Algorithms of data processing in the residual classes system

Alina Yanko
Department of Computer Engineering,
Poltava National Technical Yuri Kondratyuk University,
Poltava, Ukraine
al9_yanko@ukr.net

Koshman Sergey
Automation and Computer Integrated Technologies Department,
Kharkiv Petro Vasylenko National Technical University of Agriculture,
Kharkiv, Ukraine
s_koshman@ukr.net

Victor Krasnobayev
Electronics and Control Systems Department,
V. N. Karazin Kharkiv National University,
Kharkiv, Ukraine
krasnobaev_v.a@ukr.net

***Abstract*—The coding of remainders number which submitted the appropriate modules of residual classes system (RCS), made with data from complete system of the smallest non-negative residues (CSSNR) was showed in the article. In this aspect, CSSNR is the basis for the construction of non-positional code structure in RCS. Possible field of science and engineering, where there is an urgent need for fast, reliable, and high-precision integer calculations were clarified and systematized in the paper. On the basis of studies of the properties of RCS were examined the advantages and disadvantages of using modular arithmetic (MA). Using the results of the analysis of problems of integer data and a set of positive attributes of MA, the classes of problems and algorithms, which using RCS, much more efficient binary positional numeral systems were defined in the article.**

Keywords—residual classes system; modular arithmetic; positional numeral systems; complete system of the smallest non-negative residues; computer system and a data processing means which represented in integer form; residual classes.

I. INTRODUCTION

In the present time there is a number of fields and directions of science and technology, where a need in fast, reliable and highly precise integer arithmetic calculations exists [1-7]. We can say, that in almost all fields of science the integer arithmetic calculations are used. First of all, they are such fields of science as mathematics, physics, astronomy, technical science, geodesy and meteorology, seismology etc. [8-33]. Let's note the following directions in science and technology, where there exists the necessity in fast, reliable and highly precise integer arithmetic calculations: arithmetic operations with integer numbers and polynomials; integer linear programming; operations with numbers and sets, the solution of the multidimensional NP-complete problems; implementation of routing algorithms (algorithms for finding the shortest path); problems of ways and matrix multiplication; problems of fast Fourier transform and it's applications; the creation of artificial intelligence systems (neural network data processing system); tasks for military purposes; digital signal processing, digital image processing; cryptographic transformation; highly-precise integer arithmetic; the solution of problems related to the space research; highly-precise digital-to-analog and analog-to-digital conversions and so forth[1].

The results of the researches conducted during last few decades in the field of information technologies by different groups of scientists and engineers of methods of productivity improvement, reliability, survivability, and reliability of computer systems calculations and data processing means presented as integers (CSIDPM), showed that within the positional numeral systems (PNS), it is practically impossible to achieve it [2]. First of all, it's caused by the main disadvantage of modern CSIDPM that operate in PNS: the presence of inter-bits links between the processed operands. These links significantly impact the architecture of the calculator and methods of implementation of arithmetic operations, implemented by CSIDPM; complicate the apparatus and limit the speed of the arithmetic operations of addition, subtraction and multiplication. In this regard, improving above mentioned characteristics of CSIDPM in PNS, is carried out, first of all, by increasing the clock frequency, development and application of methods and means of parallel data processing as well as by using different types of redundancy. This circumstance led to the need of finding the ways of increasing the effectiveness of CSIDPM functioning, for example, through the use of new architectural solutions by applying non-positional machine arithmetic, in particular, on the basis of non-positional numeral systems use in residual classes (NSRC). The well-known Chinese remainder theorem (the task of restoring the original number A_k by the aggregating of its remains (deductions) $\{a_i\}$ by dividing it into a series of natural numbers $m_1, m_2, ..., m_n$ (modules) of NSRC), which was previously interpreted as a structural theorem of abstract algebra, guaranteed the specified parallelism in the calculations over integers, under the conditions that the result of ring operations belongs to the range of integers, defined by models product of NSRC. The results of conducted researches of the implementation of arithmetic

978-1-xxxx-xxxx-x/17/$31.00 ©2017 IEEE

operations methods in NSRC led to the creation of new machine arithmetic. Having its ideological roots of the classical works of Euler, Gauss and Chebyshev on the theory of comparisons, NSRC introduced new ideas in the development of creation methods of highly-productive and ultra reliable CSIDPM [1, 3].

