Как видно из рис. 3 эпилептические активности (показаны темными областями) возникают генерализованно, т. е. одновременно во всех областях головы в левом и правом полушарии, что соответствует генерализованной форме активности, установленной врачом. Для данных, обозначенных 2Н было проведено аналогичное исследование, в результате которого эпилептических форм активности не было выявлено.

Выводы

Рассмотрен подход на основе прогнозирующей нейронной сети для идентификации формы эпилептической активности. В качестве исходных данных используются сигналы ЭЭГ, предоставленные Брестской областной больницей. Диагностическим критерием является старший показатель Ляпунова.

Предложенная методика исследования и анализа ЭЭГ позволит выявлять области возникновения и распространения эпилептических разрядов.

Дальнейшее развитие данного исследования предполагает тестирование на данных с различными формами эпилептической активности.

Исследования проводятся в соответствии с государственной программой фундаментальных исследований «Инфотех» Республики Беларусь.

Литература

1. Карлов, В. А. Эпилепсия / В. А. Карлов. – Москва : Медицина, 1990. – 336 с.
2. Florian Mormann, Ralph G. Andrzejak, Christian E. Elger and Klaus Lehnertz. Seizure prediction: the long and winding road // Brain, 130, 2007. P. 314–333.
3. Hyvaerinen A., Oja E. Independent component analysis: algorithms and applications // Neural Networks, № 13, 2000. – P. 411–430.
4. Головко, В. А. Нейросетевой подход к детектированию эпилепсии / В. А. Головко, С. В. Безобразова // Вестн. Брест. гос. техн. ун-та. Физика, математика, информатика. – 2005. – № 5(35). – С. 58–61.
5. Головко, В. А. Нейросетевые методы обработки хаотических процессов / В. А. Головко // Лекции по Нейроинформатике. – Москва : МИФИ, 2005. – С. 43–88.

ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ В ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМАХ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

С. В. Безобразов

Брестский государственный технический университет, Беларусь

Научный руководитель В. А. Головко

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. Вирусописатели постоянно придумывают и реализовывают новые пути и методы заражения компьютеров, разрабатывают хитроумные алгоритмы и внедряют свои вредоносные программы. Вирусописатели постоянно идут на шаг впереди разработчиков антивирусного ПО. 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 за-

щиты информации направлены на создание таких методов и алгоритмов защиты, которые были бы способны обнаружить и нейтрализовать неизвестные вирусы.

Позаимствованная у природы и построенная по основным принципам биологической иммунной системы, искусственная иммунная система (ИИС) для защиты информации позволяет обнаруживать не только известные ей вирусы, но и неизвестные, как это делает иммунная система человека, ежедневно сталкиваясь с большим количеством чужеродных бактерий и вирусов в организме [1]. Основными элементами ИИС, которые выполняют функцию обнаружения вирусов, являются детекторы. На стадиях генерации и отбора детекторы приобретают способность различать неинфицированные файлы системы от компьютерных вирусов [2].

Система безопасности на основе ИИС, разработанная нами, состоит из нескольких модулей: генерация детекторов, обучение и отбор нежелательных детекторов, циркуляция детекторов в системе, обнаружение аномалий. В данной статье рассмотрен метод формирования детекторов на основе векторного квантователя (LVQ нейронная сеть). Приведены результаты экспериментов обнаружения компьютерных вирусов.

Метод формирование детекторов на основе LVQ

Нейронная сеть для векторного квантования была предложена в 1982 г. Кохоненом и называется обучающим векторным квантователем (learning vector quantization – LVQ) [3]. LVQ представляет собой двухслойную нейронную сеть (конкурирующий и линейный слои) с прямым распространением сигналов (рис. 1). Векторный квантователь обучается в процессе поступления эталонных векторов. В процессе обучения образуются кластеры различных эталонов, каждому из которых соответствует свой нейрон. При поступлении на вход такой нейронной сети неизвестного образа он идентифицируется в соответствии с мерой близости к эталонным векторам и кодируется на выходе сети номером нейрона. Совокупность кодовых векторов называется кодовой книгой. При поступлении входного вектора на сеть происходит его сравнение с вектором из кодовой книги. В процессе этого выбирается такой кодовый вектор, который наилучшим образом аппроксимирует входной вектор и его номер используется в качестве кода. В качестве меры близости может использоваться евклидово расстояние.

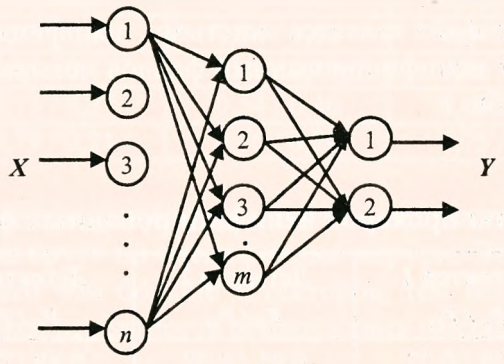

Рис. 1. Нейронная сеть для векторного квантования

Совокупность детекторов, построенных на основе LVQ, образуют популяцию детекторов, которые выполняют функцию по обнаружению компьютерных вирусов.

