УДК 621.797:621.664

АЛГОРИТМЫ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ И НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

Безобразов С.В., к.т.н., доц., Головко В.А., д.т.н., проф.
Брестский государственный технический университет
ул. Московская, 267, 224001, г. Брест, Республика Беларусь
E-mail: bescase@gmail.com, gva@bstu.by

В данной статье представлены архитектура нейросетевого иммунного детектора, входящего в состав нейросетевой искусственной иммунной системы для обнаружения вредоносных программ, а также алгоритмы его обучения и функционирования.

Ключевые слова: нейронная сеть, иммунная система, вредоносные программы.

Введение. Несмотря на активные действия со стороны производителей антивирусного программного обеспечения, компьютерные вирусы продолжают успешно проникать в компьютерные системы пользователей по всему миру и выполнять вредоносные действия по уничтожению или краже информации. Традиционные методы обнаружения вредоносных программ, применяемые сегодня, не способны обеспечить надежную защиту компьютерных систем от проникновения компьютерных вирусов.

Методы искусственного интеллекта позволяют создать принципиально новые алгоритмы обнаружения вредоносных программ, позволяющие значительно повысить уровень защищенности компьютерных систем.

Анализ предыдущих исследований. В предыдущих наших работах [1-4] мы разработали и представили искусственную иммунную систему обнаружения вредоносных программ и показали, что разработанные методы позволяют увеличить процент обнаружения неизвестных вредоносных программ. Также было показано, что качество обнаружения зависит от структуры детекторов, которые играют основную роль в обнаружении компьютерных вирусов.

Цель работы. В данной статье приводятся структура и алгоритмы обучения и функционирования нейросетевых иммунных детекторов, в основе которых лежит разработанная нами искусственная нейронная сеть. Применение таких детекторов позволяет обнаруживать разнотипные неизвестные вредоносные программы.

В первом разделе статьи приводятся алгоритмы построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ. Второй раздел содержит описание структуры и алгоритма обучения нейросетевых иммунных детекторов. В третьем разделе представлены алгоритмы функционирования нейросетевых иммунных детекторов. Четвертый раздел содержит результаты исследований.

Материал и результаты исследований.

1. Алгоритмы построения и функционирования нейросетевой искусственной иммунной системы для обнаружения вредоносных программ. Процесс построения и функционирования искусственной иммунной системы нами был в деталях приведен в [1-4]. Рассмотрим процессы генерации, обучения, отбора и функционирования иммунных детекторов на основе нейронных сетей.

Генерируется начальная популяция иммунных детекторов, каждый из которых представляет собой искусственную нейронную сеть. Представим нейросетевой иммунный детектор в виде черного ящика, который имеет n-входов и два выхода (рис. 1).

Рисунок 1 - Нейросетевой иммунный детектор

Выходные значения детектора формируются после подачи всех образов на него в соответствии со следующим выражением:

$$Z_1 = \begin{cases} 1, & \textit{если чистый файл} \\ 0, & \textit{иначе.} \end{cases}$$
$$Z_2 = \begin{cases} 1, & \textit{если вирус} \\ 0, & \textit{иначе.} \end{cases} \quad (1)$$

Для корректного функционирования нейросетевые иммунные детекторы (НИД) должны пройти процесс обучения. Обучающая выборка формируется из чистых файлов (класс чистых программ) и вредоносных программ (класс вредоносных программ). Присутствие вируса или его сигнатуры при обучении позволяет обученным иммунным детекторам находить разницу между чистыми файлами и компьютерными вирусами. Очевидно, что чем больше разнообразных файлов присутствуют в обучающей выборке, тем разнообразнее будут иммунные детекторы. Желательно также иметь представителей всех типов вредоносных программ – черви, троянские программы, макровирусы и т.д [5]. Однако это необязательное условие, потому что вредоносные программы структурно (по набору команд) отличаются от неинфицированных файлов, так как

подразумевают деструктивные функции, что влияет на решение иммунного детектора при сканировании файла. Нейронная сеть обучается путем обучения с учителем [6], т.е. мы указываем искусственной нейронной сети, где данные из чистых файлов, а где – из вредоносных программ.

