DOI: 10.15587/978-617-7319-98-5.CH1

Victor Krasnobayev, Alina Yanko, Alina Hlushko,
Oleg Kruk, Oleksandr Kruk, Vitalii Gakh

CHAPTER 1

CYBERSPACE PROTECTION SYSTEM BASED ON THE DATA COMPARISON METHOD

ABSTRACT

In the conditions of growing challenges in cyberspace, the information environment protection system is a preventive mechanism of protection against real and potential risks and threats to national interests. The study analyzed the position of Ukraine in the world rankings for cyber security and outlined promising directions for increasing its level, one of which is the improvement of information protection systems of critical infrastructure objects. A system of protection of the information environment against cyberattacks using of the modular number system based on non-positional code structures is proposed. Of the various options for the practice of intrusion detection and prevention systems, this chapter discusses the data comparison algorithm, which consists in continuously monitoring and scanning data by constantly comparing data with user and service information patterns, as well as threat patterns and indicators based on previous experience, not only own, within the local network or system, but also on a global scale.

The chapter presents an improved method of fast comparison, which allows to carry out the comparison procedure in the modular number system, both in positive and negative numerical ranges. Improving the method of fast comparison of two integers is carried out by increasing the accuracy of comparison, by representing numbers in an artificial form, which expands the area of effective use of computer systems for processing integer economic data in the modular number system. The use of an improved method for fast comparison of data in the modular number system for one-byte, two-byte, three-byte, four-byte and eight-byte numerical bit grids of the computer systems, respectively, by 16 %, 37 %, 50 %. It is 58 % and 72 % more efficient in terms of number comparison time than using the fastest of the existing number comparison methods in the modular number system, which is based on the principle of nulling. The proposed method provides maximum comparison accuracy with a minimum amount of equipment for comparing devices. This circumstance makes it possible to obtain a reliable result of the data control operation. Its use makes it possible to identify potential cyber threats and take preventive measures, which will increase the level of protection of critical infrastructure objects.

KEYWORDS

Arithmetic comparison, computer systems for processing integer economic data, cyberattacks, cybersecurity, cyber protection, data comparison methods, financial losses, information security, modular number system, non-positional number system, nulling constants, positional features of a non-positional code, single-line binary code, threats.

The digitalization processes rapid development gave an impetus to the development of cyberterrorism in the world. The growth of cyberattacks on critical infrastructure objects in recent years has made the information environment protecting issue as a basis for ensuring the countries national security as a whole. After all, their destructive influence extends to all the national economy spheres and is a threat to national interests. Losses from realized cyber incidents are measured not only by financial costs. The hybrid aggression of the Russian Federation against Ukraine since the beginning of 2022 has turned into a cyberwar and a full-scale military invasion. Mass cyberattacks against Ukraine state structures and businesses, which are aimed at disrupting the functioning of strategic life support facilities, require an increase in the cybersecurity level. Under the conditions of constant cyber risks and cyber threats growing the monitoring of Ukraine cybersecurity level, highlighting the main problems of national cyber protection system accretion and determination of their solving directions are important.

1.1 ANALYSIS OF MODERN APPROACHES TO CYBERSECURITY RESEARCH

The issue of cyber security is currently one of the leaders of current topics in the world, which is characterized and confirmed by active research by scientists. The issue of the formation of an effective mechanism for countering threats in the cyber sphere is clearly and in detail considered in the work of Yusif Salifu, Abdul Hafeez-Baig [1]. The authors investigated a model for effective cybersecurity management, which is based on such key components as a cybersecurity strategy, standardized processes, compliance with the requirements, senior management oversight, and resources. In the conditions of growing challenges in cyberspace, the subject of research of leading scientists are also the processes of legal support and management of cyber and information security in general, both at the national and international levels [2, 3].

The development and improvement of over-reliable computer systems (CS) is a strategically important and topical issue and is under the special control of the heads of states and governments of the advanced countries of the world. There are many approaches and tools that contribute to the stability and security of countries in cyberspace, which consist of political strategies such as the strategy of persistent engagement, recently used in the United States [4, 5] and technical methods. Among the main effective technical methods used by modern cyber

threat detection systems is the use of various data comparison methods, the main ones of which were researched by the American scientist Michael Collins [6].

The more unique and individual data protection and monitoring systems are (created exclusively for a specific object and not for mass application), the higher the level of protection against cyber-attacks has been proven by Zhang Hao Goh, Minzheng Hou, Hichang Cho [7].

Some Chinese scientists Jian Liu, Junjie Yan, Jun Jiang, Yitong He, Xuren Wang, Zhengwei Jiang and others have studied the existing positional binary number system and concluded that it has flaws, and the existing hacking methods, hacking attacks, viruses and information integrity violations are constructed using a binary positional code. Therefore, it is natural to search for opportunities to apply such arithmetic to which existing threats are not adapted [8]. In this regard, the non-positional number system (NNS) based on the Chinese residuals theorem, the so-called modular number system (MNS), draws attention. The results of research in the field of the creation of high-reliable CS of well-known authors (M. Valakh, A. Svoboda, N. Sabo, I. Y. Aksushskyi, D. I. Yuditskyi, V. M. Glushkov, V. A. Torgashov, V. M. Amberbaev, A. A. Kolyada, A. Shimbo, P. Paulier, M. A. Thornton, R. Dreschler, D. M. Miller, and others) showed that the use of NNS as a system of calculations of CS, intended for the implementation of reliable integer arithmetic operations, significantly increases the reliability of data processing of the solution of problems of a certain class.

Indeed, as the review of the literature showed, today the field of use of the MNS is limited to a certain class of solvable problems: implementation of integer arithmetic operations of addition, subtraction and multiplication of numbers in the positive numerical range. The lack of methods of comparing integers presented in the MNS, both in the positive and negative numerical ranges, significantly narrows the area of effective use of the MNS. Therefore, when improving the method of comparing numbers, numbers were considered in the form of a string, which makes it possible to carry out an algebraic comparison of data (taking into account the sign of the number).

The purpose of the work is to research the cybersecurity of Ukraine in the conditions of military aggression, to determine the level of cyber resilience of Ukraine and directions for improving cyber protection in the terms of deepening cyberwarfare, development of data comparison methods based on non-positional code structures, which will ensure maximum accuracy for cyber intrusion detection and prevention systems.

The research in the article is based on the application of data comparison principles and reliability improvement methods based on the use of non-traditional machine arithmetic. The set of properties of the MNS was used in the scientific research, namely: independence, equality, and low-bitness (low-digit capacity) of the residuals that define the non-positional code data structure of the MNS provides high reliable for the implementation in the CS of computational algorithms consisting of a set of arithmetic (modular) operations.

Using one more property of the arithmeticity of the MNS codes, which allows to find and correct errors in the process of performing arithmetic operations, which is the most important advantage of the MNS over all positional systems, including a binary code, where on the contrary, in an arithmetic device if an error occurs once, it multiply uncontrollably [9].

A distinctive feature of this article is that the proposed methods for improving the reliability of information processing in the CS, which consists in comparing data using MNS, are brought to algorithms, on the basis of which classes of patentable devices that implement such algorithms have been developed and for which Ukrainian patents have been obtained [10]. A significant part of the received patents has found practical application in the creation of specialized real-time CS for processing large arrays of integer economic data [3]. The paper gives examples of specific application of methods and algorithms for arithmetic and algebraic comparison of data in the MNS.

1.2 THE LEVEL OF CYBERSECURITY OF UKRAINE IN THE CONDITIONS OF GROWING THREATS

The IT technologies development, the digital environment rapid transformation along with undeniable advantages have led to the information environment risks and threats deepening [11], in cyberspace in particular. Thus, if at the beginning of 2020 the number of cyberattacks in the world was about 5 thousand per week, then at the beginning of 2021 their number increased to 200 thousand (Financial Stability Board, 2021). At the same time, 19 % of all cyberattacks in the world, recorded in 2021, were committed against Ukraine (in the first place among the countries against which cyberattacks are directed is the USA – 46 %). For comparison, the share of Belgium, Germany and Japan does not exceed 3 % (**Fig. 1.1**).

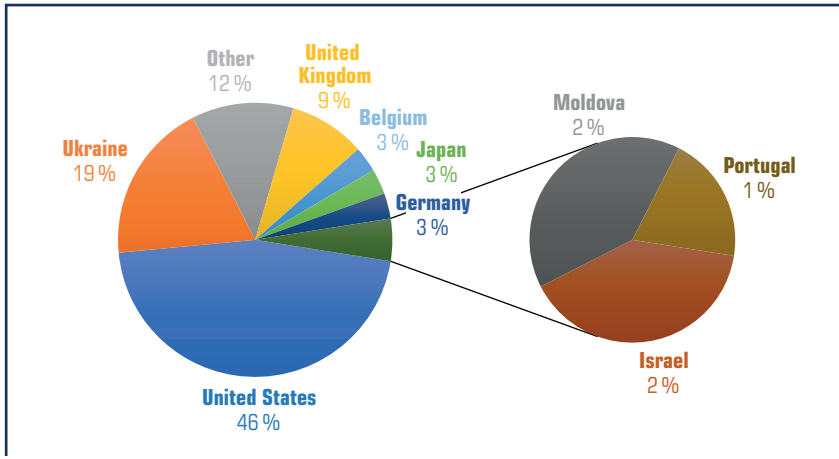

Fig. 1.1 Ranking of countries by the number of cyberattacks in 2021

According to the official data of the Microsoft company [12], the largest number of cyberattacks during the II half of 2020 and the I half of 2021 were carried out from the territory of the Russian Federation – 58 % out of the entire recorded number.

According to official data, Ukraine ranks second in the world rankings in terms of the number aimed at the country's critical infrastructure, i.e. such industries as energy, finance, telecommunications, etc., and state electronic information resources, the disruption of which is a threat to national interests [13]. Since the beginning of 2022, the Russian Federation, before a full-scale invasion, has been waging a cyberwar against Ukraine – the intensity of cyberattacks is increasing: in January alone, 6.8 million suspicious information security events, 25.5 thousand potential cyber incidents and 121 cyberattacks were stopped. For comparison, in April 2021, specialists of the Security Service of Ukraine detected 1.5 million suspicious events and stopped 53 critical cyber incidents [14]. In January-February 2022, 436 cyberattacks were carried out on critical infrastructure facilities and state information resources of Ukraine, compared to 64 in the same period of 2021. The largest of them are presented in **Fig. 1.2**.

