Сулема Евгения Станиславовна, кандидат технических наук, доцент, Национальный технический университет Украины «Киевский политехнический институт», доцент кафедры программного обеспечения компьютерных систем.
Sulema Yevgeniya, Ph.D., Assoc. Prof., National Technical University of Ukraine «Kyiv Polytechnic Institute», Assoc. Prof. of Systems Software Department.

Широчин Семен Станіславович, Національний технічний університет України «Київський політехнічний інститут», аспірант кафедри програмного забезпечення комп'ютерних систем.
E-mail: semenstsh@mail.ru
Широчин Семён Станиславович, Национальный технический университет Украины «Киевский политехнический институт», аспирант кафедры программного обеспечения компьютерных систем.
Shyrochyn Semen, National Technical University of Ukraine «Kyiv Polytechnic Institute», Ph.D. student of Systems Software Department.

УДК 004.056.53(045)

СИСТЕМА ФОРМИРОВАНИЯ ЭВРИСТИЧЕСКИХ ПРАВИЛ ДЛЯ ОЦЕНИВАНИЯ СЕТЕВОЙ АКТИВНОСТИ

Анна Корченко

На основе известного метода выявления аномалий порожденных кибератаками разработана соответствующая система, для поддержки функционирования которой необходима реализация этапа формирования множества эвристических правил. Они предназначены для создания соответствующих решающих правил, направленных на проверку истинности взаимосвязей эталонных и текущих параметров при оценивании сетевой активности в определенной среде окружения. Для решения такой задачи предложено новое структурное решение соответствующей системы, основанной на базе правил и содержащей блоки коммутации, формирования логико-лингвистических связок, ранжирования и инициализации правил, а также регистры эталонов, текущих значений, лингвистических идентификаторов и правил. Предложенное решение может быть реализовано программно или программно-аппаратно и использоваться в качестве основы систем выявления аномалий.

***Ключевые слова**: кибератаки, аномалии, системы обнаружения вторжений, системы обнаружения аномалий, системы обнаружения атак, обнаружение аномалий в компьютерных сетях, эвристические правила, оценка сетевой активности.*

Современная теоретическая и практическая база, которая используется для обнаружения атак в компьютерных сетях, имеет определенные ограничения по идентификации новых и несигнатурных типов кибератак. Применение математического аппарата теории нечетких множеств для построения средств обнаружения аномалий, порожденных атакующими действиями, позволит усовершенствовать существующие системы обнаружения вторжений. С этой целью разработана базовая модель параметров для нечетко определенной слабоформализованой среды [1] и универсальная модель эталонов лингвистических переменных [2], позволяющие формализовать процесс построения эталонных значений и устанавливать соответствие между типом атаки и необходимыми для ее идентификации атрибутами. Также построена модель эвристических правил (ЭП) [3], которая за счет множества эталонных параметров, логико-лингвистических связок и лингвистических идентификаторов позволяет формализовать процесс формирования множеств ЭП для выявления аномального состояния.

В работе [4] разработан метод выявления аномалий, который за счет указанных моделей [1-3, 5] и сформированных текущих параметров, позволяет строить средства обнаружения несигнатурных и новых типов кибератак. На основе этого метода предложено новое структурное решение системы выявления аномального состояния в компьютерных сетях [6]. Она состоит из подсистем первичной обработки, формирования нечетких эталонов [7] и формирования ЭП, а также модулей нечеткой арифметики, логического вывода и визуализации.

Это решение используется для совершенствования систем сетевой безопасности, которое основывается на реализации указанного метода обнаружения аномалий [4] и ориентировано на осуществление контроля активности в определенной среде окружения.

Для поддержки функционирования указанной системы выявления [6] актуальным является разработка соответствующего средства, обеспечивающего эффективную работу подсистемы формирования ЭП.

В связи с этим, целью данной работы является создание алгоритмического обеспечения и нового структурного решения, которое может использоваться на практике для расширения функциональных возможностей современных систем обнаружения вторжений.

Достижение поставленной цели будет основываться на методе выявления аномалий порожденных кибератаками [4], на основе которого предлагается новое структурное решение соответствующей системы формирования ЭП (рис. 1), ориентированной на построение решающих правил, направленных на проверку истинности взаимосвязей эталонных и текущих параметров для оценивания сетевой активности.