II. RESEARCH METHODOLOGY AND ANALYSIS OF RESULTS

For the first time the results of theoretical studies devoted to the possibility of practical application of NSRC as a numeral system (NS) of CSIDPM, were published in 1955-1957 in the scientific works of Czech scientists M. Valaha and A. Svoboda. Non-positional number system in NSRC is a NS where integers are presented as a set of non-negative deductions (residues) in the group of mutually pairwise prime numbers which are called bases or modules of NSRC. In this case there are no inter-bits relations between processed numbers residues, that gives opportunity to perform arithmetic operations excluding bit relations between numbers residues. The use of NSRC-based machine arithmetic allowed to create actually operating CSIDPM. In the 60s of the past century the team of scientists and engineers headed by the doctor of technical sciences, professor D. I. Yuditskii, created A-340A the world's first experimental computer and T-340A serial computers, functioning in NSRC. These computers were intended for regular polygon version of Dunay-3UP radar, which was the part of the USSR A-35 missile defense system. In the 70s of the past century for radar stations there were created such CSIDPM in NSRC as "Diamond" and 5E53 supercomputers.

However, in the 80s of the past century due to a number of objective and subjective reasons the interest to modular arithmetic (MA) is significantly reduced. It was primarily due to the death of the Director of the Microelectronics Center, developing the general theory and practical creation of a computer in NSRC located in Zelenograd, Moscow Region, the Director and the chief initiator of project Lukin Fedor Victorovich and therefore, the complete termination of practical works, connected with the use of MA. But then this direction was restrained by the imperfection of the existing at that time element base of computers, as well as the existing methodology of computer systems and components designing, principally focused at that time only on the binary system calculation.

Now the interest to the use of NSRC is increasing again. Ultimately it is caused by:

- the emergence of the numerous scientific and theoretical publications devoted to the theory and practice of the computer systems and components creating in NSRC;
- wide distribution of mobile processors that require high speed data processing at low energy consumption; the lack of inter-bits transfers during arithmetic operations of addition and multiplication of numbers in NSRC allows to reduce energy consumption;
- strong interest to NSRC is being shown by the banking structures, where it is necessary in real time to handle large amount of data safely and reliably, i.e. they are required highly-productive means for highly reliable computing with errors self-correction, that is typical to the NSRC codes;
- the elements density increasing on a single chip doesn't always allow to perform a complete and qualitative testing; in this case there is an increasing importance of providing failover operation of CSIDPM;
- the need for the use of the specialized CSIDPM to perform a large number of operations on vectors, which require high-speed performance of integer addition and multiplication operations (matrix multiplication problems, the problems of the scalar product of vectors, Fourier transformation, etc.);
- the widespread introduction of microelectronics into all spheres of human activity significantly increased relevance and importance of previously rare, and now so massive scientific and practical problems, as a digital signal and image processing, image recognition, cryptography, multi-bit data processing and storage, etc.; this circumstance requires enormous computing resources being in excess of the existing possibilities;
- the current level of microelectronics development is coming to its limits from the point of view of productive provision and reliability of existing and future computer systems and components of large data sets processing in real time;
- taking it over nanoelectronics, molecular electronics, micromechanics, bioelectronics, optical, optoelectronic and photonic computers and others are still rather far from the real industrial production and employment.
- the modern development of integrated circuit technology allows to have a fresh look at the principles of devices construction with modular arithmetic employment and provides wide opportunities to use new design techniques (such as the methodology of systems design on a chip-SOC) both in the development of individual computing units, and computer systems in general; integral technology enables more flexible design of computer systems and components and allows us to implement NSRC-based devices as effectively as on the basis of the binary system; furthermore at present in order to improve the effectiveness of computer devices development, automated design systems (ADS) are widely used; in this respect, the design of computer systems and components based on NSRC does not differ from the working with the help of ADS data of binary data-blocks in PNS;
- unfortunately, Ukraine today in contrast to the theoretical development, technologically is behind the foreign microelectronics of some leading countries; in this case, it is advisable to use the existing theoretical achievements and practical experience in the creation of

effective computer systems and components in NSRC.

