УДК 681.323

А.А. Замула[1], Б.В. Волобуев[1], В.И. Черныш[1], Ю.В. Землянко[2]

[1]*Харьковский национальный университет радиоэлектроники, Харьков*
[2]*Харьковский государственный университет питания и торговли*

МЕТОДОЛОГИЯ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОЕКТИРОВАНИИ ИНФОРМАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКИХ СЕТЕЙ

Рассматриваются вопросы, связанные с методологией анализа рисков информационной безопасности при проектировании информационных систем с использованием нечетких сетей, а также алгоритмы прямого и обратного выводов. Рассматривается процесс нечеткого моделирования базы правил.

Ключевые слова: *информационная система, информационная безопасность, риски информационной безопасности.*

Введение

Актуальность проблемы и анализ публикаций. Проект создания и внедрения информационной системы (ИС) реализуется в условиях существенной неопределенности, которая проявляется в виде неполноты или неточности информации об условиях реализации системы. Неопределенность сопутствует всем этапам каскадной модели жизненного цикла ИС. Каскадная модель жизненного цикла ИС включает ряд этапов: сбор информации; анализ; проектирование; реализация; внедрение; сопровождение.

На первом этапе проекта ИС определяются цели и формулируются требования, которые могут быть неполными, неточными и подвержены изменениям в процессе проектирования системы. На этапе анализа неопределенность связана с принимаемыми решениями по архитектуре системы и её структуре в целом. Этап проектирования связан с неопределенностью в обеспечении как функциональности системы, так и нефункциональных характеристик качества, таких как производительность, надежность, доступность, целостность, адаптируемость, интегрируемость.

Этап реализации характеризуется неопределенностью в возможности отображения исполняемых компонентов системы на узлы модели размещения, при реализации классов и подсистем проектирования. Этап внедрения ИС связан с неопределенностью качества развертывания системы, уровнем подготовки пользователей и влиянием внедрения разработанной ИС на бизнес-процессы организации.

Неопределенность, сопутствующая процессу проектирования информационной системы, может привести к созданию неблагоприятных ситуаций, которые будут препятствовать достижению поставленных целей в процессе проектирования ИС. Возможность проявления неблагоприятных ситуаций в проекте создания ИС характеризуется риском.

Процесс управления рисками предполагает их идентификацию, количественную и/или качественную оценку, разработку откликов на риски и их контроль [1].

Современные подходы к проектированию ИС основываются на объектно-ориентированных технологиях, базирующихся на итерационном и инкрементном подходе. Процесс проектирования ИС разбивается на этапы в соответствии с фазами жизненного цикла (ЖЦ) ИС. Каждая фаза ЖЦ состоит из нескольких итераций, в результате формируется инкремент, который является итогом завершенной итерации и представляет собой версию системы, содержащую добавленные или улучшенные функциональные возможности по сравнению с предыдущей версией. Риски оцениваются для каждой итерации и фазы проектирования системы. Управление рисками должно осуществляться на каждой итерации. Итерационный подход обеспечивает идентификацию, оценку и снижение рисков в ходе итераций на каждых фазах ЖЦ информационной системы, что обеспечивает снижение риска по проекту в целом.

Создание эффективной системы управления рисками проектов информационных систем предполагает распространение её сферы влияния на все фазы и все итерации жизненного цикла ИС. Анализ возникающих рисков должен проводиться регулярно в процессе создания ИС. Риски должны идентифицироваться, оцениваться и на основе оценки выявляться приоритеты рисков для текущей итерации процесса создания системы.

Оценка влияния риска на проект для конкретной фазы жизненного цикла информационной системы и конкретной итерации проекта может быть количественной и качественной. Количественные оценки базируются на имеющейся статистической информации и используемых моделях прогноза. При этом задача состоит в количественной оценке риска относительно других, имеющихся рисков, и прогнозе влияния конкретного риска на проект информационной системы.

Качественная оценка риска, как правило, базируется на экспертных оценках.

Недостатком существующих подходов к анализу рисков является отсутствие единой методологической основы, позволяющей интегрировать как качественные, так и количественные подходы к оценке рисков.

Повышение эффективности управления рисками проектов создания и развития информационных систем может быть осуществлено путем формализации и автоматизации различных этапов управления рисками. Решение данной задачи можно осуществить путем разработки методологических основ системы принятия решений для управления рисками проектов ИС, базирующихся на современных методах обработки информации в условиях существенной неопределенности, позволяющих осуществлять анализ и принимать эффективные решения на базе моделей, интегрирующих как количественные, так и качественные факторы, в чем и состоит **цель** статьи.