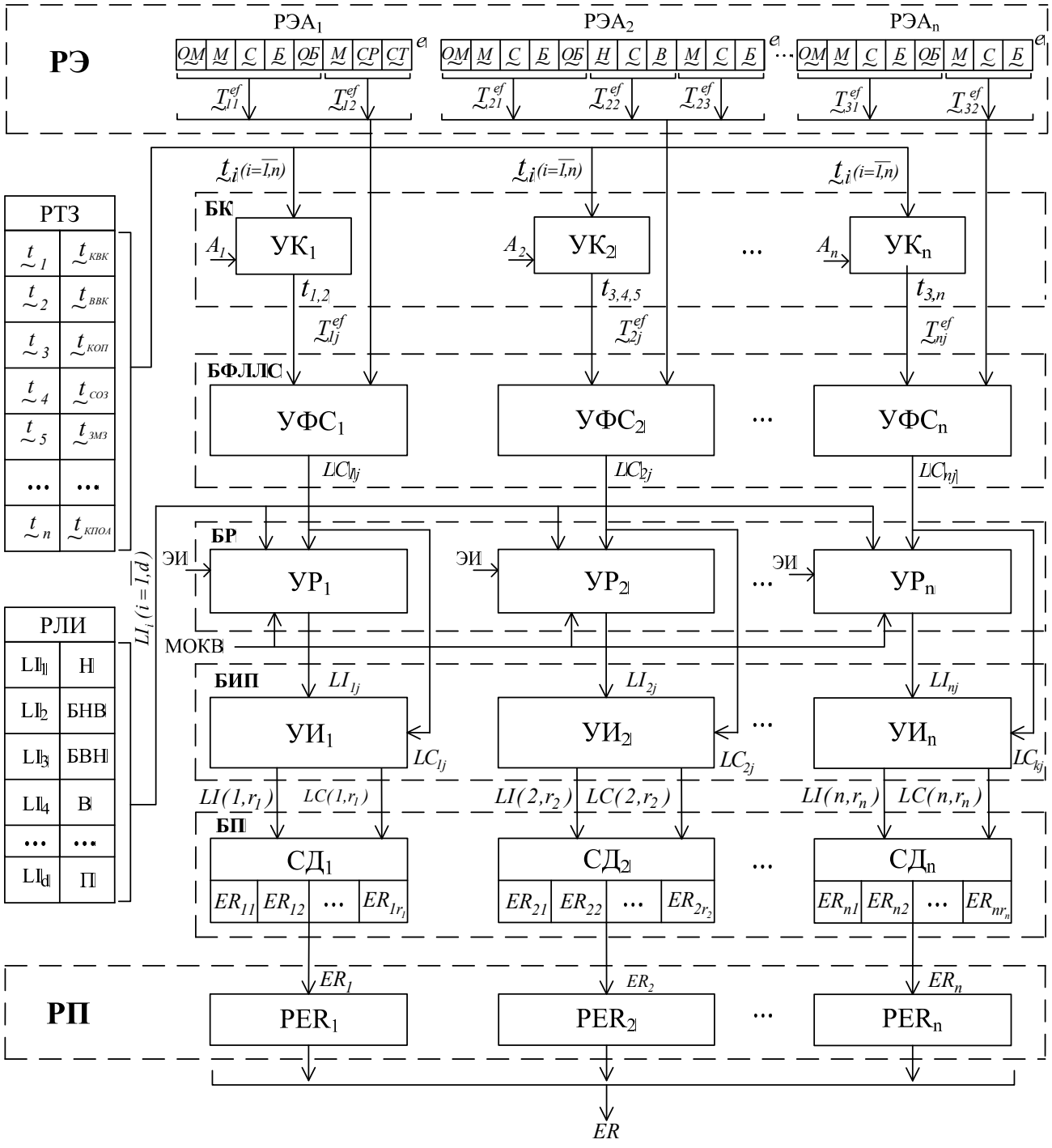

Рис. 1. Структура системы формирования эвристических правил для оценивания сетевой активности

Система содержит:

– регистр эталонов (РЭ);

– блок коммутации (БК), служащий для формирования потоков t_i [3], поступающих на блок формирования логико-лингвистических связок (БФЛЛС);

– БФЛЛС, предназначенный для логического преобразования эталонных T_{ij}^{ef} [1];

