Анна Корченко
Национальный авиационный университет
УДК 004.056.53(045)

КОРТЕЖНАЯ МОДЕЛЬ ФОРМИРОВАНИЯ НАБОРА БАЗОВЫХ КОМПОНЕНТ ДЛЯ ВЫЯВЛЕНИЯ КИБЕРАТАК

Аннотация: **На основе кортежной модели предлагается формализация подхода к формированию необходимого набора компонент, используемого для контроля в нечетких условиях состояния параметров среды окружения в заданный момент времени, посредством которого можно выявить аномальное состояние, порожденное воздействием соответствующего класса кибератак.**
Summary: **This paper, based on a tuple, proposes the formalization of approach to build up the necessary Dataset component used to control in fuzzy environment the condition of environment parameters at a given point of time what makes possible to detect an abnormal condition caused by the effects of the relevant class of cyber-attacks.**
Ключевые слова: **Кортежная модель, кибератаки, аномалии, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, обнаружение аномалий в компьютерных сетях.**

I Актуальность

В последние годы происходит значительное увеличение объемов информации, накапливаемой, хранимой и обрабатываемой с помощью компьютерных систем. При этом концентрирование в единых базах данных информации различного назначения и принадлежности, а также резкое расширение круга пользователей, имеющих непосредственный доступ к ресурсам информационных систем (РИС), порождают проблему обеспечения их защиты от различного рода вторжений. Рост сложности аппаратно-программных средств и существующие недостатки современных информационных технологий приводят к совершенствованию кибератак на РИС. Следует отметить, что несанкционированные воздействия на РИС оказывают влияние и на среду окружения [1], порождая в ней, как следствие, определенные аномалии. Такая среда обычно сложноформализуема, нечетко определенная и для решения задач выявления кибератак, породивших аномалии в этой среде необходимы соответствующие средства, которые дают возможность обнаружить вторжение по множеству различных характерных признаков. Один из подходов к решению такого рода задач основывается на использовании соответствующих моделей, методов и систем обнаружения вторжений, которые базируются на нечетких множествах, ориентированных на обработку слабоструктурированных данных с целью установления фактов несанкционированного доступа к РИС, например, через компьютерные сети. Исходя из этого, создание моделей, позволяющих формализовать процесс выявления кибератак путем контроля текущего состояния параметров среды окружения в нечетких условиях, есть актуальной научной задачей.

II Анализ существующих исследований

Известны отдельные, достаточно эффективные разработки, используемые для решения указанных задач выявления атак, например, такие как базовая модель параметров [2], универсальная модель эталонов [3], модель эвристических правил [1], метод выявления аномалий, порожденных кибератаками [4], группа соответствующих видов систем [5 – 7], а также другие разработки, используемые для решения задач защиты в нечетких условиях [8]. Указанные исследования показали эффективность соответствующего применения математического аппарата нечетких множеств, а его использование для формализации подхода к выявлению кибератак, позволит усовершенствовать процесс создания соответствующих систем обнаружения вторжений. Следует отметить, что в указанных и других источниках не формализован подход к формированию необходимого набора компонент, используемого для контроля в нечетких условиях состояния параметров среды окружения в заданный момент времени, посредством которого можно выявить аномальное состояние, порожденное воздействием соответствующего класса кибератак.

III Основная цель исследования

Исходя из актуальности и проведенного анализа существующих исследований целью данной работы является осуществление формализации подхода к формированию набора базовых компонент, посредством которого можно эффективно детектировать в слабоформализованной нечетко определенной среде аномальное состояние в заданный временной промежуток.

IV Основная часть исследования

Для решения поставленной задачи предлагается математическая модель формирования величин, основу которой составляет кортеж, состоящий из идентификатора (ИД) кибератаки, а также таких компонент, как подмножества: возможных параметров; возможных нечетких (лингвистических) эталонов; текущих значений нечетких параметров; детекционных правил.

Для формализации процесса формирования указанных компонент введем множество возможных кибератак $\mathbf{CA}$, которые могут воздействовать на РИС за определенный временной промежуток τ_f (f – номер временного промежутка, $f = \overline{1,max}$) т.е.:

$$\mathbf{CA}^{\tau_f} = \{\bigcup_{i=1}^{n} \mathbf{CA}_i^{\tau_f}\} = \{\mathbf{CA}_1^{\tau_f}, \mathbf{CA}_2^{\tau_f}, \ldots, \mathbf{CA}_n^{\tau_f}\}, (i = \overline{1,n}), \quad (1)$$

где n определяет количество возможных кибератак, каждая из которых отображается обобщенным кортежем

$$\mathbf{CA}_i^{\tau_f} = < CA_i, \mathbf{P}_i, \mathbf{T}_i^e, \mathbf{P}_i^{\tau_f}, \mathbf{ER}_i >, \quad (2)$$

в котором: CA_i – ИД i-й кибератаки; $\mathbf{P}_i$ – подмножество возможных параметров, используемых для обнаружения i-й кибератаки; $\mathbf{T}_i^e$ – подмножества возможных нечетких (лингвистических) эталонов, отображающих характерные суждения эксперта относительно аномальности состояния соответствующих параметров из подмножества $\mathbf{P}_i$ в заданной среде окружения; $\mathbf{P}_i^{\tau_f}$ – подмножество текущих значений нечетких параметров, формируемых на основе $\mathbf{T}_i^e$ в момент времени τ_f $(f = \overline{1,max})$ за временной промежуток $\tau_h = \tau_f - \tau_{f-1}$; $\mathbf{DR}_i$ – подмножество детекционных правил, используемых для обнаружения i-й кибератаки. Отметим, что в совокупности все элементы подмножества $\mathbf{CA}^{\tau_f}$ определяют атакующую среду на РИС, состояние которой фиксируется временным промежутком τ_f. Рассмотрим подходы к формированию каждого из компонент кортежа (2).

Формирование CA_i. Идентификаторы CA_i определим на основе того, что каждый элемент множества $\mathbf{CA}^{\tau_f}$ связан с определенной кибератакой, которую идентифицируют по соответствующему ей имени.

