УДК 004.056.55

РАЗРАБОТКА И ИССЛЕДОВАНИЕ ПАРАЛЛЕЛЬНОГО КОМБИНИРОВАННОГО БИОИНСПИРИРОВАННОГО МЕТОДА (ГЕНЕТИЧЕСКИЙ АЛГОРИТМ И АЛГОРИТМ ПЧЕЛИНЫХ КОЛОНИЙ) ДЛЯ РЕАЛИЗАЦИИ КРИПТОАНАЛИЗА СИММЕТРИЧНЫХ СИСТЕМ ШИФРОВАНИЯ

Ю. О. Чернышев*, А. С. Сергеев*, П. А. Панасенко**

**Донской государственный технический университет*
***Краснодарское высшее военное училище им. генерала армии С. М. Штеменко*

Поступила в редакцию 18.04.2019 г.

Аннотация. Рассматривается задача криптоанализа симметричных систем шифрования с использованием новой модели оптимизационных стратегий – комбинированного биоинспирированного алгоритма. Описано применение комбинированного биоинспирированного алгоритма на основе гибридизации вложением (генетический алгоритм и алгоритм пчелиных 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.
Ключевые слова: криптоанализ, комбинированные биоинспирированные алгоритмы, гибридизация вложением, генетический алгоритм, алгоритм пчелиных колоний, информационно-логическая граф-схема, матрица следования, матрица независимости.

1. ВВЕДЕНИЕ

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 течение последних лет были предложены разнообразные схемы эволюционных вычислений: генетический алгоритм, генетическое программирование, эволюционные стратегии, эволюционное программирование, модели поведения роя пчел, стаи птиц и колонии муравьев, модели отжига и другие конкурирующие эвристические алгоритмы [1]. В [2] авторами рассматривалось решение задач криптоанализа, относящихся к переборным задачам с экспоненциальной временной сложностью: традиционных симметричных криптосистем, использующих шифры перестановки и замены, а также шифров гаммирования с применением генетических алгоритмов, в [3] – симметричных и ассиметричных криптосистем с использованием биоинспирированных алгоритмов муравьиных и пчелиных колоний. В [4–6] исследована возможность применения методов генетического поиска для реализации криптоанализа блочных криптосистем. Поскольку данные

задачи криптоанализа в большинстве случаев являются NP-полными и имеют комбинаторную сложность, то, как отмечено в [1], основным мотивом для разработок новых алгоритмов решения комбинаторных задач являются возникшие потребности в решении задач большой и очень большой размерности.

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 [3]. Поэтому актуальной является задача исследования и разработки эвристических алгоритмов, являющихся аналогами природных систем, в которых осуществляется поэтапное построение решения задачи. В данной работе разработан 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 комбинированного биоинспирированного алгоритма (где в качестве популяционного алгоритма используется генетический алгоритм, а в качестве алгоритма локального поиска – алгоритм муравьиных колоний), а также его параллельной версии рассматривалась в работах [7, 18, 19].

2. ПОСТАНОВКА ЗАДАЧИ, ОПИСАНИЕ КОМБИНИРОВАННОГО АЛГОРИТМА

Описание возможного применения алгоритма пчелиных колоний для задач криптоанализа (на основе сведения ее к квадратичной задаче о назначениях) приведено в [3, 8], где также приведен демонстрационный пример реализации алгоритма. Структурная схема пчелиного алгоритма решения задач криптоанализа представлена в [9]. Описание применения генетического алгоритма для реализации криптоанализа классических шифров перестановок наряду с экспериментальными результатами дано в [2]. Здесь же приводится описание основных операций и схема реализации алгоритма.

В связи с этим возникает вопрос о возможности применения комбинированных биоинспирированных алгоритмов для реализации криптоанализа, в частности, о возможности разработки алгоритмов, сочетающих основные черты генетических и пчелиных алгоритмов. В этом плане отметим работу [10], посвященную разработке популяционных алгоритмов оптимизации (в том числе гибридизации вложением популяционных алгоритмов), в которой отмечается, что в гибридных алгоритмах, объединяющих различные либо однотипные алгоритмы, но с различными значениями параметров, преимущества одного алгоритма могут компенсировать недостатки другого.

Комбинированный алгоритм пчелиных колоний. Несмотря на широкую область применимости эволюционных алгоритмов, они обладают рядом недостатков (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 [3, 4, 8]. В соответствии с [4, 16] временная сложность пчелиных алгоритмов T составляет $T \approx O(n^{\lg n})$, в лучшем случае $T \approx O(n^3)$.

Отметим, что разработке комбинированного биоинспирированного алгоритма, в котором используются операторы пчелиного алгоритма, осуществляющие глобальный поиск, и операторы генетического алгоритма, осуществляющие локальный поиск, посвящена работа [11]. Будем предполагать, что пространство поиска, в котором размещены символы алфавита шифртекста, представляет собой прямоугольную матрицу A размером $m \times m$ (m – число символов текста). Используя терминологию и обозначения, введенные в [3, 4], основные операции гибридного алгоритма криптоанализа, представленного в [11, 12, 13] и разработанного на основе методов,

описанных в [16, 17], сформулируем в следующей форме.

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 $2,3,\cdots,L$; 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 целевой функции (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. Выбрать базовую позицию $a_i \in A_b$.

7. Выбрать позицию $a_s(l)$, расположенную в окрестности базовой позиции a_i, не совпадающую с ранее выбранными на данной итерации позициями, и соответствующее решение (список 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 $P_{кросс}$, получение заданного количества потомков (формирование расширенной популяции).

11. Провести операцию мутации индивидуумов популяции на основе заданной нормы мутации $n_{мут}$, 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), $l=l+1$ (перейти к следующей итерации), перейти к п. 17, иначе к п. 21.

17. Начать формирование множества базовых позиций для следующей итерации. Во множество A_{b1} включается n_{b1} 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^*.

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. Демонстрационный пример реализации «гибридного» алгоритма приведен в [11].

Отметим, что ранее в [11] 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 $П$ – группа операторов комбинированного алгоритма, соответствующая операторам алгоритма пчелиных колоний (операторы 1–9, 17–21), $Г$ – группа операторов, соответствующая операторам генетического алгоритма (операторы 10–16). Пусть $P(П)$ – вероятность того, что при реализации пчелиного алгоритма на итерации i получено решение, лучшее, чем на итерации $i-1$. Аналогично, пусть $P(Г)$ – 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 P получения на i итерации частичного решения, лучшего, чем на $i-1$ итерации, составит $P = P(П) + P(Г) - P(П)\cdot P(Г)$. Поскольку все значения P, $P(П)$, $P(Г)$ удовлетворяют условию $0 \le P \le 1$, $0 \le P(П) \le 1$, $0 \le P(Г) \le 1$, то, очевидно, произведение $P(П)\cdot P(Г)$ будет удовлетворять условию $P(П)\cdot P(Г) \le \min(P(П), P(Г))$. В то же время имеет место очевидное соотношение $P(П) + P(Г) \ge \max(P(П), P(Г))$. Отсюда следует, что будет иметь место соотношение $P = P(П) + P(Г) - P(П)\cdot P(Г) \ge \max(P(П), P(Г))$.

