

DOI 10.23859/1994-0637-2017-6-81-1
УДК 621.391

© **Баринов А.Ю., Асеев А.Ю., 2017**

Баринов Антон Юрьевич

Научный сотрудник,
Череповецкое высшее военное инженерное
училище радиоэлектроники
(Череповец, Россия)
E-mail: aybarinov@mail.ru

Barinov Anton Yurievich

Research associate, Cherepovets Higher
Military Engineering School of Radio
Electronics
(Cherepovets, Russia)
E-mail: aybarinov@mail.ru

Асеев Алексей Юрьевич

Кандидат технических наук, доцент
Череповецкий государственный университет
(Череповец, Россия)
E-mail: passionarii@rambler.ru

Aseev Aleksey Yurievich

PhD in Technical Sciences, Associate
Professor, Cherepovets State University
(Cherepovets, Russia)
E-mail: passionarii@rambler.ru

**МОДИФИЦИРОВАННАЯ
МАТЕМАТИЧЕСКАЯ МОДЕЛЬ
СИСТЕМЫ ГЕНЕРИРОВАНИЯ
ПЕРЕМЕЖЕННОЙ ДИСКРЕТНОЙ
ПОСЛЕДОВАТЕЛЬНОСТИ
ТУРБОПОДОБНОГО КОДА**

**MODIFIED MATHEMATICAL
MODEL OF SYSTEM
GENERATING TURBO-LIKE
INTERLEAVED DISCRETE CODE
SEQUENCE**

Аннотация. В статье приводится описание модифицированной математической модели системы, в рамках которой в условиях априорной неопределенности должен быть идентифицирован компонентный перемежитель турбоподобного кода (ТК). Предложенная модель отличается тем, что описывает структуру перемеженной дискретной последовательности в компактном виде с учетом перестановок перемежителя. Данная особенность позволяет разбить задачу идентификации перемежителей ТК на подзадачи малого размера. Разработаны свойства модифицированной математической модели, применение которых позволяет осуществлять правильную идентификацию перемежителей ТК в условиях помех.

Abstract. The article describes modified mathematical model of the system identifying turbo-like code component interleaver in a priory uncertainty context. Suggested model differs as it describes interleaved discrete sequence structure in compact form taking into account interleaver permutations. This feature allows to separate turbo-like interleaver identification task into smaller subtasks. The modified mathematical model properties are significant for correct identification of turbo-like code interleavers in the presence of high noise.

Ключевые слова: турбоподобный код, турбокод, перемежитель, генерирование, перфорация, идентификация, помехи

Keywords: turbo-like code, turbocode, interleaver, generation, puncturing, identification, noise

Введение

В дискретных последовательностях (ДП) современных систем спутниковой связи (ССС) активно применяется помехоустойчивое кодирование. Это напрямую связано с высокой системной ценностью энергетического выигрыша от кодирования, за счет

которого можно уменьшить размеры антенн, снизить энергопотребление, повысить надежность связи и т.д.

Благодаря своей высокой исправляющей способности, широкое распространение в ССС получили турбоподобные коды (ТК) [7], которые можно разделить на три основных класса: сверточные турбокоды (ТКС) [10]; блочные турбокоды [12]; аккумуляторные низкоплотностные помехоустойчивые коды (АНК) [11]. Отличительным признаком ТК является то, что они построены на основе нескольких относительно простых компонентных кодеров, соединенных через перемежители, а также применение итеративного декодирования.

Особенностью обработки ДП с ТК (ДПТК) является априорная неопределенность относительно характеристик ТК. Следовательно, задача анализа ДПТК заключается в выявлении характеристик компонентных кодеров и перемежителя, т.е. вектора перестановок $\Pi_{[K]} = [\pi(1), \pi(2), \dots, \pi(K)]$.

Однако если вопросам анализа компонентных кодов посвящено много работ [1], [9], то анализ перемежителей для ТК в условиях помех в канале связи представляет собой сложную и до конца нерешенную задачу. Следовательно, неизвестный перемежитель является критическим компонентом, из-за которого ТК в условиях помех не выявляется. При этом наибольшую трудность представляет анализ перемежителей для ТКС и АНК, поскольку именно в данных ТК используют псевдослучайные перемежители [7], где может быть использован почти любой из $K!$ вариантов перестановок. K – размер информационного кадра ТК, который имеет величину до нескольких десятков тысяч бит.