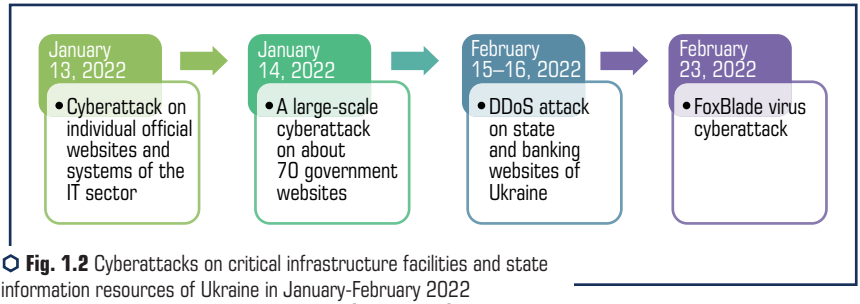

Fig. 1.2 Cyberattacks on critical infrastructure facilities and state information resources of Ukraine in January-February 2022
Note: compiled by the authors according to [12, 14–16]

According to the data of the National Security Council of the United States and the National Cybersecurity Center of Great Britain, the cyberattacks were organized by the Intelligence Department of the General Staff of the russian federation [17, 18]. In March-May 2022, along with military aggression, cyberattacks on the energy sector, logistics infrastructure, Ukrainian online media sites, and official state resources continue.

Ransom ware, insider attacks, phishing, targeted cyberattacks and DDoS attacks are identified as the main types of cyberattacks that pose the greatest threat to the national economy information security [19]. Their destructive influence causes, first of all, significant financial losses. Thus, according to the American company McAfee, which specializes in computer security, and the Center for Strategic and International Studies (CSIS), in 2020, global economic losses as a result of cyberattacks amounted to more than 1 trillion USD, which was 1 % of global GDP. Compared to 2018, this indicator increased by more than 50 %. In 2021, losses from cyberattacks increased to 4.2–6 trillion USD (**Fig. 1.3**). It is predicted that in 2025, the volume of financial losses from cybercrime will reach 10.5 trillion USD.

It should be noted that in 2021, the highest average cost of a data breach over the past 17 years was recorded – 4.24 million USD. A similar figure for 2020 was 3.86 million USD [21].

The most common cause of data leakage was phishing attacks. In addition to direct financial losses, cyberattacks cause loss of working time, as well as the loss of the company's image [13, 22]. There are other hidden losses from cybercrime – in particular, a decrease in employee job satisfaction.

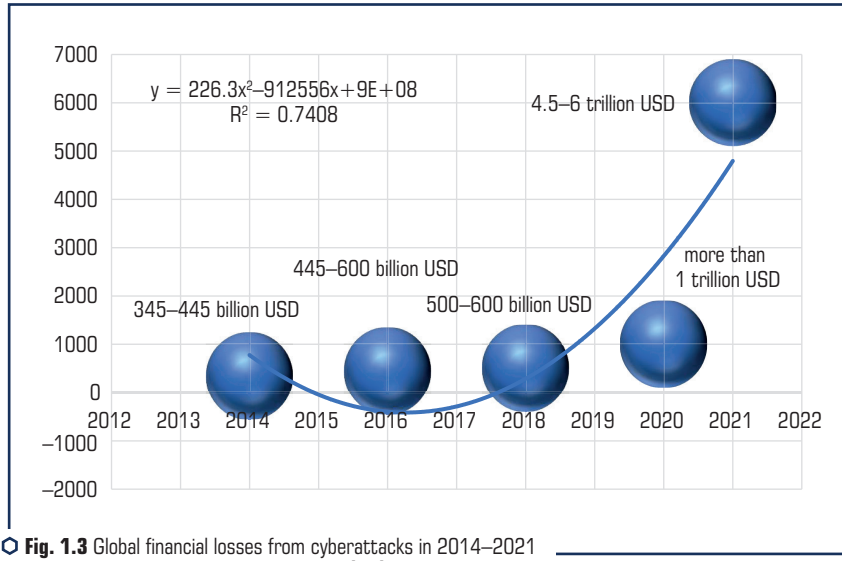

Fig. 1.3 Global financial losses from cyberattacks in 2014–2021
Note: compiled by the authors according to [20]

Taking into account the growth of negative financial consequences from the cyber threat's implementation, the need to increase the cybersecurity level under the circumstances of a cyberwar with the Russian Federation is unconditional.

To date, a number of global indices have been developed which allow determining the country capabilities in the field of cyber protection, assessing its cyber power, specifically, the regulatory measures and means ability to achieve strategic cybersecurity goals. Ukraine's high potential in this direction should be noted. This is confirmed by the positions in the world rankings, the comparative characteristics of which are presented in **Table 1.1**.

According to the National Cybersecurity Index (NCSI), which measures the countries readiness to prevent cyber threats and manage cyber incidents, Ukraine rose to 24th place among 160 countries at the end of 2021 and improved its position by 4 points compared to 2019. Ukraine is approaching Switzerland (23rd place) and Great Britain (22nd place) in terms of cyber protection capabilities of the national information space. At the same time, according to the Global Cybersecurity Index (GCI), Ukraine ranks 78th. According to the National Cyber Prowess Index (NCPI), which measures the effectiveness of government strategy, crime response and countermeasures, defense capabilities, resource allocation, private sector participation, workforce efficiency and

cybersecurity innovation, in 2020, Ukraine ranked only 26th out of 30 countries in the world and 10th among European countries. At the same time, it should be noted that the countries that had the most developed cybersecurity forces were included in the rating, which confirms the existence of potential opportunities for building up cyber capabilities and increasing the level of information security in Ukraine.

Graphical interpretation of Ukraine's positions in the world cybersecurity rankings and their dynamics are presented in **Fig. 1.4**.

Table 1.1 Comparative characteristics of global indices on cybersecurity

	National Cybersecurity Index (NCSI)	Global Cybersecurity Index (GCI)	National Cyberpower Index (NCPI)
Published last year	2021	2021	2020
Developer	Estonian Academy of e-Government	International Telecommunications Union	Belfer center
Countries Assessed	160	194	30
Indicators	12 General cybersecurity indicators	20 indicators	27 Capability 32 Intent
Ukraine's place in the ranking	24	78	26

Note: compiled by the authors according to [23–25]

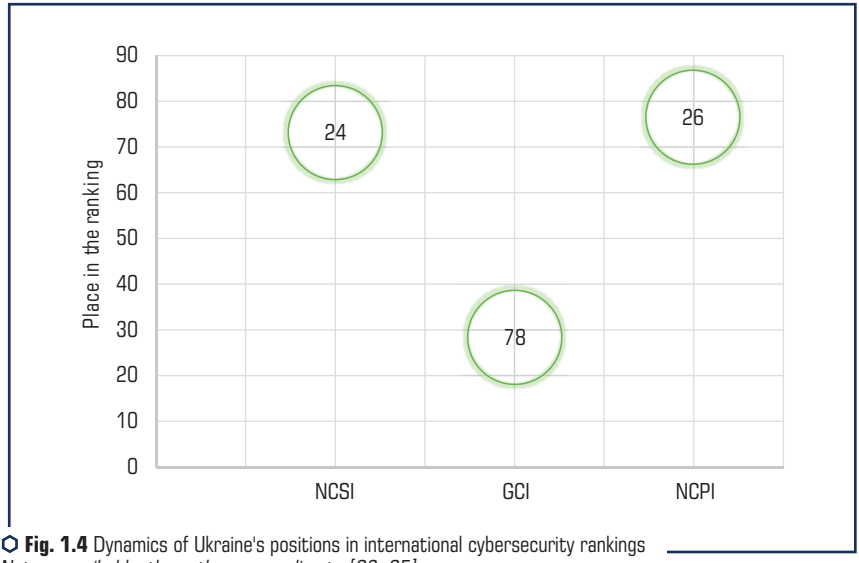

Fig. 1.4 Dynamics of Ukraine's positions in international cybersecurity rankings
Note: compiled by the authors according to [23–25]

The potential of Ukraine in the field of cybersecurity is noted not only by world ratings, but also by international organizations. Among other things, at the beginning of April 2022, Ukraine was admitted to the NATO Cooperative Cyber Defence Centre of Excellence as a contributing member.

The positive dynamics connected, inter alia, with the improvement of domestic legislation in the field of information and cybersecurity is noted. At present, the legal framework for regulating and ensuring security in the information space, including cyberspace, includes: the Constitution of Ukraine, the Law of Ukraine "On National Security of Ukraine", the Law of Ukraine "On the Concept of the National Informatization Program", the Law of Ukraine "On Basic Principles of the Development of the Information Society Development in Ukraine for 2007–2015", National Security Strategy, Information Security Strategy, Cybersecurity Strategy of Ukraine, Concept for the Development of the Digital Economy and Society of Ukraine for 2018–2020, Concept for the Development of Digital Competences, International Standards of the ISO/IEC 27000 series, regulatory papers in the field of information technical defense (RP ITD) and national standards of Ukraine on creating and functioning of CSID, other regulatory law acts which control interactions on the field of information defense.

The strengthening of cooperation with international organizations in the field of cybersecurity is also noted. In September 2021, the State Service for Special Communications and Information Protection of Ukraine made an agreement with the US Agency for Cybersecurity and Infrastructure Security, which provides: coordination of actions to protect critical information infrastructure objects and improvement of the response system to cyber incidents; exchange of experience within the framework of the risk management system, which will ensure Ukraine's national resilience to cyber threats; use of the US experience in organizing the government bodies interaction and business in the field of cybersecurity; implementation of international technical assistance projects related to the construction of a network of branch and regional Security Operation Center and Computer Security Incident Response Team (CSIRT) which are implied by the Strategy of Cybersecurity of Ukraine.