In [1] it is given a definition of NSRC. In this case NSRC is considered a generalized version of NS, in which any natural number A, including zero, is represented as a set of the smallest positive residues (deductions) of the division of the original A number on preset $m_1, m_2, \dots m_n$ natural numbers, called bases or NSRC modules. In literature it is often not entirely fair the term NSRC is identified with "residue class". In some cases, this circumstance can interfere the analysis of the results of solving the data processing problems presented in MA. In this regard it is important to consider the correlation between the notion of NSRC and RC. We'll give a definition to the notion "residue class". Let's consider the set {A} of all natural numbers, including zero. From the set of natural numbers we choose an arbitrary number (module) m_i. While dividing any natural number on m_i module we can get the following set of residues: 0 (A number is divided into the m module integrally), 1, $2 \dots m_i - 2$ and $m_i - 1$. All the set of natural numbers including zero, can be divided into m_i (0, 1, 2, ... m_i -2 and m_i -1) of different groups of numbers (residue classes), including in each RC the numbers which, while dividing into the module m_i, give the same remainder. It is considered, that these numbers are comparable with each other on module m_i.

The residue class modulo m_i of NSRC can be denoted by the symbol $RC_j^{(i)}$, where i – the number of the base of orderly ($m_i < m_{i+1}$) NSRC ($i = \overline{1, n}$); j – the RC number in the system of residues for a given module m_i ($j = \overline{0, m_i - 1}$). In the general case, the residue class of $RC_j^{(i)}$ modulo m_i we will call the set of all integers, including zero, which while dividing into the modules m_i give the same positive balance.

Taking into account the well-known correlation $(-A) \bmod m_i = (m_i \cdot k - A) \bmod m_i (k = 1, 2, 3, ...)$, all RC on arbitrary module m_i of NSRC can be represented in the form of residues:

$$
\begin{aligned}
RC_0^{(i)} &= \overline{0} \ \{ \dots, \ -m_i, \ 0, \ m_i, \dots \}, \\
RC_1^{(i)} &= \overline{1} \ \{ \dots, \ -(m_i - 1), \ 1, \ m_i + 1, \dots \}, \\
RC_2^{(i)} &= \overline{2} \ \{ \dots, \ -(m_i - 2), \ 2, \ m_i + 2, \dots \}, \\
&\vdots \\
RC_j^{(i)} &= \overline{j} \ \{ \dots, \ -(m_i - j), \ j, \ m_i + j, \dots \}, \\
&\vdots \\
RC_{m_i - 2}^{(i)} &= \overline{m_i - 2} \ \{ \dots, -2, m_i - 2, \ 2 \cdot m_i - 2, \dots \}, \\
RC_{m_i - 1}^{(i)} &= \overline{m_i - 1} \ \{ \dots, -1, \ m_i - 1, \ 2 \cdot m_i - 1, \dots \}. \qquad (1)
\end{aligned}
$$

If one arbitrary residue is taken from each RC, then such set of m_i integers will be called a complete residue system (CRS) modulo m_i. Having taken one specific residue from each RC, draw up some possible options for CRS modulo m_i: 0, 1, 2, 3, …, $m_i - 1$ – is a complete system of the smallest non-negative residues (CSSNR); m_i, 1, 2, 3, …, $m_i - 1$ – is a complete system of the smallest positive residues (CSSPR); 0, 1, 2, -2, …, -1 – is a complete system of the smallest in absolute value residues (CSSAVR) [4].

As within each module they operate only with natural numbers, including zero, for the formation of NSRC with the $m_1, m_2, ..., m_n$ bases it is necessary to use n CSSNR from each set of RS. In this case all possible RC ($C^{(1)}$) for the first m_1, for the second ($C^{(2)}$) m_2 and the last ($C^{(n)}$)m_n of NSRC modules, have been represented respectively by the expressions (2), (3) and (4).

