2. *Баушев С. В., Передрий А. В.* Разработка перспективных систем связи вооруженных сил США и объединенных вооруженных сил НАТО // Зарубежная электроника. – 2002. – №4.

3. *Антонов В.М., Пермяков О.Ю.* Комп'ютерні мережі військового призначення. – К.: МК-ПРЕС, 2005. – 320 с.

4. *Паневин О.М., Цопа А.И.* Аппаратура высокоскоростного доступа в Интернет "Антарес-115" с одновременным использованием каналов передачи данных и голоса // Сборник научных трудов II Международной конференции "Информационные технологии и безопасность-2002". – Киев-Партенит: ИПРИ НАН Украины. –2002. – С.103-106.

5. *Цопа А.И., Овчаренко Ю.Б., Власенко В.А.* Использование новой технологии G.SHDSL в системе передачи данных "Вега 2000" // Сборник тезисов докладов 9-й Международной конференции "Теория и техника передачи, приема и обработки информации". – Харьков-Туапсе: ХНУРЭ. – 2003. – С. 44-45.

6. *Цопа А.И., Тихонов В.А., Савченко И.В.* Анализ предельных длин кабельных линий системы SDSL// Научно-технический журнал "Прикладная радиоэлектроника". –2005. – № 2. – С. 400-404.

7. *Шокало В.М., Лихограй В.Г., Стрельницкий А.Е.* Вероятность битовой ошибки при воздействии помех на системы абонентского доступа с учетом характеристик направленности антенн// Радиотехника. Всеукраинский межведомственный научно-технический сборник. – 2005. – Выпуск №140. – С.28-31.

8. *Литвинов В.В.* Радиолокаторы систем контроля воздушного пространства: ретроспектива и современные проблемы интеграции и унификации // Научно-технический журнал "Прикладная радиоэлектроника". –2004. – № 4. – С. 61-74.

9. *Управление* радиочастотным спектром и электромагнитная совместимость радиосистем. Учебное пособие / Под ред. д.т.н., проф. М.А. Быковского. – М.: Эко-Трендз, 2006. – 376 с.

10. *Шокало В.М., Цопа А.И., Овчаренко Ю.Б.* Модульный компьютер для телекоммуникаций на базе процессора микроархитектуры Intel XScale // Сборник тезисов докладов 10-й Юбилейной международной конференции "Теория и техника передачи, приема и обработки информации". –Харьков-Туапсе: ХНУРЭ. – 2004, г. Харьков. – С. 69-70.

Поступила 10.04.2006

УДК 681.3.06

Хорошко В.А., Терейковский И.А.

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ В ЗАДАЧАХ РАСПОЗНАВАНИЯ АТАК НА КОМПЬЮТЕРНЫЕ СИСТЕМЫ

Введение

В последнее время в самых разных отраслях науки и техники отмечается возросший интерес к применению искусственных нейронных сетей. Во многом популярность нейронных сетей объясняется возможностью их эффективного использования в задачах, плохо решаемых «аналитическими» методами. В теоретических работах [1-4], посвященных нейронным сетям, отмечается, что их использование целесообразно в задачах:

– классификации образцов. Задача состоит в указании принадлежности входного образца, представленного вектором признаков, одному или нескольким предварительно определенным классам;

– кластеризации/категоризации. Задача отличается от классификации образцов только тем, что классы заранее не определены, хотя во многих случаях количество классов все-таки предварительно указывается;

– аппроксимации функций. Задача состоит в нахождении оценки функции по известной выборке ее параметров и значений. Нейронные сети рекомендуется использовать в случаях, когда выборка искажена шумом и найти аналитическое решение затруднительно. При этом попутно решается задача фильтрации, т.е. выделения полезного сигнала из фонового шума;

– предсказания/прогноза. Необходимо на основании множества дискретных отсчетов $\{f(t_1), f(t_2),\ldots, f(t_j)\}$ в последовательные моменты времени предсказать значение $f(t_{j+1})$ в момент времени t_{j+1};

– оптимизации, т.е. нахождения решений, которые удовлетворяют системе ограничений и максимизируют или минимизируют целевую функцию. Для решения этой задачи нейронные сети рекомендуется использовать при невозможности составить явные функциональные зависимости для ограничений и/или целевой функции;

– управления с эталонной моделью. В этих задачах целью управления является расчет такого входного управляющего воздействия на управляемую систему, при котором она следует по желаемой траектории, диктуемой эталонной моделью;

– создания информационно-вычислительных систем, обладающих памятью, адресуемой по содержанию, т.е. ассоциативной памятью. В этом случае содержание памяти может быть вызвано по частичному или искаженному содержанию, что кроме прочего положительно сказывается и на живучести таких систем. При этом ассоциативная память позволяет решать задачи сжатия информации и восстановления данных.

