

**УДК 519.876.5**

## **КЛАССИФИКАЦИЯ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ**

*Михерский Р. М.\**

*Физико-технический институт, Крымский федеральный университет имени  
В. И. Вернадского, Симферополь 295007, Россия  
\*E-mail: [mrm03@mail.ru](mailto:mrm03@mail.ru)*

Разработана и программно реализована искусственная иммунная система, позволяющая проводить классификацию данных. Показано, что данная система способна распознавать символы рукописного текста.

**Ключевые слова:** искусственная иммунная система, система искусственного интеллекта.

**PACS:** 07.05.Mh

### **ВВЕДЕНИЕ**

В настоящее время искусственные иммунные системы являются одним из самых перспективных направлений развития искусственного интеллекта. По сравнению с конкурирующими технологиями, такими как нейронные сети и генетические алгоритмы, данный подход имеет ряд существенных преимуществ, одним из которых является возможность использования искусственных иммунных систем в высокопроизводительных системах параллельных вычислений.

Теоретические основы применения искусственных иммунных систем были заложены в классических работах [1–3]. На сегодняшний день искусственные иммунные системы с успехом используются для сжатия информации [4], машинного обучения [5,6], решения задач классификации [7], оптимизации [8,9], нахождения аномалий [10], компьютерной безопасности [11], извлечения информации и обработки не структурированных данных [12], адаптивного контроля [13].

Целью данной работы явилось построение искусственной иммунной системы способной решать задачу классификации данных.

### **1. АЛГОРИТМ РАБОТЫ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ**

Предполагается, что на вход данной системы подаются кортежи бит, называемые «вирусами». Вирусы взаимодействуют с кортежами бит, называемых «лимфоцитами». Длина кортежей лимфоцитов совпадает с длиной кортежей вирусов. Задачей системы является определение, к какому классу относится данный вирус. Для этого на первом этапе систему необходимо обучить. С этой целью создается два массива: массив вирусов, представляющий собой набор различных вариантов, обрабатываемых данных относящихся к одному классу и массив лимфоцитов, на начальном этапе представляющий набор кортежей случайных чисел. В процессе обучения кортежи вирусов, для которых известно, к

какому классу они относятся, побитно сравниваются с кортежами «лимфоцитов». Обобщенной мерой, характеризующей близость кортежей вирусов и лимфоцитов в подобных системах чаще всего, является расстояние Хэмминга. Вероятность взаимодействия обычно зависит от этого расстояния: чем оно меньше, тем выше вероятность взаимодействия. В данной работе была предложена другая формула расчета вероятности  $p$  взаимодействия:

$$p = \frac{\log_2(2^{n_1} + 2^{n_2} + \dots + 2^{n_k})}{n} \quad (1)$$

где,  $n_1, n_2, \dots, n_k$  – длины последовательностей совпадающих элементов вируса и лимфоцита,  $n$  – длина кортежа вируса и лимфоцита.

В частности если все элементы вируса и лимфоцита совпадают, вероятность взаимодействия  $p = 1$ . Если же совпадают не все элементы, то  $p < 1$ . В случае если между вирусом и лимфоцитом происходит взаимодействие, данный экземпляр вируса уничтожается, а лимфоцита размножается. В рассматриваемой системе коэффициент размножения лимфоцитов равнялся 10. В случае если взаимодействие не происходит, производится мутация тех элементов лимфоцита, которые не совпадают с соответствующими элементами вируса с вероятностью  $p_1 = \frac{1}{n}$ .

Процесс происходит до тех пор, пока в массиве вирусов остается, хотя бы один элемент.

В случае если ни одного элемента в массиве не осталось, процесс обучения лимфоцитов для распознавания вирусов данного класса можно считать законченным.

Аналогичным образом получают массивы лимфоцитов для всех классов вирусов, которые нужно распознавать.

