УДК 519.766.2

Н. Б. Копытчук, д-р техн. наук,
П. М. Тишин, канд. физ-мат. наук,
М. В. Цюрупа

ПРОЦЕДУРА СОЗДАНИЯ НЕЧЕТКИХ МОДЕЛЕЙ АНАЛИЗА РИСКОВ В СЛОЖНЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Аннотация. *Рассмотрен вопрос вычисления степени истинности нечетких значений лингвистических переменных при оценке рисков в вычислительных системах. Анализ рисков предлагается осуществлять с помощью методологии Coras. Введены полные ортогональные семантические пространства для вычислений степеней истинности составных частей системы оценки рисков. Предложено описание формализованного языка представления баз знаний для анализа рисков в сложной вычислительной системе.*

Ключевые слова*: дескрипционная логика, диаграммы Coras, лингвистические переменные, нечеткие множества, полные ортогональные семантические пространства, уязвимости, активы, угрозы, диаграммы угроз, нежелательные инциденты*

N. B. Kopytchuk, ScD.,
P. M. Tishin, PhD.,
M. V. Tsyurupa

CREATION PROCEDURE OF THE FUZZY RISK ASSESSMENT MODEL FOR COMPLEX COMPUTER SYSTEMS

Abstract. *The problem of calculating the fuzzy truth degree of linguistic variables in risk assessment in computing systems . Risk analysis is proposed to carry out using the methodology Coras. Enter the complete orthogonal semantic space for computing degrees of truth of the constituent parts of risk assessment . A description of the formal language representation of knowledge bases for risk analysis in the complex computing system.*

Keywords*: description logic diagrams, Coras, linguistic variables , fuzzy sets , complete orthogonal semantic space, vulnerability , assets , threats, threats chart , undesirable incidents*

М. Б. Копитчук, д-р техн. наук,
П. М. Тішін, канд. фіз-мат. наук,
М. В. Цюрупа

ПРОЦЕДУРА СТВОРЕННЯ НЕЧІТКИХ МОДЕЛЕЙ АНАЛІЗУ РИЗИКІВ В СКЛАДНИХ ОБЧИСЛЮВАЛЬНИХ СИСТЕМАХ

Анотація. *Розглянуто питання обчислення ступеня істинності нечітких значень лінгвістичних змінних при оцінці ризиків в обчислювальних системах . Аналіз ризиків пропонується здійснювати за допомогою методології Coras . Введені повні ортогональні семантичні простору для обчислень ступенів істинності складових частин системи оцінки ризиків . Запропоновано опис формалізованої мови представлення баз знань для аналізу ризиків в складній обчислювальній системі .*

Ключові слова: *дескріпційна логіка, діаграми Coras, лінгвістичні змінні, нечіткі множини, повні ортогональні семантичні простори, уразливості, активи, загрози, діаграми загроз, небажані інциденти*

Введение. В отличие от общих языков моделирования язык Coras [11, 12] предназначен для моделирования рисков. Тот факт, что язык Coras был разработан специально для моделирования риска, имеет ряд преимуществ. В первую очередь, он поддерживает эффективное моделирование рисков, потому что он содержит только те конструкции, которые необходимы для поддержания моделирования рисков. Кроме того, поскольку этот язык ограничивается моделированием риска, его диаграммы становятся более однородными.

Метод анализа риска должен поддерживать определение оценки вероятности нежелательного инцидента и вероятностей событий и сценариев, которые могут привести к нежелательным инцидентам. Расчеты вероятностей в Coras диаграммах могут быть основаны на правилах, которые аналогичны введенным в деревьях неисправностей [13] или событий [14]. С другой стороны, язык Coras со своими правилами для рассуждений о вероятности [9] является более общим.

Однако в языке Coras уровни риска можно задавать не только определяя вероятности, но и лингвистическими термами. Дополнительными специфическими особенно-

стями, которые можно учитывать при создании систем оценки рисков, являются:

– неполнота и неопределенность исходной информации о составе и характере угроз;

– возможность задания как количественных, так и качественных показателей, которые необходимо учитывать при решении задач описания и оценки рисков.

В работах [1, 2] авторами предложен подход к описанию знаний о возникающих в системе рисках с использованием языка *ALC* на основе понятий, введенных в языке Coras. Введенные в работе [2] концепты позволяют описывать диаграммы рисков в общем виде на языке *ALC*, что дает возможность составлять онтологии и делать некоторые логические заключения на основе дескриптивной логики о причинах и следствиях рисков в системе. В свою очередь, в работе [3] этот подход расширен за счет использования многоуровневых онтологий и декомпозиции области оценки рисков в вычислительных системах на составные онтологии с применением Coras методологии.

