© Korchenko A. The detection method of identification terms for intrusion detection system // Ukrainian Scientific Journal of Information Security, 2014, vol. 20, issue 3, p. 217-223.

МЕТОД ОПРЕДЕЛЕНИЯ ИДЕНТИФИЦИРУЮЩИХ ТЕРМОВ ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Анна Корченко

Национальный авиационный университет, Украина

КОРЧЕНКО Анна Александровна, к.т.н.

Год и место рождения: 1985 год, г. Киев, Украина.
Образование: Национальный авиационный университет, 2007 год.
Должность: доцент кафедры безопасности информационных технологий.
Научные интересы: информационная безопасность, системы обнаружения вторжений, экспертное оценивание в сфере защиты информации.
Публикации: больше 40 научных публикаций, среди которых научные статьи, учебники и учебно-методические пособия.
E-mail: annakor@ukr.net

Аннотация. *Компьютерные системы все больше подвергаются воздействиям угроз, новые виды которых порождают новые кибератаки на их ресурсы. Для повышения уровня безопасности разработаны системы выявления аномального состояния в компьютерных сетях, формирования нечетких эталонов сетевых параметров и эвристических правил для оценивания сетевой активности. В основу этих систем заложен метод выявления аномалий, порожденных кибератаками. В этом методе процесс определения идентифицирующих термов не сопровождается достаточным для его эффективного использования уровнем формализации. С целью исключения этого недостатка разработан метод определения идентифицирующих термов, который базируется на математических моделях и методах нечеткой логики. Метод реализуется посредством трех базовых этапов: формирование множества признаков; определение подмножеств признаков; определение номера идентифицирующего терма. С его помощью осуществляется поиск в заданной линевистической переменной идентифицирующего эталонного терма, на основе которого с помощью эвристических правил можно определить уровень аномального состояния, характерного для определенного типа кибератак. Это позволит повысить эффективность построения соответствующих систем обнаружения вторжений.*

Ключевые слова: *кибератаки, аномалии, нечеткие эталоны, идентифицирующие термы, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, обнаружение аномалий в компьютерных сетях.*

Актуальность

Использование систем обнаружения вторжений непосредственно связано со стремительным развитием киберпространства, в котором появляются новые виды угроз информационным ресурсам. Расширение воздействий кибератак направленных на различные ресурсы информационных систем инициирует создание таких средств противодействия, которые способны оставаться эффективными при появлении новых видов угроз с неустановленными или нечетко определенными свойствами и фактически функционировать в слабоформализованной нечеткой среде окружения. Использование методов и моделей, основанных на нечетких множествах для построения средств обнаружения аномалий позволит усовершенствовать существующие системы выявления вторжений и, таким образом, эффективно решать задачи идентификации опасных аномальных состояний в компьютерных системах и сетях. В этой связи, разработка соответствующих технических решений функционирующих в нечетких условиях и позволяющих выявлять новые и модифицированные типы кибератак, является актуальной научной задачей.

Анализ существующих исследований

Известен ряд таких технических решений, как системы выявления аномального состояния в компьютерных сетях [1], формирования нечетких эталонов сетевых параметров [2] и формирования эвристических правил для оценивания сетевой активности [3]. В основу функционирования указанных систем заложен метод выявления аномалий порожденных кибератаками [4], в котором процесс определения идентифицирующих термов требует четкой формализации. Для эффективного

применения этого метода [4] необходима формальная реализация этого процесса, что позволит осуществить поиск в заданной лингвистической переменной идентифицирующий эталонный терм, по которому с помощью эвристических правил можно определить уровень аномального состояния, характерного для определенного типа атак.

Основная цель исследования

Исходя из анализа существующих исследований и актуальности поставленной задачи целью данной работы является разработка метода определения идентифицирующих термов (МОИТ) для систем обнаружения вторжений. С помощью такого метода (при решении задач выявления кибератак) можно определять в множествах эталонных лингвистических переменных такие термы, посредством которых, например, с помощью эвристических правил можно определить уровень аномального состояния, характерного определенному типу атак для конкретной среды окружения.

Основная часть исследования

Для достижения поставленной цели предлагается метод, базовый механизм которого основывается на трех этапах: формирование множества признаков; определение подмножеств признаков; определение номера идентифицирующего терма.

Этап 1 – формирование множества признаков. Для реализации этого этапа введем $\mathbf{XP_{ij}}$ – множество всех возможных характерных признаков (ХП) методов сравнения функций принадлежности (МСФП) и d подмножеств таких признаков $\mathbf{XP_{ij}^c} \subseteq \mathbf{XP_{ij}}$ $(c = \overline{1,d})$,

$$\mathbf{XP_{ij}} = \{\bigcup_{c=1}^{\mathbf{d}} \mathbf{XP_{ij}^c}\} = \{\mathbf{XP_{ij}^1}, \mathbf{XP_{ij}^2}, ..., \mathbf{XP_{ij}^d}\}, \quad (1)$$

где каждый член множества $\mathbf{XP_{ij}}$ отображает возможные ХП, сформированные посредством множества МСФП, т.е.:

$$\mathbf{МСФП} = \{\bigcup_{c=1}^{d} МСФП_c\} = \{МСФП_1, МСФП_2, ..., МСФП_d\}, (c = \overline{1,d}), \quad (2)$$

где d – количество используемых МСФП. Другими словами можно сказать, что содержимое каждого подмножества $\mathbf{XP_{ij}^c}$ формируется посредством соответствующего $МСФП_c$, $(c = \overline{1,d})$.

