



Прикладные проблемы оптимизации

<https://doi.org/10.25559/SITITO.019.202304.973-980>

УДК 004.8

Применение механизмов работы искусственной иммунной системы для решения задачи обнаружения аномалий в рядах данных

И. Ф. Астахова*, Ю. В. Хицкова

Оригинальная статья

ФГБОУ ВО «Воронежский государственный университет», г. Воронеж, Российская Федерация

Адрес: 394018, Российская Федерация, г. Воронеж, Университетская площадь, д. 1

* astachova@list.ru

Аннотация

Биология всегда была источником идей для различных наук. Не являются исключением и компьютерные науки. Так, например, уже получили широкое распространение нейронные сети и генетические алгоритмы. В последние десятилетия интерес к исследованию механизмов работы иммунной системы заметно возрос. Ее принципы работы имеют широкое приложение в ряде задач оптимизации, обработки и анализа данных и многих других. Обнаружение аномалий в поведении системы или процессов является важной задачей для многих приложений, задача заключается в изучении особенностей применения этого механизма, программно его реализовать и проанализировать его работу.

Анализ данных работ показал, что данные методы показывают хорошие результаты, однако имеют ряд недостатков, самыми существенными из которых является сложность организации и большое время, затрачиваемое на обучение. Таким образом, ставится проблема разработки новых алгоритмов, сравнимых по скорости принятия решения с искусственными сетями и экспертными системами и при этом обладающих меньшим временем обучения. Одним из путей решения этой задачи является разработка модели принятия решений на основе искусственной иммунной системы. Целью работы является разработка и исследование модели формализации процесса принятия решений в поиске аномалий данных с использованием искусственной иммунной системы. Нормальное поведение системы зачастую характеризуется дискретными временными рядами наблюдений. В этом случае задачу нахождения аномалий можно сформулировать как задачу нахождения недопустимых отклонений в характеристиках системы.

Искусственная иммунная система представляет идеализированный вариант естественного аналога и воспроизводит ключевые составляющие природного процесса: отбор лучших антител популяции в зависимости от степени их аффинитета (близости) к антигену, клонирование антител, мутация антител.

Ключевые слова: искусственный интеллект, искусственная иммунная сеть, искусственная иммунная система, ряды данных, алгоритм отрицательного отбора

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Астахова И. Ф., Хицкова Ю. В. Применение механизмов работы искусственной иммунной системы для решения задачи обнаружения аномалий в рядах данных // Современные информационные технологии и ИТ-образование. 2023. Т. 19, № 4. С. 973-980. <https://doi.org/10.25559/SITITO.019.202304.973-980>

© Астахова И. Ф., Хицкова Ю. В., 2023



Контент доступен под лицензией Creative Commons Attribution 4.0 License.
The content is available under Creative Commons Attribution 4.0 License.



Applied Optimization Problems

Application of the Mechanisms of the Artificial Immune System to Solve the Problem of Detecting Anomalies in the Data Series

I. F. Astachova, Yu. V. Khitskova

Original article

Voronezh State University, Voronezh, Russian Federation

Address: 1 Universitetskaya pl., Voronezh 394018, Russian Federation

* astachova@list.ru

Abstract

Biology has always been a source of ideas for various sciences. Computer science is no exception. For example, neural networks and genetic algorithms have already become widespread. In recent decades, I have been actively paying attention to the study of the mechanisms of the immune system. Its principles of operation have wide application in a number of optimization tasks, data processing and analysis, and many others. Detecting anomalies in the behavior of a system or processes is an important task for many applications, the task is to study the features of using this mechanism, implement it programmatically and analyze its operation.

The analysis of these works showed that these methods show good results, but they have a number of disadvantages, the most significant of which is the complexity of the organization and the long time spent on training. Thus, the problem is posed of developing new algorithms that are comparable in decision-making speed with artificial networks and expert systems and at the same time have less learning time. One of the ways to solve this problem is to develop a decision-making model based on an artificial immune system. The aim of the work is to develop and study a model for formalizing the decision-making process in the search for data anomalies using an artificial immune system. The normal behavior of the system is often characterized by discrete time series of observations. In this case, the problem of finding anomalies can be formulated as the problem of finding unacceptable deviations in the characteristics of the system.

