УДК 004.056

К.В. АГИЕВЕЦ[2], М.А. ИВАНОВ[1, 2],
М.А. КОНДАХЧАН[2], А.В. СТАРИКОВСКИЙ[1]
[1]*Государственный университет управления», Москва*
[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

АЛГОРИТМИЧЕСКОЕ МЫШЛЕНИЕ В ЗАДАЧЕ НАДЕЖНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛУ СВЯЗИ

Рассматривается пример использования алгоритмического мышления, эвристических приемов разрешения технических противоречий и метода контрольных вопросов при решении задачи защиты информации, пересылаемой по каналу связи.

При передаче данных по каналам связи приходится решать три задачи: обнаружение и исправление ошибок, вызванных действием помех в каналах связи (обеспечение помехозащищенности); обеспечение секретности информации; защиту от навязывания ложных данных (имитозащиту).

Традиционно каждая из этих задач решается на основе использования отдельного механизма – соответственно помехоустойчивого кодирования, шифрования, формирования (на стороне отправителя) и проверки (на стороне получателя) контрольного кода целостности (имитовставки). В результате реальные системы передачи данных громоздкие и недостаточно эффективные.

Итак, у нас имеется *изобретательская задача*: необходимо найти единое техническое решение, обеспечивающее защиту от случайных искажений информации в канале связи с помехами; секретность информации; защиту от умышленных искажений информации (имитозащиту).

Применим *алгоритмическое мышление*, а также воспользуемся *эвристическими приемами* разрешения технических противоречий и *методом контрольных вопросов* [1]. Сформулируем *идеальный конечный результат*: требуется код, который решает все три упомянутые выше задачи защиты информации и при этом обеспечивает наперед заданную вероятность правильного приема информации при решении первой задачи.

Используем *посредника*, создадим виртуальный (преобразованный) канал связи с нужными нам свойствами, когда все вектора ошибок на выходе преобразованного канала связи будут равновероятны. Таким образом, на выходе реального канала связи нужен блок преобразования R (Random), на входе которого будет реальный вектор ошибок e, а на выходе – будет сформирован преобразованный вектор ошибок e' с вышеупомянутыми свойствами. В криптографии есть термин, близкий к термину вектор ошибок, а именно дифференциал (или разница) двух двоичных строк. Криптографические преобразования обладают свойством непредсказуемости, которое означает, что при любом входном дифференциале все выходные дифференциалы равновероятны. По этой причине блок R логично назвать блоком стохастического (т.е. непредсказуемого) преобразования.

Применим принцип *предварительного антидействия* и получим схему, показанную на рис. 1. Как показано на рис. 1, преобразованный дискретный канал работает не с битами, а с L-разрядными двоичными наборами данных. Если эти наборы назвать Q-ичными символами, принимающими значения от 0 до $2^L - 1$, полученный преобразованный дискретный канал с учетом свойств блока R^{-1}, можно с полным основанием назвать Q-ичным симметричным каналом. В случае ошибки каждый из $(2^L - 1)$ ненулевых векторов ошибки появляется на его выходе с вероятностью $p/(2^L - 1)$, где p – вероятность ошибки в канале связи.

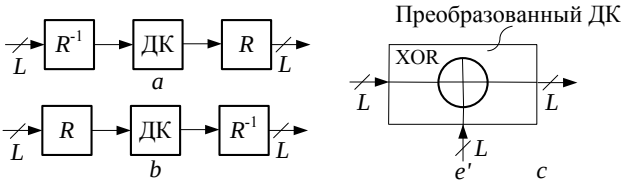

Рис. 1. Преобразованный дискретный канал: *a* – первоначальная схема; *b* – окончательная схема, предложенная автором стохастического кода [2]; *c* – преобразованный ДК, действия помех в котором, т.е. искажение Q-ичных символов, задается преобразованным вектором ошибок e'. ДК – реальный дискретный канал

Список литературы

1. Иванов М.А. Алгоритмическое мышление в задачах защиты информации. − Настоящий сборник.

2. Осмоловский С.А. Стохастические методы защиты информации. – М.: Радио и связь, 2003.