ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И НЕЙРОННЫЕ СЕТИ

УДК 004.056.57:032.26

АЛГОРИТМЫ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ И НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Безобразов С.В., Рубанов В.С.
УО «Брестский государственный технический университет», г. Брест

Введение. Современные антивирусные продукты представляют собой сложные программные модули, тесно интегрированные в ядро операционной системы и работающие с ней как одно целое. Это не только сканеры, выполняющие простой поиск вирусов по сигнатуре, но и эвристические анализаторы, сетевые экраны, ревизоры и др. Несмотря на это, на сегодняшний день они проигрывают борьбу создателям вредоносных программ. Киберпреступники постоянно придумывают и реализовывают новые пути и методы заражения компьютеров, разрабатывают хитроумные алгоритмы и внедряют свои вредоносные программы.

С момента появления нового вируса до появления ответной реакции на этот вирус со стороны антивирусной индустрии может проходить какое-то, иногда продолжительное время. Как показала практика, за это время вирусы способны заразить сотни тысяч компьютеров, вызвать настоящую вирусную эпидемию и принести огромные убытки. Современные исследования в области защиты информации направлены на создание таких методов и алгоритмов защиты, которые были бы способны обнаружить и нейтрализовать неизвестные вирусы.

Методы искусственных иммунных систем (ИИС) [1] позволяют сконструировать такую систему обнаружения вирусов, которая способна обнаруживать неизвестные вредоносные программы. Основными элементами ИИС, которые выполняют функцию обнаружения вирусов, являются иммунные детекторы. Нами был предложен алгоритм формирования иммунных детекторов на основе искусственных нейронных сетей.

Метод формирование детекторов на основе нейронной сети. Рассмотрим процесс формирования иммунных детекторов на основе нейронных сетей. Вначале генерируется начальная популяция иммунных детекторов, каждый из которых представляет собой искусственную нейронную сеть [2]. Затем формируется набор чистых файлов, состоящий, как правило, из утилит операционной системы, различных документов, файлов разнообразного программного обеспечения. На следующем шаге выбирается несколько компьютерных вирусов или их сигнатур. Набор из чистых файлов и вирусов образует обучающую выборку для нейросетевых детекторов. В процессе обучения нейронная сеть учится распознавать вредоносные программы от «чистого» ПО. Механизм обучения детектора представлен на рисунке 1.

Набор обученных нейронных сетей образует популяцию иммунных детекторов, которые циркулируют в компьютерной системе и производят обнаружение компьютерных вирусов. Наличие разнообразных файлов для обучения и элемента случайности в формировании входных векторов дает возможность получить большое количество различных по своей структуре иммунных детекторов. В процессе сканирования неизвестного файла нейрон-

ная сеть идентифицирует неизвестный образ, в результате чего иммунный детектор принимает решение о принадлежности файла к классу вредоносных программ или к классу чистых файлов.

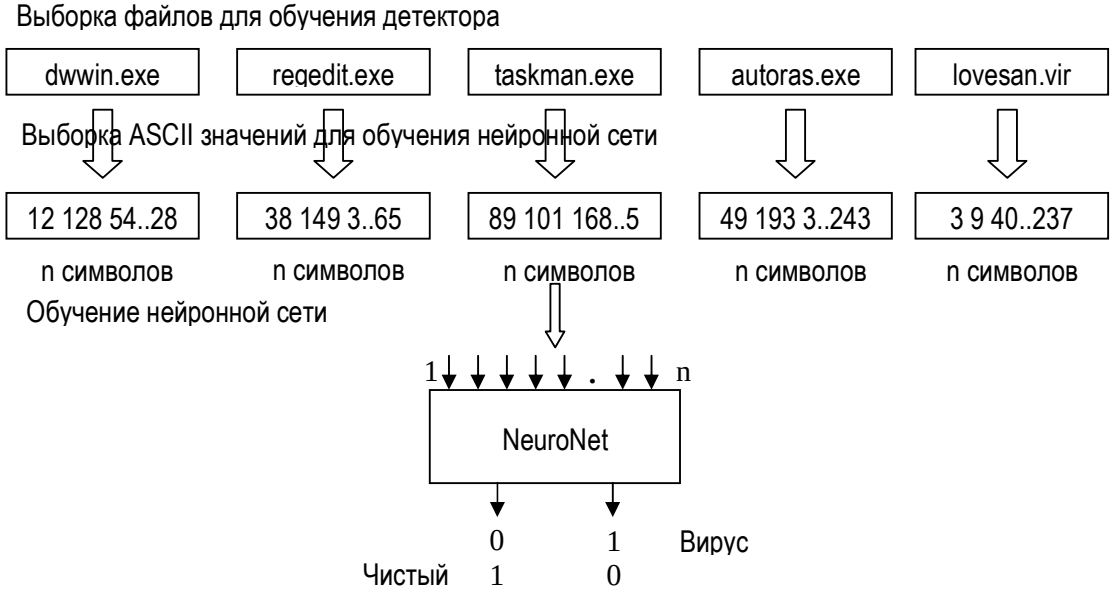

Рисунок 1 – Механизм обучения иммунного детектора на основе нейронной сети

Общий алгоритм функционирования нейросетевых иммунных детекторов можно представить в виде следующих шагов:

1. Генерация начальной популяции иммунных детекторов.
2. Обучение сформированных иммунных нейросетевых детекторов.
3. Отбор (селекция) нейросетевых иммунных детекторов.
4. Функционирование детекторов в компьютерной системе.
5. Уничтожение нейросетевых детекторов по истечению времени.
6. Обнаружение вредоносной программы.
7. Клонирование и мутация нейросетевых иммунных детекторов.
8. Формирование детекторов иммунной памяти.

Отметим основные отличия предложенного алгоритма от существующих. В данном случае каждый нейросетевой иммунный детектор является полностью самостоятельным объектом, т.е. сам выбирает себе область сканирования. Для этого он получает список файлов, хранящихся на жестком диске, и случайным образом выбирает файл из списка для его проверки. После проверки одного файла, детектор переходит к следующему файлу, также выбранному случайным образом из существующего списка. Сканирование файлов нейросетевым иммунным детектором продолжается до тех пор, пока детектор не обнаруживает вредоносную программу, либо до истечения времени, отведенного для функционирования данного детектора.

Популяция нейросетевых иммунных детекторов обеспечивает достаточную область покрытия сканирования файлов на жестком диске для своевременного обнаружения проникшего потенциального компьютерного вируса.

Таким образом, соблюдается принцип децентрализации системы безопасности, построенной на основе комбинации методов нейронных сетей и искусственных иммунных систем, что значительно повышает отказоустойчивость и защищенность системы в целом.

Структура нейросетевого иммунного детектора. На рисунке 2 изображена архитектура нейросетевого иммунного детектора, который состоит из трех слоев нейронных элементов и арбитра.

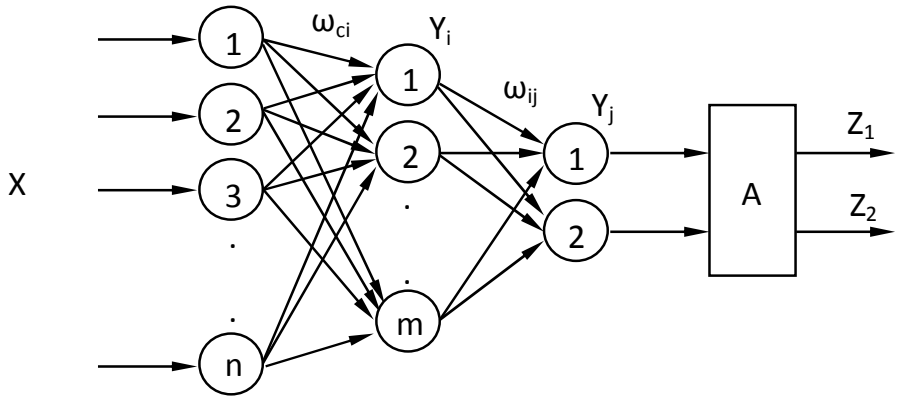

Рисунок 2 – Нейросетевой иммунный детектор

На вход такого детектора в режиме функционирования подаются фрагменты проверяемого файла, которые формируются в соответствии с методом скользящего окна. Первый слой нейронных элементов является распределительным. Он распределяет входные сигналы на нейронные элементы второго (скрытого) слоя. Количество нейронных элементов распределительного слоя равняется размерности скользящего окна.

Второй слой состоит из нейронов Кохонена, которые используют конкурентный принцип обучения и функционирования в соответствии с правилом «победитель берет все».

Третий слой состоит из двух линейных нейронных элементов, которые используют линейную функцию активации. Арбитр осуществляет процедуру окончательного решения о принадлежности сканируемого файла к вирусному или чистому классу.

Результаты экспериментов. На рисунке 3 приведены результаты экспериментальной и теоретической вероятности обнаружения вредоносной программы в зависимости от количества детекторов.