The artificial immune system represents an idealized version of the natural analogue and reproduces the key components of the natural process: selection of the best antibodies of the population depending on the degree of their affinity (proximity) to the antigen, cloning of antibodies, mutation of antibodies.

Keywords: artificial neural network, artificial immune system, artificial immune system, data series, algorithm of negative selection

Conflict of interests: The authors declare no conflict of interests.

For citation: Astachova I.F., Khitskova Yu.V. Application of the Mechanisms of the Artificial Immune System to Solve the Problem of Detecting Anomalies in the Data Series. *Modern Information Technologies and IT-Education*. 2023;19(4):973-980. <https://doi.org/10.25559/SITITO.019.202304.973-980>



Введение

Биология всегда была источником идей для различных наук. Не являются исключением и компьютерные науки. Так, например, уже получили широкое распространение нейронные сети и генетические алгоритмы. В последние десятилетия проявляется активное внимание к изучению механизмов иммунной системы. Ее принципы работы имеют широкое приложение в ряде задач оптимизации, обработки и анализа данных и многих других.

Обнаружение аномалий в системах и процессах является актуальной задачей. Одним из решений данной задачи является применение механизма работы иммунной системы¹ [1-5].

Упрощенно схему иммунного ответа можно описать следующим образом. Патоген, проникший в организм, частично разрушается. Образовавшиеся чужеродные фрагменты «презентируются» на поверхности макрофагов и В-клеток. При помощи специфических рецепторов Т-клетки распознают и связывают такие фрагменты в комплексе со специальным белком. Однако далеко не большое число клеток иммунной системы имеют соответствующие рецепторы. Этот факт приводит к необходимости клональной селекции, т.е. к созданию клонов с антигенспецифичными рецепторами. Такие активизированные и клонированные Т-клетки выполняют различные функции. Некоторые из них, называемые Т-киллерами, разрушают клетки организма, инфицированные вирусом. Некоторые – Т-хелперы – взаимодействуют с В-клетками. В-лимфоциты при активации начинают выделять в плазму антитела, которые связываются с соответствующими антигенами, что ведет к их последующему уничтожению. При этом часть антител (и Т-, и В-клеток) становятся «клетками памяти», они остаются в организме на долгое время. Именно они участвуют при вторичном иммунном ответе² [6-9].

Иммунную систему можно рассматривать как источник множества принципов и механизмов, имеющих широкое применение. Ведь иммунная система – это самоорганизующаяся, распределенная и не имеющая центрального управления система, ее поведение определяется общей суммой локальных взаимодействий.

Одной из главных задач иммунной системы является распознавание своих клеток и любых чужеродных клеток и молекул. За распознавание чужеродных белков отвечают Т-лимфоциты, которые имеют на своей поверхности специальные рецепторы. Эти рецепторы специфически распознают чужеродные антигены, поэтому возникает необходимость наличия Т-лимфоцитов с разнообразными рецепторами. Это

многообразие достигается в результате псевдослучайного процесса перестановки фрагментов генома в ходе деления Т-лимфоцитов. После деления Т-лимфоциты и их рецепторы подвергаются отрицательному отбору, в процессе которого клетки, рецепторы которых реагируют на собственные комбинации белков, отвергаются. Таким образом, в организм попадают лишь те Т-лимфоциты, рецепторы которых реагируют только на чужеродные антигены. Этот процесс отбора крайне важен для способности иммунной системы разделять клетки на свои и чужеродные.

Цель работы

Целью работы является разработка и исследование модели формализации процесса принятия решений в поиске аномалий данных с использованием искусственной иммунной системы.

Материалы и методы

Алгоритм отрицательного отбора основывается на следующих компонентах [6], [10].

- Свои (*self*) определяются как совокупность S строк длины l . В контексте рассматриваемой задачи своими считаются нормальные показатели активности или устойчивого поведения исследуемой системы или процесса.

- Создание набора детекторов R , ни один из которых не должен соответствовать никакой строке из S . Если строки имеют достаточно большую длину, то точное соответствие маловероятно. Поэтому применяется правило частичного соответствия, при котором две строки соответствуют друг другу, тогда и только тогда, когда они совпадают по крайней мере в g следующих друг за другом позициях, где g – некоторый целочисленный параметр, выбирается в зависимости от решаемой задачи.

