НЕЙРОННЫЕ ТЕХНОЛОГИИ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Южаков

Кафедра автоматики и телемеханики
Пермский государственный технический университет
ул. Профессора Поздеева, 7, Пермь, Россия, 614061

В статье представлен материал по использованию нейросетевых технологий в системах информационной безопасности. В качестве примера предложена эквистерная нейронная сеть для построения устройств обнаружения вторжений. Для данного типа сети представлен формальный нейронный элемент, который реализует функцию обнаружения вторжений/атак.

Ключевые слова: информационная безопасность, нейронные технологии, информационные технологии, экспертные системы.

Современные научные достижения в таких областях информатики, как математическое моделирование состояния внешнего мира, искусственный интеллект, теория принятия решений, обработка изображений, сигналов и сцен распознавания образов, оптимальное управление и др., позволяют говорить о реальной возможности перехода к новому поколению средств информационной защиты — интеллектуальным системам информационной безопасности [1]. Стремительно растет и перечень задач информационной безопасности, решаемых с использованием интеллектуальных методов и средств [2]. Пожалуй, первой актуальной задачей в сфере информационной безопасности, потребовавшей использования мощного арсенала методов и средств искусственного интеллекта, стала задача обнаружения вторжений и атак на автоматизированные информационные системы [1].

Современные средства обнаружения вторжений неизбежно должны включать в себя интеллектуальные подсистемы по крайней мере в качестве одной из своих составных частей. В настоящее время основу таких интеллектуальных подсистем составляют преимущественно экспертные системы и искусственные нейронные сети [2].

Предположим, что устройства обнаружения вторжений (УОВ) как устройства, реконфигурируемые в процессе рабочего функционирования, могут быть реализованы как автоматы с настраиваемой структурой (АНС) [3]. Исследованные принципы построения АНС на основе нейронных сетей, обеспечивающих параллельность, переменность и однородность структуры [5], показывают, что при этом АНС состоит из одинаковых и однотипно соединяемых друг с другом универсальных элементов с настраиваемым изменением связей между ними. Это позволяет за счет настройки (реконфигурации) связей выделять группы универсальных элементов, выполняющих упорядочение сообщений $\{X_i\}$, поступающих по определенному входному каналу $(1 \div G)$.

При этом в структуре сети организуется несколько процессов упорядочения, протекающих параллельно во времени. Разработанные логические основы реали-

зации УОВ на базе нейронных технологий позволяют утверждать, что базовым универсальным элементом структуры УОВ, выполненного на основе нейронных технологий, является формальный нейронный элемент (ФНЭ), реализующий функцию обнаружения вторжения с осуществляемой настройкой по заданной уязвимости [4].

Тогда функция преобразования ФНЭ имеет вид

$$Y_i = f_{2i}\left(\sum_{i=1}^{G}\left(X_i f_{1i}\right)\right)\left(\sum_{j=1}^{k}\left(X_{\hat{i}\tilde{n}j} f_{4j}\right)\right) f_3,$$

где X_i ($i = \overline{1, G}$) — входные сигналы ФНЭ; Y_i ($i = \overline{1, G}$) — выходные сигналы; $X_{\text{ос}j}$ — сигналы обратных связей всех ФНЭ в сети ($j = \overline{1, k}$), $k = G(G - 1)$; f_{1i}, f_{2i} — функции коммутации входных и выходных сигналов соответственно; f_3 — функция настройки ФНЭ (место нейрона, тип уязвимости/вторжения); f_{4j} — функция коммутации обратных связей, зависящая от f_3.

Разработана типовая обобщенная структура УОВ (рис. 1).