The accession of Ukraine to the Joint Center of Advanced Technologies for NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which took place in April 2022, provides an opportunity to exchange experience in detecting and countering modern cyber threats, practicing the skills of joint response to cyberattacks and conducting defense and deterrence operations in cyberspace.

The development of international cooperation in the direction of strengthening Ukraine's cyber resilience is a priority task in order to prevent global information threats, ensure a high-level quality of cybercrime investigations, arrest and prosecute malicious agents, and overcome cybersecurity problems.

At the same time, there are directions in the field of cybersecurity that have a negative impact on Ukraine's position in the specified ratings and require improvement. In particular, the low level of contribution to global cybersecurity to date, the insufficient level of digital services protection, the insufficiently developed direction of military cyber operations.

It should be noted that since the beginning of 2022, vigorous activities have been conducted in all the noted problematic aspects: Ukraine has become an active participant in international cooperation in the field of cybersecurity; there is a process of forming a cyber-army [26, 27], which is responsible for information security, protection of critical infrastructure and intelligence.

Considering Ukraine's achievements in cyberspace, it is legitimate to define it as an equal participant in the international arena in the field of cybersecurity. Prospective tasks should be the further improvement of information protection systems of critical infrastructure objects based on best global practices, as well as the coordination of actions with international organizations to counter threats related to the development of the digital economy and information society.

The construction of an effective cybersecurity system in the aspect of comprehensive counteraction to cyber threats will contribute to the formation of a preventive mechanism for countering threats and their containment, anticipatory response to dynamic changes occurring in cyberspace, which is necessary in the conditions of cyberwar. Methods and algorithms of security systems against unauthorized intruders are, as a rule, developed for a specific object of protection. But regardless of the protection object, whether it is a large commercial network, a state-level server, or a simple user's mobile device, there is one common goal, which is to protect data as the main element of information security.

In order to protect any system, it is necessary first to detect an intrusion (attack) regardless of the type, whether it will be viruses (classic file viruses or ransomware viruses, so-called Ransomware encryptors), phishing, DDoS attacks, botnets, backdoors, or other hacking attempts it is the task of Intrusion Detection System (IDS). The next step is to decide how to eliminate this cyberattack and, based on this experience, create a reliable algorithm for protection against threats of this type, this is the task of Intrusion Prevention System (IPS). There are various modes of systems for detecting and preventing intruders, but, as a rule, the algorithm is the same, when detecting and eliminating attacks, the task of security systems is also to create templates of potential threats. In the further process of continuous data monitoring and scanning, a constant comparison of data with user templates and service information, as well as with threats templates and indicators based on previous experience, not only within the local network or system, but also on a global scale [6].

At the moment there are various programs (Azure Security Center, Microsoft Advanced Threat Analytics) with a templates database of all threats that had been identified before that in the world. Also, there are many sites with which you can get information about new indicators and templates, as well as make your own contribution to the cyber protection IT community by sharing your types of attacks, if they are not available on this platform [28].

It is very important that cyberattack protection systems compare all data on a wide scale and make correlations not only by the traffic pattern, but also by the user profile, since otherwise the chances of false positives increase. It is possible to use different security centers, software and hardware protection, but all of them make decisions as a result of monitoring based on certain data comparison methods. Since all data is presented in the form of a binary code, the task is reduced to comparing numbers [29].

In previous studies, the advantage of using computer systems for processing integer economic data (CSPIED) based on the system of final classes was proven modular number system (MNS). It is known that using a non-positional number system in the MNS enables the organization of

integer data rapid processing procedure, i.e. the possibility of creating methods and tools that provide high user productivity in solving a certain class of problems (implementation of arithmetic operations of addition, subtraction, multiplication). This is achieved due to the use of such properties of the MNS as independence and small-scale residuals $\{s_i\}$, the set of which is a number $S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$ according to n bases (modules m_n) of this MNS, by using tabular machine arithmetic. The need to perform non-positional operations of comparing two numbers $S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$ and $T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)$ when solving CSPIED problems and algorithms of various purposes reduces the overall efficiency of using MNS. This is due to the significant implementation time (compared to the time of performing the above-mentioned arithmetic operations) of the comparing two numbers in the MNS operation. Therefore, the research and development of mathematical models, methods and algorithms for comparing numbers in the MNS is an important and urgent task [30].

At present, it is possible to distinguish three groups of methods of comparing numbers in the MNS. The first group includes methods of direct comparison based on the transformation of numbers S_{MNS} and T_{MNS} from the MNS code to the positional number system (PNS) $S_{PNS} = \overline{s_{m-1}, s_{m-2} \ldots s_0}$ and $T_{PNS} = \overline{t_{m-1}, t_{m-2}, \ldots . t_0}$ (ρ – digits of numbers S_{MNS} and T_{MNS}) and their further comparison based on the use of binary positional adders. The second group of methods includes methods based on the principle of nulling. The procedure of the nulling process consists of moving from the initial number $S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$ presented in the MNS to the species $S_{MNS}^{(N)} = (0, 0, \ldots, 0, \chi_n^{(S)})$. After that, by value $\chi_n^{(S)}$ the interval $\left[gm_i, (g+1)m_i \right)$ hitting numbers S_{MNS} is determined. Nulling of the number is carried out similarly $T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)$, from where let's get the values $\chi_n^{(T)}$. Positional comparison of the obtained values $\chi_n^{(S)}$ and $\chi_n^{(T)}$ determines the result of comparing numbers S_{MNS} and T_{MNS}. The third group of methods includes methods based on the determination (selection) or formation of special features, so-called positional features of a non-positional code (PFNC). PFNC data (for example, rank r numbers S_{MNS}) carry additional information about the magnitude of the numbers that are compared [31].

The common disadvantages of all currently existing groups of methods comparisons are the time and hardware complexity of organizing an effective comparison, as well as the possibility of obtaining an unreliable result of comparing two numbers operation due to calculated errors. The abovementioned material is the basis for using a new comparison method.

1.3 METHOD OF ARITHMETIC COMPARISON OF DATA IN THE MNS

Let's consider the numbers arithmetic comparison method of $S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$ and $T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)$, based on the use of PFNC of these numbers, by forming a single-line binary code (SLBC). Let the MNS be given by the set $\{m_i\}$, $i = \overline{1, n}$, pairs of prime numbers. The greatest common divisor (GCD) of any pair is based on m_i and m_g $\left(i, g = \overline{1, n}; i \neq g\right)$ is equal to unity, i.e., $\text{GCD}\left(m_i, m_g\right) = 1$. For the sake of common sense, let the MNS be ordered $\left(m_i < m_{i+1}\right)$.

The essence of the proposed method is that the initial numbers S_{MNS} and T_{MNS} by means of nulling constants (NC) of the form $NC_{m_i}^{(S)} = (s'_1, s'_2, \ldots, s'_{i-1}, s_i, s'_{i+1}, \ldots, s'_n)$ and $NC_{m_i}^{(T)} = (t'_1, t'_2, \ldots, t'_{i-1}, t_i, t'_{i+1}, \ldots, t'_n)$ are reduced to numbers $S_{t_i} = S_{MNS} - NC_{m_i}^{(S)} = (s_1, s_2, \ldots, s_{k-1}, s_k, s_{k+1}, \ldots, s_n) - (s'_1, s'_2, \ldots, s'_{i-1}, s_i, s'_{i+1}, \ldots, s'_n) = (s_1^{(1)}, s_2^{(1)}, \ldots, s_{i-1}^{(1)}, 0, s_{i+1}^{(1)}, \ldots, s_n^{(1)})$, $T_{m_i} = T_{MNS} - NC_{m_i}^{(T)} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n) - (t'_1, t'_2, \ldots, t'_{i-1}, t_i, t'_{i+1}, \ldots, t'_n) = (t_1^{(1)}, t_2^{(1)}, \ldots, t_{i-1}^{(1)}, 0, t_{i+1}^{(1)}, \ldots, t_n^{(1)})$, a multiple of a certain chosen one p_i MNS module. Further, by means of the aggregate $0, m_i, 2 \cdot m_i, \ldots, (N-2) \cdot m_i, (N-1) \cdot m_i$ of N constants multiples of the base m_i, subtraction operations are carried out in parallel in time $S_{m_i} - K_S \cdot m_i = Z_{K_S}^{(S)}$ and $T_{m_i} - K_T \cdot m_i = Z_{K_T}^{(T)}$, $(K_S(K_T) = \overline{0, N-1})$ that:

$$\begin{cases} S_{m_i} - 0 \cdot m_i = Z_0^{(S)}, \\ S_{m_i} - 1 \cdot m_i = Z_1^{(S)}, \\ S_{m_i} - 2 \cdot m_i = Z_2^{(S)}, \\ \quad \ldots \\ S_{m_i} - (N-1) \cdot m_i = Z_{N-1}^{(S)}; \end{cases} \quad \begin{cases} T_{m_i} - 0 \cdot m_i = Z_0^{(T)}, \\ T_{m_i} - 1 \cdot m_i = Z_1^{(T)}, \\ T_{m_i} - 2 \cdot m_i = Z_2^{(T)}, \\ \quad \ldots \\ T_{m_i} - (N-1) \cdot m_i = Z_{N-1}^{(T)}, \end{cases} \tag{1.1}$$

where

$$N_{m_i} = \prod_{k=1;\ k \neq i}^{n} m_k,$$

N_{m_i} – the number of binary digits in SLBC records $K_{N_{m_i}}^{(n_S)}$ and $K_{N_{m_i}}^{(n_T)}$ or the number of adders performing type operations $S_{m_i} - K_S \cdot m_i = Z_{K_S}^{(S)}$ or $T_{m_i} - K_T \cdot m_i = Z_{K_T}^{(T)}$.