- Контроль поступающих данных осуществляется путем непрерывного сопоставления этих данных с набором детекторов. Если обнаруживается совпадение с детектором, значит произошло изменение (отклонение) в поведении контролируемой системы.

Таким образом, задача обнаружения аномалий сводится к обнаружению изменений в строке (совпадение с детектором).

Обнаружение аномалий в поведении системы или процессов является важной задачей для многих приложений, задача заключается в изучении особенностей применения этого механизма, программно его реализовать и проанализировать его работу.

Нормальное поведение системы зачастую характеризуется дискретными временными рядами наблюдений. В этом случае задачу нахождения аномалий можно сформулировать как задачу нахождения недопустимых отклонений в характеристиках системы.

Для работы с поступающими данными необходимо изменить их форму представления. Но при этом должно

¹ Искусственные иммунные системы и их применение : сб. статей / под ред. Д. Дасгупты. М.: Физматлит, 2006. 344 с.; Timmis J., Knight T. Artificial immune systems: Using the immune system as inspiration for data mining. Data Mining: A Heuristic Approach. Idea Group, 2001. p. 209-230.

² Dasgupta D., Forrest S. Tool breakage detection in milling operations using a negative selection algorithm. Technical Report CS95-5. Department of Computer Science, University of New Mexico, NM, 1995.



сохраниться информационное содержание. Кроме того, в новой форме записи должны полностью отображаться любые изменения, которые выходят за границы допустимых вариаций паттернов данных. Этот момент может вызвать затруднения, если нужно будет выявлять небольшие изменения в потоке реальных данных. Данную проблему можно решить, используя следующий вариант кодирования входных данных.

Для аналоговой величины имеются ограничения: минимальное значение MIN и максимальное MAX. Интервал (MIN, MAX) делится на множество интервалов. Далее определяется, к какому интервалу относится аналоговая величина. И уже принадлежность к определенному интервалу кодируется в бинарной форме.

В зависимости от требуемой точности выбирается величина m , она равна количеству двоичных знаков необходимых для кодирования одного набора данных. Если величина расположена за пределами (MIN, MAX), то она кодируется всеми нулями или всеми единицами, в зависимости от того, за какую границу она вышла. Тогда между MIN и MAX значениями можно выделить $2^m - 2$ интервала. Соответственно, длина интервала L вычисляется по следующей формуле

$$L = (MAX - MIN) / (2^m - 2) \quad (1)$$

Таким образом, для аналоговой величины v имеем

$$MIN \leq v \leq MAX, \quad (2)$$

где $MAX = MIN + (2^m - 2)L$.

Т.е. она может быть отнесена к определенному интервалу и закодирована двоичным числом, соответствующим номеру этого интервала, т.е. если величина v такова, что

$$MIN + nL \leq v \leq MIN + (n+1)L \quad (3)$$

то она кодируется двоичным числом, соответствующим номеру интервала n .

Наиболее близко генерацию Т-клеток в иммунной системе отражает исчерпывающий алгоритм генерации детекторов. Кандидаты в детекторы генерируются случайным образом и сверяются со всеми строками из множества своих строк S . Если они не соответствуют ни одной из своих строк, то они сохраняются как действительные детекторы. Этот процесс случайной генерации и проверки на соответствие строкам из S повторяется до тех пор, пока не будет сформировано необходимое количество действительных детекторов.

Определим вероятность соответствия P_m как вероятность того, что случайным образом выбранная строка и детектор соответствуют друг другу в соответствии с некоторым правилом.

Далее определим вероятность отказа (неудачи) P_f как вероятность того, что произвольная не своя строка не будет соответствовать ни одному из детекторов из R .

Для данного алгоритма требуется сгенерировать множество кандидатов в детекторы, размер которого экспоненциально зависит от размера множества своих строк N_s .

Начальная мощность совокупности детекторов до отрицательного отбора при фиксированном P_m вычисляется по следующей формуле:

$$N_{R_0} = \frac{-\ln(P_f)}{P_m * (1 - P_m)^{N_s}}. \quad (4)$$

Для независимых детекторов можно приблизить вероятность отказа P_f для набранных детекторов N_R :

$$P_f \approx (1 - P_m)^{N_R}. \quad (5)$$

Для достаточно малого P_m и достаточно большого N_R получим:

$$N_R \approx \frac{-\ln(P_f)}{P_m}. \quad (6)$$

Предположение о независимости детекторов не совсем справедливо. При увеличении N_s или P_m множество кандидатов в детекторы будет сокращаться, поэтому выбранные детекторы будут менее независимыми.