Поскольку одной из сложностей составления диаграмм рисков некоторой системы является неопределенность и неточность описаний составляющих системы, то аппаратом для описания неопределенностей выбрана теория нечетких множеств [15], которая получила широкое распространение и применяется в различных областях науки.

В соответствии с работой [2] введение нечеткости в описание рисков требует дополнительной формализации предметной области в рамках языка ALC.

Полные ортогональные семантические пространства. Удобным математическим аппаратом, позволяющим формализовать неопределенности в данных задачах, являются полные ортогональные семантические пространства (ПОСП) [4, 5].

Для построения ПОСП некоторой лингвистической переменной $\tilde{p}_i$ определим множества нечетких термов $\tilde{D}_i = \{\tilde{p}_i^k\}, (k = 1...K_i)$, где K_i – количество нечетких термов, принимаемых *i*-м параметром в виде нечетких чисел с трапецеидальной функцией принадлежности μ_i^k, которая положительно определена на некотором интервале (p_{ib}^k, p_{ie}^k), где $p_{ib}^k, p_{ie}^k \in D_i$ – значения начала и конца интервала соответственно, а D_i – базовое множество нечетких значений параметра $\tilde{p}_i$.

Каждый нечеткий терм $\tilde{p}_k^i \in \tilde{D}_i$ определим через функцию принадлежности следующего вида:

$$\tilde{p}_k^i \Rightarrow \mu_k^i(p_i') = \begin{cases} 0, & p_i' \le p_{kb}^i, p_i' \ge p_{ke}^i \\ \dfrac{p_i' - p_{kb}^i}{p_{kb_1}^i - p_{kb}^i}, & p_{kb}^i < p_i' < p_{kb_1}^i \\ 1, & p_{kb_1}^i \le p_i' \le p_{ke_1}^i \\ \dfrac{p_i' - p_{ke}^i}{p_{ke_1}^i - p_{ke}^i}, & p_{ke_1}^i < p_i' < p_{ke}^i \end{cases}, \quad (1)$$

$$i = 1..\tilde{N}_P, k = 1..K_i$$

где p_i' - некоторое четкое значение i-го параметра, p_{kb}^i, p_{ke}^i – начальное и конечное значения соответственно интервала значений базового множества D_i, на котором функция принадлежности *k*-го нечеткого значения *i*-го параметра положительно определена;

$p_{kb_1}^i, p_{ke_1}^i$ – начальное и конечное значения соответственно интервала значений базового множества D_i, на котором функция принадлежности *k*-го нечеткого значения *i*-го параметра равна единице.

При этом на множестве нечетких термов i-го параметра должны выполняться следующие условия:

$$\begin{cases} \mu_k^i(p_i') = 1 - \mu_{k-1}^i(p_i'), p_{kb}^i < p_i' < p_{kb_1}^i \\ \mu_k^i(p_i') = 1 - \mu_{k+1}^i(p_i'), p_{ke_1}^i < p_i' < p_{ke}^i \end{cases}, \quad (2)$$

$$k = 2..(K-1),$$

$$\begin{cases} p_{1b}^i = p_{1b_1}^i = \min\limits_{D_i}(p_i') \\ p_{Ke}^i = p_{Ke_1}^i = \max\limits_{D_i}(p_i') \end{cases}, \quad i = 1..\tilde{N}_P. \quad (3)$$

Для использования ПОСП, определенного для лингвистических переменных при анализе рисков, определим некоторые математические операции, которые можно производить над данными нечеткими величинами.

Обозначим через $\tilde{x} = \{x_b, x_{b_1}, x_{e_1}, x_e\}$, $\tilde{y} = \{y_b, y_{b_1}, y_{e_1}, y_e\}$ и $\tilde{z} = \{z_b, z_{b_1}, z_{e_1}, z_e\}$

некоторые нечеткие термы, соответствующие лингвистическим переменным с функциями принадлежности вида (1–3). Тогда согласно [6] можно записать

$$\tilde{z} = \tilde{x} @ \tilde{y} = \underset{\alpha}{\cup} z_\alpha = \underset{\alpha}{\cup} x_\alpha @ y_\alpha, \qquad (4)$$