Отметим, что частично или в комплексе решать перечисленные задачи приходится при разработке методов и средств защиты информации. В [5] указано на применение нейронных сетей в компонентах систем оповещения об атаках (СОА), а также в системах обнаружения уязвимостей (СОУ). Однако подробного описания механизма такого применения в доступной литературе нами не найдено. Скорее всего, речь идет об использовании в указанных средствах защиты управляющего элемента на базе относительно давней разновидности нейронной сети – многослойного перспетрона. С его помощью решается задача распознавания реализации атаки на компьютерную систему, т.е. задача распознавания образов. СОА на основании нейронных сетей получили определенное распространение. Однако все они обладают рядом существенных недостатков, которые ограничивают их практическую ценность [5]. К указанным недостаткам относятся: высокий уровень ложных тревог, сложность подбора оптимальных граничных параметров, сложность ввода в систему нового субъекта/объекта наблюдений, недостаточная адаптация ко многим особенностям современного состояния отрасли информационных технологий. Это свидетельствует о необходимости дальнейшего усовершенствования таких систем. При этом следует учитывать определенный прогресс в развитии теории искусственных нейронных сетей, что в свою очередь должно отражаться и на методике их использования в задачах защиты информации. Так, кроме перспетрона уже достаточно хорошо изучены еще несколько разновидностей нейронных сетей, каждая из которых обладает своими специфическими возможностями. Этим объясняется актуальность исследования применимости различного рода нейронных сетей в задачах защиты информации.

Постановка задачи

Оценка возможностей применения управляющих элементов на базе нейронных сетей при разработке методов и средств защиты информации.

Общий принцип работы нейронных сетей

Нейроны представляют собой простые процессоры, вычислительные возможности которых ограничиваются некоторым правилом комбинирования входных сигналов и правилом активации, позволяющим вычислить выходной сигнал по совокупности входных сигналов. Выходной сигнал нейрона может посылаться другим нейронам сети по взвешенным связям, с каждой из которых связан весовой коэффициент, называемый также весом связи. Правило комбинирования входящих сигналов нейрона заключается в

суммировании их взвешенных значений. Общий входной сигнал нейрона (net) рассчитывается так:

$$\text{net} = w_0 + \sum_{i=1}^{n} x_i w_i, \quad (1)$$

где w_0 – сдвиг, n – число входящих связей, x_i – величина i-й связи, w_i – вес i-й связи.

Правило (функция) активации представляет собой правило вычисления выходного значения нейрона, которое предполагается передать другим нейронам или во внешнюю среду. В качестве функции активации чаще всего используют линейную (2), линейную с погашением отрицательных импульсов (3), пороговую (4) и сигмоидальную функции (5):

$$f(\text{net}) = \text{net}, \quad (2)$$

$$f(\text{net}) = \begin{cases} \text{net}, \exists \text{net} > z \\ 0, \exists \text{net} \le z \end{cases}, \quad (3)$$

$$f(\text{net}) = \begin{cases} 1, \exists \text{net} \ge z \\ 0, \exists \text{net} < z \end{cases}, \quad (4)$$

$$f(\text{net}) = \frac{1}{1 + e^{-a \times \text{net}}}, \quad (5)$$

где z – некоторое пороговое значение; a – некоторый коэффициент.

Линейная и линейная с погашением отрицательных импульсов функции активации используются в основном для нейронов, которые принимают сигналы от внешней среды. Такие нейроны называются входными. Выходной сигнал нейрона в соответствии с функцией активации может иметь как положительное, так и отрицательное значение. При этом связи, по которым к нейрону поступают положительные сигналы, называются возбуждающими. Связи, по которым поступают отрицательные сигналы, называются тормозящими.

