Increasing Information Protection in the Information Security Management System of the Enterprise

Svitlana Onyshchenko, Alina Yanko, Alina Hlushko, and Svitlana Sivitska

Abstract The article actualizes the problem of management and strengthening of enterprises information security. It is proved that in the conditions of information and technological development it is the information that has become a factor that forms the competitiveness of many business entities. A statistical analysis of the level of cybercrime and financial losses from crimes in cyberspace. It is substantiated that construction of an effective information security management system based on international standards of the ISO series is the key to the successful operation of enterprises. The method of error correction in the system of residual classes is determined by the basis of improving the information security of economic entities.

The method of enterprise data errors correction in the system of residual classes is developed in the article, which is based on the application of corrective properties of L-codes, which are formed when using mutually pairwise difficult bases. This method enables expanding the class of corrected errors that are corrected, which expands the corrective capabilities of L-codes. Examples of performing the correction operation are given, as well as the features of the implementation of the device for detecting data errors are described.

Keywords Computer system for processing enterprise data · Conditional alternative sets · Data protection · Error correction · Information · Information security · Linear codes · System of residual classes

1 Protection of Information in the Information Security Management System

In terms of information technology development, characterized by on the one hand the intensification of modern information technology in all sectors of the national economy, and on the other hand, increasing the scale and frequency of cyber attacks,

S. Onyshchenko · A. Yanko · A. Hlushko (✉) · S. Sivitska
National University «Yuri Kondratyuk Poltava Polytechnic»,
Pershotravnevyj Avenue 24, Poltava 36011, Ukraine

V. Onyshchenko et al. (eds.), *Proceedings of the 3rd International Conference on Building Innovations*, Lecture Notes in Civil Engineering 181,
https://doi.org/10.1007/978-3-030-85043-2_67

the emergence of new risks and security threats to businesses and the state as a whole, the issue of increasing the level of information security becomes particularly relevant.

Noting the role and importance of existing research on information security [1–4], it is obvious that in the context of intensification of informatization and progressive development of the IT sector, one of the most pressing issues is the problem of cyber attacks, which necessitates increased protection of information.

Information security of enterprises characterizes the state of their access to information, its security and storage, efficiency of use, business intelligence, information and analytical work with external and internal entities, the ability of information and analytical system of economic entities to develop.

Analysis of the internal and external environment of enterprises is the first and integral function of management [5]. Therefore, the quality of information and analytical support directly affects the effectiveness of management and further development of the enterprise. But for this, the system of information and analytical support of the process of economic entities economic security managing should include the following elements: information, a set of indicators, indicators, methods of assessment and analysis of information security [6].

Of course, the system of analytical information for management decisions is characterized by complexity. And there is a tendency to complicate the relationships in the information flow. At the same time there is a systematic increase in the amount of information, its redundancy in terms of lack of information to make optimal management decisions. Information on the business entities security is quite heterogeneous [7]. All this complicates its use in the management of security and viability of the entity. In most businesses, information that managers use to ensure their safety comes predominantly from internal sources. A specialized analytical group or security service is created, the functional responsibilities of which include all or part of the information support.

The key issue is the concept of essential information. Information is considered significant, the non-provision or distortion of which may influence the decisions of its users. The main objectives of information security management of economic entities are to ensure timely detection of information loss channels, threats and their level of importance, types of information theft, methods of their actions; ensure prompt response to threats; create conditions for the maximum possible compensation for damage; avoidance of economic and industrial espionage.

Thus, information security of enterprises is designed to protect their interests and their staff from the misuse of inside information and protection of trade secrets, which often constitute a significant part of the intellectual property of the business entity.

However, despite attempts to protect trade secrets and other sources of information, it is often the case that information is disseminated to persons who have no right to do so. Under modern business conditions, this phenomenon is quite common, because information about know-how, technology, methods of conducting business and management of individual business processes forms the competitiveness of many businesses [8]. And in conditions of constant competition, even a drop of the necessary information can dramatically change market conditions for an individual business entity, and for another—to turn into losses and damages. That is why, in Western Europe and the United States, 20% loss of confidential information can lead to bankruptcy [9].

Current dependence of enterprises on information systems and their services means that businesses are becoming increasingly vulnerable to information security threats. Interaction of public and private networks, as well as sharing of information resources increases the difficulties of access control and ensuring guarantees of services and security of information and communication systems and networks.

Intensification of the processes of economic activity digitalization creates preconditions for increase in cases of unauthorized use of computers, telecommunications systems, computer networks and telecommunications networks [10], i.e. cybercrime.

