УДК 004.056.53(045)

МЕТОД ФОРМИРОВАНИЯ БАЗОВЫХ ДЕТЕКЦИОННЫХ ПРАВИЛ ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Николай Карпинский, Анна Корченко, Санзира Ахметова

Вследствие интенсивного развития цифрового бизнеса, вредоносное программное обеспечение и другие киберугрозы становятся все более распространенными. Для повышения уровня безопасности необходимы соответствующие специальные средства противодействия, которые способны оставаться эффективными при появлении новых видов угроз и позволяющие в нечетких условиях выявить кибератаки, ориентированные на множество ресурсов информационных систем. Различные атакующие воздействия на соответствующие ресурсы порождают различные множества аномалий в гетерогенной параметрической среде окружения. Известна кортежная модель формирования набора базовых компонент, которые позволяют выявить кибератаки. Для ее эффективного применения необходима формальная реализация подхода к формированию наборов базовых детекционных правил. С этой целью разработан метод, ориентированный на решение задач выявления кибератак в компьютерных системах, который реализуется посредством трех базовых этапов: формирование подмножеств идентификаторов аномальности; формирование решающих функций; формирование условных детекционных выражений. С помощью такого метода можно сформировать необходимое множество детекционных правил, по которым определяется уровень аномального состояния величин в гетерогенной параметрической среде окружения, характерный для воздействия определенного типа атак. Использование данного метода при построении систем обнаружения вторжений позволит расширить их функциональные возможности относительно выявления кибератак в слабоформализованной нечеткой среде окружения.

Ключевые слова: *детекционные правила, атаки, кибератаки, аномалии, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак.*

Актуальность

Формирование многих рынков и отраслей сегодня сложно представить без использования информационных технологий. Вследствие развития цифрового бизнеса и Интернета, вредоносное программное обеспечение, а также другие киберугрозы становятся все более распространенными и всепроникающими. В связи с этим необходимы соответствующие средства выявления кибератак на различные ресурсы информационных систем. Для этого используются специальные средства противодействия, которые способны оставаться эффективными при появлении новых видов угроз, характеризующихся неустановленными или нечетко определенными критериями. Следует отметить, что такие средства фактически могут оставаться функциональными в слабоформализованной нечеткой среде окружения. Применение необходимых методов и моделей информационной безопасности, основанных на нечетких множествах для построения средств обнаружения аномалий, порожденных соответствующей атакующей средой [1], является основой для успешного противодействия кибератакам. Одним из важных этапов выявления аномалий является построение нечетких (детекционных) правил [2-12]. Исходя из этого, актуальной научной задачей является формализация процесса создания детекционных правил, позволяющих в нечетких условиях выявить кибератаки ориентированные на различные ресурсы информационных систем.

Анализ существующих исследований

Известен ряд, достаточно эффективных разработок, используемых для решения указанных задач выявления кибератак, например, таких как: кортежная модель формирования набора базовых компонент для выявления кибератак [1], нечеткие подходы к обнаружению вторжений [2, 3] и детектированию аномалий [13]; соответствующие нечеткие модели [14-16], методы [4, 17-21] и системы обнаружения вторжений [22-24]; наборы нечетких правил [2-12]; а также другие разработки, используемые для решения задач защиты в нечетких условиях [25]. Эти исследования показали эффективность 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 множество атакующих воздействий на ресурсы информационных систем порождают множество аномалий среди величин в гетерогенной параметрической среде окружения [1, 26]. Для эффективного применения известной модели [1] необходима формальная реализация процесса формирования наборов базовых детекционных

правил, что позволит осуществить в заданной лингвистической переменной поиск идентифицирующего терма [18-21]. По этому терму с помощью соответствующего множества правил можно определить уровень аномального состояния, порожденного воздействием соответствующего класса кибератак.

Основная цель исследования

Исходя из анализа существующих исследований и актуальности поставленной задачи целью данной работы является разработка метода формирования базовых детекционных правил (МФДП) для систем обнаружения вторжений, функционирующих в слабоформализованной нечеткой среде окружения. С помощью такого метода (при решении задач выявления кибератак) можно эффективно детектировать уровень аномального состояния, характерного определенному типу атак относительно конкретной гетерогенной параметрической среды окружения в заданный временной промежуток.

Основная часть исследования

Для построения подмножеств базовых детекционных правил $\mathbf{DR_i}$ (см. (19) в [1]) разработаем соответствующий метод, который позволит формализовать процесс получения соответствующих правил, используемых для обнаружения i-й кибератаки на основе параметрических подсред различной размерности [1, 26]. Предлагаемый МФДП ориентирован на решение задач выявления атак в компьютерных системах, и основывается на трех этапах: формирование подмножеств идентификаторов аномальности; формирование решающих функций; формирование условных детекционных выражений.

Этап 1 – формирование подмножеств идентификаторов аномальности. Построение подмножества $\mathbf{IA_i}$ осуществляется на основе множества всех возможных идентификаторов (ИД) аномальности $\mathbf{IA}$, представляемых как

$$\mathbf{IA} = \{\bigcup_{o=1}^{\xi} IA_o\} = \{IA_1, IA_2, ..., AI_\xi\}, \quad (o = \overline{1,\xi}), \tag{1}$$

и посредством которых (в лингвистический форме) можно отобразить возможные уровни аномального состояния в среде окружения, которое может быть порождено кибератакой с ИД CA_i [1], а ξ – количество ИД аномальности.

Например, при $\xi = 9$ согласно (1) множество $\mathbf{IA}$ можно представить в следующем виде:

$$\begin{gathered}\mathbf{IA} = \{\bigcup_{o=1}^{9} IA_o\} = \{IA_1, IA_2, ..., AI_9\} = \\ \{IA_H, IA_{БНВ}, IA_{НС}, IA_C, IA_{ВС}, \\ IA_{ББН}, IA_B, IA_П, IA_Г\} = \\ \{"Н", "БНВ", "НС", "С", "ВС", \\ "ББН", "В", "П", "Г"\},\end{gathered} \tag{2}$$

где $IA_1 = IA_H = "Н"$, $IA_2 = IA_{БНВ} = "БНВ"$, $IA_3 = IA_{НС} = "НС"$, $IA_4 = IA_C = "С"$, $IA_5 = IA_{ВС} = "ВС"$, $IA_6 = IA_{ББН} = "ББН"$, $IA_7 = IA_B = "В"$, $IA_8 = IA_П = "П"$ и $IA_9 = IA_Г = "Г"$ соответственно являются ИД аномальности, посредством которых в лингвистических формах «НИЗКИЙ» (при $\xi = 1$), «БОЛЬШЕ НИЗКИЙ ЧЕМ ВЫСОКИЙ» (при $\xi = 2$), «НИЖЕ СРЕДНЕГО» (при $\xi = 3$), «СРЕДНИЙ» (при $\xi = 4$), «ВЫШЕ СРЕДНЕГО» (при $\xi = 5$), «БОЛЬШЕ ВЫСОКИЙ ЧЕМ НИЗКИЙ» (при $\xi = 6$), «ВЫСОКИЙ» (при $\xi = 7$), «ПРЕДЕЛЬНЫЙ» (при $\xi = 8$) и «ГРАНИЧНЫЙ» (при $\xi = 9$) можно отобразить возможные уровни аномальности.

Далее сформируем подмножества ИД аномальности для подмножества правил $\mathbf{DR_i}$ [1] т.е.:

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{IA_i}\} = \{\mathbf{IA_1}, \mathbf{IA_2}, \ldots, \mathbf{IA_n}\}, \tag{3}$$

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

$$\mathbf{IA_i} = \{\bigcup_{u=1}^{v_i} IA_{iu}\} = \{IA_{i1}, IA_{i2}, ..., IA_{iv_i}\}, \quad (u = \overline{1,v_i}), \tag{4}$$

при этом v_i обозначает количество ИД аномальности, посредством которых в лингвистических формах можно отобразить возможные уровни аномальности, порожденные кибератакой с ИД CA_i. Таким образом выражение (3) с учетом (4) представим в следующем виде:

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{IA_i}\} = \{\bigcup_{i=1}^{n}\{\bigcup_{u=1}^{v_i} IA_{iu}\}\} = \\ \{\{IA_{11}, IA_{12}, ..., IA_{1v_1}\}, \\ \{IA_{21}, IA_{22}, ..., IA_{2v_2}\}, \ldots, \\ \{IA_{u1}, IA_{u2}, ..., AI_{nv_n}\}\}.\end{gathered} \tag{5}$$