Таким образом, показано (как и ранее в [11]), что при реализации комбинированного биоинспирированного алгоритма вероятность P улучшения частичного решения на i итерации по сравнению с $i-1$ итерацией удовлетворяет условию $P \ge \max(P_1, P_2)$, где P_1, P_2 – вероятности улучшения частичного решения при использовании классических биоинспирированных алгоритмов. При этом увеличение вероятности может быть определено из соотношения $P = P_1 + P_2 - P_1\cdot P_2$. 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. Данные рассуждения справедливы для любого числа n биоинспирированных алгоритмов и вероятностей $P_1, P_2 \ldots P_n$.

3. ПАРАЛЛЕЛЬНЫЙ КОМБИНИРОВАННЫЙ АЛГОРИТМ

Одной из актуальных на сегодняшний день задач является исследование возможности параллельной реализации комбинированных алгоритмов оптимизации, оценки их эффективности и необходимого числа процессоров. Данная задача решалась, например, в [4, 9]. На первоначальном этапе отметим этапы, выполняемые параллельно на глобальном уровне [13]:

– параллельное размещение n_r пчел-разведчиков в пространстве поиска;

– параллельный выбор базовых позиций, позиций в их окрестности, получение решений E_s и соответствующих значений ЦФ R каждым агентом-фуражиром;

– параллельная реализация операций кроссинговера для случайно выбранных списков, получение заданного количества потомков;

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

– параллельное размещение случайным образом n_{rl} агентов для выбора n_{rl} позиций в пространстве поиска, параллельный выбор этих позиций.

Таким образом, с учетом данных параллельно выполняемых этапов может быть составлена структурная схема комбинированного алгоритма, показанная на рис. 1 (аналогично схеме, приведенной в [9]).

Для дальнейшего определения множества независимых операторов, допускающих параллельное выполнение, возможно, аналогично [4, 9], использовать методы, описанные в [14]. Для структурной схемы комбинированного алгоритма составляется информационно-логическая граф-схема G, в которой отображаются связи по управлению (двойная стрелка) и по информации (одинарная стрелка) (рис. 2). При проведении исследований использовались допущения (аналогично [9]), что максимальный размер популяции $M = 10$, число пчел-разведчиков $n_r = 5$, число базовых позиций $n_b = 4$, количество агентов-фуражиров $n_f = 5$; число потомков после кроссинговера $M \cdot P_{кросс} = 4$; число хромосом, подвергающихся мутации, $M \cdot n_{мут} = 3$; длина строки текста (максимальная длина списка) $E_{макс} = 12$; $n_{b1} = 2$ – количество базовых позиций, формируемых из лучших позиций a^*, найденных на $l-1$ итерации; $n_{rl} = 4$ – количество агентов-разведчиков, выбирающих случайным образом новые позиции на итерациях $2,3,\ldots,L$; $n_{b2} = 2$ – количество базовых позиций, формируемых из n_{rl} новых лучших позиций, найденных агентами-разведчиками на l итерации.

Далее в соответствии с [14] вводится в рассмотрение матрица следования S. В соответствии с [14] элемент $S(i, j) = *$, если существует связь по управлению от j к i, и $S(i, j) = 1$, если существует связь по информации от j к i (рис. 3).

Далее с использованием методов, описанных в [14], матрица следования S дополняется транзитивными связями, при этом все элементы, не равные 0, полагаются равными $S(i, j) = 1$. В соответствии с методами, описанными в [14], формируется симметричная матрица следования S', а также вводится в рассмотрение матрица L логической несовместимости операторов. Данная матрица L содержит следующие ненулевые элементы, соответствующие логически несовместимым операторам:

$$L(38,39) = L(39,38) = 1,$$
$$L(41,42) = L(41,43) = L(41,44) =$$
$$= \cdots = L(41,50) = 1,$$
$$L(42,41) = L(43,41) = L(44,41) =$$
$$= \ldots = L(50,41) = 1.$$

Путем дизъюнктивного сложения матриц S' и L формируется матрица независимости $M_{нез}$ (рис. 4).По данной матрице независимости $M_{нез}$ можно, очевидным образом, определить множества операторов алгоритма, которые допускают параллельное выполнение. Размерность максимального внутренне устойчивого множества определяет максимальное число процессоров, используемых для реализации алгоритма.

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) [4]. Для повышения эффективности реализации алгоритма на локальном уровне в соответствии с [4] 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, как и ранее в [4], возможно использование методов, описанных в [14]. При этом в качестве времени $T_{зад}$ примем, как и ранее, время $T_{кр}$ – длину критического пути в информационно-логическом графе G. На первоначальном этапе при рассмотрении однородных вычислительных систем необходимо определение скалярных весов вершин в информационно-логическом графе, отражающих время выполнения операторов.

Как и в [4, 9], для решения данной задачи использовались методы, описанные в [14, 15].

