неоднородных газоплазменных потоков : монография / В. С. Славин, В. С. Соколов, К. А. Финников и др. ; под ред. В, С. Славина ; Краснояр. гос. техн. ун-т. Красноярск, 2004.

4. Marcusic, T. E. Phenomenological model of current sheet canting in pulsed electromagnetic accelerators / T. E. Marcusic, E. Y. Choueiri // 28th Intern. Electric Propulsion Conf. Toulouse, France, 2003. P. 0293.

5. Marcusic, T. E. Measurements of current sheet canting in pulsed electromagnetic accelerator / T. E. Marcusic, E. Y. Choueiri, J. W. Berkery // Physics of plasmas. 2004. Vol. 11. № 10.

6. Минаков, А. В. Численное моделирование нестационарных процессов, протекающих в канале рельсотрона : дисс. … магистра / А. В. Минаков ; Краснояр. гос. техн. ун-т. Красноярск, 2005.

7. Кузоватов, И. А. Анализ влияния эффекта Холла на структуру неравновесного плазменного слоя в канале МГД-генератора / И. А. Кузоватов, Т. А. Миловидова, В. С. Славин // Вычисл. технологии. Новосибирск, 2007. Т. 12, № 4. С. 73–84.

8. Марчук, Г. И. Методы расщепления / Г. И. Марчук. М. : Наука, 1988.

V. S. Slavin, I. A. Kuzovatov, A. V. Minakov

APPLICATION OF FINITE DIFFERENCE SCHEME WITH EXPONENTIAL FITTING FOR NUMERICAL SIMULATION OF UNSTEADY PROCESSES IN THE MHD CHANNEL

The highly effective numerical algorithm is developed and tested. It allows to solve a wide class of bidimentional non-stationary problems. Mathematical modeling of the non-stationary processes proceeding in the channel linear MHD – the accelerator is lead. In full statement the bidimentional problem of magnetic hydrodynamics in view of effect of the Hall is solved. In the result of modeling the deviation current effect of a layer from a direction, perpendicular to electrodes of the accelerator is found out. The results are will qualitatively coordinated with experimental data.

Keywords: exponential fitting, mathematical simulation of physical processes, computational meth-ods, computational hydrodynamics.

УДК 004.056.55

Т. А. Чалкин, К. М. Волощук

РАЗРАБОТКА АЛГОРИТМА ПОСТРОЕНИЯ УЗЛОВ ЗАМЕН АЛГОРИТМА ШИФРОВАНИЯ ГОСТ 28147–89

Рассмотрены основные требования к проектированию узлов замен (S-блоков) блочных шифров и разработанный на их основе алгоритм построения узлов замен алгоритма шифрования ГОСТ 28147–89, обеспечивающий заданный уровень устойчивости шифра к линейному и дифференциальному криптоанализу.

Ключевые слова: шифрование, таблица замен, булева функция, криптостойкость, криптоанализ, алгоритм.

Отечественный стандарт алгоритма блочного симметричного шифрования – ГОСТ 28147–89 – [1] согласно действующему в Российской Федерации законодательству является обязательным к применению при криптографической защите секретных сведений любой степени секретности и рекомендуется к применению при защите конфиденциальных сведений, не составляющих государственную тайну, в частности при защите коммерческой тайны. При этом, помимо стандартной для всех симметричных шифров ключевой информации – последовательности бит фиксированной длины, называемой ключом шифрования (для ГОСТ 28147–89 длина ключа составляет 256 бит), этот стандарт в качестве элемента ключевой информации предусматривает использование таблицы замен, представляющей собой матрицу чисел размерности 8 × 16, которая содержит в своих ячейках числа от 0 до 15. Строки таблицы замен называются узлами замен. Назначение этой таблицы в целом аналогично назначению S-блоков алгоритма DES и подобных ему шифров, основанных на сети Фейстеля, – это перемешивание битов данных в ходе раунда шифрования путем замены отрезков блока данных по таблице, определяющей соответствие выходного значения входному.

Таблица замен является долговременным ключевым элементом, т. е. действует в течение гораздо более длительного срока, чем ключ шифрования. Предполагается, что она является общей для всех узлов шифрования в рамках одной криптосистемы. Также известно, что даже при нарушении секретности таблицы замен (когда она становится известной криптоаналитику) стойкость шифра остается достаточно высокой и не снижается ниже определенного предела [2].

Согласно действующему российскому законодательству, используемые при шифровании секретных сведе-

ний таблицы замен предоставляются уполномоченной организацией субъекту, осуществляющему криптографическую защиту информации. При шифровании сведений, не составляющих государственной тайны, встает задача выбора ключевой информации, обеспечивающей криптографическую стойкость зашифрованных данных. Стандарт ГОСТ 28147–89 не определяет требований к выбору значений ключей и таблиц замен. И если для ключа шифрования существует ряд общепринятых критериев качества, общих для всех блочных симметричных шифров (это равная вероятность появления 0 и 1 в последовательности бит и отсутствие статистических закономерностей в ней), то для таблиц замен эти критерии требуют определенной адаптации при их применении к построению таблиц замен шифра ГОСТ 28147–89 в силу его некоторых особенностей, о которых будет сказано ниже.

В настоящее время существуют два основных, наиболее распространенных и хорошо разработанных метода криптоанализа – линейный и дифференциальный криптоанализ [3].

Линейный криптоанализ состоит в нахождении линейной зависимости выходных данных от входных, близкой по своим выходным значениям к нелинейной функции шифрования, и в определении битов ключа с использованием этой функции.

Дифференциальный криптоанализ изучает процесс изменения различий для пары открытых текстов, имеющих определенные исходные различия в нескольких битах, в процессе их прохождения через циклы шифрования с одним и тем же ключом.

Необходимо разработать алгоритм выбора таблиц замен для блочного шифра ГОСТ 28147–89, обеспечивающий устойчивость шифрования к линейному и дифференциальному методам криптоанализа. В данной статье представлены результаты текущего этапа работы по созданию такого алгоритма, на котором предполагается независимый выбор по определенным правилам 8 узлов замен, участвующих в построении таблицы замен.

Рассмотрим подробнее отдельный раунд шифрования по ГОСТ 28147–89 (рис. 1).

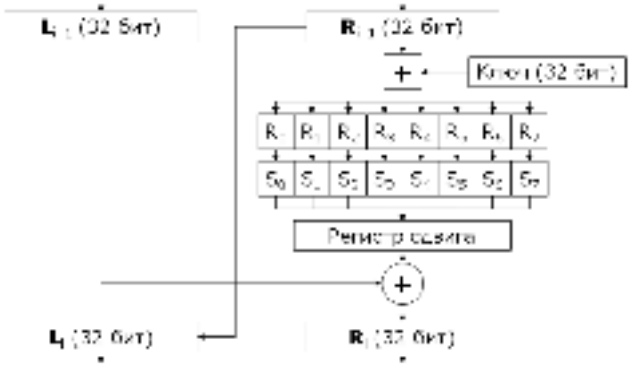

Рис. 1. Схема одного раунда блочного шифра ГОСТ 28147–89

Как и во всех шифрах, построенных на основе сети Фейстеля, на вход i-го раунда шифрования поступают два блока данных длиной 32 бит: левая и правая половины 64-битного блока L_{i-1} и R_{i-1} соответственно, получившиеся в результате выполнения предыдущего раунда. В ходе выполнения i-го раунда блок R_{i-1} сначала суммируется по модулю 2^{32} с подключом раунда (отрезком ключа длиной 32 бит). Затем результат операции суммирования разбивается на 8 отрезков длиной 4 бит $R_0, R_1, \ldots, R_7$, которые поступают на вход узлов замен $S_0, S_1, \ldots, S_7$ используемой таблицы замен (напомним, что узлами замен мы называем строки таблицы замен). Каждый такой узел определяет правило, по которому входному 4-битовому вектору сопоставляется выходной 4-битовый вектор. Результаты замен всех узлов объединяются в 32-битный блок, являющийся выходным значением таблицы замен. Затем этот блок подвергается операции побитового циклического сдвига влево (в сторону старших бит) на 11 бит. Наконец, результат сдвига побитово суммируется по модулю 2 с блоком L_{i-1} и передается на выход раунда шифрования в качестве правой половины выходного блока R_i. В качестве левой половины выходного блока L_i на выход подается значение R_{i-1}.

Рассмотрим теперь процесс замены бит при помощи таблицы замен. Каждый узел замен содержит 16 различных чисел от 0 до 15 в произвольном порядке. Выходное значение для каждого узла определяется следующим образом: входной 4-битный вектор представляется в виде числа от 0 до 15 и из строки узла замен выбирается значение с порядковым номером, равным этому числу (нумерация ведется с нуля). А поскольку элементами узла замен являются числа от 0 до 15, то выход узла в двоичном виде также будет иметь длину 4 бита.

Ключевыми требованиями к операциям преобразования бит в раунде шифрования с точки зрения криптостойкости являются нелинейность, т. е. невозможность подобрать линейную функцию, хорошо аппроксимирующую данное преобразование, и лавинный эффект, при котором изменения в одном бите входных данных должны распространяться по всем битам выходных данных, поскольку выполнение этих требований затрудняет проведение линейного и дифференциального криптоанализа шифра соответственно [4].

Если рассмотреть с этих позиций операции преобразования в раунде шифрования по ГОСТ 28147–89, то легко убедиться в том, что криптостойкость обеспечивают лишь операции сложения с ключом и выполнения замены бит по таблице, так как операции побитового сдвига и суммирования по модулю 2 являются линейными и не обладают лавинным эффектом. Из этого можно сделать вывод, что определяющим фактором надежности шифрования по ГОСТ 28147–89 является надлежащим образом выбранная ключевая информация, т. е. ключ и таблица замен. Очевидно, что в случае зашифрования данных с нулевым ключом и тривиальной таблицей замен, все узлы которой содержат числа от 0 до 15 в порядке возрастания, найти открытый текст по известному шифр-тексту достаточно просто при помощи как линейного, так и дифференциального криптоанализа.

Более того, как показано в [5], операция сложения данных с подключом не может произвести достаточного лавинного эффекта, поскольку при изменении одного бита на входе этой процедуры лишь один бит на выходе меняется с вероятностью 0,5, остальные биты меняются с существенно меньшей вероятностью. Это говорит о том, что

для поддержания криптостойкости шифрования необходимо не только обеспечить достаточное качество ключа, но и использовать сильные таблицы замен с высокими показателями нелинейности и лавинного эффекта. Это показано в работе [6], где предложен метод криптоанализа ГОСТ 28147–89, позволяющий с низкой вычислительной сложностью вскрыть шифр в случае использования слабых ключей и таблиц замен. Таким образом, задача выбора таблиц замен, устойчивых к линейному и дифференциальному криптоанализу, является одной из основных при реализации криптосистем на основе ГОСТ 28147–89.

Как было сказано выше, авторы предполагают независимое формирование узлов замен с их последующим объединением в таблицу замен. Поэтому в дальнейшем изложении будем рассматривать отдельные узлы замен с точки зрения их устойчивости к методам криптоанализа.

Общие требования к узлам замен блочных шифров (S-блокам) повторяют требования к функции шифрования в целом – это нелинейность и лавинный эффект. В идеале любые изменения входных данных узла должны приводить к случайным изменениям выходных данных (если рассматривать узел замен как черный ящик).

Существует ряд общеизвестных критериев для проектирования устойчивых к дифференциальному криптоанализу узлов замен для любых блочных шифров [7]:

– строгий критерий лавинного эффекта (Strict Avalanche Criterion, SAC) требует, чтобы для любых i и j при инвертировании входного бита i на входе узла замен выходной бит j изменялся с вероятностью 0,5;

– критерий независимости битов (Bit Independence Criterion, BIC) требует, чтобы для любых значений i, j и k при инвертировании входного бита i на входе узла замен выходные биты j и k изменялись независимо, т. е. вероятность одновременного изменения битов должна быть равна произведению вероятностей изменения отдельных бит. Считается, что одновременное выполнение критериев SAC и BIC для всех узлов замен обеспечивает шифру достаточный уровень лавинного эффекта;

– критерий гарантированного лавинного эффекта (Guaranteed Avalanche Criterion, GAC) порядка γ выполняется, если при изменении одного бита на входе узла замен на выходе меняются как минимум γ выходных битов. Выполнение критерия GAC порядка γ в диапазоне от 2 до 5 для узлов замен обеспечивает любому шифру очень высокий лавинный эффект благодаря распространению изменений в битах при прохождении данных по раундам шифрования в схеме Фейстеля.

Существуют следующие наиболее распространенные способы выбора узлов замен:

– случайный выбор, когда элементы узлов замен выбираются с помощью генератора псевдослучайных чисел. Это наиболее простой способ, однако в случае небольшого размера узлов, как в алгоритме ГОСТ 28147–89 (4×4 бит), такой способ может привести к генерации таблицы замен с нежелательными с точки зрения стойкости шифрования характеристиками нелинейности и лавинного эффекта;

– случайный выбор с последующей проверкой. В этом способе элементы узлов замен выбираются случайным образом, но после этого полученные результаты проверяются на соответствие различным критериям с отсеиванием тех узлов, которые не выдержали такой проверки. Этот способ так же прост, как и первый, и в то же время он устраняет недостаток первого способа, однако в таком случае встает вопрос о том, по каким критериям проверять выбранные случайным образом узлы, так как не существует узлов замен, удовлетворяющих всем предъявляемым к ним критериям одновременно;

– выбор вручную, когда элементы узлов замен выбираются вручную с использованием математических преобразований. Именно этот способ был положен в основу разработки алгоритма DES с его фиксированными S-блоками. Такой подход является наиболее сложным, так как требует разработки и теоретического обоснования методики выбора замен, что не всегда возможно;

– математический подход, при котором элементы узлов замен генерируются при помощи определенного алгоритма, основанного на тех или иных математических принципах. Такой способ обеспечивает выбор узлов замен, гарантирующих заданный уровень надежности по отношению к методам линейного и дифференциального криптоанализа.

Мы предлагаем использовать для генерации узлов замен шифра ГОСТ 28147–89 аппарат булевых функций. В данном случае один узел замен будет представлен в виде набора из 16 различных 4-битовых строк (рис. 2).

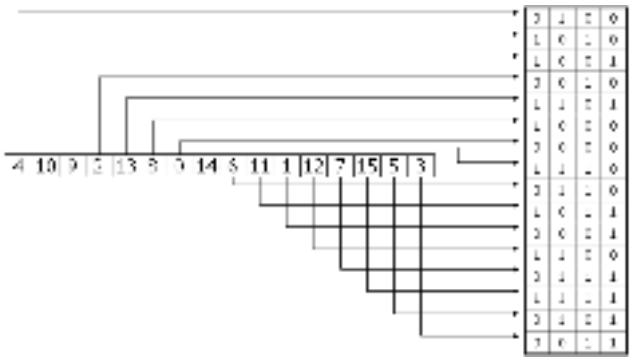

Рис. 2. Схема представления узла замен в виде битовой матрицы

В силу требования ГОСТ 28147–89 об отсутствии повторяющихся элементов в узле замен, битовая матрица узла не должна содержать повторяющихся строк. Столбцы такой битовой матрицы можно рассматривать как булевы функции от 4 переменных $f_i : \{0,1\}^4 \to \{0,1\}$, $i = 1, 2, 3, 4$. Для них можно вычислить числовые характеристики нелинейности и лавинного эффекта [4].

Так, нелинейность функции f определяется по формуле

$$\mathrm{nl}(f) = \min_{l \in A_4} wt(f \oplus l), \qquad (1)$$

где wt – функция веса Хэмминга (число различных входных комбинаций бит, для которых функция дает на выходе 1); $\oplus$ – операция побитового сложения по модулю 2; A_4 – множество аффинных булевых функций от 4 переменных (линейных функций и их побитовых инверсий).

Нелинейность всего узла замен S тогда будет представлена в виде

$$\mathrm{nl}(\mathrm{S}) = \min_{f \in C} \mathrm{nl}(f), \qquad (2)$$

где C – множество всех линейных комбинаций столбцов битовой матрицы M размерностью 16 × 4 узла замен S, $C = \left\{ Mc, c \in \{0,1\}^4 \right\}$. Вычисление произведения матрицы M на вектор c производится с использованием суммирования по модулю 2.

Таким образом, требование нелинейности узла замен можно сформулировать следующим образом: необходимо, чтобы все линейные комбинации столбцов битовой матрицы узла имели как можно большую нелинейность, определяемую формулой (1). Путем полного перебора всех булевых функций от 4 переменных было установлено, что нелинейность столбца может принимать только значения 0, 2 и 4.

Степень лавинного эффекта, обеспечиваемого узлом замен, характеризуется показателем динамического расстояния столбцов его битовой матрицы порядка j [4]:

$$\mathrm{DD}_j(f) = \max_{\substack{d \in \{0,1\}^4 \\ 1 \le \mathrm{wt}(d) \le j}} \frac{1}{2} \left| 2^{n-1} - \sum_{x=0}^{2^n-1} f(x) \oplus f(x \oplus d) \right|. \quad (3)$$

Тогда динамическое расстояние всего узла замен S порядка (i, j) определяется как

$$\mathrm{DD}_{i,j}(S) = \max_{\substack{c \in \{0,1\}^4 \\ 1 \le \mathrm{wt}(c) \le i}} \mathrm{DD}_j(Mc), \quad (4)$$

где M – битовая матрица узла замен S.

Так, критерий SAC для узла замен S выполняется тогда и только тогда, когда $\mathrm{DD}_{1,1}(\mathrm{S}) = 0$, или, что то же самое, все столбцы битовой матрицы узла замен S имеют динамическое расстояние порядка 1, равное 0, а критерий BIC выполняется, когда $\mathrm{DD}_{2,1}(\mathrm{S}) = 0$, т. е. все линейные комбинации пар столбцов битовой матрицы узла замен S имеют динамическое расстояние порядка 1, равное 0.

Таким образом, требование обеспечения лавинного эффекта для узла замен можно сформулировать следующим образом: необходимо, чтобы все линейные комбинации столбцов битовой матрицы узла имели как можно меньшее динамическое расстояние как можно более высокого порядка, определяемое формулой (3).

Дополнительной характеристикой устойчивости узла замен к дифференциальному криптоанализу, определенной в [4], является XOR-таблица размерностью 15 × 16, элементы которой вычисляются по формуле

$$\mathrm{XOR}(\mathrm{S}, \alpha, \beta) = \\ = \#\left\{ x \in \{0,1\}^4 : S(x) \oplus S(x \oplus \alpha) = \beta \right\}, \quad (5)$$

где $\alpha \in \{0,1\}^4 \setminus \{0\}$ и может быть представлено в виде числа от 1 до 15; $\beta \in \{0,1\}^4$ и (может быть представлено в виде числа от 0 до 15); $\mathrm{S}(x)$ – x-я строка битовой матрицы узла замен S; $\#X$ – мощность множества X.

XOR-значение узла замен S определяется по следующей формуле:

$$\mathrm{XOR}(\mathrm{S}) = \max_{\alpha,\beta} \mathrm{XOR}(\mathrm{S}, \alpha, \beta). \quad (6)$$

Таким образом, можно сформулировать свойства идеального узла замен ГОСТ 28147–89:

1) все линейные комбинации столбцов битовой матрицы узла имеют нелинейность 4, или, что то же самое, узел замен имеет нелинейность 4;

2) все линейные комбинации столбцов битовой матрицы узла имеют динамическое расстояние порядка 4, равное 0, или, что то же самое, узел замен имеет динамическое расстояние порядка (4, 4), равное 0;

3) все элементы XOR-таблицы узла замен равны 0 или 2, или, что то же самое, узел замен имеет XOR-значение 2.

Свойство 1 обеспечивает устойчивость шифрования к линейному криптоанализу, свойства 2 и 3 – к дифференциальному криптоанализу. В ходе исследований выяснилось, что при построении узлов замен шифра ГОСТ 28147–89 невозможно одновременно добиться максимальных показателей нелинейности и динамического расстояния даже порядка 1. Это, в частности, является следствием того, что узел замен должен быть перестановкой чисел от 0 до 15, т. е. в битовой матрице узла замен не должно быть одинаковых строк.

Авторами предложен следующий алгоритм построения узлов замен, предполагающий формирование узла замен поэтапно – по столбцам:

– *шаг 1.* Выбирается минимально допустимый уровень нелинейности $\mathrm{nl}_{\min}$ и максимальное допустимое динамическое расстояние порядка 1 $\mathrm{DD}_{\max}$ линейных комбинаций столбцов битовой матрицы узла замен;

– *шаг 2.* Из всех возможных $2^{16} = 65\,536$ булевых функций от 4 переменных методом полного перебора выбирается подмножество, удовлетворяющее выбранным на шаге 1 критериям;

– *шаг 3.* Из построенного на шаге 2 подмножества выбирается функция-«кандидат» и помещается в первый столбец битовой матрицы узла замен;

– *шаг 4.* Из построенного на шаге 2 подмножества выбирается функция-«кандидат» и помещается во второй столбец битовой матрицы, после чего сумма по модулю 2 первого и второго столбцов проверяется на соответствие критериям, выбранным на шаге 1. Если эта функция им не удовлетворяет, то функция, помещенная во второй столбец, отбрасывается и выполняется возврат к шагу 3;

– *шаг 5.* Функции-«кандидаты» выбираются из построенного на шаге 2 подмножества и помещаются в столбцы битовой матрицы, следующие за последним заполненным столбцом, после чего выполняются проверки всех линейных комбинаций заполненных столбцов с участием столбца-«кандидата» до тех пор, пока заполненными не окажутся все 4 столбца матрицы;

– *шаг 6.* Полученная в итоге битовая матрица узла замен дополнительно проверяется на соответствие GAC, а также на устойчивость к дифференциальному криптоанализу путем построения XOR-таблицы узла замен. Если эти критерии выполняются, то узел замен становится выходом алгоритма, если нет, то последний столбец битовой матрицы отбрасывается и выполняется возврат к шагу 5, т. е. процесс тестирования функций-«кандидатов» продолжается.

Данный алгоритм был программно реализован, протестирован и успешно использован для выбора подмножества таблиц замен при выбранных на шаге 1 параметрах $\mathrm{nl}_{\min} = 4$ и $\mathrm{DD}_{\max} = 0$. В результате работы алгоритма было получено множество из 1 032 192 всех возможных узлов замен ГОСТ 28147–89, имеющих нелинейность 4 и удовлетворяющих SAC, BIC и более сильному аналогу BIC для всех выходных бит (при изменении любого входного бита все выходные биты узла меняются независи-

мо). В то же время для всех узлов из этого множества XOR-значение равно 8, что является нежелательным показателем с точки зрения устойчивости к дифференциальному криптоанализу.

По всем приведенным выше критериям был также проведен анализ тестовой таблицы замен из стандарта функции хеширования ГОСТ Р 34.10–94, который показал, что в них достигается баланс между степенью удовлетворения всех трех критериев идеального узла замен.

Следующей важнейшей задачей, стоящей перед авторами, является разработка методики выбора оптимальных значений nl_{min} и DD_{max}, полученных на шаге 1, а также минимально допустимого порядка критерия GAC и максимально допустимого XOR-значения узла замен при проверке готового узла замен на шаге 6.

Еще одним направлением работы является построение интегральной оценки качества узла замен с точки зрения криптостойкости исходя из показателей нелинейности, динамического расстояния определенного порядка, элементов XOR-таблицы узла замен и минимального порядка γ, при котором узел замен удовлетворяет критерию GAC. Тогда задача выбора узла замен сведется к задаче однокритериальной оптимизации на множестве всех возможных узлов, которая может быть решена с помощью как классических методов, так и, например, генетических алгоритмов.

Другие не менее важные с нашей точки зрения направления исследований связаны с решением следующих вопросов:

– разработки методики формирования таблицы замен из отдельных узлов, позволяющей оценить влияние отдельного узла на стойкость шифрования в целом, а также описать правила, по которым из узлов с различными характеристиками нелинейности и лавинного эффекта можно сформировать таблицу замен, оптимальную с точки зрения устойчивости к линейному и дифференциальному методам криптоанализа;

– исследования взаимного влияния качества ключа и таблицы замен на криптостойкость. В настоящее время практикуется независимый выбор ключа и таблицы замен. Однако возможно, что выбор ключа влияет на силу таблицы замен с точки зрения криптостойкости, и наоборот, что могут существовать ключи, сильные при одних выбранных узлах замен и слабые при других. Открытые материалы публикаций по этому вопросу авторам неизвестны;

– практического исследования криптостойкости алгоритма ГОСТ 28147–89 путем реализации атак методом линейного и дифференциального криптоанализа на упрощенную версию шифра, например с меньшим числом раундов или меньшей длиной блока и (или) ключа. В таком случае, возможно, удастся получить оценки вычислительной сложности вскрытия упрощенного шифра обоими методами криптоанализа, а затем экстраполировать их на полноценный ГОСТ 28147–89, исходя из предположения, что более высокая вычислительная сложность вскрытия упрощенного шифра влечет за собой пропорциональное увеличение сложности вскрытия полного алгоритма.

Таким образом, авторами разработан и программно реализован алгоритм построения узлов замен блочного шифра ГОСТ 28147–89, который применяется для выработки таблиц замен при шифровании несекретной информации ограниченного доступа. Этот алгоритм может быть применен при проектировании и реализации криптографических систем защиты несекретной информации ограниченного доступа, передаваемой по открытым каналам.

Библиографический список

1. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. М. : Изд-во стандартов, 1996.

2. Винокуров, А. Алгоритм шифрования ГОСТ 28147–89, его использование и реализация для компьютеров платформы x86 [Электронный ресурс] / А. Винокуров. Электрон. дан. Режим доступа: http://re-tech.narod.ru/inf/crypto/gost.htm. Загл. с экрана.

3. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа : учеб. пособие / Л. К. Бабенко, Е. А. Ищукова. М. : Гелиос АРВ, 2006.

4. Mister, S. Practical S-box design / S. Mister, C. Adams // Proc. Workshop in selected areas of cryptography (SAC'96). Philadelphia, PA, 1996. P. 61–76.

5. Further comments on the soviet encryption algorithm / C. Charnes, L. O'Connor, J. Pieprzyk et al. ; University of Wollongong. Wollongong, 1994.

6. О стойкости ГОСТ 28147-89 / А. Г. Ростовцев, Е. Б. Маховенко, А. С. Филиппов, А. А. Чечулин ; С.-Петерб. гос. политехн. ун-т, 2001.

7. Столлингс, В. Криптография и защита сетей: принципы и практика / В. Столлингс. М. : Вильямс, 2001.

T. A. Chalkin, K. M. Voloshchuk

DEVELOPMENT OF THE ALGORITHM OF NODES CONSTRUCTION CHANGE FOR GOST 28147–89 ENCRYPTION ALGORITHM

The basic requirements for block ciphers nodes (S-boxes) design change are considered. The algorithm of change nodes construction for GOST 28147–89 encryption algorithm on the basis of these requirements providing necessary level of cipher resistance to linear and differential cryptanalysis is developed.

Keywords: encryption, change table, Boolean function, cryptographic security, cryptanalysis, algorithm.