

Север Константин Олегович – Южный федеральный университет; e-mail: sever@sfedu.ru; г. Таганрог, Россия; кафедра теоретических основ радиотехники; аспирант.

Алексеев Кирилл Николаевич – e-mail: kalekseev@sfedu.ru; кафедра вычислительной техники; к.т.н., доцент.

Турулин Игорь Ильич – e-mail: iiturulin@sfedu.ru; кафедра теоретических основ радиотехники; д.т.н.; профессор.

Sever Konstantin Olegovich – Southern Federal University; e-mail: sever@sfedu.ru; Taganrog, Russia; the Department of Theoretical Foundations of Radio Engineering; post-graduate student.

Alekseev Kirill Nikolaevich – e-mail: kalekseev@sfedu.ru; the Department of Computer Science; cand. of eng. sc.; associate professor.

Turulin Igor Ilyich – e-mail: iiturulin@sfedu.ru; the Department of Theoretical Foundations of Radio Engineering; dr. of eng. sc.; professor.

УДК 004

DOI 10.18522/2311-3103-2024-3-168-176

В.А. Цыганков, О.А. Шабалина, А.В. Катаев**ИССЛЕДОВАНИЕ ВОЗДЕЙСТВИЯ РАЗМЕРА ПОПУЛЯЦИИ
НА БЫСТРОДЕЙСТВИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА**

Исследованы способы определения размера популяции в генетическом алгоритме и изучена зависимость между количеством особей и скоростью работы алгоритма. Описываются методы определения оптимального количества особей в популяции разными методами: в зависимости от размера хромосом, для древовидного типа хромосом, при наличии фактора зашумленности и по методу соседнего элемента с выставлением максимальной и минимальной границы. Данные, полученные по выполнению каждого метода, отличаются между собой, по причине этого произведена оценка с целью проверить точность теоретических данных, сравнив их с экспериментальными. Для проведения экспериментов была разработана программа на графической платформе «Unity» с возможностью изменения количества особей в популяции. После получения результатов было проведено сравнение экспериментальных данных с данными, полученными на основе методов определения размера популяции в генетическом алгоритме из первой части работы. Эксперимент показал, что оптимальный размер популяции лежит в диапазоне 100-160 особей. При уменьшении их количества время выполнения поставленной задачи начинает существенно увеличиваться, а при увеличении за расчетный предел – сокращение времени выполнения не соответствует затрачиваемым вычислительным ресурсам. Сами полученные экспериментальные данные имеют наименьшую погрешность с методом, используемым древовидное представление хромосом. Результаты исследования могут быть использованы для выбора размера популяции при обучении для достижения лучшего соотношения затрачиваемой вычислительной мощности к скорости обучения, а определенный в процессе работы метод может помочь в теоретических расчетах.

Генетический алгоритм; размер популяции; метод определения размера популяции; имитационная модель; хромосома; коэффициент зашумленности; оптимизация; объект с изменяемым поведением; неигровой персонаж; мутация.

V.A. Tsygankov, O.A. Shabalina, A.V. Kataev**INVESTIGATION OF THE IMPACT OF POPULATION SIZE
ON THE PERFORMANCE OF A GENETIC ALGORITHM**

The paper investigates ways to determine the population size in a genetic algorithm and studies the relationship between the number of individuals and the speed of the algorithm. Methods for determining the optimal number of individuals in a population by different methods are described: depending on the size of the chromosomes, for a tree-like type of chromosomes, in the presence of a noise factor and by the method of a neighboring element with a maximum and minimum boundary. The data obtained by performing each method differ from each other, for this reason, an assessment was made in order to verify the accuracy of theoretical data by comparing them with experimental ones. To conduct experiments, a pro-

gram was developed on the Unity graphics platform with the ability to change the number of individuals in the population. After receiving the results, the experimental data were compared with the data obtained on the basis of methods for determining the population size in the genetic algorithm from the first part of the work. The experiment showed that the optimal population size lies in the range of 100-160 individuals. With a decrease in their number, the execution time of the task begins to increase significantly, and with an increase beyond the calculated limit, the reduction in execution time does not correspond to the computing resources expended. The experimental data obtained themselves have the smallest error with the method used by the tree representation of chromosomes. The results of the study can be used to select the size of the population during training in order to achieve a better ratio of computing power to learning speed, and a method defined in the course of work can help in theoretical calculations.

Genetic algorithm; population size; population size determination method; simulation model; chromosome; noise factor; optimization; object with variable behavior; non-player character; mutation.

