

УДК 681

## НЕЧЕТКИЕ ЛИНГВИСТИЧЕСКИЕ МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

В. О. Шапорин, к. ф.-м. н. П. М. Тишин, д. т. н. Н. Б. Копытчук,  
к. т. н. Р. О. Шапорин

Одесский национальный политехнический университет

Украина, г. Одесса

shaporin\_onpu@inbox.ru, tik88@mail.ru, knb47@mail.ru, shaporin@ics.opu.ua

*Рассмотрены методы построения моделей рисков вторжений в компьютерные сети в условиях неопределенности с использованием математического аппарата нечеткой логики.*

*Ключевые слова: безопасность компьютерных сетей, нечеткая логика, лингвистические переменные*

Интенсивное развитие информационных систем накопления и передачи данных во всех сферах жизнедеятельности человека обуславливает необходимость обеспечения безопасности, целостности и конфиденциальности как данных, так и систем их обработки.

Основные методы защиты компьютерных сетей и систем от несанкционированного вторжения ориентированы на использование статистических и вероятностных методов реализации [1]. Указанные методы, хотя и позволяют достичь определенной степени защищенности, однако имеют и существенные недостатки:

- сложность описания многообразия возможных вариантов атак;
- зависимость качества идентификации типов атак от квалификации эксперта или группы экспертов;
- сложность обновления шаблонов атак и методов противодействия;

Основная сложность формализации процесса вторжения заключается в произвольном моменте возникновения атаки и произвольном порядке ее протекания. Известные вероятностные методы не всегда способны однозначно описывать параметры подобных процессов, характеризующихся большой степенью неопределенности. Учитывая это, процесс обеспечения защиты сети можно рассматривать как задачу, заданную в условиях неопределенности с нечетким описанием ее параметров.

Чтобы избежать многозначности трактовки семантических значений одного и того же параметра в различных ситуациях, построим полные ортогональные семантические пространства (ПОСП), которые будут служить областями нечетких значений каждого из параметров вне зависимости от рассматриваемой системы.

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

Следует иметь в виду, что для обеспечения принадлежности к ПОСП, параметры множества  $\tilde{D}_i$  должны удовлетворять требованиям соответствующих аксиом [2].

Каждое нечеткое число  $\tilde{p}_i^k \in \tilde{D}_i$  определим через функцию принадлежности следующего вида:

$$\tilde{p}_k^i \Rightarrow \mu_k^i(p'_i) = \begin{cases} 0, & p'_i \leq p_{kb}^i, p'_i \geq p_{ke}^i \\ \frac{p'_i - p_{kb}^i}{p_{kb_1}^i - p_{kb}^i}, & p_{kb}^i < p'_i < p_{kb_1}^i \\ 1, & p_{kb_1}^i \leq p'_i \leq p_{ke_1}^i \\ \frac{p'_i - p_{ke}^i}{p_{ke_1}^i - p_{ke}^i}, & p_{ke_1}^i < p'_i < p_{ke}^i \end{cases}, \quad i = 1..N_p, k = 1..K_i$$

При этом, с учетом  $\mu_1^i \prec_{\tilde{D}_i} \mu_2^i \prec_{\tilde{D}_i} \dots \prec_{\tilde{D}_i} \mu_{K_i}^i$ , где  $\prec_{\tilde{D}_i}$  — отношение строгого порядка на множестве нечетких значений  $i$ -го параметра, должны выполняться следующие условия:

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

$$\begin{cases} p_{1b}^i = p_{1b_1}^i = \min_{D_i}(p_i) \\ p_{Ke}^i = p_{Ke_1}^i = \max_{D_i}(p_i), \end{cases} \quad i = 1..N_p,$$

где  $p'_i$  — некоторое четкое значение  $i$ -го нечеткого 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.

Используя свойства ПОСП для задания лингвистических переменных, соответствующих неопределенным параметрам задачи, можно сформировать базу знаний и нечеткие модели зависимостей выходных параметров от входных. На основании полученных нечетких моделей можно сконструировать нечеткие сети Петри, позволяющие имитировать функционирование рассматриваемых систем с неопределенными параметрами. В работе рассматриваются различные модели атак, которые в формализованном виде вносятся в базу знаний. Это позволяет, изменяя параметры атаки, проводить анализ различных ситуаций осуществления вторжений в соответствии с методологией анализа рисков Coras [3].

Таким образом, разработанные модели оценки рисков вторжений учитывают не только временные параметры, как предлагается в вероятностных подходах, но допускают и неопределенные и нечеткие параметры в процессе моделирования. Задачи оценки выходных параметров предполагается решать с помощью многокритериального нечеткого подхода [4].

#### ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Радько Н. М., Скобелев И. О. – Риск-модели ИТКС при реализации угроз удаленного и непосредственного доступа.— Москва: РадиоСофт, 2010.
2. Рыжов А. П. Элементы теории нечетких множеств и ее приложений.— Москва, 2003.
3. Тишин П. М., Копытчук Н. Б., Ботнарь К. В., Цюрупа М. В. Разработка формализованного языка анализа рисков на основе дескрипционной логики // Электротехнические и компьютерные системы – Одесса: ОНПУ, 2011.— № 78 – С. 103—108.
4. Тишин П. М., Гайворонская Г. С., Ботнарь К. В. Нечеткая многокритериальная оценка проектных решений в многоуровневых иерархических системах // Вісник СНУ ім. В. Даля.— Луганськ : СНУ ім. В. Даля, 2008.— № 8.— С. 210—214.

V. O. Shaporin, P. M. Tishin, R. O. Shaporin, N. B. Kopitchuk  
**Fuzzy linguistic models for network security.**

The paper presents the methods for risk modeling of intrusion into computer networks under uncertainty using mathematical fuzzy logic.

**Keywords:** computer system security, fuzzy logic, linguistic variables.