– блок ранжирования (БР), осуществляющий формирование коэффициента важности;

– блок инициализации правил (БИП), формирующий матрицы $LI(\mathrm{i},\mathrm{r}_\mathrm{r})$ и $LC(\mathrm{i},\mathrm{r}_\mathrm{r})$ [3];

– базу правил (БП), служащей для хранения в соответствующих секторах данных ($СД_\mathrm{i}$, $\mathrm{i}=\overline{1,d}$) наборов правил ER_{ir_i} $(\mathrm{i}=\overline{1,n})$ [3];

– регистры текущих значений (РТЗ) и лингвистических идентификаторов (РЛИ), предназначенные соответственно для хранения в процессе всех вычислений значений t и LI_i $(\mathrm{i}=\overline{1,d})$;

– регистр правил (РП), предназначенный для приема и хранения подмножеств правил ER_i.

Система функционирует следующим образом (рис. 2). В каждый РЭ i-й атаки ($РЭА_\mathrm{i}$, $\mathrm{i}=\overline{1,n}$) заносятся и хранятся на протяжении всего вычислительного процесса значения группы эталонов T_{ij}^{ef} $(\mathrm{i}=\overline{1,n})$ соответствующих параметров (например, “Количество виртуальных каналов” (КВК), “Возраст виртуального канала” (ВВК), “Количество одновременных подключений к серверу” (КОП), “Скорость обработки запросов от клиентов” (СОЗ), “Задержка между запросами от одного пользователя” (ЗМЗ) и “Количество пакетов с одинаковым адресом отправителя и получателя” (КПОА)), характерных для i-й атаки (например, “Сканирование портов” (*SN*), “Отказ в обслуживании” (*DS*) или “Спуфинг” (*SP*)), а также в РТЗ поступают текущие значения t_i $(\mathrm{i}=\overline{1,n})$ (см. вершины 2–6 на рис. 2).