Введение. Генетический алгоритм (ГА) представляет собой класс оптимизационных методов, применяемый для решения широкого круга задач, таких как оптимизация, моделирование, анализ и нахождение глобального экстремума [1, 2].

Генетический алгоритм анализирует множество входных параметров оптимизированной задачи и оперирует совокупностью особей (популяцией), которые представляют собой строки с закодированным в них решением задачи. Во время подбора различных решений, наиболее подходящих по условиям задачи, «выживает» наиболее «приспособленная особь», которая является носителем оптимального решения [2–4]. Их эффективное использование зависит от способа представления и отбора решений, выбора операторов мутации и принципов формирования начальной популяции альтернативных решений. В настоящее время многие современные системы характеризуются нечеткостью входной и выходной информации, что часто делает некорректным их эффективное функционирование [4]. Это приводит к невозможности и затруднению практического применения существующих систем и методов поддержки принятия решений [5].

Одним из основных параметров ГА является размер популяции, от него зависит надежность алгоритма и время решения поставленной задачи [6, 7]. Данная работа посвящена исследованию воздействия размера популяции на быстродействие ГА и нахождению оптимального её размера. Целью работы является определение оптимального размера популяции в зависимости от входных и требуемых данных, условий и сравнение полученных результатов с уже разработанными способами.

Модели и методы определения размера популяции в генетическом алгоритме. Подбор оптимального размера популяции важен, так как он определяет эффективность поиска оптимального значения функции приспособленности. В случае выбора маленького размера возможно появление таких областей, которые не могут быть исследованы оператором кроссинговера, что отрицательно влияет на надежность алгоритма (в такой области может оказаться глобальный экстремум) [8]. Для организации оптимизирующего процесса необходимо создать направляющую силу развития популяции. В качестве такой силы выступает требование минимизации целевой функции или, в терминах генетических алгоритмов, фитнес функции. Обычно в качестве её используется аддитивный показатель оптимальности, основанный на штрафах. Преимуществом такого выбора является возможность настройки алгоритма под конкретную задачу путём варьирования коэффициентов и, тем самым, изменения приоритетов при поиске оптимального решения [9]. В случае выбора пользователем слишком большого размера популяции алгоритм будет тратить на решение поставленной задачи значительно больше времени, чем необходимо из-за большего расчёта целевой функции [10].

Однако в настоящее время данная область становится все более востребованной и появляются большое количество новых методов определения оптимального размера популяции. Так, в работе [11], размер популяции определяется от размера хромосомы и заданной вероятности события попадания битов в требуемый диапазон. Для этого были предложены формулы для определения минимального допустимого количества особей в популяции:

$$N > \log_{0.5} \left(\frac{1 - \sqrt[L]{P(S_L^N)}}{2} \right), \quad (1)$$

где N – размер популяции; P – вероятность события; L – размер хромосомы; b – i -й бит j -й хромосомы; S – событие, когда после инициализации ГА с размером популяции N и числом бит в хромосоме L для любого $1 \leq k \leq L$, выполняется неравенство:

$$0 < \sum_{j=1}^N b_k^j < N. \quad (2)$$

Формулы (1, 2) позволяют определить минимальное количество индивидуумов для решения задачи с требуемой точностью, зная только размер (битность) хромосомы.

В работе [12] рассматривалось влияние размеров популяции при древовидном представлении хромосом [13] на скорость сходимости и описывался эксперимент. В ней производилась оценка скорости сходимости от количества итераций, по прошествии которого значение приспособленности лучшей особи перестает увеличиваться. В результате эксперимента показано, что зависимость скорости работы алгоритма от количества особей имеет экспоненциальный вид. Таким образом, можно сделать вывод, что рост эффективности от добавления каждого нового члена популяции снижается. Главной задачей является найти тот размер популяции, при котором некоторое количество особей будут выдавать приемлемую скорость сходимости, но не будут перегружать машину [14].

В работе [15] описана модель для прогнозирования качества сходимости генетических алгоритмов от размера популяции в обычных условиях (3) и при наличии фактора зашумленности (4):

$$N = -2^{k-1} \ln(\alpha) \frac{\sigma_{bb} \sqrt{\pi m}}{d}. \quad (3)$$

$$N = -2^{k-1} \ln(\alpha) \frac{\sqrt{\pi m \sigma_{bb}^2 + \sigma_F^2}}{d}, \quad (4)$$

где σ_{bb} – дисперсия пригодности; α – частота отказов; bb – количество блоков; d – разность между пригодностями индивидов; m – количество разделов хромосом; $k > m$; F – коэффициент зашумленности.

