**Инженерный вестник Дона**, №4 (2017)
ivdon.ru/ru/magazine/archive/n4y2017/4518

# Применение комбинированных биоинспирированных стратегий (генетический алгоритм и алгоритм пчелиных колоний) для реализации криптоанализа классических шифров перестановок

*Ю.О. Чернышев, А.С. Сергеев*

*Донской государственный технический университет, Ростов-на-Дону*

**Аннотация:** Рассматривается задача криптоанализа с использованием новой модели оптимизационных стратегий – комбинированного биоинспирированного алгоритма**.** Описано применение комбинированного биоинспирированного алгоритма (генетический алгоритм и алгоритм муравьиных колоний) для реализации криптоанализа шифров перестановок. Приводится описание комбинированного алгоритма, отмечены его отличительные особенности, описан демонстрационный пример реализации криптоанализа строки шифртекста данным алгоритмом. Применительно к данному алгоритму показано также, что вероятность получения оптимального варианта решения при реализации комбинированных алгоритмов криптоанализа не может быть меньше вероятности получения оптимального решения при использовании классических биоинспирированных алгоритмов.

**Ключевые слова:** криптоанализ, биоинспирированный алгоритм, генетический алгоритм, алгоритм пчелиных колоний, кроссинговер, мутация, шифр перестановок.

## Введение

В настоящее время научное направление «природные вычисления», объединяющее математические методы, в которых заложен принцип природных механизмов принятия решений, получает все более широкое распространение для решения различного круга оптимизационных задач, в том числе задач криптоанализа. В данных методах и моделях основным определяющим элементом является построение начальной модели и правил, по которым она может изменяться (эволюционировать). В [1] авторами рассматривались методы решения задачи криптоанализа, относящейся к переборным задачам с экспоненциальной временной сложностью, на традиционные симметричные криптосистемы, использующие шифры перестановки и замены, а также на шифры гаммирования с использованием генетических алгоритмов, в [2] - на симметричные и ассиметричные криптосистемы с использованием биоинспирированных методов (алгоритмов муравьиных и пчелиных

колоний). В [3] исследована возможность применения методов генетического поиска для реализации криптоанализа блочных криптосистем. Поскольку данные задачи в большинстве своем являются NP-полными (имеют комбинаторную сложность), то, как отмечено в [4], основным мотивом для разработок новых алгоритмов решения комбинаторных задач являются возникшие потребности в решении задач большой и очень большой размерности. Отметим также, что разработке новых моделей биоинспирированных методов глобальной оптимизации посвящена работа [5], где рассмотрены новые биоинспирированные технологии, имитирующие поведение лягушек, кукушек, светлячков, и распространения сорняков. Основная отличительная особенность всех четырех методов состоит в возможности поиска глобального экстремума многоэкстремальных целевых функций с большим числом переменных. В этом плане можно отметить также новые подходы, связанные с применением биоинспирированных алгоритмов (алгоритмы пчелиных колоний) для криптоанализа блочных методов шифрования [18], а также подход, связанный с применением биоинспирированных методов для решения проблемы моделирования процессов распределения потока ресурсов [27].

Тем не менее, как отмечено в [6], разработанные структуры генетических алгоритмов фактически являются “слепыми” поисковыми структурами с присущими им недостатками: генерация решений с нарушениями, что требует дополнительного контроля; генерация большого количества подобных решений; генерация большого количества “плохих” решений; попаданию в локальный оптимум. Поэтому представляет интерес применение эвристических методов, инспирированных природными системами, в которых осуществляется поэтапное построение решения задачи путем добавления нового оптимального частичного решения к уже построенному частичному оптимальному решению. В этом плане можно

отметить работы [2,3,7,8], в которых рассматривалось применение алгоритмов муравьиных и пчелиных колоний для криптоанализа классических симметричных, асимметричных и блочных криптосистем. В данной работе мы рассмотрим возможность разработки и применения комбинированного биоинспирированного метода (комбинирование генетического метода и алгоритма пчелиных колоний) для криптоанализа классических шифров перестановок. Отметим также, что в [9,10] приводится обзор авторских работ, посвященных решению задачи криптоанализа классических криптографических методов, а также исследованию возможности применения «алгоритма муравья» и алгоритма «колонии пчел» для реализации криптоанализа перестановочных шифров, а также асимметричных алгоритмов шифрования на основе решения теоретико-числовых задач криптографии. В [11] приводится обзор авторских работ, посвященных решению задачи криптоанализа блочных криптографических методов на основе новых моделей искусственного интеллекта – генетических алгоритмов, методов муравьиных и пчелиных колоний.

## Постановка задачи. Генетические алгоритмы и алгоритмы пчелиных колоний.

Следует заметить, что в качестве первичного признака, по которому производится классификация шифров, используется тип преобразования, осуществляемого с открытым текстом при шифровании. Если буквы открытого текста при шифровании только меняются местами друг с другом, то данный шифр относится к классу *шифров перестановок* [1,2,7], основные виды которых описаны, например, в [12,13]. В результате применения данных шифров полученная криптограмма включает только те символы, которые составляют открытый текст, то есть задача определения открытого текста заключается в определении позиций для назначения символов

криптограммы таким образом, при котором целевая функция, определяющая оптимальность исходного текста, достигает экстремума. Данную задачу криптоанализа, таким образом, можно представить как задачу о назначениях, цель которой – определить оптимальные варианты размещения символов в позиции.

Отметим, что описание возможного применения алгоритма муравьиных колоний для задач криптоанализа (на основе сведения ее к квадратичной задаче о назначениях, описанной в [14]) приведено в [2,7]. Описание применения генетического алгоритма для реализации криптоанализа классических шифров перестановок наряду с экспериментальными результатами приведено в [1]. В соответствии с [1,3] можно выделить следующие этапы простого генетического алгоритма, впервые описанного Гольдбергом на основе работ Холланда [15,16].

1. Инициализировать и оценить популяцию.
2. Повторять пункты 2.1–2.5, пока не выполнится условие останова.

2.1. *Отбор (селекция).* Отобрать часть популяции для воспроизводства.

2.2. *Скрещивание.* Выполнить скрещивание «генов» отобранных родителей.

2.3. *Мутация.* Случайным образом осуществить мутацию полученной популяции.

2.4. *Оценивание.* Оценить пригодность популяции (функция *fitness*).

2.5. На основе полученных значений функции *fitness* выбрать выживших индивидов.

Отметим, что основные модели, отличительные черты генетических алгоритмов, а также способы реализации их основных этапов описаны, например, в [1,3,17]. Тем не менее, несмотря на имеющую место за последние годы широкую область применимости эволюционных методов, они обладают рядом недостатков, отмеченных выше (наличие «слепого»

поиска, приводящего к попаданию в локальный оптимум). Одной из последних разработок в области искусственного интеллекта является алгоритм пчел, который в последнее время используется для нахождения экстремумов сложных многомерных функций [8]. Отметим, что обзор некоторых публикаций, посвященных применению алгоритмов пчелиных колоний для решения комбинаторных теоретико-графовых задач (задача разбиения графа, раскраска графа, сравнение с другими «биоинспирированными» методами), решению задачи размещения, задачи разложения составных чисел на простые сомножители, используемой при криптоанализе асимметричных алгоритмов, приводится в [8].

Как и ранее в [2,7,8], для решения задачи криптоанализа определим целевую функцию вида

$$R = \sum_{i=1}^{n} \sum_{j=1}^{n} Q_i C_{ij} X_{ij} \longrightarrow \max$$

где $X_{ij}$=1, если символ i назначен в позицию $j$, и $X_{ij}=0$ в противном случае, $C_{ij}$ — вероятность того, что за символом в позиции i должен следовать символ в позиции $i+1$. Кроме этого, вводится параметр $Q_i$, показывающий, насколько фрагмент текста из $i$ символов носит осмысленный характер, то есть совпадает со словарным запасом языка.

Как отмечено в [8], при реализации алгоритма пчелиных колоний каждое решение представляет собой позицию в пространстве поиска, содержащую определенное количество нектара. При этом данное количество нектара определяет значение целевой функции в этой точке. Решение задачи криптоанализа представляет собой последовательность символов алфавита $x_1, x_2, ..., x_k$, пройденных при перемещении агента–пчелы в пространстве поиска. Целью поиска является определение оптимальной комбинации (последовательности прохождения) символов с максимальным значением

целевой функции $R$, которая определяется комбинациями символов, пройденных агентами–пчелами.

**Комбинированный алгоритм пчелиных колоний.**

Далее при описании алгоритма будем использовать методику и терминологию, используемую в [4,8,18]. Как отмечено в [8,18], итерационный процесс поиска решений при реализации алгоритма криптоанализа заключается в последовательном перемещении агентов–пчел в новые позиции в пространстве поиска и формировании соответствующих вариантов текста с последующей проверкой их оптимальности, а также выборе соответствующего оптимального (или квазиоптимального) варианта ключа.

В соответствии с [4,8,19] алгоритм колонии пчел включает следующие основные операции.

1. Формирование пространства поиска и создание популяции пчел.
2. Оценка целевой функции (ЦФ) пчел в популяции путем определения ЦФ, определяющей оптимальность исходного текста.
3. Формирование перспективных участков для поиска в их окрестности.
4. Отправка пчел-разведчиков и поиск агентами-разведчиками перспективных позиций для поиска в их окрестности.
5. Выбор пчел с лучшими значениями ЦФ с каждого участка.
6. Отправка рабочих пчел (пчел-фуражиров) для случайного поиска и оценка их ЦФ.
7. Формирование новой популяции пчел.
8. Проверка условия остановки алгоритма. Если они выполняются, переход к 9, иначе к 2.
9. Конец работы алгоритма.

Структурная схема алгоритма колонии пчел приведена в [19]. В соответствии с [19] в лучшем случае временная сложность пчелиных алгоритмов $T$ составляет $O \approx \Omega (n^{\lg n})$, в худшем случае $O \approx \Omega (n^3)$.