Например, при $d = 8$ множество $\mathbf{XP_{ij}}$ согласно (1) принимает вид

$$\mathbf{XP_{ij}} = \{\bigcup_{c=1}^{\mathbf{8}} \mathbf{XP_{ij}^c}\} = \{\mathbf{XP_{ij}^1}, \mathbf{XP_{ij}^2}, \mathbf{XP_{ij}^3}, \mathbf{XP_{ij}^4}, \mathbf{XP_{ij}^5}, \mathbf{XP_{ij}^6}, \mathbf{XP_{ij}^7}, \mathbf{XP_{ij}^8}\}, (c = \overline{1,8}),$$

каждый член которого отображает все возможные ХП, сформированные посредством множества (2) состоящего с известных МСФП [5], используемых в методе выявления аномалий порожденных кибератаками (см. этап. 1 в [4]). При заданном значении d множество **МСФП** имеет вид:

$$\mathbf{МСФП} = \{\bigcup_{c=1}^{8} МСФП_c\} = \{МСФП_1, МСФП_2, МСФП_3, МСФП_4, МСФП_5, МСФП_6, МСФП_7,$$
$$МСФП_8\} = \{РХ, АУР, ЦТ, ММ, БР, ФУП, УНЧ, УБО\},$$

где каждый член $\mathbf{XP_{ij}^c}$ формируется посредством соответствующего $МСФП_c$, $(c = \overline{1,8})$, т.е. $\mathbf{XP_{ij}^1}$ формируется с помощью обобщенного расстояния Хэмминга (РХ) ($МСФП_1$=РХ), $\mathbf{XP_{ij}^2}$ – с помощью α-уровневого расстояния ($МСФП_2$=АУР), а $\mathbf{XP_{ij}^3}$, $\mathbf{XP_{ij}^4}$, $\mathbf{XP_{ij}^5}$, $\mathbf{XP_{ij}^6}$, $\mathbf{XP_{ij}^7}$ и $\mathbf{XP_{ij}^8}$ соответственно формируются посредством методов центра тяжести, максминного, обобщенных операций «больше или равняется», функции упорядочивания нечетких подмножеств единичного интервала, упорядочения нечетких чисел (НЧ), которое характеризует непринятие риска, упорядочения на базе отношений т.е.: $МСФП_3$=ЦТ, $МСФП_4$=ММ, $МСФП_5$=БР, $МСФП_6$=ФУП, $МСФП_7$=УНЧ и $МСФП_8$=УБО. Эти методы чаще всего применяются в теории и практике сравнения нечетких множеств (см. этап. 1 в [4]).

Этап 2 – определение подмножеств признаков. Этот этап реализуется с помощью методов, принадлежащих множеству **МСФП**, посредством которых формируются ХП, т.е. члены подмножеств $\mathbf{XP_{ij}^c} \subseteq \mathbf{XP_{ij}}$:

$$\mathbf{XP_{ij}^c} = \{\bigcup_{s=1}^{r} XP_{ijs}^c\} = \{XP_{ij1}^c, XP_{ij2}^c, ..., XP_{ijr}^c\}, (s = \overline{1,r}). \quad (3)$$

Другими словами можно сказать, что каждый член XP^{c}_{ijs} $(s=\overline{1,r})$ подмножества $\mathbf{XP^{c}_{ij}}$ формируется с помощью $МСФП_{c}$, где по значению c определяется номер способа реализации этапа 1.

Например, при $c=1$ члены множества $\mathbf{XP^{1}_{ij}}$ формируются первым способом.

Способ 1. Используем МСФП$_1$=РХ из множества **МСФП**, т.е.

$$XP^{1}_{ijs}=h\left(\underset{\sim}{T}^{ep}_{ijs},\ \underset{\sim}{P}^{p}_{ij}\right)=\sum_{g=1}^{z}\left|x^{ep}_{ijsg}-x^{p}_{ijg}\right|=|\ x^{ep}_{ijs1}-x^{p}_{ij1}\ |+|\ x^{ep}_{ijs2}-x^{p}_{ij2}\ |+\ldots+|\ x^{ep}_{ijsg}-x^{p}_{ijg}\ |+\ldots+$$
$$|\ x^{ep}_{ijsz}-x^{p}_{ijz}\ |,\ (g=\overline{1,z}),\ (z=2\pi-1),\ (s=\overline{1,r}), \quad (4)$$

где x^{ep}_{ijsg} и x^{p}_{ijg} – соответственно суппорты (носители) преобразованного эталонного $\underset{\sim}{T}^{ep}_{ijs}$ и текущего $\underset{\sim}{P}^{p}_{ij}$ НЧ, z – количество компонент в $\underset{\sim}{T}^{ep}_{ijs}$ и $\underset{\sim}{P}^{p}_{ij}$ (см. (5) и (6) в [6]).

Рассмотрим пример реализации первым способом этапа 2 для $i=3$ ($\mathbf{AT_i}=\mathbf{AT_3}=\mathbf{AT_{SP}}$) при $j=3$ ($\mathbf{P_{ij}}=\mathbf{P_{33}}=\mathbf{P_{SPKOП}}$), $r=5$, $g=\overline{1,13}$, $\underset{\sim}{T}^{ep}_{ijs}=\underset{\sim}{T}^{ep}_{33s}$, $\underset{\sim}{P}^{p}_{ij}=\underset{\sim}{P}^{p}_{33}=\underset{\sim}{P}^{p}_{SPKOП}$ и при $j=6$ ($\mathbf{P_{ij}}=\mathbf{P_{36}}=\mathbf{P_{SPKПОА}}$), $r=3$, $g=\overline{1,9}$, $\underset{\sim}{T}^{ep}_{ijs}=\underset{\sim}{T}^{ep}_{36s}$, $\underset{\sim}{P}^{p}_{ij}=\underset{\sim}{P}^{p}_{36}=\underset{\sim}{P}^{p}_{SPKПОА}$ (т.е. AT_3=*SP* – «Спуфинг», P_3=*КОП* – «Количество одновременных подключений к серверу», P_6=*КПОА* – «Количество пакетов с одинаковым адресом отправителя и получателя» (см. [7] и пример использования (5), (6) в [6])). Подмножество всех возможных расстояний $\mathbf{XP^{1}_{ij}}=\mathbf{XP^{1}_{33}}$ и $\mathbf{XP^{1}_{ij}}=\mathbf{XP^{1}_{36}}$ (см. (3)) вычислим посредством (4) т.е.:

$$\mathbf{XP^{1}_{33}}=\{\bigcup_{s=1}^{5}XP^{1}_{33s}\}=\{XP^{1}_{331},\ XP^{1}_{332},\ XP^{1}_{333},\ XP^{1}_{334},\ XP^{1}_{335}\}=\{h\left(\underset{\sim}{T}^{ep}_{331},\ \underset{\sim}{P}^{p}_{33}\right),\ h\left(\underset{\sim}{T}^{ep}_{332},\ \underset{\sim}{P}^{p}_{33}\right),\ h\left(\underset{\sim}{T}^{ep}_{333},\ \underset{\sim}{P}^{p}_{33}\right),\ h\left(\underset{\sim}{T}^{ep}_{334},\ \underset{\sim}{P}^{p}_{33}\right),\ h\left(\underset{\sim}{T}^{ep}_{335},\ \underset{\sim}{P}^{p}_{33}\right)\}=\{($$
$$\left|x^{ep}_{3311}-x^{p}_{331}\right|+\left|x^{ep}_{3312}-x^{p}_{332}\right|+\left|x^{ep}_{3313}-x^{p}_{333}\right|+\left|x^{ep}_{3314}-x^{p}_{334}\right|+\left|x^{ep}_{3315}-x^{p}_{335}\right|+\left|x^{ep}_{3316}-x^{p}_{336}\right|+\left|x^{ep}_{3317}-x^{p}_{337}\right|+\left|x^{ep}_{3318}-x^{p}_{338}\right|+\left|x^{ep}_{3319}-x^{p}_{339}\right|+\left|x^{ep}_{331(10)}-x^{p}_{33(10)}\right|+\left|x^{ep}_{331(11)}-x^{p}_{33(11)}\right|+\left|x^{ep}_{331(12)}-x^{p}_{33(12)}\right|+\left|x^{ep}_{331(13)}-x^{p}_{33(13)}\right|),\quad($$
$$\left|x^{ep}_{3321}-x^{p}_{331}\right|+\left|x^{ep}_{3322}-x^{p}_{332}\right|+\left|x^{ep}_{3323}-x^{p}_{333}\right|+\left|x^{ep}_{3324}-x^{p}_{334}\right|+\left|x^{ep}_{3325}-x^{p}_{335}\right|+\left|x^{ep}_{3326}-x^{p}_{336}\right|+\left|x^{ep}_{3327}-x^{p}_{337}\right|+\left|x^{ep}_{3328}-x^{p}_{338}\right|+\left|x^{ep}_{3329}-x^{p}_{339}\right|+\left|x^{ep}_{332(10)}-x^{p}_{33(10)}\right|+\left|x^{ep}_{332(11)}-x^{p}_{33(11)}\right|+\left|x^{ep}_{332(12)}-x^{p}_{33(12)}\right|+\left|x^{ep}_{332(13)}-x^{p}_{33(13)}\right|),\quad($$
$$\left|x^{ep}_{3331}-x^{p}_{331}\right|+\left|x^{ep}_{3332}-x^{p}_{332}\right|+\left|x^{ep}_{3333}-x^{p}_{333}\right|+\left|x^{ep}_{3334}-x^{p}_{334}\right|+\left|x^{ep}_{3335}-x^{p}_{335}\right|+\left|x^{ep}_{3336}-x^{p}_{336}\right|+\left|x^{ep}_{3337}-x^{p}_{337}\right|+\left|x^{ep}_{3338}-x^{p}_{338}\right|+\left|x^{ep}_{3339}-x^{p}_{339}\right|+\left|x^{ep}_{333(10)}-x^{p}_{33(10)}\right|+\left|x^{ep}_{333(11)}-x^{p}_{33(11)}\right|+\left|x^{ep}_{333(12)}-x^{p}_{33(12)}\right|+\left|x^{ep}_{333(13)}-x^{p}_{33(13)}\right|),$$
$$($$
$$\left|x^{ep}_{3341}-x^{p}_{331}\right|+\left|x^{ep}_{3342}-x^{p}_{332}\right|+\left|x^{ep}_{3343}-x^{p}_{333}\right|+\left|x^{ep}_{3344}-x^{p}_{334}\right|+\left|x^{ep}_{3345}-x^{p}_{335}\right|+\left|x^{ep}_{3346}-x^{p}_{336}\right|+\left|x^{ep}_{3347}-x^{p}_{337}\right|+\left|x^{ep}_{3348}-x^{p}_{338}\right|+\left|x^{ep}_{3349}-x^{p}_{339}\right|+\left|x^{ep}_{334(10)}-x^{p}_{33(10)}\right|+\left|x^{ep}_{334(11)}-x^{p}_{33(11)}\right|+\left|x^{ep}_{334(12)}-x^{p}_{33(12)}\right|+\left|x^{ep}_{334(13)}-x^{p}_{33(13)}\right|),\ ($$
$$\left|x^{ep}_{3351}-x^{p}_{331}\right|+\left|x^{ep}_{3352}-x^{p}_{332}\right|+\left|x^{ep}_{3353}-x^{p}_{333}\right|+\left|x^{ep}_{3354}-x^{p}_{334}\right|+\left|x^{ep}_{3355}-x^{p}_{335}\right|+\left|x^{ep}_{3356}-x^{p}_{336}\right|+\left|x^{ep}_{3357}-x^{p}_{337}\right|+\left|x^{ep}_{3358}-x^{p}_{338}\right|+\left|x^{ep}_{3359}-x^{p}_{339}\right|+\left|x^{ep}_{335(10)}-x^{p}_{33(10)}\right|+\left|x^{ep}_{335(11)}-x^{p}_{33(11)}\right|+\left|x^{ep}_{335(12)}-x^{p}_{33(12)}\right|+\left|x^{ep}_{335(13)}-x^{p}_{33(13)}\right|)\}=\{($$
$$|0{,}008–0{,}095|+|0{,}008–0{,}095|+|0{,}008–0{,}095|+|0{,}008–0{,}095|+|0{,}008–0{,}157|+|0{,}008–0{,}188|+|0{,}008–0{,}28|+|0{,}032–0{,}393|+|0{,}039–0{,}43|+|0{,}055–0{,}505|+|0{,}063–0{,}543|+|0{,}125–0{,}58|+|0{,}25–0{,}58|),$$
$$(0{,}008–0{,}095|+|0{,}008–0{,}095|+|0{,}008–0{,}095|+|0{,}008–0{,}095|+|0{,}008–0{,}157|+|0{,}022–0{,}188|+|0{,}063–0{,}28|+|0{,}133–0{,}393|+|0{,}157–0{,}43|+|0{,}203–0{,}505|+|0{,}227–0{,}543|+|0{,}25–0{,}58|+|0{,}5–0{,}58|),$$
$$(0{,}008–0{,}095|+|0{,}036–0{,}095|+|0{,}049–0{,}095|+|0{,}063–0{,}095|+|0{,}125–0{,}157|+|0{,}157–0{,}188|+|0{,}25–0{,}28|+|0{,}357–0{,}393|+|0{,}393–0{,}43|+|0{,}464–0{,}505|+|0{,}5–0{,}543|+|0{,}667–0{,}58|+|1–0{,}58|),$$
$$(0{,}063–0{,}095|+|0{,}125–0{,}095|+|0{,}157–0{,}095|+|0{,}188–0{,}095|+|0{,}25–0{,}157|+|0{,}313–0{,}188|+|0{,}5–0{,}28|+|1–0{,}393|+|1–0{,}43|+|1–0{,}505|+|1–0{,}543|+|1–0{,}58|+|1–0{,}58|),$$
$$(0{,}25–0{,}095|+|0{,}333–0{,}095|+|0{,}375–0{,}095|+|0{,}417–0{,}095|+|0{,}5–0{,}157|+|0{,}625–0{,}188|+|1–0{,}28|+|1–0{,}393|+|1–0{,}43|+|1–0{,}505|+|1–0{,}543|+|1–0{,}58|+|1–0{,}58|)\}=$$
$$(0{,}087+0{,}087+0{,}087+0{,}087+0{,}149+0{,}18+0{,}272+0{,}361+0{,}391+0{,}45+0{,}48+0{,}455+0{,}033),$$
$$(0{,}087+0{,}087+0{,}087+0{,}087+0{,}149+0{,}166+0{,}217+0{,}26+0{,}273+0{,}302+0{,}316+0{,}33+0{,}08),$$
$$(0{,}087+0{,}059+0{,}046+0{,}032+0{,}032+0{,}031+0{,}03+0{,}036+0{,}039+0{,}041+0{,}043+0{,}087+0{,}42),$$
$$(0{,}032+0{,}03+0{,}062+0{,}093+0{,}093+0{,}125+0{,}22+0{,}607+0{,}57+0{,}495+0{,}457+0{,}42+0{,}42),$$
$$(0{,}155+0{,}238+0{,}28+0{,}322+0{,}343+0{,}437+0{,}72+0{,}607+0{,}57+0{,}495+0{,}457+0{,}42+0{,}42)=\{3{,}119;\ 2{,}441;\ 1{,}371;\ 3{,}624;\ 5{,}464\}$$