Thus, an SLBC of the binary sequence type is formed $K_{N_{m_i}}^{(n_S)} = \{Z_{N_{m_i}-1}^{(S)} Z_{N_{m_i}-2}^{(S)} \ldots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)}\}$ for the number S_{MNS}, with only one value $Z_{K_S}^{(S)} = 0$. In the case that $S_{m_i} - n_S \cdot m_i = 0$. Other values $Z_{K_S}^{(S)} = 1$, if $S_{m_i} - q \cdot m_i \neq 0$, $q = \overline{0, N-1}$, $q \neq n_S$. In this case, the SLBC is issued $K_{N_{m_i}}^{(n_S)}$ and $K_{N_{m_i}}^{(n_T)}$ is a sequence consisting of N_{m_i} binary levels. In this sequence, only one binary digit is zero, and the rest are ones. Locations of zero discharges of the SLBC $K_{N_{m_i}}^{(n_S)}$ and $K_{N_{m_i}}^{(n_T)}$ determine PFNC n_S and n_T respectively, the numbers S_{MNS} and T_{MNS}. In a similar way, the SLBC of the form is formed $K_{N_{m_i}}^{(n_T)} = \{Z_{N_{m_i}-1}^{(T)} Z_{N_{m_i}-2}^{(T)} \ldots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)}\}$ for the number T_{MNS}. At the same time, the meaning $Z_{K_T}^{(T)} = 0$ (if $T_{m_i} - n_T \cdot m_i = 0$), and the other values $Z_{K_T}^{(T)} = 1$, if $T_{m_i} - q \cdot m_i \neq 0$ $(q = \overline{0, N-1},\ q \neq n_T)$ [9].

The method of arithmetic comparison of two numbers in the MNS consists in performing the following steps of the algorithm:

1. Representation of compared numbers in the MNS:

$$S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$$

and

$$T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n).$$

2. Formation by values s_n and t_n of nulling constants of the species:

$$NC_{m_i}^{(S)} = \left(s'_1, s'_2, \ldots, s'_{i-1}, s_i, s'_{i+1}, \ldots, s'_n\right)$$

and

$$NC_{m_i}^{(T)} = \left(t'_1, t'_2, \ldots, t'_{i-1}, t_i, t'_{i+1}, \ldots, t'_n\right).$$

3. Determining the values of the difference of numbers S_{m_i} and T_{m_i}:

$$S_{m_i} = S_{MNS} - NC_{m_i}^{(S)} = \left(s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n\right) - \left(s'_1, s'_2, \ldots, s'_{i-1}, s_i, s'_{i+1}, \ldots, s'_n\right) =$$
$$= \left(s_1^{(1)}, s_2^{(1)}, \ldots, s_{i-1}^{(1)}, 0, s_{i+1}^{(1)}, \ldots, s_n^{(1)}\right)$$

and

$$T_{m_i} = T_{MNS} - NC_{m_i}^{(T)} = \left(t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n\right) - \left(t'_1, t'_2, \ldots, t'_{i-1}, t_i, t'_{i+1}, \ldots, t'_n\right) =$$
$$= \left(t_1^{(1)}, t_2^{(1)}, \ldots, t_{i-1}^{(1)}, 0, t_{i+1}^{(1)}, \ldots, t_n^{(1)}\right).$$

4. Definition of the SLBC components $z_i^{(S)}$ and $z_g^{(T)}$:

$$K_{N_{m_i}}^{(n_S)} = \left\{Z_{N_{m_i}-1}^{(S)} Z_{N_{m_i}-2}^{(S)} \ldots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)}\right\}$$

and

$$K_{N_{m_i}}^{(n_T)} = \left\{Z_{N_{m_i}-1}^{(T)} Z_{N_{m_i}-2}^{(T)} \ldots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)}\right\}.$$

By means of adders, using a set of constants $\left(0, m_i, \ldots, (N-1)\cdot m_i\right)$ by formulas $S_{m_i} - K_S \cdot m_i = Z_{K_S}^{(S)}$ and $T_{m_i} - K_T \cdot m_i = Z_{K_T}^{(T)}$ components are defined $z_i^{(S)}$ and $z_g^{(T)}$.

5. Formation of quantitative values of PFNC n_S and n_T. By type of the SLBC $K_{N_{m_i}}^{(n_S)} = \{Z_{N_{m_i}-1}^{(S)} Z_{N_{m_i}-2}^{(S)} \ldots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)}\}$ and $K_{N_{m_i}}^{(n_T)} = \{Z_{N_{m_i}-1}^{(T)} Z_{N_{m_i}-2}^{(T)} \ldots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)}\}$ the values of the binary digits of the SLBC are determined for which $Z_{n_S}^{(S)} = 0$ and $Z_{n_T}^{(T)} = 0$.

6. Implementation of the comparison operation result algorithm S_{MNS} and T_{MNS}:

$$S_{MNS} = T_{MNS}, \text{ if } \left(n_S = n_T\right); S_{MNS} > T_{MNS}, \text{ if } \left(n_S > n_T\right); S_{MNS} < T_{MNS}, \text{ if } \left(n_S < n_T\right).$$

Table 1.2 Algorithm for arithmetic comparison of numbers in the MNS

No.	Number comparison result	Condition for performing comparison operations
1	$S_{MNS} = T_{MNS}$	$n_S = n_T$
2	$S_{MNS} > T_{MNS}$	$n_S > n_T$
3	$S_{MNS} < T_{MNS}$	$n_S < n_T$

To illustrate the essence of the comparison method, let's consider the geometric interpretation of the proposed method for comparing two numbers. **Fig. 1.5** presents a numerical segment [0, D], corresponding to the range of representation of the compared numbers $S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$ and $T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)$, where $D = \prod_{i=1}^{n} m_i$. This segment is divided into intervals $[gm_i, (g+1)m_i)$, of length m_i units each. The operation of converting the initial numbers S_{MNS} and T_{MNS} via nulling constants $NC_{m_i}^{(S)} = (s'_1, s'_2, \ldots, s'_{i-1}, s_i, s'_{i+1}, \ldots, s'_n)$ and $NC_{m_i}^{(T)} = (t'_1, t'_2, \ldots, t'_{i-1}, t_i, t'_{i+1}, \ldots, t'_n)$ to the species:

$$S_{m_i} = S_{MNS} - NC_{m_i}^{(S)} = (s_1, s_2, \ldots, s_{k-1}, s_k, s_{k+1}, \ldots, s_n) - (s'_1, s'_2, \ldots, s'_{i-1}, s_i, s'_{i+1}, \ldots, s'_n) =$$

$$= (s_1^{(1)}, s_2^{(1)}, \ldots, s_{i-1}^{(1)}, 0, s_{i+1}^{(1)}, \ldots, s_n^{(1)})$$

and

$$T_{m_i} = T_{MNS} - NC_{m_i}^{(T)} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n) - (t'_1, t'_2, \ldots, t'_{i-1}, t_i, t'_{i+1}, \ldots, t'_n) =$$

$$= (t_1^{(1)}, t_2^{(1)}, \ldots, t_{i-1}^{(1)}, 0, t_{i+1}^{(1)}, \ldots, t_n^{(1)})$$

is equivalent to shifting comparable numbers to the left edge of the corresponding intervals $[g_1 m_i, (g_1+1)m_i)$ and $[g_2 m_i, (g_2+1)m_i)$ their initial location, which corresponds to reducing them to numbers S_{m_i} and T_{m_i}, multiple modulo m_i MNS. Then the numbers are determined $g_1 = n_S$ and $g_2 = n_T$ these intervals (see expression (1)), which is the PFNC of numbers in the MNS.

Consider an example of a specific implementation of the operation of arithmetic comparison of numbers in the MNS with bases $m_1 = 2$, $m_2 = 3$ and $m_3 = 5$, where in $D = \prod_{i=1}^{n} m_i = 2 \cdot 3 \cdot 5 = 30$; $N_{m_i} = \prod_{k=1;\, k \neq i}^{n} m_k = N_{m_3} = N_5 = \prod_{k=1;\, k \neq 3}^{2} m_k = m_1 \cdot m_2 = 2 \cdot 3 = 6$ (**Fig. 1.6**). **Table 1.3** shows the code words for this MNS. **Table 1.4** shows the NC and **Table 1.5** shows the sets of constants in the MNS with bases $m_1 = 2$, $m_2 = 3$ and $m_3 = 5$.

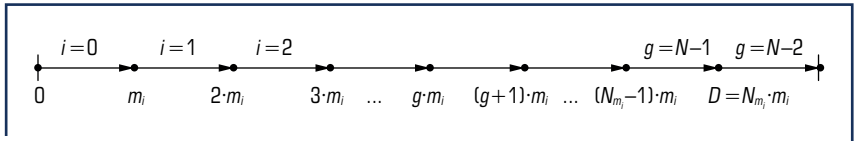

Fig. 1.5 Intervals of splitting the numerical axis [0, *D*) for an arbitrary base m_i MNS

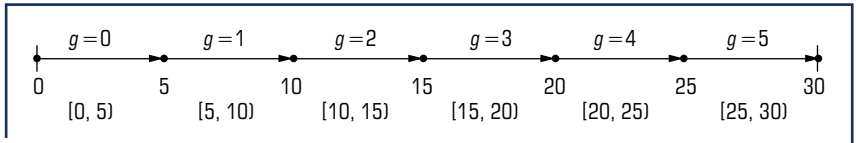

Fig. 1.6 Intervals of splitting the numerical axis [0, *D*) for the base $m_i = 5$ MNS

The application of the considered method enables to carry out an exact comparison of two numbers only if these numbers are found in different numerical intervals $\left[g_1 m_i, (g_1+1)m_i\right)$ and $\left[g_2 m_i, (g_2+1)m_i\right)$. When the values are equal to numbers $g_1 = g_2 = g$, the accuracy of the comparison depends on the size of the interval $\left[gm_i, (g+1)m_i\right)$, i.e. from the value of the value of the MNS module.