Пусть T – множество чистых файлов, а F – множество вредоносных файлов. Из них случайным образом формируется множество входных образов для обучения i-го детектора.

$$X_i = \begin{bmatrix} X_i^1 \\ X_i^2 \\ \dots \\ X_i^L \end{bmatrix} = \begin{bmatrix} X_{i1}^1 & X_{i2}^1 & \dots & X_{in}^1 \\ X_{i1}^2 & X_{i2}^2 & \dots & X_{in}^2 \\ \dots & & & \\ X_{i1}^L & X_{i2}^L & \dots & X_{in}^L \end{bmatrix}, \quad (2)$$

где L – размерность обучающей выборки.

Соответственно, множество эталонных образов выглядит следующим образом:

$$l_i = \begin{bmatrix} l_i^1 \\ l_i^2 \\ \dots \\ l_i^L \end{bmatrix} = \begin{bmatrix} l_{i1}^1 & l_{i2}^1 \\ l_{i1}^2 & l_{i2}^2 \\ \dots & \\ l_{i1}^L & l_{i2}^L \end{bmatrix}. \quad (3)$$

Эталонные выходные значения для i-го детектора формируются так:

$$l_{i1}^k = \begin{cases} 1, & \textit{если } X_i^k \in T \\ 0, & \textit{иначе}. \end{cases}$$
$$l_{i2}^k = \begin{cases} 1, & \textit{если } X_i^k \in F \\ 0, & \textit{иначе}. \end{cases} \quad (4)$$

Обучение каждого детектора осуществляется с целью минимизации суммарной квадратичной ошибки детектора. Суммарная квадратичная ошибка i-го детектора определяется следующим образом:

$$E_i = \frac{1}{2} \sum_{k=1}^{L} \sum_{j=1}^{2} (Z_{ij}^k - l_{ij}^k)^2, \quad (5)$$

где Z_{ij}^k – значение j-го выхода i-го детектора при подаче на вход его k-го образа.

Величина суммарной квадратичной ошибки характеризует приспособленность детектора к обнаружению вредоносных файлов. Чем меньше ее значение, тем больше приспособленность детектора. Поэтому величину суммарной квадратичной ошибки можно использовать для отбора лучших детекторов.

Набор обученных нейронных сетей образует популяцию иммунных детекторов, которые циркулируют в компьютерной системе и производят обнаружение вредоносных программ. 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 нейронная сеть идентифицирует неизвестный образ, в результате чего иммунный детектор принимает решение о принадлежности файла к классу вредоносных программ или к классу чистых файлов.

Общий алгоритм функционирования нейросетевой иммунной системы, в соответствии с [1], можно представить в виде следующей последовательности:

1. Генерация начальной популяции иммунных детекторов, каждый из которых представляет собой искусственную нейронную сеть со случайными синаптическими связями:

$$D = \left\{ D_i, \quad i = \overline{1, r} \right\}, \quad (6)$$

где D_i – i-й нейросетевой иммунный детектор, r – общее количество детекторов.

2. Обучение сформированных иммунных нейросетевых детекторов. Обучающая выборка формируется случайным образом из совокупности чистых файлов (как правило, это разнообразные системные утилиты операционной системы) и из совокупности вредоносных программ или их сигнатур. Эталонные выходные значения нейронной сети формируются соответственно (4).

3. Отбор (селекция) нейросетевых иммунных детекторов на тестовой выборке. На данной итерации уничтожаются те детекторы, которые оказались неспособны к обучению, и детекторы, в работе которых наблюдаются различные недостатки (например, ложные срабатывания). Для этого каждый детектор проверяется на тестовой выборке. В результате для каждого детектора определяется значение квадратичной ошибки E_i (5).

Селекция детектора производится следующим образом:

$$D_i = \begin{cases} 0, & \textit{если } E_i \neq 0 \\ D_i, & \textit{иначе}. \end{cases}, \quad (7)$$

где 0 – операция уничтожения детектора.

4. Каждый детектор наделяется временем жизни и случайным образом выбирает файл для сканирования из совокупности файлов, которые он не проверял.

5. Сканирование каждым детектором выбранного файла, в результате которого определяются выходные значения детекторов Z_{i1}, Z_{i2}, i=1, r.

6. Если i-й детектор не обнаружил вирус в сканируемом файле, т.е. $Z_{i1}=1$ и $Z_{i2}=0$, то он выбирает следующий файл для сканирования. Если время жизни i-го детектора закончилось, то он уничтожается, вместо него генерируется новый детектор.