и

$$\mathbf{XP^1_{36}}=\{\bigcup_{s=1}^{3} XP^1_{36\,s}\}=\{\,XP^1_{361},\ XP^1_{362},\ XP^1_{363}\}=\{\,h\,(\underset{\sim}{T}^{ep}_{361},\ \underset{\sim}{P}^{p}_{36}),\ h\,(\underset{\sim}{T}^{ep}_{362},\ \underset{\sim}{P}^{p}_{36}),\ h\,(\underset{\sim}{T}^{ep}_{363},\ \underset{\sim}{P}^{p}_{36})\}=\{($$
$$\left|x^{ep}_{3611}-x^{p}_{361}\right|+\left|x^{ep}_{3612}-x^{p}_{362}\right|+\left|x^{ep}_{3613}-x^{p}_{363}\right|+\left|x^{ep}_{3614}-x^{p}_{364}\right|+\left|x^{ep}_{3615}-x^{p}_{365}\right|+\left|x^{ep}_{3616}-x^{p}_{366}\right|+\left|x^{ep}_{3617}-x^{p}_{367}\right|+\left|x^{ep}_{3618}-x^{p}_{368}\right|$$
$$+\left|x^{ep}_{3619}-x^{p}_{369}\right|),\ (\ \left|x^{ep}_{3621}-x^{p}_{361}\right|+\left|x^{ep}_{3622}-x^{p}_{362}\right|+\left|x^{ep}_{3623}-x^{p}_{363}\right|+\left|x^{ep}_{3624}-x^{p}_{364}\right|+\left|x^{ep}_{3625}-x^{p}_{365}\right|+\left|x^{ep}_{3626}-x^{p}_{366}\right|+\left|x^{ep}_{3627}-x^{p}_{367}\right|$$
$$+\left|x^{ep}_{3628}-x^{p}_{368}\right|+\left|x^{ep}_{3629}-x^{p}_{369}\right|),\ (\ \left|x^{ep}_{3631}-x^{p}_{361}\right|+\left|x^{ep}_{3632}-x^{p}_{362}\right|+\left|x^{ep}_{3633}-x^{p}_{363}\right|+\left|x^{ep}_{3634}-x^{p}_{364}\right|+\left|x^{ep}_{3635}-x^{p}_{365}\right|+\left|x^{ep}_{3636}-x^{p}_{366}\right|+$$
$$\left|x^{ep}_{3637}-x^{p}_{367}\right|+\left|x^{ep}_{3638}-x^{p}_{368}\right|+\left|x^{ep}_{3639}-x^{p}_{369}\right|\ )\}=\{(\ 0{,}01–0{,}082\,|+|\,0{,}01–0{,}082\,|+|\,0{,}01–0{,}082\,|+|\,0{,}01–0{,}377\,|+|\,0{,}1–$$
$$0{,}82\,|+|\,0{,}044–1\,|+|\,0{,}066–1\,|+|\,0{,}1–1\,|+|\,1–1\,|),\quad (|\,0{,}01–0{,}082\,|+|\,0{,}01–0{,}082\,|+|\,0{,}01–0{,}082\,|+|\,0{,}046–0{,}377\,|+|\,0{,}1–$$
$$0{,}82\,|+|\,1–1\,|+|\,1–1\,|+|\,1–1\,|+|\,1–1\,|),\quad (|\,0{,}01–0{,}082\,|+|\,0{,}046–0{,}082\,|+|\,0{,}01–0{,}082\,|+|\,0{,}46–0{,}377\,|+|\,1–0{,}82\,|+|\,1–1\,|+|\,1–$$
$$1\,|+|\,1–1\,|+|\,1–1\,|\ )\}=\{(\ 0{,}072+0{,}072+0{,}072+0{,}367+0{,}72+0{,}956+0{,}934+0{,}9+0),\quad (0{,}072+0{,}072+0{,}072+0{,}331+0{,}72+0+0+0+0),$$
$$(0{,}072+0{,}036+0{,}072+0{,}083+0{,}18+0+0+0+0\ )\}=\{\ 4{,}093;\ 1{,}267;\ 0{,}443\ \}.$$

