гласованных действий предыдущих агентов. *При обучении необходимо научиться согласовывать движение частей робота таким образом, чтобы терминальный элемент попадал в целевую точку*.

В задаче управления пятизвенным роботом, благодаря декомпозиции, пятимерное пространство состояний действий было преобразовано в пять одномерных, обучение в которых происходит значительно быстрее. Относительное обучение позволило обучаться с учетом структуры многоагентной системы.

Моделирование многоагентной системы, построенной на вышерассмотренных принципах, показало следующие результаты. Во первых, сходимость обучения была на порядок быстрее, чем при объединенном обучении (60-100 эпизодов против 1000). Во вторых, была выявлена способность многоагентной системы к синхронизации действий. В третьих, был наглядно продемонстрирован принцип, что «обучение – это обобщение», т.к. робот легко перестраивался с цели на цель. В четвертых, стратегия поведения робота значительно изменялась в зависимости от выбранного алгоритма обучения. В пятых, моделирование показало наиболее оптимальное поведение для данного робота, которое значительно отличалось от ожидаемого.

**Литература**

1. Hose M. Vidal. *Fundamentals of Multiagent Systems with Net Logo Examples.* (www.multiagent.com)

2. Richard S. Sutton, Andrew G. Barto. *Reinforcement Learning: An Introduction* Cambridge : MIT Press., 1998

3. Tesauro, G. J. (1994). TD--gammon, a self-teaching backgammon program, achieves master-level play. *Neural Computation*, 6(2):215--219. (http://www.research.ibm.com/massive/tdl.html)

4. Dr. Florentin Woergoetter, Dr. Bernd Porr. Статья *Reinforcement Learning* на ресурсе *http://www.scholarpedia.org. (*http://www.scholarpedia.org/article/Reinforcement_learning ).

5. Кабыш, А.С. *Коллективное поведение агентов на основе подкрепляющего обучения.* Нейроинформатика / А.С. Кабыш, В.А. Головко. – 2009. – Часть 1. – С. 191-200.

6. Kabysh, A.S., Golovko V.A., *Collective Behavior in Multiagent Systems Based on Reinforcement Learning*, PRIP-2009: Proceedings of the Tenth International Conference (19-21 May, Minsk, Republic of Belarus) / Kabysh, A.S., Golovko V.A. – Minsk, 2009. – С. 260-264.

7. Kabysh, A.S. *Collective Behavior in Multi-Agent Systems,* OWD 2009 Ph.D. workshop, Eastern Europe Summer School, 12-24 October, Selesian University of Technology. – Poland. – 2009. – P. 92-97.

УДК 004.89

## ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ И НЕЙРОННЫХ СЕТЕЙ ДЛЯ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

***Комар М.П.***

*Тернопольский национальный экономический университет, г. Тернополь, Украина*

В настоящее время обеспечение безопасности информации является одной из ключевых задач. Развитие компьютерных сетей и их объединение в глобальную сеть Интернет привело к росту числа преступлений, связанных с нарушением основополагающих принципов информационной безопасности: доступности, целостности и конфиденциальности информации. Несмотря на развитие средств защиты, таких как брандмауэры, количество

вторжений в информационные системы компаний возрастает с каждым годом. Для обнаружения компьютерных атак используются различные классы инструментальных средств, такие как системы обнаружения атак, системы предотвращения атак, сканеры уязвимостей, комплексные системы управления безопасностью. Однако использование этих средств сегодня ограничено рядом факторов [1]:

- высокая стоимость;
- сложность в использовании;
- низкая эффективность функционирования при наличии неизвестных атак;
- высокая нагрузка на компоненты сети.

Традиционные методы обнаружения атак, такие как сигнатурный метод или метод обнаружения аномалий, не позволяют достичь оптимальных характеристик обнаружения атак. Сигнатурный метод анализа основан на том, что большинство атак на систему известны и развиваются по схожим сценариям. В данном подходе сигнатуры вторжений определяют характерные особенности, условия, устройства и взаимосвязь событий, которые ведут к попыткам или собственно к вторжению.

К недостаткам сигнатурного анализа можно отнести:

– зависимость масштабируемости и производительности от размера базы данных сигнатур;

– обновление базы данных сигнатур затруднительно ввиду отсутствия общепринятого языка описания, а добавление собственных сигнатур требует высокой квалификации;

– обновление базы данных сигнатур требуется при обнаружении нового типа атак, период обновления базы должен быть невелик.