For the first NSRC m_1 module we have the following set of RC:

$$
\begin{aligned}
RC_0^{(1)} &= \overline{0} \ \{ 0, \ m_1, \ 2 \cdot m_1, \ 3 \cdot m_1, \dots \}, \\
RC_1^{(1)} &= \overline{1} \ \{ 1, \ m_1 + 1, \ 2 \cdot m_1 + 1, \ 3 \cdot m_1 + 1, \dots \}, \\
RC_2^{(1)} &= \overline{2} \ \{ 2, \ m_1 + 2, \ 2 \cdot m_1 + 2, \ 3 \cdot m_1 + 2, \dots \}, \\
&\vdots \\
RC_{m_1 - 2}^{(1)} &= \overline{m_1 - 2} \ \{ m_1 - 2, \ 2 \cdot m_1 - 2, \ 3 \cdot m_1 - 2, \dots \}, \\
RC_{m_1 - 1}^{(1)} &= \overline{m_1 - 1} \ \{ m_1 - 1, \ 2 \cdot m_1 - 1, \ 3 \cdot m_1 - 1, \dots \}. \qquad (2)
\end{aligned}
$$

Obviously, for the module m_1 of NSRC the CSSNR will consist of residues: $0, 1, 2, ..., m_1 - 1$.

For the second m_2 module of NSRC we have the following set of RC:

$$
\begin{aligned}
RC_0^{(2)} &= \overline{0} \ \{ 0, \ m_2, \ 2 \cdot m_2, \ 3 \cdot m_2, \dots \}, \\
RC_1^{(2)} &= \overline{1} \ \{ 1, \ m_2 + 1, \ 2 \cdot m_2 + 1, \ 3 \cdot m_2 + 1, \dots \}, \\
RC_2^{(2)} &= \overline{2} \ \{ 2, \ m_2 + 2, \ 2 \cdot m_2 + 2, \ 3 \cdot m_2 + 2, \dots \}, \\
&\vdots \\
RC_{m_2 - 2}^{(2)} &= \overline{m_2 - 2} \ \{ m_2 - 2, \ 2 \cdot m_2 - 2, \ 3 \cdot m_2 - 2, \dots \}, \\
RC_{m_2 - 1}^{(2)} &= \overline{m_2 - 1} \ \{ m_2 - 1, \ 2 \cdot m_2 - 1, \ 3 \cdot m_2 - 1, \dots \}. \qquad (3)
\end{aligned}
$$

For the module m_2 of NSRC the CSSNR will consist of residues: $0, 1, 2, ..., m_2 - 1$.

$$
\begin{aligned}
RC_0^{(n)} &= \overline{0} \ \{ 0, \ m_n, \ 2 \cdot m_n, \ 3 \cdot m_n, \dots \}, \\
RC_1^{(n)} &= \overline{1} \ \{ 1, \ m_n + 1, \ 2 \cdot m_n + 1, \ 3 \cdot m_n + 1, \dots \}, \\
RC_2^{(n)} &= \overline{2} \ \{ 2, \ m_n + 2, \ 2 \cdot m_n + 2, \ 3 \cdot m_n + 2, \dots \}, \\
&\vdots \\
RC_{m_n - 2}^{(n)} &= \overline{m_n - 2} \ \{ m_n - 2, \ 2 \cdot m_n - 2, \ 3 \cdot m_n - 2, \dots \}, \\
RC_{m_n - 1}^{(2)} &= \overline{m_n - 1} \ \{ m_n - 1, \ 2 \cdot m_n - 1, \ 3 \cdot m_n - 1, \dots \}. \qquad (4)
\end{aligned}
$$

For the module m_n the CSSNR will consist of residues: $0, 1, 2, ..., m_n - 1$.

Thus, the NSRC is characterized by using of n, the number of bases of CSSNR.

Here is an example of CRS definition for the module $m_i = 5$ of NSRC. Residue classes modulo five can be represented in general form:

$\bar{0}$ { … -10, -5, 0, 5, 10, … },

$\bar{1}$ { … -9, -4, 1, 6, 11, … },

$\bar{2}$ { … -8, -3, 2, 7, 12, … },

$\bar{3}$ { … -7, -2, 3, 8, 13, … },

$\bar{4}$ { … -6, -1, 4, 9, 14, … }.

Taking one residue from each RC, we compose all the variants of the complete residues systems modulo five: 0,1,2,3,4 – CSSNR; 5,1,2,3,4 – CSSPR and 0,1,2,-2,-1 – CSSAVD. According to the definition, CSSNR 0,1,2,3,4 is used in NSRC.

