

ЭВРИСТИЧЕСКИЙ ПОИСК КОМПЬЮТЕРНЫХ ВИРУСОВ НА ОСНОВЕ МЕТОДА НЕЧЕТКОГО ВЫВОДА МАМДАНИ

*канд. техн. наук, доц. С.Ю. Гавриленко, студ. Д.Н. Саенко,
Национальный технический университет "Харьковский
политехнический институт", г. Харьков*

Компьютерные вирусы являются одними из наиболее распространенных угроз безопасности функционирования современных компьютерных систем. Именно поэтому актуальной является разработка эффективных методов и средств противодействия компьютерным вирусам. Известно, что одним из перспективных направлений исследований данной отрасли является использование методов нечеткой логики [1, 2].

Методы нечеткой логики используются при построении эвристических анализаторов, позволяющих обнаружить угрозы, которые невозможно определить с помощью сигнатурного анализа, то есть с помощью антивирусных баз. Эвристический анализ позволяет находить файлы, которые подозреваются в заражении неизвестным вирусом или новой модификацией известного вируса. Объектам, обнаруженным с помощью эвристического анализа, присваивается статус возможно зараженного.

В работе предложен эвристический анализатор, который работает на основе технологии эвристического анализа, содержащего набор утверждений (правил). Каждое правило состоит из совокупностей событий (условий) и результатов (выводов). После постановки задачи в терминах правил, состоящих из условий и выводов, производится их обработка по специальному алгоритму – методу нечеткого вывода Мамдами [3].

Список литературы: 1. *Зайченко Ю.П.* Нечеткие модели и методы в интеллектуальных системах / Ю.П. Зайченко. – К.: Слово, 2008. – 344 с. 2. *Рутковская Д.* Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский. – М.: Горячая линия-Телеком, 2006. – 452 с. 3. *Гошко С.В.* Технологии борьбы с компьютерными вирусами / С.В. Гошко. – М.: Солон-Пресс, 2009. – 352 с.