Table 1.3 Code word table

$S(T)$ in PNS	$S_{MNS}(T_{MNS})$ in the MNS			$S(T)$ in PNS	$S_{MNS}(T_{MNS})$ in the MNS		
	$m_1=2$	$m_2=3$	$m_3=5$		$m_1=2$	$m_2=3$	$m_3=5$
0	0	00	000	15	1	00	000
1	1	01	001	16	0	01	001
2	0	10	010	17	1	10	010
3	1	00	011	18	0	00	011
4	0	01	100	19	1	01	100
5	1	10	000	20	0	10	000
6	0	00	001	21	1	00	001
7	1	01	010	22	0	01	010
8	0	10	011	23	1	10	011
9	1	00	100	24	0	00	100
10	0	01	000	25	1	01	000
11	1	10	001	26	0	10	001
12	0	00	010	27	1	00	010
13	1	01	011	28	0	01	011
14	0	10	100	29	1	10	100

Table 1.4 The contents of the block of nulling constant (BNC)

$s_3(t_3)$	Constants		
	$m_1=2$	$m_2=3$	$m_3=5$
000	0	00	000
001	1	01	001
010	0	10	010
011	1	00	011
100	0	01	100

Table 1.5 Constants for the formation of the SLBC

$g \cdot m_3\ (g = \overline{0, 5})$	Constants in the MNS		
	$m_1 = 2$	$m_2 = 3$	$m_3 = 5$
0	0	00	000
5	1	10	000
10	0	01	000
15	1	00	000
20	0	10	000
25	1	01	000

Let's give an example of the implementation of the operation of comparing two numbers for the case $g_1 = g_2 = g$.

Example 1. Let the compared operands $S = 23\ (S_{MNS} = (1, 10, 011))$ and $T = 21 (T_{MNS} = (1, 00, 001))$ will be presented in the form in the MNS (**Fig. 1.7**).

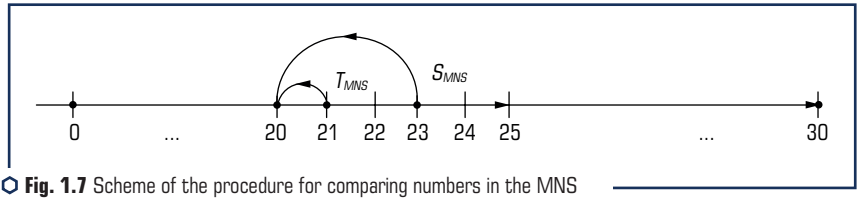

Fig. 1.7 Scheme of the procedure for comparing numbers in the MNS

By residue values s_n and t_n, where $s_n = 011$, $t_n = 001$ choose from BNC (**Table 1.4**) nulling constants, which have the form $NC^{(S)}_{m_n} = (1, 00, 011)$ and $NC^{(T)}_{m_n} = (1, 01, 001)$. Next, define the numbers $S_{m_n} = S_{MNS} - NC^{(S)}_{m_n} = (1, 10, 011) - (1, 00, 011) = (0, 10, 000)$ and $T_{m_n} = T_{MNS} - NC^{(T)}_{m_n} = = (1, 00, 001) - (1, 01, 001) = (0, 10, 000)$, which corresponds to operand shift S_{23} and T_{21} to the left edge of the interval [20, 25) (**Fig. 1.7**) their hits. Further, for the input operands, by means of the implementation of expression (1.1), form the SLBC of the form $K^{(n_S)}_{N_{m_n}} = K^{(4)}_6 = \{101111\}$, and $K^{(n_T)}_{N_{m_n}} = K^{(4)}_6 = \{101111\}$, where $N_5 = \prod_{n=1}^{i-1} m_n = 6$ and $n_S = n_T = 4$. Because $n_S = n_T = 4$, then it is considered that $S_{MNS} = T_{MNS}$. Actually $S = 23 > T = 21$. This disadvantage of the comparison method is due to the following. In the case of comparing numbers in the MNS, the accuracy W_{m_i} comparing two numbers $S_{MNS} = (s_1, s_2, ..., s_{i-1}, s_i, s_{i+1}, ..., s_n)$ and $T_{MNS} = (t_1, t_2, ..., t_{i-1}, t_i, t_{i+1}, ..., t_n)$, depends on the location of the intervals $[g_1 m_i, (g_1 + 1) m_i)$ and $[g_2 m_i, (g_2 + 1) m_i)$ finding these numbers on the numerical axis $0 \div D$ (**Fig. 1.5**), i.e. from intervals g_1 and g_2. For values equal to given numbers $g_1 = g_2 = g$, accuracy W_{p_i} comparison depends on the size of the interval $[g m_i, (g + 1) m_i)$, i.e. from the value of the quantity m_i MNS module. For this case $g_1 = g_2 = g$ have the following

equality $S_{m_i} = T_{m_i} = g \cdot m_i$. This testifies that $S_{MNS} = T_{MNS}$. However, this is not always true. In accordance with the considered method of comparison, all numbers that fall into the numerical interval $\left[gm_i, (g+1)m_i\right)$ will be equal to each other. This circumstance causes the unsuitability of this method of comparing data in the MNS for all variants of the values of the compared numbers.

1.4 ALGEBRAIC DATA COMPARISON METHOD IN THE MNS

Based on the method of arithmetic comparison proposed in subsection 4, let's move on to a possible implementation of the operation of algebraic comparison of two numbers in the MNS. Perhaps there are two fundamentally possible options for organizing the procedure for algebraic comparison: the introduction of a sign in explicit and implicit (using the artificial form (AF) representation of the compared numbers) forms. Let's consider the first option. In this case, the compared operands $S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$ and $T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)$ additionally have two iconic discharges $\Delta_{+S}(\Delta_{+T})$ and $\Delta_{-S}(\Delta_{-T})$, where:

$$\Delta_{+S}(\Delta_{+T}) = \begin{cases} 1, \text{ if } S_{MNS}(T_{MNS}) > 0, \\ 0, \text{ if } S_{MNS}(T_{MNS}) < 0; \end{cases} \quad \Delta_{-S}(\Delta_{-T}) = \begin{cases} 0, \text{ if } S_{MNS}(T_{MNS}) > 0, \\ 1, \text{ if } S_{MNS}(T_{MNS}) < 0. \end{cases} \tag{1.2}$$

Thus, the compared operands are represented as:

$$S^{(*)}_{MNS} = \left\{\Delta_{+S}, \Delta_{-S}; S_{MNS}\right\} = \left\{\Delta_{+S}, \Delta_{-S}; (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)\right\};$$
$$T^{(*)}_{MNS} = \left\{\Delta_{+T}, \Delta_{-T}; T_{MNS}\right\} = \left\{\Delta_{+T}, \Delta_{-T}; (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)\right\}, \tag{1.3}$$

where $\Delta_{+S}(\Delta_{+T})$ – positive and $\Delta_{-S}(\Delta_{-T})$ – negative features of algebraic numbers, respectively $S^{(*)}_{MNS}$ and $T^{(*)}_{MNS}$ in the MNS.

Example 1. Compare two numbers $S^{(*)} = 21$ and $T^{(*)} = -24$. Taking into account expressions (1.2) and (1.3), represent the compared operands in the form $S^{(*)}_{21} = \left\{(1, 0; (1, 00, 001)\right\}$ and $T^{(*)}_{-24} = \left\{(0, 1; (0, 00, 100)\right\}$ in the MNS. By the value of the residuals $s_n = s_3 = 001$ and $t_n = t_3 = 100$ choose from BNC (**Table 1.4**) nulling constants which has the form $NC^{(S)}_{m_n} = (1, 01, 001)$ and $NC^{(T)}_{m_n} = (0, 01, 100)$. Next, define the numbers, $S_{m_n} = S_{MNS} - NC^{(S)}_{m_n} = (1, 10, 011) - (1, 00, 011) = (0, 10, 000)$ and $T_{m_n} = T_{MNS} - NC^{(T)}_{m_n} = (1, 00, 001) - (1, 01, 001) = (0, 10, 000)$, which corresponds to operand shift $S_{21} = \left|S^{(*)}_{21}\right|$ and $T_{24} = \left|T^{(*)}_{-24}\right|$ to the left edge of the interval [20, 25).

Further, through the implementation of expression (1.1), the SLBC is formed for the input operands $S_{21} = \left|S^{(*)}_{21}\right|$ and $T_{24} = \left|T^{(*)}_{-24}\right|$ as $K^{(n_S)}_{N_{m_n}} = K^{(4)}_6 = \{101111\}$, $K^{(n_T)}_{N_{m_n}} = K^{(4)}_6 = \{101111\}$, where $N_5 = \prod_{n=1}^{i-1} m_n = 6$ and $n_S = n_T = 4$. At the same time, through $\left(n = \left[\log_2(t_n - 1)\right] + 1\right)$-th bit comparison circuit, the result of comparison of residuals is determined in parallel in time $s_n = 001 < t_n = 100$. Because $n_S = n_T = 4$, $\Delta_{+S} = 1$ and $\Delta_{-T} = 1$, then in accordance with the algorithm of algebraic

comparison (**Table 1.6**) determine that $S_{21}^{(*)} > T_{-24}^{(*)}$. Check: 21 > –24. The disadvantage of the previous comparison method, which was the low accuracy of the comparison, was eliminated.