Actually, there is an opinion [3], that it is possible for NSRC not to be called a number system. Indeed, NSRC bases are connected to each other so, that they are selected in a certain way and secured by the permanent modules for the given NS. Each residue modulo is informationally independent on other residues, however, during the implementation of arithmetic operations within each residue unitary or binary NS is generally used. Thus NSRC may be determined not as the number system, but as a special design code numeric data structure, that is specially encoded block of numerical data.

It should be noted that in the proposed approach the NSRC is not opposed to binary PNS, and serves as its extension that allows to solve effectively a certain class of problems. Therefore, the most effective in this case, is an approach that unites the use of a combined MA and binary PNS notation in constructing the control systems. Upon that, for example, control of the entire system can be carried out by the conventional binary commands and blocks; and data processing is performed on the basis of a modular representation of numbers. Thus, the use of the advantages and benefits of NSRC, along with the traditional binary method of control systems constructing can lead to the productivity increase of CSIDPM in general [5].

To answer the question of whether to use NSRC it's necessary to investigate the influence of the MA basic properties on the structure and operation principles of CSIDPM. Possible logical algorithm research diagram of NSRC effective application can be represented as follows:

- to indentify the areas and directions of science and technology where integer calculations are necessary; to show in which tasks and algorithms (specifically, to name and show the most important ones) integer calculations are used; first of all the tasks and algorithms, which include such operations as arithmetic operations of addition, subtraction and multiplication in a positive and negative number ranges, as well as arithmetic operation and algebraic comparisons of numbers;
- to justify the relevance requirements and the need to increase the speed of integer calculations, i.e. to justify the need to increase CSIDPM productivity in order to (to increase the speed of integer calculations it's necessary to create CSIDPM of increased (in comparison to the existing ones) productivity;
- to consider the existing and advanced methods for production increase of CDIDPM, operating in the PNS; possible conclusion: the existing and advanced methods of performance improving of CDIDPM in PNS do not always satisfy the increasing demands to the improved performance implementation of integer calculations (denote the main reason);
- to consider one of the possible (referred to in modern literature) options for creation of highly productive CDIDPM on the basis of NSRC; on the basis of the analysis of the NSRC properties and the results of the previous and up-to-date researches of theoretical and practical developments in the application field of non-positional number system, to justify the possibility of its effective application in order to improve the CSIDPM performance.

If the proposed algorithm research scheme is adopted, then the theoretical researches, devoted to the CSIDPM production increase on the basis of NSRC implementation can be carried out. Methods, models and data processing algorithms in NSRC are being developed. Comparative analysis of the achieved results are being conducted.

Before defining a class of tasks and algorithms for which the mathematical apparatus of the numbers theory is effectively applied, it is necessary, on the basis of the results of the NSRC properties researches, to analyze the advantages and disadvantages of the MA use.

III. Conclusion

In the present article it has been shown that the number residues coding, submitted by the respective NSRC bases, is performed by the data from CSSNR. Thus, CSSNR is the basis for the constructing of the non-positional data code structure in NSRC. This is on the one hand. On the other hand the residue classes for each module of NSRC are the basis for the CSSNR formation. Within this framework, strongly mathematically, the notions NSRC and RC cannot be identified. However, experts in the field of MA often use vernacular term RC, having in mind the NSRC.

In the paper there have been specified and systematized the possible fields of science and technology, where there is an urgent need for fast, reliable and high precision integer calculation. There have been shown, that to reach essential "breakthrough" in that direction in PNS is nearly impossible. In fact, the PNS employment in electronics has reached its potential, that is defined by the impossibility to eliminate the inter-bits links between the processed operands in CSIDPM. There is no such drawback in CSIDPM, functioning in NSRC. On the basis of the results of the NSRC properties research, there have been analized the advantages and disadvantages of the MA

use. Having used the results of the analysis of the data integer processing tasks and a set of MA positive properties, in the paper there have been formulated tasks and algorithms classes, for which the NSRC use is essentially more efficient than PNS.

REFERENCES

[1] Akushskii, I. Ya. Mashinnaya arifmetika v ostatochnykh klassakh / I. Ya. Akushskii, D. I. Yuditskii. – M. : Sov. Radio, 1968. – 440 s. (in Russian).