Back in the 1990s, computer fraud in the United States caused more than $10 billion in annual damage [11]. In the UK, where cybercrime had quadrupled at the time, the Confederation of British Industrialists estimated that the annual damage was £5 billion.

Today, financial losses from cybercrime are growing every year. According to a study conducted by experts from the Center for Strategic and International Studies (CSIS) and McAfee, a company that develops anti-virus software, the level of losses from cybercrime in the global economy is growing rapidly: if in 2014 they amounted to 345–445 billion dollars (0,6% of world GDP), then in 2016 it was already 445–600 billion dollars (0,8% of world GDP), in 2017—about 1.5 trillion dollars [12]. Global losses from the hacker attack using the NotPetya virus program alone amounted to $850 million, of which $300 million was the financial loss of the national economy of Ukraine (0,4% of GDP) [13].

Hacker attacks in 2020 cost the world economy more than a trillion dollars or 820 billion euros, which is 50% higher than in 2018 (see Fig. 1).

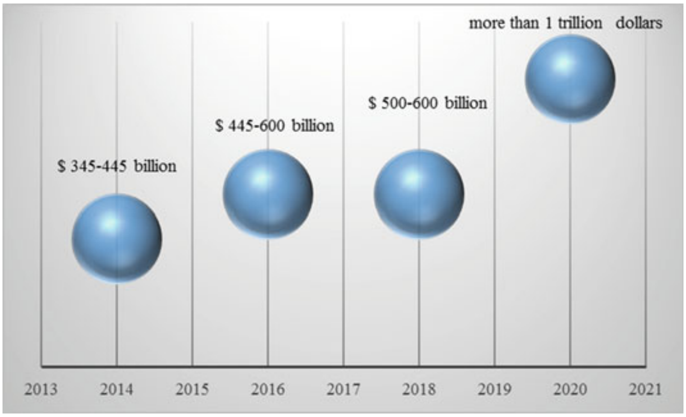

Fig. 1 Estimated average cost of cybercrime

Establishing the real scale of financial losses from the actions of cybercriminals is extremely difficult and almost impossible. However, the lack of official statistics does not diminish the relevance and importance of information security. After all, information is one of the universal types of resources that are necessary both for the decision-making process and for the formulation of strategic, tactical and operational tasks of economic development at the macro-, meso- and micro-levels.

According to domestic and foreign experts, solving the problems of investigating this type of crime is a difficult task for law enforcement agencies both in our country and abroad. Domestic and foreign criminologists classify "computer" crime as hyper latent. According to various estimates, law enforcement officers become aware of only 10–20% of such crimes [14].

A key aspect of protection against cybercrime is preparation and identification of vulnerabilities, as well as resilience in terms of interoperability with common management systems.

Fundamental in the field of information security management are the International Standards ISO/IEC 27,001 and ISO/IEC 27,002 (it was called ISO/IEC 17,799 until 2007). They are a model of the management system, which determines the overall organization of processes, data classification, access systems, planning areas, employee responsibility, the use of risk assessment, etc. in the context of information security. Thus, due to the implementation of the ISO/IEC 27,001 standard, business entities have the opportunity to assess their risks, implement control measures to mitigate them, control risks, improving, if necessary, information protection. The ISO/IEC 27,002 standard is used to establish a system of effective information protection and to improve information protection methods.

To date, there are more than 40 international standards of the ISO/IEC 27,000 series, covering everything from creation of a common dictionary (ISO/IEC 27,000), risk management (ISO/IEC 27,005), security in cloud technologies (ISO/IEC 27,017 and ISO/IEC 27,018) to forensic methods used to analyze digital evidence and investigate incidents ISO/IEC 27,042 and ISO/IEC 27,043 respectively) [15]. They enable businesses to constantly update themselves in the fight against cybercrime.

Building an effective information security management system based on international ISO series standards in modern information and communication systems and networks is an important task for every business entity. To counter external attacks, it is necessary not only to have effective means of protection, but also to know their system of operation, settings and weaknesses of operating systems [16].

Thus, strengthening the information security of enterprises is based on ensuring reliability, confidentiality, integrity of information resources. Modern methods and means of information and communication and digital technologies cannot fully ensure productive and reliable processing of ever-growing arrays of information. The existing positional binary number system, which operates in modern information technology, has shortcomings, and existing methods of unauthorized access, hacker attacks, viruses and other types of hacking and violation of the integrity of information are built using binary position code. In this aspect, correction of errors in the system of residual classes can rightly be determined as the basis for improving the information security of economic entities.

