Алгоритмы искусственных иммунных систем и нейронных сетей для обнаружения вредоносных программ и компьютерных вирусов

С. В. Безобразов

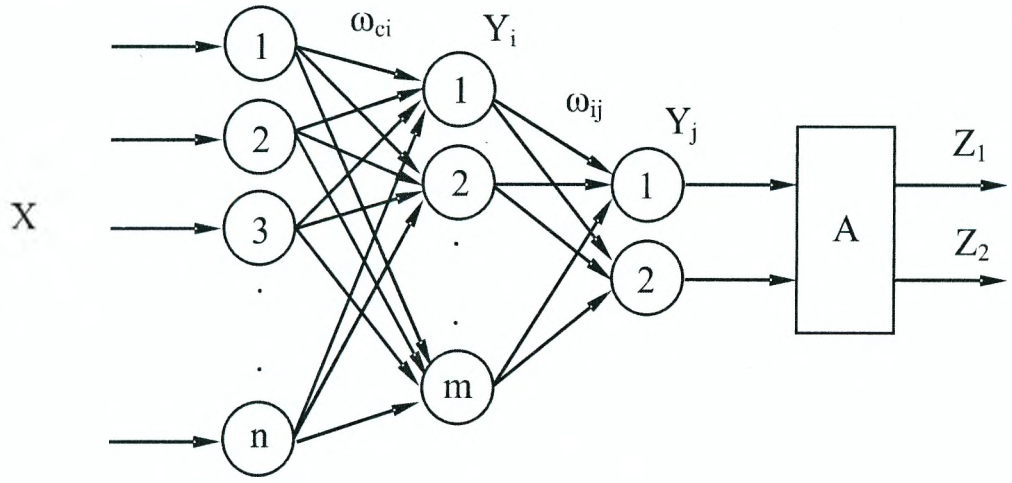
Брестский государственный технический университет

Традиционные методы обнаружения вредоносных программ сегодня не способны в полной мере обеспечить надежную защиту компьютерных систем от проникновения вредоносных программ и компьютерных вирусов, которые являются причиной утечки информации, ее разрушения и изменения. Применение сигнатурного метода в качестве реактивной защиты обеспечивает надежное обнаружение уже известных вредоносных программ, однако не дает защиты от новых, ранее неизвестных компьютерных вирусов. Для устранения этого недостатка применяются эвристические алгоритмы, которые формируют проактивную защиту [1]. Однако существующие эвристические алгоритмы далеки от совершенства и характеризуются высоким уровнем ошибок первого и второго рода. С развитием автоматизированных средств обработки информации, а также сетевой инфраструктуры для ее передачи, проблема защиты информации становится наиболее важной и острой. В связи с этим, возрастает потребность в новых эффективных алгоритмах и методах защиты вычислительных систем от вредоносных вторжений.

Разработанные алгоритмы обнаружения вредоносных программ и компьютерных вирусов опираются на методы искусственного интеллекта и позволяют повысить уровень защищенности современных компьютерных систем [3].

В данной статье представлена интеллектуальная система защиты информации, которая характеризуется адаптивностью, самоорганизацией и эффективностью обнаружения новых, ранее неизвестных вредоносных программ.

Главным элементом обнаружения вредоносных программ в разработанной нейросетевой искусственной иммунной системе (НИИС) является детектор, представляющий собой нейронную сеть и функционирующий по принципам искусственных иммунных систем (см. рисунок) [3]. Нейросетевой иммунный детектор состоит из трех слоев нейронных элементов и арбитра. Первый слой нейронных элементов является распределительным. Он распределяет входные сигналы (данные из файла) на нейронные элементы второго (скрытого) слоя. Второй слой состоит из нейронов Кохонена [4]. Третий слой, состоящий из двух линейных нейронных элементов, осуществляет отображение кластеров, сформированных слоем Кохонена, в два класса, которые характеризуют чистые и вирусные входные образы. Арбитр осуществляет процедуру окончательного решения о принадлежности сканируемого файла к вирусному или чистому классу. Для этого он вычисляет количество чистых и вредоносных фрагментов сканируемого файла.



