UDC 004.056

RESEARCH METHODS FOR INCREASING THE SECURITY OF INFORMATION TRANSFER BASED ON TIMER SIGNALS

Korchynskyi V.V., Kildishev V.I., Holev D.V., Berdnikov O.M.

O. S. Popov Odesa national academy of telecommunications,
1 Kuznechna St., Odessa, 65029, Ukraine.
vladkorchin@ukr.net

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПЕРЕДАВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ТАЙМЕРНИХ СИГНАЛІВ

Корчинський В. В., Кільдішев В.Й., Голев Д.В., Берднiков О.М.

Одеська національна академія зв'язку ім. О.С. Попова,
65029, Україна, м. Одеса, вул. Кузнечна, 1.
vladkorchin@ukr.net

ИССЛЕДОВАНИЕ МЕТОДОВ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ ТАЙМЕРНЫХ СИГНАЛОВ

Корчинский В. В., Кильдишев В.Й., Голев Д.В., Бердников А.М.

Одесская национальная академия связи им. А.С. Попова,
65029, Украина, г. Одесса, ул. Кузнечная, 1.
vladkorchin@ukr.net

Abstract. Protection of information from unauthorized access is the most important task that is assigned to modern confidential communication systems. The analysis of the risks of violating the information confidentiality justifies the necessity of its protection practically on any part of the communication system's path: storage, transformation, transmission, etc. The promising direction of protecting information from unauthorized access is a comprehensive approach that provides data protection at various levels of the OSI model. The article proposes using signals with complex structure for this task. An example of such signals are timer signals, on the basis of which the possibility of integrating the processes of noise-immunity coding and structural stealth of signal construction is explored. The analysis of timer coding possibilities for providing structural stealth and correction ability is considering parameters of construction of timer signals. Quantitative and qualitative analysis of synthesized sets of timer signals was carried out for estimation of potential possibilities of increase structural secrecy with control of fidelity transmitted data. This analysis will allow choosing the optimal parameters for constructing timer signals for the task of ensuring the required accuracy of the transmitted information and the structural secrecy of signal construction. Thus, the search of effective methods of protecting information from both random interference and unauthorized access is an important task.

Key words: security, secrecy, noise immunity, unauthorized access, information protection, channel.

Анотація. Захист інформації від несанкціонованого доступу є найважливішим завданням, що покладається на сучасні конфіденційні системи зв'язку. Аналіз ризиків порушення конфіденційності інформації обґрунтовує необхідність її захисту практично на будь-якій ділянці тракту системи зв'язку: зберігання, перетворення, передавання тощо. Перспективним напрямом розвитку захисту інформації від несанкціонованого доступу є комплексний підхід, за якого забезпечується захист даних на різних рівнях моделі OSI. Для цього завдання у статті запропоновано використовувати сигнали зі складною структурою. Прикладом таких сигналів є таймерні сигнальні конструкції, на основі яких можливо реалізувати завадостійке кодування, а також підвищити структурну прихованість передаваних комбінацій. Структурна прихованість спрямована на суттєве ускладнення розпізнавання структури сигналів за умови, що засобами радіотехнічної розвідки вирішена проблема енергійної прихованості, тобто сигнал виявлений і записаний на носій інформації. На основі таймерного кодування досліджується можливість інтегрування процесів завадостійкого кодування та структурної прихованості сигнальних конструкцій в єдине завдання. Надано аналіз можливостей таймерного

кодування щодо забезпечення структурної прихованості і коректуючої здатності з урахуванням параметрів побудови таймерних сигналів. Проведено кількісний і якісний аналіз синтезованих множин таймерних сигналів для оцінки потенційних можливостей підвищення структурної прихованості. Визначено взаємозв'язок структурної прихованості і коректуючої здатності таймерних сигнальних конструкцій. Установлено, що збільшення мінімальної кодової відстані зменшує кількість дозволених кодових комбінацій, яка знижує структурну приховані сигнальних конструкцій. Суперечливий характер показників структурної прихованості і завадостійкості слід враховувати при розробці алгоритмів обміну даними у системі зв'язку.

Ключові слова: захищеність, прихованість, завадостійкість, несанкціонований доступ, захист інформації, канал.

