OSTIS-2011
(Open Semantic Technologies for Intelligent Systems)

УДК 004.056.57:032.26

ПРОЕКТИРОВАНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ОБНАРУЖЕНИЯ АНОМАЛИЙ

В.А. Головко (*gva@bstu.by*)
Брестский государственный технический университет, г.Брест, Республика Беларусь

С.В. Безобразов (*bescase@gmail.com)*
Брестский государственный технический университет, г.Брест, Республика Беларусь

В работе приводятся основные принципы построения интеллектуальных систем для обнаружения компьютерных и медицинских атак, обнаружения вредоносных программ и диагностики эпилепсии. Для обнаружения компьютерных и медицинских атак применяются различные комбинации рециркуляционной нейронной сети и многослойного персептрона. Для обнаружения компьютерных вирусов используется подход, базирующийся на объединении искусственных иммунных и нейронных сетей. Детектирование эпилепсии базируется на вычислении старшего показателя Ляпунова, который характеризует степень хаотичности процесса.

Ключевые слова: обнаружение аномалий, вредоносные программы, компьютерные вирусы, диагностика эпилепсии, нейронные сети, искусственные иммунные системы.

Введение

В настоящее время все больше возрастает тенденция проектирования систем искусственного интеллекта на основе нейронных сетей, искусственных иммунных систем, эволюционного программирования и других, биологически инспирированных подходов. Это связано с различными аспектами в развитии искусственного интеллекта. Первый состоит в способности нейроинтеллектуальных систем к обучению и самоорганизации, что позволяет создавать на базе их различные системы, обладающие свойством адаптации к внешней среде. Второй аспект этой проблемы характеризуется способностью нейроинтеллектуальных систем после обучения обобщать и прогнозировать результаты обучения. Такое обобщение осуществляется путем интеграции частных данных, в результате чего происходит определение закономерностей процесса. Третий аспект заключается в способности таких систем решать трудно-формализуемые задачи, для которых не существует эффективного математического алгоритма. Все это позволяет создавать на базе биологических подходов интеллектуальные системы в различных областях применения. Такие интеллектуальные системы способны к самоорганизации с целью адаптации к внешней среде. Исследования в области нейроинтеллекта ориентированы в настоящее время в основном на создание специализированных систем для решения конкретных задач. Однако, несмотря на большое количество исследований по данной проблеме, в настоящее время практически отсутствует эффективный теоретический аппарат построения нейроинтеллектуальных систем для решения различных задач. Особенно актуальным в области проектирования нейроинтеллектуальных систем является интеграция различных подходов, таких как нейронные сети, искусственные иммунные системы и эволюционное программирование.

В данной статье рассматриваются принципы построения интеллектуальных систем для обнаружения аномалий. В качестве аномалий здесь рассматриваются как вредоносные

воздействия на компьютерные системы (вирусы, атаки), так и нарушения нормальной активности головного мозга (транзиторно-ишемические атаки, эпилептиформная активность), которые могут привести к катастрофическим последствиям. Для таких процессов большое значение имеет оперативное обнаружение аномалий, чтобы предотвратить катастрофическое развитие ситуации.

В данной статье рассматриваются различные подходы проектирования интеллектуальных систем. В первом разделе приводится объединение двух классов нейронных сетей для обнаружения компьютерных атак и атак на нормальное кровоснабжение головного мозга. Во втором разделе рассматривается интеграция нейронных и искусственных иммунных систем для обнаружения компьютерных вирусов. В третьем разделе предлагается метод обнаружения эпилептической активности на основе анализа сигналов электроэнцефалограмм (EEG), который основан на интеграции нейронных сетей и теории хаоса.

1. Комбинирование нейронных сетей для обнаружения атак на компьютерные системы и на нормальное кровоснабжение мозга

Вредоносные воздействия (атаки, вторжения) на нормально протекающие процессы существуют в различных областях практической деятельности. Таким атакам подвергаются как компьютерные системы, так и живые организмы и, прежде всего мозг. Несмотря на различные объекты воздействия атак, концептуальные подходы к проблеме обнаружения вредоносных воздействий, как в компьютерных системах, так и в отдельном живом организме, могут быть идентичными. В данном разделе приводится нейросетевая технология обнаружения вредоносных атак, как на нормальное кровоснабжение головного мозга, так и на компьютерные системы.

Транзиторно-ишемическая атака (ТИА) на нормальное кровоснабжение головного мозга это самостоятельная гетерогенная нозологическая единица, которая характеризует предынсультное состояние [Мастыкин и др., 2010]. Основная задача состоит в раннем обнаружении ТИА, для того чтобы предупредить последующие серьезные нарушения мозгового кровообращения. В общем случае транзиторно-ишемические атаки можно разделить на три подтипа ТИА и класс НОРМА: 1.атеротромботический подтип (СубТИА1), 2. кардиоэмболический подтип (СубТИА2), 3. гипертензивный подтип (СубТИА3), 4. норма (НОРМА). В качестве входных данных используется 41-размерный вектор, который характеризует исходные данные (признаки и симптомы) пациента, такие как возраст, хронический бронхит, диастолическое давление и т.д. [Мастыкин и др., 2010]. В качестве выходных данных используется 4-мерный вектор, где 4 это количество классов ТИА плюс нормальное состояние.

