УДК 004

НЕЙРО-НЕЧЕТКИЙ ПОДХОД К ПРОГНОЗИРОВАНИЮ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВУЗЕ

Жилина Е.В.
к.э.н., доцент каф. ИТиЗИ
black-2@mail.ru
Ефимова Е.В.
к.э.н., доцент, зав. каф. ИТиЗИ
Рутта Н.А.
к.э.н., доцент каф. ИТиЗИ
rutic79@mail.ru
Савская А.Р.
ст. преподаватель каф. ИТиЗИ
РГЭУ (РИНХ)

Аннотация: В статье описан нейро-нечеткий подход, позволяющей прогнозировать риски информационной безопасности в вузе (на примере ИТ-отдела РГЭУ (РИНХ).
Ключевые слова: риск, информационная безопасность, гибридная модель, прогнозирование.

NEURO- FUZZYAPPROACH TO FORECASTING INFORMATION SECURITY RISKS IN A UNIVERSITY

Zhilina E.V.
Efimova E.V.
Rutta N.A.
Savskaya A.R.

Abstruct: The article describes a neuro-fuzzy approach to predict the risks of information security at a university (using the example of the IT department of RSEU).
Keywords: risk, information security, hybrid model, forecasting.

В образовательных учреждениях (вузах) важной проблемой является формирование необходимых условий для обеспечения информационной

безопасности (ИБ) [1]. Используя подходы нейро-нечеткого моделирования для оценки рисков ИБ, можно получить достоверные прогнозные значения выходных лингвистических переменных моделей, как качественных, так и количественных [2-4].

Для оценки рисков ИБ в вузе (на примере статистики ИТ-отдела РГЭУ (РИНХ)) была разработана система нечёткого вывода, позволяющая определять величину каждого риска для всего выделенного экспертами перечня:

- Несанкционированный доступ к конфиденциальной информации (риск 1).

- Несанкционированный доступ к персональной информации (риск 2).

- Подбор пароля (риск 3).

- DDOS-атака (риск 4).

- Заражение вирусами и вредоносными программами (риск 5).

Для моделирования нейро-нечеткой системы оценки рисков ИБ использовался пакет MATLAB, интерактивная среда ANFIS, а также модуль нечеткого моделирования Fuzzy.

Нейро-нечеткий подход к прогнозированию рисков информационной безопасности в вузе сводится к реализации следующих последовательных этапов:

1. Подготовка исходных данных. Формирование файлов с расширением *.dat. Именование файлов согласно перечню рисков ИБ.

2. Загрузка обучающих данных в среду ANFIS. Генерация системы нечеткого вывода (FIS- структуры) на основе алгоритма Сугено, являющейся моделью гибридной сети.

В свойствах среды ANFIS можно установить параметры модели:

- количество входных /выходных переменных;

- вид функции принадлежностей (в нашем эксперименте использовались треугольные функции) для отдельных лингвистических термов (в нашем случае по 3 лингвистических терма для каждой переменной),

а также просмотреть информации о количестве строчек в выборках.

Раздел «Structure» среды ANFIS позволяет визуализировать систему нечеткого логического вывода в виде нейро-нечеткой сети. На рисунке 1 в качестве примера представлена обученная нейро-нечеткая сеть «Заражение вирусами и вредоносными программами», содержащая две входных переменных (год, месяц заражения) и одну выходную (количество заражений).

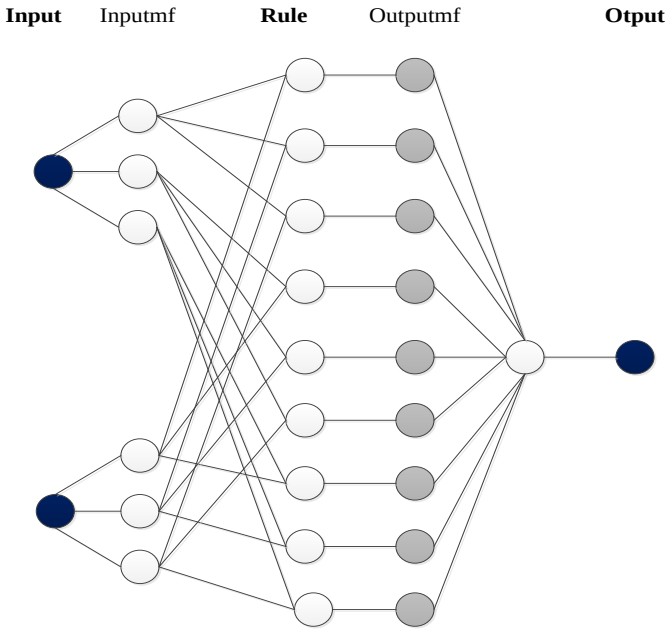

Рис. 1. Anfis Model Structure «Заражение вирусами и вредоносными программами»

3. Настройка параметров обучения нейро-нечеткой (гибридной) сети:

- Необходимо выбрать метод обучения гибридной сети:

1) метод обратного распространения (backpropa) ошибки;

2) гибридный метод (hybrid), представляющий собой комбинацию метода наименьших квадратов и метода убывания обратного градиента.