2 Features of Error Correction in the SRC

It is possible to significantly increase the reliability and credibility of processing economic data only based on the use of new machine arithmetic. Because existing positional numeral system (PNS) has a number of disadvantages. Execution of an arithmetic operation involves a sequence of elementary operations on operands (digits) according to the rules defined by its content. These operations cannot be completed until the values of all the results of the operations have been obtained, taking into account all the interconnections between the operands (digits). As a result, modern computer systems that use binary code to represent and process all types of data, i.e. based on PNS, have a significant disadvantage—the presence of inter-bit connections between the operands being processed, which affects the architecture of computer systems and methods of arithmetic operations, complicates the equipment and limits the speed of arithmetic operations.. And most importantly, due to inter-bit connections, one error in the bit leads to a block of errors, and the existing methods of error correction in the PNS are very difficult to implement and strongly affect the redundancy of the machine code [17].

In the system of residual classes (SRC), each number is represented in the form of several small-digit positional numbers, which are remainders from dividing the initial number into mutually simple bases. In the usual positional binary system, operations (for example, the addition of two numbers) were performed sequentially by bit, starting from the youngest. This creates a transfer to the next most significant digit, which determines the bitwise processing sequence. The possibility of paralleling this process appeared in the SRC: all operations on the remainders on each basis are performed separately and independently (in parallel), therefore, due to their low bitness, easily and quickly [18].

Also the SRC has a valuable property of the independence of the residuals from each other on the basis of the adopted system [19]. The independence of the residuals makes it possible to build computer system for processing enterprise data (CSPED) in the form of a set of information—independent, parallel computing paths (separate "small" computing paths of information processing, operating on a specific module m_i in the SRC, independently). Thus, CSPED have a modular design that enables maintenance and troubleshooting without interrupting the solution of the computational problem. Errors that occur due to failures of binary circuits in an arbitrary computational path on the basis m_i do not spread to neighboring paths (remain within one residual), which makes it possible to increase the reliability of calculations in the CSPED. It does not matter whether there was a single or multiple error, or even a package of errors with a length of not more than $m_i - 1$ binary digits. Thus, the error that occurred in an arbitrary path m_i of the CSPED in the SRC, or will remain in this path until the end of the calculations, or in the process of further calculations will be eliminated (for example, if after a failure in the residual a_i the intermediate result is multiplied by a number zero having a zero digit based on m_i). In this case, with the help of SRC you can build a system of error correction with the introduction of minimal redundancy, which uses the dynamics of the computational process, introducing the concept of an alternative set of numbers. The set of bases of SRC $m_{i1}, m_{i2}...m_{ik}$ by which numbers A_1, $A_2...A_k$ differ from the incorrect operand $\tilde{\mathrm{A}}$, is called an alternate set of numbers, and is denoted $\overline{\mathrm{W}}\left(\tilde{\mathrm{A}}\right)$. The basic idea of determining the erroneous residual (basis) $a_i = a_i + \Delta\, a_i$ is that for the resulting sequence of incorrect operands $\tilde{\mathrm{A}}_i = (i = \overline{1, p})$ in the dynamics of the computational process, without interrupting the solution of the problem, sequentially in time are determined by conditional alternative sets (CAS):

$$\overline{W}(\tilde{A}) = \overline{W}_{i-1}(\tilde{A}) \wedge \overline{W}_i(\tilde{A}). \quad (1)$$

For some time, CAS is charged to the erroneous basis (or to two bases m_i and m_n). After that, the known methods are used to correct the distorted residual a_i. A feature of this method of error correction is the ability to correct errors without stopping calculations, which is important for CSPED that operate in real time. A detailed study of the features of the SRC allows us to conclude that the devices that operate in the SRC, are easily controlled and easily diagnosable objects. The noted feature of CSPED functioning in SRC promotes development of effective methods of control and diagnostics [20].

This independence offers wide opportunities for constructing not only new machine arithmetic, but also a fundamentally new scheme for the implementation of CSPED, which in turn significantly expands the use of machine arithmetic.

Thus, this property of the SRC makes it possible to implement a unique system of control and correction of errors in the dynamics of the computational process with the introduction of minimal code redundancy without stopping calculations, which is very important for economic structures operating in real time [21].

3 Implementation of L-codes in the SRC

Currently, possibilities of R-codes for error correction in the SRC are being intensively investigated. This is due to the clear and simple structure of R-codes without deep interconnections, and really effective corrective properties, with a relatively simple procedure for their construction for any required minimum code distance.

Also for comprehensiveness it is necessary to consider other types of codes in non-positional systems, namely in the SRC, which are found in the literature under the name—linear codes (L-codes). When considering these L-codes in various scientific sources, it's described not by quantitative characteristics, but by qualitative ones.

