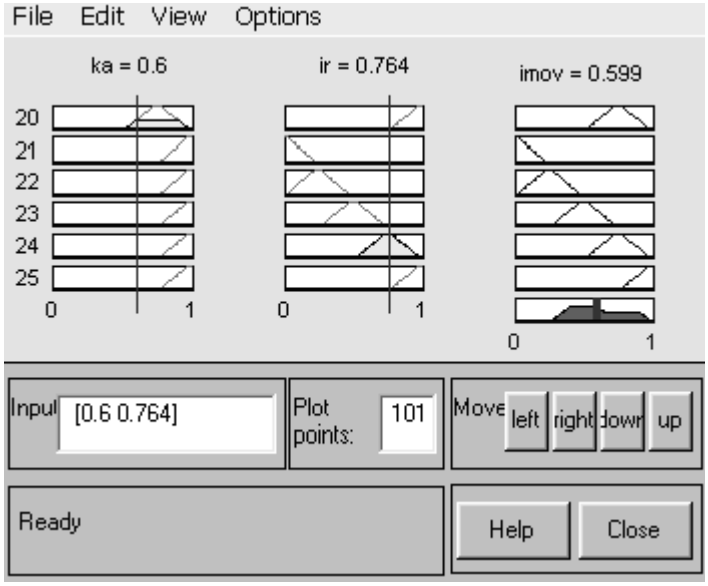

Рис. 3. Фрагмент вікна використання механізму нечіткого виводу

На основі МВКА отримала подальший розвиток модель поводження системи при впливі кібератак, що дозволяє у лінгвістичних термах виявити наслідки прояву найбільш небезпечних для конретних типів ресурсів кібератак.

Список літератури

1. *Харченко В.П., Чеботаренко Ю.Б., Корченко А.Г., Пацира Е.В., Гнатюк С.А.* Кибертерроризм на авиационном транспорте, Проблеми інформатизації та управління. Збірник наукових праць: Випуск 4(28).- К.:НАУ, 2009.

2. *Меняев М.Ф.* «Информационные технологии управления. В 3 т. Т. 2: Информационные ресурсы», Омега-Л, Учебное пособие, 2003.

3. *Захарова М.В*. Аналіз поводження інформаційної системи при впливі загроз // Тези науково-технічної конференції «Захист інформації з обмеженим доступом та автоматизація її обробки».- Київ, НАУ, 2009.

4. *Чистяков В.П*. Курс теории вероятностей. – М., Агар, 1996.

5. *Корченко А.Г., Паціра Є.В., Захарова М.В*. Оцінювання потенційного збитку інформаційних ресурсів при впливі загроз безпеки // Науково-практична конференція «Современные тренажерно-обучающие комплексы и системы –ТКС 2008», Партенит (АР Крым), 2008.

Надійшла 16.03.2010

УДК 004.056.55(045) **Корченко А.Г., Малофеев А.В., Хохлачева Ю.Е.**

КОНВЕЙЕРНЫЙ КРИПТОГРАФИЧЕСКИЙ ВЫЧИСЛИТЕЛЬ РЕАЛЬНОГО ВРЕМЕНИ

В настоящее время для надежного обеспечения конфиденциальности информации применяются криптографические алгоритмы. Использование процессоров и микроконтроллеров, позволяющих защитить информацию посредством выполнения процедур шифрования, стало одним из наиболее эффективных средств борьбы с несанкционированным доступом. Вопросы реализации в реальном времени криптографических алгоритмов остаются по-прежнему актуальными. Программное исполнение указанных алгоритмов не позволяет достичь высокой скорости шифрования. Поэтому средства защиты с такой реализацией не всегда можно использовать в системах

реального времени, особенно в тех случаях, когда преобразуются значительные объемы данных.

В [1] приведен пример построения систолического криптографического вычислителя. Его недостатком является неспособность, положенного в основу алгоритма, обеспечить достаточную криптостойкость и высокую скорость обработки данных для использования в современных системах реального времени. В большинстве публикаций не описываются особенности реализации аппаратных шифраторов, и приводится однопроцессорная структура. Так, например, в работе [2] автор в общих чертах описывает функционирование аппаратного шифратора, в основу которого положен единственный процессор, что свидетельствует о низких скоростных характеристиках представленного шифратора, а в [3] приведено описание некоторых аппаратных шифраторов, использующих различные алгоритмы шифрования (в частности ГОСТ 28147-89), их структурных составляющих, а также элементной базы. Но автор не описывает процесс шифрации информации в соответствии с конкретно взятым алгоритмом и не приводит скоростных характеристик устройств.

В этой связи целью данной работы является повышение быстродействия криптографического вычислителя. Данная цель реализовывается путем применения алгоритма шифрования ГОСТ 28147-89 с последующим отображением его на систолическую структуру, в которой очередной блок, исполняющий функцию шифрования, получает данные из предыдущего.В большинстве криптосистем с секретным ключом, таких как ГОСТ 28147-89, реализуется типовая функция, которая n-кратное число раз осуществляет обработку исходного текста. Эту особенность можно использовать для повышения производительности цифровых устройств, реализующих криптографическое преобразование [1]. С целью минимизации задержки в проектируемой структуре вычислителя некоторые преобразования (перестановки, сдвиги) нужно выполнять посредством соответствующих коммутационных сигнальных линий шин данных. Средняя скорость шифрования одного блока данных в конвейерном криптографическом вычислителе будет возрастать с увеличением объема обрабатываемой информации.

Рассмотрим пример построения конвейерного криптографического вычислителя (КрВ) на базе алгоритма ГОСТ 28147-89 (Рис.1).

Вычислитель КрВ содержит 256-битную входную шину ключа ($Ш_{вх}К$) (разряды которой представляют собой массив, упорядоченный в соответствии с исходными матрицами ключа с 1 по 8, табл. 1-8), 64-битную входную шину данных ($Ш_{вх}Д$) (разряды которой представляют собой массив, упорядоченный в соответствии с исходной матрицей данных, табл. 9), 64-битную выходную шину данных ($Ш_{вых}Д$), модуль начальной обработки данных (МНО), 32 модуля шифрования ($МШ_i$, $i = \overline{1,32}$), модуль формирования результата (МФР) и 2-разрядную шину управления (ШУ), по первому разряду которой поступает стробирующий сигнал записи *i*-й итерации шифрования или дешифрования (Ш/Д), второй – определяет режим работы КрВ Ш/Д.

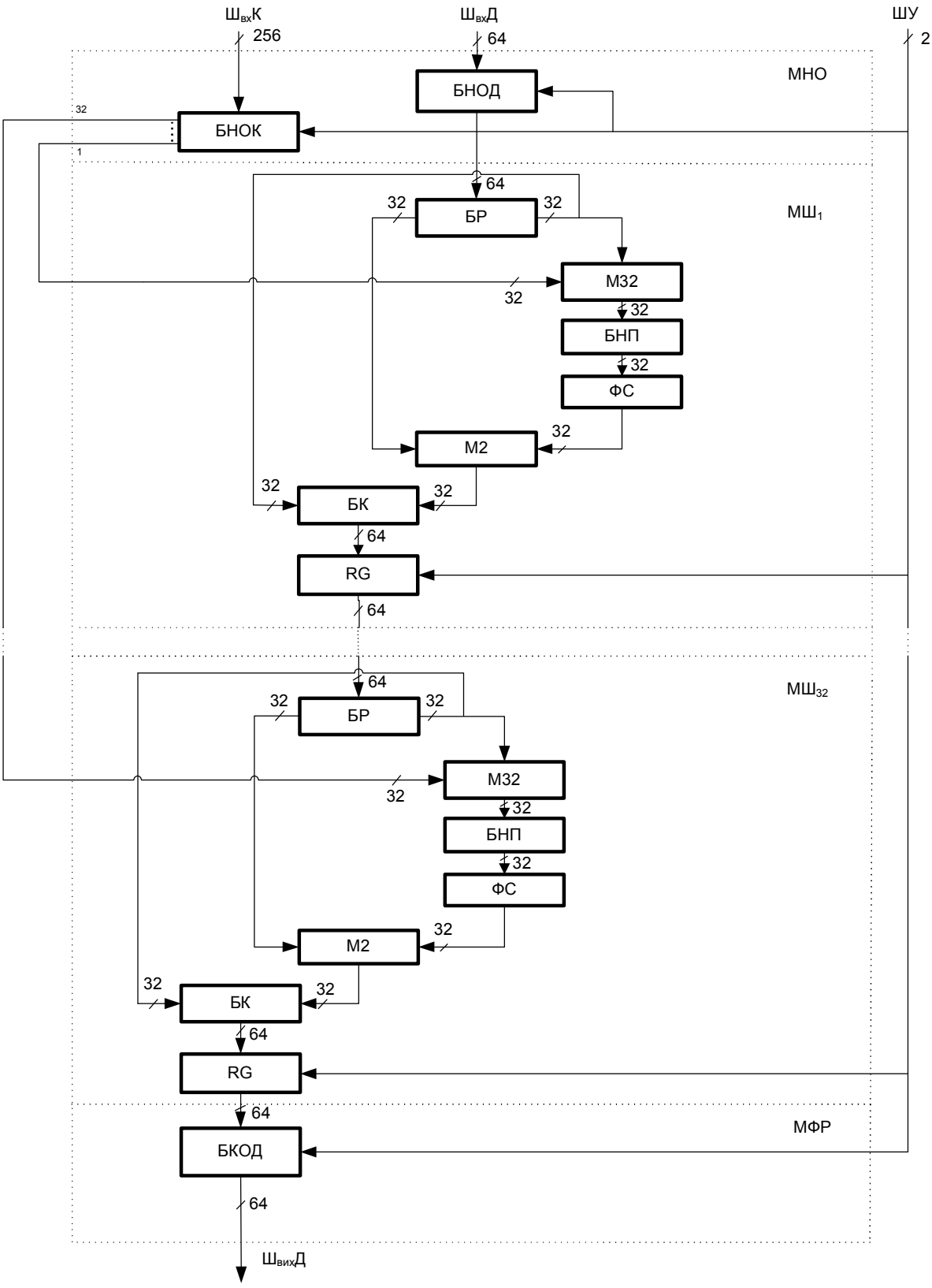

Рис.1. Схема конвейерного криптографического вычислителя

Таблица 1

Исходная матрица ключа №1

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

Таблица 2

Исходная матрица ключа №2

33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Таблица 3

Исходная матрица ключа №3

65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88
89	90	91	92	93	94	95	96

Таблица 4

Исходная матрица ключа №4

97	98	99	100	101	102	103	104
105	106	107	108	109	110	111	112
113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128

Таблица 5

Исходная матрица ключа №5

129	130	131	132	133	134	135	136
137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152
153	154	155	156	157	158	159	160

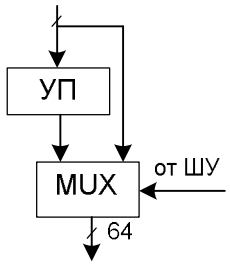

Рис.2. Структура БНПД, БКОД

Таблица 6

Исходная матрица ключа №6

169	170	171	172	173	174	175	176
177	178	179	180	181	182	183	184
185	186	187	188	189	190	191	192

Таблица 7

Исходная матрица ключа №7

193	194	195	196	197	198	199	200
201	202	203	204	205	206	207	208
209	210	211	212	213	214	215	216
217	218	219	220	221	222	223	224

Таблица 8

Исходная матрица ключа №8

225	226	227	228	229	230	231	232
233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248
249	250	251	252	253	254	255	256

Таблица 9

Исходная матрица данных

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Таблица 10

Матрица связей

33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64
1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32

Циклы Ш/Д реализуются с помощью 32 МШ$_i$ ($i = \overline{1,32}$), которые состоят из блоков разделения (БР), блоков сложения по модулю 32 (М32), блоков нелинейного преобразования (БНП), формирователей сдвигов (ФС), блоков сложения по модулю 2 (М2), блоков конкатенации (БК) и регистров (RG).

Блок БР содержит ГК, коммутирующих выходы БНПД соответственно с исходной матрицей данных (Табл.9).

Блок БНП состоит из постоянно запоминающего устройства (ПЗУ), в котором хранится таблица замен (Табл.11).

Таблица 11

Таблица замен

5	9	2	4	8	7	3	10	15	1	13	11	6	14	0	12
7	13	5	12	2	14	4	3	0	8	10	9	1	6	11	15
12	9	11	4	15	5	10	1	14	3	7	13	8	6	0	2
10	8	4	0	6	15	11	3	12	13	2	1	7	5	9	14
8	10	15	6	9	11	4	12	7	1	14	3	5	0	2	13
13	1	10	0	5	8	2	7	7	15	9	12	11	3	6	4
15	7	6	10	12	4	1	11	14	9	8	0	2	5	13	3
15	7	6	10	12	4	1	11	14	9	8	0	2	5	13	3

Блок ФС содержит ГК, коммутирующих выходы БНП согласно матрице сдвигов (Табл.12).

Таблица 12

Матрица сдвигов

12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27
28	29	30	31	32	1	2	3
4	5	6	7	8	9	10	11

Блок М2 содержит MUX, который коммутирует 32-битный код полученный с выходов БР и М2.

Группа контактов БК коммутируют 32-битный код с выхода М2 с 32-битным кодом, полученным с выхода БР согласно исходной матрице данных (Табл.9)

В RG сохраняются результаты Ш/Д, полученные на каждой итерации в $МШ_i$ ($i=\overline{1,32}$). С помощью RG в структуре КрВ формируется конвейер данных, благодаря которому эффективно реализуется функция шифрования.

Блок МФР состоит из БКОД. В БКОД входит УП, который содержит группу контактов, коммутирующих выход RG в соответствии с матрицей связей (Табл.10), и (MUX). (Рис.2)

Сформированная конвейерная структура КрВ функционирует следующим образом. 256-битный ключ поступает через $Ш_{вх}К$ в БНОК, где он разбивается на 8 32-битных частей. Исходный шифруемый текст параллельным кодом по 64-бит, поступает в БНОД и передается на выходы его MUX, который руководится сигналом Ш/Д, поступающим с ШУ. Подготовленные до Ш/Д 64-битные блоки данных (БД) поступают потактно в $МШ_i$ ($i=\overline{1,32}$), в которых указанные данные разделяются на два БД: $БД_l$ и $БД_2$ по 32 бита каждый.

Младшие разряды, содержащиеся в $БД_1$, поступают на второй вход М32, на первый вход которого, по стробирующему сигналу ШУ, БНОК подает, в соответствии с итерацией шифрования, нужную 32-битную часть ключа; а старшие, содержащиеся в $БД_2$ – на первый вход М2. Сформированное 32-битное слово на выходах М32 $МШ_i$ ($i=\overline{1,32}$) поступает на адресные входу ПЗУ БНП, где подлежит побитной замене в соответствии с таблицей замен (Табл.11). С БНП 32-разрядный код поступает в ФС, после преобразования в котором, подается на второй вход М2. В блоке М2 результат полученный с выходов ФС конкатенирует с $БД_2$ подаваемым со второго выхода БР, и поступает на входы М2. В блоке БК 32-битное слово, полученное с выходов М2 занимает позицию младших битов в 64-битном коде, а 32-битное $БД_l$ с первого выхода БР занимает позицию старших битов в 64-битном коде. Полученное 64-битное слово записывается по стробирующему сигналу ШУ в RG.

Результат, который сохраняется в RG $МШ_i$ ($i=\overline{1,32}$), представляет собой зашифрованное или расшифрованное сообщение для і-й итерации (одного цикла Ш/Д). С помощью $МШ_i$ ($i=\overline{1,32}$) в КрВ реализовуется 32-ступенчатый конвейер Ш/Д данных. Полученный в RG $МШ_i$ (i=32) 64-битный БД передается в МФР, где обрабатывается в БКОД, в соответствии с сигналом ШУ. Сформированное 64-битное сообщение поступает на 64-разрядную $Ш_{вых}Д$.

Во время разработки принципиальной схемы КрВ использованы микросхемы КН1832ИА1, КР556РТ181, КР531ЛП5, КР1531ИР23, КР1531КП16 при этом время Ш/Д для

одной итерации составляет 81 нс. В случае конвейерной обработки среднее время Ш/Д одного блока определим за формулой

$$T_{сер} = (n \cdot T + 2 \cdot T_{mux} + (N-1)T) / N,$$

где n – количество ступеней конвейера; T – время шифрования для одной итерации, T_{mux} – время переключения MUX; N – количество блоков Ш/Д данных.

Например, для сообщения размером 1 мбайт $T_{ср}$ составило 0,11 мкс, при этом продуктивность КрВ составляет 91 мбайт/с. Для Ш/Д БД большей длинны, например $N \to \infty$, $T_{ср}$ будет приближаться к T. В этом случае граничная продуктивность Ш/Д для этого типа КрВ приближается к 175 мбайт/с. Скорость шифрации 1 гигабайта информации составила порядка 100 мбайт/с, что в 5 раз превышает скоростные показатели [5]. В случае больших объемов информации скорость шифрации превышает показатели аналогов [5] даже более чем 5 раз. Такой прирост скорости был достигнут за счет использования систолической организации вычислителя для реализации криптографического алгоритма.

Список литературы

1. *Корченко А. Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения / Корченко А. Г. – К. : «МК-Пресс», 2006. – 207-214 с.

2. *Панасенко С. П.* Аппаратные шифраторы / С. П. Панасенко, В. В. Ракитин. – Мир ПК, 2002. - № 8 – 77-83 с.

3. *Онучин С.* Устройства защиты информации. Критерии выбора / С. Онучин. – Мир связи: Connect!, 1998. - №9 –104 с.

4. *ДСТУ ГОСТ 28147-89* Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования. –[Действительный от 01.01.89].

5. Сравнение аппаратных шифраторов [электронный ресурс]: http://www.s-terra.com/CSP/RU/products/itsec_table.htm.

Поступила 16.03.2010

УДК 621.31 **Рыбальский О.В., Белозеров Е.В., Соловьев В.И., Белозерова Я.А.**

МЕТОДОЛОГИЯ ПРОВЕРКИ ПОДЛИННОСТИ СИГНАЛОГРАММ ВЫДЕЛЕНИЕМ САМОПОДОБНЫХ СТРУКТУР

В работе [1] было показано, что цифровой сигнал, записанный на аппаратуре цифровой записи аналоговых сигналов (АЦЗАС), имеет фрактальную структуру, изменяющуюся при монтажных операциях с этим сигналом.

Дальнейшее изучение этого явления подтвердило, что цифровой сигнал, записанный на каждом конкретном аппарате, имеет свою индивидуальную структуру [2]. Потому это физическое явление может быть использовано, для проведения идентификации АЦЗАС при проведении экспертиз. А учитывая то, что, выявление оригинальности сигналограммы основано на идентификации аппаратуры записи, это явление полностью годно для проведения экспертизы оригинальности сигналограмм [3].

Задачей исследования является создание методологии оценки подлинности сигналограмм на основе сравнения фрактальных характеристик сигналов на различных участках сигналограммы.

Будем рассматривать цифровые данные записи звукового файла, как временной ряд отсчетов амплитуды звуковой волны, которые являются результатом взаимодействия двух составляющих - записываемой мелодии, речи и второй составляющей – аппаратурных помех. В общем случае это не обязательно сумма. Если бы статистические характеристики