Основная часть

Вероятностный подход и нечеткие сети. Учет неопределенности в известных моделях управления риском осуществляется в основном с помощью вероятностных конструкций. Вероятностный подход базируется на статистической обработке данных по реализованным проектам. В большинстве случаев получение статистически значимых оценок видов законов распределения случайных величин и процессов, а также их характеристик является проблематичным из-за недостаточных объемов выборки. Кроме того, объединение в одной модели количественных и качественных факторов представляет значительную трудность.

Разрешение противоречий существующим моделям управления рисками проектов ИС может быть получено путем применения нечетких моделей [2], применение которых эффективно, когда имеет место: недостаточность или неопределенность знаний об исследуемой системе или процессе; получение требуемой информации сопряжено с различными трудностями или вообще невозможно; основная часть информации получена на основе экспертных данных или эмпирических описаний процессов; параметры и входные данные не являются точными и корректно представленными.

Для моделирования рисков ИС нечеткие модели целесообразно представлять в виде нечетких сетей, элементы и совокупности элементов которых реализуют различные компоненты нечетких моделей и этапы нечеткого вывода.

Нечеткая продукционная модель (НПМ) может быть представлена следующим образом [3]:

$$(i): Q; P; A \Rightarrow B : S; F; N, \qquad (1)$$

где (i) – обозначение правила нечеткой продукции, которая характеризует предметную область нечеткой модели;

Q – сфера применения нечеткой продукции, которая характеризует предметную область нечеткой модели;

P – условие применения (активизация) ядра нечеткой продукции;

$A \Rightarrow B$ – ядро нечеткой продукции; A - условие ядра (антецедент);

B – заключение ядра (консеквент);

$\Rightarrow$ – знак логической секвенции (следования);

S – метод или способ определения количественного значения степени истинности заключения ядра, который определяет алгоритм нечеткого вывода в продукционной нечеткой модели;

F – коэффициент определенности или уверенности нечеткой продукции, который определен на интервале [0,1] и соответствует весовому коэффициенту нечеткого продукционного правила;

N – постусловие продукционного правила, которое определяет действия и процедуры, выполняемые в случае реализации ядра продукции.

Если A и B – некоторые выражения нечеткой логики, то ядро нечеткой продукции $A \Rightarrow B$ можно записать в следующем виде:

ЕСЛИ A, **ТО** B, (2)

где A – условие или предпосылка (антецедент);

B – заключение (консеквент).

Для использования нечеткого правила (2) необходимо определить алгоритм, который на основе антецедента A с известной степенью истинности, являющейся условиям нечетких правил продукции, позволяет оценить степень истинности консеквента B, являющегося заключением соответствующих нечетких правил продукции.

В общем случае взаимосвязь между антецедентом и консеквентом в (2) представляет собой бинарное нечеткое отношение на декартовом произведении соответствующих нечетких множеств. Если в правиле (2) нечеткое причинноследственное отношение между антецедентом A и консеквентом B задается в виде нечеткой импликации $R: A \to B$, то оно может быть представлено в виде нечеткой продукции:

ЕСЛИ x есть A, **ТО** y есть B, (3)

где x – входная переменная, $x \in X$;

X – область определения антецедента нечеткого правила;

A – нечеткое множество, определенное на X;

$\mu_A(x) \in [0,1]$ – функция принадлежности нечеткого множества A;

y – выходная переменная, $y \in Y$;

Y – область определения консеквента нечеткого правила;

B – нечеткое множество, определенное на Y;

$\mu_B(y) \in [0,1]$ – функция принадлежности нечетного множества B.

При условии, что известна функция принадлежности нечетного множества $A - \mu_A(x)$ и нечеткое бинарное отношение $R \subseteq X \times Y$, отображающее импликацию $A \to B$ имеет функцию принадлежности $\mu_R(x,y)$, тогда для нечеткого множества функция принадлежности определяется по правилу композиции как

$$\mu_B(y) = \sup\{T(\mu_A(x), \mu_R(x,y))\}, \qquad (4)$$

где sup – операция определения верхней границы множества элементов;

T – T - нормы.

Прямой и обратный выводы. Основными способами нечеткого вывода заключений в НПМ являются прямой и обратный вывод. Прямой вывод основывается на правиле вывода "нечеткий модус поненс" (fuzzy modus ponens). В общем случае правило вывода нечеткий модус поненс состоит из последовательности следующих шагов.