В общем случае нейронная сеть является совокупностью произвольным образом соединенных между собой нейронов. Нейроны, которые непосредственно не принимают сигналы от внешней среды и не посылают данные во внешнюю среду, называются скрытыми. Обучение сети начинается с инициализации весов связей (весовых коэффициентов) случайными величинами. Сети предъявляются различные данные, а весовые коэффициенты подстраиваются согласно выбранной математической схеме. После обучения сеть может распознавать входные данные либо нести какую-либо иную смысловую нагрузку. Информация о полученном во время обучения опыте хранится в виде весовых коэффициентов связей.

Основными характеристиками нейронной сети являются:

– количество входных, скрытых и выходных нейронов;
– структура связей;
– правила распространения сигналов в сети;
– правила комбинирования входящих в нейрон сигналов;
– правила вычисления выходного сигнала нейрона;
– правила обучения, корректирующие связи в сети.

Анализ [1, 4] позволяет сформулировать вывод о том, что развитие современных нейронных сетей заключается в формировании оптимальной, с точки зрения прикладной задачи, структуры связей сети, правил распространения сигналов и правил ее обучения. В настоящее время в различных сферах деятельности используется довольно много нейросетевых структур: многослойный перспетрон, сеть с радиальными базисными функциями, модель Липпмана-Хемминга, самоорганизующаяся карта признаков, сеть Хопфилда, сеть BAM, автоассоциативные сети, рекуррентные сети, машина Больцмана, сеть PNN, модульные нейронные сети, сети адаптивной резонансной теории, когнитроны, неокогнитроны, нечеткие нейронные сети. При этом для каждого класса прикладных задач применяются свои типы нейронных сетей. Проведем исследование наиболее известных и апробированных базовых нейросетевых структур с точки зрения их адаптации к решению задач защиты информации. Отметим, что этим мы несколько сужаем круг исследований.

Остаются без рассмотрения некоторые возможно и перспективные, но недостаточно апробированные виды нейронных сетей. Например, мы не будем рассматривать когнитрон или нейронные сети, базирующиеся на нечеткой логике.

Многослойный перспетрон и сеть с радиальными базисными функциями

В общем случае многослойный перспетрон представляет собой сеть, состоящую из нескольких последовательно соединенных слоев формальных нейронов. Обычно информация сначала поступает во входной слой, состоящий только из сенсорных элементов (входных нейронов). Задачей входного слоя является только прием и распространение по сети входной информации. Далее имеется один или реже несколько скрытых слоев. Выходная информация отображается в выходном слое. Чаще всего каждый нейрон скрытого слоя принимает все выходные сигналы нейронов предыдущего слоя, а его выходной сигнал рассылается всем нейронам следующего слоя. Особенностью многослойного перспетрона является наличие только прямых тормозящих и/или возбуждающих связей между соседними слоями. При этом каждый нейрон в скрытом слое характеризуется уникальным вектором весовых коэффициентов, настраиваемых в процессе обучения. Обучение перспетрона производится методом "обучение с учителем" с использованием алгоритма обратного распространения ошибок. Алгоритм базируется на минимизации функции ошибки перспетрона на всем множестве обучающей выборки. Поиск минимума ошибки осуществляется методом градиентного спуска. Указанный алгоритм обучения обладает достаточной эффективностью, но накладывает ограничение на использование только гладких функций активации нейронов в скрытых слоях.

В общем случае с помощью перспетрона возможно решить задачу аппроксимации многомерных функций, т.е. построения многомерного отображения F: x⇒y, обобщающего заданный набор примеров $\{x_n,y_n\}$. Теоретически доказано [1, 4], что одного скрытого слоя нейронов с сигмоидной функцией активации достаточно для аппроксимации любой функции со сколь угодно высокой точностью. Более того, многослойный перспетрон может одновременно аппроксимировать и саму функцию, и ее производные. Отметим, что многие практические задачи распознавания образов, фильтрации шумов, предсказания временных рядов сводятся к аппроксимации многомерных функций.

Максимальное количество запоминаемых образцов (p) в двухслойном перспетроне с пороговой активационной функцией вида (4) можно оценить следующим образом:

$$\frac{L_w}{m} < p < \frac{L_w}{m}\log\left(\frac{L_w}{m}\right), \qquad (6)$$

где L_w– число подстраиваемых весов, m – количество нейронов в выходном слое.