где $x_\alpha, y_\alpha, z_\alpha$ – α-уровни нечетких значений $\tilde{x}, \tilde{y}, \tilde{z}$ соответственно; а символом $@$ обозначается один из символов $\{+,-,\cdot,/\}$. Учитывая трапецеидальные формы функций принадлежности, можно записать следующие соотношения, которые использовались при анализе характеристик сложных вычислительных систем в работе [7]:

$$\begin{aligned}
&\tilde{z} = \tilde{x} + \tilde{y} = \{x_b + y_b, x_{b_1} + y_{b_1}, x_{e_1} + y_{e_1}, x_e + y_e\}\\
&\tilde{z} = \tilde{x} - \tilde{y} = \{x_b - y_e, x_{b_1} - y_{e_1}, x_{e_1} - y_{b_1}, x_e - y_b\}\\
&\tilde{z} = \tilde{x} \cdot \tilde{y} = \{x_b \cdot y_b, x_{b_1} \cdot y_{b_1}, x_{e_1} \cdot y_{e_1}, x_e \cdot y_e\} \qquad (5)\\
&\tilde{z} = \frac{\tilde{x}}{\tilde{y}} = \{\frac{x_b}{y_e}, \frac{x_{b_1}}{y_{e_1}}, \frac{x_{e_1}}{y_{b_1}}, \frac{x_e}{y_b}\}
\end{aligned}$$

В общем случае нечеткое значение y_i' лингвистической переменной y_i может не совпадать ни с одним из нечетких значений $\tilde{y}_i^k$ из ПОСП, построенном для лингвистической переменной y_i. Данное ПОСП для переменной y_i будем в дальнейшем обозначать Π_{y_i}.

Для определения соответствия нечеткого значения y_i' некоторому значению в ПОСП Π_{y_i} будем использовать по аналогии с работой [8] следующее соотношение, определяющее метрику между y_i' и термами ПОСП Π_{y_i}:

$$\tilde{y}_i = \arg \min_{k=1..K_{yi}} f_d(\tilde{y}_i^k, y_i'). \qquad (6)$$

Здесь

$$\begin{aligned}
f_d(\tilde{y}_i^k, y_i') = |\, & y_{ie}^k - y_{ie}' + y_{ib}^k - y_{ib}' +\\
& + \frac{y_{ie}^k y_{ie_1}^k - y_{ib}^k y_{ib_1}^k}{y_{ie}^k - y_{ib}^k} - \frac{y_{ie}' y_{ie_1}' - y_{ib}' y_{ib_1}'}{y_{ie}' - y_{ib}'} +\\
& + \frac{(y_{ie_1}^k)^2 - (y_{ib_1}^k)^2}{y_{ie}^k - y_{ib}^k} - \frac{(y_{ie_1}')^2 - (y_{ib_1}')^2}{y_{ie}' - y_{ib}'}|,
\end{aligned} \qquad (7)$$

где y_{kb}', y_{ke}' – начальное и конечное значения соответственно интервала значений базового множества D_i, на котором функция принадлежности μ_i', соответствующая нечеткой величине y_i', положительно определена, а y_{kb_1}', y_{ke_1}' – начальное и конечное значения соответственно интервала значений базового множества D_i, на котором функция принадлежности μ_i', соответствующая нечеткой величине y_i', равна единице; K_{y_i} – количество термов на Π_{y_i}.

В работе вводятся несколько различных зависимостей, которые используются при анализе рисков в сложных вычислительных системах [9]. Данные зависимости являются общими, поскольку могут использоваться на разных этапах анализа рисков. При построении данных зависимостей предполагается, что нечеткое значение выходного параметра $\tilde{y}_i^k$ определяется в соответствующем ПОСП Π_{y_i}.

Предположим, что зависимость $\tilde{y}_i$ от лингвистических переменных p_1, p_2, имеет следующий вид:

$$\tilde{y}_i = p_1 @ p_2, \qquad (8)$$

где p_1, p_2 – лингвистические переменные, а знаком $@$ обозначается одна из операций $\{+,\cdot\}$.

Тогда, если при анализе рисков используется соотношение (8), то оценка нечеткого значения параметра $\tilde{y}_i$ определяется следующим выражением:

$$\tilde{y}_i = \arg \min_{k=1..K_y} f_d(\tilde{y}_i^k, y_i'), \qquad (9)$$

где

$$y_i' = \{p_b^1 @ p_b^2, p_{b_1}^1 @ p_{b_1}^2, p_{e_1}^1 @ p_{e_1}^2, p_e^1 @ p_e^2\}.$$