Шаг 1. Задание нечеткой импликации $R: A \to B$, которая определяет нечеткое причинно - следственное отношение между антецедентом A и консеквентом B, представляемое в виде (3). Для моделирования рисков проектов создания и внедрения информационных систем в качестве правила вычисления нечеткой импликации целесообразно использовать классическую нечеткую импликацию Л. Заде:

$$\mu_R(x,y) - \max\{\min[\mu_A(x), \mu_B(y)], \quad [1 - \mu_A(x)]\}.$$

Шаг 2. Задание антецедента A в виде:

$$x' \text{ есть } A', \qquad (5)$$

где x' – фактическое значение переменной x;

A' – нечеткое множество, $A' \subseteq X, x' \in X$, функция принадлежности нечеткого множества A':

$$\mu_{A'}(x) \in [1,0].$$

Нечеткое множество A' в (5) является производным от нечеткого множества A и может принимать следующие значения: $A' = A$; $A' =$ "очень A", причем

$\mu_{A'}(x) = = \mu_{CON(A)}(x) = (\mu_{A'}(x))$; $A' =$ "почти A", причем

$\mu_{A'}(x) = = \mu_{DIL(A)}(x) = (\mu_A(x))^{0,5}$; $A' =$ "не A", причем

$$\mu_{A'}(x) = = \mu_{\bar{A}}(x) = 1 - \mu_A(x).$$

Шаг 3. Формирование вывода, то есть консеквента B в виде:

$$y' \text{ есть } B', \qquad (6)$$

где y' – фактическое значение переменной y;

B' – нечеткое множество, $B' \subseteq Y, y' \in Y$;

$\mu_{B'}(y) \in [1,0]$ – функция принадлежности нечеткого множества B'.

Нечеткое множество B' является результатом нечеткого вывода и определяется посредством применения операции композиции (4). Для моделирования рисков проектов ИС в качестве композиционного правила нечеткого логического вывода целесообразно использовать max– min - композицию следующего вида:

$$\mu_B(y) = \max_{x \in X}\{\min(\mu_A(x), \mu_R(x,y))\}. \qquad (7)$$

Композиционное правило обладает свойствами ассоциативности и дистрибутивности относительно операции max, что является важным для задач моделирования.

При построении нечеткой модели рисков проектов ИС в качестве входных переменных используются как количественные, так и качественные факторы. Интегральный учет их возможен при использовании лингвистических переменных. Для этого в продукционных моделях нечеткого вывода применяют нечеткие лингвистические высказывания [3]:

1) "β есть α_i", где β – наименование лингвистической переменной, α_i - наименование нечеткой переменной базового терм-множества $T = \{\alpha_1, \alpha_2, ...\alpha_i, ..., \alpha_n\}$ переменной β, с областью определения на множестве X_i и функцией принадлежности $\mu_{\alpha_i}(x) \in [0,1]$;

2) "β есть $\theta(\alpha)$", где $\theta(\alpha)$ – лингвистические отношения, задаваемые некоторыми синтаксическими процедурами (нечеткие логические операции "И", "ИЛИ", а также нечетких модификаторов "очень", "почти", "не").

Правила формирования вывода для оценки риска и реализация процесса нечеткого моделирования базы правил.

Пример 1. Для формирования правила оценки риска, связанного с объемом проекта ИТ, в качестве входной лингвистической переменной (x_1) используется лингвистическая переменная – "сложность проекта", которая имеет следующие терм – множество:

T1 = {"небольшая", "средняя", "большая"}.

Другой лингвистической переменной (x_2) является – "бюджет проекта" с терм – множеством:

T2 = {"малый", "средний", "значительный"}.

Выходной переменной (y) является лингвистическая переменная "риск объема проекта", которая имеет следующее терм – множество:

T2 = {"низкий", "средний", "высокий"}.

Для модели оценки риска проекта ИС сформированы следующие правила вывода:

П1:**ЕСЛИ** сложность проекта небольшая,
ТО риск объема проекта низкий.
П2: **ЕСЛИ** сложность проекта средняя **И** бюджет проекта малый,
ТО риск объема проекта средний.
ИЛИ высокий
П3: **ЕСЛИ** сложность проекта **очень** высока **И** бюджет проекта **НЕ** значительный,
ТО риск объема проекта высокий.

При построении нечеткой модели оценки рисков проектов ИС необходимо сформировать полное пространство предпосылок $X = \{x_i\}, i = \overline{1,n}$ факторов, являющихся источниками риска, и полное пространство заключений $Y = \{y_j\}, i = \overline{1,m}$ показателей риска различных областей проекта. Для нечетких продукционных правил необходимо задать функции принадлежности нечетких множеств, характеризующих терм – множества лингвистических переменных. В нечеткой модели оценки рисков проектов ИС в качестве функций принадлежности вполне допустимо использовать типовые L-R – функции треугольного и трапецеидального типов [4], определенные на 01 – носителе, конкретный вид которых определяется значениями параметров их аналитического представления и может уточнятся в соответствии с экспериментальными данными.