- Необходимо определить значение итоговой ошибки обучения (Error Tolerance), по умолчанию значение которой равняется нулю.

- Необходимо указать количество циклов обучения (Epochs), по умолчанию значение равняется 3 трем эпохам (как правило, рекомендуется увеличить количество эпох; в рассматриваемом эксперименте значение эпох равнялось 40-50).

4. Тренировка / Обучение гибридной сети (Train now).

5. Сохранение системы нечеткого вывода во внешнем файле с расширением *.fis (рисунок 2).

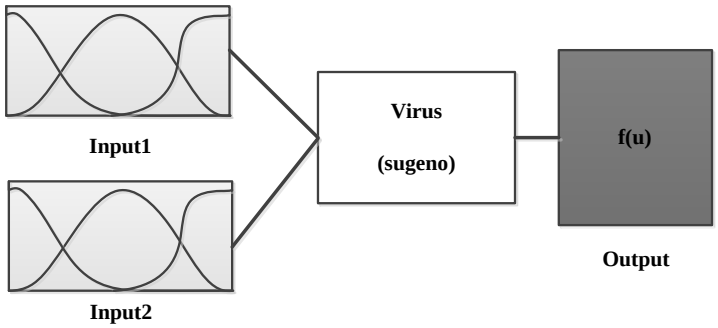

Рис. 2. Нечеткая модель «Заражение вирусами и вредоносными программами»

6. Визуализация переменных модели системы нечеткого вывода. На рисунке 3 приведены треугольные функции принадлежности одной из входных переменных (год заражения, Input1) модели «Заражение вирусами и вредоносными программами».

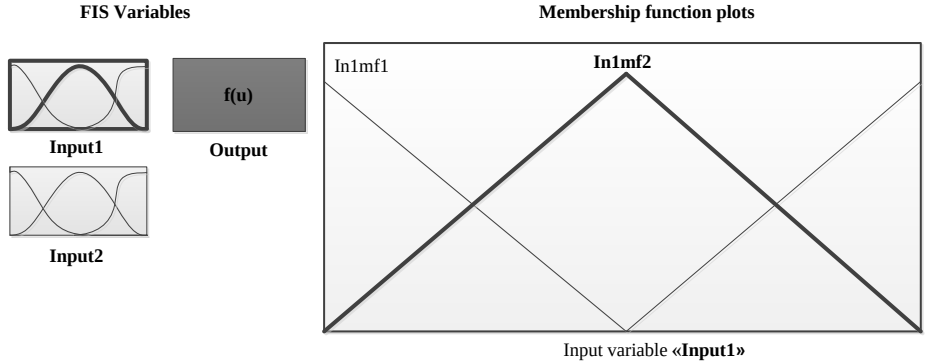

Рис. 3. Функции принадлежности системы нечеткого вывода «Заражение вирусами и вредоносными программами»

7. Проверка адекватности построенной нечеткой модели гибридной сети:

- Необходимо загрузить в рабочее пространство MATLAB необходимый fis-файл исследуемой системы нечеткого вывода через командную строку: fis=readfis().

- Спрогнозировать исследуемый риск ИБ: evalfis([2020 3], fis).

В исследовании аналогичным образом были построены гибридные модели по всему остальному перечню выделенных угроз для РГЭУ (РИНХ).

Разработанные с использованием программного инструментария Matlab и интерактивной среды Anfis модели нейро-нечеткого прогнозирования рисков информационной безопасности (в том числе, модели – «Несанкционированный доступ к конфиденциальной информации», «Несанкционированный доступ к персональной информации», «Подбор пароля», «DDOS-атака», «Заражение вирусами и вредоносными программами) в вузе на основе алгоритма Сугено позволяют объективно получать краткосрочные прогнозные значения после обучения сети исходных статистических данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Тищенко Е.Н., Жилина Е.В., Шарыпова Т.Н., Палютина Г.Н. Нечеткие модели результатов освоения образовательных программ в области информационной безопасности // Интеллектуальные ресурсы – региональному развитию. – 2018. – Т.4, № 1. – С. 292-297.
2. Сахарова Л.В. Использование теории нечетких множеств для оптимизации механизмов профессиональной подготовки // Интеллектуальные ресурсы – региональному развитию. 2016. – № 2. – С. 119-122.
3. Zhilina E.V., Popova L.K., Rutta N.A., Sheydakov N.E. Fuzzy model of functioning of educational-laboratory and production capacities of the educational cluster in the information security field //10th International Conference on Theory and Application of Soft Computing, Computing and Perceptions. – 2019. – Режим доступа: www.springer.com/la/book/9783030041632 (дата обращения: 10.03.2020).
4. Tishchenko E.N., Zhilina E.V., Sharypova T.N., Palyutina G.N. Fuzzy Models of the Results of the Mastering the Educational Programs in the Field of Information Security // 13th International Conference on Theory and Application of Fuzzy Systems and Soft Computing–ICAFS-2018. ICAFS 2018. Advances in Intelligent Systems and Computing, vol. 896, pp.694-701 (2019).