Емкость двухслойного перспетрона с гладкими активационными функциями вида (5) обычно несколько выше. При этом емкость перспетрона с количеством слоев больше двух теоретически не определена.

Проведенный анализ позволяет сделать вывод о том, что многослойный перспетрон целесообразно использовать в тех средствах защиты информации, которые базируются на анализе множества взаимокоррелируемых дискретных параметров. К таким средствам защиты относятся системы распознавания атак, системы распознавания уязвимостей, антивирусы, антикейллогеры. Возможные входные параметры многослойного перспетрона для этих средств защиты показаны в таблице.

Аналогичные перспетрону задачи позволяет решать сеть с радиальными базисными функциями. В наиболее простой форме сеть содержит три слоя: входной, скрытый и выходной. Отображение от входного слоя к скрытому является нелинейным, а отображение скрытого в выходной – линейным. Обычно в таких сетях число скрытых нейронов больше числа входных нейронов. Построение сети базируется на предпосылке о том, что для повышения вероятности линейной разделимости необходимо разместить классифицируемые образцы в пространстве высокой размерности некоторым нелинейным образом [2,3]. Для

обучения первого слоя сети с радиальными базисными функциями используется обучение без управления, а второй слой обучается "с учителем". Сравнивая радиальную базисную сеть с многослойным перспетроном, источники [1-3] указывают на более высокую мощность последнего. При этом в качестве преимущества радиальной базисной сети указывается простота ее модельной и программной реализации.

Входные параметры многослойного перспетрона в некоторых средствах защиты

Название средств защиты	Входные параметры
Система распознавания атак	Параметры сетевых запросов и событий в компьютерной системе: вход/выход пользователей, количество процессов, доступ к файлам, временные интервалы запросов к объектам компьютерной системы
Система распознавания уязвимостей	Параметры настроек компьютерной системы: количество пользователей, привилегии пользователей, параметры доступа к объектам компьютерной системы, количество и номенклатура открытых портов, запущенные сетевые службы, параметры административных настроек служб DCOM/COM+
Антивирусы, антикейллогеры	Параметры событий в компьютерной системе: количество и номенклатура запущенных программ и процессов, доступ процессов к файлам, попытки доступа к сетевым службам, попытки изменения исполняемых файлов, доступ к API операционной системы

На наш взгляд, основными ограничениями использования многослойного перспетрона и сети с радиальными базисными функциями являются:

– недостаточно изученные возможности в области обобщения и вывода новых знаний;

– невозможность самостоятельного дообучения в процессе практической эксплуатации.

На практике эти ограничения могут негативно отразиться на возможности диагностирования новых видов атак или неизвестных уязвимостей. Для решения этой проблемы необходимо разработать методику формирования качественной первоначальной обучающей выборки и провести исследование в направлении развития такой характеристики перспетрона и сети радиального базиса, как обобщение подобной входной информации. Кроме этого необходимо провести исследование в направлении комбинированного применения перспетрона с другими видами нейронных сетей.

Самоорганизующаяся карта признаков (сеть Кохонена)

Назначением сети является кластеризация образцов. Такая сеть имеет набор входных элементов, число которых соответствует размерности учебных векторов, и набор выходных элементов, которые служат в качестве прототипов. Входные нейроны предназначены только для того, чтобы распределять данные входного вектора признаков между выходными элементами сети. Выходные нейроны называются кластерными элементами. Обычно число кластерных элементов меньше числа учебных образцов. Вектор входных значений $X=(x_1,x_2,\ldots,x_m)$ передается кластерным элементам A, B, …, N. Вначале вектор весовых коэффициентов W проинициализирован случайными числами w_{1A}, w_{1b}… Сеть обучается по алгоритму «победитель забирает все», в соответствии с которым при предъявлении сети входного вектора возбуждается единственный нейрон-победитель, наиболее точно

соответствующий образцу. Вектор весовых коэффициентов нейрона-победителя модифицируется

$$W = W + cX, \quad (7)$$

где c – некоторый положительный параметр обучения.