Например, при $n=3$ (т.е. для кибератак с ИД $CA_1=CA_{SN}=SN$, $CA_2=CA_{DS}=DS$ и $CA_3=CA_{SP}=SP$) и $v_1=v_2=v_3=5$ с учетом (1) определим необходимые ИД для отображения соответствующего уровня аномальности. Тогда выражение (5) с учетом (2) будет иметь следующий вид:

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{3}}\mathbf{IA_i}\}=\{\bigcup_{i=1}^{3}\{\bigcup_{u=1}^{v_i}IA_{iu}\}\}= \\ \{\{IA_{11},IA_{12},IA_{13},IA_{14},IA_{15}\}, \\ \{IA_{21},IA_{22},IA_{23},IA_{24},IA_{25}\}, \\ \{IA_{31},IA_{32},IA_{33},IA_{34},IA_{35}\}\}= \\ \{\{IA_{SNH},IA_{SNБНВ},IA_{SNББВ},IA_{SNB},IA_{SNП}\}, \\ \{IA_{DSH},IA_{DSБНВ},IA_{DSББВ},IA_{DSB},IA_{DSП}\}, \\ \{IA_{SPH},IA_{SPБНВ},IA_{SPББВ},IA_{SPB},IA_{SPП}\}\}= \\ \{\{"Н","БНВ","ББВ","В","П"\}, \\ \{"Н","БНВ","ББВ","В","П"\}, \\ \{"Н","БНВ","ББВ","В","П"\}\},\end{gathered} \tag{6}$$

где: $IA_{11}=IA_{SNH}="Н"$, $IA_{12}=IA_{SNБНВ}="БНВ"$, $IA_{13}=IA_{SNББВ}="ББВ"$, $IA_{14}=IA_{SNB}="В"$ и $IA_{15}=IA_{SNП}="П"$ соответственно являются ИД таких состояний аномальности в атакующей среде, которые отображают разную степень уверенности эксперта относительно воздействия кибератаки с ИД $CA_1=CA_{SN}$ [1]; $IA_{21}=IA_{DSH}="Н"$, $IA_{22}=IA_{DSБНВ}="БНВ"$, $IA_{23}=IA_{DSББВ}="ББВ"$, $IA_{24}=IA_{DSB}="В"$ и $IA_{25}=IA_{DSП}="П"$ соответственно являются ИД состояний аномальности в атакующей среде, отображающие разную степень уверенности эксперта относительно воздействия кибератаки с ИД $CA_2=CA_{DS}$; $IA_{31}=IA_{SPH}="Н"$, $IA_{32}=IA_{SPБНВ}="БНВ"$, $IA_{33}=IA_{SPББВ}="ББВ"$, $IA_{34}=IA_{SPB}="В"$ и $IA_{35}=IA_{SPП}="П"$ соответственно являются ИД таких состояний аномальности в атакующей среде, которые отображают разную степень уверенности эксперта относительно воздействия кибератаки с ИД $CA_3=CA_{SP}$.

Этап 2 – формирование решающих функций. Для реализации этого этапа введем множество всех аргументов решающих функций **AF** и подмножество таких аргументов $\mathbf{AF_i}$

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{AF_i}\}=\{\mathbf{AF_1},\mathbf{AF_2},\ldots,\mathbf{AF_n}\}, \tag{7}$$

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

$$\begin{gathered}\mathbf{AF_i}=\{\bigtimes_{\mathbf{a=1}}^{\mathbf{w_i}}\mathbf{AF_{ia}}\}=\{\mathbf{AF_{i1}}\times\mathbf{AF_{i2}}\times\ldots\times\mathbf{AF_{iw_i}}\}, \\ (a=\overline{1,w_i}),\end{gathered} \tag{8}$$

при этом w_i – количество подмножеств аргументов решающих функций, используемых для обнаружения i-й кибератаки, а символ $\times$ указывает на прямое произведение множеств. С учетом выражения (8) формулу (7) запишем в следующем виде:

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{AF_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigtimes_{\mathbf{a=1}}^{\mathbf{w_i}}\mathbf{AF_{ia}}\}\}= \\ \{\{\mathbf{AF_{11}},\mathbf{AF_{12}},\ldots,\mathbf{AF_{1w_1}}\}\times \\ \times\{\mathbf{AF_{21}},\mathbf{AF_{22}},\ldots,\mathbf{AF_{2w_2}}\}\times\ldots \\ \times\{\mathbf{AF_{n1}},\mathbf{AF_{n2}},\ldots,\mathbf{AF_{nw_n}}\}, \\ (i=\overline{1,n},\ a=\overline{1,w_i}).\end{gathered} \tag{9}$$

Подмножество $\mathbf{AF_{ia}}\subseteq\mathbf{AF_i}$ определим как:

$$\begin{gathered}\mathbf{AF_{ia}}=\{\bigcup_{s=1}^{r_j}AF_{ias}\}= \\ \{AF_{ia1},AF_{ia2},\ldots,AF_{iar_j}\},\ (s=\overline{1,r_j})\end{gathered} \tag{10}$$

где r_j – количество членов в $\mathbf{AF_{ia}}$ (что отображает количество членов в $\mathbf{T_{ij}^e}$ (см. (13) в [1])).

Тогда выражение (9) с учетом (10) принимает следующий вид:

$$\begin{gathered}\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\mathbf{AF_i}\}=\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}}\{\bigtimes_{\mathbf{a=1}}^{\mathbf{w_i}}\mathbf{AF_{ia}}\}\}=\{\bigcup_{i=1}^{n}\{\bigtimes_{a=1}^{w_i}\{\bigcup_{s=1}^{r_j}AF_{ias}\}\}\}= \\ \{\{\{AF_{111},AF_{112},\ldots,AF_{11r_j}\}\times\{AF_{121},AF_{122},\ldots,AF_{12r_j}\}\times\ldots\times\{AF_{1w_11},AF_{1w_12},\ldots,AF_{1w_1r_j}\}\}, \\ \{\{AF_{211},AF_{212},\ldots,AF_{21r_j}\}\times\{AF_{221},AF_{222},\ldots,AF_{22r_j}\}\times\ldots\times\{AF_{2w_21},AF_{2w_22},\ldots,AF_{2w_2r_j}\}\},\ldots, \\ \{\{AF_{n11},AF_{n12},\ldots,AF_{n1r_j}\}\times\{AF_{n21},AF_{n22},\ldots,AF_{n2r_j}\}\times\ldots\times\{AF_{nw_n1},AF_{nw_n2},\ldots,AF_{nw_nr_j}\}\}= \\ \{\{\langle AF_{111},AF_{121},\ldots,AF_{1w_11}\rangle,\langle AF_{111},AF_{121},\ldots,AF_{1w_12}\rangle,\ldots,\langle AF_{111},AF_{121},\ldots,AF_{1w_1r_1}\rangle, \\ \langle AF_{111},AF_{122},\ldots,AF_{1w_11}\rangle,\langle AF_{111},AF_{122},\ldots,AF_{1w_12}\rangle,\ldots,\langle AF_{111},AF_{122},\ldots,AF_{1w_1r_1}\rangle,\ldots, \\ \langle AF_{111},AF_{12r_2},\ldots,AF_{1w_11}\rangle,\langle AF_{111},AF_{12r_2},\ldots,AF_{1w_12}\rangle,\ldots,\langle AF_{111},AF_{12r_2},\ldots,AF_{1w_1r_1}\rangle,\end{gathered} \tag{11}$$

