ$_i$, СЗЛ$_j$) $\in$ $>I$), если (СЗИ$_i$, СЗЛ$_j$) $\in$ $>I \wedge$ (СЗЛ$_j$, СЗИ$_i$) $\in$ $>I$;

• взаимобезразличия ((СЗИ$_i$, СЗЛ$_j$) $\in$ $>I$), если (СЗИ$_i$, СЗЛ$_j$) $\in$ $>I_б \wedge$ (СЗЛ$_j$, СЗИ$_i$) $\in$ $>I_б$.

Свойства. Рассмотрим отдельные свойства введенных бинарных отношений:

• определения (3) – (4), приведенные в [3], выражают односторонние отношения, тогда как определение 1 — двустороннее отношение;

• $= \{>I \cup >I_б\}$, $>I \cap >I_б = \varnothing$.

Заметим, что рассмотренные свойства справедливы и для симметричных отношений, введенных определением 1.

Особый интерес представляет рассмотрение отношений независимости в системе (независимость в целом), которое приводит к так называемым приведенным системам [4].

Топологическое пространство на ИС^2. Рассмотрим отношения $СЗИ_i\ d\ СЗЛ_j$, $СЗИ_i \vec{d}\ СЗЛ_j$, $СЗИ_i \vec{\vec{d}}\ СЗЛ_j$, на всем множестве ИС^2, способы их построения и ряд свойств.

При взаимодействии двух подсистем (СЗИ и СЗЛ) каждая из них стремится достичь противоположного результата, то есть вероятность достижения цели одной строной является вероятностью недостижения этой цели для другой стороны.

Построение вышевведенных отношений связано с формированием так называемых матриц достижимости $D^+(G) = [d]_{N\Gamma N}$ и недостижимости $D(G) = [d]_{N\Gamma N}$ [5]. Элементы матриц определяются следующим образом:

$$d_{ij}^{+} = \begin{cases} 1, & \text{если } СЗИ_i \vec{d}\, СЗЛ_j, \\ 0, & \text{если } СЗИ_i \vec{d}\, СЗЛ_j; \end{cases} \qquad d_{ij}^{-} = \begin{cases} 1, & \text{если } СЗИ_i \bar{d}\, СЗЛ_j, \\ 0, & \text{если } СЗИ_i \bar{d}\, СЗЛ_j. \end{cases} \tag{1}$$

Из соотношений (1) следует, что $D = |D^+|^{tr}$, где $|D^+|^{tr}$ — транспонированная матрица достижимостей D^+.

В соответствии с матрицами D^+ и D^- $\forall$ $i = \overline{1,N}$ рассмотрим сечения по $СЗИ_i$ в виде отношений $СЗИ_i \vec{d}\, СЗЛ_j$, $СЗИ_i \bar{d}\, СЗЛ_j$, которые представим следующим образом: $>I_{\partial}^{+}$ ($СЗИ_i$) = {$СЗЛ_j \subset$ ИС: $d_{ij}^{+}=1$} и $>I_{\partial}^{-}$ ($СЗИ_i$) = {$СЗЛ_j \subset$ ИС: $d_{ij}^{-}=1$}. Здесь $>I_{\partial}^{+}$ ($СЗИ_i$) — множество подсистем $СЗЛ_j \subset$ ИС, на которые может оказывать действие подсистема $СЗЛ_i$, а $>I_{\partial}^{-}$ ($СЗИ_i$) — множество подсистем $СЗЛ_j \subset$ ИС, которые могут оказывать действие на подсистему $СЗИ_i$, причем не исключается i = j. Эти множества позволяют построить и сечение $>I_{\partial}^{ss}$ ($СЗИ_i$) = $>I_{\partial}^{+}$ ($СЗИ_i$) З $>I_{\partial}^{-}$ ($СЗИ_i$) ={$СЗЛ_j \subset$ ИС: $d_{ij}^{+}=1 \wedge d_{ij}^{-}=1$} — множество подсистем $СЗЛ_j$ М ИС, таких, что каждое $СЗИ_i$ может действовать на любое $СЗЛ_j$ и наоборот, каждое $СЗЛ_j$ может действовать на любое $СЗИ_i$, причем при i = j, $d_{ij}^{+}=d_{ij}^{-}=1$ и $СЗИ_i$ может оказывать действие само на себя (т.е. существует обратная связь).

