7. Ilyushin Yu. V., Afanaseva O. V. Analysis and synthesis of distributed icedrill heating control system of mountain reconnaissance drilling rig / Intern. Multidisciplinary Scientific GeoConf. Surveying Geology and Mining Ecology Management, SGEM. 2018. Vol. 2, № 18. P. 41–48.

8. Ilyushin Yu. V., Novozhilov I. M., Kivayev I. N. Improving the quality of training specialists in subsoil use at the expense of introduction of automated training systems // IEEE 6th Forum Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations). 2018. № 3. P. 125–127.

9. Ilyushin Yu. V., Novozhilov I. M., Kivayev I. N. Classification of modern educational programs by functional purpose // IEEE 6th Forum Strategic Partnership of Universities and Enterprises of Hi-Tech Branches (Science. Education. Innovations). 2018. № 3. P. 96–99.

10. Document Improving energy efficiency of tunnel furnaces of the pipeline type-the solution of the problem / Yu. V. Ilyushin, O. V. Afanasyeva, M. P. Afanasyev, S. V. Kolesnichenko, D. A. Pervukhin // ARPN J. of Engineering and Applied Sciences. 2017. Vol. 6, № 12. P. 1801–1812.

11. Ilyushin Yu. V., Mokeev A. B. The control system of the thermal field in tunnel furnace of a Conveyor type // ARPN J. of Engineering and Applied Sciences. 2017. Vol. 22, № 12. P. 6595–6605.

12. Ilyushin Yu. V., Mokeev A. B. Tunnel furnace of a conveyor type: Technical controlling of the temperature field // Intern. J. of Applied Engineering Research 2017. Vol. 20, № 12. P. 9377–9389.

Yu. V. Ilyushin
Saint Petersburg mining university
M. Yu. Shestopalov
Saint Petersburg Electrotechnical University «LETI»

APPLICATION OF THE MODIFIED NYQUIST CRITERION FOR THE ANALYSIS OF IMPULSE DISTRIBUTED SYSTEMS

The classical results of the theory of automatic control are obtained in most cases in relation to systems with lumped parameters, whose behavior is uniquely characterized by changing controlled quantities only in time and is described most often by ordinary differential equations, which makes it impossible to expand the scope of such systems. The article discusses the modification of the Nyquist absolute stability criterion for its application in the theory of systems with distributed parameters. The limiting characteristics of parameters affecting the type and shape of spatial hodographs of typical distributed links are investigated. A modified criterion of absolute stability of nonlinear distributed control systems has been developed. A method for analyzing the absolute stability of a class of nonlinear distributed control systems has been developed. By example, the construction of a spatially distributed hodograph is considered and the stability region of the system under consideration is constructed.

System analysis, control, distributed systems, absolute stability

УДК 004.056.55

Ю. О. Чернышев, А. С. Сергеев, А. Н. Рязанов
Донской государственный технический университет

Исследование и разработка параллельного комбинированного биоинспирированного алгоритма для решения задач криптоанализа

Рассматривается задача криптоанализа с использованием новой модели оптимизационных стратегий – комбинированного биоинспирированного алгоритма. Описано применение комбинированного биоинспирированного алгоритма на основе гибридизации вложением (генетический алгоритм и алгоритм муравьиных колоний) для реализации криптоанализа шифров перестановок. Приводится описание комбинированного алгоритма, показано, что вероятность получения оптимального варианта решения при реализации гибридных алгоритмов криптоанализа не может быть меньше вероятности получения оптимального решения при использовании классических биоинспирированных алгоритмов. Приводится описание основных операций, допускающих параллельное выполнение на глобальном уровне, также представлены структурная схема параллельного алгоритма, информационно-логическая граф-схема, приведено описание матрицы следования. На основе определения множеств взаимно независимых операторов и критического пути в графе решается задача определения минимального числа процессоров для реализации параллельного комбинированного алгоритма.

Криптоанализ, комбинированные биоинспирированные алгоритмы, гибридизация вложением, генетический алгоритм, алгоритм муравьиных колоний, информационно-логическая граф-схема, матрица следования, матрица независимости

Известно, что научное направление «природные вычисления», объединяющее математические методы, в которых заложен принцип природных механизмов принятия решений, в последние годы

получает все более широкое распространение для решения различного круга задач оптимизации, в том числе задач криптоанализа. В данных методах и моделях основным определяющим элементом является построение начальной модели и правил, по которым она может оптимизироваться (эволюционировать). В [1] авторами рассматривалось решение задач криптоанализа, относящихся к переборным задачам с экспоненциальной временной сложностью: традиционных симметричных криптосистем, использующих шифры перестановки и замены, в [2] – симметричных и асимметричных криптосистем с использованием алгоритмов муравьиных и пчелиных колоний. Исследованию возможности применения методов генетического поиска для реализации криптоанализа блочных криптосистем посвящена работа [3]. Следует заметить, что, поскольку задачи криптоанализа в большинстве случаев имеют комбинаторную сложность (являются NP-полными), то, очевидным образом, актуальной является задача разработки новых алгоритмов решения комбинаторных задач вследствие возникших потребностей в решении задач большой и очень большой размерности. Этой проблеме посвящена работа [4], в которой приводится описание новых моделей биоинспирированных методов глобальной оптимизации: методы, имитирующие поведение лягушек, кукушек, светлячков, и метод, имитирующий распространение сорняков. Основная особенность этих методов состоит в возможности поиска глобального экстремума многоэкстремальных целевых функций с большим числом переменных.

Тем не менее существующие структуры алгоритмов генетического поиска фактически являются «слепыми» поисковыми структурами с присущими им недостатками: генерация решений с нарушениями, что требует дополнительного контроля; генерация большого количества аналогичных решений; генерация большого количества «плохих» решений, что приводит к попаданию в локальный оптимум [2]. Поэтому актуальной является задача исследования и разработки эвристических методов, являющихся аналогами природных систем, в которых осуществляется поэтапное построение решения задачи. К методам данного вида относятся и алгоритмы муравьиных колоний. В данной статье освещен параллельный комбинированный биоинспирированный алгоритм (комбинирование генетического алгоритма и алгоритма муравьиных колоний) для криптоанализа классических шифров перестановок. Ранее данная задача криптоанализа классических криптографических методов на основе генетических алгоритмов, а также алгоритмов муравьиных колоний рассматривалась в обзорных работах [5], [6].

