УДК 681.3.06:519.248.681

АНАЛИЗ СТОЙКОСТИ DES - ПОДОБНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ПРИ ИСПОЛЬЗОВАНИИ ТАБЛИЦ ПОДСТАНОВОК СЛУЧАЙНОГО ТИПА

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

На примере анализа свойств и показателей алгоритма DES с таблицами подстановок случайного типа излагаются результаты освоения методики проверки устойчивости DES -подобных шифров к известным атакам дифференциального криптоанализа. Обсуждаются условия обеспечения устойчивости шифра к таким атакам. Показывается, что использование ранее предложенных критериев отбора случайных таблиц подстановок все еще не приводит к достаточному усилению защиты шифра по сравнению со стандартом. Формулируются пути дальнейшего продвижения в развиваемом направлении.

В ранее представленной работе [1] поднимается вопрос об использовании в алгоритме шифрования DEA (так называется сама алгоритмическая часть американского стандарта шифрования данных DES) в качестве *S* блоков таблиц подстановок случайного типа. Естественно, речь идет не о чисто случайных таблицах, а о подстановках и таблицах подстановок, прошедших тесты на случайность, предложенные в работе [2], а также выдержавших некоторые дополнительные проверки на устойчивость против атак дифференциального и линейного криптоанализа. Развиваемый подход выходит за рамки традиционных направлений анализа и изучения характеристик стандарта, интенсивно ведущихся с момента его появления и по настоящее время (в известных источниках изучаются свойства именно стандарта и в качестве *S* блоков рассматриваются таблицы, предложенные самими разработчиками). Нам представляется, что более детальное обсуждение новых возможностей использования схемотехнических решений, заложенных в этот ставший сегодня уже классическим подход к построению симметричного шифра, может заинтересовать специалистов, занимающихся вопросами защиты информации. Актуальность проведения поисковых исследований в отмеченном направлении подкрепляется еще и тем, что сейчас ведется интенсивная работа по замене существующего стандарта новым. Однако для решения стоящих вопросов на должном уровне потребуется еще немало времени, и на переходный период необходимо найти приемлемое временное решение. В этом отношении можно отметить усилия и инициативы, которые проявляет Национальный Институт Стандартов и Технологии (NIST) США [3] по использованию тройного DES, а также Комитет X9.F.1 Американского Национального института Стандартов (ANSI) [4]. Можно отметить также работу [5], где в качестве временного стандарта предлагается алгоритм, построенный на основе использования процедуры DES -шифрования, который и сегодня продолжает интересовать исследователей.

Основное внимание настоящей работы сосредотачивается на результатах освоения самой методики проверки устойчивости DES -подобных шифров к известным атакам дифференциального криптоанализа на примере анализа свойств и показателей алгоритма DES с таблицами подстановок случайного типа, ранее представленных нами [1]. Покажем, что они все еще не обеспечивают гарантированной защиты от дифференциального криптоанализа, и определим условия, при которых эта защита возможна. Таблицы *S* блоков, приведенные в [1] в качестве примера, вместе с дополнениями, содержащими основную информацию о параметрах подстановок и таблиц подстановок, которые выявлены на первых двух уровнях проверки, проведенной по методике работы [2], представлены в табл.1. В ней использованы следующие обозначения: ***I*** -инверсии, ***V*** -возрастания, ***L*** -циклы, ***M*** -среднее. Значения входов и выходов даны в 16-ричной системе счисления. В нижних строках приведены данные о количествах совпадений элементов в столбцах. Эти строки состоят из одних нулей, т.е. табл.1 составлена из подстановок противоречивого типа. По показателям отбора третьего уровня [2] все пары рассматриваемых таблиц (табл.1) по числу совпадений не превосходят значения $q = 5$.

Кратко остановимся на основных идеях, составляющих теоретическую сущность метода дифференциального криптоанализа, поскольку он еще для многих остается малоизвестным.