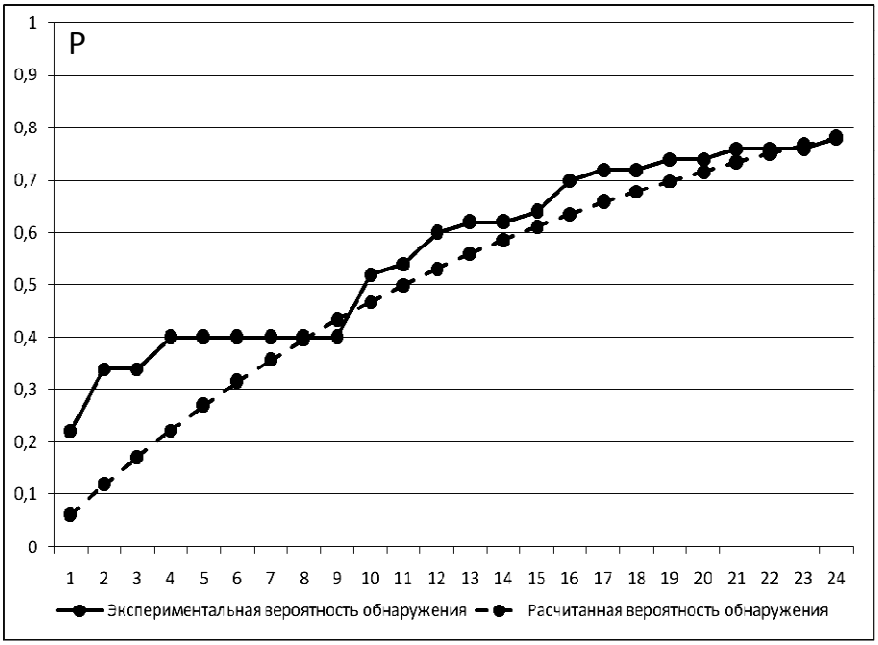

Рисунок 3 – Вероятности обнаружения вредоносных программ нейросетевыми иммунными детекторами

Как следует из рисунка, теоретическая вероятность хорошо аппроксимирует экспериментальную вероятность обнаружения вредоносных программ.

Выводы. Разработан алгоритм построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ, который характеризуется непрерывной эволюцией нейросетевых иммунных детекторов с целью эффективного обнаружения вредоносных программ. Предложенный алгоритм отличается от известных способом клональной селекции, когда мутация детекторов происходит в результате их дополнительного обучения, а отбор клонированных детекторов происходит в соответствии с их значениями суммарной квадратичной ошибки. Это позволяет адаптироваться нейросетевым иммунным детекторам к обнаружению вредоносных программ.

Разработана структура нейросетевого иммунного детектора для обнаружения вредоносных программ, которая состоит из трех слоев нейронных элементов и арбитра. Она характеризуется малым объемом обучающей выборки. Предложенный нейросетевой иммунный детектор способен обнаруживать неизвестные вирусы.

Литература

1. Искусственные иммунные системы для защиты информации: применение LVQ сети // IX Всероссийская научно-техническая конференция «Нейроинформатика - 2007»: сборник научных трудов. – М.: МИФИ, 2007. – Ч. 2.

2. Головко, В.А. Нейронные сети: обучение, организация, применение / В.А. Головко // Нейрокомпьютеры и их применение : учеб. пособие / В.А. Головко. – М., 2001 – 256 с.

УДК 004.8.032.26

МУЛЬТИАГЕНТНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СЕТЕЙ

Войцехович Л.Ю.

УО «Брестский государственный технический университет», г. Брест

Высочайший уровень угроз информационной безопасности из внешней среды сделал брандмауэр и *Систему Обнаружения Вторжений (Intrusion Detection System - IDS)* необходимой составляющей защищенной информационной системы. В современном мире развивающихся стремительными темпами компьютерных технологий и телекоммуникаций злоумышленникам стало гораздо легче достичь поставленных целей, благодаря невнимательности и неосведомленности своих жертв о существующих методах защиты.

Простейшим средством сетевой защиты может служить брандмауэр (межсетевой экран, firewall) - реализованное программно или аппаратно средство фильтрации сетевого трафика между двумя сетями или компьютером и сетью (персональный брандмауэр). При этом используются сетевые адреса отправителя и получателя запроса или конкретные службы, а анализа передаваемого трафика не происходит.

Для выполнения анализа передаваемых в сети данных необходимо более сложное и интеллектуальное средство – Система Обнаружения Вторжений [1]. Система обнаружения вторжений – программное и/или аппаратное средство для выявления фактов несанкционированной деятельности (вторжения или сетевой атаки) в компьютерной сети или отдельном узле.