7. Если i-й детектор обнаружил вирус в сканируемом файле, т.е. $Z_{i1}=0$ и $Z_{i2}=1$, то подается сигнал об обнаружении вредоносного файла и осуществляются операции клонирования и мутации соответствующего детектора. Операция мутации заключается в дополнительном обучении детекторов-клонов на обнаруженном вредоносном файле. Так создается совокупность детекторов, настроенных на обнаруженную вредоносную программу.

8. Отбор клонированных детекторов, которые являются наиболее приспособленными к

обнаружению вредоносной программы. Если $E_{ij} < E_i$, то детектор прошел отбор. Здесь E_{ij} – суммарная квадратичная ошибка j-го клона i-го детектора, которая вычисляется на вредоносном файле.

9. Детекторы-клоны осуществляют сканирование файлового пространства компьютерной системы до тех пор, пока не произойдет уничтожение всех проявлений вредоносной программы.

10. Формирование детекторов иммунной памяти. На этой итерации определяются нейросетевые иммунные детекторы, показавшие наилучшие результаты при обнаружении присутствующего в компьютерной системе вируса. Детекторы иммунной памяти находятся в системе достаточно длительное время и обеспечивают защиту от повторного заражения.

Особенностью предложенного алгоритма является то, что каждый нейросетевой иммунный детектор является полностью самостоятельным объектом (автономным агентом), т.е. сам выбирает себе область сканирования. Для этого он получает список файлов, хранящихся в пространстве памяти, 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 [1]. Широкая популяция нейросетевых иммунных детекторов обеспечивает своевременное обнаружение вредоносных программ. 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.

2. Структура и алгоритм обучения нейросетевого иммунного детектора. В предыдущем разделе была рассмотрена организация и функционирование нейросетевой искусственной иммунной системы для обнаружения вредоносных программ. В данном разделе рассматривается структура и обучение иммунного детектора, в основе которого лежит нейронная сеть. Основной задачей нейросетевого иммунного детектора является разделение пространства входных образов на два класса: чистый класс и вредоносный класс.

Рассмотрим выбор класса нейронной сети, лежащей в основе нейросетевого иммунного детектора. В процессе циркуляции НИД происходит их непрерывная эволюция путем уничтожения старых и формирования новых детекторов [1]. После генерации новых детекторов происходит процесс их обучения, трудоемкость которого пропорциональна размерности обучающей выборки. Поэтому, для увеличения быстродействия нейросетевой искусственной иммунной системы необходимо выбрать такой класс нейронной сети, который характеризуется минимальным размером обучающей выборки. Рассмотрим многослойный персептрон [6, 7], который состоит из n нейронов распределительного слоя, m нейронов скрытого слоя и 2 нейронов выходного слоя. Общее количество настраиваемых параметров (весовых коэффициентов и пороговых значений) в такой сети определяется следующим образом:

$$V = m \cdot (n + 3) + 2. \qquad (8)$$

Для хорошей классификации размер обучающей выборки должен определяться в соответствии со следующим выражением [7]:

$$L \approx V / e, \qquad (9)$$

где e - допустимая точность классификации.

Пусть $n = 128$, $m = 10$ и $e = 0{,}1$. Тогда $L \approx 13120$.

Аналогичный результат можно получить для мультирекуррентных нейронных сетей [6, 7].

Рассмотрим аналогичную сеть встречного распространения [6, 7] с идентичным количеством нейронных элементов в слоях. В скрытом слое будем использовать нейронные элементы Кохонена. В этом случае нет жестких требований к размерности обучающей выборки. Достаточно, чтобы размер обучающей выборки был следующим:

$$L \geq 2 \cdot m. \qquad (10)$$

Поэтому выберем в качестве основы нейросетевого иммунного детектора нейронную сеть встречного распространения.

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

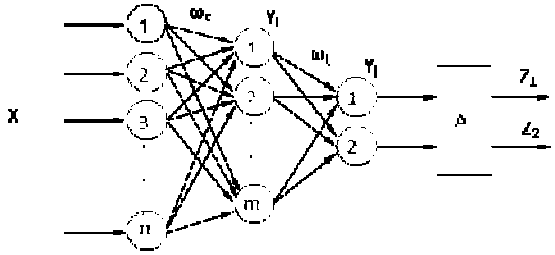

Рисунок 2 - Нейросетевой иммунный детектор

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» [6, 7]. 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.