В дифференциальном криптоанализе [6,7] используются так называемые таблицы распределения разностей для каждого *S* блока. Для построения этих таблиц просматриваются все возможные 4 -битные числа, которые могут получиться на выходе *S* блока, при поступлении на его вход различных 6 -битных комбинаций. Далее вычисляются поразрядные суммы по модулю 2 (XOR) входных (результат – также 6 битов) и XOR выходных значений (результат – 4 бита). Полученные числа являются индексами входов в ячейку таблицы разностей размера 64×16. Сама таблица разностей получается заполнением ячеек числами, которые соответствуют количеству попаданий выходов рассматриваемого *S* блока, образующих заданные значения разностей (индексов входов в ячейку таблицы по столбцам) и заданные значения входных разностей (индексов входов в ячейки по строкам) при вариации по всему множеству пар входов и выходов этого *S* блока.

Математически отмеченные действия можно описать следующим образом.

Пусть $\bar{x}_i = \left(x_{i1}, x_{i2}, x_{i3}, x_{i4}, x_{i5}, x_{i6}\right)$ – 6-битный вектор, обозначающий один из $i = \overline{1,64}$ возможных входов *S* блока, $\bar{a}_l = \left(a_{l1}, a_{l2}, a_{l3}, a_{l4}, a_{l5}, a_{l6}\right)$, $l = \overline{1,64}$ – 6-битные константы (индексы ячеек – входов в таблицу по строкам).

Пусть вектор $\bar{y}_p = \left(y_{p1}, y_{p2}, y_{p3}, y_{p4}\right)$ обозначает один из $p = \overline{1,16}$ 4-битных выходов *S* блока, $\bar{b}_m = \left(b_{m1}, b_{m2}, b_{m3}, b_{m4}\right)$, $m = \overline{1,16}$ s – 4-битные константы, являющиеся индексами ячеек – входов в таблицу по столбцам.

Таблица 1

S	№	I	V	L	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S_1	1	64	9	4	9	5	0	A	B	C	7	D	E	F	2	4	3	6	8	1
	2	54	9	2	D	0	7	9	3	A	B	6	1	4	8	C	E	F	5	2
	3	60	9	2	6	E	A	2	F	3	5	C	7	1	4	8	9	0	B	D
	4	67	9	3	8	B	D	C	E	1	F	4	2	3	0	5	7	9	A	6
	M	61,25	9	2,75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S_2	1	59	7	1	4	6	1	D	3	E	5	F	A	8	7	C	9	B	0	2
	2	67	8	1	7	B	3	6	C	D	8	5	9	A	E	2	0	F	4	1
	3	62	7	2	B	2	4	C	6	3	D	8	E	F	9	1	7	0	A	5
	4	50	9	2	3	D	F	7	8	1	2	4	0	5	6	E	B	A	9	C
	M	59,5	7,75	1,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S_3	1	54	7	4	D	2	9	6	E	4	0	5	3	A	B	1	F	8	7	C
	2	69	9	1	F	C	4	2	8	9	A	D	E	0	1	7	3	6	5	B
	3	55	9	1	5	7	8	A	3	C	4	E	F	2	0	6	1	B	9	D
	4	63	8	3	4	D	5	E	F	7	2	0	6	B	8	9	A	1	C	3
	M	60,25	8,25	2,25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S_4	1	61	8	3	E	F	7	2	5	3	9	0	4	B	C	6	A	8	1	D
	2	63	8	3	3	B	A	D	7	9	0	C	6	8	2	5	1	4	F	E
	3	68	9	2	B	0	5	C	D	6	E	F	3	7	9	A	2	1	8	4
	4	51	9	3	2	E	B	0	1	4	8	D	7	A	5	9	F	6	3	C
	M	60,75	8,5	2,75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S_5	1	50	7	4	F	4	1	7	6	0	8	9	D	B	2	3	E	A	C	5
	2	65	9	1	6	C	D	5	1	E	F	3	7	4	8	9	0	B	2	A
	3	50	8	4	E	3	B	1	2	8	7	0	5	A	9	C	D	6	F	4
	4	69	8	3	A	B	5	D	F	9	1	4	3	C	0	2	7	E	8	6
	M	58,5	8	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S_6	1	65	9	3	B	0	5	D	C	E	F	1	2	4	8	A	9	6	7	3
	2	60	9	2	6	9	D	E	F	1	3	8	4	2	0	7	5	A	C	B
	3	62	7	2	4	3	7	F	B	6	5	C	9	D	2	E	8	0	1	A
	4	50	8	2	E	F	1	2	5	4	0	9	7	A	6	C	3	B	D	8
	M	59,25	8,25	2,25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S_7	1	64	7	2	A	2	E	8	3	B	C	6	4	0	D	F	5	7	9	1
	2	67	9	3	C	D	0	6	E	F	4	2	B	5	7	8	1	3	A	9
	3	56	9	4	7	F	9	2	A	0	D	1	3	8	B	C	4	6	5	E
	4	69	8	3	8	B	1	A	C	D	E	9	2	6	5	0	3	F	7	4
	M	64	8,25	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
S_8	1	70	9	2	B	3	4	6	9	D	E	F	C	5	2	8	7	A	0	1
	2	54	8	4	9	B	8	2	A	0	C	D	3	1	4	7	6	E	F	5
	3	64	9	2	E	4	F	C	5	2	3	6	7	B	1	D	0	8	9	A
	4	55	9	3	D	E	3	F	0	4	5	1	2	6	B	A	8	9	C	7
	M	60,75	8,75	2,75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Обозначим $\overline{\Delta x_{ij}} = \bar{x}_i \oplus \bar{x}_j$, $i,j = \overline{1,64}$ входные разности (XOR входов) *S* блока, $\overline{\Delta y_{pq}} = \bar{y}_p \oplus \bar{y}_q$, $p,q = \overline{1,16}$, выходные разности *S* блока (XOR выходов). В этих выражениях $\oplus$ – операция побитного суммирования $mod\,2$.