$$\langle AF_{112}, AF_{121}, ..., AF_{1w_1 1}\rangle, \langle AF_{112}, AF_{121}, ..., AF_{1w_1 2}\rangle, ..., \langle AF_{112}, AF_{121}, ..., AF_{1w_1 r_1}\rangle,$$
$$\langle AF_{112}, AF_{122}, ..., AF_{1w_1 1}\rangle, \langle AF_{112}, AF_{122}, ..., AF_{1w_1 2}\rangle, ..., \langle AF_{112}, AF_{122}, ..., AF_{1w_1 r_1}\rangle, ...,$$
$$\langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 1}\rangle, \langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 2}\rangle, ..., \langle AF_{112}, AF_{12r_2}, ..., AF_{1w_1 r_1}\rangle, ...,$$
$$\langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 1}\rangle, \langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 2}\rangle, ..., \langle AF_{11r_1}, AF_{121}, ..., AF_{1w_1 r_1}\rangle,$$
$$\langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 1}\rangle, \langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 2}\rangle, ..., \langle AF_{11r_1}, AF_{122}, ..., AF_{1w_1 r_1}\rangle, ...,$$
$$\langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 1}\rangle, \langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 2}\rangle, ..., \langle AF_{11r_1}, AF_{12r_2}, ..., AF_{1w_1 r_1}\rangle\},$$
$$...,$$
$$\{\langle AF_{n11}, AF_{n21}, ..., AF_{nw_n 1}\rangle, \langle AF_{n11}, AF_{n21}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n11}, AF_{n21}, ..., AF_{nw_n r_j}\rangle,$$
$$\langle AF_{n11}, AF_{n22}, ..., AF_{nw_n 1}\rangle, \langle AF_{n11}, AF_{n22}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n11}, AF_{n22}, ..., AF_{nw_n r_j}\rangle, ...,$$
$$\langle AF_{n11}, AF_{n2r_2}, ..., AF_{nw_n 1}\rangle, \langle AF_{n11}, AF_{n2r_2}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n11}, AF_{n2r_2}, ..., AF_{nw_n r_j}\rangle,$$
$$\langle AF_{n12}, AF_{n21}, ..., AF_{nw_n 1}\rangle, \langle AF_{n12}, AF_{n21}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n12}, AF_{n21}, ..., AF_{nw_n r_j}\rangle,$$
$$\langle AF_{n12}, AF_{n22}, ..., AF_{nw_n 1}\rangle, \langle AF_{n12}, AF_{n22}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n12}, AF_{n22}, ..., AF_{nw_n r_j}\rangle, ...,$$
$$\langle AF_{n12}, AF_{n2r_2}, ..., AF_{nw_n 1}\rangle, \langle AF_{n12}, AF_{n2r_2}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n12}, AF_{n2r_2}, ..., AF_{nw_n r_j}\rangle, ...,$$
$$\langle AF_{n1r_1}, AF_{n21}, ..., AF_{nw_n 1}\rangle, \langle AF_{n1r_1}, AF_{n21}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n1r_1}, AF_{n21}, ..., AF_{nw_n r_j}\rangle,$$
$$\langle AF_{n1r_1}, AF_{n22}, ..., AF_{nw_n 1}\rangle, \langle AF_{n1r_1}, AF_{n22}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n1r_1}, AF_{n22}, ..., AF_{nw_n r_j}\rangle, ...,$$
$$\langle AF_{n1r_1}, AF_{n2r_2}, ..., AF_{nw_n 1}\rangle, \langle AF_{n1r_1}, AF_{n2r_2}, ..., AF_{nw_n 2}\rangle, ..., \langle AF_{n1r_1}, AF_{n2r_2}, ..., AF_{nw_n r_j}\rangle\}\} =$$
$$\{\{\langle \mathbf{SAF_{11}}\rangle, \langle \mathbf{SAF_{12}}\rangle, ..., \langle \mathbf{SAF_{1w_1}}\rangle\}, ..., \{\langle \mathbf{SAF_{i1}}\rangle, \langle \mathbf{SAF_{i2}}\rangle, ..., \langle \mathbf{SAF_{iw_i}}\rangle\}, ...,$$
$$\{\langle \mathbf{SAF_{n1}}\rangle, \langle \mathbf{SAF_{n2}}\rangle, ..., \langle \mathbf{SAF_{nw_n}}\rangle\}\},$$

где для наглядности используются угловые скобки "$\langle$", "$\rangle$", которые отделяют подмножества аргументов решающих функций ($\mathbf{SAF_{ia}}$), отображающие значения термов $\mathbf{T_{ij}^{ep}}$.

С учетом выражения (11) определим, что для выявления i-й кибератаки общее количество подмножеств аргументов вычисляется по формуле

$$w_i = \prod_{j=1}^{m_i} r_j, \ (j = \overline{1,m_i}). \quad (12)$$

Тогда (11) с учетом (12) можно записать в следующем виде

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{AF_i}\} = \{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \{\bigcup_{\mathbf{a=1}}^{\mathbf{w_i}} \langle \mathbf{SAF_{ia}}\rangle\}\}, \quad (13)$$
$$(a = \overline{1,w_i}).$$

Далее введем множество всех бинарных решающих функций $\mathbf{SF}$ и подмножество таких функций $\mathbf{SF_i}$

$$\{\bigcup_{\mathbf{i=1}}^{\mathbf{n}} \mathbf{SF_i}\} = \{\mathbf{SF_1}, \mathbf{SF_2}, ..., \mathbf{SF_n}\}, \quad (14)$$

где $\mathbf{SF_i} \subseteq \mathbf{SF}$, $(i = \overline{1,n})$ определим как

$$\mathbf{SF_i} = \{\bigcup_{a=1}^{w_i} SF_{ia}\} = \{SF_{i1}, SF_{i2}, ..., SF_{iw_i}\}, \quad (15)$$

а

$$SF_{ia} = SF_{ia}(\mathbf{SAF_{ia}}). \quad (16)$$

Отметим, что функция SF_{ia} определяет взаимосвязи в $\mathbf{SAF_{ia}}$, формируемые экспертом в виде логических цепочек (основанных на дизъюнкциях и конъюнкциях) для последующего построения детекционных выражений, ориентированных на выявление i-й кибератаки.

Эксперт для получения конкретного множества бинарных функций, которое выявляет i-ю кибератаку создает соответствующий шаблон, определяющий взаимосвязи в $\mathbf{SAF_{ia}}$. Например, если $\mathbf{SAF_{ia}} = \langle AF_{111}, AF_{112}, AF_{113}\rangle$, а шаблоны имеют вид $\langle AF \wedge AF \wedge AF\rangle$ или $\langle AF \wedge (AF \vee AF)\rangle$, то соответственно $SF_{11} = AF_{111} \wedge AF_{112} \wedge AF_{113}$ или $SF_{11} = AF_{111} \wedge (AF_{112} \vee AF_{113})$.

Конкретные значения элементов подмножества $\mathbf{AF_i}$ $(i = \overline{1,n})$ формируются на основе бинарной функции эквивалентности $E(x, y)$, принимающей значение 1 только при равенстве x и y, т.е.:

$$E(x, y)=\begin{cases}1, \text{ при } x=y\\ 0, \text{ при } x\neq y.\end{cases} \quad (17)$$

Исходя из этого определим, что $AF_{ias}=E(NUM_{ia}, s)$, а в качестве аргументов $E(x, y)$ используются индексы нечетких термов $\mathbf{T}_{ij}^{ep}$ и $\mathbf{P}_{i}^{\tau_f p}$.

Рассмотрим пример формирования решающих функций 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 $\mathbf{CA}_3^{\tau_f}=\mathbf{CA}_{SP}^{\tau_f}=\mathbf{SP}^{\tau_f}$), $m_1=m_3=2$, $m_2=3$, $r_1=5$, $r_2=r_3=3$ (см. пример (15) в [1]).

Согласно (12) $w_1=\prod_{j=1}^{m_1} r_j=r_1\cdot r_2=5\cdot 3=15$, $w_2=\prod_{j=1}^{m_2} r_j=r_1\cdot r_2\cdot r_3=5\cdot 3\cdot 3=45$, $w_3=\prod_{j=1}^{m_3} r_j=r_1\cdot r_2=5\cdot 3=15$, а выражение (11) можно определить как:

$$\{\bigcup_{i=1}^{3}\mathbf{AF}_i\}=\{\mathbf{AF}_1, \mathbf{AF}_2, \mathbf{AF}_3\}=\{\bigcup_{i=1}^{3}\{\times_{a=1}^{w_i}\mathbf{AF}_{ia}\}\}=\{\bigcup_{i=1}^{3}\{\times_{a=1}^{w_i}\{\bigcup_{s=1}^{r_j}AF_{ias}\}\}\}=$$
$$\{\{\{AF_{111}, AF_{112}, AF_{113}, AF_{114}, AF_{115}\}\times\{AF_{121}, AF_{122}, AF_{123}\}\},$$
$$\{\{AF_{211}, AF_{212}, AF_{213}, AF_{214}, AF_{215}\}\times\{AF_{221}, AF_{222}, AF_{223}\}\times\{AF_{231}, AF_{232}, AF_{233}\}\},$$
$$\{\{AF_{311}, AF_{312}, AF_{313}, AF_{314}, AF_{315}\}\times\{AF_{321}, AF_{322}, AF_{323}\}\}\}=$$
$$\{\langle AF_{111}, AF_{121}\rangle, \langle AF_{112}, AF_{121}\rangle, \langle AF_{113}, AF_{121}\rangle, \langle AF_{114}, AF_{121}\rangle, \langle AF_{115}, AF_{121}\rangle, ...,$$
$$\langle AF_{111}, AF_{123}\rangle, \langle AF_{112}, AF_{123}\rangle, \langle AF_{113}, AF_{123}\rangle, \langle AF_{114}, AF_{123}\rangle, \langle AF_{115}, AF_{123}\rangle\},$$
$$\{\langle AF_{211}, AF_{221}, AF_{231}\rangle, \langle AF_{212}, AF_{221}, AF_{231}\rangle, \langle SF_{213}, AF_{221}, AF_{231}\rangle,$$
$$\langle AF_{214}, AF_{221}, AF_{231}\rangle, \langle AF_{215}, AF_{221}, AF_{231}\rangle ...,$$
$$\langle AF_{211}, AF_{223}, AF_{233}\rangle, \langle AF_{212}, AF_{223}, AF_{233}\rangle, \langle AF_{213}, AF_{223}, AF_{233}\rangle,$$
$$\langle AF_{214}, AF_{223}, AF_{233}\rangle, \langle AF_{215}, AF_{223}, AF_{233}\rangle\},$$
$$\{\langle AF_{311}, AF_{321}\rangle, \langle AF_{312}, AF_{321}\rangle, \langle AF_{313}, AF_{321}\rangle, \langle AF_{314}, AF_{321}\rangle, \langle AF_{315}, AF_{321}\rangle, ...,$$
$$\langle AF_{311}, AF_{323}\rangle, \langle AF_{312}, AF_{323}\rangle, \langle AF_{313}, AF_{323}\rangle, \langle AF_{314}, AF_{323}\rangle, \langle AF_{315}, AF_{323}\rangle\}=$$
$$\{\{\langle\mathbf{SAF}_{11}\rangle, \langle\mathbf{SAF}_{12}\rangle, ..., \langle\mathbf{SAF}_{1\,15}\rangle\}, \{\langle\mathbf{SAF}_{21}\rangle, \langle\mathbf{SAF}_{22}\rangle, ..., \langle\mathbf{SAF}_{2\,45}\rangle\},$$
$$\{\langle\mathbf{SAF}_{31}\rangle, \langle\mathbf{SAF}_{32}\rangle, ..., \langle\mathbf{SAF}_{3\,15}\rangle\}\}. \quad (18)$$

В [1] определено, что для выявления кибератак «Сканирование портов (SN)» ($\mathbf{CA}_1^{\tau_f}=\mathbf{CA}_{SN}^{\tau_f}=\mathbf{SN}^{\tau_f}$) и «Спуфинг (SP)» ($\mathbf{CA}_3^{\tau_f}=\mathbf{CA}_{SP}^{\tau_f}=\mathbf{SP}^{\tau_f}$), необходимо одновременно использовать два параметра, определяющих 2-мерную параметрическую подсреду (КВК-ВВК-подсреду и КОП-КПОА-подсреду), а для кибератаки «Отказ в обслуживании (DS)» ($\mathbf{CA}_2^{\tau_f}=\mathbf{CA}_{DS}^{\tau_f}=\mathbf{DS}^{\tau_f}$) – три параметра, определяющих 3-мерную параметрическую подсреду (КОП-СОЗ-ЗМЗ-подсреду) (см. (9) в [1]). Эксперт для получения конкретного множества функций, которые выявляют SN и SP создает шаблон $\langle AF\wedge AF\rangle$, а для DS – $\langle AF\wedge(AF\vee AF)\rangle$.

Далее, согласно сформированных шаблонов, а также (15) и (18) определим:

$$\mathbf{SF}_1=\{\bigcup_{a=1}^{w_1}SF_{1a}\}=$$
$$\{(E(NUM_{11}, 1)\wedge E(NUM_{12}, 1)),$$
$$(E(NUM_{11}, 2)\wedge E(NUM_{12}, 1)),$$
$$(E(NUM_{11}, 3)\wedge E(NUM_{12}, 1)),$$
$$(E(NUM_{11}, 4)\wedge E(NUM_{12}, 1)),$$
$$(E(NUM_{11}, 5)\wedge E(NUM_{12}, 1))\},$$
$$\{(E(NUM_{11}, 1)\wedge E(NUM_{12}, 2)),$$
$$(E(NUM_{11}, 2)\wedge E(NUM_{12}, 2)),$$
$$(E(NUM_{11}, 3)\wedge E(NUM_{12}, 2)),$$
$$(E(NUM_{11}, 4)\wedge E(NUM_{12}, 2)),$$
$$(E(NUM_{11}, 5)\wedge E(NUM_{12}, 2))\},$$
$$\{(E(NUM_{11}, 1)\wedge E(NUM_{12}, 3)),$$
$$(E(NUM_{11}, 2)\wedge E(NUM_{12}, 3)),$$

$$(E(NUM_{11}, 3) \wedge E(NUM_{12}, 3)),$$
$$(E(NUM_{11}, 4) \wedge E(NUM_{12}, 3)),$$
$$(E(NUM_{11}, 5) \wedge E(NUM_{12}, 3))\},$$

$$\mathbf{SF_2} = \{\bigcup_{a=1}^{w_2} SF_{2a}\} =$$

$$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 1)))\},$$
$$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 2)))\},$$
$$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 3))),$$
$$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 3))),$$
$$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 3))),$$
$$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 3))),$$
$$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 1) \vee E(NUM_{23}, 3)))\},$$
$$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 1)))\},$$
$$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 2)))\},$$
$$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3))),$$
$$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3))),$$
$$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3))),$$
$$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3))),$$
$$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 2) \vee E(NUM_{23}, 3)))\},$$
$$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 4) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1))),$$
$$(E(NUM_{21}, 5) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 1)))\},$$
$$\{(E(NUM_{21}, 1) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 2) \wedge (E(NUM_{22}, 3) \vee E(NUM_{23}, 2))),$$
$$(E(NUM_{21}, 3) \wedge (E(NUM_{22}, 3) \vee$$

$$E\,(NUM_{23},\,2))),$$
$$(E\,(NUM_{21},\,4)\wedge(E\,(NUM_{22},\,3)\vee$$
$$E\,(NUM_{23},\,2))),$$
$$(E\,(NUM_{21},\,5)\wedge(E\,(NUM_{22},\,3)\vee$$
$$E\,(NUM_{23},\,2)))\},$$
$$\{(E\,(NUM_{21},\,1)\wedge(E\,(NUM_{22},\,3)\vee$$
$$E\,(NUM_{23},\,3))),$$
$$(E\,(NUM_{21},\,2)\wedge(E\,(NUM_{22},\,3)\vee$$
$$E\,(NUM_{23},\,3))),$$
$$(E\,(NUM_{21},\,3)\wedge(E\,(NUM_{22},\,3)\vee$$
$$E\,(NUM_{23},\,3))),$$
$$(E\,(NUM_{21},\,4)\wedge(E\,(NUM_{22},\,3)\vee$$
$$E\,(NUM_{23},\,3))),$$
$$(E\,(NUM_{21},\,5)\wedge(E\,(NUM_{22},\,3)\vee$$
$$E\,(NUM_{23},\,3)))\},$$

$$\mathbf{SF_3}=\{\bigcup_{a=1}^{w_3}SF_{3a}\}=$$
$$\{(E\,(NUM_{31},\,1)\wedge E\,(NUM_{32},\,1)),$$
$$(E\,(NUM_{31},\,2)\wedge E\,(NUM_{32},\,1)),$$
$$(E\,(NUM_{31},\,3)\wedge E\,(NUM_{32},\,1)),$$
$$(E\,(NUM_{31},\,4)\wedge E\,(NUM_{32},\,1)),$$
$$(E\,(NUM_{31},\,5)\wedge E\,(NUM_{32},\,1))\},$$
$$\{(E\,(NUM_{31},\,1)\wedge E\,(NUM_{32},\,2)),$$
$$(E\,(NUM_{31},\,2)\wedge E\,(NUM_{32},\,2)),$$
$$(E\,(NUM_{31},\,3)\wedge E\,(NUM_{32},\,2)),$$
$$(E\,(NUM_{31},\,4)\wedge E\,(NUM_{32},\,2)),$$
$$(E\,(NUM_{31},\,5)\wedge E\,(NUM_{32},\,2))\},$$
$$\{(E\,(NUM_{31},\,1)\wedge E\,(NUM_{32},\,3)),$$
$$(E\,(NUM_{31},\,2)\wedge E\,(NUM_{32},\,3)),$$
$$(E\,(NUM_{31},\,3)\wedge E\,(NUM_{32},\,3)),$$
$$(E\,(NUM_{31},\,4)\wedge E\,(NUM_{32},\,3)),$$
$$(E\,(NUM_{31},\,5)\wedge E\,(NUM_{32},\,3))\}.$$

На рис. 1 представлено экспертное распределение всех возможных уровней аномальности, порожденных атакующей средой и отображаемых идентификаторами атакующих действий посредством различных значений параметров КОП-КПОА-подсреды.