● **Table 1.6** Algorithm for algebraic number comparison $S_{MNS}^{(*)}$ and $T_{MNS}^{(*)}$

No.	Number comparison result	Condition for performing comparison operations
1	$S_{MNS}^{(*)} = T_{MNS}^{(*)}$	$\{(n_S = n_T) \wedge (\Delta_{+S} \wedge \Delta_{+T})\} \vee \{(n_S = n_T) \wedge (\Delta_{-S} \wedge \Delta_{-T})\}$
2	$S_{MNS}^{(*)} > T_{MNS}^{(*)}$	$\{(n_S = n_T) \wedge (\Delta_{+S} \wedge \Delta_{-T})\} \vee \{(n_S > n_T) \wedge (\Delta_{+S} \wedge \Delta_{+T})\} \vee$ $\vee \{(n_S > n_T) \wedge (\Delta_{+S} \wedge \Delta_{-T})\} \vee \{(n_S < n_T)\} \wedge \{(\Delta_{+S} \wedge \Delta_{-T})\} \vee$ $\vee \{(n_S < n_T)\} \wedge \{(\Omega_{-S} \wedge \Omega_{-T})\}$
3	$S_{MNS}^{(*)} < T_{MNS}^{(*)}$	$\{(n_S = n_T) \wedge (\Delta_{-S} \wedge \Delta_{+T})\} \vee \{(n_S > n_T) \vee (\Delta_{-S} \wedge \Delta_{+T})\} \vee$ $\vee \{(n_S > n_T) \wedge (\Delta_{-S} \wedge \Delta_{-T})\} \vee \{(n_S < n_T)\} \wedge \{(\Delta_{+S} \wedge \Delta_{+T})\} \vee$ $\vee \{(n_S < n_T)\} \wedge \{(\Delta_{-S} \wedge \Delta_{+T})\}$

Consider the second version of the method of algebraic comparison of numbers in the MNS based on the representation of the compared numbers $S_{MNS} = (s_1, s_2, \ldots, s_n)$ and $T_{MNS} = (t_1, t_2, \ldots, t_n)$ in AF, i.e. $S'_{MNS} = (s'_1, s'_2, \ldots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \ldots, t'_n)$. In this case, the following algorithm for comparing two numbers is implemented $S'_{MNS} = (s'_1, s'_2, \ldots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \ldots, t'_n)$ in the MNS:

$$\begin{cases} S'_{MNS} = T'_{MNS}, \text{ if } \{(n_{S'} = n_{T'}) \wedge [(s'_1 + t'_1) = 0(\text{mod}2)]\}; \\ S'_{MNS} > T'_{MNS}, \text{ if } \{(n_{S'} > n_{T'}) \vee \{(n_{S'} = n_{T'}) \wedge [(s'_1 = 1) \wedge (t'_1 = 0)]\}\}; \\ S'_{MNS} < T'_{MNS}, \text{ if } \{(n_{S'} < n_{T'}) \vee \{(n_{S'} = n_{T'}) \wedge [(t'_1 = 1) \wedge (s'_1 = 0)]\}\}. \end{cases} \quad (1.4)$$

The initial numbers S_{MNS} and T_{MNS} are presented in the AF:

$$\begin{cases} S'_{MNS}(T'_{MNS}) = \dfrac{D}{2} + |S_{MNS}|(|T_{MNS}|), \text{ if } S_{MNS}(T_{MNS}) \geq 0, \\ S'_{MNS}(T'_{MNS}) = \dfrac{D}{2} - |S_{MNS}|(|T_{MNS}|), \text{ if } S_{MNS}(T_{MNS}) < 0, \end{cases} \quad (1.5)$$

i.e. for positive numbers have that $S'_{MNS} = D/2 + |S_{MNS}|$, and for negative numbers have that $S'_{MNS} = D/2 - |S_{MNS}|$. To determine the result of the operation of comparing two numbers in the MNS, the following obvious relations are used:

$$\begin{aligned} &\text{if } S'_{MNS} = T'_{MNS}, \text{ then } S_{MNS} = T_{MNS}, \\ &\text{if } S'_{MNS} > T'_{MNS}, \text{ then } S_{MNS} > T_{MNS}, \\ &\text{if } S'_{MNS} < T'_{MNS}, \text{ then } S_{MNS} < T_{MNS}. \end{aligned} \quad (1.6)$$

Let's look at an example for this method of algebraic comparison of numbers in the MNS.

Example 2. Let $S = -2\ (S_{MNS} = (0,10,010))$ and $T = -3\ (T_{MNS} = (1,00,011))$. $S'_{MNS} = D/2 - S_{MNS} = (1,00,000) - (0,10,010) = (1,01,011)$ and $T'_{MNS} = D/2 - T_{MNS} = (1,00,000) - (1,00,011) = (0,00,010)$. By the value of $s'_1 = 1$ number $S'_{MNS} = (1,01,011)$ choose a constant $NC^{(S')}_{m_1} = (1,01,001)$. The adder implements the operation $S'_{m_1} = S'_{MNS} - NC^{(S')}_{m_1} = (1,01,011) - (1,01,001) = (0,00,010)$. By the value of $t'_1 = 0$ number $T'_{MNS} = (0,00,010)$ choose a constant $NC^{(T')}_{m_1} = (0,00,000)$. The adder implements the operation $T'_{m_1} = T'_{MNS} - NC^{(S')}_{m_1} = (0,00,010) - (0,00,000) = (0,00,010)$. Because $S'_{m_1} - n_{S'} \cdot m_1 = 12 - 6 \cdot 2 = 0$ and $T'_{m_1} - n_{T'} \cdot m_1 = 12 - 6 \cdot 2 = 0$, then for S'_{MNS} and T'_{MNS} the SLBC identical and equal $K^{(n_{S'})}_{N_{m_1}} = K^{(6)}_{15} = \{111111110111111\}$, where $N_{m_1} = 15$ and $n_{S'} = n_{T'} = 6$. When $(n_{S'} = n_{T'})$ the inequality is performed $S'_{MNS} > T'_{MNS}$. In accordance with the relation (1.6) have the result of the comparison operation $S_{MNS} > T_{MNS}$. Check: $S = -2 > T = -3$.

1.5 IMPROVING THE METHOD OF FAST COMPARISON OF TWO INTEGERS IN THE MNS

Obviously, the main disadvantage of all the considered methods is the insufficient accuracy of data comparison, so it is necessary to improve the above methods of comparison. In order to ensure the process of accurate comparison of numbers in the MNS, the method of comparing two numbers has been improved.

As previously noted, the most important characteristic of the process of comparing numbers is the accuracy of comparison W_{m_i}. In the case of comparing numbers in the MNS, the comparison accuracy W_{m_i} two numbers $S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$ and $T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)$ depends on the location of the intervals $[g_1 m_i, (g_1 + 1) m_i)$ and $[g_2 m_i, (g_2 + 1) m_i)$ finding these numbers on the axis $0 \div D$, i.e. from numbers g_1 and g_2 these intervals.

When $g_1 \neq g_2$, the algorithm for comparing two numbers S_{MNS} and T_{MNS} is as follows. If $g_1 > g_2$, then $S_{MNS} > T_{MNS}$, what if $g_1 < g_2$ then $S_{MNS} < T_{MNS}$.

When $g_1 = g_2 = g$ the comparison accuracy W_{m_i} depends on the size of the interval $[g m_i, (g + 1) m_i)$, i.e. from the value of the quantity m_i MNS module. For this case $g_1 = g_2 = g$, $S_{m_i} = T_{m_i} = g \cdot m_i$ it's believed that $S_{MNS} = T_{MNS}$. However, this is not always true.

Based on the geometric interpretation (**Fig. 1.5**) of the proposed method for an arbitrary module m_i of the MNS, it's obvious that the comparison accuracy W_{m_i} depends on the size of the interval $[g m_i, (g + 1) m_i)$, i.e. on the value of the module in accordance with which the SLBC was formed. In this case, the comparison accuracy in the MNS can be determined by the following expression:

$$W_{m_i} = \frac{1}{m_i}. \tag{1.7}$$

However, in the case $m_i = m_n$ number of equipment N_{m_n} devices for comparing two numbers S_{MNS} and T_{MNS}, depending mainly on the number of two groups of adders included

in it that implement the operations $S_{m_n} - K_S \cdot m_n = Z_{K_S}^{(S)}$ and $T_{m_n} - K_T \cdot m_n = Z_{K_T}^{(T)}$, is defined by the expression:

$$N_{m_n} = \prod_{k=1}^{n-1} m_k. \tag{1.8}$$

For an arbitrary value m_i of the MNS module, expression (1.8) will have the following form:

$$N_{m_i} = \prod_{\substack{k=1; \\ k \neq i.}}^{n-1} m_k. \tag{1.9}$$

Depending on the value of the module m_i let's consider variants of the method of arithmetic comparison of numbers in the MNS.

Let $m_i = m_n = \max$. In this case, the comparison accuracy W_{m_n} determined by the value of the interval $\left[gm_n, (g+1)m_n\right)$ and will be minimal. At the same time, the amount of equipment of the comparing device N_{m_n} (see expression (1.9)) will be minimal. Let $m_i = m_1 = \min$. In this case, for the ordered MNS, the maximum comparison accuracy is provided, which is determined by the value of the interval $\left[gm_1, (g+1)m_1\right)$. In this case, the number of equipment devices for arithmetic comparison of two numbers S_{MNS} and T_{MNS} in the MNS maximum and equal $N_{m_1} = \prod_{k=2}^{n} m_k = m_2 \cdot m_3 \ldots m_{n-1} \cdot m_n$.

For MNS, the minimum base is $m_1 = 2$ and the maximum comparison accuracy will be equal to two units, which does not allow achieving the maximum comparison accuracy equal to one (see expression (1.7)).

Thus, it is necessary to improve the methods of arithmetic and algebraic comparison of numbers in the MNS in such a way that the result of comparing numbers in the MNS is determined with maximum accuracy $W_{\max} = 1$ and, preferably, with a minimum number of equipment $N_{\min}$. The last condition is provided by the choice of base $m_i = m_n = \max$, since it satisfies the conditions $N_{\min}$.

To improve the method of comparing two numbers in the MNS, which provides the implementation of the functional $F_{opt} = W_{\max}\left(N_{\min}\right)$, two contradictory conditions must be met. The first, main condition – ensuring the maximum accuracy of comparison is satisfied by choosing the minimum $m_i = \min$ (for example, $m_1 = 2$) from the bases of the MNS (**Fig. 1.8**).

However, in this case, the number of device equipment $N_{\min}$ for comparing two numbers S_{MNS} and T_{MNS} will be maximum (see expressions (1.9)). The second condition is to ensure the minimum number of equipment $N_{\min}$, provided by choosing the maximum $m_i = \max$ base of the MNS.

To eliminate the above contradictions, let's introduce an additional procedure for comparing immediate residuals s_n and t_n initial numbers S_{MNS} and T_{MNS} by base m_n. In this case, the maximum accuracy of the comparison up to unit interval is achieved. So, as a positional comparison of residuals s_n and t_n are carried out in parallel in time with the formation of the SLBC, then the speed of comparing two numbers doesn't decrease.