Пусть, далее, $\upsilon_{lm}\left(\overline{\Delta y}_{pq} = \bar{b}_m,\ \overline{\Delta x}_{ij} = \bar{a}_l\right)$, $m = 1,16$, $l = \overline{1,64}$ – количество "попаданий" при заданном значении входной разности $\bar{a}_l$ в ячейку таблицы, соответствующую выходной разности $\bar{b}_m$ при вариации по всем значениям $i,j = \overline{1,64}$, $p,q = \overline{1,16}$.

Элемент таблицы разностей υ_{lm} при рассмотренном подходе позволяет вычислить вероятность $p_{lm} = \dfrac{\upsilon_{lm}}{64}$ появления разности, удовлетворяющей условию $\overline{\Delta y}_{pq} = \bar{b}_m$, на выходе *S* блока при воздействии на его вход всех пар $\bar{x}_i, \bar{x}_j$, образующих разности $\overline{\Delta x}_{ij} = \bar{a}_l$, $i,j = \overline{1,64}$. Сумма всех возможных попаданий в ячейки отдельной строки, очевидно, равна 64, поэтому, чем больше нулевых элементов в строке, тем больше будут значения заполнений оставшихся ячеек и, следовательно, выше значения вероятностей попадания в оставшиеся ячейки таблицы разностей. Просматривая эти разности при распространении шифруемых текстов через циклы DES, когда используется один и тот же ключ, можно

накапливать пары открытых текстов, которые имеют специфические различия. Если находится пара текстов со специфическими отличиями входов и выходов, характеризующаяся в определенном смысле достаточной вероятностью, то по известным выходным отличиям может быть поставлена и решена задача определения некоторой части битов и даже всего ключа шифрования [6].

Построенные в соответствии с изложенной методикой таблицы дифференциальных разностей для *S* блоков, приведенных в табл.1, дают значение максимума дифференциальной вероятности, равное $\frac{12}{64}$. Доля выходов, имеющих однобитное различие, для всех таблиц составляет 22%. Другие параметры таблиц разностей для рассматриваемых *S* блоков представлены в табл.2. При этом использованы следующие обозначения: Z – процент выходов, имеющих нулевые значения, M_{v1} – максимальное значение выходов с однобитными различиями, V_{dd} – значение элемента в таблице распределения дифференциальных разностей. Однако на успешное проведение дифференциального криптоанализа влияет не только и не столько абсолютное значение указанной вероятности, но еще и взаимосвязь входных битов нескольких *S* блоков, проявляющаяся через таблицу расширения *E*, с которой начинается цикловая функция.

В работах [6,7] эта взаимосвязь входов с выходами *S* блоков для фиксированного цикла названа характеристикой, которая может быть распространена и на несколько циклов. Пока вероятность соответствующей характеристики меньше некоторого порогового значения, дифференциальный криптоанализ неэффективен (его сложность оказывается большей, чем прямой перебор всех ключей). Как только находится характеристика с вероятностью, большей пороговой, дифференциальный криптоанализ становится эффективным.

Будем сразу рассматривать оптимизированный вариант атаки на полный 16-цикловый DES, обоснованный в [6]. Имеется в виду использование при проведении атаки максимально возможного числа тривиальных характеристик (так они названы в [7]), которые истинны с вероятностью 1.

Это достигается путем применения одноциклового "обнуляющего" разностного преобразования, которое в сочетании с тривиальным циклом позволяет сформировать двухцикловую конструкцию, допускающую итеративное продолжение. Обнуляющим разностным преобразованием мы здесь назвали преобразование некоторой разности пары открытых текстов $\overline{\Delta X} \neq \bar{0}$ на входе цикловой функции $f(R_{i-1}, K_i)$ алгоритма DES в разность $\overline{\Delta Y} = \bar{0}$. Такое преобразование позволяет, с одной стороны, исключить неконтролируемое размножение битов (лавинный эффект) при проходе последующих циклов DES -преобразования, а с другой- обеспечить получение на выходах соответствующих циклов при обработке реальных пар открытых текстов разностей $\overline{\Delta Y} \neq \bar{0}$, которые предлагают максимальные вероятности для истинных ключей. Здесь $\overline{\Delta X}$ и $\overline{\Delta Y}$ обозначают соответствующие разности на входе и выходе всей цикловой функции (когда активными являются несколько *S* блоков). Чем больше размерность вектора $\overline{\Delta Y}$ (соответственно $\overline{\Delta X}$), т. е. чем большее количество битов во входной разности (большее число *S* блоков) участвует в нуль -преобразовании, тем большее число битов ключа может быть выявлено в результате атаки. В работе [5] для атаки используется одновременно три активных *S* блока.

Заметим на дальнейшее, что 4 -блочная характеристика (4 активных *S* блока), использующая нуль-преобразование, при максимальном (завышенном) для рассматриваемой таблицы значении дифференциальной вероятности для одного *S* блока, равной $\frac{12}{64}$, приводит к вероятности результирующей тринадцатицикловой характеристики, равной

$$\left(\frac{12}{64}\right)^{4\times 6} = 2^{-57.96}.$$

Здесь имеется в виду итеративное продолжение шесть с половиной раз двухцикловой обнуляющей характеристики, образующей итоговую 13-цикловую характеристику, которая по методике Э. Бихама [6] может быть использована для 16-цикловой атаки (в циклах со 2-го по 14-й со специально подобранным первым циклом и последующей 2R -атакой).

Аналогично можно показать, что дифференциальные атаки с числом активных *S* блоков большим, чем три, для алгоритма DES также неэффективны.

В табл. 3 представлены вероятности для трехблочных двухцикловых характеристик *S* блоков табл.1.

Из этих результатов следует, что приведенные таблицы подстановок по сравнению с таблицами стандарта обеспечивают более высокую устойчивость против дифференциальной атаки, строящейся с использованием трех активных *S* блоков. Напомним, что для DES максимальное значение вероятности трехблочной двухцикловой характеристики равно $\frac{1}{234}$, что для 13-цикловой характеристики дает результат $\left(\frac{1}{234}\right)^6 = 2^{-47.2}$.

Таблица 2

S_i		S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8
Z		12,9	13,6	14,2	13,9	13,8	13,4	14,5	12,6
M_{v1}		8	8	12	8	12	8	12	10
V_{dd}	0	132	139	145	142	141	137	149	129
	2	254	20	2	10	2	253	3	5
	4	52	3	29	32	35	56	7	23
	6	213	222	196	177	201	198	226	208
	8	82	90	22	112	93	80	86	75
	10	25	26	30	33	33	33	31	33
	12	9	11	7	5	6	10	9	8

Следует заметить, что также имеет значение количество различных одновременно существующих характеристик максимального типа (имеется в виду возможность использования "метаструктур" [6]). Действительно, при наличии нескольких (например, двух и более) близких по значению (совпадающих по вероятности) характеристик для одной и той же группы S блоков возникает возможность уменьшить в 2^t раз количество необходимых открытых текстов, шифруемых на фазе сбора данных, где t – число максимально вероятных трехблочных характеристик, которые используются в атаке.

Расчеты показывают, что для того, чтобы сделать трехблочную атаку дифференциального криптоанализа (при отсутствии метаструктур) действительно неэффективной, достаточно при формировании S блоков обеспечить максимальное значение вероятности осуществления нуль-преобразования для трехблочных характеристик (три активных S блока), удовлетворяющее условию

$$\left(p_T\right)^{\frac{n-4}{2}} = {p_T}^6 \le 2^{-55},$$

или

$$p_T \le \sqrt[6]{2^{-55}} = \frac{1}{645}. \qquad (1)$$

Применение рассмотренного условия для первых трех S блоков табл. 1 с учетом того, что в этом случае $p_T = \frac{1}{341} = \frac{12}{64}\cdot\frac{8}{64}\cdot\frac{8}{64}$, позволяет получить итоговую вероятность $p_T^6 = \left(\frac{1}{341}\right)^6 = 2^{-50.48}$. Она несколько лучше, чем показатели таблиц стандарта. В то же время результирующее значение трехблочной обнуляющей характеристики оказалось недостаточным для того, чтобы обеспечить устойчивость алгоритма DEA против атак дифференциального криптоанализа. В результате требование 4.1 из работы [1] сформулировано в новой редакции:

Требование 4.1. Двухцикловая трехблочная характеристика XOR-переходов вход-выход таблиц S блоков должна обеспечивать нуль-преобразование с вероятностью, не большей, чем $p_{T_0} = \frac{1}{645}$ (при условии, что она не дублируется другими нуль-переходами).

Выполнимость этого требования была проверена моделированием. Из 14 сгенерированных по предложенной методике таблиц удалось реализовать S блоки с параметром

$$p_T = \prod_{i=0}^{2} \upsilon_{l0}\left(S_{((i+j)\bmod 8)+1}\right) = \frac{1}{640},\ l = \overline{0,63},\ j = \overline{0,7}$$

без повторений в пределах каждой тройки таблиц.

Покажем теперь, что выполнение этого требования в общем случае является достаточным для того, чтобы любая трехблочная атака оказалась неэффективной. Для этого достаточно доказать, что любая другая трехблочная дифференциальная характеристика будет иметь результирующую вероятность меньшую, чем вероятность, которая достигается при проведении атаки с максимально возможным числом тривиальных характеристик, т. е. при использовании в атаке повторяющихся двухцикловых трехблочных разностных обнуляющих преобразований, рассмотренных выше.

Прежде всего заметим, что если бы результирующая характеристика могла быть построена без использования тривиальных циклов, то даже для того маловероятного случая, когда в каждом цикле реализуется трехблочная одноцикловая характеристика с максимальной вероятностью $p_T = \left(\frac{1}{4}\right)^3 = 2^{-6}$ (для отбора таблиц в [2] назначен уровень $\frac{12}{64} < \frac{1}{4}$), потребовалось бы $\left(p_T\right)^{n-4} = \left(2^{-6}\right)^{12} = 2^{-72}$ отобранных текстов, что больше числа возможных открытых текстов, поэтому атака в этом случае не проходит. Значит, имеет смысл рассматривать только атаки, в которых используются тривиальные циклы.

Пусть теперь параметры трехблочных одноцикловых характеристик p_T S блоков выбраны так, что удовлетворяется условие (1). Покажем, что вероятность любой другой характеристики, содержащей меньшее, чем максимально возможное число тривиальных циклов, будет меньше, чем $\left(p_T\right)^{\frac{n-4}{2}}$.

Заметим, что тривиальная характеристика может быть получена только при использовании на предшествующих циклах соответствующей обнуляющей дифференциальной характеристики. Чтобы убедиться в этом, рассмотрим некоторый произвольный тривиальный цикл, представленный в нижней части рисунка. Поскольку тривиальная характеристика получается при нулевом входном значении цикловой функции, то это означает, что либо значения разностей, поступающих на входы сумматора по модулю два предыдущей цикловой функции, равны нулю (но тогда предыдущая цикловая функция является обнуляющей), либо на входы сумматора подаются идентичные значения. На рисунке эти идентичные значения обозначены символом ψ. В результате на предыдущем цикле выполняется преобразование $\psi = F(\Delta)$, где Δ – разность на входе цикловой функции, причем ψ одновременно является и входом цикловой функции более высокого "этажа", а ее выходом является уже рассмотренное значение разности Δ. Очевидно, что такое выходное значение разности для четырехцикловой характеристики (имеется в виду ее итеративное продолжение) может быть только в том случае, если преобразование $F(\psi)$ обнуляющее, т. е. если $F(\psi) = 0$. Также следует (см. рисунок), что для последнего из рассматриваемых циклов должно выполняться цикловое преобразова-

Таблица 3

Объединяемые S блоки	$S_1S_2S_3$	$S_2S_3S_4$	$S_3S_4S_5$	$S_4S_5S_6$	$S_5S_6S_7$	$S_6S_7S_8$
Максимальная вероятность характеристики (их количество)	$\frac{1}{341}$ (2)	$\frac{1}{682}$ (4)	$\frac{1}{436}$ (2)	$\frac{1}{512}$ (4)	$\frac{1}{682}$ (4)	$\frac{1}{682}$ (1)

ние $\psi = F(\Delta)$. Для вероятности этой четырехцикловой характеристики можно записать выражение

$$p_T^{(4)} = \left(p_1 p_2 p_3\right)^2 \cdot p_T, \qquad (2)$$

В то же время для четырех циклов, составленных из двух цикловых обнуляющих характеристик, имеем

$$p_T^{(4)} = \left(p_T\right)^2. \qquad (3)$$

Из сопоставления выражений (2) и (3) следует, что

$$\left(p_1 p_2 p_3\right)^2 p_T \left(p_T\right)^2 > \left(p_1 p_2 p_3\right)^2 \cdot p_T,$$

так как всегда $p_T > \left(p_1 p_2 p_3\right)^2$ и, в частности,

$$\frac{1}{341} > \left(\frac{12}{64}\right)^6.$$

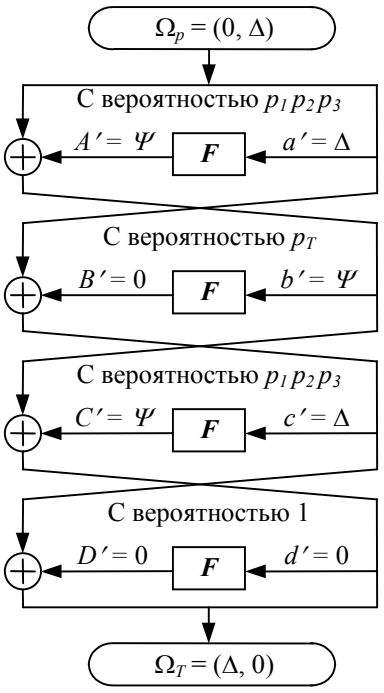
Представляется также очевидным, что реализация характеристик с меньшим числом тривиальных переходов тем более не приведет к большей угрозе дифференциальной атаки, чем рассмотренные выше.

К сожалению, и в новой редакции требование 4.1 оказывается недостаточным для обеспечения защиты от атак дифференциального криптоанализа. Обеспечив при отборе случайных таблиц должный уровень защиты от известных атак, использующих трехблочные характеристики, мы оставили без должного внимания возможность реализации характеристик, которые применяют меньшее число активных S блоков. В стандарте, как показывает анализ, эти характеристики исключены, в то время как для рассматриваемой случайной таблицы может быть построена характеристика с двумя активными S блоками и максимальным значением нуль -преобразования для одного S блока, равным $p_Д = \frac{6}{64}$. В этом случае имеем

$$\left(\frac{6}{64}\right)^{2\times 6} = 2^{-40.98},$$

что существенно хуже стойкости стандарта. Таким образом, предлагаемые критерии отбора случайных таблиц подстановок все еще не позволяют решить задачу формирования S блоков, полностью защищенных от атак дифференциального криптоанализа.

Литература: 1. *Лисицкая И.В., Головашич С.А., Олешко О.И., Олейников Р.В., Коряк А.С.* Построение таблиц подстановок для стандарта шифрования данных // Проблемы бионики. 1999. Вып. 50. С.185-194. 2. *Горбенко И.Д., Лисицкая И.В.* Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 // Радиотехника. 1997. Вып. 103. С. 121-130. 3. ANSI X9.F.1. TDEA modes of operation. Draft 5.5, X9.52, March 29, 1996. 4. NIST. AES announce-ment. Draft, June 15, 1997. 5. *Lars R.* Knudsen DEAL - A 128-bit Block Cipher. 1998. P. 1-9. 6. *E. Biham, A. Shamir* Differential Crypto-analysis of the full 16-round DES. Technical Report-Computer Science Department, Technion, Israiel, 1993. 11p. 7. *Schneier B.* Applied Cryptography. *S*econd Edition: pro-tocols, algorithms, and Source code in C. Published by John Wiley & *S*on*S*. Inc, New York, 1996. 758p.



Четырехцикловая характеристика

Поступила в редколлегию 02.03.99

Рецензент: д-р техн. наук Стасев Ю. В.

Лисицкая Ирина Викторовна, канд. техн. наук, доцент ХТУРЭ. Научные интересы : вероятностно-статистические методы и методы теории чисел в задачах криптографических преобразований и защиты информации. Адрес: Украина, 310180, Харьков, пер. Шекспира, 7, кв. 84, тел. 32-44-60.

Олейников Роман Васильевич, аспирант кафедры ЭВМ ХТУРЭ. Научные интересы : криптография, информационные технологии. Адрес: Украина, 310058, Харьков, ул. Маяковского, 14, кв. 249, тел. 30-24-52.

Головашич Сергей Александрович, аспирант кафедры ЭВМ ХТУРЭ. Научные интересы : криптография. Адрес: Украина, 310174, Харьков, пр. Победы, 61, кв. 311, тел. 30-24-52.

Коряк Алексей Сергеевич, аспирант кафедры ПО ЭВМ ХТУРЭ. Научные интересы : криптография. Адрес: Украина, 310140, Харьков, пр. Гагарина, 48, кв.24, тел. 30-24-52.

Олешко Олег Иванович, аспирант кафедры ПОЭВМ ХТУРЭ. Научные интересы : криптография. Адрес: Украина, 310202, Харьков, пр. Победы, 51Б, тел. 30-24-52.

УДК 519.711

ЗНАНИЕ-ОРИЕНТИРОВАННЫЙ ПОДХОД К РЕИНЖИНИРИНГУ БИЗНЕС-ПРОЦЕССОВ

ЧАЛЫЙ С.Ф., КАУК В.И.

Рассматриваются вопросы влияния реинжиниринга бизнес-процессов на систему знаний, накопленных в организации. Приводится структура бизнес-процессов и подход к их перепроектированию. Формулируются основные аспекты влияния реинжиниринга бизнес-процессов на систему знаний организации. Предлагаются направления реорганизации знаний при реинжиниринге бизнес-процессов на основе использования информационных технологий.

1. Реинжиниринг бизнес-процессов

Реинжиниринг бизнес-процессов – это интенсивно развивающееся направление в менеджменте, направленное на радикальное повышение эффективности функционирования организации как единого целого. Реинжиниринг предполагает "фундаментальное переосмысление и **радикальное перепроектирование** бизнес-процессов для достижения существенных улучшений в таких ключевых для современного бизнеса показателях результативности, как затраты, качество, уровень обслуживания и оперативность" [1].