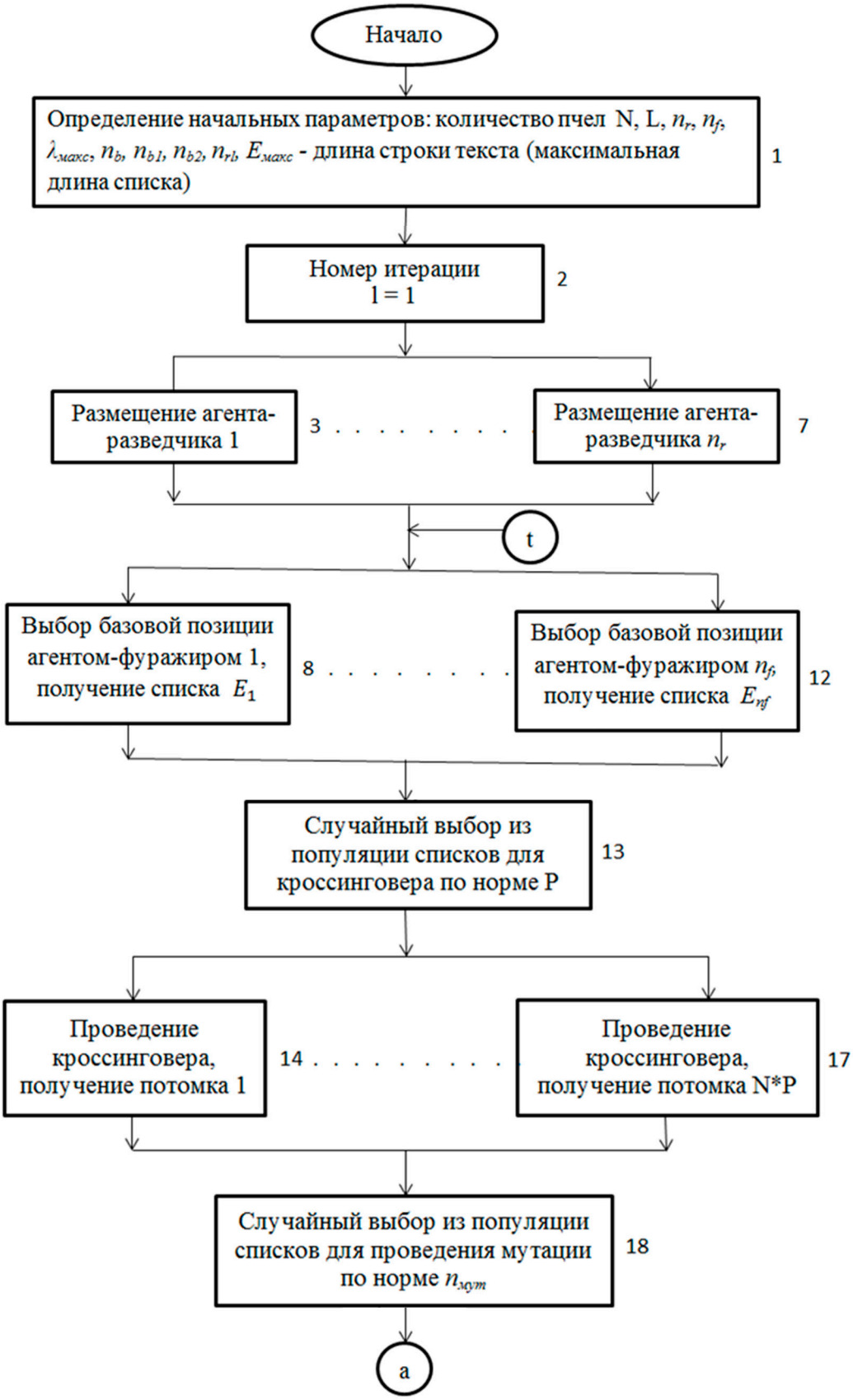

Рис. 1. Структурная схема параллельного комбинированного алгоритма криптоанализа (генетический алгоритм и алгоритм пчелиных колоний)

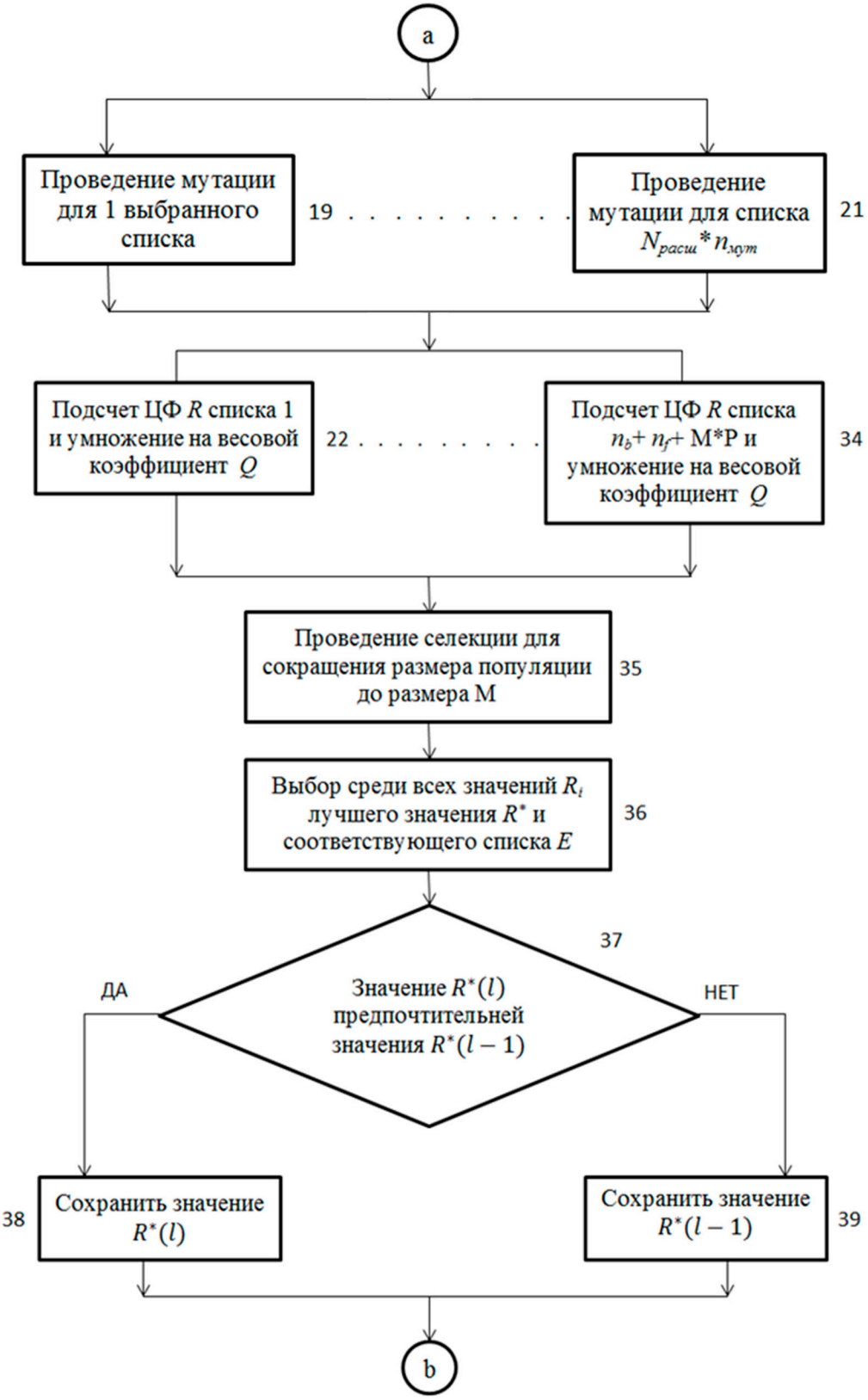

Рис. 1 (продолжение)