Иногда в алгоритм добавляют параметр "совести", который обновляется на каждой итерации и препятствует слишком частым "победам" одних и тех же нейронов. В некоторых случаях определяется не один нейрон-победитель, а множество ближайших нейронов. Отметим, что в любом случае указанный алгоритм реализует принцип обучения "без учителя". Хотя это и расширяет адаптивные возможности сети, но не позволяет использовать накопленные знания об изучаемом процессе. Поэтому в современных нейросетевых системах сеть Кохонена самостоятельно не используется [2, 3].

Сети встречного распространения

Они являются в некотором смысле модификацией сети Кохонена и используются для решения задач кластеризации образцов [1, 4]. Модификация заключается в добавлении в состав сети слоя Гроссберга (звезды Гроссберга). В режиме распознавания нейроны слоя Кохонена определяют кластер, к которому принадлежит входной образ. Затем выходная звезда слоя Гроссберга, обучаясь "с учителем", по сигналу нейрона-победителя в слое Кохонена воспроизводит на выходах сети соответствующий образ.

Обучение весов слоя Кохонена выполняется "без учителя" на основе самоорганизации. Входной вектор вначале нормируется, сохраняя направление. После выполнения одной итерации обучения определяется нейрон-победитель, состояние его возбуждения устанавливается равным единице, и теперь могут быть модифицированы веса соответствующей ему звезды Гроссберга. Темпы обучения нейронов Кохонена и Гроссберга должны быть согласованы. В слое Кохонена обучаются веса всех нейронов в окрестности победителя, которая постепенно сужается до одного нейрона.

Рекомендуется использование этой архитектуры для быстрого моделирования систем на начальных этапах исследований с дальнейшим переходом, если это потребуется, на значительно более ресурсоемкий, но более точный метод обучения с обратным распространением ошибок [2]. По этой причине использовать сеть встречного распространения в действующих системах защиты нецелесообразно.

Линейный ассоциатор

Реализует одну из форм интерполятивной памяти. Интерполятивная память – это такое отображение $X \rightarrow Y(X)$, при котором отличному от эталона вектору $X=X_i+\Delta_i$ ставится в соответствие выходной вектор $Y(X)=Y(X_i+\Delta_i)=Y_i+Y(\Delta_i)$. Таким образом, каждый эталонный образец связывается с соответствующим образом в памяти. Если же входной образец отличается от эталонного на вектор Δi, то выходной вектор тоже отличается от эталонного на величину $Y(\Delta_i)$. Кроме этого ожидаемые свойства сети базируются на предположении, что эталонные образцы составляют множество ортонормальных векторов [4]. Эти обстоятельства затрудняют практическое применение линейного ассоциатора для решения задач защиты информации.

Сети ассоциативной памяти

К известным сетям такого типа относятся сети Хопфилда, Хемминга, BAM (Bidirectional Associative Memory), а также машина Больцмана.

Сеть Хопфилда является автоассоциативной сетью, которая может классифицировать сохраненный образец даже по подсказке, представляющей собой искаженную помехами версию нужного образца. Если не учитывать входные нейроны, то сеть Хопфилда является однослойной. Все нейроны связываются друг с другом, но не сами с собой. Обучение сети заключается в применении процедуры обновления веса случайного нейрона до тех пор, пока не будет получено устойчивое состояние, соответствующее локальному минимуму энергии

сети. Таким образом, весовые значения нейронов определяются непосредственно из учебных данных перед началом функционирования сети. Доказано, что для сетей Хопфилда всегда существует функция энергии сети, обеспечивающая ее сходимость к устойчивому состоянию. Кроме использования в задачах автоассоциативной памяти сеть Хопфилда предлагается применять для решения задач оптимизации.

Сеть Хемминга, являясь модификацией сети Хопфилда, применяется в тех случаях, когда допускается определить только номер исходного образца по зашумленному входному сигналу. Преимуществом этой сети перед сетью Хопфилда являются меньшие затраты на вычислительные ресурсы.

Установлено [2], что максимальное количество образцов (p), которые можно сохранить в сетях Хопфилда и Хемминга, если требовать правильного распознавания большинства образцов, должно быть:

$$p < \frac{N}{2 \ln N}, \tag{8}$$

где N – количество нейронов в сети.