Например, при $n = 3$ (1) можно определить как:

$$\mathbf{CA}^{\tau_f} = \{\bigcup_{i=1}^{3} \mathbf{CA}_i^{\tau_f}\} = \{\mathbf{CA}_1^{\tau_f}, \mathbf{CA}_2^{\tau_f}, \mathbf{CA}_3^{\tau_f}\} = \{\mathbf{CA}_{\mathbf{SN}}^{\tau_f}, \mathbf{CA}_{\mathbf{DS}}^{\tau_f}, \mathbf{CA}_{\mathbf{SP}}^{\tau_f}\} = \{\mathbf{SN}^{\tau_f}, \mathbf{DS}^{\tau_f}, \mathbf{SP}^{\tau_f}\}, \quad (3)$$

где $\mathbf{CA}_1^{\tau_f} = \mathbf{CA}_{\mathbf{SN}}^{\tau_f} = \mathbf{SN}^{\tau_f}$, $\mathbf{CA}_2^{\tau_f} = \mathbf{CA}_{\mathbf{DS}}^{\tau_f} = \mathbf{DS}^{\tau_f}$ и $\mathbf{CA}_3^{\tau_f} = \mathbf{CA}_{\mathbf{SP}}^{\tau_f} = \mathbf{SP}^{\tau_f}$, отображают состояние атакующей среды (SN-DS-SP-среды) в момент τ_f и соответственно определяют кибератаки с именами «Сканирование портов (SN)», «Отказ в обслуживании (DS)» и «Спуфинг (SP)», которым соответственно будут присвоены ИД $CA_1 = CA_{SN} = SN$, $CA_2 = CA_{DS} = DS$ и $CA_3 = CA_{SP} = SP$.

Формирование $\mathbf{P}_i$. Построение подмножества $\mathbf{P}_i$ осуществляется на основе множества всех возможных параметров $\mathbf{P}$ [2]

$$\mathbf{P} = \{\bigcup_{j=1}^{m} P_j\} = \{P_1, P_2, \ldots, P_m\}, (j = \overline{1,m}), \quad (4)$$

характеризующих состояние среды окружения, по значениям которых можно выявить аномальное состояние, порождаемое воздействием определенных кибератак, т.е. элементов из множества $\mathbf{CA}^{\tau_f}$. Учитывая, что множество $\mathbf{P}$ содержит разнородные по своей природе параметры, характеризующие различные состояния среды окружения, то совокупность всех членов этого множества определим как m-мерную (или общую)

гетерогенную параметрическую среду. Например, 6-мерную гетерогенную параметрическую среду (т.е. $m=6$) посредством множества (4) можно представить в следующем виде:

$$\mathbf{P}=\{\bigcup_{j=1}^{6}P_j\}=\{P_1,\ P_2,\ P_3,\ P_4,\ P_5,\ P_6\}= \tag{5}$$
$$\{P_{KBK},\ P_{BBK},\ P_{KOP},\ P_{COZ},\ P_{ZMZ},\ P_{KPOA}\}=\{KBK,\ BBK,\ KOP,\ COZ,\ ZMZ,\ KPOA\},$$

где $P_1=P_{KBK}=KBK$, $P_2=P_{BBK}=BBK$, $P_3=P_{KOP}=KOP$, $P_4=P_{COZ}=COZ$, $P_5=P_{ZMZ}=ZMZ$ и $P_6=P_{KPOA}=KPOA$ соответственно являются ИД таких параметров, как: «Количество виртуальных каналов (КВК)» (при $j=1$); «Возраст виртуального канала (ВВК)» (при $j=2$); «Количество одновременных подключений к серверу (КОП)» (при $j=3$); «Скорость обработки запросов от клиентов (СОЗ)» (при $j=4$); «Задержка между запросами от одного пользователя (ЗМЗ)» (при $j=5$); «Количество пакетов с одинаковым адресом отправителя и получателя (КПОА)» (при $j=6$).

Далее сформируем подмножества параметров

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{P_i}\}=\{\mathbf{P_1},\ \mathbf{P_2},\ \ldots,\ \mathbf{P_n}\}, \tag{6}$$

где $\mathbf{P_i}\subseteq\mathbf{P}$, $(i=\overline{1,n})$ определим как:

$$\mathbf{P_i}=\{\bigcup_{j=1}^{m_i}P_{ij}\}=\{P_{i1},\ P_{i2},\ \ldots,\ P_{im_i}\}, \tag{7}$$

при этом m_i обозначает количество параметров в (8), посредством которых осуществляется обнаружение аномального состояния, порожденного кибератакой с ИД CA_i. Таким образом (6) с учетом (7) представим в следующем виде:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{P_i}\}=\{\bigcup_{i=1}^{n}\{\bigcup_{j=1}^{m_i}P_{ij}\}\}= \tag{8}$$
$$\{\{P_{11},\ P_{12},\ \ldots,\ P_{1m_1}\},\{P_{21},\ P_{22},\ \ldots,\ P_{2m_2}\},\ \ldots,\{P_{n1},\ P_{n2},\ \ldots,\ P_{nm_n}\}\}.$$

Фактически, конкретные значения членов подмножества $\mathbf{P_i}$ определяют m_i-мерную параметрическую подсреду, используемую для выявления кибератаки с ИД CA_i или CA_i-атаки.

Например, при $n=3$, $m_1=m_3=2$ и $m_2=3$ с учетом (3) из (5) определим необходимые параметры для обнаружения соответствующих кибератак, т.е. $P_{11}=P_1$, $P_{12}=P_2$, $P_{21}=P_3$, $P_{22}=P_4$, $P_{23}=P_5$, $P_{31}=P_3$ и $P_{32}=P_6$. Тогда выражение (8) с учетом (5) будет иметь следующий вид:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}}\mathbf{P_i}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}P_{ij}\}\}=\{\{P_{11},\ P_{12}\},\{P_{21},\ P_{22},\ P_{23}\},\{P_{31},\ P_{32}\}\}= \tag{9}$$
$$\{\{P_{SNKBK},\ P_{SNBBK}\},\{P_{DSKOP},\ P_{DSCOZ},\ P_{DSZMZ}\},\{P_{SPKOP},\ P_{SPKPOA}\}\}=$$
$$\{\{KBK,\ BBK\},\{KOP,\ COZ,\ ZMZ\},\{KOP,\ KPOA\}\},$$

где: $P_{11}=P_{SNKBK}=KBK$ и $P_{12}=P_{SNBBK}=BBK$ являются параметрами, определяющими 2-мерную параметрическую подсреду (КВК-ВВК-подсреду) и соответственно, отображающими «КВК» и «ВВК», посредством которых осуществляется обнаружение кибератаки с ИД CA_{SN} или SN-атаки;

$P_{21}=P_{DSKOP}=KOP$, $P_{22}=P_{DSCOZ}=COZ$ и $P_{23}=P_{DSZMZ}=ZMZ$ являются параметрами, определяющими 3-мерную параметрическую подсреду (КОП-СОЗ-ЗМЗ-подсреду) и соответственно,

отображающими «КОП», «СОЗ» и «ЗМЗ», посредством которых выявляется кибератака с ИД CA_{DS} или DS -атака;

$P_{31} = P_{SPKOP} = KOP$ и $P_{32} = P_{SPKPOA} = KPOA$ являются параметрами, определяющими 2 -мерную параметрическую подсреду (КОП-КПОА-подсреду) и соответственно, отображающими «КОП» и «КПОА», посредством которых осуществляется обнаружение кибератаки с ИД CA_{SP} или SP -атаки.