Отметим, что пример реализации алгоритма пчелиных колоний для криптоанализа шифров перестановок (на основе модели, описанной в [14]) приведен в [2,8], для криптоанализа блочных криптосистем на основе определения секретного ключа – в [18]. В связи с этим возникает актуальный вопрос о возможности применения комбинированных биоинспирированных методов для реализации криптоанализа, в том числе, о возможности разработки методов, сочетающих основные черты генетических и пчелиных алгоритмов. Очевидно, что при реализации криптоанализа текстов значительной длины применение генетических операций, производимых над полученными частичными решениями, может существенно сократить временные затраты, а также повысить разнообразие генетического материала популяции, ускоряя процесс сходимости к глобальному оптимуму.

Как отмечено в [26], в гибридных алгоритмах, объединяющих различные либо однотипные алгоритмы, но с различными значениями параметров, преимущества одного алгоритма могут компенсировать недостатки другого. Поэтому одним из основных путей повышения эффективности решения задач глобального поиска в настоящее время является разработка гибридных популяционных алгоритмов. Отметим, что в настоящее время существует значительное число способов гибридизации оптимизационных алгоритмов, некоторые разновидности классификаций данных алгоритмов приведены в [26] (одноуровневая классификация Ванга, двухуровневая классификация Эль-Абда и Камэла, четырехуровневая классификация Рейдла).

В соответствии с классификацией Ванга выделяют три категории гибридных алгоритмов, рассмотренных в [26]: вложенные алгоритмы, алгоритмы типа препроцессор/постпроцессор, коалгоритмы.

В категории методов *гибридизации вложением* выделяют высокоуровневую и низкоуровневую гибридизации.

*Высокоуровневая гибридизация* вложением предполагает слабую связь объединяемых алгоритмов, обычно при этом данные алгоритмы сохраняют значительную независимость.

При *низкоуровневой гибридизации* комбинируемые алгоритмы интегрированы достаточно сильно, так что при низкоуровневой гибридизации алгоритмов, по сути, формируется новый алгоритм.

Отметим, что в [26] приведена общая схема последовательной высокоуровневой гибридизации вложением, которая представлена в следующем виде.

1. Инициализация агентов $s_i$ популяционного алгоритма.

2. Выполнение заданного числа итераций популяционного алгоритма.

3. При полученных координатах агентов $s_i$ выполнение локального поиска с помощью второго вложенного комбинируемого алгоритма. Координаты лучших найденных точек $x_i$ полагаются равными текущим координатам агентов $s_i$.

4. Проверка выполнения условия окончания выполнения итераций. Если это условие выполнено, завершение вычислений, в противном случае переход к 2.

В качестве примера высокоуровневой гибридизации приведем комбинированный алгоритм криптоанализа шифров перестановок, где в качестве популяционного алгоритма используется алгоритм пчелиных колоний, а в качестве алгоритма локального поиска – генетический алгоритм.

Таким образом, используя терминологию и обозначения, введенные в [4,8,18,], комбинированный алгоритм криптоанализа сформулируем в следующей форме. Как и ранее, будем предполагать, что пространство поиска, в котором размещены символы алфавита шифртекста, представляет собой прямоугольную матрицу $A$ заданного размера $m_1 \times m_2$.

1. Определить начальные параметры алгоритма: количество пчел–агентов $N$; размер популяции пчел $M$; количество итераций $L$; количество агентов–разведчиков $n_r$; количество агентов–фуражиров $n_f$; значение максимального размера окрестности $\lambda_{макс}$; количество базовых позиций $n_b$; $n_{b1}$ — количество базовых позиций, формируемых из лучших позиций $a^*$, найденных на $l$-$1$ итерации; $n_{rl}$ — количество агентов–разведчиков, выбирающих случайным образом новые позиции на итерациях 2,3,..,L; $n_{b2}$ — количество базовых позиций, формируемых из $n_{rl}$ новых лучших позиций, найденных агентами–разведчиками на $l$ итерации.

2. Задать номер итерации $l$=1.

3. Разместить $n_r$ агентов–разведчиков случайным образом в пространстве поиска, то есть выбрать произвольным образом $n_r$ символов в матрице $A$. Определить значение ЦФ $R$ равным малому положительному числу.

4. Сформировать множество $n_b$ базовых решений и соответствующее множество базовых позиций $A_b=\{a_{bi}\}$ с лучшими значениями ЦФ $R$.

5. $f$=1 (задание номера агента–фуражира).

6. Выбор базовой позиции $a_i \in A_b$.

7. Выбор позиции $a_s(l)$, расположенной в окрестности базовой позиции $a_i$, не совпадающей с ранее выбранными на данной итерации позициями, и соответствующего решения (списка $E_s$).

8. Для всех вновь включенных позиций рассчитать и поставить им в соответствие списки (частичные решения) $E_s$ и соответствующие значения ЦФ $R$.

9. $f=f+1$, если $f>n_f$, переход к п. 10, иначе к п. 6.

10. Провести операцию кроссинговера (скрещивания) полученных индивидуумов (частичных решений в виде списков $E_s$, содержащих более двух символов) на основе заданной нормы, получение заданного количества потомков (формирование расширенной популяции).

11. Провести операцию мутации индивидуумов популяции на основе заданной нормы мутации, получение заданного количества мутированных потомков.

12. Подсчитать целевые функции $R$ вновь полученных индивидуумов и умножить на весовой коэффициент $Q$.

13. Провести селекцию индивидуумов расширенной популяции родителей и потомков для сокращения популяции до размера $M$.

14. Среди всех значений $R_i$ выбрать лучшее значение $R^*$ и соответствующее решение (список $E^*$).

15. Если значение $R^*(l)$ предпочтительней значения $R^*(l-1)$, то сохранить значение $R^*(l)$, в противном случае сохраненным остается значение $R^*(l-1)$.

16. Если $l<L$ (не все итерации пройдены), $l=l+1$(переход к следующей итерации), переход к п. 17, иначе к п. 21.

17. Начать формирование множества базовых позиций для следующей итерации. Во множество $A_{bl}$ включается $n_{bl}$ лучших позиций, найденных агентами на итерации $l-1$.

18. Разместить $n_{rl}$ агентов–разведчиков случайным образом в пространстве поиска для выбора $n_{rl}$ позиций в пространстве поиска, осуществить выбор этих позиций.

19. Включить в множество $A_{b2}$ $n_{b2}$ позиций из множества $n_{rl}$ новых позиций, найденных агентами–разведчиками на итерации $l$. ($n_{b2}$+$n_{b1}$= $n_b$).

20. Определить множество базовых позиций на итерации $l$ как $A_b$= $A_{b1}$ $\cup A_{b2}$, перейти к п. 5.

21. Конец работы алгоритма, список $E^*$ — вариант исходного текста с лучшим значением ЦФ $R^*$.

Таким образом, в данном алгоритме операторы 1-9, 17-21 соответствуют операторам пчелиного алгоритма, обеспечивая формирование пространства решений и глобальный поиск, операторы 10-16 соответствуют операторам генетического алгоритма и обеспечивают локальный поиск в пространстве решений.

Таким образом, применение эволюционных операторов, обеспечивающих повышение разнообразия частичных решений для получения оптимального варианта текста, может оказаться целесообразным при значительном объеме текста и может увеличить скорость схождения к глобальному оптимуму. В этом плане также может оказаться целесообразным применение некоторых модифицированных генетических операторов, описанных, например, в [20,21] (*транслокация, сегрегация, рекомбинация*), применение моделей параллельных эволюционных стратегий, таких как *глобальный параллельный гибридный алгоритм, распределенный параллельный гибридный алгоритм (островная модель)* [1,3,22,23], а также некоторые специальные модели генетических алгоритмов (*hybrid algorithms, CHC, Genitor, клеточная модель*), описанных в [1,3,22],

## Демонстрационный пример

Как и ранее в [7,8], рассмотрим реализацию представленного алгоритма на демонстрационном примере. Пусть задана строка из 12 символов ДИАИОБСУРНЯЦ, требуется определить возможную перестановку

символов, входящую в словарный состав языка. Как и ранее в [7,8], составим матрицу $C_{ij,}$ показывающую вероятность того, что за символом i может следовать символ j. Матрица $C_{ij}$ составлена на основе данных, приведенных в [13,24], и показана в табл. 1. Значения, приведенные в [13], промасштабированы и округлены до десятых долей.

Таблица № 1

Вероятность появления биграмм в тексте

| | Д | И | А | О | Б | С | У | Р | Н | Я | Ц |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Д | 0.1 | 0.8 | 0.9 | 0.8 | 0.1 | 0.7 | 0.8 | 0.6 | 0.5 | 0.2 | 0.1 |
| И | 0.7 | 0.8 | 0.4 | 0.5 | 0.6 | 0.8 | 0.1 | 0.7 | 0.8 | 0.5 | 0.1 |
| А | 0.8 | 0.7 | 0.2 | 0.4 | 0.8 | 0.7 | 0.2 | 0.7 | 0.8 | 0.5 | 0.4 |
| О | 0.8 | 0.5 | 0.2 | 0.2 | 0.9 | 0.9 | 0.1 | 0.9 | 0.8 | 0.1 | 0.1 |
| Б | 0.1 | 0.6 | 0.7 | 0.8 | 0.1 | 0.1 | 0.5 | 0.5 | 0.2 | 0.1 | 0.1 |
| С | 0.3 | 0.7 | 0.8 | 0.9 | 0.1 | 0.1 | 0.6 | 0.4 | 0.7 | 0.1 | 0.1 |
| У | 0.3 | 0.1 | 0.1 | 0.1 | 0.4 | 0.3 | 0.1 | 0.7 | 0.5 | 0.1 | 0.1 |
| Р | 0.3 | 0.7 | 0.9 | 0.9 | 0.1 | 0.3 | 0.4 | 0.1 | 0.3 | 0.2 | 0.1 |
| Н | 0.2 | 0.8 | 0.9 | 0.9 | 0.1 | 0.2 | 0.4 | 0.1 | 0.2 | 0.3 | 0.1 |
| Я | 0.2 | 0.1 | 0.1 | 0.1 | 0.1 | 0.2 | 0.1 | 0.2 | 0.3 | 0.1 | 0.1 |
| Ц | 0.1 | 0.5 | 0.4 | 0.2 | 0.1 | 0.1 | 0.2 | 0.1 | 0.1 | 0.1 | 0.1 |

Пространство поиска, как и ранее в [8], определим в виде матрицы A размером 21x24 заполненной символами из алфавита шифртекста, размещенными случайным образом в ячейках с соответствующими координатами (табл. 2).