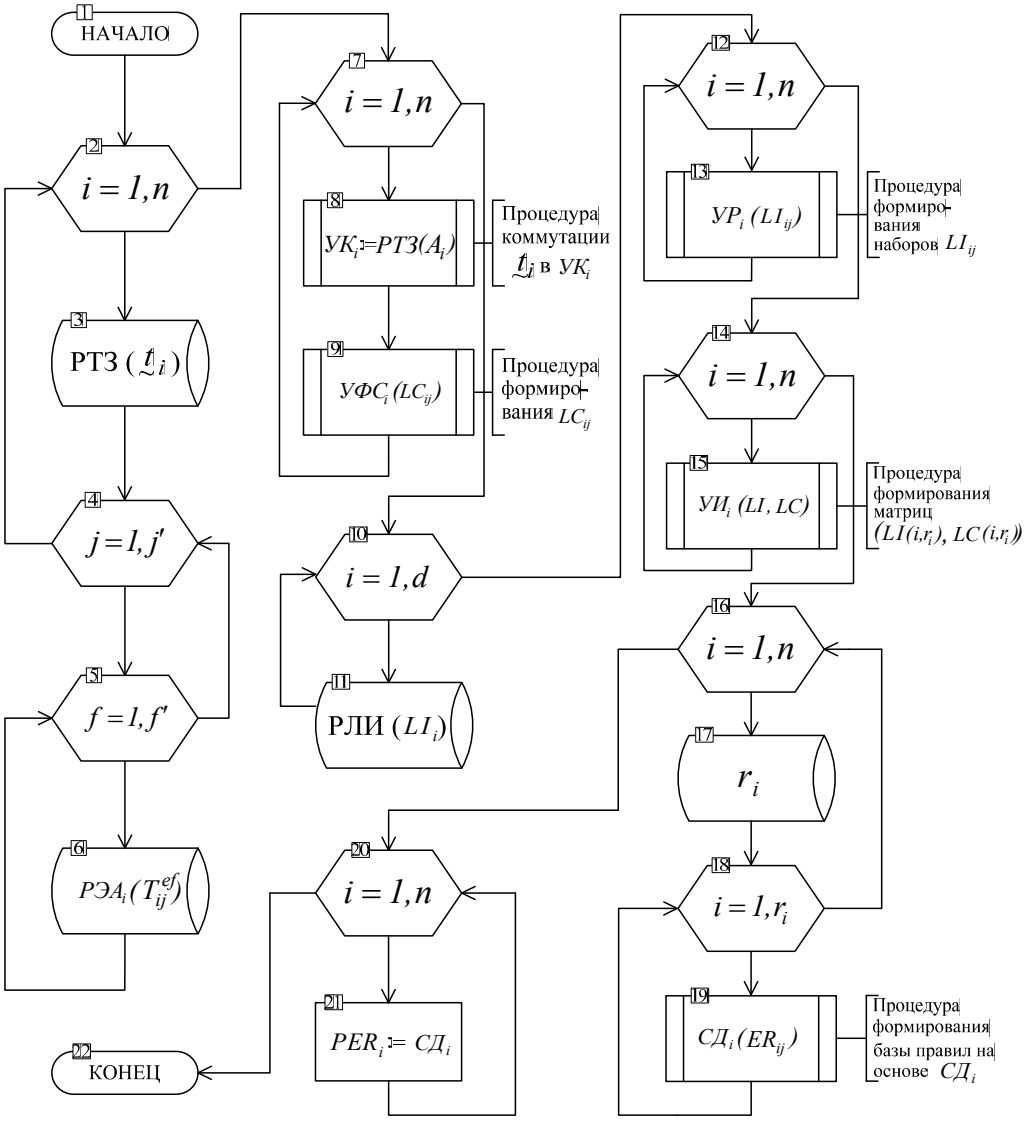

Рис 2. Алгоритм работы системы формирования ЭП для оценивания сетевой активности

В узлах формирования связок (УФС$_i$, $i=\overline{1,n}$) БФЛЛС на основе эталонных значений T_{ij}^{ef} $(i=\overline{1,n})$, поступающих с РЭА$_i$ $(i=\overline{1,n})$ и подмножества текущих параметров t_j $(i=\overline{1,n})$, поступивших с РТЗ через узлы коммутации (УК$_i$, $i=\overline{1,n}$) БК посредством управляющего сигнала A$_i$ $(i=\overline{1,n})$ (например, при значениях $i=1$, $i=2$ и $i=n$ в УФС$_1$, УФС$_2$ и УФС$_n$ с РТЗ через УК$_1$, УК$_2$ и УК$_n$ поступят соответственно значения $t_{1,2}=\{t_1, t_2\}=\{t_{КВК}, t_{ВВК}\}$, $t_{3,4,5}=\{t_3, t_4, t_5\}=\{t_{КОП}, t_{СОЗ}, t_{ЗМЗ}\}$ и $t_{3,n}=\{t_3, t_n\}=\{t_{КОП}, t_{КПОА}\}$) соответственно сформируются и поступят на выход УФС$_i$ (см. вершины 7–9 на рис. 2) логико-лингвистические свя-зки LC_{ij}, например, $LC_{21}=(t_{КПОА} \cong \underset{\sim}{Б}^e \wedge t_{КОП} \cong \underset{\sim}{ОМ}^e)$.

Отметим, что в РЛИ заносятся все значения LI_i $(i=\overline{1,d})$ и хранятся там на протяжении всего процесса формирования правил (см. вершины 10 и 11 на рис. 2). В каждом узле ранжирования (УР$_i$, $i=\overline{1,n}$) БР для каждой LC_{ij} $(i=\overline{1,n})$ в качестве возможного исхода поочередно ставятся в соответствие все лингвистические идентификаторы LI_i $(i=\overline{1,d})$, поступившие с РЛИ. Далее, на основе метода определения коэффициента важности (МОКВ) [3, 9] и экспертной информации из сформированного таким образом множества альтернативных правил ER_{ij}^k, определяется множество LI_{ij}, необходимое для инициализации ЭП (см. вершины 12 и 13 на рис 2).

Далее, в узлах инициализации (УИ$_i$, $i=\overline{1,n}$) БИП на базе данных УР$_i$ и УФС$_i$ попарно формируются элементы матриц $LC(1, r_1)$ и $LI(1, r_1)$ (см. вершины 14 и 15 на рис. 2), на основе которых осуществляется инициализация необходимых наборов правил. Сгенерированные в УИ$_i$ матрицы попарно заносятся в сектора данных (СД$_i$, $i=\overline{1,n}$) БП, формируя таким образом наборы правил ER_{ij} $(i=\overline{1,n},\ j=\overline{1,r_i})$ предназначенных для выявления аномального состояния порожденного i-й атакой (см. вершины 16–19 на рис. 2). Далее эти правила ER_i $(i=\overline{1,n})$ перезаписываются в регистры ER_i (РЕR$_i$, $i=\overline{1,n}$) и хранятся там на протяжении всего процесса функционирования системы (см. рис. 1).