Currently, no one is deeply researching the corrective capabilities of linear codes in combination with the properties of SRC. Developments in this direction would reveal broad and effective corrective properties, which necessitates the improvement of SRC-based data processing systems and the use of these systems to increase the reliability of CSPED.

The sum, difference, and product of any vectors of a linear code are code words. In this case, non-code words cannot be associated with any natural numbers. We show that error correction in the SRC with the help of L-codes leads to hardware redundancy equivalent to reservation. To this end, we consider two known theorems [22].

Theorem 1. To correct an error in the residual at an arbitrary base m_i of the number $A = (a_1,\ a_2,\ \ldots, a_n)$, specified in the system of residual classes with bases $m_1, m_2,\ \ldots,\ m_n$, it is necessary that:

$$(d_{ik} - 1)(d_{ij} - 1) \geq m_i - 1 - (K_{d_{i\,k}} + K_{d_{ij}} - K_{[d_{i\,k}, d_{ij}]}), \tag{2}$$

where $d_{ik} = (m_i,\ m_k)$, $d_{ij} = (m_i,\ m_j)$, $K_{d_{i\,k}}$ id the number of divisors, multiples of d_{ik};

$K_{d_{i\,j}}$ is the number of divisors, multiples of d_{ij};

$K_{[d_{i\,k}, d_{ij}]}$ is the number of divisors, multiples of the lowest common multiple (LCM) $[d_{i\,k}, d_{ij}]$ of the divisors d_{ik} and d_{ij}, $i \neq j$.

Proof. Calculate the values a_{ij}, a_{ik}, a_{jk}. If the error occurred at the base m_i, then $a_{ik} = 0$, $a_{ij} \neq 0$ and $a_{ik} \neq 0$. The number of different combinations of a_{ij}, a_{ik} is $(d_{ij} - 1) \cdot (d_{ik} - 1)$, where $(d_{ij} - 1)$ is the number of possible values of a_{ij} $(a_{ij} \neq 0)$, $(d_{ik} - 1)$ is the number of possible values of a_{ik} $(a_{ik} = 0)$, and the number of possible values of base errors a_{ik} is $m_i - 1$ $(\Delta a_i \neq 0)$ minus the number of undetected errors [22]. The number of undetected errors consists of the number of errors, multiples of the divisor $d_{ik} - K_{d_{ik}}$ and multiples of the divisor $d_{ik} - K_{d_{ik}}$. Thus, the number of possible values of detectable errors is:

$$m_i - 1 - (K_{d_{i\,k}} + K_{d_{ij}} - K_{[d_{i\,k}, d_{ij}]}). \tag{3}$$

To ensure compliance with the possible values of the errors on the basis m_i it is necessary to fulfill inequality (2).

Q.E.D. The necessary condition of Theorem 1 is sufficient if different values of the error values Δa_i correspond to different product values $a_{ik} \cdot a_{ij}$, and vice versa. Indeed, in this case there is a one-to-one correspondence between the possible values Δa_i and the values of the product $a_{ik} \cdot a_{ij}$, which determines the possibility of uniquely determining the magnitude of the error [23].

Based on Theorem 1, we compose an error correction algorithm for an arbitrary base m_i:

1. Determine the number of distorted residual. To do this, we calculate the values:

$$\begin{aligned} a_1 - a_2 &= a_{12}(\mathrm{mod} d_{12}) \\ a_2 - a_3 &= a_{23}(\mathrm{mod} d_{23}) \\ &\ldots \\ a_{n-1} - a_n &= a_{n-1n}(\mathrm{mod} d_{n-1n}) \\ a_n - a_1 &= a_{n2}(\mathrm{mod} d_{n1}) \end{aligned} \tag{4}$$

If all residuals are $a_{ij} = 0\big(\mathrm{mod} d_{ij}\big)$, then the number A is correct. If the error occurred at the base m_i, then $a_{ij} \neq 0$ and $a_{ik} \neq 0$, thus, the number being tested $\widetilde{A} = (a_1,\ a_2,\ ..., \widetilde{a_i},\ ...,\ a_n)$ is incorrect.

2. By the values of a_{ij} and a_{ik} appeal to the block of error constants, where we select the appropriate value of Δa_i.

3. We perform the correction of the number $\widetilde{A}$ in and we get the correct number $A = \widetilde{A} - \Delta A$, i.e.

$$A = (a_1,\ a_2,\ ..., a_i,\ ...,\ a_n). \tag{5}$$

If in the abbreviated SRC due to the exclusion of the base on which the error occurred, it is possible to unambiguously represent a number A, then instead of determining by the values of a_{ij} and a_{ik} the value of the error Δa_i, we will directly calculate the values of the correct remainder a_i.