Если зависимость между параметрами имеет вид:

$$\tilde{y}_i = p_1 + p_2 - p_1 p_2, \qquad (10)$$

где p_1, p_2 – лингвистические переменные, то оценка нечеткого значения $\tilde{y}_i$ определяется соотношением (9), в котором

$$\begin{aligned}
y_i' = \{&p_b^1 + p_b^2 - p_e^1 p_e^2, p_{b_1}^1 + p_{b_1}^2 -\\
&p_{e_1}^1 p_{e_1}^2, p_{e_1}^1 + p_{e_1}^2 - p_{b_1}^1 p_{b_1}^2, p_e^1 + p_e^2 - p_b^1 p_b^2\}.
\end{aligned}$$

Если зависимость между параметрами имеет вид:

$$\tilde{y}_i = p_1 + p_2 + p_3 - p_1p_2 - p_1p_3 - p_2p_3 + p_1p_2p_3, \quad (11)$$

где p_1, p_2, p_3 - лингвистические переменные, то нечеткая оценка $\tilde{y}_i$ определяется соотношением (9), в котором

$$y_i' = \{p_b^1 + p_b^2 + p_b^3 + p_b^1p_b^2p_b^3 - p_e^1p_e^2 - p_e^1p_e^3 - p_e^2p_e^3,$$
$$p_{b_1}^1 + p_{b_1}^2 + p_{b_1}^3 + p_{b_1}^1p_{b_1}^2p_{b_1}^3 - p_{e_1}^1p_{e_1}^2 - p_{e_1}^1p_{e_1}^3 - p_{e_1}^2p_{e_1}^3,$$
$$p_{e_1}^1 + p_{e_1}^2 + p_{e_1}^3 + p_{e_1}^1p_{e_1}^2p_{e_1}^3 - p_{b_1}^1p_{b_1}^2 - p_{b_1}^1p_{b_1}^3 - p_{b_1}^2p_{b_1}^3,$$
$$p_e^1 + p_e^2 + p_e^3 + p_e^1p_e^2p_e^3 - p_b^1p_b^2 - p_b^1p_b^3 - p_b^2p_b^3\}.$$

Введем переменные, которые будем использовать при расчете степеней истинности в диаграммах Coras [9, 10].

1. Переменные, используемые при анализе рисков Coras

Переменные	Описание
p	Степень истинности
T	Угроза
E	Сценарий угрозы/Нежелательный инцидент
$t \to e$	Отношение инициации
$e_1 \to e_2$	Отношение следствия
e(d)	Сценарий угрозы/Нежелательный инцидент *e(d),* где $d \in \Delta^I$, Δ^I – непустое множество предметной области
$t \xrightarrow{p} e$	Угроза t инициирует сценарий угрозы e со степенью истинности p
$e_1 \xrightarrow{p} e_2$	Сценарий угрозы e_1 приводит к сценарию угрозы e_2 со степенью истинности p

Отношение инициализации. Введем правило, которое позволит определять степень истинности инициализации $Initiate(t,e)$ сценария угрозы или нежелательного инцидента e, по отношению к некоторой угрозе.

Предположим, что у нас есть описание предметной области в виде предложений: $< Risk\_Value(p)\ \mu >, < hasRiskValue(t,p) >$, где p – лингвистическое описание значения риска; μ – степень истинности p; t – угроза. Отсюда следует:

$$< Risk\_Value(p)\ \mu >,$$
$$Initiate(t,e) \Leftrightarrow Initiate\_Link(l),$$
$$< hasRiskValue(l,p) >.$$

Таким образом, степень истинности возникновения отношения инициализации сценария/инцидента ***e*** по отношению к угрозе t равно степени, с которой возникает угроза t .

Отношение следования. Для сценариев/инцидентов e_1 и e_2, для которых справедливо отношение следования $Leads\_to(e_1,e_2)$, имеем:

$$< Risk\_Value(p_1)\ \mu_1 >, < hasRiskValue(e_1,p_1) >,$$
$$< Risk\_Value(p_2)\ \mu_2 >, < hasRiskValue(e_2,p_2) >.$$

Для описания значения риска отношения следования $Leads\_to(e_1,e_2)$ введем следующий набор предложений:

$$Leads\_to(e_1,e_2) \Leftrightarrow Leads\_to\_Link(l\ ),$$
$$< Risk\_Value(p\ )\mu\ >, < hasRiskValue(l\ ,p\ ) >.$$

Для оценки результирующей лингвистической переменной описывающей отношение следования $Leads\_to(e_1,e_2)$ используется формула (9), в которой @ является операцией произведения. Степень истинности результата при этом определяется по формуле: $\mu = \min(\mu_1, \mu_2)$.