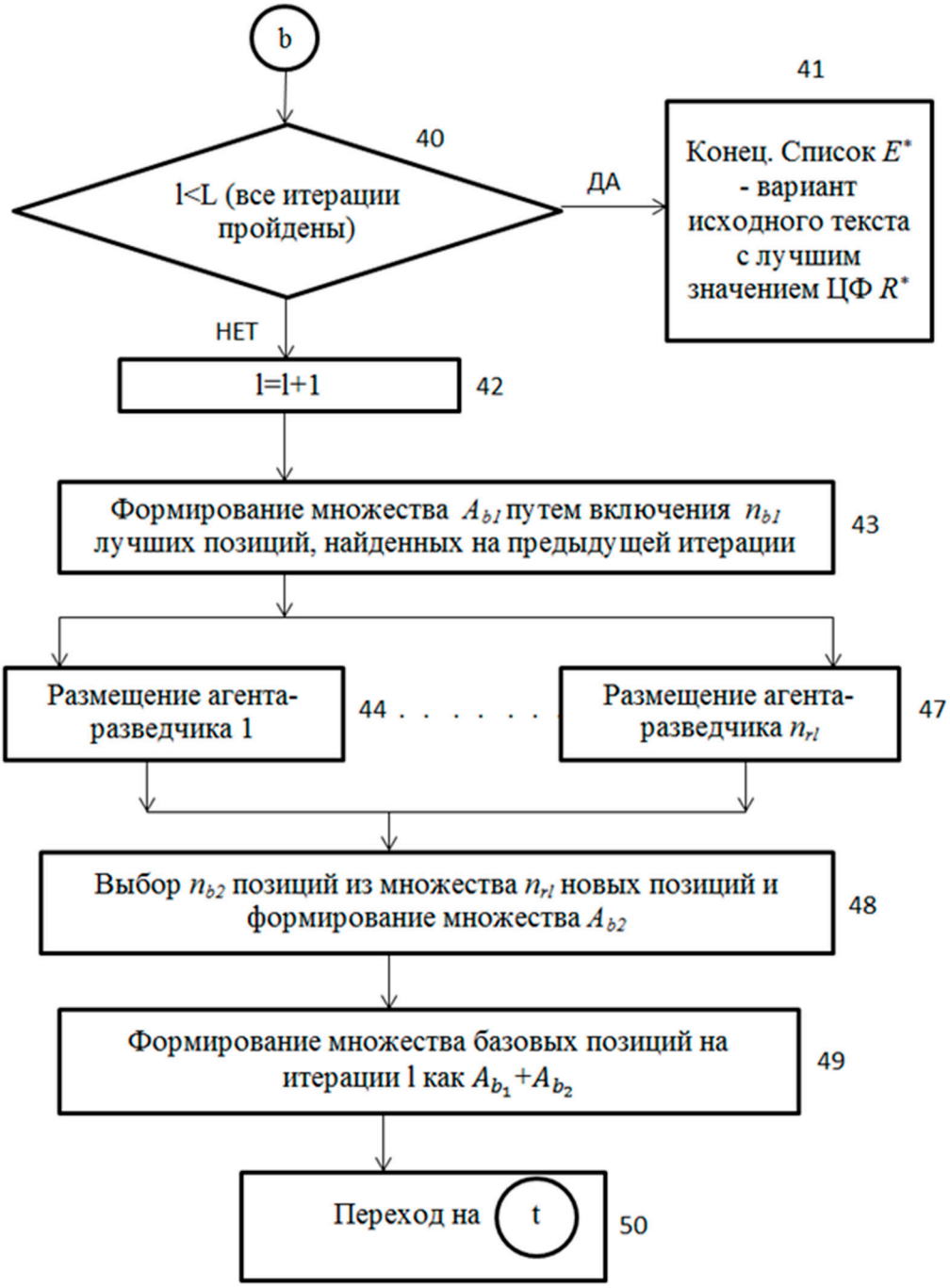

Рис. 1 (окончание)

Для информационно-логического графа G были определены следующие веса вершин:

$$G_1 = 10;\ G_2 = 1;\ G_3 = G_4 = G_5 = G_6 = G_7 = 1;$$
$$G_8 = G_9 = G_{10} = G_{11} = G_{12} = 4;\ G_{13} = 2;$$
$$G_{14} = G_{15} = G_{16} = G_{17} = 12;\ G_{18} = 3;$$
$$G_{19} = G_{20} = G_{21} = 12;$$
$$G_{22} = G_{23} = G_{24} = G_{25} = G_{26} =$$
$$= G_{27} = G_{28} = G_{29} = G_{30} = G_{31} =$$
$$= G_{32} = G_{33} = G_{34} = 14;\ G_{35} = 36;\ G_{36} = 10;$$
$$G_{37} = G_{38} = G_{39} = G_{40} = 1;\ G_{41} = 12;\ G_{42} = 1;$$
$$G_{43} = 19;\ G_{44} = G_{45} = G_{46} = G_{47} = 1;\ G_{48} = 2;$$
$$G_{49} = 4;\ G_{50} = 1.$$

Данные веса определялись в соответствии с отмеченными выше допущениями, что максимальный размер популяции $M = 10$, $n_r = 5$, $n_b = 4$, $n_f = 5$; $M \cdot P_{кросс} = 4$; $M \cdot n_{мут} = 3$;