Компьютерные атаки можно разделить на четыре основные категории: DoS, U2R, R2L и Probe [KDD, 1999], [Golovko et al., 2006]. Атака DoS – отказ в обслуживании, характеризуется генерацией большого объема трафика, что приводит к перегрузке и блокированию сервера. Атака U2R предполагает получение зарегистрированным пользователем привилегий локального суперпользователя (администратора). Атака R2L характеризуется получением доступа незарегистрированного пользователя к компьютеру со стороны удаленной машины. Атака Probe заключается в сканировании портов с целью получения конфиденциальной информации.

В качестве входных данных используются параметры сетевого соединения [Golovko et al., 2007], [Golovko et al., 2010]. Соединение это последовательность TCP пакетов за некоторое конечное время, моменты начала и завершения которого четко определены, в течение которого данные передаются от IP-адреса источника на IP-адрес приемника (и в обратном направлении) используя некоторый определенный протокол. Каждое сетевое соединение характеризуется 41-им параметром сетевого трафика. В качестве выходных данных используется 5-мерный вектор, где 5 это количество классов атак плюс нормальное состояние. Таким образом, задачи обнаружения компьютерных атак и атак на нормальное кровоснабжение мозга являются идентичными.

Рассмотрим нейросетевой подход решения данных задач, который состоит в последовательном объединении двух различных нейронных сетей. На рисунке 1 приведена система распознавания классов атак, которая состоит из рециркуляционной нейронной сети

(RNN) и многослойного персептрона (MLP), которые соединены последовательно [Головко, 2001]. Задачей такой системы является обнаружение и распознавание атак.

На первом этапе обработки входной информации происходит уменьшение размерности входного 41-размерного вектора входных данных в 12-размерный вектор выходных данных при помощи нелинейной рециркуляционной нейронной сети. Это позволяет перейти от исходного пространства данных к вспомогательному, которое характеризуется меньшей размерностью и информативностью исходного пространства. В результате экспериментов было определено оптимальное число главных компонент равное 12. Второй этап состоит в обнаружении и распознавании атак. Для этого используется многослойный персептрон, который осуществляет обработку сжатого пространства входных образов с целью распознавания класса атаки.

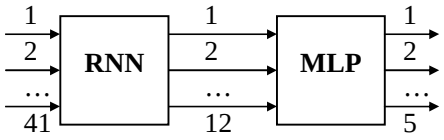

Рисунок 1 – Нейросетевая система обнаружения атак

Рассмотрим нелинейную рециркуляционную сеть, которая представляет собой нелинейный репликатор (рисунок 2).

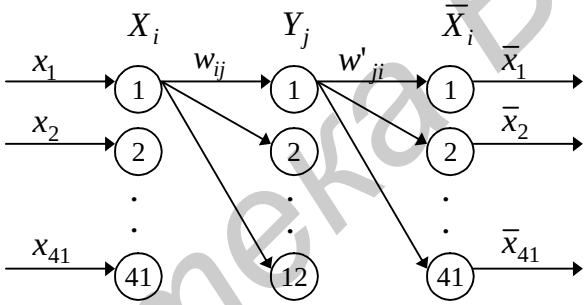

Рисунок 2 – Архитектура RNN

Такая сеть состоит из трех слоев. Скрытый слой осуществляет сжатие входных образов. Значение j-го элемента скрытого слоя определяется по формулам:

$$y_j = F(S_j), \tag{1}$$

$$S_j = \sum_{i=1}^{41} w_{ij} \cdot x_i, \tag{2}$$

где F – функция активации; S_j – взвешенная сумма j-го нейрона; w_{ij} – весовой коэффициент между i-ым нейроном входного и j-ым нейроном скрытого слоя; x_i – i-ый входной элемент.

Значения нейронных элементов выходного слоя определяются следующим образом:

$$\overline{x}_i = F(S_i), \tag{3}$$

$$S_i = \sum_{i=1}^{12} w'_{ji} \cdot y_j, \tag{4}$$

где w'_{ji} – весовой коэффициент между j-ым нейроном скрытого и i-ым нейроном выходного слоя; $\overline{x}_i$ – i-ый выходной элемент.

Для обучения нелинейной RNN использовался алгоритм обратного распространения ошибки. В соответствии с ним весовые коэффициенты модифицируются по следующим выражениям:

$$w_{ij}(t+1) = w_{ij}(t) - \alpha \cdot \gamma_j \cdot F'(S_j) \cdot x_i, \tag{5}$$

$$w'_{ij}(t+1) = w'_{ij}(t) - \alpha \cdot y_j \cdot F'(S_i)(\overline{x_i} - x_i), \tag{6}$$

где γ_j - ошибка j-го нейрона, $F'(S_j)$ – производная нелинейной функции активации по взвешенной сумме.

$$\gamma_j = \sum_{i=1}^{41} (\overline{x_i} - x_i) \cdot F'(S_i) \cdot w'_{ji}. \tag{7}$$

В процессе обучения весовые коэффициенты скрытого слоя ортонормируются в соответствии с процедурой Грамма-Шмидта. Рассмотрим отображение входного пространства образов для нормального состояния и компьютерной атаки (тип атаки neptune) на плоскость двух первых главных компонент. Из рисунка 3 видно, что данные, соответствующие разным классам концентрируются в разных областях.