Аналогично: $>I_{н}^{+}$ ($СЗИ_i$) = {$СЗЛ_j \subset$ ИС: $d_{ij}^{+}=0$, $j \neq i$} — множество подсистем $СЗЛ_j \subset$ ИС, на которые не может оказывать действие подсистема $СЗИ_i$; $>I_{н}^{-}$ ($СЗИ_i$) = {$СЗЛ_j \subset$ ИС: $d_{ij}^{-}=0$, $j \neq i$}; множество подсистем $СЗЛ_j \subset$ ИС, которые не могут оказывать действие на подсистему $СЗИ_i$; $>I_{н}^{ss}$ ($СЗИ_i$) = $>I_{н}^{+}$ ($СЗИ_i$) З $>I_{н}^{-}$ ($СЗИ_i$) ={$СЗЛ_j \subset$ ИС: $d_{ij}^{+}=0 \wedge d_{ij}^{-}=0$, $j \neq i$} — множество подсистем $СЗЛ_j \subset$ ИС, на которые, с одной стороны, не может оказывать действие подсистема $СЗИ_i$, а, с другой стороны, каждая из которых не может оказывать действие на подсистему $СЗИ_i$.

Построенные сечения позволяют определить на $ИС^2$ множества бинарных отношений $>I_{\partial}^{+} = \bigcup_i \{СЗИ_i \times >I_{\partial}^{+}\ (СЗИ_i)\}$; $>I_{\partial}^{-} = \bigcup_i \{СЗИ_i \times >I_{\partial}^{-}\ (СЗИ_i)\}$; $>I_{\partial}^{ss} = \bigcup_i \{СЗИ_i \times >I_{\partial}^{ss}\ (СЗИ_i)\}$; $>I_{н}^{+} = \bigcup_i \{СЗИ_i \times >I_{н}^{+}\ (СЗИ_i)\}$; $>I_{н}^{-} = \bigcup_i \{СЗИ_i \times >I_{н}^{-}\ (СЗИ_i)\}$; $>I_{н}^{ss} = \bigcup_i \{СЗИ_i \times >I_{н}^{ss}\ (СЗИ_i)\}$.

Эти отношения в совокупности с самим множеством $ИС^2$ и пустым множеством Ж образуют так называемую топологию $\Sigma = \{\sigma\} = \{>I_{\partial}^{+}, >I_{\partial}^{-}, >I_{н}^{+}, >I_{н}^{-}, >I_{\partial}^{ss}, >I_{н}^{ss}, ИС^2, :\varnothing\}$ на множестве $ИС^2$. И, следовательно, задают топологическое пространство $Т(ИС^2) = (ИС^2, \Sigma)$ [6].

Рассмотрим ряд свойств структуры пространства $Т(ИС^2)$, вытекающих из вышепредставленного построения и свойств бинарных отношений в соответствии с [7] :

$-{>}I_{\partial}^{+} \cup >I_{н}^{+} = ИС^2$ ($>I_{\partial}^{+} \cap >I_{н}^{+} = \varnothing$, $ИС^2 \setminus >I_{\partial}^{+} = >I_{н}^{+} \wedge ИС^2 \setminus >I_{н}^{+} = >I_{\partial}^{+} \Rightarrow >I_{н}^{+} = `>I_{\partial}^{+} \wedge >I_{\partial}^{+} = `>I_{н}^{+}$); $>I_{\partial}^{-} \cup >I_{н}^{-} = ИС^2$ ($>I_{\partial}^{-} \cap >I_{н}^{-} = \varnothing$, $ИС^2 \setminus >I_{\partial}^{-} = >I_{н}^{-} \wedge ИС^2 \setminus >I_{н}^{-} = >I_{\partial}^{-} \Rightarrow >I_{н}^{-} = `>I_{\partial}^{-} \wedge >I_{\partial}^{-} = `>I_{н}^{-}$;