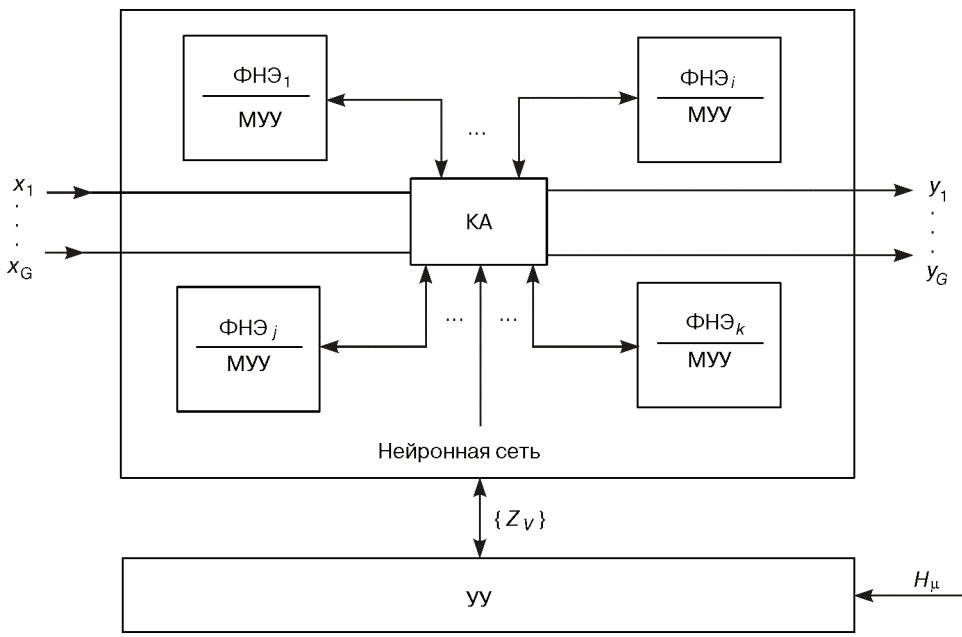

Рис. 1. Обобщенная структура УОВ:

ФНЭ$_i$ — i-нейронный элемент; МУУ — местное устройство управления; УУ — устройство управления УОВ; КА — коммутирующая аппаратура; H_μ — канал настройки УОВ; {z_v} — настроечные коды сети

Для предложенной обобщенной сетевой структуры УОВ разработана типовая структура ФНЭ (рис. 2).

В принципе мы могли бы все линейные нейроны сети слить в один нейрон и попытаться обучить его. При этом справиться с такой задачей не удастся ввиду ее декомпозиции. Данных оказывается слишком много, и они имеют низкое качество.

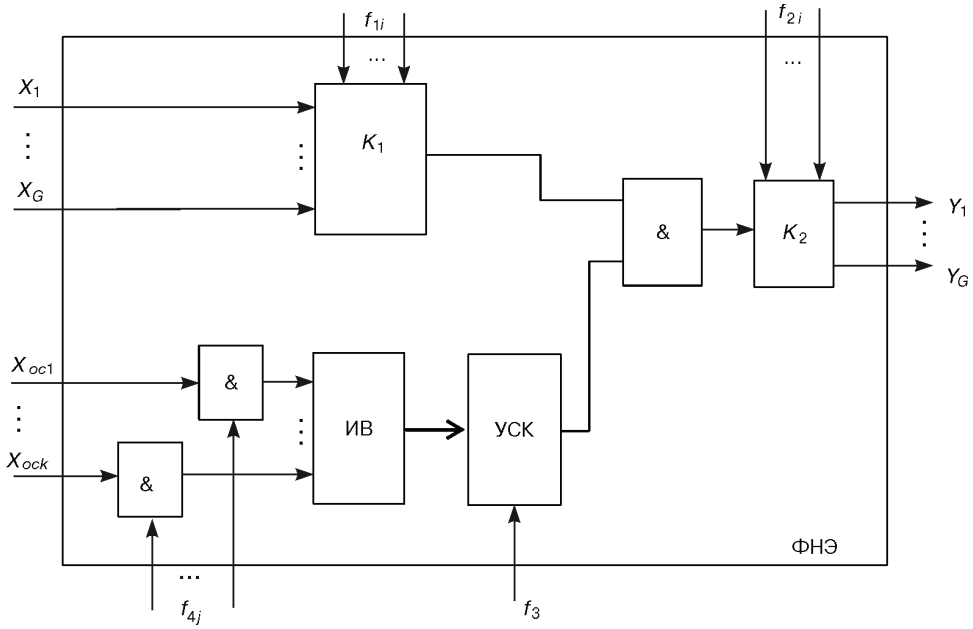

Рис. 2. Структура ФНЭ для эквисторной сети:
K_1, K_2 — коммутаторы входов/выходов соответственно; ИВ — многовходовой измеритель веса; УСК — устройство сравнения кодов; X_{ock} — сигналы обратной связи

Урегулировать задачу удастся, разбив ее на множество подзадач обучения нейронов с малым числом входов. При обучении каждого нейрона следует стремиться сжать распределения наблюдаемых классов распределений и одновременно раздвинуть их центры по отношению друг к другу.