Consider this error correction algorithm:

1. Calculate the value of residuals $a_{12},\ a_{23},\ ...,\ a_{n1}$.

2. Determine the number of distorted balance. Let the error occurred at the base m_i. In this case, this basis is excluded, and the number A is presented on the bases $m_1,\ m_2,\ ..., m_n$, i.e.

$$A = (a_1,\ a_2,\ ...,\ a_{i-1}, a_{i+1},\ ...,\ a_n). \tag{6}$$

3. Perform a convolution of the number A into positional code.

4. Determine the true value of the distorted residual:

$$a_i = A - [A/m_i]m_i, \tag{7}$$

where $[x]$ is the whole part x, not exceeding x. Corrected number $A_{cor} = (a_1,\ a_2,\ ...,\ a_i,\ ...,\ a_n)$.

Let us determine the conditions under which it is possible to exclude some bases from the SRC. To do this, we present the bases of the original SRC in the canonical form:

$$\begin{aligned} m_1 &= \beta_{11}^{a_{11}} \beta_{12}^{a_{12}} \ldots \beta_{1l_1}^{a_{1l_1}} \\ m_2 &= \beta_{21}^{a_{21}} \beta_{22}^{a_{22}} \ldots \beta_{2l_2}^{a_{2l_2}} \\ &\ldots \\ m_n &= \beta_{n1}^{a_{n1}} \beta_{n2}^{a_{n2}} \ldots \beta_{nl_n}^{a_{nl_n}} \\ M &= \beta_1^{a_1} \beta_2^{a_2} \ldots \beta_k^{a_k} \end{aligned} \tag{8}$$

To uniquely determine the number A, specified in the SRC with bases $m_1,\ m_2,\ ..., m_n$, and lying in the range $[0, M)$ it is possible to exclude only those bases for which $\beta_m = \beta_{il_i}$, $(m = \overline{1,\ k}, i = \overline{1,\ n})$. It is necessary that $a_m \geq a_{il_i}$.

Thus, the necessary and sufficient conditions for error correction are determined by eliminating the distorted base. These conditions are simultaneous fulfillment of equality and inequality:

$$\beta_m = \beta_{i\,l_i},\ a_m \geq a_{i\,l_i}. \tag{9}$$

Above, the algorithm for detecting and correcting errors in the SRC by means of L-codes was described. Let be $(a_k - a_{k+1})$ mod d_{kk+1} when calculating values, it is determined that $a_{i-1\,i} \neq 0$, $a_{i\ \ i+1} \neq 0$, and all other values are:

$$a_{k\,k+1} = (a_k - a_{k+1}) \bmod d_{k\,k+1} = 0. \tag{10}$$

Then it is stated that the number A is incorrect, and the error is present in the remainder of the base m_i, i.e.

$$\widetilde{A} = (a_1,\ a_2,\ \ldots, \widetilde{a_i},\ \ldots,\ a_n). \tag{11}$$

Referring by the values $a_{i-1\ \ i}$ and $a_{i\ \ i+1}$ to the block of error constants, we determine the error value Δa_i and then we determine the true value of the residual:

$$a_{i\ cor} = \widetilde{a_i} - \Delta a_i. \tag{12}$$

The corrected number will appear as:

$$A_{cor} = (a_1,\ a_2,\ \ldots, a_{i\ cor},\ \ldots,\ a_n). \tag{13}$$

To correct an error with the help of the developed correction method, it is necessary that the error Δa_i is not at the same time divisible by two dividers $d_{i-1\ \ i}$ and $d_{i\ \ i+1}$, which limits the class of corrected errors [24].

Thus, there is a need to develop effective methods and algorithms to expand the class of possible correctable errors.

The method of correction of one-time errors, allowing to correct errors that are multiples of one of the dividers $d_{i-1\ \ i}$ or $d_{i\ \ i+1}$, is as follows [22].

Let a SRC be set with mutually not simple bases, i.e. greatest common divider (GCD) $(m_1,\ m_2,\ \ldots, m_n) \geq 2$.

And let a number be given in the SRC $A_{cor} = (a_1,\ a_2,\ \ldots,\ a_n)$.

