УДК 004.93
***Виктория КОНДРАТЬЕВА***
ab011089kvf@gmail.com
ORCID: 0000-0003-3033-8515
***Дмитрий ЧАЙКА***
г. Николаев

# КОДИРОВАНИЕ ДЛЯ ЗАЩИТЫ ОТ ИСКАЖЕНИЙ ПРИ ПЕРЕСЫЛКЕ С ПРИМЕНЕНИЕМ СОЧИТАТЕЛЬНОЙ И ПЕРЕСТАНОВОЧНОЙ СИСТЕМ КОДИРОВАНИЯ

*Предлагаемый метод кодирования заключается в том что применяется в коде фиксированное количество единиц например 4 или 6 в заключении от длины слова 16, 32 или 64 бита. Любое число десятичное или двоичное с нерешенным количеством единиц можно перекодировать в двоично-перестановочное с фиксированным количеством единиц, тогда если пропадет или появится любое количество единиц это будет обнаружено, переспрошено и исправлено.*
*Ключевые слова: кодирование, искажение, пересылка информации, система.*

**Постановка проблемы.** В эпоху бурного развития технологий, проблемы информационной защиты встают наиболее остро. Использование автоматизированных систем обработки информации и управления обострило защиту информации, от несанкционированного доступа. Основные проблемы защиты информации в компьютерных системах возникают из-за того, что информация не является жёстко связанной с носителем. Её можно легко и быстро скопировать и передать по каналам связи. Информационная система подвержена как внешним, так и внутренним угрозам со стороны нарушителей.

Решение проблем защиты электронной информации базируется в основном на использовании криптографических методов. Притом современные методы криптографического преобразования сохраняют исходную производительность автоматизированной системы, что является немаловажным. Это является наиболее эффективным способом, обеспечивающим конфиденциальность данных, их целостность и подлинность. Использование криптографических методов в совокупности с техническими и организационными мероприятиями обеспечивают надежную защиту от широкого спектра угроз.

**Анализ последних исследований и публикаций.** Информационную безопасность в системах образования следует рассматривать в контексте общих вопросов безопасности информационных систем с опорой на соответствующие законодательные акты. Проблемы комплексной защиты информационных систем активно прорабатываются зарубежными и отечественными специалистами [4]. К вопросам информационной безопасности систем открытого образования относятся исследования безопасности личности в сети Интернет, в частности, защита от разнообразных технологий мошенничества и защита от материалов, которые нежелательны с точки зрения общественной морали и нормального развития человека. Исследователи анализируют процесс развития новых информационных технологий и считают, что наступило время контролируемого приспособления коммуникативной реальности к образовательной практике [5]. Первоочередное внимание уделяется информационной безопасности в общеобразовательных учебных заведениях на основе внедрения комплекса технических, административных и воспитательных мероприятий и предлагается функциональная модель обеспечения информационной безопасности старшеклассника в компьютерно ориентированной учебной среде [6]. Обращается внимание на необходимость формирования компетентности в области информационной безопасности. Большое значение уделяется проблемам борьбы и сотрудничества в информационной сфере [7], которые, на наш взгляд, распространяются и на сферу образовательных услуг, и на научные исследования. Проблемы информационной безопасности дистанционного взаимодействия субъектов учебного процесса рассматриваются и в контексте психологической безопасности личности [8]. В специальных трудах по исследованию информационной безопасности в системе непрерывного образования [9] очерчены вопросы несанкционированного доступа к учебным

ресурсам и персональным данным участников учебного процесса, проблемы защиты учебных ресурсов и программного обеспечения от повреждений, проблемы обеспечения надежности функционирования информационных систем учебного назначения, подчеркивается необходимость системного подхода к защите информации.

**Результаты, предложения.** Традиционно для защиты от искажений при пересылке нформациии применяется контрольная сумма проверки на четкость, в случае если потерялась одна единица или появилась вместо нуля то такое искажение обнаруживается, а если два то не обнаруживается. Применяется для надежности повторение по нескольку раз или переспрос.

Предлагаемый метод заключается в том что применяется в коде фиксированное количество единиц например 4 или 6 в заключении от длины слова 16, 32 или 64 бита. Любое число десятичное или двоичное с нерешенным количеством единиц можно перекодировать в двоично-перестановочное с фиксированным количеством единиц, тогда если пропадет или появится любое количество единиц это будет обнаружено, переспрошено и исправлено. Для этого выведена формула для нумерации сочетаний:

$$N_c = n_1 + C^2_{2-1} + C^3_{n3-1} + Cn^4_{4-1\ldots},$$

где n1,n2,n3,n4 – это номера мест по возрастанию в сочетаниях, в нашем случае это номера разрядов двоичного числа, где стоят единицы например

1 0 0 1 1 0 1 0 1 0 0

11 10 9 8 7 6 5 4 3 2 1

n1, n2, n3, n4, n5

3 5 7 8 11

Таким образом любое сочетание из пяти элементов имеет свой порядковый номер Nc, а так как нумерация сплошная то она представляет собой натуральный ряд положительных чисел и следовательно любому натуральному числу соответствует своё сочетание. Такая нумерация возможна при задании алгоритма следования, он должен быть таков чбо всегда в примере изменяется младший номер числа (увеличивается на единицу), когда перед ним уже есть такой номер, то увеличивается впереди стоящий, а младший возвращается к N1 например 3,5,7…, 4,5,7…, 1,6,7… 2,6,7….. (5,6,7…. 1,2,8).

Как показано в конце примера когда впереди несколько номеров подряд, то старший из них увеличивается на единицу, а младшие сколько бы их не было возвращаются в начало.

Такая нумерация дает нам возможность любое натуральное число изобразить в виде двоичного числа с фиксированным количеством единиц, например, пятью. Возможен и обратный переход от сочетания к числу, но описание алгоритма сложное. Для отыскания сочетания по номеру необходимо из номера вычесть ближайший младшый $C_x{}^5_{5-1}$ и записать $x_5=n_5$ затем из остатка вычесть $C^4_{x4-1}$ и т.д. Оставшееся число будет $x_1=n_1$. Для этого нужно применять таблицу которая намного упростит и отыскание номера и отыскание сочетания по номеру.

| $n_1$ | $n_2$ | $n_3$ | $n_4$ | $n_5$ |
|---|---|---|---|---|
| 1 | | | | |
| 2 | 0 | | | |
| 3 | 1 | 0 | | |
| 4 | 3 | 1 | 0 | |
| 5 | 6 | 4 | 1 | 0 |
| 6 | 10 | + 10 | 5 | 1 |
| 7 | 15 | 20 | 15 | 6 |
| 8 | 21 | 35 | 35 | 21 |
| 9 | 28 | 56 | 70 | 56 |
| 10 | 36 | 84 | 126 | 126 |

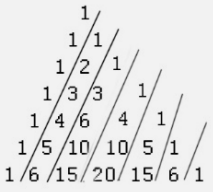


Рис. 1 Таблица отыскание номера и отыскание сочетания по номеру

Таблица легко строится, так как первый столбик есть натуральный ряд, второй наростающая сума первого, третий столбик наростающая сума второго и т.д. Кроме того каждый элемент ниже в столбике есть сума двух предыдущих как показано на обведенных блоках. А вообще эта таблица есть


ISSN 2520-2820 (online), ISSN 2524-0978 (print)

деформированный треугольник Паскаля, где первый столбец есть второй слева наклонный, но сдвинутый на одно число вверх относительно третьего. Пользоваться таблице необходимо по следующим правилам: для нахождения номера сочетания необходимо в столбике $n_5$ взять число состоящее в строке напротив значения $n_5$=11 в столбике $n_1$ затем число в столбике $n_4$ согласно приведенного примера и т.д.

3 8 7 8 11 и 252 + 35 + 20 + 6 + 3 = 316.

Обратная операция отыскания сочетания по номеру, из номера сочетания вычесть ближайшее меньшее в столбике $n_5$, а напротив него в столбике $n_1$ прочесть значение $n_5$=11 затем из остатка вычесть ближайшее меньшее в $n_4$ и прочесть в столбике $n_1$ значение $n_4$ = 8 и т. д.

Таблицу можно применять в программе по перекодировке. Таблицу по приведенному примеру можно расширить как вправо так и вниз для любых сочетаний, её можно применять в Excel для полуавтоматической работы. Одновременное же исчезновение и появления одинакового количества единиц в двух позициях хотя и возможно, выразить его намного меньше. В случае же еще больших жестких требованиях к достоверности передаваемой информации, где связано с жизнью людей или большими финансовыми потерями в банковской сфере можно применить перестановочную систему кодирования. Тогда каждое двоичное слово передаваемой информации будет перекодировано в перестановочную комбинацию, например из пяти числе от 1 до 5 4,2,1,5,3. Для этого разработан алгоритм нумерации перестановок, как и в случае нумерации сочетаний и алгоритм обратного перехода. Хотя этот алгоритм несколько сложение. Для начала его нужно объяснить с помощью таблицы.

Как известно, количество перестановок из n элементов равно n фактору Pn=n!, из 1=1 из 2=2 из 3 = 3, 1*2*3=6

Если например элементов 5, то перестановок равно 120. Если первая из них 5 4 3 2 1 N1, то последняя N120 будет 1 2 3 4 5, чтобы переномеровать промежуточное сочетания посмотрим таблицу. Чем старше число у последнего элемента справа, тем больше номер перестановки. Для того чтобы перестановка из 3 элементов стало

6 = 3! = 1 *2*3 = (1*2)*3=(2!)3=0*(2!) = 1*(2!) = 2*(2!) = 3*(2!)

| $n_1$ | $n_2$ | $n_3$ | $n_4$ | $n_5$ | |
|---|---|---|---|---|---|
| n | 1 | 0 | 0 | 0 | N1 |
| n | 2 | 2 | 6 | 24 | N2 |
| N | | 4 | 12 | 48 | N3 |
| Np | | | 18 | 72 | N4 |
| | | | | 96 | N5 |
| | | | | | |

Рис. 2 Алгоритм обратного перехода

По горизонтали $n_1$- $n_5$ - номер позиции по вертикали номер в списке по возрастанию из числа оставшихся $n_5$=3 из списка 1,2, 3, 4, 5 этот элемент номер 3 и поэтому мы взяли 48=(4!)*2 остались 4,2,1,5 по возрастанию из оставшихся 1 2 4 5 элементом 5 имеет номер 4 поэтому берем следующей столбик 18 (3!)*3 из оставшихся 4,2,1 по возрастанию его номер 1 – 1,2,4/1,2,3 поэтому берем О. Из оставшихся двух 4,2 2 – имеет номер по возрастанию 1 берем 1, если бы было 4,2 то взяли бы 2. Так как из одного элемента сочетания не существует то первая колонка пустая. Таким образом порядковый номер перестановки равен 67.

$$Np=N_{n5}=(4!)+N_{n4}(3!)+N_{n3}(2!)+N_{n2}(1!)$$

Как и в любой системе исчесления впереди стоящее нули не изменяют значение числа так и здесь, в перестановках 6 4 5 3 2 1 равносильна 3 1 2 имеет одинаковый номер и её можно сократить

6, 4, 5, ~~3, 2, 1~~

3, 3, 3

3, 1, 2

Можно и проделать обратную операцию расширить до необходимого размера 3,1,2 прибавляем справа + 3,1,2,4,3,2,1

4,4,4

7 5 6 4 3 2 1

Обратная операция получения перестановкам по её номеру производится по той же таблицу. Из номера перестановки вычисляется ближайшее меньшее значение в правой колонке. Против значения берется номер элемента. Даже из разницы вычитается ближайшее меньшее значение в следующей колонке левее, а вот номер будет соответствовать номеру по возрастанию из оставшихся, из списка, из которого выбирается истинный номер из-за этого и затруднен вывод формулы перехода, в которой может быть путаница, поэтому лучше пользоваться таблицей задав её программно. Такая система перекодировки не допускает не выявленных искажений так как при искажении или появляется два одинаковых элемента или элемент с номером не входящим в список во втором случае возможно автоматическое исправление, а в первом короткий переспрос, что бы выяснить какой элемент истинный.

С помощью перестановочного и сочетательных систем перекодировка возможно применение методо криптографии для защиты от несанкционированного доступа. Таков, например метод многослойного сочетательного перекодирования. Любое двоичное слово перекодируется, как сочетание определяется номер сочетания с соответствующим количеством единиц в этом слове на соответствующих позициях. Затем этот номер перекодится в двоичную систему и снова по единицам производится определения номера и т. д. 10,20 раз и каждый раз запоминается количество единиц например $^{1}a_2=^{1}a_c=^{2}a_2=^{2}a_c\ldots..{}^{n}a_c$

7 5 12 10 5

вместо $^{1}a_2$ пишем 7,15,12,10… $^{n}a_c$

$$Np=N_{n5}*(4!) + N_{n4}(3!)+N_{n3}(2!)+N_{n2}+N_{n2}(1!)$$

N – номер по возрастанию из оставшихся

P= $N_{n5}=Np(< / -) (4!)* N_{n5}=R_1$

$N_{n4}=R_1(< / -) (3!) N_{n4}=R_2$

$N_{n3}=R_2(< / -) (2!) N_{n3}=R_3$

$N_{n2}=R_2(< / -) (1!) (N_{n2})=R_2$

$N_{n1}=R_2$

(<) – знак ближайшего меньшего

R – разница

$N_{n4}$ – номер элемента стоящего на четвертом месте (слева на право)

(<) – ближайшее меньшее

P – перестановочная.

Половину этих значений передаём кореспонденту как ключ. При связи передаём ему оставшееся значение $a^{n}_{c}$ он производит обратную операцию и сообщает исходное $a_2$ известное нам и таким образом производится идентификация кореспондента.

**Результаты исследования.** Само же закрытие информации можно вести на переменном преобразовании информации по сочетательной или перестановочной системам, по наперед обусловленому алгоритму изменения, и постороннему наблюдателю информация будет не доступна как достоверная.

### Список используемой литературы


1. Биков В. Ю. Моделі організаційних систем відкритої освіти : монографія / В. Ю. Биков В. — К. : Атіка, 2009. — 684 с.
2. Манако А. Ф. К. М. Синица КТ в обучении: взгляд сквозь призму трансформаций [Електронний ресурс] // Образовательные Технологии и Общество. — 2012. — Том 15. — № 3. — С. 392—413. — Режим доступа: http://ifets.ieee.org/russian/depository/v15_i3/pdf/6.pdf. — Заголовок с экрана.
3. Про Доктрину інформаційної безпеки України : затверджено Указом Президента України від 8 липня 2009 року № 514/2009. [Електронний ресурс]. — Режим доступу: http://zakon4.rada.gov.ua/laws/show/514/2009.
4. Єсін В. І. Безпека інформаційних систем і технологій : навчальний посібник / В. І. Єсін, О. О. Кузнецов, Л. С. Сорока. — Харків : ХНУ імені В. Н. Каразіна, 2013. — 632 с.
5. Максименко С. Д. Цивілізаційні процеси і розвиток особистості / С. Д. Максименко [Електронний ресурс] // Проблеми сучасної психології: збірник наукових праць КПНУ імені Івана Огієнка, Інституту психології імені Г. С. Костюка НАПН України. — 2012. — Вип. 15. — С. 3—18. — Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/pspl/2012_15/3-18.pdf.
7. Спірін О. М. Методика забезпечення он-лайн безпеки старшокласників у навчально-виховному процесі школи [Електронний ресурс] / О. М. Спірін, В. Н. Ковальчук // Інформаційні технології і засоби навчання. — 2011. — № 1(21). — Режим доступу: http://archive.nbuv.gov.ua/e-journals/ITZN/2011_1/Kovalchuk.pdf.
8. Ананьїн В. О. Інформаційна безпека як чинник захисту особистості в сучасних умовах / В. О. Ананьїн, О. О. Пучков // Гілея (науковий вісник). — 2009. — Вип. 29.

9. Застело А. О. Інформаційно-психологічна безпека дистанційної освітньої взаємодії / А. О. Застело // Науковий вісник Миколаївського державного університету імені В. О. Сухомлинського. Серія: Психологічні науки. — 2011. — Т. 2. — Вип. 7. — С. 143—147. — Режим доступу: http:// archive.nbuv.gov.ua/portal/Soc_Gum/Nvmdu/psykh/2011_7/29.pdf.
10. Федорус О. М. Проблеми захисту інформації в умовах масової безперервної освіти для всіх / О. М. Федорус // Сучасна освіта і наука в Україні: традиції та інновації: Матеріали XII Всеукраїнської науково-практичної заочної конференції «Сучасна освіта і наука в Україні: традиції та інновації». — Т. 1 (м. Харків, 30—31 січня 2021 р.). — Харків : 2012. — С. 120—123. — Режим доступу: http://novaosvita.com.ua /wpcontent/uploads/2011/10/Kharkiv_XII_OSVITANAUKA_PART1.pdf.
11. Колгатін О. Г. Сучасні погляди на етику автоматизованої педагогічної діагностики / О. Г. Колгатін // Інформаційні технології і засоби навчання: електронне наукове фахове видання [Електронний ресурс] / Ін-т інформ. технологій і засобів навчання АПН України, Ун-т менеджменту освіти АПН України; гол. ред. : В. Ю. Биков. — 2009. — № 4(12). — Режим доступу http://www.ime.eduua.net/em12/content/09kogdpa.htm. — Заголовок з екрана.
12. Остроухов В. До проблеми забезпечення інформаційної безпеки України / Володимир Остроухов, Валентин Петрик // Політичний менеджмент. — 2008. — № 4. — С. 135—141. — Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/pome/2008_4/PDF/Ostroukhov.pdf.

***Victoria KONDRATIIVA, Dmitry CHAIKA***
Mykolaiv

## ENCODING TO PROTECT AGAINST CORRUPTION DURING SHIPMENT WITH THE USE OF SOCIETATILE AND PERMUTATION CODING SYSTEMS

*The proposed coding method is that used in the code a fixed number of units e.g. 4 or 6 in conclusion, word length 16, 32, or 64 bits. Any number of decimal or binary with the outstanding number of units can be recoded into a binary permutation with a fixed number of units, then if you go missing or will appear any number of units it is found peresproshennoe and fixed.*

*Keywords: encoding, distortion, shipment information system.*

***Вікторія КОНДРАТЬЄВА, Дмитро ЧАЙКА***
м. Миколаїв

## КОДУВАННЯ ДЛЯ ЗАХИСТУ ВІД СПОТВОРЕНЬ ПРИ ПЕРЕСИЛАННІ З ЗАСТОСУВАННЯМ СОЧИТАТЕЛЬНОЙ І ПЕРЕСТАНОВОЧНОЙ СИСТЕМ КОДУВАННЯ

*Пропонований метод кодування полягає в тому, що застосовується в коді фіксовану кількість одиниць наприклад 4 або 6 в ув'язненні від довжини слова 16, 32 або 64 біта. Будь-яке десяткове число або двійкове з невирішеним кількістю одиниць можна перекодувати в двійково-перестановочне з фіксованою кількістю одиниць, тоді якщо пропаде чи з'явиться будь-кількість одиниць це буде виявлено, переспрошено і виправлено.*

*Ключові слова: кодування, перекручення, пересилання інформації, система.*

Стаття надійшла до редколегії 30.03.2017