Результаты экспериментов

В наших экспериментах использовались детекторы, построенные на основе LVQ со следующей архитектурой: 128 нейронов входного слоя, 10 нейронов скрытого слоя и 2 нейрона выходного слоя (такой детектор изображен на рис. 1, $m = 128$, $n = 10$). Обучающая выборка для каждого детектора формировалась следующим образом:

– выбирались случайным образом четыре неинфицированных файлов и один вирус;

– из каждого выбранного файла случайным образом выбиралось по пять фрагментов длиной 128 бит, после чего последовательно подавались на вход LVQ.

Для обучения нейронной сети использовалось правило обучения с учителем. В результате обучения мы получали 10 кодовых векторов в скрытом слое, которые относились к двум выходным классам. Первый класс (неинфицированные файлы) содержал 8 кодовых векторов. Второй класс (вирусы) состоял из двух кодовых векторов. Так как мы разбили входное пространство образов в пропорциях 8 к 2, то необученный детектор соотносил любой входной образ (независимо от того, вирус ли это или неинфицированный файл) с первым классом с вероятностью 80 % и со вторым классом с вероятностью 20 %. Зрелый детектор соотносил чистый файл к первому классу с вероятностью больше 80 % и компьютерный вирус ко второму классу с вероятностью больше чем 20 %. Во время проверки детектор разбивал файл на фрагменты по 128 байт каждый, последовательно проверял их и вычислял суммарную вероятность попадания в тот или иной класс:

$$P = X/N \cdot 100\ \%, \qquad (1)$$

где X – количество фрагментов одного из классов; N – общее количество фрагментов. На примере файла *diskcopy.exe* это выглядит следующим образом: размер файла 7168 байт – 56 фрагментов по 128 байт. Во время проверки детектор соотнес 49 фрагментов к первому классу (неинфицированные), что составило $P_S = 49/56 \cdot 100\ \% = 87{,}5\ \%$. Соответственно, ко второму классу (вирусы) детектором было соотнесено 7 фрагментов, что составило $P_M = 7/56 \cdot 100\ \% = 12{,}5\ \%$. Детектор принял решение о том, что файл является «чистым», неинфицированным.

Результаты проверок неинфицированных файлов четырьмя различными детекторами представлены в табл. 1:

Таблица 1

Результаты проверок неинфицированных файлов

Имя файла	Детектор 1 P_S / P_M	Детектор 2 P_S / P_M	Детектор 3 P_S / P_M	Детектор 4 P_S / P_M
cacls.exe	0,78 / 0,22	0,93 / 0,07	0,89 / 0,11	0,82 / 0,18
ctfmon.exe	0,81 / 0,19	0,86 / 0,14	0,87 / 0,13	0,89 / 0,11
dbexplor.exe	0,90 / 0,10	0,93 / 0,07	0,94 / 0,06	0,90 / 0,10
dcomcnfg.exe	0,91 / 0,09	0,96 / 0,04	0,96 / 0,04	0,96 / 0,04
diskcopy.com	0,83 / 0,17	0,93 / 0,07	0,92 / 0,08	0,83 / 0,17

Окончание табл. 1

Имя файла	Детектор 1 P_S / P_M	Детектор 2 P_S / P_M	Детектор 3 P_S / P_M	Детектор 4 P_S / P_M
dllhost.exe	0,89 / 0,11	0,96 / 0,04	0,98 / 0,02	0,85 / 0,15
etm70.exe	0,91 / 0,09	0,94 / 0,06	0,95 / 0,05	0,87 / 0,13
notepad.exe	0,84 / 0,16	0,91 / 0,09	0,92 / 0,08	0,83 / 0,17
soundman.exe	0,87 / 0,13	0,93 / 0,07	0,94 / 0,06	0,93 / 0,07
taskman.exe	0,88 / 0,12	0,92 / 0,08	0,95 / 0,05	0,92 / 0,08
uninlib.exe	0,58 / 0,43	0,81 / 0,19	0,83 / 0,17	0,82 / 0,18

Как видно из таблицы детектор под номером 1 детектирует файлы *cacls.exe* и *uninlib.exe* как вирусы. Такой детектор считается негативным детектором и должен уничтожаться на стадии отбора [2].

Результаты обнаружения компьютерных вирусов отображены в табл. 2.