Анализ объективных научных предпосылок к решению данной задачи позволил выдвинуть предположение о возможности повышения вероятности правильного выявления перемежителей ТК путем исследования наблюдаемых ДП на входе и выходе кодера ТК. Решение задачи таким способом составляет предмет теории идентификации систем [6]. Согласно данной теории, в первую очередь, необходимо разработать математическую модель системы, в рамках которой должен быть найден вектор перестановок компонентного перемежителя ТК.

Цель работы – систематизировать и обобщить результаты, полученные в [3], [5], для разработки модифицированной математической модели системы генерирования перемеженной ДПТК.

Основная часть

Математическая модель разрабатывалась для ТКС и АНК, так как их перемежители представляют наибольшую трудность для анализа. В работе рассматриваются систематические ТК, т.е. в условиях, когда имеется доступ к искаженным канальными ошибками ДП на входе (систематическая (информационная) часть) кодера и выходе (проверочная часть) кодера.

Общий вид исследуемой системы изображен на рис. 1, где СК – сверточный кодер, РСК – рекурсивный сверточный кодер, перфоратор означает удаление определенных бит ДП.

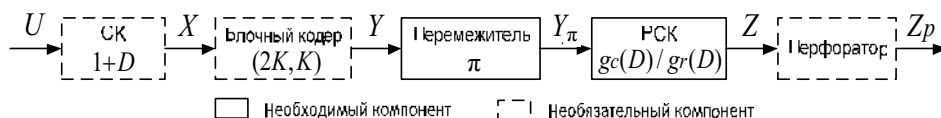


Рис. 1. Обобщенная система генерирования перемеженной ДПТК

Все операции в данной системе выполняются в поле $GF(2)$ над двоичными данными «логическими нулями и единицами» («лог. 0» и «лог. 1»), объединенными в блоки фиксированной длины, т.е. ДП U , X , Y , Y_π , Z , Z_p (см. рис. 1) представляют собой блоки из соответствующих бит. Например, блок информационной ДП на входе ТК имеет вид $U_{[K]} = [u_1, u_2, \dots, u_K]$.

В настоящей работе учитываются наиболее важные характеристики системы на рис. 1, а также тот факт, что на практике для повышения скорости передачи часто удаляют каждый второй бит проверочной ДП. Тогда исследуемая система примет вид, изображенный на рис. 2, где кодер РСК представлен как регистр сдвига с прямыми и обратными связями и характеризуется полиномом

$$g_c(D)/g_r(D) = (g_{c_0} + g_{c_1}D + \dots + g_{c_m}D^m)/(g_{r_0} + g_{r_1}D + \dots + g_{r_m}D^m), \quad (1)$$

где m – регистровая память РСК (для ТК характерно значение $m \leq 4$ [13]); $g_{c_0}, g_{c_1}, \dots, g_{c_m}$ и $g_{r_0} = 1, g_{r_1}, \dots, g_{r_m}$ – коэффициенты, соответствующие отводам регистра сдвига кодера РСК, т.е. в том месте регистра сдвига, где имеется отвод, коэффициенту присваивается значение единицы, а там, где отвод отсутствует, коэффициенту присваивается значение нуля.

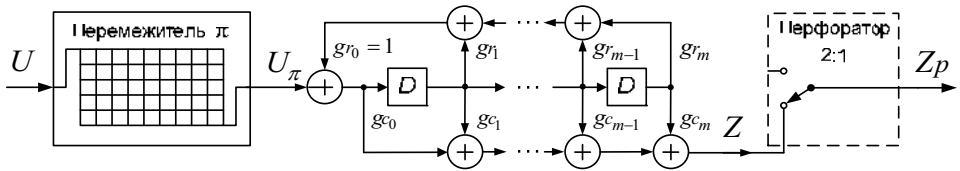


Рис. 2. Система генерирования перемеженной ДПТК

Из структуры системы, приведенной на рис. 2, можно сделать вывод о том, что коэффициент $g_{r_0} = 1$ и коэффициент $g_{c_0} = 1$.

В работе используется следующее обозначение кодера РСК (на рис. 2): $(n_c, g_c(D)_8, g_r(D)_8)$, где $n_c = m + 1$ – кодовое ограничение. Двоичные коэффициенты записываются в ряд согласно порядку $g_{c_0}, g_{c_1}, \dots, g_{c_m}$ и $g_{r_0}, g_{r_1}, \dots, g_{r_m}$, далее конвертируются в восьмеричное представление последовательными триадами, начиная с крайнего правого бита (например, 11101_2 представится, как $011\ 101$ и конвертируется в 35_8).