Возможность применения алгоритма муравьиных колоний для решения задач криптоанализа шифров перестановок описана в [2], [7] (при этом используется матрица частоты биграмм, и с ее помощью задача криптоанализа сводится к квадратичной задаче о назначениях). Применение генетического алгоритма для реализации криптоанализа классических шифров перестановок описано в [1], где наряду с результатами эксперимента также дано описание основных операций и приведена схема реализации алгоритма.

Постановка задачи. Тем не менее, поскольку методы эволюционного поиска в общем случае обладают рядом отмеченных недостатков, представляет определенный научный интерес применение эвристических методов и алгоритмов, сущность которых заключается в добавлении нового оптимального частичного решения к уже построенному частичному оптимальному или квазиоптимальному решению. К данному виду относят и алгоритмы муравьиных колоний, основная идея которых состоит в моделировании поведения муравьев и их способности быстро находить кратчайший путь от муравейника к источнику пищи.

Основными этапами построения муравьиного алгоритма для решения какой-либо задачи являются [2], [8]:

1. Представление задачи в виде набора компонент и переходов или в виде набора неориентированных взвешенных графов, на которых муравьи могут строить решения.

2. Определение значения следа феромона.

3. Определение эвристики поведения муравья при построении решения.

4. Настройка параметров алгоритма.

Примеры реализации алгоритма муравьиных колоний для криптоанализа шифров перестановок, а также для криптоанализа асимметричных алгоритмов шифрования приведены в [1], [2], [9]. Возникает вопрос о возможности применения комбинированных биоинспирированных алгоритмов для реализации криптоанализа, в частности, о возможности разработки методов, сочетающих основные черты генетических и муравьиных алгоритмов. В работе [10], посвященной разработке популяционных алгоритмов оптимизации (в том числе гибридизации популяционных алгоритмов), отмечается, что в гибридных алгорит-

мах, объединяющих различные либо однотипные алгоритмы, но с различными значениями параметров, преимущества одного алгоритма могут компенсировать недостатки другого. Таким образом, одним из основных путей повышения эффективности решения задач глобального поиска в настоящее время является разработка гибридных популяционных алгоритмов. Некоторые разновидности классификаций гибридных популяционных алгоритмов, в частности, одноуровневая классификация Ванга, в которой выделяют три категории гибридных алгоритмов, рассмотрены в [10]: 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 объединены достаточно сильно, так, что при низкоуровневой гибридизации алгоритмов, по сути, происходит формирование нового алгоритма.

Общая схема последовательной высокоуровневой гибридизации вложением включает следующие основные этапы [10].

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 итераций. Если это условие выполнено – завершение вычислений, в противном случае – переход к п. 2.

Отметим, что пример высокоуровневой гибридизации – комбинированный алгоритм криптоанализа шифров перестановок, где в качестве популяционного алгоритма используется генетический алгоритм, а в качестве алгоритма локального поиска – алгоритм муравьиных колоний – приведен в [11]–[13], в [14] рассматривается возможность применения данных методов для криптоанализа шифров замены. В [11]–[13] приводится соотношение

$$P = P(\text{М}) + P(\Г) - P(\text{М})P(\Г) \geq \max(P(\text{М}), P(\Г)),$$

где $P(\text{М})$ – вероятность того, что при реализации муравьиного алгоритма на итерации i получено решение, лучшее, чем на итерации $i-1$. $P(\Г)$ – вероятность того, что при реализации генетического алгоритма на итерации i получено решение, лучшее, чем на итерации $i-1$. Отсюда следует утверждение [11]: при реализации комбинированного биоинспирированного алгоритма вероятность P 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 $P = P_1 + P_2 - P_1P_2$. Таким образом 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. Этот вывод подтверждает целесообразность разработки и использования комбинированных биоинспирированных методов и алгоритмов для решения оптимизационных одно- и многоэкстремальных задач.

Используя аппарат теории вероятностей, аналогичные рассуждения можно провести для любого числа n классических биоинспирированных алгоритмов и вероятностей $P_1, P_2, \ldots, P_n$.

Комбинированный алгоритм. Основные этапы комбинированного алгоритма, разработанного в [11], включают следующие операции.

1. Случайным равновероятным образом выбираются m вариантов маршрутов – формируется популяция индивидуумов, вычисляются значения целевых функций $P_1, P_2, \ldots, P_m$ и умножаются на весовой коэффициент Q.

2. Проведение операции кроссинговера полученных индивидуумов на основе заданной нормы, получение заданного количества потомков (формирование расширенной популяции).

3. Проведение операции мутации индивидуумов популяции на основе заданной нормы мутации, получение заданного количества мутированных потомков. Подсчет целевых функций R вновь полученных индивидуумов и умножение на весовой коэффициент Q.

4. Проведение отбора (селекции) индивидуумов популяции для формирования нового поколения и сокращения популяции в соответствии с заданным критерием отбора.

5. Комбинациям *ik*, *l* размещения символов *k* в позиции *i* присваивается весовой коэффициент, являющийся аналогом концентрации феромона:

$$f_{ik,l} = R_l, \quad l = 1, 2, \ldots, m,$$

где *l* – номер маршрута, которому принадлежит комбинация *ik* (размещение символа *k* в позиции *i*).

6. Для каждой комбинации *ik* вычисляется результирующая концентрация:

$$F_{ik} = \sum_{l=1}^{m} f_{ik,l}$$

Для тех комбинаций *ik*, которые ни разу не встретились в популяции, задается нижнее значение концентрации феромона:

$$F_{\min} = a \max f_{ik,l},$$

где $\max f$ – максимальное значение весового коэффициента среди всех комбинаций размещения символов в позиции. Коэффициент *a* может быть выбран из условия $0 < a < 1$.

7. Проведение имитации испарения феромона со всех комбинаций *ik*, по которым прошли муравьи, в соответствии с формулой, аналогичной используемой в [7]:

$$\tau_{ij}(t) = \tau_{ij}(t)(1 - \rho),$$

где τ_{ij} – значение концентрации феромона на ребре, соединяющем вершины *i* и *j*; ρ – коэффициент испарения; *t* – номер шага.