Таблица 2

Результаты обнаружения компьютерных вирусов

Имя файла	Детектор 1 P_S / P_M	Детектор 2 P_S / P_M	Детектор3 P_S / P_M	Детектор 4 P_S / P_M
Backdoor.Agent	0,98 / 0,02	0,98 / 0,02	0,98 / 0,02	0,96 / 0,04
Backdoor.Agobot	0,91 / 0,09	0,58 / 0,42	0,68 / 0,32	0,83 / 0,17
E-Worm.Bozori	0,64 / 0,36	0,73 / 0,27	0,55 / 0,45	0,85 / 0,15
E-Worm.Zafi	0,70 / 0,30	0,58 / 0,42	0,68 / 0,32	0,87 / 0,13
E-Worm.Mydoom	0,67 / 0,13	0,65 / 0,35	0,65 / 0,35	0,79 / 0,21
E-Worm.NetSky	0,61 / 0,39	0,68 / 0,32	0,57 / 0,43	0,80 / 0,20
Exploit.DebPloit	0,85 / 0,15	0,92 / 0,08	0,92 / 0,08	0,92 / 0,08
Net-Worm.Lovesan	0,83 / 0,17	0,81 / 0,19	0,77 / 0,23	0,71 / 0,29
Net-Worm.Mytob	0,84 / 0,16	0,55 / 0,45	0,63 / 0,37	0,74 / 0,26
Trojan.Bagle	0,81 / 0,19	0,85 / 0,15	0,78 / 0,22	0,68 / 0,32
Trojan.Daemonize	0,93 / 0,07	0,84 / 0,16	0,84 / 0,16	0,84 / 0,16
Trojan.LdPinch	0,89 / 0,11	0,60 / 0,40	0,76 / 0,24	0,81 / 0,19
Virus.Gpcode	0,73 / 0,27	0,54 / 0,46	0,64 / 0,36	0,58 / 0,42
Virus.Hidrag	0,79 / 0,21	0,76 / 0,24	0,75 / 0,25	0,77 / 0,23

Как видно из полученных результатов, один вирус не способен обнаружить все вирусы, напротив, он реагирует на специфичные вирусы. Это обуславливается обучающей выборкой. Однако чем больше детекторов, тем большее пространство мы перекрываем и увеличиваем вероятность обнаружения неизвестного вируса.

Выводы

Разработан метод формирования детекторов искусственной иммунной системы для защиты информации на основе LVQ-сети. Данный метод позволяет значительно уменьшить затраты на вычислительные ресурсы компьютерной системы, следовательно, сокращается время проверки файлов на наличие вирусов. Разработанный метод позволяет одному детектору обнаруживать несколько компьютерных вирусов.

Литература

1. Иммунитет. Энциклопедия «Кругосвет». – 2004. – Режим доступа: http://krugosvet.ru.
2. Безобразов, С. В. Искусственные иммунные системы: принципы построения / С. В. Безобразов // Труды IV республиканской научной конференции молодых ученых и студентов «Современные проблемы математики и вычислительной техники», Брест, ноябрь, 2005 г. – Брест : БГТУ, 2005. – С. 3–5.
3. Kohonen, T. Sell-organised formation of topologically correct feature maps / T. Kohonen // Biological Cybernetics. – 1982. – № 43. – P. 59–69.

РЕЦИРКУЛЯЦИОННЫЕ НЕЙРОННЫЕ СЕТИ В ЗАДАЧАХ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

П. А. Кочурко

Брестский государственный технический университет, Беларусь

Научный руководитель В. А. Головко

Решения различных прикладных задач с помощью аппарата искусственных нейронных сетей (ИНС) широко известны и активно применяются на практике. В сфере обнаружения сетевых атак ИНС имеют потенциал для решения большого количества проблем, охватываемых другими современными подходами. Изначально ИНС были заявлены в качестве альтернативы компонентам статистического анализа систем выявления аномалий, в дальнейшем предлагались подходы и для обнаружения злоупотреблений и распознавания сетевых атак. В данной работе рассматриваются нейросетевые подходы, реализующие как технологию обнаружения аномалий, так и обнаружения злоупотреблений на основе нелинейных рециркуляционных нейронных сетей (РНС).

Рециркуляционные нейронные сети, называемые также иногда автоассоциативными, в общем случае представляют собой многослойный персептрон, производящий отображение входного образа в идентичный ему выходной. При этом, в зависимости от архитектуры сети, может производиться сжатие и восстановление информации или вычисляться главные компоненты – такие сети называют также PCA-сетями [1].

В процессе обнаружения аномалии система обнаружения атак (СОА) производит анализ входного образа, которым может являться информация о TCP-соединении или строка журнала регистрации сетевых событий, на предмет принадлежности его к одному единственному классу, который известен системе – классу нормальных образов. В случае, если делается вывод о его непринадлежности к данному классу, то данный образ считается атакой, т. е. относится ко второму классу. В процессе определения злоупотреблений СОА наоборот реализует поиск того класса атак из известных классов, к которому данный входной образ может относиться. Если такой класс не найден, то данный образ объявляется нормальным.

Нелинейные РНС способны выступить в качестве детекторов СОА, реализующей обе технологии. Опыт показывает [2], [3], что именно объединение обеих технологий в рамках одной системы может позволить повысить качество обнаружения и снизить уровень ложных срабатываний. При этом одинаковая природа детекторов позволяет избежать нежелательных издержек на реализацию и функционирование детекторов другой природы. Рассмотрим варианты применения РНС в качестве: а) детектора аномалий; б) комбинированного детектора; в) частного классификатора; г) основы для совокупного классификатора.