Будем предполагать, что весовой коэффициент $Q$ используется для списков длиной более 2 символов, используется также операция универсального кроссинговера по маске. Если скрещиваются хромосомы

разной длины, то случайным образом выбирается номер позиции начала скрещивания.

Таблица 2

Пространство поиска для комбинированного алгоритма

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 24 | И | Р | Б | Я | И | У | Н | И | С | Р | Ц | О | А | С | И | Р | Б | Я | Б | Р | ***У*** |
| 23 | Д | И | Н | Я | О | Р | Д | ***С*** | Я | И | Р | Н | Б | О | А | С | И | Р | Б | Я | И |
| 22 | Р | Д | С | Я | И | Р | Н | Б | У | С | А | И | Я | Б | Р | У | И | А | Ц | О | А |
| 21 | Б | Б | Д | И | Н | Я | Ц | А | С | У | С | А | И | Ц | И | ***Р*** | Б | Я | И | У | Н |
| 20 | О | А | С | И | Р | Б | Я | И | У | Н | И | С | Р | Я | И | Б | А | Р | С | У | Ц |
| 19 | Б | Я | И | У | Н | И | С | Р | А | И | Ц | С | У | Ц | Б | Р | Я | Д | С | У | Ц |
| 18 | Б | Р | У | И | А | Ц | ***О*** | А | С | И | Р | Б | Я | ***И*** | Д | Я | О | Р | И | Р | Н |
| 17 | С | А | И | Ц | И | Р | Б | Я | И | У | Н | Б | Я | И | У | Н | И | С | Р | Ц | О |
| 16 | Р | Д | С | Я | И | Р | Н | Б | У | С | А | И | Ц | С | У | Ц | Д | И | Ц | Я | Б |
| 15 | У | Б | Б | Д | И | Н | Я | О | Р | ***Д*** | С | Я | И | О | У | Р | Н | С | У | Б | Б |
| 14 | Р | Д | С | Я | И | Р | Н | Б | О | А | С | И | А | С | У | С | А | И | Ц | С | У |
| 13 | С | А | И | Я | Б | Р | У | И | А | Ц | О | С | И | Р | Б | Я | И | У | Н | И | О |
| 12 | Д | И | Н | Я | О | Р | Д | С | Я | И | Р | Н | ***Б*** | Д | С | Я | И | Р | Н | Б | У |
| 11 | А | Р | С | У | ***Ц*** | Д | Н | Я | Б | С | У | С | А | И | Ц | С | У | Ц | Б | Р | Я |
| 10 | А | Р | С | У | Ц | Д | Н | Я | Б | С | У | О | Д | Ц | Я | Б | Р | У | И | А | Ц |
| 9 | Д | И | Ц | Я | Б | Р | У | И | А | Ц | О | А | С | У | С | А | И | Ц | С | У | Ц |
| 8 | У | О | Д | А | С | Ц | О | У | ***Р*** | Н | С | У | Б | Б | Д | И | Н | Я | Ц | Ц | Я |
| 7 | О | Р | Н | С | У | Б | Б | Д | И | Н | Я | О | Р | Д | С | Я | И | Р | Н | Б | У |
| 6 | Б | Я | И | У | Н | Б | Я | И | У | Н | С | А | И | Ц | И | Р | Б | Я | И | У | Д |
| 5 | Д | С | Р | У | А | О | И | Ц | Н | Р | Д | Я | О | Р | И | Р | Н | Б | У | С | А |
| 4 | А | Д | И | Ц | Я | Б | Р | У | И | А | Ц | О | А | С | И | Р | Б | Я | И | У | Н |
| 3 | И | Ц | Б | О | Р | Д | С | Я | И | Р | Н | Б | У | С | А | И | Ц | С | У | Ц | Б |
| 2 | Н | У | Ц | Я | И | Б | А | Р | С | У | Ц | Д | Н | Я | Б | С | У | О | Д | А | С |
| 1 | Д | С | Р | У | А | О | И | Ц | Н | Р | Д | Я | О | Р | Н | ***С*** | У | Б | Б | Д | И |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |

*Итерация 1.*

1. В соответствии с этапами 1-3 алгоритма определим количество агентов–разведчиков $n_r$=10 и разместим их случайным образом в

пространстве поиска, то есть выберем произвольным образом $n_r$ символов в матрице $A$. Пусть это будут символы С(16,1), Р(9,8), Ц(5,11), Д(10,15), Б(13,12), И(14,18), О(7,18), Р(16,21), С(8,23), У(21,24), выделенные в табл. 2 жирным курсивом. Положим значение ЦФ $R$ для всех позиций равным малому положительному числу $R$=0.001. Определим размер популяции пчел $M$=10.

2. В соответствии с шагом 4 алгоритма определим множество базовых решений $n_b$=6 и соответствующие базовые позиции с лучшими значениями ЦФ (на этом этапе, как и в [8], их выберем произвольно). Пусть это будут позиции $A_b$={С(16,1), Ц(5,11), И(14,18), Д(10,15), Р(16,21), Б(13,12)}.

3. В соответствие с этапами 5-9 алгоритма определим количество агентов-фуражиров $n_f$=8, размер максимальной окрестности $\lambda_{макс}$=20. Пусть базовые позиции выбираются восемью агентами-фуражирами в следующем порядке $a_1$=Ц(5,11), $a_2$=И(14,18), $a_3$=С(16,1), $a_4$=И(14,18), $a_5$=С(16,1), $a_6$=Д(10,15), $a_7$=Б(13,12), $a_8$=Р(16,21). Пусть базовым позициям ставятся в соответствие следующие позиции $a_s$: Ц(5,11)→У(4,11); И(14,18)→И(12,16); С(16,1)→У(13,3); И(14,18)→С(14,16); С(16,1)→Я(16,7); Д(10,15)→И(10,12); Б(13,12)→Д(13,10); Р(16,21)→О(17,18).

Таким образом, в соответствии с шагом 8 будем иметь перечень позиций, списков и значений функции $R$, определенных в соответствии с табл. 1. Для позиций Ц(5,11), И(14,18), С(16,1), Д(10,15), Б(13,12), Р(16,21) $R$=0,001, списки $E_1$-$E_6$ состоят из одного символа, $R$=0.001. Для позиций: У(4,11) $E_7$={ЦУ}, $R$=0.2; И(12,16) $E_8$={ИИ}, $R$=0.8; У(13,3) $E_9$={СУ}, $R$=0.6; С(14,16) $E_{10}$={ИС}, $R$=0.8; Я(16,7) $E_{11}$={СЯ}, $R$=0.1; И(10,12) $E_{12}$={ДИ}, $R$=0.8; Д(13,10) $E_{13}$={БД}, $R$=0.1; О(17,18) $E_{14}$={РО}, $R$=0.9.

4. В соответствии с шагом 10 алгоритма проведем операцию универсального кроссинговера для списков $E_7$ -$E_{14}$, выбрав норму 75%. Пусть для получения 6 потомков $E_{15}$ –$E_{20}$ выбраны списки $E_7$-$E_{10}$, $E_{13}$-$E_{14}$, $E_{10}$-

$E_{11}$, и сформированы следующие маски: 10; 01; 01. В этом случае получим следующих потомков: $E_{15}$={ИУ}, $R$=0.1; $E_{16}$={ЦС}, $R$=0.1; $E_{17}$={БО}, $R$=0.8; $E_{18}$={РД}, $R$=0.3; $E_{19}$={ИЯ}, $R$=0.5; $E_{20}$={СС}, $R$=0.1.

5. В соответствии с шагом 11 алгоритма проведем операцию точечной мутации. Будем предполагать далее, что мутация проводится путем случайного выбора хромосом популяции, случайного выбора количества генов и произвольной замены значений выбранных генов на допустимые из произвольно выбранных позиций. Пусть после выбора хромосомы (списка) $E_{13}$ меняется значение гена Б на Р(16,21), после выбора хромосомы $E_{15}$ меняется значение У на Н(11,17), после выбора хромосомы $E_{16}$ меняется значение гена С на А(4,8). В этом случае потомки будут иметь вид: $E_{13}$={РД(13,10)}, $R$=0,3; $E_{15}$={ИН(11,17)}, $R$=0,8; $E_{16}$={ЦА(4,8)}, $R$=0,4.

Таким образом, на итерации 1 мы будем иметь следующий перечень списков (хромосом), координат и значений функции $R$:
{Ц(5,11)}, {И(14,18)}, {С(16,1)}, {Д(10,15)}, {Б(13,12)}, {Р(16,21)}, $R$=0.001; {ЦУ(4,11)}, $R$=0.2; {ЦА(4,8)}, $R$=0.4; {ИИ(12,16)}, $R$=0.8; {ИС(14,16)}, $R$=0.8; {ИН(11,17)}, $R$=0.8; {ИЯ(16,7)}, $R$=0.5; {СУ(13,3)}, $R$=0.6; {СЯ(16,7)}, $R$=0.1 {СС(14,16)}, $R$=0.1; {ДИ(10,12)}, $R$=0.8; {БО(17,18)}, $R$=0.8; {РО(17,18)}, $R$=0.9; РД(13,10)}, $R$=0.3; {РД(13,10)}, $R$=0,3.