8. После переопределения количества феромона производится возврат муравьев в начальные позиции и определение вероятностей размещения символа *k* в позиции *i* по формуле:

$$P_{ik} = F_{ik} \Big/ \sum_{i=1}^{n} F_{ik}.$$

По данным вероятностям осуществляется построение матрицы вероятностей размещения.

9. В соответствии с вычисленными вероятностями P_{ik} формируется *dm* новых маршрутов ($d < 1$), для которых определяются критерии $R_{m+1}, \ldots, R_{m+md}$. Если оптимальное значение критерия не изменяется в течение достаточно большого количества циклов, то поиск завершается с найденным значением P_{opt}, в противном случае – провести селекцию индивидуумов и возврат к шагу 2 алгоритма.

В данном алгоритме операторы 1–4, 9 соответствуют операторам генетического алгоритма, обеспечивая формирование пространства решений и глобальный поиск, операторы 5–8 соответствуют операторам алгоритма муравьиных колоний и обеспечивают локальный поиск в пространстве решений.

В [11] показано, что комбинирование генетического и муравьиного алгоритмов на основе применения генетических операций кроссинговера и мутации может очевидным образом повысить разнообразие эволюционного материала в популяции, увеличивая в ряде случаев скорость сходимости к глобальному оптимуму, отмечается также возможность применения некоторых специальных операторов генетического алгоритма, таких как *транслокация, сегрегация, оператор вставки, редукция, рекомбинация.*

Параллельный комбинированный алгоритм. Исследование возможности параллельной реализации комбинированных методов оптимизации, оценки их эффективности и необходимого числа процессоров является очередной задачей повышения эффективности решения оптимизационных проблем. Ранее данная задача решалась в [3], [15]–[17]. Отметим основные этапы, выполняемые параллельно на глобальном уровне [20]:

– параллельное формирование *m* вариантов маршрутов муравьев;

– параллельное вычисление целевых функций пригодности маршрутов муравьев и умножение на весовой коэффициент *Q*;

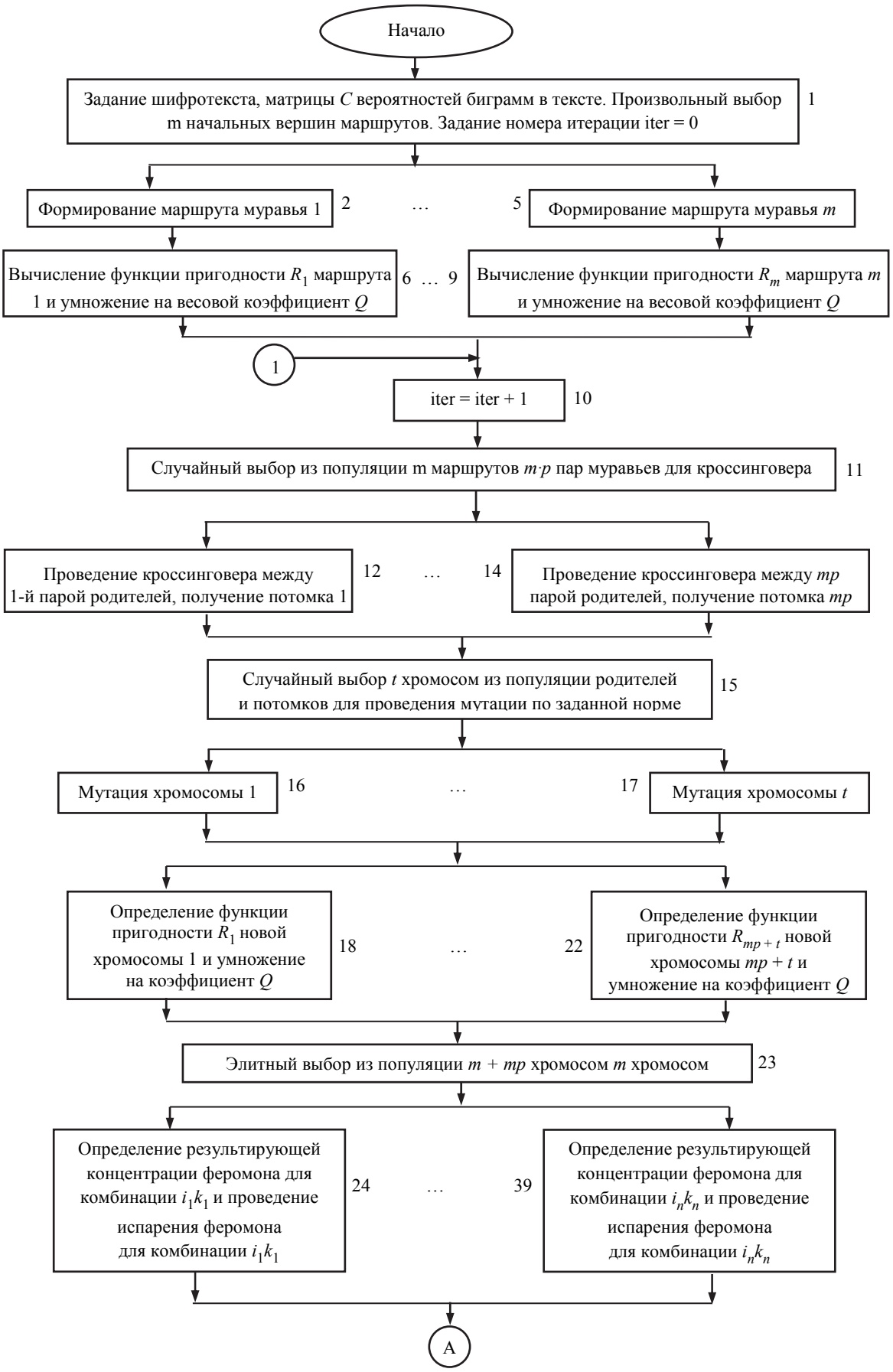
– параллельная реализация операций кроссинговера для случайно выбранных маршрутов муравьев, получение маршрутов-потомков;

– параллельная реализация операций мутации для случайно выбранных маршрутов муравьев, получение маршрутов-потомков; параллельное вычисление целевых функций пригодности маршрутов-потомков и умножение на весовой коэффициент *Q*;

