УДК 004.056.53

**А.С. ГУБКА[1], А.Г. РОЖКОВ[2]**

[1] *Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ»*
[2] *Днепропетровский национальный университет имени Олеся Гончара*

# ОБЕСПЕЧЕНИЕ ЗАЩИТЫ В СИСТЕМАХ ПЕРЕДАЧИ И ОБРАБОТКИ ИНФОРМАЦИИ ПУТЕМ МОДЕРНИЗАЦИИ АЛГОРИТМА ШИФРОВАНИЯ

*В работе проанализированы основные проблемы надежной передачи данных с использованием двусторонних каналов передачи информации. Представлен алгоритм помехоустойчивой передачи информации по открытым каналам связи с использованием решающей обратной связи и элементов криптозащиты. Криптозащита построена на базе симметричного алгоритма шифрования по ГОСТ 28147-89 и обеспечивает дополнительную защиту от перехвата информации при ее пересылке по каналам связи. Приведены расчетные и полученные, в результате работы тестовой системы, характеристики помехоустойчивости каналов передачи информации.*

***Ключевые слова:*** *двусторонняя линия связи, обратная связь, симметричный алгоритм шифрования, криптозащита, помехоустойчивость системы, ключ шифрования.*

## Введение

Проблема надежной передачи сообщений при наличии помех является одной из актуальных в теории и практике телекоммуникаций [1, 2].

В последние годы все возрастающее внимание привлекают к себе телекоммуникационные системы, в которых для повышения помехоустойчивости применяются обратные каналы связи. Часто для этой цели могут быть использованы существующие каналы обратного направления. Так, например, в системах передачи команд управления обычно имеются встречные каналы для передачи данных о выполнении этих команд. Линии связи строятся, как правило, двусторонними, и каналы обоих направлений могут использоваться для взаимного повышения надежности методами обратной связи [3, 4].

Отсюда следует актуальность предлагаемой публикации, в которой рассматривается метод обеспечения защиты информации для телекоммуникационных систем с использованием обратной связи и элементов криптозащиты.

## Постановка задачи исследования

Общепризнанно, что обратная связь позволяет обеспечивать высокую надежность передачи данных по беспроводным и проводным каналам связи. Особо благоприятные результаты получаются в случае относительно малых помех в обратном канале. Существуют системы, в которых один из каналов работает при более высокой мощности передатчика, чем другой, как, например, при связи наземной радиостанции с радиостанцией самолета. Более мощный канал, используемый для обратной связи, может обеспечить высокую надежность передачи по сравнению с каналом с относительно слабыми сигналами.

Помехоустойчивость системы и высокая достоверность приема являются одними из главных критериев качественной связи. В телекоммуникационных системах с обратной связью можно добиться высокого качества связи, применяя относительно простые коды [5].

Однако в настоящее время кроме критерия качества связи актуален критерий защищенности линии связи и/или информации, которая по нему передается. Поскольку в классических двусторонних линиях с обратной связью отсутствует возможность определить перехватывалось ли передаваемое сообщении третьими лицами (злоумышленниками) по пути следования, то в чистом виде эти линии не могут в полной мере удовлетворять реалиям сегодняшнего дня. Единственным методом, который гарантированно может решить эту проблему является криптозащита [6].

Исходя из вышесказанного, предлагается взять за основу существующие методы передачи данных с использованием двусторонних линий с обратной связью и дополнить их модулем криптозащиты.

## Решение поставленной задачи

На основании известных принципов функционирования телекоммуникационных систем составлена функциональная схема модели системы передачи информации с решающей обратной связью и криптозащитой (рис. 1).

© А.С. Губка, А.Г. Рожков

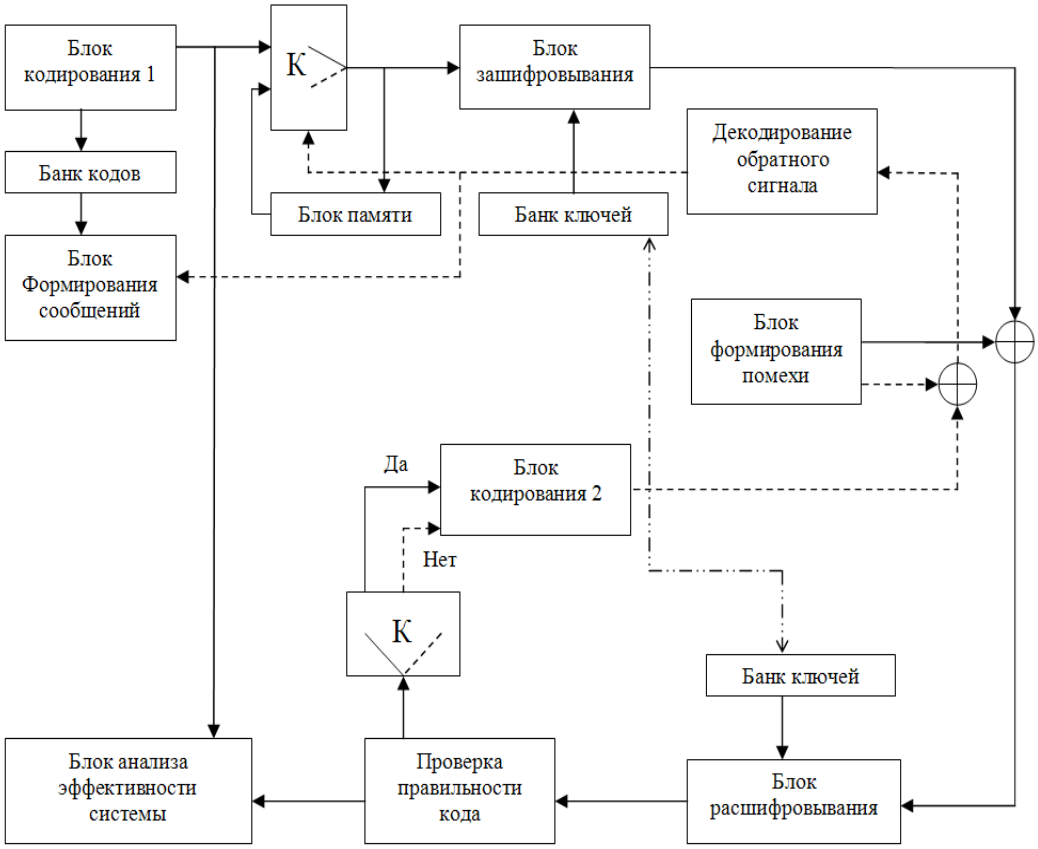


Рис. 1 Функциональная схема модели системы передачи информации с решающей обратной связью и криптозащитой

Блок формирования сообщения составляет из 64 знаков сообщение длиной в 10000 знаков путем простого циклического повтора.

Блок кодирования 1 переводит сообщение в двоичный код. Для этого каждому уникальному знаку из сообщения ставится в соответствие уникальный восьмизначный код. Каждый код состоит из четырех нулей и четырех единиц.

Блок памяти, на основе сигнала от Блока проверки обратного сигнала, передает следующий знак сообщения или повторяет ранее запомненный. Это позволяет повторно передать символ, утраченный при предыдущей передаче.

После этого информация попадает в блок зашифровывания информации, который осуществляет криптозащиту по алгоритму шифрования в соответствии с ГОСТ 28147-89 (ДСТУ ГОСТ 28147:2009) [7, 8].

Выбор в данном исследовании этого алгоритма обусловлен несколькими факторами:

1. Алгоритм не является субъектом патентного права (может свободно использоваться всеми заинтересованными лицами).
2. Хорошо реализуется как программными, так и аппаратными методами.
3. Нетребователен к ресурсам.
4. Уверенно работает с двоичной системой счисления.
5. Достаточно стоек к взломам (ключ длинной 256 бит).
6. Существует вариант реализации без гаммирования и имитовставки.

В качестве альтернативного алгоритма шифрования также может быть использован модернизированный алгоритм шифрования, представленный в работе [9]. Этот алгоритм построен на базе алгоритма по ГОСТ 28147-89, однако имеет существенно лучшую стойкость к взлому за счет дополнительных ветвей алгоритма и увеличенного ключа (512 бит). Его целесообразно использовать для передачи особо важной информации по открытым и закрытым каналам связи.

Банк ключей предназначен для хранения определенного количества ключей шифрования необходимых для работы блоков зашифровывания и расшифровывания. Банки ключей для этих блоков должны быть заранее синхронизированы.

Блок формирования помехи генерирует случайные сигналы с заданной вероятностью появления в них единиц. Это позволяет воссоздать реальное действие искажений типа «белый шум» и «марковские помехи» на передаваемый сигнал.

Канал связи используется для передачи информации в прямом и обратном направлениях. При этом ошибка, сгенерированная в блоке формирования ошибки складывается с передаваемым по каналу сигналом.

Блок расшифровывания, как и блок зашифровывания, построены по алгоритму простой замены алгоритма по ГОСТ 28147-89 [10-12]. Благодаря этому не происходит сбоя при внесении блоком формирования помехи случайных сигналов. Таким образом, блоки криптозащиты не влияют на работу системы двусторонней передачи данных с обратной связью, т.к. вся работа блоков зашифровывания и расшифровывания происходит непосредственно перед передачей уже сформированного блока информации, и перед тем как информация поступит в блок проверки правильности кода соответственно.

Блок проверки правильности кода определяет наличие искажений в принятом сигнале. Если полученный сигнал содержит четыре единицы и четыре нуля – он считается принятым верно. При обнаружении ошибки, на запоминающее устройство подается сигнал о повторной передаче искаженного символа.

Блок декодирования обратного сигнала моделирует обработку обратного сигнала, полученного от блока проверки кода. При этом, при получении сигнала продолжения передачи в блок памяти поступает сигнал о передаче следующего знака. В противном случае генерируется сигнал повторения.

Блок анализа эффективности системы сравнивает исходные данные и данные, пришедшие из блока проверки кода, и позволяет оценить эффективность работы системы с обратной связью при заданной вероятности появления ошибок в канале связи.

Модель системы передачи информации с обратной решающей связью оперирует сообщениями длиной 8 символов. Каждое правильное (разрешенное) сообщение состоит из 4-х нулей и 4-х единиц. Каждому сообщению, передаваемому в прямом направлении, соответствует сообщение в обратном направлении, сигнализирующее о типе следующего сообщения – повтор предыдущего знака или передача следующего. В качестве обратных сообщений используются два сообщения: 11110000 – как сигнал продолжения передачи, 00001111 – как сигнал повторения сообщения.

Подобная организация работы модели позволяет с достаточной точностью воспроизвести процессы, происходящие в реальных системах передачи информации с решающей обратной связью.

Алгоритм компьютерной модели системы передачи информации с решающей обратной связью представлен на рис. 2.

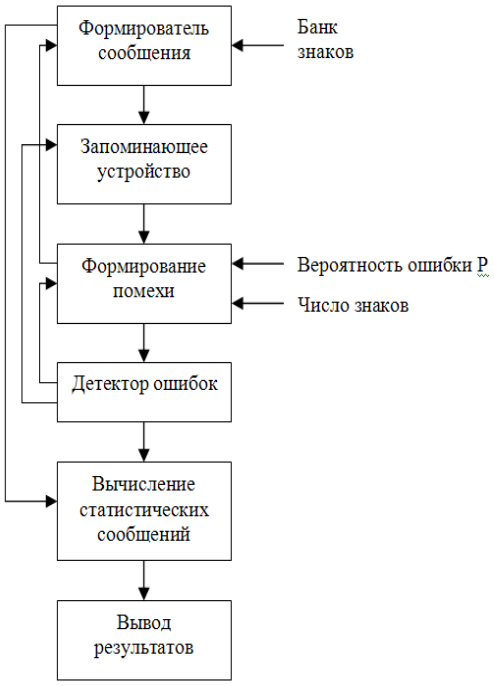


Рис. 2. Алгоритм компьютерной модели

Как известно, существуют системы с ограниченным и неограниченным числом повторений передач. В первом случае, заранее устанавливается максимальное число повторений, при достижении которого передатчик прекращает отвечать на переспрос, а приемник решает, какое из нескольких полученных сообщений считать правильными. Во втором случае, посылка нового сообщения начинается лишь после прекращения всех переспросов.

В рассматриваемой публикации, в целях более рационального использования канала связи, ограничим количество переспросов двумя. Если при этом сообщение так и не было передано без ошибок, последнее из принятых будем считать полученным верно и поэтому оно поступит на выход устройства проверки кода.

Формирователь сообщений на вход получает набор из 10000 знаков от банка знаков. Каждому знаку поставлен в соответствие 8-значный код, состоящий из 4-х нулей и 4-х единиц. Далее выбирается следующий знак и передается на запоминающее устройство.

Запоминающее устройство хранит текущий передаваемый знак.

Моделированием канала связи занимается блок формирования помехи. Для формирования помехи используются два параметра: вероятность возникновения ошибки и тип помехи. Из запоминающего устройства извлекается передаваемый знак, складывается со сформированной помехой и передается в блок детектора ошибки.

Детектор ошибки проверяет полученный знак

на наличие 4-х единиц. В случае обнаружения 4-х единиц знак считается переданным верно и формируется сигнал передачи следующего знака. Если обнаружено отклонение от количества единиц в знаке – формируется сигнал повторной передачи.

Сигнал продолжения (или повтора) поступает на блок формирования помехи для моделирования канала обратной связи. После этого он поступает на формирователь сообщения, где проверяется на корректность: если получен сигнал вида «00001111» - продолжение передачи, если вида «11110000» - повтор текущего.

После окончательного принятия решения о допустимости переданного сообщения, оно поступает на блок вычисления результатов. В этом блоке принятое сообщение сравнивается с исходным, вычисляется количество искаженных символов в знаке, и принимается решение о верности принятого сообщения. На основе этих данных, вычисленных для всех сообщений, строятся статистические характеристики модели при заданных начальных условиях: количество неискаженных символов, количество искаженных знаков, количество неискаженных знаков.

Блок вывода результатов позволяет выводить вычисленные данные на экран.

На основании представленного алгоритма разработано программное обеспечение компьютерной модели с использованием среды разработки приложений Borland Delphi 7.

Входные данные: количество символов в сообщении, которое необходимо передать, вероятность появления одиночного искажения, условные вероятности для марковского шума, количество повторов одного сообщения.

На основании этих данных, проводятся формирования сообщения и искажения сигналов, которые идентичны искажениям в реальном канале связи. Таким образом, формируется блок исходных данных.

Результаты работы компьютерной модели выводятся в виде таблицы: количество искаженных знаков без повторов, количество искаженных знаков с одним повтором и количество искаженных знаков с двумя повторами.

Разработанную компьютерную модель целесообразно использовать для исследования помехоустойчивости системы передачи информации с обратной связью. Это позволяет моделировать процессы, происходящие при передаче сообщений в канале связи с помехами типа «белый» шум и марковскими помехами.

Была проведена проверка работоспособности разработанной компьютерной модели системы передачи информации с обратной связью путем тестирования. Проверка была проведена на двух видах шума: дискретного «белого» шума и шума Маркова.

Используя вероятностную математическую модель [6] рассчитаны статистические характеристики системы передачи информации с обратной связью: вероятность приема искаженного знака и число искаженных знаков в сообщении длиной 10000 знаков (табл. 1).

При тестировании для каждого значения вероятности искажения символа проведено по 10 тестов с числом повторов, равное 0, 1 и 2. Результаты тестирования представлены в табл. 2.

Таблица 1

Расчетные статистические характеристики системы передачи информации с обратной связью

| Вероятность искажения символа, $P_{ош}$ | Вероятность искажения знака, $P_т(и)$ | Число искаженных знаков (из 10000) |
|---|---|---|
| 0,01 | 0,08 | 772 |
| 0,02 | 0,15 | 1492 |
| 0,03 | 0,22 | 2162 |
| 0,04 | 0,28 | 2786 |
| 0,05 | 0,34 | 3365 |

Таблица 2

Характеристики системы передачи информации с обратной связью, полученные при тестировании компьютерной модели

| Вероятность искажения символа, $P_{ош}$ | Число повторов | Вероятность искажения знака, $P_э(и)$ | Число искаженных знаков (из 10000) |
|---|---|---|---|
| 0,01 | 0 | 0,076 | 760 |
| | 1 | 0,006 | 6 |
| | 2 | 0,001 | 1 |
| 0,02 | 0 | 0,139 | 1309 |
| | 1 | 0,028 | 288 |
| | 2 | 0,012 | 124 |
| 0,03 | 0 | 0,206 | 2067 |
| | 1 | 0,065 | 651 |
| | 2 | 0,025 | 259 |
| 0,04 | 0 | 0,263 | 2633 |
| | 1 | 0,088 | 882 |
| | 2 | 0,042 | 427 |
| 0,05 | 0 | 0,332 | 3329 |
| | 1 | 0,117 | 1175 |
| | 2 | 0,072 | 728 |

## Заключение

Как видно из табл. 1 и 2, сравнение расчетных данных и результатов тестирования свидетельствует об их удовлетворительном совпадении. Данные о характеристиках работы алгоритмов шифрования по ГОСТ 28147-89 и модернизированного алгоритма шифрования подробно описаны в работах [9, 10] соответственно.

В заключении отметим что, разработанную компьютерную модель целесообразно применять для моделирования реальных систем передачи информации и исследования помехоустойчивости систем с выбранным типом обратной связи, изменяя, при необходимости, алгоритмы обработки информации с целью улучшения ее помехоустойчивости и учитывая, при этом, технические возможности системы передачи информации с обратной связью.

## Литература


*1. Теория электрической связи [Текст]: учебное пособие / К.К. Васильев, В.А. Глушков, А.В. Дормидонтов, А.Г. Нестеренко; под общ. ред. К.К. Васильева. – Ульяновск: УлГТУ, 2008. – 452 с.*

*2. Игнатов, В.А. Теория информации и передачи сигналов [Электронный ресурс] / В.А. Игнатов – Режим доступа: http://www.info.oglib.ru /bgl/3358.html. – 5.12.2012 г.*

*3. Молчанов, В.Н. Помехоустойчивость и эффективность систем связи [Электронный ресурс]: учеб. пособ. / В.Н. Молчанов – Режим доступа: http://nashaucheba.ru/v13080/?download=file. – 5.12.2012 г.*

*4. Каневский, З.М. Передача сообщений с информационной обратной связью [Текст] / З.М. Каневский. - М: Знание, 1969. – 47 с.*

*5. Помехоустойчивость и эффективность систем передачи информации [Текст] / под ред. А.Г. Зюко. - М: Радио и связь, 1999. – 272 с.*

*6. Дронь, М.М. Основи теорії захисту інформації [Текст]: навч. посіб. / М.М. Дронь, В.П. Малайчук, О.М. Петренко. – Д.: Вид-во Дніпрпетр. ун-ту, 2001. – 312 с.*

*7. Про прийняття міждержавних стандартів як національних методом підтвердження та скасування відповідних міждержавних стандартів: Наказ Державного комітету України з питань технічного регулювання та споживчої політики від 22.12.2008 г. №495 [Электронный ресурс]. – Режим доступа: http://www.licasoft.com.ua/index.php/component/lica/?base=1&id=x000CC641. - 5.12.2012 г.*

*8. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – Введен впервые; введ. 02.06.1989 [Электронный ресурс]. – Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=139177. – 5.12.2012 г.*

*9. Губка, А.С. Модернизация симметричного алгоритма шифрования [Текст] / С.А. Губка, А.С. Губка, Н.Ю. Носова //Радіоелектронні і комп'ютерні системи. – 2011. – № 4 (56). – С. 90-94.*

*10. Панасенко, С.П. Алгоритм шифрования ГОСТ 28147-89 [Электронный ресурс] / С.П. Панасенко. – Режим доступа: http://www.inssl.com/standart-of-cipher.html. – 5.12.2012 г.*

*11. Казарин, О.В. Безопасность программного обеспечения компьютерных систем [Текст] / О.В. Казарин. – М.: МГУЛ, 2003. – 212 с.*

*12. Основы криптографии [Текст] / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. – М.: Гелиос АРВ, 2001. – 479 с.*


*Поступила в редакцию: 05.12.2012*

**Рецензент:** д-р техн. наук, проф., заведующий кафедрой "Информационные управляющие системы" О. Е. Федорович, Национальный аэрокосмический университет им. Н.Е. Жуковского «Харьковский авиационный институт», Харьков.

### ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ В СИСТЕМАХ ПЕРЕДАЧІ І ОБРОБКИ ІНФОРМАЦІЇ ШЛЯХОМ МОДЕРНІЗАЦІЇ АЛГОРИТМА ШИФРУВАННЯ

***О.С. Губка, О.Г. Рожков***

В роботі розглянуті основні проблеми надійної передачі даних з використанням двосторонніх каналів передачі інформації. Представлено алгоритм перешкодостійкої передачі інформації по відкритих каналах зв'язку з використанням рішаючого зворотнього зв'язку та елементів криптозахисту. Криптозахист побудовано на базі симетричного алгоритму шифрування за ГОСТ 28147-89 і забезпечує додатковий захист від перехоплення інформації при її пересиланні по каналах зв'язку. Наведено розрахункові та отримані, в результаті роботи тестової системи, характеристики завадостійкості каналів передачі інформації.

**Ключові слова:** двостороння лінія зв'язку, зворотний зв'язок, симетричний алгоритм шифрування, криптозахист, завадостійкість системи, ключ шифрування

### PROTECTION IN THE TRANSMISSION AND TREATMENT INFORMATION BY UPGRADING THE ENCRYPTION ALGORITHM

***A.S. Gubka, A.G. Roghkov***

The paper discusses the main challenges reliable data transfer through bilateral channels of communication. The algorithm for noise immune data transmission through open communication channels with the use of critical feedback and cryptographic elements. Encryption is based on the symmetric encryption algorithm GOST 28147-89 and provides additional protection from eavesdropping when they sent across communication channels. The calculated and the resulting characteristics of the test system noise communication channels.

**Keywords:** two-way communication link, feedback, symmetric encryption algorithm, encryption, immunity system, the encryption key

**Губка Алексей Сергеевич** – канд. техн. наук, доцент, доцент кафедры "Информационные управляющие системы", Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина, e-mail: gubka@gala.net.

**Рожков Алексей Геннадиевич** – студент физико-технического факультета, Днепропетровский национальный университет им. О. Гончара, Днепропетровск, Украина, e-mail: agroghkov@gmail.com.