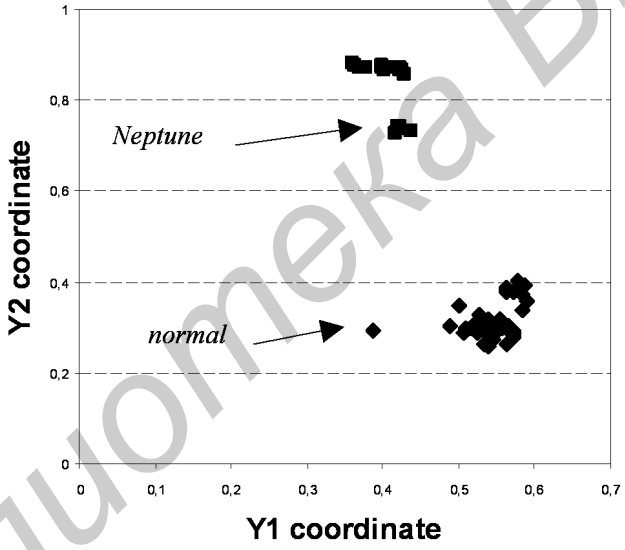

Рисунок 3 – Данные обработанные нелинейной RNN

Для обучения и тестирования использовалась база данных для 101 пациента. Каждая запись соответствует одной из четырех групп классификации ТИА. Распределение записей по классам следующее: ТИА1 – 22 записи, ТИА2 – 22 записи, ТИА3 – 22 записи и ТИА4 (норма) – 35 записей. Для обучения нейронных сетей в экспериментах использовались обучающие выборки размерностью 51 и 83. Результаты тестирования приведены в таблице 1.

Таблица 1 – Результаты тестирования для ТИА

Кол-во образов в обучающей выборке	Кол-во образов в тестовой выборке	Максимальный процент распознавания на обучающей выборке	Максимальный процент распознавания на тестовой выборке
51	50	100%	76%
83	18	100%	77%

Для системы обнаружения компьютерных атак использовалась 10% выборка из базы KDD (почти 500 000 записей!). Для обучения нейронных сетей были отобраны 6186 примеров. Далее вся 10% выборка применялась для тестирования. Результаты тестирования в режиме распознавания класса атаки приведены в таблице 2.

Таблица 2 – Результаты тестирования для компьютерных атак

класс	всего	обнаружено	распознано
DoS	391458	391441 (99.99%)	370741 (94.71%)
U2R	52	48 (92.31%)	42 (80.77%)
R2L	1126	1113 (98.85%)	658 (58.44%)
Probe	4107	4094 (99.68%)	4081 (99.37%)
нормальное состояние			
normal	97277	---	50831 (52.25%)

Наилучший результат был достигнут для атак класса DoS и Probe (почти однозначная распознаваемость). Несколько хуже определяются U2R и R2L, соответственно 80,77% и 58,44%.

Таким образом, путем комбинирования двух различных нейронных сетей, а именно RNN и MLP, можно идентифицировать и распознавать компьютерные и медицинские атаки с достаточно высокой степенью точности. Основными преимуществами использования подходов, основанных на нейронных сетях, является способность адаптироваться к динамическим условиям и быстрота функционирования, что особенно важно при работе системы в режиме реального времени.

2. Интеграция искусственных иммунных и нейронных сетей для обнаружения вредоносных программ

В настоящее время количество вредоносных программ и компьютерных вирусов постоянно увеличивается. Ущерб, наносимый вредоносными программами, составляет, по некоторым подсчетам, миллиарды долларов в год [ВирусБлокАда, 2007]. Как показала практика, традиционный подход в области обнаружения вредоносных программ, основанный на сигнатурном анализе, не приемлем для обнаружения неизвестных компьютерных вирусов. Основным недостатком сигнатурного анализа является необходимость в постоянном своевременном обновлении антивирусных баз, в которых хранятся сигнатуры известных вирусов. Вторым недостатком является задержка в ответной реакции антивирусной индустрии на появление нового вируса, которая может достигать нескольких суток. За это время вредоносные программы способны заразить сотни тысяч компьютерных систем по всему миру и привести к огромным убыткам. Для устранения недостатков методов сигнатурного анализа в антивирусных программах применяются разнообразные эвристические алгоритмы обнаружения вредоносных программ, которые основываются на анализе поведения подозрительных объектов, а также анализе их исполняемого кода. Эвристические алгоритмы позволяют с определенной долей вероятности выдавать заключение о вредоносности программ. Однако, такие алгоритмы на сегодняшний день характеризуются высоким уровнем ошибок первого и второго рода. Поэтому актуальной задачей является разработка эффективных методов обнаружения вредоносных программ, которые способны обнаруживать неизвестные компьютерные вредоносные программы.

В данном разделе рассматривается интеллектуальная система обнаружения компьютерных вирусов [Безобразов и др., 2010a], [Безобразов и др., 2010b], [Bezobrazov et al., 2010], которая базируется на применении искусственных иммунных систем и нейронных сетей. Такая система

использует основные принципы функционирования биологической иммунной системы, где в качестве отдельного детектора используется нейронная сеть.