Формирование $\mathbf{T_i^e}$. Построение подмножеств возможных нечетких (лингвистических) эталонов $\mathbf{T_i^e}$ осуществляется на основе множества всех возможных эталонов $\mathbf{T^e}$, отображающих характерные состояния соответствующих параметров из $\mathbf{P_i}$ в заданной среде окружения, т.е.

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\mathbf{T_1^e}, \mathbf{T_2^e}, \ldots, \mathbf{T_n^e}\}, \tag{10}$$

где $\mathbf{T_i^e} \subseteq \mathbf{T^e}$, $(i = \overline{1,n})$, а

$$\mathbf{T_i^e} = \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{T_{ij}^e}\} = \{\mathbf{T_{i1}^e}, \mathbf{T_{i2}^e}, \ldots, \mathbf{T_{im_i}^e}\}, \tag{11}$$

при этом $\mathbf{T_{ij}^e}$ $(j = \overline{1,m_i})$ – подмножество нечетких (лингвистических) эталонов, отображающее характерные суждения эксперта относительно аномальности состояния параметра P_{ij}. С учетом (11) формулу (10) запишем в следующем виде:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{T_{ij}^e}\}\} =$$
$$\{\{\mathbf{T_{11}^e}, \mathbf{T_{12}^e}, \ldots, \mathbf{T_{1m_1}^e}\}, \{\mathbf{T_{21}^e}, \mathbf{T_{22}^e}, \ldots, \mathbf{T_{2m_2}^e}\}, \ldots, \{\mathbf{T_{i1}^e}, \mathbf{T_{i2}^e}, \ldots, \mathbf{T_{im_i}^e}\}\}, (j = \overline{1,m_i}). \tag{12}$$

Подмножество $\mathbf{T_{ij}^e} \subseteq \mathbf{T_i^e}$ определим как:

$$\mathbf{T_{ij}^e} = \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}^e\} = \{\underset{\sim}{T}_{ij1}^e, \underset{\sim}{T}_{ij2}^e, \ldots, \underset{\sim}{T}_{ijr_j}^e\}, \tag{13}$$

где $\underset{\sim}{T}_{ijs}^e$ $(s = \overline{1,r_j})$ – эталонные нечеткие числа [8], а r_j – количество членов в $\mathbf{T_{ij}^e}$.

Тогда выражение (12) с учетом (13) принимает следующий вид:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{T_i^e}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}} \mathbf{T_{ij}^e}\}\} = \{\bigcup_{i=1}^{n} \{\bigcup_{j=1}^{m_i} \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}^e\}\}\} =$$
$$\{\{\{\underset{\sim}{T}_{111}^e, \underset{\sim}{T}_{112}^e, \ldots, \underset{\sim}{T}_{11r_1}^e\}, \{\underset{\sim}{T}_{121}^e, \underset{\sim}{T}_{122}^e, \ldots, \underset{\sim}{T}_{12r_2}^e\}, \ldots, \{\underset{\sim}{T}_{1m_1 1}^e, \underset{\sim}{T}_{1m_1 2}^e, \ldots, \underset{\sim}{T}_{1m_1 r_{m_1}}^e\}\},$$
$$\{\{\underset{\sim}{T}_{211}^e, \underset{\sim}{T}_{212}^e, \ldots, \underset{\sim}{T}_{21r_1}^e\}, \{\underset{\sim}{T}_{221}^e, \underset{\sim}{T}_{222}^e, \ldots, \underset{\sim}{T}_{22r_2}^e\}, \ldots, \{\underset{\sim}{T}_{2m_2 1}^e, \underset{\sim}{T}_{2m_2 2}^e, \ldots, \underset{\sim}{T}_{2m_2 r_{m_2}}^e\}\},$$
$$\ldots,$$
$$\{\{\underset{\sim}{T}_{n11}^e, \underset{\sim}{T}_{n12}^e, \ldots, \underset{\sim}{T}_{n1r_1}^e\}, \{\underset{\sim}{T}_{n21}^e, \underset{\sim}{T}_{n22}^e, \ldots, \underset{\sim}{T}_{n2r_2}^e\}, \ldots, \{\underset{\sim}{T}_{nm_n 1}^e, \underset{\sim}{T}_{nm_n 2}^e, \ldots, \underset{\sim}{T}_{nm_n r_{m_n}}^e\}\}\}. \tag{14}$$

Следует отметить, что совокупность конкретных значений всех членов подмножества $\mathbf{T_i^e}$ (по аналогии с параметрической средой) определяют эталонную среду, ориентированную на выявления кибератаки с ИД CA_i или CA_i -атаки.

Например, при $n = 3$ ($\mathbf{CA_1^{\tau_f}} = \mathbf{CA_{SN}^{\tau_f}} = \mathbf{SN^{\tau_f}}$, $\mathbf{CA_2^{\tau_f}} = \mathbf{CA_{DS}^{\tau_f}} = \mathbf{DS^{\tau_f}}$ и $\mathbf{CA_3^{\tau_f}} = \mathbf{CA_{SP}^{\tau_f}} = \mathbf{SP^{\tau_f}}$), $m_1 = m_3 = 2$, $m_2 = 3$, $r_1 = 5$, $r_2 = r_3 = 3$ и с учетом [2, 3] выражение (14) можно определить как:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}}\mathbf{T_i^e}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}}\{\bigcup_{\mathbf{j=1}}^{\mathbf{m_i}}\mathbf{T_{ij}^e}\}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{j=1}^{m_i}\{\bigcup_{s=1}^{r_j}\underset{\sim}{T}_{ijs}^{e}\}\}\}=$$

$$\{\{\{\underset{\sim}{T}_{111}^{e},\ \underset{\sim}{T}_{112}^{e},\ \underset{\sim}{T}_{113}^{e},\ \underset{\sim}{T}_{114}^{e},\ \underset{\sim}{T}_{11r_1}^{e}\},\{\underset{\sim}{T}_{1m_1 1}^{e},\ \underset{\sim}{T}_{1m_1 2}^{e},\ \underset{\sim}{T}_{1m_1 r_2}^{e}\}\},$$

$$\{\{\underset{\sim}{T}_{211}^{e},\ \underset{\sim}{T}_{212}^{e},\ \underset{\sim}{T}_{213}^{e},\ \underset{\sim}{T}_{214}^{e},\ \underset{\sim}{T}_{21r_1}^{e}\},\{\underset{\sim}{T}_{221}^{e},\ \underset{\sim}{T}_{222}^{e},\ \underset{\sim}{T}_{22r_2}^{e}\},\{\underset{\sim}{T}_{2m_2 1}^{e},\ \underset{\sim}{T}_{2m_2 2}^{e},\ \underset{\sim}{T}_{2m_2 r_3}^{e}\}\},$$