Данная модель использует классификацию индивидуумов, опираясь на данные от предыдущих итераций. И представляет собой комплиментарность генетических алгоритмов и одноразовых расчетов. Которая возможна благодаря использованию блоков инициализации.

В статье [16] был разработан метод для автоматического определения размера популяции для выполнения расчета размерных цепей по методу соседнего элемента (По допуску замыкающего звена подбираются допуски составляющих звеньев). Для этого предложена формула:

$$(k) = \left(\frac{1}{k} \sum_{j=1}^k D_j \right) \left(\frac{1}{N-(k+1)} \sum_{j=k+1}^N D_j \right) = \frac{1}{k(N-1)-k^2} \left(\sum_{j=1}^k D_j \right) \left(\sum_{j=k+1}^N D_j \right), \quad (5)$$

где k – размер популяции; D_j – дисперсия повторяющихся значений при заданном размере популяции; N – предельное значение размера популяции.

В основе данного метода лежит регрессионная модель, с помощью которой возможно определить размер популяции в зависимости от допустимого количества значений независимой переменной [17]. Это позволяет моделировать формирование популяции без привязки к конкретным значениям переменных. Его удобно использовать в задачах дискретной оптимизации с целевыми функциями нескольких переменных, где области допустимых значений конечны и имеют небольшую размерность.

Рассмотренные методы определения оптимального количества популяции различаются используемыми параметрами и искомыми данными. Соответственно, полученные оптимальные значения о количестве популяции могут также различаться в зависимости от выбранного способа.

В статье [18] описан эксперимент, целью которого было определение изменчивости параметров модели от различных размеров популяции. По итогам данной работы были выделены три основных параметра и определены их диапазоны: максимальная удельная

скорость роста ($0 < \mu_{\max} < 0,7$), константа «насыщенности» ($0 < k_s < 1$) и коэффициент продуктивности ($0 < Y_{S/X} < 30$). При популяции в сто особей были получены следующие данные: $\mu_{\max} = 0,4881$; $k_s = 0,012$ и $Y_{S/X} = 2,0193$. Однако сам расчет размера популяции, в данной работе, не производился.

Разработка имитационной модели поведения объектов на основе генетического алгоритма. Для нахождения зависимости скорости работы генетических алгоритмов для обучения НС от размера популяции была разработана имитационная модель целенаправленной жизни объектов с изменяемым поведением в виртуальной среде. Модель представляется кортежем вида:

$$Life = (Entities, Goals, Behavior),$$

где *Life* – имитационная модель целенаправленной жизни;

Entities – множество сущностей, способных изменять свое положение в пространстве;

Goals – множество целей сущностей;

Behavior – алгоритм поведения сущностей для достижения поставленных целей.

В течение своей жизни, определяемой заданным промежутком времени, каждый объект стремится достичь максимально возможное количество целей, предопределенных средой. Для моделирования поведения объектов использован генетический алгоритм. Для предотвращения потери лучших решений и обеспечения повышенной сходимости алгоритма селективный отбор проводился элитарным методом (Только один предок с наивысшим счетом и наименьшим временем «давал» потомство) [19].

Реализация имитационной модели в среде разработки Unity. Имитационная модель реализована в программе на графической платформе «Unity» [20]. В среде создается сцена с полем, на котором находятся некоторое количество «комнат» (рис. 1), в которых объекты представлены в виде неигровых персонажей (НИП, NPC) и Целей (рис. 2). НИП состоит из головы (Воксель, способный поворачиваться на 180° в вертикальной и на 30° в горизонтальной плоскости) и тела (пяти последовательно соединенных вокселей, способных поворачиваться на 180° в вертикальной плоскости относительно друг друга). Цель – одиночный воксель. Задачей НИП является сбор наибольшего количества целей за отведенное время. Цель появляется в пределах своей комнаты, но НИП может её покинуть. Каждый НИП видит только свою Цель и не может взять чужую. Как только он достигает Цели, она появляется в другом месте комнаты, а счетчик НИП увеличивается на единицу и записывается время достижения данной Цели.