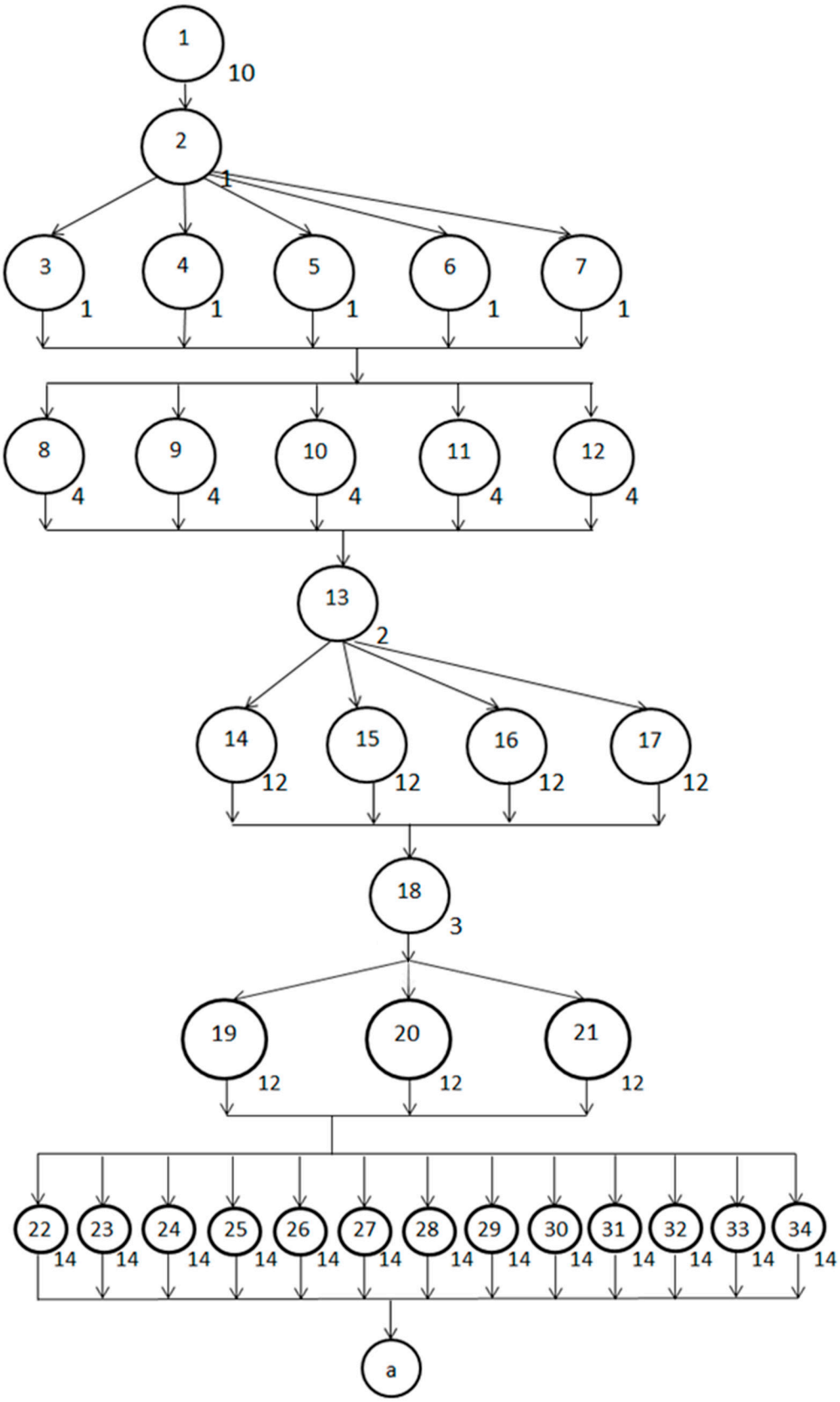

Рис. 2. Информационно-логическая граф-схема комбинированного алгоритма криптоанализа

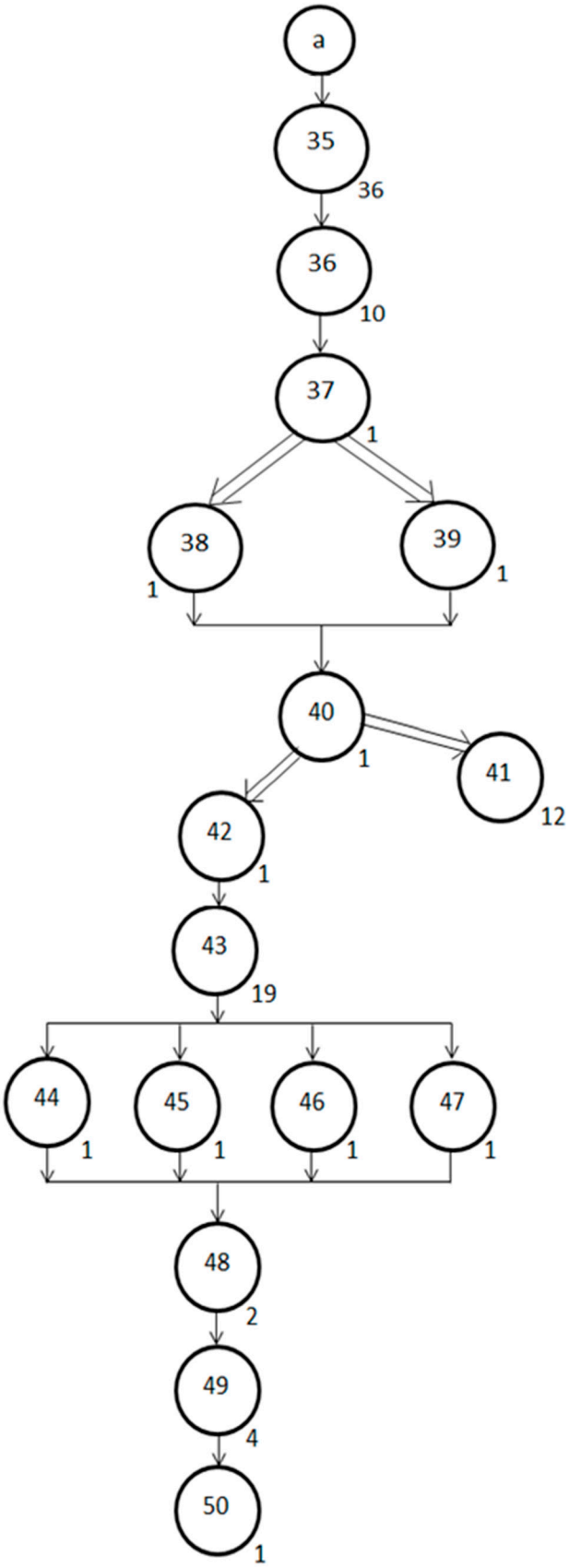

Рис. 2 (окончание)