Известная математическая модель исследуемой системы представляет собой следующую дискретную свертку [13]

$$z_i = \sum_{q=0}^{i-1} g_q u_{\pi(i-q)}, \quad i = 1(1)K, \quad (2)$$

и при наличии компоненты перфорации имеет вид

$$z_{p_{i/2}} = \sum_{q=0}^{i-1} g_q u_{\pi(i-q)}, \quad i = 2(2)K, \quad (3)$$

где K – размер блока ДП на входе системы, $g_0, g_1, \dots, g_{K-1}$ – импульсная характеристика кодера РСК $g_c(D)/g_r(D)$.

Бесконечная импульсная характеристика РСК означает, что при размере входного блока $K = 10^3 \div 10^5$, каждый из проверочных бит z_i в (2) и $z_{p_{i/2}}$ в (3) может зависеть от нескольких (десятков) тысяч входных бит.

В результате исследований выяснено, что приведение зависимостей (2), (3) к модифицированному компактному виду является предпосылкой для устранения эффекта размножения ошибок при идентификации перемежителя.

Для этого предлагается выполнять кодирование блоков проверочных бит на выходе системы при помощи полинома обратной связи РСК вида $g_r(D)$.

Тогда кодирование блока $Z_{[K]} = [z_1, z_2, \dots, z_K]$ кодером $g_r(D)$ приводит к блоку $Z_{c_{[K]}} = [z_{c_1}, z_{c_2}, \dots, z_{c_K}]$ и осуществляется как

$$z_{c_i} = \sum_{q=0}^m g_{r_q} z_{i-q}, \quad i = 1(1)K. \quad (4)$$

С другой стороны, каждый бит блока $Z_{c_{[K]}}$ можно представить в виде

$$z_{c_i} = \sum_{q=0}^m g_{c_q} u_{\pi(i-q)}, \quad i = 1(1)K. \quad (5)$$

Уравнение (5) представляет собой модифицированную математическую модель исследуемой системы, где, в отличие от (2), каждый выходной бит является суммой нескольких ($\leq m$) входных бит, независимо от длины K .

В ходе наблюдений можно получить выборку из M блоков $U_{[K]}$ (взятых с систематического выхода ТК) и соответствующих им блоков $Z_{c_{[K]}}$, т.е. две матрицы $U_{[M,K]}$ и $Z_{c_{[M,K]}}$. Тогда, если в (5) перейти от бит к столбцам матриц и учесть, что $g_{c_0} = 1$, то справедливо свойство модели

$$U_{\pi(i)}^{sim} = Z_{c_i} + \sum_{q=1}^m U_{\pi(i-q)} g_{c_q}, \quad i = 1(1)K, \quad (6)$$

где $U_{\pi(i)}$ – $\pi(i)$ -й столбец матрицы $U_{[M,K]}$; Z_{c_i} – i -й столбец матрицы $Z_{c_{[M,K]}}$, знак *sim* (сокр. от simulate) здесь и далее по тексту является обозначением моделирования.

В результате детального анализа (см. рис. 3) матриц из уравнения (8) получено, что каждый бит блока $Z_{pc_{\lfloor K/2 \rfloor}}$ можно представить в виде

$$z_{pc_{i/2}} = \sum_{q=0}^{2m} g_{p_q} u_{\pi(i-q)}, \quad i=2(2)K, \quad (9)$$

где $g_{p_0}, \dots, g_{p_{2m}}$ – коэффициенты, вычисляемые следующим образом

$$g_{p_q} = \sum_{j=0}^m g_{r_j} g_{q-2j}, \quad q=0(1)2m, \quad (10)$$

где $g_0 - g_{2m}$ первые $2m+1$ бит импульсной характеристики РСК вида $g_c(D) / g_r(D)$.

Уравнения (9) и (10) представляют собой модифицированную модель исследуемой системы для случая ТК с перфорацией, где, в отличие от (3), каждый выходной бит является суммой нескольких ($\leq 2m$) входных бит, независимо от длины K .

Переход от бит к столбцам высоты M в (9), а также анализ распределений коэффициентов $g_{p_0}, \dots, g_{p_{2m}}$ позволили выявить свойства данной модифицированной модели (в виде $(n_c, g_c(D)_8, g_r(D)_8)$ приведены примеры характерных РСК):

$$1) \quad g_{p_1} = 1: (2, 1, 2), (3, 5, 7), (4, 13, 15), (5, 21, 37), (5, 23, 35)$$

$$(U_{\pi(i)} + U_{\pi(i-1)})^{sim} = Z_{pc_{i/2}} + \sum_{q=2}^{2m} U_{\pi(i-q)} g_{p_q},$$

$$2) \quad g_{p_1} = 0, \quad g_{p_3} = 1: (4, 12, 13), (4, 15, 17), (5, 21, 27), (5, 31, 33)$$

$$(U_{\pi(i)} + U_{\pi(i-3)})^{sim} = Z_{pc_{i/2}} + U_{\pi(i-2)} g_{p_2} + \sum_{q=4}^{2m} U_{\pi(i-q)} g_{p_q},$$

$$3) \quad g_{p_1} = g_{p_3} = 0, \quad g_{p_5} = 1: (4, 11, 13), (5, 23, 27), (5, 33, 35), (5, 36, 37)$$

$$(U_{\pi(i)} + U_{\pi(i-5)})^{sim} = Z_{pc_{i/2}} + U_{\pi(i-2)} g_{p_2} + U_{\pi(i-4)} g_{p_4} + \sum_{q=6}^{2m} U_{\pi(i-q)} g_{p_q}, \quad (11)$$

$$4) \quad g_{p_1} = g_{p_3} = g_{p_5} = 0, \quad g_{p_7} = 1: (5, 22, 23), (5, 26, 27), (5, 31, 37), (5, 32, 35)$$

$$(U_{\pi(i)} + U_{\pi(i-7)})^{sim} = Z_{pc_{i/2}} + U_{\pi(i-2)} g_{p_2} + U_{\pi(i-4)} g_{p_4} + U_{\pi(i-6)} g_{p_6} + \sum_{q=8}^{2m} U_{\pi(i-q)} g_{p_q},$$

...

$$m+1) \quad g_{p_1} = g_{p_3} = g_{p_5} = g_{p_7} = \dots = g_{p_{2m-1}} = 0: (3, 4, 5), (4, 14, 17), (5, 20, 21), (5, 21, 25)$$

$$U_{\pi(i)}^{sim} = Z_{pc_{i/2}} + \sum_{q=1}^{2m} U_{\pi(i-2q)} g_{p_{2q}},$$

где $i = 2(2)K$.

Исследования показали, что свойства (11) симметричны относительно прямых и обратных связей кодера РСК, например, первое свойство справедливо как для РСК (5, 23, 35) так и для РСК (5, 35, 23), третье свойство справедливо для РСК (4, 11, 13) и для РСК (4, 13, 11).

Использование свойств (11) позволяет поэтапно построить искомый вектор перестановок перемежителя. Эффект от использования выявленных свойств основан на снижении степени влияния ошибок на результаты идентификации перемежителя, по сравнению с алгебраическим методом, основанным на решении системы линейных уравнений по Гауссу, и обеспечивается фиксированием числа данных, влияющих на идентификацию каждой перестановки.

В качестве информативного показателя идентификации перестановок перемежителя ТК выбран вес Хэмминга w_H столбца, получаемого как результат сложения столбца sim (т.е. смоделирован по свойствам модели) и столбца, получаемого на основе информационной матрицы $U_{[M,K]}$.

Тогда показатель идентификации перестановки $\pi(i) = j$ для ТК имеет вид

$$L_{ij} = w_H(U_{\pi(i)}^{sim} + U_j), \quad i = 1(1)K; \quad j = 1(1)K. \quad (12)$$

Показатель идентификации пары перестановок $\pi(i-1) = j_1, \pi(i) = j_2$ для ТК с перфорацией (вариант для РСК, попадающего под первое свойство из (11)) будет таким

$$L_{i/2_j} = w_H((U_{\pi(i)} + U_{\pi(i-1)})^{sim} + U_{j_1} + U_{j_2}), \quad (13)$$

где $i = 2(2)K$, $j_1 = 1(1)K - 1$, $j_2 = 2(1)K$, $j_1 < j_2$.

В диапазонах УВЧ и СВЧ, в которых функционируют рассматриваемые в работе ССС, широко используется модель канала с аддитивным белым гауссовским шумом (АБГШ). В связи с этим, анализируемые ДП рассматриваются в условиях, когда их биты искажены с вероятностью p_e , согласно биномиальному закону распределения. Тогда критерий идентификации будет заключаться в сравнении показателя идентификации с порогом T :

$$L = f(M, p_e) \leq T, \quad (14)$$

где L – общее обозначение для показателей из (12) и (13).

При этом необходимо определить значение выборки M и порога T .

Процедуру принятия решения об идентификации перестановок предлагается реализовать на основе гипотез H_1 – объект в состоянии S_1 и H_0 – объект в состоянии S_0 .

В условиях АБГШ вероятность ложной тревоги определена как

$$P_{10} = \sum_{i=0}^T C_M^i P_u^i (1 - P_u)^{M-i}, \quad (15)$$

где P_u – вероятность появления «лог. 1» в элементе столбца-результата, вес которого является показателем идентификации L при S_0 , исследования [2] показали что $P_u \approx 0,5$.

Вместе с тем для вероятности пропуска цели P_{01} справедливо

$$P_{01} = 1 - \sum_{i=0}^T C_M^i P_e^i (1 - P_e)^{M-i}, \quad (16)$$

где P_e – вероятность появления «лог. 1» в элементе столбца-результата для подсчета показателя при S_1 , которую можно вычислить согласно уравнению

$$P_e = \frac{1 - (1 - 2P_e)^t}{2},$$

где t – количество столбцов матриц $U_{[M,K]}$, $Z_{[M,K]}$ ($Z_{p[M,K/2]}$), участвующих в формировании столбца-результата, вес которого является показателем идентификации L .

Результирующие вероятности ложной тревоги и пропуска цели при идентификации перемежителя определены по правилам, применимым к серии независимых испытаний

$$P_{10\Sigma} = 1 - (1 - P_{10})^B, \quad P_{01\Sigma} = 1 - (1 - P_{01})^D,$$

где $B = K^2$, $D = K$ в случае ТК, $B = KC_K^2$, $D = K/2$ для случая ТК с перфорацией.

С учетом требований к значениям $P_{10\Sigma}$ и $P_{01\Sigma}$, (15) и (16) объединены в систему неравенств и найдены минимальные подходящие значения выборки M и порога T .

Проведенные вычислительные эксперименты показали, что в худшем случае (наличие перфорации и $t = 13$) для обеспечения высокой вероятности правильной идентификации $P_{id} \geq 0,999$ всех перестановок перемежителя ТК требуются сравнительно небольшие величины выборки. При вероятности битовой ошибки $p_e = 0,01$ для правильной идентификации перемежителя любого из рассматриваемых ТК (при $m \leq 4$) с длиной входного кадра K до 65536 бит, требуется выборка $M \leq 320$ кадров и порог $T \leq 71$. С данной выборкой, для отдельных случаев ТК, возможна правильная идентификация перемежителя, при уровне $p_e = 0,05$.

Выводы

Таким образом, предложенная модифицированная математическая модель системы генерирования перемеженной ДПТК в виде совокупности уравнений (5), (9), (10) позволила выявить новые информативные признаки (6), (11–13) и обусловила разработку нового метода и алгоритмов идентификации перемежителей ТК в условиях помех [2]–[4].

Указанная модель путем элементарных преобразований может быть скорректирована для описания любого ТК, соответствующего обобщенной системе генерирования перемеженной ДПТК.

Литература

1. Балунин Е.И., Баринов А.Ю. и др. Обнаружение и распознавание сигнально-кодовых конструкций. Методы и алгоритмы. М.: Радиотехника, 2013. 96 с.
2. Баринов А.Ю. Алгоритм идентификации помехоустойчивых кодов повторения-накопления // Успехи современной радиоэлектроники. 2017. № 9. С. 26–30.
3. Баринов А.Ю. Методы анализа турбоподобных кодов с учетом идентификации их компонентных перемежителей // Научные технологии. 2016. № 12. С. 4–11.
4. Баринов А.Ю., Балунин Е.И. Свидетельство о государственной регистрации программы для ЭВМ № 2017615089, опубли. 03.05.2017. Программа идентификации компонентных перемежителей турбо-подобных кодов.
5. Баринов А.Ю., Балунин Е.И., Ратушин А.П. Свойства модели дискретных последовательностей турбоподобных кодов // Антенны. 2014. № 11. С. 55–60.
6. Льюнг Л. Идентификация систем. Теория для пользователя. М.: Наука, 1991. 432 с.
7. Abbasfar A., Turbo-like Codes. Design for high speed decoding, Springer, Dordrecht, The Netherlands, 2007. 94 p.
8. Barbier J. Reconstruction of turbo-code encoders // SPIE Defense and Security Symp., Space Communications Technologies Conf., 2005, pp. 463–473.
9. Barbier J., Filiol E., Overview of Turbo-Code Reconstruction Techniques // IACR Cryptology ePrint Archive. 2009. Vol. 2009. Pp. 1–5.
10. Berrou C., Glavieux A., Thitimajshima P., Near Shannon limit error-correcting coding and decoding: Turbo codes // Proc. IEEE Int. Conf. on Communications, Geneva, Switzerland. 1993. Pp. 1064–1070.
11. Halford T.R. et al., The F-LDPC family: High-performance flexible modern codes for flexible radio // Proc. ISSSTA 2008, Bologna, Italy, 2008. Pp. 376–380.
12. Press Release, AHA announces Turbo Product Code Forward Error Correction Technology, 1998.
13. Shu Lin, Costello D., Error control coding, Pearson Prentice Hall, New Jersey, USA, 2004. 1260 p.

References

1. Balunin E.I., Barinov A.Y. et al. *Obnaruzhenie i raspoznavanie signal'no-kodovykh konstruktsii. Metody i algoritmy* [Detection and identification of the signal-code constructions. Methods and algorithms]. Moscow: Radiotekhnika, 2013. 96 p.
2. Barinov A.Y. Algorithm identifikatsii pomexoustoichivyykh kodov povtoreniia-nakopleniia [Algorithm of repeat-accumulate codes identification]. *Uspehi sovremennoi radioelektroniki* [Achievements of Modern Radioelectronics], 2017, no. 9, pp. 26–30.
3. Barinov A.Y. Metody analiza turbopodobnykh kodov s uchetom identifikatsii ih komponentnykh peremezhitel'ei [Methods of turbo-like codes analysis in view of their component interleavers identification]. *Nauchnye tekhnologii* [Science Intensive Technologies], 2016, no. 12, pp. 4–11.
4. Barinov A.Y., Balunin E.I. *Svidetel'stvo o gosud. registratsii programmy dl'a JeVM* [Certificate on the state registration of the computer program] № 2017615089, publication 03.05.2017, Programma identifikatsii komponentnykh peremezhitel'ei turbo-podobnykh kodov [Program for identification of turbo-like codes component interleavers].
5. Barinov A.Y., Balunin E.I., Ratushin A.P. Svoistva modeli diskretnykh posledovatel'nostei turbopodobnykh kodov [The properties of model of turbo-like codes discrete sequences]. *Antennas* [Antennas], 2014, no. 11, pp. 55–60.
6. L'jung L. *Identifikatsiia system. Teoriia dl'a pol'zovatel'ia* [System identification: theory for the user]. Moscow: Nauka, 1991. 432 p.

7. Abbasfar A., Turbo-like Codes. *Design for high speed decoding*, Springer, Dordrecht, The Netherlands, 2007. 94 p.
 8. Barbier J. Reconstruction of turbo-code encoders. *SPIE Defense and Security Symp., Space Communications Technologies Conf.*, 2005, pp. 463–473.
 9. Barbier J., Filiol E., Overview of Turbo-Code Reconstruction Techniques. *IACR Cryptology ePrint Archive*, 2009, vol. 2009, pp. 1–5.
 10. Berrou C., Glavieux A., Thitimajshima P. Near Shannon limit error-correcting coding and decoding: Turbo codes. *Proc. IEEE Int. Conf. on Communications*, Geneva, Switzerland, 1993, pp. 1064–1070.
 11. Halford T.R. et al. The F-LDPC family: High-performance flexible modern codes for flexible radio. *Proc. ISSSTA 2008*, Bologna, Italy, 2008, pp. 376–380.
 12. *Press Release, AHA announces Turbo Product Code Forward Error Correction Technology*, 1998.
 13. Shu Lin, Costello D. *Error control coding*, Pearson Prentice Hall, New Jersey, USA, 2004. 1260 p.
-

Баринов А.Ю., Асеев А.Ю. Модифицированная математическая модель системы генерирования перемеженной дискретной последовательности турбоподобного кода // Вестник Череповецкого государственного университета. 2017. №6 (81). С. 9–18.

For citation: Barinov A.Y., Aseev A.Y. Modified mathematical model of system generating turbo-like interleaved discrete code sequence. *Bulletin of the Cherepovets State University*, 2017, no. 6 (81), pp. 9–18.