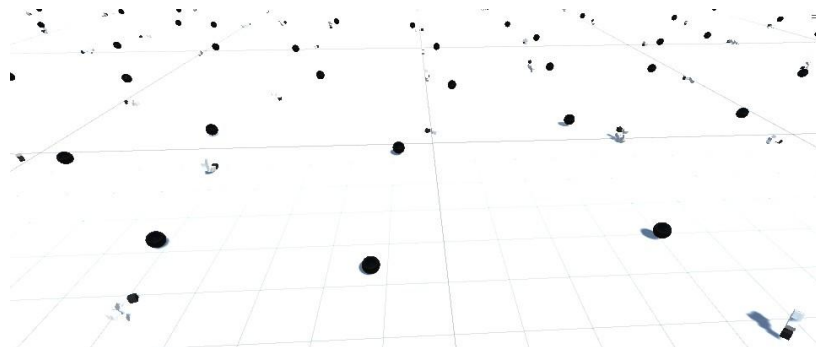


Рис. 1. Внешний вид поля с «комнатами»

Имитационная модель была успешно апробирована на задаче определения оптимального коэффициента мутации [21].

Для большей автономности работы был добавлен автостарт после завершения цикла, появилась возможность сохранения паттерна поведения в файл для его дальнейшего использования и сброс счетчиков и битов поведения без необходимости завершения работы. Для ускорения работы программы была в два раза уменьшена зона появления целей для каждой особи.

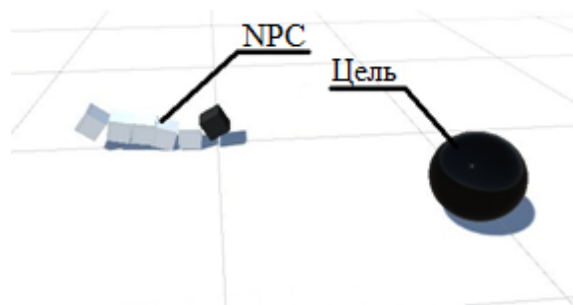


Рис. 2. НИП и Цель

В модифицированной версии был усовершенствован алгоритм работы. После базовой настройки и запуска создается случайный паттерн поведения для первой популяции и сохраняется во временный буфер. Во время запуска первой итерации включается таймер. Если за время итерации ни одна из особей достигает поставленной цели, таймер останавливается, а результаты сохраняются, паттерн поведения заменяется паттерном из буфера, а популяция увеличивается. После этого цикл начинается заново. Данная логическая схема работы программы показана на рис. 3.

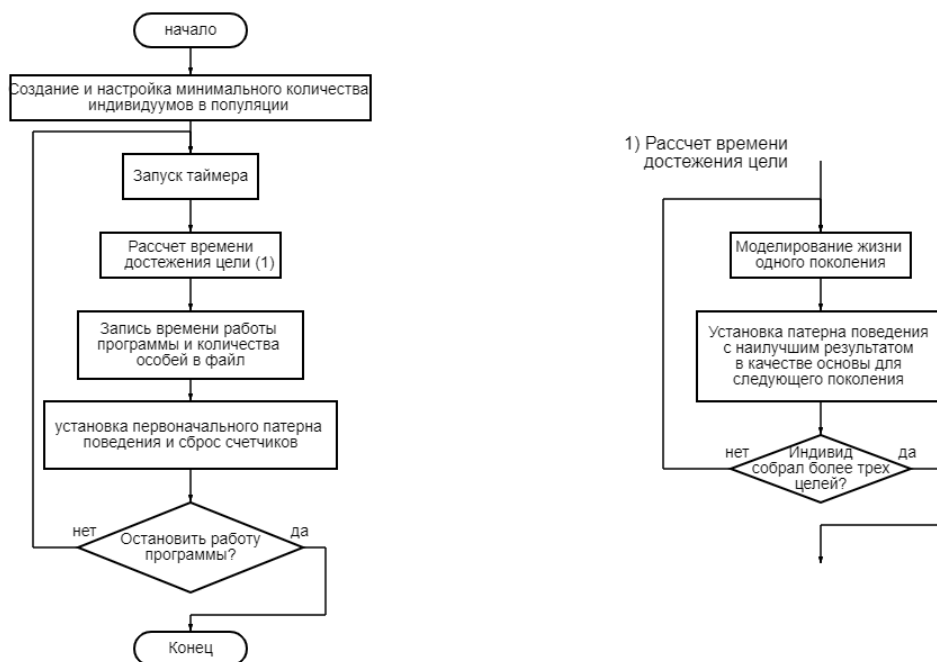


Рис. 3. Алгоритм работы программы

Примеры применения имитационной модели для определения размера популяции. Расширенная версия имитационной модели применена для исследования зависимости скорости работы программы от размера популяции. Эксперимент по определению зависимости скорости работы программы от размера популяции включал задание минимального количества особей в популяции, мониторинг нынешнего числа особей в популяции и времени выполнения поставленной задачи. Таким образом, в первой итерации создается десять особей, после выполнения поставленной цели и записи результатов, количество особей в следующий итерации увеличивается на десять. Данный цикл идет до тех пор, пока размер популяции не достигнет 300 особей или пользователь сам не остановит работу программы. В ходе работы были определены следующие параметры для

популяции в 100 особей: $\mu_{\max}=0,4092$; $k_s=0,046$ и $Y_{SX}=2,8979$. Данные значения лежат в допустимых пределах, представленные в работе [18]. Из этого можно сделать вывод, что полученные данные адекватны и их можно использовать в дальнейшем анализе.