Обучение ведется послойно [3]: сначала обучаем первый слой нейронов, затем входные данные примеров обучения транслируются через первый обученный слой, таким образом, получаются примеры для обучения второго слоя нейронов. Число слоев нейронов теоретически может быть любым. Быстрые алгоритмы послойного обучения нейронных сетей не накладывают технических ограничений на число слоев нейронной сети [3].

Автор считает, что в данной работе новыми являются следующие положения и результаты: применительно к этому случаю (нейросеть — это совокупность нескольких сотен примитивных наблюдателей нейронов), для того чтобы на фоне воспринимаемого шума увидеть и оценить вторжение, необходимо одновременно учитывать совместное влияние тысяч статистических параметров. Именно по этой причине нейросеть обучается, и потом анализируется большое число вероятностей появления вторжения в последовательности обрабатываемых и передаваемых данных.

Установлено, что для обеспечения гибкости и рационального использования общего ресурса элементов сети ФНЭ как универсальный элемент структуры сети должен обладать свойствами настраиваемости на любое место в организуемой нейронной сети, в любом из организованных в массиве ФНЭ M ($M \le G$) каналов контроля. Для этого в состав типового ФНЭ должна быть введена память, в которой располагается код признака канала ($\overline{1, G}$) поступившего сообщения.

Выполнен анализ сложности ФНЭ. Показано, что количество входов коммутаторов K_1, K_2 и ИВ ФНЭ и общий объем аппаратуры ФНЭ, линейно зависит от числа входных каналов (таблица).

Таблица 1

Аппаратурные затраты на реализацию ФНЭ

Основная аппаратура	Количество элементов	Весовой коэффициент	Эквивалентные затраты
Управляемые ключи	1	1	1
Измеритель веса	1	$G(G-1)$	$G(G-1)$
Устройство сравнения кодов	1	2^G	2^G
Логические элементы	2	1	2
Коммутационные элементы шины $Ш_1$ (K_1, K_2)	$2G$	0,5	G
Коммутационные элементы шины $Ш_2$ (K_3)	N	0,5	$0,5N$
Регистр управления ($a_1 + a_2 + 1$)	1	6	$6(\log_2(G-1) + \log_2 N + 1)$

В качестве базиса реализации принят элемент 2И—НЕ. Весовой коэффициент учитывает стоимостные и аппаратурные затраты элемента в выбранном базисе с учетом материалов, представленных в [4].

ЛИТЕРАТУРА

[1] *Барский А.Б.* Нейронные сети: распознавание, управление, принятие решений. — М.: Финансы и статистика, 2004.

[2] *Брюхомицкий Ю.А.* Нейросетевые модели для систем информационной безопасности. — Таганрог: Изд-во ТРТУ, 2005.

[3] *Волчихин В.И., Иванов А.И., Фунтиков В.А.* Быстрые алгоритмы обучения нейросетевых механизмов биометрико-криптографической защиты информации. — Пенза: Изд-во Пенз. гос. ун-та, 2005.

[4] *Южаков А.А.* Устройства динамического приоритета на основе нейронных технологий: Автореф. дисс. ... канд. техн. наук. — Пермь, 2006.

[5] *Третьяков Н.В., Южаков Ал.Ал., Южаков А.А.* Устройство динамического приоритета нейронной структуры. Информационные управляющие системы: Сб. науч. тр. — Пермь: ПГТУ, 1999. — С. 10—15.

NEURAL NETWORK TECHNOLOGIES IN THE SYSTEMS OF INFORMATION SECURITY

A.A. Yuzhakov

Automatics and telemechanics chair
The Perm state technical university
Professor Pozdeev str., 7, Perm, Russia, 614061

In the article is given the material of the use of neural network technologies in the systems of information security. As an example, neural network for the constructing of devices of finding out encroachments is offered. For this type of network presented the formal neuron element which realizes the function of detecting intrusions / attacks.

Key words: information security, neural technologies, information technology, expert systems.