УДК 681.3.06: 519.248.681

И. В. ЛИСИЦКАЯ, Т. В. ЦЕПУРИТ, В. В. ЛЕСНЯК, М. В. ПИНЧУК, А. П. МЕЛЕЦКИЙ

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ МОДЕРНИЗАЦИИ ШИФРА ГОСТ 28147-89 С ЦЕЛЬЮ ДАЛЬНЕЙШЕГО ПОВЫШЕНИЯ ЕГО БЕЗОПАСНОСТИ

Современный этап развития криптографии характеризуется появлением новых требований к системам шифрования. К наиболее актуальным можно отнести требование к увеличению длины шифруемого блока и требование обеспечения стойкости алгоритма к известным криптоаналитическим атакам. Это приводит к необходимости разработки новых алгоритмов, что само по себе является очень сложным и дорогостоящим. В данной работе была сделана попытка не разработки нового, а модернизации существующего и хорошо зарекомендовавшего себя алгоритма с целью приведения его в соответствие к современным требованиям.

Одной из наиболее универсальных и мощных криптоаналитических атак на симметричные системы шифрования в настоящее время является дифференциальный криптоанализ. Он был первым успешным криптонападением на американский стандарт DES, который до этого более 15 лет считался неуязвимым. Поэтому эта атака обязательно учитывается при оценке стойкости любой современной симметричной системы шифрования.

Напомним основные положения дифференциального криптоанализа [1]. Атакующий имеет возможность управлять разностями пар открытых (незашифрованных) блоков на входе шифратора и имеет доступ к его выходу. Для уязвимых алгоритмов существуют разности между парами открытых текстов, которые проходят через все циклы алгоритма шифрования с вероятностью, превышающей пороговую. Далее, зная входные и выходные значения открытых и зашифрованных текстов, криптоаналитик имеет возможность получить наиболее вероятные значения ключа шифрования. Успех атаки зависит от вероятности нахождения пары открытых текстов, разность которых приводит к специфической разности шифртекстов.

Для DES-подобных шифров (к числу которых относится и ГОСТ 28147-89) устойчивость к дифференциальному криптоанализу в значительной мере определяется свойствами применяемых при их построении нелинейных преобразований. В шифрах DES и ГОСТ 28147-89 нелинейными преобразованиями являются таблицы подстановок (так называемые S-блоки). Именно на основе анализа свойств S-блоков была предложена методика определения ключей для нескольких DES-подобных шифров со сложностью, меньшей, чем прямой перебор. Отечественный стандарт ГОСТ 28147-89 введен в действие гораздо позже DES. Несмотря на то, что и в ГОСТе нелинейным преобразованием, как и в DES, является подстановка, тем не менее, в открытой литературе практически нет публикаций, посвященных изучению его стойкости к различным атакам. Предполагается, что за счет использования вдвое большого числа циклов, чем DES, ГОСТ обладает более высокой защищенностью от многих известных криптоаналитических атак. Однако, в последнее время появились публикации, в которых идеи дифференциального криптоанализа успешно применены к шифру ГОСТ 28147-89 и доказано существование в этом алгоритме определённых слабостей. [2]

В нашей работе сначала предпринимаются шаги, направленные на дальнейшее повышение стойкости ГОСТ 28147-89 к атакам дифференциального криптоанализа, а затем рассматривается возможность модернизации этого алгоритма путем увеличения вдвое длины шифруемого блока. Для решения первой задачи предлагается заменить в каждом цикле стандартной процедуры криптопреобразований детерминированный сдвиг на 11 разрядов на нелинейную операцию параметрического (управляемого) циклического сдвига.

В рассматриваемой в работе реализации для определения параметра сдвига задействуются пять определенных битов шифруемого полублока, взятые после прохождения им таблицы подстановок. Эти пять битов задают текущее значение сдвига полублока на выходе цикловой функции в каждом цикле преобразований (в пределах от нуля до тридцати одного разрядов). Так как значение сдвига зависит от ключа и шифруемых данных, то он является случайной величиной.

На рис. 1 приведены результаты экспериментов по определению закона распределения значений случайного сдвига, задаваемого для обеспечения максимального быстродействия пятью младшими разрядами.

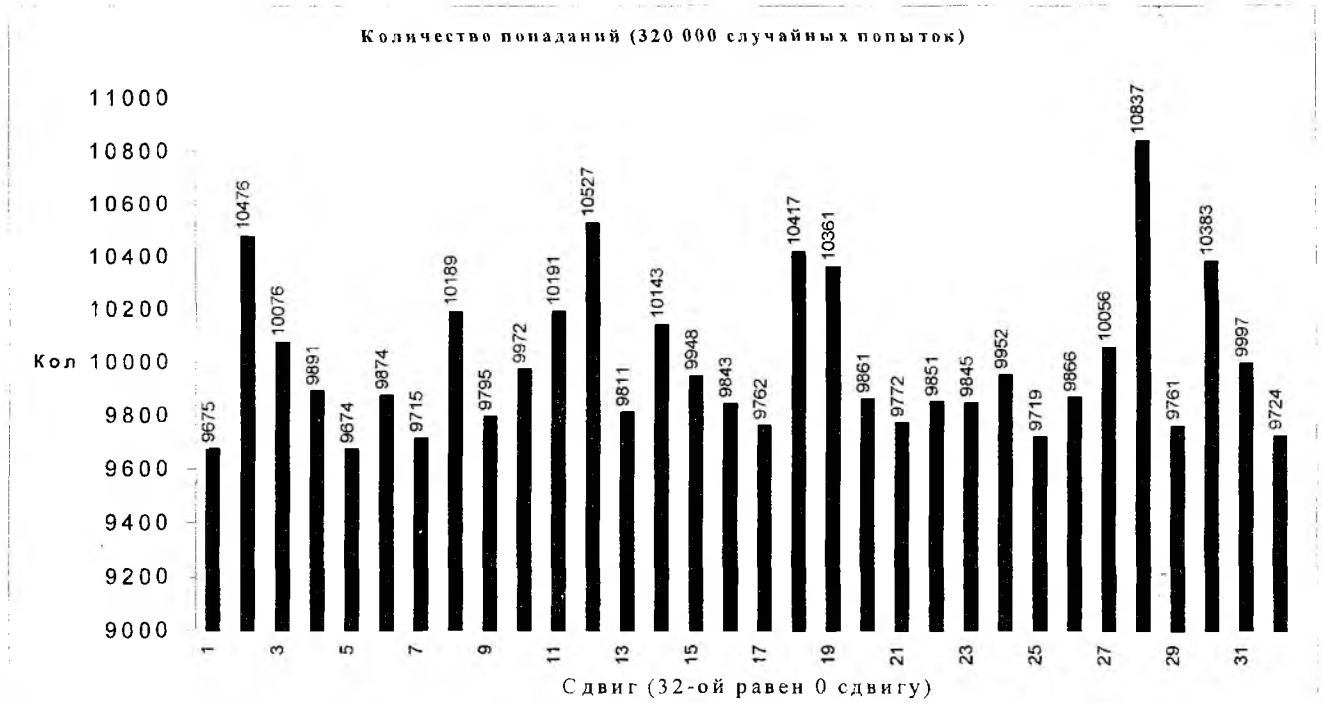

Рис. 1

На основе анализа приведенных данных сделан вывод, что закон распределения можно действительно считать достаточно близким к равномерному. Тогда, если считать, что каждое из значений сдвигов на отдельном цикле процедуры шифрования появляется равновероятно, для вероятности совпадения идентичных значений сдвигов на всех тридцати двух циклах можно получить оценку $(2^{-5})^{-32} = 2^{-160}$. Это позволяет сделать атаку дифференциального криптоанализа на модернизированный ГОСТ неэффективной даже при "благоприятных" ситуациях [2].

Проведение статистических испытаний являются, как известно, единственной стратегией испытаний больших криптографических систем с секретными ключами, построенных в виде чередующихся слоёв блоков замен и перестановок. Поэтому на следующем этапе была выполнена оценка показателей статистической безопасности стандартного и модернизированного алгоритмов.

За основу взяты три показателя стойкости (статистической безопасности [3]), которые принято сейчас использовать при проверке многоцикловых процедур современных блочных систем шифрования:

1. Число циклов алгоритма, начиная с которого две 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 определить число циклов шифрования алгоритма, начиная с которого обеспечивается влияние любого (одного) входного бита, на каждый выходной бит - это, так называемый лавинный эффект .

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

3. Коэффициент сжатия шифрованного текста при применении процедуры архивирования Лемпела-Зива, характеризующий степень его случайности.

На рис. 2-3 приведены результаты оценки глубины входа в модифицированный алгоритм при изменении одного бита сообщения для случаев выполнения процедуры шифрования на одном из долговременных ключей, сформированных разработчиками стандарта, когда сеансовый ключ случайный и когда сеансовый ключ нулевой.

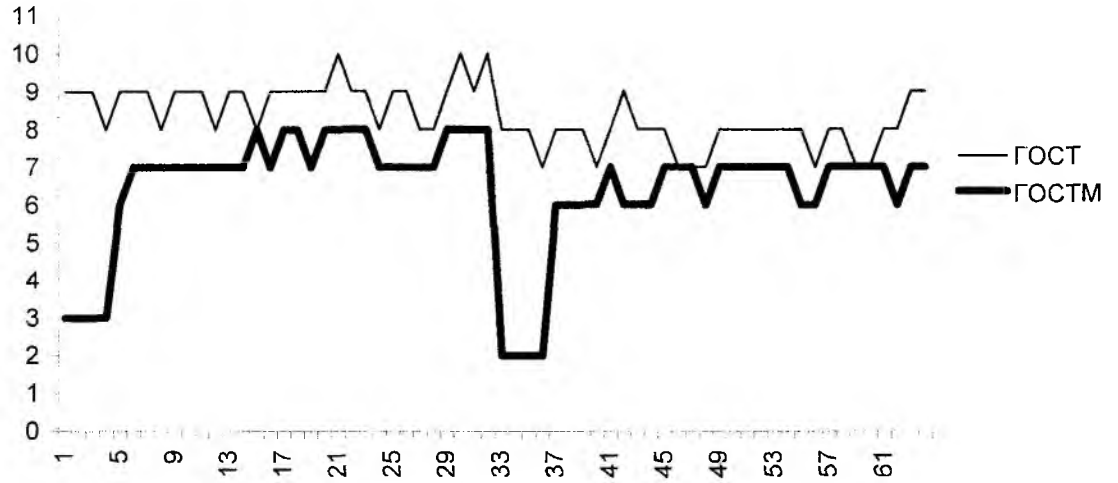

Рис. 2

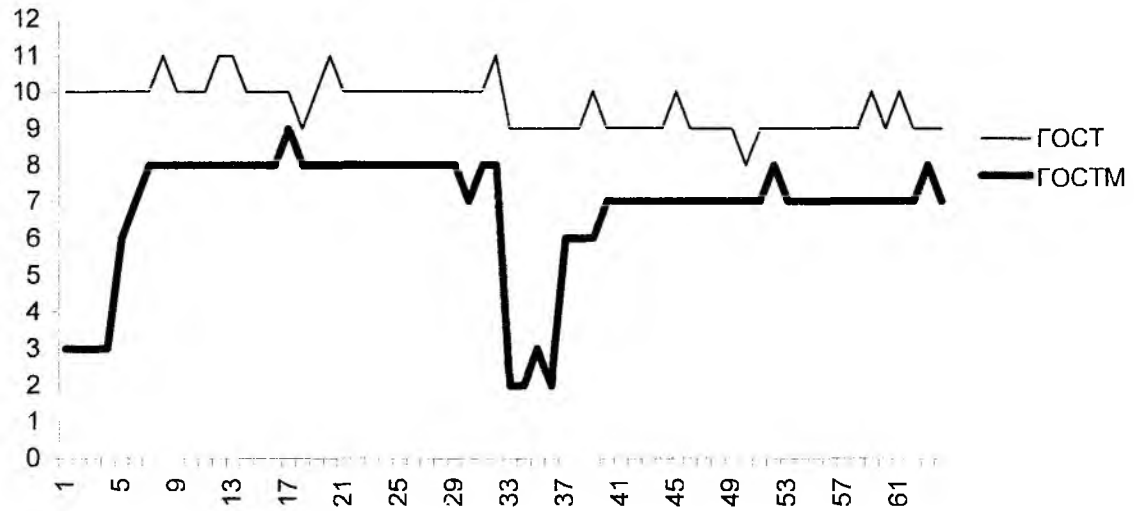

Рис. 3

Глубина входа в алгоритм при экспериментах определялась номером цикла, начиная с которого математическое ожидание числа единичных (ненулевых) бит m_w зашифрованного блока данных удовлетворяло условию $32-0{,}4 \le m_w \le 32+0{,}4$ [3].

На основе полученных данных сделан вывод, что модернизированная процедура построения шифра при использовании случайных таблиц подстановок обладает показателями лавинного эффекта, не уступающими стандартной. Глубина вхождения в алгоритм при использовании ненулевого сеансового ключа $(\overline{K} \neq 0)$, обеспечивающая зависимость всех выходных бит от любого входного бита, в стандартном ГОСТе равна 8-9 циклам. При нулевом сеансовом ключе $(\overline{K} = 0)$ появляется ещё один дополнительный "этаж". Для модернизированного ГОСТа, построенного с применением процедуры параметрического сдвига, лавинный эффект наступает на 2-8 циклах при ненулевом сеансовом ключе $(\overline{K} \neq 0)$ и на 2-9 при нулевом сеансовом ключе $(\overline{K} = 0)$.

Результаты оценки числа циклов алгоритма, при котором наступает статистическая независимость выходных (шифрованных) текстов при шифровании сообщений с помощью ключей $\vec{K}$, отличающихся одним битом, проиллюстрированы на рис 4.

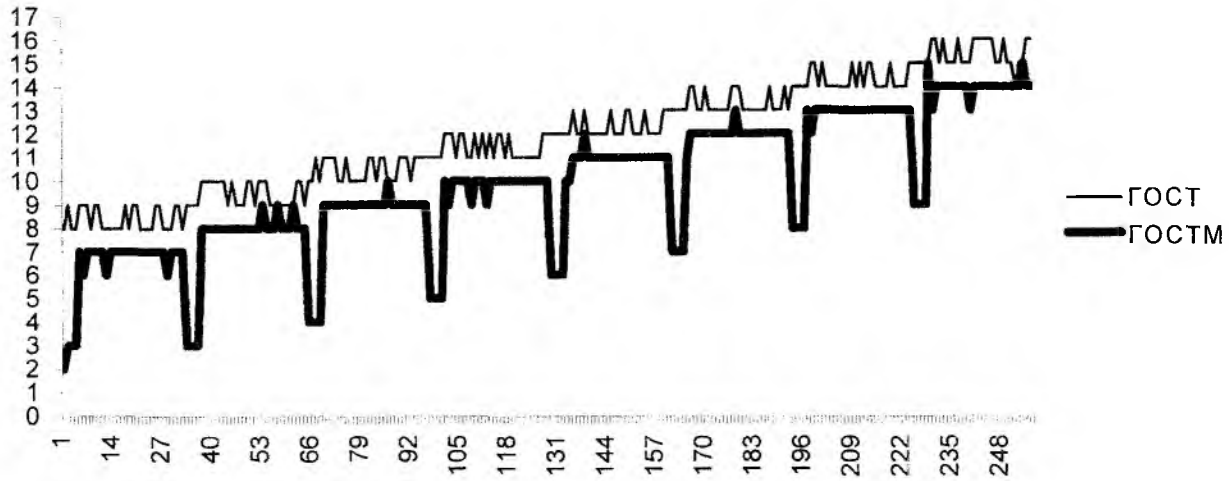

Рис. 4

Как и в предыдущем случае, экспериментальные данные показали улучшение показателей статистической безопасности при применении в алгоритме операции параметрического сдвига (8-16 циклов для ГОСТ 28147-89 и 2 –15 циклов для модернизированного алгоритма).

Таблица 1

	Исходный текст	ГОСТ	ГОСТМ
EXE	49,78	10,09	10,09
WORD	82,42	60,06	60,06
TXT	53,68	1,32	1,32

Проверка степени сжатия текстов проводилась с помощью процедуры Лемпела-Зива на ключах и подстановках случайного типа. Испытывались три варианта текстов: exe-файл, как текст усредненного типа, word-овский файл, как пример очень избыточного (с повторения-ми) текста, и обыкновенный текстовый файл. Результаты этой проверки иллюстрирует табл. 1.

Как видно из представленных результатов, во всех случаях, кроме ситуации с word-файлом, обеспечивается сжатие шифрованного текста менее, чем на 11% [3]. Результат с word-файлом свидетельствует лишь о том, что в этом случае имеется значительная часть повторяющихся (одинаковых) сообщений" при шифровании word-файла на разных сеансовых ключах он уже не сжимается.

На втором этапе была решена задача увеличения вдвое длины шифруемого блока. При построении усовершенствованного симметричного шифра сохранены все основные идеи, использованные в самом стандарте ГОСТ 28147-89, но они переработаны теперь для длины блока, равной 128 битам. Кроме того, как и в предыдущем случае, в цикловую

функцию шифра введена дополнительная операция параметрического циклического сдвига. Результаты проведенных статистических испытаний модернизированного таким образом алгоритма приведены на рис 5-6.

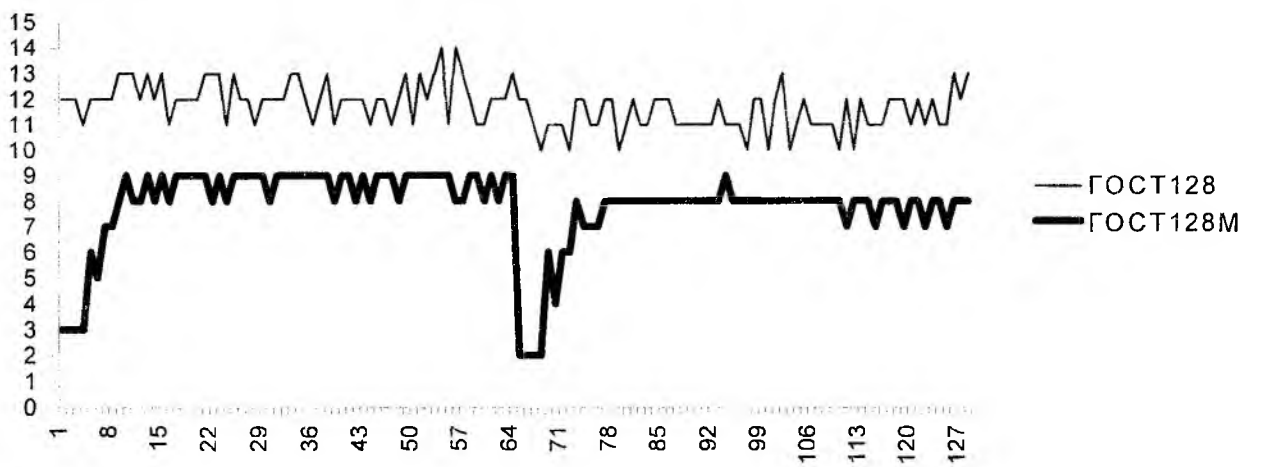

Рис. 5

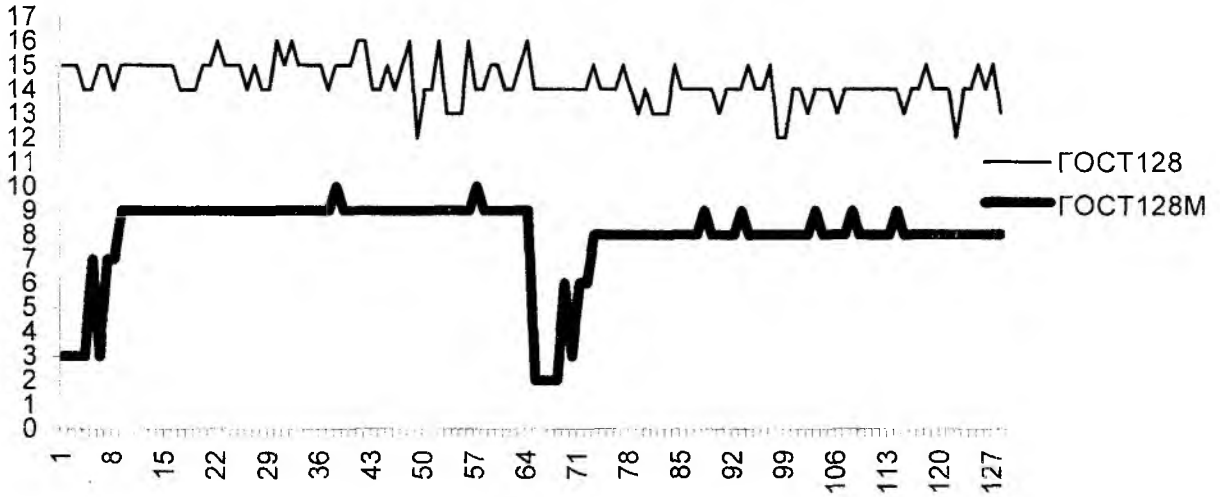

Рис. 6

При использовании в алгоритме ГОСТ–128 ненулевого сеансового ключа $(\overline{K} \neq 0)$ для обеспечения зависимости всех выходных бит от любого входного бита требуется вхождения в алгоритм на глубину до 10-14 циклов. При нулевом сеансовом ключе $(\overline{K} = 0)$ – на 12-16 циклов. Применение в алгоритме параметрического сдвига, как и в предыдущем случае, улучшает результаты.

При ненулевом сеансовом ключе $(\overline{K} \neq 0)$ лавинный эффект наступает на 2-9 циклах, при нулевом $(\overline{K} = 0)$ – на 3-10. Результаты оценки числа циклов алгоритма, при котором наступает статистическая независимость выходных (шифрованных) текстов при шифровании сообщений с помощью ключей $\vec{K}$, отличающихся одним битом, приведены на рис. 7.

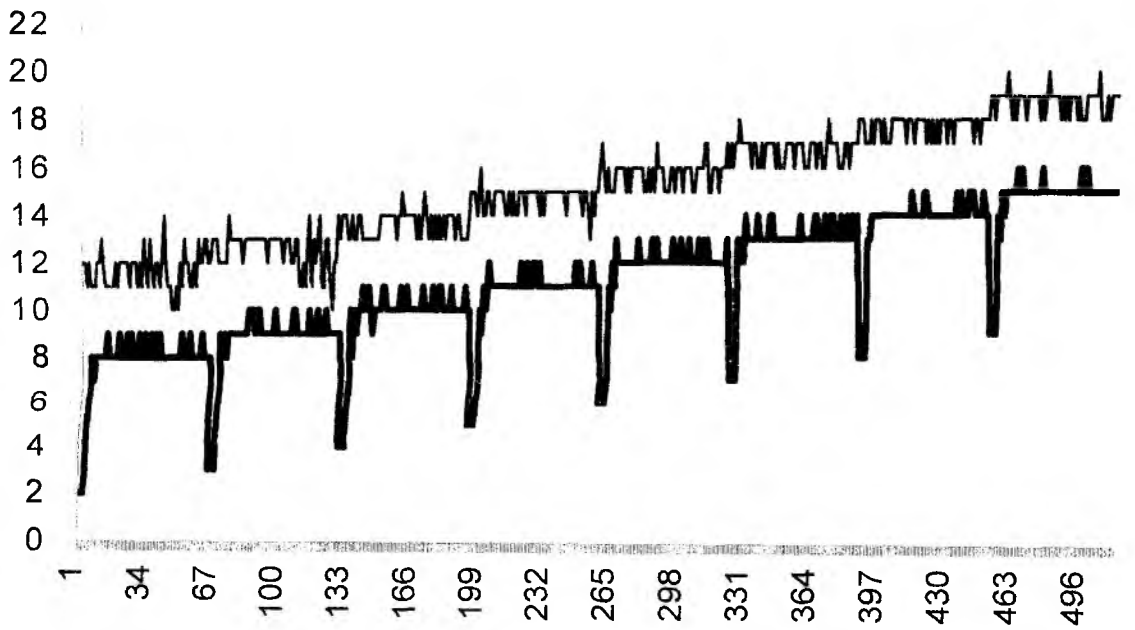

Рис. 7

Как и в предыдущем случае, экспериментальные данные показали улучшение показателей статистической безопасности при применении в алгоритме операции параметрического сдвига (10-20 циклов для ГОСТ -128 и 2–16 циклов для алгоритма с параметрическим сдвигом).

Глубина входа в алгоритм в этом случае определялась номером цикла, начиная с которого математическое ожидание числа единичных (ненулевых) бит m_w зашифрованного блока данных удовлетворяет условию $64 - 0{,}6 \le m_w \le 64 + 0{,}6$.

Результаты проверки степени сжатия текстов, зашифрованных на ключах - подстановках случайного типа, с помощью процедуры Лемпела-Зива приведены в табл. 2

Таблица 2

ТИП	Исходный текст	ГОСТ-128	ГОСТ-128М
EXE	49,78	5,752	5,744
TXT	53,68	0,145	-0,0071
WORD	77,73	39,15	39,16

Как видно, применение 128-битного алгоритма и параметрического сдвига и в данном случае улучшает характеристики случайности шифрованных блоков данных.

Несколько слов относительно быстродействия рассмотренных модернизированных алгоритмов. Наши эксперименты показывают, что введение операции параметрического сдвига не приводит к сколько-нибудь существенным потерям в скорости по отношению к стандартной процедуре шифрования.

В итоге можно сделать вывод, что существует реальная возможность повышения безопасности алгоритма шифрования по ГОСТ 28147-89. Мы продолжаем исследования в рассмотренных направлениях и считаем, что представленные в работе результаты могут заинтересовать специалистов.

Список литературы: 1. *Biham E., Shamir A.* Differential Cryptanalysis of DES-like cryptosystems. The Weizmann Institute of Science. Department of Applied Mathematics. Technical Report CS90-16. 1990. 2. *Долгов В.И., Лисицкая И.В., Олейников Р.В, Шумов А.И.* "Слабые" ключи в алгоритме шифрования ГОСТ28147-89// Радиотехника: Всеукр. межвед. науч.-техн. сб. 2000. Вып 114. С. 63-68. 3. *Горбенко И.Д., Лисицкая И.В., Коряк А.С.* Анализ стойкости алгоритма ГОСТ 28147-89 при использовании подстановок случайного типа // Радиотехника и информатика. 1998. №1(02). С.63-68.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 6.03.2001