МИНИСТЕРСТВО ОБРАЗОВАНИЯ
РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ
УНИВЕРСИТЕТ

ТРУДЫ

БЕЛОРУССКОГО ГОСУДАРСТВЕННОГО ТЕХНОЛОГИЧЕСКОГО УНИВЕРСИТЕТА

ВЫПУСК VI

Серия IV

Физико-математические науки и информатика

МИНСК 1998

УДК 681.325.6

Н.В. Пацей, аспирант;
П.П. Урбанович, профессор

КОМБИНИРОВАННОЕ ПРЕОБРАЗОВАНИЕ ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ ДЛЯ ПОВЫШЕНИЯ ЦЕЛОСТНОСТИ И НАДЕЖНОСТИ ДАННЫХ (СИСТЕМА ЗК)

The authors of the article offered new stream cryptoalgorithm for enciphering error sensitive streams of the information in communication channels. Correction of double packet errors is one of the main attribute of this algorithm. The descriptions of algorithm and block diagrams of encoding operations are given.

В некоторых случаях не только конфиденциальность, но и целостность данных, передаваемых по сетям телекоммуникаций, играет исключительно важную роль. Например, для реализации финансовых операций и при распределении открытых ключей между объектами сети. Задача состоит в том, чтобы криптографическая система, используемая для обеспечения конфиденциальности, обеспечивала также адекватную защиту целостности сообщений. Примером такого интегрированного подхода может стать предлагаемая система на основе криптопреобразований и использования корректирующих кодов (условно назовем ЗК).

В качестве криптографической функции для обеспечения конфиденциальности используется самосинхронизирующийся потоковый шифр с обратной связью по шифротексту. В самосинхронизирующихся потоковых шифрах следующее состояние системы определяется функцией, которая использует как один из входов некоторый предварительно сгенерированный шифротекст.

В режиме шифрования потока данных генерируется псевдослучайная последовательность (ПСП) битов, которая суммируется по модулю два с исходным текстом для формирования зашифрованного сообщения (рис.1). В качестве генератора псевдослучайной последовательности (ГПСП) используется схема шифрования данных симметричным блочным алгоритмом Blowfish в режиме PFB (Plaintext Feedback Mode). Алгоритм Blowfish характеризуется более высоким быстродействием в сравнении с часто используемыми DES и IDEA, не требует лицензии для использования и не запатентован (впервые был представлен в 1993 году в Cambridge Algorithms Workshop - UK Брюсом Шнейером[1]). PFB получен в результате комбинации режимов CFB и OFB [2].

Алгоритм Blowfish состоит из двух частей: распределение ключей и шифрование данных. При распределении ключи переменной длины конвертируются в несколько массивов подключей: *P*- и *S*-массивы общим

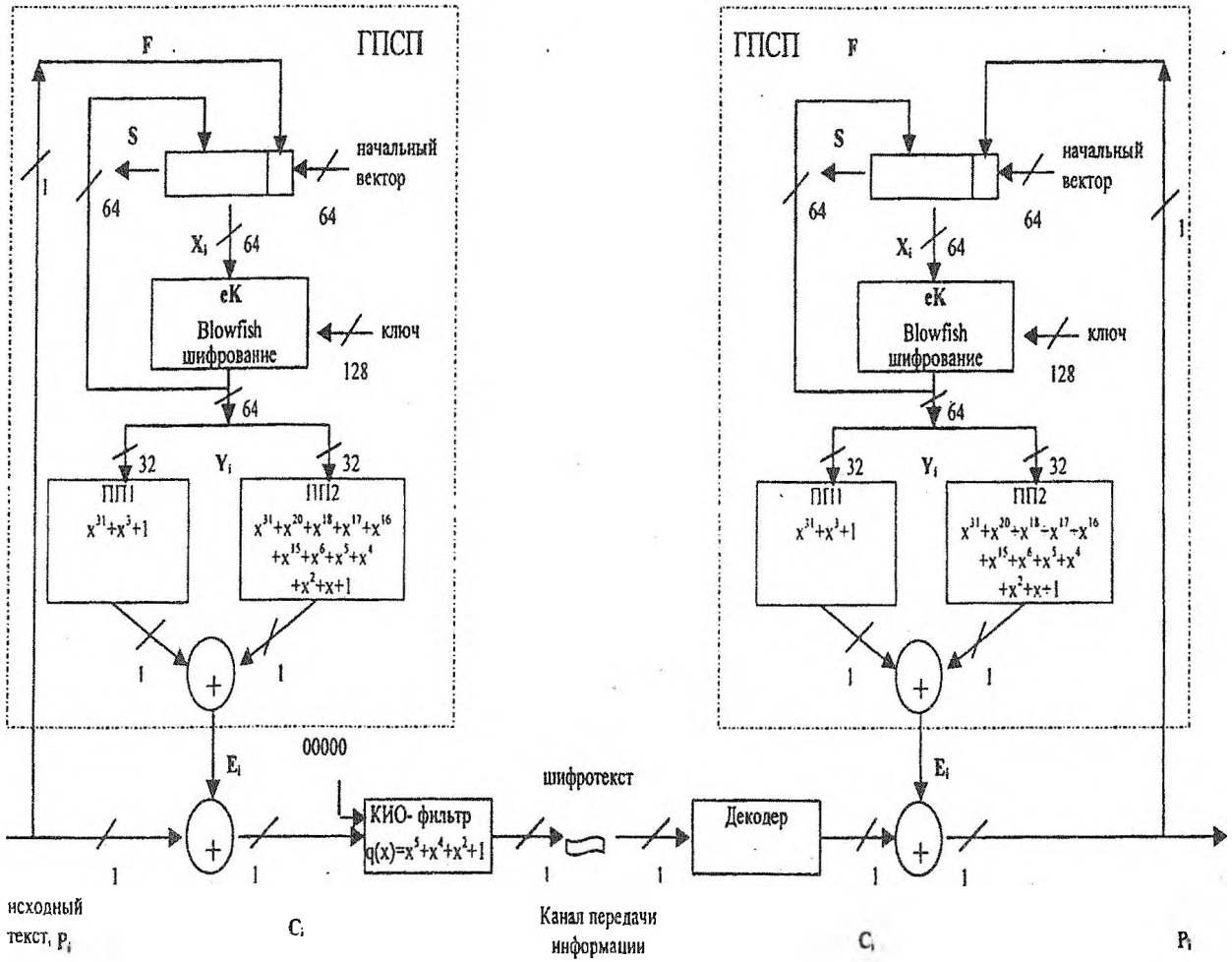

Рис. 1. Структурная схема шифрования\дешифрования 3К алгоритма

объемом 4168 бит. Эти массивы вычисляются до шифрования/дешифрования данных. *P*-массив состоит из восемнадцати 32-битных подключей P_m, а четыре 32-битных *S*- массива $S_{i,j}$ содержат по 256 записей каждый; $m=1\div18$; $i=1\div4$; $j=0\div255$.

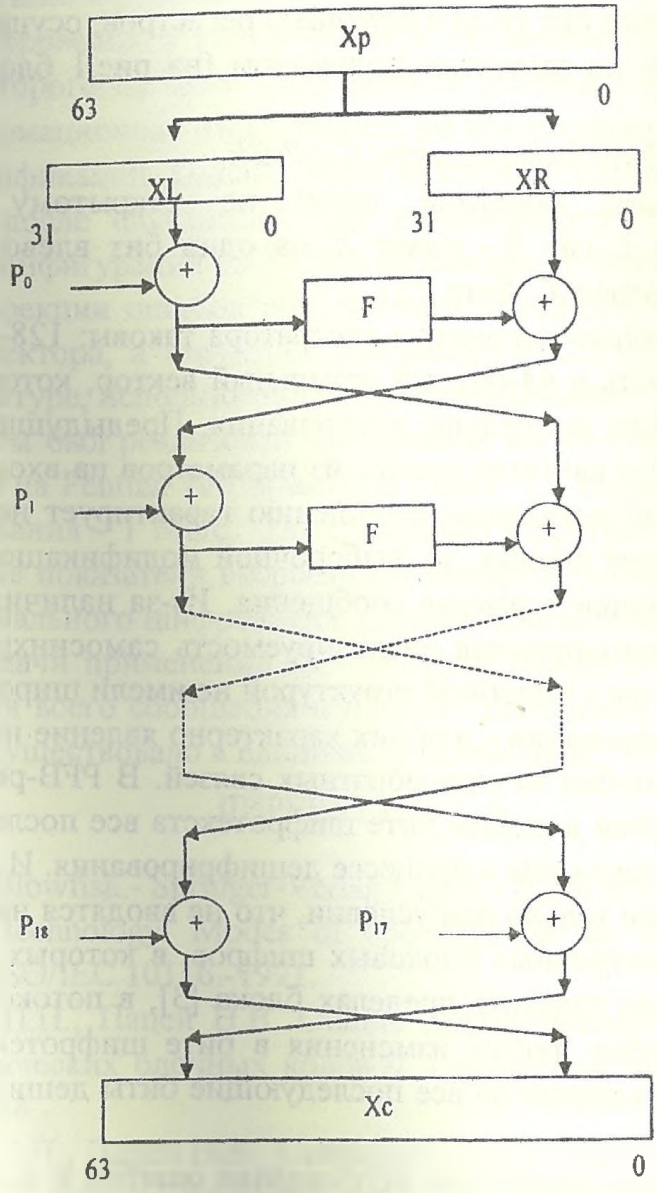

Рис.2. Схема, реализующая алгоритм шифрования Blowfish

Структура алгоритма шифрования Blowfish приведена на рис. 2. Входной блок данных X_p делится на две равные части: *XL* и *XR*. Затем *XL* делится, в свою очередь, на четыре 8-битные части: *a*, *b*, *c*, и *d*, а функция *F* выглядит следующим образом[1]:

$F(XL)=((S_{1,a}+S_{2,b} \bmod 232) XOR\ S_{3,c})+S_{4,d} \bmod 232.$

Дешифрование осуществляется точно так же, как и шифрование, однако P_m используются в обратном порядке. Необходимо отметить, что, не-

смотря на многочисленные попытки, не было осуществлено ни одной атаки (известной из публикаций), полностью разбивающей Blowfish.

Blowfish используется в ЗК-системе в режиме PFB. Генерация PFB-режима включает следующие четыре шага (рис.1):

- процедура шифрования Blowfish: $Y_i=eK(X_i)$, где eK- шифрование;
- формирование бит ПСП с помощью регистров, осуществляющих преобразование по заданным полиномам (на рис.1 блоки ПП1 и ПП2): $E_i=PR(Y_i)$;
- генерация бита шифротекста: $C_i=P_i \oplus E_i$;
- формирование обратной связи по открытому тексту: $X_i=Y_i$; $X_{i+1}=S(X_i/P_{i-1})$, где S - сдвиг X_i на один бит влево и добавление в младший разряд X_i бита P_{i-1}.

Инициирующие параметры генератора таковы: 128-битная ключевая последовательность и 64-битный начальный вектор, которые загружаются в ГПСП до начала процедуры шифрования. Предыдущий бит открытого текста поступает в качестве одного из параметров на вход генератора. Эта обратная связь по исходному сообщению гарантирует невозможность перехвата и удаления данных, их выборочной модификации или переупорядочения информации в рамках сообщения. Из-за наличия обратной связи ограничена алгоритмическая анализируемость самосинхронизирующегося шифра. Алгоритмы с подобной структурой не имели широкого применения в канальном шифровании - для них характерно явление непрерывного распространения ошибки за счет обратных связей. В PFB-режиме после возникновения ошибки в любом бите шифротекста все последующие биты за ошибкой будут искажены в процессе дешифрирования. И дешифрирование будет правильным только при условии, что не вводятся никакие ошибки. В отличие от симметричных блоковых шифров, в которых распространение ошибки возможно только в пределах блока [3], в потоковых шифрах при накоплении ошибок любые изменения в бите щифротекста будут иметь дополнительное влияние на все последующие биты дешифрированного открытого текста.

После гаммирования для исправления ошибки и выявления модификаций (умышленных и/или неумышленных) вводится избыточность. Проведенные исследования распределения ошибок при передаче дискретной информации по телефонным линиям связи показали, что многие каналы более чувствительны к одинарным ошибкам и пакетам ошибок длины 2[4].

Наиболее простыми в реализации и хорошо изученными кодами, исправляющими пакеты ошибок, являются линейные циклические коды. Для малых пакетов и умеренных длин найдено много хороших кодов[5]. Для ЗК-системы выбран двоичный циклический код, исправляющий пакет ошибок длины 2 с параметрами (15,10). При кодировании непрерывного

потока бит этим кодом информационная последовательность разбивается на блоки по 10 бит. Каждый блок дополняется "прокладкой" из пяти нулей, а результирующий поток битов пропускается через несистематический КИО-фильтр (фильтр с конечным импульсным откликом)[5] для (15,10)-кода с порождающим полиномом $q(x)=x^5+x^4+x^2+1$.

После шифрования и кодирования в ЗК-системе получаем шифротекст, объем которого на одну треть больше входного открытого текста. Введенная информационная избыточность не предохраняет данные от всех возможных модификаций. Однако текст исходного сообщения будет восстанавливаться после случайного или умышленного изменения пакета ошибок любой конфигурации из 2-х бит на каждые 10 бит информации.

Схема коррекции ошибок при декодировании состоит из буферных регистров и селектора, а структура генератора ПСП для дешифрования аналогична структуре, использованной при шифровании.

ЗК-алгоритм был реализован программно на C++. Скорость шифрования алгоритма на Pentum 100 примерно равна 1.3 Мб/с, а скорость операций декодирования - 1 Мб/с. По сравнению с другими криптоалгоритмами полученные показатели скорости не являются достаточными, в особенности для канального шифрования. Однако при возникновении ошибок в процессе передачи применение ЗК - системы намного эффективнее повторной передачи всего сообщения и просто необходимо, если передаваемое сообщение существовало в единичном экземпляре.

ЛИРЕРАТУРА

1. Schneier B. Blowfish.- Springer-Verlag.- 1994.- P.191-204.
2. Information technology. Modes of operation for an n-bit block cipher algorithm // ISO/IEC 10116.-1991.
3. Урбанович П.П., Пацей Н.В. Общие диффузионные характеристики криптографических блочных кодов // Управление защитой информации.-№6-1998.
4. Урбанович П.П., Пацей Н.В., Спиридонов В.В. Распределение ошибок в телефонных каналах передачи дискретной информации // Известия Белорусской инженерной академии.-№1(3)\1, 1997. - С.24-26.
5. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, - 1986.