На рисунке 4 представлена структура нейросетевой искусственной иммунной системы для обнаружения вредоносных программ. Она состоит из следующих основных модулей: модуль генерации детекторов, модуль обучения иммунных детекторов, модуль отбора детекторов, модуль уничтожения детекторов, модуль обнаружения вредоносных программ, модуль идентификации вирусов, модуль клонирования и мутации детекторов, модуль формирования иммунной памяти.

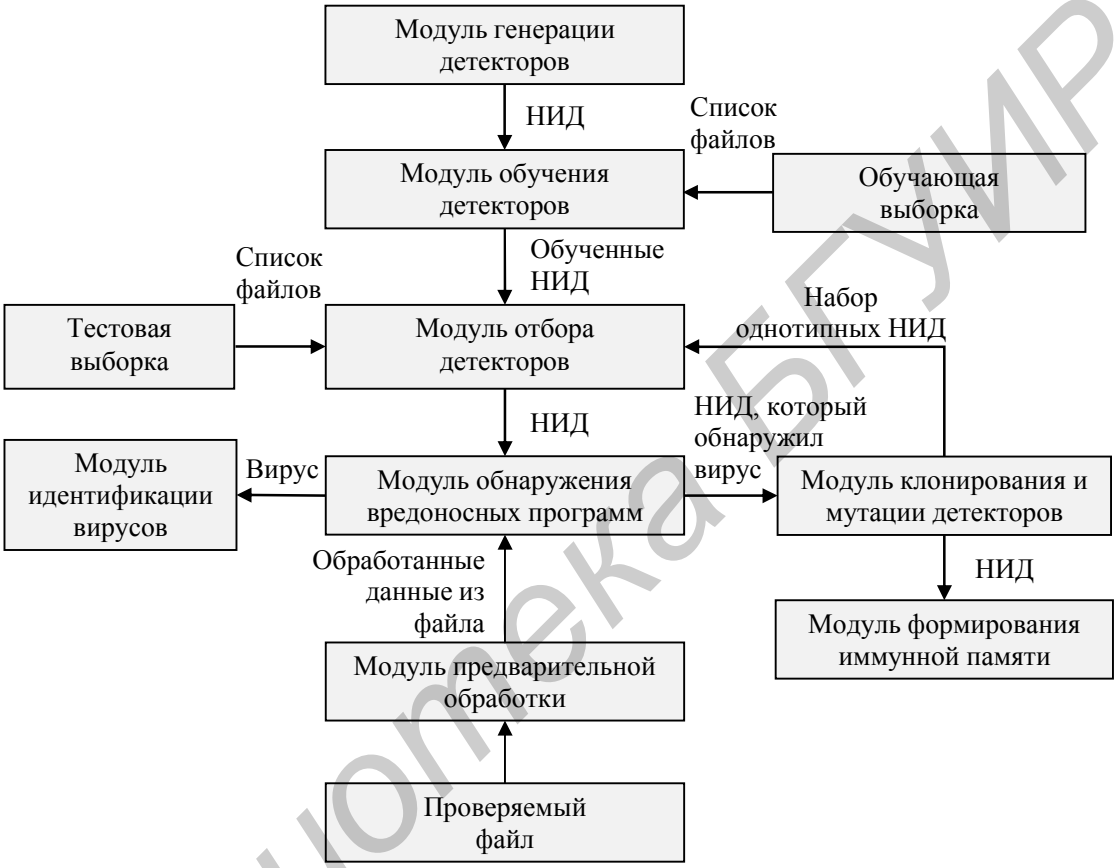

Рисунок 4 – Структура нейросетевой искусственной иммунной системы для обнаружения вредоносных программ

Нейросетевые иммунные детекторы играют ключевую роль в обнаружении вредоносных программ. Пройдя стадии обучения и отбора, детекторы приобретают способность реагировать на вредоносные программы, сканируя их структуру, и, в то же время, игнорировать чистые файлы.

Функционирование нейросетевого иммунного детектора заключается в последовательности следующих действий:

1) Случайным образом из списка существующих файлов нейросетевой иммунный детектор выбирает файл для проверки.

2) Данные из файла проходят предварительную обработку, связанную с удалением «дыр» и незначащих нулей.

3) По методу скользящего окна, детектор сканирует файл и принимает решение о принадлежности проверяемого файла к классу чистых или к классу вредоносных программ.

4) Если нейросетевой иммунный детектор принимает решение о принадлежности проверяемого файла к классу чистых программ, детектор выбирает новый файл для проверки.

5) Если нейросетевой иммунный детектор принимает решение о принадлежности проверяемого файла к классу вредоносных программ, он подает сигнал об обнаружении компьютерного вируса и нейросетевая иммунная система переходит в особый режим функционирования.

На рисунке 5 представлен нейросетевой иммунный детектор. Он состоит из нейронной сети встречного распространения [Головко, 2001] и арбитра. Нейронные элементы скрытого слоя функционируют по принципу «победитель берет все», то есть выходное значение нейрона-победителя равняется «1», а выходные значения остальных нейронных элементов равняются «0».