Временная сложность этого алгоритма пропорциональна N_R - количеству кандидатов в детекторы, которые должны быть рассмотрены, и N_s , т.к. возможно, придется сравнивать каждого кандидата с каждой своей строкой.

$$\text{Временная сложность: } O\left(\frac{-\ln(P_f)}{P_m * (1 - P_m)^{N_s}}\right) N_s,$$

$$\text{Пространственная сложность: } O(l * N_s).$$

Однако, не смотря на свою гибкость в выборе правила для сопоставления строк, эффективным данный алгоритм назвать нельзя ввиду того, что большая часть кандидатов в детекторы отвергается и с увеличением размера множества своих строк время выполнения растёт экспоненциально. Поэтому для замены были предложены два новых алгоритма: «жадный» алгоритм и алгоритм, работающий за линейное время (будем называть его линейным алгоритмом).

Линейный алгоритм является двухфазным, на первой фазе которого методом динамического программирования пересчитываются все неповторяющиеся строки, а на втором из всех допустимых детекторов формируется множество строк детектора. То есть, на первом этапе для множества своих строк S и порога соответствия r алгоритм определяет общее число строк, не совпадающих ни с одной строкой из S . На втором этапе часть этих строк используется для формирования детекторов [11-14].

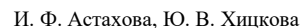
Линейный алгоритм работает за время, сопоставимое с размером множества своих строк. Однако, с увеличением r и l пространственная и временная сложность начинает расти по экспоненте, что, впрочем, проявляется только при работе с длинными строками и большим порогом соответствия r .

$$\text{Временная сложность: } O((l - r + 1) \cdot N_s M^r) + O((l - r + 1) \cdot m^r) + O(l \cdot N_R)$$

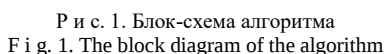
$$\text{Пространственная сложность: } O((l - r + 1)^2 \cdot m^r)$$

Исходя из всего вышесказанного, наиболее эффективным для использования алгоритмом будет пока линейный алгоритм как более быстрый и надежный.

Для линейного алгоритма используются множество своих строк и правило совпадения строк с порогом соответствия r , который означает, что если строки совпадают в r смежных битах, то они совпадают.



На рисунке 1 представлена блок-схема алгоритма.



Source: Hereinafter in this article all tables and figures were made by the authors.

```

classDiagram
    class ImmuneSystem {
        -r: int
        -l: int
        -m: int
        -windows_size: int
        -Nr: int
        -C_ts: Dict
        -S: List
        -R: List
        -T: int
        +ImmuneSystem(m, r, shift, windows_size, dataToLearnPath, Nr)
        +GenerateMinAndMax(allData, out min, out max)
        +GenerateS(path)
        +Generate_DPA()
        +RecursionCount(templates)
        +GeneratingDetectors(templates)
        +CheckMatching(newDec, i, r)
        +MatchingNumberRecursive(newDec, i, positionOfTemplate, r)
        +GenerateTemplatesWithGivenLength(length)
        +CheckData(path, out resultAnswer)
        +IsDetectorActivated(stringToCheck)
        +HaveDetectors()
    }
    class DataCoding {
        -MIN: double
        -MAX: double
        -m: int
        -amountOfIntervals: int
        -d: double
        +Operation1(MIN, MAX, m)
        +CodeData(dataToCode)
    }
    ImmuneSystem --> DataCoding : 1
    DataCoding --> ImmuneSystem : 1