Структура нейросетевого иммунного детектора

В исследованиях проверялась вероятность обнаружения неизвестных вредоносных программ у различных антивирусных продуктов и сравнивалась с результатами разработанной нами системы. Антивирус Касперского из 36 представленных вредоносных программ обнаружил 27, то есть процент обнаружения составил 75. Антивирус NOD32 обнаружил 24 вредоносных программы, и его процент обнаружения составил 67. Антивирус Dr. Web обнаружил 19 вредоносных программ, что составило 53 % обнаружения. НИИС обнаружила 100 % присутствующих в эксперименте вредоносных программ.

Разработанная и предложенная система обнаружения вредоносных программ с применением методов искусственного интеллекта позволяет с высокой эффективностью обнаруживать неизвестные вредоносные программы и компьютерные вирусы. Система характеризуется непрерывной эволюцией детекторов, что позволяет ей обучаться на протяжении всего цикла функционирования и приспосабливаться к новым вирусным атакам. НИИС может быть использована при построении как принципиально новых, не имеющих аналогов, систем защиты компьютеров от вредоносных программ, так и в дополнении к уже имеющимся методам.

Литература:

1. Касперский Е. Компьютерное зловредство / Е. Касперский. — СПб.: Питер, 2007. — 208 с.

2. Безобразов С. В. Алгоритмы искусственных иммунных систем и нейронных сетей для обнаружения вредоносных программ / С. В. Безобразов, В. А. Головко // Научная сессия МИФИ «Нейроинформатика»: материалы XII Всеросс. науч. конф., МИФИ, Москва, 25–29 янв. 2010. — Москва, 2010. — С. 273–278.

3. Kohonen T. Sell-organised formation of topologically correct feature maps / T. Kohonen // Biological Cybernetics. — 1982. — № 43. — P. 59–69.

Электронная база данных «История Могилева»

Г. Н. Беляева

Могилевский государственный университет им. А. А. Кулешова

Достаточно широкое представительство электронных энциклопедий, моделирующих и игровых программ создает впечатление о наличии богатой палитры компьютерных проектов по истории. Однако, к сожалению, существует серьезный пробел: отсутствуют компьютерные обучающие программы, обеспечивающие преподавание факультативных курсов, программы, позволяющие изучать историю родного края.

С целью обеспечения содержания факультативных курсов краеведческой направленности, предметов «История Беларуси» и «Всемирная история» была разработана электронная база данных «История Могилева». Новизна проекта заключается в том, что впервые в истории Могилева была создана электронная база данных по истории родного города в виде учебной компьютерной программы.

Ценность электронной базы данных «История Могилева» заключается в том, что на одном электронном носителе собраны богатейшие материалы по истории Могилева, что не может быть обеспечено ни одним книжным изданием (только фотографий 2000). Многие данные нигде ранее не публиковались. Данная работа не имеет аналогов в нашей стране и существенно отличается от програмных продуктов, подготовленных в России, Польше.

В работе широко применялись историко-сравнительный, историко-системный, историко-генетический, хронологический методы и метод актуализации.

Электронная база данных «История Могилева» представляет в 17 разделах историю Могилева (начиная с легенд об основании и заканчивая описанием современного Могилева). В разделах «Личности», «Документы и карты», «Памятники культуры» содержатся биографии и фотографии 920 известных исторических деятелей, чьи имена связаны с судьбой города, информацию о 400 памятниках культуры (существующих, утраченных), 120 исторических документов, 60 карт и схем, связанных с историей Могилева.

Раздел диска «Линия времени» помогает соотнести полученные данные с общеисторическими фактами, определить влияние событий Всемирной истории на развитие могилевской истории.