

УДК 004.056.5

doi:10.20998/2413-4295.2022.01.06

PUNCTURED NCC CODES FOR INFORMATION PROTECTION IN INFORMATION AND MEASUREMENT SYSTEMS

V. KRYLOVA, E. TVERYTNYKOVA*, O. VASYLCHENKOV, T. KOLISNYK

Department of of information and measuring technologies and systems, National Technical University "Kharkiv Polytechnic Institute", Kharkiv, UKRAINE

* e-mail: tveekhpi@ukr.net

ABSTRACT During development and design of information-measuring systems, enabling to carry out collection, processing and transmission of information, one of the main problems is the choice of effective methods of information protection against defects in noisy communication channels. Effective use of frequency-time resources of information communication channels, as the most valuable part of the information transmission system, is the key to provide reliable delivery of transmitted messages. One of effective directions of reliability increase and information transfer reliability in information-measuring communication networks is implementation of methods and algorithms of noise-resistant coding, providing for detection and coping with errors, arising due to interferences in the communication channel. In this case, the choice in favor of one or another coding method depends on the information characteristics of the data channel. Parameters of the noise coder must be coordinated with the source of the message, the communication channel, as well as the requirements for the reliability of bringing information to the recipient. The problem of obtaining a wide range of codec parameters with simultaneous preservation of the unified macrostructure of the codec in communication systems causes the need for research on the development of adaptive algorithms for error information protection. In the article the research results of the characteristics of variable rate slot convolutional codes for adaptive coding/decoding in information-measuring systems of information transmission are proposed. Consequently, when creating communication networks, there is no need to use a large number of different codecs, even with completely different requirements to the code rate, channel rate and gain due to coding. In addition, there is a real opportunity to create terminal equipment, working on unified algorithms of protection against errors and access.

Keywords: information protection; information systems; noise-resistant coding; convolutional codes; punctured codes

ПЕРФОРОВАНІ НСС КОДИ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ СИСТЕМАХ

В. А. КРИЛОВА, Е. Е. ТВЕРИТНИКОВА*, О. Г. ВАСИЛЬЧЕНКОВ, Т. П. КОЛІСНИК

Кафедра інформаційно-вимірювальних технологій і систем НТУ «ХПІ», Харків, УКРАЇНА

АНОТАЦІЯ При розробленні та проектуванні інформаційно-вимірювальних систем, які виконують збір, оброблення та передавання даних, одним із головних завдань є вибір ефективних методів захисту інформації від помилок у зашумлених каналах зв'язку. Ефективне використання частотно-часових ресурсів інформаційних каналів зв'язку, є ключовим при забезпеченні достовірної доставки повідомлень, що передаються. Одним з перспективних напрямів підвищення надійності та достовірності передачі інформації в інформаційно-вимірювальних мережах зв'язку є використання методів та алгоритмів завадостійкого кодування, що дозволяють виявити та справляти помилки, що виникають внаслідок дії перешкод у каналі зв'язку. При цьому вибір на користь того чи іншого методу кодування залежить від інформаційних параметрів каналу передачі даних. Параметри перешкодостійкого кодера повинні бути узгоджені з джерелом повідомлення, каналом зв'язку, а також вимогами до достовірності доведення інформації до одержувача. Проблема отримання широкого набору параметрів кодових співвідношень при одночасному збереженні єдиної макроструктури кодера в системах зв'язку викликає необхідність проведення досліджень розробки адаптивних алгоритмів захисту інформації від помилок. У статті запропоновано результати дослідження характеристик гніздових згорткових кодів із змінною швидкістю при адаптивному кодуванні/декодуванні в інформаційно-вимірювальних системах передавання інформації. Отже, при створенні мереж зв'язку немає необхідності у використанні великої кількості різних кодеків навіть при абсолютно різних вимогах швидкості передачі коду, каналної швидкості і виграшу за рахунок кодування. Крім того, виникає реальна можливість створення кінцевого обладнання, що працює на уніфікованих алгоритмах захисту від помилок та доступу.

Ключеві слова: захист інформації; інформаційні системи; завадостійке кодування; згорткові коди; перфоровані коди

Introduction

The relevance of the chosen theme strengthens the fact that the process of accumulation, storage and transmission of data by means of information-measuring systems is quite confidential. This requires certain measures to preserve the integrity of information and reliable protection. Taking this into account, the leading

place among methods and means of counteracting of information infringement threats belongs to noise-resistant coding. Often information-measuring systems are supplied with a common module that performs information security functions. But this introduces certain problems, when a separate block of information-measuring system has no its own integrated protection system. This requires the creation of new approaches in

the development and operation of modern measuring equipment.

The relevance of the chosen theme strengthens the fact that the process of accumulation, storage and transmission of data by means of information-measuring systems is quite confidential. This requires certain measures to preserve the integrity of information and reliable protection. Taking this into account, the leading place among methods and means of counteracting of information infringement threats belongs to noise-resistant coding. Often information-measuring systems are supplied with a common module that performs information security functions. But this introduces certain problems, when a separate block of information-measuring system has no its own integrated protection system. This requires the creation of new approaches in the development and operation of modern measuring equipment.

Effectiveness of using digital communication channels in information-measuring systems for information processing and transmission under conditions of natural and intentional interference is determined by the reliability of information exchange. For reliability increase and transfer reliability the methods of noise-resistant coding have wide circulation. While choosing a noise-resistant coder its parameters must be coordinated with the communication channel, as well as the requirements imposed on the reliability of bringing information to a recipient. However, it is difficult to choose in advance the code parameters, if the quality of the channel is unknown, and sometimes in general it can change during the operation of the system. Thus, the parameters of the noise-resistant code are selected on the basis of some "average" state of the communication channel, which leads to a decrease in the speed of information transmission due to the greater redundancy of the code [1–3]. This can lead to loss of communication when using codes, the parameters of which remain constant and are not designed for significant deterioration of channel quality. One of the ways to avoid this disadvantage is the use of adaptive coding systems of automatic and purposeful correction of code parameters, providing at the same time a specified probability of delivering a message at a minimum redundancy of the noise-resistant code.

Methods of noise-resistant channel coding of protected information-measuring systems are widely used. As a consequence of speed increase of information transmission is increase of interference quantity that becomes an impact for development and introduction of modern approaches to the solution of detection and correction tasks of interference [4,5]. In telecommunication and information-measuring systems with an increased noise component the noise-resistant cyclic BCH and Reed-Solomon codes are quite often used [6,7]. The application of convolutional code with punctured bits without puncturing for calculation of information symbol reliability is investigated in the paper [8].

Purpose of the work

The aim of this article is to develop and improve the unified methods and algorithms of information protection against errors in information-measuring systems, providing high reliability and speed of data transmission.

Statistical characteristics of the information state of the communication channel in adaptive coding systems are used to change the corrective capacity and redundancy of the noise-resistant code, which leads to increasing the rate of information transmission. In this case, the noise-resistant code is to operate with a simple and adaptive decoding algorithm, taking into account the changed parameters of the coder and the required reliability of the code sequence. In addition, the coder should possess the flexible structure allowing to change parameters and redundancy of a code depending on a current condition of the communication channel.

Main part

For designing adaptive coding systems among the noise-resistant codes of the greatest interest are rate-compatible, punctured convolutional codes (RCPC) and nested convolutional codes (NCC) [1]. The coding system based on RCPC and NCC codes accepts changes in two dimensions: obtaining the required value of gain at the expense of coding and providing different information and channel rate requirements.

A convolutional encoder is a shift register based device which receives k information symbols at its input during each beat that are converted into n code symbols at its output during the same beat. The parameters of the encoder are:

$R = k/n$ – code rate, m – code constraint length, G_{ij} – generating polynomials (code generators) [2]. Nested convolutional codes are a set of codes with $R=1/n$ rate, which are derived from $R = 1/n$ convolutional code rate, by finding the best generator sequences $G_{n+1}(D)$.

The convolutional code with $R = 1/n$ rate and code constraint length m consists of an m -digit shift register and two modulo-two adders.

$g_i^{(j)}$ - $j = 1, 2, 0 \leq i \leq m$ coupling coefficients belong to the finite field GF(2) of the branch elements. A convolutional encoder with m code constraint length is given by polynomials of its generators [3]:

$$G_j^m(x) = g_0^j + g_1^j(x) + g_2^j(x^2) + \dots + g_{l+1}^j(x^{l+1}) + \dots + g_m^j(x^m), \quad (1)$$

where $g_0^{(j)} = g_m^{(j)} = 1, j = 1, 2$.

Nested convolutional codes with rate $R = 1/n$ and $m-l$ code constraint length denoted as $G_{m-l}^{(j)}(x)$ for $1 \leq l \leq m-2$ and produced from $G_m^{(j)}(x)$ are defined as generators:

$$G_{m-1}^j(x) = g_0^j + g_{l+1}^j(x) + g_{l+2}^j(x^2) + \dots + g_{m-1}^j(x^{m-l-1}) + g_m^j(x^{m-l}), \quad (2)$$

where $g_0^j = g_m^j = 1, j = 1, 2$.

To decompose a basic convolutional code into a system of nested codes, there are methods for generating a code family with different values of the minimum code distance, preserving the structure of the basic convolutional code.

Table 1 shows the generator sequences of a nested convolutional code set with m code-limit length from 2 to 6 synthesized by the "forward method". For comparison purposes, the free distances and the total number of non-zero information bits per free distance length for the optimal convolutional codes are also given.

Table 1 – Nested Convolutional Codes

m	Generating polynomials	Nested codes		Optimal codes	
		d_f	N	d_f	N
6	1101101 1001111	10	36	6	36
5	1011101 1011111	8	6	5	2
4	111101 111111	6	2	4	4
3	1101 1111	6	2	3	2
2	101 111	5	1	2	1

For decoding of short convolutional codes, the most effective and easily realized way is Viterbi algorithm with the soft decision allowing to increase a gain of coding approximately up to 2 dB in comparison with the decoder with the hard decision [5].

The main problem of the high-speed convolutional codes (for example, $R = 7/8$) consists in complexity of hardware realization of Viterbi decoders for such codes. For a code with $R = k/n$ rate it is required $2^k - 1$ comparison operations. Thus, it is known, that complexity of the decoder of high-speed codes considerably decreases if the lattice structure of a code is limited by the lattice structure of a low-speed code.

Punctured convolutional codes are the class of $R = (n - 1)/n$ high-speed codes which can be decoded by means of the lattice structure of $R = 1/n$ low-speed code [1]. Decoding by Viterbi of punctured codes is carried out with the application of the same procedure, as for a base code, after achievement of synchronization of a period of punctuation and embedding of actual data in those places where initial code sequences have been erased. In adaptive coding systems the use of NCC codes with a puncturing procedure allows obtaining different gain/speed ratios.

Results and Conclusion

Punctured convolutional codes not only reduce complexity of hardware implementation of Viterbi decoder for high-speed codes, but also provide an opportunity to implement the high-speed coding system with variable rate. It is achieved by changing the way of sampling the encoder outputs. Decoding by Viterbi for punctured codes is done using the same procedure as for basic code with $R = 1/n$ rate, after reaching synchronization of the puncturing period and inserting fictive data in those places where the original code sequences have been erased.

Table 2 presents the optimal punctured codes constructed from nested convolutional codes synthesized by the "direct method" at $1/2$ rate and $2 \leq m \leq 6$ code constraint length (Table 1). The table presents data for codes with $m = 2, m = 4,$ and $m = 6$ code-limit lengths. d_f free distance of the obtained codes exceeds the free distance of the known punctured convolutional codes.

Table 2 – Optimal Punctured Codes Produced from Nested Convolutional Codes

R	$m = 2$		$m = 4$		$m = 6$	
	d_f	$N(N_a)$	d_f	$N(N_a)$	d_f	$N(N_a)$
1/2	4	1	7	4	10	36
2/3	3	1	5	29	6	3
4/6	4	66	5	90	6	6
6/9	3	2	5	79	6	9
3/4	3	15	5	6	5	42
6/8	3	30	4	57	5	74
4/5	2	1	3	14	4	12
8/10	2	2	3	7	4	18
5/6	2	2	3	10	4	92
6/7	2	5	3	39	3	5

Also, Table 2 shows the total number of non-zero bits of information in N set of all free distance lengths and the average value of this set for M puncturing period of the code:

$$N_a = \frac{N}{M}. \quad (3)$$

N_a value is an essential parameter which affects the error rate characteristic of the code. The way of code puncturing presented in the table is produced in such a way as to obtain the largest possible free distance and the smallest possible N value of the generated code.

As can be seen from the table d_f free distance is equal to 4 for the puncturing code with $R_{punct} = 4/6$ rate and $m = 2$ code restriction length, while free distance of the best-known fixed codes with $R = 2/3$ rate of the same complexity is only equal to $d_f = 3$. In addition, in several cases for codes with equal free distances, the N_a

parameter of codes with R_{punct} rate is smaller than that of codes with $R = k/n$ rate.

Figure 1 shows the bit error rate curves for punctured codes produced from nested convolutional

codes with code-limit lengths $m = 2, 4,$ and 6 and with $R = 1/2$ rate given in Table 2. This figure also shows the characteristic curve for coherent detection of unencoded BPSK modulation.

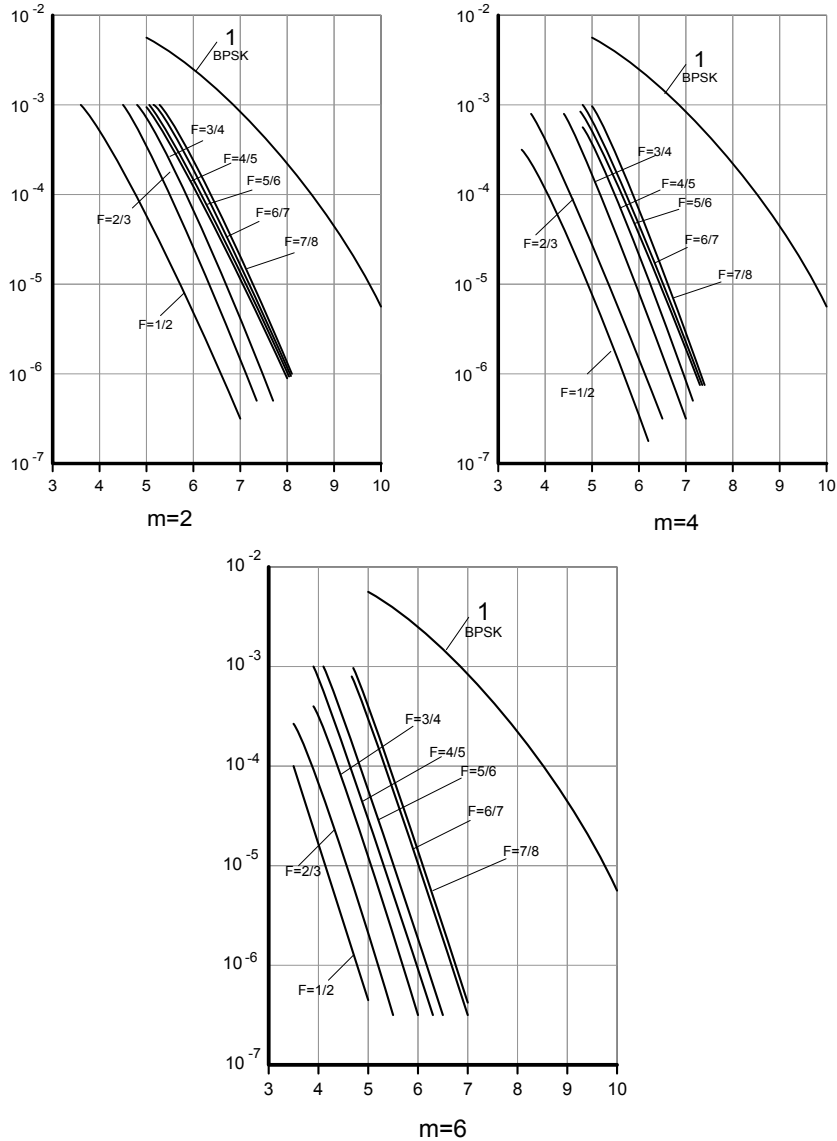


Fig. 1 – Bit Error Rate Characteristics for Punctured NCC Codes with $m = 2, 4$ and 6

In the table 3 the achievable values of gain at the expense of coding in dB depending on the rate and length of coding restriction code at $P_\sigma = 10^{-5}$ (bit error frequency) for Viterbi flexible decoder with soft solution are summarized. As expected, the gain at the expense of coding increases at the increase of decoder complexity and decreases at codes with higher rate. It is interesting to note, that if the code of small complexity $m = 2$ and rate $7/8$ is used, the gain at the expense of coding about 2 dB at $P_\sigma = 10^{-5}$ is achievable. The gain increases up to 3 or 3.5 dB if decoding rate decreases, and codes with number of memory bits $m = 4$ or 6 are used.

Table 3 – Values of coding gain (dB) at $P_\sigma = 10^{-5}$ for flexible Viterbi decoder with variable gain/rate

m	$R=7/8$	$R=6/7$	$R=5/6$	$R=4/5$	$R=3/4$	$R=2/3$	$R=1/2$
2	2,2	2,3	2,4	2,5	2,0	3,1	3,7
4	3,0	3,1	3,2	3,4	3,7	4,0	4,6
6	3,4	3,5	3,9	4,2	4,5	5,0	5,4

Conclusions

Using in communication channels the adaptive coding based on synthesis of a nested convolutional codes

family with puncturing mode, it is possible to obtain different values of the coding gain, as well as different values of the code rate and channel rate. Due to the specified properties, the adaptive codec can be used both in systems for transmitting information with direct error correction, and in systems adaptable to the communication channel state. Consequently, when creating communication networks, there is no need to use a large number of different codecs, even with completely different requirements to the code rate, channel rate and gain due to coding. In addition, there is a real opportunity to create terminal equipment, working on unified algorithms of protection against errors and access.

Список літератури

1. Cherubini G., Benvenuto N. Cherubini G. *Algorithms for communications systems and their applications*. Chichester: John Wiley & Sons, 2003. 1285 p.
2. Dieterich H. *Partitioning of Convolutional Codes and Applications*. Fortschritt-Bericht, VDI R. 10, 2000.
3. Jordan R., Johannesson R., Bossert M. On Nested Convolutional Codes and their application to woven codes. *IEEE Trans on Inform Theory*. 2004. Vol. 50, is. 2. P. 380–384.
4. Василенко В. С., Чунарьов А. В., Чунарьова А. В. Оцінка ефективності методів кодування при забезпеченні цілісності інформації в сучасних ІКСМ. *Захист інформації*. 2012. № 3. С. 46–50.
5. Гопаєнко А. В., Куц Ю. В., Монченко Е. В. Метод скритої передачі даних в комп'ютеризованих інформаційно-вимірних системах. *Захист інформації*. 2011. № 2. С. 5–9.
6. Krylova V. A., Tverytnykova E. E., Vasylychenkov O. G., Kolisnyk T. P. Modified algorithm for searching the roots of the error locators polynomial while decoding bch codes. *Radio electronics computer science control*. 2020. Vol. 3. P. 150–157. doi: 10.15588/1607-3274-2020-3-14.
7. Білецький А. Я. Кодування і декодування систематичних кодів Ріда-Соломона за методом, альтернативного алгоритму Пітерсона-Горенштейна-Цірлера. *Захист інформації*. 2018. т. 20. № 3. С. 161–173. doi: 10.18372/2410-7840.20.13071.
8. Sidorenko A. Calculation of reliability of information symbols in perforated codes. *Journal of Physics: Conference Series*. IOP Publishing. 2019. P. 1–7. doi:10.1088/1742-6596/1399/3/033011 1.
9. Bucerzan D., Dragoi V., Richmond T. The simple roots problem. *Proceedings of the Romanian Academy, (Special issue), Cryptology Science*. 2017. Vol. 18. P. 317–332.
10. Bras-Amorós M., Michael O'Sullivan E. The Symmetric Key Equation for Reed–Solomon Codes and a New Perspective on the Berlekamp–Massey Algorithm. *Symmetry*. 2019. Vol. 11 (1357). doi: 10.3390/sym11111357.
11. Jordan R., Johannesson R., Bossert M. Nested convolutional codes and their application to woven codes. *IEEE Transactions on information theory*. 2004. Vol. 50, is. 2. P. 380–384. doi: 10.1109/TIT.2003.822612.
12. Briantoro H., Astawa I., Sudarsono A. An Implementation of Error Minimization Data Transmission in OFDM using Modified Convolutional Code. *Emitter-international journal of engineering technology*. 2015. Vol. 3 (2). P. 43–59.
13. Freyman V. I. Research of the reed-solomon codes characteristic for realization within control systems devices. *Radio Electronics, Computer Science, Control*. 2019. Vol. 3. P. 143–151. doi: 10.15588/1607-3274-2019-3-1.
14. Miyagi S., Isaka M. Ternary Convolutional Codes with Optimum Distance Spectrum. *Ieice transactions on fundamentals of electronics communications and computer sciences. 41st Symposium on Information Theory and its Applications (SITA)*. 2019. Vol. E102A, no. 12. P. 1688–1690. doi: 10.1587/transfun.E102.A.1688.

References (transliterated)

1. Cherubini G., Benvenuto N. Cherubini G. *Algorithms for communications systems and their applications*. Chichester: John Wiley & Sons, 2003. 1285 p.
2. Dieterich H. *Partitioning of Convolutional Codes and Applications*. Fortschritt-Bericht, VDI R. 10, 2000.
3. Jordan R., Johannesson R., Bossert M. On Nested Convolutional Codes and their application to woven codes. *IEEE Trans on Inform Theory*. 2004. Vol. 50, is. 2, pp. 380–384.
4. Vasylenko V. S., Chunarov A. V., Chunarova A. V. Otsinka efektyvnosti metodiv koduvannya pry zabezpechenni tsilisnosti informatsii v suchasnykh IKSM. *Zakhyst informatsii*, 2012, no. 3, pp. 46–50.
5. Hopyienko A. V., Kuts Yu. V., Monchenko O. V. Metod prykhovanoi peredachi v kompiuteryzovanykh informatsiino-vymiriuvalnykh systemakh. *Zakhyst informatsii*, 2011, no 2, pp. 5–9.
6. Krylova V. A., Tverytnykova E. E., Vasylychenkov O. G., Kolisnyk T. P. Modified algorithm for searching the roots of the error locators polynomial while decoding bch codes. *Radio electronics computer science control*, 2020, Vol. 3, pp. 150–157, doi: 10.15588/1607-3274-2020-3-14.
7. Beletsky A. Coding and decoding of systematic Rida-solomon codes by method, which alternative of algorithm of Peterson-Gorenstein-Zirler. *Zakhyst informatsii*, 2018, Vol. 20, is. 3, pp. 161–173, doi: 10.18372/2410-7840.20.13071.
8. Sidorenko A. Calculation of reliability of information symbols in perforated codes. *Journal of Physics: Conference Series*. IOP Publishing, 2019, pp. 1–7, doi:10.1088/1742-6596/1399/3/033011 1.
9. Bucerzan D., Dragoi V., Richmond T. The simple roots problem. *Proceedings of the Romanian Academy, (Special issue), Cryptology Science*, 2017, Vol. 18, pp. 317–332.
10. Bras-Amorós M., Michael O'Sullivan E. The Symmetric Key Equation for Reed–Solomon Codes and a New Perspective on the Berlekamp–Massey Algorithm. *Symmetry*, 2019, Vol. 11 (1357), doi: 10.3390/sym11111357.
11. Jordan R., Johannesson R., Bossert M. Nested convolutional codes and their application to woven codes. *IEEE Transactions on information theory*, 2004, Vol. 50, is. 2, pp. 380–384, doi: 10.1109/TIT.2003.822612.
12. Briantoro H., Astawa I., Sudarsono A. An Implementation of Error Minimization Data Transmission in OFDM using Modified Convolutional Code. *Emitter-international journal of engineering technology*, 2015, Vol. 3 (2), pp. 43–59.
13. Freyman V. I. Research of the reed-solomon codes characteristic for realization within control systems devices. *Radio Electronics, Computer Science, Control*, 2019, Vol. 3, pp. 143–151, doi: 10.15588/1607-3274-2019-3-1.
14. Miyagi S., Isaka M. Ternary Convolutional Codes with Optimum Distance Spectrum. *Ieice transactions on fundamentals of electronics communications and computer sciences. 41st Symposium on Information Theory and its Applications (SITA)*, 2019, Vol. E102A, no. 12, pp. 1688–1690, doi: 10.1587/transfun.E102.A.1688.

Відомості про авторів (About authors)

Крылова Вікторія Анатоліївна – кандидат технічних наук, доцент кафедри автоматизації та управління в технічних системах Національного технічного університету «Харківський політехнічний інститут», Харків, Україна. ORCID: 0000-0002-4540-8670. e-mail: vika_hpi@outlook.com.

Krylova Victoria – PhD, Associate Professor of the Department of automation and control in technical systems National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine. ORCID: 0000-0002-4540-8670. e-mail: vika_hpi@outlook.com.

Тверитникова Олена Євгенівна – доктор історичних наук, професор кафедри інформаційно-вимірювальних технологій та систем Національного технічного університету «Харківський політехнічний інститут», Харків, Україна. ORCID: 0000-0001-6288-7362. e-mail: tveekhpi@ukr.net.

Tverytynkova Elena – Doctor of Historical Sciences, Professor of the Department of information and measuring technologies and systems National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine. ORCID: 0000-0001-6288-7362. e-mail: tveekhpi@ukr.net.

Васильченко Олег Георгійович – кандидат технічних наук, доцент кафедри автоматизації та управління в технічних системах Національного технічного університету «Харківський політехнічний інститут», Харків, Україна. ORCID: 0000-0002-0969-2248. e-mail: oll5890357@ua.fm.

Vasylichenkov Oleg – PhD, Associate Professor of the Department of automation and control in technical systems National Technical University «Kharkiv Polytechnic Institute», Kharkiv, Ukraine. ORCID: 0000-0002-0969-2248. e-mail: oll5890357@ua.fm.

Колісник Тетяна Петрівна – кандидат педагогічних наук, доцент кафедри інформаційних технологій та кібербезпеки Харківського національного університету внутрішніх справ, Харків, Україна. ORCID: 0000-0002-7442-8136. e-mail: ktp201505@gmail.com.

Kolisnyk Tatyana – PhD, Associate Professor of the Department of information technology and cybersecurity Kharkiv National University of Internal Affairs. Kharkiv, Ukraine. ORCID: 0000-0002-7442-8136. e-mail: ktp201505@gmail.com.

Please cite this article as:

Krylova V., Tverytynkova E., Vasylichenkov O., Kolisnyk T. Punctured NCC codes for information protection in information and measurement systems. *Bulletin of the National Technical University "KhPI". Series: New solutions in modern technology.* – Kharkiv: NTU "KhPI", 2022, no. 1 (11), pp. 38-43, doi:10.20998/2413-4295.2022.01.06.

Будь ласка, посилайтеся на цю статтю наступним чином:

Крылова В. А., Тверитникова О. Є., Васильченко О. Г., Колісник Т. П. Перфорировані NCC коди для захисту інформації в інформаційно-вимірювальних системах. *Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях.* – Харків: НТУ «ХПІ». 2022. № 1 (11). С. 38-43. doi:10.20998/2413-4295.2022.01.06.

Пожалуйста, ссылайтесь на эту статью следующим образом:

Крылова В. А., Тверитникова Е. Е., Васильченко О. Г., Колесник Т. П. Перфорированные NCC коды для защиты информации в информационно-измерительных системах. *Вестник Национального технического университета «ХПИ». Серия: Новые решения в современных технологиях.* – Харьков: НТУ «ХПИ». 2022. № 1 (11). С. 38-43. doi:10.20998/2413-4295.2022.01.06.

АННОТАЦІЯ При розробці та проектуванні інформаційно-вимірювальних систем, виробляючих збір, обробку та передачу даних, однією з головних задач є вибір ефективних методів захисту інформації від помилок в зашумлених каналах зв'язу. Ефективне використання частотно-часових ресурсів інформаційних каналів зв'язу є ключовим при забезпеченні достовірної доставки передаваних повідомлень. Одним з перспективних напрямків підвищення надійності та достовірності передачі інформації в інформаційно-вимірювальних мережах зв'язу є використання методів та алгоритмів помехостійкого кодування, що дозволяють виявляти та виправляти помилки, що виникають внаслідок перешкоджень в каналі зв'язу. При цьому вибір в користь того чи іншого методу кодування залежить від параметрів інформаційного каналу передачі даних. Параметри помехостійкого кодера повинні узгоджуватися з характеристиками каналу зв'язу, а також вимагати доведення інформації до отримувача. Проблема отримання широкого набору параметрів кодових співвідношень при одночасному збереженні єдиної макроструктури кодера в системах зв'язу викликає необхідність дослідження розробки адаптивних алгоритмів захисту інформації від помилок. В статті представлені результати дослідження характеристик гнучких сверточних кодів з змінною швидкістю при адаптивному кодуванні/декодуванні в інформаційно-вимірювальних системах передачі інформації. Отже, при створенні мереж зв'язу немає потреби в використанні великої кількості різних кодів навіть при ідеальному розподілі швидкості передачі коду, каналної швидкості та вищого рівня за рахунок кодування. Крім того, виникає реальна можливість створення кінцевого обладнання, що працює на уніфікованих алгоритмах захисту від помилок та доступу.

Ключові слова: захист інформації; інформаційні системи; помехостійке кодування; сверточні коди; перфорированні коди

Received 10.02.2022