6. Проводя в соответствии с шагом 13 элитную селекцию, удалим индивидуумы популяции с наименьшим значением $R$ до сокращения размера популяции до размера М=10. Это индивидуумы {Ц(5,11)}, {И(14,18)}, {С(16,1)}, {Д(10,15)}, {Б(13,12)}, {Р(16,21)}, {СС(14,16)}, {СЯ(16,7)}, {ЦУ(4,11)}, РД{(13,10)}.

7. Выбирая среди всех значений $R_i$ лучшее значение, получим, что $R^*$=0,9; $E^*$={РО}.

8. Полагаем $l$=2.

*Итерация 2.*

1. В соответствии с шагом 17 алгоритма определим число $n_{b1}$= 3; включим во множество $A_{b1}$ позиции $A_{b1}$={РО(17,18), R=0.9; ИН(11,17), R=0.8; ДИ(10,12), R=0.8}.

2. В соответствии с шагом 18 определим количество агентов-разведчиков $n_{rl}$=6 и разместим их произвольным образом в пространстве поиска. Пусть произвольным образом выбираются символы СУ(13,3), РД(13,10), Н(19,7), А(10,4), Ц(17,3), И(9,4).

3. В соответствии с шагом 19 включим во множество $A_{b2}$ $n_{b2}$=3 позиции из множества $n_{rl}$=6 позиций, найденных агентами–разведчиками на итерации 2. Пусть это будут позиции $A_{b2}$={СУ(13,3), R=0.6; РД(13,10), R=0.3; А(10,4), R=0.001}.

4. Таким образом, на итерации $l$=2 $n_{b1}$+ $n_{b2}$=6 и множество базовых позиций $A_b$={РО(17,18), ИН(11,17), ДИ(10,12), СУ(13,3), РД(13,10), А(10,4)}. Пространство поиска показано в табл. 3, базовые позиции отмечены прямым жирным шрифтом.

5. В соответствие с этапами 5-9 алгоритма определим количество агентов-фуражиров $n_f$=8, размер максимальной окрестности $\lambda_{макс}$=20. Пусть базовые позиции выбираются в следующем порядке:
$a_1$=РО(17,18), $a_2$=А(10,4), $a_3$=ИН(11,17), $a_4$=А(10,4), $a_5$=РД(13,10), $a_6$=РД(13,10), $a_7$=СУ(13,3), $a_8$=ДИ(10,12).

Пусть базовым позициям ставятся в соответствие следующие позиции $a_s$: РО(17,18)→Ц(19,16); А(10,4)→Ц(8,5); ИН(11,17)→ИИ(12,16); А(10,4)→Ц(4,4); РД(13,10)→ИЯ(16,7); РД(13,10)→ИИ(12,16); СУ(13,3)→БО(17,18); ДИ(10,12)→ЦА(4,8).

Таким образом, на данном шаге мы будем иметь следующий список позиций, решений и соответствующих значений функции $R$.

Таблица 3

Пространство поиска для комбинированного алгоритма после 1 итерации

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 24 | И | Р | Б | Я | И | У | Н | И | С | Р | Ц | О | А | С | И | Р | Б | Я | Б | Р | У |
| 23 | Д | И | Н | Я | О | Р | Д | С | Я | И | Р | Н | Б | О | А | С | И | Р | Б | Я | И |
| 22 | Р | Д | С | Я | И | Р | Н | Б | У | С | А | И | Я | Б | Р | У | И | А | Ц | О | А |
| 21 | Б | Б | Д | И | Н | Я | Ц | А | С | У | С | А | И | Ц | И | Р | Б | Я | И | У | Н |
| 20 | О | А | С | И | Р | Б | Я | И | У | Н | И | С | Р | Я | И | Б | А | Р | С | У | Ц |
| 19 | Б | Я | И | У | Н | И | С | Р | А | И | Ц | С | У | Ц | Б | Р | Я | Д | С | У | Ц |
| 18 | Б | Р | У | И | А | Ц | О | А | С | И | Р | Б | Я | И | Д | Я | **РО** ***БО*** | Р | И | Р | Н |
| 17 | С | А | И | Ц | И | Р | Б | Я | И | У | **ИН** | Б | Я | И | У | Н | И | С | Р | Ц | О |
| 16 | Р | Д | С | Я | И | Р | Н | Б | У | С | А | ***ИИ*** | Ц | ***ИС*** | У | Ц | Д | И | Ц | Я | Б |
| 15 | У | Б | Б | Д | И | Н | Я | О | Р | Д | С | Я | И | О | У | Р | Н | С | У | Б | Б |
| 14 | Р | Д | С | Я | И | Р | Н | Б | О | А | С | И | А | С | У | С | А | И | Ц | С | У |
| 13 | С | А | И | Я | Б | Р | У | И | А | Ц | О | С | И | Р | Б | Я | И | У | Н | И | О |
| 12 | Д | И | Н | Я | О | Р | Д | С | Я | **ДИ** | Р | Н | Б | Д | С | Я | И | Р | Н | Б | У |
| 11 | А | Р | С | У | Ц | Д | Н | Я | Б | С | У | С | А | И | Ц | С | У | Ц | Б | Р | Я |
| 10 | А | Р | С | У | Ц | Д | Н | Я | Б | С | У | О | **РД** | Ц | Я | Б | Р | У | И | А | Ц |
| 9 | Д | И | Ц | Я | Б | Р | У | И | А | Ц | О | А | С | У | С | А | И | Ц | С | У | Ц |
| 8 | У | О | Д | ***ЦА*** | С | Ц | О | У | Р | Н | С | У | Б | Б | Д | И | Н | Я | Ц | Ц | Я |
| 7 | О | Р | Н | С | У | Б | Б | Д | И | Н | Я | О | Р | Д | С | ***ИЯ*** | И | Р | Н | Б | У |
| 6 | Б | Я | И | У | Н | Б | Я | И | У | Н | С | А | И | Ц | И | Р | Б | Я | И | У | Д |
| 5 | Д | С | Р | У | А | О | И | Ц | Н | Р | Д | Я | О | Р | И | Р | Н | Б | У | С | А |
| 4 | А | Д | И | Ц | Я | Б | Р | У | И | **А** | Ц | О | А | С | И | Р | Б | Я | И | У | Н |
| 3 | И | Ц | Б | О | Р | Д | С | Я | И | Р | Н | Б | **СУ** | С | А | И | Ц | С | У | Ц | Б |
| 2 | Н | У | Ц | Я | И | Б | А | Р | С | У | Ц | Д | Н | Я | Б | С | У | О | Д | А | С |
| 1 | Д | С | Р | У | А | О | И | Ц | Н | Р | Д | Я | О | Р | Н | С | У | Б | Б | Д | И |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |

О(17,18), $E_1$={СУБО}, $R$=1.8; А(10,4), $E_2$={А}, $R$=0.001; Н(11,17), $E_3$={ИН}, $R$=0.8; Д(13,10), $E_4$={РД}, $R$=0.3; У(13,3), $E_5$={СУ}, $R$=0.6; И(10,12), $E_6$={ДИ}, $R$=0.8; Ц(19,16), $E_7$={РОЦ}, $R$=1; Ц(8,5), $E_8$={АЦ}, $R$=0.4; И(12,16), $E_9$={ИНИИ}, $R$=2.4; Ц(4,4), $E_{10}$={АЦ}, $R$=0.4; Я(16,7), $E_{11}$={РДИЯ}, $R$=1.6; И(12,16), $E_{12}$={РДИИ}, $R$=1.9; А(4,8), $E_{13}$={ДИЦА}, $R$=1.3; О(17,18), $E_{14}$={РО}, $R$=0.9.

6. В соответствии с шагом 10 алгоритма проведем операцию универсального кроссинговера по норме 75%, при этом для получения 9 потомков $E_{15}$-$E_{23}$ выбраны следующие списки: $E_9$–$E_{10}$ (с позиции 3, потомки $E_{15}$, $E_{16}$), $E_8$ –$E_{12}$ (с позиции 2, потомки $E_{17}$, $E_{18}$), $E_3$-$E_{11}$ (с позиции 3, потомки $E_{19}$, $E_{20}$), $E_{10}$–$E_{11}$ (с позиции 1, потомки $E_{21}$, $E_{22}$), $E_4$-$E_6$ (потомок $E_{23}$). Пусть сформированы следующие маски: 00, 01, 10, 11, 01. В этом случае получим потомков: $E_{15}$={ИНИИ}, $R$=2.4, $E_{16}$={ИНАЦ}, $R$=2.1, $E_{17}$={РАИИ}, $R$=2.4, $E_{18}$={РДЦИ}, $R$=0.9, $E_{19}$={РДИН}, $R$=1.9, $E_{20}$={РДИЯ}, $R$=1.6, $E_{21}$={РДИЯ}, $R$=1.6, $E_{22}$={АЦИЯ}, $R$=1.4, $E_{23}$={РИ}, $R$=0.7.

7. В соответствии с шагом 11 алгоритма проведем операцию точечной мутации. Пусть после выбора списка $E_{11}$ в нем меняется ген Я на Н(11,17), после выбора списка $E_{15}$ ген Н меняется на Ц, после выбора списка $E_{17}$ ген А меняется на Я, в списке $E_{23}$ ген И меняется на Д(13,10). В этом случае получим потомков: $E_{11}$={РДИН}, $R$=1.9, $E_{15}$={ИЦИИ}, $R$=1.4, $E_{17}$={РЯИИ}, $R$=1.1, $E_{23}$={РД}, $R$=0.3.

8. Таким образом, на итерации 2 мы будем иметь следующий перечень списков (хромосом), координат и значений функции $R$.