Таким образом:

$$\mathbf{XP^1_{33}}=\{\ 3{,}119;\ 2{,}441;\ 1{,}371;\ 3{,}624;\ 5{,}464\ \}\ \text{и}\ \mathbf{XP^1_{36}}=\{\ 4{,}093;\ 1{,}267;\ 0{,}443\ \}. \tag{5}$$

Этап 3 – определение номера идентифицирующего терма. Реализация этого этапа осуществляется с помощью функции поиска идентифицирующего ХП и его номера, т.е. такого идентифицирующего признака $IX^{\,c}_{ijnum}$, которому согласно соответствующей функции (тип которой определяется по значению переменной c) будет присвоено одно из значений XP^c_{ijs} $(s=\overline{1,r})$. Очевидно, что при этом $num=s$. Фактически по номеру (текущему значению s) идентифицирующего ХП в (3) можно определить соответствующий идентифицирующий терм в подмножестве $\mathbf{T^e_{ij}}$ (см. (12) в [8]). Таким образом, поиск $IX^{\,c}_{ijnum}=XP^c_{ijs}$ осуществляется посредством согласующей с МСФП функции $F^c\,(\mathbf{XP^c_{ij}})$, т.е.:

$$IX^{\,c}_{ijnum}=F^c(\bigcup_{s=1}^{r} XP^c_{ijs})=F^c_{ij}\,(\,XP^c_{ij1},\ XP^c_{ij2},\ ...,\ XP^c_{ijr}\,),\ (s=\overline{1,r}), \tag{6}$$

где по значению переменной c определяется номер способа реализации этапа 3, который также связан с номером способа, посредством которого реализуется этап 2. Например, при $c=1$ осуществляется первый способ поиска номера идентифицирующего терма, который связан с МСФП$_1$=РХ и состоит из следующих шагов.

Способ 1. Шаг 1. Определение $IX^{\,1}_{ijnum}$ осуществляется посредством согласующей с РХ функции $F^1\,(\mathbf{XP^1_{ij}})$, выполняющей поиск минимального значения из членов подмножества $\mathbf{XP^c_{ij}}$ согласно следующего выражения:

$$IX^{\,1}_{ijnum}=F^1(\bigcup_{s=1}^{r} XP^1_{ijs})=F^1_{ij}\,(\,XP^1_{ij1},\ XP^1_{ij2},\ ...,\ XP^1_{ijr}\,)\ \text{или}$$
$$IX^{\,1}_{ijnum}=\bigwedge_{s=1}^{r} XP^1_{ijs}=XP^1_{ij1}\wedge XP^1_{ij2}\wedge\ ...\ \wedge XP^1_{ijr},\ (s=\overline{1,r}). \tag{7}$$

Шаг 2. Определение идентифицирующего терма в $\mathbf{T^e_{ij}}$ (см. (12) в [8]) осуществляется на основе того, что $IX^{\,1}_{ijnum}=XP^1_{ijs}$, а значение num будет соответствовать s. Согласно этого, в подмножестве $\mathbf{T^e_{ij}}$ находится терм, у которого значение $s=num$ и принимаем его в качестве идентифицирующего.

Рассмотрим пример реализации этапа 3 первым способом для $i=3$ ($\mathbf{AT_i}=\mathbf{AT_3}=\mathbf{AT_{SP}}$) при $j=3$ ($\mathbf{P_{ij}}=\mathbf{P_{33}}=\mathbf{P_{SPKOП}}$), $r=5$, $XP^1_{ijs}=XP^1_{33s}$ и при $j=6$ ($\mathbf{P_{ij}}=\mathbf{P_{36}}=\mathbf{P_{SPKПОА}}$), $r=3$, $XP^1_{ijs}=XP^1_{36\,s}$ (см. (3)).

