РАЗРАБОТКА ЭВРИСТИЧЕСКОГО АНАЛИЗАТОРА ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Гавриленко С.Ю., Деркач А.В.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Наиболее распространенной угрозой безопасности функционирования компьютерных систем является воздействие вредоносного программного обеспечения. Одним из методов поиска вирусов является использование эвристических анализаторов [1].

В работе проводится анализ методов эвристического поиска, использующих методы нечеткой логики анализа злоумышленного программного обеспечения. Типичный процесс построения модели принятия решений состоит из следующих этапов [2]:

1) определение входов и выходов создаваемой модели;
2) задание функции принадлежности для всех переменных;
3) формирование базы правил;
4) выбор и реализация алгоритма нечёткого вывода;
5) анализ процесса управления созданной моделью.

Разработаны программные модели на примере нечёткого вывода Мамдани и Сугено. Алгоритм Мамдани более универсален. Алгоритм Сугено применяется, когда известна не форма функции соответствия выходного параметра, а весовые коэффициенты. Данные модели являются универсальными аппроксиматорами.

Исследования показали, что при больших объемах выборки идентификация с помощью Сугено даёт большую точность. Но при этом могут возникнуть трудности с интерпретацией параметров нечёткой модели и с объяснением логического вывода.

Таким образом можно сделать вывод, что для задач, где более важным является объяснение принятого решения, будут иметь преимущество модели Мамдани, а для задач, где важна точность идентификации, лучше использовать модели Сугено.

Литература:

1. Климентьев К. Компьютерные вирусы и антивирусы. Взгляд программиста. – М.: ДМК Пресс. – 2013.

2. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH. – СПб.: БХВ-Петербург. – 2005.