$$\{\{\underset{\sim}{T}_{311}^{e},\ \underset{\sim}{T}_{312}^{e},\ \underset{\sim}{T}_{313}^{e},\ \underset{\sim}{T}_{314}^{e},\ \underset{\sim}{T}_{31r_1}^{e}\},\{\underset{\sim}{T}_{3m_3 1}^{e},\ \underset{\sim}{T}_{3m_3 2}^{e},\ \underset{\sim}{T}_{3m_3 r_2}^{e}\}\}=$$

$$\{\{\{\underset{\sim}{T}_{111}^{e},\ \underset{\sim}{T}_{112}^{e},\ \underset{\sim}{T}_{113}^{e},\ \underset{\sim}{T}_{114}^{e},\ \underset{\sim}{T}_{115}^{e}\},\{\underset{\sim}{T}_{121}^{e},\ \underset{\sim}{T}_{122}^{e},\ \underset{\sim}{T}_{123}^{e}\}\},\{\{\underset{\sim}{T}_{211}^{e},\ \underset{\sim}{T}_{212}^{e},\ \underset{\sim}{T}_{213}^{e},\ \underset{\sim}{T}_{214}^{e},\ \underset{\sim}{T}_{215}^{e}\},\{\underset{\sim}{T}_{221}^{e},$$

$$\underset{\sim}{T}_{222}^{e},\ \underset{\sim}{T}_{223}^{e}\},\{\underset{\sim}{T}_{231}^{e},\ \underset{\sim}{T}_{232}^{e},\ \underset{\sim}{T}_{233}^{e}\}\},\{\{\underset{\sim}{T}_{311}^{e},\ \underset{\sim}{T}_{312}^{e},\ \underset{\sim}{T}_{313}^{e},\ \underset{\sim}{T}_{314}^{e},\ \underset{\sim}{T}_{315}^{e}\},\{\underset{\sim}{T}_{321}^{e},\ \underset{\sim}{T}_{322}^{e},$$

$$\underset{\sim}{T}_{323}^{e}\}\}=\{\{\{\underset{\sim}{OM}_{11}^{e},\ \underset{\sim}{M}_{11}^{e},\ \underset{\sim}{C}_{11}^{e},\ \underset{\sim}{Б}_{11}^{e},\ \underset{\sim}{ОБ}_{11}^{e}\},\{\underset{\sim}{M}_{12}^{e},\ \underset{\sim}{CP}_{12}^{e},\ \underset{\sim}{CT}_{12}^{e}\}\},\{\{\underset{\sim}{OM}_{21}^{e},\ \underset{\sim}{M}_{21}^{e},\ \underset{\sim}{C}_{21}^{e},\ \underset{\sim}{Б}_{21}^{e},\ (15)$$

$$\underset{\sim}{ОБ}_{21}^{e}\},\{\underset{\sim}{H}_{22}^{e},\ \underset{\sim}{C}_{22}^{e},\ \underset{\sim}{B}_{22}^{e}\},\{\underset{\sim}{M}_{23}^{e},\ \underset{\sim}{C}_{23}^{e},\ \underset{\sim}{Б}_{23}^{e}\}\},\{\{\underset{\sim}{OM}_{31}^{e},\ \underset{\sim}{M}_{31}^{e},\ \underset{\sim}{C}_{31}^{e},\ \underset{\sim}{Б}_{31}^{e},\ \underset{\sim}{ОБ}_{31}^{e}\},\{\underset{\sim}{M}_{32}^{e},\ \underset{\sim}{C}_{32}^{e},$$

$$\underset{\sim}{Б}_{32}^{e}\}\}\}=\{\{\{\underset{\sim}{T}_{SNKBK1}^{e},\ \underset{\sim}{T}_{SNKBK2}^{e},\ \underset{\sim}{T}_{SNKBK3}^{e},\ \underset{\sim}{T}_{SNKBK4}^{e},\ \underset{\sim}{T}_{SNKBK5}^{e}\},\{\underset{\sim}{T}_{SNBBK1}^{e},\ \underset{\sim}{T}_{SNBBK2}^{e},\ \underset{\sim}{T}_{SNBBK3}^{e}\}\},$$

$$\{\{\underset{\sim}{T}_{DSKOП1}^{e},\ \underset{\sim}{T}_{DSKOП2}^{e},\ \underset{\sim}{T}_{DSKOП3}^{e},\ \underset{\sim}{T}_{DSKOП4}^{e},\ \underset{\sim}{T}_{DSKOП5}^{e}\},\{\underset{\sim}{T}_{DSCO31}^{e},\ \underset{\sim}{T}_{DSCO32}^{e},\ \underset{\sim}{T}_{DSCO33}^{e}\},\{\underset{\sim}{T}_{DS3M31}^{e},$$

$$\underset{\sim}{T}_{DS3M32}^{e},\ \underset{\sim}{T}_{DS3M33}^{e}\}\},\{\{\underset{\sim}{T}_{SPKOП1}^{e},\ \underset{\sim}{T}_{SPKOП2}^{e},\ \underset{\sim}{T}_{SPKOП3}^{e},\ \underset{\sim}{T}_{SPKOП4}^{e},\ \underset{\sim}{T}_{SPKOП5}^{e}\},\{\underset{\sim}{T}_{SPKПOA1}^{e},\ \underset{\sim}{T}_{SPKПOA2}^{e},$$

$$\underset{\sim}{T}_{SPKПOA3}^{e}\}\}\}=\{\{\{\underset{\sim}{OM}_{SNKBK}^{e},\ \underset{\sim}{M}_{SNKBK}^{e},\ \underset{\sim}{C}_{SNKBK}^{e},\ \underset{\sim}{Б}_{SNKBK}^{e},\ \underset{\sim}{ОБ}_{SNKBK}^{e}\},\{\underset{\sim}{M}_{SNBBK}^{e},\ \underset{\sim}{CP}_{SNBBK}^{e},$$

$$\underset{\sim}{CT}_{SNBBK}^{e}\}\},\{\{\underset{\sim}{OM}_{DSKOП}^{e},\ \underset{\sim}{M}_{DSKOП}^{e},\ \underset{\sim}{C}_{DSKOП}^{e},\ \underset{\sim}{Б}_{DSKOП}^{e},\ \underset{\sim}{ОБ}_{DSKOП}^{e}\},\{\underset{\sim}{H}_{DSCO3}^{e},\ \underset{\sim}{C}_{DSCO3}^{e},\ \underset{\sim}{B}_{DSCO3}^{e}\},$$