Из графической интерпретации (рис. 1) видно, что наиболее значимыми для выявления SN являются опорные блоки с идентификаторами БВН, В и П. Исходя из этого пример конкретных расчетов представим только для решающих функций $(SF_{3\,11},\ ...,\ SF_{3\,15})$ из $\mathbf{SF_3}$, т.е.

$$SF_{3\,11}=(E\,(NUM_{31},\,1)\wedge E\,(NUM_{32},\,3)),$$
$$SF_{3\,12}=(E\,(NUM_{31},\,2)\wedge E\,(NUM_{32},\,3)),$$
$$SF_{3\,13}=(E\,(NUM_{31},\,3)\wedge E\,(NUM_{32},\,3)),\qquad(19)$$
$$SF_{3\,14}=(E\,(NUM_{31},\,4)\wedge E\,(NUM_{32},\,3)),$$
$$SF_{3\,15}=(E\,(NUM_{31},\,5)\wedge E\,(NUM_{32},\,3)).$$

Отметим, что при $j=1$, $r_1=5$, $NUM_{31}=3$ и $s=\overline{1,5}$ для $\mathbf{T^e_{31}}=\{\bigcup_{s=1}^{5}\underset{\sim}{T}^{ep}_{31s}\}=\{\underset{\sim}{T}^{ep}_{311},\ \underset{\sim}{T}^{ep}_{312},\ \underset{\sim}{T}^{ep}_{313},\ \underset{\sim}{T}^{ep}_{314},\ \underset{\sim}{T}^{ep}_{315}\}=\{\underset{\sim}{QM}^{ep}_{31},\ \underset{\sim}{M}^{ep}_{31},\ \underset{\sim}{C}^{ep}_{31},\ \underset{\sim}{B}^{ep}_{31},\ \underset{\sim}{QB}^{ep}_{31}\}$ (см. (27) в [18]) функция эквивалентности E согласно (17) принимает значение $E(NUM_{31},\,1)=E(NUM_{31},\,2)=E(NUM_{31},\,4)=E(NUM_{31},\,5)=0$ поскольку $NUM_{31}=3\neq1\neq2\neq4\neq5$. Это следует из того, что $\underset{\sim}{T}^{ep}_{313}\neq\underset{\sim}{T}^{ep}_{311}\neq\underset{\sim}{T}^{ep}_{312}\neq\underset{\sim}{T}^{ep}_{314}\neq\underset{\sim}{T}^{ep}_{315}$, т.е. $\underset{\sim}{C}^{ep}_{31}\neq\underset{\sim}{QM}^{ep}_{31}\neq\underset{\sim}{M}^{ep}_{31}\neq\underset{\sim}{B}^{ep}_{31}\neq\underset{\sim}{QB}^{ep}_{31}$. Также $E(NUM_{31},\,3)=1$ поскольку $NUM_{31}=3$, что следует из того, что $\underset{\sim}{T}^{ep}_{313}=\underset{\sim}{T}^{ep}_{313}$, т.е. $\underset{\sim}{C}^{ep}_{31}=\underset{\sim}{C}^{ep}_{31}$.

Аналогичным образом для $\mathbf{T^e_{32}}=\{\bigcup_{s=1}^{3}\underset{\sim}{T}^{ep}_{32s}\}=\{\underset{\sim}{T}^{ep}_{321},\ \underset{\sim}{T}^{ep}_{322},\ \underset{\sim}{T}^{ep}_{323}\}=\{\underset{\sim}{M}^{ep}_{32},\ \underset{\sim}{C}^{ep}_{32},\ \underset{\sim}{B}^{ep}_{32}\}$ при $j=2$, $r_2=3$, $NUM_{32}=3$, $s=\overline{1,3}$ (см. (27) в [18]) функция эквивалентности E согласно (17) принимает значение $E(NUM_{32},\,1)=E(NUM_{32},\,2)=0$ поскольку $NUM_{32}=3\neq1\neq2$. Это следует из того, что $\underset{\sim}{T}^{ep}_{323}\neq\underset{\sim}{T}^{ep}_{321}\neq\underset{\sim}{T}^{ep}_{322}$, т.е. $\underset{\sim}{B}^{ep}_{32}\neq\underset{\sim}{M}^{ep}_{32}\neq\underset{\sim}{C}^{ep}_{32}$, а $E(NUM_{32},\,3)=1$ поскольку $NUM_{32}=3$, что следует из того, что $\underset{\sim}{T}^{ep}_{323}=\underset{\sim}{T}^{ep}_{323}$, т.е. $\underset{\sim}{B}^{ep}_{32}=\underset{\sim}{B}^{ep}_{32}$. Таким образом

$$SF_{3\,11}=(E\,(NUM_{31},\,1)\wedge E\,(NUM_{32},\,3))=(1\wedge0)=0,$$
$$SF_{3\,12}=(E\,(NUM_{31},\,2)\wedge E\,(NUM_{32},\,3))=(1\wedge0)=0,$$
$$SF_{3\,13}=(E\,(NUM_{31},\,3)\wedge E\,(NUM_{32},\,3))=(1\wedge1)=1,\qquad(20)$$
$$SF_{3\,14}=(E\,(NUM_{31},\,4)\wedge E\,(NUM_{32},\,3))=(1\wedge0)=0,$$
$$SF_{3\,15}=(E\,(NUM_{31},\,5)\wedge E\,(NUM_{32},\,3))=(1\wedge0)=0.$$

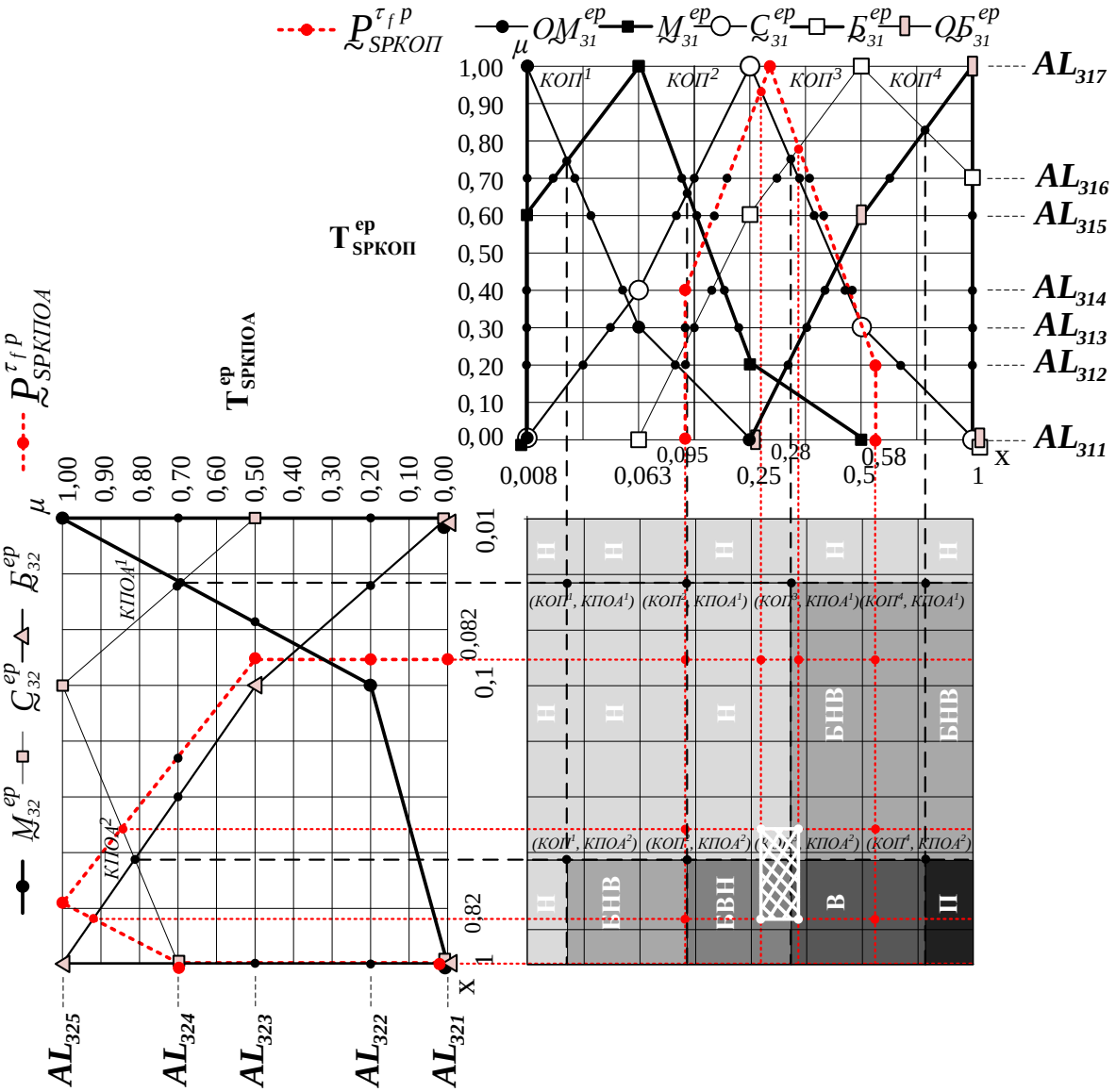

Рис. 1. Графическая интерпретация экспертного распределения идентификаторов атакующих действий (отображаемых двумерными опорными областями Н, БНВ, БВН, В, П) и фаззифицированных значений текущих параметров $\tilde{P}^{\tau_f}_{31}$, $\tilde{P}^{\tau_f}_{32}$ относительно лингвистических эталонов $\mathbf{T}^{ep}_{31}$, $\mathbf{T}^{ep}_{32}$ соответственно.