$-{>}I_{\partial}^{+}$, $>I_{\partial}^{-}$ — множества полных ($(СЗИ_i, СЗЛ_j) \in >I_{\partial}^{+} \vee (СЗИ_i, СЗЛ_j) \in >I_{\partial}^{-}$ либо $(СЗИ_i, СЗЛ_j) \in >I_{\partial}^{+} \wedge (СЗИ_i, СЗЛ_j) \in >I_{\partial}^{-}$), рефлексивных ($(СЗИ_i, СЗЛ_j) \in >I_{д}$ — всегда считается, что сама вершина $СЗИ_i$ графа G достижима из себя самой с помощью пути длиной 0), транзитивно полных (из $(ИС_1, ИС_2) \in >I_{д} \wedge (ИС_2, ИС_3) \in >I_{д} \wedge (ИС_{n-1}, ИС_n) \in >I_{д} \Rightarrow (ИС_1, ИС_n) \in >I_{д}$, n=1,2,3, ...) отношений, где $>I_{д} = >I_{\partial}^{+} \vee >I_{\partial}^{-}$;

$-{>}I_{н}^{+}$, $>I_{н}^{-}$ — множества слабополных ($\forall$ i ≠ j $(СЗИ_i, СЗЛ_j) \in >I_{н}^{+} \vee (СЗИ_i, СЗЛ_j) \in >I_{н}^{-}$ либо $(СЗИ_i, СЗЛ_j) \in >I_{н}^{+} \wedge (СЗИ_i, СЗЛ_j) \in >I_{н}^{-}$, антирефлексивных ($(СЗИ_i, СЗЛ_j) \notin >I_{н}$), негатранзитивных (из свойства 1 — дополнение отношений `$>I_{н}$ транзитивно) отношений, где $>I_{н} = >I_{н}^{+} \vee >I_{н}^{-}$;

– множество отношений $>I_{\partial}^{+}$ является обратным к $>I_{\partial}^{-}$ и наоборот, т.е. $(>I_{\partial}^{-})^{-1} = >I_{\partial}^{+} \Rightarrow \bigcup_i \{>I_{\partial}^{-}\ (СЗИ_i) \times СЗИ_i\} = \bigcup_i \{\ СЗИ_i \times >I_{\partial}^{+}\ (СЗИ_i)\}$; и $(>I_{\partial}^{+})^{-1} = >I_{\partial}^{-} \Rightarrow \bigcup_i \{>I_{\partial}^{+}\ (СЗИ_i) \times СЗИ_i\} = \bigcup_i \{СЗИ_i \times >I_{\partial}^{-}\ (СЗИ_i)\}$; аналогично: $(>I_{н}^{-})^{-1} = >I_{н}^{+} \Rightarrow \bigcup_i \{>I_{н}^{-}\ (СЗИ_i) \times СЗИ_i\} = \bigcup_i \{\ СЗИ_i \times >I_{н}^{+}\ (СЗИ_i)\}$; и $(>I_{н}^{+})^{-1} = >I_{\partial}^{-} \Rightarrow \bigcup_i \{>I_{н}^{+}\ (СЗИ_i) \times СЗИ_i\} = \bigcup_i \{СЗИ_i \times >I_{н}^{-}\ (СЗИ_i)\}$ следует из $D^- = (D^+)^{tr}$;

– множество отношений $>I_{\partial}^{ss} = >I_{\partial}^{+} \cap (>I_{\partial}^{+})^{-1} = >I_{\partial}^{-} \cap (>I_{\partial}^{-})^{-1} = >I_{\partial}^{+} \cap >I_{\partial}^{-}$ — является симметричной частью множеств $>I_{\partial}^{+}$ и $>I_{\partial}^{-}$. И так как оно рефлексивно, транзитивно и симметрично, то это множество эквивалентных отношений (эквивалентность);

– множество отношений $>I_{н}^{ss} = >I_{н}^{+} \cap (>I_{н}^{+})^{-1} = >I_{н}^{-} \cap (>I_{н}^{-})^{-1} = >I_{н}^{+} \cap >I_{н}^{-}$ — является симметричной частью $>I_{н}^{+}$ и $>I_{н}^{-}$;

– $>I_{\partial}^{ss} \cap >I_{н}^{ss} = \varnothing$ (из свойства 1), $>I_{\partial}^{ss} \cup >I_{н}^{ss}$ — является симметричной частью ИС[2].

Действие и взаимодействие подсистем СЗИ и СЗЛ в рамках рассматриваемой информационной системы ИС, а также отношения достижимости и/или контрдостижимости будут зависеть от того, насколько адекватно будет реализована основная функция системы защиты информации. А также существенно влиять на свойства системы такие, как запас и степень устойчивости, быстродействие системы [2].