В настоящее время исследования в области защиты информации ведутся в направлении разработки средств, которые позволяют решить часть этих проблем за счет использования интеллектуальных технологий. Вместе с тем, многие вопросы при построении этих систем, связанные с эффективностью применения новых методов и технологий и их реализацией в режиме реального времени, остаются открытыми и не до конца исследованными, поэтому разработка интеллектуальных систем обнаружения атак с использованием таких перспективных направлений, как искусственные иммунные системы и нейронные сети, является актуальной задачей.

Модели, основанные на принципах функционирования систем иммунитета, применяются в различных областях науки и техники. Сфера их применения включает следующие области (но не ограничивается ими): методы вычислений; когнитивные модели; искусственные иммунные системы для распознавания образов; методы обнаружения аномалий и неисправностей; мультиагентные системы; модели самоорганизации; модели коллективного интеллекта; системы поиска и оптимизации; модели автономных распределенных систем; модели искусственной жизни; системы компьютерной и интернет-безопасности; модели обучающихся систем; методы извлечения информации; искусственные иммунные системы для выявления подделок; методы обработки сигналов и изображений [2].

Для построения системы обнаружения компьютерных атак предлагается использовать методы искусственных иммунных систем и нейронных сетей.

Для достижения поставленной цели необходимо решить следующие задачи:

– предложить структуру системы обнаружения атак на основе искусственных иммунных систем и нейронных сетей;

– разработать методы и алгоритмы функционирования системы обнаружения компьютерных атак;

– разработать программное обеспечение системы.

Предполагается, что разработка системы обнаружения компьютерных атак, основанной на применении методов искусственных иммунных систем и нейронных сетей, позволит существенно повысить вероятность обнаружения неизвестных сетевых вторжений.

**Литература**

1. Кашаев, Т.Р. Применение искусственной иммунной системы для решения задачи обнаружения атак / Материалы 3-й Всероссийской зимней школы – семинара аспирантов и молодых ученых / Т.Р. Кашаев. – Уфа: УГАТУ, 2008. – С. 326-332.

2. Дасгупта, Д. Искусственные иммунные системы и их применение / Д. Дасгупта; пер. с англ. под ред. А.А. Романюхи. – М.: ФИЗМАТЛИТ, 2006. – 344 с.

УДК 004.8.032.26

## НАСТРОЙКА ПОРОГОВ НЕЙРОСЕТЕВЫХ ДЕТЕКТОРОВ ДЛЯ РАСПОЗНАВАНИЯ КЛАССОВ СЕТЕВЫХ АТАК

***Кочурко П.А.***

*УО «Брестский государственный технический университет», г. Брест*

При решении задач обнаружения попыток несанкционированного доступа к системе можно выделить два основных подхода: обнаружение аномалий и обнаружение злоупотреблений.

Нелинейные рециркуляционные нейронные сети (РНС) способны выступить в качестве детекторов СОА, реализующей обе технологии. Известно [1], что именно объединение обеих технологий в рамках одной системы может позволить повысить качество обнаружения и снизить уровень ложных срабатываний.

В случае применения нелинейных рециркуляционных сетей (РНС) в качестве детектора аномалий [2] обучение РНС производится на нормальных соединениях таким образом, чтобы входные вектора на выходе восстанавливались в себя, при этом, чем соединение более похоже на нормальное, тем меньше ошибка реконструкции:

$$E^k = \sum_j (\bar{X}_j^k - X_j^k)^2, \quad (1)$$

где $X_j^k$ – *j*-й элемент *k*-го входного вектора, $\overline{X}_j^k$ – *j*-й элемент *k*-го выходного вектора. Если $E^k > T$, где $T$ – некий заданный для данного дететора порог, то соединение признаётся аномалией, или атакой, иначе – нормальным соединением.

Таким образом, одна РНС может применяться для определения принадлежности входного вектора к одному из двух классов – тому, на котором обучалась (класс $A$), или ко второму (класс $\overline{A}$), которому соответствуют далеко отстающие вектора. Объединив в одной системе *N* подобным образом обученных детекторов, каждый из которых отвечает за анализ принадлежности входного вектора к одному из классов $A_i$, можно успешно решать задачу распознавания типа или класса атаки. Для этого необходимо анализировать относительную ошибку реконструкции

$$\delta_i^k = \frac{E_i^k}{T_i}, \quad (2)$$

где $T_i$ – порог *i*-го детектора, изначально $T_i = mean\delta_i^k$. Чем меньше $\delta_i^k$, тем более вероятна принадлежность входного *k*-го образа к классу $A_i$.