УДК 512.64, 519.21, 519.72 Вестник УрФО № 4(58) / 2025, с. 64–70

Медведева Н. В., Титов С. С.

10.14529/secur250407

АНАЛОГИ СОВЕРШЕННЫХ ШИФРОВ В ТЕОРИИ КОДИРОВАНИЯ

В работе предложена кодовая конструкция, которая оказывается связан-ной с задачами теории информации, распределения вероятностей многомерных случайных величин и многомерной задаче о системах представителей. Доказана теорема об аналогах совершенных шифров, согласно которой свойство «совершенности» (отсутствия потерь информации) является глобальным свойством канала. Построен пример аналога шифра с тремя шифрвеличинами, иллюстрирующий предложенную кодовую конструкцию. Полученные результаты отражают универсальность совершенных систем шифрования.

Ключевые слова: *защита информации, совершенные шифры, совершенные коды, многомерные случайные величины, кодовые конструкции.*

Medvedeva N. V., Titov S. S.

ANALOGUES OF PERFECT CIPHERS IN CODING THEORY

This work proposes a code construction that is related to problems in information theory, probability distributions of multivariate random variables, and the multidimensional system of representatives problem. A theorem on the analogues of perfect ciphers is proved, stating that the property of «perfection» (absence of information loss) is a global property of the channel. An example of a cipher analogue with three cipher values is constructed to illustrate the proposed code structure. The results reflect the universality of perfect encryption systems.

Keywords: *information protection, perfect ciphers, perfect codes, multidimensional random variables, code constructions.*

В современных условиях, когда объемы передаваемых и хранимых данных растут экспоненциально, а требования к надежности и безопасности ин-формационных систем становятся критически важными, особую значимость приобретают фундаментальные исследования на стыке теории информации и криптографии. Изучение аналогов совершенных шифров в теории кодирования представляет не только теоретический интерес, но и имеет практическое значение для решения актуальных задач в области защиты информации и обеспечения достоверности данных.

Концепция совершенного шифра, впервые строго сформулированная К. Шенноном [1], устанавливает теоретический предел в криптографии – абсолютную стойкость к криптоатакам. Построение абсолютно стойких систем передачи данных исследовалось в работах [2 – 7].

Поиск и изучение аналогичных предельно эффективных конструкций в теории коди-

рования позволяет выявить универсальные математические принципы, лежащие в основе как защиты от злоумышленника, так и обеспечения целостности данных при передаче через зашумленные каналы связи.

В настоящей работе исследуются аналоги совершенных (по Шеннону [1]) шифров при построении систем передачи данных. Здесь используется вероятностная модель $\sum_{\text{В}}$ [1] передачи данных с шифрованием и кодированием, с соответствующими обозначениями: $X = \{x1, x2,\ldots, x\lambda\} = \{1, 2,\ldots, \lambda\}$ множество шифрвеличин (алфавит открытых текстов); $Y = \{y1, y2,\ldots, y\mu\} = \{1, 2,\ldots, \mu\}$ – множество шифробозначений (алфавит закрытых текстов), с которыми оперирует некоторый шифр замены; $K = \{k_1, k_2, \ldots, k_\pi\}$ – множество ключей. По условию: $| X | = \lambda > 1$, $| Y | = \mu \geq \lambda$, $| K | = \pi \geq \mu$. Тексты представляют собою слова (ℓ-граммы, т.е. биграммы, триграммы и так далее) в соответствующих алфавитах. Под шифром $\sum_{\text{В}}$ понимается совокупность множеств правил зашифрования и правил расшифрования с заданными распределениями вероятностей на множествах открытых текстов и ключей [8, 9].

Абсолютная стойкость вероятностной модели $\sum_{\text{В}}$ системы передачи данных, согласно определению совершенного по Шеннону шифра, эквивалентна равенству апостериорных вероятностей $p(x \mid y)$, $x \in X^{\ell}$, $y \in Y^{\ell}$ открытых текстов и соответствующих им априорных вероятностей p (x) [8, 9]. В работе [2] показано, что построение абсолютно стойких систем передачи данных приводит к постановке задачи описания произвола в построении совместно распределенных случайных величин, трактуемых как посылаемые и принимаемые сигналы.

Кодовыми аналогами совершенных шифров можно считать генератор символов кода, которые зависят от двух источников – детерминированного, определяемого передаваемым сообщением (аналог символа открытого текста), и случайного, выбор которого происходит в соответствии с заданной вероятностью (аналог ключа); при этом априорные и апостериорные вероятности символов совпадают (аналог совершенности шифра). Так, если генерируемые символы кода – биты, то условная вероятность появления на выходе бита, равного единице, должна быть одинаковой для любого входного символа сообщения.

Детерминированность источников сообщений должна пониматься доста-точно относительно, поскольку она связана с логикой управления, реагирования на реальные ситуации и поэтому не входит в данную кодовую модель. По-этому можно расширить эту модель, считать появление символов источников сообщений как случайные события с некоторым распределением их вероятно-сти. Однако это оказывается излишним, потому что имеет место

Теорема. Пусть имеется канал связи с дискретными входами $x \in X$ и выходами $y \in Y$. Если существует распределение $p_0(x)$, для которого выполняется **условие аналога совершенности:** $I_{p0}(x; y) = C$ и $H_{p0}(x \mid y) = 0$, где C – пропускная способность канала, $I(x; y)$ – взаимная информация между двумя случайными величинами x и y, $H(x \mid y)$ – условная энтропия x при известном y, то для любого другого распределения $p(x)$ выполняется **расширенное условие совершенности:** $I_p(x; y) = C$ и $H_p(x \mid y) = 0$.

Доказательство. Полагаем, что матрица $p(Y \mid X)$ переходных вероятностей канала фиксирована. Условие $H_{p0}(x \mid y) = 0$ означает, что при наблюдении y вход x восстанавливается однозначно. Формально: $\forall y \in Y\ \exists! x \in X : p_0(x \mid y) = 1$. Это эквивалентно тому, что отображение $X \rightarrow Y$ инъективно на носителе распределения $p_0(X)$, т.е. для любого y существует не более одного x, для которого $p(y \mid x) > 0$ и $p_0(x) > 0$.

Из условия $H_{p0}(x \mid y) = 0$ следует, что канал не создает неопределенности при использовании $p_0(X)$. Это возможно только, если для каждого y существует не более одного x с $p(y \mid x) > 0$. Таким образом, канал ведет себя как детерминированное отображение на подмножестве входов, где $p_0(x) > 0$. Обозначим через $X_0 = \{x \in X: p_0(x) > 0\}$. Тогда для $x_1, x_2 \in X_0$, $x_1 \neq x_2$ имеем: $p(y \mid x_1) \cdot p(y \mid x_2) = 0$ для любого $y \in Y$. Это означает, что выходы для разных входов из X_0 не пересекаются.

Условие $I_{p0}(x; y) = C$, где C – пропускная способность канала, определяемая равенством $C = \max\limits_{p(x)} I_p(x; y)$, означает, что распределение $p_0(x)$ достигает пропускной способности. Так как $H_{p0}(x \mid y) = 0$, то $I_{p0}(x; y) = H_{p0}(x) = C$. Следовательно, пропускная способность канала равна максимальной энтропии входа при условии инъективности отображения $X \rightarrow Y$.

Рассмотрим произвольное распределение $p(x)$. Покажем, что $I_p(x; y) = C$ и $H_p(x \mid y) = 0$. Для любого y с $p(y) > 0$ существует един-

ственный $x \in X_0$, для которого $p(y \mid x) > 0$. Это следует из структурного свойства канала, которое не зависит от распределения $p(x)$. Поэтому при наблюдении y всегда можно однозначно определить x даже, если $p(x) \neq p_0(x)$. Следовательно, $H_p(x \mid y) = 0$ для любого $p(x)$.

Из $H_p(x \mid y)$ следует, что $I_p(x; y) = H_p(x) - H_p(x \mid y) = H_p(x)$. Однако, $I_p(x; y) \leq C$ по определению пропускной способности. Для того, чтобы достичь C необходимо максимизировать $H_p(x)$ при условии, что отображение $X \rightarrow Y$ остается инъективным. Максимальная энтропия достигается на равномерном распределении на множестве X_0 и $H(X_0) = C$. Для произвольного $p(x)$, если $supp\ p \subset X_0$, то $H_p(x) \leq C$, и равенство достигается только для равномерного распределения на X_0.

Условие теоремы гарантирует, что структура канала позволяет передавать без потерь C бит. Для произвольного $p(x)$, если $supp\ p \not\subset X_0$, то $H_p(x)$ может быть меньше C, но условие совершенности $H_p(x \mid y) = 0$ сохраняется. Следовательно, теорема утверждает, что свойство нулевой условной энтропии сохраняется, а не то, что пропускная способность достигается при любом распределении.

Выше показано, что:

1. Условие $H_{p0}(x \mid y) = 0$ влечет структурное свойство канала – инъективность отображения $X \rightarrow Y$ на $supp\ p_0$.

2. Это структурное свойство не зависит от распределения $p(x)$, поэтому $H_p(x \mid y) = 0$ выполняется для любого $p(x)$.

3. Пропускная способность C достигается при равномерном распределе-нии на X_0, а для других распределений $I_p(x; y) = H_p(x) \leq C$.

Таким образом, условие аналога совершенности выполняется в расши-ренном смысле: свойство нулевой условной энтропии сохраняется для любого распределения входных символов, что и требовалось доказать.

Другими словами, если условие аналога совершенности выполняется для одного конкретного случая (чаще всего равномерного распределения), оно будет верным и для всех остальных распределений вероятностей, т.е. схема шифрования не зависит от характера распределения исходных данных. Это обстоятельство указывает на универсальность данного подхода к созданию абсолютно стойких кодов.

В простейшем случае эта конструкция может быть представлена матрицей размерами M на N совместного распределения двух независимых случайных величин, представляющей соответствующее дискретное вероятностное пространство. В этой матрице проставлены биты, задающие характеристическую функцию подмножества множества её ячеек и, таким образом, случайное событие, которое должно обладать следующим свойством: его проекция на пространство N есть пространство с тем же (исходным) распределением вероятности. При этом пространство N столбцов может быть интерпретировано как множество источников сообщений, а пространство M строк – как множество кодировок (ключей). При равновероятных распределениях такая модель задаётся (0,1)-матрицей, у которой одинаковое количество единиц в каждом столбце и одинаковое количество единиц в каждой строке.

Такая матричная модель связана не только с теорией кодирования, но также и с задачей представителей: столбцы – вероятные ответы источника со-общений, представителя, а строки – варианты ответов всей группы. При этом выбор случайного источника и ответа не раскрывает, какой именно представитель был выбран.

Построим и проверим на совершенную секретность кодовую конструк-цию с тремя шифрвеличинами.

Пример. Пусть $X = \{x_1, x_2, x_3\}$, где $x_i \in \{0,1\}$; $K = \{k_1, k_2, k_3\}$, где $k_i \in \{0,1\}$, k_i равномерно распределены, независимы; $Y = \{y_1, y_2, y_3\}$, где $y_i = x_i \oplus k_i$ (сложение по модулю 2).

Случай 1. Равномерное распределение открытого текста. Пусть $p(X) = 1/8$ для всех восьми возможных сообщений, указанных в таблице 1.

Таблица 1

Равномерное распределение входных символов

X	000	001	010	011	100	101	110	111
$p(X)$	1/8	1/8	1/8	1/8	1/8	1/8	1/8	1/8

Тогда для любого фиксированного Y получаем, что $p(Y|X) = 1/8$. Например, для $Y = 000$ и $X = 010$ имеем: $p(Y|X = 010) = p(K = 010) = 1/8$. При этом вероятность $p(Y) = \Sigma\ p(X) \bullet p(Y|X) = 1/8$ и условная вероятность $p(X|Y) = 1/8$. Следовательно, $p(X|Y) = p(X) = 1/8$ для всех X, т.е. шифр является совершенным для равномерного распределения открытых текстов.

В этом случае все элементы матрицы размера 8×8 совместного распределения $p(X|Y)$ будут равны $1/64$. Здесь для любых X и Y: $p(X|Y) = p(X) \cdot p(Y|X) = p(X) \cdot p(K = Y \oplus X) = 1/8 \cdot 1/8 = 1/64$. Дискретное пространство элементарных событий Ω содержит 64 элементарных событий, вероятность каждого равна $1/64$.

Случай 2. Неравномерное распределение (естественный язык). Пусть распределение открытых текстов неравномерно и задано таблицей 2.

Тогда для любого фиксированного Y сравнивая, априорное распределение: $p(X) = (0{,}4\ 0{,}1\ 0{,}1\ 0{,}1\ 0{,}1\ 0{,}05\ 0{,}05\ 0{,}1)$ с апостериорным распределением: $p(X|Y) = (0{,}4\ 0{,}1\ 0{,}1\ 0{,}1\ 0{,}1\ 0{,}05\ 0{,}05\ 0{,}1)$, получим равенство $p(X|Y) = p(X)$.

Конструкция матрицы размера 8×8 совместного распределения $p(X|Y)$ представлена в таблице 3.

Случай 3. Вырожденное распределение. Пусть всегда передается сообщение X = 000 (таблица 4).

В этом случае равенство также сохраняется: $p(X|Y) = p(X)$. Например, для $Y = 000$ имеем: $p(Y = 000) = 1 \bullet 1/8 = 1/8$; $p(X = 000|\ Y = 000) = 1 \bullet (1/8) / (1/8) = 1$.

Для других X: $p(X|Y = 000) = 0$.

Здесь матрица совместного распределения $p(X|Y)$ будет также размера 8×8. При этом все элементы первой строки (соответствующей $X = 000$) равны $1/64$, а элементы остальных строк – равны 0.

Случай 4. Коррелированные сообщения. Рассмотрим случай, где биты сообщения коррелированы: $p(X = 000) = 0{,}3$; $p(X = 111) = 0{,}3$; $p(X = 001) = p(X = 010) = ... = p(X = 110) = 0{,}4/6 = 0{,}2/3$.

Таблица 2

Неравномерное распределение входных символов

X	000	001	010	011	100	101	110	111
$p(X)$	0,4	0,1	0,1	0,1	0,1	0,05	0,05	0,1

Таблица 3

Конструкция матрицы совместного неравномерного распределения

$X\backslash Y$	000	001	010	011	100	101	110	111
000	0,4/64	0,4/64	0,4/64	0,4/64	0,4/64	0,4/64	0,4/64	0,4/64
001	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64
010	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64
011	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64
100	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64
101	0,05/64	0,05/64	0,05/64	0,05/64	0,05/64	0,05/64	0,05/64	0,05/64
110	0,05/64	0,05/64	0,05/64	0,05/64	0,05/64	0,05/64	0,05/64	0,05/64
111	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64	0,1/64

Таблица 4

Вырожденное распределение входных символов

X	000	001	010	011	100	101	110	111
$p(X)$	1	0	0	0	0	0	0	0

Таблица 5

Конструкция матрицы совместного распределения коррелированных битов

$X\backslash Y$	000	001	010	011	100	101	110	111
000	0,3/64	0,3/64	0,3/64	0,3/64	0,3/64	0,3/64	0,3/64	0,3/64
001	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192
010	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192
011	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192
100	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192
101	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192
110	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192	0,2/192
111	0,3/64	0,3/64	0,3/64	0,3/64	0,3/64	0,3/64	0,3/64	0,3/64

Таблица 6

Конструкция битовой матрицы совместного распределения

$X\backslash Y$	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	10	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	011	011
101	101	100	111	110	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	111	011	010	001	000

Проверим для $Y = 101$: $p(Y = 101) = 0{,}3 \cdot 1/8 + 0{,}3 \cdot 1/8 + 6 \cdot 1/15 \cdot 1/8 = 1/8$; $p(X = 000 | Y = 101) = 0{,}3 \cdot 1/8 \,/\, (1/8) = 0{,}3$; $p(X = 111 | Y = 101) = 0{,}3 \cdot 1/8 \,/\, (1/8) = 0{,}3$.

Для других X: $p(X|Y = 101) = (1/8) \cdot (1/15) \,/\, (1/8) = 1/15$, т.е. равенство $p(X|Y) = p(X)$ сохраняется.

Конструкция матрицы размера 8×8 совместного распределения $p(X|Y)$ представлена в таблице 5.

Конструкция битовой матрицы размера $M \times N = 8 \times 8$ совместного распределения (для фиксированного K и X получаем определенный шифртекст Y) для шифра с тремя шифрвеличинами представлена в таблице 6.

Эта матрица универсальна и не зависит от $p(X)$ распределения вероятностей открытых текстов. При этом матрица совместного распределения $p(X|Y)$ выводится из битовой матрицы. Например, каждая ячейка (X, Y) в вероятностной матрице равномерного распределения (случай 1) получает вероятность $1/64$, потому что для каждой пары (K, X) в битовой матрице существует ровно один K, дающий нужный шифртекст Y.

Данный пример аналога шифра с тремя шифрвеличинами показывает, что условие совершенной секретности, выполненное для одного распределения открытых текстов (равномерного), выполняется и в расширенном смысле для любого распределения вероятностей входных символов.

Таким образом, в работе предложена кодовая конструкция, которая оказывается связанной с задачами теории информации, распределения вероятностей многомерных случайных величин и многомерной задаче о системах представителей. Доказана теорема об аналогах совершенных шифров, согласно которой свойство «совершенности» (отсутствия потерь информации) является глобальным свойством

канала. Если можно найти хотя бы одно распределение входных символов, при котором канал работает на пределе своих возможностей и без потерь, то этот канал по своей природе лишен внутренних помех, вызывающих потери информации, для любого способа его использования. Построен пример аналога шифра с тремя шифрвеличинами, иллюстрирующий предложенную кодовую конструкцию.

Полученные результаты отражают универсальность совершенных систем шифрования и делают теорию идеальной секретности пригодной для широкого спектра криптографических систем. Это, в свою очередь, дает возможность создания адаптивных систем связи, сохраняющих свои оптимальные свойства при изменении статистических характеристик передаваемых данных.

Литература

1. Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетики. М.: Наука, 1963. – С. 333–402.

2. Медведева Н.В. Об аналогах теоремы Шеннона для совершенных шифров // CEUR Workshop Proceedings. 2016. Т. 1825. С. 232–239. ISSN 1613–0073.

3. Медведева Н. В. К разработке абсолютно стойких систем передачи данных / Н. В. Медведева, С. С. Титов // Вестник УрГУПС. – 2019. – № 2(42). – С. 34–43. – DOI 10.20291/2079-0392-2019-2-34-43. – EDN TVECMI.

4. Medvedeva N. V. Construction of minimal (with respect to inclusion) per-fect ciphers / N. V. Medvedeva, S. S. Titov // International Scientific and Practical Conference "Railway Transport and Technologies" (RTT-2021): Collection of conference materials. Volume 2624, Ekaterinburg, November 24–25, 2021. Vol. 2624, Issue 1. – USA: AIP PUBLISHING, 2023. – P. 050018. – DOI 10.1063/5.0132399. – EDN LANBAV.

5. Medvedeva N. V. Construction of Absolutely Failure-free Minimal Data Transmission Systems on Railway Transport / N. V. Medvedeva, S. Titov // Trans-port: logistics, construction, Maintenance, management: Proceedings of the 1st Inter-national Scientific and Practical Conference on Transport: Logistics, Construction, Maintenance, Management, Yekaterinburg, March 17–30, 2022. – Portugal: SciTe-Press Digital Library (Science and Technology Publications, Lda), 2023. – P. 73–77. – EDN PHDLQE.

6. Медведева Н. В. Применение многократно стохастических матриц для построения абсолютно стойких систем передачи данных / Н. В. Медведева, С. С. Титов // Вестник УрГУПС. – 2023. – № 3(59). – С. 4–13. – DOI 10.20291/2079-0392-2023-3-4-13. – EDN GWKLMZ.

7. Медведева, Н. В. О совместных распределениях случайных величин при построении стойких кодов / Н. В. Медведева, С. С. Титов // Железнодорожный транспорт и технологии: сборник трудов Всероссийской научно-практической конференции с международным участием, Екатеринбург, 27–28 ноября 2024 года. – Екатеринбург: УрГУПС, 2025. – С. 410–413. – EDN XAWWUN.

8. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М.: Гелиос АРВ, 2001. – 479 с.

9. Зубов А.Ю. Совершенные шифры. М.: Гелиос АРВ, 2003. – 160 с.

References

1. Shennon K. Teoriya svyazi v sekretnykh sistemakh // Raboty po teorii in-formatsii i kibernetiki. M.: Nauka, 1963. – S. 333–402.

2. Medvedeva N.V. Ob analogakh teoremy Shennona dlya sovershennykh shifrov // CEUR Workshop Proceedings. 2016. T. 1825. S. 232–239. ISSN 1613–0073.

3. Medvedeva N. V. K razrabotke absolyutno stoykikh sistem peredachi dan-nykh / N. V. Medvedeva, S. S. Titov // Vestnik UrGUPS. – 2019. – № 2(42). – S. 34–43. – DOI 10.20291/2079-0392-2019-2-34-43. – EDN TVECMI.

4. Medvedeva N. V. Construction of minimal (with respect to inclusion) per-fect ciphers / N. V. Medvedeva, S. S. Titov // International Scientific and Practical Conference "Railway Transport and Technologies" (RTT-2021): Collection of conference materials. Volume 2624, Ekaterinburg, November 24–25, 2021. Vol. 2624, Issue 1. – USA: AIP PUBLISHING, 2023. – P. 050018. – DOI 10.1063/5.0132399. – EDN LANBAV.

5. Medvedeva N. V. Construction of Absolutely Failure-free Minimal Data Transmission Systems on Railway Transport / N. V. Medvedeva, S. Titov // Trans-port: logistics, construction, Maintenance, management: Proceedings of the 1st Inter-national Scientific and Practical Conference on Transport: Logistics, Construction, Maintenance, Management, Yekaterinburg, March 17–30, 2022. – Portugal: SciTe-Press Digital Library (Science and Technology Publications, Lda), 2023. – P. 73–77. – EDN PHDLQE.

6. Medvedeva N. V. Primeneniye mnogokratno stokhasticheskikh matrits dlya postroyeniya absolyutno stoykikh sistem peredachi dannykh / N. V. Medvede-va, S. S. Titov // Vestnik UrGUPS. – 2023. – № 3(59). – S. 4–13. – DOI 10.20291/2079-0392-2023-3-4-13. – EDN GWKLMZ.

7. Medvedeva, N. V. O sovmestnykh raspredeleniyakh sluchaynykh velichin pri postroyenii stoykikh kodov / N. V. Medvedeva, S. S. Titov // Zheleznodo-rozhnyy transport i tekhnologii: sbornik trudov Vserosciyskoy nauchno-prakticheskoy konferentsii s mezhdunarodnym uchastiyem, Yekaterinburg, 27–28 noyabrya 2024 goda. – Yekaterinburg: UrGUPS, 2025. – S. 410–413. – EDN XAWWUN.

8. Alferov A.P., Zubov A.YU., Kuz'min A.S., Cheremushkin A.V. Osnovy kriptografii. M.: Gelios ARV, 2001. – 479 s.

9. Zubov A.YU. Sovershennyye shifry. M.: Gelios ARV, 2003. – 160 s.

МЕДВЕДЕВА Наталья Валерьевна, кандидат физико-математических наук, доцент, доцент кафедры «Естественнонаучные дисциплины» ФГБОУ ВО «Уральский государственный университет путей сообщения». 650034, г. Екатеринбург, ул. Колмогорова, 66. E-mail: medvedeva_n_v@mail.ru.

ТИТОВ Сергей Сергеевич, доктор физико-математических наук, про-фессор, профессор кафедры «Естественнонаучные дисциплины» ФГБОУ ВО «Уральский государственный университет путей сообщения». 650034, г. Екатеринбург, ул. Колмогорова, 66. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: stitov@usaaa.ru.

MEDVEDEVA Natalya Valeryevna, Candidate of Physico-Mathematical Sciences, Associate Professor, Associate Professor of the Department of Natural Sciences of the Federal State Budgetary Educational Institution of Higher Education «Ural State University of Railway Transport». 620034, Yekaterinburg, str. Kolmogorova, 66. E-mail: medvedeva_n_v@mail.ru.

TITOV Sergey Sergeevich, Doctor of Physico-Mathematical Sciences, Pro-fessor, Professor of the Department of Natural Sciences of the Federal State Budgetary Educational Institution of Higher Education «Ural State University of Railway Transport». 620034, Yekaterinburg, str. Kolmogorova, 66. E-mail: stitov@usaaa.ru.