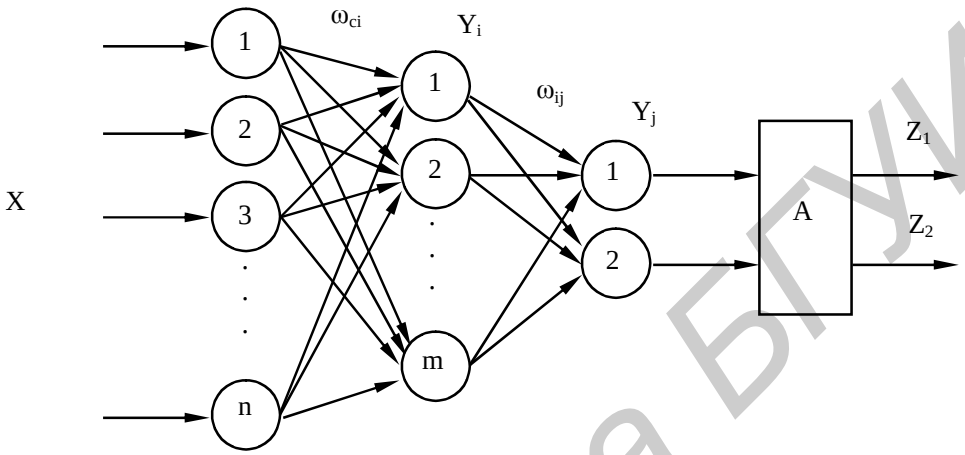

Рисунок 5 – Нейросетевой иммунный детектор

Выходное значение j-го нейрона третьего слоя определяется согласно формуле:

$$Y_j = \omega_{kj} \cdot Y_k. \tag{8}$$

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

$$\overline{Y_1} = \sum_{k=1}^{L} Y_1^k, \tag{9}$$

$$\overline{Y_2} = L - \overline{Y_1} = \sum_{k=1}^{L} Y_2^k, \tag{10}$$

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

$$P_T = \frac{\overline{Y_1}}{L} \cdot 100\%, \tag{11}$$

$$P_F = 1 - P_T = \frac{\overline{Y_2}}{L} \cdot 100\%. \tag{12}$$

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

$$Z_1 = \begin{cases} 1, & \text{если } P_T > 80\% \\ 0, & \text{иначе.} \end{cases} \quad (13)$$

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

$$Z_2 = \begin{cases} 1, & \text{если } P_F > 20\% \\ 0, & \text{иначе.} \end{cases} \quad (14)$$

Таким образом, пространство выходных значений арбитра можно представить в табличном виде (таблица 3).

Таблица 3 – Пространство выходных значений арбитра

Z_1	Z_2	класс
1	0	Чистый
0	1	Вирус
0	0	Не определено

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

В процессе сканирования проверяемого файла на нейросетевой детектор последовательно подаются фрагменты файла по методу скользящего окна.

Как было отмечено ранее, один иммунный детектор, благодаря нейросетевой архитектуре способен обнаруживать несколько вредоносных программ. Причем, детектор приобретает способность обнаруживать принципиально новые вредоносные программы.

Сравнительный анализ результатов обнаружения неизвестных вредоносных программ различными антивирусными программами показал, что разработанный нами иммунологический подход позволяет качественнее детектировать неизвестные вредоносные программы.

3. Интеграция нейронных сетей и теории хаоса для обнаружения эпилептической активности

В данном разделе рассматривается интеллектуальная система для определения эпилептической активности на основе анализа сигналов EEG, которые отражают суммарную биоэлектрическую активность головного мозга и способны хранить в себе информацию о функциональном состоянии мозга, общемозговых расстройствах и их характере [Карлов, 1990].

В качестве диагностического критерия используется значение старшего показателя Ляпунова, которое является положительным при хаотическом поведении системы, и снижается при наступлении эпилептических припадков [Maiwald et al., 2004]. Наличие у системы положительной экспоненты Ляпунова свидетельствует о том, что любые две близкие траектории быстро расходятся с течением времени, то есть имеет место чувствительность к значениям начальных условий. На рисунке 6 представлена нейросетевая система обнаружения аномалий в сигнале ЭЭГ. На вход системы поступает набор сигналов ЭЭГ одной регистрации. Система производит предобработку сигналов, чтобы отфильтровать сигналы ЭЭГ от шумов и артефактов (помехи, появляющиеся на ЭЭГ в результате моргания, движения подбородком и т.п.). Наиболее эффективным для такой обработки ЭЭГ является метод независимых компонент (ICA - Independent Component Analysis) [Hyvaerinen et al., 2000]. Результатом предобработки являются чистые сигналы ЭЭГ, содержащие электрическую активность головного мозга.