На рис. 4 представлены графики скорости сходимости от количества индивидуумов, полученные экспериментальным путем и рассчитанные по размеру хромосомы [11], при древовидном их представлении [12], при учете фактора зашумленности [15], максимального и минимального соседнего элемента [16].

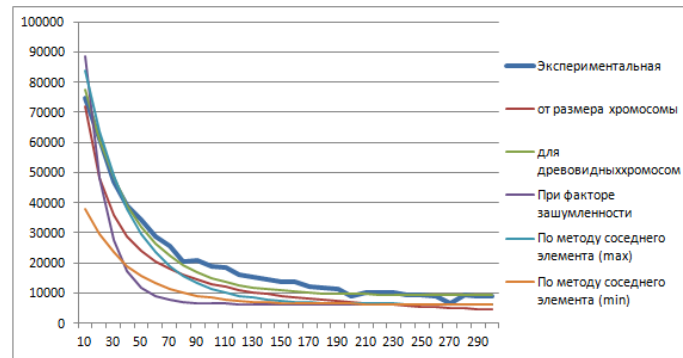


Рис. 4. Зависимости скорости сходимости от количества индивидуумов по размеру хромосомы, рассчитанные по теоретическим методам и полученные экспериментально

Результаты эксперимента показали, что размер популяции должен находиться в диапазоне 100–160 особей. Разность между соседними показателями данной области составила 0,13–0,8%. При увеличении популяции время выполнения задачи сокращается незначительно – в общей сложности не более 9,3% (Разность соседних значений не превышает 0,5%); при уменьшении – время работы критично возрастает от 2,4%. Полученные экспериментальные данные имеют наименьшую погрешность с методом [12], использующим древовидное представление хромосом.

Результаты проведенного исследования могут быть полезны при определении оптимального размера популяции для достижения наилучшего соотношения между затрачиваемой вычислительной мощностью и скоростью обучения алгоритма.

Заключение. В работе представлена имитационная модель целенаправленного поведения объектов в виртуальной среде на основе генетического алгоритма, реализованная в среде Unity. Описано применение модели для нахождения зависимости скорости работы генетических алгоритмов для обучения НС от размера популяции. Исследованы теоретические способы определения размера популяции в генетическом алгоритме разными теоретическими методами и зависимости между количеством особей и скоростью работы алгоритма.

В рамках дальнейшей работы предполагается дальнейшая модификация модели для её использования при тестировании зависимости нескольких параметров одновременно с целью определения их корреляции и нахождения оптимальных значений.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Солодовников В.И. Использование генетических алгоритмов в задачах анализа данных и построения систем правил // Новые информационные технологии в автоматизированных системах. – 2013. – № 16. – С. 72–77.
2. Шукин М.А. Генетические алгоритмы как метод решения математических задач // Вестник УРАО. – 2014. – № 5. – С. 168–172.
3. Корнеев А.С., Ляхов М.С., Тарнецкая А.В. Использование генетических алгоритмов для решения задач оптимизации в электроэнергетике // IX Всероссийская научно-практическая конференция молодых ученых «РОССИЯ МОЛОДАЯ». Апрель 2017. – 4 с. – Режим доступа: <https://science.kuzstu.ru/wp-content/Events/Conference/RM/2017/RM17/pages/Articles/0201038>.