Аннотация. Защита информации от несанкционированного доступа является важнейшей задачей, которая возлагается на современные конфиденциальные системы связи. Анализ рисков нарушения конфиденциальности информации обосновывает необходимость её защиты практически на любом участке тракта системы связи: хранения, преобразования, передачи и т.д. Перспективным направлением развития защиты информации от несанкционированного доступа является комплексный подход, при котором обеспечивается защита данных на различных уровнях модели OSI. В статье предложено использовать для этой задачи сигналы со сложной структурой. Примером таких сигналов являются таймерные сигнальные конструкции, на основании которых можно реализовать помехоустойчивое кодирование, а также повысить структурную скрытность передаваемых комбинаций. Проведен анализ возможностей таймерного кодирования по обеспечению структурной скрытности и корректирующей способности с учётом параметров построения таймерных сигналов. Проведен количественный и качественный анализ синтезируемых множеств таймерных сигналов для оценки потенциальных возможностей повышения структурной скрытности с контролем верности передаваемых данных.

Ключевые слова: защищённость, скрытность, помехоустойчивость, несанкционированный доступ, защита информации, канал.

Protection of the transmitted information from unauthorized access (UAA) is the most important task assigned to modern confidential communication systems (CCS). It is known [1] that the protection of information from unauthorized access is carried out mainly at the upper levels of the OSI model using cryptographic transformations. The increase in the amount of information transmitted in communication networks, and the constant improvement of unauthorized access tools, puts forward a new concept of building a modern CCS. At present, taking into account the risks of UAA to confidential information, it should be carried out practically at any part of the communication system: storage, transformation, transmission, etc. Therefore, the perspective direction for the development of information security is a complex approach that ensures data protection at various levels of the OSI model [2].

Obviously, the reliability and protection of information against UAA are integral components to ensure its integrity and security during transmission over a communication channel. Therefore, to assess the effectiveness of such a security system, it is advisable to use a comprehensive measure of noise immunity [3]. This will allow the assessment of both the reliability of the transmission and various characteristics of secrecy: informational, structural, energetic, spatial, temporal, etc.

One of the methods of protecting information from UAA is the use of signals from carriers with a complex structure. In this article, it is proposed to use timer signal constructions (TSC) for this task. In [2,4,6], it was shown that, on the basis of the TSC, noise-tolerant coding without the use of test elements can be realized. The further stage of the research is the research of the parametric properties of timer coding based on the synthesis of various sets signal constructions that distinguish the structure of their construction. Given the parameters of the TSC construction, the structural secrecy and the corrective ability of timer coding are analyzed. This analysis will allow choosing the optimal parameters for constructing timer signals for the task of ensuring the required accuracy of the transmitted information [4] and the structural secrecy of signal construction [5]. Thus, the search of effective methods of protecting information from both random interference and unauthorized access is an important task.

The aim of the article is a quantitative and qualitative analysis of the synthesized sets of timer signal constructions for assessing the potential abilities of increasing the structural secrecy with control of the accuracy of the transmitted data.

Time coding [6] was proposed in the 1980s for the task of increasing the transmission speed in a binary channel with a limited bandwidth

$$\Delta F = \frac{1}{t_0}, \tag{1}$$

where t_0 – Nyquist interval. Based on the TSC, it is possible [6] to implement noise immunity coding [8], but, in the difference of bit-digital codes (BDC), when building an allowed code combination, additional symbols are not required to control the accuracy of the received data. In article [4, 6], it was proposed to combine these two types of noise-immunity coding to protect data from communication channel errors. This allows the system to compensate or reduce the redundancy of the verification elements BDC. Variational possibilities of timer coding on the synthesis of various sets of TSC at a given time interval opened a new perspective on the development of various algorithms, based on which it is possible to increase the structural secrecy of information carrier signals [5].

In article [7], the feasibility of the synthesis noise immunity TSC was considered with the aim of increasing the energy and structural secrecy of signal construction in broadband communication systems. For this task, various methods of spreading the signal were adapted to the TSC: direct spreading by random sequences and random tuning of the operating frequency.