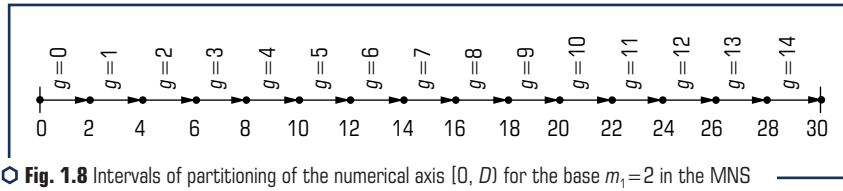

Fig. 1.8 Intervals of partitioning of the numerical axis [0, *D*) for the base $m_1 = 2$ in the MNS

Knowing the quantities s_n, t_n, n_S and n_T, mathematical procedure for comparing two numbers $S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$ and $T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n)$ in the MNS can be represented as (1.10)–(1.12):

$$S_{MNS} = T_{MNS}, \text{ if } \left[(n_S = n_T) \wedge (s_n = t_n) \right]; \tag{1.10}$$

$$S_{MNS} > T_{MNS}, \text{ if } \left\{ (n_S > n_T) \vee \left[(n_S = n_T) \wedge (s_n > t_n) \right] \right\}; \tag{1.11}$$

$$S_{MNS} < T_{MNS}, \text{ if } (n_S < n_T) \vee \left[(n_S = n_T) \wedge (s_n < t_n) \right]. \tag{1.12}$$

Improvements to the method for comparing two numbers S_{MNS} and T_{MNS} in the MNS consists in performing the following steps of the algorithm:

1. Representation of compared numbers in the MNS:

$$S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$$

and

$$T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n) \text{ in the MNS.}$$

2. Formation by values s_n and t_n of nulling constants of the species:

$$NC_{m_n}^{(S)} = (s'_1, s'_2, \ldots, s'_{i-1}, s_i, s'_{i+1}, \ldots, s'_n)$$

and

$$NC_{m_n}^{(T)} = (t'_1, t'_2, \ldots, t'_{i-1}, t_i, t'_{i+1}, \ldots, t'_n).$$

Simultaneously in time, the residuals are compared s_n and t_n compared numbers:

$$S_{MNS} = (s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n)$$

and

$$T_{MNS} = (t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n).$$

3. Determining the values of the difference of numbers S_{m_n} and T_{m_n}:

$$S_{m_n} = S_{MNS} - NC^{(S)}_{m_n} = \left(s_1, s_2, \ldots, s_{i-1}, s_i, s_{i+1}, \ldots, s_n\right) - \left(s'_1, s'_2, \ldots, s'_{i-1}, s_i, s'_{i+1}, \ldots, s'_n\right) =$$
$$= \left(s_1^{(1)}, s_2^{(1)}, \ldots, s_{i-1}^{(1)}, 0, s_{i+1}^{(1)}, \ldots, 0\right)$$

and

$$T_{m_n} = T_{MNS} - NC^{(T)}_{m_n} = \left(t_1, t_2, \ldots, t_{i-1}, t_i, t_{i+1}, \ldots, t_n\right) - \left(t'_1, t'_2, \ldots, t'_{i-1}, t_i, t'_{i+1}, \ldots, t'_n\right) =$$
$$= \left(t_1^{(1)}, t_2^{(1)}, \ldots, t_{i-1}^{(1)}, 0, t_{i+1}^{(1)}, \ldots, 0\right).$$

4. Definition of the SLBC components $z_i^{(S)}$ and $z_g^{(T)}$:

$$K_{N_{m_n}}^{(n_S)} = \left\{ Z_{N_{m_n}-1}^{(S)} Z_{N_{m_n}-2}^{(S)} \ldots Z_2^{(S)} Z_1^{(S)} Z_0^{(S)} \right\}$$

and

$$K_{N_{m_n}}^{(n_T)} = \left\{ Z_{N_{m_n}-1}^{(T)} Z_{N_{m_n}-2}^{(T)} \ldots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)} \right\}.$$

By means of adders, using a set of constants $\left(0, m_n, \ldots, (N-1)\cdot m_n\right)$ by formulas $S_{m_n} - K_S \cdot m_n = Z_{K_S}^{(S)}$ and $T_{m_n} - K_T \cdot m_n = Z_{K_T}^{(T)}$ components are defined $z_i^{(S)}$ and $z_g^{(T)}$.

5. Formation of quantitative values of PFNC n_S and n_T. By type of the SLBC:

$$K_{N_{m_n}}^{(n_T)} = \left\{ Z_{N_{m_n}-1}^{(T)} Z_{N_{m_n}-2}^{(T)} \ldots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)} \right\}$$

and

$$K_{N_{m_n}}^{(n_T)} = \left\{ Z_{N_{m_n}-1}^{(T)} Z_{N_{m_n}-2}^{(T)} \ldots Z_2^{(T)} Z_1^{(T)} Z_0^{(T)} \right\}$$

the values of the binary digits of the SLBC are determined for which $Z_{n_S}^{(S)} = 0$ and $Z_{n_T}^{(T)} = 0$.

6. Implementation of the comparison operation result algorithm S_{MNS} and T_{MNS}:

$$S_{MNS} = T_{MNS}, \text{ if } \left[\left(n_S = n_T\right) \wedge \left(s_n = t_n\right)\right];$$
$$S_{MNS} > T_{MNS}, \text{ if } \left(n_S > n_T\right) \vee \left[\left(n_S = n_T\right) \wedge \left(s_n > t_n\right)\right];$$
$$S_{MNS} < T_{MNS}, \text{ if } \left(n_S < n_T\right) \vee \left[\left(n_S = n_T\right) \wedge \left(s_n < t_n\right)\right].$$

In accordance with the improved method, **Table 1.7** presents an algorithm for arithmetic comparison of numbers in the MNS.

In order to ensure the process of accurate comparison of numbers $S_{MNS} = \left(s_1, s_2, \ldots, s_n\right)$ and $T_{MNS} = \left(t_1, t_2, \ldots, t_n\right)$ in the MNS, presented in AF, based on the method presented in **Fig. 1.8**, improved method of comparing two numbers $S'_{MNS} = \left(s'_1, s'_2, \ldots, s'_n\right)$ and $T'_{MNS} = \left(t'_1, t'_2, \ldots, t'_n\right)$.

● **Table 1.7** Algorithm for arithmetic comparison of numbers in the MNS

No.	Number comparison result	Condition for performing comparison operations
1	$S_{MNS} = T_{MNS}$	$(n_S = n_T) \wedge (s_n = t_n)$
2	$S_{MNS} > T_{MNS}$	$(n_S > n_T) \vee \left[(n_S = n_T) \wedge (s_n > t_n)\right]$
3	$S_{MNS} < T_{MNS}$	$(n_S < n_T) \vee \left[(n_S = n_T) \wedge (s_n < t_n)\right]$

An improved method for comparing two numbers $S'_{MNS} = (s'_1, s'_2, \ldots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \ldots, t'_n)$ is based on the representation of numbers in the AF. The improvement of the method of comparing two numbers in the MNS is suitable for both arithmetic comparison and algebraic comparison of data when introducing a sign in an implicit form (representing data in the AF).

An improved method of comparing two numbers in the MNS, presented in the AF consists in performing the following steps of the algorithm:

1. According to the expressions:

$$\begin{cases} S'_{MNS}(T'_{MNS}) = \dfrac{D}{2} + |S_{MNS}|(|T_{MNS}|), \text{ if } S_{MNS}(T_{MNS}) \geq 0, \\ S'_{MNS}(T'_{MNS}) = \dfrac{D}{2} - |S_{MNS}|(|T_{MNS}|), \text{ if } S_{MNS}(T_{MNS}) < 0, \end{cases}$$

initial numbers $S_{MNS} = (s_1, s_2, \ldots, s_n)$ and $T_{MNS} = (t_1, t_2, \ldots, t_n)$ are presented in the AF in the form $S'_{MNS} = (s'_1, s'_2, \ldots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \ldots, t'_n)$.

2. An algorithm for comparing two numbers is implemented $S'_{MNS} = (s'_1, s'_2, \ldots, s'_n)$ and $T'_{MNS} = (t'_1, t'_2, \ldots, t'_n)$ in the MNS as:

$$\begin{cases} S'_{MNS} = T'_{MNS}, \text{ if } \left\{(n_{S'} = n_{T'}) \wedge \left[(s'_1 + t'_1) = 0 (\mathrm{mod} 2)\right]\right\}; \\ S'_{MNS} > T'_{MNS}, \text{ if } \left\{(n_{S'} > n_{T'}) \vee \left\{(n_{S'} = n_{T'}) \wedge \left[(s'_1 = 1) \wedge (t'_1 = 0)\right]\right\}\right\}; \\ S'_{MNS} < T'_{MNS}, \text{ if } \left\{(n_{S'} < n_{T'}) \vee \left\{(n_{S'} = n_{T'}) \wedge \left[(s'_1 = 1) \wedge (t'_1 = 0)\right]\right\}\right\}. \end{cases}$$

3. Determining the result of the operation of comparing two numbers in the MNS:s

if $S'_{MNS} = T'_{MNS}$, then $S_{MNS} = T_{MNS}$,

if $S'_{MNS} > T'_{MNS}$, then $S_{MNS} > T_{MNS}$,

if $S'_{MNS} < T'_{MNS}$, then $S_{MNS} < T_{MNS}$.

The improved quick comparison method allows to carry out the comparison procedure in the MNS, both in positive and negative numerical ranges. Improving the method of quick comparison

of two integers is carried out by increasing the accuracy of the comparison, by representing numbers in an artificial form, which expands the area of effective use of the CSPIED in the MNS.

The article discusses methods for fast arithmetic comparison of two numbers in the MNS, which are based on obtaining and using PFNC numbers presented in the AF. The use of existing methods for quick comparison of data in the MNS for one-byte, two-byte, three-byte, four-byte and eight-byte numerical bit grids of the CSPIED, respectively, by 16 %, 37 %, 50 %, 58 % and 72 % more efficient in terms of number comparison time than using the fastest of the existing number comparison methods in the MNS, which is based on the principle of nulling.