4. Щеглов С.Н. Анализ моделей принятия решений в новых информационных технологиях в условиях нечеткости и неопределенности // Известия ЮФУ. Технические науки. – 2012. – № 132 (7). – С. 126-131.
5. Курейчик В.В., Курейчик Вл.Вл., Саак А.Э. Эволюционный алгоритм для решения задачи диспетчеризации // Известия ЮФУ. Технические науки. – 2021. – № 2 (219). – С. 50-59.
6. Janne Koljonen, Jarmo Alander. Effects of population size and relative elitism on optimization speed and reliability of genetic algorithms. – January 2006. – P. 1-7.
7. Yu-an Zhang, Makoto Sakamoto, Hiroshi Furutani. Effects of Population Size and Mutation Rate on Results of Genetic Algorithm. – January 2008. – P. 47-55.
8. Цой Ю.Р. Влияние размера популяции и поиска от ограничения по времени работы генетического алгоритма. – Томск: Томский политехнический университет, 2003. – 7 с.
9. Гончарова А.С., Бекетова О.С., Заросило Л.Р. Модели генетических алгоритмов // Молодой ученый. – Февраль 2015. – № 1 (1). – С. 32-33.
10. Цой Ю.Р. Решение задач линейного программирования с помощью генетического алгоритма. – Томск: Томский политехнический университет, 2003. – 2 с.
11. Чутига А.Ф., Петров Ю.Ю. Оценка выбора размера популяции в простом генетическом алгоритме // Информационное противодействие угрозам. – 2005. – № 5. – С. 26-29.
12. Глебов А.В., Стрикелев Д.А. Влияние размера популяции на скорость сходимости генетического алгоритма при древовидном представлении хромосом // Электронная библиотека БГУ. – Апрель 2010. – С. 3. – Режим доступа: <https://elibr.bsu.by/handle/123456789/28657>.
13. Glebov A., Strykelev D. Experimental convergence study of a genetic algorithm using consistency-preserving genetic operators for tree-like chromosomes // Modern problems of mathematics and computer engineering. – 2009. – P. 3-5.
14. Randy Haupt. Optimum Population Size and Mutation Rate for a Simple Real Genetic Algorithm that Optimizes Array Factors // Antennas and Propagation Society International Symposium. – 2000. – P. 173-186.
15. Harik G.R., Cantu-Paz E., Goldberg D.E., Miller B.L. The Gambler's Ruin Problem, Genetic Algorithms, and the Sizing of Populations // Association for Computing Machinery. – February 1999. – P. 231-253.
16. Фролов В.В. Определение размера популяции генетического алгоритма для задач дискретной оптимизации в САПР // Системный анализ и прикладная информатика. – 2018. – № 3. – С. 9-16.
17. Сапрыкин А.Н., Акинина К.Д., Сапрыкина Е.Н. Оптимальное число конвергируемых поколений и полезных особей при варьирующихся значениях вероятности мутации генетического алгоритма на малых пространствах поиска // Современные технологии в науке и образовании: Сб. трудов II международной научно-технической и научно-методической конференции. Т. 4. – Рязань: РПТИ, 2017. – С. 248-252.
18. Roeva O., Fidanova S., Paprzycki M. Influence of the population size on the genetic algorithm performance in case of cultivation process modeling // Computer Science and Information Systems. – 2013. – P. 371-376.
19. Частикова В.А. Идентификация механизмов реализации операторов генетического алгоритма в экспертных системах продукционного типа // Научный журнал КубГАУ. – 2012. – № 75.
20. Корнилов А. UNITY. Полное руководство. – 2-е изд. – СПб.: Наука и Техника, 2021. – 496 с.
21. Цыганков В.А., Шабалина О.А., Катаев А.В. Использование генетических алгоритмов для повышения скорости обучения нейронных сетей // Инженерный вестник Дона. – 2023. – № 3.

REFERENCES

1. Solodovnikov V.I. Ispol'zovanie geneticheskikh algoritmov v zadachakh analiza dannykh i postroeniya sistem pravil [The use of genetic algorithms in data analysis tasks and the construction of rule systems], *Novye informatsionnye tekhnologii v avtomatizirovannykh sistemakh* [New information technologies in automated systems], 2013, No. 16, pp. 72-77.
2. Shchukin M.A. Geneticheskie algoritmy kak metod resheniya matematicheskikh zadach [Genetic algorithms as a method of solving mathematical problems], *Vestnik URAO* [Bulletin of the University of the Russian Academy of Education], 2014, No. 5, pp. 168-172.
3. Korneev A.S., Lyakhov M.S., Tarnetskaya A.V. Ispol'zovanie geneticheskikh algoritmov dlya resheniya zadach optimizatsii v elektroenergetike [The use of genetic algorithms for solving optimization problems in the electric power industry], *IX Vserossiyskaya nauchno-prakticheskaya konferentsiya molodykh uchenykh «ROSSIYA MOLODAYA». April' 2017* [IX All-Russian Scientific and Practical Conference of Young Scientists "YOUNG RUSSIA". April 2017], 4 p. Available at: <https://science.kuzstu.ru/wp-content/Events/Conference/RM/2017/RM17/pages/Articles/0201038>.