[2] Siora, A. A. Otkazoustoichivye sistemy s versionno-informatsionnoi izbytochnost'yu v ASU TP: monografiya / A. A. Siora, V. A. Krasnobaev, V. S. Kharchenko. – Kh. : MON, NAU im. N. E. Zhukovskogo (KhAI), 2009. – 320 s. (in Russian).

[3] Matthew, Morgado, "Modular arithmetic" [Electronic resource]. Access mode: http://math.uchicago.edu/~may/REU2014/REUPapers/Morgado.pdf. 10.09.2015.

[4] Krasnobayev V.A., Yanko A.S., Koshman S.A. A Method for arithmetic comparison of data represented in a residue number system // Cybernetics and Systems Analysis. – January 2016. – Volume 52, Issue 1, pp. 145-150.

[5] V.A. Krasnobaev, S.A. Koshman, A.S. Yanko "Conception of Realization of Criptographic RSA Transformations with Using of the Residue Number System," ISCI'2017: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov. LAP Lambert Academic Publishing, Omni Scriptum GmbH & Co. KG. Germany, 2017, p. 216. ISBN: 978-3-330-06136-1 [Chapter № 3 in monograph, pp. 81-92].

[6] Krasnobayev V.A., Koshman S.A., Mavrina M.A. A Method for Increasing the Reliability of Verification of Data Represented in a Residue Number System // Cybernetics and Systems Analysis. – November 2014, Volume 50, Issue 6, pp 969–976.

[7] Kuznetsov, O., Gorbenko, Y., Kolovanova, I. Combinatorial properties of block symmetric ciphers key schedule. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 55-58. DOI: 10.1109/INFOCOMMST.2016.7905334

[8] Naumenko, N.I., Stasev, Yu.V., Kuznetsov, A.A. Methods of synthesis of signals with prescribed properties // Cybernetics and Systems Analysis, Volume 43, Issue 3, May 2007, Pages 321-326.

[9] Karpenko O., Kuznetsov A., Sai V., Stasev Yu. Discrete Signals with Multi-Level Correlation Function // Telecommunications and Radio Engineering. - Volume 71, 2012 Issue 1. pages 91-98.

[10] Stasev Yu.V., Kuznetsov A.A., Nosik A.M. Formation of pseudorandom sequences with improved autocorrelation properties // Cybernetics and Systems Analysis, Volume 43, Issue 1, January 2007, Pages 1 – 11. DOI: 10.1007/s10559-007-0021-2

[11] Stasev Yu. V., Kuznetsov A.A. Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes // Cybernetics and Systems Analysis, Volume 41, Issue 3, May 2005, Pages 354 – 363. DOI: 10.1007/s10559-005-0069-9

[12] Yuriy Izbenko, Vladislav Kovtun, Alexandr Kuznetsov. The design of boolean functions by modified hill climbing method // Information technology – New Generation, 2009. ITNG'2009. Proceedings of the 6th International Conference on Information Technology: New Generations, April 27-29, Las Vegas, Nevada, USA., pp: 356-361. DOI: 10.1007/s10559-007-0052-8

[13] Oleksandr Potii, Oleg Illiashenko, Dmitry Komin. Advanced Security Assurance Case Based on ISO/IEC 15408. // Theory and Engineering of Complex Systems and Dependability Advances in Intelligent Systems and Computing Volume 365, 2015, pp 391-401.

[14] Potii A.V., Pesterev A.K. A System Approach to Certification of Pseudorandom Numbers Generators Used in Information Protection Systems // Telecommunications and Radio Engineering. - Volume 52, 1998 Issue 4. pages 97-102.

[15] Gorbenko I.D., Zamula A.A., Semenko Ye.A. Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. - Volume 75, 2016 Issue 2. pages 169-178.

[16] Gorbenko, I.D., Dolgov, V.I.,Rublinetskii, V.I.,Korovkin, K.V. Methods of Information Protection in Communications Systems and Methods of Their Cryptoanalysis // Telecommunications and Radio Engineering. - Volume 52, 1998 Issue 4, pages 89-96.

[17] Gorbenko, I., Ponomar, V. Examining a possibility to use and the benefits of post-quantum algorithms dependent on the conditions of their application // EasternEuropean Journal of Enterprise Technologies. - Vol 2, No 9 (86) (2017), pages 21-32.