{СУБО(17,18)}, $R_1$=1.8; {А(10,4)}, $R_2$=0.001; {ИН(11,17)}, $R_3$=0.8; {РД(13,10)}, $R_4$=0.3; {СУ(13,3)}, $R_5$=0.6; {ДИ(10,12)}, $R_6$=0.8; {РОЦ(19,16)}, $R_7$=1; {АЦ(8,5)}, $R_8$=0.4; {ИНИИ(12,16)}, $R_9$=2.4; {АЦ(4,4)}, $R_{10}$=0.4; {РДИН(11,17)}, $R_{11}$=1.9; {РДИИ(12,16)}, $R_{12}$=1.9; {ДИЦА(4,8)}, $R_{13}$=1.3; {РО(17,18)}, $R_{14}$=0.9; {ИЦИИ(12,16)}, $R_{15}$=1.4; {ИНАЦ(4,4)}, $R_{16}$=2.1; {РЯИИ(12,16)}, $R_{17}$=2.4; {РДЦИ(12,16)}, $R_{18}$=0.9; {РДИН(11,17)}, $R_{19}$=1.9; {РДИЯ(16,7)}, $R_{20}$=1.6; {РДИЯ(16,7)}, $R_{21}$=1.6; {АЦИЯ(16,7)}, $R_{22}$=1.4; {РД(13,10)}, $R_{23}$=0.3.

Для списков, состоящих из 3 и более символов, применим весовой коэффициент $Q$. Определим для списка $E_1$ $Q$=1 и $R_1$=1.8; для списка $E_7$ $Q$=0.8 и $R_7$=0.8; для списка $E_9$ $Q$=0.6 и $R_9$=1.44; для списка $E_{11}$ $Q$=1 и $R_{11}$=1.9; для

списка $E_{12}$ $Q$=0.7 и $R_{12}$=1.33; для списка $E_{13}$ $Q$=0.7, $R_{13}$=0.91; для списка $E_{15}$ $Q$=0.9, $R_{15}$=1.26; для списка $E_{16}$ $Q$=0.8, $R_{16}$=1.68; для списка $E_{17}$ $Q$=0.5, $R_{17}$=1.2; для списка $E_{18}$ $Q$=0.4, $R_{18}$=0.36; для списка $E_{19}$ $Q$=1, $R_{19}$=1.9; для списка $E_{20}$ $Q$=0.85, $R_{20}$=1.36; для списка $E_{21}$ $Q$=0.85, $R_{21}$=1.36; для списка $E_{22}$ $Q$=1, $R_{22}$=1.4.

В этом случае перечень списков будет следующий:

{СУБО(17,18)}, $R_1$=1.8; {А(10,4)}, $R_2$=0.001; {ИН(11,17)}, $R_3$=0.8; {РД(13,10)}, $R_4$=0.3; {СУ(13,3)}, $R_5$=0.6; {ДИ(10,12)}, $R_6$=0.8; {РОЦ(19,16)}, $R_7$=0.8; {АЦ(8,5)}, $R_8$=0.4; {ИНИИ(12,16)}, $R_9$=1.44; {АЦ(4,4)}, $R_{10}$=0.4; {РДИН(11,17)}, $R_{11}$=1.9; {РДИИ(12,16)}, $R_{12}$=1.33; {ДИЦА(4,8)}, $R_{13}$=0.91; {РО(17,18), $R_{14}$=0.9}; {ИЦИИ(12,16)}, $R_{15}$=1.26; {ИНАЦ(4,4)}, $R_{16}$=1.68; {РЯИИ(12,16)}, $R_{17}$=1.2; {РДЦИ(12,16)}, $R_{18}$=0.36; {РДИН(11,17)}, $R_{19}$=1.9; {РДИЯ(16,7)}, $R_{20}$=1.36; {РДИЯ(16,7)}, $R_{21}$=1.36; {АЦИЯ(16,7)}, $R_{22}$=1.4; {РД(13,10)}, $R_{23}$=0.3.

9. Проводя элитную селекцию (в соответствии с шагом 12 алгоритма), удалим индивидуумы популяции с наименьшим значением $R$ до сокращения размеров популяции до размеров M=10. Это индивидуумы {А(10,4)}, {РД(13,10)}, {РД(13,10)}, {СУ(13,3)}, {ДИ(10,12)}, {ИН(11,17)}, {АЦ(8,5)}, {АЦ(4,4)}, {РДЦИ(12,16)}, {РОЦ(19,16)}, {РО(17,18)}, {ДИЦА(4,8)}, {РЯИИ(12,16)}.

10. Выбирая среди всех значений $R_i$ лучшее значение, получим, что $R_{11}$=$R_{19}$=1.9; $R^*$=1.9; $E_{11}$={РДИН}.

11. Полагаем $l$ =3.

*Итерация 3.*

1. В соответствии с шагом 19 алгоритма определим число $n_{b1}$=3; включим во множество $A_{b1}$ лучшие позиции из популяции, определенной на итерации 2. $A_{b1}$={РДИН(11,17), $R$=1.9; СУБО(17,18), $R$=1.8; ИНАЦ(4,4), $R$=1.68}.

2. Как и на предыдущей итерации 2, определим количество агентов-разведчиков $n_{rl}$=6 и разместим их произвольным образом в пространстве поиска. Пусть произвольным образом выбираются символы АЦИЯ(16,7), РДИИ(12,16), У(4,5), Я(4,9), С(16,2), Р(11,18).

3. В соответствии с шагом 19 включим во множество $A_{b2}$ $n_{b2}$=3 позиции из множества $n_{rl}$=6 позиций, найденных агентами–разведчиками на итерации 2. Пусть это будут позиции $A_{b2}$={У(4,5), $R$=1.4; РДИИ(12,16), $R$=1.14; С(16,2), $R$=0.001}.

4. Таким образом, на итерации $l$=3, $n_{b1}$+ $n_{b2}$=6 и множество базовых позиций $A_b$={РДИН(11,17), СУБО(17,18), ИНАЦ(4,4), У(4,5), РДИИ(12,16), С(16,2)}. Пространство поиска показано в табл. 4, базовые позиции отмечены прямым жирным шрифтом.

5. Определим количество агентов-фуражиров, как и ранее, $n_f$=8, размер максимальной окрестности $\lambda_{макс}$=20. Пусть базовые позиции выбираются в следующем порядке: $a_1$=РДИН(11,17), $a_2$=ИНАЦ(4,4), $a_3$=РДИИ(12,16), $a_4$=С(16,2), $a_5$=СУБО(17,18), $a_6$=У(4,5), $a_7$=С(16,2), $a_8$=ИНАЦ(4,4).

6. Пусть базовым позициям ставятся в соответствие следующие позиции $a_s$: РДИН(11,17)→ИЦИИ(12,16); ИНАЦ(4,4)→И(7,5); РДИИ(12,16)→РДИЯ(16,7); С(16,2)→У(10,2); СУБО(17,18)→РДИЯ(16,7); У(4,5)→А(12,9); С(16,2)→АЦИЯ(16,7); ИНАЦ(4,4)→И(9,4).

Таким образом, на данном шаге мы будем иметь следующий список позиций, решений и соответствующих значений функции $R$.

Н(11,17), $E_1$={РДИН}, $R$=1.9; Ц(4,4), $E_2$={ИНАЦ}, $R$=2.1; И(12,16), $E_3$={РДИИ}, $R$=1.9; С(16,2), $E_4$={С}, $R$=0.001; О(17,18), $E_5$={СУБО}, $R$=1.8; У(4,5), $E_6$={У}, $R$=0.001; И(12,16), $E_7$={РДИНИЦИИ}, $R$=4.1; И(7,5), $E_8$={ИНАЦИ}, $R$=2.6; Я(16,7), $E_9$={РДИИРДИЯ}, $R$=4.2; У(10,2), $E_{10}$={СУ}, $R$=0.6; Я(16,7), $E_{11}$={СУБОРДИЯ}, $R$=4.3; А(12,9), $E_{12}$={УА}, $R$=0.1; Я(16,7),

$E_{13}$={САЦИЯ}, *R*=2.2; И(9,4), $E_{14}$={ИНАЦИ}, *R*=2.6, И(12,16), $E_{15}$={ИНИИ}, *R*=2.4.