$$\{\underset{\sim}{M}_{DS3M3}^{e},\ \underset{\sim}{C}_{DS3M3}^{e},\ \underset{\sim}{Б}_{DS3M3}^{e}\}\},\{\{\underset{\sim}{OM}_{SPKOП}^{e},\ \underset{\sim}{M}_{SPKOП}^{e},\ \underset{\sim}{C}_{SPKOП}^{e},\ \underset{\sim}{Б}_{SPKOП}^{e},\ \underset{\sim}{ОБ}_{SPKOП}^{e}\},\{\underset{\sim}{M}_{SPKПOA}^{e},$$

$$\underset{\sim}{C}_{SPKПOA}^{e},\ \underset{\sim}{Б}_{SPKПOA}^{e}\}\}\},$$

где: $\underset{\sim}{T}_{111}^{e}=\underset{\sim}{OM}_{11}^{e}=\underset{\sim}{T}_{SNKBK1}^{e}=\underset{\sim}{OM}_{SNKBK}^{e}$, $\underset{\sim}{T}_{112}^{e}=\underset{\sim}{M}_{11}^{e}=\underset{\sim}{T}_{SNKBK2}^{e}=\underset{\sim}{M}_{SNKBK}^{e}$, $\underset{\sim}{T}_{113}^{e}=\underset{\sim}{C}_{11}^{e}=\underset{\sim}{T}_{SNKBK3}^{e}=\underset{\sim}{C}_{SNKBK}^{e}$, $\underset{\sim}{T}_{114}^{e}=\underset{\sim}{Б}_{11}^{e}=\underset{\sim}{T}_{SNKBK4}^{e}=\underset{\sim}{Б}_{SNKBK}^{e}$, $\underset{\sim}{T}_{115}^{e}=\underset{\sim}{ОБ}_{11}^{e}=\underset{\sim}{T}_{SNKBK5}^{e}=\underset{\sim}{ОБ}_{SNKBK}^{e}$ и $\underset{\sim}{T}_{121}^{e}=\underset{\sim}{M}_{12}^{e}=\underset{\sim}{T}_{SNBBK1}^{e}=\underset{\sim}{M}_{SNBBK}^{e}$, $\underset{\sim}{T}_{122}^{e}=\underset{\sim}{CP}_{12}^{e}=\underset{\sim}{T}_{SNBBK2}^{e}=\underset{\sim}{CP}_{SNBBK}^{e}$, $\underset{\sim}{T}_{123}^{e}=\underset{\sim}{CT}_{12}^{e}=\underset{\sim}{T}_{SNBBK3}^{e}=\underset{\sim}{CT}_{SNBBK}^{e}$ – являются компонентами лингвистических эталонов, отображающими параметры $P_1=P_{KBK}=KBK$, $P_2=P_{BBK}=BBK$ или соответственно «КВК», «ВВК» и в совокупности определяют эталонную КВК-ВВК-среду, посредством которой осуществляется обнаружение кибератаки с ИД CA_{SN} или SN-атаки;

$\underset{\sim}{T}_{211}^{e}=\underset{\sim}{OM}_{21}^{e}=\underset{\sim}{T}_{DSKOП1}^{e}=\underset{\sim}{OM}_{DSKOП}^{e}$, $\underset{\sim}{T}_{212}^{e}=\underset{\sim}{M}_{21}^{e}=\underset{\sim}{T}_{DSKOП2}^{e}=\underset{\sim}{M}_{DSKOП}^{e}$, $\underset{\sim}{T}_{213}^{e}=\underset{\sim}{C}_{21}^{e}=\underset{\sim}{T}_{DSKOП3}^{e}=\underset{\sim}{C}_{DSKOП}^{e}$, $\underset{\sim}{T}_{214}^{e}=\underset{\sim}{Б}_{21}^{e}=\underset{\sim}{T}_{DSKOП4}^{e}=\underset{\sim}{Б}_{DSKOП}^{e}$, $\underset{\sim}{T}_{215}^{e}=\underset{\sim}{ОБ}_{21}^{e}=\underset{\sim}{T}_{DSKOП5}^{e}=\underset{\sim}{ОБ}_{DSKOП}^{e}$, $\underset{\sim}{T}_{221}^{e}=\underset{\sim}{H}_{22}^{e}=\underset{\sim}{T}_{DSCO31}^{e}=\underset{\sim}{H}_{DSCO3}^{e}$, $\underset{\sim}{T}_{222}^{e}=\underset{\sim}{C}_{22}^{e}=\underset{\sim}{T}_{DSCO32}^{e}=\underset{\sim}{C}_{DSCO3}^{e}$, $\underset{\sim}{T}_{223}^{e}=\underset{\sim}{B}_{22}^{e}=\underset{\sim}{T}_{DSCO33}^{e}=\underset{\sim}{B}_{DSCO3}$ и $\underset{\sim}{T}_{231}^{e}=\underset{\sim}{M}_{23}^{e}=\underset{\sim}{T}_{DS3M31}^{e}=\underset{\sim}{M}_{DS3M3}^{e}$, $\underset{\sim}{T}_{232}^{e}=\underset{\sim}{C}_{23}^{e}=\underset{\sim}{T}_{DS3M32}^{e}=\underset{\sim}{C}_{DS3M3}^{e}$, $\underset{\sim}{T}_{233}^{e}=\underset{\sim}{Б}_{23}^{e}=\underset{\sim}{T}_{DS3M33}^{e}=\underset{\sim}{Б}_{DS3M3}^{e}$ – являются компонентами лингвистических эталонов, отображающими параметры $P_3=P_{KOП}=KOП$, $P_4=P_{CO3}=CO3$, $P_5=P_{3M3}=3M3$ или соответственно «КОП», «СОЗ», «ЗМЗ» и в совокупности определяют эталонную КОП-СОЗ-ЗМЗ-среду, посредством которой осуществляется обнаружение кибератаки с ИД CA_{DS} или DS-атаки;