Пусть теперь на вход системы подается вирус, о котором нет сведений, к какому классу он относится. На первом этапе проводится клонирование этого вируса для того что бы создать массив таких вирусов. Далее из каждого ранее полученного массива лимфоцитов отбирается одинаковое их количество в новый массив. Лимфоциты из этого нового массива взаимодействуют с вирусами до полного их уничтожения. На последнем этапе производится подсчет лимфоцитов, и определяется, лимфоциты какого класса размножились наиболее успешно. Соответственно, считается, что вирус принадлежал именно к этому классу.

## 2. ПРИМЕНЕНИЕ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ ДЛЯ РАСПОЗНАВАНИЯ РУКОПИСНОГО ТЕКСТА

На основании вышеизложенного алгоритма была разработана и программно реализована искусственная иммунная система. Программная реализация иммунной системы была осуществлена с помощью интегрированной среды разработки Visual

Studio 2015 и языка программирования C#. Тестирования данной иммунной системы проводилось на ноутбуке Dell Inspiron 5520 с встроенной Web-камерой (процессор Intel Core i5-3210M CPU 2.50 GHz, объем оперативной памяти 6 ГБ).

Разработанная программная система работает следующим образом. На экране компьютера отображается изображение, получаемое с Web-камеры. Изображение рукописного текста, образ которого необходимо записать в систему, размещается в поле зрения камеры так, чтобы оно оказалось в центре отображаемой картинке, и проводится обучение системы. После обучения система используется для распознавания рукописного текста.

В ходе проведенного эксперимента система была обучена распознавать десять цифр. На этапе тестирования правильности распознавания системой образов, ей предъявлялось десять вариантов рукописного написания полного набора цифр (от 0 до 9). Соответственно, всего было предъявлено для распознавания 100 цифр.

В таблице 1 представлена зависимость процента правильно распознанных цифр от значения этих цифр.

Таблица 1. Процент правильно распознанных цифр

Цифра	0	1	2	3	4	5	6	7	8	9
Процент правильно распознанных цифр, %	90	90	80	80	100	70	100	90	80	90

Как видно из этой таблицы, наиболее хорошо система распознает цифры 4 и 6, хуже всего – цифру 5. Средний процент правильно распознанных цифр составил 87%.

### **ЗАКЛЮЧЕНИЕ**

Таким образом, разработанная искусственная иммунная система позволяет проводить устойчивую классификацию данных.

Следует отметить, что представленная в данной работе искусственная иммунная система может быть успешно применена не только для распознавания символов рукописного текста, но и для распознавания других зрительных образов, таких как: лица людей, изображения знаков дорожного движения и т.д.

### **Список литературы**

1. Farmer J. D., Packard N. H., Perelson A. S. The immune system, adaptation, and machine learning // *Physical D*. 1986. Vol. 22. Pp. 187–204.
2. Kephart J. O. A biologically inspired immune system for computer // *In Artificial Life IV: Proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems*. 1994. Pp. 130–139.
3. *Artificial Immune Systems and Their Applications* / D. Dasgupta (Editor) // Springer-Verlag, Inc. Berlin. 1999. 306 p. ISBN 3-540-64390-7.

4. Станкевич Л. А., Казанский А. Б. Иммунологическая система обеспечения безопасности гуманоидного робота // Актуальные проблемы защиты и безопасности: тр. 9-й Всерос. науч.-практич. конф. 2006. № 5. С. 145–152.
  5. Hunt J. E., Cooke D. E. Learning using an artificial immune system // *Journ. of Network Computing Applications*. 1996. Vol. 19. Pp. 189–212.
  6. Dasgupta D., Yua S., Nino F. Recent advances in artificial immune systems : Models and applications // *Applied Soft Computing*. 2011. Vol. 11. Pp. 1574–1587.
  7. Бардачев Ю. Н., Дидык А. А. Использование положений теории опасности в искусственных иммунных системах // *Автоматика, автоматизация, электротехнические комплексы и системы*. 2007. № 2. С. 107–111.
  8. Брюховецкий А. А., Скатков А. В. Применение моделей искусственных иммунных систем для решения задач многомерной оптимизации // *Оптимізація виробничих процесів*. 2010. № 7. С. 119–122.
  9. Clonal optimization-based negative selection algorithm with applications in motor fault detection./ X. Z. Gao, S. J. Ovaska, X. Wang, M. Y. Chow // *Neural Computing and Applications*. 2009. Vol. 18. No. 7. Pp. 719–729.
  10. Garrett S. M. How do we evaluate artificial immune systems? // *Evolutionary Computation*. 2005. Vol. 13. Pp. 145–178.
  11. Kim J., Bentley P. Towards an artificial immune system for network intrusion detection: An investigation of dynamic clonal selection // *In Proc. Congress on Evolutionary Computation, Honolulu, HI, USA*. 2002. Pp. 1244–1252.
  12. Knight T., Timmis J. Aine: An immunological approach to data mining // *IEEE Intern. Conf. on Data Mining*. 2001. Pp. 297–304.
  13. Krishna K. K., Neidhoefer J. Immunized adaptive critic for an autonomous aircraft control application // Ed. by Dasgupta D. // *Springer-Verlag Inc.*. 1999. Vol. 20, Pp. 221–240.
- 