In this article, the research is aimed at assessing the possibilities of timer coding on the synthesis of various sets of allowed signal construction with given minimum code distance d_0. Information about the value d_0 will allow the creation of algorithms to increase the structural secrecy, considering the corrective ability of the timer signals. Structural secrecy of signal construction is aimed at significantly complicating the recognition of their structure, provided that the problem of energetic secrecy is solved by means of radio intelligence (RI) and UAA, i.e. the signal is detected and recorded on the storage medium. Structural secrecy depends on the variety of used signal constructions, both at the channel level and at the physical level. The increase in structural secrecy is possible using of different sets of signal structures for each transmission session. Potential structural secrecy is determined by considering the total number N of possible signal structures that are used to transmit information symbols:

Consider the features of the construction of timer signals. For this, select the time interval

$$T_s = nt_0, \tag{3}$$

where n – the number of Nyquist elements. Value n affects a lot of synthesized combinations, as well as the complexity of the implementation of the coding and decoding devices.

The next parameter to build a TSC is the base time element Δ, by which within an interval T_s determined by the duration of the pulses

$$t_s = t_0 + k\Delta, \tag{4}$$

where $k = 0, 1, 2, ..., s \cdot (n-2)$. As can be seen from (4) pulse duration t_s not multiple t_0, as with BDC, and are multiples of the base element Δ (where $\Delta = t_0/s$; $s = 1, 2, 3, ..., l$ – whole numbers). Thus, during the formation of pulses t_s on the interval T_s, the Nyquist condition is observed, at which

$$t_s \geq t_0. \tag{5}$$

Parameter s determines the quantity Δ on the interval t_0, i.e.

$$s = \frac{t_0}{\Delta}. \tag{6}$$

Increase the number of timer signals realizations N_r on interval T_s compared to the BDC. It is achieved by reducing the energy distance between them and is determined by the value $\Delta < t_0$, then

$$N_{\text{r}} = \frac{[ns - i(s-1)]!}{i!(ns-is)!}, \tag{7}$$

where i – the number of modulation information moments. By varying the parameters n, s and i it is possible to synthesize different sets of signal constructions that differ in the structure of construction and the number of realizations N_{r}. However, the increase in the number of realizations N_{r} when Δ decreases leads to a decrease in noise immunity, which should be considered when choosing s.

Table 1 shows the values N_{r} depending on parameters n, s and i. For $n=7$, $i=3$, s =5 can get N_{r} = 1771 realizations, whereas for BDC only $N_{\text{r BDC}} = 2^7 = 128$. For the same TSC parameters, but for s = 6 the number of realizations is N_{r} = 2925 a lot more. Also, a significant increase in the number of realizations is achieved by lengthening the interval for constructing signal constructions T_{s}. For $n=8$, $i=3$, s = 5 value N_{r} = 3276. Examples of the formation of the TSC were considered with a minimum code distance $d_0 = 1$. Obviously, such sets of signal constructions do not have corrective properties. Provided that $d_0 \geq 2$ based on the TSC, noise-tolerant coding can be implemented. For determining d_0 It is proposed to use Hamming code distance considering the base element Δ:

$$d_0 = \sum_{j=1}^{W} x_j \oplus z_j, \tag{8}$$

where x_j and z_j – logical state of segments TSC (0 or 1) by elements Δ; $W = n \cdot s$ – amount of elements Δ on the time interval T_{s}. As an example in Fig. 1 shows the implementation of signal constructions with different pulse durations and code distances with parameters $n=7$, $i=3$, s = 5:

1) $t_{\text{s1}} = 5\Delta$, $t_{\text{s2}} = 6\Delta$, $t_{\text{s3}} = 24\Delta$ for TSC-1;
2) $t_{\text{s1}} = 6\Delta$, $t_{\text{s2}} = 10\Delta$, $t_{\text{s3}} = 19\Delta$ – TSC-2;
3) $t_{\text{s1}} = 10\Delta$, $t_{\text{s2}} = 17\Delta$, $t_{\text{s3}} = 8\Delta$ – TSC-3.

Combinations TSC-1 and TSC-2 have d_0 = 6, between TSC-1 and TSC-3 – d_0 = 21, TSC-2 and TSC-3 – d_0 =15.

As can be seen from table 1 with increasing d_0 number of implementations N_r decreases, which, according to (2), reduces the structural secrecy of signal constructions. The contradictory character of the indicators secrecy and noise immunity should be considered when developing data exchange algorithms in a communication system. Obviously, in this case, to compensate the fall of the indicator S_{TSC}, it is advisable to use interchangeable multiplies of signal construction $\{N_{\text{TSC}_i}(d_0)\}$ with given d_0 for different sessions of confidential information transmission, therefore

$$S_{\text{TSC}} = \log_2\left(\sum_{z=1}^{L} N_{\text{TSC}_i}(d_0)\right). \tag{9}$$

Consequently, the parameters n, s and i can affect both on the noise immunity and on structural secrecy of signal construction.

Consider the of the formation features of allowed TSC with the help of the quality equation [6]:

$$\sum_{k=1}^{i} A_k x_k \equiv 0 (\text{mod}\, A_0), \tag{10}$$

where $A_k(k=1,i)$ – weight coefficient, which is a set of prime numbers; A_0 – module values; x_k – report numbers of significant modulation moments (SMM) pulses t_{si}. If the signal construct satisfies (10), then it is allowed.

Samples N_r of allowed code combinations that are forming the quality equation with $A_0 = 19$, $A_1 = 2$, $A_2 = 3$, $A_3 = 7$ and parameters of construction n, s, i, are given in Table 2.

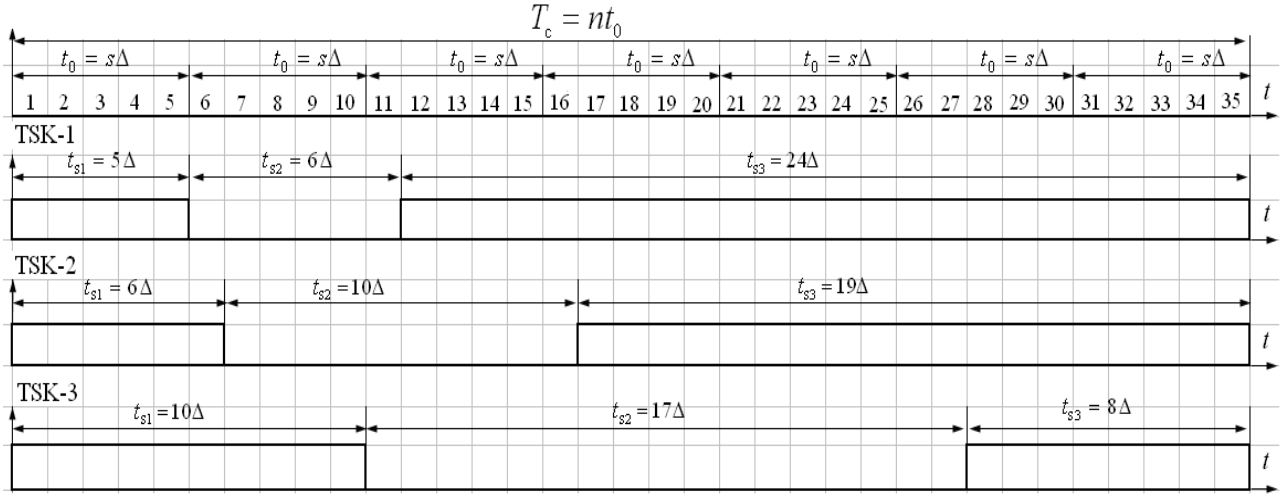

Figure 1 – An example of the implementation TSC with different values d_o

Table 1 – The number of implementations of the TSC, depending on the parameters n, s, i and d_0

№	Parameters TSC			Sample TSC depending on d_0								
	N	*i*	*s*	1	2	3	4	5	6	7	8	9
1	7	3	5	1771	891	248	146	79	53	36	28	22
2	7	3	6	2925	1469	395	231	121	85	53	44	31
3	7	3	7	4495	2255	591	344	176	121	76	60	44
4	8	3	5	3276	1638	438	252	133	91	59	47	33
5	8	3	6	5456	2736	714	408	316	146	94	70	50
6	8	3	7	8436	4218	1079	615	316	212	137	102	75

Table 2 – Samples of realizations TSC according to the equation of quality with A_0=19, A_1=2, A_2=3, A_3=7 and n, s, i, d_o

№	Parameters TSC			Total amount realizations	Samples allowed TSC depending on d_o					
	m	*i*	*s*		4	5	6	7	8	9
1	7	3	5	1771	93	37	27	24	15	13
2	7	3	6	2925	154	59	43	41	23	19
3	7	3	7	4495	236	88	68	58	34	29
4	8	3	5	3276	173	65	52	40	27	22
5	8	3	6	5456	288	106	82	68	42	35
6	8	3	7	8436	444	156	123	98	60	49

As can be seen from the Table 2 the number of allowed TSC satisfying the quality equation with given $A_k(k=1,i)$ and A_0 significantly less than with full enumeration of the whole multiples TSC with using (7). At the same time, the samples of allowed signal constructions have $d_o = 4$. For $n = 7$, $i = 3$, $s = 5$ can get $N_r = 93$ with minimum code distance d_o =4 from the total number of realizations $N_{r\,tot} = 1771$, whereas with full brute force $N_r = 146$ (Table 1). When $d_o = 5$ the number of realizations is significantly reduced $N_r = 37$ (Table 2), whereas with full brute force

N_r = 79 (Table 1). On the one hand, the quality equation is a convenient tool for implementing noise immunity coding based on TSC. On the other hand, the number of allowed combinations is less, which must be considering when developing algorithms for enhancing the structural secrecy of transmission based on TSC.

In Table 3 and 4 show the allowed TSC for other values of A_0, A_1, A_2, A_3. From these tables by changing the value of A_0, A_1, A_2, A_3, it is possible to obtain new sets of signal constructions with different initial values d_o.

Table 3 – Samples of TSC realizations according to the quality equation with $A_0 = 7$, $A_1 = 2$, $A_2 = 3$, $A_3 = 5$ and n, s, i, d_o

№	Parameters TSC			Total amount Realizations	Samples allowed TSC depending on d_o							
	m	*i*	*S*		2	3	4	5	6	7	8	9
1	7	3	5	1771	253	144	87	57	34	28	21	14
2	7	3	6	2925	418	233	135	87	52	43	34	22
3	7	3	7	4495	643	354	204	134	78	67	48	33
4	8	3	5	3276	468	260	151	100	60	52	35	23
5	8	3	6	5456	780	426	242	158	91	79	57	38
6	8	3	7	8436	1206	652	365	239	137	114	86	54

Table 4 – Samples of TSC realizations according to the quality equation with A_0 = 11, $A_1 = 2$, $A_2 = 3$, $A_3 = 7$ and n, s, i, d_o

№	Parameters TSC			Total amount realizations	Samples allowed TSC depending on minimum code distance								
	m	*i*	*s*		2	3	4	5	6	7	8	9	10
1	7	3	5	1771	161	–	92	40	33	27	17	15	12
2	7	3	6	2925	266	–	148	63	50	47	28	23	17
3	7	3	7	4495	409	–	225	92	74	62	39	34	27
4	8	3	5	3276	299	–	166	72	56	49	30	25	20
5	8	3	6	5456	496	–	271	111	89	76	47	39	30
6	8	3	7	8436	767	–	415	166	135	113	66	57	43

Table 5 – The coefficients of the quality equation for the forming allowed TSC

№	d_o	A_0	A_1	A_2	A_3
1	4	19	2	3	7
2	2	7	2	3	5
3	2	11	2	3	7
4	3	13	2	3	7
5	-	17	2	3	7

In Table 5 shows the minimum code distance d_o = 2 - 4, which were obtained for the values A_0, A_1, A_2, A_3. All multiplies of allowed TSC differ from each other in the number of combinations, the structure of construction and the code distance.

The research results showed the formation features of timer signals by various methods. The exhaustive full method (7) makes it possible to more fully use the multiply set of signal constructs to form allowed combinations, therefore, there will always be more of them than when using the quality equation (10).

By changing the parameters of the quality equation A_0, A_1, A_2, A_3 it is possible to synthesize sets of signal constructions, which differ in the number of combinations and the minimum code

distance d_0. This makes it possible, on their basis, to develop algorithms for enhancing the structural secrecy with the requirements for noise immunity.