$\underset{\sim}{T}_{311}^{e}=\underset{\sim}{OM}_{31}^{e}=\underset{\sim}{T}_{SPKOП1}^{e}=\underset{\sim}{OM}_{SPKOП}^{e}$, $\underset{\sim}{T}_{312}^{e}=\underset{\sim}{M}_{31}^{e}=\underset{\sim}{T}_{SPKOП2}^{e}=\underset{\sim}{M}_{SPKOП}^{e}$, $\underset{\sim}{T}_{313}^{e}=\underset{\sim}{C}_{31}^{e}=\underset{\sim}{T}_{SPKOП3}^{e}=\underset{\sim}{C}_{SPKOП}^{e}$, $\underset{\sim}{T}_{314}^{e}=\underset{\sim}{Б}_{31}^{e}=\underset{\sim}{T}_{SPKOП4}^{e}=\underset{\sim}{Б}_{SPKOП}^{e}$, $\underset{\sim}{T}_{315}^{e}=\underset{\sim}{ОБ}_{31}^{e}=\underset{\sim}{T}_{SPKOП5}^{e}=\underset{\sim}{ОБ}_{SPKOП}^{e}$ и $\underset{\sim}{T}_{321}^{e}=\underset{\sim}{M}_{32}^{e}=\underset{\sim}{T}_{SPKПOA1}^{e}=\underset{\sim}{M}_{SPKПOA}^{e}$, $\underset{\sim}{T}_{322}^{e}=\underset{\sim}{C}_{32}^{e}=\underset{\sim}{T}_{SPKПOA2}^{e}=\underset{\sim}{C}_{SPKПOA}^{e}$, $\underset{\sim}{T}_{323}^{e}=\underset{\sim}{Б}_{32}^{e}=\underset{\sim}{T}_{SPKПOA3}^{e}=\underset{\sim}{Б}_{SPKПOA}^{e}$ – являются компонентами лингвистических эталонов, отображающими параметры $P_3=P_{KOП}=KOП$, $P_6=P_{KПOA}=KПOA$ или соответственно «КОП», «КПОА» и в совокупности определяют эталонную КОП-КПОА-среду, посредством которой осуществляется обнаружение кибератаки с ИД CA_{SP} или SP-атаки.

Формирование $\mathbf{P_i^{\tau_f}}$. Построение подмножества $\mathbf{P_i^{\tau_f}} \subseteq \mathbf{P^{\tau_f}}$ ($\mathbf{P^{\tau_f}}$ – множество всех возможных текущих значений нечетких параметров) осуществляется посредством $\mathbf{T_i^e}$ в момент времени τ_f за временной промежуток, длительность которого $\tau_h = \tau_f - \tau_{f-1}$ $(f = \overline{1,max})$, при этом f является номером временного интервала, максимальное значение которого определяется величиной max. Таким образом, $\mathbf{P_i^{\tau_f}}$ определим как:

$$\mathbf{P_i^{\tau_f}} = \{\bigcup_{j=1}^{m_i} \underset{\sim}{P}_{ij}^{\tau_f}\} = \{\underset{\sim}{P}_{i1}^{\tau_f}, \underset{\sim}{P}_{i2}^{\tau_f}, \ldots, \underset{\sim}{P}_{im_i}^{\tau_f}\}, \tag{16}$$

где $\underset{\sim}{P}_{ij}^{\tau_f}$, $(j = \overline{1,m_i})$ – текущий нечеткий параметр, формируемый в момент времени τ_f, а m_i – количество нечетких текущих параметров, по состоянию аномальности которых осуществляется выявление кибератак с ИД CA_i.

По аналогии с параметрической и эталонной средой совокупность конкретных значений всех членов подмножества $\mathbf{P_i^{\tau_f}}$ определяют текущую среду, используемую для выявления аномального состояния в общей гетерогенной параметрической среде и, как следствие, в m_i-мерной параметрической подсреде, порожденного кибератакой с ИД CA_i в момент времени τ_f.

Например, при $n = 3$, $i = \overline{1,3}$ ($\mathbf{CA_1^{\tau_f}} = \mathbf{CA_{SN}^{\tau_f}} = \mathbf{SN^{\tau_f}}$, $\mathbf{CA_2^{\tau_f}} = \mathbf{CA_{DS}^{\tau_f}} = \mathbf{DS^{\tau_f}}$ и $\mathbf{CA_3^{\tau_f}} = \mathbf{CA_{SP}^{\tau_f}} = \mathbf{SP^{\tau_f}}$), $m_1 = m_3 = 2$ и $m_2 = 3$ выражение (16) можно определить как:

$$\mathbf{P_1^{\tau_f}} = \{\bigcup_{j=1}^{2} \underset{\sim}{P}_{1j}^{\tau_f}\} = \{\underset{\sim}{P}_{11}^{\tau_f}, \underset{\sim}{P}_{12}^{\tau_f}\} = \{\underset{\sim}{P}_{SNKBK}^{\tau_f}, \underset{\sim}{P}_{SNBBK}^{\tau_f}\}, \text{(для } i = 1,\ m_1 = 2\text{)};$$

$$\mathbf{P_2^{\tau_f}} = \{\bigcup_{j=1}^{3} \underset{\sim}{P}_{2j}^{\tau_f}\} = \{\underset{\sim}{P}_{21}^{\tau_f}, \underset{\sim}{P}_{22}^{\tau_f}, \underset{\sim}{P}_{23}^{\tau_f}\} = \{\underset{\sim}{P}_{DSKOП}^{\tau_f}, \underset{\sim}{P}_{DSCO3}^{\tau_f}, \underset{\sim}{P}_{DS3M3}^{\tau_f}\}, \text{(для } i = 2,\ m_2 = 3\text{)}; \tag{17}$$

$$\mathbf{P_3^{\tau_f}} = \{\bigcup_{j=1}^{2} \underset{\sim}{P}_{3j}^{\tau_f}\} = \{\underset{\sim}{P}_{31}^{\tau_f}, \underset{\sim}{P}_{32}^{\tau_f}\} = \{\underset{\sim}{P}_{SPKOП}^{\tau_f}, \underset{\sim}{P}_{SPKПOA}^{\tau_f}\}, \text{(для } i = 3,\ m_3 = 2\text{)},$$

где: $\underset{\sim}{P}_{11}^{\tau_f} = \underset{\sim}{P}_{SNKBK}^{\tau_f}$ и $\underset{\sim}{P}_{12}^{\tau_f} = \underset{\sim}{P}_{SNBBK}^{\tau_f}$ – являются нечеткими текущими значениями, отображающими параметры $P_1 = P_{KBK} = KBK$ и $P_2 = P_{BBK} = BBK$ т.е. «КВК» и «ВВК» соответственно, конкретные значения которых в совокупности составляют текущую КВК-ВВК-среду, используемую для выявления аномального состояния в 2-мерной параметрической подсреде, порожденной SN-атакой;

$\underset{\sim}{P}_{21}^{\tau_f} = \underset{\sim}{P}_{DSKOП}^{\tau_f}$, $\underset{\sim}{P}_{22}^{\tau_f} = \underset{\sim}{P}_{DSCO3}^{\tau_f}$ и $\underset{\sim}{P}_{23}^{\tau_f} = \underset{\sim}{P}_{DS3M3}^{\tau_f}$ – являются нечеткими текущими значениями, отображающими параметры $P_3 = P_{KOП} = KOП$, $P_4 = P_{CO3} = CO3$ и $P_5 = P_{3M3} = 3M3$ т.е. «КОП», «СОЗ» и «ЗМЗ» соответственно, конкретные значения которых в совокупности составляют текущую КОП-СОЗ-ЗМЗ-среду, используемую для выявления аномального состояния в 3-мерной параметрической подсреде, порожденной DS-атакой;

$\underset{\sim}{P}_{31}^{\tau_f} = \underset{\sim}{P}_{SPKOП}^{\tau_f}$ и $\underset{\sim}{P}_{32}^{\tau_f} = \underset{\sim}{P}_{SPKПOA}^{\tau_f}$ – являются нечеткими текущими значениями, отображающими параметры $P_3 = P_{KOП} = KOП$ и $P_6 = P_{KПOA} = KПOA$ т.е. «КОП» и «КПОА» соответственно, конкретные значения которых в совокупности составляют текущую КОП-КПОА-среду, используемую для выявления аномального состояния в 2-мерной параметрической подсреде, порожденной SP-атакой.