Этап 3 – формирование условных детекционных выражений. Условные детекционные выражения, отображающие формируемые базовые правила для выявления i-й кибератаки (см. (19) в [1]) представим в следующем виде:

$$\mathbf{DR_i} = \{\bigcup_{a=1}^{w_i} \mathbf{DR_{ia}}\} =$$

$$\{\mathbf{DR_{i1}}, \mathbf{DR_{i2}}, \ldots, \mathbf{DR_{iw_i}}\} =$$

$$\{\ \mathbf{DR_{i1}} \Rightarrow \{ if\ SF_{i1}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\ \}\},$$

$$\mathbf{DR_{i2}} \Rightarrow \{ if\ SF_{i2}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\ \}\},\ ...,$$

$$\mathbf{DR_{iw_i}} \Rightarrow \{ if\ SF_{ia}\ then\ \{\bigcup_{u=1}^{v_i} IA_{iu}\ \}\}\}, \quad (21)$$

$$(a = \overline{1,w_i}\ ,\ u = \overline{1,v_i}\ ).$$

Отметим, что формально каждая SF_{ia} может быть связана с v_i-м количеством идентификаторов аномальности и, таким образом, каждое базовое правило может породить v_i детекционных выражений, т.е.:

$$\mathbf{DR_i} = \{\mathbf{DR_{i1}}, \mathbf{DR_{i2}}, \ldots, \mathbf{DR_{iw_i}}\} =$$

$$\{\ \mathbf{DR_{i1}} \Rightarrow \quad (22)$$

$$\{ if\ SF_{i1}\ then\ IA_{i1}, if\ SF_{i1}\ then\ IA_{i2}, ...,$$

$$if\ SF_{i1}\ then\ IA_{iv_i}\ \},$$

$$\mathbf{DR_{i2}} \Rightarrow$$

$$\{ if\ SF_{i2}\ then\ IA_{i1},\ if\ SF_{i2}\ then\ IA_{i2},\ ...,$$

$$if\ SF_{i2}\ then\ IA_{iv_i}\ \},\ ...,$$

$$\mathbf{DR_{iw_i}} \Rightarrow$$

$$\{ if\ SF_{iw_i}\ then\ IA_{i1},\ if\ SF_{iw_i}\ then\ IA_{i2},\ ...,$$

$$if\ SF_{iw_i}\ then\ IA_{iv_i}\ \}\}$$

или

$$\mathbf{DR_i} = \{ \bigcup_{a=1}^{w_i} \{ \bigcup_{u=1}^{v_i} if\ SF_{ia}\ then\ IA_{iu}\ \}\},$$

$$(a = \overline{1,w_i},\ u = \overline{1,v_i}).$$

Очевидно, что возможное количество условных детекционных выражений для выявления i-й кибератаки определяется по формуле

$$CDR_i = w_i \cdot v_i, \qquad (23)$$

а их количество для выявления n атак вычисляется по выражению

$$CDR = \sum_{i=1}^{n} CDR_i .$$

Следует отметить, что из общего количества возможных детекционных выражений не все являются определяющими (т.е. влияют на процесс обнаружения вторжения) для выявления i-й кибератаки, что также следует из рис. 1 и (20) (здесь определяющими будут $\mathbf{DR_{3\ 11}} - \mathbf{DR_{3\ 15}}$).

С учетом этого, рассмотрим пример реализации этапа 3 при $i = 3$ $(CA_3 = CA_{SP} = SP)$, $j = \overline{1,2}$ $(P_{31} = P_{SPKOP} = KOP, P_{32} = P_{SPKPOA} = KPOA)$, $u_3 = 5$, $w_3 = 15$. Тогда общее количество правил определим по формуле (23), т.е. $CDR_3 = w_3 \cdot v_3 = 15 \cdot 5 = 75$, а выражение (22) будет иметь следующий вид:

$$\mathbf{DR_3} = \{ ...,\ \mathbf{DR_{3\ 11}} \Rightarrow$$

$$\{ if\ SF_{3\ 11}\ then\ IA_{31},\ if\ SF_{3\ 11}\ then\ IA_{32},$$

$$if\ SF_{3\ 11}\ then\ IA_{33},$$

$$if\ SF_{3\ 11}\ then\ IA_{34},\ if\ SF_{3\ 11}\ then\ IA_{35}\ \},$$

$$\mathbf{DR_{3\ 12}} \Rightarrow \qquad (24)$$

$$\{ if\ SF_{3\ 12}\ then\ IA_{31},\ if\ SF_{3\ 12}\ then\ IA_{32},$$

$$if\ SF_{3\ 12}\ then\ IA_{33},$$

$$if\ SF_{3\ 12}\ then\ IA_{34},\ if\ SF_{3\ 12}\ then\ IA_{35}\ \},$$

$$\mathbf{DR_{3\ 13}} \Rightarrow$$

$$\{ if\ SF_{3\ 13}\ then\ IA_{31},\ if\ SF_{3\ 13}\ then\ IA_{32},$$

$$if\ SF_{3\ 13}\ then\ IA_{33},$$

$$if\ SF_{3\ 13}\ then\ IA_{34},\ if\ SF_{3\ 13}\ then\ IA_{35}\ \},$$

$$\mathbf{DR_{3\ 14}} \Rightarrow$$

$$\{ if\ SF_{3\ 14}\ then\ IA_{31},\ if\ SF_{3\ 14}\ then\ IA_{32},$$

$$if\ SF_{3\ 14}\ then\ IA_{33},$$

$$if\ SF_{3\ 14}\ then\ IA_{34},\ if\ SF_{3\ 14}\ then\ IA_{35}\ \},$$

$$\mathbf{DR_{3\ 15}} \Rightarrow$$

$$\{ if\ SF_{3\ 15}\ then\ IA_{31},\ if\ SF_{3\ 15}\ then\ IA_{32},$$

$$if\ SF_{3\ 15}\ then\ IA_{33},$$

$$if\ SF_{3\ 15}\ then\ IA_{34},\ if\ SF_{3\ 15}\ then\ IA_{35}\ \}\}.$$

Согласно заданных в примере исходных данных, а также с учетом выражения (20) и графической визуализации (см. рис. 1) видно, что определяющей является решающая функция $SF_{3\ 13}$, которая входит в подмножество детекционных выражений $\mathbf{DR_{3\ 13}}$, т.е.:

$$\mathbf{DR_{3\ 13}} \Rightarrow \{ if\ SF_{3\ 13}\ then\ IA_{31},\ if\ SF_{3\ 13}\ then\ IA_{32},$$

$$if\ SF_{3\ 13}\ then\ IA_{33},$$

$$if\ SF_{3\ 13}\ then\ IA_{34},\ if\ SF_{3\ 13}\ then\ IA_{35}\ \} =$$

$$\{ if\ \ (E(NUM_{31},\ 1) \wedge E(NUM_{32},\ 3))$$

$$then\ \ IA_{31},$$

$$if\ \ (E(NUM_{31},\ 2) \wedge E(NUM_{32},\ 3))$$

$$then\ \ IA_{32},$$

$$if\ \ (E(NUM_{31},\ 3) \wedge E(NUM_{32},\ 3))$$

$$then\ \ IA_{33},$$

$$if\ \ (E(NUM_{31},\ 4) \wedge E(NUM_{32},\ 3))$$

$$then\ \ IA_{34},$$

$$if\ \ (E(NUM_{31},\ 5) \wedge E(NUM_{32},\ 3))$$

$$then\ \ IA_{35}\ \} =$$

$$\{ if\ \ (E(NUM_{SPKOP},\ 1) \wedge E(NUM_{SPKPOA},\ 3))$$

$$then\ "H",$$

$$if\ \ (E(NUM_{SPKOP},\ 2) \wedge E(NUM_{SPKPOA},\ 3))$$

$$then\ "БНВ",$$

$$if\ \ (E(NUM_{SPKOP},\ 3) \wedge E(NUM_{SPKPOA},\ 3))$$

$$then\ "БВН",$$

$$if\ \ (E(NUM_{SPKOP},\ 4) \wedge E(NUM_{SPKPOA},\ 3))$$

$$then\ "В",$$

$$if\ \ (E(NUM_{SPKOP}, 5) \wedge E(NUM_{SPKPOA}, 3))\ then\ "П"\}.$$

После проверки всех правил в $\mathbf{DR}_{3\ 13}$ определим, что идентификация аномального состояния осуществляется посредством условного выражения

$$if\ \ (E(NUM_{SPKOP}, 3) \wedge E(NUM_{SPKPOA}, 3))\ then\ "БВН" = if\ (1 \wedge 1)\ then\ "БВН".$$