Рассмотрим выбор количества нейронов в слое Кохонена. Нейронный слой Кохонена осуществляет кластеризацию входного пространства образов, в результате чего образуются кластеры различных образов, каждому из которых соответствует свой нейронный элемент. Количество нейронов слоя Кохонена равняется m. Причем

$$m = p + r, \tag{11}$$

где p – количество первых нейронов слоя Кохонена, которые соответствуют классу чистых программ; r – количество последних нейронов слоя Кохонена, активность которых характеризует класс вредоносных программ.

При обучении нейросетевых иммунных детекторов используется обучающая выборка, состоящая из 80% образов чистого класса и из 20% образов вредоносного класса. Таким образом, соотношение файлов в обучающей выборке равняется четыре к одному. Данное соотношение было получено экспериментальным путем и показало наилучшие результаты [4].

Алгоритм формирования обучающей выборки состоит из следующих шагов: 1) формируется совокупность чистых и вирусных файлов; 2) из сформированной выборки случайным образом выбираются k чистых и h вредоносных файлов; 3) из каждого файла случайным образом выбираются A фрагментов длиной n, в результате образуется обучающая выборка размерностью L = (k+h)·A.

Для обучения нейронов слоя Кохонена используется контролируемое конкурентное обучение [6, 7]. При таком обучении весовые коэффициенты нейрона победителя модифицируются только тогда, когда происходит корректная классификация входного образа, т.е. входной образ соответствует заданному множеству нейронов в слое Кохонена. Так как в слое Кохонена используется p нейронов для чистых входных образов и r нейронов для вредоносных входных образов, то корректная классификация происходит, если при подаче на вход сети чистого фрагмента победителем является один из первых p нейронов слоя Кохонена. Аналогичным образом корректная классификация происходит, если при подаче на вход сети вирусного фрагмента победителем является один из r последних нейронов слоя Кохонена. В остальных случаях происходит некорректная классификация.

Пусть P и J характеризуют соответственно чистый и вредоносный файл. Тогда правило корректной классификации можно представить в виде следующей импликации:

$$\begin{aligned} P \wedge k = 1,2 \ldots p \rightarrow T, \\ J \wedge k = p+1, r \rightarrow T, \end{aligned} \tag{12}$$

где T обозначает корректную классификацию.

При корректной классификации весовые коэффициенты нейрона-победителя усиливаются:

$$w_{ck}(t+1) = w_{ck}(t) + g(X_c - w_{ck}(t)), \tag{13}$$

а при некорректной классификации ослабляются:

$$w_{ck}(t+1) = w_{ck}(t) - g(X_c - w_{ck}(t)), \tag{14}$$

где γ – шаг обучения.

Алгоритм обучения слоя Кохонена состоит из следующих шагов:

1. Случайная инициализация весовых коэффициентов нейронов слоя Кохонена.

2. Подается входной образ из обучающей выборки на нейронную сеть и производятся следующие вычисления:

– вычисляется Евклидово расстояние между входным образом и весовыми векторами нейронных элементов слоя Кохонена

$$\begin{aligned} D_i &= \left|X - w_i\right| = \\ &= \sqrt{(X_1 - w_{1i})^2 + (X_2 - w_{2i})^2 + (X_n - w_{ni})^2}, \end{aligned} \tag{15}$$

где $i = \overline{1, m}$;

– определяется нейронный элемент победитель с номером k

$$D_k = \min_j D_j; \tag{16}$$

– производится модификация весовых коэффициентов нейрона-победителя в соответствии с (14), если при подаче на вход сети чистого фрагмента победителем является один из первых p нейронов или при подаче на вход сети вредоносного фрагмента победителем является один из r последних нейронов сети Кохонена. В противном случае производится модификация весовых коэффициентов нейрона-победителя в соответствии с (14).

Процесс повторяется, начиная с пункта 2 для всех входных образов.

Обучение производится до желаемой степени согласования между входными и весовыми векторами, т.е. до тех пор, пока значение суммарной квадратичной ошибки не станет равной заданному порогу.