– формирование матрицы результирующих концентраций феромона путем параллельного определения каждого элемента матрицы;

– проведение испарения феромона путем параллельного определения значения каждого элемента матрицы;

– формирование матрицы вероятности размещения символов в позиции путем параллельного определения каждого столбца матрицы;


Начало
Задание шифротекста, матрицы C вероятностей биграмм в тексте. Произвольный выбор m начальных вершин маршрутов. Задание номера итерации iter = 0
1
Формирование маршрута муравья 1
2
…
5
Формирование маршрута муравья m
Вычисление функции пригодности R_1 маршрута 1 и умножение на весовой коэффициент Q
6 … 9
Вычисление функции пригодности R_m маршрута m и умножение на весовой коэффициент Q
1
iter = iter + 1
10
Случайный выбор из популяции m маршрутов m·p пар муравьев для кроссинговера
11
Проведение кроссинговера между 1-й парой родителей, получение потомка 1
12
…
14
Проведение кроссинговера между mp парой родителей, получение потомка mp
Случайный выбор t хромосом из популяции родителей и потомков для проведения мутации по заданной норме
15
Мутация хромосомы 1
16
…
17
Мутация хромосомы t
Определение функции пригодности R_1 новой хромосомы 1 и умножение на коэффициент Q
18
…
22
Определение функции пригодности R_{mp+t} новой хромосомы mp + t и умножение на коэффициент Q
Элитный выбор из популяции m + mp хромосом m хромосом
23
Определение результирующей концентрации феромона для комбинации i_1k_1 и проведение испарения феромона для комбинации i_1k_1
24
…
39
Определение результирующей концентрации феромона для комбинации i_nk_n и проведение испарения феромона для комбинации i_nk_n
A

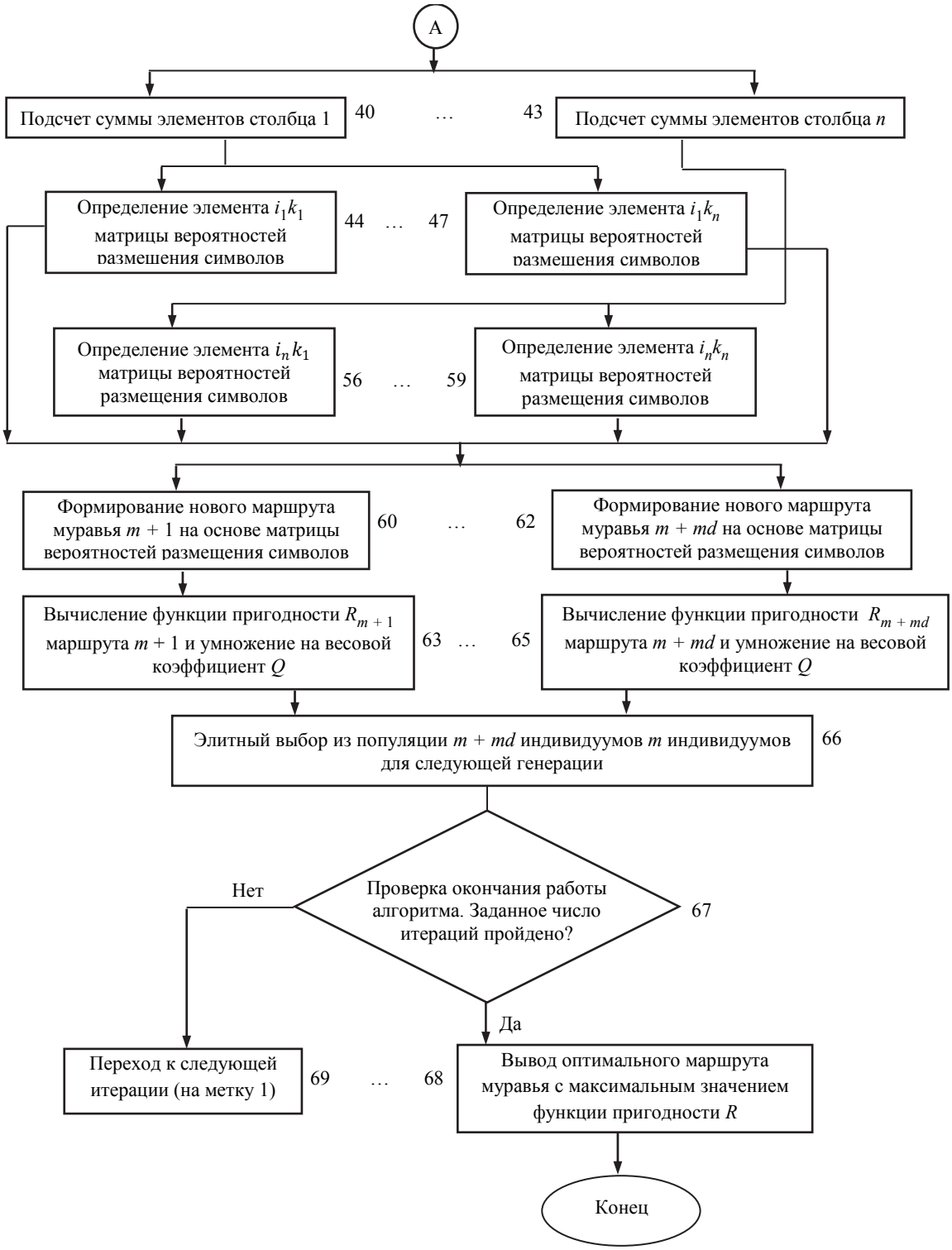


Рис. 1

– параллельное формирование *dm* вариантов маршрутов муравьев;

– параллельное вычисление целевых функций пригодности сформированных *dm* маршрутов муравьев и умножение на весовой коэффициент *Q*.

Таким образом, с учетом данных параллельно выполняемых этапов структурную схему комбинированного алгоритма можно представить в виде, показанном на рис. 1.

По аналогии с [3], [15]–[17] для данной структурной схемы составим информационно-логическую граф-схему алгоритма, показанную на рис. 2. Связи по управлению показаны двойной линией, по информации – одинарной линией.