Сформированная база правил нечеткой модели оценки риска проектов ИС на основе эмпирических гипотез (информации от экспертов) может быть модифицирована с учетом реальных условий ведения проектов организациями. Правила могут быть добавлены, удалены или изменены.

Пример 2. Рассмотрим реализацию процесса нечеткого моделирования базы правил. Моделирование проведем с использованием специализированного пакета Fuzzy Logic Toolbox средства MATLAB [5]. Выполнение нечеткого вывода будем реализовывать на основе алгоритма Мамдани.

Шаг 1. Фазификация – введение нечеткости. На этом шаге необходимо задать функции принадлежности для терм – множеств входных и выходных лингвистических переменных: input1 – в модели соответствует лингвистической переменной "Цель проекта" – x_1; input2 – в модели соответствует лингвистической переменной "Соответствие цели проекта" – x_2; output1 – в модели соответствует лингвистической переменной "Соответствие цели проекта" – y_1.

Для входной переменной input1терм – множество состоит из трех термов T = {Низкий (H), Средний (C), Высокий (B)}, которые характеризуют низкое, среднее и высокое соответствие проекта бизнес-целям. Функции принадлежности для входной переменной input1 являются треугольными. В общем случае треугольная функция принадлежности имеет следующий вид:

$$\mu_\Delta(x,a,b,c) = \begin{cases} 0, & x \le a \\ \dfrac{x-a}{b-a}, & a \le x \le b \\ \dfrac{c-x}{c-b}, & b \le x \le c \\ 0, & c \le x \end{cases}, \qquad (8)$$

где a, b, c – числовые параметры, характеризующие основание треугольника (a, c) и его вершину (b), причем должно выполняться следующее условие $a \le b \le c$.

С учетом (8) функции принадлежности нечетких терм – множеств лингвистической переменной "Цель проекта" будут иметь следующий вид:

$$\mu_\Delta^H(x, 0, 0, 0.5), \ \mu_\Delta = (x, 0.5, 1.0),$$

$$\mu_\Delta^B(x, 0.5, 1.0, 1.0).$$

Для входной переменной input2 терм – множество состоит из трех термов T = {H,C,B}, функции принадлежности которых являются трапециевидными. В общем случае трапециевидная функция принадлежности имеет следующий вид:

$$\mu_T(x,a,b,c,d) = \begin{cases} 0, & x \le a \\ \dfrac{x-a}{b-a}, & a \le x \le b \\ 1, & b \le x \le c \\ 0, & d \le x \end{cases}, \qquad (10)$$

где a, b, c, d – числовые параметры, характеризующие нижнее основание трапеции, (a, d) и верхнее (b, c), причем должно выполнятся условие $a \le b \le c \ge d$.

С учетом (9) функции принадлежности нечетких терм – множеств лингвистической переменной "Границы проекта" будут иметь следующий вид:

$$\mu_T^H(x, 0, 0, 0.1, 0, 4), \ \mu_\Delta^C(x, 0, 15, 0.4, 0.6, 0, 85),$$

$$\mu_\Delta^B(x, 0.65, 0.9, 1.0, 1.0).$$

Для выходной переменной output1 (лингвистическая переменная "Соответствие цели проекта") терм – множество состоит из пяти термов:

– T={Очень низкая очевидность риска (ОНОР);
– низкая очевидность риска (НОР);
– средняя очевидность риска (СОР);
– высокая очевидность риска (ВОР);
– очень высокая очевидность риска (ОВОР)}.

Функции принадлежности лингвистических переменных являются треугольными.

С учетом (8) функции принадлежности нечетких терм – множеств лингвистической переменной "Соответствие цели проекта" будут иметь следующий вид:

$$\mu_{\Delta}^{\text{OHOP}}(x, 0, 0, 0.25),\ \mu_{\Delta}^{\text{HOP}}(x, 0, 0, 25, 0.5),$$
$$\mu_{\Delta}^{\text{COP}}(x, 0, 25, 0.5, 0.75),\ \mu_{\Delta}^{\text{BOP}}(x, 0.5, 0.75, 1.0),$$
$$\mu_{\Delta}^{\text{OBOP}}(x, 0.75, 1.0, 1.0).$$

Шаг 2. Задание нечетких правил.

В алгоритме Мамдани база правил должна задаваться в виде структуры с двумя входами и одним выходом.