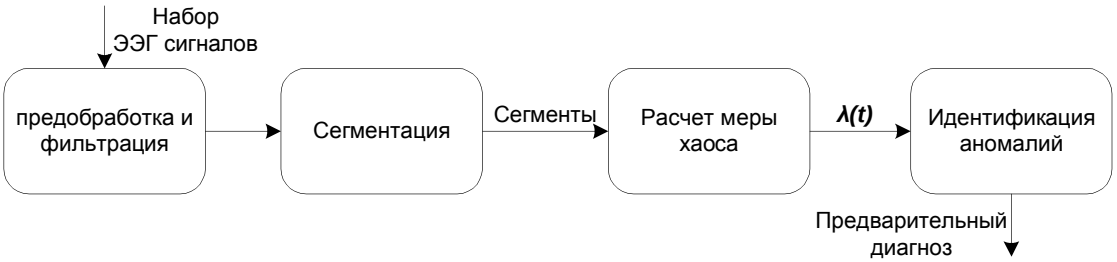

Рисунок 6 – Нейросетевая система обнаружения эпилептиформной активности; на вход системы подается набор сигналов электроэнцефалограмм; $\lambda(t)$ - ряд значений старшего показателя Ляпунова

Каждый сигнал, полученный после фильтрации, подвергается адаптивной сегментации при помощи многослойного персептрона (MLP). Затем для каждого выделенного сегмента производится вычисление старшего показателя Ляпунова. Таким образом, после расчета меры хаоса получается детерминированный ряд показателей Ляпунова для каждого чистого сигнала EEG.

$$\lambda(t) = (\lambda_1, \lambda_2, ...), \tag{15}$$

Идентификация аномалий производится в соответствии со следующим критерием:

$$\begin{cases} \lambda > 0, \textit{нормальная активность}; \\ \lambda \le 0, \textit{эпилептиформная активность}. \end{cases} \tag{16}$$

Для расчета старшего показателя Ляпунова используется подход, базирующийся на применении прогнозирующей нейронной сети [Головко и др., 2004], [Golovko et al., 2004], [Головко, 2005], [Golovko et al., 2007]. Для этого необходимо вначале определить временную задержку τ и размерность пространства вложения m. В качестве нейронной сети используется многослойный персептрон, который состоит из $k \ge m-1$ входных нейронов, p скрытых и одного выходного нейронного элемента. Здесь m – размерность пространства вложения. Вначале необходимо обучить такую нейронную сеть прогнозированию в соответствии с методом скользящего окна:

$$x(t+i\tau)=F(x(t+(i-1)\tau), x(t+(i-2)\tau),\ldots, x(t+(i-k)\tau)), \quad i=\overline{1,n}, \tag{17}$$

где τ – временная задержка.

После обучения сети легко осуществить эволюцию двух точек на фазовой траектории, используя итерационный подход. Таким образом, ключевой идеей предлагаемого метода является вычисление при помощи прогнозирующей нейронной сети расхождения двух близлежащих траекторий на n шагов вперёд, используя итерационный подход. Схематично процедура вычисления старшего показателя Ляпунова представлена на рисунке 7.

По полученному значению старшего показателя Ляпунова можно судить о состоянии системы. В частности, если значение показателя снижается, то при анализе сигналов EEG это свидетельствует о наличие аномалии в сигнале . Данный метод позволяет достаточно просто вычислить старший показатель Ляпунова при малом объеме экспериментальных данных.

Рассмотрим результаты экспериментов. В качестве исходных данных использовались EEG данные для двух пациентов Брестской областной больницы (таблица 4). У каждого пациента снимались данные EEG в течение 10 секунд. Эти данные представляют собой набор из 19 сигналов по количеству установленных на голове электродов как показано на рисунке 8.

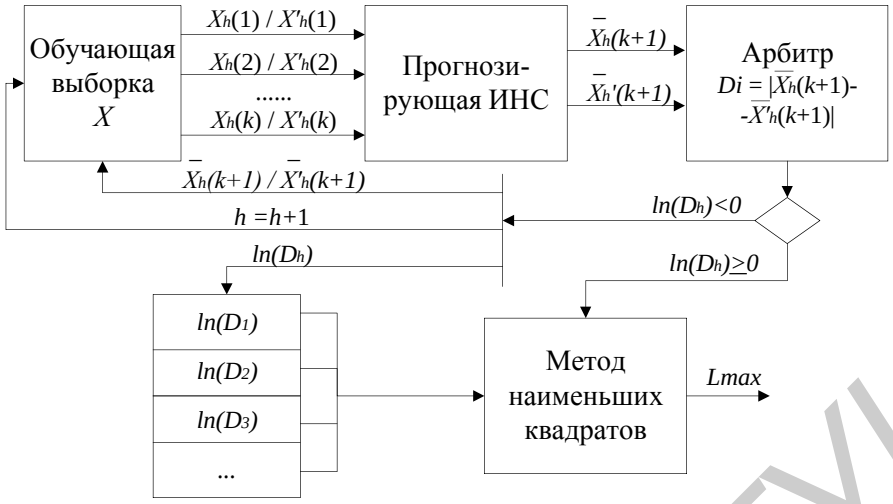

Рисунок 7 – Схема расчета старшего показателя Ляпунова

Таблица 4 – Описание исходных данных (EEG) для тестирования системы

Обозна-чение	Возраст пациента	Диагноз	Форма активности	Тип эпилептиформной активности
1Э	30	Эпилепсия	Генерализо-ванная	Комплексы острая - медленная волны в ϑ и Δ диапазонах
2Н	56	Условная норма	-	-

Примечание - Под условной нормой понимается отсутствие в сигнале ЭЭГ эпилептической активности.