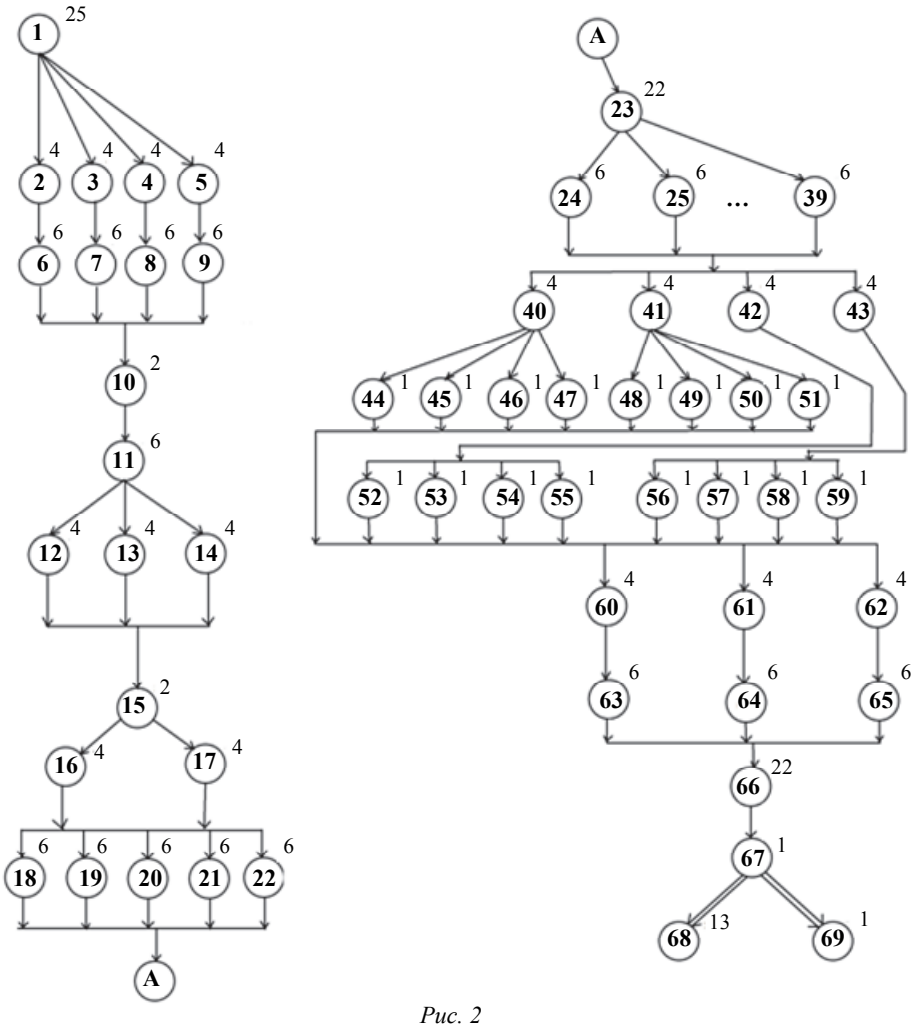


Рис. 2

Далее будем предполагать, что число маршрутов m = 4, длина маршрута (число символов) n = 4, число потомков mp = 3, число хромосом, подвергающихся мутации t = 2, параметр d = 0.9 (dm = = 3,6; число новых маршрутов равно 3).

Для дальнейшего определения множества независимых операторов, допускающих параллельное выполнение, будем, как и ранее, использовать методы, описанные в [18]. Для данного графа введем в рассмотрение матрицу следования S. Элемент S_{ij} = *, если существует связь по управлению, и S_{ij} = 1, если существует связь по информации. Как следует из рис. 2, матрица следования S будет содержать следующие ненулевые элементы:

$$S(2,1) = \ldots = S(5,1) = S(6,2) = S(7,3) = S(8,4) =$$
$$= S(9,5) = S(10,6) = \ldots = S(10,9) = S(11,10) =$$
$$= S(12,11) = \ldots = S(14,11) = S(15,12) = \ldots =$$
$$= S(15,14) = S(16,15) = S(17,15) =$$
$$= S(18,16) = \ldots = S(22,16) = S(18,17) = \ldots =$$
$$= S(22,17) = S(23,18) = \ldots = S(23,22) =$$
$$= S(24,23) = \ldots = S(39,23) = S(40,24) = \ldots =$$
$$= S(40,39) = S(41,24) = \ldots =$$
$$= S(41,39) = S(42,24) = \ldots = S(42,39) =$$
$$= S(43,24) = \ldots = S(43,39) = S(44,40) = \ldots =$$
$$= S(47,40) = S(48,41) = \ldots =$$
$$= S(51,41) = S(52,42) = \ldots = S(55,42) =$$
$$= S(56,43) = \ldots = S(59,43) = S(60,44) = \ldots =$$
$$= S(60,59) = S(61,44) = \ldots =$$
$$= S(61,59) = S(62,44) = \ldots = S(62,59) =$$
$$= S(63,60) = S(64,61) = S(65,62) = S(66,63) = \ldots$$
$$= S(66,65) = S(67,66) = 1; S(68,67) = S(69,67) = *.$$

Затем матрица S дополняется транзитивными связями с использованием алгоритмов, приведенных в [18].

Далее аналогично [3], [15]–[17] формируется симметричная матрица следования S'.

Введем в рассмотрение матрицу L логической несовместимости операторов. Данная матрица будет содержать 2 ненулевых элемента, соответствующих логически несовместимым операторам: $L(68, 69) = L(69, 68) = 1$. Путем дизъюнктивного сложения этих матриц S' и L формируется матрица независимости M.

По данной матрице M можно очевидным образом определить множества операторов алгоритма, которые допускают параллельное выполнение. Размерность максимального внутренне устойчивого множества определяет максимальное число процессоров, используемых для реализации алгоритма. Отметим, что данная матрица независимости M приведена в [20].

Оценка необходимого числа процессоров. Как отмечалось в [3], для повышения быстродействия и эффективности алгоритма за счет минимизации времени работы T возможна организация процесса распараллеливания как на глобальном уровне (параллельная обработка P элементов популяции на n процессорах), так и на локальном (параллельная реализация процесса оценки одного элемента популяции). Таким образом, для повышения эффективности реализации алгоритма на локальном уровне также актуальной является задача: для алгоритма криптоанализа на основе построенного информационно-логического графа G и для заданного времени $T_{зад}$ найти необходимое наименьшее число процессоров однородной вычислительной системы и определить план выполнения операторов на них.