4. *Shcheglov S.N.* Analiz modeley prinyatiya resheniy v novykh informatsionnykh tekhnologiyakh v usloviyakh nechetkosti i neopredelennosti [Analysis of decision-making models in new information technologies in conditions of fuzziness and uncertainty], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2012, No. 132 (7), pp. 126-131.
5. *Kureychik V.V., Kureychik V.I., Saak A.E.* Evolyutsionnyy algoritm dlya resheniya zadachi dispetcherizatsii [An evolutionary algorithm for solving the dispatching problem. Iyul], *Izvestiya YuFU. Tekhnicheskie nauki* [Izvestiya SFedU. Engineering Sciences], 2021, No. 2 (219), pp. 50-59.
6. *Janne Koljonen, Jarmo Alander.* Effects of population size and relative elitism on optimization speed and reliability of genetic algorithms. January 2006, pp. 1-7.
7. *Yu-an Zhang, Makoto Sakamoto, Hiroshi Furutani.* Effects of Population Size and Mutation Rate on Results of Genetic Algorithm, January 2008, pp. 47-55.
8. *Tsoy Yu.R.* Vliyaniye razmera populyatsii i poiska ot ogranicheniya po vremeni raboty geneticheskogo algoritma [The influence of population size and search time limit on genetic algorithm]. Tomsk: Tomskiy politekhnicheskii universitet, 2003, 7 p.
9. *Goncharova A.S., Beketova O.S., Zarosilo L.R.* Modeli geneticheskikh algoritmov [Models of genetic algorithms], *Molodoy uchenyy* [Young scientist], Fevral' 2015, No. 1 (1), pp. 32-33.
10. *Tsoy Yu.R.* Reshenie zadach lineynogo programmirovaniya s pomoshch'yu geneticheskogo algoritma [Solving linear programming problems using a genetic algorithm]. Tomsk: Tomskiy politekhnicheskii universitet, 2003, 2 p.
11. *Chipiga A.F., Petrov Yu.Yu.* Otsenka vybora razmera populyatsii v prostom geneticheskom algoritme [Estimating the choice of population size in a simple genetic algorithm], *Informatsionnoe protivodeystvie ugrozam* [Information counteraction to threats], 2005, No. 5, pp. 26-29.
12. *Glebov A.V., Strikelev D.A.* Vliyaniye razmera populyatsii na skorost' skhodimosti geneticheskogo algoritma pri drevovidnom predstavlenii khromosom [The influence of population size on the convergence rate of a genetic algorithm with a tree-like representation of chromosomes], *Elektronnaya biblioteka BGU* [Electronic Library of the BSU]. April' 2010, pp. 3. Available at: <https://elib.bsu.by/handle/123456789/28657>.
13. *Glebov A., Strykelev D.* Experimental convergence study of a genetic algorithm using consistency-preserving genetic operators for tree-like chromosomes, *Modern problems of mathematics and computer engineering*, 2009, pp. 3-5.
14. *Randy Haupt.* Optimum Population Size and Mutation Rate for a Simple Real Genetic Algorithm that Optimizes Array Factors, *Antennas and Propagation Society International Symposium*, 2000, pp. 173-186.
15. *Harik G.R., Cantu-Paz E., Goldberg D.E., Miller B.L.* The Gambler's Ruin Problem, Genetic Algorithms, and the Sizing of Populations, *Association for Computing Machinery*, February 1999, pp. 231-253.
16. *Frolov V.V.* Opredeleniye razmera populyatsii geneticheskogo algoritma dlya zadach diskretnoy optimizatsii v SAPR [Determining the population size of a genetic algorithm for discrete optimization problems in CAD], *Sistemnyy analiz i prikladnaya informatika* [System analysis and applied informatics], 2018, No. 3, pp. 9-16.
17. *Saprykin A.N., Akinina K.D., Saprykina E.N.* Optimal'noe chislo konvergiruyemykh pokoleniy i poleznykh osobey pri var'iruyushchikhsya znacheniyakh veroyatnosti mutatsii geneticheskogo algoritma na mal'kh prostranstvakh poiska [The optimal number of convergent generations and useful individuals with varying values of the mutation probability of a genetic algorithm in small search spaces] *Sovremennye tekhnologii v nauke i obrazovanii: Sb. trudov II mezhdunarodnoy nauchno-tekhnicheskoy i nauchno-metodicheskoy konferentsii* [Modern technologies in science and education: Collection of proceedings of the II international scientific-technical and scientific-methodological conference]. Vol. 4. Ryazan': RRTI, 2017, pp. 248-252.
18. *Roewa O., Fidanova S., Paprzycki M.* Influence of the population size on the genetic algorithm performance in case of cultivation process modeling, *Computer Science and Information Systems*, 2013, pp. 371-376.
19. *Chastikova V.A.* Identifikatsiya mekhanizmov realizatsii operatorov geneticheskogo algoritma v ekspertnykh sistemakh produktsionnogo tipa [Identification of mechanisms for implementing genetic algorithm operators in production-type expert systems], *Nauchnyy zhurnal KubGAU* [Scientific journal of KubSAU], 2012, No. 75.
20. *Kornilov A.* UNITY. Polnoe rukovodstvo [UNITY. Complete guide]. 2nd ed. Saint Petersburg: Nauka i Tekhnika, 2021, 496 p.
21. *Tsygankov V.A., Shabalina O.A., Kataev A.V.* Ispol'zovaniye geneticheskikh algoritmov dlya povysheniya skorosti obucheniya neyronnykh setey [Using genetic algorithms to increase the speed of learning of neural networks], *Inzhenernyy vestnik Dona* [Engineering Bulletin of the Don], 2023, No. 3.