Взаимоисключающие инциденты. Для двух взаимоисключающих друг друга инцидентов/сценариев e_1 и e_2 будет истинно следующее утверждение:

$$< Risk\_Value(p_1)\ \mu_1 >, < hasRiskValue(e_1,p_1) >$$
$$< Risk\_Value(p_2)\ \mu_2 >, < hasRiskValue(e_2,p_2) >$$

Для оценки результирующей лингвистической переменной можно использовать формулу (9). Данная модель позволяет определить лингвистический терм соответствующий лингвистической переменной результата. Степень истинности результата при этом определяется по формуле: $\mu = \min(\mu_1, \mu_2)$.

Независимые инциденты/сценарии. Если сценарии/инциденты e_1 и e_2 являются независимыми, то имеем:

$$< Risk\_Value(p_1)\ \mu_1 >, < hasRiskValue(e_1,p_1) >,$$
$$< Risk\_Value(p_2)\ \mu_2 >, < hasRiskValue(e_2,p_2) >.$$

Для оценки результирующей лингвистической переменной можно использовать зависимость (10). Данная модель позволяет определить лингвистический терм, соответствующий лингвистической переменной результата. Степень истинности результата при этом определяется по формуле: $\mu = \max(\mu_1, \mu_2)$.

Пример. Рассмотрим нежелательный инцидент *UI* – нарушение целостности контролера сетевого устройства. Инцидент может быть вызван либо причинами изнутри системы или за счет внешнего воздействия на систему. Для построения диаграммы рисков в соответствии с Coras введем в рассмотрение следующие угрозы: Th1 – отказ в контролере сетевого устройства, Th2 – физическое воздействие, Th3 – максимальная нагрузка на контролер сетевого устройства, Th4 – изменение выходной мощности устройства, Th5 – изменение мощности при передаче сообщения, Th6 – помехи, действующие на среду передачи.

Введены следующие сценарии угрозы, которые будут использоваться: физическое или конструктивное воздействие (сценарий угрозы ThS1), перегрузка сетевого устройства (сценарий угрозы ThS2), воздействие изнутри системы (сценарий угрозы ThS3), электрическое воздействие на систему (сценарий угрозы ThS4), внешнее воздействие на систему (сценарий угрозы ThS5).

Диаграмма рисков Coras, соответствующая описываемому случаю, представлена на рис. 1.

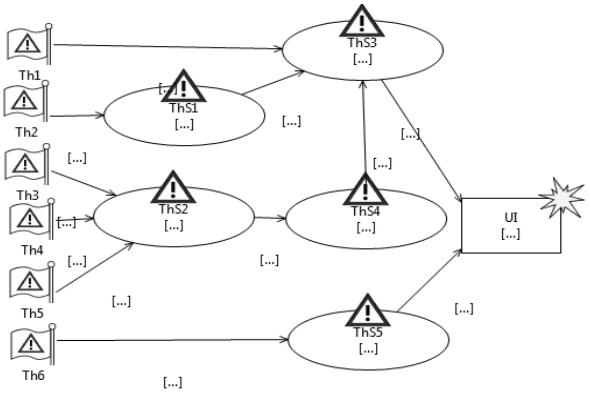


Рис. 1. Диаграмма рисков Coras

Приведем нечеткую базу знаний, которая создается для анализа рисков в изучаемом случае.

Для описания значения риска угроз $Th_i, i = \overline{1,6}$ введем предложение:

$$< Risk\_Value(p_i)\ \mu_i >,$$
$$< hasRiskValue(Th_i, p_i) >, i = \overline{1,6}.$$

Для описания значения риска отношения инициации введем предложения:

$$Initiate(Th_1, ThS_3) \Leftrightarrow Initiate\_Link(l_1),$$
$$< hasRiskValue(l_1, p_1) >,$$
$$< Risk\_Value(p_1)\ \mu_1 >,$$
$$Initiate(Th_2, ThS_1) \Leftrightarrow Initiate\_Link(l_2),$$
$$< hasRiskValue(l_2, p_2) >,$$
$$< Risk\_Value(p_2)\ \mu_2 >,$$
$$Initiate(Th_3, ThS_2) \Leftrightarrow Initiate\_Link(l_3),$$
$$< hasRiskValue(l_3, p_3) >,$$
$$< Risk\_Value(p_3)\ \mu_3 >,$$
$$Initiate(Th_4, ThS_2) \Leftrightarrow Initiate\_Link(l_4),$$
$$< hasRiskValue(l_4, p_4) >,$$
$$< Risk\_Value(p_4)\ \mu_4 >,$$
$$Initiate(Th_5, ThS_2) \Leftrightarrow Initiate\_Link(l_5),$$
$$< hasRiskValue(l_5, p_5) >,$$
$$< Risk\_Value(p_5)\ \mu_5 >,$$
$$Initiate(Th_6, ThS_5) \Leftrightarrow Initiate\_Link(l_6),$$
$$< hasRiskValue(l_6, p_6) >,$$
$$< Risk\_Value(p_6)\ \mu_6 >.$$