Для решения данной задачи возможно использование методов, описанных в [18]. При этом в качестве времени $T_{зад}$ примем время $T_{кр}$ – длину критического пути в информационно-логическом графе G. На первоначальном этапе решения данной задачи при рассмотрении однородных вычислительных систем необходимо определение скалярных весов вершин в информационно-логическом графе, отражающих время выполнения операторов, составляющих схему на рис. 2. Для определения данного времени воспользуемся основными правилами анализа программ, описанными в [19], которые определяют время выполнения операторов присваивания, чтения, записи (O(1)), время выполнения последовательности операторов (правило сумм). Веса операторов, показывающие время их выполнения и определенные в соответствии с основными правилами анализа программ, описанными [19], приведены на рис. 2. Данные веса определены в соответствии с отмеченными ранее допущениями, что число маршрутов $m = 4$, длина маршрута (число символов в маршруте) $n = 4$, число потомков $mp = 3$, число хромосом, подвергающихся мутации $t = 2$, параметр $d = 0.9$ (число новых маршрутов равно 3). Вершине 1 присваивается вес $V(1) = 25$ ($n + nn + m + 1$); для вершин 2–5 $V(2) = \ldots = V(5) = 4$ (длина маршрута n); для вершин 6–9 $V(6) = \ldots = V(9) = 6$ (длина маршрута n, а также операции умножения и присваивания); для вершины 10 $V(10) = 2$ (операции сложения и присваивания); для вершины 11 $V(11) = 6$ (mp пар родителей); для вершин 12–14 $V(12) = \ldots = V(14) = 4$ (длина маршрута n); для вершины 15 $V(15) = 2$ (число хромосом, подвергающихся мутации t); для вершин 16–17 $V(16) = V(17) = 4$ (длина маршрута n); для вершин 18–22 $V(18) = \ldots = V(22) = 6$ (длина маршрута n, а также операции умножения и присваивания); для вершины 23 $V(23) = 22$ (последовательный просмотр $m + mp$, $m + mp - 1$, $m + mp - 2$, ..., m элементов популяции); для вершин 24–39 $V(24) = \ldots = V(39) = 6$ (длина маршрута n, а также операции умножения и присваивания); для вершин 40–43 $V(40) = \ldots = V(43) = 4$ (число элементов столбца матрицы результирующей концентрации феромона); для вершин 44–59 $V(44) = \ldots = V(59) = 1$ (определение элемента матрицы вероятностей размещения символов); для вершин 60–62 $V(60) = \ldots = V(62) = 4$ (длина маршрута n); для вершин 63–65 $V(63) = \ldots = V(65) = 6$ (длина маршрута n, а также операции умножения и присваивания); для вершины 66 $V(66) = 22$ (последовательный просмотр $m+md$, $m + md - 1$, $m + m - 2$, ..., m элементов популяции); для вершины 67 $V(67) = 1$ (проверка выполнения условия логического оператора); для вершины 68 $V(68) = 13$ (последовательный просмотр m, $m - 1$, $m - 2$, ... элементов популяции значений целевой функции и вывод n элементов оптимального маршрута); для вершины 69 $V(69) = 1$ (переход к следующей итерации).

Критический путь в графе $T_{кр} = 138$. Он проходит, например, через вершины 1-2-6-10-11-12-15-16-18-23-24-40-44-60-63-66-67-68.

Предполагая, что $T_{зад} = T_{кр}$ для представленного на рис. 2 информационно-логического графа и матрицы следования, найдем ранние τ_{pi} и поздние сроки τ_{ni} окончания выполнения операторов.

Ранние сроки:

$$\tau_{p1}=25,\ \tau_{p2}=\tau_{p3}=\tau_{p4}=\tau_{p5}=29,\ \tau_{p6}=$$
$$=\tau_{p7}=\tau_{p8}=\tau_{p9}=35,\ \tau_{p10}=37,\ \tau_{p11}=43,$$
$$\tau_{p12}=\tau_{p13}=\tau_{p14}=47,\ \tau_{p15}=49,\ \tau_{p16}=\tau_{p17}=53,$$
$$\tau_{p18}=\tau_{p19}=\tau_{p20}=\tau_{p21}=\tau_{p22}=59,$$
$$\tau_{p23}=81,\ \tau_{p24}=\ \tau_{p25}=\tau_{p26}=\tau_{p27}=\tau_{p28}=$$
$$=\tau_{p29}=\tau_{p30}=\tau_{p31}=\tau_{p32}=\tau_{p33}=\tau_{p34}=$$
$$=\tau_{p35}=\tau_{p36}=\tau_{p37}=\tau_{p38}=\tau_{p39}=87,$$
$$\tau_{p40}=\tau_{p41}=\tau_{p42}=\tau_{p43}=91,$$
$$\tau_{p44}=\tau_{p455}=\tau_{p46}=\tau_{p47}=\tau_{p48}=\tau_{p49}=$$
$$=\tau_{p50}=\tau_{p51}=\tau_{p52}=\tau_{p53}=\tau_{p54}=\tau_{p55}=$$
$$=\tau_{p56}=\tau_{p57}=\tau_{p58}=\tau_{p59}=92,\ \tau_{p60}=\tau_{p61}=$$
$$=\tau_{p62}=96,\ \tau_{p63}=\tau_{p64}=\tau_{p65}=102,$$
$$\tau_{p66}=124,\ \tau_{p67}=125,\ \tau_{p68}=138,\ \tau_{p69}=126.$$