We define all values $a_{k\ k+1}$, i.e. $a_{12},\ a_{23},\ a_{34},\ \ldots,\ a_{n-1\ \ n},\ a_{n\ \ 1}$. Without breaking the generality of reasoning, we assume that $a_{i\ \ i+1} \neq 0$, and all other values are $a_{k\ \ k+1} \neq 0$. Because:

$$a_{i\ \ i+1} = (a_i - a_{i+1}) \bmod d_{i\ \ i+1} \neq 0. \tag{14}$$

error may be present only in residues on the bases m_i or m_{i+1}. In this regard, two hypotheses are possible:

- an error is present in the residual a_i;
- an error is present in the residual a_{i+1}.

Before we consider the error correction process by the proposed method, we formulate and prove a theorem, the result of which we use in determining the convergence process for the totality of numbers of the form:

$$A^{(k_i)} = (a_1,\ ...,\ a_{i-1},\ a_{i\,k_i},\ a_{i+1}, ...,\ a_n), \tag{15}$$

to the correct number:

$$A^{(\rho)} = (a_1,\ ...,\ a_{i-1},\ a_{i\,\rho},\ a_{i+1}, ...,\ a_n). \tag{16}$$

First consider the lemma.

Lemma. The sum, difference, and product of any L-code code words are also code words.

Theorem 2. Let in the ordered ($m_{i-1} < m_i;\ i = \overline{1,\ n}$) system of residual classes with bases $m_1,\ m_2,\ ..., m_n$ an incorrect (distorted in one residue) number be given $\widetilde{A} = (a_1,\ a_2,\ ...,\ a_{i-1},\ \widetilde{a_i},\ a_{i+1}, ...,\ a_n)$ and let $\Delta a_i = \widetilde{a_i} - a_i = k_i d_{i-1\,i}$.

Then in the set of values $a_{ik_i} = (\widetilde{a_i} - k_i d_{i-1\,i}) \bmod m_i$ there is a single value of $a_{i\rho}$, at which the number:

$$A^{(\rho)} = (a_1,\ a_2,\ a_{i\,\rho},\ ...,\ a_n), \tag{17}$$

is the correct number, where $d_{i-1\,i}(m_{i-1},\ \ m_i)$, and k_i may take values $k_i = 1,\ 2, ...,\ m_i/d_{i-1\,i} - 1$.

Proof. We show that there is such a value of $a_{i\rho_1}$, at which the number $A = (a_1,\ a_2,\ ...,\ a_{i\,\rho},\ ...,\ a_n)$ is the correct number. By the condition of the theorem, the error Δa_i is a multiple of the divisor $d_{i-1\,i}$. The expression $k_i d_{i-1\,i}$ contains all possible multiples of $d_{i-1\,i}$.

Thus, there will be at least one value of $k_i = \rho_1$, at which:

$$\Delta a_{i\rho_1} = \rho_1 d_{i-1\,i}, \tag{18}$$

and

$$a_{1\rho_1} = \widetilde{a_i} - \Delta a_{i\rho_1}. \tag{19}$$

We show that $A^{(\rho_1)}$ is the only correct number from the set of numbers of the form $A^{(k_i)}$.

Suppose there is such a value:

$$a_{1\rho_2} = \widetilde{a_i} - \rho_2 d_{i-1\,i}, \tag{20}$$

at which the number $A^{(\rho_2)}$ is also correct. Then, in accordance with lemma, the number:

$$A^{(\rho_1)} - A^{(\rho_2)} = (0, \ldots, a_{i\ \rho_1} - a_{i\ \rho_2},\ \ldots,\ 0), \tag{21}$$

is correct. If the number $A^{(\rho_1)} - A^{(\rho_2)}$ is correct, then in accordance with lemma we have:

$$\begin{array}{c} (\rho_2 - \rho_1)d_{i-1\ i} \equiv 0(\mathrm{mod} d_{1-i}) \\ (\rho_2 - \rho_1)d_{i-1\ i} \equiv 0(\mathrm{mod} d_{2-i}) \\ \ldots \\ (\rho_2 - \rho_1)d_{i-1\ i} \equiv 0(\mathrm{mod} d_{n-i}) \end{array} \tag{22}$$

If $i \neq n$, then the only correct number $A^{(\rho_1)} - A^{(\rho_2)}$ is the zero code word. This is due to the fact that $d_{i-1\ i} \neq 0$ and $d_{i-1\ i}$ is not equal to the GCD of the dividers $d_{1i},\ d_{2i},\ \ldots,\ d_{ni}$.

Moreover, inequality $d_{i-1\ i} \neq [d_{1i},\ d_{2i},\ \ldots,\ d_{ni}]$ contradicts the condition of arbitrary choice of bases $m_1,\ m_2,\ \ldots, m_n$. Therefore, the following equality holds $A^{(\rho_1)} - A^{(\rho_2)} = (0,\ 0, \ldots, 0,\ \ldots,\ 0)$.