При этом для безошибочной работы сети максимальное количество образцов должно быть:

$$p < 0{,}15N. \tag{9}$$

Известной модификацией сети Хопфилда является машина Больцмана [2]. Ее отличительная черта – это обучение методом модельной "закалки". Данный метод частично позволяет обойти локальные минимумы функции энергии сети и установить равновесное состояние, соответствующее глобальному минимуму.

Еще одним видом сетей ассоциативной памяти является сеть BAM [2,4]. В общем случае сеть BAM представляет собой гертероассоциативную рекуррентную сеть, состоящую из двух слоев. Связи между слоями устроены таким образом, что каждый нейрон одного слоя связан с каждым нейроном другого слоя. Внутри слоев связи между нейронами отсутствуют, число нейронов на каждом слое может быть различным. Обучение задается правилом Хебба. Поскольку связи между нейронами разных слоев являются двунаправленными, то веса связей необходимо определить для обоих направлений. Если рассматривать набор ассоциаций вида $<X_1,X_1>$, $<X_2,X_2>$, то сеть BAM можно классифицировать как двунаправленную ассоциативную память. В этом случае второй слой нейронов можно исключить, при этом необходимо установить двунаправленные связи между всеми нейронами оставшегося слоя.

Распространенность сетей Хопфилда, Хемминга и BAM объясняется простотой построения программных и аппаратных моделей. Так как весовые коэффициенты в этих сетей могут быть найдены с помощью простых матричных вычислений, такие сети не требуют длительного обучения.

К основным недостаткам данных сетей относится:

– равновесное состояние сети, которое по критерию минимума энергии не обязательно соответствует глобальному минимуму для моделируемой системы. Общего метода решения этой проблемы не существует. Таким образом, сети Хопфилда и Хемминга не обязательно правильно воспроизводят исходный образец по зашумленным данным. При этом нельзя точно определить уровень шума, выше которого сеть становится неработоспособной;

– при использовании сетей в задачах оптимизации не существует общего метода отображения ограничений оптимизации в функцию энергии сети;

– относительно невысокая емкость сетей.

Несмотря на указанные недостатки, существует достаточно много примеров использования сетей Хопфилда и Хемминга, а также сети BAM. Например, в [2, 3] показано удачное применение таких сетей в системах распознавания текста. Отметим, что количество параметров, учитываемых в системах распознавания текста, соизмеримо с количеством параметров, анализируемых в СОА и СОУ. При этом в СОА и СОУ количество эталонных

образцов должно быть намного больше. Кроме этого некоторым ограничением применения указанных сетей являются проблемы ложной памяти [1, 4].

Сети PNN (вероятностные нейронные сети)

Предназначены для классификации образцов на основе статистических оценок их близости соседним образцам [3]. Формальным правилом соответствия неизвестного образца x k-му классу является выражение:

$$h_k c_k f_k(x) > h_i c_i f_i(x), \exists i \in \{N\} \ , \qquad (10)$$

где {N}–множество всех классов; i–произвольный класс; h_k (h_i) – априорная вероятность классификации образца как класса k (i); c_k (c_i) – цена ошибки классификации образца как класса k (i); $f_k(x)$ и $f_i(x)$ – функции плотности вероятности классов k и i.

На практике расчет априорных вероятностей и ошибок классификации во многих случаях затруднителен. Поэтому часто эти величины выбираются одинаковыми для всех классов. Оценка функции плотности вероятности производится на основании учебных образцов с использованием метода Парцена. При этом используется весовая функция (ядро), имеющая центр в точке, представляющей учебный образец. Чаще всего в качестве ядра используют функцию Гаусса. Сеть состоит из трех слоев нейронов, количество которых определяется структурой учебных данных. Число входных нейронов равно числу признаков класса. Число элемента слоя образцов равно числу учебных образцов. Число элементов слоя суммирования равно числу классов. Для входящих в элемент слоя образцов связей весовые коэффициенты устанавливаются равными элементам соответствующего вектора-образца. Таким образом, все параметры сети PNN определяются непосредственно учебными данными. За счет этого обучение сети производится относительно быстро. Кроме этого достоинствами сети PNN являются возможность качественной классификации на малых наборах учебных данных, а также низкая чувствительность к наличию ошибочных данных в учебных образцах. К общим недостаткам сети относят высокую вычислительную ресурсоемкость и возможность применения только в задачах классификации. Отметим, что указанные недостатки не столь критичны в задачах защиты информации. Например, для решения проблемы ресурсоемкости можно реализовать сеть с помощью аппаратных средств. Поэтому использование сети PNN в разнообразных средствах защиты информации имеет хорошие перспективы. При этом необходимо решить следующие задачи:

– организовать эффективную систему сбора и обработки первоначальной статистической информации;

– адаптировать сеть к распознаванию как можно более широкой номенклатуры классов (опасностей);

– адаптировать сеть к дообучению в процессе эксплуатации для распознавания новых опасностей.