Designed the method for quick comparison of two integers in the MNS, both in positive and negative numerical ranges, was improved by representing numbers in an artificial form, based on the use of PFNC, which increases the accuracy of comparing numbers in the system of residual classes. The proposed method provides maximum comparison accuracy with a minimum amount of equipment for comparing devices. This circumstance makes it possible to obtain a reliable result of the operation of checking two numbers in the MNS. Based on the developed methods, data comparison algorithms were obtained, in accordance with which devices for their implementation were synthesized. The technical devices, for which patents of Ukraine has been received, is recommended for use in the practical implementation of the CSPIED, which functions as a MNS [3, 10].

The types and methods of cyberattacks are growing exponentially every day, so it is very important to use effective methods and methods of protection. A very important element of various cyberattack detection systems is the data monitoring process, which consists of various methods and algorithms for comparing data. The above method of data comparison for threat detection provides many advantages, but one of the most important is the ability to quickly detect attacks at an early stage and take corrective measures to contain the attacks.

CONCLUSIONS

Based on the conducted research, it is legitimate to draw the following conclusions.

1. In the terms of the development of cyber terrorism in the world, the deployment of cyberwar against Ukraine by the russian federation as a component of direct military aggression, there is an increase in risks and threats to cybersecurity. The increase in the number of cyberattacks on critical infrastructure objects and state information resources confirms the urgency of the problem of increasing the cyber resilience of the national information space.

2. Taking into account the growth of negative financial consequences from the implementation of cyber threats, the need to implement comprehensive and coordinated measures at the national and international levels to prevent the implementation of cyber incidents by authorities, businesses and society has been proven.

3. Based on the study of Ukraine's positions in international cybersecurity rankings and the establishment of indicators that are the basis of the global NCSI, GCI and NCPI indexes,

the country's cyber capability strengths and weaknesses are substantiated. Promising tasks are defined as improvement of information protection systems of critical infrastructure objects based on best global practices, as well as coordination of actions with international organizations regarding countering threats related to the development of the digital economy and information society.

4. The formation of a preventive mechanism for combating threats in cyberspace requires a significant increase in the speed and reliability of economic data processing, which is possible based on the use of new machine arithmetic. In this aspect, the proposed non-positional number system in residual classes is one of the promising methods of improving the cybersecurity of critical infrastructure objects, as it enables detecting cyberattacks in the early stages and taking preventive measures to contain them.

5. As a result, the method for quick comparison of two integers in the MNS, both in positive and negative numerical ranges, was improved by representing numbers in an artificial form, based on the use of a positional features of a non-positional code, which increases the accuracy of comparing numbers in the system of residual classes. The proposed method provides maximum comparison accuracy with a minimum amount of equipment for comparing devices. This circumstance makes it possible to obtain a reliable result of the operation of checking two numbers in the MNS. Based on the developed methods, data comparison algorithms were obtained, in accordance with which devices for their implementation were synthesized. The technical device, for which a patent of Ukraine has been received, is recommended for use in the practical implementation of the CSPIED, which functions as a MNS. The above method of data comparison for threat detection provides many advantages, but one of the most important is the ability to quickly detect attacks at an early stage and take corrective measures to contain the cyberattacks.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

REFERENCES

1. Yusif, S., Hafeez-Baig, A. (2021). A Conceptual Model for Cybersecurity Governance. Journal of Applied Security Research, 16 (4), 490–513. doi: https://doi.org/10.1080/19361610.2021.1918995
2. Protection of information and cyberspace (2022). SIEM report. Security Service of Ukraine. Available at: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky

3. Vlasenko, A. M., Krasnobaev, V. A., Yanko, A. S., Koshman, S. O., Rassomakhin, S. G., Lavrovska, T. V. (2016). Pat. No. 112731 UA. Prystrii dlia kontroliu ta diahnostyky danykh, shcho predstavleni u systemi zalyshkovykh klasiv. MPK: G06F 11/08 (2006.01). No. a201510904; declareted: 10.03.2016; published: 10.10.2016, Bul. No. 19. Available at: https://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=227851
4. Devanny, J., Martin, C., Stevens, T. (2021). On the strategic consequences of digital espionage. Journal of Cyber Policy, 6 (3), 429–450. doi: https://doi.org/10.1080/23738871.2021.2000628
5. Slayton, R. (2020). Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. Science, Technology, & Human Values, 46 (1), 81–111. doi: https://doi.org/10.1177/0162243919901159
6. Collins, M. (2017). Network Security Through Data Analysis: From Data to Action. O'Reilly Media, Inc.
7. Goh, Z. H., Hou, M., Cho, H. (2022). The impact of a cause–effect elaboration procedure on information security risk perceptions: a construal fit perspective. Journal of Cybersecurity, 8 (1). doi: https://doi.org/10.1093/cybsec/tyab026
8. Liu, J., Yan, J., Jiang, J., He, Y., Wang, X., Jiang, Z. et al. (2022). TriCTI: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network. Cybersecurity, 5 (1). doi: https://doi.org/10.1186/s42400-022-00110-3
9. Krasnobayev, V., Kuznetsov, A., Yanko, A., Koshman, S., Zamula, A., Kuznetsova, T. (2019). Data processing in the system of residual classes. ASC Academic Publishing.
10. Krasnobaev, V. A., Koshman, S. O., Yanko, A. S. (2014). Pat. No. 92069 UA. Prystrii dlia aryfmetychnoho ta alhebraichnoho porivniannia dvokh chysel klasu lyshkiv. MPK: G06F 7/04 (2006.01). No. u201402480; declareted: 12.03.2014; published: 25.07.2014, Bul. No. 14. Available at: https://base.uipv.org/searchINV/search.php?action=viewdetails&IdClaim=203104
11. Svistun, L., Glushko, A., Shtepenko, K. (2018). Organizational Aspects of Development Projects Implementation at the Real Estate Market in Ukraine. International Journal of Engineering & Technology, 7 (3.2), 447–452. doi: https://doi.org/10.14419/ijet.v7i3.2.14569
12. Special Report: Ukraine. An overview of Russia's cyberattack activity in Ukraine (2022). Microsoft Corporation. Available at: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2022). Increasing Information Protection in the Information Security Management System of the Enterprise. Proceedings of the 3rd International Conference on Building Innovations. Lecture Notes in Civil Engineering Vol. 181. Cham: Springer, 725–738. doi: https://doi.org/10.1007/978-3-030-85043-2_67
14. Shchodo kiberatak na saity derzhavnykh orhaniv (2022). The Security Service of Ukraine. Available at: https://ssu.gov.ua/novyny/shchodo-aktak-na-saity-derzhavnykh-orhaniv
15. Politsiia rozpochala kryminalne provadzhennia za faktom kiberatak na saity derzhavnykh orhaniv (2020). The Cyber Police Department of the National Police of Ukraine. Available at:

https://cyberpolice.gov.ua/news/policziya-rozpochala-kryminalne-provadzhennya-za-faktom-kiberatak-na-sajty-derzhavnyx-organiv-1549/
16. The State Service for Special Communications and Information Protection of Ukraine. Available at: https://cip.gov.ua/ua
17. Karpenko, O. (2022). USA: The special services of the Russian Federation are involved in DDoS attacks on Ukrainian websites. National Security Council of USA. Available at: https://ain.ua/2022/02/19/do-ddos-atak-prychetni-speczsluzhby-rf/
18. Government response: UK assesses Russian involvement in cyberattacks on Ukraine (2022). The UK's National Cyber Security Centre. Available at: https://www.gov.uk/government/news/uk-assess-russian-involvement-in-cyber-attacks-on-ukraine
19. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S. (2020). Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. International Journal of Management, 11 (12), 1709–1726. doi: https://doi.org/10.34218/ijm.11.12.2020.157
20. Center for Internet Security. Available at: https://www.cisecurity.org/
21. Year in Review: What 2021 Was Like for Cyber Security (2022). Company ESET. Available at: https://eset.ua/ua/news/view/933/itogi-goda-kakim-byl-2021-dlya-kiberbezopasnosti
22. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., Skryl, V.; Onyshchenko, V., Mammadova, G., Sivitska, S., Gasimov, A. (Eds.) (2023). The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference on Building Innovations. ICBI 2022. Lecture Notes in Civil Engineering Vol. 299. Cham: Springer, 791–803. doi: https://doi.org/10.1007/978-3-031-17385-1_67
23. The new global cybersecurity index is the National Cyber Power Index (2020). The official website of the Public Organization "International University of Cyber Security". Available at: https://www.icu-ng.org/icu-ng/novyny/novyj-globalnyj-indeks-kiberbezpeky-naczionalnyj-indeks-kiberpotuzhnosti/#_ftn1
24. Cyber security management best practices. Review report (2022). Committee on Digital Transformation. Available at: https://www1.undp.org/content/dam/ukraine/img/demgov/Rada%20for%20Europe/Report_on_Cybersecurity_04.pdf
25. NCSI Project Team. Available at: https://ncsi.ega.ee/country/ua/
26. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro nevidkladni zakhody z kiberoborony derzhavy". Ukaz Prezydenta Ukrainy No. 446/2021. 26.08.2021. Available at: https://zakon.rada.gov.ua/laws/show/446/2021#Text
27. Glushko, A. D. (2013). Directions of Efficiency of State Regulatory Policy in Ukrain. World Applied Sciences Journal. Pakistan: International Digital Organization for Scientific Information, 27 (4), 448–453.
28. Diogenes, Y., Ozkaya, E. (2019). Cybersecurity Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals. Packt Publishing Ltd.

29. Bosilca, G., Delmas, R., Dongarra, J., Langou, J. (2009). Algorithm-based fault tolerance applied to high performance computing. Journal of Parallel and Distributed Computing, 69 (4), 410–416. doi: https://doi.org/10.1016/j.jpdc.2008.12.002
30. Hlushko, A., Yanko, A. (2019). Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the national economy. Economics and Region, 4 (75), 35–44. doi: https://doi.org/10.26906/eir.2019.4(75).1814
31. Krasnobaev, V. A., Kurchanov, V. N., Yanko, A. S. (2015). Method of quick comparison of two integers in the system of final classes. Problems of Informatization. Cherkasy, 45.