Thus, $\rho_1 = \rho_2$, that confirms the uniqueness of existence ρ_1, at which:

$$A^{(\rho_1)} = (a_1,\ a_2,\ \ldots,\ a_{i\,\rho_1},\ \ldots,\ a_n), \tag{23}$$

is correct. Q.E.D.

Thus, the developed method of error correction in the SRC allows to extend the class of corrected errors. This greatly expands the corrective possibilities of the *L*-codes in the class of deductions.

Consider the operation of the device for detecting errors using L-codes, in accordance with the above algorithm. This device contains the input register, modulo adders m_i and d_{1i} $(i = \overline{2,\ n})$ and $(n - 1)$—the input element OR (see Fig. 2).

The algorithm of operation of this device corresponds to the error detection algorithm developed above [25].

As can be seen from the considered materials of the performance of the error correction operation, using the L-codes, the error detection process is implemented extremely simply.

The time of error detection for the SRC given by any system of bases is always equal to three conditional time ticks and does not depend (as is observed for *R*-codes) on the number n of information bases [26].

The above-discussed variants of devices for detecting errors in the SRC make it possible to guarantee the detection of a number A, distortion, however, this does not determine the number of the base on which the residue was distorted [22].

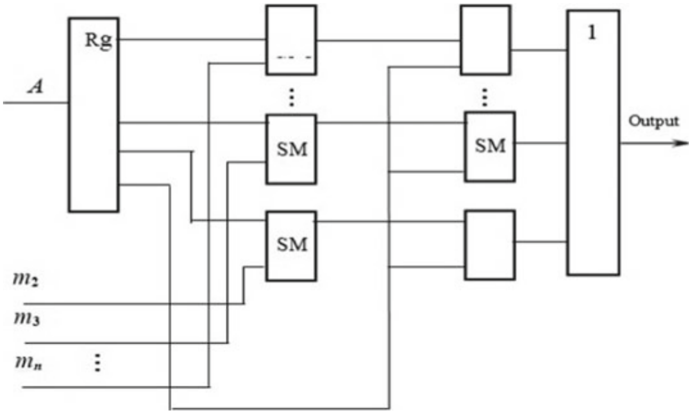

Fig. 2 Device for detecting errors

4 Conclusion

The need to eliminate threats and destructive factors of progressive information and technological development of the national economy became the basis for substantiation of conceptual and practical provisions for the formation of a secure information environment. It is proved that strengthening the information security of the business entity should be based on ensuring the reliability, confidentiality, integrity of information. It is established that modern methods and means of information and communication and digital technologies cannot entirely provide full protection and reliable processing of ever-growing arrays of information. Therefore, the basis for ensuring the information security of enterprises is determined by improvement of methods of errors diagnosis and correction in the system of residual classes.

Thus, the error correction algorithms in the SRC with mutual in pairs non-simple bases make it relatively easy to implement a procedure for detecting and correcting one-time errors [27]. The considered scheme of detecting and correcting one-time errors makes it possible to localize the erroneous base and correct the error in one residual in just five conventional time ticks for any number of the SRC bases. The main advantages of the *L*-codes in the SRC is the simplicity of the procedure for detecting the location of an error and its localization. By the simplicity of decoding schemes, the *L*-codes have no analogues, both in the PNS and in the SRC.

References

1. Antonyuk V Mechanisms of state response to modern challenges and threats to information security. http://www.dy.nayka.com.ua/?op=1&z=747
2. Baranov O (2014) On the interpretation and definition of "cybersecurity." Inf Law 2(42):54–62