Таблица 4

Пространство поиска комбинированного алгоритма после 2 итерации

| | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 24 | И | Р | Б | Я | И | У | Н | И | С | Р | Ц | О | А | С | И | Р | Б | Я | Б | Р | У |
| 23 | Д | И | Н | Я | О | Р | Д | С | Я | И | Р | Н | Б | О | А | С | И | Р | Б | Я | И |
| 22 | Р | Д | С | Я | И | Р | Н | Б | У | С | А | И | Я | Б | Р | У | И | А | Ц | О | А |
| 21 | Б | Б | Д | И | Н | Я | Ц | А | С | У | С | А | И | Ц | И | Р | Б | Я | И | У | Н |
| 20 | О | А | С | И | Р | Б | Я | И | У | Н | И | С | Р | Я | И | Б | А | Р | С | У | Ц |
| 19 | Б | Я | И | У | Н | И | С | Р | А | И | Ц | С | У | Ц | Б | Р | Я | Д | С | У | Ц |
| 18 | Б | Р | У | И | А | Ц | О | А | С | И | Р | Б | Я | И | Д | Я | **СУБО** | Р | И | Р | Н |
| 17 | С | А | И | Ц | И | Р | Б | Я | И | У | **РДИН** | Б | Я | И | У | Н | И | С | Р | Ц | О |
| 16 | Р | Д | С | Я | И | Р | Н | Б | У | С | А | ***ИНИИ*** **РДИИ** ***ИЦИИ*** | Ц | С | У | Ц | Д | И | Ц | Я | Б |
| 15 | У | Б | Б | Д | И | Н | Я | О | Р | Д | С | Я | И | О | У | Р | Н | С | У | Б | Б |
| 14 | Р | Д | С | Я | И | Р | Н | Б | О | А | С | И | А | С | У | С | А | И | Ц | С | У |
| 13 | С | А | И | Я | Б | Р | У | И | А | Ц | О | С | И | Р | Б | Я | И | У | Н | И | О |
| 12 | Д | И | Н | Я | О | Р | Д | С | Я | И | Р | Н | Б | Д | С | Я | И | Р | Н | Б | У |
| 11 | А | Р | С | У | Ц | Д | Н | Я | Б | С | У | С | А | И | Ц | С | У | Ц | Б | Р | Я |
| 10 | А | Р | С | У | Ц | Д | Н | Я | Б | С | У | О | Д | Ц | Я | Б | Р | У | И | А | Ц |
| 9 | Д | И | Ц | Я | Б | Р | У | И | А | Ц | О | А | С | У | С | А | И | Ц | С | У | Ц |
| 8 | У | О | Д | А | С | Ц | О | У | Р | Н | С | У | Б | Б | Д | И | Н | Я | Ц | Ц | Я |
| 7 | О | Р | Н | С | У | Б | Б | Д | И | Н | Я | О | Р | Д | С | ***РДИЯ*** ***АЦИЯ*** | И | Р | Н | Б | У |
| 6 | Б | Я | И | У | Н | Б | Я | И | У | Н | С | А | И | Ц | И | Р | Б | Я | И | У | Д |
| 5 | Д | С | Р | **У** | А | О | И | Ц | Н | Р | Д | Я | О | Р | И | Р | Н | Б | У | С | А |
| 4 | А | Д | И | **ИНАЦ** | Я | Б | Р | У | И | А | Ц | О | А | С | И | Р | Б | Я | И | У | Н |
| 3 | И | Ц | Б | О | Р | Д | С | Я | И | Р | Н | Б | У | С | А | И | Ц | С | У | Ц | Б |
| 2 | Н | У | Ц | Я | И | Б | А | Р | С | У | Ц | Д | Н | Я | Б | **С** | У | О | Д | А | С |
| 1 | Д | С | Р | У | А | О | И | Ц | Н | Р | Д | Я | О | Р | Н | С | У | Б | Б | Д | И |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |

7. Проведем операцию универсального кроссинговера по норме 70%, при этом для получения 10 потомков $E_{16}$-$E_{25}$ выбраны следующие индивидуумы: $E_1$-$E_3$ (потомки $E_{16}$, $E_{17}$, маска 0100), $E_7$ –$E_9$ (потомки $E_{18}$, $E_{19}$, маска 00110100), $E_6$-$E_{14}$ (потомки $E_{20}$, $E_{21}$ с позиции 1, маска 1), $E_{13}$-$E_{14}$ (потомки $E_{22}$, $E_{23}$, маска 00110), $E_{10}$-$E_{13}$ (потомки $E_{24}$, $E_{25}$ с позиции 1, маска 01). В этом случае получим потомков: $E_{16}$={РДИН}, *R*=1.9; $E_{17}$={РДИИ},

*R*=1.9; $E_{18}$={РДИИИДИИ}, *R*=5; $E_{19}$={РДИНРЦИЯ}, *R*=3.1; $E_{20}$={ИНАЦИ}, *R*=2.6; $E_{21}$={УНАЦИ}, *R*=2.3; $E_{22}$={САЦЯ}, *R*=1.5; $E_{23}$={ИНЦИИ}, *R*=2.2; $E_{24}$={САЦИЯ}, *R*=2.2; $E_{25}$={СУЦИЯ}, *R*=1.7.

8. В соответствии с шагом 11 алгоритма проведем операцию точечной мутации. Пусть после выбора списка $E_7$ в нем меняется 5 и 8 гены И на А и Я, после выбора списка $E_9$ 4 ген И меняется на Н, после выбора списка $E_{19}$ 5 ген Р меняется на А. В этом случае получим потомков: $E_7$={РДИНАЦИЯ}, *R*=4.2; $E_9$={РДИНРДИЯ}, *R*=3.6; $E_{19}$={РДИНАЦИЯ}, *R*=4.2.

9. Таким образом, на итерации 3 мы будем иметь следующий перечень списков (хромосом), координат и значений функции *R*.

$E_1$={РДИН}, *R*=1.9; $E_2$={ИНАЦ}, *R*=2.1; $E_3$={РДИИ}, *R*=1.9; $E_4$={С}, *R*=0.001; $E_5$={СУБО}, *R*=1.8; $E_6$={У}, *R*=0.001; $E_7$={РДИНАЦИЯ}, *R*=4.2; $E_8$={ИНАЦИ}, *R*=2.6; $E_9$={РДИНРДИЯ}, *R*=3.6; $E_{10}$={СУ}, *R*=0.6; $E_{11}$={СУБОРДИЯ}, *R*=4.3; $E_{12}$={УА}, *R*=0.1; $E_{13}$={САЦИЯ}, *R*=2.2; $E_{14}$={ИНАЦИ}, *R*=2.6, $E_{15}$=={ИНИИ}, *R*=2.4; $E_{16}$={РДИН}, *R*=1.9; $E_{17}$={РДИИ}, *R*=1.9; $E_{18}$={РДИИИДИИ}, *R*=5; $E_{19}$={РДИНАЦИЯ}, *R*=4.2; $E_{20}$={ИНАЦИ}, *R*=2.6; $E_{21}$={УНАЦИ}, *R*=2.3; $E_{22}$={САЦЯ}, *R*=1.5; $E_{23}$={ИНЦИИ}, *R*=2.2; $E_{24}$={САЦИЯ}, *R*=2.2; $E_{25}$={СУЦИЯ}, *R*=1.7.

10. Для списков, состоящих из 3 и более символов, применим весовой коэффициент *Q*. Определим для списка $E_1$ *Q*=1 и $R_1$=1.9; для списка $E_2$ *Q*=0.7 и $R_2$=1.47; для списка $E_3$ *Q*=0.6 и $R_3$=1.14; для списка $E_5$ *Q*=1 и $R_5$=1.8; для списка $E_7$ *Q*=1 и $R_7$=4.2; для списка $E_8$ *Q*=0.8, $R_8$=2.08; для списка $E_9$ *Q*=0.4, $R_9$=1.44; для списка $E_{11}$ *Q*=0.9, $R_{11}$=3.87; для списка $E_{13}$ *Q*=0.7, $R_{13}$=1.54; для списка $E_{14}$ *Q*=0.8, $R_{14}$=2.08; для списка $E_{15}$ *Q*=0.6, $R_{15}$=1.44; для списка $E_{16}$ *Q*=1, $R_{16}$=1.9; для списка $E_{17}$ *Q*=0.6, $R_{17}$=1.14; для списка $E_{18}$ *Q*=0.3, $R_{17}$=1.5; для списка $E_{19}$ *Q*=1, $R_{19}$=4.2; для списка $E_{20}$ *Q*=0.8, $R_{20}$=2.08; для списка $E_{21}$ *Q*=0.4, $R_{21}$=0.92; для списка $E_{22}$ *Q*=0.3, $R_{22}$=0.45; для списка $E_{23}$ *Q*=0.5, $R_{23}$=1.1; для списка $E_{24}$ *Q*=0.7, $R_{24}$=1.54; для списка $E_{25}$ *Q*=0.3, $R_{25}$=0.51.

В этом случае перечень списков будет следующий:

$E_1$={РДИН}, $R$=1.9; $E_2$={ИНАЦ}, $R$=1.47; $E_3$={РДИИ}, $R$=1.14; $E_4$={С}, $R$=0.001; $E_5$={СУБО}, $R$=1.8; $E_6$={У}, $R$=0.001; $E_7$={РДИНАЦИЯ}, $R$=4.2; $E_8$={ИНАЦИ}, $R$=2.08; $E_9$={РДИНРДИЯ}, $R$=1.44; $E_{10}$={СУ}, $R$=0.6; $E_{11}$={СУБОРДИЯ}, $R$=3.87; $E_{12}$={УА}, $R$=0.1; $E_{13}$={САЦИЯ}, $R$=1.54; $E_{14}$={ИНАЦИ}, $R$=2.08; $E_{15}$={ИНИИ}, $R$=1.44; $E_{16}$={РДИН}, $R$=1.9; $E_{17}$={РДИИ}, $R$=1.14; $E_{18}$={РДИИИДИИ}, $R$=1.5; $E_{19}$={РДИНАЦИЯ}, $R$=4.2; $E_{20}$={ИНАЦИ}, $R$=2.08; $E_{21}$={УНАЦИ}, $R$=0.92; $E_{22}$={САЦЯ}, $R$=0.45; $E_{23}$={ИНЦИИ}, $R$=1.1; $E_{24}$={САЦИЯ}, $R$=1.54; $E_{25}$={СУЦИЯ}, $R$=0.51.

11. Проводя элитную селекцию, удалим индивидуумы популяции с наименьшим значением $R$ до сокращения размеров популяции до размеров M=10. Это индивидуумы {С(16,2)}, {У(4,5), $R$=0.001}, {УА(12,9)}, $R$=0.1, {СУ(10,2)}, $R$=0.6, {СУЦИЯ(16,7)}, $R$=0.51, {САЦЯ(16,7) , $R$=0.45}, {ИНИИ(12,16), $R$=1.44}, {САЦИЯ(16,7) , $R$=1.54}, {ИНЦИИ(9,4) , $R$=1.1}, {РДИИ(12,16) , $R$=1.14}, {РДИИ(12,16) , $R$=1.14}, {РДИНРДИЯ(16,7), $R$=1.44}, {РДИИИДИИ(12,16), $R$=1.5}, {ИНАЦ(4,4), $R$=1.47}, {УНАЦИ(9,4), $R$=0.92}.

12. Выбирая лучшее значение среди всех значений $R_i$, получим, что $R_7$=$R_{19}$=4,2; $E_7$={РДИНАЦИЯ}.

13. Полагаем $l$ =4.