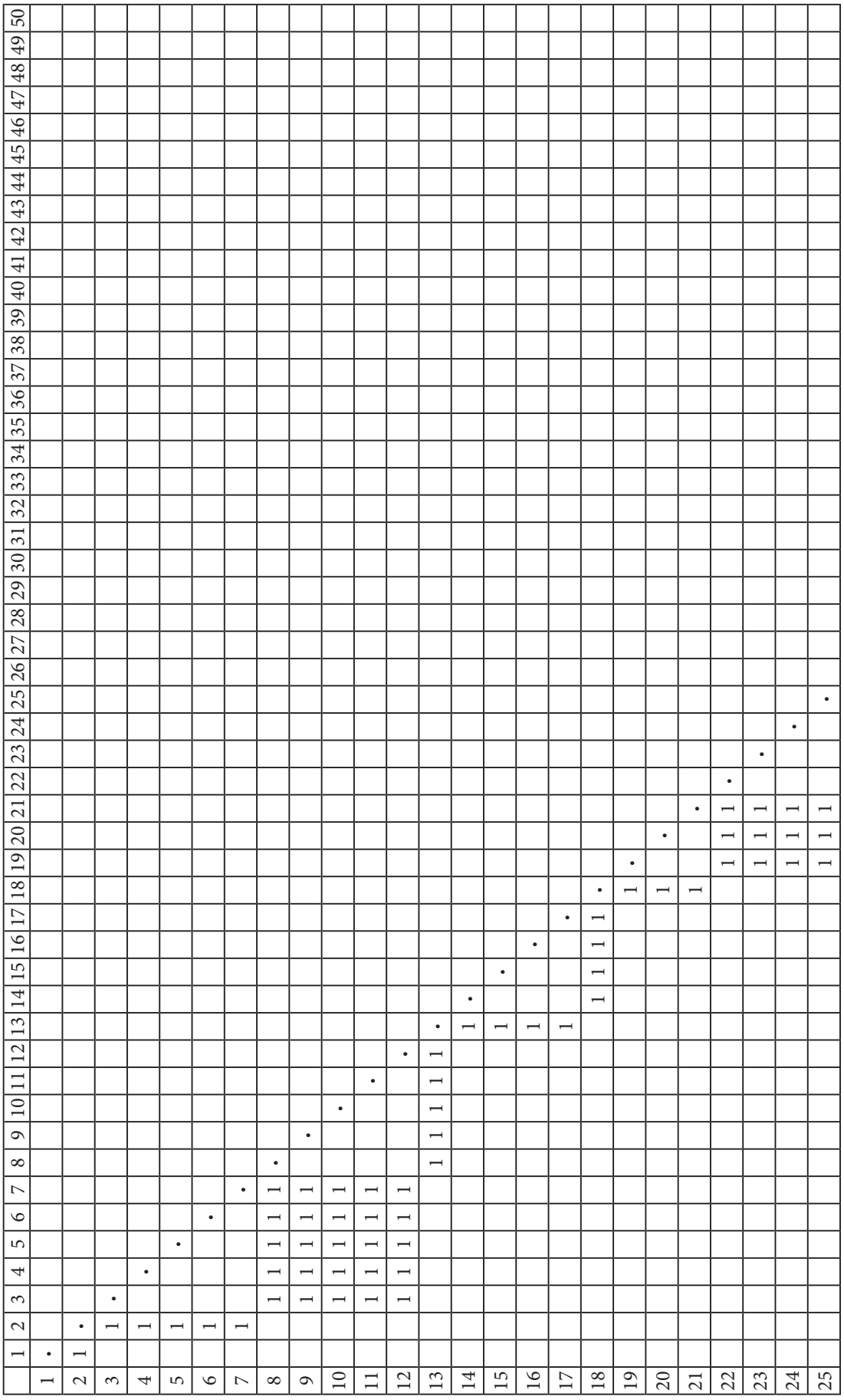

Рис. 3. Матрица следования комбинированного генетического и пчелиного алгоритма

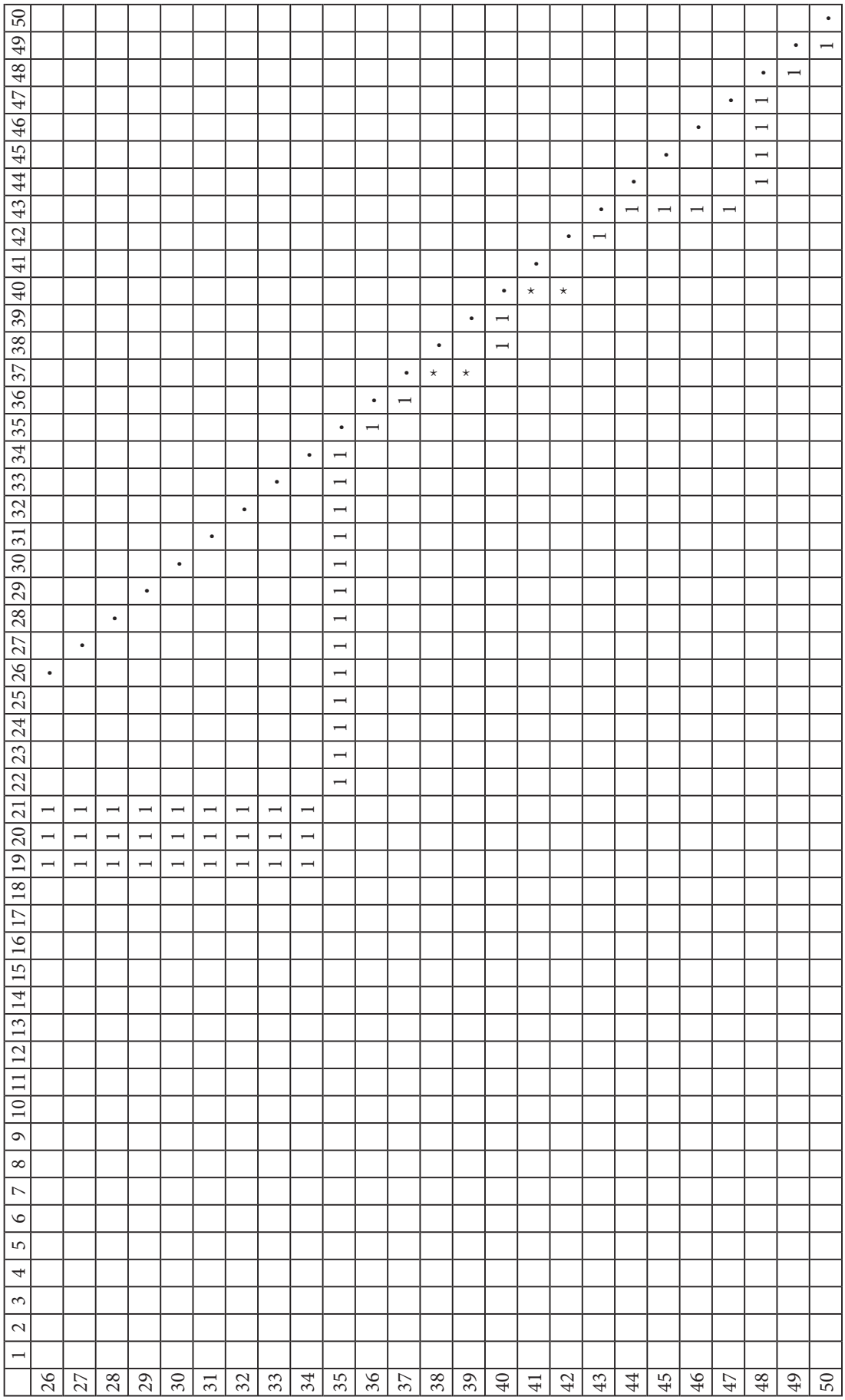

Рис. 3 (окончание)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1	·	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	·	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
3	1	1	·					1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
4	1	1		·				1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	1	1			·			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	1	1				·		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	1	1					·	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
8	1	1	1	1	1	1	1	·					1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
9	1	1	1	1	1	1	1		·				1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	1	1	1	1	1	1	1			·			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1				·		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
12	1	1	1	1	1	1	1					·	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	·	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
14	1	1	1	1	1	1	1	1	1	1	1	1	1	·				1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
15	1	1	1	1	1	1	1	1	1	1	1	1	1		·			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
16	1	1	1	1	1	1	1	1	1	1	1	1	1			·		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
17	1	1	1	1	1	1	1	1	1	1	1	1	1				·	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
18	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	·	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	·			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
20	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		·		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
21	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			·	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
22	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	·													1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
23	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		·												1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
24	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			·											1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
25	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				·										1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Рис. 4. Матрица независимости параллельного комбинированного генетического и пчелиного алгоритма

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
26	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					•								1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
27	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1						•								1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
28	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							•							1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
29	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1								•						1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1									•					1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
31	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1										•				1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
32	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1											•			1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
33	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1												•		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
34	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1													•	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
35	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
36	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1	1	1	1	1	1	1	1
37	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1	1	1	1	1	1	1
38	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1	1	1	1	1	1
39	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1	1	1	1	1
40	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1	1	1	1
41	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1	1	1
42	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1	1
43	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1	1
44	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1	1
45	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1	1
46	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1	1
47	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1	1
48	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1	1
49	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•	1
50	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	•

Рис. 4 (окончание)

$E_{макс}=12;\ n_{b1}=2;\ n_{rl}=4;\ n_{b2}=2$. Для данного множества весов вершин критический путь в графе G $T_{кр}=136$. Он проходит, например, через вершины $G_1-G_2-G_3-G_8-$ $-G_{13}-G_{14}-G_{18}-G_{19}-G_{22}-G_{35}-G_{36}-G_{38}-$ $-G_{40}-G_{42}-G_{43}-G_{44}-G_{48}-G_{49}-G_{50}$. Используя отмеченное выше допущение, что $T_{зад}=T_{кр}$, для информационно-логического графа G и матрицы следования найдем ранние τ_{pi} и поздние сроки τ_{ni} окончания выполнения операторов.