Рассмотрим работу системы формирования ЭП на конкретном примере. Отметим, что каждому ER_{ij} [3] соответствует эвристическое выражение (правило), т.е. формируются связки $ER_{11}=LC_{11} \to LI(1,1)$, $ER_{12}=LC_{12} \to LI(1,2)$, $ER_{13}=LC_{13} \to LI(1,3)$, $ER_{14}=LC_{14} \to LI(1,4)$, $ER_{15}=LC_{15} \to LI(1,5)$, которые интерпретируются одним из сообщений – Н, БНВ, ББН, В, П и соответственно отображаются текстовыми значениями “Низкий”, “Больше низкий чем высокий”, “Больше высокий чем низкий”, “Высокий” и “Предельный”.

Например, посредством сформированных в [3] матриц инициализации для $\mathbf{AT}_i$ и $\mathbf{P}_j$ (при $i=1$ и $j=\overline{1,2}$), использования выражения (7) в [3] и наборов ЭП, направленных на выявление $AT_1=SN$ (при P_1=КВК и P_2=ВВК), определяются для $\boldsymbol{ER_1}$ значения $ER_{11}\ldots ER_{15}$ т.е.:

$$\boldsymbol{ER_1}=\{ ER_{11}=(t_{ВВК} \cong \underset{\sim}{M}^e \wedge t_{КВК} \cong \underset{\sim}{ОМ}^e) \to Н,$$

$$ER_{12}=(t_{ВВК} \cong \underset{\sim}{M}^e \wedge t_{КВК} \cong \underset{\sim}{M}^e) \to БНВ,$$

$$ER_{13}=(t_{ВВК} \cong \underset{\sim}{M}^e \wedge t_{КВК} \cong \underset{\sim}{C}^e) \to ББН,$$

$$ER_{14}=(t_{ВВК} \cong \underset{\sim}{M}^e \wedge t_{КВК} \cong \underset{\sim}{Б}^e) \to В,$$

$$ER_{15}=(t_{ВВК} \cong \underset{\sim}{M}^e \wedge t_{КВК} \cong \underset{\sim}{ОБ}^e) \to П \}.$$

Тогда этим значениям будут соответствовать следующие наборы решающих правил

ER$_{11}$ = “Если $t_{ВВК}$ наиболее близко к $\underset{\sim}{M}^e$, входящего в $T_{ВВК}^e$ и $t_{КВК}$ наиболее близко к $\underset{\sim}{ОМ}^e$, входящего в $T_{ВВК}^e$, то уровень аномального состояния, порожденного SN будет НИЗКИЙ”;

ER$_{12}$ = “Если $t_{ВВК}$ наиболее близко к $\underset{\sim}{M}^e$, входящего в $T_{ВВК}^e$ и $t_{КВК}$ наиболее близко к $\underset{\sim}{M}^e$, входящего в $T_{КВК}^e$, то уровень аномального состояния, порожденного SN будет БОЛЬШЕ НИЗКИЙ, ЧЕМ ВЫСОКИЙ”;

ER$_{13}$ = “Если $t_{ВВК}$ наиболее близко к $\underset{\sim}{M}^e$, входящего в $T_{ВВК}^e$ и $t_{КВК}$ наиболее близко к $\underset{\sim}{C}^e$, входящего в $T_{КВК}^e$, то уровень аномального состояния, порожденного SN будет БОЛЬШЕ ВЫСОКИЙ, ЧЕМ НИЗКИЙ”;

ER$_{14}$ = “Если $t_{ВВК}$ наиболее близко к $\underset{\sim}{M}^e$, входящего в $T_{ВВК}^e$ и $t_{КВК}$ наиболее близко к $\underset{\sim}{Б}^e$,

входящего в $\underset{\sim}{T}^{e}_{КВК}$, то уровень аномального состояния, порожденного *SN* будет ВЫСОКИЙ";

ER_{15} = "Если $\underset{\sim}{t}_{ВВК}$ наиболее близко к $\underset{\sim}{M}^{e}$, входящего в $\underset{\sim}{T}^{e}_{ВВК}$ и $\underset{\sim}{t}_{КВК}$ наиболее близко к $\underset{\sim}{ОБ}^{e}$, входящего в $\underset{\sim}{T}^{e}_{КВК}$, то уровень аномального состояния, порожденного *SN* будет ПРЕДЕЛЬНЫЙ".