На структурной модели взаимодействия (рис. 4) СЗИ и СЗЛ в рамках ИС толстыми пунктирными линиями показано, что $(СЗИ_i, СЗЛ_j) \in >I_6$, если система защиты информации достижима для системы «проникновения» $\wedge q'_j(b_{ij}) = 0$. И $(СЗЛ_j, СЗИ_i) \in >I_6$, если система защиты информации контрдостижима (недостижима) для системы «проникновения» $\wedge q'_i(b_{ji}) = 0$. А толстыми сплошными линиями показано, что $(СЗИ_i, СЗЛ_j) \in >I$, если $\wedge q'_j(b_{ij}) < 0$ и $(СЗЛ_j, СЗИ_i) \in >I$, если $\wedge q'_i(b_{ji}) < 0$.

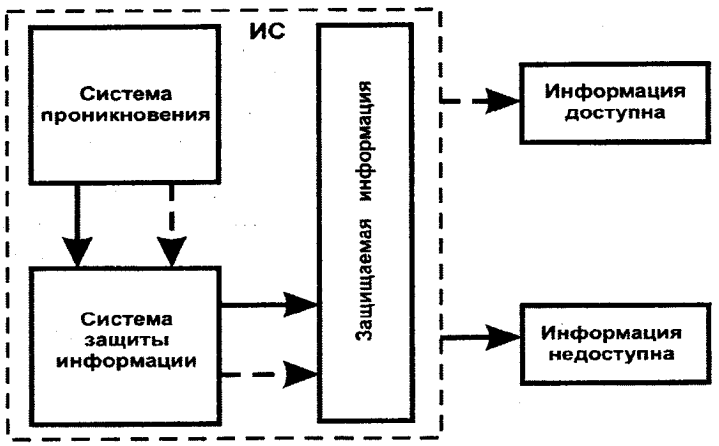

Рис. 4. Структурная модель взаимодействия СЗИ и СЗЛ

Литература

1. Сысоев В.В. Действие и взаимодействие систем: структурно-параметрическое представление / В.В. Сысоев, Д.В. Сысоев. – Воронеж : Центрально-черноземное книжное издательство, 2004. – 70 с.

2. Лавлинский В.В. Моделирование взаимодействия систем защиты информации вычислительных сетей с внешней средой / В.В. Лавлинский, Ю.С. Сербулов, Д.В. Сысоев. – Воронеж : Центрально-черноземное книжное издательство, 2004. – 135 с.

3. Лавлинский В.В. Взаимодействие систем защиты информации и систем «проникновения» при выбранной политике безопасности / В.В. Лавлинский, Д.В. Сысоев // Моделирование систем и информационные технологии: межвуз. сб. науч. тр. – Воронеж : Научная книга, 2007. – Вып. 4. – С. 69–72.

4. Сысоев В.В. Приведенные системы и условия возникновения частичного конфликта // Вестник ВГТА (Воронеж). – 2000. – № 5. – С. 47–54.

5. Гантмахер Ф.Р. Лекции по аналитической механике. – М. : Физматгиз, 1960. – 296 с.

6. Ильин В.А. Математический анализ / В.А. Ильин, В.А. Садовничий, Бл.Х. Сендов. – М. : Наука, 1979. – 720 с.

7. Юдин Д.Б. Вычислительные методы теории принятия решений. – М. : Наука, 1989. – 320 с.

Лавлинский Валерий Викторович
Канд. техн. наук, доцент каф. информационных систем
Воронежского института высоких технологий
Тел.: (4732) 79 43 08; 20 56 50
Эл. почта: lavlinsk@box.vsi.ru

Сысоев Дмитрий Валериевич
Канд. техн. наук, доцент каф. информационных систем
Воронежского института высоких технологий
Тел.: (4732) 27 51 50; 20 56 50
Эл. почта: SysoevD@yandex.ru

Чурко Олег Васильевич
Директор НПРУП «Научно-исследовательский институт технической защиты информации»
Тел.; 285 31 86
Эл. почта: och@niitzi.by

Югов Николай Тихонович
Д-р физ.-мат. наук, профессор каф. высшей математики ТУСУРа,
Тел.: (3822) 41 74 33
Эл. почта: M.T.Yugov@mail.ru

V.V. Lavlinskiy, D.V. Sysoev, O.V. Churko, N.T Yugov
Building topological space interactions of the system of protection to information with external ambience

They are considered estimations of the achievement of the firm result of the interaction of the subsystems of protection to information and subsystems "penetrations", as well as building topological space information system as a whole.