Поздние сроки:

$$\tau_{n69}=138,\ \tau_{n68}=138,\ \tau_{n67}=125,\ \tau_{n66}=124,$$
$$\tau_{n63}=\tau_{n64}=\tau_{n65}=102,\ \tau_{n60}=\tau_{n61}=\tau_{n62}=96,$$
$$\tau_{n44}=\ \tau_{n45}=\tau_{n46}=\tau_{n47}=\tau_{n48}=\tau_{n48}=\tau_{n50}=$$
$$=\tau_{n51}=\tau_{n52}=\tau_{n53}=\tau_{n54}=\tau_{n55}=\tau_{n56}=$$
$$=\tau_{n57}=\tau_{n58}=\tau_{n59}=92,\ \tau_{n40}=\tau_{n41}=\tau_{n42}=$$
$$=\tau_{n43}=91,\ \tau_{n24}=\tau_{n25}=\tau_{n26}=\tau_{n27}=\tau_{n28}=$$
$$=\tau_{n29}=\tau_{n30}=\tau_{n31}=\tau_{n32}=\tau_{n33}=\tau_{n34}=\tau_{n35}=$$
$$=\ \tau_{n36}=\tau_{n37}=\tau_{n38}=\tau_{n39}=87,\ \tau_{n23}=81,$$
$$\tau_{n18}=\tau_{n19}=\tau_{n20}=\tau_{n21}=\tau_{n22}=59,\ \tau_{n16}=$$
$$=\tau_{n17}=53,\ \tau_{n15}=49,\ \tau_{n12}=\tau_{n13}=\tau_{n14}=47,$$
$$\tau_{n11}=43,\ \tau_{n10}=37,\ \tau_{n6}=\tau_{n7}=\tau_{n8}=\tau_{n9}=35,$$
$$\tau_{n2}=\tau_{n3}=\tau_{n4}=\tau_{n5}=29,\ \tau_{n1}=25.$$

На основе значений τ_{pi} и τ_{ni} найдем оценку минимального числа процессоров для выполнения алгоритма за время $T_{\text{кр}}$ путем построения диаграмм ранних и поздних сроков окончания выполнения операторов и находя такое распределение временных границ операторов для всех внутренне устойчивых множеств графа G, при котором число используемых процессоров n минимально. Для этой цели, как и ранее, в матрице независимости, приведенной в [20], найдем внутренне устойчивые множества, представляющие множества взаимно независимых операторов (ВНО). Легко убедиться, что максимальными внутренне устойчивыми множествами являются множества:

(24, 25, 26, 27, 28, 29, 30, 31, 32,
33, 34, 35, 36, 37, 38, 39),
(44, 45, 46, 47, 48, 49, 50, 51, 52,
53, 54, 55, 56, 57, 58, 59).

Данные множества содержат $f = 16$ элементов, при этом, так как операторы, входящие в данные множества ВНО, имеют равные ранние и поздние сроки окончания выполнения (принадлежат критическому пути), то оценка числа процессоров $f = 16$, полученная для данных множеств, позволяет выполнить алгоритм криптоанализа за минимальное время $T_{\text{кр}}$ при отмеченных выше допущениях. Данная оценка является решением задачи, поскольку, в соответствии с [18], в матрице независимости нет множеств ВНО, содержащих число операторов r, для которых $r > f$.

Таким образом, отсюда очевидным образом следует утверждение.

При реализации описанного параллельного алгоритма криптоанализа, представленного информационно-логическим графом G на рис. 2 (в соответствии с технологией распараллеливания, описанной в [18]), необходимое минимальное число процессоров может быть определено как число элементов, составляющих максимальное множество ВНО, содержащее операторы с равными ранними и поздними сроками окончания (т. е. принадлежащими критическому пути). В графе G на рис. 2 такими множествами ВНО являются:

– множества ВНО (2, 3, 4, 5) и (6, 7, 8, 9) (число элементов равно числу маршрутов муравьев m);

– множество ВНО (12, 13, 14) (число элементов равно числу потомков, полученных после кроссинговера mp);

– множество ВНО (16, 17) (число элементов равно числу потомков мутирующих хромосом t);

– множество ВНО (18, 19, 20, 21, 22) (число элементов равно общему числу потомков, полученных после кроссинговера и мутации $mp + t$);

– множество ВНО (24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39) (число элементов равно общему числу элементов матрицы результирующих концентраций феромона $n \cdot n$);

– множество ВНО (40, 41, 42, 43) (число элементов равно общему числу столбцов матрицы результирующих концентраций феромона n);

– множество ВНО (44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59) (число элементов равно общему числу элементов матрицы вероятностей размещения символов nn);

– множества ВНО (60, 61, 62) и (63, 64, 65) (число элементов равно числу новых маршрутов муравьев *dm*).

Таким образом, для графа *G* на рис. 2 необходимое минимальное число процессоров может быть определено как max(*m*; *mp*; *t*; *mp* + *t*; *nn*; *dm*).

При этом время реализации алгоритма в общем случае может составить $T = QT_{кр}$, где Q – количество итераций, являющееся в общем случае случайной величиной, зависящей от выбора параметров алгоритма и статистических характеристик текста. $T_{кр}$ – длина критического пути в информационно-логическом графе *G*, определенная в соответствии с правилами анализа программ, описанными в [19].

Таким образом, в данной статье дана структурная схема комбинированного биоинспирированного алгоритма (генетический алгоритм и алгоритм муравьиных колоний), используемого для криптоанализа; определены основные параллельно выполняемые этапы алгоритма, и на их основе построена информационно-логическая граф-схема алгоритма; построены матрицы следования и независимости, позволяющие определить основные параллельно выполняемые операции алгоритма; приведена оценка числа процессоров, необходимых для реализации алгоритма.

Работа выполнена при финансовой поддержке РФФИ (проекты 17–01–00375, 18–01–00314).

СПИСОК ЛИТЕРАТУРЫ

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

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

3. Применение биоинспирированных методов оптимизации для реализации криптоанализа блочных методов шифрования / Ю. О. Чернышев, А. С. Сергеев, Е. О. Дубров, А. Н. Рязанов. Ростов-н/Д: Изд-во ДГТУ, 2016. 177 с.

4. Орловская Н. М. Анализ эффективности биоинспирированных методов глобальной оптимизации // Тр. МАИ: электрон. науч. журн. 2014. № 73. С. 4.

5. Чернышев Ю. О., Сергеев А. С., Дубров Е. О. Обзор алгоритмов решения задач криптоанализа на основе биоинспирированных технологий искусственного интеллекта // Вестн. Воронежского гос. ун-та. Сер. «Системный анализ и информационные технологии». 2014. № 2. С. 83–89.