Таким образом, для группы правил $\boldsymbol{ER_1}$, ориентированных на идентификацию AT_1=*SN* можно получить графическое отображение нечетких опорных двумерных областей (Н, БНВ, БВН, В, П), характеризующих возможные уровни аномального состояния относительно ЛП **КВК** и **ВВК** (см. рис. 3). Имея эталоны, а также вычислив текущие значения параметров, можно с помощью ЭП определить уровень аномального состояния в компьютерных системах, идентификатором которого будет одна из полученных опорных областей.

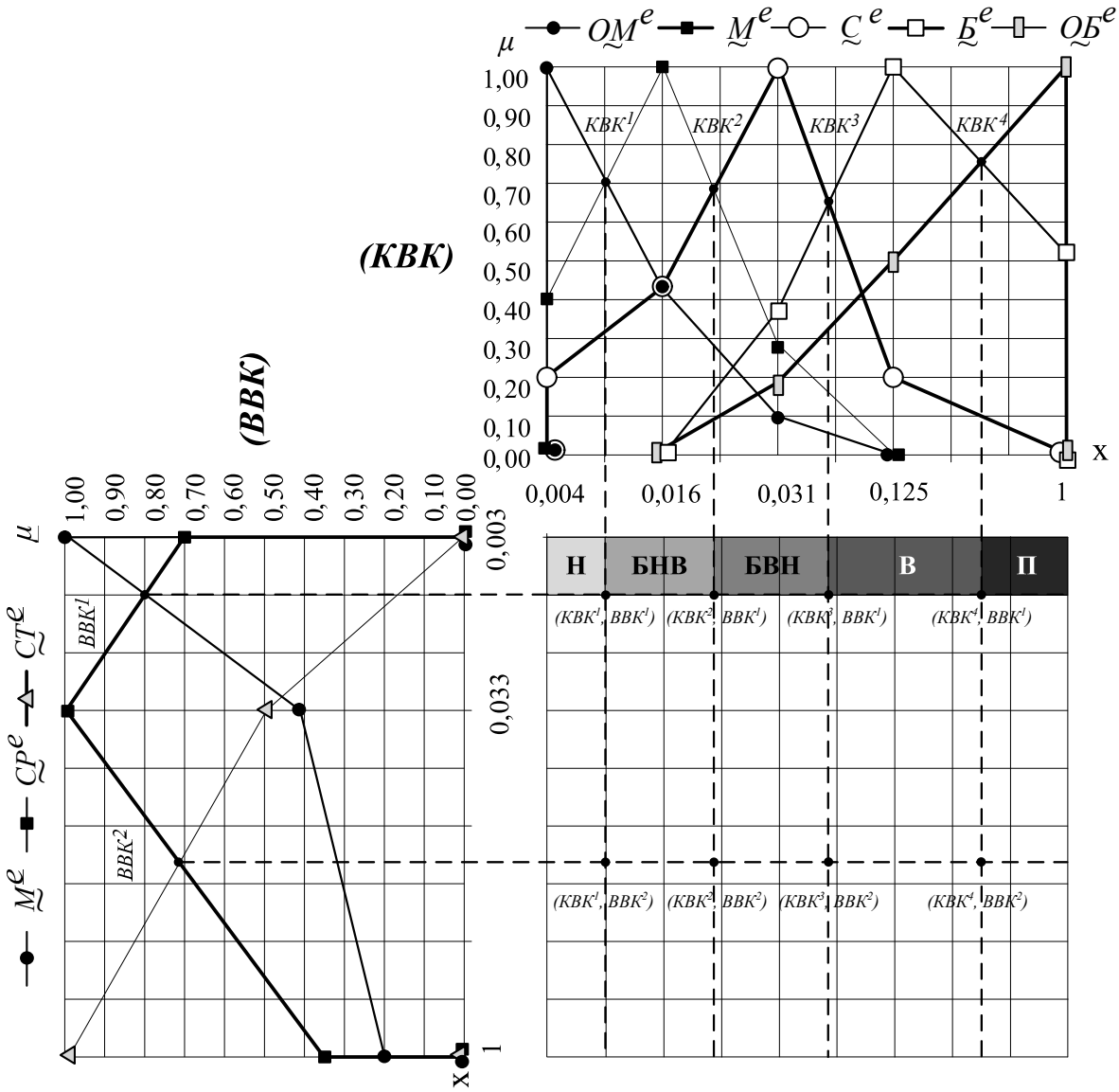

Рис. 3. Нечеткие опорные блоки для $\boldsymbol{ER_1}$

Предложенное новое структурное решение системы формирования ЭП для оценивания сетевой активности (см. рис. 1) может быть реализована программно или программно-аппаратно и использоваться для формирования решающих правил, направленных на проверку истинности взаимосвязей эталонных и текущих параметров для оценивания сетевой активности в среде окружения, а также применяться в качестве основы при построении систем выявления аномалий.

ЛИТЕРАТУРА

[1]. 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.

[2]. 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.
[3]. 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.
[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. Модели систем выявления аномалий, порожденных кибератаками / А.А. Корченко // Эвристические алгоритмы и распределенные вычисления в прикладных задачах : Коллективная монография / Под ред. Б.Ф. Мельникова. – Ульяновск, 2013. – Выпуск 2. – С. 56-86.
[6]. Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. – 2012. – № 2 (18). – С. 80-84.
[7]. Корченко А.А. Система формирования нечетких эталонов сетевых параметров / А.А. Корченко // Захист інформації. – Т.15, №3. – 2013. – С. 240-246.
[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.

REFERENCES

[1]. 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.
[2]. 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.
[3]. 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.
[4]. 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.
[5]. Korchenko A.A. The system models of anomaly detection caused by cyber-attacks, heuristic algorithms and distributed computing applications, Ulianovsk, 2013, V 2, pp. 56-86.
[6]. Korchenko A.A. Anomaly-based detection system in computer networks, Bezpeka ìnformacìï, 2012, №2 (18), pp. 80-84.
