УДК 004.021

Е.А. Толоманенко

Дифференциальный анализ трех раундов шифра «Кузнечик»

«Кузнечик» – это новый симметричный алгоритм шифрования, принятый в качестве стандарта шифрования ГОСТ Р 34.12–2015, построенный по принципу SP-сети. До сих пор нет публикаций о дифференциальных свойствах алгоритма «Кузнечик». В данной работе исследованы и описаны свойства основных операций и предложен метод дифференциального анализа трех раундов алгоритма шифрования «Кузнечик». В результате исследования дифференциальных свойств нелинейной функции S и линейной функции L было установлено, что возможна ситуация, когда один ненулевой байт разности в результате функции L разворачивается в 16 ненулевых байтов, проходит через блок замены S и затем сворачивается снова в один ненулевой байт. Разработанная схема позволяет затрагивать активный S-блок минимальное количество раз. Таким образом, общая сложность анализа, включая поиск правильных пар текстов и поиск битов секретного ключа шифрования составляет $2^{-108} + 6*2^{-120}$ зашифрований.

Ключевые слова: криптография, блочный шифр, SP-сеть, криптоанализ, дифференциальный криптоанализ, шифр «Кузнечик», ГОСТ Р 34.12–2015.
doi: 10.21293/1818-0442-2018-21-2-22-26

Алгоритм шифрования «Кузнечик» представляет собой часть стандарта шифрования ГОСТ Р 34.12–2015, официально вступившего в силу 01.01.2016, поэтому исследование его надежности на сегодняшний день является актуальной задачей. Описание алгоритма шифрования «Кузнечик» как части нового принятого стандарта шифрования содержится в документе Технического комитета по стандартизации ТК 26 «Криптографическая защита информации» в ГОСТ Р 34.12–2015 [1]. Есть несколько статей, посвященных различным способам реализации алгоритма «Кузнечик», в том числе и с использованием специальных таблиц предвычислений [2]. Метод дифференциального криптоанализа был впервые предложен Эли Бихамом и Ади Шамиром, которые применили его к анализу алгоритма шифрования DES [3, 4]. Также криптоанализ был рассмотрен в работах [5–7]. На данный момент в открытой печати не фигурируют публикации, содержащие информацию о дифференциальных свойствах и о итоговых количественных оценках сложности дифференциального криптоанализа алгоритма шифрования «Кузнечик» и предлагающие применение данного метода криптоанализа к некоторому сокращенному количеству раундов шифра «Кузнечик».

В данной работе предложен метод построения трехраундового дифференциала для алгоритма шифрования «Кузнечик». Разработанная схема анализа основана на использовании дифференциальных свойств преобразований S и L алгоритма «Кузнечик» и предназначена для того, чтобы можно было определить правильную пару текстов для дальнейшего анализа, целью которого является определение секретного ключа шифрования. Схема разработана таким образом, чтобы затрагивать активные нелинейные компоненты (S-блоки) минимальное количество раз. В результате для предложенной схемы вероятность нахождения правильных пар текстов составляет 2^{-108} зашифрований. Также был разработан алгоритм нахождения секретного ключа, сложность которого составляет $6*2^{-120}$ зашифрований с использованием шифра «Кузнечик». Таким образом, общая сложность анализа, включая поиск правильных пар текстов и поиск битов секретного ключа шифрования, составляет $2^{-108} + 6*2^{-120}$ зашифрований. Сложность предложенной схемы является достаточно высокой в сравнении с возможностями современных вычислительных средств, но гораздо более низкой, чем сложность компрометации ключа методом полного перебора.

Описание алгоритма шифрования «Кузнечик»

Кузнечик – это симметричный блочный шифр с длиной мастер-ключа, равной 256 бит, и длиной блока – 128 бит. Шифр построен по принципу SP-сети, что позволяет выполнить преобразование всего входного блока целиком, а не только его части.

Шифрование реализуется с использованием 9 раундов и поочередным применением трех преобразований: XOR-блока данных с раундовым ключом, с помощью блока замены (S) и линейное преобразование (L). Десять раундовых ключей вырабатываются из 256-битного мастер-ключа.

Расшифрование осуществляется наоборот, снизу вверх, с помощью преобразований, обратных к тем, которые применялись при зашифровании.

Более подробно с процессами зашифрования и расшифрования, их программной реализацией, а также с применяемыми в алгоритме «Кузнечик» преобразованиями можно ознакомиться в [8–11].

Разработка алгоритма для дифференциального криптоанализа шифра «Кузнечик»

Общий метод дифференциального криптоанализа симметричных блочных шифров описан в [12].

Для применения метода дифференциального криптоанализа применительно к шифру «Кузнечик» необходимо пару открытых текстов X и X', объединенную дифференциалом ΔX, отправить на вход алгоритма. На выходе получим пару текстов Y и Y', соответствующую входным текстам и объединенную дифференциалом ΔY. Значение раундового

ключа не влияет на дифференциалы, так как при выполнении операции XOR его биты будут взаимно уничтожены – $X \oplus K_i \oplus X' \oplus K_i$.

Анализ алгоритма подразумевает создание таблицы вероятностей для блока замены *S*. В строках таблицы обозначены значения ΔA, являющиеся входом в блок подстановок, а в столбцах – значения ΔC, получаемые на выходе из блока подстановок, соответствующие ΔA. Ячейки на пересечении показывают, сколько пар дифференциалов $\Delta A/\Delta C$ имеют данные входные и выходные значения. Таблица отражает значение вероятности, с которой при конкретном дифференциале ΔA, поданном на вход блока *S*, на выходе будет получено конкретное значение ΔC. Алгоритм получения дифференциальных характеристик *S*-блоков замены описан в работе [13]. Малая часть полученной таблицы со значениями вероятностей содержится в таблице.

Фрагмент таблицы со значениями вероятностей, построенной для блока замены *S*

ΔC/ΔA	0	1	2	…	3e	3f	…	fe	ff
0	256/ 256	0/256	0/256	…	0/256	0/256	…	0/256	0/256
1	0/256	0/256	2/256	…	2/256	4/256	…	0/256	2/256
…	…	…	…	…	…	…	…	…	…
ff	0/256	2/256	2/256	…	0/256	4/256	…	0/256	0/256

В результате криптоанализа должен быть скомпрометирован раундовый ключ. Процесс компрометации в данной ситуации подразумевает, что для конкретного значения ΔA соответствующие ΔC имеют разную вероятность быть полученными. Таблица свидетельствует о том, что в данном случае вероятность может быть равна 2/256, 4/256, 6/256 и 8/256, а также может быть равной нулю. Пара дифференциалов ΔA и ΔC позволяет предположить значения $A \oplus K_i$ и $A' \oplus K_i$. При известных A и A' это позволяет определить K_i [14].

На сегодняшний день в открытой печати нет информации о дифференциальных свойствах алгоритма шифрования «Кузнечик». Существующий метод дифференциального криптоанализа применялся к различным известным шифрам [15], а схема применения данного метода криптоанализа к шифру «Кузнечик», аналогов которой не существует, была разработана и описана в данной работе. В результате исследования свойств функций *S* и *L* было установлено, что возможна ситуация, когда 1 байт в результате функции *L* разворачивается на 16 байт, проходит через блок замены *S* и затем сворачивается в 1 байт. Разработанная схема позволяет затрагивать *S*-блок минимальное количество раз. Разработанный метод анализа для трех раундов шифрования изображен на рис. 1. На основании данной схемы был разработан алгоритм.

Первый этап соответствует первому раунду:

1. Случайно сгенерированный текст X и парный ему текст X' отличаются лишь значением ΔA, Эти значения подаются на вход.

2. После уничтожения ключей в результате использования блока замены *S* данный байт меняется на другой по таблице вероятностей

3. Далее преобразование *L* раскладывает данный байт на 16 байт.

Второй этап соответствует второму раунду:

1. После уничтожения ключа преобразование *S* изменит каждый из 16 байтов на другой в соответствии с таблицей.

2. После преобразования *L* во 2-м раунде 16 байт наиболее вероятных значений преобразуются снова в 1 байт.

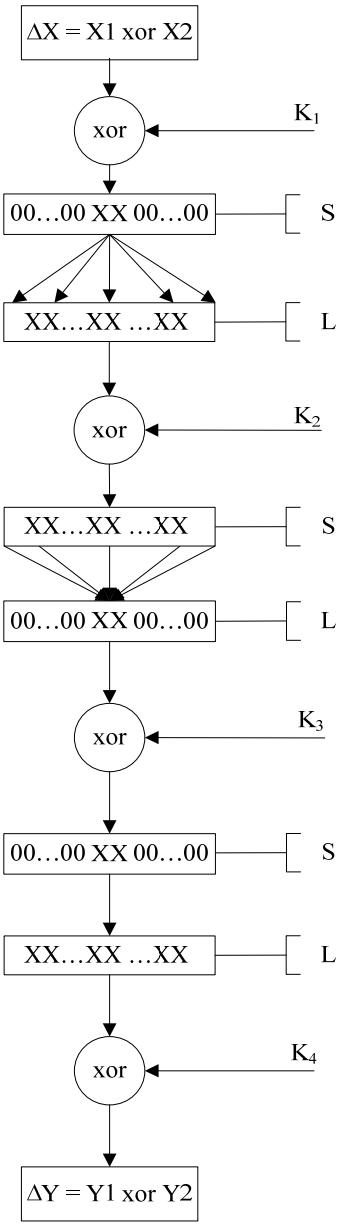

Рис. 1. Схема дифференциального анализа трех раундов шифрования

Третий этап соответствует третьему раунду:

1. Преобразованное на втором этапе значение после уничтожения ключа меняется на другое по таблице вероятности

2. В итоге преобразование L раскладывает этот 1 байт на 16, и на выходе будет получен результат по итогам трех раундов шифрования.

Таким образом, для рассматриваемой схемы анализа получается всего 18 активных S-блоков вместо 33, как было рассмотрено ранее.

Даже если предположить, что можно подобрать значения дифференциалов, которые будут соответствовать рис. 1, с минимальными значениями вероятностей для каждого из активных S-блоков $2/256 = 1/2^7$, получится трехраундовый дифференциал с вероятностью в $(1/2^7)^{18} = 1/2^{126}$, что меньше, чем ранее предположенное значение $1/2^{165}$. Нужно отметить, что удалось получить трехраундовую характеристику, вероятность появления которой равна $1/2^{108}$, что означает, что при использовании активных S-блоков были задействованы не самые минимальные вероятности.

Алгоритм нахождения правильных пар текстов для трехраундовой характеристики

Алгоритм нахождения правильных пар тестов для проведения анализа не может быть прямо реализован из-за маленькой вероятности получения правильных пар текстов. Мощности обычного персонального компьютера для этого недостаточно. Поэтому для осуществления проверки работоспособности предложенного метода был разработан способ «от обратного». Применение данного способа подразумевает, что будут подобраны такие правильные пары текстов, которые при конкретных значениях раундовых секретных ключей будут формировать необходимые значения дифференциалов.

На основе данного способа был разработан алгоритм нахождения правильных пар текстов. Данный алгоритм, найденные значения и проверка его работоспособности подробно описаны в работе [14].

Всего было найдено 13 пар значений $\Delta A/\Delta C$. Например, для ΔA=f3ab8c55c199996f0c5a4f2381976846 найдено ΔC=51ac91f0df24701900ad86a256131163, а для ΔA=1a76bc71665284b01a3e595982599369 найдено ΔC=ba5a9d5e6d2b64310ac6b9cb72dc5a7a1.

После нахождения всех байтов исходных текстов, составляющих данные дифференциалы, можно сделать вывод, что общее число всех вариантов значений X и X': P=2*2*4*4*2*2*2*2*2*2*2*2*2*4*2*2 = = 524288.

Из найденных значений $\Delta A/\Delta C$ легко можно определить значения дифференциалов на входе и выходе 3-раундового алгоритма «Кузнечик» $\Delta X/\Delta Y$, а также вероятность их появления.

Нахождение конкретных текстов на входе и выходе трехраундового алгоритма было выполнено с помощью прямых и обратных преобразований над найденными значениями во втором и третьем раунде.

Алгоритм компрометации секретного ключа на основе найденных правильных пар текстов

Метод дифференциального криптоанализа, как правило, заключается в компрометации раундовых ключей с целью расшифрования информации. Описать технологию криптоанализа с помощью найденных ранее правильных пар текстов можно следующим образом.

В рассмотренных 3 раундах алгоритма шифрования используется 4 раундовых ключа (см. рис. 1). Необходимо обратить внимание на то, что в алгоритме «Кузнечик» первыми двумя раундовыми ключами являются левая и правая части 256-битного мастер-ключа, разделенного напополам. На этом факте основан разработанный мной алгоритм, который подразумевает поиск первого ключа K1, после него – K2, с помощью которых затем можно выработать остальные ключи – K3 и K4. Предложенный алгоритм состоит из таких этапов, как:

1. Проведение обратных операций $S_{\text{inv}}(L_{\text{inv}}(\Delta A))$ и $L_{\text{inv}}(\Delta A)$ для получения входа и выхода преобразования S первого раунда соответственно.

2. На вход алгоритма (см. рис. 1) подается ранее подобранная пара текстов X и X', которая при сложении с числом, получившимся в результате операции $S_{\text{inv}}(L_{\text{inv}}(\Delta A))$, дает значение ключа K1.

3. Получившееся значение $S_{\text{inv}}(L_{\text{inv}}(\Delta A))$ состоит из одного байта и его вероятность равна 6 по таблице, содержащей значения вероятностей. Это говорит о том, что будет 6 возможных значений одного байта ключа K1. Таким образом, количество всех возможных вариантов 128-битного ключа K1 будет равно $2^{120}\times 6$.

4. Производится поиск правильного ключа K1, подразумевающий следующие операции:

Подаются на вход 2 подобранных текста X и X', складываются с первым возможным ключом K1. Полученные значения проходят преобразования S и L первого раунда. Результат складывается со значениями A и A', объединенными дифференциалом ΔA, поступающими на вход преобразования S второго раунда. Данные преобразования позволяют найти одно из возможных значений ключа K2. Ключи K1 и K2 объединяются в 256-битный мастер-ключ и из него вырабатываются ключи K3 и K4. Далее два возможных шифртекста Y и Y', полученных в результате применения алгоритма нахождения правильных пар текстов, складываются с ключом K4. Полученные значения претерпевают преобразования L_{inv} и S_{inv} третьего раунда, складываются с ключом K3 и затем проходят преобразование L_{inv} второго раунда.

Результаты преобразования L_{inv} второго раунда сравниваются со значениями, составляющими дифференциал ΔC. Если значения равны, то ключи сохраняются как вероятно правильные. Если значения не равны, то алгоритм повторяется заново.

Фактически опробование ключей сводится к выполнению всех операций трехраундового зашифрования. Поэтому сложность алгоритма нахождения ключей будет задействовать максимум $2^{120}\times 6$ зашифрований. При данном условии будут скомпрометированы все 4 ключа с гораздо меньшей сложностью, чем при условии полного перебора, сложность которого равна 2^{256}.

Общая сложность дифференциального криптоанализа трех раундов алгоритма шифрования «Кузнечик» может быть оценена как $2^{120}\times6+2^{108}$ зашифрований.

Выводы

В результате работы над данным проектом впервые были исследованы и получены дифференциальные свойства алгоритма шифрования «Кузнечик». На основе проведенных исследований была выявлена связь между преобразованиями *S* и *L*, которая позволила разработать алгоритм дифференциального криптоанализа трех раундов шифра «Кузнечик», ранее никем не предложенный в открытых литературных источниках.

На основе предложенной схемы трехраундового дифференциала были разработаны алгоритм нахождения правильных пар текстов для анализа шифра и алгоритм нахождения секретного ключа с гораздо меньшей сложностью, чем сложность при поиске ключа полным перебором. Разработанные алгоритмы позволяют оценить общую сложность проведения анализа, которая составляет $2^{108} + 6*2^{120}$. Результаты работы использованы при выполнении исследовательских работ по гранту РФФИ №17-07-00654-а «Разработка и исследование последовательных и параллельных алгоритмов анализа современных симметричных шифров с использованием технологий MPI, NVIDIA CUDA, SageMath».

Литература

1. Криптографическая защита информации. Блочные шифры. ГОСТ Р 34.12–2015 [Электронный ресурс]. – Режим доступа: http://tc26.ru/en/standard/gost/GOST_R_34_12_2015_ENG.pdf, свободный (дата обращения: 04.04.2018).

2. Ishchukova E.A. Fast Implementation and Cryptanalysis of GOST R 34.12-2015 Block Ciphers / E.A. Ishchukova, L.K. Babenko, M.V. Anikeev // 9th International Conference on Security of Information and Networks SIN 2016. – Newark, Nj: 20–22 July 2016. – P. 104–111. – URL: https://dl.acm.org/citation.cfm?doid=2947626.2947657

3. Biham E. Differential cryptanalysis of DES-like cryptosystems / E. Biham, A. Shamir // Journal of Cryptology 1991. – Vol. 4, No. 1. – PP. 3–72. – URL: http://www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/Biham-DC.pdf

4. Biham E. Differential cryptanalysis of the full 16-round DES / E. Biham, A. Shamir // Advances in cryptology, proceedings of CRYPTO'92 1992. – Vol 740. – PP. 487–496. (URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.720.215&rep=rep1&type=pdf)

5. Biham E. Differential Cryptanalysis in Stream Ciphers / E. Biham, O. Dunkelman // Cryptology ePrint Archive, Report 2007/218 2007. – URL: https://eprint.iacr.org/2007/218.pdf

6. Biham E. Differential Cryptanalysis of Hash Functions / E. Biham, A. Shamir // Differential Cryptanalysis of The Data Encryption Standard, Springer 1993. – P. 133–148. – URL: https://link.springer.com/chapter/10.1007/978-1-4613-9314-6_8

7. Бабенко Л.К. Применение методов криптоанализа для исследования стойкости современных блочных шифров / Л.К. Бабенко, Е.А. Мишустина (Ищукова) // Тезисы докл. X Всерос. науч. конф. «Проблемы информационной безопасности в системе высшей школы». – М.: МИФИ, 2003. – URL: http://cyberrus.com/wp-content/uploads/2015/05/vkb_10_02.pdf

8. Кузнечик (шифр) [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Кузнечик_(шифр), свободный (дата обращения: 04.04.2018).

9. Толоманенко Е.А. Программная реализация шифра «Кузнечик» // Матер. IX Междунар. студ. электрон. науч. конф. «Студенческий научный форум». – 2017. Актуальные проблемы информационной безопасности. – URL: https://www.scienceforum.ru/2017/pdf/36883.pdf

10. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. – М.: ТРИУМФ, 2002. – 648 с. – URL: https://htrd.su/wiki/_media/zhurnal/2012/03/23/todo_prikladnaja_kriptografija/cryptoshn.pdf

11. В ГОСТе сидел «Кузнечик» [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/266359/, свободный (дата обращения: 04.04.2018).

12. Дифференциальный криптоанализ [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Дифференциаль-ный_криптоанализ, свободный (дата обращения: 04.04.2018).

13. Ищукова Е.А. Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147–89 / Е.А. Ищукова, И.А. Калмыков // Инженерный вестник Дона. – 2015. – №4. – URL: https://cyberleninka.ru/article/n/differentsialnye-svoystva-s-blokov-zameny-dlya-algoritma-gost-28147-89).

14. Бабенко Л.К. Дифференциальный анализ шифра «Кузнечик» / Л.К. Бабенко, Е.А. Ищукова, Е.А. Толоманенко // Изв. ЮФУ. Технические науки. – Таганрог: Изд-во ЮФУ, 2017. – №5. – С. 25–37. – URL: http://izv-tn.tti.sfedu.ru/wp-content/uploads/2017/5/3.pdf

15. Бабенко Л.К. Анализ современных криптографических систем с помощью метода дифференциального криптоанализа / Л.К. Бабенко, Е.А. Ищукова // Актуальные аспекты защиты информации в Южном федеральном университете. – Таганрог: ТТИ ЮФУ, 2011. – С. 102–181.

Толоманенко Екатерина Алексеевна
Аспирантка 1-го года обучения
каф. безопасности информационных технологий (БИТ),
Инженерно-технологической академии
Южного федерального университета (ИТА ЮФУ)
Чехова ул., д. 2, г. Таганрог, Россия, 347928
Тел.: +7 (863-4) 37-19-05, +7-908-504-73-92
Эл. почта: kat.tea@mail.ru

Tolomanenko E.A.

Differential analysis of three rounds of cipher «Kuznyechik»

«Kuznyechik» is a new symmetric encryption algorithm, adopted as an encryption standard GOST R 34.12–2015, built on the principle of SP-network. There are still no publications on the differential properties of the algorithm «Kuznyechik». In this paper, the properties of the main operations are researched and described, and a method of differential analysis of three rounds of the algorithm of encryption «Kuznyechik» is proposed. In the issue of the investigation of the differential properties of the nonlinear function *S* and linear function *L*, it was established that a 1 non-zero byte of the difference as a result of the function *L* can be expanded into 16 non-zero bytes, passes through the replacement block *S*, and then folded again into 1 nonzero byte. The developed scheme allows to

affect the active *S*-unit a minimum number of times. Thus, the overall complexity of the analysis, including searching for the correct pairs of texts and searching for bits of the secret encryption key is $2^{108} + 6 * 2^{120}$ encryptions.

Keywords: cryptography, block cipher, SP-network, cryptanalysis, differential cryptanalysis, cipher «Kuznyechik», GOST R 34.12-2015.

doi: 10.21293/1818-0442-2018-21-2-22-26

References

1. Cryptographic protection of information. Block ciphers. GOST R 34.12–2015. Available at: http://tc26.ru/en/standard/gost/GOST_R_34_12_2015_ENG.pdf (accessed: 04 April 2018).