Ранние сроки:

$$\tau_{p1}=10,\ \tau_{p2}=11,\ \tau_{p3}=\tau_{p4}=\tau_{p5}=$$
$$=\tau_{p6}=\tau_{p7}=12,$$
$$\tau_{p8}=\tau_{p9}=\tau_{p10}=\tau_{p11}=\tau_{p12}=16,\ \tau_{p13}=18,$$
$$\tau_{p14}=\tau_{p15}=\tau_{p16}=\tau_{p17}=30,\ \tau_{p18}=33,$$
$$\tau_{p19}=\tau_{p20}=\tau_{p21}=45,\ \tau_{p22}=\tau_{p23}=\tau_{p24}=$$
$$=\tau_{p25}=\tau_{p26}=\tau_{p27}=\tau_{p28}=\tau_{p29}=$$
$$=\tau_{p30}=\tau_{p31}=\tau_{p32}=\tau_{33}=\tau_{34}=59,\ \tau_{p35}=95,$$
$$\tau_{p36}=105,\ \tau_{p37}=106,\ \tau_{p38}=\tau_{p39}=107,$$
$$\tau_{p40}=108,\ \tau_{p41}=120,\ \tau_{p42}=109,\ \tau_{p43}=128,$$
$$\tau_{p44}=\tau_{p45}=\tau_{p46}=\tau_{p47}=129,\ \tau_{p48}=131,$$
$$\tau_{p49}=135,\ \tau_{p50}=136.$$

Поздние сроки:

$$\tau_{n50}=136,\ \tau_{n49}=135,\ \tau_{n48}=131,$$
$$\tau_{n47}=\tau_{n46}=\tau_{n45}=\tau_{n44}=129,\ \tau_{n43}=128,$$
$$\tau_{n42}=109,\ \tau_{n41}=136,\ \tau_{n40}=108,$$
$$\tau_{n39}=\tau_{n38}=107,\ \tau_{n37}=106,\ \tau_{n36}=105,$$
$$\tau_{n35}=95,$$
$$\tau_{n22}=\tau_{n23}=\tau_{n24}=\tau_{n25}=\tau_{n26}=\tau_{n27}=\tau_{n28}=$$
$$=\tau_{n29}=\tau_{n30}=\tau_{n31}=\tau_{n32}=\tau_{n33}=\tau_{n34}=59,$$
$$\tau_{n19}=\tau_{n20}=\tau_{n21}=45,\ \tau_{n18}=33,$$
$$\tau_{n14}=\tau_{n15}=\tau_{n16}=\tau_{n17}=30,\ \tau_{n13}=18,$$
$$\tau_{n8}=\tau_{n9}=\tau_{n10}=\tau_{n11}=\tau_{n12}=16,$$
$$\tau_{n3}=\tau_{n4}=\tau_{n5}=\tau_{n6}=\tau_{n7}=12,\ \tau_{n2}=11,$$
$$\tau_{n1}=10.$$

В соответствии с методикой, описанной в [14], на основе значений τ_{pi} и τ_{ni} найдем оценку минимального числа процессоров для выполнения алгоритма за время $T_{кр}$ 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 (функция t) минимально. Для этой цели в матрице независимости найдем внутренне устойчивые множества, представляющие множества взаимно независимых операторов (ВНО).

Это множества (3, 4, 5, 6, 7), (8, 9, 10, 11, 12), (14, 15, 16, 17), (19, 20, 21), (22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34), (44, 45, 46, 47).

Легко убедиться, что максимальным внутренне устойчивым множеством является множество (22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34), включающее 13 элементов. При этом, так как операторы, входящие в данное множество ВНО, имеют равные ранние и поздние сроки окончания выполнения (принадлежат критическому пути), то оценка числа процессоров $t=13$, полученная для данного множества, позволяет выполнить алгоритм криптоанализа за минимальное время $T_{кр}$ при отмеченных выше допущениях. Данная оценка является решением задачи, поскольку, в соответствии с [14], в матрице независимости нет множеств ВНО, содержащих число операторов r, для которых $r>t$.

Таким образом, отсюда следует *утверждение* [13].

При реализации описанного параллельного комбинированного алгоритма криптоанализа, разработанного на основе построения информационно-логического графа G (в соответствии с технологией распараллеливания, описанной в [14]), необходимое минимальное число процессоров может в общем случае быть определено как число элементов, составляющих максимальное множество ВНО, содержащее операторы с равными ранними и поздними сроками окончания (то есть принадлежащими критическому пути). Такими множествами ВНО являются: (3, 4, 5, 6, 7) (число элементов равно числу агентов-разведчиков n_r), (8, 9, 10, 11, 12) (число элементов равно числу агентов-фуражиров n_f), (14, 15, 16, 17) (число элементов равно числу потомков после кроссинговера $M\cdot P_{кросс}$), (19, 20, 21) (число элементов равно числу хромосом, подвергающихся мутации $M\cdot n_{мут}$), (22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34) (число элементов равно общему числу базовых позиций, агентов-фуражиров, полученных потомков $n_b+n_f+M\cdot P_{кросс}$), (44, 45, 46, 47) (число

элементов равно количеству агентов-разведчиков n_{rl}, выбирающих случайным образом новые позиции на итерациях $2,3,\ldots,L$).

Таким образом, для графа G и матрицы независимости комбинированного алгоритма криптоанализа необходимое минимальное число процессоров может быть определено как $\max(n_r; n_f; M \cdot P_{кросс}; M \cdot n_{мут}; n_b + n_f + M \cdot P; n_{rl})$. При этом общее время реализации алгоритма в общем случае может составить $T = Q \cdot T_{кр}$, 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 [15].