Формирование $\mathbf{DR_i}$. Построение подмножеств детекционных правил $\mathbf{DR_i} \subseteq \mathbf{DR}$, $i = \overline{1,n}$ ($\mathbf{DR}$ – множество всех возможных правил), используемых для обнаружения i-й кибератаки осуществляется на основе выражения (18)

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{DR_i}\} = \{\mathbf{DR_1}, \mathbf{DR_2}, \ldots, \mathbf{DR_n}\}, \tag{18}$$

где

$$\mathbf{DR_i} = \{\bigcup_{\mathbf{a=1}}^{\mathbf{w_i}} \mathbf{DR_{ia}}\} = \{DR_{i1}, DR_{i2}, \ldots, DR_{iw_i}\}, (a = \overline{1,w_i}), \tag{19}$$

а w_i – количество детекционных правил, используемых для обнаружения i-й кибератаки. С учетом (19) формулу (18) запишем в следующем виде:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{DR_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{a=1}}^{\mathbf{w_i}} \mathbf{DR_{ia}}\}\} = \{\{DR_{11}, DR_{12}, \ldots, DR_{1w_1}\}, \{DR_{21}, DR_{22}, \ldots, DR_{2w_2}\}, \ldots, \{DR_{n1}, DR_{n2}, \ldots, DR_{nw_n}\}, (i = \overline{1,n}, a = \overline{1,w_i}). \tag{20}$$

Отметим, что в совокупности все элементы подмножества $\mathbf{DR_i}$ определяют детекционную среду, используемую для обнаружения кибератаки с ИД CA_i в атакующей среде.

Например, при $n = 3$ ($\mathbf{CA_1^{\tau_f}} = \mathbf{CA_{SN}^{\tau_f}} = \mathbf{SN^{\tau_f}}$, $\mathbf{CA_2^{\tau_f}} = \mathbf{CA_{DS}^{\tau_f}} = \mathbf{DS^{\tau_f}}$ и $\mathbf{CA_3^{\tau_f}} = \mathbf{CA_{SP}^{\tau_f}} = \mathbf{SP^{\tau_f}}$) и $w_1 = w_2 = w_3 = 5$ выражение (20) можно определить как:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \mathbf{DR_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{3}} \{\bigcup_{\mathbf{a=1}}^{\mathbf{w_i}} \mathbf{DR_{ia}}\}\} = \{\mathbf{DR_1}, \mathbf{DR_2}, \mathbf{DR_3}\} = \{\{DR_{11}, DR_{12}, DR_{13}, DR_{14}, DR_{15}\}, \{DR_{21}, DR_{22}, DR_{23}, DR_{24}, DR_{25}\}, \{DR_{31}, DR_{32}, DR_{33}, DR_{34}, DR_{35}\}\}, \tag{21}$$

где в совокупности все элементы соответствующих подмножеств $\mathbf{DR_1} = \{DR_{11}, DR_{12}, DR_{13}, DR_{14}, DR_{15}\}$, $\mathbf{DR_2} = \{DR_{21}, DR_{22}, DR_{23}, DR_{24}, DR_{25}\}$ и $\mathbf{DR_3} = \{DR_{31}, DR_{32}, DR_{33}, DR_{34}, DR_{35}\}$ определяют детекционные среды, содержащие конкретные детекционные правила, используемые соответственно для обнаружения SN-, DS- и SP-атак.

Таким образом, сформированы все компоненты кортежа (2), позволяющие определять m_i-мерные параметрические подсреды, а также атакующие, эталонные, текущие и детекционные среды.

Например, при $n = 3$ на основе обобщенного кортежа (2) можно сформировать его частные отображения в $\mathbf{CA_1^{\tau_f}} = \mathbf{CA_{SN}^{\tau_f}} = \mathbf{SN^{\tau_f}}$, $\mathbf{CA_2^{\tau_f}} = \mathbf{CA_{DS}^{\tau_f}} = \mathbf{DS^{\tau_f}}$ и $\mathbf{CA_3^{\tau_f}} = \mathbf{CA_{SP}^{\tau_f}} = \mathbf{SP^{\tau_f}}$ т.е.:

$$\mathbf{CA_1^{\tau_f}} = <CA_1, \mathbf{P_1}, \mathbf{T_1^e}, \mathbf{P_1^{\tau_f}}, \mathbf{DR_1}>,$$
$$\mathbf{CA_2^{\tau_f}} = <CA_2, \mathbf{P_2}, \mathbf{T_2^e}, \mathbf{P_2^{\tau_f}}, \mathbf{DR_2}> \text{ и } \mathbf{CA_3^{\tau_f}} = <CA_3, \mathbf{P_3}, \mathbf{T_3^e}, \mathbf{P_3^{\tau_f}}, \mathbf{DR_3}>, \tag{22}$$

а с учетом (9), (15), (17) и (21) выражение (22) примет вид:

$$\mathbf{CA_1^{\tau_f}} = <CA_1, \{P_{11}, P_{12}\}, \{\{\underset{\sim}{T}^e_{111}, \underset{\sim}{T}^e_{112}, \underset{\sim}{T}^e_{113}, \underset{\sim}{T}^e_{114}, \underset{\sim}{T}^e_{115}\}, \{\underset{\sim}{T}^e_{121}, \underset{\sim}{T}^e_{122}, \underset{\sim}{T}^e_{123}\}\}, \{\underset{\sim}{P}^{\tau_f}_{11}, \underset{\sim}{P}^{\tau_f}_{12}\}, \{DR_{11}, DR_{12}, DR_{13}, DR_{14}, DR_{15}\}> \text{ или}$$

