О.О. Борисенко *(Сумський державний університет, Україна)*
О.Є. Горячев *(Сумський державний університет, Україна)*

ЗАВАДОСТІЙКА ПЕРЕДАЧА ЕКОНОМІЧНОЇ ІНФОРМАЦІЇ НА БАЗІ ПЕРЕСТАНОВОК

У статті запропоновано метод підвищення завадостійкості економічної інформації за допомогою коду на перестановках. Застосування даного методу дозволяє підвищити ефективність роботи економічних систем. Розглянуто методи кодування і декодування економічної інформації, яка передається перестановками, а також методи виявлення й виправлення помилок у них.

Ключові слова: *економічна інформація, економічні системи, завадостійка передача даних, перестановки, факторіальні числа, знаходження і виправлення помилок, алгоритми.*
Рис. 1. Літ. 11.

А.А. Борисенко *(Сумской государственный университет, Украина)*
А.Е. Горячев *(Сумской государственный университет, Украина)*

ПОМЕХОУСТОЙЧИВАЯ ПЕРЕДАЧА ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ НА ОСНОВЕ ПЕРЕСТАНОВОК

В статье предложен метод повышения помехоустойчивости экономической информации с помощью кода на перестановках при ее передаче и хранении. Применение данного метода позволяет повысить эффективность работы экономических систем. Рассмотрены методы кодирования и декодирования передаваемой экономической информации с помощью перестановок, а также методы обнаружения и исправления ошибок в них.

Ключевые слова: *экономическая информация, экономические системы, помехоустойчивая передача данных, перестановки, факториальные числа, обнаружение и исправление ошибок, алгоритмы.*

O.O. Borysenko *(Sumy State University, Ukraine)*
O.E. Goryachev *(Sumy State University, Ukraine)*

NOISE-RESISTANT TRANSFER OF ECONOMIC INFORMATION BASING ON PERMUTATIONS

The article suggests a method for increasing the noise-resistance of economic information by means of code on permutations at transfer of this information and its storage. Application of this method enables increasing the efficiency of economic systems' performance. Methods of coding and decoding of the transferred economic information by means of permutations are considered as well as the methods of errors detection and correction in them.

Keywords: *economic information; economic systems; noise-resistant transfer of data; permutations; factorial numbers; errors detection and error corrections; algorithms.*

Постановка проблемы. Сегодня, когда экономические системы, образуемые организованной совокупностью хозяйственных отношений и связей на производстве, все шире внедряются во все сферы деятельности человека, как никогда ранее стоит вопрос о повышении эффективности их работы. Во многом этот вопрос решается применением современных информационных технологий в системах управления, автоматизированного проектирования, конторах, банках и т.д., которые немыслимы без систем передачи и хранения информации, в том числе и экономической [7].

Однако такие системы не всегда могут правильно функционировать, так как при передаче информации по каналам связи и ее хранении, вследствие различного вида помех, в том числе вызванных и человеческим фактором, часто возникают ошибки. В результате данные не могут быть эффективно использованы принимающей стороной для дальнейшей обработки. Экономический ущерб от таких ошибок трудно поддается учету, но несомненно, он достаточно большой. Его уменьшение достигается разными методами, одним из которых, широко используемым на практике, является метод защиты информации с помощью помехоустойчивого кодирования [5–8; 10].

Анализ последних исследований и публикаций. Защита информации от помех проводится или за счет использования содержащейся в ней естественной избыточности, или за счет внешне вводимой искусственной избыточности. Естественная избыточность широко используется для выявления и исправления ошибок в устной и письменной речи, однако для защиты экономической информации ее количество в соответствующих документах явно недостаточное. Поэтому во многих случаях необходимо в эти документы вводить еще и искусственную избыточность.

Основным способом получения искусственной избыточности на практике является помехоустойчивое кодирование с помощью специальных помехоустойчивых кодов – разделимых и неразделимых. В разделимых кодах передаваемые кодовые слова (сообщения) содержат информационные разряды и к ним искусственно добавляются контрольные разряды, а в неразделимых кодах такого разделения нет – в них все разряды являются информационными. Однако эти коды все же неявно содержат в себе искусственную избыточность, вводимую, как правило, путем преобразования исходных сообщений в неразделимые кодовые слова.

Так, разделимым кодом будет часто применяемый в бухгалтерской практике код, получаемый на основе метода контрольных сумм, когда к массиву элементов прикрепляется их сумма, являющейся контрольной [6; 8]. На приемном конце, после передачи, она сравнивается с суммой, полученной в результате суммирования элементов в переданном массиве, и при несовпадении значений переданной и вычисленной контрольных сумм считается, что при передаче массива появилась ошибка, которая могла произойти то ли в массиве, то ли в контрольной сумме. Затем происходит переспрос массива и его контрольной суммы и производится ее новое сравнение с предварительно вычисленной суммой элементов массива после его получения. Так происходит несколько раз, до тех пор, пока не наступит положительный результат или не будет принято решение о прекращении передачи информации.

Метод контрольных сумм, в силу своей алгоритмической простоты, доказал свою эффективность при передаче экономической информации, однако он требует для своей реализации относительно большого времени, так как при его применении необходимо производить суммирование всех элементов передаваемого массива как перед его передачей, так и после его приема. Кроме того, он в простейшем варианте не способен исправлять ошибки без переспроса всех элементов массива и контрольной суммы, а это требует дополнительного времени. Если же канал связи слишком шумит, то переспросов мо-

жет быть много, и тогда время передачи снизится, вплоть до полной остановки процесса передачи информации.

Среди других разделимых кодов хорошим уровнем помехоустойчивости в настоящее время обладают циклические коды, которые способны во многих случаях не только обнаруживать, но и исправлять ошибки, причем многократные [5; 6; 8; 10]. Среди них простейшими будут коды с проверкой на четность, но они только обнаруживают ошибки. Все эти коды эффективно решают задачу обнаружения ошибок на аппаратном уровне и трудно реализуются программно. Поэтому в экономических системах их используют редко, предпочитая коды на основе методов типа контрольных сумм.

Общим недостатком разделимых кодов является то, что их кодовые комбинации обычно формируются относительно небольшой длины, так как для ее увеличения требуется увеличивать сложность алгоритмов кодирования и декодирования, что снижает скорость их работы и увеличивает емкость требуемой для них памяти. Но малая длина кодовых слов приводит к тому, что относительное количество контрольных разрядов по отношению к информационным разрядам увеличивается, таким образом скорость передачи информации уменьшается.

Неразделимые коды, обладающие теми или иными свойствами, позволяющими обнаруживать, а в ряде случаев и исправлять ошибки в кодовых словах без переспроса, менее распространены на практике, чем разделимые, в силу необходимости преобразования исходных массивов информации в массивы неразделимых кодов, что представляет определенную трудность. Однако если задача преобразования успешно решена, то в преобразованных массивах появляется ряд полезных и интересных свойств, которые позволяют говорить об их преимуществах по сравнению с другими способами кодирования для экономических систем. Прежде всего – это простота обнаружения и исправления ошибок, хорошая помехоустойчивость, возможность увеличения скорости передачи информации за счет передачи массивов данных большой длины.

На практике в экономических системах широкое распространение нашел такой неразделимый код, как равновесный, который активно используется в различных информационных экономических системах и не только для защиты от помех, а и для сжатия информации [1; 5; 10]. Достоинством равновесных кодов является простота обнаружения в них ошибок. Для этого требуется лишь подсчитать число содержащихся в равновесных кодах единиц, которое для любых кодовых комбинаций постоянно. Если оно равно требуемому числу, то ошибки нет, в противном случае ошибка имеется. Однако этот код предназначен для массивов, состоящих из единиц и нулей, и, кроме того, не решает задачу исправления ошибок.

Недостаток неразделимых кодов (необходимость преобразования сообщений из исходного кода в помехоустойчивый неразделимый код), в ряде случаев может рассматриваться как его достоинство, так как он защищает исходную информацию от нежелательного внешнего вмешательства. Причем эффект такой защиты, при соответствующем кодировании, может быть не меньшим, чем в используемых в настоящее время шифрах для защиты информа-

ции от несанкционированного доступа. Однако здесь, наряду с эффектом защиты от постороннего несанкционированного вмешательства, будет наблюдаться и эффект защиты от помех, что выгодно отличает неразделимые коды от разделимых кодов.

Нерешённые части проблемы. Существующие методы защиты от помех в целом пока что достаточно эффективно справляются с задачей обнаружения и исправления ошибок, в том числе и при передаче экономической информации. Однако повышение её объёмов и скоростей передачи, а также рост требований, предъявляемых к помехоустойчивости (вероятности обнаружения и исправления ошибок в сообщениях) в системах передачи данных, вызывает необходимость в разработке новых и усовершенствовании существующих методов защиты экономических информации от помех, которая обладает определенной спецификой. Она состоит в том, что передающие ее массивы данных обладают повышенной длиной, имеют специфическую структуру, например, для бухгалтерской отчетности, и требуют, в силу их большого объема, повышенной скорости передачи.

Целью исследования является задача поиска эффективного метода защиты экономической информации, который бы, с одной стороны, не снижал значительно скорость передачи информации, а с другой – в достаточной мере защищал её от помех.

Основные результаты исследования. ***Обнаружение ошибок.*** В данном исследовании для помехоустойчивого кодирования экономической информации предлагается рассмотреть более сильный в плане помехоустойчивости код, чем известные неразделимые коды, в котором сообщения представляются перестановками.

Перестановкой называется любая кодовая последовательность, состоящая из n различных элементов, в которой ни один элемент не повторяется. Хотя существуют перестановки и с повторениями, но в данной работе такие объекты не рассматриваются. Например, рассматриваемыми перестановками без повторений из трех элементов будут перестановки 123, 132, 213, 231, 312, 321. Их число в общем виде определяется как $n!$, где n – длина (число элементов) перестановки. Очевидно, что чем больше длина перестановок n, тем более эффективным будет основанный на них помехоустойчивый код с точки зрения уровня его помехоустойчивости. Этот результат для наглядности показан на рис. 1, в котором доля обнаруживаемых ошибок $Z = 1 - n! / n^n$ меняется от величины 0,5, при двух элементах перестановки, до величины близкой к 1 [2; 4].

К одному из достоинств помехоустойчивого кода на перестановках относится отсутствие в нем необходимости передачи контрольной суммы, так как в нем контрольная сумма всегда одна и та же – n x $(N + 1) / 2$. Значит, нет необходимости вычислять контрольную сумму в массиве и после приема информации, что экономит время кодирования передаваемых массивов данных и сокращает их длину. Хотя сам метод обнаружения ошибок в коде на перестановках аналогичен способу их обнаружения в методе контрольных сумм, после приема массива вычисляется сумма содержащихся в нем элементов, и

результат вычисления сравнивается с контрольной суммой. Несовпадение суммы элементов массива с контрольной суммой является признаком ошибки. В рассмотренном ранее примере контрольная сумма всегда равна числу 6. Если придет сообщение из 3 элементов (113 вместо 213), то контрольное число, после подсчета суммы элементов, для него примет значение 5, значит при передаче данного сообщения произошла ошибка.

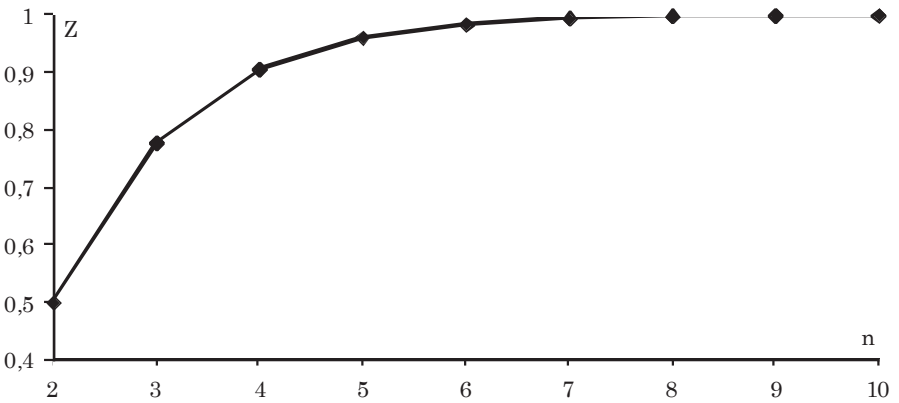

Рис. 1. **Зависимость вероятности обнаружения ошибочной комбинации** *Z* **от длины перестановки** *n*, *авторская разработка*

Правда, возможен случай, что происходит не одна ошибка, а две и более. Тогда возможно, что одна ошибка покрывает другую и обнаружение ошибки не произойдет. Так, если в предыдущем примере вместо сообщения 213 придет сообщение 123 с двойной ошибкой, когда первый элемент 2 перешел в 1, а второй с 1 в 2, то ошибка контрольной суммой не будет замечена и сообщение воспримется как правильное.

Свойство сообщений, представляемых в виде перестановок, состоящее в том, что ни один из их элементов не повторяется, является другим важным их достоинством, отличающим их от свойств сообщений, используемых в обычном методе контрольных сумм, где такого ограничения нет. Наличие данного свойства позволяет ошибку в конкретном элементе перестановки найти путем последовательного сравнения этого элемента со всеми оставшимися ее элементами. Если хотя бы при одном сравнении элементов будет обнаружено их равенство, то это уже будет признак ошибки. Такой способ обнаружения ошибок в перестановках будет более эффективным по сравнению со способом обнаружения ошибок в методе контрольных сумм, так как он указывает элементы перестановки, которые подверглись искажениям, а не просто то, что в передаваемом массиве элементов где-то произошла ошибка. Эта информация затем более эффективно может быть использована для обнаружения и исправления ошибок.

Исправление ошибок. Исправление ошибки – это необходимый этап после ее обнаружения. Если на ошибку нет никакой реакции, то нет смысла ее и обнаруживать. Поэтому всегда нужно говорить об обнаружении и исправлении ошибок. Существует 3 возможных реакции на ошибку:

1. Сообщение с ошибкой не воспринимается вообще и пропускается приемником. Например, такое может быть при статистических испытаниях, где результаты опытов усредняются.

2. Ошибку можно исправить путем повторной передачи исходного сообщения в виде перестановки и если, например, в ее результате придет перестановка 213, то можно считать, что она и будет представлять правильное сообщение, правда, в предположении, что во время повторной передачи не произошла двойная ошибка.

3. Передача сообщений с исправлением ошибок. Ошибка исправляется на приемной стороне с помощью помехоустойчивого кода, исправляющего ошибки.

Каждая из этих реакций имеет свои сильные и слабые стороны. Первая из них – пропуск сообщения – возможна в случае невысокой ценности передаваемой этим сообщением информации. Однако она сопровождается потерей информации. Вторая – повтор сообщений, хотя и достаточно прост в реализации, но требует дополнительного времени передачи и в ряде случаев довольно значительного. Третья – исправление ошибок на приемной стороне, нуждается в помехоустойчивых кодах с повышенной избыточностью, что приводит к усложнению алгоритмов кодирования и декодирования и соответственно требует увеличения минимально необходимой емкости памяти.

Для повтора сообщений в перестановках достаточно несовпадения вычисленной суммы на приемном конце с контрольной суммой. Сложнее обстоит дело с методом, при котором происходит сравнение элементов перестановок, так как там надо организовывать сравнение каждого их элемента с остальными. Но зато для исправления ошибки достаточно повторить не весь массив элементов перестановки, как это имеет место в методе контрольных сумм, а только совпадающие по значению элементы. Очевидно, что время передачи сообщения, содержащего, например, два элемента перестановки будет значительно меньше, чем время передачи всех элементов перестановки. Правда, время анализа перестановки на предмет ошибки при этом увеличится, особенно с ростом длины перестановки n. Но этот анализ происходит после получения сообщения на приемной стороне, и поэтому он не влияет на увеличение времени повторной передачи. Ведь вместо массива из n элементов повторно передается всего два элемента.

Исправить ошибку в одном элементе перестановки на приемном конце без повторной передачи достаточно легко. Для этого следует ввести над каждым элементом перестановки дополнительное кодирование, которое будет подсказывать, какой элемент перестановки искажен. Тогда исправление будет состоять в вычитании из общей известной суммы элементов перестановки суммы правильных элементов [4]. В результате будет получено правильное значение искаженного элемента. Существенным в данном методе исправления будет то, что при большой длине перестановок, например, состоящих из 124 элементов будет исправляться не одна двоичная ошибка, а целый их пакет. Для примера, в перестановке из 124 элементов можно исправить максимум 5 двоичных ошибок, так как каждый элемент перестановки будет состоять из 5 бит. И чем больше будет длина перестановки, тем больше будет длина пакета

исправляемых двоичных ошибок, которая увеличивается логарифмически в зависимости от длины перестановок.

Таким образом, код на перестановках, который является эффективным по быстродействию и помехоустойчивости, обладает структурной избыточностью и не требует формирования контрольных сумм. Дополнительная избыточность, введенная в каждый элемент перестановки, позволяет обнаруживать и исправлять большинство ошибок даже при высокой вероятности искажения передаваемых данных. Структура перестановок позволяет выявлять в них отдельные элементы, содержащие ошибки, и осуществлять для их исправления повторную передачу только этих элементов. Эффективность применения перестановок при передаче информации возрастает с увеличением их длины в связи с увеличением количества передаваемых ими информации и вероятности обнаружения ошибок.

Кодирование и декодирование данных на основе перестановок. Однако при использовании перестановок в качестве помехоустойчивого кода необходимо передаваемые данные преобразовывать в перестановки и далее, после их передачи и исправления ошибок осуществить обратное преобразование перестановок в исходные данные. Эти процедуры как раз и представляют главную трудность при использовании перестановок в качестве помехоустойчивого кода. Существующие методы получения перестановок большой длины достаточно сложны для их эффективной практической реализации [9]. Одним из наиболее простых путей, выбранных авторами для преобразования передаваемых данных в перестановки, будет использование факториальной системы счисления [2; 11]. Однако это тема отдельной работы.

Выводы. Рассмотренный метод помехоустойчивого кодирования на основе перестановок позволяет эффективно обнаруживать и исправлять ошибки, возникающие при передаче экономической информации.

Предложенные алгоритмы обнаружения ошибок в перестановках не требуют введения дополнительных проверочных разрядов и обеспечивают их большую длину.

Алгоритмы исправления ошибок могут использовать в своей работе как различные виды переспроса, так и дополнительные проверочные разряды в каждом элементе перестановок.

Кодирование и декодирование передаваемых данных перестановками наиболее эффективно осуществлять на основе использования факториальных чисел как промежуточного шага при переходе от информации, представленной в виде двоичных сообщений, к перестановкам и обратно.

1. *Борисенко А.А., Бережная О.В.* О моделях помехоустойчивых каналов связи // Вісник Сумського державного університету.– Серія: Технічні науки.– 2005.– №9. – С. 5–12.

2. *Борисенко А.А., Горячев А.Е., Онанченко Е.Л.* Обнаружение и исправление ошибок в перестановках // Міжнародна науково-практична конференція «Інформаційні технології та комп'ютерна інженерія». – Вінниця: ВНТУ, 2010. – С. 348–349.

3. *Борисенко О.А., Кулик І.А., Горячев О.Є.* Електронна система генерації перестановок на базі факторіальних чисел // Вісник Сумського державного університету.– Серія: Технічні науки.– 2007.– №1. – С. 183–188.

4. *Горячев А.Е.* Обнаружение ошибок в перестановках // Вісник Сумського державного університету.– Серія: Технічні науки.– 2009.– №3. – С. 169–174.

5. *Кузьмин И.В., Кедрус В.А.* Основы теории информации и кодирования. – К.: Вища школа, Головное изд-во, 1977. – 280 с.

6. *Кушнір О.І., Тимочко О.І., Сєвєрінов О.В.* Аналіз методів завадостійкого кодування у цифрових системах зв'язку // Системи обробки інформації.– 2007.– №9. – С. 63–65.

7. *Мандрыкин А.В., Непышневский А.В.* Информационные технологии в экономике: Учеб. пособие. – Воронеж: ВГТУ, 2008. – 235 с.

8. *Олифер В.Г., Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов. – 4-ое изд. – СПб.: Питер, 2010. – 944 с.

9. *Рейнгольд Э., Нивергельт Ю., Део Н.* Комбинаторные алгоритмы: теория и практика. – М.: Мир, 1980. – 477 с.

10. *Цимбал В.П.* Теория информации и кодирования. – К.: Вища школа, 1992. – 263 с.

11. *Borisenko, A.A., Kalashnikov, V.V., Kulik, I.A., Goryachev, A.E.* (2008). Generation of Permutations Based Upon Factorial Numbers. Intelligent Systems Design and Applications. Eighth International Conference on Intelligent Systems Design and Applications (Kaohiung, Taiwan, 2008), 3: 57–61.

Стаття надійшла до редакції 21.09.2013.

КНИЖКОВИЙ СВІТ

Менеджмент: Підручник / За заг. ред. д.е.н., проф. М.М. Єрмошенка. – К.: Національна академія управління, 2011. – 656 с. Ціна без доставки – 130 грн.

Авторський колектив: **М.М. Єрмошенко, С.А. Єрохін, М.П. Денисенко, О.А. Кириченко, О.І. Соскін.**

Має гриф підручника від МОН України.

У даному підручнику викладено матеріал, який дає системне уявлення щодо менеджменту. Комплекс представлених навчальних матеріалів стосується відносин управління на макро- та мікрорівні економічної системи, що дозволяє сформувати сутнісне бачення щодо менеджмент-взаємозв'язків різноманітних видів діяльності. У цілому викладений матеріал суттєво поширює теоретичні і методичні уявлення щодо менеджменту.

Підручнник включає теоретичні засади менеджменту, історію його виникнення і розвитку, форми і методи документообороту при здійсненні управлінської діяльності, основи операційного менеджменту, розкриває нові тенденції у розвиткові стратегічного менеджменту. Містить також менеджмент-практикум щодо основних засад управління.

Призначений для студентів вищих навчальних закладів, викладачів, аспірантів, а також всіх тих, хто цікавиться питаннями управління.