УДК 004.056.55

МЕТОДЫ РЕШЕНИЯ ЗАДАЧ КРИПТОАНАЛИЗА БЛОЧНЫХ КРИПТОСИСТЕМ НА ОСНОВЕ БИОИНСПИРИОВАННЫХ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Ю. О. Чернышев*, А. С. Сергеев*, А. Н. Рязанов, Е. О. Дубров*****

**Донской государственный технический университет*
*** Открытое акционерное общество «711 Военпроект», г Ростов-на-Дону*
**** Федеральное государственное унитарное предприятие «Ростовский НИИ радиосвязи»*

Поступила в редакцию 16.06.2018 г.

Аннотация. Статья посвящена решению задачи криптоанализа на основе новых моделей и методов искусственного интеллекта – биоинспирированных стратегий направленно-случайного поиска (генетических методов, методов муравьиных и пчелиных колоний). Приводится обзор авторских публикаций, посвященных рассмотрению задач криптоанализа блочных криптографических методов. Отмечено применение генетических методов для криптоанализа стандарта шифрования DES, стандарта шифрования России и AES, также рассмотрено применение алгоритмов муравьиных и пчелиных колоний для криптоанализа блочных систем шифрования. Приведены временные оценки и оценки числа процессоров при параллельной реализации, отмечается применение целевой функции специального типа (функции Якобсена) для использования на текстах, имеющих достаточный объем.
Ключевые слова: биоинспирированные методы, криптоанализ, генетические алгоритмы, блочные криптосиситемы, муравьиные и пчелиные алгоритмы, матрица независимости.
Annotation. Article is devoted to the solution of a task of cryptanalysis on the basis of new models and methods of artificial intelligence – the bioinspired strategy of directed-random search (genetic methods, methods of ant and bee colonies). The review of the author's publications devoted to consideration of tasks of cryptanalysis of block cryptographic methods is provided. Application of genetic methods for cryptanalysis of the standard of enciphering of DES, the standard of enciphering of Russia and AES is noted, application of algorithms of ant and bee colonies for cryptanalysis of block systems of enciphering is also considered. The estimates of time and estimates of number of processors at parallel realization are given, application of criterion function of special type (Jacobsen's function) for use on the texts having sufficient volume is noted.
Keywords: bioinspired methods, cryptanalysis, genetic algorithms, block cryptosystems, ant and bee algorithms, independence matrix.

1. ВВЕДЕНИЕ

При разработке компьютерных информационных технологий, обеспечивающих защиту информации, основное применение в настоящее время находят методы криптографической защиты информации. Для решения данной NP-полной задачи (оптимальное решение которой в общем случае может быть найдено комбинаторным перебором) в последние годы применяются алгоритмы, основанные на моделировании процессов эволюции природных экосистем (эволюционные методы, генетические алгоритмы (ГА), методы моделирования отжига, алгоритмы роевого интеллекта и т. д.) [1]. Таким образом, научное направление «эволюционные вычисления» в последние годы получает все более широкое распространение для реше-

ния различного круга оптимизационных задач, в том числе задач криптоанализа [2, 3]. В данных моделях и методах основным моментом является формирование начальной структуры, а также правил, определяющих способы ее изменения (эволюционирования). Среди последних разработок эвристических методов, используемых для решения задачи параметрической оптимизации технических объектов, можно отметить стохастический алгоритм, основанный на модели поведения роя светлячков, рассмотренный в [4].

Ранее в [1, 5] авторами рассматривались вопросы исследования возможности реализации биоинспирированных методов для криптоанализа классических методов и алгоритмов шифрования (симметричных и асимметричных методов). В [1] рассматриваются методы и алгоритмы, используемые при решении задач криптоанализа. Приведен обзор основных криптографических методов, а также анализ тенденций развития криптографии. Описаны основные методы криптоанализа с использованием нового научного направления – генетических алгоритмов, приведены результаты экспериментальной реализации. Рассмотрена реализация алгоритмов генетического поиска для криптоанализа перестановочных шифров (шифрующие таблицы, маршрутные перестановки и магические квадраты), классических шифров замены (аффинный шифр, шифр Цезаря, блочные и многоалфавитные шифры замены), также рассматриваются вопросы реализации криптоанализа шифров гаммирования, приводится обзор некоторых оригинальных подходов, разработанных за последнее время и основанных на применении генетических алгоритмов для криптоанализа (в частности, для криптоанализа тригонометрических шифров, а также оригинального нестандартного метода, отличительной особенностью которого является, по мнению авторов, бесконечный период гаммирования). В [5] рассматриваются методы и алгоритмы, предназначенные для криптоанализа с использованием биоинспирированных алгоритмов муравьиных колоний и пчелиного роя (описано применение данных методов для криптоанализа классических симметричных криптосистем, а также асимметричных криптосистем на основе решения таких задач как факторизация составных чисел (то есть их разложения на два взаимно простых сомножителя), нахождения простого делителя составных чисел).

Отметим, что среди обзорных авторских публикаций, посвященных рассмотрению криптоанализа классических методов с помощью биоинспирированных алгоритмов, можно отметить работы [6, 7, 8].

В данной работе рассматривается обзор авторских публикаций, а также применение биоинспирированных технологий для криптоанализа блочных стандартов шифрования, а также приводятся некоторые экспериментальные результаты.

2. ПОСТАНОВКА ЗАДАЧИ КРИПТОАНАЛИЗА БЛОЧНЫХ КРИПТОСИСТЕМ НА ОСНОВЕ ЭВОЛЮЦИОННЫХ АЛГОРИТМОВ

Таким образом, актуальным является вопрос о возможности реализации биоинспирированных методов для криптоанализа современных блочных методов шифрования. Основные способы построения блочных шифров, их структура (схема Фейстеля) описаны в [9].