Третий слой, состоящий из двух линейных нейронных элементов, осуществляет отображение кластеров, сформированных слоем Кохонена, в два класса, которые характеризуют чистые и вирусные входные образы. В общем случае выходное значение j-го нейрона третьего слоя определяется следующим образом:

$$Y_j = \sum_{i=1}^{m} w_{ij} \cdot Y_i, \tag{17}$$

где ω_{ij} – весовой коэффициент между i-м нейроном слоя Кохонена и j-м нейроном линейного слоя.

Если нейрон-победитель в слое Кохонена имеет номер k, то выходное значение j-го нейрона третьего слоя равняется:

$$Y_j = w_{kj} \cdot Y_k. \tag{18}$$

Для соответствующего отображения входных образов в два класса матрица весовых коэффициентов третьего слоя должна формироваться следующим образом:

$$w_{kj} = \begin{cases} 1, \text{ если } k = 1, 2 \ldots p \text{ и } j = 1 \\ \text{ или } k = p+1 \ldots r \text{ и } j = 2 \\ 0, \text{ если } k = 1, 2 \ldots p \text{ и } j = 2 \\ \text{или } k = p+1 \ldots r \text{ и } j = 1. \end{cases} \quad (19)$$

Арбитр принимает окончательное решение о том, является ли сканируемый файл вредоносным. Для этого он вычисляет количество чистых и вредоносных фрагментов сканируемого файла в соответствии со следующими выражениями:

$$\overline{Y_1} = \sum_{k=1}^{L} Y_1^k, \quad (20)$$

$$\overline{Y_2} = L - \overline{Y_1} = \sum_{k=1}^{L} Y_2^k, \quad (21)$$

где L – множество образов сканируемого файла, Y_i^k – выходное значение i-го нейрона линейного слоя при подаче на вход сети k-го образа.

Далее определяются вероятности принадлежности сканируемого файла соответственно к чистому и вредоносному классу:

$$P_T = \frac{\overline{Y_1}}{L} \cdot 100\%, \quad (22)$$

$$P_F = 1 - P_T = \frac{\overline{Y_2}}{L} \cdot 100\%. \quad (23)$$

Окончательное решение о принадлежности файла к чистому классу арбитр принимает следующим образом:

$$Z_1 = \begin{cases} 1, & \text{если } P_T > 80\% \\ 0, & \text{иначе.} \end{cases} \quad (24)$$

Соответственно, решение о принадлежности сканируемого файла к вредоносному классу принимается в соответствии со следующим выражением:

$$Z_2 = \begin{cases} 1, & \text{если } P_F > 20\% \\ 0, & \text{иначе.} \end{cases} \quad (25)$$

Таким образом, пространство выходных значений арбитра можно представить таблицей.

Таблица 1 - Пространство выходных значений арбитра

Z_1	Z_2	класс
1	0	чистый
0	1	вредоносный
0	0	не определено

Если выходные значения арбитра имеют нулевые значения, то сканируемый файл отправляется на дополнительную проверку другому нейросетевому иммунному детектору.

В данном разделе предложена архитектура нейросетевого иммунного детектора, которая состоит из трех слоев нейронных элементов и арбитра. Она характеризуется малым объемом обучающей выборки и соотношением количества нейронов в слое Кохонена, характеризующих соответственно чистый и вредоносный классы кратно 4/1. Представлен алгоритм обучения нейросетевых иммунных детекторов.

3. Алгоритм функционирования нейросетевого иммунного детектора. В процессе сканирования проверяемого файла на нейросетевой детектор последовательно подаются фрагменты файла по методу скользящего окна.

Алгоритм функционирования нейросетевого иммунного детектора в режиме сканирования файла можно свести к следующей последовательности шагов:

1. Устанавливаются следующие начальные значения:

$$\overline{Y_1}(k-1) = 0, \overline{Y_2}(k-1) = 0. \quad (26)$$

2. По методу скользящего окна последовательно подаются входные образы (k=1, L) из сканируемого файла на нейронную сеть и для каждого входного образа производятся следующие вычисления:

- определяется Евклидово расстояние между входным образом и весовыми векторами нейронов слоя Кохонена (15);
- определяется нейронный элемент-победитель с номером k (16);

вычисляются выходные значения линейных нейронных элементов третьего слоя (18);

определяется количество чистых и вредоносных фрагментов сканируемого файла:

$$\overline{Y_1}(k) = \overline{Y_1}(k-1) + Y_1^k, \quad (27)$$

$$\overline{Y_2}(k) = \overline{Y_2}(k-1) + Y_2^k. \quad (28)$$

3. Вычисляются вероятности принадлежности сканируемого файла соответственно к чистому и вредоносному классу (22) и (23) соответственно.