Для описания значения риска сценария угрозы ThS_1 введем предложение

$$< Risk\_Value(p_1)\mu_2 >,$$
$$< hasRiskValue(ThS_1, p_1) >.$$

По аналогии введем предложения для описания всех сценариев угроз представленных на рис. 1:

$$< Risk\_Value(p_6, \mu_6 >,$$
$$< hasRiskValue(ThS_5, p_6) >,$$
$$< Risk\_Value(q_1)\mu_{ThS_2} >,$$
$$< hasRiskValue(ThS_2, q_1) >,$$

где q_1 вычисляется с использованием формулы (10), а значение μ_{ThS_2} определяется формулой $\mu_{ThS_2} = \max(\mu_3, \mu_4, \mu_5)$.

Для описания значения риска сценария угрозы ThS_4 введем предложение

$$< Risk\_Value(q_2)\mu_{ThS_4} >,$$
$$< hasRiskValue(ThS_4, q_2) >,$$

где q_2 вычисляется с использованием формулы (8), в которой @ является операцией произведения, а значение μ_{ThS_4} определяется формулой $\mu_{ThS_4} = \min(\mu_{ThS_2}, \mu_8)$.

Для описания значения риска сценария угрозы ThS_3 введем предложение

$$< Risk\_Value(q_3)\mu_{ThS_3} >,$$
$$< hasRiskValue(ThS_3, q_3) >,$$

где q_3 вычисляется с использованием формулы (10), а значение μ_{ThS_3} определяется формулой $\mu_{ThS_3} = \max(\mu_1, \mu_7, \mu_9)$.

Для описания значения риска отношения следования

$$Leads\_to(ThS_1, ThS_3),$$
$$Leads\_to(ThS_2, ThS_4),$$
$$Leads\_to(ThS_4, ThS_3),$$
$$Leads\_to(ThS_3, UI),$$
$$Leads\_to(ThS_5, UI),$$

введем предложения

$$Leads\_to(ThS_1, ThS_3) \Leftrightarrow Leads\_to\_Link(l_8),$$
$$< Risk\_Value(p_7)\mu_7 >, < hasRiskValue(l_8, p_7) >,$$
$$Leads\_to(ThS_2, ThS_4) \Leftrightarrow Leads\_to\_Link(l_7),$$
$$< Risk\_Value(p_8)\mu_8 >, < hasRiskValue(l_7, p_8) >,$$
$$Leads\_to(ThS_4, ThS_3) \Leftrightarrow Leads\_to\_Link(l_9),$$
$$< Risk\_Value(p_9)\mu_9 >, < hasRiskValue(l_9, p_9) >,$$
$$Leads\_to(ThS_3, UI) \Leftrightarrow Leads\_to\_Link(l_{10}),$$
$$< Risk\_Value(p_{10})\mu_{10} >, < hasRiskValue(l_{10}, p_{10}) >,$$
$$Leads\_to(ThS_5, UI) \Leftrightarrow Leads\_to\_Link(l_{11}),$$
$$< Risk\_Value(p_{11})\mu_{11} >,$$
$$< hasRiskValue(l_{11}, p_{11}) >.$$

Для описания значения степени риска нежелательного инцидента UI введем предложение

$$< Risk\_Value(q_4)\mu_{UI} >,$$
$$< hasRiskValue(UI, q_4) >,$$

где $q_4 = q_3 p_{10} + p_6 p_{11}$, а значение μ_{UI} определяется формулой

$$\mu_{UI} = \max(\min(\mu_{10}, \mu_{ThS_3}), \min(\mu_{11}, \mu_6)).$$

Вывод. Рассмотрена возможность построения базы знаний с использованием аппарата нечетких множеств и ПОСП для формализации нечеткостей при оценке рисков в вычислительной системе. Введены модели, которые позволяют решать задачи формализации оценки рисков. Определены правила, позволяющие формировать нечеткую базу знаний по исходным диаграммам Coras. Приведен пример использования данной методики для формализации рисков в вычислительных системах.

Список использованной литературы

1. Копытчук Н. Б. Разработка формализованного языка анализа рисков на основе дескрипционной логики. / Н. Б. Копытчук, П. М. Тишин, К. В. Ботнарь, М. В. Цюрупа // Электротехнические и компьютерные системы. – К. : – 2011. – № 02(78). – С. 103 – 108.