[7]. Korchenko A.A. The system development of fuzzy standards of network parameters, Zahist ìnformacìï, T.15, №3, 2013, pp. 240-246.
[8]. Korchenko A.G. The development of information protection systems based on the fuzzy sets, The theory and practical solutions, Kuev, 2006, 320 p.

СИСТЕМА ФОРМУВАННЯ ЕВРИСТИЧНИХ ПРАВИЛ ДЛЯ ОЦІНЮВАННЯ МЕРЕЖЕВОЇ АКТИВНОСТІ

На основі відомого методу виявлення аномалій породжених кібератаками розроблена відповідна система, для підтримки функціонування якої необхідна реалізація етапу формування множини евристичних правил. Вони призначені для створення відповідних вирішальних правил, спрямованих на перевірку істинності взаємозв'язків еталонних і поточних параметрів при оцінюванні мережевої активності в певному середовищі оточення. Для вирішення такого завдання запропоновано нове структурне рішення відповідної системи, яке засновано на базі правил та містить блоки комутації, формування логіко-лінгвістичних зв'язок, ранжирування і ініціалізації правил, а також регістри еталонів, поточних значень, лінгвістичних ідентифікаторів і правил. Запропоноване рішення може бути реалізовано програмно або програмно-апаратно і використовуватися в якості основи систем виявлення аномалій.

Ключові слова: кібератаки, аномалії, системи виявлення вторгнень, системи виявлення аномалій, системи виявлення атак, виявлення аномалій в комп'ютерних мережах, евристичні правила, оцінка мережевої активності.

THE SYSTEM OF HEURISTIC RULES FORMATION FOR NETWORK ACTIVITY ASSESSMENT

Based on the known method for anomalies detection caused by the cyberattacks the corresponding system has been developed. The implementation of this system requires the realization phase of multiple set of heuristic rules formation. They are intended to create the appropriating critical rules directed on truth verification of reference and current parameters interrelations when the network activity is being assessed in a specific environment. This paper suggests a new structural solution of the corresponding system based on the critical rules and containing switching units, the formation of linguistic variables, rules ranking and initialization, as well as registers of standards, current values, linguistic identifiers and rules. The proposed solution can be implemented through software or hardware and to be used as the basis of systems for anomalies detection.