4. На основании вычислений вероятностей принимается решение о принадлежности сканируемого файла к одному из классов, в соответствии с (24) и (25).

5. Если *Z1=0* и *Z2=0*, то назначается другой нейросетевой иммунный детектор для повторной проверки файла.

В данном разделе представлен алгоритм функционирования нейросетевого иммунного детектора. Он позволяет обнаруживать вредоносные программы, которые не входили в обучающую выборку, и в то же время «игнорировать» чистые файлы, не имеющие вредоносных функций.

4. Результаты исследований. В табл. 2 представлены результаты сравнительного анализа обнаружения вредоносных программ различными антивирусными продуктами. Для теста были выбраны следующие антивирусные продукты: Антивирус Касперского с актуальными вирусными базами; Антивирус Касперского с устаревшими вирусными базами; антивирусный продукт NOD 32 с отключенными вирусными базами, но с задействованным эвристическим анализатором и разработанная нами нейросетевая искусственная иммунная система. В таблице «ОК» означает решение антивирусной программы о том, что файл является чистым.

Как видно из полученных результатов, антивирус с актуальными вирусными базами обнаружил все вредоносные программы, которые

использовались в эксперименте. Это объясняется тем, что в антивирусных базах содержались сигнатуры используемых в эксперименте вредоносных программ. Антивирус с устаревшими базами обнаружил только половину присутствующих вирусов, что наглядно отражает неспособность сигнатурного метода обнаруживать неизвестные вредоносные программы. Антивирус NOD 32, который использовал эвристический анализатор, обнаружил только семь вирусов, что является очень низким показателем для надежной современной системы безопасности и отражает проблемную ситуацию обнаружения неизвестных вредоносных программ с помощью эвристических методов. Искусственная иммунная система показала наилучшие результаты.

Один нейросетевой иммунный детектор способен обнаруживать несколько вредоносных программ. Причем детектор приобретает способность обнаруживать принципиально новые вредоносные программы.

Таблица 2 - Результаты сравнительного анализа обнаружения

Имя файла	Антивирус Касперского (актуал. базы)	Антивирус Касперского (устар. базы)	NOD32 (эвристическ. анализатор)	ИИС (на основе 4-х детекторов)
Backdoor.Win32.Agent.lw	*Backdoor*	OK	OK	OK
Backdoor.Win32.Agobot	*Backdoor*	Backdoor	Win32/Agobot	Вирус
Email-Worm.BAT.Maddas	*Email-Worm*	Email-Worm	OK	Вирус
Email-Worm.JS.Gigger	*Email-Worm*	Email-Worm	OK	Вирус
Email-Worm.VBS.Loding	*Email-Worm*	Email-Worm	OK	Вирус
Email-Worm.Win32.Zafi.d	*Email-Worm*	OK	NewHeur_PE	Вирус
Net-Worm.Win32.Bozori.a	*Net-Worm*	OK	Win32/Bozori	Вирус
Net-Worm.Win32.Mytob.a	*Net-Worm*	OK	Win32/Mytob	Вирус
Trojan-Downl.JS.Psyme.y	*Trojan*	OK	OK	Вирус
Trojan-Downl.Win32.Bagle	*Trojan*	OK	Win32/Bagle	Вирус
Trojan-Proxy.Daemonize	*Trojan*	Trojan	OK	OK
Trojan-Proxy.Mitglieder	*Trojan*	Trojan	Win32/Trojan	Вирус
Trojan-Proxy.Win32.Agent	*Trojan*	Trojan	OK	Вирус
Trojan-PSW.LdPinch	*Trojan*	Trojan	Win32/PSW	Вирус
Virus.Win32.Gpcode.ac	*Virus.Win32*	OK	OK	Вирус

Выводы. Разработана структура нейросетевого иммунного детектора для обнаружения вредоносных программ, которая состоит из трех слоев нейронных элементов и арбитра. Она характеризуется малым объемом обучающей выборки и отношением количества нейронов в слое Кохонена, характеризующих соответственно чистый и вредоносный классы кратно 4/1. Предложенный нейросетевой иммунный детектор способен обнаруживать неизвестные вредоносные программы.