2. Копытчук Н. Б. Применение нечеткой дескрипционной логики при разработке формализованного языка анализа рисков / Н. Б. Копытчук, П. М. Тишин, К. В. Ботнарь, М. В. Цюрупа // Электротехнические и компьютерные системы. – К. : – 2011. – № 04(80). – С. 168 – 176.

3. Копытчук Н. Б. Анализ вычислительных сетей с помощью многоуровневой онтологии оценки рисков с применением методологии CORAS / Н. Б. Копытчук, П. М. Тишин, К. В. Ботнарь, М. В. Цюрупа // Электротехнические и компьютерные системы, – К. : – 2013. – № 10(86) – С. 120 – 126.

4. Копытчук Н. Б. Создание нечетких баз знаний при анализе рисков в диаграммах Coras / Н. Б. Копытчук, П. М. Тишин, М. В. Цюрупа // Материалы Второй Международной научно-технической конференции «Вычислительный интелект (СИ – 2013)». – Черкассы : – 2013. – С. 196 – 197.

5. Рыжов А. П. Элементы теории нечетких множеств и ее приложений / А. П. Рыжов. – М. : – Диалог-МГУ. – 2003. – 81 с.

6. Поспелова Д. А. Нечеткие множества в моделях управления и искусственного интеллекта / Д. А. Поспелова – М. : Наука, 1986, 312 с.

7. Дилигенский Н. В. Нечеткое моделирование и многокритериальная оптимизация производственных систем в условиях неопределенности: технология, экономика, экология / Н. В. Дилигенский, Л. Г. Дымова, П. В. Севастьянов. – М. : – Машиностроение − 1. – 2004. – 397 с.

8. Тишин П. М. Нечеткие модели сетей связи / П. М. Тишин, К. В. Ботнарь // Холодильная техника и технология. – Одесса : 2009. – № 8. – С. 60 – 67.

9. Lund M.S., Solhaug B., and Stølen K., (2011), Model-driven Risk Analysis. The CORAS Approach, Springer, 476 p.

10. Lund M.S., Solhaug B., and Stølen K., (2011), Risk Analysis of Changing and Evolving Systems Using CORAS. *Foundations of Security Analysis and Design VI (FOSAD'11), number 6858 in Lecture Notes in Computer Science,* Springer, pp. 231 – 274

11. Dahl H.E.I., (2008), The CORAS Method for Security Risk Analysis. *Tutorial Presentation at 7th Estonian Summer School on Computer and Systems Science in Cooperation with the Nordic Network On Dependable Systems (NODES),* Otepää, Estonia, pp. 24 – 29.

12. Mayer N., Heymans P., and Matulevicius R., (2007), Design of a Modelling Language for Information System Security Risk Management. *In: Proceedings of the First International Conference on Research Challenges in Information Science*, *RCIS,* pp. 121 – 132.

13. International Electrotechnical Commission: IEC 61025 Fault Tree Analysis (FTA), (1990).

14. International Electrotechnical Commission: *IEC 60300-3-9 Dependability management,* (1995), Part 3: Application Guide – Section 9: Risk Analysis of Technological Systems – *Event Tree Analysis (ETA)*.

15. Zadeh L.A. Fuzzy Sets. Information and Control, 1965, Vol..8, pp. 338 – 353.

Получено 16.02.2014

References

1. Kopytchuk N. B., Tishin P. M., Botnar' K.V., and Cjurupa M.V. Razrabotka formalizovan-nogo jazyka analiza riskov na osnove deskripcionnoj logiki. [Develop a Formalized Language of Risk Analysis Based Deskriptsionnoy Logic], (2011), *Publ. in the Journal Elektrotehnic and Compputer Systems,* Kiev, Ukraine, No. 2(78), pp. 103 –108 (In Russian).

2. Kopytchuk N. B., Tishin P. M., Botnar' K. V., and Cjurupa M. V. Primenenie nechetkoj deskripcionnoj logiki pri razrabotke formalizovannogo jazyka analiza riskov [Application of fFuzzy Logic in the Development Deskriptsionnoy Formalized Language of Risk Analysis], (2011), *Publ. in the Journal Elektrotehnic and Compputer Systems,* Kiev, Ukraine, No. 4(80), pp 168 – 176 (In Russian).

3. Kopytchuk N.B., Tishin P.M., Botnar' K.V., and Cjurupa M.V. Analiz vychislitel'nyh setej s pomoshh'ju mnogourovnevoj ontologii ocenki riskov s primeneniem metodologii CORAS [Analysis of Computer Networks Using a Multi-level Ontology of Risk Assessment Methodology Using CORAS], (2013), *Publ. in the Journal Elektrotehnic and Compputer Systems,* Kiev, Ukraine, No. 10(86), pp. 120 – 126 (In Russian).