Способ 1. Шаг 1. Определение $IX^{\,1}_{33num}$ и $IX^{\,1}_{36\,num}$ осуществляется посредством функции $F^1\,(\mathbf{XP^1_{33}})$ и $F^1\,(\mathbf{XP^1_{36}})$, выполняющей поиск минимального значения из членов подмножества $\mathbf{XP^1_{33}}$ и $\mathbf{XP^1_{36}}$ (см. (8)) согласно (6), (7) т.е.: $IX^{\,1}_{33num}=\bigwedge_{s=1}^{5} XP^1_{33s}=XP^1_{331}\wedge XP^1_{332}\wedge XP^1_{333}\wedge XP^1_{334}\wedge XP^1_{335}=3{,}119\wedge 2{,}441\wedge 1{,}371\wedge 3{,}624\wedge 5{,}464=XP^1_{333}=1{,}371$ и $IX^{\,1}_{36\,num}=\bigwedge_{s=1}^{3} XP^1_{36\,s}=XP^1_{361}\wedge XP^1_{362}\wedge XP^1_{363}=4{,}093\wedge 1{,}267\wedge 0{,}443=XP^1_{363}=0{,}443$.

Шаг 2. Определение идентифицирующего терма в $\mathbf{T}^{\mathbf{e}}_{\mathbf{33}}$ осуществляется на основе того, что $IX^{1}_{33num} = XP^{1}_{33s} = XP^{1}_{333}$, а $num = s = 3$. Исходя из этого идентифицирующим будет терм $\underset{\sim}{T}^{e}_{333}$ (см. пример (12) в [8]), у которого значение $s = 3$, что соответствует номеру минимального значения идентифицирующего ХП.

Аналогичное значение определяется в $\mathbf{T}^{\mathbf{e}}_{\mathbf{36}}$ на основе того, что $IX^{1}_{36num} = XP^{1}_{36s} = XP^{1}_{363}$ и $num = s = 3$. Следовательно, идентифицирующим будет терм $\underset{\sim}{T}^{e}_{363}$ (см. пример (12) в [8]).

Исходя из вычислений видно, что идентифицирующим в $\mathbf{T}^{\mathbf{e}}_{\mathbf{33}}$ будет терм $\underset{\sim}{T}^{e}_{333} = \underset{\sim}{C}^{e}_{33}$ (см. пример (12) в [8]), а соответствующее ему преобразованное эталонное $\underset{\sim}{T}^{ep}_{333} = \underset{\sim}{T}^{ep}_{SPKOП3} = \underset{\sim}{C}^{ep}_{33}$ (см. пример (4) этапа 2 в [6]). Фактически вычисления показывают, что XP^{1}_{333}=1,371, следовательно преобразованное текущее НЧ $\underset{\sim}{P}^{p}_{33} = \underset{\sim}{P}^{p}_{SPKOП}$ наиболее близко расположено к преобразованному эталонному $\underset{\sim}{T}^{ep}_{333} = \underset{\sim}{C}^{ep}_{33}$. А поскольку $\underset{\sim}{P}^{p}_{SPKOП}$ и $\underset{\sim}{C}^{ep}_{33}$ есть отображением $\underset{\sim}{P}_{SPKOП}$ и $\underset{\sim}{C}^{e}_{33}$, то $\underset{\sim}{P}_{SPKOП}$ наиболее ближе расположен к эталонному $\underset{\sim}{C}^{e}_{33}$.

Аналогично идентифицирующим в $\mathbf{T}^{\mathbf{e}}_{\mathbf{36}}$ является значение $\underset{\sim}{T}^{e}_{363} = \underset{\sim}{Б}^{e}_{36}$ (см. пример (12) в [8]) и при этом $\underset{\sim}{T}^{ep}_{363} = \underset{\sim}{T}^{ep}_{SPKПОА3} = \underset{\sim}{Б}^{ep}_{36}$ (см. пример (4) этапа 2 в [6]). Также учитывая, что XP^{1}_{363}=0,443, то преобразованное текущее НЧ $\underset{\sim}{P}^{p}_{36} = \underset{\sim}{P}^{p}_{SPKПОА}$ наиболее близко к преобразованному эталонному $\underset{\sim}{T}^{ep}_{363} = \underset{\sim}{Б}^{ep}_{36}$. И следовательно, если $\underset{\sim}{P}^{p}_{SPKПОА}$ и $\underset{\sim}{Б}^{ep}_{36}$ являются отображением $\underset{\sim}{P}_{SPKПОА}$ и $\underset{\sim}{Б}^{e}_{36}$, то $\underset{\sim}{P}_{SPKПОА}$ есть наиболее близким к $\underset{\sim}{Б}^{e}_{36}$.