Разработан алгоритм обучения нейросетевого иммунного детектора, позволяющий эффективно обучать НИД для обнаружения вредоносных программ. При корректной классификации каждому образу соответствует не конкретный нейрон слоя Кохонена, а совокупность нейронных элементов.

Предложен алгоритм функционирования нейросетевых иммунных детекторов, который характеризуется вероятностным принципом работы, а также тем, что окончательный результат классификации происходит после подачи всех образов сканируемого файла на нейронную сеть. Отличительной особенностью алгоритма является способность НИД обнаруживать неизвестные вредоносные программы.

Получено приближенное выражение для оценки вероятности обнаружения вредоносной программы искусственной иммунной системой. Показано, что с увеличением количества детекторов увеличивается вероятность обнаружения. Предложена приближенная оценка количества детекторов для заданной вероятности обнаружения вредоносной программы.

Проведены эксперименты по тестированию нейросетевой искусственной иммунной системы. Они показали способность нейросетевых иммунных детекторов обнаруживать разнотипные неизвестные вредоносные программы. В отличие от известных антивирусных программ, нейросетевая искусственная иммунная система обнаруживает в среднем в 1,5 раза больше неизвестных вредоносных программ.

Приведены теоретическая и экспериментальная оценки вероятности обнаружения вредоносной программы в зависимости от количества детекторов.

Разработанная система может быть использована при построении как новых систем защиты компьютеров от вредоносных программ, так и в дополнении к уже имеющимся средствам.

ЛИТЕРАТУРА

1. Безобразов С. В. Искусственные иммунные системы для защиты информации: применение LVQ сети / С. В. Безобразов // Нейроинформатика-2007: материалы IX Всеросс. науч.-техн. конф.,

Москва, 23-26 января 2007 г. / Московский инженерно-физический институт (государственный университет). – Москва, 2007. – С. 27-35.

2. Безобразов С. В. Искусственные иммунные системы для защиты информации: обнаружение и классификация компьютерных вирусов / С. В. Безобразов, В. А. Головко // Научная сессия МИФИ «Нейроинформатика»: материалы Всеросс. науч. конф., МИФИ, Москва, 20-23 янв. 2008. – С. 23-27.

3. Bezobrazov, S. Neural Networks for Artificial Immune Systems: LVQ for Detectors Construction / S. Bezobrazov, V. Golovko // IDAACS'2007: proceedings of the 4 IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications. – Dortmund, 2007. – P. 180-184.

4. Bezobrazov, S. Neural networks and artificial immune systems – malware detection tool / S. Bezobrazov, V.Golovko // ICNNAI'2008: proceedings of the 5 International Conference on Neural Networks and Artificial Intelligence, Minsk, 27-30 May 2008. / Brest State University of Informatics and Radioelectronics. – Minsk, 2008. – P. 49-52.

5. Касперский Е. Компьютерное зловредство / Е. Касперский. – СПб.: Питер, 2007. – 208 с.

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

7. Хайкин С. Нейронные сети: полный курс / С. Хайкин. – М.: Вильямс, 2006. – 1104 с.

АЛГОРИТМИ ШТУЧНИХ ІМУННИХ СИСТЕМ І НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМ

Безобразов С.В., к.т.н., доц., Головко В.А., д.т.н., проф.
Брестський державний технічний університет
вул. Московська, 267, 224001, м. Брест, Республіка Бєларусь
E-mail: bescase@gmail.com, gva@bstu.by

У даній статті представлена архітектура нейромережевого імунного детектора, що входить до складу нейромережевої штучної імунної системи для виявлення шкідливих програм, а також алгоритми його навчання й функціонування.

Ключові слова: нейронна мережа, імунна система, шкідливі програми.

THE ALGORITHMS OF THE ARTIFICIAL IMMUNE SYSTEMS AND NEURAL NETWORKS FOR MALICIOUS CODE DETECTION

Bezobrazov S., Cand. of Sc. (Tech.), Assoc. Prof., Golovko V., Doc. Sc. (Tech.), Prof.
Brest State Technical University
Moskovskaja St., 267, 224001, Brest, Belarus
E-mail: bescase@gmail.com, gva@bstu.by

The article presents the architecture of the neural network immune detector of the neural network artificial immune system for malicious code detection also its algorithms of training and functioning.

Key words: neural network, immune system, malware.