УДК 681.327

**А.С. ШПАК, И.В. ЛЫСЕНКО**

***Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ»***

# ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МОДЕЛИ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ СООБЩЕНИЙ ПОСРЕДСТВОМ СИММЕТРИЧНЫХ КРИПТОПРЕОБРАЗОВАНИЙ НА ОСНОВЕ ВНУТРИСЕАНСОВОЙ ДИВЕРСНОСТИ

*Описывается подход к формированию кода аутентификации сообщения на основе внутрисеансовой диверсности посредством симметричных криптопреобразований. Модель разрабатывалась по принципу черного ящика. Представлены структуры подмоделей трех используемых режимов работы блочных симметричных шифров (БСШ). Кратко описан процесс программной реализации модели формирования кода аутентификации сообщения (КАС). Приведены результаты исследования скорости обработки данных программной реализацией модели.*

***Ключевые слова:*** *диверсность, вычислительная стойкость, код аутентификации сообщения, криптостойкость, модулярное преобразование.*

## Введение

Целостность и аутентичность – важные услуги (функции) защиты данных, передаваемых по открытым каналам. Как известно, они реализуются посредством использования ключевых и бесключевых однонаправленных (необратимых) криптопреобразований над документом (сообщением), позволяющих сформировать криптографическую контрольную сумму, которая зависит от документа и длина которой обычно значительно меньше размерности самого документа. Для бесключевых однонаправленных криптопреобразований эту криптографическую контрольную сумму принято называть хэш-значением или дайджестом документа, а для ключевых – кодом аутентификации сообщения ( КАС ) или имитовставкой.

В отличие от хэш-значения, которое в целях обеспечения подлинности и целостности данных должно передаваться в зашифрованном виде, сформированный КАС добавляется к исходному тексту и отправляется по открытому каналу; на стороне получателя КАС отделяется от основного текста и получатель формирует КАС по тому же алгоритму, что и на стороне отправителя. В завершении КАС (отправителя) сравнивается с КАС , рассчитанным получателем, после чего делается вывод о норме или не норме целостности и аутентичности отправленных данных.

Идея предлагаемого подхода описана в [3]. И его суть в применении разных блочных симметричных криптоалгоритмов для шифрования разных блоков исходного сообщения в рамках одного из трех режимов работы блочных шифров. Таким образом, в каждом сеансе взаимодействия КАС формируется на основе определенного множества блочных алгоритмов и режима шифрования, которые могут выбираться пользователями из заданного их множества в соответствии с некоторым правилом, остающимся неизвестным для криптоаналитика. В таком случае можно говорить о внутрисеансовой диверсности при вычислении КАС для обеспечения целосности и аутентичности.

В статье описаны: модель обеспечения целостности сообщений на основе диверсного подхода, её программная реализация и анализ временных характеристик работы программного средства.

## 1. Разработка модели

Если изначально представить модель как “черный ящик” (рис. 1), то сразу же видно, чем мы должны оперировать и какого результата достичь. На входе имеем:

– исходный текст сообщения $M$ ;

– секретный ключ $K$ ;

– множество блочных алгоритмов $MA_c$ : 3-way; GOST; BlowFish; DES.

– множество режимов работы $MR$ : CBC; CFB; IGE.

Поскольку существует возможность вычисления КАС с использованием трех разных режимов, то целесообразно рассмотреть применение этих режимов как отдельные подмодели. Структура этих подмоделей изображена на рис. 2 и разработаны они на основе модели, описанной в [3].

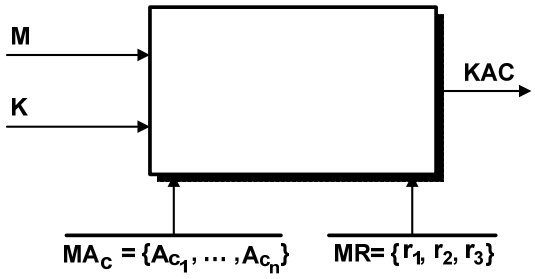


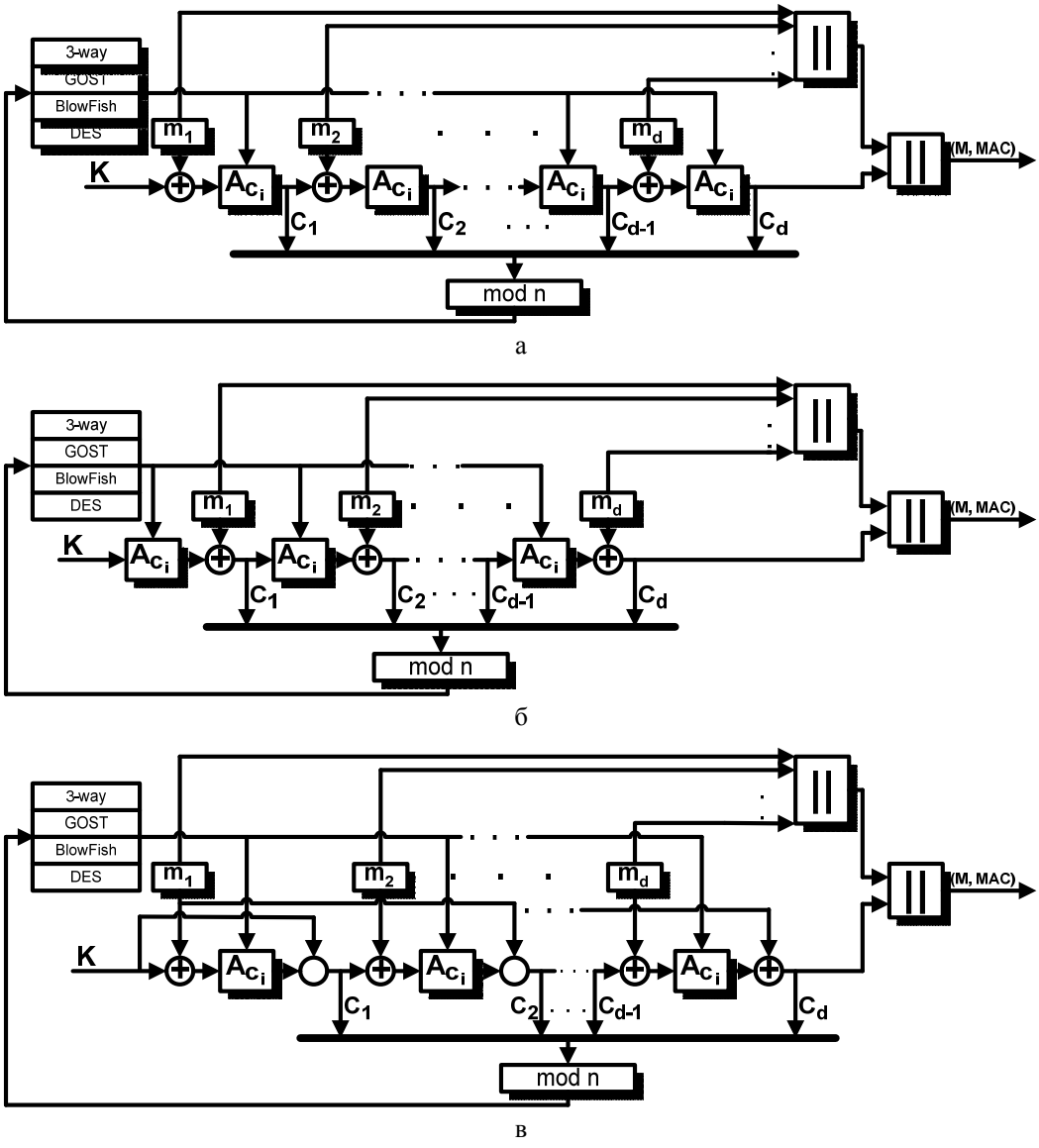

Рис. 1. Модель по принципу "черного ящика"

Особенностью реализации общей модели является то, что в каждой подмодели используются разные режимы и вместо инициализирующего вектора используется ключ. Выбор алгоритма шифрования производится по правилу модулярного преобразования:

$$N_{A_i} = c_i \bmod n,$$

где $N_{A_i}$ – номер алгоритма, которым будет шифроваться следующий блок данных; $c_i$ – текущий блок шифртекста; $n$ – количество используемых блочных шифров.

При объединении всех трех моделей в одну общую структуру получим необходимый результат, иллюстрируемый на рис. 3. На нем показана модель внутрисеансовой диверсности с возможностью смены режима работы блочных шифров в зависимости от ключа.




а

б

в

Рис. 2. Подмодели трех режимов использования БСШ:
а – режим CBC; б – режим CFB; в – режим IGE

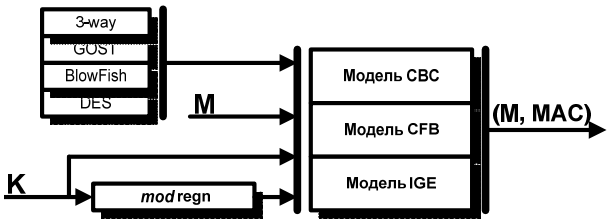



Рис. 3. Общая модель

Правило, по которому устанавливается, какой именно режим работы БСШ используется в данном сеансе, описывается следующим образом:

$$N_R = K \bmod regn ,$$

где $N_R$ – номер режима для данного сеанса; $K$ – секретный ключ для данного сеанса; $regn$ – количество режимов.

## 2. Программная реализация модели

При программной реализации предложенной модели следовало учесть:

– разницу в длине блоков обрабатываемого сообщения, соответствующей длине блока используемого БСШ (для 3-way – длина блока равна 96 битам, а для GOST, BlowFish, DES – 64 битам);

– разные подходы к работе с секретными ключами (их инициализацию и т.п.).

Для решения проблемы разной длины обрабатываемых БСШ блоков был применен подход, основанный на «дроблении» исходного текста на подблоки меньшей длины, как показано на рис. 4. Длина подблока – 32 бита. Таким образом, из подблоков можно сформировать блок любой длины, поскольку длины блоков используемых алгоритмов кратны 32.

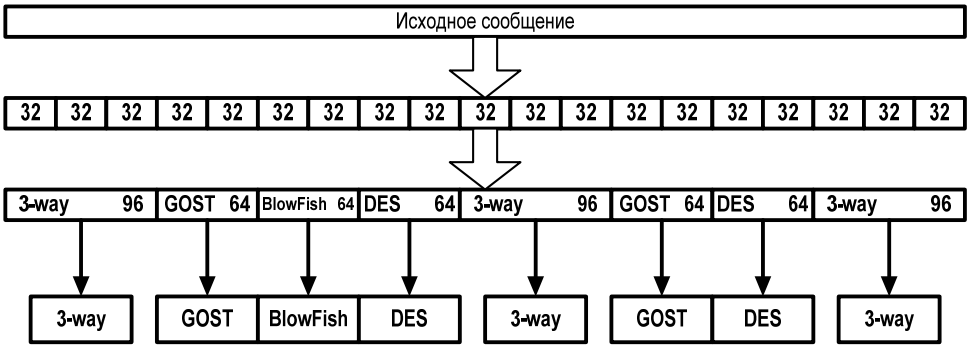



Рис. 4. Дробление исходного сообщения

Поскольку алгоритм с длиной обрабатываемого блока 96 бит всего один, а все остальные имеют длину блока – 64 бита, то целесообразно считать, что КАС будет равен 64 битам. Это связано с тем, что при работе алгоритма КАС формируется в отдельной переменной с длиной в 96 бит и алгоритм 3-way может вообще не участвовать в формировании КАС. И этот факт заставляет исключить старшие 32 бита, поскольку переменная для вычисления КАС инициализируется ключом и это может привести к открытию части секретного ключа. Блочная схема алгоритма результирующей программы показана на рис. 5.

Правило, по которому осуществляется выбор режима работы шифров, можно описать так:

$$keysum = key[0] \oplus key[1] \oplus key[2],$$

$$regnum = keysum \bmod regn,$$

где $key$ – ключевой массив;

$keysum$ – величина, равная сложенным по XOR трем частям ключа $key$;

$regnum$ – вычисляемый порядковый номер режима;

$regn$ – количество задействованных режимов (равное трем).

Режимы реализованы в виде отдельных процедур и имеют схожую структуру. Процедуры циклически выполняют следующий фрагмент псевдокода до полной обработки сообщения:

```
switch (cs){
  case 0:
//шифрование блока данных
//алгоритмом 3-way
//вычисление КАС
//работа режима
// вычисление следующего алгоритма
      break;
  case 1:
//шифрование блока данных
//алгоритмом GOST
//вычисление КАС
//работа режима
// вычисление следующего алгоритма
      break;}
```

В этой программе было реализовано три процедуры:

– CBCreg_ciph – процедура вычисления КАС в режиме CBC;

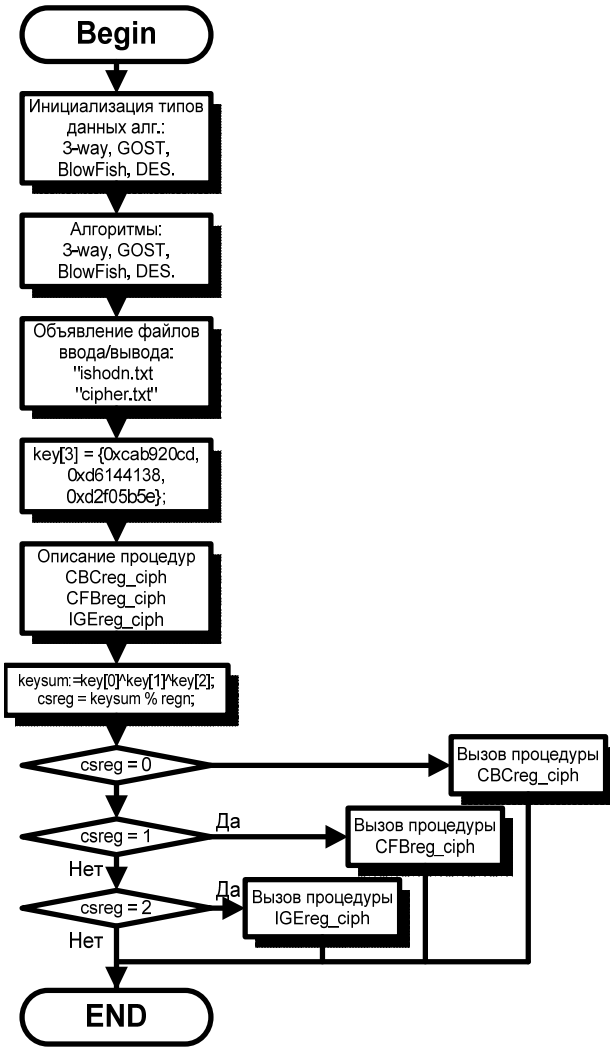



Рис. 5. Блочная схема алгоритма программной реализации

– CFBreg_ciph – процедура вычисления КАС в режиме CFB;

– IGEreg_ciph – процедура вычисления КАС в режиме IGE.

В зависимости от regnum и keysum производится вызов соответствующей процедуры для формирования КАС с программной реализацией режимов CBC, CFB и IGE.

## 3. Анализ быстродействия программной реализации модели

Рассмотрим временные характеристики каждого алгоритма по отдельности (табл. 1). Для этого в ходе проводимого эксперимента измерялось время
(в миллисекундах) выполнения той части программного кода, которая отвечает за шифрование и дешифрование данных (без инициализации, вычисления ключей и т.п.). Полученные данные не являются точными, но проанализировать скорость выполнения процесса в программной реализации позволяют.

Таблица 1

Характеристики быстродействия алгоритмов

| Алгоритмы | Число подблоков | | | |
|---|---|---|---|---|
| | 10000 | 25000 | 50000 | 100000 |
| 3-way | 23,52 | 57,4 | 100,34 | 179,32 |
| GOST | 28,44 | 57,2 | 108,68 | 163,02 |
| BlowFish | 30,34 | 64,24 | 109,96 | 173,44 |
| DES | 29,08 | 68,08 | 115,06 | 171,52 |

Из анализа данных видно, что все блочные алгоритмы тратят практически одинаковое количество времени на шифрование. Однако шифры 3-way и GOST всё же более быстродействующие.

Теперь проведем оценку скорости работы реализованного программного средства (табл. 2). Проводилось измерение времени, затрачиваемого на криптопреобразование, отдельно для каждого из трех режимов.

Таблица 2

Характеристики быстродействия разных режимов с диверсионным подходом

| Режимы | Число подблоков | | | |
|---|---|---|---|---|
| | 10000 | 25000 | 50000 | 100000 |
| CBC | 35,5 | 79,5 | 121,7 | 189,5 |
| CFB | 60,4 | 113,8 | 174,2 | 287,1 |
| IGE | 63,6 | 123,3 | 179 | 291,5 |

Из табл. 2 видно, что при шифровании наиболее быстрым является режим CBC – у него самое малое время шифрования. В то же самое время режимы CFG и IGE практически не отличаются друг от друга.

Также заметна тенденция увеличения разницы в быстродействии для режима CBC по сравнению с режимы CFG и IGE при увеличении числа подблоков (объёма данных).

Полученные результаты не связаны с возможными дефектами программной реализации модели, поскольку вычисление последовательности применения алгоритмов в каждом режиме зависит от разных параметров и может быть связано применением более скоростных и более медленных алгоритмов шифрования.

Также это может быть связано с тем, что сами режимы CFB и IGE имеют более сложную структуру по сравнению с режимом CBC.

## Заключение

Отличительной особенностью предлагаемого подхода обеспечения целостности сообщений на основе внутрисеансовой диверсности является то, что код аутентификации сообщения формируется на основе множества алгоритмов и режима шифрования, которые могут выбираться пользователями из заданного их множества в соответствии с некоторым правилом, остающимся неизвестным для криптоаналитика.

На основе этой модели была разработана и описана программа, позволяющая формировать код аутентификации сообщения.

Дальнейшими направлениями работы в этой области являются:

– модификация метода дробления сообщения на подблоки;

– модификация метода работы с ключами;

– более тщательное и более точное измерение времени вычисления КАС и рассмотрение возможной модификации с целью ускорить этот процесс;

– глубокое тестирование программной реализации;

– рассмотрение возможности аппаратной реализации данного подхода.

## Литература

*1. Конеев И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев – СПб.: БХВ – Петербург, 2003. – 752 с.*

*2. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник / Дан Х.К.А. Тилборг – М.: Мир, 2006, – 471 с.*

*3. Лысенко И.В. Модель формирования кода аутентификации сообщения на основе использования внутрисеансовой диверсности / И.В. Лысенко, А.С. Шпак // Системи управління, навігації та зв'язку. – К: ЦНДІ НіУ, 2008. – № 3 (7). – С. 144-147.*

*4. Шнайер Б. Прикладная криптография: протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – М.: Триумф, 2002. – 448 с.*

*Поступила в редакцию 2.02.2009*

**Рецензент:** д-р техн. наук, проф., зав. каф. Инженении программного обеспечения И.Б. Туркин, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

### ПРОГРАМНА РЕАЛІЗАЦІЯ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ПОВІДОМЛЕННЯ ЗА ДОПОМОГОЮ СИМЕТРИЧНИХ КРИПТОПЕРЕТВОРЕНЬ НА ОСНОВІ ВНУТРІШНЬОСЕАНСОВОЇ ДИВЕРСНОСТІ

***О.С. Шпак, І.В. Лисєнко***

Описується підхід до формування кода аутентифікації повідомлення на основі внутрішньосеансової диверсності за допомогою симетричних криптоперетворень. Модель розроблялася за принципом "чорного ящика". Представлені структури підмоделей трьох використовуваних режимів роботи блокових симетричних шифрів (БСШ). Коротко описаний процес програмної реалізації моделі формування коди аутентифікації повідомлення (КАП). Приведені результати дослідження швидкості обробки даних програмною реалізацією моделі.

**Ключові слова***:* диверсність, обчислювальна стійкість, код аутентифікації повідомлень, криптостійкість, модулярне перетворення.

### SOFTWARE IMPLEMENTATION OF MESSAGES INTEGRITY PROVISION MODEL THROUGH SYMMETRIC CRYPTOGRAPHICAL TRANSFORMATION ON THE BASE OF INTRA-SESSION DIVERSITY

***A.S. Shpak, I.V. Lysenko***

An approach to forming of message's authentication code (MAC) based on interior diversity by symmetric cryptographical transformation is described. Model has been developed using a "black box principle". Sub models structures of used working modes of block symmetrical algorithm is represented. Process of software implementation of MAC model is briefly described. Performance results of data processing by software model implementation is outlined.

**Key words***:* diversity, calculation ability, message's authentication code, cryptographically secure, modular transformation.

**Шпак Александр Сергеевич** – аспирант, ассистент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: shpakalexandr@rambler.ru.

**Лысенко Игорь Владимирович** – к.т.н., доцент, доцент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: I.Lisenko@csac.khai.edu.