## CLASSIFICATION OF DATA WITH THE USE OF THE ARTIFICIAL IMMUNE SYSTEM

*Michersky R. M.*

*Institute of Physics and Technology, V.I. Vernadsky Crimean Federal University, Simferopol 295007, Russia*

*\*E-mail: [mrm03@mail.ru](mailto:mrm03@mail.ru)*

An artificial immune system has been developed and software implemented, which makes it possible to classify data. It is shown that this system is able to recognize characters of handwritten text.

**Keywords:** artificial immune system, artificial intelligence system.

### References

1. J. D. Farmer, N. H. Packard, A. S. Perelson *Physical D* **22**, 187–204 (1986).
2. J. O. Kephart, “A biologically inspired immune system for computer” In *Artificial Life IV: Proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems* (1994) Pp. 130–139.
3. *Artificial Immune Systems and Their Applications* (Ed. By D. Dasgupta; Springer-Verlag, Inc. Berlin. 1999). 306 p.
4. L. A. Stankevich, A. B. Kazanskij, “Immunologicheskaya sistema obespecheniya bezopasnosti gumanoidnogo robota,” [“Immunological safety system for a humanoid robot,”] in *Actual problems of protection and safety: thesis of 9-th Russian scientific-practical conference No. 5* (2006) Pp. 145–152. [in Russian].

5. J. E. Hunt, D. E. Cooke, *Journ. of Network Computing Applications* **19**, 189–212 (1996).
6. D. Dasgupta, S. Yua, F. Nino. *Applied Soft Computing*. **11**, 1574–1587 (2011).
7. Yu. N. Bardachev, A. A. Didyk, *Avtomatika, avtomatizatsiya, ehlektrotekhnicheskie komplekсы i sistemy* [*Automation, automation, electrotechnical complexes and systems*], No. 2, 107–111 (2007). [in Russian].
8. A. A. Bryukhovetskij, A. V. Skatkov, *Optimization of productive processes* [Avtomatishhatsiya vyrobnychikh protsesiv], No. 7, 119–122 (2010). [in Ukrainian]
9. X. Z. Gao, S. J. Ovaska, X. Wang, M. Y. Chow, *Neural Computing and Applications* **18**, No. 7, 719–729 (2009).
10. S. M. Garrett, *Evolutionary Computation*. **13**, 145–178 (2005).
11. J. Kim, P. Bentley, “Towards an artificial immune system for network intrusion detection: An investigation of dynamic clonal selection”, *In Proc. Congress on Evolutionary Computation* (Honolulu, HI, USA, 2002) Pp. 1244–1252.
12. T. Knight, J. Timmis, “Aine: An immunological approach to data mining”, *in IEEE Intern. Conf. on Data Mining* (2001) Pp. 297–304.
13. K. K. Krishna, J. Neidhoefer, *Immunized adaptive critic for an autonomous aircraft control application* **20** (Ed. by D. Dasgupta, Springer-Verlag Inc., 1999) Pp. 221–240.

*Поступила в редакцию 25.03.2017 г. Принята к публикации 4.05.2017 г.  
Received March 25, 2017. Accepted for publication May 04, 2017*