3. Lipkan V (2011) Modern content of information operations against Ukraine. Curr issues Int Relat 102(1):34–43 (2011). http://nbuv.gov.ua/UJRN/apmv_2011_102%281%29__7
4. Lytvynenko O (2017) Information component in the modern hybrid war against Ukraine: challenges and threats. Ukrainian Stud Almanac 19:171–174
5. Glushko A, Marchyshynets O (2018) Institutional provision of the state regulatory policy in Ukraine. J Adv Res Law Econ 9(3):941–948 (2018). ASERS Publishing House. https://doi.org/10.14505/jarle.v93(33).18.
6. Onyshchenko SV, Matkovskyi AV, Puhach AA (2014) Analysis of threats to economic security of Ukraine in conditions of innovative economic development. Econ Ann XXI 1–2(2):8–11
7. Svystun L, Glushko A, Shtepenko K (2018) Organizational aspects of investment and construction projects implementation at the real estate market in Ukraine. Int J Eng Technol 7(3.2):447–452. https://doi.org/10.14419/ijet.v7i3.2.14569
8. Kozachenko H, Onyshchenko S, Masliy O (2018) Region building complex social and economic security threats. Int J Eng Technol 7(3.2):79–85. https://doi.org/10.14419/ijet.v7i3.2.14405
9. Kavun SV, Pylypenko AA, Ripka DO (2013) Economic and information security of enterprises in the system of consolidated information: a textbook. Kharkiv: View. KhNEU, 364 p
10. Onyshchenko S, Hlushko A (2020) Conceptual principles of information security of the national economy in terms of digitalization. Soc Econ KhNU 59:14–24
11. Zhivko Z, Zhivko M, Ortynsky V, Kernytsky I (2009) Economic security of enterprises, organizations and institutions. Alerta, 544 p
12. Economic impact of cybercrime – no slowing down. Report of the Center for Strategic and International Studies (CSIS), 2018. Homepage https://www.csis.org/analysis/economic-impact-cybercrime
13. The analysis of regulatory impact of draft regulations of the Cabinet of Ministers of Ukraine "On amendments to the Rules of protection of information in information, telecommunication and information-telecommunication systems". State service of special communication and information protection of Ukraine. Homepage http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288142&cat_id=38837&ctime=1522850564776
14. Bilenchuk P, Malyi M (2019) Cybersworld in the new millennium. Who are they: cybercriminals, cybercriminals, cyberterrorists? Legal Bull Ukraine 39:14–15
15. Official site the International Organization for Standardization. Homepage https://www.iso.org/home.html
16. 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. Int J Manage (IJM). 11(12), 1709–1726 (2020). Homepage https://iaeme.com/MasterAdmin/Journal_uploads/IJM/VOLUME_11_ISSUE_12/IJM_11_12_157.pdf. https://doi.org/10.34218/IJM.11.12.2020.157
17. Akushsky IY, Yuditsky DI (1968) Machine arithmetic in residual classes. Moscow: Sov. Radio, 440 p (in Russian)
18. Torgashov VA (1973) System of residual classes and the reliability of a computer. M.: Sov. Radio, 118 p (in Russian)
19. Krasnobayev V, Yanko A, Koshman S (2017) Algorithms of data processing in the residual classes system. In: 4th international scientific-practical conference problems of infocommunications, science and technology (PIC S&T), Kharkov, pp 117–121
20. Krasnobayev VA, Yanko AS, Koshman SA (2016) A Method for arithmetic comparison of data represented in a residue number system. Cybern Syst Anal 52(1):145–150
21. Hariri A, Navi K, Rastegar R (2005) A simplified modulo $(2n-1)$ squaring scheme for residue number system. In: EUROCON 2005: the international conference on "computer as a tool", Belgrade, 2005, pp 615–618. https://doi.org/10.1109/EURCON.2005.1630004
22. Krasnobayev A, Kuznetsov A, Yanko A, Koshman S, Zamula A, Kuznetsova T (2019). Data processing in the system of residual classes. Monograph. ASC Academic Publishing, 208 p. ISBN 978-0-9989826-6-3 (Hardback). ISBN 978-0-9989826-7-0 (Ebook)

23. Krasnobayev V, Kuznetsov A, Kononchenko A, Kuznetsova T (2019) Method of data control in the residue classes. In Proceedings of the 2nd international workshop on computer modeling and intelligent systems, CMIS-2019, Zaporizhzhia, Ukraine, 15–19 April 2019, pp 241–252
24. Yatskiv V, Tsavolyk T, Yatskiv N (2017)The correcting codes formation method based on the residue number system. In: 2017 14th international conference the experience of designing and application of CAD systems in microelectronics (CADSM), Lviv, 2017, pp 237–240. https://doi.org/10.1109/CADSM.2017.7916124
25. Krasnobayev A, Kuznetsov A, Lokotkova I, Dyachenko A (2019) The method of single errors correction in the residue class. In: 2019 3rd international conference on advanced information and communications technologies (AICT), Lviv, Ukraine, 2019, pp 125–128. https://doi.org/10.1109/AIACT.2019.8847845
26. Roshanzadeh M, Saqaeeyan S (2012) Error detection & correction in wireless sensor networks by using residue number systems. Int J Comput Netw Inf Secur 4(2):29–35. https://doi.org/10.5815/ijcnis.2012.02.05
27. Krasnobayev A, Kuznetsov A, Yanko A, Kuznetsova T (2020) The analysis of the methods of data diagnostic in a residue number system. In: 2st international workshop on cyber hygiene & conflict management in global information networks, Kyiv