Также следует заметить, что основной особенностью использования биоинспирированных алгоритмов криптоанализа является возможность реализации шифрующего алгоритма в качестве функции оценки оптимальности ключа, определенного с помощью операций биоинспирированного метода. Здесь и далее под качеством (оптимальностью) ключа шифрования, определенного с помощью операций биоинспирированного метода, будем понимать процент оптимальных символов, полученных с помощью алгоритма криптоанализа, применяемого к заданному шифрованному тексту, при использовании данного сформированного ключа. Это означает, что для оценки оптимальности ключа шифрования нет необходимости использовать какие-либо дополнительные операции и методы, для этой цели может быть использован сам алго-

ритм шифрования, при реализации которого определяется качество используемого ключа (процент оптимальных символов). Таким образом, основным моментом является тот факт, что при использовании генетических методов процесс криптоанализа определяется не столько качеством и сложностью шифрующих преобразований, сколько качеством биоинспирированного метода (настройкой его параметров), который должен обеспечивать достаточное популяционное разнообразие индивидуумов (вариантов ключей). Этот факт также свидетельствует об актуальности исследования и разработки биоинспирированных методов и алгоритмов для криптоанализа блочных стандартов шифрования.

Криптоанализ блочного стандарта DES. Криптоанализ блочных методов (на примере классического представителя – стандарта DES) описан в работах [10–12, 14, 15]. В этом плане можно отметить также работу [21], в которой рассмотрен ряд параллельных алгоритмов, используемых при различных методах анализа. Приводится классификация М. Флинна архитектур высокопроизводительных вычислительных систем, описываются основные особенности программирования параллельных вычислений (параллельная и конвейерная обработка), приводятся оценки эффективности параллельных алгоритмов (ускорение и эффективность программы). Также в [21] рассматриваются параллельные алгоритмы теоретико-числовых задач защиты информации, в т. ч. задача нахождения простых чисел в интервале, задача разложения числа на множители, задача дискретного логарифмирования. В этой связи для разработки криптоанализа алгоритма DES с помощью эволюционного алгоритма вначале рассматривается параллельная реализация составляющих его этапов. Структурная схема цикла алгоритма, полученная на основе данных преобразований, представлена в [10–12]. Дальнейшее определение множества независимых параллельных операторов производится на основе методов, описанных в [13]. Осуществляется построение информационно-логической граф-схемы $G = (X, U)$ алгоритма, где множество операторов алгоритма соответствует множеству X вершин, множество U ребер включает ребра, определяющие связи по информации и по управлению. Для данной граф-схемы вводятся в рассмотрение матрицы следования S, логической несовместимости L и независимости M с использованием алгоритмов, описанных в [13]. По нулевым элементам матрицы M в строке можно определить множество операторов, допускающих параллельное выполнение с оператором, соответствующим строке. Структуры данных матриц S, L, M приводятся в [10, 11, 12, 14].

С использованием данной параллельной схемы алгоритма в [10] представлена структурная схема и описание метода криптоанализа 2 типа. Вначале осуществляется формирования начальной популяции ключей, далее осуществляется оценка их пригодности (проверка, насколько полученный с их помощью шифртекст совпадает с исходным). После определения целевой функции (ЦФ) осуществляется селекция индивидуумов для проведения множества операций биоинспирированного метода и получения множества потомков, после чего для полученной расширенной популяции производится дальнейшее оценивание целевой функции индивидуумов. Критерием останова процесса является либо прекращение эволюционирования популяции, либо исчерпание заданного временного ресурса. Таким образом, при формировании популяции из P индивидуумов, время работы алгоритма T может составить $T = P * t$, где t – время оценки одного варианта ключа (индивидуума).

Отметим, что при значительном объеме популяции для определения функции пригодности индивидуумов можно использовать конвейерный принцип организации специализированных вычислений. Описание процесса реализации и схема выполнения потока операций представлены в [11].

Отметим, что после разработки параллельной схемы реализации криптоанализа возможна постановка следующей задачи: для алгоритма шифрования на основе построенного информационно-логического графа G и для заданного времени $T_{зад}$ найти наимень-

шее необходимое число процессоров, а также план реализации операторов на них. Решение данной задачи на основе методов, изложенных в [13], представлено в [14]. При этом полученная с использованием визуальной методики [13] минимальная оценка числа процессоров составляет $n = 2$, критический путь в графе G равен $T_{кр} = 24$, заданное время принимается $T_{зад} = T_{кр}$. В [14] показано, что эта оценка является минимальной, также описан план выполнения операторов.

Отметим, что пошаговое описание алгоритма и его программной реализации приведено в [10, 15, 18].

Описание полученных при реализации ГА криптоанализа экспериментальных результатов, полученных с использованием процессора CORE I5-2400, также приведено в [10]. При проведении эксперимента задавались следующие параметры: количество итераций – 100, тип кроссинговера – простой двухточечный, размер начальной популяции – 1000, норма мутации и инверсии – 0,05, количество итераций – 100. Результаты для одной серии экспериментов представлены в табл. 1.

В 1 столбце таблиц показан номер итерации, во 2 столбце – количество хромосом, подвергнувшихся мутации и инверсии, столбцы с 3 по 12 представляют значение процента, определяющего совпадение полученного текста с исходным для 10 лучших хромосом популяции.

Как показывают полученные результаты, на 25 генерации совпадение полученного текста с исходным обеспечивается на 50 %, на 30 генерации – на 62,5 %. Временные затраты алгоритма для получения квазиоптимального ключа составили порядка 53 мин. (при одноточечном кроссинговере, норме мутации и инверсии 5 %), при кроссинговере по маске порядка 29 мин., при двухточечном кроссинговере порядка 55 мин., что не превышает временных затрат при реализации дифференциального криптоанализа, описанного в [28]. Результаты эксперимента по определению оптимального и квазиоптимального ключей, обеспечивающих совпадение полученного текста с заданным с помощью разбиения исходного текста на 8-буквенные блоки также приведены в [10, 15].

Приведем результаты эксперимента по определению квазиоптимального ключа, обеспечивающего максимальное совпадение полученного текста с исходным. В качестве исходного был использован следующий текст:

«я_вас_любил:_любовь_еще,_быть_может,_в_душе_моей_угасла_не_совсем;_но_пусть_она_вас_больше_не_тревожит;_я_не_хочу_печалить_вас_ничем.___»

При реализации алгоритма криптоанализа путем разбиения исходного текста на 8-буквенные блоки и использовании параллельного вычислительного процесса был определен квазиоптимальный ключ, обеспечивающий

Таблица 1

Результаты сходимости ГА криптоанализа при 1 генерации

0	1000	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
1	1800	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
4	5372	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
5	7735	25,0	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5
8	23094	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0
17	614816	37,5	37,5	25,0	25,0	25,0	25,0	25,0	25,0	25,0	25,0
18	885334	37,5	37,5	37,5	37,5	37,5	37,5	37,5	25,0	25,0	25,0
20	1835828	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
22	3806771	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
23	5481748	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
25	11366950	50,0	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5	37,5
30	23681145	62,5	50,0	50,0	50,0	50,0	50,0	37,5	37,5	37,5	37,5

получение следующего текста (неоптимальные символы заменены символом «*»):

*«я*в*с*любил***юб*вь*еще**б*ть_ *ожее***в_д*шем*ей_**аслаа* не**овс*м*_н*_*ус*ь*о*а_в*с* бол**е_н*_т*ев*ж*т;*я*н**хочу_п*ч*л*т*_ ва*_**че*.__*»*

Как можно заметить, полученный текст достаточно близок к исходному (совпадение в пределах 62,5 %), содержит осмысленные слова (хочу, любил) или почти осмысленные (т*ев*ж*т, п*ч*л*т), из чего следует, что процесс расшифрования (например, при использовании ГА для криптоанализа 1 типа) может быть доведен до конца вручную.

Криптоанализ стандарта шифрования России. Реализация криптоанализа стандарта шифрования ГОСТ 28147-89 с использованием генетических методов аналогичным образом описана в [16]. Описаны основные режимы работы алгоритма, а также параллельно выполняемые этапы на глобальном уровне в режиме простой замены. Структурные схемы шифрования в режиме простой замены и в режиме гаммирования представлены в [17]. Приведена структурная схема одного цикла режима простой замены с учетом параллельно выполняемых этапов. Для данной структурной схемы осуществляется построение информационно-логической граф-схемы, матриц следования, логической несовместимости и независимости.

Очевидно, что в общем случае реализация ГА криптоанализа заключается в формировании популяции секретных ключей (синхропосылок или таблиц перестановок), а также дальнейшей оценкой их оптимальности и последующим применением множества генетических операций.

Как и ранее, для повышения эффективности реализации ГА на локальном уровне необходимо определение оценки минимального числа процессоров при заданных временных оценках операторов, составляющих информационно-логическую граф-схему. Решение данной задачи представлено в [16], где получена оценка числа процессоров $n = 2$, при которой алгоритм оценки элемента популяции может быть реализован за минимальное время $T = T_{кр}$. Таким образом, при наличии популяции из P индивидуумов, время T работы ГА при последовательной оценке элементов популяции составит $T = P*t$, где t – время оценки одного индивидуума с учетом параллельно выполняемых операций. При параллельной реализации и наличии n параллельных процессоров время оценки составит $T = (P/n)*t$ [17, 18].

В [16, 18] приводится также описание некоторых экспериментальных результатов криптоанализа, который был реализован с использованием процессора CORE I7-4820K, CPU 3,7 GHz, ОЗУ 64 Гб. Основные параметры: количество итераций – 100, размер начальной популяции – 1000, тип кроссинговера – простой двухточечный, норма мутации и инверсии – 0,05. Временные затраты алгоритма криптоанализа для получения оптимального или квазиоптимального ключа (обеспечивающего совпадение полученного текста с исходным на 50 %) составило при норме мутации и инверсии 5 % и двухточечном кроссинговере от 74 мин. до 24 часов. Наилучшая хромосома обеспечивает совпадение полученного текста с исходным на 50 % на 24 генерации, на 62,5 % на 32–33 генерации.

Криптоанализ стандарта AES. Отметим, что исследованию возможности применения генетических методов для реализации криптоанализа блочного стандарта шифрования AES посвящена работа [25, 26]. Приводится описание стандарта шифрования, описание метода криптоанализа на основе параллельной версии алгоритма, приведены оценки минимального числа процессоров для реализации алгоритма, а также экспериментальные результаты.

Следует заметить, что экспериментальная реализация описанного выше алгоритма криптоанализа осуществлялась следующим образом. На начальном этапе исходный текст подвергался шифрованию с помощью алгоритма AES для получения шифртекста. Далее производилось разбиение полученного шифртекста на блоки, для каждого блока осуществлялась реализация генетического алгоритма криптоанализа, при этом использовались одно- и двухточечный кроссинговер, а также

мутация и инверсия с нормой 5 %. После генерации популяции ключей и реализации генетических операций проводилось оценивание элементов популяции путем подсчета количества оптимальных символов в расшифрованном тексте (т.е. символов, совпадающих с символами исходного текста). При проведении экспериментов количество таких символов составляло порядка 25 % – 31%. Эксперименты с подсчетом оптимальных символов при оценивании множества ключей популяции производились достаточно большое число раз, после чего осуществлялось наложение оптимальных символов, полученных при использовании различных элементов популяции ключей. В этом случае при достаточно большом количестве запусков и большом количестве вариантов ключей, полученных при реализации генетических операций, возможно получение исходного текста. Следует заметить, что конкретное значение числа запусков и количество вариантов ключей может быть определено на основе экспериментальных данных.

В [25, 26] приводится пример исходного текста и для первого блока приводится таблица генераций получения строк исходного текста в машинных 16-ричных кодах при 10 значениях ключей, полученных при проведении генетических операций. В качестве примера используется следующий текст:

Вороне_где-то_бо/
г_послал_кусочек/
_сыру;_На_ель_во/
рона_взгромоздяс/
ь,_Позавтракать_/
было_совсем_уж_с/
обралась,_Да_при/
задумалась, _а_сы/
р_во_рту_держала

Для первых трех блоков (строк) текста приведем таблицу генераций получения строк исходного текста в машинных 16-ричных кодах при 6–10 значениях ключей, полученных при проведении генетических операций (табл. 2–4). Коды, соответствующие оптимальным символам в полученных строках, отмечены жирным курсивом. Как видно из приведенных результатов, при их совмещении в общем случае возможно получение исходного текста.

В качестве основных выводов в [25, 26] отмечаются следующие:

– основной отличительной особенностью применения биоинспирированных методов криптоанализа (в том числе ГА) является возможность применения самого шифрующего алгоритма в качестве алгоритма, определяющего целевую функцию пригодности ключа, определенного с помощью операций биоинспирированного метода; вследствие этого при использовании биоинспирированных мето-

Таблица 2

Полученные строки исходного текста для 10 значений ключей 1-й строки

	в	о	р	о	н	Е	_	г	д	е	-	т	о	_	б	о
	C2	EE	F0	EE	ED	E5	5F	E3	E4	E5	2D	F2	EE	5F	E1	EE
1	***C2***	AF	4E	***EE***	0E	58	1C	EB	60	9B	E0	***F2***	***EE***	E5	55	F0
2	62	13	34	8C	***ED***	82	C9	***E3***	67	6B	43	***F2***	C9	D0	***E1***	21
3	***C2***	C9	3F	90	***ED***	BE	3C	8D	3F	***E5***	AD	7D	***EE***	67	02	C2
4	CE	***EE***	EA	4E	77	30	B9	D2	73	C3	5A	***F2***	***EE***	***5F***	34	E4
5	B5	DD	62	DC	72	8B	***5F***	F6	88	BD	***2D***	***F2***	CF	***5F***	09	AB
6	***C2***	AF	4E	***EE***	0E	58	1C	EB	60	9B	E0	***F2***	***EE***	E5	55	F0
7	D7	94	A6	BD	***ED***	1A	43	E7	48	98	***2D***	***F2***	D0	75	B4	***EE***
8	***C2***	15	72	***EE***	33	C5	43	27	***E4***	37	95	1C	***EE***	F5	0F	9D
9	F9	8D	***F0***	5F	60	3C	21	35	91	86	72	***F2***	3F	***5F***	***E1***	E2
10	***C2***	96	3B	74	3E	***E5***	9B	***E3***	24	E0	2E	CA	CA	***5F***	9D	58

Таблица 3

Полученные строки исходного текста для 8 значений ключей 2-й строки

	г	_	п	о	с	л	а	л	_	к	у	с	о	ч	е	к
	E3	5F	EF	EE	F1	EB	E0	EB	5F	EA	F3	F1	EE	F7	E5	EA
1	50	21	44	***EE***	31	***EB***	8B	76	47	***EA***	B3	***F1***	B5	B3	C9	F5
2	***E3***	D4	***EF***	5D	BB	8E	FA	2F	***5F***	6C	D8	6B	D5	51	D8	***EA***
3	***E3***	AA	C5	1A	E3	***EB***	***E0***	A2	75	***EA***	52	00	3C	70	35	CF
4	5D	4D	A4	E9	AC	***EB***	87	2F	***5F***	15	***F3***	24	99	6F	***E5***	AE
5	5B	2A	32	8D	***F1***	A8	A0	FA	A3	4B	***F3***	***F1***	90	2C	***E5***	16
6	6F	AC	5E	45	***F1***	98	***E0***	FA	25	32	5A	***F1***	***EE***	E7	33	99
7	***E3***	***5F***	25	81	7B	FB	11	***EB***	95	69	92	***F1***	1A	44	5D	8A
8	84	67	***EF***	E1	1B	AC	***E0***	***EB***	F9	A6	E9	39	33	***F7***	4F	2A

Таблица 4

Полученные строки исходного текста для 8 значений ключей 3-й строки

	_	с	ы	р	у	;	_	н	а	_	е	л	ь	_	в	о
	5F	F1	FB	F0	F3	3B	5F	CD	E0	5F	E5	EB	FC	5F	C2	EE
1	***5F***	F6	64	***F0***	02	F2	86	36	E7	D2	4F	***EB***	4A	09	D1	***EE***
2	D8	B2	50	***F0***	***F3***	17	EA	***CD***	D0	D2	72	3B	80	***5F***	39	D4
3	CF	FA	9E	29	4E	***3B***	3A	C2	***E0***	***5F***	CB	CD	DE	62	***C2***	E0
4	D7	E0	***FB***	CD	***F3***	68	9F	***CD***	52	35	06	12	8F	***5F***	A2	34
5	***5F***	***F1***	16	49	D2	EE	83	96	F1	***5F***	FD	A4	AA	D6	D1	***EE***
6	***5F***	***F1***	CA	57	96	20	***5F***	1A	A9	04	59	B5	FD	C3	FB	***EE***
7	8D	9C	87	DB	***F3***	***3B***	1F	2A	C2	49	5B	BE	***FC***	43	C2	11
8	5B	23	3D	C2	C9	28	1C	***CD***	84	BC	***E5***	***EB***	***FC***	32	A4	3D

дов криптоанализа процесс определения секретного ключа зависит в первую очередь не столько от сложности преобразований алгоритма шифрования, сколько от качества самого биоинспирированного метода и настройки его параметров, при которой должно обеспечиваться достаточное разнообразие генерации ключей;

– при использовании биоинспирированных методов криптоанализа обеспечивается возможность получения некоторого множества квазиоптимальных вариантов ключей, при применении которых для криптоанализа возможно получение некоторого множества вариантов исходного текста; при сопоставлении данных вариантов возможно определение оптимальных символов расшифрованного текста, из которых далее путем комбинирования возможно получение оптимального (или квазиоптимального) исходного текста.

3. КРИПТОАНАЛИЗ БЛОЧНЫХ КРИПТОСИСТЕМ С ИСПОЛЬЗОВАНИЕМ АЛГОРИТМОВ МУРАВЬИНЫХ КОЛОНИЙ

Алгоритм муравьиных колоний и его применение для криптоанализа блочных криптосистем рассматривается в [19]. В данной работе показано, как задача формирования секретного ключа может быть в общем случае представлена как задача о назначениях. Таким образом, реализация алгоритма заключается в общем случае в нахождении позиций для символов ключа таким образом, при котором целевая функция оптимальности шифртекста достигает экстремума. То есть данная задача в общем случае является частным случаем квадратичной задачи о назначениях, являющейся основной тестовой задачей для оценки эффективности поисковых методов.

Математическая модель (целевая функция) для задачи криптоанализа имеет вид:

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

где C_{ij} – параметр, показывающий вероятность следования друг за другом в тексте символов в позиции i и в позиции j, Q_i – параметр, индексирующий, осмысленность блока из i символов, т.е. его совпадение со словарным запасом языка.

Необходимо отметить, что основным моментом при реализации описанного алгоритма является вычисление на каждой итерации значения Q – оценки приспособленности особей. Одним из методов вычисления данной функции является использование функции Якобсена [1, 6, 7], которая использует критерий минимума разности $R(T)$ между реальной и среднестатистической частотой встречаемости биграмм в тексте и может быть реализована на текстах достаточной длины. Данная целевая функция имеет вид:

$$R(T) = \sum_{ij} \left| D_{ij}(T) - E_{ij} \right| \to \min,$$

где D_{ij} – элемент матрицы D, равный количеству встретившихся в тексте T биграмм ij, E_{ij} – эталонные частоты биграмм ij. Матрица E, таким образом, представляет среднестатистическое распределение, поэтому большее значение приспособленности особи будет соответствовать меньшему значению целевой функции R (возможно также использование функции $R(T) = (1/R) \to \max$). Как отмечено в [1, 6, 7], среднестатистические частоты биграмм заранее известны, поэтому, как показывают приведенные в [6, 7] примеры, применение функции Якобсена при криптоанализе обеспечивает получение результатов, достаточно близких к оптимальным.

Таким образом, значение целевой функции R может быть определено как длина маршрута, соединяющего выбранные элементы декартова произведения [«номер позиции» х «номер символа»]. В этом случае секретному ключу, представляющему маршрут с более оптимальным значением R, соответствует более значительная концентрация феромона F, используемая как вероятность выбора очередного маршрута, представляющего очередной вариант ключа. Необходимо отметить, что основным моментом в теории муравьиных алгоритмов является использование феромона для выбора пути муравьями-агентами.

В [19] приведено пошаговое описание алгоритма, основными операциями которого являются следующие.

1. Равновероятный случайный выбор множества вариантов маршрутов, представляющих варианты секретного ключа, и вычисление значения целевых функций R_i на основе определения оптимальности блока открытого текста при реализации алгоритма дешифрования.

2. Присвоение комбинациям размещения символов в позиции весового коэффициента R_i.

3. Вычисление для каждой комбинации размещения результирующей концентрации.

4. Проведение имитации испарения феромона.

5. После переопределения количества феромона определение новых вероятностей размещения символов в позиции.

6. Формирование нового множества маршрутов, являющихся вариантами секретного ключа, и определение для них соответствующих блоков открытого текста и значения R_i, далее осуществляется выборка множества лучших вариантов. Если не наблюдается изменения оптимального значения критерия в течение заданного количества циклов, то поиск завершается, в противном случае осуществляется возврат к пункту 2.

В [19] приводится структурная схема криптоанализа, а также демонстрационный пример, где требуется определить блок исходного текста и секретный ключ на основе блока шифртекста незначительной длины (6 символов). При этом используются 6-битовые блоки открытого текста, шифртекста, и секретный ключ, а также используются допущения, что каждый бит шифртекста определяется каждым битом исходного текста и каждым битом ключа (т. е. зная секретный ключ и шифртекст, можно сразу определить исходный текст и наоборот), а также что шиф-

ртект и исходный текст содержат символы из одного и того же алфавита. Данный пример иллюстрирует, как на основе блока шифртекста «ИОСАКБ» осуществляется формирование блока исходного текста «СОБАКИ» с оптимальным значением целевой функции, соответствующего секретному оптимальному ключу.

Параллельная реализация алгоритма муравьиных колоний. Возможности параллельной реализации алгоритмов муравьиных колоний для криптоанализа блочных криптосистем посвящена работа [20]. Здесь отмечаются основные недостатки методов генетического поиска («слепой» поиск, приводящий к генерации решений с нарушениями, и увеличивающий время поиска; генерации одинаковых и плохо приспособленных решений; попадание в локальный оптимум). Поэтому актуальной является задача исследования возможности применения эвристических методов, имитирующих процессы эволюции природных систем и реализующих поэтапное построение решения задачи. К данным методам относят и алгоритмы муравьиных колоний, моделирующих поведение колонии муравьев, обладающей способностью находить кратчайший путь к источнику пищи. Несмотря на примитивное поведению отдельных муравьев-агентов поведение всей колонии в общем случае может оказаться достаточно разумным. Как и ранее в предыдущих работах, отмечается, что возможность использования шифрующего алгоритма в качестве целевой функции для оценки оптимальности ключа, определенного с помощью операций биоинспирированного метода, является основной отличительной особенностью применения биоинспирированных методов криптоанализа. В связи с этим актуальной становится задача исследования возможности применения биоинспирированных методов для криптоанализа блочных криптосистем, поскольку при использовании данных методов процесс определения секретного ключа зависит не столько от сложности преобразований блочного алгоритма шифрования, сколько от качества самого биоинспирированного метода и настройки его параметров, при которой должно обеспечиваться достаточное разнообразие индивидуумов популяции ключей. Также отмечается возможность увеличения производительности «природных» алгоритмов как на основе параллельной реализации на «низшем» уровне (параллельная реализация самого шифрующего алгоритма, обеспечивающего оценку целевой функции оптимальности ключа), так и при параллельной реализации на «высшем» уровне (параллельная реализация «биоинспирированного» алгоритма, обеспечивающего формирование популяции решений, оценку и проведение множества операций, имитирующих процессы эволюции живой природы).

В [20] приводится структурная схема криптоанализа на основе метода муравьиных колоний, а также получена информационно-логическая граф-схема алгоритма криптоанализа. Далее, как и в предыдущих работах, осуществляется построение матриц следования, логической несовместимости, а также матрицы независимости, для которой число внутренней устойчивости соответствующего данной матрице графа (число вершин в наибольшем внутренне устойчивом множестве) $\lambda = 4$, приводится также оценка числа процессоров, необходимых для параллельной реализации алгоритма.

Для определения оценки числа процессоров, обеспечивающих реализацию алгоритма при имеющихся временных ограничениях, используются, как и ранее методы, описанные в [13]. Рассматривается задача: найти необходимое наименьшее число процессоров вычислительной системы, а также план реализации операторов на них для алгоритма криптоанализа при построенном информационно-логическом графе и заданном времени $T_{зад}$. В [20] приводится решение данной задачи (на основе определения весов вершин, отражающих время выполнения операций, определения критического пути, ранних и поздних сроков окончания выполнения операций, проведения фиктивных связей в информационно-логическом графе), для заданного времени $T_{кр}$ приводится план выполнения операторов.

4. ПРИМЕНЕНИЕ АЛГОРИТМА ПЧЕЛИНЫХ КОЛОНИЙ ДЛЯ КРИПТОАНАЛИЗА БЛОЧНЫХ КРИПТОСИСТЕМ

Как отмечено в ряде работ (например, в [22, 24]), недостатком методов эволюционной адаптации и генетических алгоритмов является наличие «слепого» поиска, что приводит к увеличению времени поиска, формированию множества одинаковых, а также плохо приспособленных решений, что приводит к попаданию в локальный оптимум. В области роевого интеллекта одной из последних разработок является алгоритм колонии пчел, который довольно успешно в последнее время используется для определения глобальных экстремумов многомерных функций.

Обзор некоторых публикаций, посвященных пчелиным алгоритмам, приводится в [22] (решение комбинаторных теоретико-графовых задач, задача размещения, решаемая с помощью моделирования поведения пчелиной колонии, задача разложения составных чисел на простые сомножители с использованием пчелиных колоний). Отличительные особенности алгоритмов муравьиных колоний, пчелиных колоний и генетического поиска описаны в [5]. Возможный подход для реализации криптоанализа блочных алгоритмов шифрования, сведение этой задачи к задаче нахождения экстремума немонотонной функции, решаемой с помощью алгоритма пчелиного роя, а также оптимизационная модель, применяемая для криптоанализа, описаны в [24]. Процесс криптоанализа реализуется аналогично [22], при этом целевая функция R определяется для каждого варианта текста, сформированного на каждом шаге с помощью алгоритма пчелиных колоний. Таким образом, ключ, обеспечивающий получение исходного текста с максимальным значением функции R, является искомым. Формирование множества перспективных областей-источников осуществляется с помощью пчел-разведчиков на первом уровне, исследование окрестностей данных областей производится с помощью рабочих пчел (пчел-фуражиров) на втором уровне. При этом нахождение источника с максимальным количеством нектара является основной целью колонии пчел. Таким образом, решение задачи криптоанализа представляет собой последовательность символов, пройденных при перемещении агента-пчелы в пространстве поиска (сформированный вариант ключа). Целью поиска, таким образом, является определение оптимальной комбинации (последовательности прохождения) символов, соответствующих оптимальному варианту текста, с максимальным значением R.

В соответствие с [5, 22, 23] основными операциями алгоритма колонии пчел являются следующие.

1. Формируется пространство поиска и популяция пчел.

2. На основе ЦФ, определяющей оптимальность исходного текста, осуществляется оценка целевой функции пчел в популяции.

3. Нахождение наиболее перспективных участков для проведения поиска в их ближайшей окрестности.

4. Отправка пчел-разведчиков и поиск ими перспективных позиций, в окрестности которых будет осуществляться дальнейший поиск.

5. С каждого участка осуществляется выбор пчел с лучшими значениями ЦФ.

6. Отправка рабочих пчел (пчел-фуражиров) для случайного поиска и оценка их ЦФ.

7. Формируется новая популяция пчел.

8. Если выполняются условия окончания работы алгоритма, переход к 9, иначе к 2.

9. Конец.

Отметим, что в [24] приводится структурная схема алгоритма колонии пчел для организации поисковых процедур, а также оценки временной сложности алгоритма пчелиных колоний (от $T \approx O(n^{\lg n})$, до $T \approx O(n^3)$).

Таким образом, в соответствии с [22, 24] можно привести следующее описание алгоритма колонии пчел. На первоначальном этапе работы алгоритма производится случайное размещение N пчел на m участках. На следующем шаге осуществляется определение ЦФ участков. Далее элитные участки (участки с большими значениями ЦФ) отбираются для более детального поиска решений в их окрестностях, то есть на эти участки от-

правляется большее количество пчёл. На следующем шаге проводится оценка значений ЦФ и осуществляется выбор лучших пчёл на основе значений ЦФ участков, которые они исследуют. На основе данного множества пчёл производится формирование новой популяции решений для следующей итерации алгоритма. Далее рабочие пчелы отправляются в окрестности элитных участков и осуществляют случайный поиск для формирования новых решений. Данная операция продолжается до достижения критерия останова алгоритма.

Отметим, что в [23, 24] приводится описание реализации этапов данного алгоритма для решения задачи криптоанализа, а также приводится демонстрационный пример, в котором при заданном блоке шифртекста определяется блок исходного текста с помощью пчелиного алгоритма (аналогично примеру, приведенному в [19, 22]), и на их основе соответствующий секретный ключ. Данный пример, таким образом, иллюстрирует возможность применения метода пчелиной колонии для реализации криптоанализа блочного шифрования, при котором применение секретного ключа осуществляет реализацию шифров перестановок для блока текста, а также наличие исходного и полученного текста позволяет определить секретный ключ.

Как и ранее в [22], в [24] отмечается, что при реализации алгоритма существенным является тот момент, что в задаче криптоанализа осуществляется поиск экстремума немонотонной функции, то есть построение списка E с наилучшим значением ЦФ не означает его оптимальность на последующих итерациях. Отличительные особенности алгоритма, возникающие при реализации в связи с этим, отмечены в [22] (такие как: достаточно большое пространство поиска для предотвращения попадания в локальный оптимум; применение операций, применяемых в эволюционном моделировании, для предотвращения попадания в локальный оптимум; реализация алгоритма как аналога генетического алгоритма при достаточно большом числе итераций и достаточно большом числе списков). В [24] также отмечается тот момент, что поскольку задача криптоанализа является оптимизационной задачей и в общем случае может интерпретироваться как задача формирования упорядоченных списков, то, как отмечено в [22], алгоритмы пчелиных колоний могут являться эффективным способом поиска рациональных решений для данного класса задач.

Отметим, что возможность параллельной реализации алгоритма пчелиных колоний, применение которого для реализации методов криптоанализа описано в [22], исследована в [23, 27]. Как и ранее, в соответствии со структурной схемой на глобальном уровне можно отметить следующие параллельно выполняемые этапы:

– параллельное размещение n_r пчел-разведчиков случайным образом в пространстве поиска;

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

– параллельное формирование областей D_i и выбор в них лучших позиций a_i^* с лучшим значением ЦФ R_i^*;

– параллельное размещение n_{rl} агентов-разведчиков в пространстве поиска для выбора n_{rl} позиций.

С учетом данных преобразований для структурной схемы алгоритма составляется информационно-логическая граф-схема G, в которой отображаются связи по управлению и по информации, а также матрица следования S, матрица логической несовместимости L. Путем дизъюнктивного сложения симметричной матрицы следования S' и L получим матрицу независимости M, по которой можно определить множества операторов алгоритма, которые допускают параллельное выполнение. Размерность максимального внутренне устойчивого множества определяет максимальное число процессоров, используемых для реализации алгоритма [27].

Как и ранее, в соответствии с [16] для повышения быстродействия и эффективности алгоритма за счет минимизации времени работы T может быть исследована возмож-

ность 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). Как и в предыдущих случаях, для повышения эффективности реализации алгоритма пчелиных колоний на локальном уровне в соответствии с [10] 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 план выполнения операторов на них; для решения данной задачи также используются методы, описанные в [13]. В [23, 27] приводится утверждение: при реализации параллельного алгоритма криптоанализа на основе метода пчелиных колоний необходимое минимальное число процессоров может быть определено как $\max(n_r, n_f, n_b)$, где n_r – количество агентов-разведчиков; n_f – количество рабочих пчел-фуражиров; n_b – количество базовых позиций. При этом общее время реализации алгоритма в общем случае составляет $T = Q * T_{кр}$, где Q – количество итераций (в общем случае не превышающее длину блока текста), $T_{кр}$ – длина критического пути в информационно-логическом графе G, определенная в соответствии с правилами анализа программ.

ЗАКЛЮЧЕНИЕ

Таким образом, в данной статье был представлен обзор авторских работ, посвященных решению задачи криптоанализа блочных алгоритмов шифрования на основе новых технологий искусственного интеллекта – биоинспирированных методов (генетических алгоритмов, алгоритмов муравьиных и пчелиных колоний), имитирующих процессы эволюции живой природы. Несмотря на то, что для данных технологий в литературе и сети Интернет не удалось найти 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 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 статье описаны основные технологии применения данных методов для решения задачи криптоанализа на основе параллельной реализации как на локальном, так и на глобальном уровне, представлены также некоторые экспериментальные результаты.

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

СПИСОК ЛИТЕРАТУРЫ

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

2. *Курейчик, В. В.* Концепция природных вычислений, инспирированных природными системами / В. В. Курейчик, В. М. Курейчик, С. И. Родзин // Известия ЮФУ. – 2009. – № 4. – С. 16–24.

3. *Курейчик, В. М.* Эволюционные алгоритмы: генетическое программирование (обзор) / В. М. Курейчик, С. И. Родзин // Известия РАН. Теория и системы управления. – 2002. – № 1. – С. 127–137.

4. *Курейчик, В. В.* Алгоритм параметрической оптимизации на основе модели поведения роя светлячков / В. В. Курейчик, Д. В. Заруба, Д.Ю. Запорожец // Известия ЮФУ. – 2015. – № 6(167). – С. 6–15.

5. *Чернышев, Ю. О.* Биоинспирированные алгоритмы решения задач криптоанализа классических и асимметричных криптосистем: монография / Ю. О. Чернышев, А. С. Сергеев,

Е. О. Дубров, А. В. Крупенин, С. А. Капустин, А. Н. Рязанов. – Краснодар : КВВУ. – 2015. – 132 с.

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

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

8. *Чернышев, Ю. О.* Разработка теоретических основ и принципов реализации алгоритмов криптоанализа на основе биоинспирированных методов / Ю. О. Чернышев, А. С. Сергеев, А. Н. Рязанов, В. М. Москалев // Информационные и математические технологии в науке и управлении / Труды XX Байкальской Всероссийской конференции. Часть III. – Иркутск : ИСЭМ СО РАН, 2015. – С. 196–204.

9. *Бабенко, Л. К.* Современные алгоритмы блочного шифрования и методы их анализа / Л. К. Бабенко, Е. А. Ищукова. – М. : Гелиос АРВ, 2006. – 376 с.

10. *Чернышев, Ю. О.* Исследование возможности применения генетических алгоритмов для реализации криптоанализа блочных криптосистем / Ю. О. Чернышев, А. С. Сергеев, Н. Н. Венцов, А. Н. Рязанов // Вестник Донского государственного технического университета. – 2015. – № 3(82). – С. 65–72.

11. *Сергеев, А. С.* Исследование и разработка методов генетического поиска для организации криптоанализа блочных криптосистем в системах управления безопасностью и защиты информации на примере стандарта шифрования DES / А. С. Сергеев // Третья Международная конференция по проблемам управления: Пленарные доклады и избранные труды. – М. : Институт проблем управления, 2006. – С. 328–335.

12. *Сергеев, А. С.* Применение методов генетического поиска для организации криптоанализа блочных криптосистем на примере стандарта DES / А. С. Сергеев // Научная мысль Кавказа: Приложение. – 2006. – № 15. – С. 185–193.

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

14. *Сергеев, А. С.* Разработка генетического метода криптоанализа блочных криптосистем и исследование возможности их параллельной реализации в системах защиты информации на примере стандарта DES / А. С. Сергеев // Системный анализ в проектировании и управлении: Труды 10 Международной научно-практической конференции. – СПб. : Изд-во Политехн. ун-та. – 2006. – С. 258–265.

15. *Чернышев, Ю. О.* Разработка метода криптоанализа блочных шифров в системах защиты информации на основе параллельного генетического поиска / Ю. О. Чернышев, А. С. Сергеев, А. Н. Рязанов, В. М. Москалев // Сборник докладов XVII Международной конференции по мягким вычислениям и измерениям. – Т. 1. – СПб. : Изд-во СПбГЭТУ «ЛЭТИ», 2015. – С. 408–411.

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

17. *Сергеев, А. С.* Разработка методов криптоанализа на основе генетического поиска при реализации стратегий и технологий информационной защиты на примере стандартов шифрования России / А. С. Сергеев // Коммуникативные стратегии информационного общества: Труды международной научно-технической конференции. – СПб. : изд-во политехнического университета, 2007. – С. 56–65.

18. *Чернышев, Ю. О.* Применение методов генетического поиска для реализации криптоанализа блочных методов шифрования / Ю. О. Чернышев, А. С. Сергеев, А. Н. Ря-

занов // Всероссийская научная конференция по проблемам управления в технических системах (ПУТС-2015): материалы конференции. –СПб. : Изд-во СПбГЭТУ, 2015. – С. 274-277.

19. *Чернышев, Ю. О.* Применение метода муравьиных колоний для реализации криптоанализа блочных криптосистем / Ю. О. Чернышев, А. С. Сергеев, Е. О. Дубров, А. Н. Рязанов // Программные продукты и системы: международный научно-практический журнал. – 2014. – № 1(105). – С. 10–19.

20. *Чернышев, Ю. О.* Разработка и исследование параллельного алгоритма муравьиных колоний для криптоанализа блочных криптосистем / Ю. О. Чернышев, А. С. Сергеев, А. Н. Рязанов, С. А. Капустин // Программные продукты и системы: международный научно-практический журнал. – 2015. – № 4(112). – С. 148–157.

21. *Бабенко, Л. К.* Параллельные алгоритмы для решения задач защиты информации / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидоров. – М. : Горячая линия – Телеком, 2014. – 304 с.

22. *Чернышев, Ю. О.* Исследование возможности применения бионических методов пчелиных колоний для реализации криптоанализа классических шифров перестановок / Ю. О. Чернышев, А. С. Сергеев, Е. О. Дубров, А. Н. Рязанов // Вестник Дон. гос. техн. ун-та. – 2014. – Т. 14. – № 1(76). – С. 62–75.

23. *Сергеев, А. С.* Исследование возможности применения бионических методов пчелиных колоний для реализации криптоанализа блочных методов шифрования / А. С. Сергеев // Радиоэлектронные устройства и системы для инфокоммуникационных технологий (REDS-2016): международная конференция. – М., 2016. – С. 587–593.

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

25. *Сергеев, А. С.* Исследование возможности применения методов эволюционной оптимизации для реализации криптоанализа блочного стандарта шифрования AES // Системный анализ в проектировании и управлении: сб. научн. тр. XX Междунар. науч.-практ. конф. – Ч. 1. – СПб. : Изд-во Политехн. ун-та, 2016. – С. 456–470.

26. *Капустин, С. А.* Применение методов эволюционной оптимизации для реализации криптоанализа блочного метода шифрования AES / С. А. Капустин, А. С. Сергеев, А. Н. Рязанов, Е. О. Дубров // Известия СПбГЭТУ «ЛЭТИ». – 2016. – № 8. – С. 25–40.

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

28. *Бабенко, Л. К.* Применение параллельных вычислений при решении задач защиты информации / Л. К. Бабенко, Е. А. Ищукова, И. Д. Сидоров // Программные системы: теория и приложения. – 2013. – № 3(17). – С. 25–42.

Чернышев Юрий Олегович – почетный профессор ДГТУ, заслуженный деятель науки, д-р техн. наук, профессор, кафедра «Автоматизация производственных процессов», Донской государственный технический университет, г. Ростов-на-Дону.
Тел.: (918) 599-16-45

Chernyshev Yury Olegovich – honorary Professor DSTU, honored scientist , doctor of technical Sciences, Professor, the dept. «Automation of Production Processes», Don State Technical University.
Tel. (918) 599-16-45.

Сергеев Александр Сергеевич – *контактный автор* – канд. техн. наук, научный сотрудник, Донской государственный технический университет, г. Ростов-на-Дону.
Тел.: (928) 758-57-19
E-mail: sergeev00765@mail.ru

Рязанов Александр Николаевич – помощник генерального директора открытого акционерного общества «711 Военпроект», г. Ростов-на-Дону.
Тел.: (928) 279-87-55

Дубров Евгений Олегович – инженер Федерального государственного унитарного предприятия «Ростовский-на-Дону научно-исследовательский институт радиосвязи».
Тел.: (918) 506-31-03

Sergeev Aleksandr Sergeevich – *contact the author* – candidate of technical Sciences, scientific researcher, Don State Technical University.
Tel.: (928) 758-57-19
E-mail: sergeev00765@mail.ru

Ryazanov Alexandr Nikolaevich – General director assistant of Open joint-stock company «711 Voyenproyekt», Rostov-on-Don.
Tel.: (928) 279-87-55

Dubrov Evgeny Olegovich – Engineer of Federal state unitary the company «Rostov research institute of the radio communication», Roston-on-Don.
Tel.: (918) 506-31-03