```

Fig. 2. Class diagram

Создание детекторов

Значение г: 5

Значение т: 5

Количество детекторов: 100

Размер окна: 3

Сдвиг: 1

Путь: C:\Users\Ilya\Desktop\Data1

Открыть

Создать

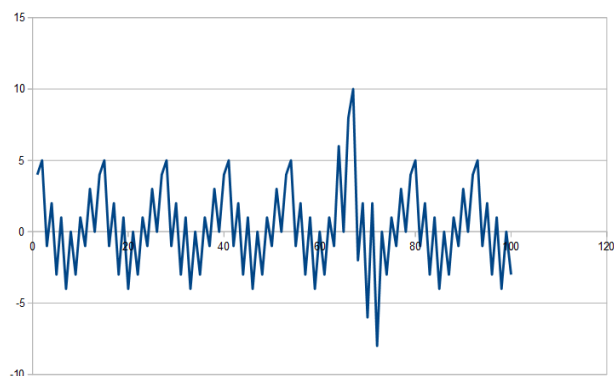
Все тесты проводятся для различных заданных наборов точности кодирования, порога соответствия, набора детекторов, сдвига паттерна и размера окна. Все тесты запускаются 15 раз. Все результаты представлены в таблице 1. В таблице представлены следующие столбцы: первый столбец содержит в себе значения точности кодирования, сдвига паттерна и размер окна; во втором столбце содержится значение порога



соответствия; в третьем – количество детекторов; в четвертом – процентное соотношение успешных находений аномалий к общему количеству [15-18].

Т а б л и ц а 1. Результаты тестирования программы на большом наборе данных, содержащем значительные изменения, не выходящие за граничные значения нормальных данных
Table 1. Test Results on a Large Dataset with Significant Changes within Normal Boundary Values

	r	N_R	Выявление аномалий
$m = 5$ $patternSize = 4$ $shift = 4$	9	150	100%
	10	200	100%
$m = 5$ $patternSize = 6$ $shift = 4$	10	150	93,3%
	14	200	93,3%



Р и с. 4. Результаты тестирования программы на большом наборе данных, содержащем значительные отклонения

Fig. 4. The results of testing the program on a large data set containing significant deviations

Заклучение

В работе была рассмотрена проблема обнаружения аномалий в рядах данных. Был исследован один из подходов к ее решению, а именно применение механизмов работы естественной иммунной системы. Данный метод позволяет обнаружить любые отклонения от нормального поведения системы, в отличие от большинства методов, которые распознают

только конкретные виды аномалий, т.е. для рассматриваемого метода не требуется априорная информация о возможных дефектах, он не проверяет новые данные на совпадение с какими-либо конкретными классами аномалий, а проверяет, соответствуют ли новые данные нормальным. Однако требуется достаточный набор нормальных данных, чтобы на их основе можно было создать набор детекторов, которые с некоторой вероятностью обнаружат отклонения от нормального поведения системы.

Создание набора детекторов – важная подзадача, требующая анализа для каждого конкретного применения алгоритма. Существуют различные способы создания детекторов, в работе анализируются два различных метода и рассматривается дополнение одного из них [19-22].

Рассматриваемый алгоритм имеет широкую область применения. При использовании различных наборов параметров, различных способов кодирования аналоговых данных, алгоритм может работать фактически с любыми данными. Даже если система характеризуется несколькими параметрами, то паттерны данных можно создавать на основе комбинаций этих параметров. А изменяя значения таких параметров как размер паттерна, точность кодирования, параметр соответствия строк, можно регулировать уровень надежности работы алгоритма [23-25].

В ходе работы была программно реализована работа данного алгоритма, проведено его тестирование и оценка эффективности.

Результаты тестирования программы показали, что данный алгоритм одинаково эффективен как для наборов с однородными данными, так и для данных с большим изменением амплитуды. Также тестирование показало, что алгоритм достаточно эффективно обнаруживает отклонения в данных, которые выходят за границы нормальных значений (т.е. за пределы минимального и максимального значений), и такие отклонения, которые находятся в этих границах. А также по результатам тестирования видно, что алгоритм способен обнаруживать аномалии в данных даже при малом объеме нормальных данных [17-24].

