ПРИОРИТИЗАЦИЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ НЕЙРО-НЕЧЕТКОЙ СИСТЕМЫ

Татаринова Ю.Е.
Научный руководитель - д.т.н., проф. Винокурова Е.А.,
к.т.н. Синельникова О.И.
Харьковский национальный университет радиоэлектроники
(61166, Харьков, просп. Науки 14)
e-mail: yullia.tatarinova@gmail.com

The article is devoted to the process of vulnerability risk assessment of information systems with application of fuzzy set theory. It defines proposed model, which defines the set of linguistic variables and one output variable that describes degree of vulnerability exposure on target computer system. Linguistic variables characterize vulnerability information obtained from public resources. Base of rules and membership functions generated automatically by applying neuro fuzzy logic system.

С ростом количества уязвимостей и сложности вычислительных систем возникает необходимость в автоматической оценке и приоритизации рисков влияния уязвимости на продукт с учетом межкомпонентных взаимодействий. В работе рассматривается задача построения нечеткой продукционной модели с целью вычисления рисков угроз раскрытых уязвимостей, автоматическое построение базы правил, функций принадлежности и их параметров для нейро-нечеткого вывода на, поскольку это является трудоемкой задачей при большом количестве входных переменных параметров.

Общая концепция системы была представлена в [1]. В качестве исходных данных используется база данных общеизвестных уязвимостей – CVE ($x_1, \dots x_n$). На ее основании с применением открытых источников проводится анализ и извлечение характеристик по типу уязвимости и источника, характеру затрагиваемого компонента, степени заинтересованности сообщества по информационной безопасности и т.д. ($y_1, \dots y_m$). Второй набор характеристик ($z_1, \dots z_k$) извлекается из целевой вычислительной системы, а именно: перечень программных компонентов, граф потока управления и данных между ними, права доступа, настройки сети. Результатом исследования является построение системы оценки рисков $I(CVE_i)$ с использованием нечеткой нейронной сети и с предварительным обучением, а также фаззификатора для автоматического формирования нормированных интервалов, функций принадлежности ($\mu(A)$) и их положение в полученных интервалах в качестве компонентов модуля нечеткого логического вывода. Общая схема показана на рисунке 1. Исходные характеристики преобразовываются в лингвистические переменные, которые подаются вместе с терм множествами на вход

фаззификатора. Далее используется нечеткая нейронная продукционная сеть Anfis [2]. Элементы базы правил преобразованы во фрагменты нейронной сети (рис.1.). Первый слой (1) формирует посылки соответствующего правила, выход – степень выполнения правила. Второй слой (2) рассчитывает нормализацию степеней выполнения правил. Третий слой (3) производит заключение правил в выход сети. На последнем этапе вклады всех правил суммируются.

Данная процедура выполняется для каждой уязвимости отдельно. Полученные результаты позволяют приоритизировать задачи по анализу и исправлению ошибок в вычислительной системе. В [2] и [3] работа фаззификатора реализована на базе нечеткого вывода по Мамдани. В данной работе используется сеть из искусственных нейронов на основании их внешней сходимости. Выходом сети есть степени принадлежности активизированных терм.

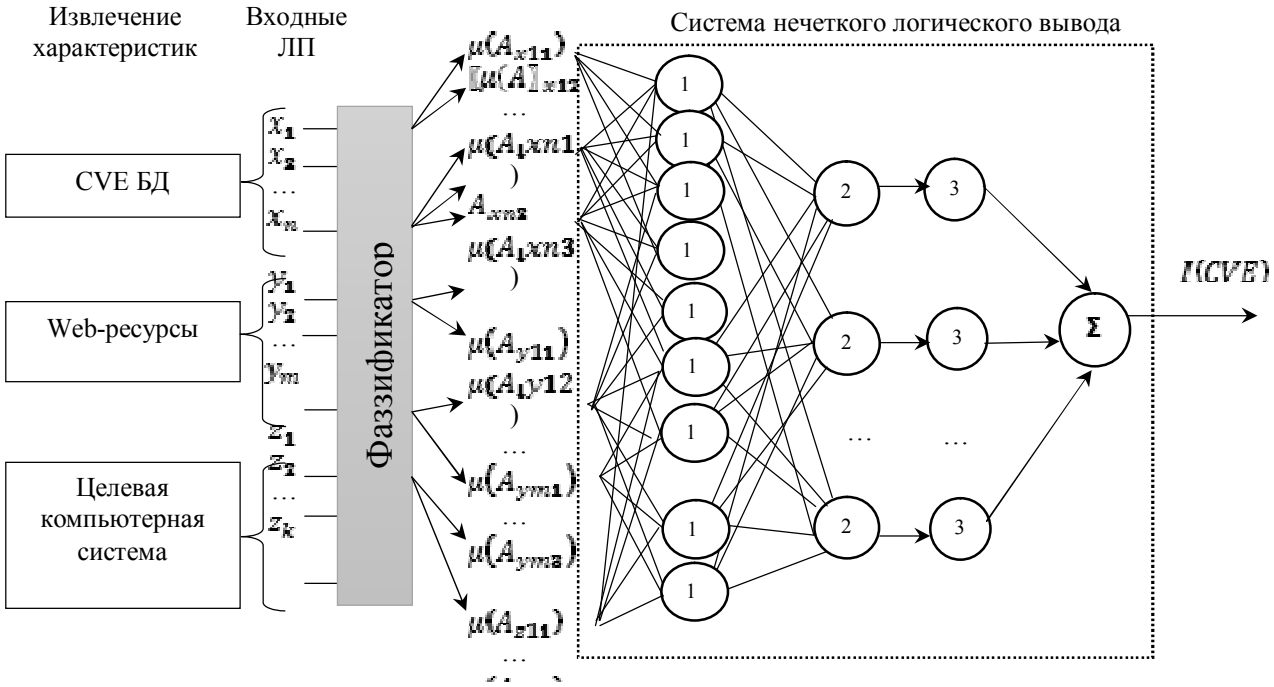

Рисунок 1 – Структурная схема оценки рисков уязвимости

Список использованных источников:

1. Tatarinova, Y. (2018). AVIA: Automatic Vulnerability Impact Assessment on the Target System. 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP), 364-368.

2. Glushenko S. A. An adaptive … ro-fuzzy inference system for assessment of risks to an organization's information security //Бизнес-информатика. – 2017. – №. 1 (39).

3. RAIKHAN M. et al. ASSESSING INFORMATION SECURITY RISK WITH THE FUZZY SET THEORY //Journal of Theoretical & Applied Information Technology. – 2018. – Т. 96. – №. 11.