Рекуррентные сети

Рекуррентную сеть можно рассматривать как модификацию сети с прямыми связями. Модификация заключается в добавлении рекуррентных связей, когда нейрон посылает сигналы себе или элементам своего слоя или элементам более низких слоев. При этом алгоритм работы рекуррентных сетей представляет собой непосредственную модификацию алгоритма работы соответствующей сети с прямыми связями. Основным достоинством рекуррентных сетей является то, что при фиксированных размерах они в состоянии обрабатывать структуры переменной длины. К известным архитектурам рекуррентных сетей относятся сеть Джордана и простая рекуррентная сеть SRN (Simple Recurrent Network). Доказано, что с помощью сети SRN можно реализовать любой конечный автомат. В литературе [3] представлены примеры использования рекуррентных сетей в области распознавания смысла текстовой информации. Отметим, что к данной области относится задача распознавания смысла электронных писем, решение которой является важнейшим этапом разработки средств защиты от спама.

Выводы

Из апробированных нейронных сетей наиболее перспективными для применения в средствах защиты компьютерных систем являются многослойный перспетрон, сеть Кохонена, сеть PNN, а также рекуррентные сети.

Многослойный перспетрон, сеть Кохонена и сеть PNN целесообразно использовать в управляющих элементах СОА, СОУ, антивирусных системах и в системах защиты от кейллогеров. При этом в качестве анализируемых возможно применение параметров представленных в таблице.

Рекуррентные сети, а также сеть PNN возможно использовать в системах защиты от спама.

Вследствие того что возможности указанных нейронных сетей во многом дополняют друг друга, перспективным путем дальнейших исследований является разработка комбинированной нейронной сети. Ее основными характеристиками должны быть достаточно высокая емкость и точность, а также возможность дообучения в процессе функционирования.

Список литературы

1. *Ежов А.А., Шумский С.А.* Нейрокомпьютинг и его применение в экономике и бизнесе. – М.: МИФИ, 1998. – 224 с.

2. *Круглов В.В., Борисов В.В.* Искусственные нейронные сети. – М.: Горячая линия-Телеком, 2002. – 382 с.

3. *Каллан Р.* Основные концепции нейронных сетей: Пер. с англ. – М.: Вильямс, 2003. – 288 с.

4. *Люгер Ф.* Искусственный интеллект: стратегии и методы решения сложных проблем, 4-е издание.: Пер. с англ. – М.: Вильямс, 2003. – 864 с.

5. *Архипов А., Ишутин А.* Применение моделей обнаружения аномалий для выявления атак // Четверта науково-технічна конференція. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Тези доповідей. – 2006. – с.71-72.

Поступила 01.06.2006

УДК 681.621.396 **Павлов И.Н.**

ПРОЕКТНЫЙ АНАЛИЗ МАКСИМАЛЬНОГО КОЛИЧЕСТВА БАРЬЕРОВ В СОСТАВЕ МЕХАНИЗМА ЗАЩИТЫ ПРИ ОЦЕНКЕ ЖИВУЧЕСТИ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

1. Вступление

Специфика проектирования СЗИ на этапе оформления технического задания требует качественной оценки необходимости и достаточности количественных значений барьеров в составе механизма защиты комплексной системы защиты информации (КСЗИ). Другими словами, необходимо определить, насколько увеличение барьеров в составе механизма защиты способно качественно увеличить живучесть самих механизмов защиты, так как нельзя создать действительно живучую КСЗИ, опираясь только на увеличение барьеров в составе механизмов защиты КСЗИ.

2. Основная часть

2.1. Определение показателей живучести механизмов защиты КСЗИ

Как было показано в [1], учитывая общее количество барьеров в МЗ и изменение задач защиты, можно вывести выражение: