Проблемы бионики
1999. Вып. 50. С. 185–194
ХТУРЭ
УДК 681.3.06: 519.248.681

С.А. ГОЛОВАШИЧ, А.С. КОРЯК, И.В. ЛИСИЦКАЯ,
Р.В. ОЛЕЙНИКОВ, О.И. ОЛЕШКО

ПОСТРОЕНИЕ ТАБЛИЦ ПОДСТАНОВОК ДЛЯ СТАНДАРТА ШИФРОВАНИЯ ДАННЫХ

Одним из актуальнейших направлений дальнейшего развития и совершенствования информационных технологий, их применения в особо ответственных системах управления жизнедеятельностью государства и общества является все большая интеллектуализация таких систем, придание им свойств самоорганизации и адаптации к изменяющимся условиям функционирования. Вместе с тем усложнение информационных технологий резко обострило необходимость решения целого комплекса сложных вопросов, связанных с защитой информации, обеспечением безопасности функционирования сложных систем, особенно в таких критических областях как энергетика, транспорт, армия, финансы.

Одним из путей решения стоящих задач, как известно, считается применение криптографических методов защиты информации на всех этапах ее жизненного цикла. В настоящей работе рассматриваются пути совершенствования теоретических и практических методов построения шифров симметричного типа, которые и сегодня занимают важное место в комплексе криптографических средств и методов защиты информации в вычислительных и информационных сетях.

В частности, речь пойдет о правилах построения таблиц подстановок, которые выступают в качестве одной из основных процедур криптопреобразований во многих современных и классических шифрах, таких как DES, ГОСТ 28147 и др.

Идея этой работы состоит в том, чтобы развить методику отбора случайных таблиц подстановок, изложенную в наших предыдущих публикациях [1-3], применительно к построению S блоков для алгоритма шифрования DEA (так мы будем называть по уже установившейся терминологии использование именно алгоритмической части DES) и показать, что таблица подстановок, предложенная разработчиками стандарта DES, является далеко не лучшей. Предлагаемая методика позволяет построить таблицы S блоков, которые намного эффективнее известной таблицы в отношении защиты от атак как дифференциального, так и линейного криптоанализа [4,5].

1. Анализ свойств и характеристик S блоков стандарта DES

Напомним, что в алгоритме DES в каждом из S блоков входные 6 бит заменяются на 4 выходных, причем взаимосвязи между входными и выход-

ными символами определяется с помощью 8 фиксированных таблиц подстановок, т.е. в этом алгоритме применяется не общепринятое представление подстановки в виде отображения конечного множества различных чисел самого в себя (перестановки чисел), а отображение $GF(2^6) \rightarrow GF(2^4)$. Однако если внимательно посмотреть на таблицы S блоков для стандарта DES, приведенные, например, в [6], то можно прийти к выводу, что каждый из S блоков (в том виде, в каком они представлены в [6]) является числовой конструкцией из четырех перестановок ($m = 4$) степени $n = 16$, и эту числовую конструкцию можно интерпретировать как таблицу полиподстановки, т.е. по существу и в этом случае при формирования S блоков для алгоритма DEA, как и при формировании таблиц для алгоритма ГОСТ 28147–89, исходным можно считать преобразование вида $GF(2^4) \rightarrow GF(2^4)$. Это позволяет задачу построения S блоков для алгоритма DEA сформулировать как задачу формирования (отбора) 8 таблиц подстановок (из 4-х подстановок 16-й степени каждая), удовлетворяющих некоторым ограничениям. В этой работе для решения сформулированной задачи предлагается воспользоваться методикой отбора случайных таблиц подстановок по трем уровням проверки, сформулированным в [1], дополнив ее некоторыми вспомогательными ограничениями и проверками, учитывающими усиление защиты от известных из литературы "каналов уязвимости" стандарта DES (имеется в виду обеспечение устойчивости к атакам дифференциального и линейного криптоанализа).

Остановимся сначала на результатах анализа свойств и характеристик случайности подстановок и таблиц подстановок стандарта DES, т.е. будем интересоваться степенью близости их показателей случайности к показателям случайных равновероятных постановок и случайных таблиц подстановок.

Напомним, что в [1] предлагается использовать показатели и критерии случайности трех уровней. На первом уровне проверки оценивается соответствие индивидуальных характеристик отдельно взятой подстановки свойствам случайной равновероятной подстановки. Подстановки, прошедшие первый уровень проверки, считаются уже подстановками "случайного" типа.

На втором уровне оценивается соответствие характеристик случайности системы подстановок, попавших в таблицу, свойствам среднестатистической таблицы случайных подстановок. Таблицы подстановок, прошедшие первые два уровня проверки, считаются случайными таблицами подстановок (заметим, что здесь и выше точнее было бы говорить о подстановках и таблицах подстановок, принадлежащих множеству наиболее вероятных подстановок и таблиц подстановок случайного типа).

На третьем уровне осуществляется оценка характеристик множества случайных таблиц подстановок, из которого отбираются таблицы, удовлетворяющие требованиям использования в системе защиты нескольких (или смен-

ных) долговременных ключей, а в рассматриваемом случае – условиям одновременного использования в шифре нескольких таблиц подстановок.

Для первого уровня проверки подстановок по индивидуальным показателям случайности расчеты числовых значений параметров отбора подстановок по числу инверсий η_n, числу циклов ξ_n и числу возрастаний ζ_n при $n=16$ приводят к результатам, приведенным в [1] для алгоритма ГОСТ 28147–89, т.е. $|\eta_n - 60| \le 10$, $|\xi_n - 3| \le 2$, $|\zeta_n - 8| \le 1$.

На втором уровне проверки сначала отбираются случайные подстановки, которые не имеют совпадающих элементов с верхней строкой традиционного матричного представления подстановки в каноническом виде (верхняя строка – это упорядоченный ряд чисел $1, 2, 3, \ldots, n$). Затем для сформированной таким образом таблицы строится ее "метрический портрет" и сравнивается с "эталонным метрическим портретом".

Чтобы построить двумерный эталонный метрический портрет случайной таблицы подстановок, рассчитывают закон распределения вероятностей числа повторений различных элементов в столбце таблицы, составленной из случайных равновероятных подстановок, и закон распределения вероятностей числа совпадений элементов в паре наложенных строк такой таблицы. Соответствующие законы распределения вероятностей, рассчитанные для $n=16$, $m=4$ по методике, изложенной в [3], представлены в табл. 1 и 2.

Из табл.1 следует, что произвольно выбранная (случайная) таблица, состоящая из четырех подстановок (имеющая 16 столбцов и 4 строки), будет содержать с большой вероятностью 11 столбцов, не имеющих повторяющихся (совпадающих) элементов, и 5 столбцов с двумя повторяющимися элементами (с одной парой повторяющихся элементов). Все другие конфигурации существенно менее вероятные (суммарная вероятность оставшихся трех вариантов совпадений менее чем 0,026).

Аналогично для таблицы из $N_k = 6$ пар строк и закона распределения вероятностей, приведенного в табл. 2, получаем, что среднестатистический метрический портрет случайной таблицы подстановок в этом случае состоит:

из $t_0 = 2$ пар строк с 0 совпадений элементов;

из $t_1 = 3$ пар строк с 1 совпадением;

из $t_2 = 1$ пары строк с 2 совпадениями.

Все другие варианты совпадений элементов в парах строк таблицы подстановок и здесь оказываются маловероятными (на все остальные варианты приходится вероятность, близкая к 0,015).

Таблица 1

Закон распределения вероятностей $P^{(i)}$ числа повторений i различных элементов в столбце таблицы подстановок

i	$P^{(i)}$
0	0,6665
1	0,3225
2	0,0109

Таблица 2

Закон распределения вероятностей $P(\gamma)$ числа совпадений γ элементов в паре наложенных строк

γ	$P(\gamma)$
0	0,356
1	0,3798
2	0,1899
3	0,0591
4	0,0128
5	0,0020
...	...

Таким образом, результирующий эталонный метрический портрет случайной таблицы подстановок представляет собой конфигурацию вида $(\zeta_0, \zeta_2, \zeta_3) = (11,\ 5,\ 0,)$ совпадений элементов по столбцам и конфигурацию вида $(t_0, t_1, t_2, \ldots, t_{16}) = (2, 3, 1, 0, \ldots, 0)$ совпадений элементов во всех попарных декомпозициях строк.

В этой работе мы несколько отойдем от определенного в [3] правила отбора на втором уровне проверки, ориентированного на использование для оценки близости конфигурации совпадений в столбцах и строках проверяемой таблицы к эталонной критерия согласия χ^2 как такового (по объему выборки ситуация оказывается далеко выходящей за условия применимости критерия χ^2 [5]). Будем использовать саму идею расчета величины χ^2 просто как метод отбора (выбора) таблиц подстановок, реализуемый с помощью соотношений

$$\chi_q^2 \le \chi_{q_{CT}}^2,$$

$$\chi_q^2 \le \chi_{q_{n_{\alpha}}}^2.$$

В этих соотношениях $\chi_{q_{CT}}^2$ и $\chi_{q_{n_{\alpha}}}^2$ – пороговые значения для величин χ_q^2, а сами значения χ_q^2 определяются в виде

$$\chi_q^2 = \sum_{i=0}^{2} \frac{\left(\zeta_i - nP^{(i)}\right)^2}{nP^{(i)}}$$

для конфигураций $(\zeta_0, \zeta_1, \zeta_2)$ совпадений элементов по столбцам и

$$\chi_q^2 = \sum_{i=0}^{16} \frac{\left(t_i - N_k P(\gamma)\right)^2}{N_k P(\gamma)}$$

– для конфигураций $(t_0, t_1, t_2, \ldots, t_{16})$ совпадений элементов в парах строк.

Чтобы задать пороговые значения $\chi^2_{q_{CT}}$ и $\chi^2_{q_{n_n}}$, воспользуемся следующими соображениями. Представляется достаточно очевидным, что наиболее предпочтительной ситуацией построения интересующих нас таблиц можно считать наибольшую "непохожесть" друг на друга входящих в них подстановок, т.е. ситуацию, когда подстановки, образующие таблицу, вообще не имеют совпадений по столбцам, а следовательно, не имеют совпадений и в любых попарных сочетаниях строк (являются противоречивыми). Поэтому вряд ли целесообразно вводить ограничение на максимальное число несовпадений, тем более, что, как показал анализ [7,8], и в предельном случае использования таблиц в виде латинских прямоугольников (таблиц, составленных из противоречивых подстановок) они проходят все проверки на статистическую безопасность, как и случайные таблицы подстановок, отобранные по критериям работы [3]. Исходя из этого, предлагается задать параметры отбора так, чтобы выполняемые проверки пропускали таблицы, состоящие из противоречивых подстановок, что можно осуществить, если воспользоваться пороговыми значениями $\chi^2_{q_{CT}}$ и $\chi^2_{q_{n_n}}$ для предельных конфигураций совпадений $(6, 0, 0)$ по столбцам и $(16, 0, 0, \ldots, 0)$ по парам строк. Расчеты, выполненные для законов распределения вероятностей табл. 1 и 2, приводят к результатам $\chi^2_{q_{CT}} = 8$, $\chi^2_{q_{n_n}} = 10{,}8$.

При проверке на третьем уровне по числу совпадений элементов q в паре наложенных случайных таблиц подстановок можно воспользоваться односторонним ограничением в виде $q \le 5$, близким по смыслу к проверке, предложенной в [1].

В соответствии с приведенными соображениями и был выполнен анализ свойств случайности таблиц подстановок, предложенных разработчиками стандарта DES. Полученные результаты позволяют сделать следующие выводы:

1) По индивидуальным показателям (числу инверсий, возрастаний и циклов) подстановки, из которых построены таблицы, удовлетворяют определенным в [1] критериям случайности, т.е. являются случайными подстановками (кроме небольшого отличия 4-й подстановки в 5-м S блоке по числу инверсий и отличиях в одной из подстановок в 4-м и 8-м S блоках по числу возрастаний).

2) По метрическим характеристикам все таблицы подстановок укладываются в границы числа совпадений по столбцам и парам строк, задаваемые оговоренными правилами проверки. Ровно половина из всех таб-

лиц подстановок представляет собой нормализованные латинские прямоугольники (состоят из противоречивых подстановок). Следует, однако, заметить, что таблицы подстановок всех S блоков стандарта имеют элементы, совпадающие с нулевой строкой [1].

3) По показателям отбора третьего уровня таблицы подстановок DES можно считать практически укладывающимися в определенные в [1] рамки случайных таблиц подстановок. Имеется, правда, небольшой выход за указанные пределы (один раз встречается 9 совпадений из 49 возможных вариантов по числу совпадений, два раза 7 и три раза 6).

В целом, однако, можно сделать общий вывод, что свойства таблиц подстановок стандарта DES оказываются достаточно близкими к свойствам случайных таблиц подстановок.

2. Проверка статистической безопасности случайных *S* блоков

В этом разделе излагаются результаты сопоставительной оценки статистической безопасности таблиц подстановок, построенных по методике работы [1], и S блоков стандарта DES (устанавливается их статистическая эквивалентность).

Таблицы строились с помощью программного комплекса генерации таблиц подстановок для S блоков, реализующего представленные выше принципы отбора случайных таблиц подстановок.

Проверка статистической безопасности сформированных с помощью этого комплекса таблиц выполнялась по методике, изложенной в работе [8].

Использовались три основных показателя статистической безопасности, характерные для блочных симметричных шифров, построенных на основе чередования слоёв замен и подстановок.

1. Число циклов алгоритма, начиная с которого криптограммы, полученные шифрованием двух отличающихся на один бит блоков данных (открытых текстов), становятся устойчиво независимыми (в том смысле, что при большем числе циклов они остаются независимыми). Другими словами, необходимо было определить число циклов входа в алгоритм, начиная с которого изменение одного бита открытого текста приводит к изменению шифрованного текста приблизительно (в среднем) в половине битов. Это так называемый лавинный эффект.

2. Число циклов шифрования, при котором один и тот же открытый текст зашифрованный на ключах, отличающихся на один бит, порождает устойчиво независимые (некоррелированные) криптограммы.

3. Коэффициент сжатия шифрованного текста при применении процедуры архивирования Лемпела-Зива.

Результаты проведенных статистических экспериментов полностью подтвердили эффективность использования в качестве S блоков для DEA (с

точки зрения рассматриваемых показателей статистической безопасности) случайных таблиц подстановок, построенных по предлагаемой методике.

Действительно, использование разработанных в [1-3] критериев отбора позволяет исключить все вырожденные конфигурации. При этом для случайных таблиц из разрешенного множества, как и для таблицы S блоков стандарта DES, "глубина" вхождения в алгоритм для обеспечении статистической независимости (зависимости) всех выходных бит шифрованного текста от любого входного бита не превышает 5 циклов (отсчёт числа циклов, при котором считается, что изменение входного бита практически не влияет на все выходные биты, ведется по моменту "накрытия" случайного интервала $(\overline{X} - 0{,}4, \overline{X} + 0{,}4)$, выступающего в качестве доверительной оценки математического ожидания $\overline{X}$ с мерой надёжности $1 - \alpha = 0{,}999$, значения $m_w' = 32$).

Выполняется также необходимая зависимость шифрованного текста от любого бита ключа при вхождении в алгоритм на глубину не более чем 5 циклов. Во всех случаях обеспечивается сжатие шифрованного текста по Лемпелу-Зиву менее чем на 10 % (аналогичное сжатию, достигаемому при шифровании с использованием стандартных S блоков).

Таким образом, действительно подтверждается полная статистическая эквивалентность в рассмотренном смысле S блоков стандарта DES и таблиц подстановок, отобранных по рассмотренной методике.

3. Проверка устойчивости случайных таблиц подстановок к атакам дифференциального и линейного криптоанализа

Дифференциальный криптоанализ был предложен Эли Бихамом и Ади Шамиром в 1990 году и впоследствии ими же неоднократно усовершенствовался [4]. Они обосновали новую атаку против алгоритма DES на основе специально подбираемых текстов, которая оказалась более эффективной, чем прямой перебор ключей. Атака для DES сильно зависит от структуры S блоков (от их "асимметрии"), которые для DES, как утверждают некоторые авторы [5], оказались оптимизированными (может быть, и не случайно) против дифференциального криптоанализа. Напомним, что дифференциальный криптоанализ строится на особенностях ("асимметрии") таблиц XOR переходов вход-выход для каждого S блока (в такой таблице строки-входы представляют возможные XORы (побитовые булевы суммы) двух различных входов S блока, столбцы-входы представляют возможные XORы двух выходов S блока, а элементы таблицы указывают, сколько раз определенный выходной XOR встречается для данного входного XORa).

Соответственно была поставлена задача оценки эффективности в этом смысле S блоков, отобранных по изложенной выше методике. Оказалось, что в числе "случайных" S блоков сразу встретились S блоки с показателями

таблиц XOR переходов более хорошими, чем определенных в стандарте, но в то же время основная масса случайных S блоков в экспериментах получалась уступающей по показателю асимметрии S блокам стандарта. Вместе с тем первый положительный вывод, который был получен на основе этих экспериментальных данных, состоял в том, что существуют S блоки лучше, чем стандартные (можно просто заменить некоторые S блоки стандарта более эффективными). Второй важный вывод состоял в том, что использование только критериев отбора случайных подстановок и случайных таблиц подстановок [1] не обеспечивает хорошие показатели симметрии для всех таблиц подстановок, т.е. возникает необходимость введения еще одного уровня проверки (вычисление вероятностной зависимости XOR битов на выходе S блока от XOR входных битов и оценка максимального значение несимметрии для каждого S блока). В итоге методика отбора таблиц подстановок была дополнена следующим требованием проверки четвертого уровня:

Требование 1. Таблицы подстановок (S блоки) должны по максимальному значению асимметрии соответствующих им таблиц XOR переходов вход-выход не превосходить значения s = 12 (установлено экспериментально).

Рассматривалась также задача определения минимально возможного значения асимметрии. Попытки получить значение асимметрии, меньшее чем s = 12, к успеху не привели.

Наконец, остановимся кратко на идеях линейного криптоанализа. Автором этих идей является Мицури Мацуи [5]. В их основе лежит так называемая линейная аппроксимация для описания операций, выполняемых при блочном шифровании. Применительно к алгоритму DES линейная аппроксимация заключается в установлении связи между булевой побитной суммой (XOR) некоторых бит открытого текста, XOR некоторых бит шифрованного текста и XOR некоторых ключевых бит.

Мацуи показывает, что для алгоритма DES и его модификаций побитная сумма некоторых бит открытого текста и некоторых бит соответствующего ему шифрованного текста позволяет вычислить единственный бит, который является побитной суммой некоторых ключевых бит. Это и есть линейная аппроксимация. И если указанная связь поддерживается с некоторой вероятностью $p \neq \frac{1}{2}$, то это смещение может быть использовано путём анализа собранных открытых текстов и соответствующих им шифрованных текстов для угадывания значений ключевых битов. Большее смещение увеличивает шансы успеха при тех же исходных данных.

Как известно [5], таблицы S блоков стандарта DES считаются не оптимизированными по отношению к атакам линейного криптоанализа. Максимальное значение смещения свойственно 5-му S блоку и составляет 12/64.

Соответственно была поставлена задача проверки показателей асимметрии таблиц подстановок (S блоков), формируемых предлагаемым методом.

Интересно отметить, что построение линейных аппроксимационных таблиц для S блоков с применением требования 1 привело к тому, что их показатели получились лучшими, чем у таблиц стандарта (максимальное значение асимметрии получилось равным 16). Соответственно отобранные с учетом требования 1 таблицы были оптимизированы по критерию достижимого минимального уровня асимметрии линейных аппроксимационных характеристик таблиц S блоков. Экспериментально удалось получить таблицы с максимальными показателями линейных аппроксимационных таблиц, не превосходящими значения $l = \pm 10$ (против -20 в стандарте DES). Поэтому для получения таблиц S блоков, устойчивых и к линейному криптоанализу, было введено еще одно требование к отбору таблиц подстановок, которое мы также отнесли к четвертому уровню проверок.

Требование 2. Таблицы подстановок (S блоков) по максимальному значению асимметрии соответствующих им линейных аппроксимационных таблиц не должны превосходить значения $|l| = 10$ (установлено экспериментально).

В результате удалось сформировать таблицы подстановок для алгоритма DEA, существенно превосходящие по своим характеристикам защищенности от атак дифференциального и линейного криптоанализа аналогичные таблицы S блоков для DES. В табл. 3 представлена одна из реализаций S блоков, составленных из противоречивых подстановок.

Общие выводы из приведенных результатов состоят в следующем:

1. S блоки стандарта DES, хотя они в единственной реализации используются вот уже более 20 лет, не являются уникальными. Их можно построить достаточно большое количество, так что таблицы подстановок в DEA, как и в российском стандарте ГОСТ 28147–89, могут выступать в качестве переменного параметра (долговременного ключа), правда, его размерность в 4 раза превосходит размерность ключа в ГОСТ 28147–89.

2. Развитая в работе методика проверок позволяет решить задачу формирования таблиц S блоков для алгоритма DEA (DES), при этом показатели и характеристики этих таблиц превосходят по своим характеристикам аналогичные показатели таблиц подстановок для DES, предложенных разработчиками. Можно сделать общий вывод о том, что таблицы стандарта DES являются далеко не лучшими (они не оптимизированы против атаки линейного криптоанализа и недостаточно оптимизированы против атаки дифференциального криптоанализа).

