Секция «Математика и механика»

Использование статистического анализа при решении задачи обнаружении вредоносного программного обеспечения.

Иринархова Алена Константиновна
Аспирант
Казанский национальный исследовательский технический университет им. А.Н.Туполева-КАИ, Институт технической кибернетики и информатики, Казань, Россия
E-mail: a.irinarkhova@mail.ru

Одной из серьезных угроз информационной безопасности для компьютерных сетей и систем является компьютерное вредоносное программное обеспечение, в связи, с чем его обнаружении на ранней стадии становится важной задачей. В работе показаны возможные подходы обнаружения вредоносного программного обеспечения на примере сетевого «червя» с использованием методов нечеткого [1] и четкого анализа данных.

В качестве основной цели работы рассматривается исследование влияния параметров операционной системы на определение факта заражения вирусом компьютерной системы.

Для достижения цели были решены следующие задачи:

- выбраны совокупности основных статистических показателей, описывающих состояние ОС – параметры журналов счетчиков ОС для зараженной и незараженной вредоносным программным обеспечением среды;
- вычислены основные статистические характеристики ИСД [3,4];
- проведен регрессионный анализ, получено уравнение регрессии, которое устанавливает зависимость между выбранными показателями ОС и выходом нейронной сети [2,4];
- проанализированы изменения зависимости значений между выбранными показателями ОС с течением времени, при условии, что не появятся и не изменяться внешние факторы, влияющие на ее работу.

В результате проделанной работы можно установить, что при помощи регрессионного анализа существует возможность установить факт смены состояния зараженности компьютерной системы и величина ошибки очень мала, так как выход нейронной сети и значения, полученные при помощи регрессионного уравнения, очень близки.

Литература

1. Головко В. А. Нейронные сети - обучение, организация, применение. -Изд. «Радиотехника»: Москва,2001.

2. Шмайлова Р.А., Минашкин В.Г., Садовникова Н.А., Шувалова Е.Б.. Теория статистики: Учебник. М.: Финансы и статистика, 2004.

3. Якимов И.М., Яхина З.Т. Моделирование систем: Лабораторный практикум. Казань: Изд-во Казан. гос. техн. ун-та, 2002.

4. www.statsoft.ru. (Электронный учебник по ППП Statistica 6.0)