УДК 519.725, 625.7, 681.3

Укорачивание циклических кодов на основе альтернативного деления полиномов

Дяченко Олег Николаевич, Дяченко Валерий Олегович
Донецкий национальный технический университет
Донецк, Донецкая Народная Республика

Аннотация

Предлагается использование альтернативного метода укорачиванияциклическихкодов, исправляющих пакеты ошибок. В статье обоснована актуальность использования укорачивания кодов, в особенности для кодов, исправляющих пакеты ошибок большой длины. Выполнен анализ существующих способов, а также их аппаратной реализации. Рассмотрена идея предлагаемого метода укорачивания, сначала на примере элементов полей Галуа, а затем для кодов, исправляющих пакеты ошибок. По сравнению с традиционными подходами укорачивания кодов предлагаемый авторами отличается простотой применения, в том числе для кодов с большим параметром укорачивания.

Ключевые слова: *поле Галуа, циклические коды, укороченные коды, двойственный полином, порождающий полином, пакет ошибок.*

Shortening cyclic codes based on alternative division of polynomials

Dyachenko Oleg, Dyachenko Valery
Donetsk national technical university
Donetsk, Donetsk National Republic

Abstract

It is proposed to use an alternative method of shortening burst-error-correcting cyclic codes. In the article the urgency of the use of shortened codes, especially for codes which correct bursts error of large lengths. The existing methods and hardware implementation have been analyzed. The idea the proposed method of shortening, first, on the example of the elements Galois fields, and then for burst-error-correcting codes, has been considered. In comparison with the traditional approaches of shortening the codes proposed by the authors approach is easily to use, including for codes with the large parameter of shortening.

Keywords*: Galois field, cyclic codes, shortened codes, dual polynomial, generator polynomial, error burst.*

Введение

Изменения в различных сферах деятельности общества характеризуются стремительным ростом объемов самой различной информации: военной, коммерческой, мультимедийной, производственной, научной, технической, культурной и др. Все это признаки информационной революции.

В последние десятилетия достижения в области внедрения информационных технологий являются одним из определяющих факторов экономического и военного потенциала общества. В результате появляется и развивается информационная инфраструктура, которая предоставляет новые услуги, такие как дистанционное образование, знакомство и общение по Интернету, электронная торговля, интернет-банкинг, оплата счетов по Интернету и многие другие, а также лавина электронных игр и фильмов.

Увеличение количества информации приводит к требованиям обеспечения ее достоверности. Для решения этой задачи используются методы и средства помехоустойчивого кодирования. Одними из наиболее эффективных для исправления ошибок являются циклические коды. При практической реализации кодов довольно часто приходится их

укорачивать. В данной работе предлагается укорачивание кодов, основанное на альтернативном вычислении остатка от деления полинома X^{n-k+i} на порождающий полином.

Альтернативное деление полинома X^{n-k+i} на порождающий полином

Коды, исправляющие пакеты ошибок [1-7], наиболее часто необходимо укорачивать.

Пусть n – длина кода, k – количество информационных символов, 0<i<k – параметр укорачивания. Из любого (n, k) циклического кода, кроме (3,1) можно получить (n-i, k-i) укороченный код [2]. Для упрощения декодирования укороченных кодов необходимо предварительное вычисление остатка от деления полинома X^{n-k+i} на порождающий полином. Для большого параметра укорачивания либо сложно, либо и вовсе невозможно получить такой остаток традиционным способом.

Альтернативное деление полинома X^{n-k+i} на порождающий полином предполагает исключение параметра укорачивания для определения требуемого остатка. Предлагаемый способ основан на свойстве элементов полей Галуа, полученных для двойственных порождающих полиномов. Анализ таблицы 1 показывает взаимосвязь элементов этих полей. Учитывая, что эти элементы зеркально равны, получить элемент одного поля можно из соответствующего элемента другого поля, записанного в обратномпорядке, что соответствует умножению элемента от (X^{-1}) на $X^{deg(p(z)-1)}$. Например, получаем пары α^5=00101 и $\alpha^{30}=\alpha^{-1}$=10100, α^6=01010 и $\alpha^{29}=\alpha^{-2}$=01010, α^7=10100 и $\alpha^{28}=\alpha^{-3}$=00101 и т.д.

Таблица 1. Элементы полей Галуа GF(2^5) с двойственными (dual) порождающими полиномами

$p(X)=X^5+X^2+1$				$pd(X)=X^5+X^3+1$			
В виде степени	В двоичном	В виде степени	В двоичном	В виде степени	В двоичном	В виде степени	В двоичном
0	00000	α^{15}	11111	0	00000	$\alpha^{15}=\alpha^{-16}$	00110
α^0	00001	α^{16}	11011	$\alpha^0=\alpha^{-31}$	00001	$\alpha^{16}=\alpha^{-15}$	01100
α^1	00010	α^{17}	10011	$\alpha^1=\alpha^{-30}$	00010	$\alpha^{17}=\alpha^{-14}$	11000
α^2	00100	α^{18}	00011	$\alpha^2=\alpha^{-29}$	00100	$\alpha^{18}=\alpha^{-13}$	11001
α^3	01000	α^{19}	00110	$\alpha^3=\alpha^{-28}$	01000	$\alpha^{19}=\alpha^{-12}$	11011
α^4	10000	α^{20}	01100	$\alpha^4=\alpha^{-27}$	10000	$\alpha^{20}=\alpha^{-11}$	11111
α^5	00101	α^{21}	11000	$\alpha^5=\alpha^{-26}$	01001	$\alpha^{21}=\alpha^{-10}$	10111
α^6	01010	α^{22}	10101	$\alpha^6=\alpha^{-25}$	10010	$\alpha^{22}=\alpha^{-9}$	00111
α^7	10100	α^{23}	01111	$\alpha^7=\alpha^{-24}$	01101	$\alpha^{23}=\alpha^{-8}$	01110
α^8	01101	α^{24}	11110	$\alpha^8=\alpha^{-23}$	11010	$\alpha^{24}=\alpha^{-7}$	11100
α^9	11010	α^{25}	11001	$\alpha^9=\alpha^{-22}$	11101	$\alpha^{25}=\alpha^{-6}$	10001
α^{10}	10001	α^{26}	10111	$\alpha^{10}=\alpha^{-21}$	10011	$\alpha^{26}=\alpha^{-5}$	01011
α^{11}	00111	α^{27}	01011	$\alpha^{11}=\alpha^{-20}$	01111	$\alpha^{27}=\alpha^{-4}$	10110
α^{12}	01110	α^{28}	10110	$\alpha^{12}=\alpha^{-19}$	11110	$\alpha^{28}=\alpha^{-3}$	00101
α^{13}	11100	α^{29}	01001	$\alpha^{13}=\alpha^{-18}$	10101	$\alpha^{29}=\alpha^{-2}$	01010
α^{14}	11101	α^{30}	10010	$\alpha^{14}=\alpha^{-17}$	00011	$\alpha^{30}=\alpha^{-1}$	10100
		α^0	00001			α^0	00001
		α^1	00010			α^1	00010
		α^2	00100			α^2	00100
		α^3	01000			α^3	01000
		α^4	10000			α^4	10000

Таким образом, для альтернативного способа сначала вычисляется остаток от деления полинома в степени длины нового укороченного кода, уменьшенной на единицу, на

двойственный полином: $R_{pd(X)}[X^{n-1}]$. Затем $R_{pd(X)}[X^{n-1}](X^{-1})$ умножается на $X^{degp(X)-1}$. В итоге получаем искомый остаток $R_{p(X)}[X^{degp(X)+i}]$.

Укороченные коды, исправляющие пакеты ошибок

Укороченный (272, 260)-код, исправляющийчетыреошибки, получен укорачиванием систематического циклического кода(511, 499) на 239 символов. Порождающий полином $p(X)=X^{12}+X^8+X^5+X^3+1$ этого кода найден с помощью поиска на компьютере, $X^{n-k+i}=X^{251}$, остаток от деления, полученный традиционным способом $R_{p(X)}[X^{239+12}]=X^{11}+X^9+X^7+X^3+X^2+1$.

Для предлагаемого способа определяем остаток от деления полинома в степени длины нового укороченного кода, уменьшенной на единицу, т.е. X^{272-1}, на двойственный pd(X) полином. $pd(X)=X^{degp(X)}p(X^{-1})=X^{12}(X^{-12}+X^{-8}+X^{-5}+X^{-3}+1)=(X^{12}+X^9+X^7+X^4+1)$. Получив остаток $R_{pd(X)}[X^{272-1}]=X^{11}+X^9+X^8+X^4+X^2+1$ и умножив $R_{pd(X)}[X^{271}](X^{-1})$ на полином $X^{degp(X)-1}$, находим искомый остаток:

$R_{g(X)}[X^{272-1}]=X^{11}(X^{-11}+X^{-9}+X^{-8}+X^{-4}+X^{-2}+1)=X^{11}+X^9+X^7+X^3+X^2+1=R_{g(X)}[X^{239+12}]$.

Следует отметить важное отличие предлагаемого способа от известных. Из вычислений остатка исключается параметр укорачивания i, и таким образом, становится возможной реализация кодов с большим параметром укорачивания и длиной исправляемого пакета ошибок.

Перемеженный укороченный систематический циклический код, построенный на основе кода, найденного с помощью моделирования на компьютере

Определение параметров исходного кода.

Параметр укорачивания i = 3

Исходный код: (15, 9), образующий полином: $C(X) = X^6 + X^5 + X^4 + X^3 + 1$, длина исправляемого пакета ошибок исходного кода b = 3.

Пусть j = 2, i = 3, где i – параметр укорачивания, j – параметр перемежения.

Определение параметров данного кода.

(2*15-3, 2*9-3) = (27, 15), n = 27, k = 15.

Определение длины исправляемого пакета ошибок:

b’ = j*b = 2*b = 2*3 = 6.

Определение порождающего полинома C’(X).

$C'(X) = X^{6*j} + X^{5*j} + X^{4*j} + X^{3*j} + 1 = X^{12} + X^{10} + X^8 + X^6 + 1$

Определение количества проверочных символов p.

p = n – k = 27 – 15 = 12

Определение остатка от деления $X^{(p+i)}$ на образующий полином $R_{C'(X)}[X^{p+i}]$.

$$\begin{array}{l|l} X^{15} & X^{12}+X^{10}+X^8+X^6+1 \\ \underline{X^{15}+X^{13}+X^{11}+X^9+X^3} & \overline{X^3+X} \\ X^{13}+X^{11}+X^9+X^3 & \\ \underline{X^{13}+X^{11}+X^9+X^7+X} & \\ X^7+X^3+X & \end{array}$$

$R_{C'(X)}[X^{p+i}] = X^7 + X^3 + X$

Определение двойственного полинома $C^{*}{}'(X)$ порождающего полинома C’(X).

$C^{*}{}'(X) = X^{12}(X^{-12} + X^{-10} + X^{-8} + X^{-6} + 1)=X^{12} + X^6 + X^4 + X^2 + 1$

Определение остатка от деления $X^{(n-1)}$ на образующий полином $R_{C^{*}{}'(X)}[X^{n-1}]$.

$R_{C^{*}{}'(X)}[X^{26}] = X^{10} + X^8 + X^4$

Определение зеркального остатка

$X^{11}(X^{-10} + X^{-8} + X^{-4}) = X^7 + X^3 + X = R_{C'(X)}[X^{p+i}]$.

Таким образом, полученные остатки $R_{C'(X)}[X^{p+i}]$ разными способами совпадают, что подтверждает применимость предлагаемого способа определения остатка и для перемеженных укороченных кодов.

Построение кодера для (27, 15)-кода.

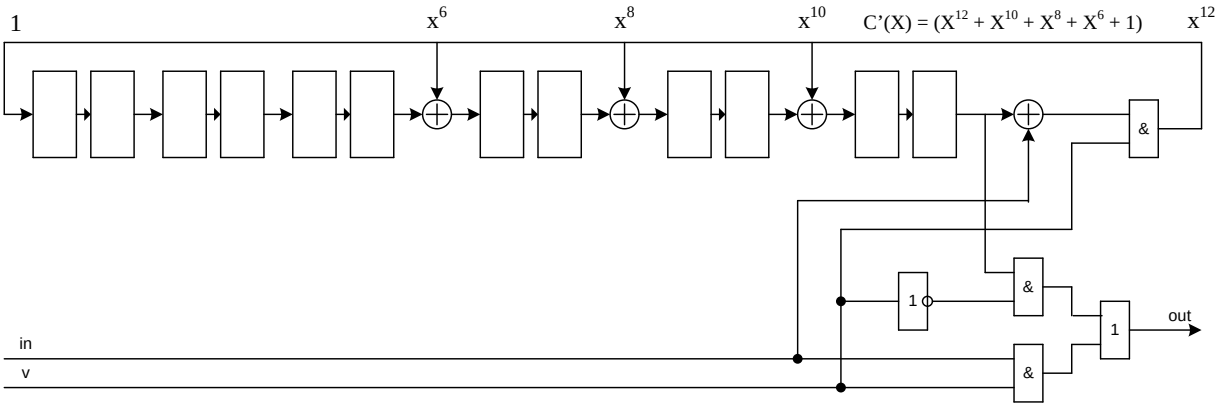

Рисунок 1 – Кодер для перемеженного укороченного систематического (27, 15)-кода

Сигнал V используется для переключения ключей кодера. Он должен быть высокого уровня первые k=15 тактов и потом переключаться в низкий уровень.

Построение декодера для кода (27, 15).

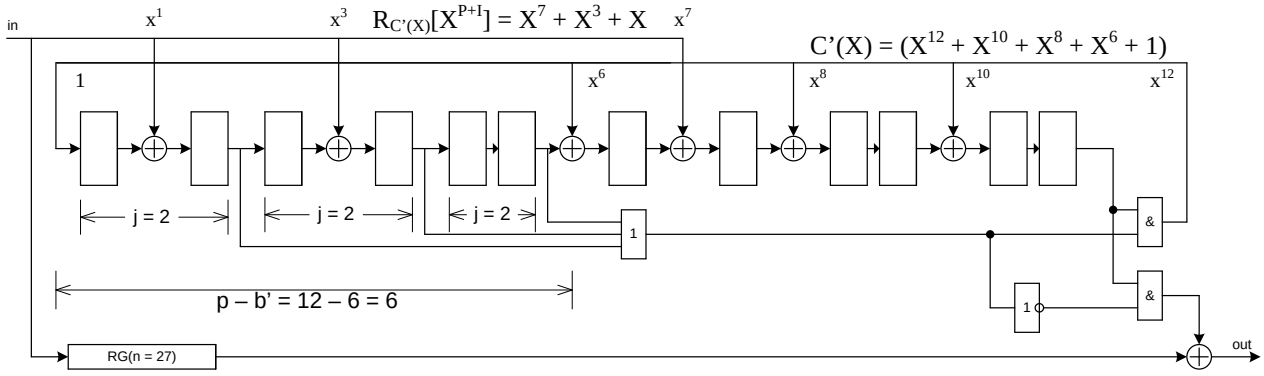

Рисунок 2 – Декодер для перемеженного укороченного систематического (27, 15)-кода

Укороченный систематический циклический код Файра

Определение параметров исходного кода.

Пусть параметр укорачивания i = 14

Длина исправляемого пакета ошибок b = 4

Параметры кода: (105-i, 94-i) => (105-14, 94-14) => (91, 80)

Определение порождающего полинома F(X).

$F(X) = (X^{2b-1} + 1)(X^4 + X + 1) = (X^7 + 1)(X^4 + X + 1) = X^{11} + X^8 + X^7 + X^4 + X + 1$

$$\begin{array}{r} \times \quad X^4 + X + 1 \\ \hline X^7 + 1 \\ \hline X^4 + X + 1 \\ + \quad X^{11} + X^8 + X^7 \\ \hline X^{11} + X^8 + X^7 + X^4 + X + 1 \end{array}$$

Определение количества проверочных символов p.

p = n – k = 91 – 80 = 11

Определение остатка от деления $X^{(p+i)}$ на образующий полином $R_{F(X)}[X^{p+i}]$.

$$
\begin{array}{l|l}
X^{25} & X^{11}+X^{8}+X^{7}+X^{4}+X+1 \\
\underline{X^{25}+X^{22}+X^{21}+X^{18}+X^{15}+X^{14}} & \overline{X^{14}+X^{11}+X^{10}+X^{8}+X^{7}+X^{6}+X^{5}+X+1} \\
X^{22}+X^{21}+X^{18}+X^{15}+X^{14} & \\
\underline{X^{22}+X^{19}+X^{18}+X^{15}+X^{12}+X^{11}} & \\
X^{21}+X^{19}+X^{14}+X^{12}+X^{11} & \\
\underline{X^{21}+X^{18}+X^{17}+X^{14}+X^{11}+X^{10}} & \\
X^{19}+X^{18}+X^{17}+X^{12}+X^{10} & \\
\underline{X^{19}+X^{16}+X^{15}+X^{12}+X^{9}+X^{8}} & \\
X^{18}+X^{17}+X^{16}+X^{15}+X^{10}+X^{9}+X^{8} & \\
\underline{X^{18}+X^{15}+X^{14}+X^{11}+X^{8}+X^{7}} & R_{F(X)}[X^{p+i}] = X^9 + X^7 + X^4 + X^2 + 1 \\
X^{17}+X^{16}+X^{14}+X^{11}+X^{10}+X^{9}+X^{7} & \\
\underline{X^{17}+X^{14}+X^{13}+X^{10}+X^{7}+X^{6}} & \\
X^{16}+X^{13}+X^{11}+X^{9}+X^{6} & \\
\underline{X^{16}+X^{13}+X^{12}+X^{9}+X^{6}+X^{5}} & \\
X^{12}+X^{11}+X^{5} & \\
\underline{X^{12}+X^{9}+X^{8}+X^{5}+X^{2}+X} & \\
X^{11}+X^{9}+X^{8}+X^{2}+X & \\
\underline{X^{11}+X^{8}+X^{7}+X^{4}+X+1} & \\
X^{9}+X^{7}+X^{4}+X^{2}+1 &
\end{array}
$$

Определение двойственного полинома $F^*(X)$ порождающего полинома F(X).

$F^*(X) = X^{11}(X^{-11} + X^{-8} + X^{-7} + X^{-4} + X^{-1} + 1) = X^{11} + X^{10} + X^7 + X^4 + X^3 + 1$

Определение остатка от деления $X^{(n-1)}$ на двойсвенный полином $R_{F^*(X)}[X^{n-1}]$.

$R_{F^*(X)}[X^{90}] = X^{10} + X^8 + X^6 + X^3 + X$

Определение зеркального остатка

$X^{10}(X^{-10} + X^{-8} + X^{-6} + X^{-3} + X^{-1}) = X^9 + X^7 + X^4 + X^2 + 1 = R_{F(X)}[X^{p+i}]$.

Таким образом, полученные остатки $R_{F(X)}[X^{p+i}]$ разными способами совпадают, что подтверждает применимость предлагаемого способа определения остатка и для кодов Файра с небольшим параметром укорачивания.

Построение кодера для (91, 80)-кода.

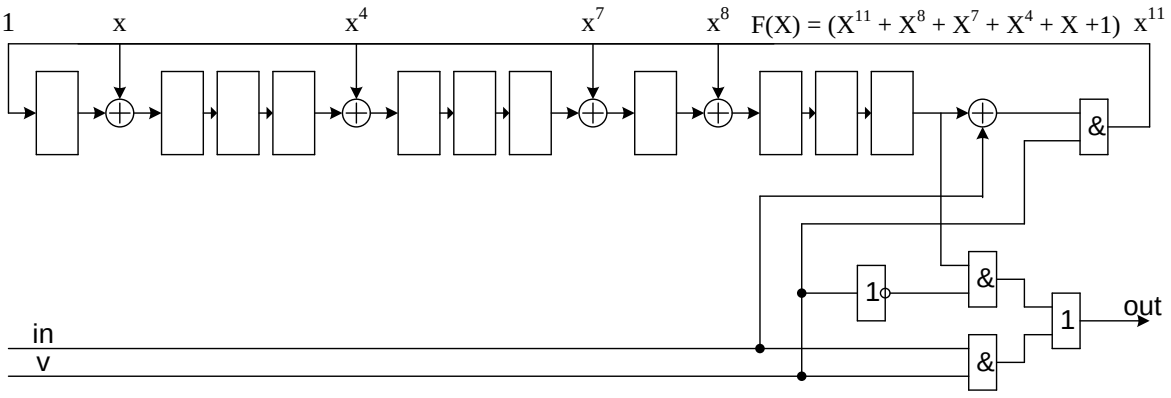

Рисунок 3 – Кодер для укороченного систематического (91, 80)-кода Файра

Сигнал V используется для переключения ключей кодера. Он должен быть высокого уровня первые k=80 тактов и потом переключаться в низкий уровень.

Построение декодера для кода (91, 80).

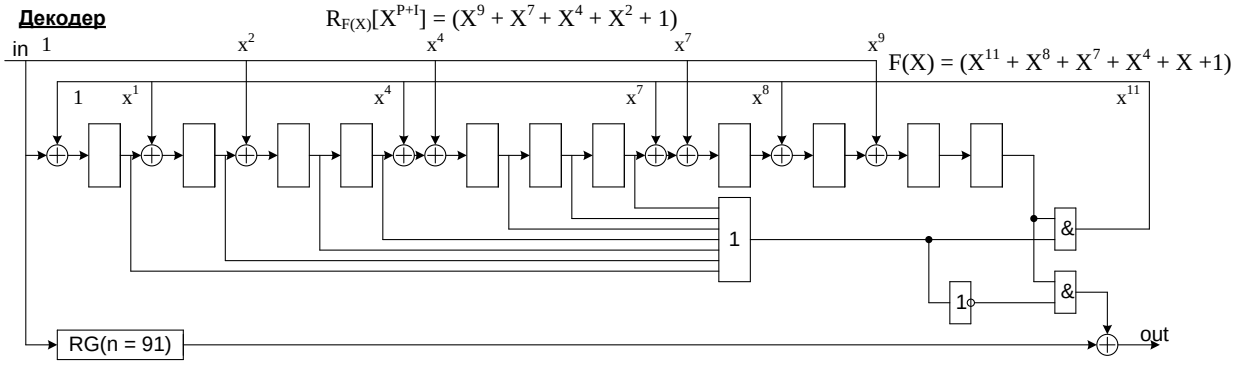

Рисунок 4 – Декодер для укороченного систематического (91, 80)-кода Файра

Заключение

В работе предложен метод построения укороченных циклических кодов, основанный на альтернативном вычислении остатка от деления полинома X^{n-k+i} на порождающий полином. В результате появляется возможность укорачивания для кодов с большой длиной исправляемого пакета ошибок с использованием традиционной аппаратной или программной реализации кодеров и декодеров.

Литература

1. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования – методы, алгоритмы, применение. – М.: Техносфера, 2005. — 320 с.

2. Richard E.Blahut. Algebraic Codes for Data Transmission/ Cambridge University Press, 2012. – 498 p.

3. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 595 с.: ил.

4. Дяченко В.О., Зинченко Ю.Е., Дяченко О.Н. Исследование способов проектирования кодов Рида-Соломона// Інформаційні управляючі системи та комп'ютерний моніторинг (ІУС КМ-2014): V Всеукраїнська науково-технічна конференція студентів, аспірантів та молодих вчених, 22-23 квітня 2014 р., м. Донецьк : зб. доп./ Донец. національ. техн. ун-т; редкол. В.А.Світлична. – Донецьк: ДонНТУ, 2014. – в 2 тт. – т.2. – С. 72-78.

5. Дяченко В.О., Дяченко О.Н. Анализ способов реализации кодов Рида-Соломона, исправляющих двойные ошибки// Современные тенденции развития и перспективы внедрения инновационных технологий в машиностроении, образовании и экономике: материалы Международной научно-практической конференции (Азов, 19 мая 2014 г.). – Ростов н/Д, ДГТУ, 2014. – С. 18-22.

6. Дяченко В.О., Дяченко О.Н. Особенности применения двойственных полиномов для аппаратной реализации циклических кодов // Информационные управляющие системы и компьютерный мониторинг в рамках форума "Инновационные перспективы Донбасса" (ИУС КМ-2015): VI Международная научно-техническая конференция студентов, аспирантов и молодых ученых, 20-22 мая 2015, г.Донецк: / Донец.национал. техн. ун-т; сост.: К.Н.Маренич (председатель) и др. – Донецк: ДонНТУ, 2015. – С. 130–136.

7. Дяченко В.О., Дяченко О.Н. Циклическое кодирование цифровой информации на основе двойственных полиномов // Современные тенденции развития и перспективы внедрения инновационных технологий в машиностроении, образовании и экономике: материалы II Международной научно-практической конференции (Азов, 19 мая 2015 г.) [Электронный ресурс]. – Ростов н/Д, ДГТУ, 2015. – С. 71-76. – Режим доступа: http://atidstu.ru/atidgtu-rf/node/1163.