4. Kopytchuk N.B., Tishin P.M., and Cjurupa M.V. Sozdanie nechetkih baz znanij pri analize riskov v diagrammah Coras, [Creating Fuzzy Knowledge Bases in Risk Analysis Diagrams CORAS], (2013), *Materialy Vtoroj Mezhdunarodnoj Nauchno-tehnicheskoj Konferencii "Vychislitel'nyj Intelekt* (SI–2013)", Cherkassy, Ukraine, pp. 196 – 197 (in Russian).

5. Ryzhov A.P. Jelementy teorii nechetkih mnozhestv i ee prilozhenij. [Elements of the theory of Fuzzy Sets and its Applications], (1998), *Dialog–Moskovskij Gosudarstvennyj Universitet*, Moskva, Russian Federation, 81 p. (In Russian).

6. Pospelov D.A. Nechetkie mnozhestva v modeljah upravlenija i iskusstvennogo intellekta. [Fuzzy Sets in Management Models and Artificial Intelligence], (1986), *Nauka Publ.,* Moskva, Russian Federation, 312 p. (In Russian).

7. Diligenskij N.V., and Dymova L.G., Sevast'janov P.V. Nechetkoe modelirovanie i mnogokriterial'naja optimizacija proizvodstvennyh sistem v uslovijah neopredelennosti: tehnologija, jekonomika, jekologija [Fuzzy Modeling and Multi-criteria Optimization of Production Systems under Uncertainty: Technology, Economy, Ecology], (2004), Moskva, Russian Federation, *Publ. Izdatel'stvo Mashinostroenie,* 397 p. (In Russian).

8. Tishin P.M., Botnar' K.V. Nechetkie modeli setej svjazi [Fuzzy Models of Communication Networks], (2009), Odessa, Ukraine, *Odesskaja Gosudarstvennaja Akademija Holoda,* No. 8, pp. 60 – 67 (In Russian).

9. Lund, M.S., Solhaug, B., Stølen, K.: Model-driven Risk Analysis. The CORAS Approach, Springer, (2011), 476 p. [In English].

10. Lund M.S., Solhaug B., and Stølen K. Risk Analysis of Changing and Evolving Systems using CORAS, (2011), *Foundations of Security Analysis and Design VI (FOSAD'11), Number 6858 in Lecture Notes in Computer Science,* Springer, pp. 231 – 274 [In English].

11. Dahl H.E.I. The CORAS Method for Security Risk Analysis, (2008), *Tutorial Presentation at 7th Estonian Summer School on Computer and Systems Science in Cooperation with the Nordic Network On Dependable Systems (NODES)*, Otepää, Estonia, pp. 24 – 29 [In English].

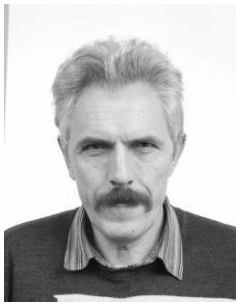
12. Mayer N., Heymans P., and Matulevicius R. (2007), Design of a Modelling Language for Information System Security Risk Management. *In: Proceedings of the First International Conference on Research Challenges in Information Science, RCIS 2007,* pp 121 – 132 [In English].

13. International Electrotechnical Commission: IEC 61025, (1990), *Fault Tree Analysis (FTA)* [In English].

14. International Electrotechnical Commission: *IEC 60300-3-9 Dependability Management,* Part 3: Application guide, Section 9: Risk Analysis of Technological Systems, (1995), *Event Tree Analysis (ETA)* [In English].

15. Zadeh L.A. Fuzzy Sets. Information and Control, (1965), Vol. 8, pp. 338 – 353 [In English].

Копытчук
Николай Борисович,
д.т.н., проф. каф. компьютерных интеллектуальных систем и сетей Одесского нац. политехн. ун-та.
Тел.: 067-4861023.
E-mail: knb47@mail.ru



Тишин Петр
Металинович, канд. физико-математических наук, доц. каф. компьютерных интеллектуальных систем и сетей Одесского нац. политехн. ун-та.
Тел.: 098-8050448.
E-mail: tik88@mail.ru

Цюрупа
Марат Владимирович,
аспирант каф. компьютерных интеллектуальных систем и сетей Одесского нац. политехн. ун-та.
Тел.: 093-6454288.
E-mail:
frostlans@gmail.com