В алгоритме Мамдани для агрегирования степени истинности предпосылок используем Т – норму min-конъюнкция:

$$T(\mu_A(x), \mu_B(x)) = \min(\mu_A(x), \mu_B(x)).$$

Определение степени истинности заключений по каждому правилу (импликация) основано на операции min – активизации:

$$\mu_R(x, y) = \min\{\mu_A(x), \mu_B(y)\}.$$

Шаг 3. Аккумулирование заключения по всем правилам проведено с применением операции max-дизъюнкции. При дефазификации использован метод центра тяжести для дискретного множества значений функций принадлежности:

$$y' = \sum_{r=1}^{Y_{max}} y_r \mu_{B'}(y_r) \Big/ \sum_{r=1}^{Y_{max}} \mu_{B'}(y_r),$$

где Y_{max} – число элементов в y_r в дискретизированной для вычисления "центра тяжести" области Y.

На рис. 1 приведена поверхность системы нечеткой модели для базы правил.

Вывод

Модель оценки рисков проектов ИС в виде нечеткой продукционной сети содержит 17 баз правил и позволяет проводить качественный анализ рисков проектов, которые несут потенциальные угрозы процессу разработки ИС, а также выявить приоритеты рисков (очень высокий, высокий, средний, низкий, несущественный), которые важны для менеджмента проектов.

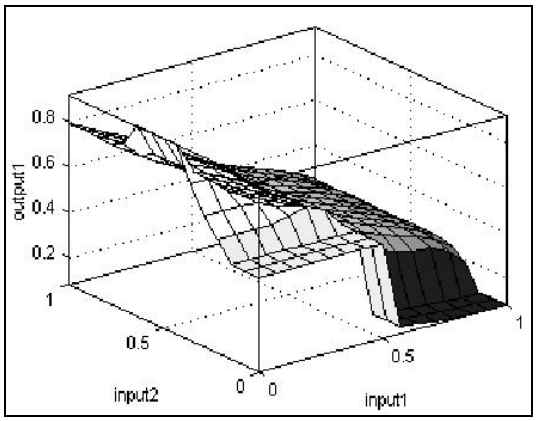

Рис. 1. Поверхность системы нечеткой модели для базы правил

Список литературы

1. Шафер Д.Ф. Управление программными проектами: достижение оптимального качества при минимуме затрат / Д.Ф. Шафер, Р.Т. Фатрел, Л.И. Шафер. – М.: Изд. дом "Вильямс", 2004. – 1136с.

2. Заде Л.А. Понятие лингвистической переменной и его применение к принятию приближенных решений / Л.А. Заде – М.: Мир,1976. – 220 с.

3. Борисов В.В. Нечеткие модели и сети / В.В. Борисов, В.В. Круглов, А.С. Федулов. – М.: Горячая линия – Телеком, 2007. – 284 с.

4. Рыжов А.П. Элементы теории нечетких множеств и измерения нечеткости / Рыжов А.П. – М.: Диалог-МГУ, 1998. – 242 с

5. Леоненков А.В. Нечеткое моделирование в среде MATlAB и fuzzyTECH / Леоненков А.В. – СПб.: БХВ-Петербург, 2005. – 736 с.

Поступила в редколлегию 22.09.2011

Рецензент: д-р техн. наук проф. В.А. Краснобаев, Харьковский национальный технический университет сельского хозяйства им. П. Василенко, Харьков.

МЕТОДОЛОГІЯ АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ПРОЕКТУВАННІ ІНФОРМАЦІЙНИХ СИСТЕМ ІЗ ВИКОРИСТАННЯМ НЕЧІТКИХ МЕРЕЖ

О.А. Замула, Б.В. Волобуєв, В.І. Черниш, Ю.В. Землянко

Розглядаються питання, пов'язані з методологією аналізу ризиків інформаційної безпеки при проектуванні інформаційних систем із використанням нечітких мереж, а також алгоритми прямого та зворотного висновків. Розглядається процес нечіткого моделювання бази правил.

Ключові слова: *інформаційна система,інформаційна безпека, ризики інформаційної безпеки.*

METHODOLOGY ANALYSIS OF RISK INFORMATION SECURITY FOR THE DESIGN OF INFORMATION SYSTEMS USING FUZZY NETWORKS

A.A. Zamula, B.V. Volobuiev, V.I. Chernish, Y.V. Zemlyanko

Problems associated with the methodology of the analysis of information security risks in the design of information systems using fuzzy networks, as well as algorithms for forward and revers conclusions. Represented the process of fuzzy modeling framework of rules.

Keywords: *information system, information security, information security risks.*