2. Ishchukova E.A., Babenko L.K., Anikeev M.V. Fast Implementation and Cryptanalysis of GOST R 34.12–2015 Block Ciphers. *9th International Conference on Security of Information and Networks SIN 2016.* Newark, Nj, 2016. pp. 104–111. URL: https://dl.acm.org/citation.cfm?doid=2947626.2947657

3. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 1991, vol. 4, no. 1, pp. 3–72. URL: http://www.cs.bilkent.edu.tr/~selcuk/teaching/cs519/Biham-DC.pdf

4 Biham E., Shamir A. Differential cryptanalysis of the full 16-round DES. *Advances in cryptology*. Proc. of CRYPTO'92 conference? 1992? vol. 740, pp. 487–496? URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.720.215&rep=rep1&type=pdf

5. Biham E., Dunkelman O. Differential Cryptanalysis in Stream Ciphers. *Cryptology ePrint Archive*, Report 2007/218 2007. – URL: https://eprint.iacr.org/2007/218.pdf

6. Biham E., Shamir A. Differential Cryptanalysis of Hash Functions. Differential Cryptanalysis of The Data Encryption Standard. *Springer,* 1993, pp. 133–148. URL: https://link.springer.com/chapter/10.1007/978-1-4613-9314-6_8

7. Babenko L.K., Ishchukova E.A. Primenenie metodov kriptoanaliza dlya issledovania stoikosti sovremennikh blochnikh shifrov [The use of cryptanalysis methods to study the persistence of modern block ciphers]. Problemi informacionnoy bezopasnosti v sisteme vishchey shkoli. Tezisi dokladov X Vserossiyskoy nauchnoy conferencii [*The problems of information security in the system of higher education.* Proc. of the tenth AllRussian scientific conference]. Moscow, MIFI, 2003. URL: http://cyberrus.com/wp-content/uploads/2015/05/vkb_10_02.pdf

8. Kuznyechik (cipher). Available at: https://ru.wikipedia.org/wiki/Кузнечик_(шифр) (accessed: 04 April 2018).

9. Tolomanenko E. A. Programnaya realizaciya shifra Kuznyechik [Software implementation of the cipher Kuznyechik]. Studencheskiy nauchniy forum. Materiali IX mezhdunarodnoy studencheskoy elektronnoy nauchnoy konferentsii. [*Student Science Forum*. Proc. of ninth International Student Electronic Scientific Conference]. 2017. URL: https://www.scienceforum.ru/2017/pdf/36883.pdf

10. Schneier B. *Prikladnaya kriptografiya: Protocoli, algoritmy, iskhodnyye teksty na yazyke Ci* [Applied cryptography: Protocols, algorithms, C source code]. Moscow, TRIUMPH, 2002. 648 p. URL: https://htrd.su/wiki/_media/ zhurnal/2012/03/23/todo_prikladnaja_kriptografija/cryptoshn.pdf

11. In the GOST there was a «Kuznyechik». Available at: https://habrahabr.ru/post/266359/ (accessed: 04 April 2018).

12. Differential cryptanalysis. Available at: https://ru.wikipedia.org/wiki/Дифференциальный_криптоанализ (accessed: 04 April 2018).

13. Ishchukova E.A., Kalmikov I.A. Differential properties of S-replacement blocks for the algorithm GOST 28147-89. *The engineer's messenger of the Don*, 2015, no 4. – URL: https://cyberleninka.ru/article/n/differentsialnye-svoystva-s-blokov-zameny-dlya-algoritma-gost-28147-89

14. Babenko L.K., Ishchukova E.A., Tolomanenko E.A. Differential analysis of cipher Kuznyechik. *News of SFedU. Technical science*. Taganrog, Publishing house SFedU, 2017, no. 5, pp. 25–37. URL: http://izv-tn.tti.sfedu.ru/wp-content/uploads/2017/5/3.pdf

15. Babenko L.K., Ishchukova E.A. *Analiz sovremennykh kriptograficheskikh sistem s pomoshch'yu metoda differentsial'nogo kriptoanaliza* [Analysis of modern cryptographic systems using differential cryptanalysis]. Topical aspects of information security in the Southern Federal University, 2011, Taganrog, TTI SFedU, pp. 102–181.

Ekaterina A. Tolomanenko
PhD student,
Department of Security of Information Technologies
Engineering and Technology Academy
of the Southern Federal University
2, Chekhova st., Taganrog, Russia, 347928
Phone: +7 (863-4) 37-19-05, +7-908-504-73-92
Email: kat.tea@mail.ru