На рис. 1 графически показан текущий блок (в виде заштрихованной прямоугольной области, образованный с помощью $\underset{\sim}{P}_{31}^{\tau_f}$, $\underset{\sim}{P}_{32}^{\tau_f}$) интерпретирующий аномалию в 2-мерной параметрической КОП-КПОА-подсреде, порожденную соответствующей атакующей SP-средой в момент времени τ_f. Здесь, даже при визуальном сравнении, можно определить, что полученный текущий блок ближе всего расположен к нечеткой опорной двумерной области с идентификатором *"БВН"*, а используемое правило буквально можно интерпретировать как: «Если текущее значение нечеткого параметра «Количество одновременных подключений к серверу» в момент времени τ_f наиболее близко к эталонному нечеткому числу «Среднее» и, при этом, текущее значение нечеткого параметра «Количество пакетов с одинаковым адресом отправителя и получателя» в момент времени τ_f наиболее близко к эталонному нечеткому числу «Большое», то уровень аномального состояния, который может быть порожден спуфингом будет «Больше высокий чем низкий». Аналогичным образом при различных исходных данных определяются другие типы кибератак, порождающие определенные аномалии в информационных системах.

Таким образом, в работе предложен МФДП, который на основе базовой кортежной модели [1] за счет механизма формирования подмножеств идентификаторов аномальности, формализации процесса построения решающих функций и условных детекционных выражений позволяет сформировать необходимое множество детекционных правил, используемых для определения уровня аномального состояния, характерного воздействию определенного типа атак. Использование данного метода при построении систем обнаружения вторжений позволит расширить их функциональные возможности относительно выявления кибератак в слабоформализованной нечеткой среде окружения.

ЛИТЕРАТУРА

[1]. Корченко А.А. Кортежная модель формирования набора базовых компонент для выявления кибератак / А.А. Корченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – В.2 (28). – С. 29-36.

[2]. Yao J.T., Zhao S.L., Saxton L.V. «A study on fuzzy intrusion detection» Proc. of SPIE Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, Orlando, Florida, USA, Vol. 5812, 2005, pp. 23-30.

[3]. Fries P. «A Fuzzy-Genetic Approach to Network Intrusion Detection Terrence» Genetic and Evolutionary Computation Conference, GECCO (Companion) July 12-16, 2008, pp. 2141-2146.

[4]. Wijayasekara D., Linda O., Manic M., Rieger C.G. Mining Building Energy Management System Data Using Fuzzy Anomaly Detection and Linguistic Descriptions. IEEE Trans. Industrial Informatics. Vol. 10, № 3, 2014, pp. 1829-1840.

[5]. Shanmugavadivu R., Nagarajan N. «Network Intrusion Detection System Using Fuzzy Logic», Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2, No. 1, pp. 101-111, 2011.

[6]. Linda O., Vollmer T., Wright J., Manic M. «Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor», in Proc. IEEE Symposium Series on Computational Intelligence, Paris, France, April, 2011, pp. 202-209.

[7]. Bridges S.M., Vaughn R.B. «Fuzzy data mining and genetic algorithms applied to intrusion detection». In: Proceedings of the 23rd National Information Systems Security Conference. October 2000, pp. 13-31.

[8]. Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha, Mat Kiah, Sanjay Misra «Anomaly Detection using Fuzzy Q-learning Algorithm» Acta Polytechnica Hungarica. Vol. 11, № 8, 2014, pp. 5-28.

[9]. John E. Dickerson, Jukka Juslin, Ourania Koukousoula, Julie A. Dickerson «Fuzzy Intrusion Detection» IFSA World Congress and 20th NAFIPS International Conference, 2001. Joint 9th. Vol. 3, pp. 1506-1510.

[10]. Chi-Ho Tsang, Sam Kwong, Hanli Wang « Genetic-Fuzzy Rule Mining Approach and Evaluation of Feature Selection Techniques for Anomaly Intrusion Detection » Pattern Recognition, Vol. 40, №. 9, Sept. 2007, pp. 2373-2391.

[11]. Zadeh L.A. «Outline of a New Approach to the Analysis of Complex Systems and Decision Processes» IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-3, №. 1, January 1973, pp. 28-44.

[12]. Gómez J., González F., Dasgupta D. «An Immuno-Fuzzy Approach to Anomaly Detection» The 12th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 25-28 May 2003, pp. 1219-1224.

[13]. A Fuzzy Approach For Detecting Anomalous Behaviour in E-mail Traffic [Electronic resource] / Mark JynHuey Lim, Michael Negnevitsky, Jacky Hartnett // About Research Online @ ECU. – Electronic data. – Perth Western Australia] : Edith Cowan University, 2006. – Mode of access: World Wide Web. – URL: http://ro.ecu.edu.au/adf/29/. – Title from title screen. – Description based on home page (viewed on May 26, 2015).

[14]. 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.

[15]. 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.

[16]. 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.

[17]. 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.

[18]. Корченко А.А. Метод формирования лингвистических эталонов для систем выявления вторжений / А.А. Корченко // Захист інформації. – Т.16, №1. – 2014. – С. 5-12.

[19]. Корченко А.А. Метод фаззификации параметров на лингвистических эталонах для систем выявления кибератак / А.А. Корченко // Безпека інформації. – 2014. – № 1 (20). – С. 21-28.

[20]. Корченко А.А. Метод α-уровневой номинализации нечетких чисел для систем обнаружения вторжений / А.А. Корченко // Захист інформації. – Т.16, №4. – 2014. – С. 292-304.

[21]. Корченко А.А. Метод определения идентифицирующих термов для систем обнаружения вторжений / А.А. Корченко // Безпека інформації. – Т.20, № 3. – 2014. – С. 217-223.

[22]. Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84.

[23]. Корченко А.А. Система формирования нечетких эталонов сетевых параметров / А.А. Корченко // Захист інформації. – 2013. – Т.15, №3. – С. 240-246.

[24]. Корченко А.А. Система формирования эвристических правил для оценивания сетевой активности / А.А. Корченко // Захист інформації. – 2013. – №4. Т.15. – С. 353-359.

[25]. Корченко А.Г. Построение систем защиты информации на нечетких множествах [Текст] : Теория и практические решения / А.Г. Корченко. – К. : МК-Пресс, 2006. – 320 с.

[26]. Anna Korchenko, Kornel Warwas, Aleksandra Kłos-Witkowska. The Tupel Model of Basic Components' Set Formation for Cyberattacks // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – pp. 478-483.

REFERENCES

[1]. Korchenko A.A. The tupel model of basic components' set formation for cyberattacks, Legal, regulatory and metrological support information security system in Ukraine, 2014, V.2 (28), pp. 29-36.

[2]. Yao J.T., Zhao S.L., Saxton L.V. «A study on fuzzy intrusion detection» Proc. of SPIE Data Mining, Intrusion Detection, Information Assurance, And Data Networks Security, Orlando, Florida, USA, Vol. 5812, 2005, pp. 23-30.

[3]. Fries P. «A Fuzzy-Genetic Approach to Network Intrusion Detection Terrence» Genetic and Evolutionary Computation Conference, GECCO (Companion) July 12-16, 2008, pp. 2141-2146.

[4]. Wijayasekara D., Linda O., Manic M., Rieger C.G. Mining Building Energy Management System Data Using Fuzzy Anomaly Detection and Linguistic Descriptions. IEEE Trans. Industrial Informatics. Vol. 10, № 3, 2014, pp 1829-1840.

[5]. Shanmugavadivu R., Nagarajan N. «Network Intrusion Detection System Using Fuzzy Logic», Indian Journal of Computer Science and Engineering (IJCSE), Vol. 2, No. 1, pp. 101-111, 2011.