6. Чернышев Ю. О., Сергеев А. С. Дубров Е. О. Информационная безопасность и биоинспирированные алгоритмы решения задач криптоанализа // Тр. Междунар. симп. «Надежность и качество–2014». Пенза: ПГУ, 2014. С. 342–346.

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

8. Муравьиные алгоритмы. URL: http://rain.ifmo.ru/cat/data/theory/unsorted/ant-algo-2006/article.pdf (дата обращения 29.03.2015).

9. Биоинспирированные методы криптоанализа асимметричных алгоритмов шифрования на основе факторизации составных чисел / А. С. Сергеев, О. П. Третьяков, А. Е. Васильев, Ю. О. Чернышев // Вестн. ДГТУ. 2011. Т. 11, № 9(60). С. 1544–1554.

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

11. Чернышев Ю. О., Сергеев А. С. Применение комбинированного биоинспирированного алгоритма (генетический алгоритм и алгоритм муравьиных колоний) для реализации криптоанализа шифров перестановок // Изв. СПбГЭТУ «ЛЭТИ». 2017. № 9. С. 33–44.

12. Сергеев А. С. Применение комбинированных биоинспирированных интеллектуальных технологий в задачах оптимизации для реализации криптоанализа классических систем шифрования // Математика, ее приложения и математическое образование (МПМО17): матер. VI Междунар. конф. Улан-Удэ: Изд-во ВСГУТУ, 2017. С. 327–332.

13. Чернышев Ю. О., Сергеев А. С. Применение комбинированных биоинспирированных алгоритмов для реализации криптоанализа симметричных алгоритмов шифрования // XX Междунар. конф. по мягким вычислениям и измерениям: сб. науч. тр. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2017. С. 497–500.

14. Сергеев А. С. Применение комбинированных биоинспирированных технологий искусственного интеллекта для реализации криптоанализа шифров замены // Наука и образование–2017: матер. Всерос. науч.-практ. конф., Мурманск, 27 марта 2017 г. Мурманск: Изд-во МГТУ, 2017. С. 96–102.

15. Чернышев Ю. О., Сергеев А. С., Капустин С. А. Исследование возможности применения методов эволюционной оптимизации для реализации криптоанализа блочных методов шифрования // Изв. СПбГЭТУ «ЛЭТИ». 2015. № 10. С. 32–40.

16. Исследование возможности применения генетических алгоритмов для реализации криптоанализа блочных криптосистем / Ю. О. Чернышев, А. С. Сергеев, Н. Н. Венцов и др. // Вестн. ДГТУ. 2015. № 3(82). С. 65–72.

17. Разработка и исследование параллельной модели алгоритмов пчелиных колоний для решения задач криптоанализа / Ю. О. Чернышев, А. С. Сергеев, А. Н. Рязанов, Е. О. Дубров // Вестн. ДГТУ. 2017. Т. 17, № 1(88). С. 144–159.

18. Сергеев А. С. Параллельное программирование. Ростов-н/Д: Издательский центр ДГТУ, 2002. 77 с.

19. Ахо Альфред В., Джон Ульман Джеффри Д. Структуры данных и алгоритмы. М.: Издательский дом «Вильямс», 2003. 384 с.

20. Сергеев А. С. Разработка параллельного комбинированного биоинспирированного метода (генетический алгоритм и алгоритм муравьиных колоний) для решения задач криптоанализа // Системный анализ в проектировании и управлении: сб. науч. тр. XXII Междунар. науч.-практ. конф. Ч. 1. СПб.: Изд-во Политехн. ун-та, 2018. С. 359–370.

Yu. O. Chernyshev, A. S. Sergeyev, A. N. Ryasanov
Don State technical university

RESEARCH AND DEVELOPMENT OF THE PARALLEL COMBINED BIOINSPIRED ALGORITHM FOR THE SOLUTION OF CRYPTANALYSIS TASKS

The cryptanalysis task with the use of a new model of optimizing strategy – the combined bioinspired algorithm is considered. Application of the combined bioinspired algorithm based on hybridization by an investment (a genetic algorithm and an algorithm of ant colonies) for implementing the cryptanalysis of shift codes is described. The description of the combined algorithm is provided, and it is shown that the probability of obtaining an optimal variant of the decision while applying the hybrid algorithms of cryptanalysis can't be less then the probability of obtaining an optimal solution when using the classical bioinspired algorithms. The description of the main operations enabling parallel performance at the global level is provided, as well as the block diagram of a parallel algorithm and the data-logical graph-scheme, and the description of the following matrix is given. On the basis of definition of the sets of mutually independent operators and a critical way in the graph the problem of determining the minimum number of processors for the realization of a parallel combined algorithm is solved.

Cryptanalysis, the combined bioinspired algorithms, hybridization by an investment, a genetic algorithm, an algorithm of ant colonies, the data-logical graph-scheme, a following matrix, an independence matrix

УДК 004.9

И. А. Щербаков
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

А. В. Пономарев
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

SemanTags: семантическая разметка объектов с использованием технологии краудсорсинга

Дополнение объектов (например, ресурсов сети Интернет) семантическими метками, характеризующими их содержание, позволяет существенно повысить качество выдачи поисковых машин и в целом способствует более эффективной работе с информацией. Однако полностью автоматическая семантическая разметка не всегда дает адекватный результат из-за существующих ограничений при алгоритмической обработке естественного языка, а ручная оказывается достаточно трудоемкой, особенно, если количество объектов велико. Частично снять проблему трудоемкости ручной разметки в ряде случаев позволяет технология краудсорсинга. В статье предлагается система (веб-сервис) SemanTags, позволяющая использовать технологию краудсорсинга для того, чтобы снабдить произвольные объекты (научные статьи, страницы в Интернете и пр.) метками (тегами), являющимися классами некоторой проблемно-ориентированной онтологии, записанной на языке OWL 2. Описана архитектура и особенности реализации системы, а также предложен новый механизм обеспечения качества, адаптированный для совместной разметки объектов классами онтологии.

Краудсорсинг, крауд-вычисления, онтологии, OWL 2, таксономия, семантическая разметка, семантический поиск

Семантический поиск информации, т. е. поиск, при котором происходит анализ не только синтаксических конструкций, описывающих ресурсы (непосредственно термов языка), но и се-