[18] Gorbenko, I., Hanzia, R. Examination and implementation of the fast method for computing the order of elliptic curve // EasternEuropean Journal of Enterprise Technologies. - Vol 2, No 9 (86) (2017), pages 11-21.

[19] Gorbenko, I.,Yesina, M.,Ponomar, V. Anonymous electronic signature method // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 47-50.

[20] Kazymyrov, O.,Oliynykov, R.,Raddum, H. Influence of addition modulo 2n on algebraic attacks // Cryptography and Communications. – April 2016, Volume 8, Issue 2, pp 277–289.

[21] Lavrovska, T., Rassomahin, S. Physical model of pseudorandom codes in multidimensional Euclidean space. // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 67-70.

[22] Kavun, S., Mykhalchuk, I., Kalashnykova, N., Zyma, A. (2012). A Method of Internet-Analysis by the Tools of Graph Theory. En: Watada, J., Phillips-Wren, G., Jain, L.C., and Howlett, R.J. (Eds.), Advances in Intelligent Decision Technologies, SpringerVerlag Series "Smart Innovation, Systems and Technologies", Vol. 15, Part 1, Heidelber, Germany, pp. 35-44, DOI: 10.1007/978-3-642-29977-3_4

[23] Kavun, S., Sorbat, I., Kalashnikov, V. (2012). Enterprise Insider Detection as an Integer Programming Problem. En: Watada, J., Phillips-Wren, G., Jain, L.C., and Howlett, R.J. (Eds.), Advances in Intelligent Decision Technologies, SpringerVerlag Series "Smart Innovation, Systems and Technologies", Vol. 12, Heidelber, Germany, pp. 820-829. ISBN 978-3-642-22193-4. ISSN: 2190-3018, DOI: 10.1007/978-3-642-29920-9_29.

[24] Kuznetsov, O., Lutsenko, M., Ivanenko, D. Strumok stream cipher: Specification and basic properties // 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016,, pp. 59-62. DOI: 10.1109/INFOCOMMST.2016.7905335

[25] Kuznetsov, A.A., Smirnov, A.A., Danilenko, D.A., Berezovsky, A. The statistical analysis of a network traffic for the intrusion detection and prevention systems // Telecommunications and Radio Engineering. - Volume 74, 2015, Issue 1, pages 61-78.

[26] Brumnik R., Kovtun V., Okhrimenko A., and Kavun S. (2014). Techniques for Performance Improvement of Integer Multiplication in Cryptographic Applications, Mathematical Problems in Engineering, vol. 2014, Article ID 863617, 7 pages, 2014.

[27] Trydid, O., Kavun, S., Goykhman, M. (2014). Synthesis concept of information and analytical support for bank security system. Actual Problems of Economics,11(161), 449-461. Available from: http://eco-science.net/archive2014/336--11161.html

[28] Vyacheslav Kalashnikov, Timothy I. Matis, José Fernando Camacho Vallejo, and Sergii V. Kavun, "Bilevel Programming, Equilibrium, and Combinatorial Problems with Applications to Engineering," Mathematical Problems in Engineering, vol. 2015, Article ID 490758, 3 pages, 2015. doi:10.1155/2015/490758

[29] Kavun, S. (2015) 'Conceptual fundamentals of a theory of mathematical interpretation', Int. J. Computing Science and Mathematics, Vol. 6, No. 2, pp. 107-121.

[30] Kavun S. (2016). Indicative-geometric method for estimation of any business entity. Int. J. Data Analysis Techniques and Strategies, Vol. 8, No. 2, pp. 87-107.

[31] Alina Zamula and Sergii Kavun, "Complex systems modeling with intelligent control elements", International Journal of Modeling, Simulation, and Scientific Computing Vol. 8, No. 1, 1750009 (2017) [19 pages]

[32] Dolgov, V.I.,Lisitska, I.V.,Lisitskyi, K.Ye. The new concept of block symmetric ciphers design // // Telecommunications and Radio Engineering. - Volume 76, 2017 Issue 2. pages 157-184. DOI: 10.1615/TelecomRadEng.v76.i2.60

[33] Shamov S. Use of quality control of activity processes descriptions to the initial documents of re-engineering project. Radioelectronic and computer systems. Scientific and technical magazine, 6, 158-163, 2012.