References

1. Aickelin U., Dasgupta D., Gu F. Artificial Immune Systems. In: Burke E., Kendall G. (eds.) Search Methodologies. Boston, MA: Springer; 2014. p. 187-211. https://doi.org/10.1007/978-1-4614-6940-7_7
2. Dasgupta D., Nino F. Immunological Computation: Theory and Applications. CRC Press; 2008. 296 p. <https://doi.org/10.1201/9781420065466>
3. D'haeseleer P., Forrest S., Helman P. An immunological approach to change detection: algorithms, analysis and implications. In: Proceedings 1996 IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE Press; 1996. p. 110-119. <https://doi.org/10.1109/SECPRI.1996.502674>
4. D'haeseleer P. An immunological approach to change detection: theoretical results. In: Proceedings 9th IEEE Computer Security Foundations Workshop. Kenmare, Ireland: IEEE Press; 1996. p. 18-26. <https://doi.org/10.1109/CSFW.1996.503687>
5. Nebili W., Farou B., Kouahla Z., Seridi H. Revised Artificial Immune Recognition System. *IEEE Access*. 2021;9:167477-167488. <https://doi.org/10.1109/ACCESS.2021.3133731>
6. Dasgupta D., Forrest S. Novelty Detection in Time Series Data using Ideas from Immunology. In: ISCA 5th International Conference on Intelligent Systems. Reno, Nevada, June 19- 21, 1996.



7. Dasgupta D., Forrest S. Artificial immune systems in industrial applications. In: Proceedings of the Second International Conference on Intelligent Processing and Manufacturing of Materials. IPMM'99 (Cat. No.99EX296). Vol. 1. Honolulu, HI, USA: IEEE Press; 1999. p. 257-267. <https://doi.org/10.1109/IPMM.1999.792486>
8. de Castro L.N. Fundamentals of Natural Computing: An overview. *Physics of Life Reviews*. 2007;4(1):1-36. <https://doi.org/10.1016/j.plrev.2006.10.002>
9. Percus J.K., Percus O.E., Perelson A.S. Predicting the size of the T-cell receptor and antibody combining region from consideration of efficient self-nonself discrimination. *PNAS*. 1993;90(5):1691-1695. <https://doi.org/10.1073/pnas.90.5.1691>
10. Forrest S., Perelson A.S., Allen L., Cherukuri R. Self-nonself discrimination in a computer. In: Proceedings of 1994 IEEE Computer Society Symposium on Research in Security and Privacy. Oakland, CA, USA: IEEE Press; 1994. p. 202-212. <https://doi.org/10.1109/RISP.1994.296580>
11. Astachova I.F., Ushakov S.A., Shashkin A.I., Belyaeva N.V. The application of artificial immune system for parallel process of calculation and their comparison with existing methods. *Journal of Physics: Conference Series*. 2019;1202:02003. <https://doi.org/10.1088/1742-6596/1202/1/012003>
12. Astachova I.F., Kiseleva E.I. The algorithm is the use of artificial immune systems to optimize the target component of the information educational system. *Proceedings of Voronezh State University. Series: Systems Analysis and Information Technologies*. 2017;(2):61-65. (In Russ., abstract in Eng.) EDN: ZDWOMN
13. Yang H., Li T., Hu X., Wang F., Zou Y. A Survey of Artificial Immune System Based Intrusion Detection. *The Scientific World Journal*. 2014;156790. <https://doi.org/10.1155/2014/156790>
14. Park H., Choi J.E., Kim D., Hong S.J. Artificial immune system for fault detection and classification of semiconductor equipment. *Electronics*. 2021;10(8):944. <https://doi.org/10.3390/electronics10080944>
15. Pinto R., Gonçalves G. Application of artificial immune systems in advanced manufacturing. *Array*. 2022;15:100238. <https://doi.org/10.1016/j.array.2022.100238>
16. Wawryn K., Widuliński P. Detection of anomalies in compiled computer program files inspired by immune mechanisms using a template method. *Journal of Computer Virology and Hacking Techniques*. 2021;17:47-59. <https://doi.org/10.1007/s11416-020-00364-w>
17. Rizwan R., Khan F.A., Abbas H., Chauhdary S.H. Anomaly Detection in Wireless Sensor Networks Using Immune-Based Bioinspired Mechanism. *International Journal of Distributed Sensor Networks*. 2015;2015:1-10. <https://doi.org/10.1155/2015/684952>
18. Ray S., McEvoy D.S., Aaron S., Hickman T.T., Wright A. Using statistical anomaly detection models to find clinical decision support malfunctions. *Journal of the American Medical Informatics Association*. 2018;25(7):862-871. <https://doi.org/10.1093/jamia/ocy041>
19. Javaid M., Haleem A., Singh R.P., Suman R. Artificial intelligence applications for industry 4.0: A literature-based study. *Journal of Industrial Integration and Management*. 2022;7(01):83-111. <https://doi.org/10.1142/S2424862221300040>
20. Wawrzyński P., Arabas J., Cichosz P. Predictive Control for Artificial Intelligence in Computer Games. In: Rutkowski L., Tadeusiewicz R., Zadeh L.A., Zurada J.M. (eds.) Artificial Intelligence and Soft Computing – ICAISC 2008. ICAISC 2008. *Lecture Notes in Computer Science*. Vol. 5097. Berlin, Heidelberg: Springer; 2008. p. 1137-1148. https://doi.org/10.1007/978-3-540-69731-2_107
21. Fan X., Wu J., Tian L. A Review of Artificial Intelligence for Games. In: Liang Q., Wang W., Mu J., Liu X., Na Z., Chen B. (eds) Artificial Intelligence in China. *Lecture Notes in Electrical Engineering*. Vol. 572. Singapore: Springer; 2020. p. 298-303. https://doi.org/10.1007/978-981-15-0187-6_34
22. Lee Y.J. et al. Self-supervised Contrastive Learning for Predicting Game Strategies. In: Arai K. (eds) Intelligent Systems and Applications. IntelliSys 2022. *Lecture Notes in Networks and Systems*. Vol. 542. Cham: Springer; 2023. p. 136-147. https://doi.org/10.1007/978-3-031-16072-1_10
23. Cain C.B. Weiqi and Artificial Intelligence: Potential for Strategic Decision Making. In: Lai D. (eds.) U.S.-China Strategic Relations and Competitive Sports. Cham: Palgrave Macmillan; 2022. p. 325-359. https://doi.org/10.1007/978-3-030-92200-9_13
24. Caci B., Dhou K. The Interplay Between Artificial Intelligence and Users' Personalities: A New Scenario for Human-Computer Interaction in Gaming. In: Stephanidis C., et al. HCI International 2020 – Late Breaking Papers: Cognition, Learning and Games. HCII 2020. *Lecture Notes in Computer Science*. Vol. 12425. Cham: Springer; 2020. p. 619-630. https://doi.org/10.1007/978-3-030-60128-7_45
25. Michael Franklin D. Communicative Artificial Intelligence in Multi-agent Gaming. In: Arai K. (eds.) Advances in Information and Communication. FICC 2021. *Advances in Intelligent Systems and Computing*. Vol. 1363. Cham: Springer; 2021. p. 541-546. https://doi.org/10.1007/978-3-030-73100-7_38