[6]. Linda O., Vollmer T., Wright J., Manic M. «Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor», in Proc. IEEE Symposium Series on Computational Intelligence, Paris, France, April, 2011, pp. 202-209.

[7]. Bridges S.M., Vaughn R.B. «Fuzzy data mining and genetic algorithms applied to intrusion detection». In: Proceedings of the 23rd National Information Systems Security Conference. October 2000, pp. 13-31.

[8]. Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha, Mat Kiah, Sanjay Misra «Anomaly Detection using Fuzzy Q-learning Algorithm» Acta Polytechnica Hungarica. Vol. 11, № 8, 2014, pp. 5-28.

[9]. John E. Dickerson, Jukka Juslin, Ourania Koukousoula, Julie A. Dickerson «Fuzzy Intrusion Detection» IFSA

World Congress and 20th NAFIPS International Conference, 2001. Joint 9th. Vol. 3, pp. 1506-1510.

[10]. Chi-Ho Tsang, Sam Kwong, Hanli Wang « Genetic-Fuzzy Rule Mining Approach and Evaluation of Feature Selection Techniques for Anomaly Intrusion Detection » Pattern Recognition, Vol. 40, №. 9, Sept. 2007, pp. 2373-2391.

[11]. Zadeh L.A. «Outline of a New Approach to the Analysis of Complex Systems and Decision Processes» IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-3, №. 1, January 1973, pp. 28-44.

[12]. Gómez J., González F., Dasgupta D. «An Immuno-Fuzzy Approach to Anomaly Detection» The 12th IEEE International Conference on Fuzzy Systems, FUZZ-IEEE 25-28 May 2003, pp. 1219-1224.

[13]. A Fuzzy Approach For Detecting Anomalous Behaviour in E-mail Traffic [Electronic resource] / Mark JynHuey Lim, Michael Negnevitsky, Jacky Hartnett // About Research Online @ ECU. – Electronic data. – Perth Western Australia] : Edith Cowan University, 2006. – Mode of access: World Wide Web. – URL: http://ro.ecu.edu.au/adf/29/. – Title from title screen. – Description based on home page (viewed on May 26, 2015).

[14]. Korchenko A.A. The model of heuristic rules on the set of logical-linguistic tangles for abnormality detection in computer systems, Zahist ìnformacìï, 2012, №4 (57), pp. 112-118.

[15]. Stasiuk A.I., Korchenko A.A. The basic model of parameters in attack detection (Identification) systems construction, Zahist ìnformacìï, 2012, №2 (55), pp. 47-51.

[16]. Lutskiy M.G., Korchenko A.A., Gavrylenko A.V., Okhrimenko A.A. The models of linguistic variables for attack detection systems, Zahist ìnformacìï, 2012, №2 (55), pp. 71-78.

[17]. Stasiuk A.I., Korchenko A.A. A method of abnormality detection caused by cyber attacks in computer networks, Zahist ìnformacìï, 2012, №4 (57), pp. 129-134.

[18]. Korchenko A.A. The formation method of linguistic standards created for the intrusion detection systems, Zahist ìnformacìï, T.16, №1, 2014, pp. 5-12.

[19]. Korchenko A.A. The method of parameter fuzzification based on linguistic standards for cyber attacks detection, Bezpeka ìnformacìï, T.20, №1, 2014, pp. 21-28.

[20]. Korchenko A.A. The method of α-level of nominalization for intrusion detection systems, Zahist ìnformacìï, T.16, №4, 2014, pp. 292-304.

[21]. Korchenko A.A. The detection method of identification terms for intrusion detection system, Bezpeka ìnformacìï, T.20, №3, 2014, pp. 217-223.

[22]. Korchenko A.A. Anomaly-based detection system in computer networks, Bezpeka ìnformacìï, 2012, №2 (18), pp. 80-84.

[23]. Korchenko A.A. The system development of fuzzy standards of network parameters, Zahist ìnformacìï, T.15, №3, 2013, pp. 240-246.

[24]. Korchenko A.A. The system of heuristic rules formation for network activity assessment, Zahist ìnformacìï, T.15, №4, 2013, pp. 353-359.

[25]. Korchenko A.G. The development of information protection systems based on the fuzzy sets, The theory and practical solutions, Kuev, 2006, 320 p.

[26]. Anna Korchenko, Kornel Warwas, Aleksandra Kłos-Witkowska. The Tupel Model of Basic Components' Set Formation for Cyberattacks // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015), Warsaw, Poland, September 24-26, 2015: Vol. 1. – pp. 478-483.

МЕТОД ФОРМУВАННЯ БАЗОВИХ ДЕТЕКЦІЙНИХ ПРАВИЛ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Внаслідок інтенсивного розвитку цифрового бізнесу, шкідливе програмне забезпечення та інші кіберзагрози стають все більш поширеними. Для підвищення рівня безпеки необхідні відповідні спеціальні засоби протидії, які здатні залишатися ефективними при появі нових видів загроз і дозволяють в нечітких умовах виявити кібератаки орієнтовані на множини ресурсів інформаційних систем. Різні атакуючі впливи на відповідні ресурси породжують різні множини аномалій в гетерогенному параметричному середовищі оточення. Відома кортежна модель формування набору базових компонент, що дозволяють виявити кібератаки. Для її ефективного застосування необхідна формальна реалізація підходу до формування наборів базових детекційних правил. З цією метою розроблено метод, орієнтований на вирішення задач виявлення кібератак в комп'ютерних системах, який реалізується за допомогою трьох базових етапів: формування підмножин ідентифікаторів аномальності; формування вирішальних функцій; формування умовних детекційних виразів. За допомогою такого методу можна сформувати необхідну множину детекційних правил, за якими визначається рівень аномального стану величин в гетерогенному параметричному середовищі оточення, характерний для впливу певного типу атак. Використання даного методу при побудові систем виявлення вторгнень дозволить розширити їх функціональні можливості, щодо виявлення кібератак в слабоформалізованому нечіткому середовищі оточення.

Ключові слова: детекційні правила, атаки, кібератаки, аномалії, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак.

THE METHOD OF DEVELOPMENTOF BASIC DETECTION RULES FOR INTRUSION DETECTION SYSTEMS

Due to the intensive development of digital business, malicious software and other cyber threats become more and more common. To increase the security level there is a need of relevant special control, which can remain effective when new types of threats are appeared and allows to detect the cyber attacks in fuzzy conditions targeting on many different resources of information systems. The various attacking effects on appropriate resources, generate different sets of anomalies in the heterogeneous parametric environment. It is also known the tuple model of set formation of basic components allowing us to detect cyber attacks. For its effective use it is required a formal approach implementation towards the sets formation of basic detection rules. With this objective the method focused on cyber attacks detection in computer systems was developed. This method is realized through three basic stages: formation of subsets of the anomalous IDs; the formation of critical functions; formation of a conditional detection expression. Using this method, it is possible to generate the necessary set of detection rules that determine the level of abnormal condition of values in the heterogeneous parametric environment. The implementation of this method in building intrusion detection systems will expand their functionality with respect to the cyber attacks detection in the weakly-formalized fuzzy environment.

Keywords: detection rules, attacks, cyber attacks, anomalies, intrusion detection systems, anomaly detection systems, intrusion detection systems.

Карпинский Николай Петрович, доктор технических наук, профессор, заведующий кафедрой информатики и автоматики Университет в Бельско-Бялой (г. Бельско-Бяла, Польша).
E-mail: mpkarpinski@gmail.com.

Карпінський Микола Петрович, доктор технічних наук, професор, завідувач кафедри інформатики та автоматики Університет у Бєльсько-Бялій (м. Бєльсько-Бяла, Польща).

Karpinski Mikolaj, Dr.Sc., Professor, Chairman of Department of Computer Science and Automatics University of Bielsko-Biala (Bielsko-Biala, Poland).

Корченко Анна Александровна, кандидат технических наук, доцент, доцент кафедры безопасности информационных технологий Национального авиационного университета.
E-mail: annakor@ukr.net

Корченко Анна Олександрівна, кандидат технічних наук, доцент, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.

Korchenko Anna, PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

Ахметова Санзира Тынымбаевна, научный сотрудник Казахского национального исследовательского технического университета им. К.И. Сатпаева (Алматы, Казахстан).
E-mail: sanzira52@mail.ru

Ахметова Санзіра Тинимбаєвна, науковий співробітник Казахського національного дослідницького технічного університету ім. К.І. Сатпаева (Алмати, Казахстан).

Akhmetova Sanzira, researcher, Kazakh National Research Technical University after K.I. Satpayev (Almaty, Republic of Kazakhstan).