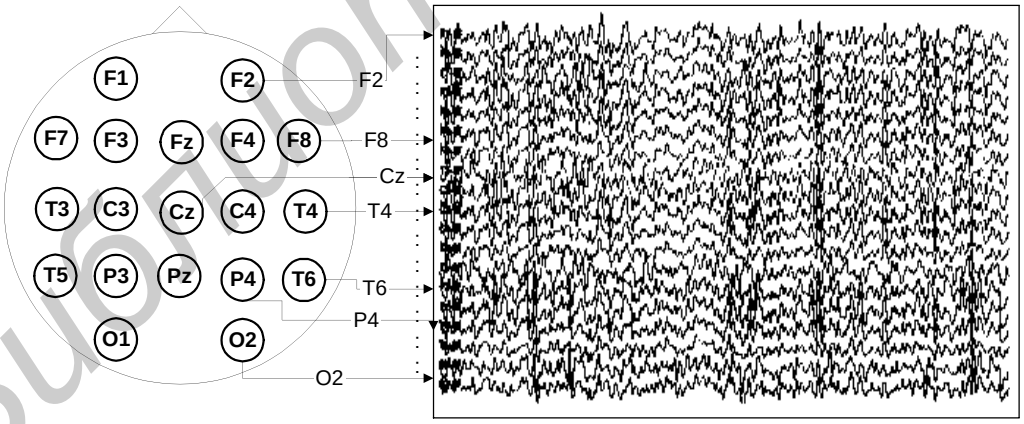

Рисунок 8 – Пример регистрации электроэнцефалограммы

Так как сигнал снимается с кожи головы, то он может содержать шумы и артефакты (электрические сигналы, являющиеся результатом моргания глаз, сердечной активности и т.п.).

Для выделения электрической активности мозга используем метод независимых компонент ICA, который позволяет из линейных смесей независимых сигналов от различных источников выделить исходные несмешанные сигналы. Сигналы разделяются на восемь групп по зонам головы:

- лобная левая FL = {F1, F3, F7,Fz};
- лобная правая FR = {F2, F4, F8,Fz};

- височная левая TL = {T3, T5, C3, Cz};
- височная правая TR = {T4, T6, C4, Cz};
- теменная левая PL = {P3, C3, Pz, Cz};
- теменная правая PR = {P4, C4, Pz, Cz };
- затылочная левая OL = {O1, Pz, Cz};
- затылочная правая OR = {O2, Pz, Cz};

для левого и правого полушария соответственно.

Таким образом, после фильтрации получаем 8 сигналов ЭЭГ, которые подвергаются сегментации и анализу по представленной схеме. Результаты обнаружения эпилептической активности в сигналах ЭЭГ для первых данных (1Э), приведенных в таблице 4, показаны на рисунке 9.

Как видно из рисунка 9 эпилептическая активность (черная область) возникает генерализованно, то есть одновременно во всех областях головы в левом и правом полушарии, что соответствует генерализованной форме активности, установленной врачом. Для данных, обозначенных в таблице 4 идентификатором 2Н, было проведено аналогичное исследование, в результате которого эпилептических форм активности не было выявлено.

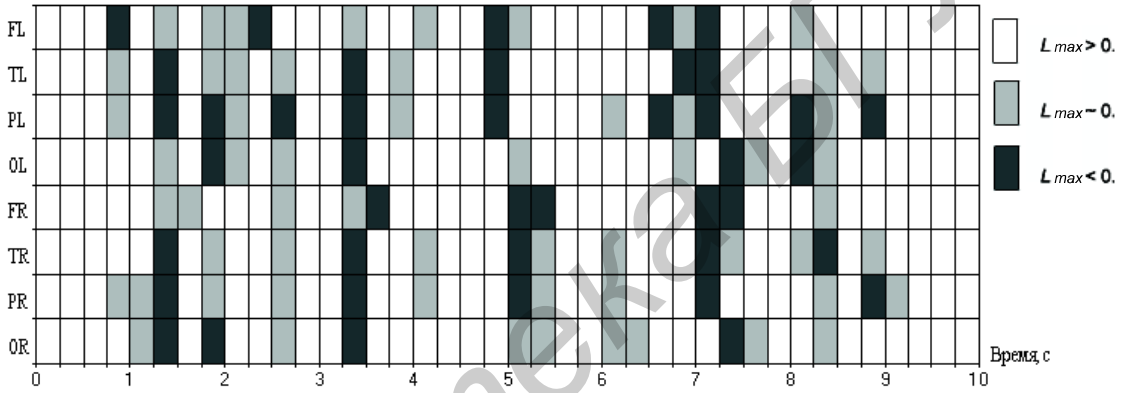

Рисунок 9 – Результаты работы экспериментальной системы в виде двумерной карты обнаружения эпилептической активности по значению старшего показателя Ляпунова L_{max}

Как показали эксперименты разработанная система показала способность выполнять классификацию EEG данных на два состояния (нормальная и эпилептическая активность) с 99,6% вероятностью.

Заключение

В данной статье рассмотрены основные принципы построения интеллектуальных систем для обнаружения компьютерных и медицинских атак, обнаружения вредоносных программ и диагностики эпилепсии. Для обнаружения компьютерных и медицинских атак применяются различные комбинации рециркуляционной нейронной сети и многослойного персептрона. Для обнаружения вредоносных программ и компьютерных вирусов используется подход, базирующийся на объединении искусственных иммунных и нейронных сетей. Детектирование эпилепсии базируется на вычислении старшего показателя Ляпунова, который характеризует степень хаотичности процесса. Для определения старшего показателя Ляпунова используется многослойный персептрон. Эксперименты показали эффективность предложенных подходов. Авторы выражают глубокую признательность сотрудникам кафедры «Интеллектуальне информационные технологии» Брестского государственного технического университета Лаврентьевой С.В., Кочурко П.А. и Войцеховичу Л.Ю. за помощь в подготовке статьи.