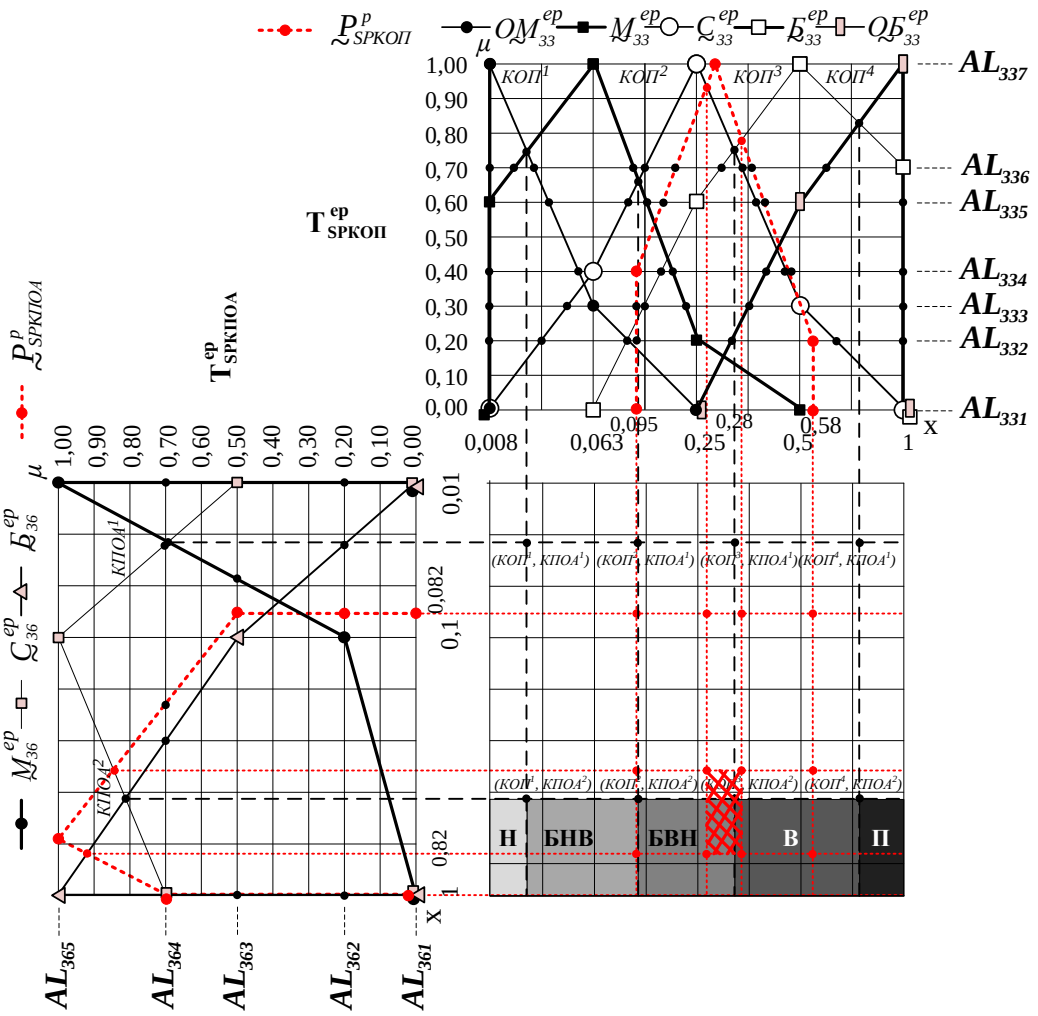

Рис. 1. Графическая интерпретация нечеткого текущего блока, посредством которого определяется уровень аномального состояния порожденного $\mathbf{AT_3} = \mathbf{AT_{SP}}$

Для визуализации полученных результатов можно осуществить графическую интерпретацию эталонных нечетких термов $\tilde{T}^e_{33s}$ и $\tilde{T}^e_{36s}$. С их помощью по аналогии с [9] строятся пять нечетких опорных двумерных областей (см. рис. 1), характеризующих возможные уровни аномального состояния относительно лингвистических эталонов $\mathbf{T^e_{33} = T^e_{SPKOП}}$ и $\mathbf{T^e_{36} = T^e_{SPKПОА}}$, которые обозначаются одним из текстовых значений – Н, БНВ, БВН, В, П [9]. С помощью этих эталонов осуществляем поиск нечетких термов, которые наиболее близки к соответствующим значениям текущих параметров $\tilde{P}_{SPKOП}$ и $\tilde{P}_{SPKПОА}$. По аналогии с опорными областями также можно визуализировать так называемый нечеткий текущий блок (см. заштрихованную прямоугольную область на рис. 1), образованный посредствам пересечения $\tilde{P}_{SPKOП}$ и $\tilde{P}_{SPKПОА}$. Посредством этого блока осуществляется графическая интерпретация текущего аномального состояния.

На основе полученных текущих значений и с учетом набора решающих правил, направленных на выявление, например, спуфинга [9], в соответствии с этапом 8 метода выявления аномалий [4] для обнаружения атаки $\mathbf{AT_3 = AT_{SP}}$ (см. рис. 1 в [9]), идентификация аномального состояния может быть инициирована правилом $ER_{33} = (\tilde{P}_{SPKПОА} \cong \tilde{Б}^e_{36} \wedge \tilde{P}_{SPKOП} \cong \tilde{C}^e_{33}) \rightarrow БВН$ (см. (10) в [10]), которое буквально можно интерпретировать как: «Если $\tilde{P}_{SPKПОА} \cong \tilde{Б}^e_{36}$ и при этом $\tilde{P}_{SPKOП} \cong \tilde{C}^e_{33}$, то уровень аномального состояния, который может быть порожден спуфингом будет БОЛЬШЕ ВЫСОКИЙ ЧЕМ НИЗКИЙ». На рис. 1 эта зона маркирована литерами БВН и фактически отображает уровень аномального состояния, характерным носителем которого является нечеткий текущий блок.

Аналогичным способом можно произвести вычисления для выявления аномалий порожденных, например, $\mathbf{AT_2 = AT_{DS}}$ («Отказ в обслуживании (DoS)») [7]. Для этого используются эталоны и текущие значения лингвистических переменных «Количество одновременных подключений к серверу» (КОП), «Скорость обработки запросов от клиентов» (СОЗ) и «Задержка между запросами от одного пользователя» (ЗМЗ) [7]. В отличие от предыдущего примера, здесь посредством указанных значений можно сформировать пять нечетких опорных трехмерных областей (рис. 2), которые показаны различными оттенками серого и обозначены литерами П, В, БВН, БНВ и Н, отражающих разную степень уверенности эксперта относительно аномального состояния в среде окружения, которое порождено ожидаемой атакой.