Статью рекомендовал к опубликованию д.т.н., профессор Ю.А. Кравченко.

Цыганков Владимир Андреевич – Волгоградский государственный технический университет; e-mail: Vladimir.Tsygankov27@yandex.ru; г. Волгоград, Россия; тел.: 89176476959; магистр.

Шабалина Ольга Аркадьевна – e-mail: O.A.Shabalina@gmail.com; тел.: 89197958943; к.т.н.; доцент.

Катаев Александр Вадимович – e-mail: alexander.kataev@gmail.com; к.т.н.; доцент.

Tsygankov Vladimir Andreevich – Volgograd State technical University; e-mail: Vladimir.Tsygankov27@yandex.ru; Volgograd, Russia; phone: +79176476959; master.

Shabalina Olga Arkadevna – e-mail: O.A.Shabalina@gmail.com; phone: +79197958943; cand. of eng. sc.; associate professor.

Kataev Alexander Vadimovich – e-mail: alexander.kataev@gmail.com; cand. of eng. sc.; associate professor.

УДК 621.396.624

DOI 10.18522/2311-3103-2024-3-176-186

А.П. Плёткин

НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К СИСТЕМЕ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Рассматриваются вопросы современного состояния исследований и тенденции в области защиты передаваемых данных передовыми криптографическими методами. Приведено описание процесса шифрования и дешифрования информации при помощи абсолютно стойкого метода одноразового блокнота – шифра Вернама. В статье представлены типичные примеры задач, реализованные в области квантовой криптографии. Последнее включает в себя такие элементы, как неопределенность исходов, запутанность на квантовом уровне и принцип неопределенности Гейзенберга. Обсуждается подход к шифрованию данных с использованием симметричных алгоритмов и выдвигаются критерии для ключей шифрования, которые гарантируют полностью конфиденциальную передачу информации. Приводится краткий обзор истории развития квантовых коммуникационных систем и криптографии, подчеркивается важность дальнейших исследований в этой сфере. Отмечается, что в криптографии ключевым аспектом безопасности является распределение ключей шифрования среди авторизованных пользователей. Квантовая криптография предлагает решение для создания и распределения ключей с помощью методов, основанных на принципах квантовой механики, которые применяются в системах квантового распределения ключей. Современные реализации систем КРК всесторонне исследуются, в том числе на предмет различного рода атак, но подавляющее большинство исследований сосредоточено на поиске уязвимостей в работе квантовых протоколов, например, через техническое несовершенство компонентов систем КРК. В работе рассматривается способ осуществления несанкционированного доступа к системе КРК в процессе калибровки аппаратуры детектирования. Исследован способ получения несанкционированного доступа к работе системы квантового распределения ключей в режиме калибровки и предложен метод противодействия. Приведены результаты натурных исследований, которые показывают, что системы квантового распределения ключей имеют уязвимости не только при работе квантового протокола, но и в других жизненно важных стадиях функционирования системы. Описанный тип атаки позволяет несанкционированно получить данные о квантовом канале связи и осуществлять управляемую помеху процессу работы системы. Предложен способ построения автокомпенсационных систем оптической связи, обеспечивающий защищенность процесса калибровки от несанкционированного доступа. Показано влияние ослабленных до фотонного уровня синхроимпульсов на вероятность верного обнаружения отрезка времени с оптическим сигналом. В статье описаны результаты экспериментов, демонстрирующие различия между теоретическими данными и фактическими характеристиками отдельных элементов системы квантовой связи.

Синхроимпульсы; распределение ключей; квантовые коммуникации; алгоритм поиска; контрмеры; атаки на квантовый канал.