*Итерация 4.*

1. Как и ранее, определим число $n_{b1}$=3; включим во множество $A_{b1}$ лучшие позиции из популяции, определенной на итерации 3. $A_{b1}$={РДИНАЦИЯ(16,7), $R$=4.2; СУБОРДИЯ(16,7), $R$=3.87; ИНАЦИ(7,5), $R$=2.08}.

2. Как и на ранее, определим количество агентов-разведчиков $n_{rl}$=6 и разместим их произвольным образом в пространстве поиска. Пусть

произвольным образом выбираются символы САЦИЯ(16,7), РДИН(11,17), СУБО(17,18), Р(16,24), И(17,23), У(4,5).

3. Включим во множество $A_{b2}$ $n_{b2}$=3 позиции из множества $n_{rl}$=6 позиций, найденных агентами–разведчиками на итерации 4. Пусть это будут позиции $A_{b2}$={РДИН(11,17), $R$=1.9; САЦИЯ(16,7), $R$=1.54; СУБО(17,18), $R$=1.8}.

4. Таким образом, на итерации $l$=4 множество базовых позиций $A_b$={РДИНАЦИЯ(16,7), СУБОРДИЯ(16,7), ИНАЦИ(7,5), САЦИЯ(16,7), РДИН(11,17), СУБО(17,18)}.

5. После определения количества агентов-фуражиров $n_f$=8, размера максимальной окрестности $\lambda_{макс}$=20 выберем базовые позиции в следующем порядке:

$a_1$=САЦИЯ(16,7), $a_2$=ИНАЦИ(7,5), $a_3$=СУБО(17,18), $a_4$=СУБОРДИЯ(16,7), $a_5$=СУБО(17,18), $a_6$=РДИН(11,17), $a_7$=РДИН(11,17), $a_8$=РДИНАЦИЯ(16,7).

Таким образом, если базовой позиции О(17,18) (список СУБО) ставится в соответствие позиция Я(16,7) (список РДИНАЦИЯ), то на данной итерации возможно получение оптимального варианта текста с максимальным значением целевой функции $R$=6.9. Такой же потомок может быть получен в случае, если базовой позиции Я(16,7) (список СУБОРДИЯ) ставится в соответствие позиция Н(11,17) (список РДИН), полученный потомок СУБОРДИЯРДИН подвергается скрещиванию со списком САЦИЯ (с позиции 8 по маске 01101), и в полученном потомке СУБОРДИЯАЦИЯ 8 ген Я заменяется на Н. Следует заметить, что при реализации криптоанализа текстовых фрагментов значительной длины применение комбинированных биоинспирированных стратегий может существенно повысить разнообразие генетического материала популяции, увеличивая скорость схождения к глобальному оптимуму. В общем случае, как и при реализации классических эволюционных методов, размер популяции, нормы реализации генетических

операторов и этапы их могут определяться экспериментально, исходя из условий задачи. Определяющими для эффективности реализации алгоритма являются: размер популяции, нормы и тип генетических операций (кроссинговер, мутация, селекция), оптимальный выбор весового коэффициента $Q$, применение которых обеспечивает появление в популяции оптимальных вариантов потомков, разнообразие их оптимальных частей и схождение популяции к оптимальному (квазиоптимальному) варианту.

Ранее в [25] было показано, что при использовании комбинированных биоинспирированных алгоритмов вероятность улучшения частичного решения на каждой итерации не может быть меньше вероятности улучшения частичного решения при использовании каждого классического биоинспирированного алгоритма. Отметим здесь еще раз этот существенный момент. Пусть $Ï$ - группа операторов комбинированного алгоритма, соответствующая операторам алгоритма пчелиных колоний (операторы 1-9, 17-21), $Ã$ - группа операторов, соответствующая операторам генетического алгоритма (операторы 10-16). Пусть $Ð(Ï)$ - вероятность того, что при реализации пчелиного алгоритма на итерации $i$ получено решение, лучшее, чем на итерации $i-1$. Аналогично, пусть $Ð(Ã)$ - вероятность того, что реализации генетического алгоритма на итерации $i$ получено решение, лучшее, чем на итерации $i-1$. Поскольку эти события совместны (улучшение частичного решения может иметь место одновременно при реализации обоих групп операторов), то, используя аппарат теории вероятностей, получим, что при реализации комбинированного алгоритма вероятность $Ð$ получения на $i$ итерации частичного решения, лучшего, чем на $i-1$ итерации, составит $P = P(Ï) + Ð(Ã) - P(Ï) * P(Ã)$. Поскольку все значения $P, P(Ï), Ð(Ã)$ удовлетворяют условию $0 \le P \le 1, 0 \le P(Ï) \le 1$, $0 \le P(Ã) \le 1$, то, очевидно, произведение $P(Ï) * P(Ã)$ будет удовлетворять условию $Ð(Ï) * Ð(Ã) \le min(P(Ï), P(Ã))$. В то же время имеет

место очевидное соотношение $Ð(M)+Ð(\tilde{A})\geq màõ(P(M),P(\tilde{A}))$. Отсюда следует, что будет иметь место соотношение $P=P(\ddot{I})+Ð(\tilde{A})-P(\ddot{I})*P(\tilde{A})\geq max(P(\ddot{I}),P(\tilde{A}))$.

Таким образом, мы еще раз показали (аналогично [25]) применительно к комбинированному алгоритму пчелиных колоний), что при реализации комбинированного биоинспирированного алгоритма вероятность $Ð$ улучшения частичного решения на $i$ итерации по сравнению с $i-1$ итерацией удовлетворяет условию $P\geq max(P_1,P_2)$, где $P_1,P_2$ - вероятности улучшения частичного решения при использовании классических биоинспирированных алгоритмов. При этом увеличение вероятности может быть определено из соотношения $P=P_1+Ð_2-P_1*P_2$. Данные расчеты показывают, что при использовании комбинированных биоинспирированных алгоритмов вероятность улучшения частичного решения на каждой итерации не может быть меньше вероятности улучшения частичного решения при использовании каждого классического биоинспирированного алгоритма, что подтверждает целесообразность разработки и использования комбинированных биоинспирированных стратегий и их применения для решения оптимизационных одно- и многоэкстремальных задач. Очевидно, что данные рассуждения справедливы для любого числа $n$ биоинспирированных алгоритмов и вероятностей $P_1,P_2,...,P_n$.

## Основные выводы

Таким образом, основные результаты работы заключаются в следующем:

- исследована возможность применения комбинированного биоинспирированного алгоритма (генетический алгоритм и алгоритм пчелиных колоний) для реализации задачи криптоанализа систем шифрования; представлены описания основных операций комбинированного биоинспирированного алгоритма;

- представлен демонстрационный пример реализации комбинированного алгоритма криптоанализа, показана возможность получения оптимального варианта решения за конечное число итераций;

- применительно к данному алгоритму показано, что вероятность получения оптимального варианта решения при реализации комбинированных алгоритмов криптоанализа не может быть меньше вероятности получения оптимального решения при использовании классических биоинспирированных алгоритмов, что подтверждает целесообразность использования комбинированных биоинспирированных методов для решения оптимизационных задач.

**Работа выполнена при финансовой поддержке РФФИ (проекты 17-01-00375, 15-01-05129).**

## Литература

1. Чернышев Ю.О., Сергеев А.С., Дубров Е.О., Крупенин А.В., Третьяков О.П. Криптографические методы и генетические алгоритмы решения задач криптоанализа: монография. - Краснодар: ФВАС, 2013. - 138 с.

2. Чернышев Ю.О., А.С. Сергеев, Дубров Е.О., Крупенин А.В., Капустин С.А., Рязанов А.Н. Биоинспирированные алгоритмы решения задач криптоанализа классических и асимметричных криптосистем: монография. – Краснодар: КВВУ, 2015. – 132 с.

3. Чернышев Ю.О., Сергеев А.С., Дубров Е.О., Рязанов А.Н. Применение биоинспирированных методов оптимизации для реализации криптоанализа блочных методов шифрования: монография. - Ростов-на-Дону: издательство ДГТУ, 2016. - 177 с.

4. Лебедев В. Б. Модели адаптивного поведения колонии пчел для решения задач на графах // Известия ЮФУ, 2012, № 7, С. 42–49.

5. Орловская Н.М. Анализ эффективности биоинспирированных методов глобальной оптимизации // Труды МАИ: электронный научный журнал, 2014, № 73, С. 4.

6. Лебедев О. Б. Трассировка в канале методом муравьиной колонии // Известия ЮФУ, 2009, № 4, С. 46–52.

7. Фатхи В.А., Сергеев А.С. Исследование возможности применения алгоритма муравьиных колоний для реализации криптоанализа шифров перестановок // Вестник ДГТУ, том 11, № 1(52), 2011, с. 10-20.

8. Чернышев Ю.О., Сергеев А.С., Дубров Е.О., Рязанов А.Н. Исследование возможности применения бионических методов пчелиных колоний для реализации криптоанализа классических шифров перестановок // Вестник ДГТУ. - 2014.- Т. 14. - № 1(76). – с. 62-75.

9. Чернышев Ю.О., Сергеев А.С. Дубров Е.О. Обзор алгоритмов решения задач криптоанализа на основе биоинспирированных технологий искусственного интеллекта. - Вестник Воронежского государственного университета, № 2, сер. «Системный анализ и информационные технологии», Воронеж, 2014, с. 83-89.

10. Чернышев Ю.О., Сергеев А.С., Дубров Е.О. Информационная безопасность и биоинспирированные алгоритмы решения задач криптоанализа. - Труды Международного симпозиума «Надежность и качество - 2014». -Пенза: ПГУ, 2014, с. 342-346.

11. Чернышев Ю. О., Сергеев А.С., Рязанов А.Н., Дубров Е.О. Обзор авторских методов решения задач криптоанализа блочных криптосистем на основе биоинспирированных технологий искусственного интеллекта // Наука и образование – 2016: материалы всероссийской научно-практической конференции. – Мурманск: Изд-во МГТУ, 2016, С. 184-190.

12. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001, 376 с.

13. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ, 2002, 480 с.

14. Васильев Е.М., Свистунов А.А. Решение комбинаторных задач моделированием поведения муравьиных колоний // Электротехнические комплексы и системы управления: научно-технический журнал, 2008, № 1, С. 54-55.

15. Holland J. H. Adaptation in natural and artificial systems. An introductory analysis with application to biology, control, and artificial intelligence. University of Michigan, 1975, 183 p.

16. Goldberd David E. Genetic Algorithms in Search, Optimization and Machine Learning. Addision-Wesley Publishing Company, Inc. 1989, 432 p.

17. Сергеев А.С. Методы оптимизации: учебное пособие. – Ростов н/Д: Издательский центр ДГТУ, 2005, 113 С.

18. Сергеев А.С., Рязанов А.Н., Дубров Е.О. Применение алгоритмов пчелиных колоний для реализации криптоанализа блочных методов шифрования. // Инженерный вестник Дона, 2016, №2 URL: ivdon.ru/ru/magazine/archive/n2y2016/3621.

19. Курейчик В. В., Жиленков М.А. Пчелиный алгоритм для решения оптимизационных задач с явно выраженной целевой функцией //Информатика, вычислительная техника и инженерное образование, 2015, № 1(21), С. 1-8.

20. Гладков Л. А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы: учебное пособие. – М: Физматлит, 2006. – 320 с.

21. Курейчик В.М. Модифицированные генетические операторы // Известия ЮФУ, сер. «Технические науки», тем. выпуск «Интеллектуальные САПР», 2009, № 12, С. 7–14.

22. Дискретная математика: алгоритмы. URL: rain.ifmo.ru/cat/view.php/theory/unsorted/genetic-2005 (дата обращения: 09.12.2017).

23. Тимченко С.В. Сравнение трех подходов к построению параллельных генетических алгоритмов на примере некоторых задач функциональной оптимизации и генетического программирования. URL: botik.ru/PSI/RCMS/publications/publ-texts/2005/grishagine.pdf (дата обращения 09.12.2017).

24. Вероятности биграмм в тексте. URL: hakinfo.narod.ru/cripto/kr8.html (дата обращения: 09.12.2017).

25. Чернышев Ю.О., Сергеев А.С. Применение комбинированных биоинспирированных алгоритмов для реализации криптоанализа симметричных алгоритмов шифрования // XX международная конференция по мягким вычислениям и измерениям: сборник научных трудов. – С-Пб.: Изд-во СПбГЭТУ «ЛЭТИ», 2017, С. 497-500.

26. Карпенко А.П. Современные алгоритмы поисковой оптимизации. Алгоритмы вдохновленные природой. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2017, 446 с.

27. Венцов Н.Н. Эволюционный подход к моделированию распределительных процессов // Инженерный вестник Дона, 2013, № 4 URL: ivdon.ru/ru/magazine/archive/n4y2013/1886.

## References

1. Chernyshev Ju.O., Sergeev A.S., Dubrov E.O., Krupenin A.V., Tret'jakov O.P. Kriptograficheskie metody i geneticheskie algoritmy reshenija zadach kriptoanaliza: monografija [Cryptographic methods and genetic algorithms of the solution of problems of cryptanalysis: monograph.]. Krasnodar: FVAS, 2013, 138 p.

2. Chernyshev Ju.O., Sergeev A.S., Dubrov E.O., Krupenin A.V., Kapustin S.A., Rjazanov A.N. Bioinspirirovannye algoritmy reshenija zadach kriptoanaliza klassicheskih i asimmetrichnyh kriptosistem: monografija [The bioinspired algorithms of the solution of problems of cryptanalysis of classical and asymmetric cryptosystems: monograph.]. Krasnodar: KVVU, 2015, 132 p.

3. Chernyshev Ju.O., Sergeev A.S., Dubrov E.O., Rjazanov A.N. Primenenie bioinspirirovannyh metodov optimizacii dlja realizacii kriptoanaliza blochnyh metodov shifrovanija: monografija [The application of bioinspired optimization techniques for the implementation of the cryptanalysis of block encryption methods: monograph]. Rostov-na-Donu, DGTU, 2016, 177 p.

4. Lebedev V. B. Izvestija JuFU. 2012. № 7. pp. 42-49.

5. Orlovskaja N. M. Trudy MAI: jelektronnyj nauchnyj zhurnal, 2014, № 73, p. 4.

6. Lebedev O. B. Izvestija JuFU. 2009. № 4. pp. 46-52.

7. Fathi V.A., Sergeev A.S. Vestnik DGTU, T. 11, № 1(52), 2011, pp. 10-20.

8. Chernyshev Ju.O., Sergeev A.S., Dubrov E.O., Rjazanov A.N. Vestnik DGTU, T. 14, № 1(76), 2014, pp. 62-75.

9. Chernyshev Ju.O., Sergeev A.S. Dubrov E.O. Vestnik Voronezhskogo gosudarstvennogo universiteta, № 2, 2014, pp. 83-89.

10. Chernyshev Ju.O., Sergeev A.S. Dubrov E.O. Informacionnaja bezopasnost' i bioinspirirovannye algoritmy reshenija zadach kriptoanaliza [Information security and bioinspired algorithms for solving problems of cryptanalysis]. Trudy Mezhdunarodnogo simpoziuma «Nadezhnost' i kachestvo - 2014». Penza: PGU, 2014, pp. 342-346.

11. Chernyshev Ju. O., Sergeev A.S., Rjazanov A.N., Dubrov E.O. Obzor avtorskih metodov reshenija zadach kriptoanaliza blochnyh kriptosistem na osnove bioinspirirovannyh tehnologij iskusstvennogo intellekta [Review of author's

methods for solving problems of cryptanalysis of block cryptosystems based on bioinspired artificial intelligence technologies]. Nauka i obrazovanie – 2016: materialy vserossijskoj nauchno-prakticheskoj konferencii. Murmansk: Izd-vo MGTU, 2016, pp. 184-190.

12. Romanec Ju.V., Timofeev P.A., Shan'gin V.F. Zashhita informacii v komp'juternyh sistemah i setjah [Protection of information in computer systems and networks]. M.: Radio i svjaz', 2001, 376 p.

13. Alferov A.P., Zubov A.Ju., Kuz'min A.S., Cheremushkin A.V. Osnovy kriptografii [The basics of cryptography.]. M.: Gelios ARV, 2002, 480 p.

14. Vasil'ev E.M., Svistunov A.A. Jelektrotehnicheskie kompleksy i sistemy upravlenija: nauchno-tehnicheskij zhurnal, 2008, № 1, pp. 54-55.

15. Holland J. H. Adaptation in natural and artificial systems. An introductory analysis with application to biology, control, and artificial intelligence. University of Michigan, 1975, 183 p.

16. Goldberg David E. Genetic Algorithms in Search, Optimization and Machine Learning. Addision-Wesley Publishing Company, Inc. 1989, 432 p.

17. Sergeev A.S. Metody optimizacii: uchebnoe posobie [Optimization techniques: a tutorial]. Rostov n/D: Izdatel'skij centr DGTU, 2005. 113 p.

18. Sergeev A.C., Rjazanov A.H., Dubrov E.O. Inženernyj vestnik Dona (Rus), 2016, № 2, URL: ivdon.ru/ru/magazine/archive/n2y2016/3621.

19. Kurejchik V. V., Zhilenkov M.A. Informatika, vychislitel'naja tehnika i inzhenernoe obrazovanie, 2015, № 1(21), pp. 1-8.

20. Gladkov L. A., Kurejchik V.V., Kurejchik V.M. Geneticheskie algoritmy: uchebnoe posobie [Genetic algorithms: a tutorial.]. M: Fizmatlit, 2006. 320 p.

21. Kurejchik V.M. Izvestija JuFU, ser. «Tehnicheskie nauki», tem. vypusk «Intellektual'nye SAPR», 2009, № 12, pp. 7–14.

22. Diskretnaja matematika: algoritmy [Discrete mathematics: algorithms]. URL: rain.ifmo.ru/cat/view.php/theory/unsorted/genetic-2005 (accessed 09.12.2017).

23. Timchenko S.V. Sravnenie treh podhodov k postroeniju parallel'nyh geneticheskih algoritmov na primere nekotoryh zadach funkcional'noj optimizacii i geneticheskogo programmirovanija [Comparison of three approaches to parallel genetic algorithms on the example of some problems of functional optimization and genetic programming]. URL: www.botik.ru/PSI/RCMS/publications/publ-texts/2005/grishagine.pdf (accessed 09.12.2017).

24. Verojatnosti bigramm v tekste [The probability of bigrams in the text]. URL: hakinfo.narod.ru/cripto/kr8.html (accessed 09.12.2017).

25. Chernyshev Ju.O., Sergeev A.S. Primenenie kombinirovannyh bioinspirirovannyh algoritmov dlja realizacii kriptoanaliza simmetrichnyh algoritmov shifrovanija [The use of combined bioinspired algorithms for the implementation of the cryptanalysis of symmetric encryption algorithms]. XX mezhdunarodnaja konferencija po mjagkim vychislenijam i izmerenijam: sbornik nauchnyh trudov. S-Pb.: Izd-vo SPbGJeTU «LJeTI», 2017, pp. 497-500.

26. Karpenko A.P. Sovremennye algoritmy poiskovoj optimizacii. Algoritmy vdohnovlennye prirodoj [Modern algorithms of search engine optimization. Algorithms inspired by nature]. M.: Izd-vo MGTU im. N.Je. Baumana, 2017, 446 p.

27. Vencov N.N. Inženernyj vestnik Dona (Rus), 2013, № 4. URL: ivdon.ru/ru/magazine/archive/n4y2013/1886.