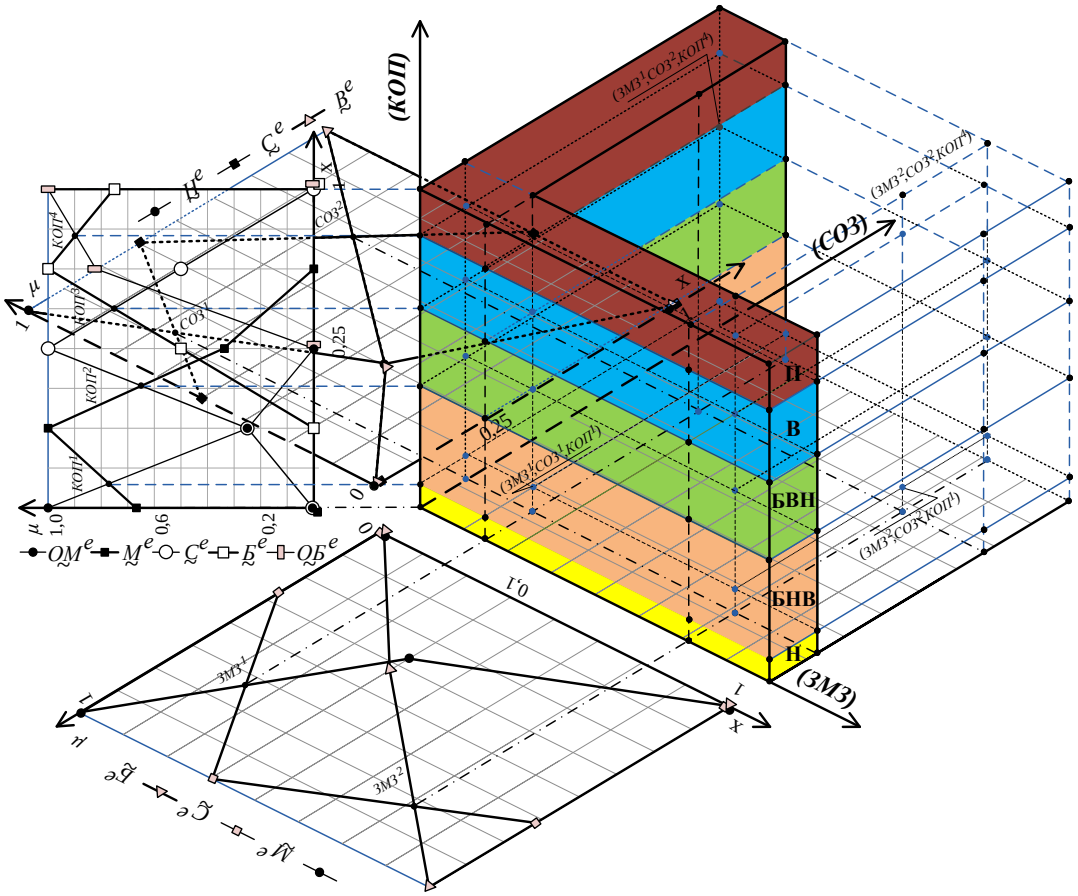

Рис. 2. Графическая интерпретация нечетких опорных трехмерных областей, используемых для обнаружения аномального состояния порожденного $\mathbf{AT_2 = AT_{DS}}$

Выводы

Таким образом, в работе предложен МОИТ, в котором, за счет базового механизма реализующего формирование элементов множества характерных признаков и использования согласующей функции определяется идентифицирующий признак, позволяющий осуществить поиск в заданной лингвистической переменной идентифицирующий преобразованный эталонный терм, по которому с помощью эвристических правил, определяется уровень аномального состояния, характерного соответствующему типу атак.

Далее, для последующего выявления аномального состояния в компьютерных системах, следует определить необходимый набор правил, которые будут свидетельствовать об уровне аномального состояния в компьютерных системах.

Литература

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

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

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

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

[6] 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.

[7] 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.

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

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

[10] 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.

УДК 004.056.53 (045)

Корченко А.О. Метод визначення ідентифікуючих термів для систем виявлення вторгнень

Анотація. *Комп'ютерні системи все більше піддаються впливам загроз, нові види яких породжують нові кібератаки на їх ресурси. Для підвищення рівня безпеки розроблені системи виявлення аномального стану в комп'ютерних мережах, формування нечітких еталонів мережевих параметрів і формування евристичних правил для оцінювання мережевої активності. В основу цих систем закладено метод виявлення аномалій, породжених кібератаками. У цьому методі процес визначення ідентифікуючих термів не супроводжується достатнім для його ефективного використання рівнем формалізації. З метою виключення цього недоліку розроблено метод визначення ідентифікуючих термів, який базується на математичних моделях і методах нечіткої логіки. Метод реалізується на основі трьох базових етапів: формування множин ознак; визначення підмножин ознак; визначення номера ідентифікуючого терма. За його допомогою здійснюється пошук у заданій лінгвістичній змінній ідентифікуючого еталонного терма, на основі якого за допомогою евристичних правил можна визначити рівень аномального стану, характерного для певного типу кібератак. Це дозволить підвищити ефективність побудови відповідних систем виявлення вторгнень.*

Ключові слова: *кібератаки, аномалії, нечіткі еталони, ідентифікуючі терми, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, виявлення аномалій в комп'ютерних мережах.*

Korchenko A. The detection method of identification terms for intrusion detection system

Abstract. *Computer systems are increasingly exposed to threats, new types of which generate new types of cyberattacks on their resources. To increase the security level there were developed special systems focus on detecting abnormal condition in computer networks and formation of fuzzy measurement standards of the network parameters and the formation of heuristic rules for network activity assessment. The basis of these systems is the method of anomalies detection caused by cyber attacks. In this method, the detection process of terms identification is not accompanied by sufficient level of formalisation for its effective use. In order to eliminate this shortcoming, the detection method of terms identification, which is based on mathematical models and fuzzy logic methods is developed. The method is implemented through three basic stages: formation of multitude features; raiting the subsets of features; defining the number of term identification. It makes possible to search in a given linguistic variable the reference term according to which, with a help of heuristic rules, it can be possible to define the level of abnormal conditions specific to a particular type of cyber-attacks. This will increase the efficiency of the intrusion detection systems.*

Key words: *cyber attacks, anomalies, fuzzy standards, identification terms, intrusion detection systems, anomaly detection systems, attack detection systems, anomaly detection in computer networks.*

Отримано *2 жовтня 2014 року*, затверджено редколегією *22 жовтня 2014 року*