ЗАКЛЮЧЕНИЕ

Таким образом, в данной работе разработана структурная схема комбинированного биоинспирированного алгоритма (генетический алгоритм и алгоритм пчелиных колоний), используемого для криптоанализа, являющегося представителем новых технологий искусственного интеллекта – биоинспирированных методов, имитирующих процессы эволюции живой природы. Следует заметить, что, несмотря на то, что для данных технологий в литературе и сети Интернет не приводится каких-либо строгих математических доказательств корректности реализации (так же как и экспериментальных результатов их применения, поскольку биоинспирированные методы являются вероятностными технологиями, основанными на имитации процессов живой природы, и их оптимальность может быть доказана только путем проведения экспериментальных исследований), данные технологии получают в последние годы все более широкое применение для решения комбинаторных NP-полных задач, используя для нахождения оптимального решения направленно-случайный поиск (в отличие от классических комбинаторных методов полного перебора). В данной работе определены основные параллельно выполняемые этапы комбинированного биоинспирированного 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. *Лебедев В. Б.* Модели адаптивного поведения колонии пчел для решения задач на графах / В. Б. Лебедев // Известия ЮФУ. – 2012. – № 7. – С. 42–49.

2. Криптографические методы и генетические алгоритмы решения задач криптоанализа: монография / Ю. О.Чернышев [и др.]. – Краснодар: ФВАС, 2013. – 138 с.

3. Биоинспирированные алгоритмы решения задач криптоанализа классических и асимметричных криптосистем: монография / Ю. О. Чернышев [и др.]. – Краснодар: КВВУ, 2015. – 132 с.

4. Применение биоинспирированных методов оптимизации для реализации криптоанализа блочных методов шифрования: монография / Ю.О. Чернышев [и др.]. Ростов-на-Дону: издательство ДГТУ, 2016. – 177 с.

5. Исследование возможности применения генетических алгоритмов для реализации криптоанализа блочных криптосистем / Чернышев Ю. О. [и др.] // Вестник Донского государственного технического университета. – 2015. – № 3(82). – С. 65–72.

6. Исследование возможности применения методов эволюционной оптимизации для реализации криптоанализа блочных методов шифрования / Ю. О. Чернышев [и др.] // Изв. СПбГЭТУ «ЛЭТИ». – 2015. – № 10. – С. 32–40.

7. *Сергеев, А. С.* Разработка параллельного комбинированного биоинспирированного метода (генетический алгоритм и алгоритм муравьиных колоний) для решения задач криптоанализа / А. С. Сергеев // Системный

анализ в проектировании и управлении: сб. научн. тр. XXII Междунар.науч.-практич. конф. Ч. 1. – СПб. : Изд-во Политехн. ун-та, 2018. – С. 359–370.

8. Исследование возможности применения бионических методов пчелиных колоний для реализации криптоанализа классических шифров перестановок / Ю. О. Чернышев [и др.] // Вестник ДГТУ. – 2014. – Т. 14, № 1(76). – С. 62–75.

9. Разработка и исследование параллельной модели алгоритмов пчелиных колоний для решения задач криптоанализа / Ю. О. Чернышев [и др.] // Вестник Донского государственного технического университета. – 2017. – Т. 17, № 1(88). – С. 144–159.

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

11. *Чернышев Ю. О.* Применение комбинированных биоинспирированных стратегий (генетический алгоритм и алгоритм пчелиных колоний) для реализации криптоанализа классических шифров перестановок / Чернышев Ю. О., Сергеев А. С. // Инженерный вестник Дона. – 2017. – № 4. – URL:ivdon.ru/ru/magazine/archive/n4y2017/4518.

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

13. *Сергеев А. С.* Разработка и исследование параллельного комбинированного биоинспирированного метода (генетический алгоритм и алгоритм пчелиных колоний) для реализации криптоанализа симметричных систем шифрования / А. С. Сергеев // Международная конференция «Радиоэлектронные устройства и системы инфокоммуникационных технологий – РЭУС-2018». – М., 2018. – С. 366–371.

14. *Сергеев, А. С.* Параллельное программирование / А. С. Сергеев. – Ростов-на-Дону : Издательский центр ДГТУ, 2002. – 77 с.

15. *Ахо, А. В.* Структуры данных и алгоритмы / А. В. Ахо, Д. Э. Хопкрофт, Д. Д. Ульман. – М. : Издательский дом «Вильямс», 2003. – 384 с.

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

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

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

19. *Чернышев, Ю. О.* Исследование и разработка параллельного комбинированного биоинспирированного алгоритма для решения задач криптоанализа / Ю. О. Чернышев, А. С. Сергеев, А. Н. Рязанов // Известия СПбГЭТУ «ЛЭТИ». – 2019. – № 3. – С. 46–56.

Чернышев Юрий Олегович – почетный профессор ДГТУ, заслуженный деятель науки, доктор технических наук, профессор, кафедра «Автоматизация производственных процессов», Донской государственный технический университет, г. Ростов-на-Дону.

Сергеев Александр Сергеевич – канд. техн. наук, научный сотрудник, Донской государственный технический университет, г. Ростов-на-Дону.
E-mail: sergeev00765@mail.ru

Панасенко Павел Александрович – канд. техн. наук, преподаватель 21 кафедры 2 факультета Краснодарского высшего военного училища им. генерала армии С. М. Штеменко.

DEVELOPMENT AND RESEARCH OF COMBINED PARALLEL BIOINSPIRED METHODS (GENETIC ALGORITHM AND THE ALGORITHM OF BEE COLONIES) FOR THE IMPLEMENTATION OF THE SYMMETRIC ENCRYPTION SYSTEMS CRYPTANALYSIS

Yu. O. Chernyshev*, A. S. Sergeev*, P. A. Panasenko**

**Don State Technical University*
***Krasnodar higher military school of a name of the General S. M. Shtemenko*

Annotation. The paper deals with the problem of cryptanalysis of symmetric encryption systems using a new model of optimization strategies – a combined bioinspired algorithm. Application of the combined bioinspired algorithm on the basis of hybridization by attachment (the genetic algorithm and an algorithm of bee colonies) for implementation of cryptanalysis of ciphers of permutations is described. The description of the combined algorithm is provided, it is shown that the probability of receiving an optimal variant of a solution at implementation of hybrid algorithms of cryptanalysis cannot be less than the probability of receiving an optimal solution when using of the classical bioinspired algorithms. The description of the main operations allowing parallel execution at the global level is provided, the block diagram of a parallel algorithm, the information-logical graph-scheme are also submitted, the description of a matrix of following is provided. On the basis of definition of sets of mutually independent operators and a critical path in the graph the problem of definition of the minimum number of processors for implementation of the parallel combined algorithm is solved.
Keywords: cryptanalysis, combined bioinspired algorithms, hybridization by attachment, genetic algorithm, the algorithm of bee colonies, the information-logical graph-scheme, the matrix of following, matrix independence.

Chernyshev, Yury Olegovich – honorary Professor DSTU, honored scientist, doctor of technical Sciences, Professor, the dept. «Automation of Production Processes», Don State Technical University.

Sergeev, Aleksandr Sergeevich – candidate of technical Sciences, scientific researcher, Don State Technical University.
E-mail: sergeev00765@mail.ru.

Panasenko, Pavel Alexandrovich – candidate of technical Sciences, teacher of 21 departments 2 faculty of Krasnodar higher military school of a name of the General S. M. Shtemenko.