Поступила 01.10.2023; одобрена после
рецензирования 07.11.2023; принята к публикации
06.12.2023.

Submitted 01.10.2023; approved after reviewing
07.11.2023; accepted for publication 06.12.2023.



Об авторах:

Астахова Ирина Федоровна, профессор кафедры математического обеспечения ЭВМ факультета прикладной математики, информатики и механики, ФГБОУ ВО «Воронежский государственный университет» (394018, Российская Федерация, г. Воронеж, Университетская площадь, д. 1), доктор технических наук, профессор, **ORCID:** <https://orcid.org/0000-0002-2627-8508>, astachova@list.ru

Хицкова Юлия Владимировна, доцент кафедры региональной экономики и территориального управления экономического факультета, ФГБОУ ВО «Воронежский государственный университет» (394018, Российская Федерация, г. Воронеж, Университетская площадь, д. 1), кандидат экономических наук, **ORCID:** <https://orcid.org/0000-0001-6322-8633>, prosvetovau@list.ru

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the authors:

Irina F. Astachova, Professor of the Chair of Computer Hardware, Faculty of Applied Mathematics, Informatics and Mechanics, Voronezh State University (1 Universitetskaya pl., Voronezh 394018, Russian Federation), Dr. Sci. (Eng.), Professor, **ORCID:** <https://orcid.org/0000-0002-2627-8508>, astachova@list.ru

Yulia V. Khitskova, Associate Professor of the Department of Regional Economics and Territorial Administration of the Faculty of Economics, Voronezh State University (1 Universitetskaya pl., Voronezh 394018, Russian Federation), Cand. Sci. (Econ.), **ORCID:** <https://orcid.org/0000-0001-6322-8633>, prosvetovau@list.ru

All authors have read and approved the final manuscript.