Библиографический список

[Безобразов и др., 2010а] Безобразов, С.В. Алгоритмы искусственных иммунных систем и нейронных сетей для обнаружения вредоносных программ / С.В. Безобразов, В.А. Головко // Научная

сессия НИЯУ МИФИ «Нейроинформатика»: материалы Всеросс. науч. конф., МИФИ, Москва, 25-29 янв. 2010. – Москва, 2010. – С. 273-287.

[Безобразов и др., 2010b] Безобразов, С.В. Применение нейросетевых детекторов в искусственных иммунных системах для обнаружения и классификации компьютерных вирусов / С.В. Безобразов, В.А. Головко // Нейрокомпьютеры. – 2010. – № 5. – С. 17-31.

[ВирусБлокада, 2007] Пресс-Центр // Антивирус ВирусБлокАда [Электронный ресурс]. – 2005. – Режим доступа: http://www.anti-virus.by/press/viruses/1485.html. – Дата доступа: 25.08.2007.

[Головко, 2001] Головко В.А. Нейронные сети: обучение, организация и применение: Кн. 4: учеб. пособие для вузов/ Общая ред. А.И. Галушкина. – М.: ИПРЖР, 2001. – 256 с.

[Головко, 2005] Головко В.А. Нейросетевые методы обработки хаотических процессов // В книге «Лекции по Нейроинформатике». – М.: МИФИ, 2005. – С. 43-88.

[Головко и др., 2004] Головко В.А., Чумерин Н.Ю. Нейросетевые методы определения спектра Ляпунова хаотических процессов // Нейрокомпьютеры: разработка и применение, 2004. – №1.

[Карлов, 1990] Карлов В.А Эпилепсия. – М.: Медицина, 1990. - 336с.

[Мастыкин и др., 2010] Мастыкин, А.С. Нейросетевой подход к решению проблемы предотвращения атак на нормальное кровоснабжение мозга // А.С.Мастыкин, В.В.Евстигнеев, В.А.Головко, Е.Н.Апанель, Г.Ю.Войцехович // Доклады Академии наук Беларуси. – 2010. – Т.54 – № 5. – С. 81–90.

[Bezobrazov et al., 2010] Bezobrazov, S. Artificial immune systems of the neural network for the malicious code detection / S. Bezobrazov, V.Golovko // ICNNAI'2010: proceedings of the 6th International Conference on Neural Networks and Artificial Intelligence, Brest, 1-4 June 2010. / Brest State Technical University. – Brest, 2010. – P. 147-153.

[Golovko et al., 2010] Golovko, V. S. Bezobrazov, P. Kachurka, L. Vaitsekhovich. Neural Network and Artificial Immune Systems for Malware and Network Intrusion Detection / V. Golovko, S. Bezobrazov, P. Kachurka, L. Vaitsekhovich // Studies in computational intelligence. – Springer Berlin/Heidelberg, 2010. – Vol. 263: Advances in machine learning II. – P. 485–513.

[Golovko et al., 2007] Golovko, V., Bezobrazova, S., Bezobrazov, S., Rubanau, U. Application of Neural Networks to the Electroencephalogram Analysis for Epilepsy Detection // Proceedings of the International Joint Conference on Neural Networks (IJCNN 2007), Orlando, FL , USA- Orlando, 2007. - P. 2707-2711.

[Golovko et al., 2004] Golovko, V., Doudkin, A., Maniakov, N. Application of Neural Networks Techniques to Chaotic Signal Processing //Optical Memory and Neural Networks. – 2004. - Vol.13, N. 4. - P.195-215.

[Golovko et al., 2006] Golovko, V., Vaitsekhovich, L. Neural Networks approaches for Intrusion Detection and Recognition / V. Golovko, L. Vaitsekhovich // Computing. – 2006. - Vol. 5, N.3. - P. 118-125.

[Golovko et al., 2007] Golovko, V., Vaitsekhovich, L., Kochurko, P., Rubanau, U. Dimensionality Reduction and Attack Recognition using Neural Network Approaches / V. Golovko, L. Vaitsekhovich, P. Kochurko, U, Rubanau // Proceedings of the International Joint Conference on Neural Networks (IJCNN 2007), Orlando, FL, USA – Orlando, 2007. - P. 2734-2739.

[Hyvaerinen et al., 2000] Hyvaerinen A., Oja E. Independent component analysis: algorithms and applications // Neural Networks, №13, 2000, - P. 411-430.

[KDD, 1999] 1999 KDD Cup Competition. - Information on: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[Maiwald et al., 2004] Maiwald Th., Winterhalder M., Aschenbrenner-Scheibe R., Voss H. U., Schulze-Bonhage A., Timmer J. Comparison of three nonlinear seizure prediction methods by means of the seizure prediction characteristic // Physica D, 194 (2004), - P. 357–368.