The analysis of the interconnection of the structural secrecy and the corrective ability of the timer signal constructions, considering the parameters of their construction. Increasing the code distance d_0 reduces the number of allowed code combinations, which reduces the structural secrecy of signal constructions. The contradictory character of indicators structural secrecy and noise immunity should be considered when developing data exchange algorithms in the communication system.

REFERENCES:

1. Kupriyanov A.I., Sakharov A. V. “Theoretical foundations of electronic warfare.” M.: “University book”, 2007: 356 c.
2. Zakharchenko M., Korchynskyi V., Kildishev V. “Integrated methods of information security in telecommunication systems.” 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo’2017), IEEE Xplore Digital Library. 11-15 September 2017. V. 1. P. 78-81. Electronic resource. Access mode: http://ieeexplore.ieee.org/document/8095366/.
3. Korchynskyi V.V., Kildishev V.I., Berdnikov A.M. “Methods for assessing the security of communication systems of special purpose.” Scientific works ONAT, 2017, №2: 101-107.
4. Zakharchenko V.M. “Synthesis of multi-position time codes.” Kyiv: Engineering, 2012: 284.
5. Zakharchenko N., Korchinskyi V., Radzimovsky B. “Information security of Time-Controlled Signals in Confidential Communication Systems.” Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 February 2012), Lviv: Publishing House of Lviv Polyteshnic, 2012: 317.
6. Zakharchenko N., Krysko A. “Basics of coding: a training manual.” Odessa: UGAS named after A. S Popov 1999: 240.
7. Korchinskyi V., Kildyshev V., et al. "Spectral methods of information protection on the basis of timer signals and random processing of the working frequency.” Perspectives of the Day of Protection of Information: Materials of the Third All-Ukrainian Sciences. Conf. (Odessa, 02-06 September 2017), Odessa: ONAT, 2017: 36-39.
8. Skopa O., Korchinsky V. “Management of Relative Effective Transmission Rate in Packet Switching Networks.” Proceedings of the International Conference TCSET’2002, February 18-23, 2002 Lviv-Slavsko, Ukraine: 2.

ЛІТЕРАТУРА:

1. Куприянов А.И. Теоретические основы радиоэлектронной борьбы / А. И. Куприянов, А.В. Сахаров. – М.: Вузовская книга, 2007. – 356 с.
2. Zakharchenko M., Korchynskyi V., Kildishev V. “Integrated methods of information security in telecommunication systems.” 2017 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo’2017), IEEE Xplore Digital Library. 11-15 September 2017.
   V. 1. P. 78-81. Electronic resource. Access mode: http://ieeexplore.ieee.org/document/8095366/.
3. Korchynskyi V.V., Kildishev V.I., Berdnikov A.M. “Methods for assessing the security of communication systems of special purpose.” Scientific works ONAT, 2017, №2: 101-107.
4. Захарченко В.М. Синтез багатопозиційних часових кодів / Захарченко В.М. – К.: Техніка, 2012. – 284 с.
5. Zakharchenko N., Korchinskyi V., Radzimovsky B. “Information security of Time-Controlled Signals in Confidential Communication Systems.” Modern problems of radio engineering, telecommunications and computer science: XI International Conference TCSET 2012, (Lviv-Slavske, 21-24 February 2012) – Lviv: Publishing House of Lviv Polyteshnic, 2012: 317.
6. Захарченко Н. В. Основы кодирования: учеб. пособ. / Н. В. Захарченко, А. С. Крысько. – Одесса: УГАС им. А. С. Попова, 1999. – 240 с.
7. Корчинский В.В., Кильдишев В.Й., Бердников А.М., Русаловская А.А. Спектральные методы защиты информации на основе таймерных сигналов и псевдослучайной перестройки рабочей частоты / Матеріали третьої Всеукраїнської наук.-практ. конф. [«Перспективні няпрями захисту інформації”], (Одеса, 02-06 вересня 2017). – Одеса: ОНАЗ, 2017. – С. 36-39.
8. Skopa O., Korchinsky V. “Management of Relative Effective Transmission Rate in Packet Switching Networks.” Proceedings of the International Conference TCSET’2002, February 18-23, 2002, Lviv-Slavsko, Ukraine: 2.

DOI 10.33243/2518-7139-2018-1-2-109-116