Keywords: cyber attacks, anomalies, intrusion detection systems, anomaly detection systems, attack detection

systems, anomaly detection in computer networks, heuristic rules, network activity assessment.

Корченко Анна Олександрівна, кандидат технічних наук, доцент кафедри безпеки інформаційних технологій Національного авіаційного університету.
E-mail: annakor@ukr.net

Корченко Анна Александровна, кандидат технических наук, доцент кафедры безопасности информационных технологий Национального авиационного университета.
Anna Korchenko PhD in Eng., Associate Professor of Academic Department of IT-Security, National Aviation University (Kyiv, Ukraine).

УДК 004.056.5(045)

МЕТОД ПРЕОБРАЗОВАНИЯ ЭТАЛОНОВ ПАРАМЕТРОВ ДЛЯ СИСТЕМ АНАЛИЗА И ОЦЕНИВАНИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр Корченко, Светлана Казмирчук, Андрей Гололобов

Для реализации процесса анализа и оценивания информационных рисков основанного на суждениях экспертов, как правило, требуется привлечение методов и средств, позволяющих обрабатывать нечеткие исходные данные, например, представленные в лингвистической форме. Известна система, в которой оценивание реализовано на основе параметрических трапециевидных нечетких чисел. При ее практическом использовании возникает необходимость применения других типов нечетких чисел. Расширить возможности такой системы можно путем дополнительного использования другого типа параметрических нечетких чисел – треугольных. Для решения такой задачи предложен метод преобразования эталонов параметров, в основе которого заложена аналитическая функция, позволяющая осуществлять трансформирование (эквивалентное преобразование) термов лингвистических переменных. Такое решение позволит повысить гибкость разрабатываемых средств анализа и оценивания рисков информационной безопасности, которые основываются на логико-лингвистическом подходе и используют для описания лингвистических переменных треугольные нечеткие числа.

Ключевые слова: *риск, риски информационной безопасности, анализ рисков, оценивание рисков, метод преобразования эталонов параметров, система анализа и оценивания рисков, параметры риска, лингвистическая переменная, нечеткая переменная, эталонные значения, трансформирование термов лингвистических переменных, эквивалентное преобразование термов лингвистических переменных.*

Для реализации процесса анализа и оценивания информационных рисков, основанного на суждениях экспертов, как правило, требуется привлечение методов и средств, позволяющих обрабатывать нечеткие исходные данные [1-3], например, представленные в лингвистической форме. Известна система [2], в которой оценивание реализовано на основе лингвистических переменных (ЛП), базирующихся на эталонных параметрических трапециевидных нечетких числах (НЧ) с различным количеством определяющих термов [1, 3]. Эффективность практического использования указанной системы зависит от ее возможностей обрабатывать другие типы НЧ, на основе которых осуществляется определения ЛП и переопределение числа их термов.

Исходя из этого, актуальной является задача эквивалентного преобразования ЛП посредством создания эталонов параметров треугольных НЧ с возможностью варьирования числом термов. Расширить возможности указанной системы [2] можно путем использования дополнительного типа параметрических нечетких чисел – треугольных.

В связи с этим, целью данной работы является разработка метода преобразования эталонов параметров для систем анализа и оценивания рисков информационной безопасности. Это будет способствовать дальнейшему развитию методов трансформирования термов и расширит их возможности по использованию треугольных НЧ.

Достижение поставленной цели осуществим с помощью метода, в основе которого заложена аналитическая функция, позволяющая осуществлять трансформирование (эквивалентное преобразование) термов ЛП. И так, в работе [1] НЧ описываются (для целей компактного представления трапециевидных функций принадлежности $\mu(dr)$) в виде $\underset{\sim}{X}_{DR}=(a_j, b_{1j}, b_{2j}, c_j)_{LR}$, где a и c – абсциссы нижнего основания, b_1 и b_2 – абсциссы верхнего основания трапеции, а $j=\overline{1,m}$ (m – количество термов). Если приравняем $b_{1j}=b_{2j}$, то получим другой тип параметрических НЧ – треугольные.