$$\mathbf{CA_{SN}^{\tau_f}} = <CA_{SN}, \{P_{SNKBK}, P_{SNBBK}\}, \{\{\underset{\sim}{T}^e_{SNKBK1}, \underset{\sim}{T}^e_{SNKBK2}, \underset{\sim}{T}^e_{SNKBK3}, \underset{\sim}{T}^e_{SNKBK4}, \underset{\sim}{T}^e_{SNKBK5}\}, \{\underset{\sim}{T}^e_{SNBBK1}, \underset{\sim}{T}^e_{SNBBK2}, \underset{\sim}{T}^e_{SNBBK3}\}\}, \{\underset{\sim}{P}^{\tau_f}_{SNKBK}, \underset{\sim}{P}^{\tau_f}_{SNBBK}\}, \{DR_{11}, DR_{12}, DR_{13}, DR_{14}, DR_{15}\}> \tag{23}$$
(при $m_1 = 2$, $r_1 = 5$, $r_2 = 3$ и $w_1 = 5$);

$$\mathbf{CA_2^{\tau_f}} = <CA_2, \{P_{21}, P_{22}, P_{23}\}, \{\{\underset{\sim}{T}^e_{211}, \underset{\sim}{T}^e_{212}, \underset{\sim}{T}^e_{213}, \underset{\sim}{T}^e_{214}, \underset{\sim}{T}^e_{215}\}, \{\underset{\sim}{T}^e_{221}, \underset{\sim}{T}^e_{222}, \underset{\sim}{T}^e_{223}\}, \{\underset{\sim}{T}^e_{231}, \underset{\sim}{T}^e_{232}, \underset{\sim}{T}^e_{233}\}\}, \{\underset{\sim}{P}^{\tau_f}_{21}, \underset{\sim}{P}^{\tau_f}_{22}, \underset{\sim}{P}^{\tau_f}_{23}\}, \{DR_{21}, DR_{22}, DR_{23}, DR_{24}, DR_{25}\}> \text{ или}$$

$$\mathbf{CA}_{\mathbf{DS}}^{\tau_f} = < CA_{DS}, \{ P_{DSKOП}, P_{DSCO3}, P_{DS3M3} \}, \{ \{ T^e_{DSKOП1}, T^e_{DSKOП2}, T^e_{DSKOП3}, T^e_{DSKOП4}, T^e_{DSKOП5} \}, \{ T^e_{DSCO31}, T^e_{DSCO32}, T^e_{DSCO33} \}, \{ T^e_{DS3M31}, T^e_{DS3M32}, T^e_{DS3M33} \} \}, \{ P^{\tau_f}_{DSKOП}, P^{\tau_f}_{DSCO3}, P^{\tau_f}_{DS3M3} \}, \{ DR_{21}, DR_{22}, DR_{23}, DR_{24}, DR_{25} \} >$$

(при $m_2 = 3$, $r_1 = 5$, $r_2 = r_3 = 3$ и $w_2 = 5$);

$$\mathbf{CA}_{\mathbf{3}}^{\tau_f} = < CA_3, \{ P_{31}, P_{32} \}, \{ \{ T^e_{311}, T^e_{312}, T^e_{313}, T^e_{314}, T^e_{315} \}, \{ T^e_{321}, T^e_{322}, T^e_{323} \} \}, \{ P^{\tau_f}_{31}, P^{\tau_f}_{32} \}, \{ DR_{31}, DR_{32}, DR_{33}, DR_{34}, DR_{35} \} >$$ или

$$\mathbf{CA}_{\mathbf{SP}}^{\tau_f} < CA_{SP}, \{ P_{SPKOП}, P_{SPKПOA} \}, \{ \{ T^e_{SPKOП1}, T^e_{SPKOП2}, T^e_{SPKOП3}, T^e_{SPKOП4}, T^e_{SPKOП5} \}, \{ T^e_{SPKПOA1}, T^e_{SPKПOA2}, T^e_{SPKПOA3} \} \}, \{ P^{\tau_f}_{SPKOП}, P^{\tau_f}_{SPKПOA} \}, \{ DR_{31}, DR_{32}, DR_{33}, DR_{34}, DR_{35} \} >$$

(при $m_3 = 2$, $r_1 = 5$, $r_2 = 3$ и $w_3 = 5$).

Исходя из предложенных теоретических положений (описывающих структуру кортежной модели) и из приведенного примера можно отметить, что посредством сформированных множеств обобщенных кортежей определяется состояние аномальности в m-мерной гетерогенной параметрической среде, которое порождается не только атакующей SN-DS-SP-средой в момент времени τ_f, но и средами с другими классами кибератак, для которых можно сформировать подобный кортеж.

V Выводы

Таким образом, предложена кортежная модель формирования набора базовых компонент, которая за счет формализации процесса создания m_i-мерных параметрических подсред, а также атакующих, эталонных, текущих и детектирующих сред, позволяет сформировать набор частных кортежей, отображающих процесс выявления аномального состояния в m-мерной гетерогенной параметрической среде, порожденного соответствующей атакующей средой в заданный временной промежуток.

С учетом существующих разработок [1 – 8] для практического использования предложенной кортежной модели, при совершенствовании систем обнаружения вторжений, необходимо создать соответствующую модель детекционных правил. Для контроля за состоянием аномальности общей гетерогенной параметрический среды на протяжении всех временных промежутков следует разработать соответствующую мониторинговую модель кибератак.

Список использованной литературы: ***1.*** *Корченко А. А. Модель эвристических правил на логико-лингвистических связках для обнаружения аномалий в компьютерных системах / А. А. Корченко // Захист інформації. – 2012. – № 4 (57). – С. 112-118.* ***2.*** *Стасюк А. И. Базовая модель параметров для построения систем выявления атак / А. И. Стасюк, А. А. Корченко // Захист інформації. – 2012. – № 2 (55). – С. 47-51.* ***3.*** *Модели эталонов лингвистических переменных для систем выявления атак / М. Г. Луцкий, А. А. Корченко, А. В. Гавриленко, А. А Охрименко // Захист інформації. – 2012. – № 2 (55). – С. 71-78.* ***4.*** *Стасюк А. И. Метод выявления аномалий порожденных кибератаками в компьютерных сетях / А. И. Стасюк, А. А. Корченко // Захист інформації. – 2012. – №4 (57). – С. 129-134.* ***5.*** *Корченко А. А. Система выявления аномального состояния в компьютерных сетях / А. А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84.* ***6.*** *Корченко А. А. Система формирования нечетких эталонов сетевых параметров / А.А. Корченко // Захист інформації. – 2013. – Т.15, №3. – С. 240-246.* ***7.*** *Корченко А. А. Система формирования эвристических правил для оценивания сетевой активности / А. А. Корченко // Захист інформації. – 2013. – №4. Т.15. – С. 353-359.* ***8.*** *Корченко А. Г. Построение систем защиты информации на нечетких множествах [Текст]: Теория и практические решения / А. Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.*