3. Таблицы S блоков, сформированные по предлагаемой методике, позволяют существенно улучшить устойчивость шифра DEA против атак дифференциального и линейного криптоанализа. С большой степенью уверенности можно утверждать, что шифр DEA (DES) при использовании в нем таблиц подста-

новок, оптимизированных по рассмотренным в работе критериям, окажется более стойким к атакам дифференциального и линейного криптоанализа.

Таблица 3

Пример построенных таблиц подстановок

S_1:	S_5:
9 5 0 A B C 7 D E F 2 4 3 6 8 1	F 4 1 7 6 0 8 9 D B 2 3 E A C 5
D 0 7 9 3 A B 6 1 4 8 C E F 5 2	6 C D 5 1 E F 3 7 4 8 9 0 B 2 A
6 E A 2 F 3 5 C 7 1 4 8 9 0 B D	E 3 B 1 2 8 7 0 5 A 9 C D 6 F 4
8 B D C E 1 F 4 2 3 0 5 7 9 A 6	A B 5 D F 9 1 4 3 C 0 2 7 E 8 6
S_2:	S_6:
4 6 1 D 3 E 5 F A 8 7 C 9 B 0 2	B 0 5 D C E F 1 2 4 8 A 9 6 7 3
7 B 3 6 C D 8 5 9 A E 2 0 F 4 1	6 9 D E F 1 3 8 4 2 0 7 5 A C B
B 2 4 C 6 3 D 8 E F 9 1 7 0 A 5	4 3 7 F B 6 5 C 9 D 2 E 8 0 1 A
3 D F 7 8 1 2 4 0 5 6 E B A 9 C	E F 1 2 5 4 0 9 7 A 6 C 3 B D 8
S_3:	S_7:
D 2 9 6 E 4 0 5 3 A B 1 F 8 7 C	A 2 E 8 3 B C 6 4 0 D F 5 7 9 1
F C 4 2 8 9 A D E 0 1 7 3 6 5 B	C D 0 6 E F 4 2 B 5 7 8 1 3 A 9
5 7 8 A 3 C 4 E F 2 0 6 1 B 9 D	7 F 9 2 A 0 D 1 3 8 B C 4 6 5 E
4 D 5 E F 7 2 0 6 B 8 9 A 1 C 3	8 B 1 A C D E 9 2 6 5 0 3 F 7 4
S_4:	S_8:
E F 7 2 5 3 9 0 4 B C 6 A 8 1 D	B 3 4 6 9 D E F C 5 2 8 7 A 0 1
3 B A D 7 9 0 C 6 8 2 5 1 4 F E	9 B 8 2 A 0 C D 3 1 4 7 6 E F 5
B 0 5 C D 6 E F 3 7 9 A 2 1 8 4	E 4 F C 5 2 3 6 7 B 1 D 0 8 9 A
2 E B 0 1 4 8 D 7 A 5 9 F 6 3 C	D E 3 F 0 4 5 1 2 6 B A 8 9 C 7

Список литературы: 1. *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 2847-89 // Радиотехника. 1997. Вып 103. С. 121–130. 2. *Горбенко И.Д., Лисицкая И.В.* К оценке метрических характеристик таблиц подстановок для алгоритма криптографического преобразования по ГОСТ 28147-89 // Радиотехника. 1997. Вып 104. С. 151–162. 3. *Бильчук В.М., Лисицкая И.В.* Информационно-управляющие системы на железнодорожном транспорте. 1998. № 1. С. 10–17. 4. *E. Biham, A. Shamir,* Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology. 1991. Vol. 4. № 1. P. 3-72. 5. *Sheier B.* Applied Cryptography. Second Edition: protocols, algorithms, and source code in C. Published by John Wiley & Sons. Inc, New York: Chichester Brisbane Toronto Singapore, 1996. 158 p. 6. *Барсуков В.С., Дворянкин С.В., Шеремет И.А.* Безопасность связи в каналах телекоммуникаций. М.: Россия, 1993. Т.20. 123 с. 7. *Кононова И.В.* Противоречивые подстановки в алгоритме ГОСТ 28147-89 // Информационные системы. Харьков: НАНУ, ПАНУ, ХВУ. 1995. С. 70–77. 8. *Горбенко И.Д., Лисицкая И.В., Коряк А.С.* Анализ стойкости алгоритма ГОСТ 28147-89 при использовании подстановок случайного типа // Радиоэлектроника и информатика. 1998. №1 (02). С. 39–43.

Поступила в редколлегию 14.12.98